Tell us about your PDF experience.

Azure Stack Hub Operator

Documentation

Microsoft Azure Stack Hub is a hybrid cloud platform that lets you provide Azure

services from your datacenter. Learn how to manage Azure Stack Hub.

About Azure Stack Hub

ｅ OVERVIEW

What is Azure Stack Hub?

What is Azure Stack HCI?

ｈ WHAT'S NEW

Security updates

Release notes

Azure Stack Hub Capacity Planner

Get started

ｄ TRAINING

Use the administration portal

Offer a service to users

Test a service offering

ｐ CONCEPT

Compare connection models

Connected deployment

Disconnected deployment

Azure Stack Hub tools

ａ DOWNLOAD

Download Azure Stack Hub tools from GitHub

Install Azure Stack PowerShell

Connect with Azure Stack PowerShell

Download the Azure Stack Development Kit (ASDK)

Try Azure Stack Hub

｀ DEPLOY

Prepare the ASDK host

Install the ASDK

ASDK admin basics

Offer services

｀ DEPLOY

Create an offer for a virtual machine

Create a highly available MySQL database

Create apps for any platform

Manage Azure Stack Hub

ｃ HOW-TO GUIDE

Monitor health and alerts

Install updates and monitor progress

Back up and restore configuration and service data

Azure Stack Hub overview

Article • 07/29/2022

Azure Stack Hub is an extension of Azure that provides a way to run apps in an onpremises environment and deliver Azure services in your datacenter. With a consistent

cloud platform, organizations can confidently make technology decisions based on

business requirements, rather than business decisions based on technology limitations.

Azure provides a rich platform for developers to build modern apps. However, some

cloud-based apps face obstacles like latency, intermittent connectivity, and regulations.

Azure and Azure Stack Hub unlock new hybrid cloud use cases for both customer-facing

and internal line-of-business apps:

Edge and disconnected solutions. Address latency and connectivity requirements

by processing data locally in Azure Stack Hub and then aggregating it in Azure for

further analytics, with common app logic across both. You can even deploy Azure

Stack Hub disconnected from the internet without connectivity to Azure. Think of

factory floors, cruise ships, and mine shafts as examples.

Cloud apps that meet varied regulations. Develop and deploy apps in Azure with

full flexibility to deploy on-premises with Azure Stack Hub to meet regulatory or

policy requirements. No code changes are needed. App examples include global

audit, financial reporting, foreign exchange trading, online gaming, and expense

reporting.

Cloud app model on-premises. Use Azure services, containers, serverless, and

microservice architectures to update and extend existing apps or build new ones.

Use consistent DevOps processes across Azure in the cloud and Azure Stack Hub

on-premises to speed up app modernization for core mission-critical apps.

For information on comparing Azure Stack Hub with other Azure offerings, see

Differences between global Azure, Azure Stack Hub, and Azure Stack HCI.

If the customer deploys Azure Stack Hub disconnected from global Azure and from the

internet, no data that is stored on the appliance is sent to Microsoft. Azure Stack Hub is

an on-premises appliance. Customers fully own and control the appliance, access to the

appliance, and any data stored on the appliance. Disconnected deployment allows for

Why use Azure Stack Hub?

Data residency

complete control over data location by the customer. A customer can alternatively elect

to connect an Azure Stack Hub appliance to global Azure or to the Internet in a hybrid

workload scenario (for example, a solution that uses resources deployed on Azure Stack

Hub and public Azure with data transmitting between both) or with hybrid cloud

management (for example, connecting a virtual machine deployed on Azure Stack Hub

to Azure Monitor in public Azure for monitoring.) In such scenarios, the customer is

responsible for validating whether the Azure or other online services used with the

appliance satisfy any data residency concerns. For more information about data

residency, please see Data residency in Azure .

Azure Stack Hub integrated systems are comprised in racks of 4-16 servers built by

trusted hardware partners and delivered straight to your datacenter. After delivery, a

solution provider will work with you to deploy the integrated system and ensure the

Azure Stack Hub solution meets your business requirements. You can prepare your

datacenter by ensuring all required power and cooling, border connectivity, and other

required datacenter integration requirements are in place.

For more information about the Azure Stack Hub datacenter integration experience,

see Azure Stack Hub datacenter integration.

Azure Stack Hub is built on industry standard hardware and is managed using the same

tools you already use for managing Azure subscriptions. As a result, you can apply

consistent DevOps processes whether you're connected to Azure or not.

The Azure Stack Hub architecture lets you provide Azure services at the edge for remote

locations or intermittent connectivity, disconnected from the internet. You can create

hybrid solutions that process data locally in Azure Stack Hub and then aggregate it in

Azure for additional processing and analytics. Finally, because Azure Stack Hub is

installed on-premises, you can meet specific regulatory or policy requirements with the

flexibility of deploying cloud apps on-premises without changing any code.

Azure Stack Hub integrated systems are offered through a partnership of Microsoft and

hardware partners, creating a solution that offers cloud-paced innovation and

computing management simplicity. Because Azure Stack Hub is offered as an integrated

hardware and software system, you have the flexibility and control you need, along with

the ability to innovate from the cloud.

Azure Stack Hub architecture

Deployment options

An Azure Stack Hub integrated system can range in size from 4-16 servers, called a scale

unit. Integrated systems are jointly supported by the hardware partner and Microsoft.

The following diagram shows an example of a scale unit.

.

Connection models

You can choose to deploy Azure Stack Hub either connected to the internet (and to

Azure) or disconnected from it.

For more information, see the considerations for connected and disconnected

deployment models.

Azure Stack Hub uses either Azure Active Directory (Azure AD) or Active Directory

Federation Services (AD FS). Azure AD is Microsoft's cloud-based, multi-tenant identity

provider. Most hybrid scenarios with internet-connected deployments use Azure AD as

the identity store.

For disconnected deployments of Azure Stack Hub, you need to use AD FS. Azure Stack

Hub resource providers and other apps work similarly with AD FS or Azure AD. Azure

Stack Hub includes its own Active Directory instance and an Active Directory Graph API.

Azure Stack Hub uses the same operations model as Azure. An Azure Stack Hub

operator can deliver a variety of services and apps to tenant users, similar to how

Microsoft delivers Azure services to tenant users.

You can manage Azure Stack Hub with the administrator portal, user portal, or

PowerShell. The Azure Stack Hub portals are each backed by separate instances of Azure

Resource Manager. An Azure Stack Hub Operator uses the administrator portal to

Identity provider

How is Azure Stack Hub managed?

manage Azure Stack Hub, and to do things like create tenant offerings and maintain the

health and monitor status of the integrated system. The user portal provides a selfservice experience for consumption of cloud resources like virtual machines (VMs),

storage accounts, and web apps.

For more information about managing Azure Stack Hub using the administrator

portal, see the use the Azure Stack Hub administration portal quickstart.

As an Azure Stack Hub operator, you can deliver VMs, web apps, highly available SQL

Server, and MySQL Server databases.

An operator can manage Azure Stack Hub with the administrator portal or PowerShell.

You can configure Azure Stack Hub to deliver services to tenants using plans, quotas,

offers, and subscriptions. Tenant users can subscribe to multiple offers. Offers can have

one or more plans, and plans can have one or more services. Operators also manage

capacity and respond to alerts.

Users consume services that the operator offers. Users can provision, monitor, and

manage services that they've subscribed to, like web apps, storage, and VMs. Users can

manage Azure Stack Hub with the user portal or PowerShell.

To learn more about managing Azure Stack Hub, including what accounts to use

where, typical operator responsibilities, what to tell your users, and how to get help,

review Azure Stack Hub administration basics.

Resource providers are web services that form the foundation for all Azure Stack Hub

IaaS and PaaS services. Azure Resource Manager relies on different resource providers to

provide access to services. Each resource provider helps you configure and control its

respective resources. Service admins can also add new custom resource providers.

There are three foundational IaaS resource providers:

Compute: The Compute Resource Provider lets Azure Stack Hub tenants to create

their own VMs. The Compute Resource Provider includes the ability to create VMs

as well as VM extensions. The VM extension service helps provide IaaS capabilities

for Windows and Linux VMs. As an example, you can use the Compute Resource

Resource providers

Foundational resource providers

Provider to provision a Linux VM and run Bash scripts during deployment to

configure the VM.

Network Resource Provider: The Network Resource Provider delivers a series of

Software Defined Networking (SDN) and Network Function Virtualization (NFV)

features for the private cloud. You can use the Network Resource Provider to

create resources like software load balancers, public IPs, network security groups,

and virtual networks.

Storage Resource Provider: The Storage Resource Provider delivers four Azureconsistent storage services: blob, queue, table, and Key Vault account management

providing management and auditing of secrets, such as passwords and certificates.

The storage resource provider also offers a storage cloud administration service to

facilitate service provider administration of Azure-consistent storage services.

Azure Storage provides the flexibility to store and retrieve large amounts of

unstructured data, like documents and media files with Azure Blobs, and structured

NoSQL based data with Azure Tables.

There are three optional PaaS resource providers that you can deploy and use with

Azure Stack Hub:

App Service: Azure App Service on Azure Stack Hub is a PaaS offering of Microsoft

Azure available to Azure Stack Hub. The service enables your internal or external

customers to create web, API, and Azure Functions apps for any platform or device.

SQL Server: Use the SQL Server resource provider to offer SQL databases as a

service of Azure Stack Hub. After you install the resource provider and connect it to

one or more SQL Server instances, you and your users can create databases for

cloud-native apps, websites that use SQL, and other workloads that use SQL.

MySQL Server: Use the MySQL Server resource provider to expose MySQL

databases as an Azure Stack Hub service. The MySQL resource provider runs as a

service on a Windows Server 2019 Server Core VM.

Differences between global Azure, Azure Stack Hub, and Azure Stack HCI

Administration basics

Quickstart: use the Azure Stack Hub administration portal

Understand usage and billing.

Optional resource providers

Next steps

Differences between global Azure,

Azure Stack Hub, and Azure Stack HCI

Article • 10/24/2022

Microsoft provides Azure and the Azure Stack Hub family of services in one Azure

ecosystem. Use the same application model, self-service portals, and APIs with Azure

Resource Manager to deliver cloud-based capabilities whether your business uses global

Azure or on-premises resources.

This article describes the differences between global Azure, Azure Stack Hub, and Azure

Stack HCI capabilities. It provides common scenario recommendations to help you make

the best choice for delivering Microsoft cloud-based services for your organization.

Microsoft Azure is an ever-expanding set of cloud services to help your organization

meet your business challenges. It's the freedom to build, manage, and deploy apps on a

massive, global network using your favorite tools and frameworks.

Global Azure offers more than 100 services available in 54 regions around the globe. For

the most current list of global Azure services, see the Products available by region . The

services available in Azure are listed by category and also by whether they're generally

available or available through preview.

For more information about global Azure services, see Get started with Azure.

Global Azure

Azure Stack Hub is an extension of Azure that brings the agility and innovation of cloud

computing to your on-premises environment. Deployed on-premises, Azure Stack Hub

can be used to provide Azure consistent services either connected to the internet (and

Azure) or in disconnected environments with no internet connectivity. Azure Stack Hub

uses the same underlying technologies as global Azure, which includes the core

components of Infrastructure-as-a-Service (IaaS), Software-as-a-Service (SaaS), and

optional Platform-as-a-Service (PaaS) capabilities. These capabilities include:

Azure VMs for Windows and Linux

Azure Web Apps and Functions

Azure Key Vault

Azure Resource Manager

Azure Marketplace

Containers

Admin tools (Plans, offers, RBAC, and so on)

The PaaS capabilities of Azure Stack Hub are optional because Azure Stack Hub isn't

operated by Microsoft--it's operated by our customers. This means you can offer

whatever PaaS service you want to end users if you're prepared to abstract the

underlying infrastructure and processes away from the end user. However, Azure Stack

Hub does include several optional PaaS service providers including App Service, SQL

databases, and MySQL databases. These are delivered as resource providers so they're

multi-tenant ready, updated over time with standard Azure Stack Hub updates, visible in

the Azure Stack Hub portal, and well integrated with Azure Stack Hub.

In addition to the resource providers described above, there are additional PaaS services

available and tested as Azure Resource Manager template-based solutions that run in

IaaS. As an Azure Stack Hub operator, you can offer them as PaaS services to your users

including:

Service Fabric

Kubernetes Container Service

Ethereum Blockchain

Cloud Foundry

Financial modeling

Clinical and claims data

IoT device analytics

Azure Stack Hub

Example use cases for Azure Stack Hub

Retail assortment optimization

Supply-chain optimization

Industrial IoT

Predictive maintenance

Smart city

Citizen engagement

Learn more about Azure Stack Hub at What is Azure Stack Hub.

Azure Stack HCI is a hyperconverged cluster that uses validated hardware to run

virtualized Windows and Linux workloads on-premises and easily connect to Azure for

cloud-based backup, recovery, and monitoring. Initially based on Windows Server 2019,

Azure Stack HCI is now delivered as an Azure service with a subscription-based licensing

model and hybrid capabilities built-in. Although Azure Stack HCI is based on the same

core operating system components as Windows Server, it's an entirely new product line

focused on being the best virtualization host.

Azure Stack HCI uses Microsoft-validated hardware from an OEM partner to ensure

optimal performance and reliability. The solutions include support for technologies such

as NVMe drives, persistent memory, and remote-direct memory access (RDMA)

networking.

Remote or branch office systems

Datacenter consolidation

Virtual desktop infrastructure

Business-critical infrastructure

Lower-cost storage

High availability and disaster recovery in the cloud

Virtualizing enterprise apps like SQL Server

Run containers with Azure Kubernetes Service (AKS) on Azure Stack HCI

Run Azure Arc enabled services such as Azure data services, which includes SQL

Managed Instance and PostgreSQL Hyperscale, and Azure enabled application

services (preview), which includes App Service, Functions, Logic Apps, API

Management, and Event Grid.

Visit the Azure Stack HCI website to view 70+ Azure Stack HCI solutions currently

available from Microsoft partners.

Azure Stack HCI

Example use cases for Azure Stack HCI

Azure Stack Hub administration basics

Quickstart: use the Azure Stack Hub administration portal

Next steps

Azure Stack Hub security updates

Article • 09/14/2023

This article lists all the security updates in the last three updates of Azure Stack Hub. This

information is provided for reference purposes only.

Review update activity checklist

Review list of known issues

Next steps

Azure Stack Hub release notes

Article • 09/14/2023

This article describes the contents of Azure Stack Hub update packages. The update

includes improvements and fixes for the latest release of Azure Stack Hub.

To access release notes for a different version, use the version selector dropdown above

the table of contents on the left.

Before applying the update, make sure to review the following information:

Checklist of activities before and after applying the update

Known issues

Hotfixes

Security updates

For help with troubleshooting updates and the update process, see Troubleshoot patch

and update issues for Azure Stack Hub.

You can download the Azure Stack Hub update package using the Azure Stack Hub

update downloader tool .

） Important

If your Azure Stack Hub instance is behind by more than two updates, it's

considered out of compliance. You must update to at least the minimum

supported version to receive support.

） Important

If your Azure Stack Hub instance does not have an active support contract with the

hardware partner, it's considered out of compliance. You must have an active

support contract for the hardware to receive support.

Update planning

Download the update

You can access older versions of Azure Stack Hub release notes in the table of contents

on the left side, under Resources > Release notes archive. Select the desired archived

version from the version selector dropdown in the upper left. These archived articles are

provided for reference purposes only and do not imply support for these versions. For

information about Azure Stack Hub support, see Azure Stack Hub servicing policy. For

further assistance, contact Microsoft Customer Support Services.

2102 archived release notes

Azure Stack Hub hotfix 1.2206.2.76

Article • 09/21/2023

Removed health HTTP metrics from being sent to table server.

Improved Network Controller stability.

Fixed bugs in SDN routing by ordering UDRs for better route resolution.

SRP and DiskRP now include resource tags for billing.

Fixed usage registration for DRP-deployed services.

Added PEP cmdlets to enable and disable root hint query when using DNS

forwarder.

Fixed an issue in which the removal of GPU VMs did not update the subscription's

GPU resource consumption, causing the GPU quota enforcement to fail on

subsequent GPU VM deployments. In other words, if a subscription's compute

quota limit for GPUs was N, removing a GPU VM without the fix did not cause the

usage to go down by one unit, eventually causing the deployments to fail when

the limit was reached, even though there were less than N GPU VMs.

Decreased maximum length of Graph ApplicationName parameter in the

PowerShell API to match the maximum length of a Graph application name.

Authorization changes to Health Agent.

Improved stability of SDN components.

Improved the PnP device attached alert and moved it back to Preview.

Fixed an issue that could cause excessive disk space usage on infra VMs and hosts.

Fixed an issue in which scaling a VMSS in and out would eventually fill a subnet's IP

address space.

Removed IIS default website to prevent server IP address leak vulnerability.

Fixed an issue that was blocking the update from 2108 to the 2206 build due to

MetadataServer being unhealthy.

Fixed an issue that could lead to a BlobSasManager service crash during VM

deletion.

Improvements to support tools.

Fixed an issue in the Virtual Machine Scale Set portal creation experience that

caused the addition of an existing load balancer to fail.

Removed unsupported Reapply feature in the virtual machine portal experience.

Summary

Fixes rolled up from previous hotfix releases

Fixed an issue in which the infrastructure backup information displayed on the

portal is not consistent with the alert.

Improved blob metadata backup stability by skipping unnecessary dependency.

Optimized reading of disk IOPS values to support VMs with a large number of data

disks.

CRP will self-heal a VM with a SCSI disk that failed to attach instead of requiring

operator removal of the disk from the VM.

Added support for Azure Stack Hub root certificate rotation.

Fixed an issue that prevented guest operating system activation of Windows Server

2022.

Fixed a null reference issue when calling the Compute Resource Provider API to

power off a virtual machine without doing a shutdown.

Fixed stability bugs in Azure Kubernetes Service, reliability issues in usage

reporting, and Azure Stack update operations based on availability fixes for an

internal settings service.

Updated AMD GPU driver VM extension with new default driver path.

Fixed an issue preventing health remediation of the Compute Host Agent service.

To apply this hotfix, you must have version 1.2206.0.6 or later.

Download the following files. Then, follow the instructions on the Apply updates in

Azure Stack page on the Microsoft Docs website to apply this update to Azure Stack.

Download the zip file now .

Download the hotfix xml file now .

Hotfix information

） Important

As outlined in the release notes for the 2206 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

More information

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

Azure Stack Hub hotfix 1.2301.2.63

Article • 09/20/2023

Upgraded portal to version 9.393.0.

Fixed a persistent portal cache issue that impacted portal loading.

Removed unused health metrics from table server.

Improved Network Controller stability.

Bug fixes in SDN routing by ordering UDRs for better route resolution.

PMC now returns the correct count for CPU cores on the physical host

SRP and DiskRP include resource tags for billing.

CRP now returns an error when creating a VM with invalid Chinese characters.

CRP automatically extends VM guest agent encryption certificates 90 days before

expiry.

Fixed Set-ServiceAdminUpn PEP cmdlet.

Azure Resource Manager ETW events redundancy fix.

Authorization changes to health agent.

To apply this hotfix, you must have version 1.2301.2.58 or later.

Download the following files. Then, follow the instructions on the Apply updates in

Azure Stack page on the Microsoft Docs website to apply this update to Azure Stack.

Summary

Fixes rolled up from previous hotfix releases

Hotfix information

） Important

As outlined in the release notes for the 2301 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

Download the zip file now .

Download the hotfix xml file now .

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

More information

Azure Stack Hub hotfix 1.2301.2.60

Article • 07/26/2023

Improved Network Controller stability.

Bug fixes in SDN routing by ordering UDRs for better route resolution.

PMC now returns the correct count for CPU cores on the physical host

SRP and DiskRP include resource tags for billing.

CRP now returns an error when creating a VM with invalid Chinese characters.

CRP automatically extends VM guest agent encryption certificates 90 days before

expiry.

To apply this hotfix, you must have version 1.2301.2.58 or later.

Download the following files. Then, follow the instructions on the Apply updates in

Azure Stack page on the Microsoft Docs website to apply this update to Azure Stack.

Download the zip file now .

Download the hotfix xml file now .

Azure Stack Hub update resources

Apply updates in Azure Stack

Summary

Hotfix information

） Important

As outlined in the release notes for the 2301 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

More information

Monitor updates in Azure Stack by using the privileged endpoint

Azure Stack Hub hotfix 1.2206.2.66

Article • 04/17/2023

Added PEP cmdlets to enable and disable root hint query when using DNS

forwarder.

Fixed an issue in which the removal of GPU VMs did not update the subscription's

GPU resource consumption, causing the GPU quota enforcement to fail on

subsequent GPU VM deployments. In other words, if a subscription's compute

quota limit for GPUs was N, removing a GPU VM without the fix did not cause the

usage to go down by one unit, eventually causing the deployments to fail when

the limit was reached, even though there were less than N GPU VMs.

Decreased maximum length of Graph ApplicationName parameter in the

PowerShell API to match the maximum length of a Graph application name.

Authorization changes to Health Agent.

Improved stability of SDN components.

Improved the PnP device attached alert and moved it back to Preview.

Fixed an issue that could cause excessive disk space usage on infra VMs and hosts.

Fixed an issue in which scaling a VMSS in and out would eventually fill a subnet's IP

address space.

Removed IIS default website to prevent server IP address leak vulnerability.

Fixed an issue that was blocking the update from 2108 to the 2206 build due to

MetadataServer being unhealthy.

Fixed an issue that could lead to a BlobSasManager service crash during VM

deletion.

Improvements to support tools.

Fixed an issue in the Virtual Machine Scale Set portal creation experience that

caused the addition of an existing load balancer to fail.

Removed unsupported Reapply feature in the virtual machine portal experience.

Fixed an issue in which the infrastructure backup information displayed on the

portal is not consistent with the alert.

Improved blob metadata backup stability by skipping unnecessary dependency.

Optimized reading of disk IOPS values to support VMs with a large number of data

disks.

Summary

Fixes rolled up from previous hotfix releases

CRP will self-heal a VM with a SCSI disk that failed to attach instead of requiring

operator removal of the disk from the VM.

Added support for Azure Stack Hub root certificate rotation.

Fixed an issue that prevented guest operating system activation of Windows Server

2022.

Fixed a null reference issue when calling the Compute Resource Provider API to

power off a virtual machine without doing a shutdown.

Fixed stability bugs in Azure Kubernetes Service, reliability issues in usage

reporting, and Azure Stack update operations based on availability fixes for an

internal settings service.

Updated AMD GPU driver VM extension with new default driver path.

Fixed an issue preventing health remediation of the Compute Host Agent service.

To apply this hotfix, you must have version 1.2206.0.6 or later.

Download the following files. Then, follow the instructions on the Apply updates in

Azure Stack page on the Microsoft Docs website to apply this update to Azure Stack.

Download the zip file now .

Download the hotfix xml file now .

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

Hotfix information

） Important

As outlined in the release notes for the 2206 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

More information

Azure Stack Hub hotfix 1.2108.2.130

Article • 01/04/2023

Improved the exception handling in Cluster Manager to avoid falsely reporting

memory exhaustion alerts.

Added labels for on-demand log collection when "infrastructure service

unavailable" alert is generated.

Improvements to support tools.

Fixed a bug in storage table re-encryption that was causing secret rotation to fail.

Fixed an issue in which the BlobSasManager service might crash during VM

deletion.

Support for the .default scope has been added to AD FS. Now the client libraries

supporting the OAUTH 2.0 flow can be used against AD FS environments.

Improved stability of SDN components.

Improved the PnP device attached alert and moved it back to preview.

Introduced health probe for SecretService to improve service resilience and

availability.

Fixed an issue in which scaling a VMSS in and out would eventually fill a subnet's IP

address space.

Optimized reading of disk IOPS values to support VMs with a large number of data

disks.

CRP now self-heals a VM with a SCSI disk that failed to attach, instead of requiring

operator removal of the disk from the VM.

Removed IIS default website to prevent server IP address leak vulnerability.

Fixed an issue in the Virtual Machine Scale Set portal creation experience that

caused the addition of an existing load balancer to fail.

Removed unsupported Reapply feature in the virtual machine portal experience.

Fixed an issue in which the SRP container portal cannot display more than 1 page

of containers.

Fixed an issue with searching for a container by prefix in the SRP container portal.

Improved blob metadata backup stability by skipping unnecessary dependency.

Added support for Azure Stack Hub root certificate rotation.

Summary

Fixes rolled up from previous hotfix releases

Fixed an issue that prevented guest operating system activation of Windows Server

2022.

Fixed a null reference issue when calling the Compute Resource Provider API to

power off a virtual machine without doing a shutdown.

Fixed an issue in which some StorageController requests might time out under

high concurrency.

Removed some of the network performance counters and reduced collection

interval for other perf counters.

Cleaned up unneeded networking traces from Baremetal, NC and XRP VMs.

Fixed an issue deleting Microsoft.ContainerService/managedCluster resources

that occurred when resources managed by the AKS resource provider were

manually deleted beforehand.

Fixed a regression in which VM status is reported as UNKNOWN in the portal.

Fixed an issue that could impact updating from 2102 to 2108.

Support for new Kubernetes versions in AKS.

Fixed bugs in trace collector.

Fixed a bug related to physical disk health when repairing a node with SED drives.

Improvements to support tools.

Fixed bugs in log collection.

Fixed code defect leading to VM deployment failures.

Improved the resolution of the Network Resource Provider.

Fixed a bug in incremental disk snapshots in which a failed snapshot can block any

future snapshot operations.

Fixed a disk snapshot failure and VM IO hang when taking snapshots.

Shortened the PEP tokens and made them human-readable.

Fix to improve SLB throughput after enabling Simultaneous Multi-Threading (SMT).

Fixed an issue in which the table service partition was offline when its underlying

storage was out of space.

Added retry logic around Get-Volume calls in Test-AzureStack InfraCapacity

validation.

To apply this hotfix, you must have version 1.2108.2.65 or later.

Hotfix information

） Important

As outlined in the release notes for the 2108 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

Download the following files. Then, follow the instructions on the Apply updates in

Azure Stack page on the Microsoft Docs website to apply this update to Azure Stack.

Download the zip file now .

Download the hotfix xml file now .

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

More information

Azure Stack Hub hotfix 1.2102.31.153

Article • 01/04/2023

N/A

Improved stability of SDN components.

Improved the PnP device attached alert and moved it back to Preview.

Optimized reading of disk IOPS values to support VMs with a large number of data

disks.

CRP will self-heal a VM with a SCSI disk that failed to attach instead of requiring

operator removal of the disk from the VM.

Fixed an issue in VM power-off operation in which CRP service always ignored the

value of the non-graceful VM shutdown parameter.

Fixed an issue that prevented health remediation of the Compute Host Agent

service.

Fixed a bug in incremental disk snapshots in which a failed snapshot can block any

future snapshot operation.

Fixed a mismatched cluster name issue in FRP.

Fixed an issue that could impact updating to 2108.

Resolved an issue in which the Create a Virtual Machine image dropdown displays

image options that are not available or were not downloaded to the stamp.

Fixed an issue in which the PrivateWorkingSet queried value overflows if larger

than 4 GB.

Removed some unnecessary detailed error information on the administrator portal.

Improvements to support tools.

Resolved an issue with some Key Vault applications being in an unhealthy state

while updating from 2102 to later builds.

Add retry for get-volume requests in Test-AzureStack infra capacity check.

Shorten the "break-glass" tokens and make them human-readable.

Fixed a bug related to physical disk health when repairing a node with SED drives.

Improved Datapruner processing to minimize actor timeout alerts.

Enabled rotation of health agent SSL certificate as part of internal secret rotation.

Added graphs to Storage area that show volume performance.

Improved logic for incremental snapshot creation and deletion.

Summary

Fixes rolled up from previous hotfix releases

Improved resiliency in PEP startup script.

Fixed an issue in which System Center Operations Manager (SCOM) was unable to

close operator portal alerts.

Improved auto-remediation workflow for memory utilization.

Improved incremental snapshot creation and deletion.

Addressed an issue in the Reset-CloudAdminPassword cmdlet.

Updated Network Controller to fix bugs in PA VIP allocation and IP-MAC leaks.

Improved performance when querying for usage data.

Improved resiliency of compute admin operations.

Removed overly verbose logging from Software Load Balancer VMs.

Fixed a memory leak issue and improved memory efficiency for monitoring

services.

Fixed an issue in which the backup blade showed a "rainy" page when backup

share was inaccessible.

Fixed an issue that prevented transcript collection when closing Privileged

Endpoint (PEP) session.

Fixed a multi-tenancy website security issue.

Improved reliability of update from 2008 to 2102.

Fix for adding availability set to SQL VM in the SQL VM creation process.

Fix for setting storage size in SQL VM configuration to more than 1000 GB.

Fixed group-based authorization errors for users that require group expansion.

Newer API version support for Key Vault resource provider. The Key Vault control

plane supports the 2019-09-01 API version, and the Key Vault data plane supports

API version 7.1.

Added banner to warn users when a certificate will expire soon.

Fix to show accurate status of node in portal if a repair operation on it has failed.

ETW trace sessions are configured to use 16 MB of non-pagedpool memory. Trace

sessions now report lost event count (if any) per session, during ETL file rotation in

TraceCollector Eventlog. This releases critical non-paged pool memory for other

services on hosts and VMs. Also fixed various bugs in Tracecollector.

Fixed bugs that increased memory pressure on infrastructure.

Fixed bugs in AD FS and Azure Stack Graph to improve deployment and upgrade

reliability.

Fixed bugs in SRP and DiskRP in which performance counters were missing in the

WAC client.

Fixed a bug in resource provider (for example, Event Hubs) deployment, update, or

secret rotation. The operation previously failed with no apparent failure cause. The

fix allows the operation to complete successfully.

Fixed a bug that incorrectly raised a PnPDevice.Attached alert for a set of devices

(mouse, keyboard, etc.) that were safe.

Set memory alert to preview.

Addressed an issue with host agent monitors.

Fixed a trust relationship issue with container applications in FabricRing.

Improved RdAgent availability by removing empty RdAgent files.

Improved reliability of full update.

Extended the update readiness checks to cover more Service Fabric health and VM

health checks; for example, memory usage and storage disk capacity checks.

Updated memory configuration for VM sizes Standard\_NC16as\_T4\_v3 and

Standard\_NC64as\_T4\_v3.

Removed legacy SRP SQL instances and DB files to free up stamp resources.

Fixed a bug in which the cluster status can be stuck in "Configuring Storage" after

adding a new node.

Fixed health package registration, removing duplicate artifact creation.

Fixed a bug that sometimes caused health blades in the operator portal to become

unavailable.

Fixed a bug in which BCDR runner logs filled up MASLogs folders on physical

hosts.

Added monitoring of WMIProvider health and remediation.

Added Network Controller IMOS size check to Test-AzureStack.

Fixed a bug in SSL certificate validation during internal secret rotation.

Fixed process watchdog memory leaks.

Updated Defender platform to version 4.18.2103.7.

Enabled the alert module for customers depending on Syslog for alerts. The

services will continue to emit alerts to the Syslog pipeline.

To apply this hotfix, you must have version 1.2102.28.82 or later.

Hotfix information

） Important

As outlined in the release notes for the 2102 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

Download the following files. Then, follow the instructions on the Apply updates in

Azure Stack page on the Microsoft Docs website to apply this update to Azure Stack.

Download the zip file now .

Download the hotfix xml file now .

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

More information

Azure Stack Hub hotfix 1.2206.2.52

Article • 01/04/2023

Improved stability of SDN components.

Improved the PnP device attached alert and moved it back to Preview.

Fixed an issue that could cause excessive disk space usage on infra VMs and hosts.

Fixed an issue in which scaling a VMSS in and out would eventually fill a subnet's IP

address space.

Removed IIS default website to prevent server IP address leak vulnerability.

Fixed an issue that was blocking the update from 2108 to the 2206 build due to

MetadataServer being unhealthy.

Fixed an issue that could lead to a BlobSasManager service crash during VM

deletion.

Improvements to support tools.

Fixed an issue in the Virtual Machine Scale Set portal creation experience that

caused the addition of an existing load balancer to fail.

Removed unsupported Reapply feature in the virtual machine portal experience.

Fixed an issue in which the infrastructure backup information displayed on the

portal is not consistent with the alert.

Improved blob metadata backup stability by skipping unnecessary dependency.

Optimized reading of disk IOPS values to support VMs with a large number of data

disks.

CRP will self-heal a VM with a SCSI disk that failed to attach instead of requiring

operator removal of the disk from the VM.

Added support for Azure Stack Hub root certificate rotation.

Fixed an issue that prevented guest operating system activation of Windows Server

2022.

Fixed a null reference issue when calling the Compute Resource Provider API to

power off a virtual machine without doing a shutdown.

Fixed stability bugs in Azure Kubernetes Service, reliability issues in usage

reporting, and Azure Stack update operations based on availability fixes for an

internal settings service.

Updated AMD GPU driver VM extension with new default driver path.

Summary

Fixes rolled up from previous hotfix releases

Fixed an issue preventing health remediation of the Compute Host Agent service.

To apply this hotfix, you must have version 1.2206.0.6 or later.

Download the following files. Then, follow the instructions on the Apply updates in

Azure Stack page on the Microsoft Docs website to apply this update to Azure Stack.

Download the zip file now .

Download the hotfix xml file now .

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

Hotfix information

） Important

As outlined in the release notes for the 2206 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

More information

Azure Stack Hub hotfix 1.2108.2.127

Article • 10/18/2022

Improved stability of SDN components.

Improved the PnP device attached alert and moved it back to preview.

Introduced health probe for SecretService to improve service resilience and

availability.

Fixed an issue in which scaling a VMSS in and out would eventually fill a subnet's IP

address space.

Optimized reading of disk IOPS values to support VMs with a large number of data

disks.

CRP now self-heals a VM with a SCSI disk that failed to attach, instead of requiring

operator removal of the disk from the VM.

Removed IIS default website to prevent server IP address leak vulnerability.

Fixed an issue in the Virtual Machine Scale Set portal creation experience that

caused the addition of an existing load balancer to fail.

Removed unsupported Reapply feature in the virtual machine portal experience.

Fixed an issue in which the SRP container portal cannot display more than 1 page

of containers.

Fixed an issue with searching for a container by prefix in the SRP container portal.

Improved blob metadata backup stability by skipping unnecessary dependency.

Added support for Azure Stack Hub root certificate rotation.

Fixed an issue that prevented guest operating system activation of Windows Server

2022.

Fixed a null reference issue when calling the Compute Resource Provider API to

power off a virtual machine without doing a shutdown.

Fixed an issue in which some StorageController requests might time out under

high concurrency.

Removed some of the network performance counters and reduced collection

interval for other perf counters.

Cleaned up unneeded networking traces from Baremetal, NC and XRP VMs.

Fixed an issue deleting Microsoft.ContainerService/managedCluster resources

that occurred when resources managed by the AKS resource provider were

Summary

Fixes rolled up from previous hotfix releases

manually deleted beforehand.

Fixed a regression in which VM status is reported as UNKNOWN in the portal.

Fixed an issue that could impact updating from 2102 to 2108.

Support for new Kubernetes versions in AKS.

Fixed bugs in trace collector.

Fixed a bug related to physical disk health when repairing a node with SED drives.

Improvements to support tools.

Fixed bugs in log collection.

Fixed code defect leading to VM deployment failures.

Improved the resolution of the Network Resource Provider.

Fixed a bug in incremental disk snapshots in which a failed snapshot can block any

future snapshot operations.

Fixed a disk snapshot failure and VM IO hang when taking snapshots.

Shortened the PEP tokens and made them human-readable.

Fix to improve SLB throughput after enabling Simultaneous Multi-Threading (SMT).

Fixed an issue in which the table service partition was offline when its underlying

storage was out of space.

Added retry logic around Get-Volume calls in Test-AzureStack InfraCapacity

validation.

To apply this hotfix, you must have version 1.2108.2.65 or later.

Download the following files. Then, follow the instructions on the Apply updates in

Azure Stack page on the Microsoft Docs website to apply this update to Azure Stack.

Download the zip file now .

Download the hotfix xml file now .

Hotfix information

） Important

As outlined in the release notes for the 2108 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

More information

Azure Stack Hub hotfix 1.2102.31.152

Article • 10/18/2022

Improved stability of SDN components.

Improved the PnP device attached alert and moved it back to Preview.

Optimized reading of disk IOPS values to support VMs with a large number of data

disks.

CRP will self-heal a VM with a SCSI disk that failed to attach instead of requiring

operator removal of the disk from the VM.

Fixed an issue in VM power-off operation in which CRP service always ignored the

value of the non-graceful VM shutdown parameter.

Fixed an issue that prevented health remediation of the Compute Host Agent

service.

Fixed a bug in incremental disk snapshots in which a failed snapshot can block any

future snapshot operation.

Fixed a mismatched cluster name issue in FRP.

Fixed an issue that could impact updating to 2108.

Resolved an issue in which the Create a Virtual Machine image dropdown displays

image options that are not available or were not downloaded to the stamp.

Fixed an issue in which the PrivateWorkingSet queried value overflows if larger

than 4 GB.

Removed some unnecessary detailed error information on the administrator portal.

Improvements to support tools.

Resolved an issue with some Key Vault applications being in an unhealthy state

while updating from 2102 to later builds.

Add retry for get-volume requests in Test-AzureStack infra capacity check.

Shorten the "break-glass" tokens and make them human-readable.

Fixed a bug related to physical disk health when repairing a node with SED drives.

Improved Datapruner processing to minimize actor timeout alerts.

Enabled rotation of health agent SSL certificate as part of internal secret rotation.

Added graphs to Storage area that show volume performance.

Improved logic for incremental snapshot creation and deletion.

Improved resiliency in PEP startup script.

Summary

Fixes rolled up from previous hotfix releases

Fixed an issue in which System Center Operations Manager (SCOM) was unable to

close operator portal alerts.

Improved auto-remediation workflow for memory utilization.

Improved incremental snapshot creation and deletion.

Addressed an issue in the Reset-CloudAdminPassword cmdlet.

Updated Network Controller to fix bugs in PA VIP allocation and IP-MAC leaks.

Improved performance when querying for usage data.

Improved resiliency of compute admin operations.

Removed overly verbose logging from Software Load Balancer VMs.

Fixed a memory leak issue and improved memory efficiency for monitoring

services.

Fixed an issue in which the backup blade showed a "rainy" page when backup

share was inaccessible.

Fixed an issue that prevented transcript collection when closing Privileged

Endpoint (PEP) session.

Fixed a multi-tenancy website security issue.

Improved reliability of update from 2008 to 2102.

Fix for adding availability set to SQL VM in the SQL VM creation process.

Fix for setting storage size in SQL VM configuration to more than 1000 GB.

Fixed group-based authorization errors for users that require group expansion.

Newer API version support for Key Vault resource provider. The Key Vault control

plane supports the 2019-09-01 API version, and the Key Vault data plane supports

API version 7.1.

Added banner to warn users when a certificate will expire soon.

Fix to show accurate status of node in portal if a repair operation on it has failed.

ETW trace sessions are configured to use 16 MB of non-pagedpool memory. Trace

sessions now report lost event count (if any) per session, during ETL file rotation in

TraceCollector Eventlog. This releases critical non-paged pool memory for other

services on hosts and VMs. Also fixed various bugs in Tracecollector.

Fixed bugs that increased memory pressure on infrastructure.

Fixed bugs in AD FS and Azure Stack Graph to improve deployment and upgrade

reliability.

Fixed bugs in SRP and DiskRP in which performance counters were missing in the

WAC client.

Fixed a bug in resource provider (for example, Event Hubs) deployment, update, or

secret rotation. The operation previously failed with no apparent failure cause. The

fix allows the operation to complete successfully.

Fixed a bug that incorrectly raised a PnPDevice.Attached alert for a set of devices

(mouse, keyboard, etc.) that were safe.

Set memory alert to preview.

Addressed an issue with host agent monitors.

Fixed a trust relationship issue with container applications in FabricRing.

Improved RdAgent availability by removing empty RdAgent files.

Improved reliability of full update.

Extended the update readiness checks to cover more Service Fabric health and VM

health checks; for example, memory usage and storage disk capacity checks.

Updated memory configuration for VM sizes Standard\_NC16as\_T4\_v3 and

Standard\_NC64as\_T4\_v3.

Removed legacy SRP SQL instances and DB files to free up stamp resources.

Fixed a bug in which the cluster status can be stuck in "Configuring Storage" after

adding a new node.

Fixed health package registration, removing duplicate artifact creation.

Fixed a bug that sometimes caused health blades in the operator portal to become

unavailable.

Fixed a bug in which BCDR runner logs filled up MASLogs folders on physical

hosts.

Added monitoring of WMIProvider health and remediation.

Added Network Controller IMOS size check to Test-AzureStack.

Fixed a bug in SSL certificate validation during internal secret rotation.

Fixed process watchdog memory leaks.

Updated Defender platform to version 4.18.2103.7.

Enabled the alert module for customers depending on Syslog for alerts. The

services will continue to emit alerts to the Syslog pipeline.

To apply this hotfix, you must have version 1.2102.28.82 or later.

Download the following files. Then, follow the instructions on the Apply updates in

Azure Stack page on the Microsoft Docs website to apply this update to Azure Stack.

Hotfix information

） Important

As outlined in the release notes for the 2102 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

Download the zip file now .

Download the hotfix xml file now .

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

More information

Azure Stack Hub hotfix 1.2206.2.38

Article • 09/21/2022

Fixed an issue in the Virtual Machine Scale Set portal creation experience that

caused the addition of an existing load balancer to fail.

Removed unsupported Reapply feature in the virtual machine portal experience.

Fixed an issue in which the infrastructure backup information displayed on the

portal is not consistent with the alert.

Improved blob metadata backup stability by skipping unnecessary dependency.

Optimized reading of disk IOPS values to support VMs with a large number of data

disks.

CRP will self-heal a VM with a SCSI disk that failed to attach instead of requiring

operator removal of the disk from the VM.

Added support for Azure Stack Hub root certificate rotation.

Fixed an issue that prevented guest operating system activation of Windows Server

2022.

Fixed a null reference issue when calling the Compute Resource Provider API to

power off a virtual machine without doing a shutdown.

Fixed stability bugs in Azure Kubernetes Service, reliability issues in usage

reporting, and Azure Stack update operations based on availability fixes for an

internal settings service.

Updated AMD GPU driver VM extension with new default driver path.

Fixed an issue preventing health remediation of the Compute Host Agent service.

To apply this hotfix, you must have version 1.2206.0.6 or later.

Summary

Fixes rolled up from previous hotfix releases

Hotfix information

） Important

As outlined in the release notes for the 2108 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

Download the following files. Then, follow the instructions in Apply updates in Azure

Stack to apply this update.

Download the zip file now .

Download the hotfix xml file now .

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

More information

Azure Stack Hub hotfix 1.2108.2.113

Article • 09/21/2022

Fixed an issue in the Virtual Machine Scale Set portal creation experience that

caused the addition of an existing load balancer to fail.

Removed unsupported Reapply feature in the virtual machine portal experience.

Fixed an issue in which the SRP container portal cannot display more than 1 page

of containers.

Fixed an issue with searching for a container by prefix in the SRP container portal.

Improved blob metadata backup stability by skipping unnecessary dependency.

Added support for Azure Stack Hub root certificate rotation.

Fixed an issue that prevented guest operating system activation of Windows Server

2022.

Fixed a null reference issue when calling the Compute Resource Provider API to

power off a virtual machine without doing a shutdown.

Fixed an issue in which some StorageController requests might time out under

high concurrency.

Removed some of the network performance counters and reduced collection

interval for other perf counters.

Cleaned up unneeded networking traces from Baremetal, NC and XRP VMs.

Fixed an issue deleting Microsoft.ContainerService/managedCluster resources

that occurred when resources managed by the AKS resource provider were

manually deleted beforehand.

Fixed a regression in which VM status is reported as UNKNOWN in the portal.

Fixed an issue that could impact updating from 2102 to 2108.

Support for new Kubernetes versions in AKS.

Fixed bugs in trace collector.

Fixed a bug related to physical disk health when repairing a node with SED drives.

Improvements to support tools.

Fixed bugs in log collection.

Fixed code defect leading to VM deployment failures.

Improved the resolution of the Network Resource Provider.

Summary

Fixes rolled up from previous hotfix releases

Fixed a bug in incremental disk snapshots in which a failed snapshot can block any

future snapshot operations.

Fixed a disk snapshot failure and VM IO hang when taking snapshots.

Shortened the PEP tokens and made them human-readable.

Fix to improve SLB throughput after enabling Simultaneous Multi-Threading (SMT).

Fixed an issue in which the table service partition was offline when its underlying

storage was out of space.

Added retry logic around Get-Volume calls in Test-AzureStack InfraCapacity

validation.

To apply this hotfix, you must have version 1.2108.2.65 or later.

Download the following files. Then, follow the instructions in Apply updates in Azure

Stack to apply this update.

Download the zip file now .

Download the hotfix xml file now .

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

Hotfix information

） Important

As outlined in the release notes for the 2108 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

More information

Azure Stack Hub hotfix 1.2102.30.148

Article • 09/21/2022

Optimized reading of disk IOPS values to support VMs with a large number of data

disks.

CRP will self-heal a VM with a SCSI disk that failed to attach instead of requiring

operator removal of the disk from the VM.

Fixed an issue in VM power-off operation in which CRP service always ignored the

value of the non-graceful VM shutdown parameter.

Fixed an issue that prevented health remediation of the Compute Host Agent

service.

Fixed a bug in incremental disk snapshots in which a failed snapshot can block any

future snapshot operation.

Fixed a mismatched cluster name issue in FRP.

Fixed an issue that could impact updating to 2108.

Resolved an issue in which the Create a Virtual Machine image dropdown displays

image options that are not available or were not downloaded to the stamp.

Fixed an issue in which the PrivateWorkingSet queried value overflows if larger

than 4 GB.

Removed some unnecessary detailed error information on the administrator portal.

Improvements to support tools.

Resolved an issue with some Key Vault applications being in an unhealthy state

while updating from 2102 to later builds.

Add retry for get-volume requests in Test-AzureStack infra capacity check.

Shorten the "break-glass" tokens and make them human-readable.

Fixed a bug related to physical disk health when repairing a node with SED drives.

Improved Datapruner processing to minimize actor timeout alerts.

Enabled rotation of health agent SSL certificate as part of internal secret rotation.

Added graphs to Storage area that show volume performance.

Improved logic for incremental snapshot creation and deletion.

Improved resiliency in PEP startup script.

Fixed an issue in which System Center Operations Manager (SCOM) was unable to

close operator portal alerts.

Summary

Fixes rolled up from previous hotfix releases

Improved auto-remediation workflow for memory utilization.

Improved incremental snapshot creation and deletion.

Addressed an issue in the Reset-CloudAdminPassword cmdlet.

Updated Network Controller to fix bugs in PA VIP allocation and IP-MAC leaks.

Improved performance when querying for usage data.

Improved resiliency of compute admin operations.

Removed overly verbose logging from Software Load Balancer VMs.

Fixed a memory leak issue and improved memory efficiency for monitoring

services.

Fixed an issue in which the backup blade showed a "rainy" page when backup

share was inaccessible.

Fixed an issue that prevented transcript collection when closing Privileged

Endpoint (PEP) session.

Fixed a multi-tenancy website security issue.

Improved reliability of update from 2008 to 2102.

Fix for adding availability set to SQL VM in the SQL VM creation process.

Fix for setting storage size in SQL VM configuration to more than 1000 GB.

Fixed group-based authorization errors for users that require group expansion.

Newer API version support for Key Vault resource provider. The Key Vault control

plane supports the 2019-09-01 API version, and the Key Vault data plane supports

API version 7.1.

Added banner to warn users when a certificate will expire soon.

Fix to show accurate status of node in portal if a repair operation on it has failed.

ETW trace sessions are configured to use 16 MB of non-pagedpool memory. Trace

sessions now report lost event count (if any) per session, during ETL file rotation in

TraceCollector Eventlog. This releases critical non-paged pool memory for other

services on hosts and VMs. Also fixed various bugs in Tracecollector.

Fixed bugs that increased memory pressure on infrastructure.

Fixed bugs in AD FS and Azure Stack Graph to improve deployment and upgrade

reliability.

Fixed bugs in SRP and DiskRP in which performance counters were missing in the

WAC client.

Fixed a bug in resource provider (for example, Event Hubs) deployment, update, or

secret rotation. The operation previously failed with no apparent failure cause. The

fix allows the operation to complete successfully.

Fixed a bug that incorrectly raised a PnPDevice.Attached alert for a set of devices

(mouse, keyboard, etc.) that were safe.

Set memory alert to preview.

Addressed an issue with host agent monitors.

Fixed a trust relationship issue with container applications in FabricRing.

Improved RdAgent availability by removing empty RdAgent files.

Improved reliability of full update.

Extended the update readiness checks to cover more Service Fabric health and VM

health checks; for example, memory usage and storage disk capacity checks.

Updated memory configuration for VM sizes Standard\_NC16as\_T4\_v3 and

Standard\_NC64as\_T4\_v3.

Removed legacy SRP SQL instances and DB files to free up stamp resources.

Fixed a bug in which the cluster status can be stuck in "Configuring Storage" after

adding a new node.

Fixed health package registration, removing duplicate artifact creation.

Fixed a bug that sometimes caused health blades in the operator portal to become

unavailable.

Fixed a bug in which BCDR runner logs filled up MASLogs folders on physical

hosts.

Added monitoring of WMIProvider health and remediation.

Added Network Controller IMOS size check to Test-AzureStack.

Fixed a bug in SSL certificate validation during internal secret rotation.

Fixed process watchdog memory leaks.

Updated Defender platform to version 4.18.2103.7.

Enabled the alert module for customers depending on Syslog for alerts. The

services will continue to emit alerts to the Syslog pipeline.

To apply this hotfix, you must have version 1.2102.28.82 or later.

Download the following files. Then, follow the instructions in Apply updates in Azure

Stack to apply this update.

Download the zip file now .

Hotfix information

） Important

As outlined in the release notes for the 2102 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

Download the hotfix xml file now .

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

More information

Azure Stack Hub hotfix 1.2206.1.25

Article • 09/21/2022

Fixed stability bugs in Azure Kubernetes Service, reliability issues in usage

reporting, and Azure Stack update operations based on availability fixes for an

internal settings service.

Updated AMD GPU driver VM extension with new default driver path.

Fixed an issue preventing health remediation of the Compute Host Agent service.

To apply this hotfix, you must have version 1.2206.0.6 or later.

Download the following files. Then, follow the instructions in Apply updates in Azure

Stack to apply this update.

Download the zip file now .

Download the hotfix xml file now .

Azure Stack Hub update resources

Summary

Fixes rolled up from previous hotfix releases

Hotfix information

） Important

As outlined in the release notes for the 2108 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

More information

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

Azure Stack Hub hotfix 1.2206.1.24

Article • 09/21/2022

Updated AMD GPU driver VM extension with new default driver path.

Fixed an issue preventing health remediation of the Compute Host Agent service.

To apply this hotfix, you must have version 1.2206.0.6 or later.

Download the following files. Then, follow the instructions in Apply updates in Azure

Stack to apply this update.

Download the zip file now .

Download the hotfix xml file now .

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

Summary

Hotfix information

） Important

As outlined in the release notes for the 2108 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

More information

Azure Stack Hub hotfix 1.2108.2.111

Article • 09/21/2022

Fixed an issue in which some StorageController requests might time out under

high concurrency.

Removed some of the network performance counters and reduced collection

interval for other perf counters.

Cleaned up unneeded networking traces from Baremetal, NC and XRP VMs.

Fixed an issue deleting Microsoft.ContainerService/managedCluster resources

that occurred when resources managed by the AKS resource provider were

manually deleted beforehand.

Fixed a regression in which VM status is reported as UNKNOWN in the portal.

Fixed an issue that could impact updating from 2102 to 2108.

Support for new Kubernetes versions in AKS.

Fixed bugs in trace collector.

Fixed a bug related to physical disk health when repairing a node with SED drives.

Improvements to support tools.

Fixed bugs in log collection.

Fixed code defect leading to VM deployment failures.

Improved the resolution of the Network Resource Provider.

Fixed a bug in incremental disk snapshots in which a failed snapshot can block any

future snapshot operations.

Fixed a disk snapshot failure and VM IO hang when taking snapshots.

Shortened the PEP tokens and made them human-readable.

Fix to improve SLB throughput after enabling Simultaneous Multi-Threading (SMT).

Fixed an issue in which the table service partition was offline when its underlying

storage was out of space.

Added retry logic around Get-Volume calls in Test-AzureStack InfraCapacity

validation.

To apply this hotfix, you must have version 1.2108.2.65 or later.

Summary

Fixes rolled up from previous hotfix releases

Hotfix information

Download the following files. Then, follow the instructions in Apply updates in Azure

Stack to apply this update.

Download the zip file now .

Download the hotfix xml file now .

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

） Important

As outlined in the release notes for the 2108 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

More information

Azure Stack Hub hotfix 1.2102.30.146

Article • 09/21/2022

Fixed a bug in incremental disk snapshots in which a failed snapshot can block any

future snapshot operation.

Fixed a mismatched cluster name issue in FRP.

Fixed an issue that could impact updating to 2108.

Resolved an issue in which the Create a Virtual Machine image dropdown displays

image options that are not available or were not downloaded to the stamp.

Fixed an issue in which the PrivateWorkingSet queried value overflows if larger

than 4 GB.

Removed some unnecessary detailed error information on the administrator portal.

Improvements to support tools.

Resolved an issue with some Key Vault applications being in an unhealthy state

while updating from 2102 to later builds.

Add retry for get-volume requests in Test-AzureStack infra capacity check.

Shorten the "break-glass" tokens and make them human-readable.

Fixed a bug related to physical disk health when repairing a node with SED drives.

Improved Datapruner processing to minimize actor timeout alerts.

Enabled rotation of health agent SSL certificate as part of internal secret rotation.

Added graphs to Storage area that show volume performance.

Improved logic for incremental snapshot creation and deletion.

Improved resiliency in PEP startup script.

Fixed an issue in which System Center Operations Manager (SCOM) was unable to

close operator portal alerts.

Improved auto-remediation workflow for memory utilization.

Improved incremental snapshot creation and deletion.

Addressed an issue in the Reset-CloudAdminPassword cmdlet.

Updated Network Controller to fix bugs in PA VIP allocation and IP-MAC leaks.

Improved performance when querying for usage data.

Improved resiliency of compute admin operations.

Removed overly verbose logging from Software Load Balancer VMs.

Summary

Fixes rolled up from previous hotfix releases

Fixed a memory leak issue and improved memory efficiency for monitoring

services.

Fixed an issue in which the backup blade showed a "rainy" page when backup

share was inaccessible.

Fixed an issue that prevented transcript collection when closing Privileged

Endpoint (PEP) session.

Fixed a multi-tenancy website security issue.

Improved reliability of update from 2008 to 2102.

Fix for adding availability set to SQL VM in the SQL VM creation process.

Fix for setting storage size in SQL VM configuration to more than 1000 GB.

Fixed group-based authorization errors for users that require group expansion.

Newer API version support for Key Vault resource provider. The Key Vault control

plane supports the 2019-09-01 API version, and the Key Vault data plane supports

API version 7.1.

Added banner to warn users when a certificate will expire soon.

Fix to show accurate status of node in portal if a repair operation on it has failed.

ETW trace sessions are configured to use 16 MB of non-pagedpool memory. Trace

sessions now report lost event count (if any) per session, during ETL file rotation in

TraceCollector Eventlog. This releases critical non-paged pool memory for other

services on hosts and VMs. Also fixed various bugs in Tracecollector.

Fixed bugs that increased memory pressure on infrastructure.

Fixed bugs in AD FS and Azure Stack Graph to improve deployment and upgrade

reliability.

Fixed bugs in SRP and DiskRP in which performance counters were missing in the

WAC client.

Fixed a bug in resource provider (for example, Event Hubs) deployment, update, or

secret rotation. The operation previously failed with no apparent failure cause. The

fix allows the operation to complete successfully.

Fixed a bug that incorrectly raised a PnPDevice.Attached alert for a set of devices

(mouse, keyboard, etc.) that were safe.

Set memory alert to preview.

Addressed an issue with host agent monitors.

Fixed a trust relationship issue with container applications in FabricRing.

Improved RdAgent availability by removing empty RdAgent files.

Improved reliability of full update.

Extended the update readiness checks to cover more Service Fabric health and VM

health checks; for example, memory usage and storage disk capacity checks.

Updated memory configuration for VM sizes Standard\_NC16as\_T4\_v3 and

Standard\_NC64as\_T4\_v3.

Removed legacy SRP SQL instances and DB files to free up stamp resources.

Fixed a bug in which the cluster status can be stuck in "Configuring Storage" after

adding a new node.

Fixed health package registration, removing duplicate artifact creation.

Fixed a bug that sometimes caused health blades in the operator portal to become

unavailable.

Fixed a bug in which BCDR runner logs filled up MASLogs folders on physical

hosts.

Added monitoring of WMIProvider health and remediation.

Added Network Controller IMOS size check to Test-AzureStack.

Fixed a bug in SSL certificate validation during internal secret rotation.

Fixed process watchdog memory leaks.

Updated Defender platform to version 4.18.2103.7.

Enabled the alert module for customers depending on Syslog for alerts. The

services will continue to emit alerts to the Syslog pipeline.

To apply this hotfix, you must have version 1.2102.28.82 or later.

Download the following files. Then, follow the instructions in Apply updates in Azure

Stack to apply this update.

Download the zip file now .

Download the hotfix xml file now .

Azure Stack Hub update resources

Apply updates in Azure Stack

Hotfix information

） Important

As outlined in the release notes for the 2102 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

More information

Monitor updates in Azure Stack by using the privileged endpoint

Azure Stack Hub hotfix 1.2008.41.161

Article • 09/21/2022

Fixes and performance enhancements.

Improvements to support tools.

Added graphs to Storage area that show volume performance.

Improved Datapruner processing to minimize actor timeout alerts.

Improved auto-remediation workflow for memory utilization.

Addressed an issue in the Reset-CloudAdminPassword cmdlet.

Updated Network Controller to fix bugs in PA VIP allocation and IP-MAC leaks.

Improved resiliency of PEP startup script.

Improved performance when querying for usage data.

Improved resiliency of compute admin operations.

Removed overly verbose logging from Software Load Balancer VMs.

Fixed a trust relationship issue for container applications in FabricRing.

Added banner to warn users when a certificate will expire soon.

Improved reliability of update from 2008 to 2102.

Improved reliability of update from 2005 to 2008.

Improved RdAgent availability by removing empty RdAgent files.

Fix for more ghost NIC scenarios when deleting a resource group.

Fixed an issue that, in rare cases, deleted VNet peerings.

ETW trace sessions are configured to use 16 MB of non-pagedpool memory. Trace

sessions now report lost event count (if any) per session, during ETL file rotation in

TraceCollector Eventlog. This releases critical non-paged pool memory for other

services on hosts and VMs. Also fixed various bugs in Tracecollector.

Fixed a bug in resource provider (for example, Event Hubs) deployment, update, or

secret rotation. The operation previously failed with no apparent failure cause. The

fix allows the operation to complete successfully.

Extended the update readiness checks to cover more Service Fabric health and VM

health checks; for example, memory usage and storage disk capacity checks.

Fixed bugs that increased memory pressure on infrastructure.

Fixed bugs that caused operator portal blades to fail to load.

Improved reliability of Process Watchdog.

Summary

Fixes rolled up from previous hotfix releases

Improved update reliability by adding detection and self-healing for low available

memory conditions on ERCS VMs at the beginning of the update orchestration.

Fixed a bug in which BCDR runner logs fill up MASLogs folders on physical hosts.

Added monitoring for WMI and remediation.

Added Network Controller IMOS size check to Test-AzureStack.

Fixed internal secret rotation failures (failing at the NC:Secret rotate step), seen

after updating to Azure Stack Hub version 1.2008.25.114 or higher from the latest

2005 release.

Configured stamp ADFS to monitor corporate ADFS signing certificate rollover.

This is for Azure Stack Hub with ADFS identity systems when Azure Stack Hub is

configured with corp ADFS and a federation metadata endpoint.

Fixed alert to remediation linking. Moved memory-critical alert to preview.

Fixed health package registration, removing duplicate artifact creation.

Improved reliability of RdAgent upgrade.

Enhanced idempotent logic in handling malfunctioning TPMs.

Fixed an issue in which uninstalling some extensions put previously deployed

extensions into a failed state.

Fixed an issue in which duplicate installed updates were shown in the update

history list.

Fixed an intermittent issue in which FRU of SRNG could fail connecting to the ECE

agent.

Fixed VM NICs getting a different hardware identifier after VM is deallocated and

restarted.

Monitored and rebooted VMs based on memory pressure.

Added AzsGBRReadiness in Test-AzureStack to check physical disks' health for

granular bitmap repair readiness.

Reactivated firewall rules to enable SNMP traffic on ERCS VMs.

Fixed an issue in which modifying any properties on the Local Network Gateway

was causing other VPN connections on that gateway to disconnect.

Fixed an issue in which infrastructure VM deployment can fail after applying a

hotfix.

Cleaned up stale user profile folders to clear disk space.

Fixed an issue in which a secondary blob data partition cannot be loaded in some

error cases.

Fixed some bugs with the use of temporary domain accounts.

Enhanced temporary domain account naming to ensure uniqueness.

Patched SDN-related binaries on the physical nodes.

Improved reliability and diagnosing capabilities of patch and update.

Added auto-remediation for SQL cluster.

Updated Healthagent to use Nugetstore.

Filtered WHS alert for Netadapter.

Fixed an issue in which the copy of a certificate used by Service Fabric was

overwritten.

Fixed appearance of ghost NICs when deleting a resource group.

Fixed regression in Test-AzureStack that caused VM deployment test case to

automatically skip.

Improved resiliency of VM provisioning, extension, and image operations.

Fixed an invalid state in Storage resource provider for storage accounts migrated

from 1910 with suspended state.

Fixed a bug in local health system that potentially increased memory pressure on

infrastructure.

Fixed issue in internal secret rotation that would fail with a timeout error if valueadd resource providers were unhealthy.

Fixed a bug in which closed alerts' Last Modified Time was updated in the

operator portal even if the alert stayed closed.

Optimized operator alert request handling, which reduces the chance of timeouts

when viewing alerts in the operator portal or monitoring them via System Center

Operations Manager (SCOM).

Check and enforce key protectors on cluster shared volumes per host.

Fixed issue in which Managed Disk usage data was not being reported after the

2008 update.

Fixed VMs losing connectivity while SuspendNode is occurring in MAS, as part of

host reboot during patch and update.

Added PEP to retrieve current registration details, stale object cleanup for

Remove-Registration.

Fixed a bug that caused the Infrastructure Roles panel in the operator portal to

display incorrect health information.

Improved reliability of log collection for SDN roles by collecting logs on the file

share.

Fixed an issue that can raise an audit scanner health alert in PEP cmdlet.

Removed invalid repair interface for seedringservices.

Improved SDN network reliability on the physical nodes.

Enabled SQL container logs.

Fixed an issue that erroneously raises an alert: "Node inaccessible for VM

Placement."

Fixed a remote management enabling issue for Azure Stack registrations done

prior to 1910 release.

Improved reliability of host node update.

Critical fix for disk space exhaustion on physical hosts, network controllers,

gateways, and load balancers.

Fixed remote management resource replication for resource arrays with

continuation token.

Fixed an issue in which a storage account might be partially restored due to a KVS

race condition in the SRP background usage job.

Fixed an issue in which a virtual subnet was not being cleaned up if the tunnel was

moved to a different GW VM and then the VGW was deleted.

Fixed an issue that could cause registration and internal secret rotation to fail.

Fixed an issue in the internal secret rotation, which might cause a failure in the next

update.

Addressed an issue with internal secret rotation for NRP with a large number of

subscriptions.

Mitigated connection problems to ERCS following startup.

Mitigated a potential issue with upgrading to future versions.

Addressed memory leak based on health runners and suppressed faulty alerts.

Added memory-specific settings to crash dump settings.

Remediated ERCS memory pressure during patch & update.

Included AzsInfraRoleSummary Test-Azurestack test as UpdateReadiness.

Fixed an issue where certificate rotation on IoT Hub fails with "Internal execution

error."

To apply this hotfix, you must have version 1.2008.13.88 or later.

Download the following files. Then, follow the instructions in Apply updates in Azure

Stack to apply this update.

Download the zip file now .

Download the hotfix xml file now .

Hotfix information

） Important

As outlined in the release notes for the 2008 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

More information

Azure Stack Hub hotfix 1.2108.2.102

Article • 09/21/2022

Fixed an issue that could impact updating from 2102 to 2108.

Support for new Kubernetes versions in AKS.

Fixed bugs in trace collector.

Fixed a bug related to physical disk health when repairing a node with SED drives.

Improvements to support tools.

Fixed bugs in log collection.

Fixed code defect leading to VM deployment failures.

Improved the resolution of the Network Resource Provider.

Fixed a bug in incremental disk snapshots in which a failed snapshot can block any

future snapshot operations.

Fixed a disk snapshot failure and VM IO hang when taking snapshots.

Shortened the PEP tokens and made them human-readable.

Fix to improve SLB throughput after enabling Simultaneous Multi-Threading (SMT).

Fixed an issue in which the table service partition was offline when its underlying

storage was out of space.

Added retry logic around Get-Volume calls in Test-AzureStack InfraCapacity

validation.

To apply this hotfix, you must have version 1.2108.2.65 or later.

Summary

Fixes rolled up from previous hotfix releases

Hotfix information

） Important

As outlined in the release notes for the 2108 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

Download the following files. Then, follow the instructions in Apply updates in Azure

Stack to apply this update.

Download the zip file now .

Download the hotfix xml file now .

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

File information

More information

Azure Stack Hub hotfix 1.2102.30.132

Article • 09/21/2022

Fixed an issue that could impact updating to 2108.

Resolved an issue in which the Create a Virtual Machine image dropdown displays

image options that are not available or were not downloaded to the stamp.

Fixed an issue in which the PrivateWorkingSet queried value overflows if larger

than 4 GB.

Removed some unnecessary detailed error information on the administrator portal.

Improvements to support tools.

Resolved an issue with some Key Vault applications being in an unhealthy state

while updating from 2102 to later builds.

Add retry for get-volume requests in Test-AzureStack infra capacity check.

Shorten the "break-glass" tokens and make them human-readable.

Fixed a bug related to physical disk health when repairing a node with SED drives.

Improved Datapruner processing to minimize actor timeout alerts.

Enabled rotation of health agent SSL certificate as part of internal secret rotation.

Added graphs to Storage area that show volume performance.

Improved logic for incremental snapshot creation and deletion.

Improved resiliency in PEP startup script.

Fixed an issue in which System Center Operations Manager (SCOM) was unable to

close operator portal alerts.

Improved auto-remediation workflow for memory utilization.

Improved incremental snapshot creation and deletion.

Addressed an issue in the Reset-CloudAdminPassword cmdlet.

Updated Network Controller to fix bugs in PA VIP allocation and IP-MAC leaks.

Improved performance when querying for usage data.

Improved resiliency of compute admin operations.

Removed overly verbose logging from Software Load Balancer VMs.

Fixed a memory leak issue and improved memory efficiency for monitoring

services.

Fixed an issue in which the backup blade showed a "rainy" page when backup

share was inaccessible.

Summary

Fixes rolled up from previous hotfix releases

Fixed an issue that prevented transcript collection when closing Privileged

Endpoint (PEP) session.

Fixed a multi-tenancy website security issue.

Improved reliability of update from 2008 to 2102.

Fix for adding availability set to SQL VM in the SQL VM creation process.

Fix for setting storage size in SQL VM configuration to more than 1000 GB.

Fixed group-based authorization errors for users that require group expansion.

Newer API version support for Key Vault resource provider. The Key Vault control

plane supports the 2019-09-01 API version, and the Key Vault data plane supports

API version 7.1.

Added banner to warn users when a certificate will expire soon.

Fix to show accurate status of node in portal if a repair operation on it has failed.

ETW trace sessions are configured to use 16 MB of non-pagedpool memory. Trace

sessions now report lost event count (if any) per session, during ETL file rotation in

TraceCollector Eventlog. This releases critical non-paged pool memory for other

services on hosts and VMs. Also fixed various bugs in Tracecollector.

Fixed bugs that increased memory pressure on infrastructure.

Fixed bugs in AD FS and Azure Stack Graph to improve deployment and upgrade

reliability.

Fixed bugs in SRP and DiskRP in which performance counters were missing in the

WAC client.

Fixed a bug in resource provider (for example, Event Hubs) deployment, update, or

secret rotation. The operation previously failed with no apparent failure cause. The

fix allows the operation to complete successfully.

Fixed a bug that incorrectly raised a PnPDevice.Attached alert for a set of devices

(mouse, keyboard, etc.) that were safe.

Set memory alert to preview.

Addressed an issue with host agent monitors.

Fixed a trust relationship issue with container applications in FabricRing.

Improved RdAgent availability by removing empty RdAgent files.

Improved reliability of full update.

Extended the update readiness checks to cover more Service Fabric health and VM

health checks; for example, memory usage and storage disk capacity checks.

Updated memory configuration for VM sizes Standard\_NC16as\_T4\_v3 and

Standard\_NC64as\_T4\_v3.

Removed legacy SRP SQL instances and DB files to free up stamp resources.

Fixed a bug in which the cluster status can be stuck in "Configuring Storage" after

adding a new node.

Fixed health package registration, removing duplicate artifact creation.

Fixed a bug that sometimes caused health blades in the operator portal to become

unavailable.

Fixed a bug in which BCDR runner logs filled up MASLogs folders on physical

hosts.

Added monitoring of WMIProvider health and remediation.

Added Network Controller IMOS size check to Test-AzureStack.

Fixed a bug in SSL certificate validation during internal secret rotation.

Fixed process watchdog memory leaks.

Updated Defender platform to version 4.18.2103.7.

Enabled the alert module for customers depending on Syslog for alerts. The

services will continue to emit alerts to the Syslog pipeline.

To apply this hotfix, you must have version 1.2102.28.82 or later.

Download the following files. Then, follow the instructions in Apply updates in Azure

Stack to apply this update.

Download the zip file now .

Download the hotfix xml file now .

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

Hotfix information

） Important

As outlined in the release notes for the 2102 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

More information

Azure Stack Hub hotfix 1.2008.41.159

Article • 09/21/2022

Improvements to support tools.

Added graphs to Storage area that show volume performance.

Improved Datapruner processing to minimize actor timeout alerts.

Improved auto-remediation workflow for memory utilization.

Addressed an issue in the Reset-CloudAdminPassword cmdlet.

Updated Network Controller to fix bugs in PA VIP allocation and IP-MAC leaks.

Improved resiliency of PEP startup script.

Improved performance when querying for usage data.

Improved resiliency of compute admin operations.

Removed overly verbose logging from Software Load Balancer VMs.

Fixed a trust relationship issue for container applications in FabricRing.

Added banner to warn users when a certificate will expire soon.

Improved reliability of update from 2008 to 2102.

Improved reliability of update from 2005 to 2008.

Improved RdAgent availability by removing empty RdAgent files.

Fix for more ghost NIC scenarios when deleting a resource group.

Fixed an issue that, in rare cases, deleted VNet peerings.

ETW trace sessions are configured to use 16 MB of non-pagedpool memory. Trace

sessions now report lost event count (if any) per session, during ETL file rotation in

TraceCollector Eventlog. This releases critical non-paged pool memory for other

services on hosts and VMs. Also fixed various bugs in Tracecollector.

Fixed a bug in resource provider (for example, Event Hubs) deployment, update, or

secret rotation. The operation previously failed with no apparent failure cause. The

fix allows the operation to complete successfully.

Extended the update readiness checks to cover more Service Fabric health and VM

health checks; for example, memory usage and storage disk capacity checks.

Fixed bugs that increased memory pressure on infrastructure.

Fixed bugs that caused operator portal blades to fail to load.

Improved reliability of Process Watchdog.

Summary

Fixes rolled up from previous hotfix releases

Improved update reliability by adding detection and self-healing for low available

memory conditions on ERCS VMs at the beginning of the update orchestration.

Fixed a bug in which BCDR runner logs fill up MASLogs folders on physical hosts.

Added monitoring for WMI and remediation.

Added Network Controller IMOS size check to Test-AzureStack.

Fixed internal secret rotation failures (failing at the NC:Secret rotate step), seen

after updating to Azure Stack Hub version 1.2008.25.114 or higher from the latest

2005 release.

Configured stamp ADFS to monitor corporate ADFS signing certificate rollover.

This is for Azure Stack Hub with ADFS identity systems when Azure Stack Hub is

configured with corp ADFS and a federation metadata endpoint.

Fixed alert to remediation linking. Moved memory-critical alert to preview.

Fixed health package registration, removing duplicate artifact creation.

Improved reliability of RdAgent upgrade.

Enhanced idempotent logic in handling malfunctioning TPMs.

Fixed an issue in which uninstalling some extensions put previously deployed

extensions into a failed state.

Fixed an issue in which duplicate installed updates were shown in the update

history list.

Fixed an intermittent issue in which FRU of SRNG could fail connecting to the ECE

agent.

Fixed VM NICs getting a different hardware identifier after VM is deallocated and

restarted.

Monitored and rebooted VMs based on memory pressure.

Added AzsGBRReadiness in Test-AzureStack to check physical disks' health for

granular bitmap repair readiness.

Reactivated firewall rules to enable SNMP traffic on ERCS VMs.

Fixed an issue in which modifying any properties on the Local Network Gateway

was causing other VPN connections on that gateway to disconnect.

Fixed an issue in which infrastructure VM deployment can fail after applying a

hotfix.

Cleaned up stale user profile folders to clear disk space.

Fixed an issue in which a secondary blob data partition cannot be loaded in some

error cases.

Fixed some bugs with the use of temporary domain accounts.

Enhanced temporary domain account naming to ensure uniqueness.

Patched SDN-related binaries on the physical nodes.

Improved reliability and diagnosing capabilities of patch and update.

Added auto-remediation for SQL cluster.

Updated Healthagent to use Nugetstore.

Filtered WHS alert for Netadapter.

Fixed an issue in which the copy of a certificate used by Service Fabric was

overwritten.

Fixed appearance of ghost NICs when deleting a resource group.

Fixed regression in Test-AzureStack that caused VM deployment test case to

automatically skip.

Improved resiliency of VM provisioning, extension, and image operations.

Fixed an invalid state in Storage resource provider for storage accounts migrated

from 1910 with suspended state.

Fixed a bug in local health system that potentially increased memory pressure on

infrastructure.

Fixed issue in internal secret rotation that would fail with a timeout error if valueadd resource providers were unhealthy.

Fixed a bug in which closed alerts' Last Modified Time was updated in the

operator portal even if the alert stayed closed.

Optimized operator alert request handling, which reduces the chance of timeouts

when viewing alerts in the operator portal or monitoring them via System Center

Operations Manager (SCOM).

Check and enforce key protectors on cluster shared volumes per host.

Fixed issue in which Managed Disk usage data was not being reported after the

2008 update.

Fixed VMs losing connectivity while SuspendNode is occurring in MAS, as part of

host reboot during patch and update.

Added PEP to retrieve current registration details, stale object cleanup for

Remove-Registration.

Fixed a bug that caused the Infrastructure Roles panel in the operator portal to

display incorrect health information.

Improved reliability of log collection for SDN roles by collecting logs on the file

share.

Fixed an issue that can raise an audit scanner health alert in PEP cmdlet.

Removed invalid repair interface for seedringservices.

Improved SDN network reliability on the physical nodes.

Enabled SQL container logs.

Fixed an issue that erroneously raises an alert: "Node inaccessible for VM

Placement."

Fixed a remote management enabling issue for Azure Stack registrations done

prior to 1910 release.

Improved reliability of host node update.

Critical fix for disk space exhaustion on physical hosts, network controllers,

gateways, and load balancers.

Fixed remote management resource replication for resource arrays with

continuation token.

Fixed an issue in which a storage account might be partially restored due to a KVS

race condition in the SRP background usage job.

Fixed an issue in which a virtual subnet was not being cleaned up if the tunnel was

moved to a different GW VM and then the VGW was deleted.

Fixed an issue that could cause registration and internal secret rotation to fail.

Fixed an issue in the internal secret rotation, which might cause a failure in the next

update.

Addressed an issue with internal secret rotation for NRP with a large number of

subscriptions.

Mitigated connection problems to ERCS following startup.

Mitigated a potential issue with upgrading to future versions.

Addressed memory leak based on health runners and suppressed faulty alerts.

Added memory-specific settings to crash dump settings.

Remediated ERCS memory pressure during patch & update.

Included AzsInfraRoleSummary Test-Azurestack test as UpdateReadiness.

Fixed an issue where certificate rotation on IoT Hub fails with "Internal execution

error."

To apply this hotfix, you must have version 1.2008.13.88 or later.

Download the following files. Then, follow the instructions in Apply updates in Azure

Stack to apply this update.

Download the zip file now .

Download the hotfix xml file now .

Hotfix information

） Important

As outlined in the release notes for the 2008 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

More information

Azure Stack Hub hotfix 1.2108.2.83

Article • 09/21/2022

Support for new Kubernetes versions in AKS.

Fixed bugs in trace collector.

Fixed a bug related to physical disk health when repairing a node with SED drives.

Improvements to support tools.

Fixed bugs in log collection.

Fixed code defect leading to VM deployment failures.

Improved the resolution of the Network Resource Provider.

Fixed a bug in incremental disk snapshots in which a failed snapshot can block any

future snapshot operations.

Resolved an issue in which the Create a Virtual Machine image dropdown displays

image options that are not available or were not downloaded to the stamp.

Fixed a disk snapshot failure and VM IO hang when taking snapshots.

Shortened the PEP tokens and made them human-readable.

Fix to improve SLB throughput after enabling Simultaneous Multi-Threading (SMT).

Fixed an issue in which the table service partition was offline when its underlying

storage was out of space.

Added retry logic around Get-Volume calls in Test-AzureStack InfraCapacity

validation.

To apply this hotfix, you must have version 1.2108.2.65 or later.

Summary

Fixes rolled up from previous hotfix releases

Hotfix information

） Important

As outlined in the release notes for the 2108 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

Download the following files. Then, follow the instructions in Apply updates in Azure

Stack to apply this update.

Download the zip file now .

Download the hotfix xml file now .

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

File information

More information

Azure Stack Hub hotfix 1.2102.30.118

Article • 09/21/2022

Various bug fixes and enhancements.

Add retry for get-volume requests in Test-AzureStack infra capacity check.

Shorten the "break-glass" tokens and make them human-readable.

Fixed a bug related to physical disk health when repairing a node with SED drives.

Improved Datapruner processing to minimize actor timeout alerts.

Enabled rotation of health agent SSL certificate as part of internal secret rotation.

Added graphs to Storage area that show volume performance.

Improved logic for incremental snapshot creation and deletion.

Improved resiliency in PEP startup script.

Fixed an issue in which System Center Operations Manager (SCOM) was unable to

close operator portal alerts.

Improved auto-remediation workflow for memory utilization.

Improved incremental snapshot creation and deletion.

Addressed an issue in the Reset-CloudAdminPassword cmdlet.

Updated Network Controller to fix bugs in PA VIP allocation and IP-MAC leaks.

Improved performance when querying for usage data.

Improved resiliency of compute admin operations.

Removed overly verbose logging from Software Load Balancer VMs.

Fixed a memory leak issue and improved memory efficiency for monitoring

services.

Fixed an issue in which the backup blade showed a "rainy" page when backup

share was inaccessible.

Fixed an issue that prevented transcript collection when closing Privileged

Endpoint (PEP) session.

Fixed a multi-tenancy website security issue.

Improved reliability of update from 2008 to 2102.

Fix for adding availability set to SQL VM in the SQL VM creation process.

Fix for setting storage size in SQL VM configuration to more than 1000 GB.

Fixed group-based authorization errors for users that require group expansion.

Summary

Fixes rolled up from previous hotfix releases

Newer API version support for Key Vault resource provider. The Key Vault control

plane supports the 2019-09-01 API version, and the Key Vault data plane supports

API version 7.1.

Added banner to warn users when a certificate will expire soon.

Fix to show accurate status of node in portal if a repair operation on it has failed.

ETW trace sessions are configured to use 16 MB of non-pagedpool memory. Trace

sessions now report lost event count (if any) per session, during ETL file rotation in

TraceCollector Eventlog. This releases critical non-paged pool memory for other

services on hosts and VMs. Also fixed various bugs in Tracecollector.

Fixed bugs that increased memory pressure on infrastructure.

Fixed bugs in AD FS and Azure Stack Graph to improve deployment and upgrade

reliability.

Fixed bugs in SRP and DiskRP in which performance counters were missing in the

WAC client.

Fixed a bug in resource provider (for example, Event Hubs) deployment, update, or

secret rotation. The operation previously failed with no apparent failure cause. The

fix allows the operation to complete successfully.

Fixed a bug that incorrectly raised a PnPDevice.Attached alert for a set of devices

(mouse, keyboard, etc.) that were safe.

Set memory alert to preview.

Addressed an issue with host agent monitors.

Fixed a trust relationship issue with container applications in FabricRing.

Improved RdAgent availability by removing empty RdAgent files.

Improved reliability of full update.

Extended the update readiness checks to cover more Service Fabric health and VM

health checks; for example, memory usage and storage disk capacity checks.

Updated memory configuration for VM sizes Standard\_NC16as\_T4\_v3 and

Standard\_NC64as\_T4\_v3.

Removed legacy SRP SQL instances and DB files to free up stamp resources.

Fixed a bug in which the cluster status can be stuck in "Configuring Storage" after

adding a new node.

Fixed health package registration, removing duplicate artifact creation.

Fixed a bug that sometimes caused health blades in the operator portal to become

unavailable.

Fixed a bug in which BCDR runner logs filled up MASLogs folders on physical

hosts.

Added monitoring of WMIProvider health and remediation.

Added Network Controller IMOS size check to Test-AzureStack.

Fixed a bug in SSL certificate validation during internal secret rotation.

Fixed process watchdog memory leaks.

Updated Defender platform to version 4.18.2103.7.

Enabled the alert module for customers depending on Syslog for alerts. The

services will continue to emit alerts to the Syslog pipeline.

To apply this hotfix, you must have version 1.2102.28.82 or later.

Download the following files. Then, follow the instructions in Apply updates in Azure

Stack to apply this update.

Download the zip file now .

Download the hotfix xml file now .

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

Hotfix information

） Important

As outlined in the release notes for the 2102 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

More information

Azure Stack Hub hotfix 1.2008.40.156

Article • 09/21/2022

Added graphs to Storage area that show volume performance.

Improved Datapruner processing to minimize actor timeout alerts.

Improved auto-remediation workflow for memory utilization.

Addressed an issue in the Reset-CloudAdminPassword cmdlet.

Updated Network Controller to fix bugs in PA VIP allocation and IP-MAC leaks.

Improved resiliency of PEP startup script.

Improved performance when querying for usage data.

Improved resiliency of compute admin operations.

Removed overly verbose logging from Software Load Balancer VMs.

Fixed a trust relationship issue for container applications in FabricRing.

Added banner to warn users when a certificate will expire soon.

Improved reliability of update from 2008 to 2102.

Improved reliability of update from 2005 to 2008.

Improved RdAgent availability by removing empty RdAgent files.

Fix for more ghost NIC scenarios when deleting a resource group.

Fixed an issue that, in rare cases, deleted VNet peerings.

ETW trace sessions are configured to use 16 MB of non-pagedpool memory. Trace

sessions now report lost event count (if any) per session, during ETL file rotation in

TraceCollector Eventlog. This releases critical non-paged pool memory for other

services on hosts and VMs. Also fixed various bugs in Tracecollector.

Fixed a bug in resource provider (for example, Event Hubs) deployment, update, or

secret rotation. The operation previously failed with no apparent failure cause. The

fix allows the operation to complete successfully.

Extended the update readiness checks to cover more Service Fabric health and VM

health checks; for example, memory usage and storage disk capacity checks.

Fixed bugs that increased memory pressure on infrastructure.

Fixed bugs that caused operator portal blades to fail to load.

Improved reliability of Process Watchdog.

Improved update reliability by adding detection and self-healing for low available

memory conditions on ERCS VMs at the beginning of the update orchestration.

Summary

Fixes rolled up from previous hotfix releases

Fixed a bug in which BCDR runner logs fill up MASLogs folders on physical hosts.

Added monitoring for WMI and remediation.

Added Network Controller IMOS size check to Test-AzureStack.

Fixed internal secret rotation failures (failing at the NC:Secret rotate step), seen

after updating to Azure Stack Hub version 1.2008.25.114 or higher from the latest

2005 release.

Configured stamp ADFS to monitor corporate ADFS signing certificate rollover.

This is for Azure Stack Hub with ADFS identity systems when Azure Stack Hub is

configured with corp ADFS and a federation metadata endpoint.

Fixed alert to remediation linking. Moved memory-critical alert to preview.

Fixed health package registration, removing duplicate artifact creation.

Improved reliability of RdAgent upgrade.

Enhanced idempotent logic in handling malfunctioning TPMs.

Fixed an issue in which uninstalling some extensions put previously deployed

extensions into a failed state.

Fixed an issue in which duplicate installed updates were shown in the update

history list.

Fixed an intermittent issue in which FRU of SRNG could fail connecting to the ECE

agent.

Fixed VM NICs getting a different hardware identifier after VM is deallocated and

restarted.

Monitored and rebooted VMs based on memory pressure.

Added AzsGBRReadiness in Test-AzureStack to check physical disks' health for

granular bitmap repair readiness.

Reactivated firewall rules to enable SNMP traffic on ERCS VMs.

Fixed an issue in which modifying any properties on the Local Network Gateway

was causing other VPN connections on that gateway to disconnect.

Fixed an issue in which infrastructure VM deployment can fail after applying a

hotfix.

Cleaned up stale user profile folders to clear disk space.

Fixed an issue in which a secondary blob data partition cannot be loaded in some

error cases.

Fixed some bugs with the use of temporary domain accounts.

Enhanced temporary domain account naming to ensure uniqueness.

Patched SDN-related binaries on the physical nodes.

Improved reliability and diagnosing capabilities of patch and update.

Added auto-remediation for SQL cluster.

Updated Healthagent to use Nugetstore.

Filtered WHS alert for Netadapter.

Fixed an issue in which the copy of a certificate used by Service Fabric was

overwritten.

Fixed appearance of ghost NICs when deleting a resource group.

Fixed regression in Test-AzureStack that caused VM deployment test case to

automatically skip.

Improved resiliency of VM provisioning, extension, and image operations.

Fixed an invalid state in Storage resource provider for storage accounts migrated

from 1910 with suspended state.

Fixed a bug in local health system that potentially increased memory pressure on

infrastructure.

Fixed issue in internal secret rotation that would fail with a timeout error if valueadd resource providers were unhealthy.

Fixed a bug in which closed alerts' Last Modified Time was updated in the

operator portal even if the alert stayed closed.

Optimized operator alert request handling, which reduces the chance of timeouts

when viewing alerts in the operator portal or monitoring them via System Center

Operations Manager (SCOM).

Check and enforce key protectors on cluster shared volumes per host.

Fixed issue in which Managed Disk usage data was not being reported after the

2008 update.

Fixed VMs losing connectivity while SuspendNode is occurring in MAS, as part of

host reboot during patch and update.

Added PEP to retrieve current registration details, stale object cleanup for

Remove-Registration.

Fixed a bug that caused the Infrastructure Roles panel in the operator portal to

display incorrect health information.

Improved reliability of log collection for SDN roles by collecting logs on the file

share.

Fixed an issue that can raise an audit scanner health alert in PEP cmdlet.

Removed invalid repair interface for seedringservices.

Improved SDN network reliability on the physical nodes.

Enabled SQL container logs.

Fixed an issue that erroneously raises an alert: "Node inaccessible for VM

Placement."

Fixed a remote management enabling issue for Azure Stack registrations done

prior to 1910 release.

Improved reliability of host node update.

Critical fix for disk space exhaustion on physical hosts, network controllers,

gateways, and load balancers.

Fixed remote management resource replication for resource arrays with

continuation token.

Fixed an issue in which a storage account might be partially restored due to a KVS

race condition in the SRP background usage job.

Fixed an issue in which a virtual subnet was not being cleaned up if the tunnel was

moved to a different GW VM and then the VGW was deleted.

Fixed an issue that could cause registration and internal secret rotation to fail.

Fixed an issue in the internal secret rotation, which might cause a failure in the next

update.

Addressed an issue with internal secret rotation for NRP with a large number of

subscriptions.

Mitigated connection problems to ERCS following startup.

Mitigated a potential issue with upgrading to future versions.

Addressed memory leak based on health runners and suppressed faulty alerts.

Added memory-specific settings to crash dump settings.

Remediated ERCS memory pressure during patch & update.

Included AzsInfraRoleSummary Test-Azurestack test as UpdateReadiness.

Fixed an issue where certificate rotation on IoT Hub fails with "Internal execution

error."

To apply this hotfix, you must have version 1.2008.13.88 or later.

Download the following files. Then, follow the instructions in Apply updates in Azure

Stack to apply this update.

Download the zip file now .

Download the hotfix xml file now .

Hotfix information

） Important

As outlined in the release notes for the 2008 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

More information

Azure Stack Hub hotfix 1.2102.30.116

Article • 09/21/2022

Add retry for get-volume requests in Test-AzureStack infra capacity check.

Shortened the PEP tokens and made them human-readable.

Fixed a bug related to physical disk health when repairing a node with SED drives.

Improved Datapruner processing to minimize actor timeout alerts.

Enabled rotation of health agent SSL certificate as part of internal secret rotation.

Added graphs to Storage area that show volume performance.

Improved logic for incremental snapshot creation and deletion.

Improved resiliency in PEP startup script.

Fixed an issue in which System Center Operations Manager (SCOM) was unable to

close operator portal alerts.

Improved auto-remediation workflow for memory utilization.

Improved incremental snapshot creation and deletion.

Addressed an issue in the Reset-CloudAdminPassword cmdlet.

Updated Network Controller to fix bugs in PA VIP allocation and IP-MAC leaks.

Improved performance when querying for usage data.

Improved resiliency of compute admin operations.

Removed overly verbose logging from Software Load Balancer VMs.

Fixed a memory leak issue and improved memory efficiency for monitoring

services.

Fixed an issue in which the backup blade showed a "rainy" page when backup

share was inaccessible.

Fixed an issue that prevented transcript collection when closing Privileged

Endpoint (PEP) session.

Fixed a multi-tenancy website security issue.

Improved reliability of update from 2008 to 2102.

Fix for adding availability set to SQL VM in the SQL VM creation process.

Fix for setting storage size in SQL VM configuration to more than 1000 GB.

Fixed group-based authorization errors for users that require group expansion.

Newer API version support for Key Vault resource provider. The Key Vault control

plane supports the 2019-09-01 API version, and the Key Vault data plane supports

Summary

Fixes rolled up from previous hotfix releases

API version 7.1.

Added banner to warn users when a certificate will expire soon.

Fix to show accurate status of node in portal if a repair operation on it has failed.

ETW trace sessions are configured to use 16 MB of non-pagedpool memory. Trace

sessions now report lost event count (if any) per session, during ETL file rotation in

TraceCollector Eventlog. This releases critical non-paged pool memory for other

services on hosts and VMs. Also fixed various bugs in Tracecollector.

Fixed bugs that increased memory pressure on infrastructure.

Fixed bugs in AD FS and Azure Stack Graph to improve deployment and upgrade

reliability.

Fixed bugs in SRP and DiskRP in which performance counters were missing in the

WAC client.

Fixed a bug in resource provider (for example, Event Hubs) deployment, update, or

secret rotation. The operation previously failed with no apparent failure cause. The

fix allows the operation to complete successfully.

Fixed a bug that incorrectly raised a PnPDevice.Attached alert for a set of devices

(mouse, keyboard, etc.) that were safe.

Set memory alert to preview.

Addressed an issue with host agent monitors.

Fixed a trust relationship issue with container applications in FabricRing.

Improved RdAgent availability by removing empty RdAgent files.

Improved reliability of full update.

Extended the update readiness checks to cover more Service Fabric health and VM

health checks; for example, memory usage and storage disk capacity checks.

Updated memory configuration for VM sizes Standard\_NC16as\_T4\_v3 and

Standard\_NC64as\_T4\_v3.

Removed legacy SRP SQL instances and DB files to free up stamp resources.

Fixed a bug in which the cluster status can be stuck in "Configuring Storage" after

adding a new node.

Fixed health package registration, removing duplicate artifact creation.

Fixed a bug that sometimes caused health blades in the operator portal to become

unavailable.

Fixed a bug in which BCDR runner logs filled up MASLogs folders on physical

hosts.

Added monitoring of WMIProvider health and remediation.

Added Network Controller IMOS size check to Test-AzureStack.

Fixed a bug in SSL certificate validation during internal secret rotation.

Fixed process watchdog memory leaks.

Updated Defender platform to version 4.18.2103.7.

Enabled the alert module for customers depending on Syslog for alerts. The

services will continue to emit alerts to the Syslog pipeline.

To apply this hotfix, you must have version 1.2102.28.82 or later.

Download the following files. Then, follow the instructions in Apply updates in Azure

Stack to apply this update.

Download the zip file now .

Download the hotfix xml file now .

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

Hotfix information

） Important

As outlined in the release notes for the 2102 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

More information

Azure Stack Hub hotfix 1.2102.30.109

Article • 09/21/2022

Improved logic for incremental snapshot creation and deletion.

Improved resiliency in PEP startup script.

Fixed an issue in which System Center Operations Manager (SCOM) was unable to

close operator portal alerts.

Improved auto-remediation workflow for memory utilization.

Improved incremental snapshot creation and deletion.

Addressed an issue in the Reset-CloudAdminPassword cmdlet.

Updated Network Controller to fix bugs in PA VIP allocation and IP-MAC leaks.

Improved performance when querying for usage data.

Improved resiliency of compute admin operations.

Removed overly verbose logging from Software Load Balancer VMs.

Fixed a memory leak issue and improved memory efficiency for monitoring

services.

Fixed an issue in which the backup blade showed a "rainy" page when backup

share was inaccessible.

Fixed an issue that prevented transcript collection when closing Privileged

Endpoint (PEP) session.

Fixed a multi-tenancy website security issue.

Improved reliability of update from 2008 to 2102.

Fix for adding availability set to SQL VM in the SQL VM creation process.

Fix for setting storage size in SQL VM configuration to more than 1000 GB.

Fixed group-based authorization errors for users that require group expansion.

Newer API version support for Key Vault resource provider. The Key Vault control

plane supports the 2019-09-01 API version, and the Key Vault data plane supports

API version 7.1.

Added banner to warn users when a certificate will expire soon.

Fix to show accurate status of node in portal if a repair operation on it has failed.

ETW trace sessions are configured to use 16 MB of non-pagedpool memory. Trace

sessions now report lost event count (if any) per session, during ETL file rotation in

Summary

Fixes rolled up from previous hotfix releases

TraceCollector Eventlog. This releases critical non-paged pool memory for other

services on hosts and VMs. Also fixed various bugs in Tracecollector.

Fixed bugs that increased memory pressure on infrastructure.

Fixed bugs in AD FS and Azure Stack Graph to improve deployment and upgrade

reliability.

Fixed bugs in SRP and DiskRP in which performance counters were missing in the

WAC client.

Fixed a bug in resource provider (for example, Event Hubs) deployment, update, or

secret rotation. The operation previously failed with no apparent failure cause. The

fix allows the operation to complete successfully.

Fixed a bug that incorrectly raised a PnPDevice.Attached alert for a set of devices

(mouse, keyboard, etc.) that were safe.

Set memory alert to preview.

Addressed an issue with host agent monitors.

Fixed a trust relationship issue with container applications in FabricRing.

Improved RdAgent availability by removing empty RdAgent files.

Improved reliability of full update.

Extended the update readiness checks to cover more Service Fabric health and VM

health checks; for example, memory usage and storage disk capacity checks.

Updated memory configuration for VM sizes Standard\_NC16as\_T4\_v3 and

Standard\_NC64as\_T4\_v3.

Removed legacy SRP SQL instances and DB files to free up stamp resources.

Fixed a bug in which the cluster status can be stuck in "Configuring Storage" after

adding a new node.

Fixed health package registration, removing duplicate artifact creation.

Fixed a bug that sometimes caused health blades in the operator portal to become

unavailable.

Fixed a bug in which BCDR runner logs filled up MASLogs folders on physical

hosts.

Added monitoring of WMIProvider health and remediation.

Added Network Controller IMOS size check to Test-AzureStack.

Fixed a bug in SSL certificate validation during internal secret rotation.

Fixed process watchdog memory leaks.

Updated Defender platform to version 4.18.2103.7.

Enabled the alert module for customers depending on Syslog for alerts. The

services will continue to emit alerts to the Syslog pipeline.

To apply this hotfix, you must have version 1.2102.28.82 or later.

Hotfix information

Download the following files. Then, follow the instructions in Apply updates in Azure

Stack to apply this update.

Download the zip file now .

Download the hotfix xml file now .

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

） Important

As outlined in the release notes for the 2102 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

More information

Azure Stack Hub hotfix 1.2102.30.106

Article • 09/21/2022

Fixed an issue in which System Center Operations Manager (SCOM) was unable to

close operator portal alerts.

Improved auto-remediation workflow for memory utilization.

Improved incremental snapshot creation and deletion.

Addressed an issue in the Reset-CloudAdminPassword cmdlet.

Updated Network Controller to fix bugs in PA VIP allocation and IP-MAC leaks.

Improved performance when querying for usage data.

Improved resiliency of compute admin operations.

Removed overly verbose logging from Software Load Balancer VMs.

Fixed a memory leak issue and improved memory efficiency for monitoring

services.

Fixed an issue in which the backup blade showed a "rainy" page when backup

share was inaccessible.

Fixed an issue that prevented transcript collection when closing Privileged

Endpoint (PEP) session.

Fixed a multi-tenancy website security issue.

Improved reliability of update from 2008 to 2102.

Fix for adding availability set to SQL VM in the SQL VM creation process.

Fix for setting storage size in SQL VM configuration to more than 1000 GB.

Fixed group-based authorization errors for users that require group expansion.

Newer API version support for Key Vault resource provider. The Key Vault control

plane supports the 2019-09-01 API version, and the Key Vault data plane supports

API version 7.1.

Added banner to warn users when a certificate will expire soon.

Fix to show accurate status of node in portal if a repair operation on it has failed.

ETW trace sessions are configured to use 16 MB of non-pagedpool memory. Trace

sessions now report lost event count (if any) per session, during ETL file rotation in

TraceCollector Eventlog. This releases critical non-paged pool memory for other

services on hosts and VMs. Also fixed various bugs in Tracecollector.

Fixed bugs that increased memory pressure on infrastructure.

Summary

Fixes rolled up from previous hotfix releases

Fixed bugs in AD FS and Azure Stack Graph to improve deployment and upgrade

reliability.

Fixed bugs in SRP and DiskRP in which performance counters were missing in the

WAC client.

Fixed a bug in resource provider (for example, Event Hubs) deployment, update, or

secret rotation. The operation previously failed with no apparent failure cause. The

fix allows the operation to complete successfully.

Fixed a bug that incorrectly raised a PnPDevice.Attached alert for a set of devices

(mouse, keyboard, etc.) that were safe.

Set memory alert to preview.

Addressed an issue with host agent monitors.

Fixed a trust relationship issue with container applications in FabricRing.

Improved RdAgent availability by removing empty RdAgent files.

Improved reliability of full update.

Extended the update readiness checks to cover more Service Fabric health and VM

health checks; for example, memory usage and storage disk capacity checks.

Updated memory configuration for VM sizes Standard\_NC16as\_T4\_v3 and

Standard\_NC64as\_T4\_v3.

Removed legacy SRP SQL instances and DB files to free up stamp resources.

Fixed a bug in which the cluster status can be stuck in "Configuring Storage" after

adding a new node.

Fixed health package registration, removing duplicate artifact creation.

Fixed a bug that sometimes caused health blades in the operator portal to become

unavailable.

Fixed a bug in which BCDR runner logs filled up MASLogs folders on physical

hosts.

Added monitoring of WMIProvider health and remediation.

Added Network Controller IMOS size check to Test-AzureStack.

Fixed a bug in SSL certificate validation during internal secret rotation.

Fixed process watchdog memory leaks.

Updated Defender platform to version 4.18.2103.7.

Enabled the alert module for customers depending on Syslog for alerts. The

services will continue to emit alerts to the Syslog pipeline.

To apply this hotfix, you must have version 1.2102.28.82 or later.

Hotfix information

） Important

Download the following files. Then, follow the instructions in Apply updates in Azure

Stack to apply this update.

Download the zip file now .

Download the hotfix xml file now .

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

As outlined in the release notes for the 2102 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

More information

Azure Stack Hub hotfix 1.2102.30.104

Article • 09/21/2022

Improved auto-remediation workflow for memory utilization.

Improved incremental snapshot creation and deletion.

Addressed an issue in the Reset-CloudAdminPassword cmdlet.

Updated Network Controller to fix bugs in PA VIP allocation and IP-MAC leaks.

Improved performance when querying for usage data.

Improved resiliency of compute admin operations.

Removed overly verbose logging from Software Load Balancer VMs.

Fixed a memory leak issue and improved memory efficiency for monitoring

services.

Fixed an issue in which the backup blade showed a "rainy" page when backup

share was inaccessible.

Fixed an issue that prevented transcript collection when closing Privileged

Endpoint (PEP) session.

Fixed a multi-tenancy website security issue.

Improved reliability of update from 2008 to 2102.

Fix for adding availability set to SQL VM in the SQL VM creation process.

Fix for setting storage size in SQL VM configuration to more than 1000 GB.

Fixed group-based authorization errors for users that require group expansion.

Newer API version support for Key Vault resource provider. The Key Vault control

plane supports the 2019-09-01 API version, and the Key Vault data plane supports

API version 7.1.

Added banner to warn users when a certificate will expire soon.

Fix to show accurate status of node in portal if a repair operation on it has failed.

ETW trace sessions are configured to use 16 MB of non-pagedpool memory. Trace

sessions now report lost event count (if any) per session, during ETL file rotation in

TraceCollector Eventlog. This releases critical non-paged pool memory for other

services on hosts and VMs. Also fixed various bugs in Tracecollector.

Fixed bugs that increased memory pressure on infrastructure.

Fixed bugs in AD FS and Azure Stack Graph to improve deployment and upgrade

reliability.

Summary

Fixes rolled up from previous hotfix releases

Fixed bugs in SRP and DiskRP in which performance counters were missing in the

WAC client.

Fixed a bug in resource provider (for example, Event Hubs) deployment, update, or

secret rotation. The operation previously failed with no apparent failure cause. The

fix allows the operation to complete successfully.

Fixed a bug that incorrectly raised a PnPDevice.Attached alert for a set of devices

(mouse, keyboard, etc.) that were safe.

Set memory alert to preview.

Addressed an issue with host agent monitors.

Fixed a trust relationship issue with container applications in FabricRing.

Improved RdAgent availability by removing empty RdAgent files.

Improved reliability of full update.

Extended the update readiness checks to cover more Service Fabric health and VM

health checks; for example, memory usage and storage disk capacity checks.

Updated memory configuration for VM sizes Standard\_NC16as\_T4\_v3 and

Standard\_NC64as\_T4\_v3.

Removed legacy SRP SQL instances and DB files to free up stamp resources.

Fixed a bug in which the cluster status can be stuck in "Configuring Storage" after

adding a new node.

Fixed health package registration, removing duplicate artifact creation.

Fixed a bug that sometimes caused health blades in the operator portal to become

unavailable.

Fixed a bug in which BCDR runner logs filled up MASLogs folders on physical

hosts.

Added monitoring of WMIProvider health and remediation.

Added Network Controller IMOS size check to Test-AzureStack.

Fixed a bug in SSL certificate validation during internal secret rotation.

Fixed process watchdog memory leaks.

Updated Defender platform to version 4.18.2103.7.

Enabled the alert module for customers depending on Syslog for alerts. The

services will continue to emit alerts to the Syslog pipeline.

To apply this hotfix, you must have version 1.2102.28.82 or later.

Hotfix information

） Important

As outlined in the release notes for the 2102 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

Download the following files. Then, follow the instructions in Apply updates in Azure

Stack to apply this update.

Download the zip file now .

Download the hotfix xml file now .

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

More information

Azure Stack Hub hotfix 1.2008.40.154

Article • 09/21/2022

Improved auto-remediation workflow for memory utilization.

Addressed an issue in the Reset-CloudAdminPassword cmdlet.

Updated Network Controller to fix bugs in PA VIP allocation and IP-MAC leaks.

Improved resiliency of PEP startup script.

Improved performance when querying for usage data.

Improved resiliency of compute admin operations.

Removed overly verbose logging from Software Load Balancer VMs.

Fixed a trust relationship issue for container applications in FabricRing.

Added banner to warn users when a certificate will expire soon.

Improved reliability of update from 2008 to 2102.

Improved reliability of update from 2005 to 2008.

Improved RdAgent availability by removing empty RdAgent files.

Fix for more ghost NIC scenarios when deleting a resource group.

Fixed an issue that, in rare cases, deleted VNet peerings.

ETW trace sessions are configured to use 16 MB of non-pagedpool memory. Trace

sessions now report lost event count (if any) per session, during ETL file rotation in

TraceCollector Eventlog. This releases critical non-paged pool memory for other

services on hosts and VMs. Also fixed various bugs in Tracecollector.

Fixed a bug in resource provider (for example, Event Hubs) deployment, update, or

secret rotation. The operation previously failed with no apparent failure cause. The

fix allows the operation to complete successfully.

Extended the update readiness checks to cover more Service Fabric health and VM

health checks; for example, memory usage and storage disk capacity checks.

Fixed bugs that increased memory pressure on infrastructure.

Fixed bugs that caused operator portal blades to fail to load.

Improved reliability of Process Watchdog.

Improved update reliability by adding detection and self-healing for low available

memory conditions on ERCS VMs at the beginning of the update orchestration.

Fixed a bug in which BCDR runner logs fill up MASLogs folders on physical hosts.

Added monitoring for WMI and remediation.

Summary

Fixes rolled up from previous hotfix releases

Added Network Controller IMOS size check to Test-AzureStack.

Fixed internal secret rotation failures (failing at the NC:Secret rotate step), seen

after updating to Azure Stack Hub version 1.2008.25.114 or higher from the latest

2005 release.

Configured stamp ADFS to monitor corporate ADFS signing certificate rollover.

This is for Azure Stack Hub with ADFS identity systems when Azure Stack Hub is

configured with corp ADFS and a federation metadata endpoint.

Fixed alert to remediation linking. Moved memory-critical alert to preview.

Fixed health package registration, removing duplicate artifact creation.

Improved reliability of RdAgent upgrade.

Enhanced idempotent logic in handling malfunctioning TPMs.

Fixed an issue in which uninstalling some extensions put previously deployed

extensions into a failed state.

Fixed an issue in which duplicate installed updates were shown in the update

history list.

Fixed an intermittent issue in which FRU of SRNG could fail connecting to the ECE

agent.

Fixed VM NICs getting a different hardware identifier after VM is deallocated and

restarted.

Monitored and rebooted VMs based on memory pressure.

Added AzsGBRReadiness in Test-AzureStack to check physical disks' health for

granular bitmap repair readiness.

Reactivated firewall rules to enable SNMP traffic on ERCS VMs.

Fixed an issue in which modifying any properties on the Local Network Gateway

was causing other VPN connections on that gateway to disconnect.

Fixed an issue in which infrastructure VM deployment can fail after applying a

hotfix.

Cleaned up stale user profile folders to clear disk space.

Fixed an issue in which a secondary blob data partition cannot be loaded in some

error cases.

Fixed some bugs with the use of temporary domain accounts.

Enhanced temporary domain account naming to ensure uniqueness.

Patched SDN-related binaries on the physical nodes.

Improved reliability and diagnosing capabilities of patch and update.

Added auto-remediation for SQL cluster.

Updated Healthagent to use Nugetstore.

Filtered WHS alert for Netadapter.

Fixed an issue in which the copy of a certificate used by Service Fabric was

overwritten.

Fixed appearance of ghost NICs when deleting a resource group.

Fixed regression in Test-AzureStack that caused VM deployment test case to

automatically skip.

Improved resiliency of VM provisioning, extension, and image operations.

Fixed an invalid state in Storage resource provider for storage accounts migrated

from 1910 with suspended state.

Fixed a bug in local health system that potentially increased memory pressure on

infrastructure.

Fixed issue in internal secret rotation that would fail with a timeout error if valueadd resource providers were unhealthy.

Fixed a bug in which closed alerts' Last Modified Time was updated in the

operator portal even if the alert stayed closed.

Optimized operator alert request handling, which reduces the chance of timeouts

when viewing alerts in the operator portal or monitoring them via System Center

Operations Manager (SCOM).

Check and enforce key protectors on cluster shared volumes per host.

Fixed issue in which Managed Disk usage data was not being reported after the

2008 update.

Fixed VMs losing connectivity while SuspendNode is occurring in MAS, as part of

host reboot during patch and update.

Added PEP to retrieve current registration details, stale object cleanup for

Remove-Registration.

Fixed a bug that caused the Infrastructure Roles panel in the operator portal to

display incorrect health information.

Improved reliability of log collection for SDN roles by collecting logs on the file

share.

Fixed an issue that can raise an audit scanner health alert in PEP cmdlet.

Removed invalid repair interface for seedringservices.

Improved SDN network reliability on the physical nodes.

Enabled SQL container logs.

Fixed an issue that erroneously raises an alert: "Node inaccessible for VM

Placement."

Fixed a remote management enabling issue for Azure Stack registrations done

prior to 1910 release.

Improved reliability of host node update.

Critical fix for disk space exhaustion on physical hosts, network controllers,

gateways, and load balancers.

Fixed remote management resource replication for resource arrays with

continuation token.

Fixed an issue in which a storage account might be partially restored due to a KVS

race condition in the SRP background usage job.

Fixed an issue in which a virtual subnet was not being cleaned up if the tunnel was

moved to a different GW VM and then the VGW was deleted.

Fixed an issue that could cause registration and internal secret rotation to fail.

Fixed an issue in the internal secret rotation, which might cause a failure in the next

update.

Addressed an issue with internal secret rotation for NRP with a large number of

subscriptions.

Mitigated connection problems to ERCS following startup.

Mitigated a potential issue with upgrading to future versions.

Addressed memory leak based on health runners and suppressed faulty alerts.

Added memory-specific settings to crash dump settings.

Remediated ERCS memory pressure during patch & update.

Included AzsInfraRoleSummary Test-Azurestack test as UpdateReadiness.

Fixed an issue where certificate rotation on IoT Hub fails with "Internal execution

error."

To apply this hotfix, you must have version 1.2008.13.88 or later.

Download the following files. Then, follow the instructions in Apply updates in Azure

Stack to apply this update.

Download the zip file now .

Download the hotfix xml file now .

Azure Stack Hub update resources

Hotfix information

） Important

As outlined in the release notes for the 2008 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

More information

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

Azure Stack Hub hotfix 1.2005.48.137

Article • 09/21/2022

Addressed an issue in the Reset-CloudAdminPassword cmdlet.

Updated Network Controller to fix bugs in PA VIP allocation and IP-MAC leaks.

Removed overly verbose logging from Software Load Balancer VMs.

Fix for more ghost NIC scenarios when deleting a resource group.

Added banner to warn users when a certificate will expire soon.

Fix for more ghost NIC scenarios when deleting a resource group.

Fixed an issue that, in rare cases, deleted VNet peerings.

Improved RdAgent availability by removing empty RdAgent files.

Improved reliability of update from 2005 to 2008.

Accounted for some ghost NIC scenarios when deleting a resource group.

Improved reliability of process watchdog.

Fixed bugs that increased memory pressure on infrastructure.

Patched missing Hyper-V endpoint, enabling compute control plane operations to

call the appropriate endpoint.

Fixed a bug in which BCDR runner logs filled up MASLogs folders on physical

hosts.

Added monitoring for WMI and remediation.

Enhanced idempotent logic in handling malfunctioning TPMs.

Fixed an issue in which uninstalling some extensions put previously deployed

extensions into a failed state.

Fixed an issue in which partner node certificates required by nchostagent might be

deleted.

Fixed VM NICs getting a different hardware identifier after VM is deallocated and

restarted.

Fixed an issue in which infrastructure VM deployment can fail after applying a

hotfix.

Fixed an issue in which a secondary blob data partition cannot be loaded in some

error cases.

Fixed a bug in local health system that potentially increased memory pressure on

infrastructure.

Summary

Fixes rolled up from previous hotfix releases

Patched SDN-related binaries on the physical nodes.

Fixed an invalid state in Storage resource provider for storage accounts migrated

from 1910 with suspended state.

Improved resiliency of VM provisioning, extension, and image operations.

Added PEP to retrieve current registration details, stale object cleanup for

Remove-Registration.

Improved reliability of log collection for SDN roles by collecting on file share.

Fixed an issue that erroneously raises an alert: "Node inaccessible for VM

Placement."

Removed invalid repair interface for seedringservices.

Improved SDN network reliability on the physical nodes.

Disabled winrm runner

Fixed a bug check and enforced external key protectors on cluster shared volumes.

Fixed an issue in which a storage account might be partially restored due to a KVS

race condition in the SRP background usage job.

Fixed an issue in which a virtual subnet was not being cleaned up if the tunnel was

moved to a different GW VM and then the VGW was deleted.

Fixed an issue that could cause registration and internal secret rotation to fail.

Fixed an issue in the internal secret rotation, which might cause a failure in the next

update.

Added memory-specific settings to crash dump settings.

Restarted SQL VMs to mitigate potential issue with database access that affected

access to portal.

Remediated SMB handle invalidation issue triggered by ESENT error 59 event in

TableServer.

Included AzsInfraRoleSummary Test-Azurestack test as UpdateReadiness.

Remediated ERCS memory pressure during patch & update.

Include deployment provider identity certificate into the internal secret rotation.

Improved Network Controller stability.

Increased Network Controller log retention to aid in diagnosis.

Added Get-NetView as a part of Get-AzureStackLog collection by default.

Fixed an issue where marketplace downloads could fail due to a certificate

validation error.

Improved HealthAgent binary switchover logic.

Improved cluster shared volumes rebalance after Patch & Update (PnU).

Used ADSI to fetch localgroup members in HealthAgent.

Added the missing records, when WASP VMs fail to synchronize records and zones

by using DNS cmdlet during scale in and scale out.

Improved storage service reliability during PnU.

Removed public IP quota validation that caused an issue when creating an internal

load balancer.

Improved reliability of VM deletion: ensure new VMs that could not be fully

created or added to the cluster are deleted.

Check and enforce key protectors on cluster shared volumes.

Fixed "access denied" issue causing update and admin operations to fail.

Fixed WhsFaultScanner to re-launch when it gets stuck to make sure alerts are

correctly generated for users.

Fixed orchestration bug that prevented storage regeneration telemetry events

from being emitted.

Fixed an issue which impacted the reliability of downloading subsequent updates.

Improved ability to diagnose failures based on orchestrator telemetry.

Fixed SRP race condition in moving system storage accounts to system internal

subscription during 2005 PnU.

Fixed time unit scaling error in the server latency metrics

Restarted SQL VMs to mitigate potential issue with database access that affected

access to portal.

Fixed an issue in which the configuration of the retention period for deleted

storage accounts was reverted.

Improved reliability of storage blob and table service.

Addressed issue in the Send-AzureStackDiagnosticLog PEP cmdlet.

Increased the HRP repair time when an update failure occurs.

To apply this hotfix, you must have version 1.2005.6.53 or later.

Download the following files. Then, follow the instructions in Apply updates in Azure

Stack to apply this update.

Download the zip file now .

Hotfix information

） Important

As outlined in the release notes for the 2005 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

Download the hotfix xml file now .

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

More information

Azure Stack Hub hotfix 1.2102.30.102

Article • 09/21/2022

Improved resiliency of compute admin operations.

Removed overly verbose logging from Software Load Balancer VMs.

Fixed a memory leak issue and improved memory efficiency for monitoring

services.

Fixed an issue in which the backup blade showed a "rainy" page when backup

share was inaccessible.

Fixed an issue that prevented transcript collection when closing Privileged

Endpoint (PEP) session.

Fixed a multi-tenancy website security issue.

Improved reliability of update from 2008 to 2102.

Fix for adding availability set to SQL VM in the SQL VM creation process.

Fix for setting storage size in SQL VM configuration to more than 1000 GB.

Fixed group-based authorization errors for users that require group expansion.

Newer API version support for Key Vault resource provider. The Key Vault control

plane supports the 2019-09-01 API version, and the Key Vault data plane supports

API version 7.1.

Added banner to warn users when a certificate will expire soon.

Fix to show accurate status of node in portal if a repair operation on it has failed.

ETW trace sessions are configured to use 16 MB of non-pagedpool memory. Trace

sessions now report lost event count (if any) per session, during ETL file rotation in

TraceCollector Eventlog. This releases critical non-paged pool memory for other

services on hosts and VMs. Also fixed various bugs in Tracecollector.

Fixed bugs that increased memory pressure on infrastructure.

Fixed bugs in AD FS and Azure Stack Graph to improve deployment and upgrade

reliability.

Fixed bugs in SRP and DiskRP in which performance counters were missing in the

WAC client.

Fixed a bug in resource provider (for example, Event Hubs) deployment, update, or

secret rotation. The operation previously failed with no apparent failure cause. The

fix allows the operation to complete successfully.

Summary

Fixes rolled up from previous hotfix releases

Fixed a bug that incorrectly raised a PnPDevice.Attached alert for a set of devices

(mouse, keyboard, etc.) that were safe.

Set memory alert to preview.

Addressed an issue with host agent monitors.

Fixed a trust relationship issue with container applications in FabricRing.

Improved RdAgent availability by removing empty RdAgent files.

Improved reliability of full update.

Extended the update readiness checks to cover more Service Fabric health and VM

health checks; for example, memory usage and storage disk capacity checks.

Updated memory configuration for VM sizes Standard\_NC16as\_T4\_v3 and

Standard\_NC64as\_T4\_v3.

Removed legacy SRP SQL instances and DB files to free up stamp resources.

Fixed a bug in which the cluster status can be stuck in "Configuring Storage" after

adding a new node.

Fixed health package registration, removing duplicate artifact creation.

Fixed a bug that sometimes caused health blades in the operator portal to become

unavailable.

Fixed a bug in which BCDR runner logs filled up MASLogs folders on physical

hosts.

Added monitoring of WMIProvider health and remediation.

Added Network Controller IMOS size check to Test-AzureStack.

Fixed a bug in SSL certificate validation during internal secret rotation.

Fixed process watchdog memory leaks.

Updated Defender platform to version 4.18.2103.7.

Enabled the alert module for customers depending on Syslog for alerts. The

services will continue to emit alerts to the Syslog pipeline.

To apply this hotfix, you must have version 1.2102.28.82 or later.

Hotfix information

） Important

As outlined in the release notes for the 2102 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

Download the following files. Then, follow the instructions in Apply updates in Azure

Stack to apply this update.

Download the zip file now .

Download the hotfix xml file now .

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

More information

Azure Stack Hub hotfix 1.2008.40.151

Article • 09/21/2022

Improved resiliency of compute admin operations.

Removed overly verbose logging from Software Load Balancer VMs.

Fixed a trust relationship issue for container applications in FabricRing.

Added banner to warn users when a certificate will expire soon.

Improved reliability of update from 2008 to 2102.

Improved reliability of update from 2005 to 2008.

Improved RdAgent availability by removing empty RdAgent files.

Fix for more ghost NIC scenarios when deleting a resource group.

Fixed an issue that, in rare cases, deleted VNet peerings.

ETW trace sessions are configured to use 16 MB of non-pagedpool memory. Trace

sessions now report lost event count (if any) per session, during ETL file rotation in

TraceCollector Eventlog. This releases critical non-paged pool memory for other

services on hosts and VMs. Also fixed various bugs in Tracecollector.

Fixed a bug in resource provider (for example, Event Hubs) deployment, update, or

secret rotation. The operation previously failed with no apparent failure cause. The

fix allows the operation to complete successfully.

Extended the update readiness checks to cover more Service Fabric health and VM

health checks; for example, memory usage and storage disk capacity checks.

Fixed bugs that increased memory pressure on infrastructure.

Fixed bugs that caused operator portal blades to fail to load.

Improved reliability of Process Watchdog.

Improved update reliability by adding detection and self-healing for low available

memory conditions on ERCS VMs at the beginning of the update orchestration.

Fixed a bug in which BCDR runner logs fill up MASLogs folders on physical hosts.

Added monitoring for WMI and remediation.

Added Network Controller IMOS size check to Test-AzureStack.

Fixed internal secret rotation failures (failing at the NC:Secret rotate step), seen

after updating to Azure Stack Hub version 1.2008.25.114 or higher from the latest

2005 release.

Summary

Fixes rolled up from previous hotfix releases

Configured stamp ADFS to monitor corporate ADFS signing certificate rollover.

This is for Azure Stack Hub with ADFS identity systems when Azure Stack Hub is

configured with corp ADFS and a federation metadata endpoint.

Fixed alert to remediation linking. Moved memory-critical alert to preview.

Fixed health package registration, removing duplicate artifact creation.

Improved reliability of RdAgent upgrade.

Enhanced idempotent logic in handling malfunctioning TPMs.

Fixed an issue in which uninstalling some extensions put previously deployed

extensions into a failed state.

Fixed an issue in which duplicate installed updates were shown in the update

history list.

Fixed an intermittent issue in which FRU of SRNG could fail connecting to the ECE

agent.

Fixed VM NICs getting a different hardware identifier after VM is deallocated and

restarted.

Monitored and rebooted VMs based on memory pressure.

Added AzsGBRReadiness in Test-AzureStack to check physical disks' health for

granular bitmap repair readiness.

Reactivated firewall rules to enable SNMP traffic on ERCS VMs.

Fixed an issue in which modifying any properties on the Local Network Gateway

was causing other VPN connections on that gateway to disconnect.

Fixed an issue in which infrastructure VM deployment can fail after applying a

hotfix.

Cleaned up stale user profile folders to clear disk space.

Fixed an issue in which a secondary blob data partition cannot be loaded in some

error cases.

Fixed some bugs with the use of temporary domain accounts.

Enhanced temporary domain account naming to ensure uniqueness.

Patched SDN-related binaries on the physical nodes.

Improved reliability and diagnosing capabilities of patch and update.

Added auto-remediation for SQL cluster.

Updated Healthagent to use Nugetstore.

Filtered WHS alert for Netadapter.

Fixed an issue in which the copy of a certificate used by Service Fabric was

overwritten.

Fixed appearance of ghost NICs when deleting a resource group.

Fixed regression in Test-AzureStack that caused VM deployment test case to

automatically skip.

Improved resiliency of VM provisioning, extension, and image operations.

Fixed an invalid state in Storage resource provider for storage accounts migrated

from 1910 with suspended state.

Fixed a bug in local health system that potentially increased memory pressure on

infrastructure.

Fixed issue in internal secret rotation that would fail with a timeout error if valueadd resource providers were unhealthy.

Fixed a bug in which closed alerts' Last Modified Time was updated in the

operator portal even if the alert stayed closed.

Optimized operator alert request handling, which reduces the chance of timeouts

when viewing alerts in the operator portal or monitoring them via System Center

Operations Manager (SCOM).

Check and enforce key protectors on cluster shared volumes per host.

Fixed issue in which Managed Disk usage data was not being reported after the

2008 update.

Fixed VMs losing connectivity while SuspendNode is occurring in MAS, as part of

host reboot during patch and update.

Added PEP to retrieve current registration details, stale object cleanup for

Remove-Registration.

Fixed a bug that caused the Infrastructure Roles panel in the operator portal to

display incorrect health information.

Improved reliability of log collection for SDN roles by collecting logs on the file

share.

Fixed an issue that can raise an audit scanner health alert in PEP cmdlet.

Removed invalid repair interface for seedringservices.

Improved SDN network reliability on the physical nodes.

Enabled SQL container logs.

Fixed an issue that erroneously raises an alert: "Node inaccessible for VM

Placement."

Fixed a remote management enabling issue for Azure Stack registrations done

prior to 1910 release.

Improved reliability of host node update.

Critical fix for disk space exhaustion on physical hosts, network controllers,

gateways, and load balancers.

Fixed remote management resource replication for resource arrays with

continuation token.

Fixed an issue in which a storage account might be partially restored due to a KVS

race condition in the SRP background usage job.

Fixed an issue in which a virtual subnet was not being cleaned up if the tunnel was

moved to a different GW VM and then the VGW was deleted.

Fixed an issue that could cause registration and internal secret rotation to fail.

Fixed an issue in the internal secret rotation, which might cause a failure in the next

update.

Addressed an issue with internal secret rotation for NRP with a large number of

subscriptions.

Mitigated connection problems to ERCS following startup.

Mitigated a potential issue with upgrading to future versions.

Addressed memory leak based on health runners and suppressed faulty alerts.

Added memory-specific settings to crash dump settings.

Remediated ERCS memory pressure during patch & update.

Included AzsInfraRoleSummary Test-Azurestack test as UpdateReadiness.

Fixed an issue where certificate rotation on IoT Hub fails with "Internal execution

error."

To apply this hotfix, you must have version 1.2008.13.88 or later.

Download the following files. Then, follow the instructions in Apply updates in Azure

Stack to apply this update.

Download the zip file now .

Download the hotfix xml file now .

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

Hotfix information

） Important

As outlined in the release notes for the 2008 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

More information

Azure Stack Hub hotfix 1.2005.47.135

Article • 09/21/2022

Removed overly verbose logging from Software Load Balancer VMs.

Fix for more ghost NIC scenarios when deleting a resource group.

Added banner to warn users when a certificate will expire soon.

Fix for more ghost NIC scenarios when deleting a resource group.

Fixed an issue that, in rare cases, deleted VNet peerings.

Improved RdAgent availability by removing empty RdAgent files.

Improved reliability of update from 2005 to 2008.

Accounted for some ghost NIC scenarios when deleting a resource group.

Improved reliability of process watchdog.

Fixed bugs that increased memory pressure on infrastructure.

Patched missing Hyper-V endpoint, enabling compute control plane operations to

call the appropriate endpoint.

Fixed a bug in which BCDR runner logs filled up MASLogs folders on physical

hosts.

Added monitoring for WMI and remediation.

Enhanced idempotent logic in handling malfunctioning TPMs.

Fixed an issue in which uninstalling some extensions put previously deployed

extensions into a failed state.

Fixed an issue in which partner node certificates required by nchostagent might be

deleted.

Fixed VM NICs getting a different hardware identifier after VM is deallocated and

restarted.

Fixed an issue in which infrastructure VM deployment can fail after applying a

hotfix.

Fixed an issue in which a secondary blob data partition cannot be loaded in some

error cases.

Fixed a bug in local health system that potentially increased memory pressure on

infrastructure.

Patched SDN-related binaries on the physical nodes.

Summary

Fixes rolled up from previous hotfix releases

Fixed an invalid state in Storage resource provider for storage accounts migrated

from 1910 with suspended state.

Improved resiliency of VM provisioning, extension, and image operations.

Added PEP to retrieve current registration details, stale object cleanup for

Remove-Registration.

Improved reliability of log collection for SDN roles by collecting on file share.

Fixed an issue that erroneously raises an alert: "Node inaccessible for VM

Placement."

Removed invalid repair interface for seedringservices.

Improved SDN network reliability on the physical nodes.

Disabled winrm runner

Fixed a bug check and enforced external key protectors on cluster shared volumes.

Fixed an issue in which a storage account might be partially restored due to a KVS

race condition in the SRP background usage job.

Fixed an issue in which a virtual subnet was not being cleaned up if the tunnel was

moved to a different GW VM and then the VGW was deleted.

Fixed an issue that could cause registration and internal secret rotation to fail.

Fixed an issue in the internal secret rotation, which might cause a failure in the next

update.

Added memory-specific settings to crash dump settings.

Restarted SQL VMs to mitigate potential issue with database access that affected

access to portal.

Remediated SMB handle invalidation issue triggered by ESENT error 59 event in

TableServer.

Included AzsInfraRoleSummary Test-Azurestack test as UpdateReadiness.

Remediated ERCS memory pressure during patch & update.

Include deployment provider identity certificate into the internal secret rotation.

Improved Network Controller stability.

Increased Network Controller log retention to aid in diagnosis.

Added Get-NetView as a part of Get-AzureStackLog collection by default.

Fixed an issue where marketplace downloads could fail due to a certificate

validation error.

Improved HealthAgent binary switchover logic.

Improved cluster shared volumes rebalance after Patch & Update (PnU).

Used ADSI to fetch localgroup members in HealthAgent.

Added the missing records, when WASP VMs fail to synchronize records and zones

by using DNS cmdlet during scale in and scale out.

Improved storage service reliability during PnU.

Removed public IP quota validation that caused an issue when creating an internal

load balancer.

Improved reliability of VM deletion: ensure new VMs that could not be fully

created or added to the cluster are deleted.

Check and enforce key protectors on cluster shared volumes.

Fixed "access denied" issue causing update and admin operations to fail.

Fixed WhsFaultScanner to re-launch when it gets stuck to make sure alerts are

correctly generated for users.

Fixed orchestration bug that prevented storage regeneration telemetry events

from being emitted.

Fixed an issue which impacted the reliability of downloading subsequent updates.

Improved ability to diagnose failures based on orchestrator telemetry.

Fixed SRP race condition in moving system storage accounts to system internal

subscription during 2005 PnU.

Fixed time unit scaling error in the server latency metrics

Restarted SQL VMs to mitigate potential issue with database access that affected

access to portal.

Fixed an issue in which the configuration of the retention period for deleted

storage accounts was reverted.

Improved reliability of storage blob and table service.

Addressed issue in the Send-AzureStackDiagnosticLog PEP cmdlet.

Increased the HRP repair time when an update failure occurs.

To apply this hotfix, you must have version 1.2005.6.53 or later.

Download the following files. Then, follow the instructions in Apply updates in Azure

Stack to apply this update.

Download the zip file now .

Download the hotfix xml file now .

Hotfix information

） Important

As outlined in the release notes for the 2005 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

More information

Azure Stack Hub hotfix 1.2102.30.101

Article • 09/21/2022

Fixed a multi-tenancy website security issue.

Improved reliability of update from 2008 to 2102.

Fix for adding availability set to SQL VM in the SQL VM creation process.

Fix for setting storage size in SQL VM configuration to more than 1000 GB.

Fixed group-based authorization errors for users that require group expansion.

Newer API version support for Key Vault resource provider. The Key Vault control

plane supports the 2019-09-01 API version, and the Key Vault data plane supports

API version 7.1.

Added banner to warn users when a certificate will expire soon.

Fix to show accurate status of node in portal if a repair operation on it has failed.

ETW trace sessions are configured to use 16 MB of non-pagedpool memory. Trace

sessions now report lost event count (if any) per session, during ETL file rotation in

TraceCollector Eventlog. This releases critical non-paged pool memory for other

services on hosts and VMs. Also fixed various bugs in Tracecollector.

Fixed bugs that increased memory pressure on infrastructure.

Fixed bugs in AD FS and Azure Stack Graph to improve deployment and upgrade

reliability.

Fixed bugs in SRP and DiskRP in which performance counters were missing in the

WAC client.

Fixed a bug in resource provider (for example, Event Hubs) deployment, update, or

secret rotation. The operation previously failed with no apparent failure cause. The

fix allows the operation to complete successfully.

Fixed a bug that incorrectly raised a PnPDevice.Attached alert for a set of devices

(mouse, keyboard, etc.) that were safe.

Set memory alert to preview.

Addressed an issue with host agent monitors.

Fixed a trust relationship issue with container applications in FabricRing.

Improved RdAgent availability by removing empty RdAgent files.

Improved reliability of full update.

Summary

Fixes rolled up from previous hotfix releases

Extended the update readiness checks to cover more Service Fabric health and VM

health checks; for example, memory usage and storage disk capacity checks.

Updated memory configuration for VM sizes Standard\_NC16as\_T4\_v3 and

Standard\_NC64as\_T4\_v3.

Removed legacy SRP SQL instances and DB files to free up stamp resources.

Fixed a bug in which the cluster status can be stuck in "Configuring Storage" after

adding a new node.

Fixed health package registration, removing duplicate artifact creation.

Fixed a bug that sometimes caused health blades in the operator portal to become

unavailable.

Fixed a bug in which BCDR runner logs filled up MASLogs folders on physical

hosts.

Added monitoring of WMIProvider health and remediation.

Added Network Controller IMOS size check to Test-AzureStack.

Fixed a bug in SSL certificate validation during internal secret rotation.

Fixed process watchdog memory leaks.

Updated Defender platform to version 4.18.2103.7.

Enabled the alert module for customers depending on Syslog for alerts. The

services will continue to emit alerts to the Syslog pipeline.

To apply this hotfix, you must have version 1.2102.28.82 or later.

Download the following files. Then, follow the instructions in Apply updates in Azure

Stack to apply this update.

Download the zip file now .

Download the hotfix xml file now .

Hotfix information

） Important

As outlined in the release notes for the 2102 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

More information

Azure Stack Hub hotfix 1.2008.40.150

Article • 09/21/2022

Added banner to warn users when a certificate will expire soon.

Improved reliability of update from 2008 to 2102.

Improved reliability of update from 2005 to 2008.

Improved RdAgent availability by removing empty RdAgent files.

Fix for more ghost NIC scenarios when deleting a resource group.

Fixed an issue that, in rare cases, deleted VNet peerings.

ETW trace sessions are configured to use 16 MB of non-pagedpool memory. Trace

sessions now report lost event count (if any) per session, during ETL file rotation in

TraceCollector Eventlog. This releases critical non-paged pool memory for other

services on hosts and VMs. Also fixed various bugs in Tracecollector.

Fixed a bug in resource provider (for example, Event Hubs) deployment, update, or

secret rotation. The operation previously failed with no apparent failure cause. The

fix allows the operation to complete successfully.

Extended the update readiness checks to cover more Service Fabric health and VM

health checks; for example, memory usage and storage disk capacity checks.

Fixed bugs that increased memory pressure on infrastructure.

Fixed bugs that caused operator portal blades to fail to load.

Improved reliability of Process Watchdog.

Improved update reliability by adding detection and self-healing for low available

memory conditions on ERCS VMs at the beginning of the update orchestration.

Fixed a bug in which BCDR runner logs fill up MASLogs folders on physical hosts.

Added monitoring for WMI and remediation.

Added Network Controller IMOS size check to Test-AzureStack.

Fixed internal secret rotation failures (failing at the NC:Secret rotate step), seen

after updating to Azure Stack Hub version 1.2008.25.114 or higher from the latest

2005 release.

Configured stamp ADFS to monitor corporate ADFS signing certificate rollover.

This is for Azure Stack Hub with ADFS identity systems when Azure Stack Hub is

configured with corp ADFS and a federation metadata endpoint.

Fixed alert to remediation linking. Moved memory-critical alert to preview.

Summary

Fixes rolled up from previous hotfix releases

Fixed health package registration, removing duplicate artifact creation.

Improved reliability of RdAgent upgrade.

Enhanced idempotent logic in handling malfunctioning TPMs.

Fixed an issue in which uninstalling some extensions put previously deployed

extensions into a failed state.

Fixed an issue in which duplicate installed updates were shown in the update

history list.

Fixed an intermittent issue in which FRU of SRNG could fail connecting to the ECE

agent.

Fixed VM NICs getting a different hardware identifier after VM is deallocated and

restarted.

Monitored and rebooted VMs based on memory pressure.

Added AzsGBRReadiness in Test-AzureStack to check physical disks' health for

granular bitmap repair readiness.

Reactivated firewall rules to enable SNMP traffic on ERCS VMs.

Fixed an issue in which modifying any properties on the Local Network Gateway

was causing other VPN connections on that gateway to disconnect.

Fixed an issue in which infrastructure VM deployment can fail after applying a

hotfix.

Cleaned up stale user profile folders to clear disk space.

Fixed an issue in which a secondary blob data partition cannot be loaded in some

error cases.

Fixed some bugs with the use of temporary domain accounts.

Enhanced temporary domain account naming to ensure uniqueness.

Patched SDN-related binaries on the physical nodes.

Improved reliability and diagnosing capabilities of patch and update.

Added auto-remediation for SQL cluster.

Updated Healthagent to use Nugetstore.

Filtered WHS alert for Netadapter.

Fixed an issue in which the copy of a certificate used by Service Fabric was

overwritten.

Fixed appearance of ghost NICs when deleting a resource group.

Fixed regression in Test-AzureStack that caused VM deployment test case to

automatically skip.

Improved resiliency of VM provisioning, extension, and image operations.

Fixed an invalid state in Storage resource provider for storage accounts migrated

from 1910 with suspended state.

Fixed a bug in local health system that potentially increased memory pressure on

infrastructure.

Fixed issue in internal secret rotation that would fail with a timeout error if valueadd resource providers were unhealthy.

Fixed a bug in which closed alerts' Last Modified Time was updated in the

operator portal even if the alert stayed closed.

Optimized operator alert request handling, which reduces the chance of timeouts

when viewing alerts in the operator portal or monitoring them via System Center

Operations Manager (SCOM).

Check and enforce key protectors on cluster shared volumes per host.

Fixed issue in which Managed Disk usage data was not being reported after the

2008 update.

Fixed VMs losing connectivity while SuspendNode is occurring in MAS, as part of

host reboot during patch and update.

Added PEP to retrieve current registration details, stale object cleanup for

Remove-Registration.

Fixed a bug that caused the Infrastructure Roles panel in the operator portal to

display incorrect health information.

Improved reliability of log collection for SDN roles by collecting logs on the file

share.

Fixed an issue that can raise an audit scanner health alert in PEP cmdlet.

Removed invalid repair interface for seedringservices.

Improved SDN network reliability on the physical nodes.

Enabled SQL container logs.

Fixed an issue that erroneously raises an alert: "Node inaccessible for VM

Placement."

Fixed a remote management enabling issue for Azure Stack registrations done

prior to 1910 release.

Improved reliability of host node update.

Critical fix for disk space exhaustion on physical hosts, network controllers,

gateways, and load balancers.

Fixed remote management resource replication for resource arrays with

continuation token.

Fixed an issue in which a storage account might be partially restored due to a KVS

race condition in the SRP background usage job.

Fixed an issue in which a virtual subnet was not being cleaned up if the tunnel was

moved to a different GW VM and then the VGW was deleted.

Fixed an issue that could cause registration and internal secret rotation to fail.

Fixed an issue in the internal secret rotation, which might cause a failure in the next

update.

Addressed an issue with internal secret rotation for NRP with a large number of

subscriptions.

Mitigated connection problems to ERCS following startup.

Mitigated a potential issue with upgrading to future versions.

Addressed memory leak based on health runners and suppressed faulty alerts.

Added memory-specific settings to crash dump settings.

Remediated ERCS memory pressure during patch & update.

Included AzsInfraRoleSummary Test-Azurestack test as UpdateReadiness.

Fixed an issue where certificate rotation on IoT Hub fails with "Internal execution

error."

To apply this hotfix, you must have version 1.2008.13.88 or later.

Download the following files. Then, follow the instructions in Apply updates in Azure

Stack to apply this update.

Download the zip file now .

Download the hotfix xml file now .

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

Hotfix information

） Important

As outlined in the release notes for the 2008 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

More information

Azure Stack Hub hotfix 1.2005.46.133

Article • 09/21/2022

Fix for more ghost NIC scenarios when deleting a resource group.

Added banner to warn users when a certificate will expire soon.

Fix for more ghost NIC scenarios when deleting a resource group.

Fixed an issue that, in rare cases, deleted VNet peerings.

Improved RdAgent availability by removing empty RdAgent files.

Improved reliability of update from 2005 to 2008.

Accounted for some ghost NIC scenarios when deleting a resource group.

Improved reliability of process watchdog.

Fixed bugs that increased memory pressure on infrastructure.

Patched missing Hyper-V endpoint, enabling compute control plane operations to

call the appropriate endpoint.

Fixed a bug in which BCDR runner logs filled up MASLogs folders on physical

hosts.

Added monitoring for WMI and remediation.

Enhanced idempotent logic in handling malfunctioning TPMs.

Fixed an issue in which uninstalling some extensions put previously deployed

extensions into a failed state.

Fixed an issue in which partner node certificates required by nchostagent might be

deleted.

Fixed VM NICs getting a different hardware identifier after VM is deallocated and

restarted.

Fixed an issue in which infrastructure VM deployment can fail after applying a

hotfix.

Fixed an issue in which a secondary blob data partition cannot be loaded in some

error cases.

Fixed a bug in local health system that potentially increased memory pressure on

infrastructure.

Patched SDN-related binaries on the physical nodes.

Fixed an invalid state in Storage resource provider for storage accounts migrated

from 1910 with suspended state.

Summary

Fixes rolled up from previous hotfix releases

Improved resiliency of VM provisioning, extension, and image operations.

Added PEP to retrieve current registration details, stale object cleanup for

Remove-Registration.

Improved reliability of log collection for SDN roles by collecting on file share.

Fixed an issue that erroneously raises an alert: "Node inaccessible for VM

Placement."

Removed invalid repair interface for seedringservices.

Improved SDN network reliability on the physical nodes.

Disabled winrm runner

Fixed a bug check and enforced external key protectors on cluster shared volumes.

Fixed an issue in which a storage account might be partially restored due to a KVS

race condition in the SRP background usage job.

Fixed an issue in which a virtual subnet was not being cleaned up if the tunnel was

moved to a different GW VM and then the VGW was deleted.

Fixed an issue that could cause registration and internal secret rotation to fail.

Fixed an issue in the internal secret rotation, which might cause a failure in the next

update.

Added memory-specific settings to crash dump settings.

Restarted SQL VMs to mitigate potential issue with database access that affected

access to portal.

Remediated SMB handle invalidation issue triggered by ESENT error 59 event in

TableServer.

Included AzsInfraRoleSummary Test-Azurestack test as UpdateReadiness.

Remediated ERCS memory pressure during patch & update.

Include deployment provider identity certificate into the internal secret rotation.

Improved Network Controller stability.

Increased Network Controller log retention to aid in diagnosis.

Added Get-NetView as a part of Get-AzureStackLog collection by default.

Fixed an issue where marketplace downloads could fail due to a certificate

validation error.

Improved HealthAgent binary switchover logic.

Improved cluster shared volumes rebalance after Patch & Update (PnU).

Used ADSI to fetch localgroup members in HealthAgent.

Added the missing records, when WASP VMs fail to synchronize records and zones

by using DNS cmdlet during scale in and scale out.

Improved storage service reliability during PnU.

Removed public IP quota validation that caused an issue when creating an internal

load balancer.

Improved reliability of VM deletion: ensure new VMs that could not be fully

created or added to the cluster are deleted.

Check and enforce key protectors on cluster shared volumes.

Fixed "access denied" issue causing update and admin operations to fail.

Fixed WhsFaultScanner to re-launch when it gets stuck to make sure alerts are

correctly generated for users.

Fixed orchestration bug that prevented storage regeneration telemetry events

from being emitted.

Fixed an issue which impacted the reliability of downloading subsequent updates.

Improved ability to diagnose failures based on orchestrator telemetry.

Fixed SRP race condition in moving system storage accounts to system internal

subscription during 2005 PnU.

Fixed time unit scaling error in the server latency metrics

Restarted SQL VMs to mitigate potential issue with database access that affected

access to portal.

Fixed an issue in which the configuration of the retention period for deleted

storage accounts was reverted.

Improved reliability of storage blob and table service.

Addressed issue in the Send-AzureStackDiagnosticLog PEP cmdlet.

Increased the HRP repair time when an update failure occurs.

To apply this hotfix, you must have version 1.2005.6.53 or later.

Download the following files. Then, follow the instructions in Apply updates in Azure

Stack to apply this update.

Download the zip file now .

Download the hotfix xml file now .

Hotfix information

） Important

As outlined in the release notes for the 2005 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

More information

Azure Stack Hub hotfix 1.2102.28.89

Article • 09/21/2022

ETW trace sessions are configured to use 16 MB of non-pagedpool memory. Trace

sessions now report lost event count (if any) per session, during ETL file rotation in

TraceCollector Eventlog. This releases critical non-paged pool memory for other

services on hosts and VMs. Also fixed various bugs in Tracecollector.

Fixed bugs that increased memory pressure on infrastructure.

Fixed bugs in AD FS and Azure Stack Graph to improve deployment and upgrade

reliability.

Fixed bugs in SRP and DiskRP in which performance counters were missing in the

WAC client.

Fixed a bug in resource provider (for example, Event Hubs) deployment, update, or

secret rotation. The operation previously failed with no apparent failure cause. The

fix allows the operation to complete successfully.

Fixed a bug that incorrectly raised a PnPDevice.Attached alert for a set of devices

(mouse, keyboard, etc.) that were safe.

Set memory alert to preview.

Addressed an issue with host agent monitors.

Fixed a trust relationship issue with container applications in FabricRing.

Improved RdAgent availability by removing empty RdAgent files.

Improved reliability of full update.

Extended the update readiness checks to cover more Service Fabric health and VM

health checks; for example, memory usage and storage disk capacity checks.

Updated memory configuration for VM sizes Standard\_NC16as\_T4\_v3 and

Standard\_NC64as\_T4\_v3.

Removed legacy SRP SQL instances and DB files to free up stamp resources.

Fixed a bug in which the cluster status can be stuck in "Configuring Storage" after

adding a new node.

Fixed health package registration, removing duplicate artifact creation.

Fixed a bug that sometimes caused health blades in the operator portal to become

unavailable.

Summary

Fixes rolled up from previous hotfix releases

Fixed a bug in which BCDR runner logs filled up MASLogs folders on physical

hosts.

Added monitoring of WMIProvider health and remediation.

Added Network Controller IMOS size check to Test-AzureStack.

Fixed a bug in SSL certificate validation during internal secret rotation.

Fixed process watchdog memory leaks.

Updated Defender platform to version 4.18.2103.7.

Enabled the alert module for customers depending on Syslog for alerts. The

services will continue to emit alerts to the Syslog pipeline.

To apply this hotfix, you must have version 1.2102.28.87 or later.

Download the following files. Then, follow the instructions in Apply updates in Azure

Stack to apply this update.

Download the zip file now .

Download the hotfix xml file now .

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

Hotfix information

） Important

As outlined in the release notes for the 2102 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

More information

Azure Stack Hub hotfix 1.2008.40.148

Article • 09/21/2022

ETW trace sessions are configured to use 16 MB of non-pagedpool memory. Trace

sessions now report lost event count (if any) per session, during ETL file rotation in

TraceCollector Eventlog. This releases critical non-paged pool memory for other

services on hosts and VMs. Also fixed various bugs in Tracecollector.

Fixed a bug in resource provider (for example, Event Hubs) deployment, update, or

secret rotation. The operation previously failed with no apparent failure cause. The

fix allows the operation to complete successfully.

Extended the update readiness checks to cover more Service Fabric health and VM

health checks; for example, memory usage and storage disk capacity checks.

Fixed bugs that increased memory pressure on infrastructure.

Fixed bugs that caused operator portal blades to fail to load.

Improved reliability of Process Watchdog.

Improved update reliability by adding detection and self-healing for low available

memory conditions on ERCS VMs at the beginning of the update orchestration.

Fixed a bug in which BCDR runner logs fill up MASLogs folders on physical hosts.

Added monitoring for WMI and remediation.

Added Network Controller IMOS size check to Test-AzureStack.

Fixed internal secret rotation failures (failing at the NC:Secret rotate step), seen

after updating to Azure Stack Hub version 1.2008.25.114 or higher from the latest

2005 release.

Configured stamp ADFS to monitor corporate ADFS signing certificate rollover.

This is for Azure Stack Hub with ADFS identity systems when Azure Stack Hub is

configured with corp ADFS and a federation metadata endpoint.

Fixed alert to remediation linking. Moved memory-critical alert to preview.

Fixed health package registration, removing duplicate artifact creation.

Improved reliability of RdAgent upgrade.

Enhanced idempotent logic in handling malfunctioning TPMs.

Fixed an issue in which uninstalling some extensions put previously deployed

extensions into a failed state.

Summary

Fixes rolled up from previous hotfix releases

Fixed an issue in which duplicate installed updates were shown in the update

history list.

Fixed an intermittent issue in which FRU of SRNG could fail connecting to the ECE

agent.

Fixed VM NICs getting a different hardware identifier after VM is deallocated and

restarted.

Monitored and rebooted VMs based on memory pressure.

Added AzsGBRReadiness in Test-AzureStack to check physical disks' health for

granular bitmap repair readiness.

Reactivated firewall rules to enable SNMP traffic on ERCS VMs.

Fixed an issue in which modifying any properties on the Local Network Gateway

was causing other VPN connections on that gateway to disconnect.

Fixed an issue in which infrastructure VM deployment can fail after applying a

hotfix.

Cleaned up stale user profile folders to clear disk space.

Fixed an issue in which a secondary blob data partition cannot be loaded in some

error cases.

Fixed some bugs with the use of temporary domain accounts.

Enhanced temporary domain account naming to ensure uniqueness.

Patched SDN-related binaries on the physical nodes.

Improved reliability and diagnosing capabilities of patch and update.

Added auto-remediation for SQL cluster.

Updated Healthagent to use Nugetstore.

Filtered WHS alert for Netadapter.

Fixed an issue in which the copy of a certificate used by Service Fabric was

overwritten.

Fixed appearance of ghost NICs when deleting a resource group.

Fixed regression in Test-AzureStack that caused VM deployment test case to

automatically skip.

Improved resiliency of VM provisioning, extension, and image operations.

Fixed an invalid state in Storage resource provider for storage accounts migrated

from 1910 with suspended state.

Fixed a bug in local health system that potentially increased memory pressure on

infrastructure.

Fixed issue in internal secret rotation that would fail with a timeout error if valueadd resource providers were unhealthy.

Fixed a bug in which closed alerts' Last Modified Time was updated in the

operator portal even if the alert stayed closed.

Optimized operator alert request handling, which reduces the chance of timeouts

when viewing alerts in the operator portal or monitoring them via System Center

Operations Manager (SCOM).

Check and enforce key protectors on cluster shared volumes per host.

Fixed issue in which Managed Disk usage data was not being reported after the

2008 update.

Fixed VMs losing connectivity while SuspendNode is occurring in MAS, as part of

host reboot during patch and update.

Added PEP to retrieve current registration details, stale object cleanup for

Remove-Registration.

Fixed a bug that caused the Infrastructure Roles panel in the operator portal to

display incorrect health information.

Improved reliability of log collection for SDN roles by collecting logs on the file

share.

Fixed an issue that can raise an audit scanner health alert in PEP cmdlet.

Removed invalid repair interface for seedringservices.

Improved SDN network reliability on the physical nodes.

Enabled SQL container logs.

Fixed an issue that erroneously raises an alert: "Node inaccessible for VM

Placement."

Fixed a remote management enabling issue for Azure Stack registrations done

prior to 1910 release.

Improved reliability of host node update.

Critical fix for disk space exhaustion on physical hosts, network controllers,

gateways, and load balancers.

Fixed remote management resource replication for resource arrays with

continuation token.

Fixed an issue in which a storage account might be partially restored due to a KVS

race condition in the SRP background usage job.

Fixed an issue in which a virtual subnet was not being cleaned up if the tunnel was

moved to a different GW VM and then the VGW was deleted.

Fixed an issue that could cause registration and internal secret rotation to fail.

Fixed an issue in the internal secret rotation, which might cause a failure in the next

update.

Addressed an issue with internal secret rotation for NRP with a large number of

subscriptions.

Mitigated connection problems to ERCS following startup.

Mitigated a potential issue with upgrading to future versions.

Addressed memory leak based on health runners and suppressed faulty alerts.

Added memory-specific settings to crash dump settings.

Remediated ERCS memory pressure during patch & update.

Included AzsInfraRoleSummary Test-Azurestack test as UpdateReadiness.

Fixed an issue where certificate rotation on IoT Hub fails with "Internal execution

error."

To apply this hotfix, you must have version 1.2008.13.88 or later.

Download the following files. Then, follow the instructions in Apply updates in Azure

Stack to apply this update.

Download the zip file now .

Download the hotfix xml file now .

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

Hotfix information

） Important

As outlined in the release notes for the 2008 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

More information

Azure Stack Hub hotfix 1.2005.42.126

Article • 09/21/2022

Accounted for some ghost NIC scenarios when deleting a resource group.

Improved reliability of process watchdog.

Fixed bugs that increased memory pressure on infrastructure.

Patched missing Hyper-V endpoint, enabling compute control plane operations to

call the appropriate endpoint.

Fixed a bug in which BCDR runner logs filled up MASLogs folders on physical

hosts.

Added monitoring for WMI and remediation.

Enhanced idempotent logic in handling malfunctioning TPMs.

Fixed an issue in which uninstalling some extensions put previously deployed

extensions into a failed state.

Fixed an issue in which partner node certificates required by nchostagent might be

deleted.

Fixed VM NICs getting a different hardware identifier after VM is deallocated and

restarted.

Fixed an issue in which infrastructure VM deployment can fail after applying a

hotfix.

Fixed an issue in which a secondary blob data partition cannot be loaded in some

error cases.

Fixed a bug in local health system that potentially increased memory pressure on

infrastructure.

Patched SDN-related binaries on the physical nodes.

Fixed an invalid state in Storage resource provider for storage accounts migrated

from 1910 with suspended state.

Improved resiliency of VM provisioning, extension, and image operations.

Added PEP to retrieve current registration details, stale object cleanup for

Remove-Registration.

Improved reliability of log collection for SDN roles by collecting on file share.

Fixed an issue that erroneously raises an alert: "Node inaccessible for VM

Placement."

Summary

Fixes rolled up from previous hotfix releases

Removed invalid repair interface for seedringservices.

Improved SDN network reliability on the physical nodes.

Disabled winrm runner

Fixed a bug check and enforced external key protectors on cluster shared volumes.

Fixed an issue in which a storage account might be partially restored due to a KVS

race condition in the SRP background usage job.

Fixed an issue in which a virtual subnet was not being cleaned up if the tunnel was

moved to a different GW VM and then the VGW was deleted.

Fixed an issue that could cause registration and internal secret rotation to fail.

Fixed an issue in the internal secret rotation, which might cause a failure in the next

update.

Added memory-specific settings to crash dump settings.

Restarted SQL VMs to mitigate potential issue with database access that affected

access to portal.

Remediated SMB handle invalidation issue triggered by ESENT error 59 event in

TableServer.

Included AzsInfraRoleSummary Test-Azurestack test as UpdateReadiness.

Remediated ERCS memory pressure during patch & update.

Include deployment provider identity certificate into the internal secret rotation.

Improved Network Controller stability.

Increased Network Controller log retention to aid in diagnosis.

Added Get-NetView as a part of Get-AzureStackLog collection by default.

Fixed an issue where marketplace downloads could fail due to a certificate

validation error.

Improved HealthAgent binary switchover logic.

Improved cluster shared volumes rebalance after Patch & Update (PnU).

Used ADSI to fetch localgroup members in HealthAgent.

Added the missing records, when WASP VMs fail to synchronize records and zones

by using DNS cmdlet during scale in and scale out.

Improved storage service reliability during PnU.

Removed public IP quota validation that caused an issue when creating an internal

load balancer.

Improved reliability of VM deletion: ensure new VMs that could not be fully

created or added to the cluster are deleted.

Check and enforce key protectors on cluster shared volumes.

Fixed "access denied" issue causing update and admin operations to fail.

Fixed WhsFaultScanner to re-launch when it gets stuck to make sure alerts are

correctly generated for users.

Fixed orchestration bug that prevented storage regeneration telemetry events

from being emitted.

Fixed an issue which impacted the reliability of downloading subsequent updates.

Improved ability to diagnose failures based on orchestrator telemetry.

Fixed SRP race condition in moving system storage accounts to system internal

subscription during 2005 PnU.

Fixed time unit scaling error in the server latency metrics

Restarted SQL VMs to mitigate potential issue with database access that affected

access to portal.

Fixed an issue in which the configuration of the retention period for deleted

storage accounts was reverted.

Improved reliability of storage blob and table service.

Addressed issue in the Send-AzureStackDiagnosticLog PEP cmdlet.

Increased the HRP repair time when an update failure occurs.

To apply this hotfix, you must have version 1.2005.6.53 or later.

Download the following files. Then, follow the instructions in Apply updates in Azure

Stack to apply this update.

Download the zip file now .

Download the hotfix xml file now .

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

Hotfix information

） Important

As outlined in the release notes for the 2005 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

More information

Azure Stack Hub hotfix 1.2102.28.87

Article • 09/21/2022

Updated memory configuration for VM sizes Standard\_NC16as\_T4\_v3 and

Standard\_NC64as\_T4\_v3.

Removed legacy SRP SQL instances and DB files to free up stamp resources.

Fixed a bug in which the cluster status can be stuck in "Configuring Storage" after

adding a new node.

Fixed health package registration, removing duplicate artifact creation.

Fixed a bug that sometimes caused health blades in the operator portal to become

unavailable.

Fixed a bug in which BCDR runner logs filled up MASLogs folders on physical

hosts.

Added monitoring of WMIProvider health and remediation.

Added Network Controller IMOS size check to Test-AzureStack.

Fixed a bug in SSL certificate validation during internal secret rotation.

Fixed process watchdog memory leaks.

Updated Defender platform to version 4.18.2103.7.

Enabled the alert module for customers depending on Syslog for alerts. The

services will continue to emit alerts to the Syslog pipeline.

To apply this hotfix, you must have version 1.2102.28.82 or later.

Download the following files. Then, follow the instructions in Apply updates in Azure

Stack to apply this update.

Summary

Hotfix information

） Important

As outlined in the release notes for the 2102 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

Download the zip file now .

Download the hotfix xml file now .

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

More information

Azure Stack Hub hotfix 1.2008.37.139

Article • 09/21/2022

Improved update reliability by adding detection and self-healing for low available

memory conditions on ERCS VMs at the beginning of the update orchestration.

Fixed a bug in which BCDR runner logs fill up MASLogs folders on physical hosts.

Added monitoring for WMI and remediation.

Added Network Controller IMOS size check to Test-AzureStack.

Fixed internal secret rotation failures (failing at the NC:Secret rotate step), seen

after updating to Azure Stack Hub version 1.2008.25.114 or higher from the latest

2005 release.

Configured stamp ADFS to monitor corporate ADFS signing certificate rollover.

This is for Azure Stack Hub with ADFS identity systems when Azure Stack Hub is

configured with corp ADFS and a federation metadata endpoint.

Fixed alert to remediation linking. Moved memory-critical alert to preview.

Fixed health package registration, removing duplicate artifact creation.

Improved reliability of RdAgent upgrade.

Enhanced idempotent logic in handling malfunctioning TPMs.

Fixed an issue in which uninstalling some extensions put previously deployed

extensions into a failed state.

Fixed an issue in which duplicate installed updates were shown in the update

history list.

Fixed an intermittent issue in which FRU of SRNG could fail connecting to the ECE

agent.

Fixed VM NICs getting a different hardware identifier after VM is deallocated and

restarted.

Monitored and rebooted VMs based on memory pressure.

Added AzsGBRReadiness in Test-AzureStack to check physical disks' health for

granular bitmap repair readiness.

Reactivated firewall rules to enable SNMP traffic on ERCS VMs.

Fixed an issue in which modifying any properties on the Local Network Gateway

was causing other VPN connections on that gateway to disconnect.

Summary

Fixes rolled up from previous hotfix releases

Fixed an issue in which infrastructure VM deployment can fail after applying a

hotfix.

Cleaned up stale user profile folders to clear disk space.

Fixed an issue in which a secondary blob data partition cannot be loaded in some

error cases.

Fixed some bugs with the use of temporary domain accounts.

Enhanced temporary domain account naming to ensure uniqueness.

Patched SDN-related binaries on the physical nodes.

Improved reliability and diagnosing capabilities of patch and update.

Added auto-remediation for SQL cluster.

Updated Healthagent to use Nugetstore.

Filtered WHS alert for Netadapter.

Fixed an issue in which the copy of a certificate used by Service Fabric was

overwritten.

Fixed appearance of ghost NICs when deleting a resource group.

Fixed regression in Test-AzureStack that caused VM deployment test case to

automatically skip.

Improved resiliency of VM provisioning, extension, and image operations.

Fixed an invalid state in Storage resource provider for storage accounts migrated

from 1910 with suspended state.

Fixed a bug in local health system that potentially increased memory pressure on

infrastructure.

Fixed issue in internal secret rotation that would fail with a timeout error if valueadd resource providers were unhealthy.

Fixed a bug in which closed alerts' Last Modified Time was updated in the

operator portal even if the alert stayed closed.

Optimized operator alert request handling, which reduces the chance of timeouts

when viewing alerts in the operator portal or monitoring them via System Center

Operations Manager (SCOM).

Check and enforce key protectors on cluster shared volumes per host.

Fixed issue in which Managed Disk usage data was not being reported after the

2008 update.

Fixed VMs losing connectivity while SuspendNode is occurring in MAS, as part of

host reboot during patch and update.

Added PEP to retrieve current registration details, stale object cleanup for

Remove-Registration.

Fixed a bug that caused the Infrastructure Roles panel in the operator portal to

display incorrect health information.

Improved reliability of log collection for SDN roles by collecting logs on the file

share.

Fixed an issue that can raise an audit scanner health alert in PEP cmdlet.

Removed invalid repair interface for seedringservices.

Improved SDN network reliability on the physical nodes.

Enabled SQL container logs.

Fixed an issue that erroneously raises an alert: "Node inaccessible for VM

Placement."

Fixed a remote management enabling issue for Azure Stack registrations done

prior to 1910 release.

Improved reliability of host node update.

Critical fix for disk space exhaustion on physical hosts, network controllers,

gateways, and load balancers.

Fixed remote management resource replication for resource arrays with

continuation token.

Fixed an issue in which a storage account might be partially restored due to a KVS

race condition in the SRP background usage job.

Fixed an issue in which a virtual subnet was not being cleaned up if the tunnel was

moved to a different GW VM and then the VGW was deleted.

Fixed an issue that could cause registration and internal secret rotation to fail.

Fixed an issue in the internal secret rotation, which might cause a failure in the next

update.

Addressed an issue with internal secret rotation for NRP with a large number of

subscriptions.

Mitigated connection problems to ERCS following startup.

Mitigated a potential issue with upgrading to future versions.

Addressed memory leak based on health runners and suppressed faulty alerts.

Added memory-specific settings to crash dump settings.

Remediated ERCS memory pressure during patch & update.

Included AzsInfraRoleSummary Test-Azurestack test as UpdateReadiness.

Fixed an issue where certificate rotation on IoT Hub fails with "Internal execution

error."

To apply this hotfix, you must have version 1.2008.13.88 or later.

Hotfix information

） Important

As outlined in the release notes for the 2008 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

Download the following files. Then, follow the instructions in Apply updates in Azure

Stack to apply this update.

Download the zip file now .

Download the hotfix xml file now .

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

More information

Azure Stack Hub hotfix 1.2005.41.124

Article • 09/21/2022

Patched missing Hyper-V endpoint, enabling compute control plane operations to

call the appropriate endpoint.

Fixed a bug in which BCDR runner logs filled up MASLogs folders on physical

hosts.

Added monitoring for WMI and remediation.

Enhanced idempotent logic in handling malfunctioning TPMs.

Fixed an issue in which uninstalling some extensions put previously deployed

extensions into a failed state.

Fixed an issue in which partner node certificates required by nchostagent might be

deleted.

Fixed VM NICs getting a different hardware identifier after VM is deallocated and

restarted.

Fixed an issue in which infrastructure VM deployment can fail after applying a

hotfix.

Fixed an issue in which a secondary blob data partition cannot be loaded in some

error cases.

Fixed a bug in local health system that potentially increased memory pressure on

infrastructure.

Patched SDN-related binaries on the physical nodes.

Fixed an invalid state in Storage resource provider for storage accounts migrated

from 1910 with suspended state.

Improved resiliency of VM provisioning, extension, and image operations.

Added PEP to retrieve current registration details, stale object cleanup for

Remove-Registration.

Improved reliability of log collection for SDN roles by collecting on file share.

Fixed an issue that erroneously raises an alert: "Node inaccessible for VM

Placement."

Removed invalid repair interface for seedringservices.

Improved SDN network reliability on the physical nodes.

Disabled winrm runner

Summary

Fixes rolled up from previous hotfix releases

Fixed a bug check and enforced external key protectors on cluster shared volumes.

Fixed an issue in which a storage account might be partially restored due to a KVS

race condition in the SRP background usage job.

Fixed an issue in which a virtual subnet was not being cleaned up if the tunnel was

moved to a different GW VM and then the VGW was deleted.

Fixed an issue that could cause registration and internal secret rotation to fail.

Fixed an issue in the internal secret rotation, which might cause a failure in the next

update.

Added memory-specific settings to crash dump settings.

Restarted SQL VMs to mitigate potential issue with database access that affected

access to portal.

Remediated SMB handle invalidation issue triggered by ESENT error 59 event in

TableServer.

Included AzsInfraRoleSummary Test-Azurestack test as UpdateReadiness.

Remediated ERCS memory pressure during patch & update.

Include deployment provider identity certificate into the internal secret rotation.

Improved Network Controller stability.

Increased Network Controller log retention to aid in diagnosis.

Added Get-NetView as a part of Get-AzureStackLog collection by default.

Fixed an issue where marketplace downloads could fail due to a certificate

validation error.

Improved HealthAgent binary switchover logic.

Improved cluster shared volumes rebalance after Patch & Update (PnU).

Used ADSI to fetch localgroup members in HealthAgent.

Added the missing records, when WASP VMs fail to synchronize records and zones

by using DNS cmdlet during scale in and scale out.

Improved storage service reliability during PnU.

Removed public IP quota validation that caused an issue when creating an internal

load balancer.

Improved reliability of VM deletion: ensure new VMs that could not be fully

created or added to the cluster are deleted.

Check and enforce key protectors on cluster shared volumes.

Fixed "access denied" issue causing update and admin operations to fail.

Fixed WhsFaultScanner to re-launch when it gets stuck to make sure alerts are

correctly generated for users.

Fixed orchestration bug that prevented storage regeneration telemetry events

from being emitted.

Fixed an issue which impacted the reliability of downloading subsequent updates.

Improved ability to diagnose failures based on orchestrator telemetry.

Fixed SRP race condition in moving system storage accounts to system internal

subscription during 2005 PnU.

Fixed time unit scaling error in the server latency metrics

Restarted SQL VMs to mitigate potential issue with database access that affected

access to portal.

Fixed an issue in which the configuration of the retention period for deleted

storage accounts was reverted.

Improved reliability of storage blob and table service.

Addressed issue in the Send-AzureStackDiagnosticLog PEP cmdlet.

Increased the HRP repair time when an update failure occurs.

To apply this hotfix, you must have version 1.2005.6.53 or later.

Download the following files. Then, follow the instructions in Apply updates in Azure

Stack to apply this update.

Download the zip file now .

Download the hotfix xml file now .

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

Hotfix information

） Important

As outlined in the release notes for the 2005 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

More information

Azure Stack Hub hotfix 1.2002.69.179

Article • 09/21/2022

Fixed a bug in which BCDR runner logs filled up MASLogs folders on physical

hosts.

Patched SDN-related binaries on the physical nodes.

Fixed an invalid state in Storage Resource Provider for storage accounts migrated

from 1910 with suspended state.

Improved resiliency of VM provisioning and extension operations.

Improved SDN network reliability on the physical nodes.

Fixed an issue in which a virtual subnet was not being cleaned up if the tunnel was

moved to a different GW VM and then the VGW was deleted.

Fixed an issue that could cause registration and internal secret rotation to fail.

Added memory-specific settings to crash dump settings.

Remediated SMB handle invalidation issue triggered by ESENT error 59 event in

TableServer.

Fixed an issue which impacted the reliability of downloading subsequent updates.

Improved reliability of NuGet package installation after unexpected failure.

Fixed an issue where subscription dropdown validation fails when the user only has

RG write permission.

Fixed an issue in which the blob download page has an issue when downloading

large items.

Fixed an issue in which the configuration of the retention period for deleted

storage accounts is reverted.

Improved Network Controller stability.

Increased Network Controller log retention to aid in diagnosis.

Fixed an issue where marketplace downloads could fail due to a certificate

validation error.

Include deployment provider identity certificate into the internal secret rotation.

Fixed Windows storage WMI to keep call responsive, to improve the reliability of

storage management operations.

Added TPM status monitor for physical hosts.

Summary

Fixes rolled up from previous hotfix releases

Restarted SQL VMs to mitigate potential issue with database access which affects

access to portal.

Improved reliability of storage blob and table service.

Fixed an issue in which virtual machine scale set creation with the Standard\_DS2\_v2

SKU through UI always failed.

Configuration update improvements.

Fixed KVS enumerator leak in DiskRP to improve reliability of disk operations.

Re-enabled the ability to generate host crash dumps and trigger NMI crashes for

hangs.

Addressed DNS server vulnerability described in CVE-2020-1350.

Changes that addressed cluster instability.

Improved reliability of JEA endpoint creation.

Fixed bug to unblock concurrent VM creation in batch sizes of 20 or above.

Improved the reliability and stability of the portal, adding a monitoring capability

to restart the hosting service if it experiences any downtime.

Addressed an issue where some alerts were not paused during update.

Improved diagnostics around failures in DSC resources.

Improved error message generated by an unexpected failure in bare metal

deployment script.

Added resiliency during physical node repair operations.

Fixed a code defect that sometimes caused HRP SF app to become unhealthy. Also

fixed a code defect that prevented alerts from being suspended during update.

Added resiliency to image creation code when the destination path is

unexpectedly not present.

Added disk cleanup interface for ERCS VMs and ensured that it runs prior to

attempting to install new content to those VMs.

Improved quorum check for Service Fabric node repair in the auto-remediation

path.

Improved logic around bringing cluster nodes back online in rare cases where

outside intervention puts them into an unexpected state.

Improved resiliency of engine code to ensure typos in machine name casing do

not cause unexpected state in the ECE configuration when manual actions are used

to add and remove nodes.

Added a health check to detect VM or physical node repair operations that were

left in a partially completed state from previous support sessions.

Improved diagnostic logging for installation of content from NuGet packages

during update orchestration.

Fixed the internal secret rotation failure for customers who use AAD as identity

system, and block ERCS outbound internet connectivity.

Increased the default timeout of Test-AzureStack for AzsScenarios to 45 minutes.

Improved HealthAgent update reliability.

Fixed an issue where VM repair of ERCS VMs was not being triggered during

remediation actions.

Made host update resilient to issues caused by a silent failure to clean up stale

infrastructure VM files.

Added a preventative fix for certutil parsing errors when using randomly generated

passwords.

Added a round of health checks prior to the engine update, so that failed admin

operations can be allowed to continue running with their original version of

orchestration code.

Fixed ACS backup failure when the ACSSettingsService backup finished first.

Upgraded Azure Stack AD FS farm behavior level to v4. Azure Stack Hubs deployed

with 1908 or later are already on v4.

Improved reliability of the host update process.

Fixed a certificate renewal issue that could have caused internal secret rotation to

fail.

Fixed the new time server sync alert to correct an issue where it incorrectly detects

a time sync issue when the time source was specified with the 0x8 flag.

Corrected a validation constraint error that occurred when using the new

automatic log collection interface, and it detected https://login.windows.net/ as

an invalid Azure AD endpoint.

Fixed an issue that prevented the use of SQL auto backup via the

SQLIaaSExtension.

Corrected the alerting used in Test-AzureStack when validating the network

controller certificates.

Upgraded Azure Stack AD FS farm behavior level to v4. Azure Stack Hubs deployed

with 1908 or later are already on v4.

Improved reliability of the host update process.

Fixed a certificate renewal issue that could have caused internal secret rotation to

fail.

Reduced alert triggers in order to avoid unnecessary proactive log collections.

Improved reliability of storage upgrade by eliminating Windows Health Service

WMI call timeout.

To apply this hotfix, you must have version 1.2002.0.35 or later.

Hotfix information

） Important

Download the following files. Then, follow the instructions in Apply updates in Azure

Stack to apply this update.

Download the zip file now .

Download the hotfix xml file now .

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

As outlined in the release notes for the 2002 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

More information

Azure Stack Hub hotfix 1.2008.33.131

Article • 09/21/2022

Enhanced idempotent logic in handling malfunctioning TPMs.

Fixed an issue in which uninstalling some extensions put previously deployed

extensions into a failed state.

Fixed an issue in which duplicate installed updates were shown in the update

history list.

Fixed an intermittent issue in which FRU of SRNG could fail connecting to the ECE

agent.

Fixed VM NICs getting a different hardware identifier after VM is deallocated and

restarted.

Monitored and rebooted VMs based on memory pressure.

Added AzsGBRReadiness in Test-AzureStack to check physical disks' health for

granular bitmap repair readiness.

Reactivated firewall rules to enable SNMP traffic on ERCS VMs.

Fixed an issue in which modifying any properties on the Local Network Gateway

was causing other VPN connections on that gateway to disconnect.

Fixed an issue in which infrastructure VM deployment can fail after applying a

hotfix.

Cleaned up stale user profile folders to clear disk space.

Fixed an issue in which a secondary blob data partition cannot be loaded in some

error cases.

Fixed some bugs with the use of temporary domain accounts.

Enhanced temporary domain account naming to ensure uniqueness.

Patched SDN-related binaries on the physical nodes.

Improved reliability and diagnosing capabilities of patch and update.

Added auto-remediation for SQL cluster.

Updated Healthagent to use Nugetstore.

Filtered WHS alert for Netadapter.

Fixed an issue in which the copy of a certificate used by Service Fabric was

overwritten.

Fixed appearance of ghost NICs when deleting a resource group.

Summary

Fixes rolled up from previous hotfix releases

Fixed regression in Test-AzureStack that caused VM deployment test case to

automatically skip.

Improved resiliency of VM provisioning, extension, and image operations.

Fixed an invalid state in Storage resource provider for storage accounts migrated

from 1910 with suspended state.

Fixed a bug in local health system that potentially increased memory pressure on

infrastructure.

Fixed issue in internal secret rotation that would fail with a timeout error if valueadd resource providers were unhealthy.

Fixed a bug in which closed alerts' Last Modified Time was updated in the

operator portal even if the alert stayed closed.

Optimized operator alert request handling, which reduces the chance of timeouts

when viewing alerts in the operator portal or monitoring them via System Center

Operations Manager (SCOM).

Check and enforce key protectors on cluster shared volumes per host.

Fixed issue in which Managed Disk usage data was not being reported after the

2008 update.

Fixed VMs losing connectivity while SuspendNode is occurring in MAS, as part of

host reboot during patch and update.

Added PEP to retrieve current registration details, stale object cleanup for

Remove-Registration.

Fixed a bug that caused the Infrastructure Roles panel in the operator portal to

display incorrect health information.

Improved reliability of log collection for SDN roles by collecting logs on the file

share.

Fixed an issue that can raise an audit scanner health alert in PEP cmdlet.

Removed invalid repair interface for seedringservices.

Improved SDN network reliability on the physical nodes.

Enabled SQL container logs.

Fixed an issue that erroneously raises an alert: “Node inaccessible for VM

Placement."

Fixed a remote management enabling issue for Azure Stack registrations done

prior to 1910 release.

Improved reliability of host node update.

Critical fix for disk space exhaustion on physical hosts, network controllers,

gateways, and load balancers.

Fixed remote management resource replication for resource arrays with

continuation token.

Fixed an issue in which a storage account might be partially restored due to a KVS

race condition in the SRP background usage job.

Fixed an issue in which a virtual subnet was not being cleaned up if the tunnel was

moved to a different GW VM and then the VGW was deleted.

Fixed an issue that could cause registration and internal secret rotation to fail.

Fixed an issue in the internal secret rotation, which might cause a failure in the next

update.

Addressed an issue with internal secret rotation for NRP with a large number of

subscriptions.

Mitigated connection problems to ERCS following startup.

Mitigated a potential issue with upgrading to future versions.

Addressed memory leak based on health runners and suppressed faulty alerts.

Added memory-specific settings to crash dump settings.

Remediated ERCS memory pressure during patch & update.

Included AzsInfraRoleSummary Test-Azurestack test as UpdateReadiness.

Fixed an issue where certificate rotation on IoT Hub fails with “Internal execution

error.”

To apply this hotfix, you must have version 1.2008.13.88 or later.

Download the following files. Then, follow the instructions in Apply updates in Azure

Stack to apply this update.

Download the zip file now .

Download the hotfix xml file now .

Azure Stack Hub update resources

Hotfix information

） Important

As outlined in the release notes for the 2008 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

More information

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

Azure Stack Hub hotfix 1.2005.35.112

Article • 09/21/2022

Enhanced idempotent logic in handling malfunctioning TPMs.

Fixed an issue in which uninstalling some extensions put previously deployed

extensions into a failed state.

Fixed an issue in which partner node certificates required by nchostagent might be

deleted.

Fixed VM NICs getting a different hardware identifier after VM is deallocated and

restarted.

Fixed an issue in which infrastructure VM deployment can fail after applying a

hotfix.

Fixed an issue in which a secondary blob data partition cannot be loaded in some

error cases.

Fixed a bug in local health system that potentially increased memory pressure on

infrastructure.

Patched SDN-related binaries on the physical nodes.

Fixed an invalid state in Storage resource provider for storage accounts migrated

from 1910 with suspended state.

Improved resiliency of VM provisioning, extension, and image operations.

Added PEP to retrieve current registration details, stale object cleanup for

Remove-Registration.

Improved reliability of log collection for SDN roles by collecting on file share.

Fixed an issue that erroneously raises an alert: “Node inaccessible for VM

Placement."

Removed invalid repair interface for seedringservices.

Improved SDN network reliability on the physical nodes.

Disabled winrm runner

Fixed a bug check and enforced external key protectors on cluster shared volumes.

Fixed an issue in which a storage account might be partially restored due to a KVS

race condition in the SRP background usage job.

Fixed an issue in which a virtual subnet was not being cleaned up if the tunnel was

moved to a different GW VM and then the VGW was deleted.

Summary

Fixes rolled up from previous hotfix releases

Fixed an issue that could cause registration and internal secret rotation to fail.

Fixed an issue in the internal secret rotation, which might cause a failure in the next

update.

Added memory-specific settings to crash dump settings.

Restarted SQL VMs to mitigate potential issue with database access that affected

access to portal.

Remediated SMB handle invalidation issue triggered by ESENT error 59 event in

TableServer.

Included AzsInfraRoleSummary Test-Azurestack test as UpdateReadiness.

Remediated ERCS memory pressure during patch & update.

Include deployment provider identity certificate into the internal secret rotation.

Improved Network Controller stability.

Increased Network Controller log retention to aid in diagnosis.

Added Get-NetView as a part of Get-AzureStackLog collection by default.

Fixed an issue where marketplace downloads could fail due to a certificate

validation error.

Improved HealthAgent binary switchover logic.

Improved cluster shared volumes rebalance after Patch & Update (PnU).

Used ADSI to fetch localgroup members in HealthAgent.

Added the missing records, when WASP VMs fail to synchronize records and zones

by using DNS cmdlet during scale in and scale out.

Improved storage service reliability during PnU.

Removed public IP quota validation that caused an issue when creating an internal

load balancer.

Improved reliability of VM deletion: ensure new VMs that could not be fully

created or added to the cluster are deleted.

Check and enforce key protectors on cluster shared volumes.

Fixed "access denied" issue causing update and admin operations to fail.

Fixed WhsFaultScanner to re-launch when it gets stuck to make sure alerts are

correctly generated for users.

Fixed orchestration bug that prevented storage regeneration telemetry events

from being emitted.

Fixed an issue which impacted the reliability of downloading subsequent updates.

Improved ability to diagnose failures based on orchestrator telemetry.

Fixed SRP race condition in moving system storage accounts to system internal

subscription during 2005 PnU.

Fixed time unit scaling error in the server latency metrics

Restarted SQL VMs to mitigate potential issue with database access that affected

access to portal.

Fixed an issue in which the configuration of the retention period for deleted

storage accounts was reverted.

Improved reliability of storage blob and table service.

Addressed issue in the Send-AzureStackDiagnosticLog PEP cmdlet.

Increased the HRP repair time when an update failure occurs.

To apply this hotfix, you must have version 1.2005.6.53 or later.

Download the following files. Then, follow the instructions in Apply updates in Azure

Stack to apply this update.

Download the zip file now .

Download the hotfix xml file now .

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

Hotfix information

） Important

As outlined in the release notes for the 2005 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

More information

Azure Stack Hub hotfix 1.2008.31.126

Article • 09/21/2022

Fixed VM NICs getting a different hardware identifier after VM is deallocated and

restarted.

Monitored and rebooted VMs based on memory pressure.

Added AzsGBRReadiness in Test-AzureStack to check physical disks' health for

granular bitmap repair readiness.

Reactivated firewall rules to enable SNMP traffic on ERCS VMs.

Fixed an issue in which modifying any properties on the Local Network Gateway

was causing other VPN connections on that gateway to disconnect.

Fixed an issue in which infrastructure VM deployment can fail after applying a

hotfix.

Cleaned up stale user profile folders to clear disk space.

Fixed an issue in which a secondary blob data partition cannot be loaded in some

error cases.

Fixed some bugs with the use of temporary domain accounts.

Enhanced temporary domain account naming to ensure uniqueness.

Patched SDN-related binaries on the physical nodes.

Improved reliability and diagnosing capabilities of patch and update.

Added auto-remediation for SQL cluster.

Updated Healthagent to use Nugetstore.

Filtered WHS alert for Netadapter.

Fixed an issue in which the copy of a certificate used by Service Fabric was

overwritten.

Fixed appearance of ghost NICs when deleting a resource group.

Fixed regression in Test-AzureStack that caused VM deployment test case to

automatically skip.

Improved resiliency of VM provisioning, extension, and image operations.

Fixed an invalid state in Storage resource provider for storage accounts migrated

from 1910 with suspended state.

Fixed a bug in local health system that potentially increased memory pressure on

infrastructure.

Summary

Fixes rolled up from previous hotfix releases

Fixed issue in internal secret rotation that would fail with a timeout error if valueadd resource providers were unhealthy.

Fixed a bug in which closed alerts' Last Modified Time was updated in the

operator portal even if the alert stayed closed.

Optimized operator alert request handling, which reduces the chance of timeouts

when viewing alerts in the operator portal or monitoring them via SCOM.

Check and enforce key protectors on cluster shared volumes per host.

Fixed issue in which Managed Disk usage data was not being reported after the

2008 update.

Fixed VMs losing connectivity while SuspendNode is occurring in MAS, as part of

host reboot during patch and update.

Added PEP to retrieve current registration details, stale object cleanup for

Remove-Registration.

Fixed a bug which caused the Infrastructure Roles panel in the operator portal to

display incorrect health information.

Improved reliability of log collection for SDN roles by collecting logs on the file

share.

Fixed an issue that can raise an audit scanner health alert in PEP cmdlet.

Removed invalid repair interface for seedringservices.

Improved SDN network reliability on the physical nodes.

Enabled SQL container logs.

Fixed an issue that erroneously raises an alert: “Node inaccessible for VM

Placement."

Fixed a remote management enabling issue for Azure Stack registrations done

prior to 1910 release.

Improved reliability of host node update.

Critical fix for disk space exhaustion on physical hosts, network controllers,

gateways, and load balancers.

Fixed remote management resource replication for resource arrays with

continuation token.

Fixed an issue in which a storage account might be partially restored due to a KVS

race condition in the SRP background usage job.

Fixed an issue in which a virtual subnet was not being cleaned up if the tunnel was

moved to a different GW VM and then the VGW was deleted.

Fixed an issue that could cause registration and internal secret rotation to fail.

Fixed an issue in the internal secret rotation, which might cause a failure in the next

update.

Addressed an issue with internal secret rotation for NRP with a large number of

subscriptions.

Mitigated connection problems to ERCS following startup.

Mitigated a potential issue with upgrading to future versions.

Addressed memory leak based on health runners and suppressed faulty alerts.

Added memory specific settings to crash dump settings.

Remediated ERCS memory pressure during patch & update.

Included AzsInfraRoleSummary Test-Azurestack test as UpdateReadiness.

Fixed an issue where certificate rotation on IoT Hub fails with “Internal execution

error.”

To apply this hotfix, you must have version 1.2008.13.88 or later.

Download the following files. Then, follow the instructions in Apply updates in Azure

Stack to apply this update.

Download the zip file now .

Download the hotfix xml file now .

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

Hotfix information

） Important

As outlined in the release notes for the 2008 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

More information

Azure Stack Hub hotfix 1.2005.33.108

Article • 09/21/2022

Fixed an issue in which partner node certificates required by nchostagent might be

deleted.

Fixed VM NICs getting a different hardware identifier after VM is deallocated and

restarted.

Fixed an issue in which infrastructure VM deployment can fail after applying a

hotfix.

Fixed an issue in which a secondary blob data partition cannot be loaded in some

error cases.

Fixed a bug in local health system that potentially increased memory pressure on

infrastructure.

Patched SDN-related binaries on the physical nodes.

Fixed an invalid state in Storage resource provider for storage accounts migrated

from 1910 with suspended state.

Improved resiliency of VM provisioning, extension, and image operations.

Added PEP to retrieve current registration details, stale object cleanup for

Remove-Registration.

Improved reliability of log collection for SDN roles by collecting on file share.

Fixed an issue that erroneously raises an alert: “Node inaccessible for VM

Placement."

Removed invalid repair interface for seedringservices.

Improved SDN network reliability on the physical nodes.

Disabled winrm runner

Fixed a bug check and enforced external key protectors on cluster shared volumes.

Fixed an issue in which a storage account might be partially restored due to a KVS

race condition in the SRP background usage job.

Fixed an issue in which a virtual subnet was not being cleaned up if the tunnel was

moved to a different GW VM and then the VGW was deleted.

Fixed an issue that could cause registration and internal secret rotation to fail.

Fixed an issue in the internal secret rotation, which might cause a failure in the next

update.

Summary

Fixes rolled up from previous hotfix releases

Added memory specific settings to crash dump settings.

Restarted SQL VMs to mitigate potential issue with database access which affects

access to portal.

Remediated SMB handle invalidation issue triggered by ESENT error 59 event in

TableServer.

Included AzsInfraRoleSummary Test-Azurestack test as UpdateReadiness.

Remediated ERCS memory pressure during patch & update.

Include deployment provider identity certificate into the internal secret rotation.

Improved Network Controller stability.

Increased Network Controller log retention to aid in diagnosis.

Added Get-NetView as a part of Get-AzureStackLog collection by default.

Fixed an issue where marketplace downloads could fail due to a certificate

validation error.

Improved HealthAgent binary switchover logic.

Improved cluster shared volumes re-balance after Patch & Update (PnU).

Used ADSI to fetch localgroup members in HealthAgent.

Added the missing records, when WASP VMs fail to synchronize records and zones

by using DNS cmdlet during scale in and scale out.

Improved storage service reliability during PnU.

Removed public IP quota validation which caused an issue when creating an

internal load balancer.

Improved reliability of VM deletion: ensure new VMs that could not be fully

created or added to the cluster are deleted.

Check and enforce key protectors on cluster shared volumes.

Fixed "access denied" issue causing update and admin operations to fail.

Fixed WhsFaultScanner to re-launch when it gets stuck to make sure alerts are

correctly generated for users.

Fixed orchestration bug that prevented storage regeneration telemetry events

from being emitted.

Fixed an issue which impacted the reliability of downloading subsequent updates.

Improved ability to diagnose failures based on orchestrator telemetry.

Fixed SRP race condition in moving system storage accounts to system internal

subscription during 2005 PnU.

Fixed time unit scaling error in the server latency metrics

Restarted SQL VMs to mitigate potential issue with database access which affects

access to portal.

Fixed an issue in which the configuration of the retention period for deleted

storage accounts was reverted.

Improved reliability of storage blob and table service.

Addressed issue in the Send-AzureStackDiagnosticLog PEP cmdlet.

Increased the HRP repair time when an update failure occurs.

To apply this hotfix, you must have version 1.2005.6.53 or later.

Download the following files. Then, follow the instructions in Apply updates in Azure

Stack to apply this update.

Download the zip file now .

Download the hotfix xml file now .

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

Hotfix information

） Important

As outlined in the release notes for the 2005 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

More information

Azure Stack Hub hotfix 1.2008.27.118

Article • 09/21/2022

Patched SDN-related binaries on the physical nodes.

Improved reliability and diagnosing capabilities of patch and update.

Added auto-remediation for SQL cluster.

Updated Healthagent to use Nugetstore.

Filtered WHS alert for Netadapter.

Fixed an issue in which the copy of a certificate used by Service Fabric was

overwritten.

Fixed appearance of ghost NICs when deleting a resource group.

Fixed regression in Test-AzureStack that caused VM deployment test case to

automatically skip.

Improved resiliency of VM provisioning, extension, and image operations.

Fixed an invalid state in Storage resource provider for storage accounts migrated

from 1910 with suspended state.

Fixed a bug in local health system that potentially increased memory pressure on

infrastructure.

Fixed issue in internal secret rotation that would fail with a timeout error if valueadd resource providers were unhealthy.

Fixed a bug in which closed alerts' Last Modified Time was updated in the

operator portal even if the alert stayed closed.

Optimized operator alert request handling, which reduces the chance of timeouts

when viewing alerts in the operator portal or monitoring them via SCOM.

Check and enforce key protectors on cluster shared volumes per host.

Fixed issue in which Managed Disk usage data was not being reported after the

2008 update.

Fixed VMs losing connectivity while SuspendNode is occurring in MAS, as part of

host reboot during patch and update.

Added PEP to retrieve current registration details, stale object cleanup for

Remove-Registration.

Fixed a bug which caused the Infrastructure Roles panel in the operator portal to

display incorrect health information.

Summary

Fixes rolled up from previous hotfix releases

Improved reliability of log collection for SDN roles by collecting logs on the file

share.

Fixed an issue that can raise an audit scanner health alert in PEP cmdlet.

Removed invalid repair interface for seedringservices.

Improved SDN network reliability on the physical nodes.

Enabled SQL container logs.

Fixed an issue that erroneously raises an alert: “Node inaccessible for VM

Placement."

Fixed a remote management enabling issue for Azure Stack registrations done

prior to 1910 release.

Improved reliability of host node update.

Critical fix for disk space exhaustion on physical hosts, network controllers,

gateways, and load balancers.

Fixed remote management resource replication for resource arrays with

continuation token.

Fixed an issue in which a storage account might be partially restored due to a KVS

race condition in the SRP background usage job.

Fixed an issue in which a virtual subnet was not being cleaned up if the tunnel was

moved to a different GW VM and then the VGW was deleted.

Fixed an issue that could cause registration and internal secret rotation to fail.

Fixed an issue in the internal secret rotation, which might cause a failure in the next

update.

Addressed an issue with internal secret rotation for NRP with a large number of

subscriptions.

Mitigated connection problems to ERCS following startup.

Mitigated a potential issue with upgrading to future versions.

Addressed memory leak based on health runners and suppressed faulty alerts.

Added memory specific settings to crash dump settings.

Remediated ERCS memory pressure during patch & update.

Included AzsInfraRoleSummary Test-Azurestack test as UpdateReadiness.

Fixed an issue where certificate rotation on IoT Hub fails with “Internal execution

error.”

To apply this hotfix, you must have version 1.2008.13.88 or later.

Hotfix information

） Important

Download the following files. Then, follow the instructions in Apply updates in Azure

Stack to apply this update.

Download the zip file now .

Download the hotfix xml file now .

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

As outlined in the release notes for the 2008 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

More information

Azure Stack Hub hotfix 1.2005.32.106

Article • 09/21/2022

Fixed a bug in local health system that potentially increased memory pressure on

infrastructure.

Patched SDN-related binaries on the physical nodes.

Fixed an invalid state in Storage resource provider for storage accounts migrated

from 1910 with suspended state.

Improved resiliency of VM provisioning, extension, and image operations.

Added PEP to retrieve current registration details, stale object cleanup for

Remove-Registration.

Improved reliability of log collection for SDN roles by collecting on file share.

Fixed an issue that erroneously raises an alert: “Node inaccessible for VM

Placement."

Removed invalid repair interface for seedringservices.

Improved SDN network reliability on the physical nodes.

Disabled winrrm runner

Fixed a bug check and enforced external key protectors on cluster shared volumes.

Fixed an issue in which a storage account might be partially restored due to a KVS

race condition in the SRP background usage job.

Fixed an issue in which a virtual subnet was not being cleaned up if the tunnel was

moved to a different GW VM and then the VGW was deleted.

Fixed an issue that could cause registration and internal secret rotation to fail.

Fixed an issue in the internal secret rotation, which might cause a failure in the next

update.

Added memory specific settings to crash dump settings.

Restarted SQL VMs to mitigate potential issue with database access which affects

access to portal.

Remediated SMB handle invalidation issue triggered by ESENT error 59 event in

TableServer.

Included AzsInfraRoleSummary Test-Azurestack test as UpdateReadiness.

Remediated ERCS memory pressure during patch & update.

Include deployment provider identity certificate into the internal secret rotation.

Summary

Fixes rolled up from previous hotfix releases

Improved Network Controller stability.

Increased Network Controller log retention to aid in diagnosis.

Added Get-NetView as a part of Get-AzureStackLog collection by default.

Fixed an issue where marketplace downloads could fail due to a certificate

validation error.

Improved HealthAgent binary switchover logic.

Improved cluster shared volumes re-balance after Patch & Update (PnU).

Used ADSI to fetch localgroup members in HealthAgent.

Added the missing records, when WASP VMs fail to synchronize records and zones

by using DNS cmdlet during scale in and scale out.

Improved storage service reliability during PnU.

Removed public IP quota validation which caused an issue when creating an

internal load balancer.

Improved reliability of VM deletion: ensure new VMs that could not be fully

created or added to the cluster are deleted.

Check and enforce key protectors on cluster shared volumes.

Fixed "access denied" issue causing update and admin operations to fail.

Fixed WhsFaultScanner to re-launch when it gets stuck to make sure alerts are

correctly generated for users.

Fixed orchestration bug that prevented storage regeneration telemetry events

from being emitted.

Fixed an issue which impacted the reliability of downloading subsequent updates.

Improved ability to diagnose failures based on orchestrator telemetry.

Fixed SRP race condition in moving system storage accounts to system internal

subscription during 2005 PnU.

Fixed time unit scaling error in the server latency metrics

Restarted SQL VMs to mitigate potential issue with database access which affects

access to portal.

Fixed an issue in which the configuration of the retention period for deleted

storage accounts was reverted.

Improved reliability of storage blob and table service.

Addressed issue in the Send-AzureStackDiagnosticLog PEP cmdlet.

Increased the HRP repair time when an update failure occurs.

To apply this hotfix, you must have version 1.2005.6.53 or later.

Hotfix information

） Important

Download the following files. Then, follow the instructions in Apply updates in Azure

Stack to apply this update.

Download the zip file now .

Download the hotfix xml file now .

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

As outlined in the release notes for the 2005 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

More information

Azure Stack Hub hotfix 1.2002.67.175

Article • 09/21/2022

Patched SDN-related binaries on the physical nodes.

Fixed an invalid state in Storage Resource Provider for storage accounts migrated

from 1910 with suspended state.

Improved resiliency of VM provisioning and extension operations.

Improved SDN network reliability on the physical nodes.

Fixed an issue in which a virtual subnet was not being cleaned up if the tunnel was

moved to a different GW VM and then the VGW was deleted.

Fixed an issue that could cause registration and internal secret rotation to fail.

Added memory-specific settings to crash dump settings.

Remediated SMB handle invalidation issue triggered by ESENT error 59 event in

TableServer.

Fixed an issue which impacted the reliability of downloading subsequent updates.

Improved reliability of NuGet package installation after unexpected failure.

Fixed an issue where subscription dropdown validation fails when the user only has

RG write permission.

Fixed an issue in which the blob download page has an issue when downloading

large items.

Fixed an issue in which the configuration of the retention period for deleted

storage accounts is reverted.

Improved Network Controller stability.

Increased Network Controller log retention to aid in diagnosis.

Fixed an issue where marketplace downloads could fail due to a certificate

validation error.

Include deployment provider identity certificate into the internal secret rotation.

Fixed Windows storage WMI to keep call responsive, to improve the reliability of

storage management operations.

Added TPM status monitor for physical hosts.

Restarted SQL VMs to mitigate potential issue with database access which affects

access to portal.

Improved reliability of storage blob and table service.

Summary

Fixes rolled up from previous hotfix releases

Fixed an issue in which virtual machine scale set creation with the Standard\_DS2\_v2

SKU through UI always failed.

Configuration update improvements.

Fixed KVS enumerator leak in DiskRP to improve reliability of disk operations.

Re-enabled the ability to generate host crash dumps and trigger NMI crashes for

hangs.

Addressed DNS server vulnerability described in CVE-2020-1350.

Changes that addressed cluster instability.

Improved reliability of JEA endpoint creation.

Fixed bug to unblock concurrent VM creation in batch sizes of 20 or above.

Improved the reliability and stability of the portal, adding a monitoring capability

to restart the hosting service if it experiences any downtime.

Addressed an issue where some alerts were not paused during update.

Improved diagnostics around failures in DSC resources.

Improved error message generated by an unexpected failure in bare metal

deployment script.

Added resiliency during physical node repair operations.

Fixed a code defect that sometimes caused HRP SF app to become unhealthy. Also

fixed a code defect that prevented alerts from being suspended during update.

Added resiliency to image creation code when the destination path is

unexpectedly not present.

Added disk cleanup interface for ERCS VMs and ensured that it runs prior to

attempting to install new content to those VMs.

Improved quorum check for Service Fabric node repair in the auto-remediation

path.

Improved logic around bringing cluster nodes back online in rare cases where

outside intervention puts them into an unexpected state.

Improved resiliency of engine code to ensure typos in machine name casing do

not cause unexpected state in the ECE configuration when manual actions are used

to add and remove nodes.

Added a health check to detect VM or physical node repair operations that were

left in a partially completed state from previous support sessions.

Improved diagnostic logging for installation of content from NuGet packages

during update orchestration.

Fixed the internal secret rotation failure for customers who use AAD as identity

system, and block ERCS outbound internet connectivity.

Increased the default timeout of Test-AzureStack for AzsScenarios to 45 minutes.

Improved HealthAgent update reliability.

Fixed an issue where VM repair of ERCS VMs was not being triggered during

remediation actions.

Made host update resilient to issues caused by a silent failure to clean up stale

infrastructure VM files.

Added a preventative fix for certutil parsing errors when using randomly generated

passwords.

Added a round of health checks prior to the engine update, so that failed admin

operations can be allowed to continue running with their original version of

orchestration code.

Fixed ACS backup failure when the ACSSettingsService backup finished first.

Upgraded Azure Stack AD FS farm behavior level to v4. Azure Stack Hubs deployed

with 1908 or later are already on v4.

Improved reliability of the host update process.

Fixed a certificate renewal issue that could have caused internal secret rotation to

fail.

Fixed the new time server sync alert to correct an issue where it incorrectly detects

a time sync issue when the time source was specified with the 0x8 flag.

Corrected a validation constraint error that occurred when using the new

automatic log collection interface, and it detected https://login.windows.net/ as

an invalid Azure AD endpoint.

Fixed an issue that prevented the use of SQL auto backup via the

SQLIaaSExtension.

Corrected the alerting used in Test-AzureStack when validating the network

controller certificates.

Upgraded Azure Stack AD FS farm behavior level to v4. Azure Stack Hubs deployed

with 1908 or later are already on v4.

Improved reliability of the host update process.

Fixed a certificate renewal issue that could have caused internal secret rotation to

fail.

Reduced alert triggers in order to avoid unnecessary proactive log collections.

Improved reliability of storage upgrade by eliminating Windows Health Service

WMI call timeout.

To apply this hotfix, you must have version 1.2002.0.35 or later.

Hotfix information

） Important

As outlined in the release notes for the 2002 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

Download the following files. Then, follow the instructions in Apply updates in Azure

Stack to apply this update.

Download the zip file now .

Download the hotfix xml file now .

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

More information

Azure Stack Hub hotfix 1.2008.26.116

Article • 09/21/2022

Fixed appearance of ghost NICs when deleting a resource group.

Fixed regression in Test-AzureStack that caused VM deployment test case to

automatically skip.

Improved resiliency of VM provisioning, extension, and image operations.

Fixed an invalid state in Storage resource provider for storage accounts migrated

from 1910 with suspended state.

Fixed a bug in local health system that potentially increased memory pressure on

infrastructure.

Fixed issue in internal secret rotation that would fail with a timeout error if valueadd resource providers were unhealthy.

Fixed a bug in which closed alerts' Last Modified Time was updated in the

operator portal even if the alert stayed closed.

Optimized operator alert request handling, which reduces the chance of timeouts

when viewing alerts in the operator portal or monitoring them via SCOM.

Check and enforce key protectors on cluster shared volumes per host.

Fixed issue in which Managed Disk usage data was not being reported after the

2008 update.

Fixed VMs losing connectivity while SuspendNode is occurring in MAS, as part of

host reboot during patch and update.

Added PEP to retrieve current registration details, stale object cleanup for

Remove-Registration.

Fixed a bug which caused the Infrastructure Roles panel in the operator portal to

display incorrect health information.

Improved reliability of log collection for SDN roles by collecting logs on the file

share.

Fixed an issue that can raise an audit scanner health alert in PEP cmdlet.

Removed invalid repair interface for seedringservices.

Improved SDN network reliability on the physical nodes.

Enabled SQL container logs.

Summary

Fixes rolled up from previous hotfix releases

Fixed an issue that erroneously raises an alert: “Node inaccessible for VM

Placement."

Fixed a remote management enabling issue for Azure Stack registrations done

prior to 1910 release.

Improved reliability of host node update.

Critical fix for disk space exhaustion on physical hosts, network controllers,

gateways, and load balancers.

Fixed remote management resource replication for resource arrays with

continuation token.

Fixed an issue in which a storage account might be partially restored due to a KVS

race condition in the SRP background usage job.

Fixed an issue in which a virtual subnet was not being cleaned up if the tunnel was

moved to a different GW VM and then the VGW was deleted.

Fixed an issue that could cause registration and internal secret rotation to fail.

Fixed an issue in the internal secret rotation, which might cause a failure in the next

update.

Addressed an issue with internal secret rotation for NRP with a large number of

subscriptions.

Mitigated connection problems to ERCS following startup.

Mitigated a potential issue with upgrading to future versions.

Addressed memory leak based on health runners and suppressed faulty alerts.

Added memory specific settings to crash dump settings.

Remediated ERCS memory pressure during patch & update.

Included AzsInfraRoleSummary Test-Azurestack test as UpdateReadiness.

Fixed an issue where certificate rotation on IoT Hub fails with “Internal execution

error.”

To apply this hotfix, you must have version 1.2008.13.88 or later.

Hotfix information

） Important

As outlined in the release notes for the 2008 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

Download the following files. Then, follow the instructions in Apply updates in Azure

Stack to apply this update.

Download the zip file now .

Download the hotfix xml file now .

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

More information

Azure Stack Hub hotfix 1.2005.30.102

Article • 09/21/2022

Fixed an invalid state in Storage resource provider for storage accounts migrated

from 1910 with suspended state.

Improved resiliency of VM provisioning, extension, and image operations.

Added PEP to retrieve current registration details, stale object cleanup for

Remove-Registration.

Improved reliability of log collection for SDN roles by collecting on file share.

Fixed an issue that erroneously raises an alert: “Node inaccessible for VM

Placement."

Removed invalid repair interface for seedringservices.

Improved SDN network reliability on the physical nodes.

Disabled winrrm runner

Fixed a bug check and enforced external key protectors on cluster shared volumes.

Fixed an issue in which a storage account might be partially restored due to a KVS

race condition in the SRP background usage job.

Fixed an issue in which a virtual subnet was not being cleaned up if the tunnel was

moved to a different GW VM and then the VGW was deleted.

Fixed an issue that could cause registration and internal secret rotation to fail.

Fixed an issue in the internal secret rotation, which might cause a failure in the next

update.

Added memory specific settings to crash dump settings.

Restarted SQL VMs to mitigate potential issue with database access which affects

access to portal.

Remediated SMB handle invalidation issue triggered by ESENT error 59 event in

TableServer.

Included AzsInfraRoleSummary Test-Azurestack test as UpdateReadiness.

Remediated ERCS memory pressure during patch & update.

Include deployment provider identity certificate into the internal secret rotation.

Improved Network Controller stability.

Increased Network Controller log retention to aid in diagnosis.

Added Get-NetView as a part of Get-AzureStackLog collection by default.

Summary

Fixes rolled up from previous hotfix releases

Fixed an issue where marketplace downloads could fail due to a certificate

validation error.

Improved HealthAgent binary switchover logic.

Improved cluster shared volumes re-balance after Patch & Update (PnU).

Used ADSI to fetch localgroup members in HealthAgent.

Added the missing records, when WASP VMs fail to synchronize records and zones

by using DNS cmdlet during scale in and scale out.

Improved storage service reliability during PnU.

Removed public IP quota validation which caused an issue when creating an

internal load balancer.

Improved reliability of VM deletion: ensure new VMs that could not be fully

created or added to the cluster are deleted.

Check and enforce key protectors on cluster shared volumes.

Fixed "access denied" issue causing update and admin operations to fail.

Fixed WhsFaultScanner to re-launch when it gets stuck to make sure alerts are

correctly generated for users.

Fixed orchestration bug that prevented storage regeneration telemetry events

from being emitted.

Fixed an issue which impacted the reliability of downloading subsequent updates.

Improved ability to diagnose failures based on orchestrator telemetry.

Fixed SRP race condition in moving system storage accounts to system internal

subscription during 2005 PnU.

Fixed time unit scaling error in the server latency metrics

Restarted SQL VMs to mitigate potential issue with database access which affects

access to portal.

Fixed an issue in which the configuration of the retention period for deleted

storage accounts was reverted.

Improved reliability of storage blob and table service.

Addressed issue in the Send-AzureStackDiagnosticLog PEP cmdlet.

Increased the HRP repair time when an update failure occurs.

To apply this hotfix, you must have version 1.2005.6.53 or later.

Hotfix information

） Important

As outlined in the release notes for the 2005 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

Download the following files. Then, follow the instructions in Apply updates in Azure

Stack to apply this update.

Download the zip file now .

Download the hotfix xml file now .

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

More information

Azure Stack Hub hotfix 1.2002.66.173

Article • 09/21/2022

Fixed an invalid state in Storage Resource Provider for storage accounts migrated

from 1910 with suspended state.

Improved resiliency of VM provisioning and extension operations.

Improved SDN network reliability on the physical nodes.

Fixed an issue in which a virtual subnet was not being cleaned up if the tunnel was

moved to a different GW VM and then the VGW was deleted.

Fixed an issue that could cause registration and internal secret rotation to fail.

Added memory-specific settings to crash dump settings.

Remediated SMB handle invalidation issue triggered by ESENT error 59 event in

TableServer.

Fixed an issue which impacted the reliability of downloading subsequent updates.

Improved reliability of NuGet package installation after unexpected failure.

Fixed an issue where subscription dropdown validation fails when the user only has

RG write permission.

Fixed an issue in which the blob download page has an issue when downloading

large items.

Fixed an issue in which the configuration of the retention period for deleted

storage accounts is reverted.

Improved Network Controller stability.

Increased Network Controller log retention to aid in diagnosis.

Fixed an issue where marketplace downloads could fail due to a certificate

validation error.

Include deployment provider identity certificate into the internal secret rotation.

Fixed Windows storage WMI to keep call responsive, to improve the reliability of

storage management operations.

Added TPM status monitor for physical hosts.

Restarted SQL VMs to mitigate potential issue with database access which affects

access to portal.

Improved reliability of storage blob and table service.

Summary

Fixes rolled up from previous hotfix releases

Fixed an issue in which virtual machine scale set creation with the Standard\_DS2\_v2

SKU through UI always failed.

Configuration update improvements.

Fixed KVS enumerator leak in DiskRP to improve reliability of disk operations.

Re-enabled the ability to generate host crash dumps and trigger NMI crashes for

hangs.

Addressed DNS server vulnerability described in CVE-2020-1350.

Changes that addressed cluster instability.

Improved reliability of JEA endpoint creation.

Fixed bug to unblock concurrent VM creation in batch sizes of 20 or above.

Improved the reliability and stability of the portal, adding a monitoring capability

to restart the hosting service if it experiences any downtime.

Addressed an issue where some alerts were not paused during update.

Improved diagnostics around failures in DSC resources.

Improved error message generated by an unexpected failure in bare metal

deployment script.

Added resiliency during physical node repair operations.

Fixed a code defect that sometimes caused HRP SF app to become unhealthy. Also

fixed a code defect that prevented alerts from being suspended during update.

Added resiliency to image creation code when the destination path is

unexpectedly not present.

Added disk cleanup interface for ERCS VMs and ensured that it runs prior to

attempting to install new content to those VMs.

Improved quorum check for Service Fabric node repair in the auto-remediation

path.

Improved logic around bringing cluster nodes back online in rare cases where

outside intervention puts them into an unexpected state.

Improved resiliency of engine code to ensure typos in machine name casing do

not cause unexpected state in the ECE configuration when manual actions are used

to add and remove nodes.

Added a health check to detect VM or physical node repair operations that were

left in a partially completed state from previous support sessions.

Improved diagnostic logging for installation of content from NuGet packages

during update orchestration.

Fixed the internal secret rotation failure for customers who use AAD as identity

system, and block ERCS outbound internet connectivity.

Increased the default timeout of Test-AzureStack for AzsScenarios to 45 minutes.

Improved HealthAgent update reliability.

Fixed an issue where VM repair of ERCS VMs was not being triggered during

remediation actions.

Made host update resilient to issues caused by a silent failure to clean up stale

infrastructure VM files.

Added a preventative fix for certutil parsing errors when using randomly generated

passwords.

Added a round of health checks prior to the engine update, so that failed admin

operations can be allowed to continue running with their original version of

orchestration code.

Fixed ACS backup failure when the ACSSettingsService backup finished first.

Upgraded Azure Stack AD FS farm behavior level to v4. Azure Stack Hubs deployed

with 1908 or later are already on v4.

Improved reliability of the host update process.

Fixed a certificate renewal issue that could have caused internal secret rotation to

fail.

Fixed the new time server sync alert to correct an issue where it incorrectly detects

a time sync issue when the time source was specified with the 0x8 flag.

Corrected a validation constraint error that occurred when using the new

automatic log collection interface, and it detected https://login.windows.net/ as

an invalid Azure AD endpoint.

Fixed an issue that prevented the use of SQL auto backup via the

SQLIaaSExtension.

Corrected the alerting used in Test-AzureStack when validating the network

controller certificates.

Upgraded Azure Stack AD FS farm behavior level to v4. Azure Stack Hubs deployed

with 1908 or later are already on v4.

Improved reliability of the host update process.

Fixed a certificate renewal issue that could have caused internal secret rotation to

fail.

Reduced alert triggers in order to avoid unnecessary proactive log collections.

Improved reliability of storage upgrade by eliminating Windows Health Service

WMI call timeout.

To apply this hotfix, you must have version 1.2002.0.35 or later.

Hotfix information

） Important

As outlined in the release notes for the 2002 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

Download the following files. Then, follow the instructions in Apply updates in Azure

Stack to apply this update.

Download the zip file now .

Download the hotfix xml file now .

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

More information

Azure Stack Hub hotfix 1.2008.25.114

Article • 09/21/2022

Fixed issue in internal secret rotation that would fail with a timeout error if valueadd resource providers were unhealthy.

Fixed a bug in which closed alerts' Last Modified Time was updated in the

operator portal even if the alert stayed closed.

Optimized operator alert request handling, which reduces the chance of timeouts

when viewing alerts in the operator portal or monitoring them via System Center

Operations Manager.

Check and enforce key protectors on cluster shared volumes per host.

Fixed issue in which Managed Disk usage data was not being reported after the

2008 update.

Fixed VMs losing connectivity while SuspendNode is occurring in MAS, as part of

host reboot during patch and update.

Added PEP to retrieve current registration details, stale object cleanup for

Remove-Registration.

Fixed a bug which caused the Infrastructure Roles panel in the operator portal to

display incorrect health information.

Improved reliability of log collection for SDN roles by collecting logs on the file

share.

Fixed an issue that can raise an audit scanner health alert in PEP cmdlet.

Removed invalid repair interface for seedringservices.

Improved SDN network reliability on the physical nodes.

Enabled SQL container logs.

Fixed an issue that erroneously raises an alert: “Node inaccessible for VM

Placement."

Fixed a remote management enabling issue for Azure Stack registrations done

prior to 1910 release.

Improved reliability of host node update.

Critical fix for disk space exhaustion on physical hosts, network controllers,

gateways, and load balancers.

Summary

Fixes rolled up from previous hotfix releases

Fixed remote management resource replication for resource arrays with

continuation token.

Fixed an issue in which a storage account might be partially restored due to a KVS

race condition in the SRP background usage job.

Fixed an issue in which a virtual subnet was not being cleaned up if the tunnel was

moved to a different GW VM and then the VGW was deleted.

Fixed an issue that could cause registration and internal secret rotation to fail.

Fixed an issue in the internal secret rotation, which might cause a failure in the next

update.

Addressed an issue with internal secret rotation for NRP with a large number of

subscriptions.

Mitigated connection problems to ERCS following startup.

Mitigated a potential issue with upgrading to future versions.

Addressed memory leak based on health runners and suppressed faulty alerts.

Added memory specific settings to crash dump settings.

Remediated ERCS memory pressure during patch & update.

Included AzsInfraRoleSummary Test-Azurestack test as UpdateReadiness.

Fixed an issue where certificate rotation on IoT Hub fails with “Internal execution

error.”

To apply this hotfix, you must have version 1.2008.13.88 or later.

Download the following files. Then, follow the instructions in Apply updates in Azure

Stack to apply this update.

Download the zip file now .

Download the hotfix xml file now .

Hotfix information

） Important

As outlined in the release notes for the 2008 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

File information

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

More information

Azure Stack Hub hotfix 1.2005.29.100

Article • 09/21/2022

Added PEP to retrieve current registration details, stale object cleanup for RemoveRegistration.

Improved reliability of log collection for SDN roles by collecting on file share.

Fixed an issue that erroneously raises an alert: “Node inaccessible for VM

Placement."

Removed invalid repair interface for seedringservices.

Improved SDN network reliability on the physical nodes.

Disabled winrrm runner

Fixed a bug check and enforced external key protectors on cluster shared volumes.

Fixed an issue in which a storage account might be partially restored due to a KVS

race condition in the SRP background usage job.

Fixed an issue in which a virtual subnet was not being cleaned up if the tunnel was

moved to a different GW VM and then the VGW was deleted.

Fixed an issue that could cause registration and internal secret rotation to fail.

Fixed an issue in the internal secret rotation, which might cause a failure in the next

update.

Added memory specific settings to crash dump settings.

Restarted SQL VMs to mitigate potential issue with database access which affects

access to portal.

Remediated SMB handle invalidation issue triggered by ESENT error 59 event in

TableServer.

Included AzsInfraRoleSummary Test-Azurestack test as UpdateReadiness.

Remediated ERCS memory pressure during patch & update.

Include deployment provider identity certificate into the internal secret rotation.

Improved Network Controller stability.

Increased Network Controller log retention to aid in diagnosis.

Added Get-NetView as a part of Get-AzureStackLog collection by default.

Fixed an issue where marketplace downloads could fail due to a certificate

validation error.

Improved HealthAgent binary switchover logic.

Summary

Fixes rolled up from previous hotfix releases

Improved cluster shared volumes re-balance after Patch & Update (PnU).

Used ADSI to fetch localgroup members in HealthAgent.

Added the missing records, when WASP VMs fail to synchronize records and zones

by using DNS cmdlet during scale in and scale out.

Improved storage service reliability during PnU.

Removed public IP quota validation which caused an issue when creating an

internal load balancer.

Improved reliability of VM deletion: ensure new VMs that could not be fully

created or added to the cluster are deleted.

Check and enforce key protectors on cluster shared volumes.

Fixed "access denied" issue causing update and admin operations to fail.

Fixed WhsFaultScanner to re-launch when it gets stuck to make sure alerts are

correctly generated for users.

Fixed orchestration bug that prevented storage regeneration telemetry events

from being emitted.

Fixed an issue which impacted the reliability of downloading subsequent updates.

Improved ability to diagnose failures based on orchestrator telemetry.

Fixed SRP race condition in moving system storage accounts to system internal

subscription during 2005 PnU.

Fixed time unit scaling error in the server latency metrics

Restarted SQL VMs to mitigate potential issue with database access which affects

access to portal.

Fixed an issue in which the configuration of the retention period for deleted

storage accounts was reverted.

Improved reliability of storage blob and table service.

Addressed issue in the Send-AzureStackDiagnosticLog PEP cmdlet.

Increased the HRP repair time when an update failure occurs.

To apply this hotfix, you must have version 1.2005.6.53 or later.

Hotfix information

） Important

As outlined in the release notes for the 2005 update, make sure that you refer to

the update activity checklist on running Test-AzureStack (with specified

parameters), and resolve any operational issues that are found, including all

warnings and failures. Also, review active alerts and resolve any that require action.

Download the following files. Then, follow the instructions in Apply updates in Azure

Stack to apply this update.

Download the zip file now .

Download the hotfix xml file now .

Azure Stack Hub update resources

Apply updates in Azure Stack

Monitor updates in Azure Stack by using the privileged endpoint

File information

More information

Azure Stack Hub known issues

Article • 09/14/2023

This article lists known issues in Azure Stack Hub releases. The list is updated as new

issues are identified.

To access known issues for a different version, use the version selector dropdown above

the table of contents on the left.

You can access older versions of Azure Stack Hub known issues in the table of contents

on the left side, under the Resources > Release notes archive. Select the desired

archived version from the version selector dropdown in the upper left. These archived

articles are provided for reference purposes only and do not imply support for these

versions. For information about Azure Stack Hub support, see Azure Stack Hub servicing

policy. For further assistance, contact Microsoft Customer Support Services.

） Important

If your Azure Stack Hub instance is behind by more than two updates, it's

considered out of compliance. You must update to at least the minimum

supported version to receive support.

2102 archived known issues

Manage updates in Azure Stack Hub

Article • 11/14/2022

Full and express updates, hotfixes, as well as driver and firmware updates from the

original equipment manufacturer (OEM) all help keep Azure Stack Hub up to date. This

article explains the different types of updates, when to expect their release, and where

to find more about the current release.

There are three types of update packages for integrated systems:

Azure Stack Hub software updates. Microsoft is responsible for the end-to-end

servicing lifecycle for the Microsoft software update packages. These packages can

include the latest Windows Server security updates, non-security updates, and

Azure Stack Hub feature updates. You download theses update packages directly

from Microsoft.

Each update package has a corresponding type: Full or Express.

Full update packages update the physical host operating systems in the scale unit

and require a larger maintenance window.

Express update packages are scoped and don't update the underlying physical

host operating systems.

Azure Stack Hub hotfixes. Microsoft provides hotfixes for Azure Stack Hub that

address a specific issue that's often preventive or time-sensitive. Each hotfix is

released with a corresponding Microsoft Knowledge Base article that details the

fixes in that package. You download and install hotfixes just like the regular full

update packages for Azure Stack Hub. Hotfixes are cumulative and can install in

minutes.

Before you update to the new major version, apply the latest hotfix in the current

major version.

７ Note

You can't apply Azure Stack Hub update packages to the Azure Stack Development

Kit (ASDK). The update packages are designed for integrated systems. For

information, see Redeploy the ASDK.

Update package types

Starting with build 2005, when you update to a new major version (for example,

1.2005.x to 1.2008.x), the latest hotfixes (if any are available at the time of package

download) in the new major version are installed automatically. Your 2008

installation is then current with all hotfixes. From that point forward, if a hotfix is

released for 2008, you should install it.

OEM hardware-vendor-provided updates. Azure Stack Hub hardware partners are

responsible for the end-to-end servicing lifecycle (including guidance) for the

hardware-related firmware and driver update packages. In addition, Azure Stack

Hub hardware partners own and maintain guidance for all software and hardware

on the hardware lifecycle host. The OEM hardware vendor hosts these update

packages on their own download site.

The three types of updates are released with the following cadence:

Azure Stack Hub software updates. Microsoft releases multiple full and express

software update packages per year.

Azure Stack Hub hotfixes. Hotfixes are time-sensitive releases that can be released

at any time. If you are upgrading from one major version to another (for example,

1.2002.x to 1.2005.x), the latest hotfixes, if any have been released for that new

major version, are installed automatically.

OEM hardware vendor-provided updates. OEM hardware vendors release their

updates on an as-needed basis.

To continue to receive support, you must keep your Azure Stack Hub environment on a

supported Azure Stack Hub software version. For more information, see Azure Stack Hub

Servicing Policy.

Notice of updates varies on a couple of factors, such as your connection to the internet

and the type of update.

When to update

） Important

Make sure you have installed the latest available OEM update version before

installing the latest MS version.

How to know an update is available

Microsoft software updates and hotfixes

An update alert for Microsoft software updates and hotfixes will appear in the

Update blade for Azure Stack Hub instances that are connected to the internet.

If your instance isn't connected and you would like to be notified about each hotfix

release, subscribe to the RSS feed .

OEM hardware vendor-provided updates

OEM updates depend on your manufacturer. You must establish a communication

channel with your OEM so that you can be aware of updates from your OEM that

need to be applied. For more information about the OEMs and the OEM update

process, see Apply Azure Stack Hub original equipment manufacturer (OEM)

updates.

An update from major version to major version must be step by step: the current

environment can only update to the next major version, and you can't skip a major

version update.

For example, if your Azure Stack Hub environment is 1908.x, and the latest available

update version is 2002.x, you should update from 1908 to 1910, then update to 2002.

Starting with build 2005, when you update to a new major version (for example, 1.2002.x

to 1.2005.x), the latest hotfixes (if any) in the new major version are installed

automatically.

Within the same major version number, Azure Stack Hub may release multiple hotfixes.

Hotfixes are cumulative; the latest hotfix package includes all past hotfixes for that

version. For more information, see Hotfixes.

Once you know you have an update, apply it by using the following steps.

Major version to major version

Hotfixes within major versions

Update process

1. Plan for the update

Prepare your Azure Stack Hub to make the update process go as smoothly as

possible so that there's minimal impact on your users. Notify your users of any

possible service outage and then follow the steps to prepare your instance for the

update. Be sure to follow all steps in the Azure Stack Hub pre-update checklist to

ensure that you've completed the required prerequisites for applying an update.

Also make sure to schedule an appropriate maintenance window for the update

type being applied.

2. Upload and prepare the update package

For internet-connected Azure Stack Hub environments, Azure Stack Hub software

updates and hotfixes are automatically imported into the system and prepared for

update.

For internet-disconnected Azure Stack Hub environments and environments with

weak or intermittent internet connectivity, update packages are imported into

Azure Stack Hub storage via the Azure Stack Hub administrator portal. For more

steps to upload and prepare the update package, see Upload and prepare an

Azure Stack Hub update package.

All OEM update packages are manually imported into your environment,

regardless of your Azure Stack Hub system's internet connectivity. For more steps

to import and prepare the update package, see Upload and prepare an Azure

Stack Hub update package.

） Important

Before proceeding with the update, make sure that the culture session

settings are set correctly using PowerShell. A culture is a locale for

unmanaged code development. The information includes the names for the

culture, the alphabet, the calendar, and formatting for dates and strings. For

more information, see the CultureInfo class.

3. Apply the update

Apply the update using the Update blade in the Azure Stack Hub portal. During

the update, monitor and troubleshoot the update progress. For more information,

see Apply an Azure Stack Hub update.

Azure Stack Hub includes an update resource provider that handles the application of

Microsoft software updates. This provider checks that updates are applied across all

physical hosts, Service Fabric apps and runtimes, and all infrastructure virtual machines

and their associated services.

As updates install, you can view high-level status as the update process targets the

various subsystems in Azure Stack Hub (for example, physical hosts and infrastructure

virtual machines).

To begin the update process, follow the steps in see Azure Stack Hub update

activity checklist.

To learn what versions of Azure Stack Hub are in support, see Azure Stack Hub

Servicing Policy.

To learn more about the current and recent updates, see the Azure Stack Hub

release notes.

The update resource provider

Next steps

Azure Stack Hub servicing policy

Article • 09/12/2023

Azure Stack Hub follows the Modern Lifecycle Policy. This article describes the servicing

policy for Azure Stack Hub integrated systems and what you must do to keep your

system in a supported state.

Microsoft releases both full update packages and hotfix packages to address specific

issues.

Full update packages are hosted in a secure Azure endpoint. You can download them

manually using the Azure Stack Hub Updates downloader tool . If your scale unit is

connected, the update appears automatically in the administrator portal as Update

available. For more information about each release, you can click any release from the

Update package release cadence section of this article.

Hotfix update packages are hosted in the same secure Azure endpoint. You can

download them using the embedded links in each of the respective hotfix KB articles; for

example, Azure Stack Hub Hotfix 1.1809.12.114 . Similar to the full, monthly update

packages, Azure Stack Hub operators can download the .xml and .zip files and import

them using the procedure in Apply updates in Azure Stack Hub. Azure Stack Hub

operators with connected scale units will see the hotfixes automatically appear in the

administrator portal with the message Update available.

If your scale unit isn't connected and you want to be notified about each hotfix release,

subscribe to the RSS feed to be notified about each hotfix release.

There are two types of update packages for integrated systems:

Microsoft software updates. Microsoft is responsible for the end-to-end servicing

lifecycle for the Microsoft software update packages. These packages can include

the latest Windows Server security updates, non-security updates, and Azure Stack

Hub feature updates. You can download theses update packages directly from

Microsoft.

Download update packages for integrated

systems

Update package types

OEM hardware vendor-provided updates. Azure Stack Hub hardware partners are

responsible for the end-to-end servicing lifecycle (including guidance) for the

hardware-related firmware and driver update packages. In addition, Azure Stack

Hub hardware partners own and maintain guidance for all software and hardware

on the hardware lifecycle host. The OEM hardware vendor hosts these update

packages on their own download site.

Microsoft expects to release software update packages multiple times throughout the

year.

OEM hardware vendors release their updates on an as-needed basis. Check with your

OEM for the latest updates to hardware.

Find documentation on how to plan for and manage updates, and how to determine

your current version in Manage updates overview.

For information about a specific update, including how to download it, see the release

notes for that update:

Azure Stack Hub 2306 update

Azure Stack Hub 2301 update

Azure Stack Hub 2206 update

Occasionally, Microsoft provides hotfixes for Azure Stack Hub that address a specific

issue that's often preventative or time-sensitive. Each hotfix is released with a

corresponding Microsoft Knowledge Base (KB) article that details the issues addressed in

that hotfix.

Hotfixes are downloaded and installed just like the regular full update packages for

Azure Stack Hub. However, unlike a full update, hotfixes can install in minutes. We

recommend Azure Stack Hub operators set maintenance windows when installing

hotfixes. Hotfixes update the version of your Azure Stack Hub cloud so you can easily

determine if the hotfix has been applied. A separate hotfix is provided for each version

of Azure Stack Hub that's still in support. Each hotfix for a specific iteration is

cumulative and includes the previous hotfixes for that same version. You can read

more about the applicability of a specific hotfix in the corresponding KB article. See the

release notes links in the previous section.

Update package release cadence

Hotfixes

Before you update to a new major version, apply the latest hotfix in the current major

version. It is recommended that cloud operators keep their scale units updated with

hotfixes as they are released; for example, installing hotfixes within 45 days of their

release date, if possible.

Starting with build 2005, when you update to a new major version (for example, 1.2005.x

to 1.2008.x), the latest hotfixes (if any are available at the time of package download) in

the new major version are installed automatically. Your 2008 installation is then current

with all hotfixes. From that point forward, if a hotfix is released for 2008, you should

install it.

For information about currently available hotfixes, see the release notes "Hotfixes"

section for that update.

Operators should maintain their OEM packages, and the recommendation is to be

within N-2 OEM packages.

For your Azure Stack Hub instance to remain in a supported state, the instance must run

the most recently released update version (N) or run either of the two preceding update

versions (N-1, N-2). The following support restrictions apply to systems that aren't

within our general two preceding versions support policy:

Hotfixes for the platform are provided for the current version and two preceding

versions (N-1, N-2).

Root Cause Analysis (RCA) is provided for the current version and two preceding

versions (N-1, N-2).

Issues on systems for unsupported versions (preceding N-2) are not entitled to

receive support from Microsoft unless you're performing an update.

You must also have an active support agreement with the hardware partner that

manufactured the system. Microsoft is not able to support you without a hardware

support agreement in place.

Hotfixes aren't considered major update versions. If your Azure Stack Hub instance is

behind by more than two updates, it's considered out of compliance. You must update

to at least the minimum supported version (N-2) to receive support.

OEM packages

Keep your system under support

For example, if the most recent update version available is 2206 (N), the two previous

update versions were 2108 and 2102, which means both 2108 (N-1) and 2102 (N-2)

remain in support. However, the 2008 version would be out of support, as 2008 would

be N-3 when the 2206 update was released.

Microsoft software update packages are non-cumulative and require the previous

update package and latest hotfix to be installed as a prerequisite. If you decide to defer

one or more updates, consider the overall runtime required to update to the latest

version.

For Azure Stack Hub resource providers, it's important to note that only the most

recently released version of a given resource provider that is compatible with your

supported version of Azure Stack Hub is supported, even though you may be using an

older version of Azure Stack Hub that is still within the support window.

For more information about resource provider compatibility, see the release notes for

that specific resource provider.

Azure Stack Hub follows the same support process as Azure. Enterprise customers can

follow the process described in How to create an Azure support request. If you're a

customer of a Cloud Solution Provider (CSP), contact your CSP for support. For more

information, see the Azure Support FAQs .

For help with troubleshooting update issues, see Best practices for troubleshooting

Azure Stack Hub patch and update issues.

Manage updates in Azure Stack Hub

Best practices for troubleshooting Azure Stack Hub patch and update issues

Resource provider version support

Get support

Next steps

Azure Stack Hub update activity

checklist

Article • 07/29/2022

Review this checklist in order to prepare for an Azure Stack Hub update. This article

contains a checklist of update-related activities for Azure Stack Hub operators.

Activity

Details

Review

known

issues

List of known issues.

Review

security

updates

List of security updates.

Review addon resource

provider

updates

App Service

Event Hubs

MySQL

SQL

Apply latest

OEM

package

Contact your OEM to ensure your system meets the minimum OEM package

requirements for the Azure Stack Hub version your system is being updated to.

Ensure your OEM package is compatible with the Azure Stack Hub version you are

updating to. If your OEM package is not compatible with the Azure Stack Hub

version you are updating to, you will need to perform an OEM package update

before running an Azure Stack Hub update. For instructions, see "Apply Azure

Stack Hub original equipment manufacturer (OEM) updates."

Optional:

Configure

automatic

log

collection

It is recommended that you configure automatic log collection on your Azure

Stack Hub environment to streamline the process of collecting system logs in the

event that you need to open a support ticket. To configure automatic log

collection, see the instructions in Send logs proactively.

Apply latest

hotfixes

Apply the latest hotfixes that apply to the currently installed release. For a list of

the latest hotfixes, see the release notes Hotfixes section.

Prepare for Azure Stack Hub update

Activity

Details

Run capacity

planner tool

Make sure to use the latest version of the Azure Stack Hub Capacity Planner tool

to perform your workload planning and sizing. The latest version contains bug

fixes and provides new features that are released with each Azure Stack Hub

update.

Run TestAzureStack

Run Test-AzureStack -Group UpdateReadiness to identify operational issues. The

cmdlet is accessible through the Privileged Endpoint Session (PEP). For more

information, see Validate Azure Stack Hub system state.

Resolve

issues

Resolve any operational issues identified by Test-AzureStack .

Update

available

In connected scenarios only, Azure Stack Hub deployments periodically check a

secured endpoint and automatically notify you if an update is available for your

cloud. Disconnected customers can download and import new packages using the

process described here.

Schedule a

maintenance

window and

notify your

users

You should notify users of any maintenance operations, and schedule normal

maintenance windows during non-business hours if possible. Maintenance

operations can affect existing tenant workloads and cause new tenants operations

(for example, creating, reconfiguring, or deleting VMs) to fail - whether the

operation is initiated from the portal or programmatically from the Azure Resource

Manager API. Other operations such as backup may also be unavailable until the

update is complete. For Azure Stack Hub express and full updates, you can check

the release notes for a forecast of how long the update is expected to take for the

version you are applying.

Activity Details

Manage the

update

Manage updates in Azure Stack Hub using the operator portal.

Monitor the

update

If the operator portal is unavailable, monitor updates in Azure Stack Hub using

the privileged endpoint.

Resume

updates

After remediating a failed update, resume updates in Azure Stack Hub using the

privileged endpoint.

During Azure Stack Hub update

） Important

Activity Details

Apply

latest

hotfixes

Apply the latest hotfixes applicable to the updated version.

Retrieve

encryption

keys

Retrieve the data at rest encryption keys and securely store them outside of your

Azure Stack Hub deployment. Follow the instructions on how to retrieve the keys.

Re-enable

multitenancy

In case of a multi-tenanted Azure Stack Hub, make sure you configure all guest

directory tenants after a successful update.

Review list of known issues

Review list of security updates

Do not run Test-AzureStack during an update, as this causes the update to stall.

Do not run node repair during an update regardless of its state. Please contact

Microsoft Support if node repair is needed during update.

After Azure Stack Hub update

Next steps

Prepare an Azure Stack Hub update

package

Article • 11/25/2021

This article provides an overview of preparing Azure Stack Hub update packages so they

can be used to update your Azure Stack Hub environment. This process consists of the

following steps:

Download the update package.

Import the update package into your Azure Stack Hub environment using the

Azure Stack Hub administrator portal.

On systems that can connect to the automatic update endpoints, Azure Stack Hub

software updates and hotfixes are automatically downloaded and prepared. On systems

without connectivity, and for any update from the original equipment manufacturer

(OEM), the update package must be prepared as explained in this article.

The following table shows when update packages require manual preparation and when

they're prepared automatically.

Update Type Connectivity Action Required

Azure Stack Hub

software updates

Connected Update is automatically downloaded and prepared

when the update is applied.

Azure Stack Hub

hotfixes

Connected Update is automatically downloaded and prepared

when the update is applied.

OEM package

updates

Connected The update package must be prepared. Follow the

steps in this article.

Azure Stack Hub

software updates

Disconnected or

weak connection

The update package must be prepared. Follow the

steps in this article.

Azure Stack Hub

hotfixes

Disconnected or

weak connection

The update package must be prepared. Follow the

steps in this article.

OEM package

updates

Disconnected or

weak connection

The update package must be prepared. Follow the

steps in this article.

The update package for Azure Stack Hub updates and hotfixes is available for connected

systems through the update blade in the portal. Download the package and move the

Download the update package

package to a location that's accessible to your Azure Stack Hub instance if you're

updating an OEM package or if you're supporting a disconnected system. You also

might need to download and then upload the package to an accessible location if

you're running a system with an intermittent connection.

Review the package contents. An update package typically consists of the following files:

One or more .zip files named <PackageName>.zip. These files contain the payload

for the update.

A metadata.xml file. This file contains essential information about the update; for

example, the publisher, name, prerequisite, size, and support path URL.

SHA256 hashes are computed for the .zip file(s) with update package content and

inserted into the metadata.xml associated with the package. The metadata.xml file itself

is signed with an embedded signature using a certificate trusted by the Azure Stack Hub

system.

Azure Stack Hub software updates and hotfixes are prepared automatically for systems

with connectivity to the Azure Stack Hub automatic update endpoints:

https://\*.azureedge.net and https://aka.ms/azurestackautomaticupdate . For more

information about setting up connectivity to the Azure Stack Hub automatic update

endpoints, see the Patch and Update endpoints described in Azure Stack Hub firewall

integration.

Azure Stack Hub updates for full and express updates are hosted at a secure Azure

endpoint. When updates become available, Azure Stack Hub operators with connected

instances will see the Azure Stack Hub updates automatically appear in the

administrator portal.

For disconnected systems or systems with weak internet connectivity, full update

packages can be downloaded using the Azure Stack Hub updates downloader tool .

Hotfix packages can be downloaded from the hotfix KB link listed in Azure Stack Hub

release notes. Azure Stack Hub software update packages may contain updates to Azure

Stack Hub services and updates to the operating system of your Azure Stack Hub's scale

units.

Automatic download and preparation for update

packages

Where to download Azure Stack Hub update packages

Packages for Azure Stack Hub hotfixes are hosted in the same secure Azure endpoint as

Azure Stack Hub updates. Azure Stack Hub operators with connected instances will see

the Azure Stack Hub updates automatically appear in the administrator portal when they

become available. You can download them using the embedded links in each of the

respective hotfix KB articles. You can also find links to hotfix KB articles in the release

notes corresponding to your Azure Stack Hub version.

Your OEM vendor might also release updates, such as driver and firmware updates.

While these updates are delivered as separate OEM package updates by your hardware

vendor, they're still imported, installed, and managed the same way as update packages

from Microsoft. You can find a list of vendor contact links in the article Apply Azure

Stack Hub OEM updates.

The following procedure shows how to import and install update packages in the

administrator portal.

1. In the administrator portal, select All services. Then, under the STORAGE category,

select Storage accounts. Or, in the filter box, start typing storage accounts, and

then select it.

７ Note

The update package itself and its contents (such as binaries, PowerShell scripts, and

so on) are signed with Microsoft-owned certificates. Tampering with the package

will make the signature invalid.

Where to download Azure Stack Hub hotfix packages

Where to download OEM update packages

Import and install updates

） Important

Notify users of any maintenance operations, and ensure you schedule normal

maintenance windows during non-business hours as much as possible.

Maintenance operations can affect both user workloads and portal operations.

2. In the filter box, type update, and select the updateadminaccount storage

account.

3. In All services, under Essentials or Blob service, select Containers.

4. In Containers, select + Container to create a container. Enter a name (for example,

update-2102), and then select Create.





5. After the container is created, select the container name, and then select Upload to

upload the package files to the container.

6. Under Upload blob, select the folder icon, browse to the update package .zip file,

and then select Open in the file explorer window.

7. Under Upload blob, select Upload.

8. Repeat steps 6 and 7 for the Metadata.xml file and any additional .zip files in the

update package. Don't import the Supplemental Notice.txt file if included.

9. When done, you can review the notifications (select the bell icon in the top-right

corner of the portal). A notification should indicate that the upload has finished.

10. Go back to the Update blade on the dashboard. The blade should show that an

update is available. This indicates that the update has been prepared successfully.

Select the blade to review the newly-added update package.

11. Verify no updates are running. If an update is installing, an alert banner displays

The exclusive operation is in progress. Additional update operations are disabled





while the operation is running. Wait for the update to finish before starting another

update.

12. To install the update, select the package that's marked as Ready, and then select

Update now.

13. When you select the installing update package, you can view the status in the

Update run details area. From here, you can also select Download summary to

download the log files. Logs from update runs are available for six months after the

attempt ended.

14. When the update finishes, the Update blade shows the updated Azure Stack Hub

version.

You can manually delete updates from the storage account after they've been installed

on Azure Stack Hub. Azure Stack Hub periodically checks for older update packages and

removes them from storage. It may take Azure Stack Hub up to two weeks to remove

the old packages.

Apply the update

Next steps

Install Azure Stack Hub Updates

Article • 07/27/2021

You can install update packages using the Update blade in the Azure Stack Hub

administrator portal. This article describes the steps to update, monitor, and

troubleshoot the update process. Use the Update blade to view update info, install

updates, monitor update progress, review update history, and view the current Azure

Stack Hub and OEM package version.

You can manage updates from the administrator portal and use the Updates section of

the dashboard to:

View important info, such as the current version.

Install updates and monitor progress.

Review update history for previously installed updates.

View the cloud's current OEM package version.

You can view the current version of Azure Stack Hub in the Update pane. To open:

1. Open the Azure Stack Hub administrator portal.

2. Select Dashboard. In the Update pane, the current version is listed:

Determine the current version



Install updates and monitor progress

） Important

1. Open the Azure Stack Hub administrator portal.

2. Select Dashboard. Select Update.

3. Select the available update that you want to install. If you don't have an update

marked as Available, prepare the update package.

4. Select Install now.

5. You can view high-level status as the update process iterates through various

subsystems in Azure Stack Hub. Example subsystems include physical hosts,

Service Fabric, infrastructure virtual machines, and services that provide both the

admin and user portals. Throughout the update process, the update resource

provider reports additional details about the update, such as the number of steps

that have succeeded, and the number in progress.

6. Select Download summary from the update run details blade to download full

logs.

If you experience an issue while monitoring the update, you can use the privileged

endpoint to monitor the progress of an Azure Stack Hub update run. You can also

use the privileged endpoint to resume a failed update run from the last successful

step if the Azure Stack Hub portal becomes unavailable. For instructions, see

Monitor updates in Azure Stack Hub using PowerShell.

Before applying updates in Azure Stack Hub, ensure you have completed all steps

in the pre-update checklist and have scheduled an appropriate maintenance

window for the update type that you are applying.



7. When complete, the update resource provider displays a Succeeded confirmation

to show that the update process has finished, and how long it took. From there,

you can view info on all updates, available updates, or installed updates using the

filter.

If the update fails, the Update blade reports Needs attention. Use the Download

full logs option to get a high-level status of where the update failed. Azure Stack

Hub log collection helps with diagnostics and troubleshooting.

1. Open the administrator portal.

2. Select Dashboard, then select Update.

3. Select the Update history tab.

Review update history

Manage updates in Azure Stack Hub overview

Azure Stack Hub servicing policy



Next steps

Apply Azure Stack Hub original

equipment manufacturer (OEM) updates

Article • 07/29/2022

You can apply original equipment manufacturer (OEM) updates to your Azure Stack Hub

hardware components to get driver updates, firmware updates, and security patches.

These updates are done while minimizing impact on your users. In this article, you can

learn about OEM updates, OEM contact information, and how to apply an OEM update.

In addition to Microsoft Azure Stack Hub updates, many OEMs also release regular

updates for your Azure Stack Hub hardware, such as driver and firmware updates. These

updates are referred to as OEM package updates. To understand whether your OEM

releases OEM package updates, check your OEM's Azure Stack Hub documentation.

These OEM package updates are uploaded into the updateadminaccount storage

account and applied via the Azure Stack Hub administrator portal. For more information,

see Applying OEM updates.

Ask your OEM about their specific notification process to ensure OEM package update

notifications reach your organization.

Some hardware vendors may require a hardware vendor VM that handles the internal

firmware update process. For more information, see Configure hardware vendor VM.

This section contains OEM contact information and links to OEM Azure Stack Hub

reference material.

Hardware

Partner

Region URL

Cisco All Cisco Integrated System for Microsoft Azure Stack Hub Operations

Guide

UCS C-Series Rack-Mount UCS-Managed Server Software

Overview of OEM updates

OEM contact information

Hardware

Partner

Region URL

Dell EMC All Cloud for Microsoft Azure Stack Hub 14G (account and login

required)

Cloud for Microsoft Azure Stack Hub 13G (account and login

required)

Fujitsu JAPAN Fujitsu managed service support desk (account and login

required)

EMEA &

US

Fujitsu support IT products and systems

HPE All HPE ProLiant for Microsoft Azure Stack Hub

Lenovo All ThinkAgile SXM Best Recipes

Microsoft All Azure Stack Hub Ruggedized

Wortmann OEM/firmware package

terra Azure Stack Hub documentation (including FRU)

Apply the OEM packages with the following steps:

1. Contact your OEM to:

Determine the current version of your OEM package.

Find the best method to download your OEM package.

2. Before applying an OEM package update, always apply the latest Azure Stack Hub

hotfix available on your system's current Azure Stack Hub version. For more

information on hotfixes, see Azure Stack Hub hotfixes.

3. Prepare your OEM package with the steps outlined in Download update packages

for integrated systems.

4. Apply the updates with the steps outlined in Apply updates in Azure Stack Hub.

Apply OEM updates

） Important

Before applying updates in Azure Stack Hub, ensure you've completed ALL steps in

the Pre-update checklist and have scheduled an appropriate maintenance window

for the update type that you're applying.

Some hardware vendors may require a virtual machine (VM) to help with the OEM

update process. Your hardware vendor is responsible for creating these VMs and

documenting if you require ProxyVM or HardwareManager for -VMType when running the

Set-OEMExternalVM cmdlet, as well as which credential should be used for -Credential.

Once the VMs are created, configure them with the Set-OEMExternalVM from the

privileged endpoint.

For more information on the privileged endpoint in Azure Stack Hub, see Using the

privileged endpoint in Azure Stack Hub.

1. Access the privileged endpoint.

PowerShell

2. Configure the hardware vendor VM using the Set-OEMExternalVM cmdlet. The

cmdlet validates the IP address and credentials for -VMType ProxyVM . For -

VMType HardwareManager , the cmdlet won't validate the input. The -Credential

parameter provided to Set-OEMExternalVM is one that will be clearly documented

by the hardware vendor documentation. It is NOT the CloudAdmin credential used

with the privileged endpoint, or any other existing Azure Stack Hub credential.

PowerShell

Azure Stack Hub updates

Configure hardware vendor VM

$cred = Get-Credential

$session = New-PSSession -ComputerName <IP Address of ERCS> `

-ConfigurationName PrivilegedEndpoint -Credential $cred `

-SessionOption (New-PSSessionOption -Culture en-US -UICulture en-US)

$VmCred = Get-Credential

Invoke-Command -Session $session

{

Set-OEMExternalVM -VMType <Either "ProxyVM" or "HardwareManager">

-IPAddress <IP Address of hardware vendor VM> -Credential

$using:VmCred

}

Next steps

Monitor updates with PowerShell in

Azure Stack Hub

Article • 07/29/2022

You can use the Azure Stack Hub administrative endpoints to monitor and manage your

updates. They're accessible with PowerShell. For instructions on getting set up with

PowerShell on Azure Stack Hub, see Install PowerShell for Azure Stack Hub.

You can use the following PowerShell cmdlets to manage your updates:

Cmdlet Description

Get-AzsUpdate Get the list of available updates.

Get-AzsUpdateLocation Get the list of update locations.

Get-AzsUpdateRun Get the list of update runs.

Install-AzsUpdate Apply a specific update at an update location.

Resume-AzsUpdateRun Resumes a previously started update run that failed.

To get the list of update runs, run the following command:

PowerShell

If the update fails, you can resume the update run where it left off by running the

following command:

PowerShell

Get a list of update runs

Get-AzsUpdateRun -UpdateName Microsoft1.0.180302.1

Resume a failed update operation

Get-AzsUpdateRun -Name 5173e9f4-3040-494f-b7a7-738a6331d55c -UpdateName

Microsoft1.0.180305.1 | Resume-AzsUpdateRun

For more information on troubleshooting updates, see Azure Stack Troubleshooting.

Managing updates in Azure Stack Hub

Troubleshoot

Next steps

Monitor updates in Azure Stack Hub

using the privileged endpoint

Article • 07/29/2022

You can use the privileged endpoint to monitor the progress of an Azure Stack Hub

update run. You can also use the privileged endpoint to resume a failed update run from

the last successful step should the Azure Stack Hub portal become unavailable. Using

the Azure Stack Hub portal is the recommended method to manage updates in Azure

Stack Hub.

The following new PowerShell cmdlets for update management are included in the 1710

update for Azure Stack Hub integrated systems.

Cmdlet Description

GetAzureStackUpdateStatus

Returns the status of the currently running, completed, or failed update.

Provides the high-level status of the update operation and an XML

document that describes both the current step and the corresponding

state.

ResumeAzureStackUpdate

Resumes a failed update at the point where it failed. In certain

scenarios, you may have to complete mitigation steps before you

resume the update.

Because the cmdlets are new in the 1710 update package for Azure Stack Hub, the 1710

update process needs to get to a certain point before the monitoring capability is

available. Typically, the cmdlets are available if the status in the administrator portal

indicates that the 1710 update is at the Restart Storage Hosts step. Specifically, the

cmdlet update occurs during Step: Running step 2.6 - Update PrivilegedEndpoint

allowlist.

You can also determine whether the cmdlets are available programmatically by querying

the command list from the privileged endpoint. To do this query, run the following

commands from the hardware lifecycle host or from a Privileged Access Workstation.

Also, make sure the privileged endpoint is a trusted host. For more information, see step

1 of Access the privileged endpoint.

1. Create a PowerShell session on any of the ERCS virtual machines (VMs) in your

Azure Stack Hub environment (Prefix-ERCS01, Prefix-ERCS02, or Prefix-ERCS03).

Verify the cmdlets are available

Replace Prefix with the VM prefix string that's specific to your environment.

PowerShell

When prompted for credentials, use the <Azure Stack Hub domain>\cloudadmin

account, or an account that's a member of the CloudAdmins group. For the

CloudAdmin account, enter the same password that was provided during

installation for the AzureStackAdmin domain administrator account.

2. Get the full list of commands that are available in the privileged endpoint.

PowerShell

3. Determine if the privileged endpoint was updated.

PowerShell

4. List the commands specific to the Microsoft.AzureStack.UpdateManagement

module.

PowerShell

For example:

PowerShell

$cred = Get-Credential

$pepSession = New-PSSession -ComputerName <Prefix>-ercs01 -Credential

$cred -ConfigurationName PrivilegedEndpoint -SessionOption (NewPSSessionOption -Culture en-US -UICulture en-US)

$commands = Invoke-Command -Session $pepSession -ScriptBlock { GetCommand }

$updateManagementModuleName = "Microsoft.Azurestack.UpdateManagement"

if (($commands | ? Source -eq $updateManagementModuleName)) {

Write-Host "Privileged endpoint was updated to support update

monitoring tools."

} else {

Write-Host "Privileged endpoint has not been updated yet. Please try

again later."

}

$commands | ? Source -eq $updateManagementModuleName

Run the following commands to create a PowerShell session on any of the ERCS VMs in

your Azure Stack Hub environment (Prefix-ERCS01, Prefix-ERCS02, or Prefix-ERCS03),

and to assign a session variable.

PowerShell

When prompted for credentials, use the <Azure Stack Hub domain>\cloudadmin

account, or an account that's a member of the CloudAdmins group. For the CloudAdmin

account, enter the same password that was provided during installation for the

AzureStackAdmin domain administrator account.

$commands | ? Source -eq $updateManagementModuleName

CommandType Name

Version Source

PSComputerName

----------- ---- ---

---- ------ -------

-------

Function Get-AzureStackUpdateStatus 0.0

Microsoft.Azurestack.UpdateManagement Contoso-ercs01

Function Resume-AzureStackUpdate 0.0

Microsoft.Azurestack.UpdateManagement Contoso-ercs01

Use the update management cmdlets

７ Note

Run the following commands from the hardware lifecycle host or from a Privileged

Access Workstation. Also, make sure the privileged endpoint is a trusted host. For

more information, see step 1 of Access the privileged endpoint.

Connect to the privileged endpoint and assign session

variable

$cred = Get-Credential

$pepSession = New-PSSession -ComputerName <Prefix>-ercs01 -Credential $cred

-ConfigurationName PrivilegedEndpoint -SessionOption (New-PSSessionOption -

Culture en-US -UICulture en-US)

Get high-level status of the current update run

To get a high-level status of the current update run, run the following commands:

PowerShell

Possible values include:

Running

Completed

Failed

Canceled

You can run these commands repeatedly to see the most up-to-date status. You don't

have to re-establish a connection to check again.

You can get the full update run summary as an XML string. You can write the string to a

file for examination, or convert it to an XML document and use PowerShell to parse it.

The following command parses the XML to get a hierarchical list of the currently running

steps:

PowerShell

In the following example, the top-level step (Cloud Update) has a child plan to update

and restart the storage hosts. It shows that the Restart Storage Hosts plan is updating

the Blob Storage service on one of the hosts.

PowerShell

$statusString = Invoke-Command -Session $pepSession -ScriptBlock { GetAzureStackUpdateStatus -StatusOnly }

$statusString.Value

Get the full update run status with details

[xml]$updateStatus = Invoke-Command -Session $pepSession -ScriptBlock { GetAzureStackUpdateStatus }

$updateStatus.SelectNodes("//Step[@Status='InProgress']")

[xml]$updateStatus = Invoke-Command -Session $pepSession -ScriptBlock { GetAzureStackUpdateStatus }

$updateStatus.SelectNodes("//Step[@Status='InProgress']")

FullStepIndex : 2

Index : 2

If the update fails, you can resume the update run where it left off.

PowerShell

The privileged endpoint is available on all ERCS VMs in the Azure Stack Hub

environment. Because the connection isn't made to a highly available endpoint, you may

experience occasional interruptions, warning, or error messages. These messages may

indicate that the session was disconnected or that there was an error communicating

with the ECE Service. This behavior is expected. You can retry the operation in a few

minutes or create a new privileged endpoint session on one of the other ERCS VMs.

For more information on troubleshooting updates, see Azure Stack Troubleshooting

Name : Cloud Update

Description : Perform cloud update.

StartTimeUtc : 2017-10-13T12:50:39.9020351Z

Status : InProgress

Task : Task

FullStepIndex : 2.9

Index : 9

Name : Restart Storage Hosts

Description : Restart Storage Hosts.

EceErrorAction : Stop

StartTimeUtc : 2017-10-13T15:44:06.7431447Z

Status : InProgress

Task : Task

FullStepIndex : 2.9.2

Index : 2

Name : PreUpdate ACS Blob Service

Description : Check function level, update deployment artifacts,

configure Blob service settings

StartTimeUtc : 2017-10-13T15:44:26.0708525Z

Status : InProgress

Task : Task

Resume a failed update operation

Invoke-Command -Session $pepSession -ScriptBlock { Resume-AzureStackUpdate }

Troubleshoot

Next steps

Managing updates in Azure Stack Hub

Use the administrator portal in Azure

Stack Hub

Article • 07/29/2022

There are two portals in Azure Stack Hub: the administrator portal and the user portal.

As an Azure Stack Hub operator, you use the administrator portal for day-to-day

management and operations of Azure Stack Hub.

To access the administrator portal, browse to the portal URL and sign in by using your

Azure Stack Hub operator credentials. For an integrated system, the portal URL varies

based on the region name and external fully qualified domain name (FQDN) of your

Azure Stack Hub deployment. The administrator portal URL is always the same for Azure

Stack Development Kit (ASDK) deployments.

Environment Administrator Portal URL

ASDK https://adminportal.local.azurestack.external

Integrated systems https://adminportal.<region>.<FQDN>

Access the administrator portal

 Tip

For an ASDK environment, you need to first make sure that you can connect to the

development kit host through Remote Desktop Connection or through a virtual

private network (VPN).

７ Note

You can also use the The Operator Access Workstation (OAW) to access the

privileged endpoint (PEP), the Administrator portal for support scenarios, and Azure

Stack Hub GitHub Tools. For more information see Azure Stack Hub Operator

Access Workstation.

The default time zone for all Azure Stack Hub deployments is set to Coordinated

Universal Time (UTC).

In the administrator portal, you can do things like:

Register Azure Stack Hub with Azure

Populate the marketplace

Create plans, offers, and subscriptions for users

Monitor health and alerts

Manage Azure Stack Hub updates

The Quickstart tutorial tile provides links to online documentation for the most

common tasks.

Although an operator can create resources such as virtual machines (VMs), virtual

networks, and storage accounts in the administrator portal, you should sign in to the

user portal to create and test resources.

７ Note

The Create a virtual machine link in the quickstart tutorial tile has you create a VM

in the administrator portal, but this is only intended to validate that Azure Stack

Hub has been deployed successfully.

Understand subscription behavior

There are three subscriptions created by default in the administrator portal:

consumption, default provider, and metering. As an operator, you'll mostly use the

Default Provider Subscription. You can't add any other subscriptions and use them in the

administrator portal.

Other subscriptions are created by users in the user portal based on the plans and offers

you create for them. However, the user portal doesn't provide access to any of the

administrative or operational capabilities of the administrator portal.

The administrator and user portals are backed by separate instances of Azure Resource

Manager. Because of this Azure Resource Manager separation, subscriptions don't cross

portals. For example, if you, as an Azure Stack Hub operator, sign in to the user portal,

you can't access the Default Provider Subscription. Although you don't have access to

any administrative functions, you can create subscriptions for yourself from available

public offers. As long as you're signed in to the user portal, you're considered a tenant

user.

The dashboard contains a set of default tiles. You can select Edit dashboard to modify

the default dashboard, or select New dashboard to add a custom dashboard. You can

also add tiles to a dashboard. For example, select + Create a resource, right-click Offers

+ Plans, and then select Pin to dashboard.

Sometimes, you might see a blank dashboard in the portal. To recover the dashboard,

click Edit Dashboard, and then right-click and select Reset to default state.

To access the Azure Stack Hub operator documentation, use the help and support icon

(question mark) in the upper-right corner of the administrator portal. Move your cursor

７ Note

In an ASDK environment, if a user belongs to the same tenant directory as the

Azure Stack Hub operator, they're not blocked from signing in to the administrator

portal. However, they can't access any of the administrative functions or add

subscriptions to access offers that are available to them in the user portal.

Administrator portal tips

Customize the dashboard

Quick access to online documentation

to the icon, and then select Help + support.

If you click the help icon (question mark) in the upper-right corner of the administrator

portal, click Help + support, and then click New support request under Support, one of

the following results happens:

If you're using an integrated system, this action opens a site where you can directly

open a support ticket with Microsoft Support. Refer to Where to get support to

understand when you should go through Microsoft support or through your

original equipment manufacturer (OEM) hardware vendor support.

If you're using the ASDK, this action opens the Azure Stack Hub forums site

directly. These forums are regularly monitored. Because the ASDK is an evaluation

environment, there's no official support offered through Microsoft Support.

If you select Help and support (the question mark) in the upper right corner of the

administrator portal, and then select Azure roadmap, a new browser tab opens and

takes you to the Azure roadmap. By typing Azure Stack Hub in the Products search box,

you can see all Azure Stack Hub roadmap updates.

Similar to Azure, we recommend that you use the most up-to-date browser that's

compatible with your operating system. For a list of Azure recommended browsers, see

Recommended browsers.

Register Azure Stack Hub with Azure and populate Azure Stack Hub Marketplace with

items to offer your users.

Quick access to help and support

Quick access to the Azure roadmap

Recommended browsers

Next steps

Create a service offering for users in

Azure Stack Hub

Article • 07/29/2022

This tutorial shows an operator how to create an offer. An offer makes services available

to users on a subscription basis. Once subscribed to an offer, a user is entitled to create

and deploy resources within the services specified by the offer.

In this tutorial, you learn how to:

An offer consists of one or more plans. A plan entitles access to one or more services, by

specifying each service's corresponding resource provider and a quota. Plans can be

added to an offer as the base plan, or they can extend the offer as an add-on plan. To

learn more, see the Service, plan, offer, subscription overview.

＂ Create an offer.

＂ Create a plan.

＂ Assign services and quotas to a plan.

＂ Assign a plan to an offer.

Overview

Resource providers

A resource provider supports creation, deployment, and management of its resources as

services. A common example is the Microsoft.Compute resource provider, which offers

the ability to create and deploy virtual machines (VMs). See Azure Resource Manager for

an overview of the Azure resource management model.

In Azure Stack Hub, there are two general categories of resource providers: ones that

deploy resources as foundational services, and ones that deploy as value-add services.

Foundational services are supported by the following resource providers, which are

available natively with every installation of Azure Stack Hub:

Resource Provider Example resources

Microsoft.Compute VMs, disks, virtual machine scale sets

Microsoft.KeyVault Key Vaults, secrets

Microsoft.Network Virtual networks, public IP addresses, load balancers

Microsoft.Storage Storage accounts, blobs, queues, tables

Value-add services are supported by resource providers that are installed after Azure

Stack Hub has been deployed. Examples include:

Resource Provider Example resources

Foundational services

７ Note

In this tutorial, you learn how to create an offer based on foundational services.

Value-add services

７ Note

In order to offer a value-add service, the corresponding resource provider must first

be installed in Azure Stack Hub Marketplace. Once installed, its resources are

offered to users in the same way as foundational services. Please see the How-to

guides section of the TOC for the current set of resource providers that support

value-add service offerings.

Resource Provider Example resources

Microsoft.Web App Service function apps, web apps, API apps

Microsoft.MySqlAdapter MySQL hosting server, MySQL database

Microsoft.SqlAdapter SQL Server hosting server, SQL Server database

Microsoft.EventHub Event Hubs

During the offer creation process, you create both an offer and a plan. The plan is used

as the offer's base plan. During plan creation, you specify the services made available in

the plan and their respective quotas.

1. Sign in to the administrator portal with a cloud admin account.

For an integrated system, the URL varies based on your operator's region and

external domain name. The URL uses the format https://adminportal.

<region>.<FQDN> .

If you're using the Azure Stack Development Kit, the URL is

https://adminportal.local.azurestack.external .

Then select + Create a resource > Offers + Plans > Offer.

Create an offer

2. In Create a new offer under the Basics tab, enter a Display name, Resource name,

and select an existing or create a new Resource group. The Display name is the

offer's friendly name. Only the cloud operator can see the Resource name, which is

the name that admins use to work with the offer as an Azure Resource Manager

resource.

3. Select the Base plans tab, then select Create new plan to create a new plan. The

plan will also be added to the offer as a base plan.

4. In New plan under the Basics tab, enter a Display name and Resource name. The

Display name is the plan's friendly name that users see. Only the cloud operator

can see the Resource name, which is the name that cloud operators use to work

with the plan as an Azure Resource Manager resource. Resource group will be set

to the one specified for the Offer.

5. Select the Services tab, and you see a list of services available from the installed

resource providers. Select Microsoft.Compute, Microsoft.Network, and

Microsoft.Storage.

6. Select the Quotas tab, and you see the list of services you enabled for this plan.

Select Create New to specify a custom quota for Microsoft.Compute. Quota Name

is required; you can accept or change each quota value. Select OK when finished,

then repeat these steps for the remaining services.

7. Select the Review + create tab. You should see a green "Validation passed" banner

at the top, indicating the new base plan is ready to be created. Select Create. You

should also see a notification indicating that the plan has been created.

8. After returning to the Base plans tab of the Create a new offer page, you notice

that the plan has been created. Be sure the new plan is selected for inclusion in the

offer as the base plan, then select Review + create.

9. On the Review + create tab, you should see a green "Validation passed" banner at

the top. Review the "Basic" and "Base Plans" info, and select Create when ready.

10. The "Your deployment is underway" page shows initially, followed by "Your

deployment is complete" once the offer is deployed. Select on the name of the

offer under the Resource column.

11. Notice the banner, showing your offer is still private, which prevents users from

subscribing to it. Change it to public by selecting Change State, and then chose

Public.

In this tutorial you learned how to:

Advance to the next tutorial to learn how to:

Next steps

＂ Create an offer.

＂ Create a plan.

＂ Assign services and quotas to a plan.

＂ Assign a plan to an offer.

Test the services offered in this tutorial

Tutorial: Test a service offering

Article • 07/29/2022

In the previous tutorial, you created an offer for users. This tutorial shows you how to

test that offer, by using it to create a subscription. You then create and deploy resources

to the foundational services entitled by the subscription.

In this tutorial, you learn how to:

Before starting this tutorial, you must complete the following prerequisites:

Complete the Offer a service to users tutorial. In it, you learn how to create the

offer used by this tutorial.

The offer you subscribe to in this tutorial enables deployment of a virtual machine

(VM) resource. If you'd like to test VM deployment, you must first make a VM

image available in Azure Stack Hub Marketplace, by downloading it from Azure

Marketplace. See Download marketplace items from Azure to Azure Stack Hub for

instructions.

1. Sign in to the user portal with a user account

For an integrated system, the URL varies based on your operator's region and

external domain name, using the format https://portal.<region>.<FQDN>.

If you're using the Azure Stack Development Kit, the portal address is

https://portal.local.azurestack.external .

2. Select the Get a Subscription tile.

＂ Create a subscription

＂ Create and deploy resources

Prerequisites

Subscribe to the offer

3. In Get a Subscription, enter a name for your new subscription in the Display Name

field. Select Offer, and then choose the offer you created in the previous tutorial,

from the Choose an offer list. Select Create.

4. To view the subscription, select All services, and then under the GENERAL category

select Subscriptions. Select your new subscription to view the offer it's associated

with, and its properties.

From the user portal, you provision a storage account using the subscription you

created in the previous section.

７ Note

After you subscribe to an offer, you might have to refresh the portal to see

which services are part of the new subscription.

Deploy a storage account resource

1. Sign in to the user portal with a user account.

2. Select +Create a resource > Data + Storage > Storage account - blob, file, table,

queue.

3. In Create storage account, provide the following information:

Enter a Name

Select your new Subscription

Select a Resource group (or create a one.)

Select Create to create the storage account.

4. Once deployment starts, you return to the dashboard. To see the new storage

account, select All resources. Search for the storage account and select its name

from the search results. From here, you can manage the storage account and its

contents.

From the user portal, you provision a virtual machine using the subscription you created

in the previous section.

1. Sign in to the user portal with a user account.

2. Select +Create a resource > Compute > <image-name>, where "image-name" is

the name of the virtual machine you downloaded in prerequisites.

3. In Create virtual machine / Basics, provide the following information:

Enter a Name for the VM.

Enter a User name for the administrator account.

For Linux VMs, select "Password" for Authentication type.

Enter a Password and the same for Confirm password, for the administrator

account.

Select your new Subscription.

Select a Resource group (or create a one).

Select OK to validate this information and continue.

4. In Choose a size, filter the list if necessary, select a VM SKU, and select Select.

5. In Settings, specify the port(s) to be opened under Select public inbound ports,

and select OK.

Deploy a virtual machine resource

７ Note

6. In Summary, review your choices, then select OK to create the virtual machine.

7. Once deployment starts, you return to the dashboard. To see the new virtual

machine, select All resources. Search for the virtual machine and select its name

from the search results. From here, you can access and manage the virtual

machine.

In this tutorial you learned how to:

Next, learn about deploying resource providers for value-add services. They allow you to

offer even more services to users in your plans:

Offer SQL on Azure Stack Hub

Offer MySQL on Azure Stack Hub

Offer App Service on Azure Stack Hub

Offer Event Hubs on Azure Stack Hub

Selecting "RDP(3389)", for example, allows you to connect to the VM remotely

when it's running.

７ Note

Full deployment and starting of the VM can take several minutes. Once the

VM is ready for use, the status will change to "Running".

Next steps

＂ Create a subscription

＂ Create and deploy resources

Capacity planning for Azure Stack Hub

overview

Article • 07/29/2022

When you're evaluating an Azure Stack Hub solution, consider the hardware

configuration choices that have a direct impact on the overall capacity of the Azure

Stack Hub cloud.

For example, you need to make choices regarding the CPU, memory density, storage

configuration, and overall solution scale or number of servers. However, determining

usable capacity will be different than a traditional virtualization solution because some

capacity is already in use. Azure Stack Hub is built to host the infrastructure or

management components within the solution itself. Also, some of the solution's capacity

is reserved to support resiliency. Resiliency is defined as the updating of the solution's

software in a way to minimize disruption of tenant workloads.

An Azure Stack Hub solution is built as a hyperconverged cluster of compute and

storage. The convergence allows for the sharing of the hardware capacity in the cluster,

referred to as a scale unit. In Azure Stack Hub, a scale unit provides the availability and

scalability of resources. A scale unit consists of a set of Azure Stack Hub servers, referred

to as hosts. The infrastructure software is hosted within a set of virtual machines (VMs),

and shares the same physical servers as the tenant VMs. All Azure Stack Hub VMs are

then managed by the scale unit’s Windows Server clustering technologies and individual

Hyper-V instances.

The scale unit simplifies the acquisition and management of Azure Stack Hub. The scale

unit also allows for the movement and scalability of all services (tenant and

infrastructure) across Azure Stack Hub.

） Important

This capacity planning information and the Azure Stack Hub Capacity Planner

are a starting point for Azure Stack Hub planning and configuration decisions. This

information isn't intended to serve as a substitute for your own investigation and

analysis. Microsoft makes no representations or warranties, express or implied, with

respect to the information provided here.

Hyperconvergence and the scale unit

Azure Stack Hub compute capacity

Azure Stack Hub storage capacity planning

Azure Stack Hub Capacity Planner

Next steps

Azure Stack Hub compute capacity

Article • 07/29/2022

The virtual machine (VM) sizes supported on Azure Stack Hub are a subset of those

supported on Azure. Azure imposes resource limits along many vectors to avoid

overconsumption of resources (server local and service-level). Without imposing some

limits on tenant consumption, the tenant experiences will suffer when other tenants

overconsume resources. For networking egress from the VM, there are bandwidth caps

in place on Azure Stack Hub that match Azure limitations. For storage resources on

Azure Stack Hub, storage IOPS limits avoid basic over consumption of resources by

tenants for storage access.

The Azure Stack Hub placement engine places tenant VMs across the available hosts.

Azure Stack Hub uses two considerations when placing VMs. One, is there enough

memory on the host for that VM type? And two, are the VMs a part of an availability set

or are they virtual machine scale sets?

To achieve high availability of a multi-VM production workload in Azure Stack Hub,

virtual machines (VMs) are placed in an availability set that spreads them across multiple

fault domains. A fault domain in an availability set is defined as a single node in the

scale unit. Azure Stack Hub supports having an availability set with a maximum of three

fault domains to be consistent with Azure. VMs placed in an availability set will be

physically isolated from each other by spreading them as evenly as possible over

multiple fault domains (Azure Stack Hub nodes). If there's a hardware failure, VMs from

the failed fault domain will be restarted in other fault domains. If possible, they'll be

kept in separate fault domains from the other VMs in the same availability set. When the

host comes back online, VMs will be rebalanced to maintain high availability.

Virtual machine scale sets use availability sets on the back end and make sure each

virtual machine scale set instance is placed in a different fault domain. This means they

） Important

The Azure Stack Hub Capacity Planner does not consider or guarantee IOPS

performance. The administrator portal shows a warning alert when the total system

memory consumption has reached 85%. This alert can be remediated by adding

additional capacity, or by removing virtual machines that are no longer required.

VM placement

use separate Azure Stack Hub infrastructure nodes. For example, in a four-node Azure

Stack Hub system, there may be a situation where a virtual machine scale set of three

instances will fail at creation due to the lack of the four-node capacity to place three

virtual machine scale set instances on three separate Azure Stack Hub nodes. In

addition, Azure Stack Hub nodes can be filled up at varying levels before trying

placement.

Azure Stack Hub doesn't overcommit memory. However, an overcommit of the number

of physical cores is allowed.

Since placement algorithms don't look at the existing virtual to physical core

overprovisioning ratio as a factor, each host could have a different ratio. As Microsoft,

we don't provide guidance on the physical-to-virtual core ratio because of the variation

in workloads and service level requirements.

There is a limit on the total number of VMs that can be created. The maximum number

of VMs on Azure Stack Hub is 700 and 60 per scale unit node. For example, an eightserver Azure Stack Hub VM limit would be 480 (8 \* 60). For a 12 to 16 server Azure Stack

Hub solution, the limit would be 700. This limit has been created keeping all the

compute capacity considerations in mind, such as the resiliency reserve and the CPU

virtual-to-physical ratio that an operator would like to maintain on the stamp.

If the VM scale limit is reached, the following error codes are returned as a result:

VMsPerScaleUnitLimitExceeded , VMsPerScaleUnitNodeLimitExceeded .

In releases prior to and including 2002, 2-5 VMs per batch with 5 mins gap in between

batches provided reliable VM deployments to reach a scale of 700 VMs. With the 2005

version of Azure Stack Hub onwards, we are able to reliably provision VMs at batch sizes

of 40 with 5 mins gap in between batch deployments. Start, Stop-deallocate, and update

operations should be done at a batch size of 30, leaving 5 mins in between each batch.

Consideration for total number of VMs

７ Note

A portion of the 700 VM maximum is reserved for Azure Stack Hub infrastructure

VMs. For more information, refer to the Azure Stack Hub capacity planner .

Consideration for batch deployment of VMs

Azure Stack hub reserves memory for the infrastructure and tenant VMs to failover.

Unlike other VMs, GPU VMs run in a non-HA (high availability) mode and therefore do

not failover. As a result, reserved memory for a GPU VM-only stamp is what is required

by the infrastructure to failover, as opposed to accounting for HA tenant VM memory

too.

Azure Stack Hub is designed to keep VMs running that have been successfully

provisioned. For example, if a host is offline because of a hardware failure, Azure Stack

Hub will attempt to restart that VM on another host. A second example during patching

and updating of the Azure Stack Hub software. If there's a need to reboot a physical

host, an attempt is made to move the VMs executing on that host to another available

host in the solution.

This VM management or movement can only be achieved if there's reserved memory

capacity to allow for the restart or migration to occur. A portion of the total host

memory is reserved and unavailable for tenant VM placement.

You can review a pie chart in the administrator portal that shows the free and used

memory in Azure Stack Hub. The following diagram shows the physical memory capacity

on an Azure Stack Hub scale unit in the Azure Stack Hub:

Used memory is made up of several components. The following components consume

the memory in the use section of the pie chart:

Consideration for GPU VMs

Azure Stack Hub memory

Host OS usage or reserve: The memory used by the operating system (OS) on the

host, virtual memory page tables, processes that are running on the host OS, and

the Spaces Direct memory cache. Since this value is dependent on the memory

used by the different Hyper-V processes running on the host, it can fluctuate.

Infrastructure services: The infrastructure VMs that make up Azure Stack Hub. As

discussed previously, these VMs are part of the 700 VM maximum. The memory

utilization of the infrastructure services component may change as we work on

making our infrastructure services more scalable and resilient. For more

information see the Azure Stack Hub capacity planner

Resiliency reserve: Azure Stack Hub reserves a portion of the memory to allow for

tenant availability during a single host failure as well as during patch and update to

allow for successful live migration of VMs.

Tenant VMs: The tenant VMs created by Azure Stack Hub users. In addition to

running VMs, memory is consumed by any VMs that have landed on the fabric.

This means that VMs in "Creating" or "Failed" state, or VMs shut down from within

the guest, will consume memory. However, VMs that have been deallocated using

the stop deallocated option from portal/powershell/cli won't consume memory

from Azure Stack Hub.

Value-add resource providers (RPs): VMs deployed for the value-add RPs like SQL,

MySQL, App Service, and so on.

The best way to understand memory consumption on the portal is to use the Azure

Stack Hub Capacity Planner to see the impact of various workloads. The following

calculation is the same one used by the planner.

This calculation results in the total available memory that can be used for tenant VM

placement. This memory capacity is for the entirety of the Azure Stack Hub scale unit.

Available memory for VM placement = total host memory - resiliency reserve - memory

used by running tenant VMs - Azure Stack Hub Infrastructure Overhead

Total host memory = Sum of memory from all nodes

Resiliency reserve = H + R \* ((N-1) \* H) + V \* (N-2)

Memory used by tenant VMs = Actual memory consumed by tenant workload,

does not depend on HA configuration

Azure Stack Hub Infrastructure Overhead = 268 GB + (4GB x N)

Where:

H = Size of single server memory

N = Size of Scale Unit (number of servers)

R = The operating system reserve for OS overhead, which is .15 in this

formula

1

2

V = Largest HA VM in the scale unit

Azure Stack Hub Infrastructure overhead = 268 GB + (4 GB x # of nodes).

Approximately 31 VMs are used to host Azure Stack Hub's infrastructure and, in total,

consume about 268 GB + (4 GB x # of nodes) of memory and 146 virtual cores. The

rationale for this number of VMs is to satisfy the needed service separation to meet

security, scalability, servicing, and patching requirements. This internal service structure

allows for the future introduction of new infrastructure services as they're developed.

Operating system reserve for overhead = 15% (.15) of node memory. The operating

system reserve value is an estimate and will vary based on the physical memory capacity

of the server and general operating system overhead.

The value V, largest HA VM in the scale unit, is dynamically based on the largest tenant

VM memory size. For example, the largest HA VM value is a minimum of 12 GB

(accounting for the infrastructure VM) or 112 GB or any other supported VM memory

size in the Azure Stack Hub solution. Changing the largest HA VM on the Azure Stack

Hub fabric will result in an increase in the resiliency reserve and also to the increase in

the memory of the VM itself. Remember that GPU VMs run in non-HA mode.

We have a small four-node Azure Stack Hub deployment with 768 GB RAM on each

node. We plan to place a virtual machine for SQL server with 128GB of RAM

(Standard\_E16\_v3). What will be the available memory for VM placement?

Total host memory = Sum of memory from all nodes = 4 \* 768 GB = 3072 GB

Resiliency reserve = H + R \* ((N-1) \* H) + V \* (N-2) = 768 + 0.15 \* ((4 - 1) \* 768) +

128 \* (4 - 2) = 1370 GB

Memory used by tenant VMs = Actual memory consumed by tenant workload,

does not depend on HA configuration = 0 GB

Azure Stack Hub Infrastructure Overhead = 268 GB + (4GB x N) = 268 + (4 \* 4) =

284 GB

Available memory for VM placement = total host memory - resiliency reserve - memory

used by running tenant VMs - Azure Stack Hub Infrastructure Overhead

Available memory for VM placement = 3072 - 1370 - 0 - 284 = 1418 GB

1

2

Sample calculation

Considerations for deallocation

When a VM is in the deallocated state, memory resources aren't being used. This allows

others VMs to be placed in the system.

If the deallocated VM is then started again, the memory usage or allocation is treated

like a new VM placed into the system and available memory is consumed. If there's no

available memory, then the VM won't start.

Current deployed large VMs show that the allocated memory is 112 GB, but the memory

demand of these VMs is about 2-3 GB.

Name Memory Assigned

(GB)

Memory Demand

(GB)

ComputerName

ca7ec2ea-40fd-4d41-9d9bb11e7838d508

112 2.2392578125 LISSA01PNODE01

10cd7b0f-68f4-40ee-9d98-

b9637438ebf4

112 2.2392578125 LISSA01PNODE01

2e403868-ff81-4abb-b087-

d9625ca01d84

112 2.2392578125 LISSA01PNODE04

There are three ways to deallocate memory for VM placement using the formula

Resiliency reserve = H + R \* ((N-1) \* H) + V \* (N-2):

Reduce the size of the largest VM

Increase the memory of a node

Add a node

Reducing the size of the largest VM to the next smallest VM in stamp (24 GB) will reduce

the size of the resiliency reserve.

Reduce the size of the largest VM

Resiliency reserve = 384 + 172.8 + 48 = 604.8 GB

Total

memory

Infra

GB

Tenant

GB

Resiliency

reserve

Total memory

reserved

Total GB available for

placement

1536 GB 258

GB

329.25

GB

604.8 GB 258 + 329.25 + 604.8

= 1168 GB

~344 GB

Adding an Azure Stack Hub node will deallocate memory by equally distributing the

memory between the two nodes.

Add a node

Resiliency reserve = 384 + (0.15) ((5)\*384) + 112 \* (3) = 1008 GB

Total

Memory

Infra

GB

Tenant

GB

Resiliency

reserve

Total memory

reserved

Total GB available for

placement

1536 GB 258

GB

329.25

GB

604.8 GB 258 + 329.25 + 604.8

= 1168 GB

~ 344 GB

Increasing the memory of each node will increase the total available memory.

Resiliency reserve = 512 + 230.4 + 224 = 966.4 GB

Total

Memory

Infra

GB

Tenant

GB

Resiliency

reserve

Total memory

reserved

Total GB available for

placement

2048

(4\*512) GB

258

GB

505.75

GB

966.4 GB 1730.15 GB ~ 318 GB

Q: My tenant deployed a new VM, how long will it take for the capability chart on the

administrator portal to show remaining capacity?

A: The capacity blade refreshes every 15 minutes, so take that into consideration.

Q: How can I see the available cores and assigned cores?

Increase memory on each node to 512 GB

Frequently Asked Questions

A: In PowerShell run test-azurestack -include AzsVmPlacement -debug , which generates

an output like this:

Console

Q: The number of deployed VMs on my Azure Stack Hub hasn't changed, but my

capacity is fluctuating. Why?

A: The available memory for VM placement has multiple dependencies, one of which is

the host OS reserve. This value is dependent on the memory used by the different

Hyper-V processes running on the host, which isn't a constant value.

Q: What state do tenant VMs have to be in to consume memory?

A: In addition to running VMs, memory is consumed by any VMs that have landed on

the fabric. This means that VMs that are in a "Creating" or "Failed" state will consume

memory. VMs shut down from within the guest as opposed to stop deallocated from

portal/powershell/cli will also consume memory.

Q: I have a four-host Azure Stack Hub. My tenant has 3 VMs that consume 56 GB of

RAM (D5\_v2) each. One of the VMs is resized to 112 GB RAM (D14\_v2), and available

memory reporting on dashboard resulted in a spike of 168 GB usage on the capacity

blade. Subsequent resizing of the other two D5\_v2 VMs to D14\_v2 resulted in only 56

GB of RAM increase each. Why is this so?

A: The available memory is a function of the resiliency reserve maintained by Azure

Stack Hub. The Resiliency reserve is a function of the largest VM size on the Azure Stack

Starting Test-AzureStack

Launching AzsVmPlacement

Azure Stack Scale Unit VM Placement Summary Results

Cluster Node VM Count VMs Running Physical Core Total Virtual Co

Physical Memory Total Virtual Mem

------------ -------- ----------- ------------- ---------------- ----

----------- -----------------

LNV2-Node02 20 20 28 66 256

119.5

LNV2-Node03 17 16 28 62 256

110

LNV2-Node01 11 11 28 47 256

111

LNV2-Node04 10 10 28 49 256

101

PASS : Azure Stack Scale Unit VM Placement Summary

Hub stamp. At first, the largest VM on the stamp was 56 GB memory. When the VM was

resized, the largest VM on the stamp became 112 GB memory which not only increased

the memory used by that tenant VM but also increased the resiliency reserve. This

change resulted in an increase of 56 GB (56 GB to 112 GB tenant VM memory increase)

+ 112 GB resiliency reserve memory increase. When subsequent VMs were resized, the

largest VM size remained as the 112 GB VM and therefore there was no resultant

resiliency reserve increase. The increase in memory consumption was only the tenant

VM memory increase (56 GB).

Learn about Azure Stack Hub storage

７ Note

The capacity planning requirements for networking are minimal as only the size of

the public VIP is configurable. For information about how to add more public IP

addresses to Azure Stack Hub, see Add public IP addresses.

Next steps

Azure Stack Hub storage capacity

planning

Article • 07/29/2022

The following sections provide Azure Stack Hub storage capacity planning information

to assist in planning for the solution's storage needs.

The hyperconverged configuration of Azure Stack Hub allows for the sharing of physical

storage devices. There are three main divisions of the available storage that can be

shared: the infrastructure, the temporary storage of the tenant virtual machines (VMs),

and the storage backing the blobs, tables, and queues of the Azure Consistent Storage

(ACS) services.

There's storage capacity used for the operating system, local logging, dumps, and other

temporary infrastructure storage needs. This local storage capacity is separate (devices

and capacity) from the storage devices brought under management of the Storage

Spaces Direct configuration. The rest of the storage devices are placed in a single pool

of storage capacity, regardless of the number of servers in the scale unit.

These devices are of two types: cache and capacity. Storage Spaces Direct consumes

cache devices for write-back and read caching. The capacities of these cache devices,

while used, aren't committed to the formatted and "visible" capacity of the formatted

virtual disks. By contrast, Storage Spaces Direct does use capacity devices for this

purpose, providing the "home location" of the managed data.

The Azure Stack Hub infrastructure directly allocates and manages all storage capacity.

The operator doesn't need to make choices about configuration, allocation, capacity

expansion. Azure Stack Hub automates these design decisions to align with the solution

requirements, during either the initial installation and deployment or capacity

expansion. Azure Stack Hub takes into consideration resiliency, reserved capacity for

rebuilds, and other details, as part of the design.

Operators can choose between either an all flash or a hybrid storage configuration:

Uses and organization of storage capacity

Storage Spaces Direct cache and capacity tiers

In the all flash configuration, the configuration can be either a two-tier or a single-tier

configuration. If the configuration is single-tier, all capacity devices are of the same type

(for example, NVMe or SATA SSD or SAS SSD), and cache devices aren't used. In a twotier all flash configuration, the typical configuration is NVMe as the cache devices, and

then either SATA or SAS SSDs as the capacity devices.

In the hybrid two-tier configuration, the cache is a choice among NVMe, SATA, or SAS

SSD, and the capacity is HDD.

A brief summary of the Storage Spaces Direct and Azure Stack Hub storage

configuration is as follows:

One Storage Spaces Direct pool per scale unit (all storage devices are configured

within a single pool).

Virtual disks are created as a three-copy mirror for best performance and

resiliency.

Each virtual disk is formatted as an ReFS file system.

Virtual disk capacity is calculated and allocated in a way as to leave one capacity

device's amount of data capacity unallocated in the pool. This is the equivalent of

one capacity drive per server.

Each ReFS file system has BitLocker enabled for data-at-rest encryption.

The virtual disks created automatically and their capacities are as follows:

Name Capacity

calculation

Description

Local/boot

device

Minimum of

340 GB

Individual server storage for operating system images and

"local" infrastructure VMs.

Infrastructure 3.5 TB All Azure Stack Hub infrastructure usage.

VmTemp See below Tenant VMs have a temporary disk attached and that data is

stored in these virtual disks.

ACS See below Azure Consistent Storage capacity for servicing blobs, tables,

and queues.

Minimum storage capacity required of the Azure Stack Hub solution partner.

The virtual disk size used for tenant VM temporary disks is calculated as a ratio of the

physical memory of the server. The temporary disk is a ratio of the physical memory

assigned to the VM. The allocation done for "temp disk" storage in Azure Stack Hub

captures most use cases but might not be able to satisfy all temp disk storage needs.

The ratio is a trade-off between making temporary storage available and not consuming

a majority of the solution's storage capacity for temp disk capacity only. One temporary

storage disk is created per server in the scale unit. The capacity of the temporary

storage doesn't grow beyond 10 percent of the overall available storage capacity in the

storage pool of the scale unit. The calculation is something like the following example:

The virtual disks created for use by ACS are a simple division of the remaining capacity.

As noted, all virtual disks are a three-way mirror and one capacity drive's worth of

capacity for each server is unallocated. The various virtual disks previously enumerated

are allocated first and the remaining capacity is then used for the ACS virtual disks.

Learn about the Azure Stack Hub Capacity Planner.

1

2

3

1

2

DesiredTempStoragePerServer = PhysicalMemory \* 0.65 \* 8

TempStoragePerSolution = DesiredTempStoragePerServer \* NumberOfServers

PercentOfTotalCapacity = TempStoragePerSolution / TotalAvailableCapacity

If (PercentOfTotalCapacity <= 0.1)

TempVirtualDiskSize = DesiredTempStoragePerServer

Else

TempVirtualDiskSize = (TotalAvailableCapacity \* 0.1) / NumberOfServers

3

Next steps

Azure Stack Hub storage infrastructure

overview

Article • 07/29/2022

This article provides Azure Stack Hub storage infrastructure concepts. It covers

information about drives and volumes and how they are used in Azure Stack Hub.

Azure Stack Hub integrated system partners offer many solution variations, including a

wide range of storage flexibility. You can select up to two drive types from the three

supported drive types:

1. NVMe (non-volatile memory express)

2. SATA/SAS SSD (solid-state drive)

3. HDD (hard disk drive).

Azure Stack Hub uses Storage Spaces Direct (S2D) with Windows Server Failover

Clustering. This combination provides a performant, scalable, and resilient storage

service.

Azure Stack deployments can maximize storage performance, or balance performance

and capacity.

Storage Spaces Direct uses a cache to maximize storage performance.

When an Azure Stack Hub appliance has one drive type, all drives are used for capacity.

If there are two drive types, Storage Spaces Direct automatically uses all drives of the

"fastest" (NVMe > SSD > HDD) type for caching. The remaining drives are used for

capacity.

Drives

Drive types

Performance vs capacity

How drive types are used

All-flash or hybrid

The drives could be grouped into either an "all-flash" or "hybrid" deployment.

All-flash deployments aim to maximize storage performance and don't include

rotational HDDs.

Hybrid deployments aim to balance performance and capacity or to maximize capacity

and do include rotational HDDs.

The behavior of the cache is determined automatically based on the type(s) of drives.

When caching for SSDs (such as NVMe caching for SSDs), only writes are cached. This

reduces wear on the capacity drives, reducing the cumulative traffic to the capacity

drives and extending their lifetime.

Reads aren't cached. They aren't cached because reads don't significantly affect the

lifespan of flash and because SSDs universally offer low read latency.

When caching for HDDs (such as SSDs caching for HDDs), both reads and writes are

cached, to provide flash-like latency (often /~10x better) for both.

Caching behavior

For the available configuration of storage, you can check Azure Stack Hub OEM partner

(https://azure.microsoft.com/overview/azure-stack/partners/ ) for detailed

specification.

The storage service partitions the available storage into separate volumes that are

allocated to hold system and tenant data. Volumes combine the drives in the storage

pool to provide the fault tolerance, scalability, and performance benefits of Storage

Spaces Direct.

７ Note

The Azure Stack Hub appliance can be delivered in a hybrid deployment, with both

HDD and SSD (or NVMe) drives. But the drives of faster type would be used as

cache drives, and all remaining drives would be used as capacity drives as a pool.

The tenant data (blobs, tables, queues, and disks) would be placed on capacity

drives. Provisioning premium disks or selecting a premium storage account type

doesn't guarantee the objects will be allocated on SSD or NVMe drives.

Volumes

There are three types of volumes created on Azure Stack Hub storage pool:

1. Infrastructure volumes host files used by Azure Stack Hub infrastructure VMs and

core services.

2. VM Temp volumes host the temporary disks attached to tenant VMs and that data

is stored in these disks.

3. Object Store volumes host tenant data servicing blobs, tables, queues, and VM

disks.

In a multi-node deployment, there are three Infrastructure volumes.

The number of VM Temp volumes and Object Store volumes is equal to the number of

the nodes in the Azure Stack Hub deployment:

On a four-node deployment, there are four equal VM Temp volumes and four

equal Object Store volumes.

If you add a new node to the cluster, there would be a new volume for both types

created.

The number of volumes remains the same even if a node malfunctioning or is

removed.

Volume types

Volumes in a multi-node deployment

Volumes in Storage Spaces Direct provide resiliency to protect against hardware

problems, such as drive or server failures. They enable continuous availability

throughout server maintenance, like software updates.

Mirroring provides fault tolerance by keeping multiple copies of all data. How that data

is striped and placed is non-trivial, but any data stored using mirroring is written in its

entirety multiple times. Each copy is written to different physical hardware (different

drives in different servers) that are assumed to fail independently.

Azure Stack Hub deployment uses three-way mirroring to ensure data resilience. Threeway mirroring can safely tolerate at least two hardware problems (drive or server) at a

time. For example, if you're rebooting one server when suddenly another drive or server

fails, all data remains safe and continuously accessible.

Three copies of tenant data are written to different servers, where they land in cache:

Manage storage capacity

７ Note

If you use the Azure Stack Development Kit (ASDK), there's a single volume with

multiple shares.

Fault tolerance and mirroring

Next step

Azure Stack Hub Capacity Planner

Article • 07/29/2022

The Azure Stack Hub Capacity Planner is a spreadsheet that shows how different

allocations of computing resources would fit across a selection of hardware offerings.

The following table describes each worksheet in the Azure Stack Hub Capacity Planner,

which can be downloaded from https://aka.ms/azstackcapacityplanner .

Worksheet name Description

Version-Disclaimer Purpose of the calculator, version number, and release date.

Instructions Step-by-step instructions to model capacity planning for a

collection of virtual machines (VMs).

DefinedSolutionSKUs Table with up to five hardware definitions. The entries are examples.

Change the details to match system configurations under

consideration.

DefineByVMFootprint Find the appropriate hardware SKU by comparing configurations

with different sizes and quantities of VMs.

DefineByWorkloadFootprint Find the appropriate hardware SKU by creating a collection of

Azure Stack Hub workloads.

This worksheet has up to six hardware definition examples. Change details to match the

system configurations under consideration.

Azure Stack Hub is delivered as an integrated system with software installed by solution

partners. Solution partners provide their own authoritative versions of Azure Stack Hub

capacity planning tools. Use those tools for final discussions of solution capacity.

Worksheet descriptions

DefinedSolutionSKUs instructions

Hardware selections provided by authorized hardware

partners

Multiple ways to model computing resources

Resource modeling within the Azure Stack Hub Capacity Planner depends upon the

various sizes of Azure Stack Hub VMs. VMs range in size from the smallest, Basic 0, up to

the largest, Standard\_Fsv2. You can also choose from three GPU models that are

available in NVIDIA V100, NVIDIA T4 and AMD MI25 GPUs. You can model computing

resource allocations in two different ways:

Select a specific hardware offering and see which combinations of different

resources fit.

Create a specific combination of VM allocations and let Azure Resource Calculator

show which available hardware SKUs can support this VM configuration.

This tool provides two methods for allocating VM resources: either as one single

collection of VM resource allocations, or as a collection of up to six differing workload

configurations. Each workload configuration can contain a different allocation of

available VM resources. The next sections have step-by-step instructions to create and

use each of these allocation models. Only values contained in non-background shaded

cells or within SKU pull-down lists on this worksheet should be modified. Changes made

within shaded cells might break resource calculations.

To create a model by using a single collection of various sizes and quantities of VMs,

select the DefineByVMFootprint tab and follow these steps:

1. In the upper right corner of this worksheet, use the provided pull-down list box

controls to select an initial number of servers (between 4 and 16) that you want

installed in each hardware system (SKU). This number of servers can be modified at

any time during the modeling process to see how this affects overall available

resources for your resource allocation model.

2. If you want to model various VM resource allocations against one specific

hardware configuration, find the blue pull-down list box directly below the Current

SKU label in the upper right corner of the page. Pull down this list box and select

your desired hardware SKU.

3. You're now ready to begin adding variously sized VMs to your model. To include a

particular VM type, enter a quantity value into the blue outlined box to the left of

that VM entry.

DefineByVMFootprint instructions

７ Note

4. As you add VMs, you'll see the charts that show available SKU resources changing.

These charts allow you to see the effects of adding various sizes and quantities of

VMs during the modeling process. Another way to view the effect of changes is to

watch the Consumed and Still Available numbers, listed directly below the list of

available VMs. These numbers reflect estimated values based on the currently

selected hardware SKU.

5. If GPU VMs were selected in the DefinedSolutionSKUs tab then the selected GPU

type will be available to enter quantity. Please note: ONLY GPU type selected in the

DefinedSolutionSKUs tab will be available for capacity planning, any other GPU

choices made will be ignored.

6. When you've created your set of VMs, you can find the suggested hardware SKU

by selecting Suggested SKU. This button is located in the upper right corner of the

page, directly below the Current SKU label. Using this button, you can then modify

your VM configurations and see which hardware supports each configuration.

To create a model by using a collection of Azure Stack Hub workloads, select the

DefineByWorkloadFootprint tab and follow this sequence of steps. You create Azure

Stack Hub workloads by using available VM resources.

Total VM Storage refers to the total capacity of the data disk of the VM (the

number of supported disks multiplied by the maximum capacity of a single

disk [1 TB]). Based on the configuration indicators, we've populated the

Available Storage Configurations table so you can choose your desired level

of storage resource for each Azure Stack Hub VM. However, it's important to

note that you can add or change the Available Storage Configurations table as

necessary.

Each VM starts with an initially assigned local temp storage. To reflect the thin

provisioning of temp storage, you can change the local-temp number to

anything in the drop-down menu, including the maximum allowable temp

storage amount.

DefineByWorkloadFootprint instructions

 Tip

To change the provided storage size for an Azure Stack Hub VM, see the note from

step 3 in the preceding section.

1. In the upper right corner of this worksheet, use the provided pull-down list box

controls to select an initial number of servers (between 4 and 16) that you want

installed in each hardware system (SKU).

2. If you want to model various VM resource allocations against one specific

hardware configuration, find the blue pull-down list box directly below the Current

SKU label in the upper right corner of the page. Pull down this list box and select

your desired hardware SKU.

3. Select the appropriate storage size for each of your desired Azure Stack Hub VMs

on the DefineByVMFootprint page. This process is described in step three of the

previous section. The storage size per VM is defined in the DefineByVMFootprint

sheet.

4. Starting on the upper left of the DefineByWorkloadFootprint page, create

configurations for up to six different workload types. Enter the quantity of each VM

type contained within that workload. You do this by placing numeric values into

the column directly below that workload's name. You can modify workload names

to reflect the type of workloads that will be supported by this particular

configuration.

5. If you want to add GPU workloads here, add them to the Custom Workloads.

Please note: ONLY GPU type selected in the DefinedSolutionSKUs tab will be

available for capacity planning, any other GPU choices entered will be ignored.

6. You can include a particular quantity of each workload type by entering a value at

the bottom of that column, directly below the Quantity label.

7. When you've created workload types and quantities, select Suggested SKU in the

upper right corner of the page, directly below the Current SKU label. The smallest

SKU with enough resources to support this overall configuration of workloads will

display.

8. You can accomplish further modeling by modifying the number of servers selected

for a hardware SKU or by changing the VM allocations or quantities within your

workload configurations. The associated graphs display immediate feedback,

showing how your changes affect the overall resource consumption.

9. When you're satisfied with your changes, select Suggested SKU again to display

the SKU suggested for your new configuration. You can also select the drop-down

menu to select your desired SKU.

Learn about datacenter integration considerations for Azure Stack Hub.

Next steps

Azure Stack Hub datacenter integration

walkthrough

Article • 07/29/2022

This article describes the end-to-end process for Azure Stack Hub datacenter

integration, from purchasing to post-deployment support. The integration is a

collaborative project between the customer, a solution provider, and Microsoft. Click the

following tabs to see the specific steps for each member of the project, and see the next

sections for a summary of different phases for the project timeline.

1. Describe use cases and requirements

2. Determine the billing model

3. Review and approve contracts

4. Complete the Deployment Worksheet

5. Make sure deployment prerequisites are met

6. Prepare the datacenter

7. Provide subscription info during deployment

8. Resolve any questions about the provided data

Microsoft or an Azure Stack Hub solution partner will help evaluate your goals. They'll

help you decide questions like:

Is Azure Stack Hub the right solution for your organization?

What type of billing and licensing model will work for your organization?

What size solution will you need?

What are the power and cooling requirements?

Use the Azure Stack Hub Capacity Planner to investigate and analyze the best

hardware capacity and configuration for your needs.

Your organization commits to purchasing Azure Stack Hub, signs contracts and purchase

orders, and provides the integration requirements data to the solution provider.

Customer

Planning

Order process

You decide how to integrate Azure Stack Hub into your datacenter. Microsoft

collaborated with solution providers to publish a deployment worksheet to help you

gather the necessary information. The general datacenter integration considerations

article provides information that helps you complete the template, known as the

Deployment Worksheet.

You'll choose the following items:

Azure Stack Hub connection model and identity provider. You can choose to

deploy Azure Stack Hub either connected to the internet (and to Azure) or

disconnected. To get the most benefit from Azure Stack Hub, including hybrid

scenarios, you'd want to deploy connected to Azure. Choosing Active Directory

Federation Services (AD FS) or Azure Active Directory (Azure AD) is a one-time

decision that you must make at deployment time. You can't change your identity

provider later without redeploying the entire system.

Licensing model. The licensing model options for you to choose from depend on

the kind of deployment you'll have. Your identity provider choice has no bearing

on tenant virtual machines or the identity system and accounts they use.

Customers that are in a disconnected deployment have only one option:

capacity-based billing.

Customers that are in a connected deployment can choose between capacitybased billing and pay-as-you-use. Capacity-based billing requires an Enterprise

Agreement (EA) Azure Subscription for registration. This is necessary for

registration, which provides for the availability of items in Azure Marketplace

through an Azure Subscription.

Network integration. Network integration is crucial for deployment, operation,

and management of Azure Stack Hub systems. There are several considerations

that go into ensuring the Azure Stack Hub solution is resilient and has a highly

available physical infrastructure to support its operations.

Pre-deployment

） Important

All prerequisites are investigated before ordering the solution to help prevent

deployment delays. Verifying prerequisites can take time and require coordination

and data gathering from different departments within your organization.

Firewall integration. It's recommended that you use a firewall to help secure Azure

Stack Hub. Firewalls can help prevent DDOS attacks, intrusion detection, and

content inspection. However, it should be noted that it can become a throughput

bottleneck for Azure storage services.

Certificate requirements. It's critical that all required certificates are available

before an onsite engineer arrives at your datacenter for deployment.

After all the pre-requisite information is gathered through the deployment worksheet,

the solution provider will kick off the factory process based on the data collected to

ensure a successful integration of Azure Stack Hub into your datacenter.

The following table lists changes to your Azure Stack Hub deployment that require redeploying the entire system:

Option Re-deployment

Change identity system from Azure AD to AD FS Yes

Change the Azure AD directory that was used for deployment Yes

Change the network IP ranges Yes

Change the AD FS integrated Active Directory No

Change the billing model No

Change the Azure subscription used for registration No

Your solution provider will work with you on scheduling when the solution will arrive to

your facility. Once received and put in place, you'll need to schedule time with the

solution provider to have an engineer come onsite to perform the Azure Stack Hub

deployment.

It's crucial that all prerequisite data is locked and available before the onsite engineer

arrives to deploy the solution.

All certificates must be purchased and ready.

Region name must be decided on.

Changes that require re-deployment

Hardware delivery

All network integration parameters are finalized and match with what you have

shared with your solution provider.

To deploy Azure Stack Hub, an onsite engineer from your hardware solution provider

will need to be present to kick off the deployment. To ensure a successful deployment,

ensure that all information provided through the deployment worksheet hasn't

changed.

The following checks are what you should expect from the onsite engineer during the

deployment experience:

Check all the cabling and border connectivity to ensure the solution is properly put

together and meets your requirements.

Configure the solution Hardware Lifecycle Host (HLH), if present.

Check to make sure all BMC, BIOS, and network settings are correct.

Make sure firmware for all components is at the latest approved version by the

solution.

Start the deployment.

Several steps must be performed by the partner before the solution is handed off to the

customer in the post-integration phase. In this phase, validation is important to ensure

the system is deployed and performing correctly.

Actions that should be taken by the OEM Partner are:

Run test-azurestack.

 Tip

If any of this information has changed, make sure to communicate the change with

the solution provider before you schedule the actual deployment.

Onsite deployment

７ Note

A deployment procedure by the onsite engineer might take about one business

week to complete.

Post deployment

Register with Azure.

Ensure Azure Stack Hub Marketplace syndication.

Back up Switch Configuration and HLH Configuration files.

Remove DVM.

Prepare a customer summary for deployment.

Check updates to make sure the solution software is updated to the latest version.

There are several steps that are required or optional depending on the installation type.

If deployment was completed using AD FS, then the Azure Stack Hub stamp will

need to be integrated with customer's own AD FS.

Integration with an existing monitoring system from the respective partner.

System Center Operations Manager Integration also supports fleet management

capabilities.

Nagios Integration.

７ Note

This step is the responsibility of the customer, although the partner may

optionally choose to offer services to do this.

Schedule

Support

Azure Stack Hub enables an Azure-consistent, integrated support experience that covers

the full system lifecycle. To fully support Azure Stack Hub integrated systems, customers

need two support contracts: one with Microsoft (or their Cloud Solution Provider) for

Azure services support and one with the hardware provider for system support. The

integrated support experience provides coordinated escalation and resolution so that

customers get a consistent support experience no matter whom they call first. For

customers who already have Premier, Azure -Standard / ProDirect or Partner support

with Microsoft, Azure Stack Hub software support is included.

The integrated support experience makes use of a Case Exchange mechanism for bidirectional transfer of support cases and case updates between Microsoft and the

hardware partner. Microsoft Azure Stack Hub will follow the Modern Lifecycle policy .

Learn more about general datacenter integration considerations.

Next steps

Datacenter integration planning

considerations for Azure Stack Hub

integrated systems

Article • 07/29/2022

If you're interested in an Azure Stack Hub integrated system, you should understand the

major planning considerations around deployment and how the system fits into your

datacenter. This article provides a high-level overview of these considerations to help

you make important infrastructure decisions for your Azure Stack Hub integrated

systems. An understanding of these considerations helps when working with your OEM

hardware vendor while they deploy Azure Stack Hub to your datacenter.

To deploy Azure Stack Hub, you need to provide planning information to your solution

provider before deployment starts to help the process go quickly and smoothly. The

information required ranges across networking, security, and identity information with

many important decisions that may require knowledge from many different areas and

decision makers. You'll need people from multiple teams in your organization to ensure

that you have all required information ready before deployment. It can help to talk to

your hardware vendor while collecting this information because they might have helpful

advice.

While researching and collecting the required information, you might need to make

some pre-deployment configuration changes to your network environment. These

changes could include reserving IP address spaces for the Azure Stack Hub solution as

well as configuring your routers, switches, and firewalls to prepare for the connectivity

to the new Azure Stack Hub solution switches. Make sure to have the subject area expert

lined up to help you with your planning.

When you evaluate an Azure Stack Hub solution for acquisition, you make hardware

configuration choices which have a direct impact on the overall capacity of the Azure

Stack Hub solution. These include the classic choices of CPU, memory density, storage

７ Note

Azure Stack Hub integrated systems can only be purchased from authorized

hardware vendors.

Capacity planning considerations

configuration, and overall solution scale (for example, number of servers). Unlike a

traditional virtualization solution, the simple arithmetic of these components to

determine usable capacity doesn't apply. The first reason is that Azure Stack Hub is

architected to host the infrastructure or management components within the solution

itself. The second reason is that some of the solution's capacity is reserved in support of

resiliency by updating the solution's software in a way that minimizes disruption of

tenant workloads.

The Azure Stack Hub capacity planner spreadsheet helps you make informed

decisions for planning capacity in two ways. The first is by selecting a hardware offering

and attempting to fit a combination of resources. The second is by defining the

workload that Azure Stack Hub is intended to run to view the available hardware SKUs

that can support it. Finally, the spreadsheet is intended as a guide to help in making

decisions related to Azure Stack Hub planning and configuration.

The spreadsheet isn't intended to serve as a substitute for your own investigation and

analysis. Microsoft makes no representations or warranties, express or implied, with

respect to the information provided within the spreadsheet.

Azure Stack Hub is a sealed system, where the infrastructure is locked down both from a

permissions and network perspective. Network access control lists (ACLs) are applied to

block all unauthorized incoming traffic and all unnecessary communications between

infrastructure components. This system makes it difficult for unauthorized users to

access the system.

For daily management and operations, there's no unrestricted admin access to the

infrastructure. Azure Stack Hub operators must manage the system through the

administrator portal or through Azure Resource Manager (via PowerShell or the REST

API). There's no access to the system by other management tools like Hyper-V Manager

or Failover Cluster Manager. To help protect the system, third-party software (for

example, agents) can't be installed inside the components of the Azure Stack Hub

infrastructure. Interoperability with external management and security software occurs

via PowerShell or the REST API.

Contact Microsoft Support when you need a higher level of access for troubleshooting

issues that aren't resolved through alert mediation steps. Through support, there's a

method to provide temporary full admin access to the system for more advanced

operations.

Management considerations

You'll need to consider which identity provider you want to use for Azure Stack Hub

deployment, either Azure AD or AD FS. You can't switch identity providers after

deployment without full system redeployment. If you don't own the Azure AD account

and are using an account provided to you by your Cloud Solution Provider, and if you

decide to switch provider and use a different Azure AD account, you'll have to contact

your solution provider to redeploy the solution for you at your cost.

Your identity provider choice has no bearing on tenant virtual machines (VMs), the

identity system, accounts they use, or whether they can join an Active Directory domain,

and so on. These things are separate.

You can deploy multiple Azure Stack Hub systems with the same Azure Active Directory

tenant or Active Directory.

If you choose to deploy Azure Stack Hub using AD FS as the identity provider, you must

integrate the AD FS instance on Azure Stack Hub with an existing AD FS instance

through a federation trust. This integration allows identities in an existing Active

Directory forest to authenticate with resources in Azure Stack Hub.

You can also integrate the Graph service in Azure Stack Hub with the existing Active

Directory. This integration lets you manage Role-Based Access Control (RBAC) in Azure

Stack Hub. When access to a resource is delegated, the Graph component looks up the

user account in the existing Active Directory forest using the LDAP protocol.

The following diagram shows integrated AD FS and Graph traffic flow.

Identity considerations

Choose identity provider

AD FS and Graph integration

You must decide which licensing model you want to use. The available options depend

on if you deploy Azure Stack Hub connected to the internet:

For a connected deployment, you can choose either pay-as-you-use or capacitybased licensing. Pay-as-you-use requires a connection to Azure to report usage,

which is then billed through Azure commerce.

Only capacity-based licensing is supported if you deploy disconnected from the

internet.

For more information about the licensing models, see Microsoft Azure Stack Hub

packaging and pricing .

You'll need to think about how you want to plan your Azure Stack Hub namespace,

especially the region name and external domain name. The external fully qualified

domain name (FQDN) of your Azure Stack Hub deployment for public-facing endpoints

is the combination of these two names: <region>.<fqdn>. For example,

east.cloud.fabrikam.com. In this example, the Azure Stack Hub portals would be available

at the following URLs:

https://portal.east.cloud.fabrikam.com

https://adminportal.east.cloud.fabrikam.com

Licensing model

Naming decisions

） Important

The region name you choose for your Azure Stack Hub deployment must be unique

and will appear in the portal addresses.

The following table summarizes these domain naming decisions.

Name Description

Region

name

The name of your first Azure Stack Hub region. This name is used as part of the FQDN

for the public virtual IP addresses (VIPs) that Azure Stack Hub manages. Typically, the

region name would be a physical location identifier such as a datacenter location.

The region name must consist of only letters and numbers between 0-9. No special

characters (like - , # , and so on) are allowed.

External

domain

name

The name of the Domain Name System (DNS) zone for endpoints with external-facing

VIPs. Used in the FQDN for these public VIPs.

Private

(internal)

domain

name

The name of the domain (and internal DNS zone) created on Azure Stack Hub for

infrastructure management.

For deployment, you'll need to provide Secure Sockets Layer (SSL) certificates for publicfacing endpoints. At a high level, certificates have the following requirements:

You can use a single wildcard certificate or you can use a set of dedicated

certificates, and then use wildcards only for endpoints like storage and Key Vault.

Certificates can be issued by a public trusted certificate authority (CA) or a

customer-managed CA.

For more information about what PKI certificates are required to deploy Azure Stack

Hub, and how to obtain them, see, Azure Stack Hub Public Key Infrastructure certificate

requirements.

Certificate requirements

） Important

The provided PKI certificate information should be used as general guidance.

Before you acquire any PKI certificates for Azure Stack Hub, work with your OEM

hardware partner. They'll provide more detailed certificate guidance and

requirements.

You must choose a specific time server which is used to synchronize Azure Stack Hub.

Time synchronization is critical to Azure Stack Hub and its infrastructure roles because

it's used to generate Kerberos tickets. Kerberos tickets are used to authenticate internal

services with each other.

You must specify an IP for the time synchronization server. Although most of the

components in the infrastructure can resolve a URL, some only support IP addresses. If

you're using the disconnected deployment option, you must specify a time server on

your corporate network that you're sure you can reach from the infrastructure network

in Azure Stack Hub.

For hybrid cloud scenarios, you'll need to plan how you want to connect Azure Stack

Hub to Azure. There are two supported methods to connect virtual networks in Azure

Stack Hub to virtual networks in Azure:

Site-to-site: A virtual private network (VPN) connection over IPsec (IKE v1 and IKE

v2). This type of connection requires a VPN device or Routing and Remote Access

Service (RRAS). For more information about VPN gateways in Azure, see About

VPN Gateway. The communication over this tunnel is encrypted and secure.

However, bandwidth is limited by the maximum throughput of the tunnel (100-200

Mbps).

Outbound NAT: By default, all VMs in Azure Stack Hub will have connectivity to

external networks via outbound NAT. Each virtual network that's created in Azure

Stack Hub gets a public IP address assigned to it. Whether the VM is directly

assigned a public IP address or is behind a load balancer with a public IP address,

it will have outbound access via outbound NAT using the VIP of the virtual

network. This method only works for communication that's initiated by the VM and

destined for external networks (either internet or intranet). It can't be used to

communicate with the VM from outside.

Time synchronization

） Important

If your time server isn't a Windows-based NTP server, you need to append ,0x8 the

end of the IP address. For example, 10.1.1.123,0x8 .

Connect Azure Stack Hub to Azure

For hybrid connectivity, it's important to consider what kind of deployment you want to

offer and where it will be deployed. You'll need to consider whether you need to isolate

network traffic per tenant, and whether you'll have an intranet or internet deployment.

Single-tenant Azure Stack Hub: An Azure Stack Hub deployment that looks, at

least from a networking perspective, as if it's one tenant. There can be many tenant

subscriptions, but like any intranet service, all traffic travels over the same

networks. Network traffic from one subscription travels over the same network

connection as another subscription and doesn't need to be isolated via an

encrypted tunnel.

Multi-tenant Azure Stack Hub: An Azure Stack Hub deployment where each

tenant subscription's traffic that's bound for networks that are external to Azure

Stack Hub must be isolated from other tenants' network traffic.

Intranet deployment: An Azure Stack Hub deployment that sits on a corporate

intranet, typically on private IP address space and behind one or more firewalls.

The public IP addresses aren't truly public because they can't be routed directly

over the public internet.

Internet deployment: An Azure Stack Hub deployment that's connected to the

public internet and uses internet-routable public IP addresses for the public VIP

range. The deployment can still sit behind a firewall, but the public VIP range is

directly reachable from the public internet and Azure.

The following table summarizes the hybrid connectivity scenarios with the pros, cons,

and use cases.

Scenario Connectivity

Method

Pros Cons Good For

Single

tenant

Azure Stack

Hub,

intranet

deployment

Outbound

NAT

Better

bandwidth

for faster

transfers.

Simple to

implement;

no

gateways

required.

Traffic not

encrypted;

no isolation

or encryption

outside the

stack.

Enterprise deployments where all

tenants are equally trusted.

Enterprises that have an Azure

ExpressRoute circuit to Azure.

Hybrid connectivity options

Scenario Connectivity

Method

Pros Cons Good For

Multitenant

Azure Stack

Hub,

intranet

deployment

Site-to-site

VPN

Traffic from

the tenant

VNet to

destination

is secure.

Bandwidth is

limited by

site-to-site

VPN tunnel.

Requires a

gateway in

the virtual

network and

a VPN device

on the

destination

network.

Enterprise deployments where

some tenant traffic must be secured

from other tenants.

Single

tenant

Azure Stack

Hub,

internet

deployment

Outbound

NAT

Better

bandwidth

for faster

transfers.

Traffic not

encrypted;

no isolation

or encryption

outside the

stack.

Hosting scenarios where the tenant

gets their own Azure Stack Hub

deployment and a dedicated circuit

to the Azure Stack Hub

environment. For example,

ExpressRoute and Multiprotocol

Label Switching (MPLS).

Multitenant

Azure Stack

Hub,

internet

deployment

Site-to-site

VPN

Traffic from

the tenant

VNet to

destination

is secure.

Bandwidth is

limited by

site-to-site

VPN tunnel.

Requires a

gateway in

the virtual

network and

a VPN device

on the

destination

network.

Hosting scenarios where the

provider wants to offer a multitenant cloud, where the tenants

don't trust each other and traffic

must be encrypted.

You can connect Azure Stack Hub to Azure via ExpressRoute for both single-tenant

intranet and multi-tenant scenarios. You'll need a provisioned ExpressRoute circuit

through a connectivity provider.

The following diagram shows ExpressRoute for a single-tenant scenario (where

"Customer's connection" is the ExpressRoute circuit).

Using ExpressRoute

The following diagram shows ExpressRoute for a multi-tenant scenario.

To get a single view of all alerts from your Azure Stack Hub deployment and devices,

and to integrate alerts into existing IT Service Management workflows for ticketing, you

can integrate Azure Stack Hub with external datacenter monitoring solutions.

Included with the Azure Stack Hub solution, the hardware lifecycle host is a computer

outside Azure Stack Hub that runs OEM vendor-provided management tools for

External monitoring

hardware. You can use these tools or other solutions that directly integrate with existing

monitoring solutions in your datacenter.

The following table summarizes the list of currently available options.

Area External Monitoring Solution

Azure Stack Hub software Azure Stack Hub Management Pack for Operations

Manager

Nagios plug-in

REST-based API calls

Physical servers (BMCs via IPMI) OEM hardware - Operations Manager vendor management

pack

OEM hardware vendor-provided solution

Hardware vendor Nagios plug-ins.

OEM partner-supported monitoring solution (included)

Network devices (SNMP) Operations Manager network device discovery

OEM hardware vendor-provided solution

Nagios switch plug-in

Tenant subscription health

monitoring

System Center Management Pack for Windows Azure

Note the following requirements:

The solution you use must be agentless. You can't install third-party agents inside

Azure Stack Hub components.

If you want to use System Center Operations Manager, Operations Manager 2012

R2 or Operations Manager 2016 is required.

Planning for backup and disaster recovery involves planning for both the underlying

Azure Stack Hub infrastructure that hosts IaaS VMs and PaaS services, and for tenant

apps and data. Plan for these things separately.

You can back up Azure Stack Hub infrastructure components to an SMB share that you

specify:

You'll need an external SMB file share on an existing Windows-based file server or

a third-party device.

Backup and disaster recovery

Protect infrastructure components

Use this same share for the backup of network switches and the hardware lifecycle

host. Your OEM hardware vendor will help provide guidance for backup and

restore of these components because these are external to Azure Stack Hub. You're

responsible for running the backup workflows based on the OEM vendor's

recommendation.

If catastrophic data loss occurs, you can use the infrastructure backup to reseed

deployment data such as:

Deployment inputs and identifiers

Service accounts

CA root certificate

Federated resources (in disconnected deployments)

Plans, offers, subscriptions, and quotas

RBAC policy and role assignments

Key Vault secrets

Azure Stack Hub doesn't back up tenant apps and data. You must plan for backup and

disaster recovery protection to a target external to Azure Stack Hub. Tenant protection is

a tenant-driven activity. For IaaS VMs, tenants can use in-guest technologies to protect

file folders, app data, and system state. However, as an enterprise or service provider,

you may want to offer a backup and recovery solution in the same datacenter or

externally in a cloud.

To back up Linux or Windows IaaS VMs, you must use backup products with access to

the guest operating system to protect file, folder, operating system state, and app data.

You can use Azure Backup, System Center Datacenter Protection Manager, or supported

third-party products.

２ Warning

By default your Azure Stack Hub stamp is configured with only one CloudAdmin

account. There are no recovery options if the account credentials are lost,

compromised, or locked. You will lose access to the privileged endpoint and other

resources.

It is highly recommended that you create additional CloudAdmin accounts, to

avoid redeployment of your stamp at your own expense. Make sure you

document these credentials based on your company's guidelines.

Protect tenant apps on IaaS VMs

To replicate data to a secondary location and orchestrate application failover if a disaster

occurs, you can use Azure Site Recovery or supported third-party products. Also, apps

that support native replication, like Microsoft SQL Server, can replicate data to another

location where the app is running.

For information about use cases, purchasing, partners, and OEM hardware vendors,

see the Azure Stack Hub product page.

For information about the roadmap and geo-availability for Azure Stack Hub

integrated systems, see the white paper: Azure Stack Hub: An extension of Azure .

Azure Stack Hub deployment connection models

Learn more

Next steps

Azure Stack Hub integrated systems

connection models

Article • 07/29/2022

If you're interested in purchasing an Azure Stack Hub integrated system, you need to

understand several datacenter integration considerations for Azure Stack Hub

deployment to determine how the system will fit into your datacenter. In addition, you

need to decide how you'll integrate Azure Stack Hub into your hybrid cloud

environment. This article provides an overview of these major decisions including Azure

connection models, identity store options, and billing model options.

If you decide to purchase an integrated system, your original equipment manufacturer

(OEM) hardware vendor will help guide you through the planning process in more

detail. The OEM hardware vendor also performs the actual deployment.

You can choose to deploy Azure Stack Hub either connected to the internet (and to

Azure) or disconnected. Deploy connected to Azure to get the most benefit from Azure

Stack Hub, including hybrid scenarios between Azure Stack Hub and Azure. This choice

defines which options are available for your identity store (Azure Active Directory or

Active Directory Federation Services) and billing model (pay as you use-based billing or

capacity-based billing) as summarized in the following diagram and table:

Choose an Azure Stack Hub deployment

connection model

） Important

Options Connected to Azure Disconnected from

Azure

Azure AD

AD FS

Consumptionbased billing AD FS supported

Capacity-based

billing

Licensing Enterprise Agreement or Cloud Solution Provider Enterprise

Agreement

Patch and

update

Update package can be downloaded directly from the

Internet to Azure Stack Hub

Required

Also requires

removable media

and a separate

connected device

Registration Automated Required

Also requires

removable media

and a separate

connected device

After you've decided on the Azure connection model to be used for your Azure Stack

Hub deployment, additional connection-dependent decisions must be made for the

identity store and billing method.

Azure connected Azure Stack Hub deployment decisions

Azure disconnected Azure Stack Hub deployment decisions

This is a key decision point! Choosing Active Directory Federation Services (AD FS)

or Azure Active Directory (Azure AD) is a one-time decision that you must make at

deployment time. You can't change this later without re-deploying the entire

system.

Next steps

Azure-connected deployment planning

decisions for Azure Stack Hub

integrated systems

Article • 07/29/2022

After you've decided how you'll integrate Azure Stack Hub into your hybrid cloud

environment, you can finalize your Azure Stack Hub deployment decisions.

Deploying Azure Stack Hub connected to Azure means that you can have either Azure

Active Directory (Azure AD) or Active Directory Federation Services (AD FS) for your

identity store. You can also choose from either billing model: pay-as-you-use or

capacity-based. A connected deployment is the default option because it allows

customers to get the most value out of Azure Stack Hub, particularly for hybrid cloud

scenarios that involve both Azure and Azure Stack Hub.

With a connected deployment, you can choose between Azure AD or AD FS for your

identity store. A disconnected deployment, with no internet connectivity, can only use

AD FS.

Your identity store choice has no bearing on tenant virtual machines (VMs). Tenant VMs

may choose which identity store they want to the connect to depending on how they'll

be configured: Azure AD, Windows Server Active Directory domain-joined, workgroup,

and so on. This is unrelated to the Azure Stack Hub identity provider decision.

For example, if you deploy IaaS tenant VMs on top of Azure Stack Hub, and want them

to join a Corporate Active Directory Domain and use accounts from there, you still can.

You aren't required to use the Azure AD identity store you select here for those

accounts.

Using Azure AD for your identity store requires two Azure AD accounts: a global admin

account and a billing account. These accounts can be the same accounts, or different

accounts. While using the same user account might be simpler and useful if you have a

limited number of Azure accounts, your business needs might suggest using two

accounts:

Choose an identity store

Azure AD identity store

1. Global admin account (only required for connected deployments). This is an Azure

account that's used to create apps and service principals for Azure Stack Hub

infrastructure services in Azure AD. This account must have directory admin

permissions to the directory that your Azure Stack Hub system will be deployed

under. It will become the "cloud operator" Global Admin for the Azure AD user and

is used for the following tasks:

To provision and delegate apps and service principals for all Azure Stack Hub

services that need to interact with Azure AD and Graph API.

As the Service Administrator account. This account is the owner of the default

provider subscription (which you can later change). You can log into the

Azure Stack Hub administrator portal with this account, and can use it to

create offers and plans, set quotas, and perform other administrative

functions in Azure Stack Hub.

2. Billing account (required for both connected and disconnected deployments). This

Azure account is used to establish the billing relationship between your Azure

Stack Hub integrated system and the Azure commerce backend. This is the account

that's billed for Azure Stack Hub fees. This account will also be used for offering

items in the marketplace and other hybrid scenarios.

Choose this option if you want to use your own identity store, such as your corporate

Active Directory, for your Service Administrator accounts.

You can choose either Pay-as-you-use or the Capacity billing model. Pay-as-you-use

billing model deployments must be able to report usage through a connection to Azure

at least once every 30 days. Therefore, the pay-as-you-use billing model is only available

for connected deployments.

） Important

The global administrator account is not required to run Azure Stack Hub and

can be disabled post-deployment.

Secure the global administrator account following the best practices

documented here.

AD FS identity store

Choose a billing model

With the pay-as-you-use billing model, usage is charged to an Azure subscription. You

only pay when you use the Azure Stack Hub services. If this is the model you decide on,

you'll need an Azure subscription and the account ID associated with that subscription

(for example, serviceadmin@contoso.onmicrosoft.com). EA, CSP, and CSP Shared

Services subscriptions are supported. Usage reporting is configured during Azure Stack

Hub registration.

If you're going to use a CSP subscription, review the table below to identify which CSP

subscription to use, as the correct approach depends on the exact CSP scenario:

Scenario Domain and subscription options

You're a Direct CSP Partner or an

Indirect CSP Provider, and you'll

operate the Azure Stack Hub

Use a CSP Shared Services subscription.

or

Create an Azure AD tenant with a descriptive name in

Partner Center. For example, <your organization>CSPAdmin

with an Azure CSP subscription associated with it.

You're an Indirect CSP Reseller,

and you'll operate the Azure Stack

Hub

Ask your indirect CSP Provider to create an Azure AD tenant

for your organization with an Azure CSP subscription

associated with it using Partner Center.

If you decide to use the capacity billing model, you must purchase an Azure Stack Hub

Capacity Plan SKU based on the capacity of your system. You need to know the number

of physical cores in your Azure Stack Hub to purchase the correct quantity.

Capacity billing requires an Enterprise Agreement (EA) Azure subscription for

registration. The reason is that registration sets up the availability of items in the

Marketplace, which requires an Azure subscription. The subscription isn't used for Azure

Stack Hub usage.

Pay-as-you-use

７ Note

In most cases, Enterprise customers will use EA subscriptions, and service providers

will use CSP or CSP Shared Services subscriptions.

Capacity-based billing

Learn more

For information about use cases, purchasing, partners, and OEM hardware vendors,

see the Azure Stack Hub product page.

For information about the roadmap and geo-availability for Azure Stack Hub

integrated systems, see the white paper: Azure Stack Hub: An extension of Azure .

To learn more about Microsoft Azure Stack Hub packaging and pricing, download

the .pdf .

Datacenter network integration

Next steps

Azure disconnected deployment

planning decisions for Azure Stack Hub

integrated systems

Article • 07/29/2022

After you've decided how you'll integrate Azure Stack Hub into your hybrid cloud

environment, you can finish your Azure Stack Hub deployment decisions.

You can deploy and use Azure Stack Hub without a connection to the internet. However,

with a disconnected deployment, you're limited to an Active Directory Federation

Services (AD FS) identity store and the capacity-based billing model. Because

multitenancy requires the use of Azure Active Directory (Azure AD), multitenancy isn't

supported for disconnected deployments.

Choose this option if:

You have security or other restrictions that require you to deploy Azure Stack Hub

in an environment that isn't connected to the internet.

You want to block data (including usage data) from being sent to Azure.

You want to use Azure Stack Hub purely as a private cloud solution that's deployed

to your corporate intranet, and aren't interested in hybrid scenarios.

A disconnected deployment doesn't restrict you from later connecting your Azure Stack

Hub instance to Azure for hybrid tenant VM scenarios. It means that you don't have

connectivity to Azure during deployment or you don't want to use Azure AD as your

identity store.

Azure Stack Hub was designed to work best when connected to Azure, so it's important

to note that there are some features and functionality that are either impaired or

completely unavailable in the disconnected mode.

 Tip

Sometimes, this kind of environment is also referred to as a submarine scenario.

Features that are impaired or unavailable in

disconnected deployments

Feature Impact in Disconnected mode

VM deployment with

DSC extension to

configure VM post

deployment

Impaired - DSC extension looks to the internet for the latest WMF.

VM deployment with

Docker Extension to

run Docker commands

Impaired - Docker will check the internet for the latest version and this

check will fail.

Documentation links in

the Azure Stack Hub

Portal

Unavailable - Links like Give Feedback, Help, and Quickstart that use an

internet URL won't work.

Alert

remediation/mitigation

that references an

online remediation

guide

Unavailable - Any alert remediation links that use an internet URL won't

work.

Marketplace - The

ability to select and

add Gallery packages

directly from Azure

Marketplace

Impaired - When you deploy Azure Stack Hub in a disconnected mode,

you can't download marketplace items by using the Azure Stack Hub

portal. However, you can use the marketplace syndication tool to

download the marketplace items to a machine that has internet

connectivity and then transfer them to your Azure Stack Hub

environment.

Using Azure AD

federation accounts to

manage an Azure

Stack Hub deployment

Unavailable - This feature requires connectivity to Azure. AD FS with a

local Active Directory instance must be used instead.

App Services Impaired - WebApps may require internet access for updated content.

Command Line

Interface (CLI)

Impaired - CLI has reduced functionality for authentication and

provisioning of service principals.

Visual Studio - Cloud

discovery

Impaired - Cloud Discovery will either discover different clouds or won't

work at all.

Visual Studio - AD FS Impaired - Only Visual Studio Enterprise and Visual Studio Code support

AD FS authentication.

Telemetry Unavailable - Telemetry data for Azure Stack Hub and any third-party

gallery packages that depend on telemetry data.

Feature Impact in Disconnected mode

Certificate Authority

(CA)

Public/external Certificate Authority (CA)

Unavailable – Deployment will fail if certificates were issued from a

public CA, as internet connectivity is required to access the Certificate

Revocation List (CRL) and Online Certificate Status Protocol (OCSP)

services in the context of HTTPS.

Private/internal Certificate Authority (CA)

No impact - In cases where the deployment uses certificates issued by a

private CA, such as an internal CA within an organization, only internal

network access to the CRL endpoint is required. Internet connectivity is

not required, but you should verify that your Azure Stack Hub

infrastructure has the required network access to contact the CRL

endpoint defined in the certificates CDP extension.

Key Vault Impaired - A common use case for Key Vault is to have an app read

secrets at runtime. For this use case, the app needs a service principal in

the directory. In Azure AD, regular users (non-admins) are by default

allowed to add service principals. In Azure AD (using AD FS), they're not.

This impairment places a hurdle in the end-to-end experience because

one must always go through a directory admin to add any app.

Containers Impaired - Unable to import container images in disconnected mode

from an Azure Container Registry in Azure public or another accessible

registry. See FAQ entry at Azure Container Registry on Azure Stack Hub

for information on how to import container images in Azure Container

Registry to a disconnected Azure Stack Hub deployment running

Kubernetes.

For information about use cases, purchasing, partners, and OEM hardware vendors,

see the Azure Stack Hub product page.

For information about the roadmap and geo-availability for Azure Stack Hub

integrated systems, see the white paper: Azure Stack Hub: An extension of Azure .

To learn more about Microsoft Azure Stack Hub packaging and pricing, download

the .pdf .

Datacenter network integration

Learn more

Next steps

Network integration planning for Azure

Stack Hub

Article • 07/29/2022

This article provides Azure Stack Hub network infrastructure information to help you

decide how to best integrate Azure Stack Hub into your existing networking

environment.

The Azure Stack Hub solution requires a resilient and highly available physical

infrastructure to support its operation and services. To integrate Azure Stack Hub to the

network it requires uplinks from the Top-of-Rack switches (ToR) to the nearest switch or

router, which on this documentation is referred as Border. The ToRs can be uplinked to a

single or a pair of Borders. The ToR is pre-configured by our automation tool, it expects

a minimum of one connection between ToR and Border when using BGP Routing and a

minimum of two connections (one per ToR) between ToR and Border when using Static

Routing, with a maximum of four connections on either routing options. These

connections are limited to SFP+ or SFP28 media and a minimum of one GB speed.

Please check with your original equipment manufacturer (OEM) hardware vendor for

availability. The following diagram presents the recommended design:

７ Note

To resolve external DNS names from Azure Stack Hub (for example, www.bing.com),

you need to provide DNS servers to forward DNS requests. For more information

about Azure Stack Hub DNS requirements, see Azure Stack Hub datacenter

integration - DNS.

Physical network design

Azure Stack Hub is built using Windows Server 2019 Failover Cluster and Spaces Direct

technologies. A portion of the Azure Stack Hub physical network configuration is done

to utilize traffic separation and bandwidth guarantees to ensure that the Spaces Direct

storage communications can meet the performance and scale required of the solution.

The network configuration uses traffic classes to separate the Spaces Direct, RDMAbased communications from that of the network utilization by the Azure Stack Hub

Bandwidth Allocation

infrastructure and/or tenant. To align to the current best practices defined for Windows

Server 2019, Azure Stack Hub is changing to use an additional traffic class or priority to

further separate server to server communication in support of the Failover Clustering

control communication. This new traffic class definition will be configured to reserve 2%

of the available, physical bandwidth. This traffic class and bandwidth reservation

configuration is accomplished by a change on the top-of-rack (ToR) switches of the

Azure Stack Hub solution and on the host or servers of Azure Stack Hub. Note that

changes are not required on the customer border network devices. These changes

provide better resiliency for Failover Cluster communication and are meant to avoid

situations where network bandwidth is fully consumed and as a result Failover Cluster

control messages are disrupted. Note that the Failover Cluster communication is a

critical component of the Azure Stack Hub infrastructure and if disrupted for long

periods, can lead to instability in the Spaces Direct storage services or other services that

will eventually impact tenant or end-user workload stability.

Logical networks represent an abstraction of the underlying physical network

infrastructure. They're used to organize and simplify network assignments for hosts,

virtual machines (VMs), and services. As part of logical network creation, network sites

are created to define the virtual local area networks (VLANs), IP subnets, and IP

subnet/VLAN pairs that are associated with the logical network in each physical location.

The following table shows the logical networks and associated IPv4 subnet ranges that

you must plan for:

Logical

Network

Description Size

７ Note

The described changes are added at the host level of an Azure Stack Hub system in

the 2008 release. Please contact your OEM to arrange making the required changes

at the ToR network switches. This ToR change can be performed either prior to

updating to the 2008 release or after updating to 2008. The configuration change

to the ToR switches is required to improve the Failover Cluster communications.

Logical Networks

Logical

Network

Description Size

Public VIP Azure Stack Hub uses a total of 31 addresses from this network

and the rest are used by tenant VMs. From the 31 addresses, 8

public IP addresses are used for a small set of Azure Stack Hub

services. If you plan to use App Service and the SQL resource

providers, 7 more addresses are used. The remaining 16 IPs are

reserved for future Azure services.

/26 (62 hosts) -

/22 (1022

hosts)

Recommended

= /24 (254

hosts)

Switch

infrastructure

Point-to-point IP addresses for routing purposes, dedicated

switch management interfaces, and loopback addresses

assigned to the switch.

/26

Infrastructure Used for Azure Stack Hub internal components to communicate. /24

Private Used for the storage network, private VIPs, Infrastructure

containers and other internal functions. For more details

reference the Private network section in this article.

/20

BMC Used to communicate with the BMCs on the physical hosts. /26

The network infrastructure for Azure Stack Hub consists of several logical networks that

are configured on the switches. The following diagram shows these logical networks and

how they integrate with the top-of-rack (TOR), baseboard management controller

(BMC), and border (customer network) switches.

７ Note

An alert on the portal will remind the operator to run the PEP cmdlet SetAzsPrivateNetwork to add a new /20 Private IP space. For more information and

guidance on selecting the /20 private IP space, please see the Private network

section in this article.

Network infrastructure

This network is dedicated to connecting all the baseboard management controllers (also

known as BMC or service processors) to the management network. Examples include:

iDRAC, iLO, iBMC, and so on. Only one BMC account is used to communicate with any

BMC node. If present, the Hardware Lifecycle Host (HLH) is located on this network and

may provide OEM-specific software for hardware maintenance or monitoring.

The HLH also hosts the Deployment VM (DVM). The DVM is used during Azure Stack

Hub deployment and is removed when deployment completes. The DVM requires

internet access in connected deployment scenarios to test, validate, and access multiple

components. These components can be inside and outside of your corporate network

(for example: NTP, DNS, and Azure). For more information about connectivity

requirements, see the NAT section in Azure Stack Hub firewall integration.

This /20 (4096 IPs) network is private to the Azure Stack Hub region (doesn't route

beyond the border switch devices of the Azure Stack Hub system) and is divided into

multiple subnets, here are some examples:

Storage network: A /25 (128 IPs) network used to support the use of Spaces Direct

and Server Message Block (SMB) storage traffic and VM live migration.

Internal virtual IP network: A /25 network dedicated to internal-only VIPs for the

software load balancer.

Container network: A /23 (512 IPs) network dedicated to internal-only traffic

between containers running infrastructure services.

The Azure Stack Hub system requires an additional /20 private internal IP space. This

network will be private to the Azure Stack Hub system (doesn't route beyond the border

BMC network

Private network

switch devices of the Azure Stack Hub system) and can be reused on multiple Azure

Stack Hub systems within your datacenter. While the network is private to Azure Stack, it

must not overlap with other networks in the datacenter. The /20 private IP space is

divided into multiple networks that enable running the Azure Stack Hub infrastructure

on containers. In addition, this new Private IP space enables ongoing efforts to reduce

the required routable IP space prior to deployment. The goal of running the Azure Stack

Hub infrastructure in containers is to optimize utilization and enhance performance. In

addition, the /20 private IP space is also used to enable ongoing efforts that will reduce

required routable IP space before deployment. For guidance on Private IP space, we

recommend following RFC 1918 .

This /24 network is dedicated to internal Azure Stack Hub components so that they can

communicate and exchange data among themselves. This subnet can be routable

externally of the Azure Stack Hub solution to your datacenter, we do not recommend

using Public or Internet routable IP addresses on this subnet. This network is advertised

to the Border but most of its IPs are protected by Access Control Lists (ACLs). The IPs

allowed for access are within a small range equivalent in size to a /27 network and host

services like the privileged end point (PEP) and Azure Stack Hub Backup.

The public VIP network is assigned to the network controller in Azure Stack. It's not a

logical network on the switch. The SLB uses the pool of addresses and assigns /32

networks for tenant workloads. On the switch routing table, these /32 IPs are advertised

as an available route via BGP. This network contains the external-accessible or public IP

addresses. The Azure Stack Hub infrastructure reserves the first 31 addresses from this

public VIP network while the remainder is used by tenant VMs. The network size on this

subnet can range from a minimum of /26 (64 hosts) to a maximum of /22 (1022 hosts).

We recommend that you plan for a /24 network.

Azure Stack Hub uses virtual networks for customer resources such as virtual machines,

load balancers, and others.

There are several different options for connecting from resources inside the virtual

network to on-premises/corporate resources:

Use public IP addresses from the public VIP network.

Azure Stack Hub infrastructure network

Public VIP network

Connecting to on-premises networks

Use Virtual Network Gateway or Network Virtual Appliance (NVA).

When a S2S VPN tunnel is used to connect resources to or from on-premises networks,

you may encounter a scenario in which a resource also has a public IP address assigned,

and it is no longer reachable via that public IP address. If the source attempts to access

the public IP fall within the same subnet range that is defined in the Local Network

Gateway Routes (Virtual Network Gateway) or user-defined route for NVA solutions,

Azure Stack Hub attempts to route the traffic outbound back to the source through the

S2S tunnel, based on the routing rules that are configured. The return traffic uses the

private IP address of the VM, rather than be source NATed as the public IP address:

There are two solutions to this issue:

Route the traffic directed to the public VIP network to the internet.

Add a NAT device to NAT any subnet IPs defined in the local network gateway

directed to the public VIP network.



This /26 network is the subnet that contains the routable point-to-point IP /30 (two host

IPs) subnets and the loopbacks, which are dedicated /32 subnets for in-band switch

management and BGP router ID. This range of IP addresses must be routable outside

the Azure Stack Hub solution to your datacenter. They may be private or public IPs.

This /29 (six host IPs) network is dedicated to connecting the management ports of the

switches. It allows out-of-band access for deployment, management, and

troubleshooting. It's calculated from the switch infrastructure network mentioned above.

The Deployment Worksheet has a field allowing the operator to change some access

control list (ACL)s to allow access to network device management interfaces and the

hardware lifecycle host (HLH) from a trusted datacenter network range. With the access

control list change, the operator can allow their management jumpbox VMs within a

specific network range to access the switch management interface, the HLH OS and the



Switch infrastructure network

Switch management network

Permitted networks

HLH BMC. The operator can provide one or multiple subnets to this list, if left blank it

will default to deny access. This new functionality replaces the need for postdeployment manual intervention as it used to be described on the Modify specific

settings on your Azure Stack Hub switch configuration.

Virtual network traffic routing

Learn about network planning: Border connectivity.

Next steps

Border connectivity

Article • 07/29/2022

Network integration planning is an important prerequisite for successful Azure Stack

Hub integrated systems deployment, operation, and management. Border connectivity

planning begins by choosing if you want use dynamic routing with border gateway

protocol (BGP). This requires assigning a 16-bit autonomous system number (ASN),

public or private, or using static routing.

Using a dynamic routing protocol like BGP guarantees that your system is always aware

of network changes and facilitates administration. For enhanced security, a password

may be set on the BGP peering between the TOR and the Border.

As shown in the following diagram, advertising of the private IP space on the TOR switch

is blocked using a prefix-list. The prefix list denies the advertisement of the Private

Network and it's applied as a route-map on the connection between the TOR and the

border.

The Software Load Balancer (SLB) running inside the Azure Stack Hub solution peers to

the TOR devices so it can dynamically advertise the VIP addresses.

To ensure that user traffic immediately and transparently recovers from failure, the VPC

or MLAG configured between the TOR devices allows the use of multi-chassis link

aggregation to the hosts and HSRP or VRRP that provides network redundancy for the

IP networks.

） Important

The top of rack (TOR) switches require Layer 3 uplinks with Point-to-Point IPs (/30

networks) configured on the physical interfaces. Layer 2 uplinks with TOR switches

supporting Azure Stack Hub operations isn't supported. The Border device can

support 32-bit BGP autonomous system number (ASN).

The physical connectivity between the border devices and Azure Stack Hub's top of

rack (TOR) switches require network transceivers. It is important to ensure the

required module type (SR, LR, ER, or other) is discussed with the hardware solution

provider prior to the onsite deployment.

BGP routing

Static routing requires additional configuration to the border devices. It requires more

manual intervention and management as well as thorough analysis before any change.

Issues caused by a configuration error may take more time to rollback depending on the

changes made. This routing method isn't recommended, but it's supported.

To integrate Azure Stack Hub into your networking environment using static routing, all

four physical links between the border and the TOR device must be connected. High

availability can't be guaranteed because of how static routing works.

The border device must be configured with static routes pointing to each one of the

four P2P IP's set between the TOR and the Border for traffic destined to any network

inside Azure Stack Hub, but only the External or Public VIP network is required for

operation. Static routes to the BMC and the External networks are required for initial

deployment. Operators can choose to leave static routes in the border to access

management resources that reside on the BMC and the Infrastructure network. Adding

static routes to switch infrastructure and switch management networks is optional.

The TOR devices are configured with a static default route sending all traffic to the

border devices. The one traffic exception to the default rule is for the private space,

Static routing

which is blocked using an Access Control List applied on the TOR to border connection.

Static routing applies only to the uplinks between the TOR and border switches. BGP

dynamic routing is used inside the rack because it's an essential tool for the SLB and

other components and can't be disabled or removed.

The BMC network is optional after deployment.

The Switch Infrastructure network is optional, as the whole network can be included in

the Switch Management network.

The Switch Management network is required and can be added separately from the

Switch Infrastructure network.

DNS integration

Transparent proxy for Azure Stack Hub

\*

\*\*

\*\*\*

Next steps

Change settings on your Azure Stack

Hub switch configuration

Article • 07/29/2022

You can change a few environmental settings for your Azure Stack Hub switch

configuration. You can identify which of the settings you can change in the template

created by your original equipment manufacturer (OEM). This article explains each of

those customizable settings and how the changes can affect your Azure Stack Hub.

These settings include password update, syslog server, simple network management

protocol (SNMP) monitoring, authentication, and the access control list.

During deployment of the Azure Stack Hub solution, the original equipment

manufacturer (OEM) creates and applies the switch configuration for both TORs and

BMC. The OEM uses the Azure Stack Hub automation tool to validate that the required

configurations are properly set on these devices. The configuration is based on the

information in your Azure Stack Hub deployment worksheet.

However, there are some values that can be added, removed, or changed on the

configuration of the network switches.

The operator can update the password for any user on the network switches at any time.

There's no requirement to change any information on the Azure Stack Hub system, or to

use the steps for Rotate secrets in Azure Stack Hub.

２ Warning

After the OEM creates the configuration, do not alter the configuration without

consent from either the OEM or the Microsoft Azure Stack Hub engineering team.

A change to the network device configuration can significantly impact the

operation or troubleshooting of network issues in your Azure Stack Hub instance.

For more information about these functions on your network device, how to make

these changes, contact your OEM hardware provider or Microsoft support. Your

OEM has the configuration file created by the automation tool based on your Azure

Stack Hub deployment worksheet.

Password update

Operators can redirect the switch logs to a syslog server on their datacenter. Use this

configuration to ensure the logs from a particular point in time can be used for

troubleshooting. By default, the logs are stored on the switches, but their capacity for

storing logs is limited. Check the Access control list updates section for an overview of

how to configure the permissions for switch management access.

The operator can configure SNMP v2 or v3 to monitor the network devices and send

traps to a network monitoring app on the datacenter. For security reasons, use SNMPv3

since it's more secure than v2. Consult your OEM hardware provider for the MIBs and

configuration required. Check the Access control list updates section for an overview of

how to configure the permissions for switch management access.

The operator can configure either RADIUS or TACACS to manage authentication on the

network devices. Consult your OEM hardware provider for supported methods and

configuration required. Check the Access control list updates section for an overview of

how to configure the permissions for Switch Management access.

The operator can change some access control lists (ACL)s to allow access to network

device management interfaces and the hardware lifecycle host (HLH) from a trusted

datacenter network range. With the access control list, the operator can allow their

management jumpbox VMs within a specific network range to access the switch

management interface, the HLH OS, and the HLH BMC.

Syslog server

SNMP monitoring

Authentication

Access control list updates

７ Note

Starting in 1910, the deployment worksheet will have a new field for Permitted

Networks which replaces the manual steps required to allow access to network

device management interfaces and the hardware lifecycle host (HLH) from a trusted

datacenter network range. For more information on this new feature, see Network

integration planning for Azure Stack Hub.

Azure Stack Hub datacenter integration - DNS

Next steps

Azure Stack Hub datacenter DNS

integration

Article • 08/24/2023

To be able to access Azure Stack Hub endpoints such as portal, adminportal,

management, and adminmanagement from outside Azure Stack Hub, you need to

integrate the Azure Stack Hub DNS services with the DNS servers that host the DNS

zones you want to use in Azure Stack Hub.

You're required to provide some important information related to DNS when you deploy

Azure Stack Hub.

Field Description Example

Region The geographic location of your Azure Stack Hub

deployment.

east

External

Domain

Name

The name of the zone you want to use for your Azure Stack

Hub deployment.

cloud.fabrikam.com

Internal

Domain

Name

The name of the internal zone that's used for infrastructure

services in Azure Stack Hub. It's Directory Serviceintegrated and private (not reachable from outside the

Azure Stack Hub deployment).

azurestack.local

DNS

Forwarders

DNS servers that are used to forward DNS queries, DNS

zones, and records that are hosted outside Azure Stack

Hub, either on the corporate intranet or public internet. You

can edit the DNS Forwarder value with the SetAzSDnsForwarder cmdlet after deployment.

Naming

Prefix

(Optional)

The naming prefix you want your Azure Stack Hub

infrastructure role instance machine names to have. If not

provided, the default is azs .

azs

The fully qualified domain name (FQDN) of your Azure Stack Hub deployment and

endpoints is the combination of the Region parameter and the External Domain Name

parameter. Using the values from the examples in the previous table, the FQDN for this

Azure Stack Hub deployment would be the following name:

east.cloud.fabrikam.com

Azure Stack Hub DNS namespace

As such, examples of some of the endpoints for this deployment would look like the

following URLs:

https://portal.east.cloud.fabrikam.com https://management.east.cloud.fabrikam.com

https://adminportal.east.cloud.fabrikam.com

https://adminmanagement.east.cloud.fabrikam.com

To use this example DNS namespace for an Azure Stack Hub deployment, the following

conditions are required:

The zone fabrikam.com is registered either with a domain registrar, an internal

corporate DNS server, or both, depending on your name resolution requirements.

The child domain cloud.fabrikam.com exists under the zone fabrikam.com .

The DNS servers that host the zones fabrikam.com and cloud.fabrikam.com can be

reached from the Azure Stack Hub deployment.

To be able to resolve DNS names for Azure Stack Hub endpoints and instances from

outside Azure Stack Hub, you need to integrate the DNS servers that host the external

DNS zone for Azure Stack Hub with the DNS servers that host the parent zone you want

to use.

Azure Stack Hub supports adding a DNS name label to a public IP address to allow

name resolution for public IP addresses. DNS labels are a convenient way for users to

reach apps and services hosted in Azure Stack Hub by name. The DNS name label uses a

slightly different namespace than the infrastructure endpoints. Following the previous

example namespace, the namespace for DNS name labels appears as follows:

\*.east.cloudapp.cloud.fabrikam.com

Therefore, if a tenant indicates a value Myapp in the DNS name label field of a public IP

address resource, it creates an A record for myapp in the zone

east.cloudapp.cloud.fabrikam.com on the Azure Stack Hub external DNS server. The

resulting fully qualified domain name appears as follows:

myapp.east.cloudapp.cloud.fabrikam.com

If you want to use this functionality and namespace, you must integrate the DNS servers

that host the external DNS zone for Azure Stack Hub with the DNS servers that host the

parent zone you want to use. This namespace is different than the namespace for the

DNS name labels

Azure Stack Hub service endpoints, so you must create another delegation or

conditional forwarding rule.

For more information about how the DNS Name label works, see Using DNS in Azure

Stack Hub.

There are two types of DNS servers:

An authoritative DNS server hosts DNS zones. It answers DNS queries for records

in those zones only.

A recursive DNS server doesn't host DNS zones. It answers all DNS queries by

calling authoritative DNS servers to gather the data it needs.

Azure Stack Hub includes both authoritative and recursive DNS servers. The recursive

servers are used to resolve names of everything except for the internal private zone and

the external public DNS zone for that Azure Stack Hub deployment.

Resolution and delegation

east.cloudapp.cloud.fabrikam.com

east.cloud.fabrikam.com

east.cloudapp.cloud.fabrikam.com

To resolve DNS names for endpoints outside Azure Stack Hub (for example:

www.bing.com ), you must provide DNS servers that Azure Stack Hub can use to

forward DNS requests for which Azure Stack Hub isn't authoritative. For deployment,

DNS servers to which Azure Stack Hub forwards requests are required in the

Resolving external DNS names from Azure

Stack Hub

deployment worksheet (in the DNS Forwarder field). Provide at least two servers in this

field for fault tolerance. Without these values, Azure Stack Hub deployment fails. You

can edit the DNS Forwarder values with the Set-AzSDnsForwarder cmdlet after

deployment.

If the external DNS forwarder servers are unable to resolve a DNS request forwarded

from Azure Stack Hub, by default the internal DNS recursive resolver service attempts to

contact the DNS root hints servers . This fallback behavior is consistent with DNS

server name resolution standards. The internet root hints servers are used to help

resolve DNS address information when the DNS forwarder servers are unable to resolve

the query locally from a hosted zone or the DNS server cache.

To manage the DNS root hints setting for the internal DNS name resolution service

within Azure Stack Hub, use the Get-AzSDnsServerSettings cmdlet to view the current

configuration; the default setting is enabled. The Set-AzSDnsServerSettings cmdlet

enables or disables the -UseRootHint configuration of the internal DNS servers.

To enable name resolution with your existing DNS infrastructure, configure conditional

forwarding.

To add a conditional forwarder, you must use the privileged endpoint.

For this procedure, use a computer in your datacenter network that can communicate

with the privileged endpoint in Azure Stack Hub.

1. Open an elevated Windows PowerShell session (run as administrator), and connect

to the IP address of the privileged endpoint. Use the credentials for CloudAdmin

７ Note

For scenarios in which Azure Stack Hub is unable to contact the internet DNS root

hints servers, such as UDP port 53 (DNS), in which network access is permanently

blocked or fully disconnected/air-gapped, it is recommended that you disable the

-UseRootHint setting to prevent extended timeouts in DNS name resolution. Use

the Set-AzSDnsServerSettings cmdlet to control this setting.

Configure conditional DNS forwarding

） Important

This only applies to an AD FS deployment.

authentication.

PowerShell

2. After you connect to the privileged endpoint, run the following PowerShell

command. Substitute the sample values provided with your domain name and IP

addresses of the DNS servers you want to use.

PowerShell

The authoritative servers are the ones that hold the external DNS zone information, and

any user-created zones. Integrate with these servers to enable zone delegation or

conditional forwarding to resolve Azure Stack Hub DNS names from outside Azure Stack

Hub.

To integrate your Azure Stack Hub deployment with your DNS infrastructure, you need

the following information:

DNS server FQDNs

DNS server IP addresses

The FQDNs for the Azure Stack Hub DNS servers have the following format:

<NAMINGPREFIX>-ns01.<REGION>.<EXTERNALDOMAINNAME>

<NAMINGPREFIX>-ns02.<REGION>.<EXTERNALDOMAINNAME>

If you use the sample values, the FQDNs for the DNS servers are:

azs-ns01.east.cloud.fabrikam.com

$cred=Get-Credential

Enter-PSSession -ComputerName <IP Address of ERCS> -ConfigurationName

PrivilegedEndpoint -Credential $cred

Register-CustomDnsServer -CustomDomainName "contoso.com" -

CustomDnsIPAddresses "192.168.1.1","192.168.1.2"

Resolving Azure Stack Hub DNS names from

outside Azure Stack Hub

Get DNS Server external endpoint information

azs-ns02.east.cloud.fabrikam.com

This information is also created at the end of all Azure Stack Hub deployments in a file

named AzureStackStampInformation.json . This file is located in the

C:\CloudDeployment\logs folder of the Deployment virtual machine. If you're not sure

what values were used for your Azure Stack Hub deployment, you can get the values

from here.

If the Deployment virtual machine is no longer available or is inaccessible, you can

obtain the values by connecting to the privileged endpoint and running the GetAzureStackStampInformation PowerShell cmdlet. For more information, see privileged

endpoint.

The simplest and most secure way to integrate Azure Stack Hub with your DNS

infrastructure is to do conditional forwarding of the zone from the server that hosts the

parent zone. This approach is recommended if you have direct control over the DNS

servers that host the parent zone for your Azure Stack Hub external DNS namespace.

If you're not familiar with how to do conditional forwarding with DNS, see the following

TechNet article: Assign a Conditional Forwarder for a Domain Name, or the

documentation specific to your DNS solution.

In scenarios where you specified your external Azure Stack Hub DNS Zone to look like a

child domain of your corporate domain name, conditional forwarding can't be used.

DNS delegation must be configured.

Example:

Corporate DNS Domain Name: contoso.com

Azure Stack Hub External DNS Domain Name: azurestack.contoso.com

DNS forwarder IPs are set during deployment of Azure Stack Hub. However, if the

forwarder IPs need to be updated for any reason, you can edit the values by connecting

to the privileged endpoint and running the Get-AzSDnsForwarder and SetAzSDnsForwarder [[-IPAddress] <IPAddress[]>] PowerShell cmdlets. For more

information, see privileged endpoint.

Setting up conditional forwarding to Azure

Stack Hub

Editing DNS Forwarder IPs

For DNS names to be resolvable from outside an Azure Stack Hub deployment, you

need to set up DNS delegation.

Each registrar has their own DNS management tools to change the name server records

for a domain. In the registrar's DNS management page, edit the NS records and replace

the NS records for the zone with the ones in Azure Stack Hub.

Most DNS registrars require you to provide a minimum of two DNS servers to complete

the delegation.

Firewall integration

Delegating the external DNS zone to Azure

Stack Hub

Next steps

Update the DNS forwarder in Azure

Stack Hub

Article • 07/29/2022

At least one reachable DNS forwarder is necessary for the Azure Stack Hub infrastructure

to resolve external names. A DNS forwarder must be provided for the deployment of

Azure Stack Hub. That input is used for the Azure Stack Hub internal DNS servers as a

forwarder and it enables external name resolution for services like authentication,

marketplace management, or usage.

DNS is a critical datacenter infrastructure service that can change. If it does, Azure Stack

Hub must be updated.

This article describes using the privileged endpoint (PEP) to update the DNS forwarder

in Azure Stack Hub. It's recommended that you use two reliable DNS forwarder IP

addresses.

1. Connect to the privileged endpoint. It's not necessary to unlock the privileged

endpoint by opening a support ticket.

2. Run the following command to review the current configured DNS forwarder. As

an alternative, you can also use the administrator portal region properties:

PowerShell

3. Run the following command to update Azure Stack Hub to use the new DNS

forwarder:

PowerShell

4. Review the output of the command for any errors.

Steps to update the DNS forwarder

Get-AzsDnsForwarder

Set-AzsDnsForwarder -IPAddress "IPAddress 1","IPAddress 2"

Next steps

Firewall integration

Configure the time server for Azure

Stack Hub

Article • 07/29/2022

You can use the privileged endpoint (PEP) to update the time server in Azure Stack Hub.

Use a host name that resolves to two or more NTP (Network Time Protocol) server IP

addresses.

Azure Stack Hub uses NTP to connect to time servers on the internet. NTP servers

provide accurate system time. Time is used across Azure Stack Hub's physical network

switches, hardware lifecycle host, infrastructure service, and virtual machines. If the clock

isn't synchronized, Azure Stack Hub may experience severe issues with the network and

authentication. Log files, documents, and other files may be created with incorrect

timestamps.

Providing one time server (NTP) is required for Azure Stack Hub to synchronize time.

When you deploy Azure Stack Hub, you provide the address of an NTP server. Time is a

critical datacenter infrastructure service. If the service changes, you need to update the

time.

1. Connect to the PEP.

2. Run the following command to review the current configured NTP server:

PowerShell

７ Note

Azure Stack Hub supports synchronizing time with only one time server (NTP). You

can't provide multiple NTPs for Azure Stack Hub to synchronize time with.

Configure time

７ Note

It isn't necessary to unlock the privileged endpoint by opening a support

ticket.

Get-AzsTimeSource

3. Run the following command to update Azure Stack Hub to use the new NTP server

and to immediately synchronize the time.

PowerShell

For servers other than Windows-based time servers:

PowerShell

4. Review the output of the command for any errors.

View the readiness report

General Azure Stack Hub integration considerations

７ Note

This procedure doesn't update the time server on the physical switches. If

your time server isn't a Windows-based NTP server, you need to add the flag

0x8 .

Set-AzsTimeSource -TimeServer NEWTIMESERVERIP -resync

Set-AzsTimeSource -TimeServer "NEWTIMESERVERIP,0x8" -resync

Next steps

Azure Stack Hub firewall integration

Article • 07/29/2022

It's recommended that you use a firewall device to help secure Azure Stack Hub.

Firewalls can help defend against things like distributed denial-of-service (DDOS)

attacks, intrusion detection, and content inspection. However, they can also become a

throughput bottleneck for Azure storage services like blobs, tables, and queues.

If a disconnected deployment mode is used, you must publish the AD FS endpoint. For

more information, see the datacenter integration identity article.

The Azure Resource Manager (administrator), administrator portal, and Key Vault

(administrator) endpoints don't necessarily require external publishing. For example, as a

service provider, you could limit the attack surface by only administering Azure Stack

Hub from inside your network, and not from the internet.

For enterprise organizations, the external network can be the existing corporate

network. In this scenario, you must publish endpoints to operate Azure Stack Hub from

the corporate network.

Network Address Translation (NAT) is the recommended method to allow the

deployment virtual machine (DVM) to access external resources and the internet during

deployment as well as the Emergency Recovery Console (ERCS) VMs or privileged

endpoint (PEP) during registration and troubleshooting.

NAT can also be an alternative to Public IP addresses on the external network or public

VIPs. However, it's not recommended to do so because it limits the tenant user

experience and increases complexity. One option would be a one to one NAT that still

requires one public IP per user IP on the pool. Another option is a many to one NAT that

requires a NAT rule per user VIP for all ports a user might use.

Some of the downsides of using NAT for Public VIP are:

NAT adds overhead when managing firewall rules because users control their own

endpoints and their own publishing rules in the software-defined networking

(SDN) stack. Users must contact the Azure Stack Hub operator to get their VIPs

published, and to update the port list.

While NAT usage limits the user experience, it gives full control to the operator

over publishing requests.

Network Address Translation

For hybrid cloud scenarios with Azure, consider that Azure doesn't support setting

up a VPN tunnel to an endpoint using NAT.

It's currently recommended to disable any SSL interception (for example decryption

offloading) on all Azure Stack Hub traffic. If it's supported in future updates, guidance

will be provided about how to enable SSL interception for Azure Stack Hub.

In an edge deployment, Azure Stack Hub is deployed directly behind the edge router or

the firewall. In these scenarios, it's supported for the firewall to be above the border

(Scenario 1) where it supports both active-active and active-passive firewall

configurations or acting as the border device (Scenario 2) where it only supports activeactive firewall configuration relying on equal-cost multi-path (ECMP) with either BGP or

static routing for failover.

Public routable IP addresses are specified for the public VIP pool from the external

network at deployment time. In an edge scenario, it's not recommended to use public

routable IPs on any other network for security purposes. This scenario enables a user to

experience the full self-controlled cloud experience as in a public cloud like Azure.

SSL interception

Edge firewall scenario

In an enterprise intranet or perimeter deployment, Azure Stack Hub is deployed on a

multi-zoned firewall or in between the edge firewall and the internal, corporate network

firewall. Its traffic is then distributed between the secure, perimeter network (or DMZ),

and unsecure zones as described below:

Secure zone: This is the internal network that uses internal or corporate routable IP

addresses. The secure network can be divided, have internet outbound access

through NAT on the Firewall, and is usually accessible from anywhere inside your

datacenter via the internal network. All Azure Stack Hub networks should reside in

the secure zone except for the external network's public VIP pool.

Perimeter zone. The perimeter network is where external or internet-facing apps

like Web servers are typically deployed. It's usually monitored by a firewall to avoid

attacks like DDoS and intrusion (hacking) while still allowing specified inbound

traffic from the internet. Only the external network public VIP pool of Azure Stack

Hub should reside in the DMZ zone.

Unsecure zone. This is the external network, the internet. It is not recommended to

deploy Azure Stack Hub in the unsecure zone.

Enterprise intranet or perimeter network

firewall scenario

Learn more about ports and protocols used by Azure Stack Hub endpoints.

Azure Stack Hub PKI requirements

Learn more

Next steps

Transparent proxy for Azure Stack Hub

Article • 07/29/2022

A transparent proxy (also known as an intercepting, inline, or forced proxy) intercepts

normal communication at the network layer without requiring special client

configuration. Clients don't need to be aware of the existence of the proxy.

If your datacenter requires all traffic to use a proxy, you configure a transparent proxy to

process all traffic according to policy by separating traffic between the zones on your

network.

Outbound traffic from Azure Stack Hub is categorized as either tenant traffic or

infrastructure traffic.

Tenant traffic is generated by tenants by way of virtual machines, load balancers, VPN

gateways, app services, etc.

Infrastructure traffic is generated from the first /27 range of the public virtual IP pool

assigned to infrastructure services such as identity, patch and update, usage metrics,

Marketplace syndication, registration, log collection, Windows Defender, etc. The traffic

from these services is routed to Azure endpoints. Azure does not accept traffic modified

by a proxy or TLS/SSL intercepted traffic. This reason is why Azure Stack Hub does not

support a native proxy configuration.

When configuring a transparent proxy, you can choose to send all outbound traffic or

only infrastructure traffic through the proxy.

Microsoft has partnered with leading proxy vendors in the industry to validate Azure

Stack Hub’s use case scenarios with a transparent proxy configuration. The following

diagram is an example Azure Stack Hub network configuration with HA Proxies. External

proxy devices must be placed north of the border devices.

Traffic types

Partner integration

Additionally, the border devices must be configured to route traffic from Azure Stack

Hub in one of the following ways:

Route all outbound traffic from Azure Stack Hub to the proxy devices

Route all outbound traffic from the first /27 range of the Azure Stack Hub virtual

IP pool to the proxy devices via policy-based routing.

For a sample border configuration, see Example border configuration section in this

article.

Review the following documents for validated transparent proxy configurations with

Azure Stack Hub:

Configure a Check Point Security Gateway transparent proxy

Configure a Sophos XG firewall transparent proxy

Integrate Citrix ADC, Citrix Secure Web Gateway with Azure Stack Hub

Integrate Cisco Secure Web Appliance (WSA) with Azure Stack Hub

In scenarios where outbound traffic from Azure Stack Hub is required to flow through an

explicit proxy, Sophos and Checkpoint devices provide a dual-mode feature that allows

specific ranges of traffic through transparent mode, while other ranges can be

configured to pass through an explicit mode. Using this feature, these proxy devices can

be configured such that only infrastructure traffic is sent through the transparent proxy,

while all tenant traffic is sent through the explicit mode.

The solution is based on policy-based routing (PBR) which uses an administrator defined

set of criteria implemented by an access control list (ACL). The ACL categorizes the

traffic that is directed to the next-hop IP of the proxy devices implemented in a routemap, rather than normal routing that is based only on destination IP address. Specific

infrastructure network traffic for ports 80 and 443 are routed from the border devices to

the transparent proxy deployment. The transparent proxy does URL filtering, and none

allowed traffic is dropped.

The following configuration sample is for a Cisco Nexus 9508 Chassis.

In this scenario, the source infrastructure networks that require access to the internet are

as follows:

Public VIP - First /27

Infrastructure network - Last /27

BMC Network - Last /27

The following subnets receive policy-based routing (PBR) treatment in this scenario:

Network IP Range Subnet receiving PBR treatment

Public Virtual IP pool First /27 of

172.21.107.0/27

172.21.107.0/27 = 172.21.107.1 to

172.21.107.30

Infrastructure

network

Last /27 of 172.21.7.0/24 172.21.7.224/27 = 172.21.7.225 to

172.21.7.254

BMC network Last /27 of

10.60.32.128/26

10.60.32.160/27 = 10.60.32.161 to

10.60.32.190

） Important

SSL traffic interception is not supported and can lead to service failures when

accessing endpoints. The maximum supported timeout to communicate with

endpoints required for identity is 60s with 3 retry attempts. For more information,

see Azure Stack Hub firewall integration.

Example border configuration

Enable PBR by entering the feature pbr command.

Configure border device

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

PBR Configuration for Cisco Nexus 9508 Chassis

PBR Enivronment configured to use VRF08

The test rack has is a 4-node Azure Stack stamp with 2x TOR switches and 1x

BMC switch. Each TOR switch

has a single uplink to the Nexus 9508 chassis using BGP for routing. In this

example the test rack

is in it's own VRF (VRF08)

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

!

feature pbr

!

<Create VLANs that the proxy devices will use for inside and outside

connectivity>

!

VLAN 801

name PBR\_Proxy\_VRF08\_Inside

VLAN 802

name PBR\_Proxy\_VRF08\_Outside

!

interface vlan 801

description PBR\_Proxy\_VRF08\_Inside

no shutdown

mtu 9216

vrf member VRF08

no ip redirects

ip address 10.60.3.1/29

!

interface vlan 802

description PBR\_Proxy\_VRF08\_Outside

no shutdown

mtu 9216

vrf member VRF08

no ip redirects

ip address 10.60.3.33/28

!

!

ip access-list PERMITTED\_TO\_PROXY\_ENV1

100 permit tcp 172.21.107.0/27 any eq www

110 permit tcp 172.21.107.0/27 any eq 443

120 permit tcp 172.21.7.224/27 any eq www

130 permit tcp 172.21.7.224/27 any eq 443

140 permit tcp 10.60.32.160/27 any eq www

150 permit tcp 10.60.32.160/27 any eq 443

!

!

route-map TRAFFIC\_TO\_PROXY\_ENV1 pbr-statistics

route-map TRAFFIC\_TO\_PROXY\_ENV1 permit 10

match ip address PERMITTED\_TO\_PROXY\_ENV1

set ip next-hop 10.60.3.34 10.60.3.35

!

!

interface Ethernet1/1

description DownLink to TOR-1:TeGig1/0/47

mtu 9100

logging event port link-status

vrf member VRF08

ip address 192.168.32.193/30

ip policy route-map TRAFFIC\_TO\_PROXY\_ENV1

no shutdown

!

interface Ethernet2/1

description DownLink to TOR-2:TeGig1/0/48

mtu 9100

logging event port link-status

vrf member VRF08

ip address 192.168.32.205/30

ip policy route-map TRAFFIC\_TO\_PROXY\_ENV1

no shutdown

!

<Interface configuration for inside/outside connections to proxy devices. In

this example there are 2 firewalls>

!

interface Ethernet1/41

description management interface for Firewall-1

switchport

switchport access vlan 801

no shutdown

!

interface Ethernet1/42

description Proxy interface for Firewall-1

switchport

switchport access vlan 802

no shutdown

!

interface Ethernet2/41

description management interface for Firewall-2

switchport

switchport access vlan 801

no shutdown

!

interface Ethernet2/42

description Proxy interface for Firewall-2

switchport

switchport access vlan 802

no shutdown

!

Create the new ACL that will be used to identify traffic that will get PBR treatment. That

traffic is web traffic (HTTP port 80 and HTTPS port 443) from the hosts/subnets in the

test rack that gets proxy service as detailed in this example. For example, the ACL name

is PERMITTED\_TO\_PROXY\_ENV1.

The core of the PBR functionality is implemented by the TRAFFIC\_TO\_PROXY\_ENV1

route-map. The pbr-statistics option is added to enable viewing the policy match

statistics to verify the number packets that do and do not get PBR forwarding. Routemap sequence 10 permits PBR treatment to traffic meeting ACL

PERMITTED\_TO\_PROXY\_ENV1 criteria. That traffic is forwarded to the next-hop IP

<BGP network statements for VLAN 801-802 subnets and neighbor statements for

R023171A-TOR-1/R023171A-TOR-2>

!

router bgp 65000

!

vrf VRF08

address-family ipv4 unicast

network 10.60.3.0/29

network 10.60.3.32/28

!

neighbor 192.168.32.194

remote-as 65001

description LinkTo 65001:R023171A-TOR-1:TeGig1/0/47

address-family ipv4 unicast

maximum-prefix 12000 warning-only

neighbor 192.168.32.206

remote-as 65001

description LinkTo 65001:R023171A-TOR-2:TeGig1/0/48

address-family ipv4 unicast

maximum-prefix 12000 warning-only

!

!

ip access-list PERMITTED\_TO\_PROXY\_ENV1

100 permit tcp 172.21.107.0/27 any eq www <<HTTP traffic from CL04 Public

Admin VIPs leaving test rack>>

110 permit tcp 172.21.107.0/27 any eq 443 <<HTTPS traffic from CL04 Public

Admin VIPs leaving test rack>>

120 permit tcp 172.21.7.224/27 any eq www <<HTTP traffic from CL04 INF-pubadm leaving test rack>>

130 permit tcp 172.21.7.224/27 any eq 443 <<HTTPS traffic from CL04 INF-pubadm leaving test rack>>

140 permit tcp 10.60.32.160/27 any eq www <<HTTP traffic from DVM and HLH

leaving test rack>>

150 permit tcp 10.60.32.160/27 any eq 443 <<HTTPS traffic from DVM and HLH

leaving test rack>>

addresses of 10.60.3.34 and 10.60.3.35 , which are the VIPs for the primary/secondary

proxy devices in our example configuration

ACLs are used as the match criteria for the TRAFFIC\_TO\_PROXY\_ENV1 route-map. When

traffic matches the PERMITTED\_TO\_PROXY\_ENV1 ACL, PBR overrides the normal routing

table, and instead forwards the traffic to the listed IP next-hops.

The TRAFFIC\_TO\_PROXY\_ENV1 PBR policy is applied to traffic that enters the border

device from CL04 hosts and public VIPs and from the HLH and DVM in the test rack.

Learn more about firewall integration, see Azure Stack Hub firewall integration.

!

route-map TRAFFIC\_TO\_PROXY\_ENV1 pbr-statistics

route-map TRAFFIC\_TO\_PROXY\_ENV1 permit 10

match ip address PERMITTED\_TO\_PROXY\_ENV1

set ip next-hop 10.60.3.34 10.60.3.35

Next steps

Publish Azure Stack Hub services in your

datacenter

Article • 07/29/2022

Azure Stack Hub sets up virtual IP addresses (VIPs) for its infrastructure roles. These VIPs are allocated from the

public IP address pool. Each VIP is secured with an access control list (ACL) in the software-defined network

layer. ACLs are also used across the physical switches (TORs and BMC) to further harden the solution. A DNS

entry is created for each endpoint in the external DNS zone that's specified at deployment time. For example,

the user portal is assigned the DNS host entry of portal.<region>.<fqdn>.

The following architectural diagram shows the different network layers and ACLs:

To make Azure Stack Hub services (like the portals, Azure Resource Manager, DNS, and so on) available to

external networks, you must allow inbound traffic to these endpoints for specific URLs, ports, and protocols.

In a deployment where a transparent proxy uplinks to a traditional proxy server or a firewall is protecting the

solution, you must allow specific ports and URLs for both inbound and outbound communication. These include

ports and URLs for identity, the marketplace, patch and update, registration, and usage data.

SSL traffic interception is not supported and can lead to service failures when accessing endpoints.

A set of infrastructure VIPs is required for publishing Azure Stack Hub endpoints to external networks. The

Endpoint (VIP) table shows each endpoint, the required port, and protocol. Refer to the specific resource

provider deployment documentation for endpoints that require additional resource providers, like the SQL

resource provider.

Ports and URLs

Ports and protocols (inbound)

Internal infrastructure VIPs aren't listed because they're not required for publishing Azure Stack Hub. User VIPs

are dynamic and defined by the users themselves, with no control by the Azure Stack Hub operator.

With the addition of the Extension Host, ports in the range of 12495-30015 aren't required.

Endpoint (VIP) DNS host A record Protocol Ports

AD FS Adfs.<region>.<fqdn> HTTPS 443

Portal (administrator) Adminportal.<region>.<fqdn> HTTPS 443

Adminhosting \*.adminhosting.<region>.<fqdn> HTTPS 443

Azure Resource Manager

(administrator)

Adminmanagement.<region>.

<fqdn>

HTTPS 443

Portal (user) Portal.<region>.<fqdn> HTTPS 443

Azure Resource Manager

(user)

Management.<region>.<fqdn> HTTPS 443

Graph Graph.<region>.<fqdn> HTTPS 443

Certificate revocation list Crl.<region>.<fqdn> HTTP 80

DNS \*.<region>.<fqdn> TCP & UDP 53

Hosting \*.hosting.<region>.<fqdn> HTTPS 443

Key Vault (user) \*.vault.<region>.<fqdn> HTTPS 443

Key Vault (administrator) \*.adminvault.<region>.<fqdn> HTTPS 443

Storage Queue \*.queue.<region>.<fqdn> HTTP

HTTPS

80

443

Storage Table \*.table.<region>.<fqdn> HTTP

HTTPS

80

443

Storage Blob \*.blob.<region>.<fqdn> HTTP

HTTPS

80

443

SQL Resource Provider sqladapter.dbadapter.<region>.

<fqdn>

HTTPS 44300-44304

MySQL Resource Provider mysqladapter.dbadapter.<region>.

<fqdn>

HTTPS 44300-44304

App Service \*.appservice.<region>.<fqdn> TCP 80 (HTTP)

443 (HTTPS)

8172 (MSDeploy)

\*.scm.appservice.<region>.<fqdn> TCP 443 (HTTPS)

api.appservice.<region>.<fqdn> TCP 443 (HTTPS)

44300 (Azure Resource Manager)

ftp.appservice.<region>.<fqdn> TCP, UDP 21, 1021, 10001-10100 (FTP)

990 (FTPS)

VPN Gateways IP Protocol

50 & UDP

Encapsulation Security Payload (ESP)

IPSec & UDP 500 and 4500

Azure Stack Hub supports only transparent proxy servers. In a deployment with a transparent proxy uplink to a

traditional proxy server, you must allow the ports and URLs in the following table for outbound communication.

For more information on configuring transparent proxy servers, see Transparent proxy for Azure Stack Hub.

SSL traffic interception is not supported and can lead to service failures when accessing endpoints. The

maximum supported timeout to communicate with endpoints required for identity is 60s.

Purpose Destination URL Protocol

/ Ports

Source

Network

Requirement

Identity

Allows Azure

Stack Hub to

connect to

Azure Active

Directory for

User & Service

authentication.

Azure

login.windows.net

login.microsoftonline.com

graph.windows.net

https://secure.aadcdn.microsoftonline-p.com

www.office.com

ManagementServiceUri = https://management.core.windows.net

ARMUri = https://management.azure.com

https://\*.msftauth.net

https://\*.msauth.net

https://\*.msocdn.com

Azure Government

https://login.microsoftonline.us/

https://graph.windows.net/

Azure China 21Vianet

https://login.chinacloudapi.cn/

https://graph.chinacloudapi.cn/

Azure Germany

https://login.microsoftonline.de/

https://graph.cloudapi.de/

HTTP 80,

HTTPS

443

Public VIP -

/27

Public

infrastructure

Network

Mandatory for

a connected

deployment.

Marketplace

syndication

Allows you to

download items

to Azure Stack

Hub from the

Marketplace

and make them

available to all

users using the

Azure Stack

Hub

environment.

Azure

https://management.azure.com

https://\*.blob.core.windows.net

https://\*.azureedge.net

Azure Government

https://management.usgovcloudapi.net/

https://\*.blob.core.usgovcloudapi.net/

Azure China 21Vianet

https://management.chinacloudapi.cn/

http://\*.blob.core.chinacloudapi.cn

HTTPS

443

Public VIP -

/27

Not required.

Use the

disconnected

scenario

instructions to

upload images

to Azure Stack

Hub.

Ports and URLs (outbound)

７ Note

Azure Stack Hub doesn't support using ExpressRoute to reach the Azure services listed in the following

table because ExpressRoute may not be able to route traffic to all of the endpoints.

Purpose Destination URL Protocol

/ Ports

Source

Network

Requirement

Patch & Update

When

connected to

update

endpoints,

Azure Stack

Hub software

updates and

hotfixes are

displayed as

available for

download.

https://\*.azureedge.net

https://aka.ms/azurestackautomaticupdate

HTTPS

443

Public VIP -

/27

Not required.

Use the

disconnected

deployment

connection

instructions to

manually

download and

prepare the

update.

Registration

Allows you to

register Azure

Stack Hub with

Azure to

download

Azure

Marketplace

items and set

up commerce

data reporting

back to

Microsoft.

Azure

https://management.azure.com

Azure Government

https://management.usgovcloudapi.net/

Azure China 21Vianet

https://management.chinacloudapi.cn

HTTPS

443

Public VIP -

/27

Not required.

You can use

the

disconnected

scenario for

offline

registration.

Usage

Allows Azure

Stack Hub

operators to

configure their

Azure Stack

Hub instance to

report usage

data to Azure.

Azure

https://\*.trafficmanager.net

https://\*.cloudapp.azure.com

Azure Government

https://\*.usgovtrafficmanager.net

https://\*.cloudapp.usgovcloudapi.net

Azure China 21Vianet

https://\*.trafficmanager.cn

https://\*.cloudapp.chinacloudapi.cn

HTTPS

443

Public VIP -

/27

Required for

Azure Stack

Hub

consumption

based

licensing

model.

Windows

Defender

Allows the

update

resource

provider to

download

antimalware

definitions and

engine updates

multiple times

per day.

\*.wdcp.microsoft.com

\*.wdcpalt.microsoft.com

\*.wd.microsoft.com

\*.update.microsoft.com

\*.download.microsoft.com

https://secure.aadcdn.microsoftonline-p.com

HTTPS

80, 443

Public VIP -

/27

Public

infrastructure

Network

Not required.

You can use

the

disconnected

scenario to

update

antivirus

signature files.

NTP

Allows Azure

Stack Hub to

connect to time

servers.

(IP of NTP server provided for deployment) UDP 123 Public VIP -

/27

Required

Purpose Destination URL Protocol

/ Ports

Source

Network

Requirement

DNS

Allows Azure

Stack Hub to

connect to the

DNS server

forwarder.

(IP of DNS server provided for deployment) TCP &

UDP 53

Public VIP -

/27

Required

SYSLOG

Allows Azure

Stack Hub to

send syslog

message for

monitoring or

security

purposes.

(IP of SYSLOG server provided for deployment) TCP

6514,

UDP 514

Public VIP -

/27

Optional

CRL

Allows Azure

Stack Hub to

validate

certificates and

check for

revoked

certificates.

URL under CRL Distribution Points on your certificates HTTP 80 Public VIP -

/27

Required

CRL

Allows Azure

Stack Hub to

validate

certificates and

check for

revoked

certificates.

http://crl.microsoft.com/pki/crl/products

http://mscrl.microsoft.com/pki/mscorp

http://www.microsoft.com/pki/certs

http://www.microsoft.com/pki/mscorp

http://www.microsoft.com/pkiops/crl

http://www.microsoft.com/pkiops/certs

HTTP 80 Public VIP -

/27

Not required.

Highly

recommended

security best

practice.

LDAP

Allows Azure

Stack Hub to

communicate

with Microsoft

Active Directory

on-premises.

Active Directory Forest provided for Graph integration TCP &

UDP 389

Public VIP -

/27

Required

when Azure

Stack Hub is

deployed

using AD FS.

LDAP SSL

Allows Azure

Stack Hub to

communicate

encrypted with

Microsoft

Active Directory

on-premises.

Active Directory Forest provided for Graph integration TCP 636 Public VIP -

/27

Required

when Azure

Stack Hub is

deployed

using AD FS.

LDAP GC

Allows Azure

Stack Hub to

communicate

with Microsoft

Active Global

Catalog Servers.

Active Directory Forest provided for Graph integration TCP

3268

Public VIP -

/27

Required

when Azure

Stack Hub is

deployed

using AD FS.

Purpose Destination URL Protocol

/ Ports

Source

Network

Requirement

LDAP GC SSL

Allows Azure

Stack Hub to

communicate

encrypted with

Microsoft

Active Directory

Global Catalog

Servers.

Active Directory Forest provided for Graph integration TCP

3269

Public VIP -

/27

Required

when Azure

Stack Hub is

deployed

using AD FS.

AD FS

Allows Azure

Stack Hub to

communicate

with onpremise AD FS.

AD FS metadata endpoint provided for AD FS integration TCP 443 Public VIP -

/27

Optional. The

AD FS claims

provider trust

can be created

using a

metadata file.

Diagnostic log

collection

Allows Azure

Stack Hub to

send logs either

proactively or

manually by an

operator to

Microsoft

support.

https://\*.blob.core.windows.net

https://azsdiagprdlocalwestus02.blob.core.windows.net

https://azsdiagprdwestusfrontend.westus.cloudapp.azure.com

https://azsdiagprdwestusfrontend.westus.cloudapp.azure.com

HTTPS

443

Public VIP -

/27

Not required.

You can save

logs locally.

Remote

support

Allows

Microsoft

support

professionals to

solve support

case faster by

permitting

access to the

device remotely

to performing

limited

troubleshooting

and repair

operations.

https://edgesupprd.trafficmanager.net

https://edgesupprdwestusfrontend.westus2.cloudapp.azure.com

https://edgesupprdwesteufrontend.westeurope.cloudapp.azure.com

https://edgesupprdeastusfrontend.eastus.cloudapp.azure.com

https://edgesupprdwestcufrontend.westcentralus.cloudapp.azure.com

https://edgesupprdasiasefrontend.southeastasia.cloudapp.azure.com

\*.servicebus.windows.net

HTTPS

443

Public VIP -

/27

Not required.

Telemetry

Allows Azure

Stack Hub to

send telemetry

data to

Microsoft.

https://settings-win.data.microsoft.com

https://login.live.com

\*.events.data.microsoft.com

Beginning with version 2108, the following endpoints are also

required:

https://\*.blob.core.windows.net/

https://azsdiagprdwestusfrontend.westus.cloudapp.azure.com/

HTTPS

443

Public VIP -

/27

Required

when Azure

Stack Hub

telemetry is

enabled.

Outbound URLs are load balanced using Azure traffic manager to provide the best possible connectivity based

on geographic location. With load balanced URLs, Microsoft can update and change backend endpoints without

affecting customers. Microsoft doesn't share the list of IP addresses for the load balanced URLs. Use a device

that supports filtering by URL rather than by IP.

Outbound DNS is required at all times; what varies is the source querying the external DNS and what type of

identity integration was chosen. During deployment for a connected scenario, the DVM that sits on the BMC

network needs outbound access. But after deployment, the DNS service moves to an internal component that

will send queries through a Public VIP. At that time, the outbound DNS access through the BMC network can be

removed, but the Public VIP access to that DNS server must remain or else authentication will fail.

Azure Stack Hub PKI requirements

Next steps

Prepare for extension host in Azure

Stack Hub

Article • 07/29/2022

The extension host secures Azure Stack Hub by reducing the number of required TCP/IP

ports. This article looks at preparing Azure Stack Hub for the extension host that is

automatically enabled through an Azure Stack Hub update package after the 1808

update. This article applies to Azure Stack Hub updates 1808, 1809, and 1811.

The extension host implements two new domain namespaces to guarantee unique host

entries for each portal extension. The new domain namespaces require two additional

wildcard certificates to ensure secure communication.

The table shows the new namespaces and the associated certificates:

Deployment

Folder

Required certificate subject and subject

alternative names (SAN)

Scope (per

region)

Subdomain

namespace

Admin

extension

host

\*.adminhosting.<region>.<fqdn> (Wildcard

SSL Certificates)

Admin

extension

host

adminhosting.

<region>.<fqdn>

Public

extension

host

\*.hosting.<region>.<fqdn> (Wildcard SSL

Certificates)

Public

extension

host

hosting.<region>.

<fqdn>

For detailed certificate requirements, see Azure Stack Hub public key infrastructure

certificate requirements.

The Azure Stack Hub Readiness Checker tool lets you create a certificate signing request

for the two new and required SSL certificates. Follow the steps in the article Azure Stack

Hub certificates signing request generation.

Certificate requirements

Create certificate signing request

７ Note

You may skip this step depending on how you requested your SSL certificates.

1. Open PowerShell with elevated permission on the hardware lifecycle host or the

Azure Stack Hub management workstation.

2. Run the following cmdlet to install the Azure Stack Hub Readiness Checker tool:

PowerShell

3. Run the following script to create the required folder structure:

PowerShell

4. Place the existing certificates, which you're currently using in Azure Stack Hub, in

appropriate directories. For example, put the Admin ARM certificate in the Arm

Admin folder. And then put the newly created hosting certificates in the Admin

extension host and Public extension host directories.

5. Run the following cmdlet to start the certificate check:

PowerShell

Validate new certificates

Install-Module -Name Microsoft.AzureStack.ReadinessChecker

New-Item C:\Certificates -ItemType Directory

$directories = 'ACSBlob','ACSQueue','ACSTable','Admin Portal','ARM

Admin','ARM Public','KeyVault','KeyVaultInternal','Public Portal',

'Admin extension host', 'Public extension host'

$destination = 'c:\certificates'

$directories | % { New-Item -Path (Join-Path $destination $PSITEM) -

ItemType Directory -Force}

７ Note

If you deploy with Azure Active Directory Federated Services (AD FS) the

following directories must be added to $directories in the script: ADFS , Graph .

$pfxPassword = Read-Host -Prompt "Enter PFX Password" -AsSecureString

Start-AzsReadinessChecker -CertificatePath c:\certificates -pfxPassword

$pfxPassword -RegionName east -FQDN azurestack.contoso.com -

IdentitySystem AAD

6. Check the output and if all certificates pass all tests.

Use a computer that can connect to the Azure Stack Hub privileged endpoint for the

next steps. Make sure you have access to the new certificate files from that computer.

1. Use a computer that can connect to the Azure Stack Hub privileged endpoint for

the next steps. Make sure you access to the new certificate files from that

computer.

2. Open PowerShell ISE to execute the next script blocks.

3. Import the certificate for the admin hosting endpoint.

PowerShell

4. Import the certificate for the hosting endpoint.

PowerShell

Import extension host certificates

$CertPassword = read-host -AsSecureString -prompt "Certificate

Password"

$CloudAdminCred = Get-Credential -UserName <Privileged endpoint

credentials> -Message "Enter the cloud domain credentials to access the

privileged endpoint."

[Byte[]]$AdminHostingCertContent = [Byte[]](Get-Content

c:\certificate\myadminhostingcertificate.pfx -Encoding Byte)

Invoke-Command -ComputerName <PrivilegedEndpoint computer name> `

-Credential $CloudAdminCred `

-ConfigurationName "PrivilegedEndpoint" `

-ArgumentList @($AdminHostingCertContent, $CertPassword) `

-ScriptBlock {

param($AdminHostingCertContent, $CertPassword)

Import-AdminHostingServiceCert $AdminHostingCertContent

$certPassword

}

$CertPassword = read-host -AsSecureString -prompt "Certificate

Password"

$CloudAdminCred = Get-Credential -UserName <Privileged endpoint

credentials> -Message "Enter the cloud domain credentials to access the

privileged endpoint."

IP Hostname Type

<IP> \*.Adminhosting.<Region>.<FQDN> A

<IP> \*.Hosting.<Region>.<FQDN> A

Allocated IPs can be retrieved using the privileged endpoint by running the cmdlet GetAzureStackStampInformation.

The article Azure Stack Hub datacenter integration - Publish endpoints covers the ports

and protocols that require inbound communication to publish Azure Stack Hub before

the extension host rollout.

There are two new endpoints required to be published through your firewall. The

allocated IPs from the public VIP pool can be retrieved using the following code that

must be run from your Azure Stack Hub environment's privileged endpoint.

PowerShell

[Byte[]]$HostingCertContent = [Byte[]](Get-Content

c:\certificate\myhostingcertificate.pfx -Encoding Byte)

Invoke-Command -ComputerName <PrivilegedEndpoint computer name> `

-Credential $CloudAdminCred `

-ConfigurationName "PrivilegedEndpoint" `

-ArgumentList @($HostingCertContent, $CertPassword) `

-ScriptBlock {

param($HostingCertContent, $CertPassword)

Import-UserHostingServiceCert $HostingCertContent $certPassword

}

Update DNS configuration

７ Note

This step isn't required if you used DNS Zone delegation for DNS Integration. If

individual host A records have been configured to publish Azure Stack Hub

endpoints, you need to create two additional host A records:

Ports and protocols

Publish new endpoints

# Create a PEP Session

winrm s winrm/config/client '@{TrustedHosts= "<IpOfERCSMachine>"}'

$PEPCreds = Get-Credential

$PEPSession = New-PSSession -ComputerName <IpOfERCSMachine> -Credential

$PEPCreds -ConfigurationName "PrivilegedEndpoint" -SessionOption (NewPSSessionOption -Culture en-US -UICulture en-US)

# Obtain DNS Servers and extension host information from Azure Stack Hub

Stamp Information and find the IPs for the Host Extension Endpoints

$StampInformation = Invoke-Command $PEPSession {GetAzureStackStampInformation} | Select-Object -Property

ExternalDNSIPAddress01, ExternalDNSIPAddress02, @{n="TenantHosting";e=

{($\_.TenantExternalEndpoints.TenantHosting) -replace

"https://\*.","testdnsentry"-replace "/"}}, @{n="AdminHosting";e=

{($\_.AdminExternalEndpoints.AdminHosting)-replace

"https://\*.","testdnsentry"-replace "/"}},@{n="TenantHostingDNS";e=

{($\_.TenantExternalEndpoints.TenantHosting) -replace "https://",""-replace

"/"}}, @{n="AdminHostingDNS";e={($\_.AdminExternalEndpoints.AdminHosting)-

replace "https://",""-replace "/"}}

If (Resolve-DnsName -Server $StampInformation.ExternalDNSIPAddress01 -Name

$StampInformation.TenantHosting -ErrorAction SilentlyContinue) {

Write-Host "Can access AZS DNS" -ForegroundColor Green

$AdminIP = (Resolve-DnsName -Server

$StampInformation.ExternalDNSIPAddress02 -Name

$StampInformation.AdminHosting).IPAddress

Write-Host "The IP for the Admin Extension Host is:

$($StampInformation.AdminHostingDNS) - is: $($AdminIP)" -ForegroundColor

Yellow

Write-Host "The Record to be added in the DNS zone: Type A, Name:

$($StampInformation.AdminHostingDNS), Value: $($AdminIP)" -ForegroundColor

Green

$TenantIP = (Resolve-DnsName -Server

$StampInformation.ExternalDNSIPAddress01 -Name

$StampInformation.TenantHosting).IPAddress

Write-Host "The IP address for the Tenant Extension Host is

$($StampInformation.TenantHostingDNS) - is: $($TenantIP)" -ForegroundColor

Yellow

Write-Host "The Record to be added in the DNS zone: Type A, Name:

$($StampInformation.TenantHostingDNS), Value: $($TenantIP)" -ForegroundColor

Green

}

Else {

Write-Host "Cannot access AZS DNS" -ForegroundColor Yellow

$AdminIP = (Resolve-DnsName -Name

$StampInformation.AdminHosting).IPAddress

Write-Host "The IP for the Admin Extension Host is:

$($StampInformation.AdminHostingDNS) - is: $($AdminIP)" -ForegroundColor

Yellow

Write-Host "The Record to be added in the DNS zone: Type A, Name:

$($StampInformation.AdminHostingDNS), Value: $($AdminIP)" -ForegroundColor

Green

$TenantIP = (Resolve-DnsName -Name

$StampInformation.TenantHosting).IPAddress

Write-Host "The IP address for the Tenant Extension Host is

$($StampInformation.TenantHostingDNS) - is: $($TenantIP)" -ForegroundColor

PowerShell

Endpoint (VIP) Protocol Ports

Admin Hosting HTTPS 443

Hosting HTTPS 443

Yellow

Write-Host "The Record to be added in the DNS zone: Type A, Name:

$($StampInformation.TenantHostingDNS), Value: $($TenantIP)" -ForegroundColor

Green

}

Remove-PSSession -Session $PEPSession

Sample Output

Can access AZS DNS

The IP for the Admin Extension Host is: \*.adminhosting.\<region>.\<fqdn> -

is: xxx.xxx.xxx.xxx

The Record to be added in the DNS zone: Type A, Name: \*.adminhosting.\

<region>.\<fqdn>, Value: xxx.xxx.xxx.xxx

The IP address for the Tenant Extension Host is \*.hosting.\<region>.\<fqdn>

- is: xxx.xxx.xxx.xxx

The Record to be added in the DNS zone: Type A, Name: \*.hosting.\<region>.\

<fqdn>, Value: xxx.xxx.xxx.xxx

７ Note

Make this change before enabling the extension host. This allows the Azure Stack

Hub portals to be continuously accessible.

Update existing publishing Rules (Post enablement of

extension host)

７ Note

The 1808 Azure Stack Hub Update Package does not enable extension host yet. It

lets you prepare for extension host by importing the required certificates. Don't

close any ports before extension host is automatically enabled through an Azure

Stack Hub update package after the 1808 update.

The following existing endpoint ports must be closed in your existing firewall rules.

Endpoint (VIP) Protocol Ports

Portal (administrator) HTTPS 12495

12499

12646

12647

12648

12649

12650

13001

13003

13010

13011

13012

13020

13021

13026

30015

Portal (user) HTTPS 12495

12649

13001

13010

13011

13012

13020

13021

30015

13003

Azure Resource Manager (administrator) HTTPS 30024

Azure Resource Manager (user) HTTPS 30024

Learn about Firewall integration.

Learn about Azure Stack Hub certificates signing request generation.

７ Note

It's recommended to close those ports after successful validation.

Next steps

Validate datacenter network integration

for Azure Stack Hub

Article • 10/25/2021

Use the Azure Stack Hub Readiness Checker tool (AzsReadinessChecker) to validate that

your datacenter network is ready for deployment of Azure Stack Hub. Validate

datacenter network integration before an Azure Stack Hub deployment.

The network validation in the readiness checker tool can be run in two different modes.

Prior to receiving the Azure Stack Hub hardware, use the Appliance mode to validate the

datacenter network readiness. The appliance mode requires the use of a physical server

with hardware specifications listed later in this article. After the Azure Stack Hub

hardware has arrived and connected to the datacenter network, use the HLH mode by

running the Readiness Checker tool on the hardware lifecycle host of Azure Stack Hub.

The HLH mode does not require additional hardware.

The readiness checker validates:

Border connectivity

Switch configuration

DNS integration

DNS forwarder

Time server

Azure AD connectivity

AD FS and Graph connectivity

Duplicate IP address assignments

For more information about Azure Stack Hub datacenter integration, see Network

Integration Planning for Azure Stack.

Download the latest version of the Azure Stack Hub Readiness Checker tool

(AzsReadinessChecker) from the PowerShell Gallery .

Download the latest version of the Posh-SSH module from the PowerShell Gallery .

Get the readiness checker tool

Get the virtual router image

The Azure Stack Hub Readiness Checker tool uses a virtual router image based on

SONiC switch operating system. Download the latest version of the SONiC virtual switch

image for Hyper-V at https://aka.ms/azssonic .

The hardware requirements apply only to running the Readiness Checker in the

Appliance mode.

The Readiness Checker tool can run on a hardware device that meets the following

minimum requirements:

A single x64 CPU with hardware virtualization capability

8 GB of RAM

64 GB of local storage

The number and type of network interfaces equal to the number and type of

border switch connections, for example 4 x SFP28 network ports

Standard KVM input/output

Note that the number of network interfaces in the Readiness Checker device can be

fewer than the number of border connections when using the BGP routing. Individual

border connections are validated one at a time. Having four separate network interfaces

provides the best experience. Refer to Border connectivity for routing considerations.

The software prerequisites apply to running the Readiness Checker in both the

Appliance and the HLH mode.

The computer where the tool runs must have the following software in place:

Windows Server 2019 or Windows Server 2016

Hyper-V and the Hyper-V Management Tools features installed

The latest version of the Microsoft Azure Stack Hub Readiness Checker tool.

The latest version of the SONiC virtual switch image .

The latest version of the Posh-SSH PowerShell module .

The deployment worksheet filled out and exported to the DeploymentData.json

file.

Hardware prerequisites

Software prerequisites

Validate datacenter network integration in the

Appliance mode

1. Connect a physical device that meets the prerequisites directly to the border

switch ports designated for Azure Stack Hub with the appropriate type of network

cables and transceivers.

2. Open an administrative PowerShell prompt and then run the following command

to initialize AzsReadinessChecker:

PowerShell

3. From the PowerShell prompt, run the following command to start validation.

Specify the correct values for -DeploymentDataPath and -

VirtualRouterImagePath parameters.

PowerShell

4. After the tool runs, review the output. Confirm that the status is OK for all tests. If

the status is not OK, review the details and the log file for additional information.

1. Sign in to the HLH using the HLHAdmin account.

2. Open an administrative PowerShell prompt and then run the following command

to initialize AzsReadinessChecker:

PowerShell

3. From the PowerShell prompt, run the following command to start validation.

Specify the correct values for -DeploymentDataPath and -

VirtualRouterImagePath parameters.

PowerShell

Import-Module Microsoft.AzureStack.ReadinessChecker

Invoke-AzsNetworkValidation -DeploymentDataPath C:\DeploymentData.json

-VirtualRouterImagePath C:\sonic-vs.vhdx

Validate datacenter network integration in the

HLH mode

Import-Module Microsoft.AzureStack.ReadinessChecker

Invoke-AzsNetworkValidation -DeploymentDataPath C:\DeploymentData.json

-VirtualRouterImagePath C:\sonic-vs.vhdx -HLH

4. After the tool runs, review the output. Confirm that the status is OK for all tests. If

the status is not OK, review the details and the log file for additional information.

PowerShell

PowerShell

Remove all previous progress and create a clean report.

YAML

Syntax

Invoke-AzsNetworkValidation

-DeploymentDataPath <String>

[-RunTests <String[]>]

[-SkipTests <String[]>]

[-VirtualRouterImagePath <String>]

[-DnsName <String>]

[-MtuTestDestination <String>]

[-CustomCloudArmEndpoint <Uri>]

[-CustomUrl <Uri[]>]

[-OutputPath <String>]

[-CleanReport]

[<CommonParameters>]

Invoke-AzsNetworkValidation

-DeploymentDataPath <String>

[-VirtualRouterImagePath <String>]

[-CustomCloudArmEndpoint <Uri>]

[-VirtualSwitchName <String>]

[-NoUplinksRequired]

[-NetworkToTest <String>]

[-HLH]

[-OutputPath <String>]

[-CleanReport]

[<CommonParameters>]

Parameters

-CleanReport

Type: SwitchParameter

Parameter Sets: (All)

Position: Named

Azure Resource Manager endpoint URI for custom cloud.

YAML

List of additional URLs to test.

YAML

Path to Azure Stack Hub deployment configuration file created by the Deployment

Worksheet.

YAML

Default value: False

Accept pipeline input: False

Accept wildcard characters: False

-CustomCloudArmEndpoint

Type: String

Parameter Sets: (All)

Position: Named

Default value: None

Accept pipeline input: False

Accept wildcard characters: False

-CustomUrl

Type: String[]

Parameter Sets: Hub

Position: Named

Default value: None

Accept pipeline input: False

Accept wildcard characters: False

-DeploymentDataPath

Type: String

Parameter Sets: (All)

Position: Named

Default value: None

Accept pipeline input: False

Accept wildcard characters: False

DNS name to resolve for the DNS test.

YAML

Indicates the HLH mode for the readiness checker.

YAML

DNS name or IP address for the network path MTU test.

YAML

Allows to execute the test for only one of the networks. Default is to execute tests for

the BMC and External networks.

YAML

-DnsName

Type: String

Parameter Sets: (All)

Position: Named

Default value: management.azure.com

Accept pipeline input: False

Accept wildcard characters: False

-HLH

Type: SwitchParameter

Parameter Sets: HLH

Position: Named

Default value: False

Accept pipeline input: False

Accept wildcard characters: False

-MtuTestDestination

Type: String

Parameter Sets: Hub

Position: Named

Default value: go.microsoft.com

Accept pipeline input: False

Accept wildcard characters: False

-NetworkToTest

Indicate that the ping test on P2P interfaces should be skipped.

YAML

Directory path for log and report output.

YAML

List of tests to run. Default is to run all tests.

YAML

Type: String

Parameter Sets: HLH

Accepted values: BmcNetworkOnly, ExternalNetworkOnly

Position: Named

Default value: False

Accept pipeline input: False

Accept wildcard characters: False

-NoUplinksRequired

Type: SwitchParameter

Parameter Sets: HLH

Position: Named

Default value: False

Accept pipeline input: False

Accept wildcard characters: False

-OutputPath

Type: String

Parameter Sets: (All)

Position: Named

Default value: $env:TEMP\AzsReadinessChecker

Accept pipeline input: False

Accept wildcard characters: False

-RunTests

Type: String[]

Parameter Sets: Hub

Accepted values: LinkLayer, PortChannel, BorderUplink, IPConfig, BgpPeering,

BgpDefaultRoute, DnsServer, PathMtu, TimeServer, SyslogServer,

AzureEndpoint, AdfsEndpoint, Graph, DuplicateIP, DnsDelegation

List of tests to skip. Default is to not skip any tests.

YAML

Full path to the sonic-vs.vhdx image.

YAML

External Hyper-V Switch name on the HLH.

YAML

Position: Named

Default value: None

Accept pipeline input: False

Accept wildcard characters: False

-SkipTests

Type: String[]

Parameter Sets: Hub

Accepted values: PortChannel, BorderUplink, IPConfig, BgpPeering,

BgpDefaultRoute, DnsServer, PathMtu, TimeServer, SyslogServer,

AzureEndpoint, AdfsEndpoint, Graph, DuplicateIP, DnsDelegation

Position: Named

Default value: None

Accept pipeline input: False

Accept wildcard characters: False

-VirtualRouterImagePath

Type: String

Parameter Sets: (All)

Position: Named

Default value: None

Accept pipeline input: False

Accept wildcard characters: False

-VirtualSwitchName

Type: String

Parameter Sets: HLH

Position: Named

Default value: None

Accept pipeline input: False

Accept wildcard characters: False

Each time validation runs, it logs results to AzsReadinessChecker.log and

AzsReadinessCheckerReport.json. The location of these files appears with the validation

results in PowerShell.

The validation files can help you share status before you deploy Azure Stack Hub or

investigate validation problems. Both files persist the results of each subsequent

validation check. The report gives your deployment team confirmation of the identity

configuration. The log file can help your deployment or support team investigate

validation issues.

By default, both files are written to C:\Users\

<username>\AppData\Local\Temp\AzsReadinessChecker\ .

Use:

-OutputPath : The path parameter at the end of the run command to specify a

different report location.

-CleanReport : The parameter at the end of the run command to clear

AzsReadinessCheckerReport.json of previous report information. For more

information, see Azure Stack Hub validation report.

If a validation check fails, details about the failure appear in the PowerShell window. The

tool also logs information to AzsReadinessChecker.log.

View the readiness report

General Azure Stack Hub integration considerations

Report and log file

Validation failures

Next steps

Deployment worksheet for Azure Stack

Hub integrated systems

Article • 07/29/2022

The Azure Stack Hub deployment worksheet is a Windows Forms app that aggregates

all necessary deployment information and decisions in one place. You can complete the

deployment worksheet during the planning process and review it before the

deployment starts.

The information required by the worksheet covers networking, security, and identity

information. This information may require specific knowledge in certain areas so we

recommend you consult with experts to complete the worksheet.

While filling out the worksheet, you might need to make some pre-deployment

configuration changes to your network environment. These changes can include

reserving IP address spaces for the Azure Stack Hub solution, and configuring routers,

switches, and firewalls to prepare for connectivity to the new Azure Stack Hub solution.

７ Note

For more information on how to complete the deployment worksheet tool, see

Datacenter integration planning considerations for Azure Stack Hub integrated

systems.

For each release of the deployment worksheet, you must do a one-time installation of a

PowerShell module for each machine on which you want to use the deployment

worksheet.

1. Open an elevated PowerShell prompt.

2. In the PowerShell window, install the module from the PowerShell gallery :

PowerShell

If you receive a message about installing from an untrusted repository, press Y to

continue installation.

To launch and use the deployment worksheet on a computer on which you've installed

the deployment worksheet PowerShell module, do the following steps:

1. Start Windows PowerShell (don't use the PowerShell ISE, as unexpected results can

occur). It's not necessary to run PowerShell as an administrator.

2. Import the AzS.Deployment.Worksheet PowerShell module:

PowerShell

3. Once the module is imported, launch the deployment worksheet:

PowerShell

Installing the Windows PowerShell module

７ Note

The computer must be connected to the internet for this method to work.

Install-Module -Name Azs.Deployment.Worksheet -Repository PSGallery

Use the deployment worksheet tool

Import-Module AzS.Deployment.Worksheet

Start-DeploymentWorksheet

The deployment worksheet consists of separate tabs for collecting environment settings,

like Customer Settings, Network Settings, and Scale Unit #. You must supply all values

(except for any marked Optional) on all tabs before any configuration data files can be

generated. After all required values have been entered into the tool, you can use the

Action menu to Import, Export, and Generate. The JSON files required for deployment

are as follows:

Import: Enables you to import an Azure Stack Hub configuration data file

(ConfigurationData.json) that was generated by this tool or those files created by any

previous release of the deployment worksheet. Doing an import resets the forms and

deletes any previously entered setting or generated data.

Export: Validates the data currently entered into the forms, generates the IP subnets and

assignments, and then saves the content as JSON-formatted configuration files. You can

then use these files to generate the network configuration and install Azure Stack Hub.

Generate: Validates the currently entered data and generates the network map without

exporting the deployment JSON files. Two new tabs are created if Generate is successful:

Subnet Summary and IP Assignments. You can analyze the data on these tabs to ensure

the network assignments are as expected.

Clear All: Clears all data currently entered in the forms and returns them to default

values.

Save or Open your work in-progress: You can save and open partially entered data as

you're working on it using the File->Save and File->Open menus. This function differs

from the Import and Export functions because they require all data to be entered and

validated. Open/save doesn't validate and doesn't require all fields to be entered to save

your work in progress.

Logging and Warning messages: While the form is being used, you might see noncritical warning messages displayed in the PowerShell window. Critical errors are

displayed as a pop-up message. Optional detailed logging, including a log written to

disk, can be enabled to assist in troubleshooting problems.

To start the tool with verbose logging:

PowerShell

You can find the saved log in the current user's Temp directory; for example:

C:\Users\me\AppData\Local\Temp\Microsoft\_AzureStack\DeploymentWorksheet\_Log.

txt.

Start-DeploymentWorksheet -EnableLogging

Azure Stack Hub deployment connection models

Next steps

Integrate AD FS identity with your Azure Stack

Hub datacenter

Article • 05/15/2023

You can deploy Azure Stack Hub using Azure Active Directory (Azure AD) or Active Directory

Federation Services (AD FS) as the identity provider. The choice must be made before you deploy

Azure Stack Hub. In a connected scenario, you can choose Azure AD or AD FS. For a disconnected

scenario, only AD FS is supported. This article shows how to integrate Azure Stack Hub AD FS with

your datacenter AD FS.

Deploying with AD FS allows identities in an existing Active Directory forest to authenticate with

resources in Azure Stack Hub. This existing Active Directory forest requires a deployment of AD FS to

allow the creation of an AD FS federation trust.

Authentication is one part of identity. To manage role-based access control (RBAC) in Azure Stack

Hub, the Graph component must be configured. When access to a resource is delegated, the Graph

component looks up the user account in the existing Active Directory forest using the LDAP protocol.

The existing AD FS is the account security token service (STS) that sends claims to the Azure Stack

Hub AD FS (the resource STS). In Azure Stack Hub, automation creates the claims provider trust with

the metadata endpoint for the existing AD FS.

At the existing AD FS, a relying party trust must be configured. This step isn't done by the

automation, and must be configured by the operator. The Azure Stack Hub VIP endpoint for AD FS

can be created by using the pattern https://adfs.<Region>.<ExternalFQDN>/ .

） Important

You can't switch the identity provider without redeploying the entire Azure Stack Hub solution.

Active Directory Federation Services and Graph

The relying party trust configuration also requires you to configure the claim transformation rules that

are provided by Microsoft.

For the Graph configuration, a service account must be provided that has "read" permission in the

existing Active Directory. This account is required as input for the automation to enable RBAC

scenarios.

For the last step, a new owner is configured for the default provider subscription. This account has full

access to all resources when signed in to the Azure Stack Hub administrator portal.

Requirements:

Component Requirement

Graph Microsoft Active Directory 2012/2012 R2/2016 2019

AD FS Windows Server 2012/2012 R2/2016 2019

Graph only supports integration with a single Active Directory forest. If multiple forests exist, only the

forest specified in the configuration will be used to fetch users and groups.

The following information is required as inputs for the automation parameters:

Parameter Deployment

Worksheet

Parameter

Description Example

CustomADGlobalCatalog AD FS Forest FQDN FQDN of the target Active Directory forest

that you want to integrate with

Contoso.com

CustomADAdminCredentials A user with LDAP Read permission graphservice

For Active Directory deployments having multiple sites, configure the closest Active Directory Site to

your Azure Stack Hub deployment. The configuration avoids having the Azure Stack Hub Graph

service resolve queries using a Global Catalog Server from a remote site.

Add the Azure Stack Hub Public VIP network subnet to the Active Directory Site closest to Azure Stack

Hub. For example, let's say your Active Directory has two sites: Seattle and Redmond. If Azure Stack

Hub is deployed at the Seattle site, you would add the Azure Stack Hub Public VIP network subnet to

the Active Directory site for Seattle.

For more information on Active Directory Sites, see Designing the site topology.

Setting up Graph integration

Configure Active Directory Sites

７ Note

Optionally, you can create an account for the Graph service in the existing Active Directory. Do this

step if you don't already have an account that you want to use.

1. In the existing Active Directory, create the following user account (recommendation):

Username: graphservice

Password: Use a strong password and configure the password to never expire.

No special permissions or membership is required.

For this procedure, use a computer in your datacenter network that can communicate with the

privileged endpoint in Azure Stack Hub.

1. Open an elevated Windows PowerShell session (run as administrator), and connect to the IP

address of the privileged endpoint. Use the credentials for CloudAdmin to authenticate.

PowerShell

2. Now that you have a session with the privileged endpoint, run the following command:

Run the below script for Azure Stack Hub build 2008 and newer

PowerShell

Run the below script for Azure Stack Hub build prior to 2008

If your Active Directory consist of a single site, you can skip this step. If you have a catch-all

subnet configured, validate that the Azure Stack Hub Public VIP network subnet isn't part of it.

Create user account in the existing Active Directory (optional)

Trigger automation to configure graph

$creds = Get-Credential

$pep = New-PSSession -ComputerName <IP Address of ERCS> -ConfigurationName

PrivilegedEndpoint -Credential $creds -SessionOption (New-PSSessionOption -Culture

en-US -UICulture en-US)

$i = @(

[pscustomobject]@{

CustomADGlobalCatalog="fabrikam.com"

CustomADAdminCredential= Get-Credential -Message "Do not include

the domain name of the graphservice account in the username."

SkipRootDomainValidation = $false

ValidateParameters = $true

})

Invoke-Command -Session $pep -ScriptBlock {Register-DirectoryService -

customCatalog $using:i}

PowerShell

When prompted, specify the credential for the user account that you want to use for the Graph

service (such as graphservice). The input for the Register-DirectoryService cmdlet must be the

forest name / root domain in the forest rather than any other domain in the forest.

3. The Register-DirectoryService cmdlet has optional parameters that you can use in certain

scenarios where the existing Active Directory validation fails. When this cmdlet is executed, it

validates that the provided domain is the root domain, a global catalog server can be reached,

and that the provided account is granted read access.

Parameter Description

SkipRootDomainValidation Specifies that a child domain must be used instead of the recommended root

domain.

ValidateParameters Bypasses all validation checks.

Graph service in Azure Stack Hub uses the following protocols and ports to communicate with a

writeable Global Catalog Server (GC) and Key Distribution Center (KDC) that can process login

requests in the target Active Directory forest.

Graph service in Azure Stack Hub uses the following protocols and ports to communicate with the

target Active Directory:

Type Port Protocol

LDAP 389 TCP & UDP

LDAP SSL 636 TCP

LDAP GC 3268 TCP

LDAP GC SSL 3269 TCP

Invoke-Command -Session $pep -ScriptBlock {Register-DirectoryService -

CustomADGlobalCatalog contoso.com}

） Important

Wait for the credentials pop-up (Get-Credential isn't supported in the privileged endpoint)

and enter the Graph Service Account credentials.

Graph protocols and ports

Setting up AD FS integration by downloading

federation metadata

The following information is required as input for the automation parameters:

Parameter Deployment

Worksheet

Parameter

Description Example

CustomAdfsName AD FS

Provider

Name

Name of

the claims

provider.

It appears

that way on

the AD FS

landing

page.

Contoso

CustomAD

FSFederationMetadataEndpointUri

AD FS

Metadata

URI

Federation

metadata

link.

https://ad01.contoso.com/federationmetadata/2007-

06/federationmetadata.xml

SigningCertificateRevocationCheck NA Optional

Parameter

to skip CRL

checking.

None

For this procedure, use a computer that can communicate with the privileged endpoint in Azure Stack

Hub. It's expected that the certificate used by the account STS AD FS is trusted by Azure Stack Hub.

1. Open an elevated Windows PowerShell session and connect to the privileged endpoint.

PowerShell

2. Now that you're connected to the privileged endpoint, run the following command using the

parameters appropriate for your environment:

PowerShell

3. Run the following command to update the owner of the default provider subscription using the

parameters appropriate for your environment:

PowerShell

Trigger automation to configure claims provider trust in Azure

Stack Hub (by downloading federation metadata)

$creds = Get-Credential

Enter-PSSession -ComputerName <IP Address of ERCS> -ConfigurationName

PrivilegedEndpoint -Credential $creds

Register-CustomAdfs -CustomAdfsName Contoso -

CustomADFSFederationMetadataEndpointUri

"https://ad01.contoso.com/federationmetadata/2007-06/federationmetadata.xml"

Beginning with version 1807, use this method if the either of the following conditions are true:

The certificate chain is different for AD FS compared to all other endpoints in Azure Stack Hub.

There's no network connectivity to the existing AD FS server from Azure Stack Hub's AD FS

instance.

The following information is required as input for the automation parameters:

Parameter Description Example

CustomAdfsName Name of the claims

provider. It appears that

way on the AD FS

landing page.

Contoso

CustomADFSFederationMetadataFileContent Metadata content. $using:federationMetadataFileContent

For the following procedure, you must use a computer that has network connectivity to the existing

AD FS deployment, which becomes the account STS. The necessary certificates must also be installed.

1. Open an elevated Windows PowerShell session, and run the following command using the

parameters appropriate for your environment:

PowerShell

2. Copy the metadata file to a computer that can communicate with the privileged endpoint.

For this procedure, use a computer that can communicate with the privileged endpoint in Azure Stack

Hub and has access to the metadata file you created in a previous step.

1. Open an elevated Windows PowerShell session and connect to the privileged endpoint.

Set-ServiceAdminOwner -ServiceAdminOwnerUpn "administrator@contoso.com"

Setting up AD FS integration by providing federation

metadata file

Create federation metadata file

$url = "https://win-SQOOJN70SGL.contoso.com/FederationMetadata/2007-

06/FederationMetadata.xml"

$webclient = New-Object System.Net.WebClient

$webclient.Encoding = [System.Text.Encoding]::UTF8

$metadataAsString = $webclient.DownloadString($url)

Set-Content -Path c:\metadata.xml -Encoding UTF8 -Value $metadataAsString

Trigger automation to configure claims provider trust in Azure

Stack Hub (using federation metadata file)

PowerShell

2. Now that you're connected to the privileged endpoint, run the following command using the

parameters appropriate for your environment:

PowerShell

3. Run the following command to update the owner of the default provider subscription. Use the

parameters appropriate for your environment.

PowerShell

Microsoft provides a script that configures the relying party trust, including the claim transformation

rules. Using the script is optional as you can run the commands manually.

You can download the helper script from Azure Stack Hub Tools on GitHub.

If you decide to manually run the commands, follow these steps:

1. Copy the following content into a .txt file (for example, saved as c:\ClaimIssuanceRules.txt) on

your datacenter's AD FS instance or farm member:

text

$federationMetadataFileContent = get-content c:\metadata.xml

$creds=Get-Credential

Enter-PSSession -ComputerName <IP Address of ERCS> -ConfigurationName

PrivilegedEndpoint -Credential $creds

Register-CustomAdfs -CustomAdfsName Contoso -

CustomADFSFederationMetadataFileContent $using:federationMetadataFileContent

Set-ServiceAdminOwner -ServiceAdminOwnerUpn "administrator@contoso.com"

７ Note

When you rotate the certificate on the existing AD FS (account STS), you must set up the

AD FS integration again. You must set up the integration even if the metadata endpoint is

reachable or it was configured by providing the metadata file.

Configure relying party on existing AD FS deployment

(account STS)

@RuleTemplate = "LdapClaims"

@RuleName = "Name claim"

c:[Type ==

"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",

Issuer == "AD AUTHORITY"]

=> issue(store = "Active Directory", types =

2. Validate that Windows Forms-based authentication for extranet and intranet is enabled. You can

check if its already enabled by running the following cmdlet:

PowerShell

("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name"), query =

";userPrincipalName;{0}", param = c.Value);

@RuleTemplate = "LdapClaims"

@RuleName = "UPN claim"

c:[Type ==

"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",

Issuer == "AD AUTHORITY"]

=> issue(store = "Active Directory", types =

("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"), query =

";userPrincipalName;{0}", param = c.Value);

@RuleTemplate = "LdapClaims"

@RuleName = "ObjectID claim"

c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid"]

=> issue(Type = "http://schemas.microsoft.com/identity/claims/objectidentifier",

Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType =

c.ValueType);

@RuleName = "Family Name and Given claim"

c:[Type ==

"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",

Issuer == "AD AUTHORITY"]

=> issue(store = "Active Directory", types =

("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname",

"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname"), query =

";sn,givenName;{0}", param = c.Value);

@RuleTemplate = "PassThroughClaims"

@RuleName = "Pass through all Group SID claims"

c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid",

Issuer =~ "^(AD AUTHORITY|SELF AUTHORITY|LOCAL AUTHORITY)$"]

=> issue(claim = c);

@RuleTemplate = "PassThroughClaims"

@RuleName = "Pass through all windows account name claims"

c:[Type ==

"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]

=> issue(claim = c);

Get-AdfsAuthenticationProvider | where-object { $\_.name -eq "FormsAuthentication" }

| select Name, AllowedForPrimaryExtranet, AllowedForPrimaryIntranet

７ Note

The Windows Integrated Authentication (WIA) supported user agent strings may be

outdated for your AD FS deployment and may require an update to support the latest

clients. You can read more about updating the WIA supported user agent strings in the

article Configuring intranet forms-based authentication for devices that don't support

WIA.

3. To add the relying party trust, run the following Windows PowerShell command on your AD FS

instance or a farm member. Make sure to update the AD FS endpoint and point to the file

created in Step 1.

For AD FS 2016/2019

PowerShell

For AD FS 2012/2012 R2

PowerShell

4. When you use Internet Explorer or the Microsoft Edge browser to access Azure Stack Hub, you

must ignore token bindings. Otherwise, the sign-in attempts fail. On your AD FS instance or a

farm member, run the following command:

For steps to enable Form-based authentication policy, see Configure Authentication

Policies.

） Important

For customers running Azure Stack Hub versions 2002 and later, TLS 1.2 is enforced on the

Azure Stack Hub ADFS endpoint. As such, TLS 1.2 must also be enabled on the customer

ADFS servers. Otherwise, the following error will occur when running AddADFSRelyingPartyTrust on the customer owned ADFS host/farm:

Add-ADFSRelyingPartyTrust : The underlying connection was closed: An unexpected error

occurred on a send.

Add-ADFSRelyingPartyTrust -Name AzureStack -MetadataUrl

"https://YourAzureStackADFSEndpoint/FederationMetadata/2007-

06/FederationMetadata.xml" -IssuanceTransformRulesFile "C:\ClaimIssuanceRules.txt"

-AutoUpdateEnabled:$true -MonitoringEnabled:$true -enabled:$true -

AccessControlPolicyName "Permit everyone" -TokenLifeTime 1440

Add-ADFSRelyingPartyTrust -Name AzureStack -MetadataUrl

"https://YourAzureStackADFSEndpoint/FederationMetadata/2007-

06/FederationMetadata.xml" -IssuanceTransformRulesFile "C:\ClaimIssuanceRules.txt"

-AutoUpdateEnabled:$true -MonitoringEnabled:$true -enabled:$true -TokenLifeTime

1440

） Important

You must use the AD FS MMC snap-in to configure the Issuance Authorization Rules when

using Windows Server 2012 or 2012 R2 AD FS.

７ Note

PowerShell

There are many scenarios that require the use of a service principal name (SPN) for authentication.

The following are some examples:

Azure CLI usage with AD FS deployment of Azure Stack Hub.

System Center Management Pack for Azure Stack Hub when deployed with AD FS.

Resource providers in Azure Stack Hub when deployed with AD FS.

Various apps.

You require a non-interactive sign-in.

For more information on creating an SPN, see Create service principal for AD FS.

If an error occurs that leaves the environment in a state where you can no longer authenticate, a

rollback option is available.

1. Open an elevated Windows PowerShell session and run the following commands:

PowerShell

2. Then run the following cmdlet:

PowerShell

This step isn't applicable when using Windows Server 2012 or 2012 R2 AD FS. In that case,

it's safe to skip this command and continue with the integration.

Set-AdfsProperties -IgnoreTokenBinding $true

SPN creation

） Important

AD FS only supports interactive sign-in sessions. If you require a non-interactive sign-in for an

automated scenario, you must use a SPN.

Troubleshooting

Configuration Rollback

$creds = Get-Credential

Enter-PSSession -ComputerName <IP Address of ERCS> -ConfigurationName

PrivilegedEndpoint -Credential $creds

Reset-DatacenterIntegrationConfiguration

After running the rollback action, all configuration changes are rolled back. Only authentication

with the built-in CloudAdmin user is possible.

PowerShell

If any of the cmdlets fail, you can collect additional logs by using the Get-Azurestacklogs cmdlet.

1. Open an elevated Windows PowerShell session and run the following commands:

PowerShell

2. Then run the following cmdlet:

PowerShell

Integrate external monitoring solutions

） Important

You must configure the original owner of the default provider subscription.

Set-ServiceAdminOwner -ServiceAdminOwnerUpn "azurestackadmin@[Internal Domain]"

Collecting additional logs

$creds = Get-Credential

Enter-pssession -ComputerName <IP Address of ERCS> -ConfigurationName

PrivilegedEndpoint -Credential $creds

Get-AzureStackLog -OutputPath \\myworkstation\AzureStackLogs -FilterByRole ECE

Next steps

Create a custom role for Azure Stack

Hub registration

Article • 07/29/2022

During Azure Stack Hub registration, you must sign in with an Azure Active Directory

(Azure AD) account. The account requires the following Azure AD permissions and Azure

Subscription permissions:

App registration permissions in your Azure AD tenant: Admins have app

registration permissions. The permission for users is a global setting for all users in

the tenant. To view or change the setting, see create an Azure AD app and service

principal that can access resources.

The user can register applications setting must be set to Yes for you to enable a

user account to register Azure Stack Hub. If the app registrations setting is set to

No, you can't use a user account to register Azure Stack Hub--you have to use a

global admin account.

A set of sufficient Azure Subscription permissions: Users that belong to the

Owner role have sufficient permissions. For other accounts, you can assign the

permission set by assigning a custom role as outlined in the following sections.

Rather than using an account that has Owner permissions in the Azure subscription, you

can create a custom role to assign permissions to a less-privileged user account. This

account can then be used to register your Azure Stack Hub.

To create a custom role, you must have the

Microsoft.Authorization/roleDefinitions/write permission on all AssignableScopes ,

such as Owner or User Access Administrator. Use the following JSON template to

２ Warning

This is not a security posture feature. Use it in scenarios where you want constraints

to prevent accidental changes to the Azure Subscription. When a user is delegated

rights to this custom role, the user has rights to edit permissions and elevate rights.

Only assign users you trust to the custom role.

Create a custom role using PowerShell

simplify creation of the custom role. The template creates a custom role that allows the

required read and write access for Azure Stack Hub registration.

1. Create a JSON file. For example, C:\CustomRoles\registrationrole.json .

2. Add the following JSON to the file. Replace <SubscriptionID> with your Azure

subscription ID.

JSON

3. In PowerShell, connect to Azure to use Azure Resource Manager. When prompted,

authenticate using an account with sufficient permissions such as Owner or User

Access Administrator.

Azure PowerShell

4. To create the custom role, use New-AzRoleDefinition specifying the JSON

template file.

Azure PowerShell

{

"Name": "Azure Stack Hub registration role",

"Id": null,

"IsCustom": true,

"Description": "Allows access to register Azure Stack Hub",

"Actions": [

"Microsoft.Resources/subscriptions/resourceGroups/write",

"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.AzureStack/registrations/\*",

"Microsoft.AzureStack/register/action",

"Microsoft.Authorization/roleAssignments/read",

"Microsoft.Authorization/roleAssignments/write",

"Microsoft.Authorization/roleAssignments/delete",

"Microsoft.Authorization/permissions/read",

"Microsoft.Authorization/locks/read",

"Microsoft.Authorization/locks/write"

],

"NotActions": [

],

"AssignableScopes": [

"/subscriptions/<SubscriptionID>"

]

}

Connect-AzAccount

New-AzRoleDefinition -InputFile "C:\CustomRoles\registrationrole.json"

After the registration custom role is created, assign the role to the user account that will

be used for registering Azure Stack Hub.

1. Sign in with the account with sufficient permission on the Azure subscription to

delegate rights--such as Owner or User Access Administrator.

2. In Subscriptions, select Access control (IAM) > Add role assignment.

3. In Role, choose the custom role you created: Azure Stack Hub registration role.

4. Select the users you want to assign to the role.

5. Select Save to assign the selected users to the role.

For more information on using custom roles, see manage access using RBAC and the

Azure portal.

Register Azure Stack Hub with Azure

Assign a user to registration role

Next steps

Validate Azure identity

Article • 07/29/2022

Use the Azure Stack Hub Readiness Checker tool (AzsReadinessChecker) to validate that

your Azure Active Directory (Azure AD) is ready to use with Azure Stack Hub. Validate

your Azure identity solution before you begin an Azure Stack Hub deployment.

The readiness checker validates:

Azure AD as an identity provider for Azure Stack Hub.

The Azure AD account that you plan to use can sign in as a global administrator of

your Azure AD.

Validation ensures your environment is ready for Azure Stack Hub to store information

about users, applications, groups, and service principals from Azure Stack Hub in your

Azure AD.

Download the latest version of the Azure Stack Hub Readiness Checker tool

(AzsReadinessChecker) from the PowerShell Gallery .

The following prerequisites are required:

You will need to have the Az PowerShell modules installed. For instructions, see

Install PowerShell Az preview module.

Get the readiness checker tool

Install and configure

Az PowerShell

Prerequisites

Az PowerShell modules

Azure Active Directory (Azure AD) environment

Identify the Azure AD account to use for Azure Stack Hub and ensure it's an

Azure AD global administrator.

Identify your Azure AD tenant name. The tenant name must be the primary

domain name for your Azure AD. For example, contoso.onmicrosoft.com.

1. On a computer that meets the prerequisites, open an elevated PowerShell

command prompt, and then run the following command to install

AzsReadinessChecker:

PowerShell

2. From the PowerShell prompt, run the following command. Replace

contoso.onmicrosoft.com with your Azure AD tenant name:

PowerShell

3. From the PowerShell prompt, run the following command to start validation of

your Azure AD. Replace contoso.onmicrosoft.com with your Azure AD tenant

name:

PowerShell

4. After the tool runs, review the output. Confirm the status is OK for installation

requirements. A successful validation appears like the following example:

PowerShell

Steps to validate Azure identity

Install-Module -Name Az.BootStrapper -Force -AllowPrerelease

Install-AzProfile -Profile 2020-09-01-hybrid -Force

Install-Module -Name Microsoft.AzureStack.ReadinessChecker -

AllowPrerelease

Connect-AzAccount -tenant contoso.onmicrosoft.com

Invoke-AzsAzureIdentityValidation -AADDirectoryTenantName

contoso.onmicrosoft.com

Invoke-AzsAzureIdentityValidation v1.2100.1448.484 started.

Starting Azure Identity Validation

Checking Installation Requirements: OK

Each time validation runs, it logs results to AzsReadinessChecker.log and

AzsReadinessCheckerReport.json. The location of these files displays with the validation

results in PowerShell.

These files can help you share validation status before you deploy Azure Stack Hub or

investigate validation problems. Both files persist the results of each subsequent

validation check. The report provides your deployment team confirmation of the identity

configuration. The log file can help your deployment or support team investigate

validation issues.

By default, both files are written to C:\Users\

<username>\AppData\Local\Temp\AzsReadinessChecker\AzsReadinessCheckerReport.json .

Use the -OutputPath <path> parameter at the end of the run command line to

specify a different report location.

Use the -CleanReport parameter at the end of the run command to clear

information about previous runs of the tool from

AzsReadinessCheckerReport.json.

For more information, see Azure Stack Hub validation report.

If a validation check fails, details about the failure display in the PowerShell window. The

tool also logs information to the AzsReadinessChecker.log file.

The following examples provide guidance on common validation failures.

Finished Azure Identity Validation

Log location (contains PII): C:\Users\

[\*redacted\*]\AppData\Local\Temp\AzsReadinessChecker\AzsReadinessChe

cker.log

Report location (contains PII): C:\Users\

[\*redacted\*]\AppData\Local\Temp\AzsReadinessChecker\AzsReadinessChe

ckerReport.json

Invoke-AzsAzureIdentityValidation Completed

Report and log file

Validation failures

Expired or temporary password

PowerShell

Cause - The account can't sign in because the password is either expired or temporary.

Resolution - In PowerShell, run the following command and then follow the prompts to

reset the password:

PowerShell

Another way is to sign in to the Azure portal as the account owner and the user will

be forced to change the password.

PowerShell

Invoke-AzsAzureIdentityValidation v1.1809.1005.1 started.

Starting Azure Identity Validation

Checking Installation Requirements: Fail

Error Details for Service Administrator Account

admin@contoso.onmicrosoft.com

The password for account has expired or is a temporary password that needs

to be reset before continuing. Run Login-AzureRMAccount, login with

credentials and follow the prompts to reset.

Additional help URL https://aka.ms/AzsRemediateAzureIdentity

Finished Azure Identity Validation

Log location (contains PII):

C:\Users\username\AppData\Local\Temp\AzsReadinessChecker\AzsReadinessChecker

.log

Report location (contains PII):

C:\Users\username\AppData\Local\Temp\AzsReadinessChecker\AzsReadinessChecker

Report.json

Invoke-AzsAzureIdentityValidation Completed

Login-AzureRMAccount

Unknown user type

Invoke-AzsAzureIdentityValidation v1.1809.1005.1 started.

Starting Azure Identity Validation

Checking Installation Requirements: Fail

Error Details for Service Administrator Account

admin@contoso.onmicrosoft.com

Unknown user type detected. Check the account is valid for AzureChinaCloud

Additional help URL https://aka.ms/AzsRemediateAzureIdentity

Finished Azure Identity Validation

Cause - The account can't sign in to the specified Azure AD

(AADDirectoryTenantName). In this example, AzureChinaCloud is specified as the

AzureEnvironment.

Resolution - Confirm that the account is valid for the specified Azure environment. In

PowerShell, run the following command to verify the account is valid for a specific

environment:

PowerShell

PowerShell

Log location (contains PII):

C:\Users\username\AppData\Local\Temp\AzsReadinessChecker\AzsReadinessChecker

.log

Report location (contains PII):

C:\Users\username\AppData\Local\Temp\AzsReadinessChecker\AzsReadinessChecker

Report.json

Invoke-AzsAzureIdentityValidation Completed

Login-AzureRmAccount -EnvironmentName AzureChinaCloud

Account is not an administrator

Invoke-AzsAzureIdentityValidation v1.1809.1005.1 started.

Starting Azure Identity Validation

Checking Installation Requirements: Fail

Error Details for Service Administrator Account

admin@contoso.onmicrosoft.com

The Service Admin account you entered 'admin@contoso.onmicrosoft.com' is not

an administrator of the Azure Active Directory tenant

'contoso.onmicrosoft.com'.

Additional help URL https://aka.ms/AzsRemediateAzureIdentity

Finished Azure Identity Validation

Log location (contains PII):

C:\Users\username\AppData\Local\Temp\AzsReadinessChecker\AzsReadinessChecker

.log

Report location (contains PII):

C:\Users\username\AppData\Local\Temp\AzsReadinessChecker\AzsReadinessChecker

Report.json

Invoke-AzsAzureIdentityValidation Completed

Cause - Although the account can successfully sign in, the account isn't an admin of the

Azure AD (AADDirectoryTenantName).

Resolution - Sign in into the Azure portal as the account owner, go to Azure Active

Directory, then Users, then Select the User. Then select Directory Role and ensure the

user is a Global administrator. If the account is a User, go to Azure Active Directory >

Custom domain names and confirm that the name you supplied for

AADDirectoryTenantName is marked as the primary domain name for this directory. In

this example, that's contoso.onmicrosoft.com.

Azure Stack Hub requires that the domain name is the primary domain name.

Validate Azure registration

View the readiness report

General Azure Stack Hub integration considerations

Next Steps

Validate AD FS integration for Azure

Stack Hub

Article • 07/29/2022

Use the Azure Stack Hub Readiness Checker tool (AzsReadinessChecker) to validate that

your environment is ready for Active Directory Federation Services (AD FS) integration

with Azure Stack Hub. Validate AD FS integration before you begin datacenter

integration or before an Azure Stack Hub deployment.

The readiness checker validates:

The federation metadata contains the valid XML elements for federation.

The AD FS SSL certificate can be retrieved and a chain of trust can be built. On

stamp, AD FS must trust the SSL certificate chain. The certificate must be signed by

the same certificate authority used for the Azure Stack Hub deployment certificates

or by a trusted root authority partner. For the full list of trusted root authority

partners, see List of Participants - Microsoft Trusted Root Program.

The AD FS signing certificate is trusted and not nearing expiration.

For more information about Azure Stack Hub datacenter integration, see Azure Stack

Hub datacenter integration - Identity.

Download the latest version of the Azure Stack Hub Readiness Checker tool

(AzsReadinessChecker) from the PowerShell Gallery .

The following prerequisites must be in place.

The computer where the tool runs:

Windows 10 or Windows Server 2016 with domain connectivity.

PowerShell 5.1 or later. To check your version, run the following PowerShell

command and then review the Major version and Minor versions:

PowerShell

Get the readiness checker tool

Prerequisites

$PSVersionTable.PSVersion

Latest version of the Microsoft Azure Stack Hub Readiness Checker tool.

Active Directory Federation Services environment:

You need at least one of the following forms of metadata:

The URL for AD FS federation metadata. For example:

https://adfs.contoso.com/FederationMetadata/2007-06/FederationMetadata.xml .

The federation metadata XML file. For example: FederationMetadata.xml.

1. On a computer that meets the prerequisites, open an administrative PowerShell

prompt and then run the following command to install AzsReadinessChecker:

PowerShell

2. From the PowerShell prompt, run the following command to start validation.

Specify the value for -CustomADFSFederationMetadataEndpointUri as the URI for

the federation metadata.

PowerShell

3. After the tool runs, review the output. Confirm that the status is OK for AD FS

integration requirements. A successful validation is similar to the following

example:

PowerShell

Validate AD FS integration

Install-Module Microsoft.AzureStack.ReadinessChecker -Force -

AllowPrerelease

Invoke-AzsADFSValidation -CustomADFSFederationMetadataEndpointUri

https://adfs.contoso.com/FederationMetadata/2007-

06/FederationMetadata.xml

Invoke-AzsADFSValidation v1.1809.1001.1 started.

Testing ADFS Endpoint https://sts.contoso.com/FederationMetadata/2007-

06/FederationMetadata.xml

Read Metadata: OK

Test Metadata Elements: OK

Test SSL ADFS Certificate: OK

Test Certificate Chain: OK

In production environments, testing certificate chains of trust from an operator's

workstation isn't fully indicative of the PKI trust posture in the Azure Stack Hub

infrastructure. The Azure Stack Hub stamp's public VIP network needs the connectivity

to the CRL for the PKI infrastructure.

Each time validation runs, it logs results to AzsReadinessChecker.log and

AzsReadinessCheckerReport.json. The location of these files appears with the validation

results in PowerShell.

The validation files can help you share status before you deploy Azure Stack Hub or

investigate validation problems. Both files persist the results of each subsequent

validation check. The report gives your deployment team confirmation of the identity

configuration. The log file can help your deployment or support team investigate

validation issues.

By default, both files are written to C:\Users\

<username>\AppData\Local\Temp\AzsReadinessChecker\ .

Use:

-OutputPath : The path parameter at the end of the run command to specify a

different report location.

-CleanReport : The parameter at the end of the run command to clear

AzsReadinessCheckerReport.json of previous report information. For more

information, see Azure Stack Hub validation report.

Test Certificate Expiry: OK

Details:

[-] In standalone mode, some tests should not be considered fully

indicative of connectivity or readiness the Azure Stack Hub Stamp

requires prior to Datacenter Integration.

Additional help URL: https://aka.ms/AzsADFSIntegration

Log location (contains PII):

C:\Users\username\AppData\Local\Temp\AzsReadinessChecker\AzsReadinessCh

ecker.log

Report location (contains PII):

C:\Users\username\AppData\Local\Temp\AzsReadinessChecker\AzsReadinessCh

eckerReport.json

Invoke-AzsADFSValidation Completed

Report and log file

If a validation check fails, details about the failure appear in the PowerShell window. The

tool also logs information to AzsReadinessChecker.log.

The following examples provide guidance on common validation failures.

PowerShell

Cause: PowerShell Autoload failed to load the Readiness Checker module correctly.

Resolution: Import the Readiness Checker module explicitly. Copy and paste the

following code into PowerShell and update <version> with the number for the currently

installed version.

PowerShell

View the readiness report

General Azure Stack Hub integration considerations

Validation failures

Command Not Found

Invoke-AzsADFSValidation : The term 'Invoke-AzsADFSValidation' is not

recognized as the name of a cmdlet, function, script file, or operable

program. Check the spelling of the name, or if a path was included, verify

that the path is correct and try again.

Import-Module "c:\Program

Files\WindowsPowerShell\Modules\Microsoft.AzureStack.ReadinessChecker\

<version>\Microsoft.AzureStack.ReadinessChecker.psd1" -Force

Next steps

Validate graph integration for Azure

Stack Hub

Article • 07/29/2022

Use the Azure Stack Hub Readiness Checker tool (AzsReadinessChecker) to validate that

your environment is ready for graph integration with Azure Stack Hub. Validate graph

integration before you begin datacenter integration or before an Azure Stack Hub

deployment.

The readiness checker validates:

The credentials to the service account created for graph integration have

appropriate rights to query Active Directory.

The global catalog can be resolved and is contactable.

The KDC can be resolved and is contactable.

Necessary network connectivity is in place.

For more information about Azure Stack Hub datacenter integration, see Azure Stack

Hub datacenter integration - Identity.

Download the latest version of the Azure Stack Hub Readiness Checker tool

(AzsReadinessChecker) from the PowerShell Gallery .

The following prerequisites must be in place.

The computer where the tool runs:

Windows 10 or Windows Server 2016 with domain connectivity.

PowerShell 5.1 or later. To check your version, run the following PowerShell

command and then review the Major version and Minor versions:

PowerShell

Active Directory PowerShell module.

Latest version of the Microsoft Azure Stack Hub Readiness Checker tool.

Get the readiness checker tool

Prerequisites

$PSVersionTable.PSVersion

Active Directory environment:

Identify the username and password for an account for the graph service in the

existing Active Directory instance.

Identify the Active Directory forest root FQDN.

1. On a computer that meets the prerequisites, open an administrative PowerShell

prompt and then run the following command to install the AzsReadinessChecker:

PowerShell

2. From the PowerShell prompt, run the following command to set the

$graphCredential variable to the graph account. Replace contoso\graphservice

with your account by using the domain\username format.

PowerShell

3. From the PowerShell prompt, run the following command to start validation for the

graph service. Specify the value for -ForestFQDN as the FQDN for the forest root.

PowerShell

4. After the tool runs, review the output. Confirm that the status is OK for graph

integration requirements. A successful validation is similar to the following

example:

PowerShell

Validate the graph service

Install-Module Microsoft.AzureStack.ReadinessChecker -Force -

AllowPrerelease

$graphCredential = Get-Credential contoso\graphservice -Message "Enter

Credentials for the Graph Service Account"

Invoke-AzsGraphValidation -ForestFQDN contoso.com -Credential

$graphCredential

Testing Graph Integration (v1.0)

Test Forest Root: OK

Test Graph Credential: OK

Test Global Catalog: OK

Test KDC: OK

In production environments, testing network connectivity from an operator's

workstation isn't fully indicative of the connectivity available to Azure Stack Hub. The

Azure Stack Hub stamp's public VIP network needs the connectivity for LDAP traffic to

perform identity integration.

Each time validation runs, it logs results to AzsReadinessChecker.log and

AzsReadinessCheckerReport.json. The location of these files appears with the validation

results in PowerShell.

The validation files can help you share status before you deploy Azure Stack Hub or

investigate validation problems. Both files persist the results of each subsequent

validation check. The report gives your deployment team confirmation of the identity

configuration. The log file can help your deployment or support team investigate

validation issues.

By default, both files are written to C:\Users\

<username>\AppData\Local\Temp\AzsReadinessChecker\ .

Use:

-OutputPath : The path parameter at the end of the run command to specify a

different report location.

Test LDAP Search: OK

Test Network Connectivity: OK

Details:

[-] In standalone mode, some tests should not be considered fully

indicative of connectivity or readiness the Azure Stack Hub Stamp

requires prior to Datacenter Integration.

Additional help URL: https://aka.ms/AzsGraphIntegration

AzsReadinessChecker Log location (contains PII):

C:\Users\username\AppData\Local\Temp\AzsReadinessChecker\AzsReadinessCh

ecker.log

AzsReadinessChecker Report location (contains PII):

C:\Users\username\AppData\Local\Temp\AzsReadinessChecker\AzsReadinessCh

eckerReport.json

Invoke-AzsGraphValidation Completed

Report and log file

-CleanReport : The parameter at the end of the run command to clear

AzsReadinessCheckerReport.json of previous report information. For more

information, see Azure Stack Hub validation report.

If a validation check fails, details about the failure appear in the PowerShell window. The

tool also logs information to AzsGraphIntegration.log.

View the readiness report

General Azure Stack Hub integration considerations

Validation failures

Next steps

Azure Stack Hub public key

infrastructure (PKI) certificate

requirements

Article • 07/29/2022

Azure Stack Hub has a public infrastructure network using externally accessible public IP

addresses assigned to a small set of Azure Stack Hub services and possibly tenant VMs.

PKI certificates with the appropriate DNS names for these Azure Stack Hub public

infrastructure endpoints are required during Azure Stack Hub deployment. This article

provides information about:

Certificate requirements for Azure Stack Hub.

Mandatory certificates required for Azure Stack Hub deployment.

Optional certificates required when deploying value-add resource providers.

The following list describes the general certificate issuance, security, and formatting

requirements:

Certificates must be issued from either an internal certificate authority or a public

certificate authority. If a public certificate authority is used, it must be included in

the base operating system image as part of the Microsoft Trusted Root Authority

Program. For the full list, see List of Participants - Microsoft Trusted Root Program.

Your Azure Stack Hub infrastructure must have network access to the certificate

authority's Certificate Revocation List (CRL) location published in the certificate.

This CRL must be an http endpoint. Note: for disconnected deployments,

７ Note

Azure Stack Hub by default also uses certificates issued from an internal Active

Directory-integrated certificate authority (CA) for authentication between the

nodes. To validate the certificate, all Azure Stack Hub infrastructure machines trust

the root certificate of the internal CA by means of adding that certificate to their

local certificate store. There's no pinning or filtering of certificates in Azure Stack

Hub. The SAN of each server certificate is validated against the FQDN of the target.

The entire chain of trust is also validated, along with the certificate expiration date

(standard TLS server authentication without certificate pinning).

Certificate requirements

certificates issued by a public certificate authority (CA) are not supported, if the

CRL endpoint is not accessible. For more details see Features that are impaired or

unavailable in disconnected deployments.

When rotating certificates for builds 1903 and later, certificates can be issued by

any enterprise or public certificate authority.

The use of self-signed certificates aren't supported.

For deployment and rotation, you can either use a single certificate covering all

name spaces in the certificate's Subject Name and Subject Alternative Name (SAN).

Alternatively, you can use individual certificates for each of the namespaces below

that the Azure Stack Hub services you plan to utilize require. Both approaches

require using wild cards for endpoints where they're required, such as KeyVault

and KeyVaultInternal.

The certificate signature algorithm shouldn't be SHA1.

The certificate format must be PFX, as both the public and private keys are

required for Azure Stack Hub installation. The private key must have the local

machine key attribute set.

The PFX encryption must be 3DES (this encryption is default when exporting from

a Windows 10 client or Windows Server 2016 certificate store).

The certificate pfx files must have a value "Digital Signature" and

"KeyEncipherment" in its "Key Usage" field.

The certificate pfx files must have the values "Server Authentication

(1.3.6.1.5.5.7.3.1)" and "Client Authentication (1.3.6.1.5.5.7.3.2)" in the "Enhanced

Key Usage" field.

The certificate's "Issued to:" field must not be the same as its "Issued by:" field.

The passwords to all certificate pfx files must be the same at the time of

deployment.

Password to the certificate pfx has to be a complex password. Make note of this

password because you'll use it as a deployment parameter. The password must

meet the following password complexity requirements:

A minimum length of eight characters.

At least three of the following characters: uppercase letter, lowercase letter,

numbers from 0-9, special characters, alphabetical character that's not

uppercase or lowercase.

Ensure that the subject names and subject alternative names in the subject

alternative name extension (x509v3\_config) match. The subject alternative name

field lets you specify additional host names (websites, IP addresses, common

names) to be protected by a single SSL certificate.

７ Note

The table in this section describes the Azure Stack Hub public endpoint PKI certificates

that are required for both Azure AD and AD FS Azure Stack Hub deployments.

Certificate requirements are grouped by area, and the namespaces used and the

certificates that are required for each namespace. The table also describes the folder in

which your solution provider copies the different certificates per public endpoint.

Certificates with the appropriate DNS names for each Azure Stack Hub public

infrastructure endpoint are required. Each endpoint's DNS name is expressed in the

format: <prefix>.<region>.<fqdn>.

For your deployment, the <region> and <fqdn> values must match the region and

external domain names that you chose for your Azure Stack Hub system. As an example,

if the region is Redmond and the external domain name is contoso.com, the DNS names

will have the format <prefix>.redmond.contoso.com. The <prefix> values are

predesignated by Microsoft to describe the endpoint secured by the certificate. In

addition, the <prefix> values of the external infrastructure endpoints depend on the

Azure Stack Hub service that uses the specific endpoint.

For the production environments, we recommend individual certificates are generated

for each endpoint and copied into the corresponding directory. For development

environments, certificates can be provided as a single wildcard certificate covering all

namespaces in the Subject and Subject Alternative Name (SAN) fields copied into all

directories. A single certificate covering all endpoints and services is an insecure posture

and hence development-only. Remember, both options require you to use wildcard

certificates for endpoints like acs and Key Vault where they're required.

Self-signed certificates aren't supported.

When deploying Azure Stack Hub in disconnected mode it is recommended to use

certificates issued by an enterprise certificate authority. This is important because

clients accessing Azure Stack Hub endpoints must be able to contact the certificate

revocation list (CRL).

７ Note

The presence of Intermediary Certificate Authorities in a certificate's chain-of-trusts

is supported.

Mandatory certificates

７ Note

Deployment

folder

Required certificate subject and

subject alternative names (SAN)

Scope (per

region)

Subdomain

namespace

Public Portal portal.<region>.<fqdn> Portals <region>.<fqdn>

Admin Portal adminportal.<region>.<fqdn> Portals <region>.<fqdn>

Azure Resource

Manager Public

management.<region>.<fqdn> Azure

Resource

Manager

<region>.<fqdn>

Azure Resource

Manager Admin

adminmanagement.<region>.<fqdn> Azure

Resource

Manager

<region>.<fqdn>

ACSBlob \*.blob.<region>.<fqdn>

(Wildcard SSL Certificate)

Blob Storage blob.<region>.

<fqdn>

ACSTable \*.table.<region>.<fqdn>

(Wildcard SSL Certificate)

Table Storage table.<region>.

<fqdn>

ACSQueue \*.queue.<region>.<fqdn>

(Wildcard SSL Certificate)

Queue

Storage

queue.<region>.

<fqdn>

KeyVault \*.vault.<region>.<fqdn>

(Wildcard SSL Certificate)

Key Vault vault.<region>.

<fqdn>

KeyVaultInternal \*.adminvault.<region>.<fqdn>

(Wildcard SSL Certificate)

Internal

Keyvault

adminvault.

<region>.<fqdn>

Admin Extension

Host

\*.adminhosting.<region>.<fqdn>

(Wildcard SSL Certificates)

Admin

Extension

Host

adminhosting.

<region>.<fqdn>

Public Extension

Host

\*.hosting.<region>.<fqdn> (Wildcard

SSL Certificates)

Public

Extension

Host

hosting.<region>.

<fqdn>

If you deploy Azure Stack Hub using the Azure AD deployment mode, you only need to

request the certificates listed in previous table. But, if you deploy Azure Stack Hub using

During deployment, you must copy certificates to the deployment folder that

matches the identity provider you're deploying against (Azure AD or AD FS). If you

use a single certificate for all endpoints, you must copy that certificate file into each

deployment folder as outlined in the following tables. The folder structure is prebuilt in the deployment virtual machine and can be found at:

C:\CloudDeployment\Setup\Certificates.

the AD FS deployment mode, you must also request the certificates described in the

following table:

Deployment

folder

Required certificate subject and subject

alternative names (SAN)

Scope (per

region)

Subdomain

namespace

ADFS adfs.<region>.<fqdn>

(SSL Certificate)

ADFS <region>.

<fqdn>

Graph graph.<region>.<fqdn>

(SSL Certificate)

Graph <region>.

<fqdn>

If you're planning to deploy Azure Stack Hub PaaS services (such as SQL, MySQL, App

Service, or Event Hubs) after Azure Stack Hub has been deployed and configured, you

must request additional certificates to cover the endpoints of the PaaS services.

The following table describes the endpoints and certificates required for resource

providers. You don't need to copy these certificates to the Azure Stack Hub deployment

folder. Instead, you provide these certificates during resource provider installation.

Scope

(per

region)

Certificate Required certificate subject and

Subject Alternative Names (SANs)

Subdomain namespace

App

Service

Web Traffic

Default SSL

Cert

\*.appservice.<region>.<fqdn>

\*.scm.appservice.<region>.<fqdn>

\*.sso.appservice.<region>.<fqdn>

(Multi Domain Wildcard SSL

Certificate )

appservice.<region>.

<fqdn>

scm.appservice.<region>.

<fqdn>

） Important

All the certificates listed in this section must have the same password.

Optional PaaS certificates

） Important

The certificates that you use for resource providers must have the same root

authority as those used for the global Azure Stack Hub endpoints.

1

Scope

(per

region)

Certificate Required certificate subject and

Subject Alternative Names (SANs)

Subdomain namespace

App

Service

API api.appservice.<region>.<fqdn>

(SSL Certificate )

appservice.<region>.

<fqdn>

scm.appservice.<region>.

<fqdn>

App

Service

FTP ftp.appservice.<region>.<fqdn>

(SSL Certificate )

appservice.<region>.

<fqdn>

scm.appservice.<region>.

<fqdn>

App

Service

SSO sso.appservice.<region>.<fqdn>

(SSL Certificate )

appservice.<region>.

<fqdn>

scm.appservice.<region>.

<fqdn>

Event

Hubs

SSL \*.eventhub.<region>.<fqdn>

(Wildcard SSL Certificate)

eventhub.<region>.

<fqdn>

SQL,

MySQL

SQL and

MySQL

\*.dbadapter.<region>.<fqdn>

(Wildcard SSL Certificate)

dbadapter.<region>.

<fqdn>

Requires one certificate with multiple wildcard subject alternative names. Multiple

wildcard SANs on a single certificate might not be supported by all public certificate

authorities.

A \*.appservice.<region>.<fqdn> wildcard certificate can't be used in place of these

three certificates (api.appservice.<region>.<fqdn>, ftp.appservice.<region>.<fqdn>, and

sso.appservice.<region>.<fqdn>. Appservice explicitly requires the use of separate

certificates for these endpoints.

Learn how to generate PKI certificates for Azure Stack Hub deployment.

2

2

2

1

2

Next steps

Generate certificate signing requests for

Azure Stack Hub

Article • 10/26/2022

You use the Azure Stack Hub Readiness Checker tool to create certificate signing

requests (CSRs) that are suitable for an Azure Stack Hub deployment, or for renewal of

certificates for an existing deployment. It's important to request, generate, and validate

certificates with enough lead time to test them before they're deployed.

The tool is used to request the following certificates, based on the Choose a CSR

certificate scenario selector at the top of this article:

Standard certificates for a new deployment: Choose New deployment using the

Choose a CSR certificate scenario selector at the top of this article.

Renewal certificates for an existing deployment: Choose Renewal using the Choose

a CSR certificate scenario selector at the top of this article.

Platform-as-a-service (PaaS) certificates: Can optionally be generated with both

standard and renewal certificates. See Azure Stack Hub public key infrastructure

(PKI) certificate requirements - optional PaaS certificates for more details.

Before you generate CSRs for PKI certificates for an Azure Stack Hub deployment, your

system must meet the following prerequisites:

You must be on a machine with Windows 10 or later, or Windows Server 2016 or

later.

Install the Azure Stack Hub Readiness checker tool from a PowerShell prompt

(5.1 or later) using the following cmdlet:

PowerShell

You'll need the following attributes for your certificate:

Region name

External fully qualified domain name (FQDN)

Subject

Prerequisites

Install-Module Microsoft.AzureStack.ReadinessChecker -Force -

AllowPrerelease

To prepare CSRs for new Azure Stack Hub PKI certificates, complete the following steps:

1. Open a PowerShell session on the machine where you installed the Readiness

Checker tool.

2. Declare the following variables:

PowerShell

Now generate the CSRs using the same PowerShell session. The instructions are specific

to the Subject format that you select below:

Generate CSRs for new deployment certificates

７ Note

Elevation is required to generate certificate signing requests. In restricted

environments where elevation is not possible, you can use this tool to generate

clear-text template files, which contain all the information that's required for Azure

Stack Hub external certificates. You then need to use these template files on an

elevated session to finish the public/private key pair generation. See below for

more details.

７ Note

<regionName>.<externalFQDN> forms the basis on which all external DNS

names in Azure Stack Hub are created. In the following example, the portal

would be portal.east.azurestack.contoso.com .

$outputDirectory = "$ENV:USERPROFILE\Documents\AzureStackCSR" # An

existing output directory

$IdentitySystem = "AAD" # Use "AAD" for Azure

Active Director, "ADFS" for Active Directory Federation Services

$regionName = 'east' # The region name for your

Azure Stack Hub deployment

$externalFQDN = 'azurestack.contoso.com' # The external FQDN for

your Azure Stack Hub deployment

Subject with no CN

７ Note

1. Declare a subject, for example:

PowerShell

2. Generate CSRs by completing one of the following:

For a production deployment environment, the first script will generate

CSRs for deployment certificates:

PowerShell

The second script, if desired, uses the -IncludeContainerRegistry and

will generate a CSR for Azure Container Registry at the same time as

CSRs for deployment certificates:

PowerShell

The third script will generate CSRs for any optional PaaS services you've

installed:

PowerShell

The first DNS name of the Azure Stack Hub service will be configured as the

CN field on the certificate request.

$subject = "C=US,ST=Washington,L=Redmond,O=Microsoft,OU=Azure Stack

Hub"

New-AzsHubDeploymentCertificateSigningRequest -RegionName

$regionName -FQDN $externalFQDN -subject $subject -

OutputRequestPath $OutputDirectory -IdentitySystem

$IdentitySystem

New-AzsHubDeploymentCertificateSigningRequest -RegionName

$regionName -FQDN $externalFQDN -subject $subject -

OutputRequestPath $OutputDirectory -IdentitySystem

$IdentitySystem -IncludeContainerRegistry

# App Services

New-AzsHubAppServicesCertificateSigningRequest -RegionName

$regionName -FQDN $externalFQDN -subject $subject -

OutputRequestPath $OutputDirectory

# DBAdapter (SQL/MySQL)

New-AzsHubDbAdapterCertificateSigningRequest -RegionName

$regionName -FQDN $externalFQDN -subject $subject -

For a low-privilege environment, to generate a clear-text certificate

template file with the necessary attributes declared, add the -

LowPrivilege parameter:

PowerShell

For a development and test environment, to generate a single CSR with

multiple-subject alternative names, add the -RequestType SingleCSR

parameter and value.

PowerShell

Complete the final steps:

1. Review the output:

PowerShell

OutputRequestPath $OutputDirectory

# EventHubs

New-AzsHubEventHubsCertificateSigningRequest -RegionName

$regionName -FQDN $externalFQDN -subject $subject -

OutputRequestPath $OutputDirectory

# Azure Container Registry

New-AzsHubAzureContainerRegistryCertificateSigningRequest -

RegionName $regionName -FQDN $externalFQDN -subject $subject -

OutputRequestPath $OutputDirectory

New-AzsHubDeploymentCertificateSigningRequest -RegionName

$regionName -FQDN $externalFQDN -subject $subject -

OutputRequestPath $OutputDirectory -IdentitySystem

$IdentitySystem -LowPrivilege

） Important

We do not recommend using this approach for production

environments.

New-AzsHubDeploymentCertificateSigningRequest -RegionName

$regionName -FQDN $externalFQDN -RequestType SingleCSR -

subject $subject -OutputRequestPath $OutputDirectory -

IdentitySystem $IdentitySystem

2. If the -LowPrivilege parameter was used, an .inf file was generated in the

C:\Users\username\Documents\AzureStackCSR subdirectory. For example:

C:\Users\username\Documents\AzureStackCSR\Deployment\_east\_azurestack\_contoso\_c

om\_SingleCSR\_CertRequest\_20200710165538\_ClearTextTemplate.inf

Copy the file to a system where elevation is allowed, then sign each request with

certreq by using the following syntax: certreq -new <example.inf> <example.req> .

Then complete the rest of the process on that elevated system, because it requires

matching the new certificate that's signed by the CA with its private key, which is

generated on the elevated system.

When you're ready, submit the generated .req file to your CA (either internal or public).

The directory specified by the $outputDirectory variable contains the CSRs that must be

submitted to a CA. The directory also contains, for your reference, a child directory

containing the .inf files to be used during certificate request generation. Be sure that

your CA generates certificates by using a generated request that meets the Azure Stack

Hub PKI requirements.

Once you receive your certificates back from your certificate authority, follow the steps

in Prepare Azure Stack Hub PKI certificates on the same system.

Starting Certificate Request Process for Deployment

CSR generating for following SAN(s):

\*.adminhosting.east.azurestack.contoso.com,\*.adminvault.east.azurestack

.contoso.com,\*.blob.east.azurestack.contoso.com,\*.hosting.east.azuresta

ck.contoso.com,\*.queue.east.azurestack.contoso.com,\*.table.east.azurest

ack.contoso.com,\*.vault.east.azurestack.contoso.com,adminmanagement.eas

t.azurestack.contoso.com,adminportal.east.azurestack.contoso.com,manage

ment.east.azurestack.contoso.com,portal.east.azurestack.contoso.com

Present this CSR to your Certificate Authority for Certificate

Generation:

C:\Users\username\Documents\AzureStackCSR\Deployment\_east\_azurestack\_co

ntoso\_com\_SingleCSR\_CertRequest\_20200710165538.req

Certreq.exe output: CertReq: Request Created

Next steps

Prepare Azure Stack Hub PKI certificates

for deployment or rotation

Article • 04/13/2023

The certificate files obtained from the certificate authority (CA) must be imported and

exported with properties matching Azure Stack Hub's certificate requirements.

In this article you learn how to import, package, and validate external certificates, to

prepare for Azure Stack Hub deployment or secrets rotation.

Your system should meet the following prerequisites before packaging PKI certificates

for an Azure Stack Hub deployment:

Certificates returned from Certificate Authority are stored in a single directory, in

.cer format (other configurable formats such as .cert, .sst, or .pfx).

Windows 10, or Windows Server 2016 or later.

Use the same system that generated the Certificate Signing Request (unless you're

targeting a certificate prepackaged into PFXs).

Use elevated PowerShell sessions.

Continue to the appropriate Prepare certificates (Azure Stack readiness checker) or

Prepare certificates (manual steps) section.

７ Note

This article pertains to the preparation of external certificates only, which are used

to secure endpoints on external infrastructure and services. Internal certificates are

managed separately, during the certificate rotation process.

７ Note

If you are installing Azure Container Registry (ACR), we recommend aligning the

expiration dates of your external ACR certificates with the expiration dates of your

other external Azure Stack Hub certificates. Additionally, we recommend protecting

your PFX for ACR with the same password that you use to protect your other

external certificate PFXs.

Prerequisites

Use these steps to package certificates using the Azure Stack readiness checker

PowerShell cmdlets:

1. Install the Azure Stack readiness checker module from a PowerShell prompt (5.1 or

above), by running the following cmdlet:

PowerShell

2. Specify the Path to the certificate files. For example:

PowerShell

3. Declare the pfxPassword. For example:

PowerShell

4. Declare the ExportPath where the resulting PFXs will be exported to. For example:

PowerShell

5. Convert certificates to Azure Stack Hub Certificates. For example:

PowerShell

6. Review the output:

PowerShell

Prepare certificates (Azure Stack readiness

checker)

Install-Module Microsoft.AzureStack.ReadinessChecker -Force -

AllowPrerelease

$Path = "$env:USERPROFILE\Documents\AzureStack"

$pfxPassword = Read-Host -AsSecureString -Prompt "PFX Password"

$ExportPath = "$env:USERPROFILE\Documents\AzureStack"

ConvertTo-AzsPFX -Path $Path -pfxPassword $pfxPassword -ExportPath

$ExportPath

ConvertTo-AzsPFX v1.2005.1286.272 started.

Stage 1: Scanning Certificates

Path: C:\Users\[\*redacted\*]\Documents\AzureStack Filter: CER

Certificate count: 11

adminmanagement\_east\_azurestack\_contoso\_com\_CertRequest\_20200710235648.

cer

adminportal\_east\_azurestack\_contoso\_com\_CertRequest\_20200710235645.cer

management\_east\_azurestack\_contoso\_com\_CertRequest\_20200710235644.cer

portal\_east\_azurestack\_contoso\_com\_CertRequest\_20200710235646.cer

wildcard\_adminhosting\_east\_azurestack\_contoso\_com\_CertRequest\_202007102

35649.cer

wildcard\_adminvault\_east\_azurestack\_contoso\_com\_CertRequest\_20200710235

642.cer

wildcard\_blob\_east\_azurestack\_contoso\_com\_CertRequest\_20200710235653.ce

r

wildcard\_hosting\_east\_azurestack\_contoso\_com\_CertRequest\_20200710235652

.cer

wildcard\_queue\_east\_azurestack\_contoso\_com\_CertRequest\_20200710235654.c

er

wildcard\_table\_east\_azurestack\_contoso\_com\_CertRequest\_20200710235650.c

er

wildcard\_vault\_east\_azurestack\_contoso\_com\_CertRequest\_20200710235647.c

er

Detected ExternalFQDN: east.azurestack.contoso.com

Stage 2: Exporting Certificates

east.azurestack.contoso.com\Deployment\ARM Admin\ARMAdmin.pfx

east.azurestack.contoso.com\Deployment\Admin Portal\AdminPortal.pfx

east.azurestack.contoso.com\Deployment\ARM Public\ARMPublic.pfx

east.azurestack.contoso.com\Deployment\Public

Portal\PublicPortal.pfx

east.azurestack.contoso.com\Deployment\Admin Extension

Host\AdminExtensionHost.pfx

east.azurestack.contoso.com\Deployment\KeyVaultInternal\KeyVaultInterna

l.pfx

east.azurestack.contoso.com\Deployment\ACSBlob\ACSBlob.pfx

east.azurestack.contoso.com\Deployment\Public Extension

Host\PublicExtensionHost.pfx

east.azurestack.contoso.com\Deployment\ACSQueue\ACSQueue.pfx

east.azurestack.contoso.com\Deployment\ACSTable\ACSTable.pfx

east.azurestack.contoso.com\Deployment\KeyVault\KeyVault.pfx

Following a successful validation certificates can be presented for Deployment or

Rotation without any additional steps.

Use these steps to package certificates for new Azure Stack Hub PKI certificates using

manual steps.

1. Copy the original certificate versions obtained from your CA of choice into a

directory on the deployment host.

Stage 3: Validating Certificates.

Validating east.azurestack.contoso.com-Deployment-AAD certificates in

C:\Users\

[\*redacted\*]\Documents\AzureStack\east.azurestack.contoso.com\Deploymen

t

Testing: KeyVaultInternal\KeyVaultInternal.pfx

Thumbprint: E86699\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*4617D6

PFX Encryption: OK

Expiry Date: OK

Signature Algorithm: OK

DNS Names: OK

Key Usage: OK

Key Length: OK

Parse PFX: OK

Private Key: OK

Cert Chain: OK

Chain Order: OK

Other Certificates: OK

Testing: ARM Public\ARMPublic.pfx

...

Log location (contains PII): C:\Users\

[\*redacted\*]\AppData\Local\Temp\AzsReadinessChecker\AzsReadinessChecker

.log

ConvertTo-AzsPFX Completed

７ Note

For additional usage use Get-help ConvertTo-AzsPFX -Full for further usage

such as disabling validation or filtering for different certificate formats.

Prepare certificates (manual steps)

Import the certificate

2. Right-click on the certificate and select Install Certificate or Install PFX, depending

on how the certificate was delivered from your CA.

3. In the Certificate Import Wizard, select Local Machine as the import location.

Select Next. On the following screen, select next again.

4. Choose Place all certificate in the following store and then select Enterprise Trust

as the location. Select OK to close the certificate store selection dialog box and

then select Next.

２ Warning

Don't copy files that have already been imported, exported, or altered in any

way from the files provided directly by the CA.

a. If you're importing a PFX, you'll be presented with an additional dialog. On the

Private key protection page, enter the password for your certificate files and then

enable the Mark this key as exportable. option, allowing you to back up or

transport your keys later. Select Next.

5. Select Finish to complete the import.

Open Certificate Manager MMC console and connect to the Local Machine certificate

store.

1. Open the Microsoft Management Console. To open the console in Windows 10,

right-click on the Start Menu, select Run, then type mmc and press enter.

2. Select File > Add/Remove Snap-In, then select Certificates and select Add.

７ Note

After you import a certificate for Azure Stack Hub, the private key of the certificate

is stored as a PKCS 12 file (PFX) on clustered storage.

Export the certificate

3. Select Computer account, then select Next. Select Local computer and then

Finish. Select OK to close the Add/Remove Snap-In page.

4. Browse to Certificates > Enterprise Trust > Certificate location. Verify that you see

your certificate on the right.

5. From the Certificate Manager Console taskbar, select Actions > All Tasks > Export.

Select Next.

6. Select Yes, Export the Private Key, and then select Next.

7. In the Export File Format section:

Select Include all certificates in the certificate if possible.

Select Export all Extended Properties.

Select Enable certificate privacy.

Select Next.

8. Select Password and provide a password for the certificates. Create a password

that meets the following password complexity requirements:

A minimum length of eight characters.

７ Note

Depending on how many Azure Stack Hub certificates you have, you may

need to complete this process more than once.

At least three of the following characters: uppercase letter, lowercase letter,

numbers from 0-9, special characters, alphabetical character that's not

uppercase or lowercase.

Make note of this password. You'll use it as a deployment parameter.

9. Select Next.

10. Choose a file name and location for the PFX file to export. Select Next.

11. Select Finish.

Validate PKI certificates

Next steps

Validate Azure Stack Hub PKI certificates

Article • 04/04/2023

The Azure Stack Hub Readiness Checker tool described in this article is available from

the PowerShell Gallery . Use the tool to validate that generated public key

infrastructure (PKI) certificates are suitable for pre-deployment. Validate certificates by

leaving enough time to test and reissue certificates if necessary.

The Readiness Checker tool performs the following certificate validations:

Parse PFX

Checks for valid PFX file, correct password, and whether the public information is

protected by the password.

Expiry Date

Checks for minimum validity of seven days.

Signature algorithm

Checks that the signature algorithm isn't SHA1.

Private Key

Checks that the private key is present and is exported with the local machine

attribute.

Cert chain

Checks certificate chain is intact including a check for self-signed certificates.

DNS names

Checks the SAN contains relevant DNS names for each endpoint or if a supporting

wildcard is present.

Key usage

Checks if the key usage contains a digital signature and key encipherment and

checks if enhanced key usage contains server authentication and client

authentication.

Key size

Checks if the key size is 2048 or larger.

Chain order

Checks the order of the other certificates validating that the order is correct.

Other certificates

Ensure no other certificates have been packaged in PFX other than the relevant leaf

certificate and its chain.

） Important

Your system should meet the following prerequisites before validating PKI certificates

for an Azure Stack Hub deployment:

Microsoft Azure Stack Hub Readiness Checker.

SSL Certificate(s) exported following the preparation instructions.

DeploymentData.json.

Windows 10 or Windows Server 2016.

Use these steps to validate the Azure Stack Hub PKI certificates for deployment and

secret rotation:

1. Install AzsReadinessChecker from a PowerShell prompt (5.1 or above) by running

the following cmdlet:

PowerShell

2. Create the certificate directory structure. In the example below, you can change

<C:\Certificates\Deployment> to a new directory path of your choice.

PowerShell

The PKI certificate is a PFX file and password should be treated as sensitive

information.

Prerequisites

Perform core services certificate validation

Install-Module Microsoft.AzureStack.ReadinessChecker -Force -

AllowPrerelease

New-Item C:\Certificates\Deployment -ItemType Directory

$directories = 'ACSBlob', 'ACSQueue', 'ACSTable', 'Admin Extension

Host', 'Admin Portal', 'ARM Admin', 'ARM Public', 'KeyVault',

'KeyVaultInternal', 'Public Extension Host', 'Public Portal'

$destination = 'C:\Certificates\Deployment'

$directories | % { New-Item -Path (Join-Path $destination $PSITEM) -

ItemType Directory -Force}

７ Note

Place your certificate(s) in the appropriate directories created in the previous

step. For example:

C:\Certificates\Deployment\ACSBlob\CustomerCertificate.pfx

C:\Certificates\Deployment\Admin Portal\CustomerCertificate.pfx

C:\Certificates\Deployment\ARM Admin\CustomerCertificate.pfx

3. In the PowerShell window, change the values of RegionName , FQDN and

IdentitySystem appropriate to the Azure Stack Hub environment and run the

following cmdlet:

PowerShell

4. Check the output and ensure that all certificates pass all tests. For example:

shell

AD FS and Graph are required if you're using AD FS as your identity system.

For example:

PowerShell

$directories = 'ACSBlob', 'ACSQueue', 'ACSTable', 'ADFS', 'Admin

Extension Host', 'Admin Portal', 'ARM Admin', 'ARM Public',

'Graph', 'KeyVault', 'KeyVaultInternal', 'Public Extension Host',

'Public Portal'

$pfxPassword = Read-Host -Prompt "Enter PFX Password" -AsSecureString

Invoke-AzsHubDeploymentCertificateValidation -CertificatePath

C:\Certificates\Deployment -pfxPassword $pfxPassword -RegionName east -

FQDN azurestack.contoso.com -IdentitySystem AAD

Invoke-AzsHubDeploymentCertificateValidation v1.2005.1286.272 started.

Testing: KeyVaultInternal\KeyVaultInternal.pfx

Thumbprint: E86699\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*4617D6

PFX Encryption: OK

Expiry Date: OK

Signature Algorithm: OK

DNS Names: OK

Key Usage: OK

Key Length: OK

Parse PFX: OK

Private Key: OK

Cert Chain: OK

Chain Order: OK

Other Certificates: OK

Testing: ARM Public\ARMPublic.pfx

Thumbprint: 8DC4D9\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*69DBAA

To validate certificates for other Azure Stack Hub services, change the value for -

CertificatePath . For example:

PowerShell

PFX Encryption: OK

Expiry Date: OK

Signature Algorithm: OK

DNS Names: OK

Key Usage: OK

Key Length: OK

Parse PFX: OK

Private Key: OK

Cert Chain: OK

Chain Order: OK

Other Certificates: OK

Testing: Admin Portal\AdminPortal.pfx

Thumbprint: 6F9055\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*4AC0EA

PFX Encryption: OK

Expiry Date: OK

Signature Algorithm: OK

DNS Names: OK

Key Usage: OK

Key Length: OK

Parse PFX: OK

Private Key: OK

Cert Chain: OK

Chain Order: OK

Other Certificates: OK

Testing: Public Portal\PublicPortal.pfx

Log location (contains PII): C:\Users\

[\*redacted\*]\AppData\Local\Temp\AzsReadinessChecker\AzsReadinessChecker

.log

Report location (contains PII): C:\Users\

[\*redacted\*]\AppData\Local\Temp\AzsReadinessChecker\AzsReadinessChecker

Report.json

Invoke-AzsHubDeploymentCertificateValidation Completed

# App Services

Invoke-AzsHubAppServicesCertificateValidation -CertificatePath

C:\Certificates\AppServices -pfxPassword $pfxPassword -RegionName east

-FQDN azurestack.contoso.com

# DBAdapter

Invoke-AzsHubDBAdapterCertificateValidation -CertificatePath

C:\Certificates\DBAdapter -pfxPassword $pfxPassword -RegionName east -

FQDN azurestack.contoso.com

# EventHubs

Invoke-AzsHubEventHubsCertificateValidation -CertificatePath

Each folder should contain a single PFX file for the certificate type. If a certificate

type has multi-certificate requirements, nested folders for each individual

certificate are expected and name-sensitive. The following code shows an example

folder/certificate structure for all certificate types, and the appropriate value for -

CertificatePath .

shell

C:\Certificates\EventHubs -pfxPassword $pfxPassword -RegionName east -

FQDN azurestack.contoso.com

C:\>tree c:\SecretStore /A /F

Folder PATH listing

Volume serial number is 85AE-DF2E

C:\SECRETSTORE

\---AzureStack

+---CertificateRequests

\---Certificates

+---AppServices # Invoke-AzsCertificateValidation `

| +---API # -CertificatePath

C:\Certificates\AppServices

| | api.pfx

| |

| +---DefaultDomain

| | wappsvc.pfx

| |

| +---Identity

| | sso.pfx

| |

| \---Publishing

| ftp.pfx

|

+---DBAdapter # Invoke-AzsCertificateValidation `

| dbadapter.pfx # -CertificatePath

C:\Certificates\DBAdapter

|

|

+---Deployment # Invoke-AzsCertificateValidation `

| +---ACSBlob # -CertificatePath

C:\Certificates\Deployment

| | acsblob.pfx

| |

| +---ACSQueue

| | acsqueue.pfx

./. ./. ./. ./. ./. ./. ./. <- Deployment certificate

tree trimmed.

| \---Public Portal

| portal.pfx

|

\---EventHubs # Invoke-AzsCertificateValidation `

eventhubs.pfx # -CertificatePath

Symptom: Tests are skipped

Cause: AzsReadinessChecker skips certain tests if a dependency isn't met:

Other certificates are skipped if certificate chain fails.

shell

Resolution: Follow the tool's guidance in the details section under each set of tests for

each certificate.

Symptom: HTTP CRL checking fails despite having an HTTP CDP written to x509

extensions.

Cause: Currently, the AzsReadinessChecker can't check for HTTP CDP in some

languages.

C:\Certificates\EventHubs

Known issues

Testing: ACSBlob\singlewildcard.pfx

Read PFX: OK

Signature Algorithm: OK

Private Key: OK

Cert Chain: OK

DNS Names: Fail

Key Usage: OK

Key Size: OK

Chain Order: OK

Other Certificates: Skipped

Details:

The certificate records '\*.east.azurestack.contoso.com' do not contain

a record that is valid for '\*.blob.east.azurestack.contoso.com'. Please

refer to the documentation for how to create the required certificate

file.

The other certificates check was skipped because cert chain and/or DNS

names failed. Follow the guidance to remediate those issues and

recheck.

Log location (contains PII):

C:\Users\username\AppData\Local\Temp\AzsReadinessChecker\AzsReadinessCh

ecker.log

Report location (contains PII):

C:\Users\username\AppData\Local\Temp\AzsReadinessChecker\AzsReadinessCh

eckerReport.json

Invoke-AzsCertificateValidation Completed

Resolution: Run validation with OS language set to EN-US.

Directory Certificate

ACSBlob wildcard\_blob\_<region>\_<externalFQDN>

ACSQueue wildcard\_queue\_<region>\_<externalFQDN>

ACSTable wildcard\_table\_<region>\_<externalFQDN>

Admin Extension Host wildcard\_adminhosting\_<region>\_<externalFQDN>

Admin Portal adminportal\_<region>\_<externalFQDN>

ARM Admin adminmanagement\_<region>\_<externalFQDN>

ARM Public management\_<region>\_<externalFQDN>

KeyVault wildcard\_vault\_<region>\_<externalFQDN>

KeyVaultInternal wildcard\_adminvault\_<region>\_<externalFQDN>

Public Extension Host wildcard\_hosting\_<region>\_<externalFQDN>

Public Portal portal\_<region>\_<externalFQDN>

Once your certificates are validated by AzsReadinessChecker, you're ready to use them

for Azure Stack Hub deployment or post-deployment secret rotation.

For deployment, securely transfer your certificates to your deployment engineer so

that they can copy them onto the deployment virtual machine host as specified in

Azure Stack Hub PKI requirements - Mandatory certificates.

For secret rotation, see Rotate secrets in Azure Stack Hub. Rotation of value-add

resource provider certificates is covered in the Rotate external secrets section.

Certificates

Next steps

Fix common issues with Azure Stack

Hub PKI certificates

Article • 07/29/2022

The information in this article helps you understand and resolve common issues with

Azure Stack Hub PKI certificates. You can discover issues when you use the Azure Stack

Hub Readiness Checker tool to validate Azure Stack Hub PKI certificates. The tool checks

if the certificates meet the PKI requirements of an Azure Stack Hub deployment and

Azure Stack Hub secret rotation, and then logs the results to a report.json file.

Issue - Certificate does not contain HTTP CRL in CDP Extension.

Fix - This is a non-blocking issue. Azure Stack requires HTTP CRL for revocation checking

as per Azure Stack Hub public key infrastructure (PKI) certificate requirements. A HTTP

CRL was not detected on the certificate. To ensure certificate revocation checking works,

the Certificate Authority should issue a certificate with a HTTP CRL in the CDP extension.

Issue - Cannot connect to HTTP CRL in CDP Extension.

Fix - This is a blocking issue. Azure Stack requires connectivity to a HTTP CRL for

revocation checking as per Publishing Azure Stack Hub Ports and URLs (outbound).

Issue - PFX encryption isn't TripleDES-SHA1.

Fix - Export PFX files with TripleDES-SHA1 encryption. This is the default encryption for

all Windows 10 clients when exporting from certificate snap-in or using ExportPFXCertificate .

Warning - Password only protects the private information in the certificate.

Fix - Export PFX files with the optional setting for Enable certificate privacy.

HTTP CRL - Warning

HTTP CRL - Fail

PFX Encryption

Read PFX

Issue - PFX file invalid.

Fix - Re-export the certificate using the steps in Prepare Azure Stack Hub PKI certificates

for deployment.

Issue - Signature algorithm is SHA1.

Fix - Use the steps in Azure Stack Hub certificates signing request generation to

regenerate the certificate signing request (CSR) with the signature algorithm of SHA256.

Then resubmit the CSR to the certificate authority to reissue the certificate.

Issue - The private key is missing or doesn't contain the local machine attribute.

Fix - From the computer that generated the CSR, re-export the certificate using the

steps in Prepare Azure Stack Hub PKI certificates for deployment. These steps include

exporting from the local machine certificate store.

Issue - Certificate chain isn't complete.

Fix - Certificates should contain a complete certificate chain. Re-export the certificate

using the steps in Prepare Azure Stack Hub PKI certificates for deployment and select

the option Include all certificates in the certification path if possible.

Issue - The DNSNameList on the certificate doesn't contain the Azure Stack Hub service

endpoint name or a valid wildcard match. Wildcard matches are only valid for the leftmost namespace of the DNS name. For example, \*.region.domain.com is only valid for

portal.region.domain.com , not \*.table.region.domain.com .

Fix - Use the steps in Azure Stack Hub certificates signing request generation to

regenerate the CSR with the correct DNS names to support Azure Stack Hub endpoints.

Resubmit the CSR to a certificate authority. Then follow the steps in Prepare Azure Stack

Hub PKI certificates for deployment to export the certificate from the machine that

generated the CSR.

Signature algorithm

Private key

Certificate chain

DNS names

Issue - Key usage is missing digital signature or key encipherment, or enhanced key

usage is missing server authentication or client authentication.

Fix - Use the steps in Azure Stack Hub certificates signing request generation to

regenerate the CSR with the correct key usage attributes. Resubmit the CSR to the

certificate authority and confirm that a certificate template isn't overwriting the key

usage in the request.

Issue - Key size is smaller than 2048.

Fix - Use the steps in Azure Stack Hub certificates signing request generation to

regenerate the CSR with the correct key length (2048), and then resubmit the CSR to the

certificate authority.

Issue - The order of the certificate chain is incorrect.

Fix - Re-export the certificate using the steps in Prepare Azure Stack Hub PKI certificates

for deployment and select the option Include all certificates in the certification path if

possible. Ensure that only the leaf certificate is selected for export.

Issue - The PFX package contains certificates that aren't the leaf certificate or part of the

certificate chain.

Fix - Re-export the certificate using the steps in Prepare Azure Stack Hub PKI certificates

for deployment, and select the option Include all certificates in the certification path if

possible. Ensure that only the leaf certificate is selected for export.

The AzsReadinessChecker tool contains a helper cmdlet called Repair-AzsPfxCertificate,

which can import and then export a PFX file to fix common packaging issues, including:

PFX encryption isn't TripleDES-SHA1.

Key usage

Key size

Chain order

Other certificates

Fix common packaging issues

Private key is missing local machine attribute.

Certificate chain is incomplete or wrong. The local machine must contain the

certificate chain if the PFX package doesn't.

Other certificates

Repair-AzsPfxCertificate can't help if you need to generate a new CSR and reissue a

certificate.

The following prerequisites must be in place on the computer on which the tool runs:

Windows 10 or Windows Server 2016, with internet connectivity.

PowerShell 5.1 or later. To check your version, run the following PowerShell cmdlet

and then review the Major and Minor versions:

PowerShell

Configure PowerShell for Azure Stack Hub.

Download the latest version of the Azure Stack Hub readiness checker tool.

1. On a computer that meets the prerequisites, open an elevated PowerShell prompt,

and then run the following command to install the Azure Stack Hub readiness

checker:

PowerShell

2. From the PowerShell prompt, run the following cmdlet to set the PFX password.

Enter the password when prompted:

PowerShell

Prerequisites

$PSVersionTable.PSVersion

Import and export an existing PFX File

Install-Module Microsoft.AzureStack.ReadinessChecker -Force -

AllowPrerelease

$password = Read-Host -Prompt "Enter password" -AsSecureString

3. From the PowerShell prompt, run the following command to export a new PFX file:

For -PfxPath , specify the path to the PFX file you're working with. In the

following example, the path is .\certificates\ssl.pfx .

For -ExportPFXPath , specify the location and name of the PFX file for export.

In the following example, the path is .\certificates\ssl\_new.pfx :

PowerShell

4. After the tool completes, review the output for success:

shell

Learn more about Azure Stack Hub security

Repair-AzsPfxCertificate -PfxPassword $password -PfxPath

.\certificates\ssl.pfx -ExportPFXPath .\certificates\ssl\_new.pfx

Repair-AzsPfxCertificate v1.1809.1005.1 started.

Starting Azure Stack Hub Certificate Import/Export

Importing PFX .\certificates\ssl.pfx into Local Machine Store

Exporting certificate to .\certificates\ssl\_new.pfx

Export complete. Removing certificate from the local machine store.

Removal complete.

Log location (contains PII):

C:\Users\username\AppData\Local\Temp\AzsReadinessChecker\AzsReadinessCh

ecker.log

Repair-AzsPfxCertificate Completed

Next steps

Deployment network traffic

Article • 07/29/2022

Understanding network traffic during Azure Stack Hub deployment will help make the

deployment successful. This article walks you through the network traffic flow during the

deployment process so you know what to expect.

This illustration shows all the components and connections involved in the deployment

process:

The Azure Stack Hub solution includes a group of servers that are used to host Azure

Stack Hub components and an extra server called the Hardware Lifecycle Host (HLH).

This server is used to deploy and manage the lifecycle of your solution and hosts the

Deployment VM (DVM) during deployment.

Azure Stack Hub solution providers may provision additional management VMs. Confirm

with the solution provider before making any changes to management VMs from a

solution provider.

７ Note

This article describes the requirements for a connected deployment. To learn about

other deployment methods, see Azure Stack Hub deployment connection models.

The Deployment VM

Before deployment starts, there are some minimum requirements that can be validated

by your OEM to ensure deployment completes successfully:

Certificates.

Azure subscription. You may need to check your subscription.

Internet access.

DNS.

NTP.

The DVM is configured with an IP from the BMC network and requires network access to

the internet. Although not all of the BMC network components require external routing

or access to the internet, some OEM-specific components using IPs from this network

might also require it.

During deployment, the DVM authenticates against Azure Active Directory (Azure AD)

using an Azure account from your subscription. In order to do so, the DVM requires

internet access to a list of specific ports and URLs. The DVM will utilize a DNS server to

forward DNS requests made by internal components to external URLs. The internal DNS

forwards these requests to the DNS forwarder address that you provide to the OEM

before deployment. The same is true for the NTP server: a reliable Time Server is

required to maintain consistency and time synchronization for all Azure Stack Hub

components.

The internet access required by the DVM during deployment is outbound only, no

inbound calls are made during deployment. Keep in mind that it uses its IP as source

and that Azure Stack Hub doesn't support proxy configurations. Therefore, if necessary,

you need to provide a transparent proxy or NAT to access the internet. During

deployment, some internal components will start accessing the internet through the

external network using public VIPs. After deployment completes, all communication

between Azure and Azure Stack Hub is made through the external network using public

VIPs.

Deployment requirements

７ Note

This article focuses on the last three requirements. For more information on the

first two, see the links above.

About deployment network traffic

Network configurations on Azure Stack Hub switches contain access control lists (ACLs)

that restrict traffic between certain network sources and destinations. The DVM is the

only component with unrestricted access; even the HLH is restricted. You can ask your

OEM about customization options to ease management and access from your networks.

Because of these ACLs, it's important to avoid changing the DNS and NTP server

addresses at deployment time. If you do so, you need to reconfigure all of the switches

for the solution.

After deployment is completed, the provided DNS and NTP server addresses will

continue to be used by the system's components through the SDN using the external

network. For example, if you check DNS requests after deployment is completed, the

source will change from the DVM IP to a public VIP.

Validate Azure registration

Next steps

Validate Azure registration

Article • 07/29/2022

Use the Azure Stack Hub Readiness Checker tool (AzsReadinessChecker) to validate that

your Azure subscription is ready to use with Azure Stack Hub before you begin an Azure

Stack Hub deployment. The readiness checker validates that:

The Azure subscription you use is a supported type. Subscriptions must be a Cloud

Solution Provider (CSP) or Enterprise Agreement (EA).

The account you use to register your subscription with Azure can sign in to Azure

and is a subscription owner.

For more information about Azure Stack Hub registration, see Register Azure Stack Hub

with Azure.

Download the latest version of AzsReadinessChecker from the PowerShell Gallery .

The following prerequisites are required:

You will need to have the Az PowerShell modules installed. For instructions, see

Install PowerShell Az preview module.

Identify the username and password for an account that's an owner for the

Azure subscription you'll use with Azure Stack Hub.

Identify the subscription ID for the Azure subscription you'll use.

Get the Readiness Checker tool

Install and configure

Az PowerShell

Prerequisites

Az PowerShell modules

Azure Active Directory (AAD) environment

1. Open an elevated PowerShell prompt, and then run the following command to

install AzsReadinessChecker:

PowerShell

2. From the PowerShell prompt, run the following command to set

$subscriptionID as the Azure subscription to use. Replace xxxxxxxx-xxxxxxxx-xxxx-xxxxxxxxxxxx with your own subscription ID:

PowerShell

3. From the PowerShell prompt, run the following command:

PowerShell

4. From the PowerShell prompt, run the following command to start validation of

your subscription. Provide your Azure AD administrator and your Azure AD

tenant name:

PowerShell

5. After the tool runs, review the output. Confirm the status is correct for both

sign-in and the registration requirements. Successful validation output

appears similar to the following example:

PowerShell

Steps to validate the Azure registration

Install-Module -Name Az.BootStrapper -Force -AllowPrerelease

Install-AzProfile -Profile 2020-09-01-hybrid -Force

Install-Module -Name Microsoft.AzureStack.ReadinessChecker

$subscriptionID = "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

Connect-AzAccount -subscription $subscriptionID

Invoke-AzsRegistrationValidation -RegistrationSubscriptionID

$subscriptionID

Invoke-AzsRegistrationValidation v1.2100.1448.484 started.

Checking Registration Requirements: OK

Log location (contains PII): C:\Users\

[\*redacted\*]\AppData\Local\Temp\AzsReadinessChecker\AzsReadinessChe

Each time validation runs, it logs results to AzsReadinessChecker.log and

AzsReadinessCheckerReport.json. The location of these files displays along with the

validation results in PowerShell.

These files can help you share validation status before you deploy Azure Stack Hub or

investigate validation problems. Both files persist the results of each subsequent

validation check. The report provides your deployment team confirmation of the identity

configuration. The log file can help your deployment or support team investigate

validation issues.

By default, both files are written to

C:\Users\username\AppData\Local\Temp\AzsReadinessChecker\AzsReadinessCheckerReport

.json .

Use the -OutputPath <path> parameter at the end of the run command line to

specify a different report location.

Use the -CleanReport parameter at the end of the run command to clear

information about previous runs of the tool from

AzsReadinessCheckerReport.json.

For more information, see Azure Stack Hub validation report.

If a validation check fails, details about the failure display in the PowerShell window. The

tool also logs information to the AzsReadinessChecker.log file.

The following examples provide more information about common validation failures.

shell

cker.log

Report location (contains PII): C:\Users\

[\*redacted\*]\AppData\Local\Temp\AzsReadinessChecker\AzsReadinessChe

ckerReport.json

Invoke-AzsRegistrationValidation Completed

Report and log file

Validation failures

User must be an owner of the subscription

Cause - The account is not an administrator of the Azure subscription.

Resolution - Use an account that is an administrator of the Azure subscription that will

be billed for usage from the Azure Stack Hub deployment.

shell

Cause - The account can't sign in because the password is either expired or temporary.

Resolution - In PowerShell, run the following command and follow the prompts to reset

the password.

Invoke-AzsRegistrationValidation v1.1809.1005.1 started.

Checking Registration Requirements: Fail

Error Details for registration account admin@contoso.onmicrosoft.com:

The user admin@contoso.onmicrosoft.com is role(s) Reader for subscription

3f961d1c-d1fb-40c3-99ba-44524b56df2d. User must be an owner of the

subscription to be used for registration.

Additional help URL https://aka.ms/AzsRemediateRegistration

Log location (contains PII):

C:\Users\username\AppData\Local\Temp\AzsReadinessChecker\AzsReadinessChecker

.log

Report location (contains PII):

C:\Users\username\AppData\Local\Temp\AzsReadinessChecker\AzsReadinessChecker

Report.json

Invoke-AzsRegistrationValidation Completed

Expired or temporary password

Invoke-AzsRegistrationValidation v1.1809.1005.1 started.

Checking Registration Requirements: Fail

Error Details for registration account admin@contoso.onmicrosoft.com:

Checking Registration failed with: Retrieving TenantId for subscription

[subscription ID] using account admin@contoso.onmicrosoft.com failed with

AADSTS50055: Force Change Password.

Trace ID: [Trace ID]

Correlation ID: [Correlation ID]

Timestamp: 2018-10-22 11:16:56Z: The remote server returned an error: (401)

Unauthorized.

Log location (contains PII):

C:\Users\username\AppData\Local\Temp\AzsReadinessChecker\AzsReadinessChecker

.log

Report location (contains PII):

C:\Users\username\AppData\Local\Temp\AzsReadinessChecker\AzsReadinessChecker

Report.json

Invoke-AzsRegistrationValidation Completed

PowerShell

Another way is to sign in to the Azure portal as the account owner, and the user will

be forced to change the password.

shell

Cause - The account can't sign in to the specified Azure AD environment. In this

example, AzureChinaCloud is specified as the AzureEnvironment.

Resolution - Confirm that the account is valid for the specified Azure environment. In

PowerShell, run the following command to verify the account is valid for a specific

environment:

PowerShell

Validate Azure identity

View the readiness report

General Azure Stack Hub integration considerations

Login-AzureRMAccount

Unknown user type

Invoke-AzsRegistrationValidation v1.1809.1005.1 started.

Checking Registration Requirements: Fail

Error Details for registration account admin@contoso.onmicrosoft.com:

Checking Registration failed with: Retrieving TenantId for subscription

<subscription ID> using <account> failed with unknown\_user\_type: Unknown

User Type

Log location (contains PII):

C:\Users\username\AppData\Local\Temp\AzsReadinessChecker\AzsReadinessChecker

.log

Report location (contains PII):

C:\Users\username\AppData\Local\Temp\AzsReadinessChecker\AzsReadinessChecker

Report.json

Invoke-AzsRegistrationValidation Completed

Login-AzureRmAccount -EnvironmentName AzureChinaCloud

Next Steps

Azure Stack Hub validation report

Article • 07/29/2022

Use the Azure Stack Hub Readiness Checker tool to run validations that support

deployment and servicing of an Azure Stack Hub environment. The tool writes results to

a .json report file. The report displays detailed and summarized data about the state of

prerequisites for deployment of Azure Stack Hub. The report also displays information

about secrets rotation for existing Azure Stack Hub deployments.

When the tool runs, it logs results to AzsReadinessCheckerReport.json. The tool also

creates a log named AzsReadinessChecker.log. The location of these files displays along

with the validation results in PowerShell:

Both files persist the results of subsequent validation checks when run on the same

computer. For example, the tool can be run to validate certificates, run again to validate

Azure identity, and then a third time to validate registration. The results of all three

validations are available in the resulting .json report.

By default, both files are written to

C:\Users\username\AppData\Local\Temp\AzsReadinessChecker\AzsReadinessCheckerReport

.json .

Use the -OutputPath <path> parameter at the end of the command line to specify

a different report location.

Use the -CleanReport parameter at the end of the command line to clear

information about previous runs of the tool from

AzsReadinessCheckerReport.json.

To view the report in PowerShell, supply the path to the report as a value for -

ReportPath . This command displays the contents of the report and identifies validations

Where to find the report

View the report

that don't yet have results.

For example, to view the report from a PowerShell prompt that's open to the location

where the report is located, run the following command:

PowerShell

The output is similar to the following example:

shell

Read-AzsReadinessReport -ReportPath .\AzsReadinessReport.json

Reading All Validation(s) from Report C:\ContosoAzsReadinessCheckerReport.json

############### Certificate Validation Summary ###############

Certificate Validation results not available.

############### Registration Validation Summary ###############

Azure Registration Validation results not available.

############### Azure Identity Results ###############

Test : ServiceAdministrator

Result : OK

AAD Service Admin : admin@contoso.onmicrosoft.com

Azure Environment : AzureCloud

Azure Active Directory Tenant : contoso.onmicrosoft.com

Error Details :

############### Azure Identity Validation Summary ###############

Azure Identity Validation found no errors or warnings.

############### Azure Stack Hub Graph Validation Summary ###############

Azure Stack Hub Graph Validation results not available.

############### Azure Stack Hub ADFS Validation Summary ###############

Azure Stack Hub ADFS Validation results not available.

############### AzsReadiness Job Summary ###############

Index : 0

Operations :

StartTime : 2018/10/22 14:24:16

EndTime : 2018/10/22 14:24:19

To view a summary of the report, you can add the -summary parameter to the end of the

PowerShell command. For example:

PowerShell

The summary shows validations that don't have results, and indicates pass or fail for

validations that are complete. The output is similar to the following example:

shell

To view a report that is filtered on a single type of validation, use the -ReportSections

parameter with one of the following values:

Duration : 3

PSBoundParameters :

View the report summary

Read-AzsReadinessReport -ReportPath .\Contoso-AzsReadinessReport.json -

summary

Reading All Validation(s) from Report C:\ContosoAzsReadinessCheckerReport.json

############### Certificate Validation Summary ###############

Certificate Validation found no errors or warnings.

############### Registration Validation Summary ###############

Registration Validation found no errors or warnings.

############### Azure Identity Validation Summary ###############

Azure Identity Validation found no errors or warnings.

############### Azure Stack Hub Graph Validation Summary ###############

Azure Stack Hub Graph Validation results not available.

############### Azure Stack Hub ADFS Validation Summary ###############

Azure Stack Hub ADFS Validation results not available.

View a filtered report

Certificate

AzureRegistration

AzureIdentity

Graph

ADFS

Jobs

All

For example, to view the report summary for certificates only, use the following

PowerShell command line:

PowerShell

Read-AzsReadinessReport -ReportPath .\Contoso-AzsReadinessReport.json -

ReportSections Certificate - Summary

Integrate external monitoring solution

with Azure Stack Hub

Article • 07/29/2022

For external monitoring of the Azure Stack Hub infrastructure, you need to monitor the

Azure Stack Hub software, the physical computers, and the physical network switches.

Each of these areas offers a method to retrieve health and alert information:

Azure Stack Hub software offers a REST-based API to retrieve health and alerts. The

use of software-defined technologies such as Storage Spaces Direct, storage

health, and alerts are part of software monitoring.

Physical computers can make health and alert information available via the

baseboard management controllers (BMCs).

Physical network devices can make health and alert information available via the

SNMP protocol.

Each Azure Stack Hub solution ships with a hardware lifecycle host. This host runs the

original equipment manufacturer (OEM) hardware vendor's monitoring software for the

physical servers and network devices. Check with your OEM provider if their monitoring

solutions can integrate with existing monitoring solutions in your datacenter.

The following diagram shows traffic flow between an Azure Stack Hub integrated

system, the hardware lifecycle host, an external monitoring solution, and an external

ticketing/data collection system.

） Important

The external monitoring solution you use must be agentless. You can't install thirdparty agents inside Azure Stack Hub components.

This article explains how to integrate Azure Stack Hub with external monitoring

solutions such as System Center Operations Manager and Nagios. It also includes how

to work with alerts programmatically by using PowerShell or through REST API calls.

You can use Operations Manager for external monitoring of Azure Stack Hub. The

System Center Management Pack for Microsoft Azure Stack Hub enables you to monitor

multiple Azure Stack Hub deployments with a single Operations Manager instance. The

management pack uses the health resource provider and update resource provider REST

APIs to communicate with Azure Stack Hub. If you plan to bypass the OEM monitoring

software that's running on the hardware lifecycle host, you can install vendor

management packs to monitor physical servers. You can also use Operations Manager

network device discovery to monitor network switches.

The management pack for Azure Stack Hub provides the following capabilities:

You can manage multiple Azure Stack Hub deployments.

There's support for Azure Active Directory (Azure AD) and Active Directory

Federation Services (AD FS).

７ Note

External monitoring integration directly with physical servers isn't allowed and

actively blocked by Access Control Lists (ACLs). External monitoring integration

directly with physical network devices is supported. Check with your OEM provider

on how to enable this feature.

Integrate with Operations Manager

You can retrieve and close alerts.

There's a health and a capacity dashboard.

Includes Auto Maintenance Mode detection for when patch and update (P&U) is in

progress.

Includes Force Update tasks for deployment and region.

You can add custom information to a region.

Supports notification and reporting.

To download the System Center Management Pack and the associated user guide, see

Download System Center Management Pack for Microsoft Azure Stack Hub . You can

also download it directly from Operations Manager.

For a ticketing solution, you can integrate Operations Manager with System Center

Service Manager. The integrated product connector enables bidirectional

communication that allows you to close an alert in Azure Stack Hub and Operations

Manager after you resolve a service request in Service Manager.

The following diagram shows integration of Azure Stack Hub with an existing System

Center deployment. You can automate Service Manager further with System Center

Orchestrator or Service Management Automation (SMA) to run operations in Azure

Stack Hub.

You can set up and configure the Nagios Plugin for Microsoft Azure Stack Hub.

A Nagios monitoring plugin was developed together with partner Cloudbase Solutions,

which is available under the permissive free software license - MIT (Massachusetts

Institute of Technology).

The plugin is written in Python and leverages the health resource provider REST API. It

offers basic functionality to retrieve and close alerts in Azure Stack Hub. Like the System

Center management pack, it enables you to add multiple Azure Stack Hub deployments

and to send notifications.

Integrate with Nagios

With Version 1.2 the Azure Stack Hub - Nagios plugin leverages the Microsoft ADAL

library and supports authentication using Service Principal with a secret or certificate.

Also, the configuration has been simplified using a single configuration file with new

parameters. It now supports Azure Stack Hub deployments using Azure AD and AD FS

as the identity system.

The plugin works with Nagios 4x and XI. To download the plugin, see Monitoring Azure

Stack Hub Alerts . The download site also includes installation and configuration

details.

1. Minimum Nagios Version is 4.x

2. Microsoft Azure Active Directory Python library. This library can be installed using

Python PIP.

Bash

This section describes how to install the Azure Stack Hub plugin assuming a default

installation of Nagios.

The plugin package contains the following files:

） Important

AD FS only supports interactive sign-in sessions. If you require a non-interactive

sign-in for an automated scenario, you must use a SPN.

Requirements for Nagios

sudo pip install adal pyyaml six

Install plugin

azurestack\_plugin.py

azurestack\_handler.sh

samples/etc/azurestack.cfg

samples/etc/azurestack\_commands.cfg

samples/etc/azurestack\_contacts.cfg

samples/etc/azurestack\_hosts.cfg

samples/etc/azurestack\_services.cfg

1. Copy the plugin azurestack\_plugin.py into the following directory:

/usr/local/nagios/libexec .

2. Copy the handler azurestack\_handler.sh into the following directory:

/usr/local/nagios/libexec/eventhandlers .

3. Make sure the plugin file is set to be executable:

Bash

The following parameters are available to be configured in the azurestack.cfg file.

Parameters in bold need to be configured independently from the authentication model

you choose.

For more information on how to create an SPN, see Use an app identity to access

resources.

Parameter Description Authentication

External\_domain\_fqdn External Domain FQDN

region: Region Name

tenant\_id: Tenant ID\*

client\_id: Client ID SPN with secret

client\_secret: Client Password SPN with secret

client\_cert\*\*: Path to Certificate SPN with certificate

client\_cert\_thumbprint\*\*: Certificate Thumbprint SPN with certificate

\*Tenant ID isn't required for Azure Stack Hub deployments with AD FS.

\*\* Client secret and client cert are mutually exclusive.

The other configuration files contain optional configuration settings as they can be

configured in Nagios as well.

sudo cp azurestack\_plugin.py <PLUGINS\_DIR>

sudo chmod +x <PLUGINS\_DIR>/azurestack\_plugin.py

Configure plugin

７ Note

Configuration Description

azurestack\_commands.cfg Handler configuration no changes requirement

azurestack\_contacts.cfg Notification Settings

azurestack\_hosts.cfg Azure Stack Hub Deployment Naming

azurestack\_services.cfg Configuration of the Service

1. Modify the configuration file.

2. Copy the modified configuration files into the following folder:

/usr/local/nagios/etc/objects .

The Nagios configuration needs to be updated to ensure the Azure Stack Hub - Nagios

Plugin is loaded.

1. Open the following file:

Bash

2. Add the following entry:

Bash

3. Reload Nagios.

Bash

Check the location destination in azurestack\_hosts.cfg and azurestack\_services.cfg.

Setup steps

Update Nagios configuration

/usr/local/nagios/etc/nagios.cfg

# Load the Azure Stack Hub Plugin Configuration

cfg\_file=/usr/local/Nagios/etc/objects/azurestack\_contacts.cfg

cfg\_file=/usr/local/Nagios/etc/objects/azurestack\_commands.cfg

cfg\_file=/usr/local/Nagios/etc/objects/azurestack\_hosts.cfg

cfg\_file=/usr/local/Nagios/etc/objects/azurestack\_services.cfg

sudo service nagios reload

Active alerts can be closed within Nagios using the custom notification functionality. The

custom notification must be:

An alert can also be closed using a terminal with the following command:

Bash

Troubleshooting the plugin is done by calling the plugin manually in a terminal. Use the

following method:

Bash

If you're not using Operations Manager, Nagios, or a Nagios-based solution, you can

use PowerShell to enable a broad range of monitoring solutions to integrate with Azure

Stack Hub.

1. To use PowerShell, make sure that you have PowerShell installed and

configured for an Azure Stack Hub operator environment. Install PowerShell

on a local computer that can reach the Resource Manager (administrator)

endpoint (https://adminmanagement.[region].[External\_FQDN]).

Manually close active alerts

/close-alert <ALERT\_GUID>

/usr/local/nagios/libexec/azurestack\_plugin.py --config-file

/usr/local/nagios/etc/objects/azurestack.cfg --action Close --alert-id

<ALERT\_GUID>

Troubleshooting

/usr/local/nagios/libexec/azurestack\_plugin.py --config-file

/usr/local/nagios/etc/objects/azurestack.cfg --action Monitor

Use PowerShell to monitor health and alerts

Az modules

2. Run the following commands to connect to the Azure Stack Hub environment

as an Azure Stack Hub operator:

PowerShell

3. Use commands such as the following examples to work with alerts:

PowerShell

For information about built-in health monitoring, see Monitor health and alerts in Azure

Stack Hub.

Security integration

Add-AzEnvironment -Name "AzureStackAdmin" -ArmEndpoint

https://adminmanagement.[Region].[External\_FQDN] `

-AzureKeyVaultDnsSuffix adminvault.[Region].[External\_FQDN] `

-AzureKeyVaultServiceEndpointResourceId https://adminvault.

[Region].[External\_FQDN]

Connect-AzAccount -EnvironmentName "AzureStackAdmin"

# Retrieve all alerts

$Alerts = Get-AzsAlert

$Alerts

# Filter for active alerts

$Active = $Alerts | Where-Object { $\_.State -eq "active" }

$Active

# Close alert

Close-AzsAlert -AlertID "ID"

#Retrieve resource provider health

$RPHealth = Get-AzsRPHealth

$RPHealth

# Retrieve infrastructure role instance health

$FRPID = $RPHealth | Where-Object { $\_.DisplayName -eq "Capacity" }

Get-AzsRegistrationHealth -ServiceRegistrationId

$FRPID.RegistrationId

Learn more

Next steps

Integrate Azure Stack Hub with monitoring

solutions using syslog forwarding

Article • 07/29/2022

This article shows you how to use syslog to integrate Azure Stack Hub infrastructure with external

security solution(s) already deployed in your datacenter. For example, a security information event

management (SIEM) system. The syslog channel exposes audits, alerts, and security logs from all the

components of the Azure Stack Hub infrastructure. Use syslog forwarding to integrate with security

monitoring solutions and to retrieve all audits, alerts, and security logs to store them for retention.

Starting with the 1809 update, Azure Stack Hub has an integrated syslog client that, once configured,

emits syslog messages with the payload in Common Event Format (CEF).

The following diagram describes the integration of Azure Stack Hub with an external SIEM. There are

two integration patterns that need to be considered: the first one (the one in blue) is the Azure Stack

Hub infrastructure that encompasses the infrastructure virtual machines and the Hyper-V nodes. All

the audits, security logs, and alerts from those components are centrally collected and exposed via

syslog with CEF payload. This integration pattern is described in this document page. The second

integration pattern is the one depicted in orange and covers the baseboard management controllers

(BMCs), the hardware lifecycle host (HLH), the virtual machines and virtual appliances that run the

hardware partner monitoring and management software, and the top of rack (TOR) switches. Since

these components are hardware-partner specific, contact your hardware partner for documentation

on how to integrate them with an external SIEM.

Azure Stack Hub infrastructure

HW Partner Specific

Switches

(ToR, BMC)

Hardware

Partner VMs

Hardware Lifecycle Host

Syslog Client

Hyper-V Host

BMC

Infrastructure

VMs

Microso

SIEM

Syslog message with CEF payload

The syslog client in Azure Stack Hub supports the following configurations:

1. Syslog over TCP, with mutual authentication (client and server) and TLS 1.2 encryption: In this

configuration, both the syslog server and the syslog client can verify the identity of each other

via certificates. The messages are sent over a TLS 1.2 encrypted channel.

2. Syslog over TCP with server authentication and TLS 1.2 encryption: In this configuration, the

syslog client can verify the identity of the syslog server via a certificate. The messages are sent

Configuring syslog forwarding

over a TLS 1.2 encrypted channel.

3. Syslog over TCP, with no encryption: In this configuration, the syslog client and syslog server

identities aren't verified. The messages are sent in clear text over TCP.

4. Syslog over UDP, with no encryption: In this configuration, the syslog client and syslog server

identities aren't verified. The messages are sent in clear text over UDP.

Configuring syslog forwarding requires access to the privileged endpoint (PEP). Two PowerShell

cmdlets have been added to the PEP to configure the syslog forwarding:

PowerShell

Parameters for Set-SyslogServer cmdlet:

Parameter Description Type Required

ServerName FQDN or IP address of the syslog server. String yes

ServerPort Port number the syslog server is listening on. UInt16 yes

NoEncryption Force the client to send syslog messages in clear text. flag no

SkipCertificateCheck Skip validation of the certificate provided by the syslog server during

initial TLS handshake.

flag no

SkipCNCheck Skip validation of the Common Name value of the certificate

provided by the syslog server during initial TLS handshake.

flag no

） Important

Microsoft strongly recommends to use TCP using authentication and encryption (configuration

#1 or, at the very minimum, #2) for production environments to protect against man-in-themiddle attacks and eavesdropping of messages.

Cmdlets to configure syslog forwarding

### cmdlet to pass the syslog server information to the client and to configure the

transport protocol, the encryption and the authentication between the client and the

server

Set-SyslogServer [-ServerName <String>] [-ServerPort <UInt16>] [-NoEncryption] [-

SkipCertificateCheck] [-SkipCNCheck] [-UseUDP] [-Remove]

### cmdlet to configure the certificate for the syslog client to authenticate with the

server

Set-SyslogClient [-pfxBinary <Byte[]>] [-CertPassword <SecureString>] [-

RemoveCertificate] [-OutputSeverity]

Cmdlets parameters

Parameter Description Type Required

UseUDP Use syslog with UDP as transport protocol. flag no

Remove Remove configuration of the server from the client and stop syslog

forwarding.

flag no

Parameters for Set-SyslogClient cmdlet:

Parameter Description Type

pfxBinary The contents of the pfx file, piped to a Byte[], containing the certificate to be

used by the client as identity to authenticate against the syslog server.

Byte[]

CertPassword Password to import the private key that's associated with the pfx file. SecureString

RemoveCertificate Remove certificate from the client. flag

OutputSeverity Level of output logging. Values are Default or Verbose. Default includes

severity levels: warning, critical, or error. Verbose includes all severity levels:

verbose, informational, warning, critical, or error.

String

In this configuration, the syslog client in Azure Stack Hub forwards the messages to the syslog server

over TCP, with TLS 1.2 encryption. During the initial handshake, the client verifies that the server

provides a valid, trusted certificate. The client also provides a certificate to the server as proof of its

identity. This configuration is the most secure as it provides a full validation of the identity of both

the client and the server and it sends messages over an encrypted channel.

To configure syslog forwarding with TCP, mutual authentication, and TLS 1.2 encryption, run both

these cmdlets on a PEP session:

PowerShell

The client certificate must have the same root as the one provided during the deployment of Azure

Stack Hub. It also must contain a private key.

Configuring syslog forwarding with TCP, mutual authentication,

and TLS 1.2 encryption

） Important

Microsoft strongly recommends to use this configuration for production environments.

# Configure the server

Set-SyslogServer -ServerName <FQDN or ip address of syslog server> -ServerPort <Port

number on which the syslog server is listening on>

# Provide certificate to the client to authenticate against the server

Set-SyslogClient -pfxBinary <Byte[] of pfx file> -CertPassword <SecureString, password

for accessing the pfx file>

PowerShell

In this configuration, the syslog client in Azure Stack Hub forwards the messages to the syslog server

over TCP, with TLS 1.2 encryption. During the initial handshake, the client also verifies that the server

provides a valid, trusted certificate. This configuration prevents the client from sending messages to

untrusted destinations. TCP using authentication and encryption is the default configuration and

represents the minimum level of security that Microsoft recommends for a production environment.

PowerShell

In case you want to test the integration of your syslog server with the Azure Stack Hub client by using

a self-signed or untrusted certificate, you can use these flags to skip the server validation done by the

client during the initial handshake.

PowerShell

##Example on how to set your syslog client with the certificate for mutual

authentication.

##This example script must be run from your hardware lifecycle host or privileged access

workstation.

$ErcsNodeName = "<yourPEP>"

$password = ConvertTo-SecureString -String "<your cloudAdmin account password" -

AsPlainText -Force

$cloudAdmin = "<your cloudAdmin account name>"

$CloudAdminCred = New-Object System.Management.Automation.PSCredential ($cloudAdmin,

$password)

$certPassword = $password

$certContent = Get-Content -Path C:\cert\<yourClientCertificate>.pfx -Encoding Byte

$params = @{

ComputerName = $ErcsNodeName

Credential = $CloudAdminCred

ConfigurationName = "PrivilegedEndpoint"

}

$session = New-PSSession @params

$params = @{

Session = $session

ArgumentList = @($certContent, $certPassword)

}

Write-Verbose "Invoking cmdlet to set syslog client certificate..." -Verbose

Invoke-Command @params -ScriptBlock {

param($CertContent, $CertPassword)

Set-SyslogClient -PfxBinary $CertContent -CertPassword $CertPassword }

Configuring syslog forwarding with TCP, Server authentication,

and TLS 1.2 encryption

Set-SyslogServer -ServerName <FQDN or ip address of syslog server> -ServerPort <Port

number on which the syslog server is listening on>

In this configuration, the syslog client in Azure Stack Hub forwards the messages to the syslog server

over TCP, with no encryption. The client doesn't verify the identity of the server nor does it provide its

own identity to the server for verification.

PowerShell

In this configuration, the syslog client in Azure Stack Hub forwards the messages to the syslog server

over UDP, with no encryption. The client doesn't verify the identity of the server nor does it provide

its own identity to the server for verification.

PowerShell

While UDP with no encryption is the easiest to configure, it doesn't provide any protection against

man-in-the-middle attacks and eavesdropping of messages.

#Skip validation of the Common Name value in the server certificate. Use this flag if

you provide an IP address for your syslog server

Set-SyslogServer -ServerName <FQDN or ip address of syslog server> -ServerPort <Port

number on which the syslog server is listening on>

-SkipCNCheck

#Skip entirely the server certificate validation

Set-SyslogServer -ServerName <FQDN or ip address of syslog server> -ServerPort <Port

number on which the syslog server is listening on>

-SkipCertificateCheck

） Important

Microsoft recommends against the use of -SkipCertificateCheck flag for production

environments.

Configuring syslog forwarding with TCP and no encryption

Set-SyslogServer -ServerName <FQDN or ip address of syslog server> -ServerPort <Port

number on which the syslog server is listening on> -NoEncryption

） Important

Microsoft recommends against using this configuration for production environments.

Configuring syslog forwarding with UDP and no encryption

Set-SyslogServer -ServerName <FQDN or ip address of syslog server> -ServerPort <Port

number on which the syslog server is listening on> -UseUDP

） Important

To remove the syslog server configuration altogether and stop syslog forwarding:

Remove the syslog server configuration from the client

PowerShell

Remove the client certificate from the client

PowerShell

If you successfully connected the syslog client to your syslog server, you should soon start receiving

events. If you don't see any event, verify the configuration of your syslog client by running the

following cmdlets:

Verify the server configuration in the syslog client

PowerShell

Verify the certificate setup in the syslog client

PowerShell

The syslog forwarding of the Azure Stack Hub infrastructure sends messages formatted in Common

Event Format (CEF). Each syslog message is structured based on this schema:

Syslog

Microsoft recommends against using this configuration for production environments.

Removing syslog forwarding configuration

Set-SyslogServer -Remove

Set-SyslogClient -RemoveCertificate

Verifying the syslog setup

Get-SyslogServer

Get-SyslogClient

Syslog message schema

<Time> <Host> <CEF payload>

The CEF payload is based on the structure below, but the mapping for each field varies depending on

the type of message (Windows Event, Alert created, Alert closed).

CEF

Table of events for the privileged endpoint:

Event PEP

event

ID

PEP task name Severity

PrivilegedEndpointAccessed 1000 PrivilegedEndpointAccessedEvent 5

SupportSessionTokenRequested 1001 SupportSessionTokenRequestedEvent 5

SupportSessionDevelopmentTokenRequested 1002 SupportSessionDevelopmentTokenRequestedEvent 5

SupportSessionUnlocked 1003 SupportSessionUnlockedEvent 10

SupportSessionFailedToUnlock 1004 SupportSessionFailedToUnlockEvent 10

PrivilegedEndpointClosed 1005 PrivilegedEndpointClosedEvent 5

NewCloudAdminUser 1006 NewCloudAdminUserEvent 10

RemoveCloudAdminUser 1007 RemoveCloudAdminUserEvent 10

SetCloudAdminUserPassword 1008 SetCloudAdminUserPasswordEvent 5

GetCloudAdminPasswordRecoveryToken 1009 GetCloudAdminPasswordRecoveryTokenEvent 10

ResetCloudAdminPassword 1010 ResetCloudAdminPasswordEvent 10

PrivilegedEndpointSessionTimedOut 1017 PrivilegedEndpointSessionTimedOutEvent 5

PEP Severity table:

# Common Event Format schema

CEF: <Version>|<Device Vendor>|<Device Product>|<Device Version>|<Signature ID>|<Name>|

<Severity>|<Extensions>

\* Version: 0.0

\* Device Vendor: Microsoft

\* Device Product: Microsoft Azure Stack Hub

\* Device Version: 1.0

CEF mapping for privileged endpoint events

Prefix fields

\* Signature ID: Microsoft-AzureStack-PrivilegedEndpoint: <PEP Event ID>

\* Name: <PEP Task Name>

\* Severity: mapped from PEP Level (details see the PEP Severity table below)

\* Who: account used to connect to the PEP

\* WhichIP: IP address of ERCS server hosting the PEP

Severity Level Numerical Value

0 Undefined Value: 0. Indicates logs at all levels

10 Critical Value: 1. Indicates logs for a critical alert

8 Error Value: 2. Indicates logs for an error

5 Warning Value: 3. Indicates logs for a warning

2 Information Value: 4. Indicates logs for an informational message

0 Verbose Value: 5. Indicates logs at all levels

Table of events for the recovery endpoint:

Event REP

event

ID

REP task name Severity

RecoveryEndpointAccessed 1011 RecoveryEndpointAccessedEvent 5

RecoverySessionTokenRequested 1012 RecoverySessionTokenRequestedEvent 5

RecoverySessionDevelopmentTokenRequested 1013 RecoverySessionDevelopmentTokenRequestedEvent 5

RecoverySessionUnlocked 1014 RecoverySessionUnlockedEvent 10

RecoverySessionFailedToUnlock 1015 RecoverySessionFailedToUnlockEvent 10

RecoveryEndpointClosed 1016 RecoveryEndpointClosedEvent 5

REP Severity table:

Severity Level Numerical value

0 Undefined Value: 0. Indicates logs at all levels

10 Critical Value: 1. Indicates logs for a critical alert

8 Error Value: 2. Indicates logs for an error

5 Warning Value: 3. Indicates logs for a warning

2 Information Value: 4. Indicates logs for an informational message

CEF mapping for recovery endpoint events

Prefix fields

\* Signature ID: Microsoft-AzureStack-PrivilegedEndpoint: <REP Event ID>

\* Name: <REP Task Name>

\* Severity: mapped from REP Level (details see the REP Severity table below)

\* Who: account used to connect to the REP

\* WhichIP: IP address of the device used to connect to the REP

Severity Level Numerical value

0 Verbose Value: 5. Indicates logs at all levels

Severity table for Windows events:

CEF severity value Windows event level Numerical value

0 Undefined Value: 0. Indicates logs at all levels

10 Critical Value: 1. Indicates logs for a critical alert

8 Error Value: 2. Indicates logs for an error

5 Warning Value: 3. Indicates logs for a warning

2 Information Value: 4. Indicates logs for an informational message

0 Verbose Value: 5. Indicates logs at all levels

Custom extension table for Windows events in Azure Stack Hub:

Custom extension name Windows event example

MasChannel System

MasComputer test.azurestack.contoso.com

MasCorrelationActivityID C8F40D7C-3764-423B-A4FA-C994442238AF

MasCorrelationRelatedActivityID C8F40D7C-3764-423B-A4FA-C994442238AF

MasEventData svchost!!4132,G,0!!!!EseDiskFlushConsistency!!ESENT!!0x800000

MasEventDescription The Group Policy settings for the user were processed successfully. There

were no changes detected since the last successful processing of Group

Policy.

MasEventID 1501

MasEventRecordID 26637

MasExecutionProcessID 29380

MasExecutionThreadID 25480

MasKeywords 0x8000000000000000

CEF mapping for Windows events

\* Signature ID: ProviderName:EventID

\* Name: TaskName

\* Severity: Level (for details, see the severity table below)

\* Extension: Custom Extension Name (for details, see the Custom Extension table below)

Custom extension name Windows event example

MasKeywordName Audit Success

MasLevel 4

MasOpcode 1

MasOpcodeName info

MasProviderEventSourceName

MasProviderGuid AEA1B4FA-97D1-45F2-A64C-4D69FFFD92C9

MasProviderName Microsoft-Windows-GroupPolicy

MasSecurityUserId <Windows SID>

MasTask 0

MasTaskCategory Process Creation

MasUserData KB4093112!!5112!!Installed!!0x0!!WindowsUpdateAgent Xpath:

/Event/UserData/\*

MasVersion 0

Alerts severity table:

Severity Level

0 Undefined

10 Critical

5 Warning

Custom Extension table for Alerts created in Azure Stack Hub:

Custom extension

name

Example

CEF mapping for alerts created

\* Signature ID: Microsoft Azure Stack Hub Alert Creation : FaultTypeId

\* Name: FaultTypeId : AlertId

\* Severity: Alert Severity (for details, see alerts severity table below)

\* Extension: Custom Extension Name (for details, see the Custom Extension table below)

Custom extension

name

Example

MasEventDescription DESCRIPTION: A user account <TestUser> was created for <TestDomain>. It's a potential

security risk. -- REMEDIATION: Contact support. Customer Assistance is required to

resolve this issue. Don't try to resolve this issue without their assistance. Before you open

a support request, start the log file collection process using the guidance from

https://aka.ms/azurestacklogfiles .

The example below shows a syslog message with CEF payload:

The table lists all the event types, events, message schema or properties that are send via the syslog

channel. Setup verbose switch should only be used if Windows informational events are required for

SIEM integration.

Event Type Events or message schema Requires

verbose

setting

Event Description (optional)

Azure Stack

Hub Alerts

For the alert message schema see CEF

mapping for alerts closed.

A list of all alerts in shared in a separate

document.

No System health alerts

CEF mapping for alerts closed

\* Signature ID: Microsoft Azure Stack Hub Alert Creation : FaultTypeId

\* Name: FaultTypeId : AlertId

\* Severity: Information

2018:05:17:-23:59:28 -07:00 TestHost CEF:0.0|Microsoft|Microsoft Azure Stack

Hub|1.0|3|TITLE: User Account Created -- DESCRIPTION: A user account \<TestUser\> was

created for \<TestDomain\>. It's a potential security risk. -- REMEDIATION: Please

contact Support. Customer Assistance is required to resolve this issue. Do not try to

resolve this issue without their assistance. Before you open a support request, start

the log file collection process using the guidance from

https://aka.ms/azurestacklogfiles|10

Syslog event types

Event Type Events or message schema Requires

verbose

setting

Event Description (optional)

Privileged

Endpoint

Events

For the privileged endpoint message schema

see CEF mapping for privileged endpoint

events.

PrivilegedEndpointAccessed

SupportSessionTokenRequested

SupportSessionDevelopmentTokenRequested

SupportSessionUnlocked

SupportSessionFailedToUnlock

PrivilegedEndpointClosed

NewCloudAdminUser

RemoveCloudAdminUser

SetCloudAdminUserPassword

GetCloudAdminPasswordRecoveryToken

ResetCloudAdminPassword

PrivilegedEndpointSessionTimedOut

No

Recovery

Endpoint

Events

For the recovery endpoint message schema

see CEF mapping for recovery endpoint

events.

RecoveryEndpointAccessed

RecoverySessionTokenRequested

RecoverySessionDevelopmentTokenRequested

RecoverySessionUnlocked

RecoverySessionFailedToUnlock

Recovand RecoveryEndpointClosed

No

Windows

Security

Events

For the Windows event message schema see

CEF mapping for Windows events.

Yes (To get

information

events)

Type:

- Information

- Warning

- Error

- Critical

Event Type Events or message schema Requires

verbose

setting

Event Description (optional)

ARM Events Message properties:

AzsSubscriptionId

AzsCorrelationId

AzsPrincipalOid

AzsPrincipalPuid

AzsTenantId

AzsOperationName

AzsOperationId

AzsEventSource

AzsDescription

AzsResourceProvider

AzsResourceUri

AzsEventName

AzsEventInstanceId

AzsChannels

AzsEventLevel

AzsStatus

AzsSubStatus

AzsClaims

AzsAuthorization

AzsHttpRequest

AzsProperties

AzsEventTimestamp

AzsAudience

AzsIssuer

AzsIssuedAt

AzsApplicationId

AzsUniqueTokenId

AzsArmServiceRequestId

AzsEventCategory

No Each registered ARM resource can

raise an event.

BCDR

Events

Message schema:

AuditingManualBackup {

}

AuditingConfig

{

Interval

Retention

IsSchedulerEnabled

BackupPath

}

AuditingPruneBackupStore {

IsInternalStore

}

No These events track infra backup

admin operations done by

customer manually, includes

trigger backup, change backup

configuration, and prune backup

data.

Event Type Events or message schema Requires

verbose

setting

Event Description (optional)

Infra Fault

Creation

and Closing

Events

Message schema:

InfrastructureFaultOpen {

AzsFaultId,

AzsFaultTypeName,

AzsComponentType,

AzsComponentName,

AzsFaultHash,

AzsCreatedTimeUtc,

AzsSource

}

InfrastructureFaultClose {

AzsFaultId,

AzsFaultTypeName,

AzsComponentType,

AzsComponentName,

AzsFaultHash,

AzsLastUpdatedTimeUtc,

AzsSource

}

No Faults trigger workflows that

attempt to remediate errors that

can lead to alerts. If a fault has no

remediation it does directly lead

to an Alert.

Service

Fault

Creation

and Closing

Events

Message schema:

ServiceFaultOpen {

AzsFaultId,

AzsFaultTypeName,

AzsSubscriptionId,

AzsResourceGroup,

AzsServiceName,

AzsResourceId

AzsFaultHash,

AzsCreatedTimeUtc,

AzsSource

}

ServiceFaultClose {

AzsFaultId,

AzsFaultTypeName,

AzsSubscriptionId,

AzsResourceGroup,

AzsServiceName,

AzsResourceId

AzsFaultHash,

AzsLastUpdatedTimeUtc,

AzsSource

}

No Faults trigger workflows that

attempt to remediate errors that

can lead to alerts.

If a fault has no remediation it

does directly lead to an Alert.

Event Type Events or message schema Requires

verbose

setting

Event Description (optional)

PEP WAC

events

Message schema:

Prefix fields

\* Signature ID: Microsoft-AzureStackPrivilegedEndpoint: <PEP Event ID>

\* Name: <PEP Task Name>

\* Severity: mapped from PEP Level (details see

the PEP Severity table below)

\* Who: account used to connect to the PEP

\* WhichIP: IP address of ERCS server hosting

the PEP

WACServiceStartFailedEvent

WACConnectedUserNotRetrievedEvent

WACEnableExceptionEvent

WACUserAddedEvent

WACAddUserToLocalGroupFailedEvent

WACIsUserInLocalGroupFailedEvent

WACServiceStartTimeoutEvent

WACServiceStartInvalidOperationEvent

WACGetSidFromUserFailedEvent

WACDisableFirewallFailedEvent

WACCreateLocalGroupIfNotExistFailedEvent

WACEnableFlagIsTrueEvent

WACEnableFlagIsFalseEvent

WACServiceStartedEvent

No

Servicing policy

Next steps

Integrate physical device auditing with

your Azure Stack Hub datacenter

Article • 07/29/2022

All physical devices in Azure Stack Hub, like the baseboard management controllers

(BMCs) and network switches, emit audit logs. You can integrate the audit logs into your

overall auditing solution. Since the devices vary across the different Azure Stack Hub

OEM hardware vendors, contact your vendor for the documentation on auditing

integration. The sections below provide some general information for physical device

auditing in Azure Stack Hub.

All physical devices in Azure Stack Hub support the use of TACACS or RADIUS. Support

includes access to the baseboard management controller (BMC) and network switches.

Azure Stack Hub solutions don't ship with either RADIUS or TACACS built-in. However,

the solutions have been validated to support the use of existing RADIUS or TACACS

solutions available in the market.

For RADIUS only, MSCHAPv2 was validated. This represents the most secure

implementation using RADIUS. Consult with your OEM hardware vendor to enable

TACAS or RADIUS in the devices included with your Azure Stack Hub solution.

All physical networking devices in Azure Stack Hub support syslog messages. Azure

Stack Hub solutions don't ship with a syslog server. However, the devices have been

validated to support sending messages to existing syslog solutions available in the

market.

The syslog destination address is an optional parameter collected for deployment, but it

can also be added post deployment. Consult with your OEM hardware vendor to

configure syslog forwarding on your networking devices.

Servicing policy

Physical device access auditing

Syslog forwarding for network devices

Next steps

Azure Stack Hub administration basics

Article • 01/25/2023

If you're new to Azure Stack Hub administration, there are several things you need to

know. This article provides an overview of your role as an Azure Stack Hub operator, and

what you need to tell your users to help them become productive.

If you're using an Azure Stack Hub integrated system, update packages distribute

updated versions of Azure Stack Hub. You can import these packages and apply them by

using the Updates tile in the administrator portal.

If you're using the Azure Stack Development Kit (ASDK), review What is Azure Stack

Hub? to learn the purpose and limitations of the ASDK. You can use the ASDK as a

sandbox, where you can evaluate Azure Stack Hub and develop and test your apps in a

non-production environment. For deployment information, see Azure Stack

Development Kit deployment.

Like Azure, we innovate rapidly. We'll regularly release new builds. If you're running the

ASDK and you want to move to the latest build, you must redeploy Azure Stack Hub.

You can't apply update packages. This process takes time, but the benefit is that you can

try out the latest features. The ASDK documentation on our website reflects the latest

release build.

You'll need an awareness of which services you can make available to your users. Azure

Stack Hub supports a subset of Azure services. The list of supported services will

continue to evolve.

Foundational services

By default, Azure Stack Hub includes the following "foundational services" when you

deploy Azure Stack Hub:

Understand the builds

Integrated systems

Development kit

Learn about available services

Compute

Storage

Networking

Key Vault

With these foundational services, you can offer Infrastructure-as-a-Service (IaaS) to your

users with minimal configuration.

Additional services

Currently, we support the following additional Platform-as-a-Service (PaaS) services:

App Service

Azure Functions

SQL and MySQL databases

Event Hubs

Kubernetes (in preview)

These services require additional configuration before you can make them available to

your users. For more information, see the "Tutorials" and the "How-to guides\Offer

services" sections of our Azure Stack Hub operator documentation.

Service roadmap

Azure Stack Hub will continue to add support for Azure services. For the projected

roadmap, see the Azure Stack Hub: An extension of Azure whitepaper. You can also

monitor the Azure Stack Hub blog posts for new announcements.

There are a few account considerations to be aware of when managing Azure Stack Hub.

Especially in deployments using Windows Server Active Directory Federation Services

(AD FS) as the identity provider instead of Azure Active Directory (Azure AD). The

following account considerations apply to both Azure Stack Hub integrated systems and

ASDK deployments:

Account Azure AD AD FS

Local Administrator

(.\Administrator)

ASDK host administrator. ASDK host administrator.

What account should I use?

Account Azure AD AD FS

AzureStack\AzureStackAdmin ASDK host administrator.

Can be used to sign in to the

Azure Stack Hub administrator

portal.

Access to view and administer

Service Fabric rings.

ASDK host administrator.

No access to the Azure Stack

Hub administrator portal.

Access to view and administer

Service Fabric rings.

No longer owner of the Default

Provider Subscription (DPS).

AzureStack\CloudAdmin Can access and run permitted

commands within the

privileged endpoint.

Can access and run permitted

commands within the

privileged endpoint.

Can't sign in to the ASDK host.

Owner of the Default Provider

Subscription (DPS).

Azure AD Global

Administrator

Used during installation.

Owner of the Default Provider

Subscription (DPS).

Not applicable.

You can use the administrator portal or PowerShell to manage Azure Stack Hub. The

easiest way to learn the basic concepts is through the portal. If you want to use

PowerShell, there are preparation steps. Before you get started, you might want to get

２ Warning

By default your Azure Stack Hub stamp is configured with only one CloudAdmin

account. There are no recovery options if the account credentials are lost,

compromised, or locked. You will lose access to the privileged endpoint and other

resources.

It is highly recommended that you create additional CloudAdmin accounts, to

avoid redeployment of your stamp at your own expense. Make sure you

document these credentials based on your company's guidelines.

What tools do I use to manage?

familiar with how PowerShell is used on Azure Stack Hub. For more information, see Get

started with PowerShell on Azure Stack Hub.

Azure Stack Hub uses Azure Resource Manager as its underlying deployment,

management, and organization mechanism. If you're going to manage Azure Stack Hub

and help support users, you can learn about Resource Manager. See the Getting Started

with Azure Resource Manager whitepaper.

Your users want to use services. From their perspective, your main role is to make these

services available to them. Decide which services to offer, and make those services

available by creating plans, offers, and quotas. For more information, see Overview of

offering services in Azure Stack Hub.

You'll also need to add items to Azure Stack Hub Marketplace. The easiest way is to

download marketplace items from Azure to Azure Stack Hub.

In addition to providing services, you must do the regular duties of an operator to keep

Azure Stack Hub up and running. These duties include the following tasks:

Add user accounts (for Azure AD deployment or for AD FS deployment).

Assign role-based access control (RBAC) roles (This task isn't restricted to admins.)

Monitor infrastructure health.

Manage network and storage resources.

Replace bad hardware. For example, replace a failed disk.

Here is a list of daily, weekly, and monthly tasks for an operator:

1. Check alerts.

2. Check backup state.

3. Update Defender Signature (disconnected systems).

Your typical responsibilities

７ Note

If you want to test your plans, offers, and services, you can use the user portal; not

the administrator portal.

Operator tasks

Daily

You'll need to let your users know how to work with services in Azure Stack Hub, how to

connect to the environment, and how to subscribe to offers. Besides any custom

documentation that you may want to provide your users, you can direct users to Azure

Stack Hub User Documentation.

Understand how to work with services in Azure Stack Hub

There's information your users must understand before they use services and build apps

in Azure Stack Hub. For example, there are specific PowerShell and API version

requirements. Also, there are some feature deltas between a service in Azure and the

equivalent service in Azure Stack Hub. Make sure that your users review the following

articles:

Key considerations: Using services or building apps for Azure Stack Hub

Considerations for Virtual Machines in Azure Stack Hub

Storage: differences and considerations

The information in these articles summarizes the differences between a service in Azure

and Azure Stack Hub. It supplements the information that's available for an Azure

service in the global Azure documentation.

Connect to Azure Stack Hub as a user

In an ASDK environment, if a user doesn't use Remote Desktop to connect to the ASDK

host, they can configure a virtual private network (VPN) connection to connect to Azure

Stack Hub. See Connect to Azure Stack Hub.

Your users will want to know how to access the user portal or how to connect through

PowerShell. In an integrated systems environment, the user portal address varies per

deployment. You'll need to provide your users with the correct URL.

If using PowerShell, users may have to register resource providers before they can use

services. A resource provider manages a service. For example, the networking resource

provider manages resources like virtual networks, network interfaces, and load

balancers. They must install PowerShell, download additional modules, and configure

PowerShell (which includes resource provider registration).

Subscribe to an offer

What to tell your users

Before a user can use services, they must subscribe to an offer that you've created as an

operator.

For an integrated system, there's a coordinated escalation and resolution process

between Microsoft and our original equipment manufacturer (OEM) hardware partners.

If there's a cloud services issue, support is offered through Microsoft Support. To open a

support request, select the help and support icon (question mark) in the upper-right

corner of the administrator portal. Then select Help + support and then New support

request under the Support section.

If there's an issue with deployment, patch and update, hardware (including field

replaceable units), or any hardware-branded software, like software running on the

hardware lifecycle host, contact your OEM hardware vendor first.

For anything else, contact Microsoft Support.

For the ASDK, you can ask support-related questions in the Microsoft forums . To get

to the forums, select the Help and support icon (question mark) in the upper-right

corner of the administrator portal, then select Help + support, and then select MSDN

Forums under the Support section. These forums are regularly monitored. Because the

ASDK is an evaluation environment, there's no official support offered through Microsoft

Support.

Region management in Azure Stack Hub

Where to get support

７ Note

To find support information for earlier releases of Azure Stack Hub, see Help and

Support for earlier releases Azure Stack Hub.

Integrated systems

Azure Stack Development Kit (ASDK)

Next steps

Clear portal user data from Azure Stack

Hub

Article • 02/08/2021

Azure Stack Hub operators can clear portal user data on demand when Azure Stack Hub

users request it. As an Azure Stack Hub user, the portal can be customized by pinning

tiles and changing the dashboard layout. Users can also change the theme and adjust

the default language to match personal preferences.

Portal user data includes favorites and recently accessed resources in the Azure Stack

Hub user portal. This article describes how to clear the portal user data.

Removing portal user settings should only be done after the user subscription has been

deleted.

Install PowerShell for Azure Stack Hub.

Download the latest Azure Stack Hub tools from GitHub.

The user account must still exist in the directory.

Azure Stack Hub admin credentials to access the admin Resource Manager

endpoint.

７ Note

Some user data can still exist in the system section of event logs after following the

guidance in this article. This data can remain for several days until the logs

automatically roll over.

Prerequisites

７ Note

If you attempt to delete portal user information from a user that was invited from a

guest directory (multi-tenancy), you must have read permission in that directory.

For more information, see the CSP scenario later in this article.

Clear portal user data using a user principal

name

This scenario assumes that either the default provider subscription and the user are part

of the same directory, or that you have read access to the directory in which the user

resides.

Make sure to download the latest version of the Azure Stack Hub tools from GitHub

before you proceed.

For this procedure, use a computer that can communicate with the admin Resource

Manager endpoint of Azure Stack Hub.

1. Open an elevated Windows PowerShell session (run as administrator), go to the

root folder in the AzureStack-Tools-az directory, and import the required

PowerShell module:

PowerShell

2. Run the following commands. Make sure to substitute the placeholders with values

that match your environment:

PowerShell

Import-Module

.\DatacenterIntegration\Portal\PortalUserDataUtilities.psm1

## The following Azure Resource Manager endpoint is for the ASDK. If

you are in a multinode environment, contact your operator or service

provider to get the endpoint.

$adminARMEndpoint = "https://adminmanagement.local.azurestack.external"

## Replace the following value with the Azure Stack Hub directory

tenant ID.

$azureStackDirectoryTenantId = "f5025bf2-547f-4b49-9693-6420c1d5e4ca"

## Replace the following value with the user directory tenant ID.

$userDirectoryTenantId = " 7ddf3648-9671-47fd-b63d-eecd82ed040e"

## Replace the following value with name of the user principal whose

portal user data is to be cleared.

$userPrincipalName = "myaccount@contoso.onmicrosoft.com"

Clear-AzsUserDataWithUserPrincipalName -AzsAdminArmEndpoint

$adminARMEndpoint `

-AzsAdminDirectoryTenantId $azureStackDirectoryTenantId `

-UserPrincipalName $userPrincipalName `

-DirectoryTenantId $userDirectoryTenantId

In this scenario, the Azure Stack Hub operator has no access to the guest directory in

which the user resides. This is a common scenario when you're a Cloud Solution

Provider (CSP).

For an Azure Stack Hub operator to remove the portal user data, at a minimum the user

object ID is required.

The user must query the object ID and provide it to the Azure Stack Hub operator. The

operator doesn't have access to the directory in which the user resides.

1. Open an elevated Windows PowerShell session (run as administrator), go to the

root folder in the AzureStack-Tools-az directory, and then import the necessary

PowerShell module.

PowerShell

2. Run the following commands. Make sure to substitute the placeholders with values

that match your environment.

PowerShell

７ Note

azureStackDirectoryTenantId is optional. If you don't specify this value, the

script searches for the user principal name in all tenant directories registered

in Azure Stack Hub and then clears the portal data for all matched users.

Clear portal user data in guest directory

User retrieves the user object ID

Import-Module

.\DatacenterIntegration\Portal\PortalUserDataUtilities.psm1

## The following Azure Resource Manager endpoint is for the ASDK. If

you are in a multinode environment, contact your operator or service

provider to get the endpoint.

$userARMEndpoint = "https://management.local.azurestack.external"

## Replace the following value with the directory tenant ID, which

contains the user account.

$userDirectoryTenantId = "3160cbf5-c227-49dd-8654-86e924c0b72f"

After receiving the user object ID as an Azure Stack Hub operator, run the following

commands to remove the portal user data:

1. Open an elevated Windows PowerShell session (run as administrator), go to the

root folder in the AzureStack-Tools-az directory, and then import the necessary

PowerShell module.

PowerShell

2. Run the following commands, making sure you adjust the parameter to match

your environment:

PowerShell

## Replace the following value with the name of the user principal

whose portal user data is to be cleared.

$userPrincipleName = "myaccount@contoso.onmicrosoft.com"

Get-UserObjectId -DirectoryTenantId $userDirectoryTenantId `

-AzsArmEndpoint $userARMEndpoint `

-UserPricinpalName $userPrincipleName

７ Note

As a user, you must provide the user object ID, which is the output of the

previous script, to the Azure Stack Hub operator.

Azure Stack Hub operator removes the portal

user data

Import-Module

.\DatacenterIntegration\Portal\PortalUserDataUtilities.psm1

## The following Azure Resource Manager endpoint is for the ASDK. If

you are in a multinode environment, contact your operator or service

provider to get the endpoint.

$AzsAdminARMEndpoint =

"https://adminmanagement.local.azurestack.external"

## Replace the following value with the Azure Stack Hub directory

tenant ID.

$AzsAdminDirectoryTenantId = "f5025bf2-547f-4b49-9693-6420c1d5e4ca"

## Replace the following value with the directory tenant ID of the user

to clear.

Register Azure Stack Hub with Azure and populate the Azure Stack Hub

Marketplace with items to offer your users.

$DirectoryTenantId = "3160cbf5-c227-49dd-8654-86e924c0b72f"

## Replace the following value with the name of the user principal

whose portal user data is to be cleared.

$userObjectID = "s-1-\*\*\*\*\*\*\*"

Clear-AzsUserDataWithUserObject -AzsAdminArmEndpoint

$AzsAdminARMEndpoint `

-AzsAdminDirectoryTenantId $AzsAdminDirectoryTenantId `

-DirectoryTenantID $DirectoryTenantId `

-UserObjectID $userObjectID `

Next steps

Configure Azure Stack Hub telemetry

Article • 07/29/2022

Azure Stack Hub telemetry automatically uploads system data to Microsoft via the

Connected User Experience. Microsoft teams use the data that Azure Stack Hub

telemetry gathers to improve customer experiences. This data is also used for security,

health, quality, and performance analysis.

For an Azure Stack Hub operator, telemetry can provide valuable insights into enterprise

deployments and gives you a voice that helps shape future versions of Azure Stack Hub.

Azure Stack Hub telemetry is based on the Windows Server 2019 Connected User

Experience and Telemetry component. This component uses the Event Tracing for

Windows (ETW) TraceLogging technology to gather and store events and data. Azure

Stack components use the same technology to publish events and data gathered by

using public operating system event logging and tracing APIs. Examples of these Azure

Stack Hub components include these providers: Network Resource, Storage Resource,

Monitoring Resource, and Update Resource. The Connected User Experience and

Telemetry component encrypts data using SSL and uses certificate pinning to transmit

data over HTTPS to the Microsoft Data Management service.

To enable telemetry data flow, the following outbound ports and endpoints must be

open and allowed in your network:

Endpoint Protocol /

Ports

Description

https://settingswin.data.microsoft.com

HTTPS 443 Cloud configuration endpoint for UTC, DiagTrack,

and Feedback hub

７ Note

You can also configure Azure Stack Hub to forward usage information to Azure for

billing. This is required for multi-node Azure Stack Hub customers who choose payas-you-use billing. Usage reporting is controlled independently from telemetry and

isn't required for multi-node customers who choose the capacity model or for

Azure Stack Development Kit users. For these scenarios, usage reporting can be

turned off using the registration script.

Network requirements

Endpoint Protocol /

Ports

Description

https://login.live.com HTTPS 443 Provides a more reliable device identity

\*.events.data.microsoft.com HTTPS 443 Endpoint for UTC, DiagTrack, Windows Error

Reporting, and Aria

The ETW service routes telemetry data back to protected cloud storage. The principal of

least privilege guides access to telemetry data. Only Microsoft personnel with a valid

business need are given access to the telemetry data. Microsoft doesn't share personal

customer data with third parties, except at the customer's discretion or for the limited

purposes described in the Microsoft Privacy Statement . Business reports that are

shared with OEMs and partners include aggregated, anonymized data. Data sharing

decisions are made by an internal Microsoft team including privacy, legal, and data

management stakeholders.

Microsoft believes in, and practices information minimization. We strive to gather only

the information that's needed, and store it for only as long as necessary to provide a

service or for analysis. Much of the information about how the Azure Stack Hub system

and Azure services are functioning is deleted within six months. Summarized or

aggregated data will be kept for a longer period.

We understand that the privacy and security of customer information is important.

Microsoft takes a thoughtful and comprehensive approach to customer privacy and the

protection of customer data in Azure Stack Hub. IT administrators have controls to

customize features and privacy settings at any time. Our commitment to transparency

and trust is clear:

We're open with customers about the types of data we gather.

We put enterprise customers in control -- they can customize their own privacy

settings.

We put customer privacy and security first.

We're transparent about how telemetry data gets used.

We use telemetry data to improve customer experiences.

Microsoft doesn't intend to gather sensitive data, like credit card numbers, usernames

and passwords, email addresses, or similar sensitive information. If we determine that

sensitive information has been inadvertently received, we delete it.

Privacy considerations

Telemetry plays an important role in helping to quickly identify and fix critical reliability

issues in customer deployments and configurations. Insights from telemetry data can

help identify issues with services or hardware configurations. Microsoft's ability to get

this data from customers and drive improvements to the ecosystem raises the bar for

the quality of integrated Azure Stack Hub solutions.

Telemetry also helps Microsoft to better understand how customers deploy

components, use features, and use services to achieve their business goals. These

insights help prioritize engineering investments in areas that can directly impact

customer experiences and workloads.

Some examples include customer use of containers, storage, and networking

configurations that are associated with Azure Stack Hub roles. We also use the insights

to drive improvements and intelligence into Azure Stack Hub management and

monitoring solutions. These improvements make it easier for customers to diagnose

issues and save money by making fewer support calls to Microsoft.

We don't recommend turning off telemetry in your organization. However, in some

scenarios it may be necessary.

In these scenarios, you can configure the telemetry level sent to Microsoft by using

registry settings before you deploy Azure Stack Hub, or by using the Telemetry

Endpoints after you deploy Azure Stack Hub.

Before you change telemetry settings, you should understand the telemetry levels and

what data is collected at each level.

The telemetry settings are grouped into four levels (0-3) that are cumulative and

categorized as the follows:

0 (Security)

Security data only. Information that's required to keep the operating system secure. This

includes data about the Connected User Experience and Telemetry component settings,

and Windows Defender. No telemetry specific to Azure Stack Hub is emitted at this level.

Examples of how Microsoft uses the telemetry

data

Manage telemetry collection

Telemetry levels and data collection

1 (Basic)

Security data, and Basic Health and Quality data. Basic device information, including:

quality-related data, app compatibility, app usage data, and data from the Security level.

Setting your telemetry level to Basic enables Azure Stack Hub telemetry. The data

gathered at this level includes:

Basic device information that provides an understanding about the types and

configurations of native and virtual Windows Server 2019 instances in the

ecosystem. This includes:

Machine attributes, such as the OEM, and model.

Networking attributes, such as the number of network adapters and their speed.

Processor and memory attributes, such as the number of cores, and amount of

installed memory.

Storage attributes, such as the number of drives, type of drive, and drive size.

Telemetry functionality, including the percentage of uploaded events, dropped

events, and the last data upload time.

Quality-related information that helps Microsoft develop a basic understanding of

how Azure Stack Hub is performing. For example, the count of critical alerts on a

particular hardware configuration.

Compatibility data that helps provide an understanding about which Resource

Providers are installed on a system and a virtual machine (VM). This identifies

potential compatibility problems.

2 (Enhanced)

Additional insights, including: how the operating system and Azure Stack Hub services

are used, how these services perform, advanced reliability data, and data from the

Security and Basic levels.

3 (Full)

All data necessary to identify and help to fix problems, plus data from the Security,

Basic, and Enhanced levels.

７ Note

This is the default telemetry setting.

） Important

These telemetry levels only apply to Microsoft Azure Stack Hub components. NonMicrosoft software components and services that are running in the Hardware

Turning off Windows and Azure Stack Hub telemetry also disables SQL telemetry. For

more information about the implications of the Windows Server telemetry settings, see

the Windows Telemetry Whitepaper.

You can use the Windows Registry Editor to manually set the telemetry level on the

physical host computer before you deploy Azure Stack Hub. If a management policy

already exists, such as Group Policy, it overrides this registry setting.

Before you deploy Azure Stack Hub on the development kit host, boot into

CloudBuilder.vhdx and run the following script in an elevated PowerShell window:

PowerShell

To enable or disable telemetry after deployment, you need access to the privileged

endpoint (PEP) which is exposed on the ERCS VMs.

To Enable: Set-Telemetry -Enable

To Disable: Set-Telemetry -Disable

PARAMETER details:

.PARAMETER Enable - Turn on telemetry data upload

Lifecycle Host from Azure Stack Hub hardware partners may communicate with

their cloud services outside of these telemetry levels. You should work with your

Azure Stack Hub hardware solution provider to understand their telemetry policy,

and how you can opt in or opt out.

ASDK: set the telemetry level in the Windows registry

### Get current AllowTelemetry value on DVM Host

(Get-ItemProperty -Path

"HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\DataCollection" `

-Name AllowTelemetry).AllowTelemetry

### Set & Get updated AllowTelemetry value for ASDK-Host

Set-ItemProperty -Path

"HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\DataCollection" `

-Name "AllowTelemetry" -Value '0' # Set this value to 0,1,2,or3.

(Get-ItemProperty -Path

"HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\DataCollection" `

-Name AllowTelemetry).AllowTelemetry

ASDK and Multi-Node: enable or disable telemetry after

deployment

.PARAMETER Disable - Turn off telemetry data upload

Script to enable telemetry:

PowerShell

Script to disable telemetry:

PowerShell

Register Azure Stack Hub with Azure

$ip = "<IP ADDRESS OF THE PEP VM>" # You can also use the machine name

instead of IP here.

$pwd= ConvertTo-SecureString "<CLOUD ADMIN PASSWORD>" -AsPlainText -Force

$cred = New-Object System.Management.Automation.PSCredential ("<DOMAIN

NAME>\CloudAdmin", $pwd)

$psSession = New-PSSession -ComputerName $ip -ConfigurationName

PrivilegedEndpoint -Credential $cred -SessionOption (New-PSSessionOption -

Culture en-US -UICulture en-US)

Invoke-Command -Session $psSession {Set-Telemetry -Enable}

if($psSession)

{

Remove-PSSession $psSession

}

$ip = "<IP ADDRESS OF THE PEP VM>" # You can also use the machine name

instead of IP here.

$pwd= ConvertTo-SecureString "<CLOUD ADMIN PASSWORD>" -AsPlainText -Force

$cred = New-Object System.Management.Automation.PSCredential ("<DOMAIN

NAME>\CloudAdmin", $pwd)

$psSession = New-PSSession -ComputerName $ip -ConfigurationName

PrivilegedEndpoint -Credential $cred -SessionOption (New-PSSessionOption -

Culture en-US -UICulture en-US)

Invoke-Command -Session $psSession {Set-Telemetry -Disable}

if($psSession)

{

Remove-PSSession $psSession

}

Next steps

Register Azure Stack Hub with Azure

Article • 03/14/2023

Register Azure Stack Hub with Azure so you can download Azure Marketplace items

from Azure and set up commerce data reporting back to Microsoft. After you register

Azure Stack Hub, usage is reported to Azure commerce and you can see it under the

Azure billing Subscription ID used for registration.

The information in this article describes registering Azure Stack Hub integrated systems

with Azure. For information about registering the ASDK with Azure, see Azure Stack Hub

registration in the ASDK documentation.

Complete the following prerequisites sections before you register:

Verify your credentials.

Set the PowerShell language mode.

Install PowerShell for Azure Stack Hub.

Download the Azure Stack Hub tools.

Determine your billing model.

） Important

Registration is required to support full Azure Stack Hub functionality, including

offering items in the marketplace. You'll be in violation of Azure Stack Hub licensing

terms if you don't register when using the pay-as-you-use billing model. To learn

more about Azure Stack Hub licensing models, see the How to buy page .

７ Note

For connected registrations, an Azure Active Directory application and associated

service principal is created in the Active Directory directory associated with the

registration. This service principal is used for Azure Stack Hub Marketplace

scenarios (to view and download Azure Marketplace items), uploading usage data

(if Usage Reporting is enabled), diagnostic log collection, and remote support.

Removing or changing this application or service principal results in these scenarios

not working and alerts being raised. If it is deleted, then it can be re-created by

unregistering and then re-registering Azure Stack Hub with Azure.

Prerequisites

Determine your unique registration name.

Before registering Azure Stack Hub with Azure, you must have:

The subscription ID for an Azure subscription. Only EA, CSP, or CSP shared services

subscriptions are supported for registration. CSPs need to decide whether to use a

CSP or APSS subscription.

To get the ID, go to the Azure portal and select All services > General >

Subscriptions, choose the subscription you want to use from the list. Within the

Essentials section, find the Subscription ID. As a best practice, use separate

subscriptions for production and dev or test environments.

The username and password for an account that's an owner for the subscription.

The user account needs to have access to the Azure subscription and have

permissions to create identity apps and service principals in the directory

associated with that subscription. We recommend that you register Azure Stack

Hub with Azure using least-privilege administration. For more information on how

to create a custom role definition that limits access to your subscription for

registration, see create a registration role for Azure Stack Hub.

Registered the Azure Stack Hub resource provider (see the following Register

Azure Stack Hub Resource Provider section for details).

After registration, Azure Active Directory (Azure AD) global administrator permission

isn't required. However, some operations may require the global admin credential (for

example, a resource provider installer script or a new feature requiring a permission to

be granted). You can either temporarily reinstate the account's global admin

permissions or use a separate global admin account that's an owner of the default

provider subscription.

The user that registers Azure Stack Hub is the owner of the service principal in Azure AD.

Only the user who registered Azure Stack Hub can modify the Azure Stack Hub

registration. All other users, even if they're a global admin, must be added to 'Default

Provider Subscription' through 'Access control (IAM)'. If a non-admin user that's not an

Verify your credentials

７ Note

Germany cloud subscriptions aren't currently supported.

owner of the registration service principal attempts to register or re-register Azure Stack

Hub, they may come across a 403 response. A 403 response indicates the user has

insufficient permissions to complete the operation.

If you don't have an Azure subscription that meets these requirements, you can create a

free Azure account here . Registering Azure Stack Hub incurs no cost on your Azure

subscription.

To successfully register Azure Stack Hub, the PowerShell language mode must be set to

FullLanguage. To verify that the current language mode is set to full, open an elevated

PowerShell window and run the following PowerShell cmdlets:

PowerShell

Ensure the output returns FullLanguage. If any other language mode is returned,

registration needs to be run on another machine or the language mode needs to be set

to FullLanguage before continuing.

Use the latest PowerShell for Azure Stack Hub to register with Azure.

If the latest version isn't already installed, see install PowerShell for Azure Stack Hub.

The Azure Stack Hub tools GitHub repository contains PowerShell modules that support

Azure Stack Hub functionality, including registration functionality. During the

registration process, you need to import and use the RegisterWithAzure.psm1

PowerShell module (found in the Azure Stack Hub tools repository) to register your

Azure Stack Hub instance with Azure.

７ Note

If you have more than one Azure Stack Hub, a best practice is to register each

Azure Stack Hub to its own subscription. This makes it easier for you to track usage.

Set the PowerShell language mode

$ExecutionContext.SessionState.LanguageMode

Install PowerShell for Azure Stack Hub

Download the Azure Stack Hub tools

To ensure you're using the latest version, delete any existing versions of the Azure Stack

Hub tools and download the latest version from GitHub before registering with Azure.

A connected deployment allows Azure Stack Hub to connect to the internet, and to

Azure. You can also use either Azure AD or Active Directory Federation Services (AD FS)

as your identity store, and choose from two billing models: pay-as-you-use or capacitybased. You specify the billing model later, while running the registration script.

When you run the registration script, you must provide a unique registration name. An

easy way to associate your Azure Stack Hub subscription with an Azure registration is to

use your Azure Stack Hub Cloud ID.

To determine the Cloud ID for your Azure Stack Hub deployment, see Find your cloud

ID.

Use these steps to register Azure Stack Hub with Azure using the pay-as-you-use billing

model.

７ Note

You can also use the The Operator Access Workstation (OAW) to access the

privileged endpoint (PEP), the Administrator portal for support scenarios, and Azure

Stack Hub GitHub Tools. For more information see Azure Stack Hub Operator

Access Workstation.

Determine your billing model

Determine your unique registration name

７ Note

Azure Stack Hub registrations using the capacity-based billing model will need to

change the unique name when re-registering after those yearly subscriptions expire

unless you delete the expired registration and re-register with Azure.

Register with pay-as-you-use billing

７ Note

Connected environments can access the internet and Azure. For these environments,

you need to register the Azure Stack Hub resource provider with Azure and then

configure your billing model.

1. To register the Azure Stack Hub resource provider with Azure, start PowerShell

ISE as an administrator and use the following PowerShell cmdlets with the

EnvironmentName parameter set to the appropriate Azure subscription type

(see parameters below).

2. Add the Azure account that you used to register Azure Stack Hub. To add the

account, run the Connect-AzAccount cmdlet. You're prompted to enter your

Azure account credentials and you may have to use two-factor authentication

based on your account's configuration.

PowerShell

Parameter Description

EnvironmentName The Azure cloud subscription environment name. Supported

environment names are AzureCloud, AzureUSGovernment, or if

using a China Azure Subscription, AzureChinaCloud.

3. If you have multiple subscriptions, run the following command to select the

one you want to use:

PowerShell

All these steps must be run from a computer that has access to the privileged

endpoint (PEP). For details about the PEP, see Using the privileged endpoint in

Azure Stack Hub.

Az modules

Connect-AzAccount -EnvironmentName "<environment name>"

７ Note

If your session expires, your password has changed, or you simply wish to

switch accounts, run the following cmdlet before you sign in using

Connect-AzAccount: Remove-AzAccount-Scope Process

4. Run the following command to register the Azure Stack Hub resource provider

in your Azure subscription:

PowerShell

5. Start PowerShell ISE as an administrator and navigate to the Registration

folder in the AzureStack-Tools-az directory created when you downloaded the

Azure Stack Hub tools. Import the RegisterWithAzure.psm1 module using

PowerShell:

PowerShell

6. Before proceeding, in the same PowerShell session, verify again that you're

signed in to the correct Azure PowerShell context (if not, repeat steps 2 and 3.)

This context would be the Azure account that was used to register the Azure

Stack Hub resource provider previously. In the same PowerShell session, run

the Set-AzsRegistration cmdlet:

PowerShell

For more information on the Set-AzsRegistration cmdlet, see Registration

reference.

The process takes between 10 and 15 minutes. When the command completes, you see

the message "Your environment is now registered and activated using the provided

Get-AzSubscription -SubscriptionID '<Your Azure Subscription GUID>'

| Select-AzSubscription

Register-AzResourceProvider -ProviderNamespace Microsoft.AzureStack

Import-Module .\RegisterWithAzure.psm1

$CloudAdminCred = Get-Credential -UserName <Privileged endpoint

credentials> -Message "Enter the cloud domain credentials to access

the privileged endpoint."

$RegistrationName = "<unique-registration-name>"

Set-AzsRegistration `

-PrivilegedEndpointCredential $CloudAdminCred `

-PrivilegedEndpoint <PrivilegedEndPoint computer name> `

-BillingModel PayAsYouUse `

-RegistrationName $RegistrationName

parameters."

Use these steps to register Azure Stack Hub with Azure using the capacity billing model.

Connected environments can access the internet and Azure. For these environments,

you need to register the Azure Stack Hub resource provider with Azure and then

configure your billing model.

1. To register the Azure Stack Hub resource provider with Azure, start PowerShell

ISE as an administrator and use the following PowerShell cmdlets with the

EnvironmentName parameter set to the appropriate Azure subscription type

(see parameters below).

2. Add the Azure account that you used to register Azure Stack Hub. To add the

account, run the Connect-AzAccount cmdlet. You're prompted to enter your

Azure account credentials and you may have to use two-factor authentication

based on your account's configuration.

PowerShell

Parameter Description

EnvironmentName The Azure cloud subscription environment name. Supported

environment names are AzureCloud, AzureUSGovernment, or if

using a China Azure Subscription, AzureChinaCloud.

3. If you have multiple subscriptions, run the following command to select the

one you want to use:

Register with capacity billing

７ Note

All these steps must be run from a computer that has access to the privileged

endpoint (PEP). For details about the PEP, see Using the privileged endpoint in

Azure Stack Hub.

Az modules

Connect-AzAccount -Environment "<environment name>"

PowerShell

4. Run the following command to register the Azure Stack Hub resource provider

in your Azure subscription:

PowerShell

5. Start PowerShell ISE as an administrator and navigate to the Registration

folder in the AzureStack-Tools-az directory created when you downloaded the

Azure Stack Hub tools. Import the RegisterWithAzure.psm1 module using

PowerShell:

PowerShell

6. Before proceeding, in the same PowerShell session, verify again that you're

signed in to the correct Azure PowerShell context (if not, repeat steps 2 and 3.)

This context is the Azure account that was used to register the Azure Stack

Hub resource provider. In the same PowerShell session, run the SetAzsRegistration cmdlet:

PowerShell

Use the EA agreement number where your capacity SKU licenses were

purchased.

Get-AzSubscription -SubscriptionID '<Your Azure Subscription GUID>'

| Select-AzSubscription

Register-AzResourceProvider -ProviderNamespace Microsoft.AzureStack

Import-Module .\RegisterwithAzure.psm1

$CloudAdminCred = Get-Credential -UserName <Privileged endpoint

credentials> -Message "Enter the cloud domain credentials to access

the privileged endpoint."

$RegistrationName = "<unique-registration-name>"

Set-AzsRegistration `

-PrivilegedEndpointCredential $CloudAdminCred `

-PrivilegedEndpoint <PrivilegedEndPoint computer name> `

-AgreementNumber <EA agreement number> `

-BillingModel Capacity `

-RegistrationName $RegistrationName

７ Note

For more information on the Set-AzsRegistration cmdlet, see Registration

reference.

You can use the Region management tile to verify that the Azure Stack Hub registration

was successful. This tile is available on the default dashboard in the administrator portal.

The status can be registered, or not registered. If registered, it also shows the Azure

subscription ID that you used to register your Azure Stack Hub along with the

registration resource group and name.

1. Sign in to the Azure Stack Hub administrator portal

https://adminportal.local.azurestack.external .

2. From the Dashboard, select Region management.

3. Select Properties. This blade shows the status and details of your environment. The

status can be Registered, Not registered, or Expired.

If registered, the properties include:

Registration subscription ID: The Azure subscription ID registered and

associated to Azure Stack Hub.

You can disable usage reporting with the UsageReportingEnabled

parameter for the Set-AzsRegistration cmdlet by setting the parameter

to false.

Verify Azure Stack Hub registration



Registration resource group: The Azure resource group in the associated

subscription containing the Azure Stack Hub resources.

4. You can use the Azure portal to view Azure Stack Hub registration resources, and

then verify that the registration succeeded. Sign in to the Azure portal using an

account associated to the subscription you used to register Azure Stack Hub.

Select All resources, enable the Show hidden types checkbox, and select the

registration name.

5. If the registration didn't succeed, you must re-register by following the steps here

to resolve the issue.

Alternatively, you can verify if your registration was successful by using the Marketplace

management feature. If you see a list of marketplace items in the Marketplace

management blade, your registration was successful. However, in disconnected

environments, you can't see marketplace items in Marketplace management.

You need to update your registration in the following circumstances:

After you renew your capacity-based yearly subscription.

When you change your billing model.

When your scale changes (add/remove nodes) for capacity-based billing.

You need the following information from the administrator portal to renew or change

registration:

Administrator portal Cmdlet parameter Notes

REGISTRATION

SUBSCRIPTION ID

Subscription Subscription ID used during previous

registration

Renew or change registration

７ Note

If proactive log collection is enabled and you renew or change your Azure Stack

Hub registration, you must re-enable proactive log collection. For more information

on proactive log collection, see Diagnostic log collection.

Prerequisites

Administrator portal Cmdlet parameter Notes

REGISTRATION

RESOURCE GROUP

ResourceGroupName Resource group under which the previous

registration resource exists

REGISTRATION NAME RegistrationName Registration name used during previous

registration

If you want to change the subscription you use, you must first run the RemoveAzsRegistration cmdlet, then ensure you're signed in to the correct Azure PowerShell

context. Then run Set-AzsRegistration with any changed parameters, including <billing

model> . While running Remove-AzsRegistration, you must be signed in to the

subscription used during the registration and use values of the RegistrationName and

ResourceGroupName parameters as shown in the administrator portal:

PowerShell

This section applies if you want to change the billing model, how features are offered, or

you want to re-register your instance. For all of these cases, you call the registration

function to set the new values. You don't need to first remove the current registration.

Change the subscription you use

Az modules

# select the subscription used during the registration (shown in portal)

Select-AzSubscription -Subscription '<Registration subscription ID from

portal>'

# unregister using the parameter values from portal

Remove-AzsRegistration -PrivilegedEndpointCredential

$YourCloudAdminCredential -PrivilegedEndpoint $YourPrivilegedEndpoint -

RegistrationName '<Registration name from portal>' -ResourceGroupName

'<Registration resource group from portal>'

# switch to new subscription id

Select-AzSubscription -Subscription '<New subscription ID>'

# register

Set-AzsRegistration -PrivilegedEndpointCredential

$YourCloudAdminCredential -PrivilegedEndpoint $YourPrivilegedEndpoint -

BillingModel '<Billing model>' -RegistrationName '<Registration name>' -

ResourceGroupName '<Registration resource group name>'

Change billing model, how features are offered, or reregister your instance

Sign in to the subscription ID shown in the administrator portal, and then rerun

registration with a new BillingModel value while keeping the RegistrationName and

ResourceGroupName parameters values same as shown in the administrator portal:

PowerShell

For Azure Stack Hub environments that use a capacity billing model, turn off usage

reporting with the UsageReportingEnabled parameter using either the SetAzsRegistration or the Get-AzsRegistrationToken cmdlets. Azure Stack Hub reports

usage metrics by default. Operators with capacity uses or supporting a disconnected

environment need to turn off usage reporting.

Run the following PowerShell cmdlets:

PowerShell

Az modules

# select the subscription used during the registration

Select-AzSubscription -Subscription '<Registration subscription ID from

portal>'

# rerun registration with new BillingModel (or same billing model in

case of re-registration) but using other parameters values from portal

Set-AzsRegistration -PrivilegedEndpointCredential

$YourCloudAdminCredential -PrivilegedEndpoint $YourPrivilegedEndpoint -

BillingModel '<New billing model>' -RegistrationName '<Registration name

from portal>' -ResourceGroupName '<Registration resource group from

portal>'

Disable or enable usage reporting

$CloudAdminCred = Get-Credential -UserName <Privileged endpoint credentials>

-Message "Enter the cloud domain credentials to access the privileged

endpoint."

$RegistrationName = "<unique-registration-name>"

Set-AzsRegistration `

-PrivilegedEndpointCredential $CloudAdminCred `

-PrivilegedEndpoint <PrivilegedEndPoint computer name> `

-BillingModel Capacity

-RegistrationName $RegistrationName

-UsageReportingEnabled:$false

Move a registration resource

Moving a registration resource between resource groups under the same subscription is

supported for all environments. However, moving a registration resource between

subscriptions is only supported for CSPs when both subscriptions resolve to the same

Partner ID. For more information about moving resources to a new resource group, see

Move resources to new resource group or subscription.

You can use Set-AzsRegistration to register Azure Stack Hub with Azure and enable or

disable the offer of items in the marketplace and usage reporting.

To run the cmdlet, you need:

A global Azure subscription of any type.

To be signed in to Azure PowerShell with an account that's an owner or contributor

to that subscription.

PowerShell

Parameter Type Description

PrivilegedEndpointCredential PSCredential The credentials used to access the privileged

endpoint. The username is in the format

AzureStackDomain\CloudAdmin.

） Important

To prevent accidental deletion of registration resources on the portal, the

registration script automatically adds a lock to the resource. You must remove this

lock before moving or deleting it. It's recommended that you add a lock to your

registration resource to prevent accidental deletion.

Registration reference

Set-AzsRegistration

Set-AzsRegistration [-PrivilegedEndpointCredential] <PSCredential> [-

PrivilegedEndpoint] <String> [[-AzureContext]

<PSObject>] [[-ResourceGroupName] <String>] [[-ResourceGroupLocation]

<String>] [[-BillingModel] <String>]

[-MarketplaceSyndicationEnabled] [-UsageReportingEnabled] [[-

AgreementNumber] <String>] [[-RegistrationName]

<String>] [<CommonParameters>]

Parameter Type Description

PrivilegedEndpoint String A pre-configured remote PowerShell console

that provides you with capabilities like log

collection and other post deployment tasks. To

learn more, refer to the using the privileged

endpoint article.

AzureContext PSObject

ResourceGroupName String

ResourceGroupLocation String

BillingModel String The billing model that your subscription uses.

Allowed values for this parameter are: Capacity,

PayAsYouUse, and Development.

MarketplaceSyndicationEnabled True/False Determines if the marketplace management

feature is available in the portal. Set to true if

registering with internet connectivity. Set to

false if registering in disconnected

environments. For disconnected registrations,

the offline syndication tool can be used for

downloading marketplace items.

UsageReportingEnabled True/False Azure Stack Hub reports usage metrics by

default. Operators with capacity uses or

supporting a disconnected environment need

to turn off usage reporting. Allowed values for

this parameter are: True, False.

AgreementNumber String The number of the EA agreement under which

the Capacity SKU for this Azure Stack was

ordered.

RegistrationName String Set a unique name for the registration if you're

running the registration script on more than

one instance of Azure Stack Hub using the same

Azure Subscription ID. The parameter has a

default value of AzureStackRegistration.

However, if you use the same name on more

than one instance of Azure Stack Hub, the script

fails.

Get-AzsRegistrationToken generates a registration token from the input parameters.

Get-AzsRegistrationToken

PowerShell

Parameter Type Description

PrivilegedEndpointCredential PSCredential The credentials used to access the privileged

endpoint. The username is in the format

AzureStackDomain\CloudAdmin.

PrivilegedEndpoint String A pre-configured remote PowerShell console

that provides you with capabilities like log

collection and other post deployment tasks. To

learn more, refer to the using the privileged

endpoint article.

AzureContext PSObject

ResourceGroupName String

ResourceGroupLocation String

BillingModel String The billing model that your subscription uses.

Allowed values for this parameter are: Capacity,

Custom, and Development.

MarketplaceSyndicationEnabled True/False

UsageReportingEnabled True/False Azure Stack Hub reports usage metrics by

default. Operators with capacity uses or

supporting a disconnected environment need

to turn off usage reporting. Allowed values for

this parameter are: True, False.

AgreementNumber String

You might see one of the errors below while attempting to register your Azure Stack

Hub:

Couldn't retrieve mandatory hardware info for $hostName . Check physical host and

connectivity, then try to rerun registration.

Get-AzsRegistrationToken [-PrivilegedEndpointCredential] <PSCredential> [-

PrivilegedEndpoint] <String>

[-BillingModel] <String> [[-TokenOutputFilePath] <String>] [-

UsageReportingEnabled] [[-AgreementNumber] <String>]

[<CommonParameters>]

Registration failures

Can't connect to $hostName to get hardware info. Check physical host and

connectivity, then try to rerun registration.

Cause: We tried to obtain hardware details such as UUID, Bios, and CPU from the

hosts to attempt activation and weren't able to due to the inability to connect to

the physical host.

Cloud identifier [ GUID ] is already registered. Reusing cloud identifiers isn't allowed.

Cause: this happens if your Azure Stack environment is already registered. If you

want to re-register your environment with a different subscription or billing model,

follow the Renew or change registration steps.

When trying to access Marketplace management, an error occurs when trying to

syndicate products.

Cause: this usually happens when Azure Stack Hub is unable to access the

registration resource. One common reason for this is that when an Azure

subscription's directory tenant changes, it resets the registration. You can't access

the Azure Stack Hub Marketplace or report usage if you've changed the

subscription's directory tenant. You need to re-register to fix this issue.

Download marketplace items from Azure

Next steps

Region management in Azure Stack Hub

Article • 06/04/2021

Azure Stack Hub uses the concept of regions, which are logical entities comprised of the

hardware resources that make up the Azure Stack Hub infrastructure. In region

management, you can find all resources that are required to successfully operate the

Azure Stack Hub infrastructure.

One integrated system deployment (referred to as an Azure Stack Hub cloud) makes up

a single region. Each Azure Stack Development Kit (ASDK) has one region, named local.

If you deploy a second Azure Stack Hub integrated system, or you set up another

instance of the ASDK on separate hardware, this Azure Stack Hub cloud is a different

region.

Azure Stack Hub has a set of region management capabilities available in the Region

management tile. This tile is available to an Azure Stack Hub operator on the default

dashboard in the administrator portal. In this screen, you can monitor and update your

Azure Stack Hub region and its components, which are region-specific.

If you select a region in the Region management tile, you can access the following

information:

Information available through the region

management tile

1. The resource menu: Access different infrastructure management areas, and view

and manage user resources such as storage accounts and virtual networks.

2. Alerts: List system-wide alerts and provide details on each of those alerts.

3. Updates: View the current version of your Azure Stack Hub infrastructure, available

updates, and the update history. You can also update your integrated system.

4. Resource providers: Manage the user functionality offered by the components

required to run Azure Stack Hub. Each resource provider comes with an

administrative experience. This experience can include alerts for the specific

provider, metrics, and other management capabilities specific to the resource

provider.

5. Infrastructure roles: The components necessary to run Azure Stack Hub. Only the

infrastructure roles that report alerts are listed. By selecting a role, you can view

the alerts associated with the role and the role instances where this role is running.

6. Properties: The registration status and details of your environment in the region

management blade. The status can be Registered, Not registered, or Expired. If

registered, it also shows the Azure subscription ID that you used to register your

Azure Stack Hub, along with the registration resource group and name.

Monitor health and alerts in Azure Stack Hub

Manage updates in Azure Stack Hub



Next steps

Connect Azure Stack Hub to Azure using

Azure ExpressRoute

Article • 02/08/2021

This article describes how to connect an Azure Stack Hub virtual network to an Azure

virtual network using a Microsoft Azure ExpressRoute direct connection.

You can use this article as a tutorial and use the examples to set up the same test

environment. Or, you can read the article as a walkthrough that guides you through

setting up your own ExpressRoute environment.

Azure ExpressRoute lets you extend your on-premises networks into the Microsoft cloud

over a private connection supplied by a connectivity provider. ExpressRoute is not a VPN

connection over the public internet.

For more information about Azure ExpressRoute, see the ExpressRoute overview.

This article assumes that:

You have a working knowledge of Azure.

You have a basic understanding of Azure Stack Hub.

You have a basic understanding of networking.

To connect Azure Stack Hub and Azure using ExpressRoute, you must meet the

following requirements:

A provisioned ExpressRoute circuit through a connectivity provider.

An Azure subscription to create an ExpressRoute circuit and VNets in Azure.

A router that must:

Support site-to-site VPN connections between its LAN interface and Azure Stack

Hub multi-tenant gateway.

Support creating multiple VRFs (Virtual Routing and Forwarding) if there is more

than one tenant in your Azure Stack Hub deployment.

A router that has:

Overview, assumptions, and prerequisites

Assumptions

Prerequisites

A WAN port connected to the ExpressRoute circuit.

A LAN port connected to the Azure Stack Hub multi-tenant gateway.

The following figure shows the Azure Stack Hub and Azure environments after you finish

setting up ExpressRoute using the examples in this article:

The following figure shows how multiple tenants connect from the Azure Stack Hub

infrastructure through the ExpressRoute router to Azure:

ExpressRoute network architecture

The example in this article uses the same multi-tenant architecture shown in this

diagram to connect Azure Stack Hub to Azure using ExpressRoute private peering. The

connection is done using a site-to-site VPN connection from the virtual network

gateway in Azure Stack Hub to an ExpressRoute router.

The steps in this article show you how to create an end-to-end connection between two

VNets from two different tenants in Azure Stack Hub to corresponding VNets in Azure.

Setting up two tenants is optional; you can also use these steps for a single tenant.

To set up the Azure Stack Hub environment for the first tenant, use the following steps

as a guide. If you're setting up more than one tenant, repeat these steps:

Configure Azure Stack Hub

７ Note

These steps show how to create resources using the Azure Stack Hub portal, but

you can also use PowerShell.

Before you start configuring Azure Stack Hub, you need:

An Azure Stack Hub deployment.

An offer in Azure Stack Hub that your users can subscribe to. For more information,

see Service, plan, offer, subscription overview.

Use the following procedures to create the required network resources in Azure Stack

Hub for a tenant.

1. Sign in to the Azure Stack Hub user portal.

2. In the portal, select + Create a resource.

3. Under Azure Marketplace, select Networking.

4. Under Featured, select Virtual network.

5. Under Create virtual network, enter the values shown in the following table into

the appropriate fields:

Field Value

Name Tenant1VNet1

Address space 10.1.0.0/16

Subnet name Tenant1-Sub1

Subnet address range 10.1.1.0/24

6. You should see the subscription you created earlier populated in the Subscription

field. For the remaining fields:

Under Resource group, select Create new to create a new resource group or

if you already have one, select Use existing.

Before you begin

Create network resources in Azure Stack Hub

Create the virtual network and VM subnet

Verify the default Location.

Click Create.

(Optional) Click Pin to dashboard.

1. Under Virtual network, select Tenant1VNet1.

2. Under SETTINGS, select Subnets.

3. Select + Gateway subnet to add a gateway subnet to the virtual network.

4. The name of the subnet is set to GatewaySubnet by default. Gateway subnets are

a special case and must use this name to function correctly.

5. Verify that the Address range is 10.1.0.0/24.

6. Click OK to create the gateway subnet.

1. In the Azure Stack Hub user portal, click + Create a resource.

2. Under Azure Marketplace, select Networking.

3. Select Virtual network gateway from the list of network resources.

4. In the Name field, enter GW1.

5. Select Virtual network.

6. Select Tenant1VNet1 from the drop-down list.

7. Select Public IP address, then Choose public IP address, and then click Create

new.

8. In the Name field, type GW1-PiP, and then click OK.

9. The VPN type should have Route-based selected by default. Keep this setting.

10. Verify that Subscription and Location are correct. Click Create.

The local network gateway resource identifies the remote gateway at the other end of

the VPN connection. For this example, the remote end of the connection is the LAN subinterface of the ExpressRoute router. For Tenant 1 in the previous diagram, the remote

address is 10.60.3.255.

1. Sign in to the Azure Stack Hub user portal and select + Create a resource.

2. Under Azure Marketplace, select Networking.

3. Select local network gateway from the list of resources.

4. In the Name field, type ER-Router-GW.

Create the gateway subnet

Create the virtual network gateway

Create the local network gateway

5. For the IP address field, see the previous figure. The IP address of the

ExpressRoute router LAN sub-interface for Tenant 1 is 10.60.3.255. For your own

environment, enter the IP address of your router's corresponding interface.

6. In the Address Space field, enter the address space of the VNets that you want to

connect to in Azure. The subnets for Tenant 1 are as follows:

192.168.2.0/24 is the hub VNet in Azure.

10.100.0.0/16 is the spoke VNet in Azure.

7. Verify that your Subscription, Resource Group, and Location are correct. Then

select Create.

1. In the Azure Stack Hub user portal, select + Create a resource.

2. Under Azure Marketplace, select Networking.

3. Select Connection from the list of resources.

4. Under Basics, choose Site-to-site (IPSec) as the Connection type.

5. Select the Subscription, Resource group, and Location. Click OK.

6. Under Settings, select Virtual network gateway, and then select GW1.

7. Select Local network gateway, and then select ER Router GW.

8. In the Connection name field, enter ConnectToAzure.

9. In the Shared key (PSK) field, enter abc123 and then select OK.

10. Under Summary, select OK.

After you create the virtual network gateway, you can get the gateway's public IP

address. Make a note of this address in case you need it later for your deployment.

Depending on your deployment, this address is used as the Internal IP address.

1. In the Azure Stack Hub user portal, select All resources.

2. Under All resources, select the virtual network gateway, which is GW1 in the

example.

） Important

This example assumes that you are using static routes for the site-to-site VPN

connection between the Azure Stack Hub gateway and the ExpressRoute

router.

Create the connection

Get the virtual network gateway public IP address

3. Under Virtual network gateway, select Overview from the list of resources.

Alternatively, you can select Properties.

4. The IP address that you want to note is listed under Public IP address. For the

example configuration, this address is 192.68.102.1.

To test data traffic over the VPN connection, you need VMs to send and receive data in

the Azure Stack Hub VNet. Create a VM and deploy it to the VM subnet for your virtual

network.

1. In the Azure Stack Hub user portal, select + Create a resource.

2. Under Azure Marketplace, select Compute.

3. In the list of VM images, select the Windows Server 2016 Datacenter Eval image.

4. In Create virtual machine, select Basics, then type VM01 as the Name.

5. Enter a valid user name and password. You'll use this account to sign in to the VM

after it has been created.

6. Provide a Subscription, Resource group, and a Location. Select OK.

7. Under Choose a size, select a VM size for this instance, and then select Select.

8. Under Settings, confirm that:

The virtual network is Tenant1VNet1.

The subnet is set to 10.1.1.0/24.

Use the default settings and click OK.

9. Under Summary, review the VM configuration and then click OK.

To add more tenants, repeat the steps you followed in these sections:

Create the virtual network and VM subnet

Create the gateway subnet

Create the virtual network gateway

Create a virtual machine (VM)

７ Note

If the image used for this article is not available, ask your Azure Stack Hub

operator to provide a different Windows Server image.

Create the local network gateway

Create the connection

Create a virtual machine

If you're using Tenant 2 as an example, remember to change the IP addresses to avoid

overlaps.

The ASDK is self-contained and isolated from the network where the physical host is

deployed. The VIP network that the gateways are connected to is not external; it is

hidden behind a router performing Network Address Translation (NAT).

The router is the ASDK host running the Routing and Remote Access Services (RRAS)

role. You must configure NAT on the ASDK host to enable the site-to-site VPN

connection to connect on both ends.

1. Sign in to the Azure Stack Hub host computer with your admin account.

2. Run the script in an elevated PowerShell ISE. This script returns your External

BGPNAT address.

PowerShell

3. To configure the NAT, copy and edit the following PowerShell script. Edit the script

to replace the External BGPNAT address and Internal IP address with the

following example values:

For External BGPNAT address use 10.10.0.62

For Internal IP address use 192.168.102.1

Run the following script from an elevated PowerShell ISE:

Configure the NAT VM for gateway traversal

） Important

This section is for ASDK deployments only. The NAT is not needed for multi-node

deployments.

Configure the NAT

Get-NetNatExternalAddress

PowerShell

After you finish configuring Azure Stack Hub, you can deploy the Azure resources. The

following figure shows an example of a tenant virtual network in Azure. You can use any

name and addressing scheme for your VNet in Azure. However, the address range of the

VNets in Azure and Azure Stack Hub must be unique and must not overlap:

$ExtBgpNat = 'External BGPNAT address'

$IntBgpNat = 'Internal IP address'

# Designate the external NAT address for the ports that use the IKE

authentication.

Add-NetNatExternalAddress `

-NatName BGPNAT `

-IPAddress $Using:ExtBgpNat `

-PortStart 499 `

-PortEnd 501

Add-NetNatExternalAddress `

-NatName BGPNAT `

-IPAddress $Using:ExtBgpNat `

-PortStart 4499 `

-PortEnd 4501

# Create a static NAT mapping to map the external address to the

Gateway public IP address to map the ISAKMP port 500 for PHASE 1 of the

IPSEC tunnel.

Add-NetNatStaticMapping `

-NatName BGPNAT `

-Protocol UDP `

-ExternalIPAddress $Using:ExtBgpNat `

-InternalIPAddress $Using:IntBgpNat `

-ExternalPort 500 `

-InternalPort 500

# Configure NAT traversal which uses port 4500 to establish the

complete IPSEC tunnel over NAT devices.

Add-NetNatStaticMapping `

-NatName BGPNAT `

-Protocol UDP `

-ExternalIPAddress $Using:ExtBgpNat `

-InternalIPAddress $Using:IntBgpNat `

-ExternalPort 4500 `

-InternalPort 4500

Configure Azure

The resources you deploy in Azure are similar to the resources you deployed in Azure

Stack Hub. You deploy the following components:

Virtual networks and subnets

A gateway subnet

A virtual network gateway

A connection

An ExpressRoute circuit

The example Azure network infrastructure is configured as follows:

A standard hub (192.168.2.0/24) and spoke (10.100.0.0./16) VNet model. For more

information about hub-spoke network topology, see Implement a hub-spoke

network topology in Azure.

The workloads are deployed in the spoke VNet and the ExpressRoute circuit is

connected to the hub VNet.

The two VNets are connected using VNet peering.

1. Sign in to the Azure portal with your Azure credentials.

2. Create the hub VNet using the 192.168.2.0/24 address range.

3. Create a subnet using the 192.168.2.0/25 address range, and add a gateway subnet

using the 192.168.2.128/27 address range.

4. Create the spoke VNet and subnet using the 10.100.0.0/16 address range.

For more information about creating virtual networks in Azure, see Create a virtual

network.

1. Review the ExpressRoute prerequisites in ExpressRoute prerequisites & checklist.

2. Follow the steps in Create and modify an ExpressRoute circuit to create an

ExpressRoute circuit using your Azure subscription.

3. Follow the steps in Create and modify peering for an ExpressRoute circuit to

configure private peering on the ExpressRoute circuit.

Follow the steps in Configure a virtual network gateway for ExpressRoute using

PowerShell to create a virtual network gateway for ExpressRoute in the hub VNet.

To link the ExpressRoute circuit to the hub VNet, follow the steps in Connect a virtual

network to an ExpressRoute circuit.

Peer the hub and spoke VNets using the steps in Create a virtual network peering using

the Azure portal. When configuring VNet peering, make sure you use the following

options:

Configure the Azure VNets

Configure an ExpressRoute circuit

７ Note

Give the service key for your circuit to your service so they can set up your

ExpressRoute circuit at their end.

Create the virtual network gateway

Create the connection

Peer the VNets

From the hub to the spoke, Allow gateway transit.

From the spoke to the hub, Use remote gateway.

Deploy your workload VMs into the spoke VNet.

Repeat these steps for any additional tenant VNets you want to connect in Azure

through their respective ExpressRoute circuits.

You can use the following ExpressRoute router configuration diagram as a guide for

configuring your ExpressRoute Router. This figure shows two tenants (Tenant 1 and

Tenant 2) with their respective ExpressRoute circuits. Each tenant is linked to their own

VRF (Virtual Routing and Forwarding) in the LAN and WAN side of the ExpressRoute

router. This configuration ensures end-to-end isolation between the two tenants. Take

note of the IP addresses used in the router interfaces as you follow the configuration

example.

Create a virtual machine

Configure the router

You can use any router that supports IKEv2 VPN and BGP to terminate the site-to-site

VPN connection from Azure Stack Hub. The same router is used to connect to Azure

using an ExpressRoute circuit.

The following Cisco ASR 1000 Series Aggregation Services Router configuration example

supports the network infrastructure shown in the ExpressRoute router configuration

diagram.

shell

ip vrf Tenant 1

description Routing Domain for PRIVATE peering to Azure for Tenant 1

rd 1:1

!

ip vrf Tenant 2

description Routing Domain for PRIVATE peering to Azure for Tenant 2

rd 1:5

!

crypto ikev2 proposal V2-PROPOSAL2

description IKEv2 proposal for Tenant 1

encryption aes-cbc-256

integrity sha256

group 2

crypto ikev2 proposal V4-PROPOSAL2

description IKEv2 proposal for Tenant 2

encryption aes-cbc-256

integrity sha256

group 2

!

crypto ikev2 policy V2-POLICY2

description IKEv2 Policy for Tenant 1

match fvrf Tenant 1

match address local 10.60.3.255

proposal V2-PROPOSAL2

description IKEv2 Policy for Tenant 2

crypto ikev2 policy V4-POLICY2

match fvrf Tenant 2

match address local 10.60.3.251

proposal V4-PROPOSAL2

!

crypto ikev2 profile V2-PROFILE

description IKEv2 profile for Tenant 1

match fvrf Tenant 1

match address local 10.60.3.255

match identity remote any

authentication remote pre-share key abc123

authentication local pre-share key abc123

ivrf Tenant 1

!

crypto ikev2 profile V4-PROFILE

description IKEv2 profile for Tenant 2

match fvrf Tenant 2

match address local 10.60.3.251

match identity remote any

authentication remote pre-share key abc123

authentication local pre-share key abc123

ivrf Tenant 2

!

crypto ipsec transform-set V2-TRANSFORM2 esp-gcm 256

mode tunnel

crypto ipsec transform-set V4-TRANSFORM2 esp-gcm 256

mode tunnel

!

crypto ipsec profile V2-PROFILE

set transform-set V2-TRANSFORM2

set ikev2-profile V2-PROFILE

!

crypto ipsec profile V4-PROFILE

set transform-set V4-TRANSFORM2

set ikev2-profile V4-PROFILE

!

interface Tunnel10

description S2S VPN Tunnel for Tenant 1

ip vrf forwarding Tenant 1

ip address 11.0.0.2 255.255.255.252

ip tcp adjust-mss 1350

tunnel source TenGigabitEthernet0/1/0.211

tunnel mode ipsec ipv4

tunnel destination 10.10.0.62

tunnel vrf Tenant 1

tunnel protection ipsec profile V2-PROFILE

!

interface Tunnel20

description S2S VPN Tunnel for Tenant 2

ip vrf forwarding Tenant 2

ip address 11.0.0.2 255.255.255.252

ip tcp adjust-mss 1350

tunnel source TenGigabitEthernet0/1/0.213

tunnel mode ipsec ipv4

tunnel destination 10.10.0.62

tunnel vrf VNET3

tunnel protection ipsec profile V4-PROFILE

!

interface GigabitEthernet0/0/1

description PRIMARY ExpressRoute Link to AZURE over Equinix

no ip address

negotiation auto

!

interface GigabitEthernet0/0/1.100

description Primary WAN interface of Tenant 1

description PRIMARY ER link supporting Tenant 1 to Azure

encapsulation dot1Q 101

ip vrf forwarding Tenant 1

ip address 192.168.1.1 255.255.255.252

!

interface GigabitEthernet0/0/1.102

description Primary WAN interface of Tenant 2

description PRIMARY ER link supporting Tenant 2 to Azure

encapsulation dot1Q 102

ip vrf forwarding Tenant 2

ip address 192.168.1.17 255.255.255.252

!

interface GigabitEthernet0/0/2

description BACKUP ExpressRoute Link to AZURE over Equinix

no ip address

negotiation auto

!

interface GigabitEthernet0/0/2.100

description Secondary WAN interface of Tenant 1

description BACKUP ER link supporting Tenant 1 to Azure

encapsulation dot1Q 101

ip vrf forwarding Tenant 1

ip address 192.168.1.5 255.255.255.252

!

interface GigabitEthernet0/0/2.102

description Secondary WAN interface of Tenant 2

description BACKUP ER link supporting Tenant 2 to Azure

encapsulation dot1Q 102

ip vrf forwarding Tenant 2

ip address 192.168.1.21 255.255.255.252

!

interface TenGigabitEthernet0/1/0

description Downlink to ---Port 1/47

no ip address

!

interface TenGigabitEthernet0/1/0.211

description LAN interface of Tenant 1

description Downlink to --- Port 1/47.211

encapsulation dot1Q 211

ip vrf forwarding Tenant 1

ip address 10.60.3.255 255.255.255.254

!

interface TenGigabitEthernet0/1/0.213

description LAN interface of Tenant 2

description Downlink to --- Port 1/47.213

encapsulation dot1Q 213

ip vrf forwarding Tenant 2

ip address 10.60.3.251 255.255.255.254

!

router bgp 65530

bgp router-id <removed>

bgp log-neighbor-changes

description BGP neighbor config and route advertisement for Tenant 1 VRF

address-family ipv4 vrf Tenant 1

network 10.1.0.0 mask 255.255.0.0

network 10.60.3.254 mask 255.255.255.254

network 192.168.1.0 mask 255.255.255.252

network 192.168.1.4 mask 255.255.255.252

neighbor 10.10.0.62 remote-as 65100

neighbor 10.10.0.62 description VPN-BGP-PEER-for-Tenant 1

neighbor 10.10.0.62 ebgp-multihop 5

neighbor 10.10.0.62 activate

neighbor 10.60.3.254 remote-as 4232570301

neighbor 10.60.3.254 description LAN peer for CPEC:INET:2112 VRF

neighbor 10.60.3.254 activate

neighbor 10.60.3.254 route-map BLOCK-ALL out

neighbor 192.168.1.2 remote-as 12076

neighbor 192.168.1.2 description PRIMARY ER peer for Tenant 1 to Azure

neighbor 192.168.1.2 ebgp-multihop 5

neighbor 192.168.1.2 activate

neighbor 192.168.1.2 soft-reconfiguration inbound

neighbor 192.168.1.2 route-map Tenant 1-ONLY out

neighbor 192.168.1.6 remote-as 12076

neighbor 192.168.1.6 description BACKUP ER peer for Tenant 1 to Azure

neighbor 192.168.1.6 ebgp-multihop 5

neighbor 192.168.1.6 activate

neighbor 192.168.1.6 soft-reconfiguration inbound

neighbor 192.168.1.6 route-map Tenant 1-ONLY out

maximum-paths 8

exit-address-family

!

description BGP neighbor config and route advertisement for Tenant 2 VRF

address-family ipv4 vrf Tenant 2

network 10.1.0.0 mask 255.255.0.0

network 10.60.3.250 mask 255.255.255.254

network 192.168.1.16 mask 255.255.255.252

network 192.168.1.20 mask 255.255.255.252

neighbor 10.10.0.62 remote-as 65300

neighbor 10.10.0.62 description VPN-BGP-PEER-for-Tenant 2

neighbor 10.10.0.62 ebgp-multihop 5

neighbor 10.10.0.62 activate

neighbor 10.60.3.250 remote-as 4232570301

neighbor 10.60.3.250 description LAN peer for CPEC:INET:2112 VRF

neighbor 10.60.3.250 activate

neighbor 10.60.3.250 route-map BLOCK-ALL out

neighbor 192.168.1.18 remote-as 12076

neighbor 192.168.1.18 description PRIMARY ER peer for Tenant 2 to Azure

neighbor 192.168.1.18 ebgp-multihop 5

neighbor 192.168.1.18 activate

neighbor 192.168.1.18 soft-reconfiguration inbound

neighbor 192.168.1.18 route-map VNET-ONLY out

neighbor 192.168.1.22 remote-as 12076

neighbor 192.168.1.22 description BACKUP ER peer for Tenant 2 to Azure

neighbor 192.168.1.22 ebgp-multihop 5

neighbor 192.168.1.22 activate

neighbor 192.168.1.22 soft-reconfiguration inbound

neighbor 192.168.1.22 route-map VNET-ONLY out

maximum-paths 8

exit-address-family

!

ip forward-protocol nd

!

ip as-path access-list 1 permit ^$

ip route vrf Tenant 1 10.1.0.0 255.255.0.0 Tunnel10

ip route vrf Tenant 2 10.1.0.0 255.255.0.0 Tunnel20

!

ip prefix-list BLOCK-ALL seq 5 deny 0.0.0.0/0 le 32

!

route-map BLOCK-ALL permit 10

match ip address prefix-list BLOCK-ALL

Test your connection after you establish the site-to-site connection and the

ExpressRoute circuit.

Perform the following ping tests:

Sign in to one of the VMs in your Azure VNet and ping the VM you created in

Azure Stack Hub.

Sign in to one of the VMs you created in Azure Stack Hub and ping the VM you

created in the Azure VNet.

By default, Windows Server 2016 does not allow incoming ICMP packets through the

firewall. For every VM that you use for ping tests, you must allow incoming ICMP

packets. To create a firewall rule for ICMP, run the following cmdlet in an elevated

PowerShell window:

PowerShell

1. Sign in to the Azure Stack Hub user portal.

2. Find the VM that you created and select it.

!

route-map VNET-ONLY permit 10

match as-path 1

!

Test the connection

７ Note

To make sure you are sending traffic over the site-to-site and ExpressRoute

connections, you must ping the dedicated IP (DIP) address of the VM at both ends

and not the VIP address of the VM.

Allow ICMP in through the firewall

# Create ICMP firewall rule.

New-NetFirewallRule `

-DisplayName "Allow ICMPv4-In" `

-Protocol ICMPv4

Ping the Azure Stack Hub VM

3. Select Connect.

4. From an elevated Windows or PowerShell command prompt, enter ipconfig /all.

Note the IPv4 address returned in the output.

5. Ping the IPv4 address from the VM in the Azure VNet.

In the example environment, the IPv4 address is from the 10.1.1.x/24 subnet. In

your environment, the address might be different, but it should be in the subnet

you created for the tenant VNet subnet.

If you want to know how much traffic is passing through your connection, you can find

this information on the Azure Stack Hub user portal. Viewing data transfer statistics is

also a good way to find out whether or not your ping test data went through the VPN

and ExpressRoute connections:

1. Sign in to the Azure Stack Hub user portal and select All resources.

2. Navigate to the resource group for your VPN Gateway and select the Connection

object type.

3. Select the ConnectToAzure connection from the list.

4. Under Connections > Overview, you can see statistics for Data in and Data out.

You should see some non-zero values.

Deploy apps to Azure and Azure Stack Hub

View data transfer statistics

Next steps

Enable Azure CLI for Azure Stack Hub

users

Article • 03/30/2023

You can provide the CA root certificate to users of Azure Stack Hub so that they can

enable Azure CLI on their development machines. Your users need the certificate to

manage resources through CLI.

The Azure Stack Hub CA root certificate is required if users are using CLI from a

workstation outside the Azure Stack Development Kit (ASDK).

The virtual machine (VM) aliases endpoint provides an alias, like "UbuntuLTS" or

"Win2012Datacenter," that references an image publisher, offer, SKU, and version

as a single parameter when deploying VMs.

The following sections describe how to get these values.

If you're using an integrated system, you don't need to export the CA root certificate.

You need to export the CA root certificate on the ASDK.

To export the ASDK root certificate in PEM format, sign in and run the following script:

PowerShell

Export the Azure Stack Hub CA root certificate

$label = "AzureStackSelfSignedRootCert"

Write-Host "Getting certificate from the current user trusted store with

subject CN=$label"

$root = Get-ChildItem Cert:\CurrentUser\Root | Where-Object Subject -eq

"CN=$label" | select -First 1

if (-not $root)

{

Write-Error "Certificate with subject CN=$label not found"

return

}

Write-Host "Exporting certificate"

Export-Certificate -Type CERT -FilePath root.cer -Cert $root

Write-Host "Converting certificate to PEM format"

certutil -encode root.cer root.pem

Azure Stack Hub operators should set up a publicly accessible endpoint that hosts a VM

alias file. The VM alias file is a JSON file that provides a common name for an image. You

use the name when you deploy a VM as an Azure CLI parameter.

Before you add an entry to an alias file, make sure that you download images from the

Azure Marketplace or have published your own custom image. If you publish a custom

image, make note of the publisher, offer, SKU, and version info that you specified during

publishing. If it's an image from the marketplace, you can view the info by using the

Get-AzureVMImage cmdlet.

A sample alias file with many common image aliases is available. You can use that as a

starting point. Host this file in a space where your CLI clients can reach it. One way is to

host the file in a blob storage account and share the URL with your users:

1. Download the sample file from GitHub.

2. Create a storage account in Azure Stack Hub. When that's done, create a blob

container. Set the access policy to "public."

3. Upload the JSON file to the new container. When that's done, you can view the

URL of the blob. Select the blob name and then select the URL from the blob

properties.

Deploy templates with Azure CLI

Connect with PowerShell

Manage user permissions

Set up the VM aliases endpoint

Next steps

Azure Stack Hub VPN Fast Path public

preview for operators

Article • 05/18/2023

Azure Stack Hub is introducing the three new SKUs described in this article as part of the

VPN Fast Path public preview. Previously, S2S tunnels were limited to a maximum

bandwidth of 200 Mbps using the HighPerformance SKU. The new SKUs enable

customer scenarios in which higher network throughput is necessary. The throughput

values for each SKU are unidirectional values, meaning it supports the given throughput

on either of send or receive traffic.

With the introduction of the VPN Fast Path feature in Azure Stack Hub, tenant users can

create VPN connections using 3 new SKUs:

Basic

Standard

High Performance

VpnGw1 (new)

VpnGw2 (new)

VpnGw3 (new)

To make any update process go as smoothly as possible so that there's minimal impact

on your users, it's important to prepare your Azure Stack Hub stamp.

As the Azure Stack Hub operator enabling VPN Fast Path, we recommend that you

coordinate with tenant users to schedule a maintenance window during which the

changeover can happen. Notify your users of any possible VPN connection service

outages, and then follow the steps here to prepare your stamp for the update.

What is the Azure Stack Hub VPN Fast Path

feature?

New VPN Fast Path virtual network gateway

SKUs

Important considerations before enabling

Azure Stack Hub VPN Fast Path

Azure Stack Hub VPN Fast Path relies on the new SDN Gateway service, and it comes

with a new requirement when planning.

List of existing virtual network gateway resources settings.

List of existing connections resources settings.

List of IPSec policies and settings used on their existing connections.

This step ensures your users have policies configured that work with their

device, including custom IPSec policies.

List local network gateway settings. Tenant users can re-use local network gateway

resources and configurations. However, we also recommend that you save the

existing configuration in case they need to be re-created.

Once VPN Fast Path is enabled, tenants must re-create their virtual network

gateways and connections as appropriate if they want to use the new SKUs.

With the release of the VPN Fast Path public preview, there is a new PowerShell

command that operators can call to list all the existing connections created by their

tenants. This cmdlet can help the operator manage capacity and reach out to the tenant

admins if they need to recreate their Virtual Network gateways:

PowerShell

For more information, see Get-AzsVirtualNetworkGatewayConnection.

For the VPN Fast Path public preview, operators can enable the new feature using the

following PowerShell commands. Once the feature reaches general availability, the

operators can also enable the feature using the Azure Stack Hub administrator portal.

You can adjust existing setups by re-creating the virtual network gateway and its

connections with one of the new SKUs.

VPN Fast Path requires NAT-T on remote VPN devices

Plan with tenant users before enabling VPN Fast Path

Get-AzsVirtualNetworkGatewayConnection

How to enable Azure Stack Hub VPN Fast Path

Enable Azure Stack Hub VPN Fast Path using PowerShell

From the Azure Stack Hub privileged endpoint, you can run the following PowerShell

command to enable the VPN Fast Path feature:

For more information about the Azure Stack Hub PEP, see Access privileged endpoint.

PowerShell

Once the VPN Fast Path feature is enabled, you can validate the current state of the

Gateway VMs and the used capacity using the following PowerShell command:

PowerShell

Set-AzSVPNFastPath -Enable



Validate Azure Stack Hub VPN Fast Path is enabled using

PowerShell

Get-AzSVPNFastPath



PowerShell

If you need to disable VPN Fast Path, you must first work with your tenant to delete and

recreate all their Virtual Network Gateways using VPN Fast Path SKUs. Because stamp

VPN capacity increases when VPN Fast Path is enabled, you can't disable VPN Fast Path

if the overall in-use capacity exceeds the total capacity when Azure Stack Hub isn't using

VPN Fast Path.

There are three multi-tenant gateway infrastructure VMs in Azure Stack Hub. Two of

these VMs are in active mode, and the third is in redundant mode. Active VMs enable

the creation of VPN connections on them, and the redundant VM only accepts VPN

connections if a failover happens. If an active gateway VM becomes unavailable, the

VPN connection fails over to the redundant VM after a short period (a few seconds) of

connection loss.

Gateway connection failovers are expected during an OEM or an Azure Stack Hub

update, as the VMs are patched and live migrated. This failover can result in a temporary

disconnect of the tunnels.

Disable Azure Stack Hub VPN Fast Path using PowerShell

Set-AzSVPNFastPath -Disable

Azure Stack Hub Gateway Pool architecture

The overall Gateway Pool capacity of an Azure Stack Hub stamp is 4 Gbps. This capacity

is divided between the two Active Gateway VMs, with each Gateway VM supporting up

to 2 Gbps of throughput. When a connection resource is created, twice its SKU is

reserved on the Gateway VM. This design ensures that the maximum throughput of the

SKU (measured in one direction) can be reached with either Tx or Rx traffic, depending

on the requirements of the user workload.

For example, a HighPerformance SKU reserves 400 Mbps on a Gateway VM (200 for Tx,

200 for Rx). This means that on the existing engine, a HighPerformance connection

reserves one tenth of the overall Gateway Pool capacity.

The following table shows the gateway types and the estimated aggregate throughput

for each tunnel/connection by gateway SKU when VPN Fast Path is disabled:

SKU Max VPN Connection

throughput (1)

Max # of VPN

Connections per active

GW VM

Max # of VPN

Connections per stamp

(2)

Basic (3) 100 Mbps Tx/Rx 10 20

Standard 100 Mbps Tx/Rx 10 20



New Gateway Pool total capacity

SKU Max VPN Connection

throughput (1)

Max # of VPN

Connections per active

GW VM

Max # of VPN

Connections per stamp

(2)

High

Performance

200 Mbps Tx/Rx 5 10

(1) - Tunnel throughput is not a guaranteed throughput for cross-premises connections

across the internet; it's the maximum possible throughput measurement. The total

aggregate in one direction is 2 Gbps.

(2) - Max tunnels is the total per Azure Stack Hub deployment for all subscriptions.

(3) - BGP routing isn't supported for the Basic SKU.

Once the operator enables VPN Fast Path on the Azure Stack Hub stamp, the overall

Gateway Pool capacity is increased to 10 Gbps. Since the capacity is divided between the

two active Gateway VMs, each Gateway VM has a capacity of 5 Gbps. The amount of

capacity reserved for each connection is the same as outlined in the previous section.

Therefore, a VpnGw3 SKU (1250 Mbps) reserves 2500 Mbps of capacity on a Gateway

VM:

SKU Max VPN Connection

throughput (1)

Max # of VPN

Connections per active

GW VM

Max # of VPN

Connections per stamp

(2)

Basic (3) 100 Mbps Tx/Rx 25 50

Standard 100 Mbps Tx/Rx 25 50

High

Performance

200 Mbps Tx/Rx 12 24



Estimated aggregate tunnel throughput by SKU with VPN

Fast Path Enabled

SKU Max VPN Connection

throughput (1)

Max # of VPN

Connections per active

GW VM

Max # of VPN

Connections per stamp

(2)

VPNGw1 650 Mbps Tx/Rx 3 6

VPNGw2 1000 Mbps Tx/Rx 2 4

VPNGw3 1250 Mbps Tx/Rx 2 4

(1) - Tunnel throughput is not a guaranteed throughput for cross-premises connections

across the internet; it's the maximum possible throughput measurement. The total

aggregate in one direction is 5 Gbps.

(2) - Max tunnels is the total per Azure Stack Hub deployment for all subscriptions.

(3) - BGP routing isn't supported for the Basic SKU.

VPN gateway configuration settings for Azure Stack Hub



Next steps

Install PowerShell Az and Azure Stack

modules for Azure Stack Hub

Article • 08/16/2023

Azure Stack Hub Version AzureStack PowerShell version

2102 2.1.1

2108 2.2.0

2206 2.3.0

2301 2.4.0

For more information about AzureStack modules, see the PSGallery .

This article explains how to install the Azure PowerShell Az and compatible Azure Stack

Hub administrator modules using PowerShellGet. The Az modules can be installed on

Windows, macOS, and Linux platforms.

You can also run the Az modules for Azure Stack Hub in a Docker container. For

instructions, see Use Docker to run PowerShell for Azure Stack Hub.

If you would like to install PowerShell Resource Modules (AzureRM) module for Azure

Stack Hub, see Install PowerShell AzureRM module for Azure Stack Hub.

You can use API profiles to specify the compatible endpoints for the Azure Stack Hub

resource providers.

API profiles provide a way to manage version differences between Azure and Azure

Stack Hub. An API version profile is a set of Azure Resource Manager PowerShell

modules with specific API versions. Each cloud platform has a set of supported API

version profiles. For example, Azure Stack Hub supports a specific profile version such as

2020-09-01-hybrid. When you install a profile, the Azure Resource Manager PowerShell

modules that correspond to the specified profile are installed.

） Important

There will likely not be new Azure Resource Modules module releases. The Azure

Resource Modules modules are under support for critical fixes only. Going forward

there will only be Az releases for Azure Stack Hub.

You can install Azure Stack Hub compatible PowerShell Az modules in Internetconnected, partially connected, or disconnected scenarios. This article walks you

through the detailed instructions for these scenarios.

Az modules are supported on Azure Stack Hub with Update 2002 or later and with the

current hotfixes installed. See the Azure Stack Hub release notes for more information.

The Azure PowerShell Az modules work with PowerShell 5.1 or higher on Windows, or

PowerShell Core 6.x and later on all platforms. You should install the latest version of

PowerShell Core available for your operating system. Azure PowerShell has no other

requirements when run on PowerShell Core.

To check your PowerShell version, run the command:

PowerShell

To use Azure PowerShell in PowerShell 5.1 on Windows:

1. Update to Windows PowerShell 5.1 if needed. If you're on Windows 10, you

already have PowerShell 5.1 installed.

2. Install .NET Framework 4.7.2 or later.

3. Make sure you have the latest version of PowerShellGet. Run the following cmdlets

from an elevated prompt:

PowerShell

1. Verify your prerequisites

$PSVersionTable.PSVersion

Prerequisites for Windows

[Net.ServicePointManager]::SecurityProtocol =

[Net.SecurityProtocolType]::Tls12

powershell -noprofile

$PSVersionTable

Uninstall-Module PowershellGet -AllVersions -Force -Confirm:$false

Get-module PowershellGet

Find-module PowershellGet

Install-Module PowershellGet -MinimumVersion 2.2.3 -Force

PowerShell Core 6.x or later version is needed. Follow the link for instructions

Before installing the required version, make sure that you uninstall any previously

installed Azure Stack Hub Azure Resource Manager or Az PowerShell modules. Uninstall

the modules by using one of the following two methods:

1. To uninstall the existing Azure Resource Manager and Az PowerShell modules,

close all the active PowerShell sessions, and run the following cmdlets:

PowerShell

If you hit an error such as 'The module is already in use', close the PowerShell

sessions that are using the modules and rerun the above script.

2. If the Uninstall-Module did not succeed, delete all the folders that start with Azure ,

Az , or Azs. from the $env:PSModulePath locations. For Windows PowerShell, the

locations might be C:\Program Files\WindowsPowerShell\Modules and C:\Users\

{yourusername}\Documents\WindowsPowerShell\Modules . For PowerShell Core, the

locations might be C:\Program Files\PowerShell\7\Modules and C:\Users\

{yourusername}\Documents\PowerShell\Modules . Deleting these folders removes any

existing Azure PowerShell modules.

The Azure Stack Az module will work with PowerShell 5.1 or greater on a Windows

machine, or PowerShell 6.x or greater on a Linux or macOS platform. Using the

PowerShellGet cmdlets is the preferred installation method. This method works the

same on the supported platforms.

2. Prerequisites for Linux and Mac

3. Uninstall existing versions of the Azure Stack

Hub PowerShell modules

Get-Module -Name Azure\* -ListAvailable | Uninstall-Module -Force -

Verbose -ErrorAction Continue

Get-Module -Name Azs.\* -ListAvailable | Uninstall-Module -Force -

Verbose -ErrorAction Continue

Get-Module -Name Az.\* -ListAvailable | Uninstall-Module -Force -Verbose

-ErrorAction Continue

4. Connected: Install with internet connectivity

1. Run the following command from a PowerShell session to update PowerShellGet to

a minimum of version 2.2.3

PowerShell

2. Close your PowerShell session, then open a new PowerShell session so that update

can take effect.

3. Run the following to install Az modules.

PowerShell

4. Install AzureStack PowerShell modules.

PowerShell

In a disconnected scenario, you first download the PowerShell modules to a machine

that has internet connectivity. Then, you transfer them to the Azure Stack Development

Kit (ASDK) for installation.

[Net.ServicePointManager]::SecurityProtocol =

[Net.SecurityProtocolType]::Tls12

Install-Module PowerShellGet -MinimumVersion 2.2.3 -Force

[Net.ServicePointManager]::SecurityProtocol =

[Net.SecurityProtocolType]::Tls12

Install-Module -Name Az.BootStrapper -Force

Install-AzProfile -Profile 2020-09-01-hybrid -Force

Install-Module -Name AzureStack -RequiredVersion 2.1.1

２ Warning

You can't have both the Azure Resource Manager (AzureRM) and Az modules

installed for PowerShell 5.1 for Windows at the same time. If you need to keep

Azure Resource Manager available on your system, install the Az module for

PowerShell Core 6.x or later. To do this, install PowerShell Core 6.x or later and

then follow these instructions in a PowerShell Core terminal.

5. Disconnected: Install without internet

connection

Sign in to a computer with internet connectivity and use the following scripts to

download the Azure Resource Manager and Azure Stack Hub packages, depending on

your version of Azure Stack Hub.

Installation has five steps:

1. Install Azure Stack Hub PowerShell to a connected machine.

2. Enable additional storage features.

3. Transport the PowerShell packages to your disconnected workstation.

4. Manually bootstrap the NuGet provider on your disconnected workstation.

5. Confirm the installation of PowerShell.

1. You could either use AzureRM or Az modules. The following code saves Az

modules from trustworthy online repository https://www.powershellgallery.com/ .

PowerShell

2. After the Az modules are installed, proceed with installing the AzureStack modules.

PowerShell

Install Azure Stack Hub PowerShell

[Net.ServicePointManager]::SecurityProtocol =

[Net.SecurityProtocolType]::Tls12

Install-module -Name PowerShellGet -MinimumVersion 2.2.3 -Force

Import-Module -Name PackageManagement -ErrorAction Stop

$savedModulesPath = "<Path that is used to save the packages>"

Save-Package -ProviderName NuGet -Source

https://www.powershellgallery.com/api/v2 -Name Az -Path

$savedModulesPath -Force -RequiredVersion 2.0.1

Save-Package -ProviderName NuGet -Source

https://www.powershellgallery.com/api/v2 -Name AzureStack -Path

$savedModulesPath -Force -RequiredVersion 2.1.1

７ Note

On machines without an internet connection, we recommend executing the

following cmdlet for disabling the telemetry data collection. You may experience a

performance degradation of the cmdlets without disabling the telemetry data

collection. This is applicable only for the machines without internet connections

PowerShell

1. Copy the downloaded packages to a USB device.

2. Sign in to the disconnected workstation and copy the packages from the USB

device to a location on the workstation.

3. Manually bootstrap the NuGet provider on your disconnected workstation. For

instructions, see Manually bootstrapping the NuGet provider on a machine that

isn't connected to the internet.

4. Register this location as the default repository and install the AzureRM and

AzureStack modules from this repository:

PowerShell

5. Install the Az modules.

PowerShell

6. Install the AzureStack modules.

PowerShell

Disable-AzDataCollection

Add your packages to your workstation

# requires -Version 5

# requires -RunAsAdministrator

# requires -Module PowerShellGet

# requires -Module PackageManagement

$SourceLocation = "<Location on the development kit that contains the

PowerShell packages>"

$RepoName = "MyNuGetSource"

[Net.ServicePointManager]::SecurityProtocol =

[Net.SecurityProtocolType]::Tls12

Register-PSRepository -Name $RepoName -SourceLocation $SourceLocation

-InstallationPolicy Trusted

Install-Module -Name Az -Repository $RepoName -RequiredVersion 2.0.1 -

Scope AllUsers

Install-Module -Name AzureStack -Repository $RepoName -RequiredVersion

2.1.1 -Scope AllUsers

Confirm the installation by running the following command:

PowerShell

In scenarios that require a proxy server to access the internet, you first configure

PowerShell to use an existing proxy server:

1. Open an elevated PowerShell prompt.

2. Run the following commands:

PowerShell

You can use the cmdlets and code samples based on AzureRM modules. However, you

will want to change the name of the modules and cmdlets. The module names have

been changed so that AzureRM and Azure become Az , and the same for cmdlets. For

example, the AzureRM.Compute module has been renamed to Az.Compute . New-AzureRMVM

has become New-AzVM , and Get-AzureStorageBlob is now Get-AzStorageBlob .

For a more thorough discussion and guidance for moving AzurRM script to Az and

breaking changes in Azure Stack Hub's Az module, see Migrate from AzureRM to Azure

PowerShell Az.

Confirm the installation of PowerShell

Get-Module -Name "Az\*" -ListAvailable

Get-Module -Name "Azs\*" -ListAvailable

6. Configure PowerShell to use a proxy server

#To use Windows credentials for proxy authentication

[System.Net.WebRequest]::DefaultWebProxy.Credentials =

[System.Net.CredentialCache]::DefaultCredentials

#Alternatively, to prompt for separate credentials that can be used for

#proxy authentication

[System.Net.WebRequest]::DefaultWebProxy.Credentials = Get-Credential

7. Use the Az module

Known issues

Applicable: This issue applies to 2002 and later

Cause: When installing the module, an error is thrown. The error message begins:

Register-PacakgeSource : A parameter cannot be found that matches parameter

name. 'PackageManagementProvider'. Or the error message may include the

following text: PackageManagement\Install-Package : Cannot convert value "2.0.1-

preview" to type "System.Version". Error: "Input string was not in a correct

format."

Remediation: Run the following cmdlet in the same session:

Install-Module PowershellGet -MinimumVersion 2.3.0 -Force

Close your session and start a new elevated PowerShell session.

Occurrence: Common

Applicable: This issue applies to 2002 and later

Cause: When installing the module from an elevated prompt, an error is thrown.

The error says, Administrator rights required .

Remediation: Close your session and start a new elevated PowerShell session.

Make sure there isn't an existing Az. Accounts module loaded in the session.

Occurrence: Common

Applicable: This issue applies to the 2020-09-01-hybrid profile.

Cause: The cmdlet New-AzVmss does not work with the 2020-09-01-hybrid profile.

Remediation: Use a template for creating virtual machine scale set. You can find a

sample the Azure Stack Hub Resource Manager templates in the GitHub

Repository AzureStack-QuickStart-Templates/101-vmss-windows-vm and you

can find instruction on using Azure Stack Hub Resource Managers with Visual

Studio Code.

Occurrence: Common

Applicable: This issue applies to 2002 and later.

Error thrown when installing the Az modules

When installing Az module falsely throws Admin rights

required error

Cmdlet New-AzVmss fails when using 2020-09-01-hybrid

profile

Error thrown when running a PowerShell script

Cause: When running scripts or PowerShell commands using the Azure Stack Hub

specific modules, you will need your script or command to be available in the

module. You may see the following error:

PowerShell

The current module is the PowerShell Az module, which has replaced the

PowerShell AzureRM module. If you attempt to run a script that calls for AzureRM

commands when the Az module is installed, your script will throw errors. Or if you

attempt to run a script that calls Az commands when the AzureRM module is

installed, your script will throw errors.

Remediation: Uninstall the AzureRM module and install the Az module. For

instructions, see Install PowerShell Az module for Azure Stack Hub. If you're using

the Azure Stack Hub Tools, use the Az tools. Clone the tools repository from the az

branch, or download the AzureStack-Tools from the az branch. For instructions, see

Download Azure Stack Hub tools from GitHub

Occurrence: Common

Applicable: Azure Stack environments using Azure Active Directory (Azure AD).

Cause: Azure Active Directory Graph introduced a breaking change to restrict the

IdentifierUri for Active Directory applications to be the subdomains of a verified

domain in the directory. Before the change, this restriction was only enforced for

the multi-tenant apps. Now this restriction applies to single tenant apps as well.

The change will result in the following error: Values of identifierUris property

must use a verified domain of the organization or its subdomain' is displayed

when running .

Remediation: You can work around this restriction in two ways.

Method 'get\_SerializationSettings' in type

'Microsoft.Azure.Management.Internal.Resources.ResourceManagementClient

' from assembly 'Microsoft.Azure.Commands.ResourceManager.Common,

Version=4.0.0.0,

Culture=neutral, PublicKeyToken=31bf3856ad364e35' does not have an

implementation.

Error thrown with New-AzADServicePrincipal and NewAzADApplication

You'll need to use a service principle name that is a subdomain of the directory

tenant. For example, if the directory is contoso.onmicrosoft.com , the service

principal name has to be of the form of <foo>.contoso.onmicrosoft.com . Use the

following cmdlet:

PowerShell

For more information about identity and using service principals with Azure

Stack Hub, see Overview of identity providers for Azure Stack Hub.

Create the Azure AD app providing a valid IdentifierUri and then create the

service principal associating the app using the following cmdlet:

PowerShell

Occurrence: Common

Applicable: This issue applies to all supported releases.

Cause: A SharedTokenCacheCredential authentication failed error is thrown when

having multiple versions of AzAccounts installed with Azure Stack Hub PowerShell

Module version 2.1.1.

Remediation: Remove all versions of AzAccounts and only install the supported

AzAccounts version 2.2.8.

Occurrence: Common

Download Azure Stack Hub tools from GitHub

Configure the Azure Stack Hub user's PowerShell environment

Configure the Azure Stack Hub operator's PowerShell environment

Manage API version profiles in Azure Stack Hub

New-AzADServicePrincipal -Role Owner -DisplayName

<foo>.contoso.onmicrosoft.com

$app=New-AzADApplication -DisplayName 'newapp' -IdentifierUris

http://anything.contoso.onmicrosoft.com

New-AzADServicePrincipal -Role Owner -ApplicationId

$app.ApplicationId

Error: "SharedTokenCacheCredential authentication

failed"

Next steps

Install PowerShell AzureRM module for

Azure Stack Hub

Article • 07/29/2022

Azure PowerShell Azure Resource Manager (AzureRM) provides a set of cmdlets that use

the Azure Resource Manager model for managing your Azure Stack Hub resources.

You also need to use API profiles to specify the compatible endpoints for the Azure Stack

Hub resource providers.

API profiles provide a way to manage version differences between Azure and Azure

Stack Hub. An API version profile is a set of Azure Resource Manager PowerShell

modules with specific API versions. Each cloud platform has a set of supported API

version profiles. For example, Azure Stack Hub supports a specific profile version such as

2019-03-01-hybrid. When you install a profile, the Azure Resource Manager PowerShell

modules that correspond to the specified profile are installed.

You can install Azure Stack Hub compatible PowerShell modules in internet-connected,

partially connected, or disconnected scenarios. This article walks you through the

detailed instructions for these scenarios.

You can also run the Azure Resource Manager modules for Azure Stack Hub in a Docker

container. For instructions, see Use Docker to run PowerShell for Azure Stack Hub.

） Important

You've reached a webpage for an outdated version of Azure Stack Hub PowerShell.

All versions of the Azure Resource Manager (AzureRM) PowerShell module are

outdated, but not out of support. AzureRM modules will no longer be updated in

future Azure Stack Hub builds. Az modules will be used for builds 2002 and later.

The 2020-09-01-hybrid profile is not supported for AzureRM modules.

The Az PowerShell module is now the recommended PowerShell module for

interacting with Azure and Azure Stack Hub. To get started with the Az PowerShell

module, see Install PowerShell Az preview module for Azure Stack Hub. To learn

how to migrate to the Az PowerShell module. see Migrate from AzureRM to Azure

PowerShell Az in Azure Stack Hub. For details on the increased functionality of the

Az modules, which have been adopted across global Azure, see Introducing the

Azure Az PowerShell module.

Before you get started with Azure Stack Hub and the PowerShell Azure Resource

Manager module, you must have the following prerequisites:

PowerShell Version 5.1

To check your version, run $PSVersionTable.PSVersion and compare the Major

version. If you don't have PowerShell 5.1, follow the Installing Windows PowerShell.

Run PowerShell in an elevated command prompt.

PowerShell Gallery access

You need access to the PowerShell Gallery . The gallery is the central repository

for PowerShell content. The PowerShellGet module contains cmdlets for

discovering, installing, updating, and publishing PowerShell artifacts. Examples of

these artifacts are modules, DSC resources, role capabilities, and scripts from the

PowerShell Gallery and other private repositories. If you're using PowerShell in a

disconnected scenario, you must retrieve resources from a machine with a

connection to the internet and store them in a location accessible to your

disconnected machine.

Validate if PSGallery is registered as a repository.

Open an elevated PowerShell prompt, and run the following cmdlets:

PowerShell

1. Verify your prerequisites

７ Note

PowerShell 5.1 requires a Windows machine.

2. Validate the PowerShell Gallery accessibility

７ Note

This step requires internet access.

Install-module -Name PowerShellGet -Force

Import-Module -Name PackageManagement -ErrorAction Stop

Get-PSRepository -Name "PSGallery"

If the repository isn't registered, open an elevated PowerShell session and run the

following command:

PowerShell

Before installing the required version, make sure that you uninstall any previously

installed Azure Stack Hub Azure Resource Manager PowerShell modules. Uninstall the

modules by using one of the following two methods:

1. To uninstall the existing Azure Resource Manager and Az PowerShell modules,

close all the active PowerShell sessions, and run the following cmdlets:

PowerShell

If you hit an error such as 'The module is already in use', close the PowerShell

sessions that are using the modules and rerun the above script.

2. Delete all the folders that start with Azure , Az or Azs. from the C:\Program

Files\WindowsPowerShell\Modules and C:\Users\

{yourusername}\Documents\WindowsPowerShell\Modules folders. Deleting these

folders removes any existing PowerShell modules.

The API version profile and Azure Stack Hub PowerShell modules you require will

depend on the version of Azure Stack Hub you're running.

Register-PSRepository -Default

Set-PSRepository -Name "PSGallery" -InstallationPolicy Trusted

3. Uninstall existing versions of the Azure Stack

Hub PowerShell modules

Get-Module -Name Azure\* -ListAvailable | Uninstall-Module -Force -

Verbose -ErrorAction Continue

Get-Module -Name Azs.\* -ListAvailable | Uninstall-Module -Force -

Verbose -ErrorAction Continue

Get-Module -Name Az.\* -ListAvailable | Uninstall-Module -Force -Verbose

-ErrorAction Continue

4. Connected: Install PowerShell for Azure Stack

Hub with internet connectivity

Run the following PowerShell script to install these modules on your development

workstation:

For Azure Stack Hub 2002 or later:

You can use either user AzureRm modules or Az preview modules. The use of the Az

modules requires Azure Stack Hub 2002 or later.

To use Az preview modules, follow the instructions at Install PowerShell Az module.

PowerShell

Confirm the installation by running the following command:

PowerShell

If the installation is successful, the AzureRm and AzureStack modules are displayed in the

output.

In a disconnected scenario, you first download the PowerShell modules to a machine

that has internet connectivity. Then, you transfer them to the Azure Stack Development

Kit (ASDK) for installation.

Sign in to a computer with internet connectivity and use the following scripts to

download the Azure Resource Manager and Azure Stack Hub packages, depending on

Install Azure Stack Hub PowerShell

# Install the AzureRM.BootStrapper module. Select Yes when prompted to

install NuGet

Install-Module -Name AzureRM.BootStrapper

# Install and import the API Version Profile required by Azure Stack Hub

into the current PowerShell session.

Use-AzureRmProfile -Profile 2019-03-01-hybrid -Force

Install-Module -Name AzureStack -RequiredVersion 1.8.3

Confirm the installation of PowerShell

Get-Module -Name "Azure\*" -ListAvailable

Get-Module -Name "Azs\*" -ListAvailable

5. Disconnected: Install PowerShell without an

internet connection

your version of Azure Stack Hub.

Installation has five steps:

1. Install Azure Stack Hub PowerShell to a connected machine.

2. Enable additional storage features.

3. Transport the PowerShell packages to your disconnected workstation.

4. Manually bootstrap the NuGet provider on your disconnected workstation.

5. Confirm the installation of PowerShell.

Azure Stack Hub 2002 or later.

You could either use Azure Resource Manager or Az preview modules. For Az modules,

see instructions at Install PowerShell Az module.

PowerShell

Install Azure Stack Hub PowerShell

Install-module -Name PowerShellGet -Force

Import-Module -Name PackageManagement -ErrorAction Stop

$Path = "<Path that is used to save the packages>"

Save-Package -ProviderName NuGet -Source

https://www.powershellgallery.com/api/v2 -Name AzureRM -Path $Path -Force -

RequiredVersion 2.5.0

Save-Package -ProviderName NuGet -Source

https://www.powershellgallery.com/api/v2 -Name AzureStack -Path $Path -Force

-RequiredVersion 1.8.3

７ Note

On machines without an internet connection, we recommend executing the

following cmdlet for disabling the telemetry data collection. You may experience a

performance degradation of the cmdlets without disabling the telemetry data

collection. This is applicable only for the machines without internet connections

PowerShell

Disable-AzureRmDataCollection

Add your packages to your workstation

1. Copy the downloaded packages to a USB device.

2. Sign in to the disconnected workstation and copy the packages from the USB

device to a location on the workstation.

3. Manually bootstrap the NuGet provider on your disconnected workstation. For

instructions, see Manually bootstrapping the NuGet provider on a machine that

isn't connected to the internet.

4. Register this location as the default repository and install the Azure Resource

Manager and AzureStack modules from this repository:

PowerShell

Confirm the installation by running the following command:

PowerShell

In scenarios that require a proxy server to access the internet, you first configure

PowerShell to use an existing proxy server:

1. Open an elevated PowerShell prompt.

# requires -Version 5

# requires -RunAsAdministrator

# requires -Module PowerShellGet

# requires -Module PackageManagement

$SourceLocation = "<Location on the development kit that contains the

PowerShell packages>"

$RepoName = "MyNuGetSource"

Register-PSRepository -Name $RepoName -SourceLocation $SourceLocation -

InstallationPolicy Trusted

Install-Module -Name AzureRM -Repository $RepoName

Install-Module -Name AzureStack -Repository $RepoName

Confirm the installation of PowerShell

Get-Module -Name "Azure\*" -ListAvailable

Get-Module -Name "Azs\*" -ListAvailable

6. Configure PowerShell to use a proxy server

2. Run the following commands:

PowerShell

Cause: The PowerShell Az module and PowerShell Azure Resource Manager

modules are not compatible.

The following error indicates that the Azure Resource Manager modules and Az

modules are loaded in the same session:

PowerShell

Remediation: Uninstall the conflicting modules.

If you would like to use the Azure Resource Manager modules, uninstall the Az

modules. Or uninstall the Azure Resource Manager if you would like to use the Az

modules. Close your PowerShell session and uninstall either the Az or Azure

Resource Manager modules.

You can find instructions at Uninstall existing versions of the Azure Stack Hub

PowerShell modules.

Applicable: Azure Stack environments using Azure Active Directory (Azure AD).

#To use Windows credentials for proxy authentication

[System.Net.WebRequest]::DefaultWebProxy.Credentials =

[System.Net.CredentialCache]::DefaultCredentials

#Alternatively, to prompt for separate credentials that can be used for

#proxy authentication

[System.Net.WebRequest]::DefaultWebProxy.Credentials = Get-Credential

Known issue

Method get\_SerializationSettings error

> Method 'get\_SerializationSettings' in type

'Microsoft.Azure.Management.Internal.Resources.ResourceManagementClient

' from assembly 'Microsoft.Azure.Commands.ResourceManager.Common,

Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35' does

not have an implementation.

Error thrown with NewAzureRMADServicePrincipal and

NewAzureRMAdApplication

Cause: Azure Active Directory Graph introduced a breaking change to restrict the

IdentifierUri for Active Directory applications to be the subdomains of a verified

domain in the directory. Before the change, this restriction was only enforced for

the multi-tenant apps. Now this restriction applies to single tenant apps as well.

The change will result in the following error: Values of identifierUris property

must use a verified domain of the organization or its subdomain' is displayed

when running .

Remediation: You can work around this restriction in two ways.

You'll need to use a service principal name that is a subdomain of the directory

tenant. For example, if the directory is contoso.onmicrosoft.com , the service

principal name has to be of the form of <foo>.contoso.onmicrosoft.com . Use the

following cmdlet:

PowerShell

For more information about identity and using service principals with Azure

Stack Hub, see Overview of identity providers for Azure Stack Hub.

Create the Azure AD app providing a valid IdentifierUri and then create the

service principal associating the app using the following cmdlet:

PowerShell

Occurrence: Common

Download Azure Stack Hub tools from GitHub

Configure the Azure Stack Hub user's PowerShell environment

Configure the Azure Stack Hub operator's PowerShell environment

Manage API version profiles in Azure Stack Hub

NewAzureRMADServicePrincipal -Role Owner -DisplayName

<foo>.contoso.onmicrosoft.com

$app=NewAzureRMAdApplication -DisplayName 'newapp' -IdentifierUris

http://anything.contoso.onmicrosoft.com

NewAzureRMADServicePrincipal -Role Owner -ApplicationId

$app.ApplicationId

Next steps

Migrate from AzureRM to Azure

PowerShell Az in Azure Stack Hub

Article • 03/06/2023

The Az module has feature parity with AzureRM, but uses shorter and more consistent

cmdlet names. Scripts written for the AzureRM cmdlets won't automatically work with

the new module. To make the transition easier, Az offers tools to allow you to run your

existing scripts using AzureRM. No migration to a new command set is ever convenient,

but this article will help you get started on transitioning to the new module.

To see the full list of breaking changes between AzureRM and Az, see the Migration

guide for Az 1.0.0

Before taking any migration steps, check which versions of AzureRM are installed on

your system. Doing so allows you to make sure scripts are already running on the latest

release, and let you know if you can enable command aliases without uninstalling

AzureRM.

To check which version(s) of AzureRM you have installed, run the command:

PowerShell

This is the most important step! Run your existing scripts, and make sure that they work

with the latest release of AzureRM (2.5.0). If your scripts don't work, make sure to read

the AzureRM migration guide.

The first step is to install the Az module on your platform. When you install Az, it's

recommended that you uninstall AzureRM. In the following steps, you'll learn how to

keep running your existing scripts and enable compatibility for old cmdlet names.

To install the Azure PowerShell Az module, follow these steps:

Check for installed versions of AzureRM

Get-InstalledModule -Name AzureRM -AllVersions

Check current scripts work with AzureRM

Install the Azure PowerShell Az module

Recommended: Uninstall the AzureRM module. Make sure that you remove all

installed versions of AzureRM, not just the most recent version.

Install the Az module

With AzureRM uninstalled and your scripts working with the latest AzureRM version, the

next step is to enable the compatibility mode for the Az module. Compatibility is

enabled with the command:

PowerShell

Aliases enable the ability to use old cmdlet names with the Az module installed. These

aliases are written to the user profile for the selected scope. If no user profile exists, one

is created.

Once the alias mode is enabled, run your scripts again to confirm that they still function

as expected.

Enable AzureRM compatibility aliases

） Important

Only enable compatibility mode if you've uninstalled all versions of AzureRM.

Enabling compatibility mode with AzureRM cmdlets still available may result in

unpredictable behavior. Skip this step if you decided to keep AzureRM installed,

but be aware that any AzureRM cmdlets will use the older modules and not call any

Az cmdlets.

Enable-AzureRmAlias -Scope CurrentUser

２ Warning

You can use a different -Scope for this command, but it's not recommended.

Aliases are written to the user profile for the selected scope, so keep enabling them

to as limited a scope as possible. Enabling aliases system-wide could also cause

issues for other users which have AzureRM installed in their local scope.

Change module and cmdlet names

In general, the module names have been changed so that AzureRM and Azure become

Az , and the same for cmdlets. For example, the AzureRM.Compute module has been

renamed to Az.Compute . New-AzureRMVM has become New-AzVM , and GetAzureStorageBlob is now Get-AzStorageBlob .

There are exceptions to this naming change that you should be aware of. Some modules

were renamed or merged into existing modules without this affecting the suffix of their

cmdlets, other than changing AzureRM or Azure to Az . Otherwise, the full cmdlet suffix

was changed to reflect the new module name.

AzureRM module Az module Cmdlet suffix changed?

AzureRM.Profile Az.Accounts Yes

AzureRM.Insights Az.Monitor Yes

AzureRM.Tags Az.Resources No

AzureRM.UsageAggregates Az.Billing No

AzureRM.Consumption Az.Billing No

By following these steps, you can update all of your existing scripts to use the new

module. If you have any questions or problems with these steps that made your

migration difficult, please comment on this article so that we can improve the

instructions.

This document provides detailed information on the changes between AzureRM 6.x and

the new Az module, version 1.x and later. The table of contents will help guide you

through a full migration path, including module-specific changes that may affect your

scripts.

This section details the general breaking changes that are part of the redesign of the Az

module.

Summary

Breaking changes for Az 1.0.0

General breaking changes

In the AzureRM module, cmdlets used either AzureRM or Azure as a noun prefix. Az

simplifies and normalizes cmdlet names, so that all cmdlets use 'Az' as their cmdlet noun

prefix. For example:

PowerShell

Has changed to:

PowerShell

To make the transition to these new cmdlet names simpler, Az introduces two new

cmdlets, Enable-AzureRmAlias and Disable-AzureRmAlias. Enable-AzureRmAlias creates

aliases for the older cmdlet names in AzureRM that map to the newer Az cmdlet names.

Using the -Scope argument with Enable-AzureRmAlias allows you to choose where

aliases are enabled.

For example, the following script in AzureRM:

PowerShell

Can be run with minimal changes using Enable-AzureRmAlias :

PowerShell

Running Enable-AzureRmAlias -Scope CurrentUser will enable the aliases for all

PowerShell sessions you open, so that after executing this cmdlet, a script like this would

not need to be changed at all:

PowerShell

Cmdlet noun prefix changes

Get-AzureRMVM

Get-AzureKeyVaultSecret

Get-AzVM

Get-AzKeyVaultSecret

#Requires -Modules AzureRM.Storage

Get-AzureRmStorageAccount | Get-AzureStorageContainer | Get-AzureStorageBlob

#Requires -Modules Az.Storage

Enable-AzureRmAlias -Scope Process

Get-AzureRmStorageAccount | Get-AzureStorageContainer | Get-AzureStorageBlob

For complete details on the usage of the alias cmdlets, see the Enable-AzureRmAlias

reference.

When you're ready to disable aliases, Disable-AzureRmAlias removes the created aliases.

For complete details, see the Disable-AzureRmAlias reference.

The module names have changed from AzureRM.\* to Az.\* , except for the following

modules:

AzureRM module Az module

Azure.Storage Az.Storage

Azure.AnalysisServices Az.AnalysisServices

AzureRM.Profile Az.Accounts

AzureRM.Insights Az.Monitor

AzureRM.RecoveryServices.Backup Az.RecoveryServices

AzureRM.RecoveryServices.SiteRecovery Az.RecoveryServices

AzureRM.Tags Az.Resources

AzureRM.MachineLearningCompute Az.MachineLearning

AzureRM.UsageAggregates Az.Billing

AzureRM.Consumption Az.Billing

The changes in module names mean that any script that uses #Requires or ImportModule to load specific modules will need to be changed to use the new module instead.

For modules where the cmdlet suffix has not changed, this means that although the

module name has changed, the suffix indicating the operation space has not.

Get-AzureRmStorageAccount | Get-AzureStorageContainer | Get-AzureStorageBlob

） Important

When disabling aliases, make sure that they are disabled for all scopes which had

aliases enabled.

Module name changes

Scripts that use #Requires or Import-Module to declare a dependency on AzureRM

modules must be updated to use the new module names. For example:

PowerShell

Should be changed to:

PowerShell

For Import-Module :

PowerShell

Should be changed to:

PowerShell

Scripts that use module-qualified cmdlet invocations, such as:

PowerShell

Must be changed to use the new module and cmdlet names:

PowerShell

Migrating requires and import module statements

#Requires -Module AzureRM.Compute

#Requires -Module Az.Compute

Import-Module -Name AzureRM.Compute

Import-Module -Name Az.Compute

Migrating fully qualified cmdlet invocations

AzureRM.Compute\Get-AzureRmVM

Az.Compute\Get-AzVM

Migrating module manifest dependencies

Modules that express dependencies on AzureRM modules through a module manifest

(.psd1) file will need to updated the module names in their RequiredModules section:

PowerShell

Must be changed to:

PowerShell

The following modules have been removed:

AzureRM.Backup

AzureRM.Compute.ManagedService

AzureRM.Scheduler

The tools for these services are no longer actively supported. Customers are encouraged

to move to alternative services as soon as it is convenient.

Using Az with PowerShell 5.1 for Windows requires the installation of .NET Framework

4.7.2. Using PowerShell Core 6.x or later does not require .NET Framework.

Due to changes in the authentication flow for .NET Standard, we are temporarily

removing user login via PSCredential. This capability will be re-introduced in the

1/15/2019 release for PowerShell 5.1 for Windows. This is discussed in detail in this

GitHub issue.

Due to changes in the authentication flow for .NET Standard, we are using device login

as the default login flow during interactive login. Web browser based login will be reRequiredModules = @(@{ModuleName="AzureRM.Profile"; ModuleVersion="5.8.2"})

RequiredModules = @(@{ModuleName="Az.Accounts"; ModuleVersion="1.0.0"})

Removed modules

Windows PowerShell 5.1 and .NET 4.7.2

Temporary removal of user login using PSCredential

Default device code login instead of web browser prompt

introduced for PowerShell 5.1 for Windows as the default in the 1/15/2019 release. At

that time, users will be able to choose device login using a Switch parameter.

This section details specific breaking changes for individual modules and cmdlets.

Removed the following cmdlets:

New-AzureRmApiManagementHostnameConfiguration

Set-AzureRmApiManagementHostnames

Update-AzureRmApiManagementDeployment

Import-AzureRmApiManagementHostnameCertificate

Use Set-AzApiManagement cmdlet to set these properties instead

Removed the following properties:

Removed property PortalHostnameConfiguration , ProxyHostnameConfiguration ,

ManagementHostnameConfiguration and ScmHostnameConfiguration of type

PsApiManagementHostnameConfiguration from PsApiManagementContext . Instead

use PortalCustomHostnameConfiguration , ProxyCustomHostnameConfiguration ,

ManagementCustomHostnameConfiguration and ScmCustomHostnameConfiguration

of type PsApiManagementCustomHostNameConfiguration .

Removed property StaticIPs from PsApiManagementContext. The property

has been split into PublicIPAddresses and PrivateIPAddresses .

Removed required property Location from NewAzureApiManagementVirtualNetwork cmdlet.

The InvoiceName parameter was removed from the Get-AzConsumptionUsageDetail

cmdlet. Scripts will need to use other identity parameters for the invoice.

IdentityIds are removed from Identity property in PSVirtualMachine and

PSVirtualMachineScaleSet objects Scripts should no longer use the value of this

field to make processing decisions.

Module breaking changes

Az.ApiManagement (previously

AzureRM.ApiManagement)

Az.Billing (previously AzureRM.Billing,

AzureRM.Consumption, and AzureRM.UsageAggregates)

Az.Compute (previously AzureRM.Compute)

The type of InstanceView property of PSVirtualMachineScaleSetVM object is

changed from VirtualMachineInstanceView to

VirtualMachineScaleSetVMInstanceView

AutoOSUpgradePolicy and AutomaticOSUpgrade properties are removed from

UpgradePolicy property

The type of Sku property in PSSnapshotUpdate object is changed from DiskSku to

SnapshotSku

VmScaleSetVMParameterSet is removed from Add-AzVMDataDisk cmdlet, you can no

longer add a data disk individually to a ScaleSet VM.

The PurgeDisabled property was removed from the PSKeyVaultKeyAttributes ,

PSKeyVaultKeyIdentityItem , and PSKeyVaultSecretAttributes objects Scripts

should no longer reference the PurgeDisabled property to make processing

decisions.

Removed plural names Categories and Timegrains parameter in favor of singular

parameter names from Set-AzDiagnosticSetting cmdlet Scripts using

PowerShell

Should be changed to

PowerShell

Removed deprecated ResourceId parameter from GetAzServiceEndpointPolicyDefinition cmdlet

Removed deprecated EnableVmProtection property from PSVirtualNetwork object

Removed deprecated Set-AzVirtualNetworkGatewayVpnClientConfig cmdlet

Az.KeyVault (previously AzureRM.KeyVault)

Az.Monitor (previously AzureRM.Insights)

Set-AzureRmDiagnosticSetting -Timegrains PT1M -Categories Category1,

Category2

Set-AzDiagnosticSetting -Timegrain PT1M -Category Category1, Category2

Az.Network (previously AzureRM.Network)

Scripts should no longer make processing decisions based on the values fo these fields.

Removed Sku parameter from New/Set-AzPolicyAssignment cmdlet

Removed Password parameter from New-AzADServicePrincipal and NewAzADSpCredential cmdlet Passwords are automatically generated, scripts that

provided the password:

PowerShell

Should be changed to retrieve the password from the output:

PowerShell

To support creating an Oauth storage context with only the storage account name,

the default parameter set has been changed to OAuthParameterSet

Example: $ctx = New-AzureStorageContext -StorageAccountName $accountName

The Location parameter has become mandatory in the Get-AzStorageUsage cmdlet

The Storage API methods now use the Task-based Asynchronous Pattern (TAP),

instead of synchronous API calls. The following examples demonstrate the new

asynchronous commands:

AzureRM:

PowerShell

Az.Resources (previously AzureRM.Resources)

New-AzAdSpCredential -ObjectId 1f99cf81-0146-4f4e-beae-2007d0668476 -

Password $secPassword

$credential = New-AzAdSpCredential -ObjectId 1f99cf81-0146-4f4e-beae2007d0668476

$secPassword = $credential.Secret

Az.Storage (previously Azure.Storage and

AzureRM.Storage)

Blob snapshot

$b = Get-AzureStorageBlob -Container $containerName -Blob $blobName -Context

$ctx

Az:

PowerShell

AzureRM:

PowerShell

Az:

PowerShell

AzureRM:

PowerShell

Az:

PowerShell

$b.ICloudBlob.Snapshot()

$b = Get-AzStorageBlob -Container $containerName -Blob $blobName -Context

$ctx

$task = $b.ICloudBlob.SnapshotAsync()

$task.Wait()

$snapshot = $task.Result

Share snapshot

$Share = Get-AzureStorageShare -Name $containerName -Context $ctx

$snapshot = $Share.Snapshot()

$Share = Get-AzStorageShare -Name $containerName -Context $ctx

$task = $Share.SnapshotAsync()

$task.Wait()

$snapshot = $task.Result

Undelete soft-deleted blob

$b = Get-AzureStorageBlob -Container $containerName -Blob $blobName -

IncludeDeleted -Context $ctx

$b.ICloudBlob.Undelete()

AzureRM:

PowerShell

Az:

PowerShell

Removed deprecated properties from the PSAppServicePlan , PSCertificate ,

PSCloningInfo , and PSSite objects

Learn more about PowerShell on Azure Stack Hub, see Get started with PowerShell

in Azure Stack Hub

$b = Get-AzStorageBlob -Container $containerName -Blob $blobName -

IncludeDeleted -Context $ctx

$task = $b.ICloudBlob.UndeleteAsync()

$task.Wait()

Set blob tier

$blockBlob = Get-AzureStorageBlob -Container $containerName -Blob

$blockBlobName -Context $ctx

$blockBlob.ICloudBlob.SetStandardBlobTier("hot")

$pageBlob = Get-AzureStorageBlob -Container $containerName -Blob

$pageBlobName -Context $ctx

$pageBlob.ICloudBlob.SetPremiumBlobTier("P4")

$blockBlob = Get-AzStorageBlob -Container $containerName -Blob

$blockBlobName -Context $ctx

$task = $blockBlob.ICloudBlob.SetStandardBlobTierAsync("hot")

$task.Wait()

$pageBlob = Get-AzStorageBlob -Container $containerName -Blob $pageBlobName

-Context $ctx

$task = $pageBlob.ICloudBlob.SetPremiumBlobTierAsync("P4")

$task.Wait()

Az.Websites (previously AzureRM.Websites)

Next steps

Install the PowerShell Az module, see Install PowerShell Az module for Azure Stack

Hub

Download Azure Stack Hub tools from

GitHub

Article • 07/29/2022

AzureStack-Tools is a GitHub repository that hosts PowerShell modules for managing

and deploying resources to Azure Stack Hub. If you're planning to establish VPN

connectivity, you can download these PowerShell modules to the Azure Stack

Development Kit (ASDK), or to a Windows-based external client.

You use the tools using the Az PowerShell modules, or the AzureRM modules.

To get these tools, clone the GitHub repository from the az branch or download

the AzureStack-Tools folder by running the following script:

PowerShell

７ Note

You can also use the The Operator Access Workstation (OAW) to access the

privileged endpoint (PEP), the Administrator portal for support scenarios, and Azure

Stack Hub GitHub Tools. For more information see Azure Stack Hub Operator

Access Workstation.

Get the tools

Az modules

# Change directory to the root directory.

cd \

# Download the tools archive.

[Net.ServicePointManager]::SecurityProtocol =

[Net.SecurityProtocolType]::Tls12

invoke-webrequest `

https://github.com/Azure/AzureStack-Tools/archive/az.zip `

-OutFile az.zip

# Expand the downloaded files.

expand-archive az.zip `

-DestinationPath . `

-Force

# Change to the tools directory.

The AzureStack-Tools repository has PowerShell modules that support the following

functionalities for Azure Stack Hub:

Functionality Description Who can

use this

module?

CapacityManagement Use this module to generate Performance and Capacity

Dashboard of storage volumes.

Cloud

operators

Cloud capabilities Use this module to get the cloud capabilities of a cloud. For

example, you can get cloud capabilities like API version and

Azure Resource Manager resources. You can also get the VM

extensions for Azure Stack Hub and Azure clouds.

Cloud

operators

and users

Resource Manager

policy for Azure Stack

Hub

Use this module to configure an Azure subscription or an

Azure resource group with the same versioning and service

availability as Azure Stack Hub.

Cloud

operators

and users

Register with Azure Use this module to register your ASDK instance with Azure.

After registering, you can download Azure Marketplace items

use them in Azure Stack Hub.

Cloud

operators

Azure Stack Hub

deployment

Use this module to prepare the Azure Stack Hub host

computer to deploy and redeploy by using the Azure Stack

Hub virtual hard disk (VHD) image.

Cloud

operators

Connecting to Azure

Stack Hub

Use this module to configure VPN connectivity to Azure

Stack Hub.

Cloud

operators

and users

Template validator Use this module to verify if an existing or a new template can

be deployed to Azure Stack Hub.

Cloud

operators

and users

Get started with PowerShell on Azure Stack Hub.

Configure the Azure Stack Hub user's PowerShell environment.

Connect to Azure Stack Development Kit over a VPN.

cd AzureStack-Tools-az

Functionality provided by the modules

Next steps

Connect to Azure Stack Hub with

PowerShell

Article • 07/29/2022

You can configure Azure Stack Hub to use PowerShell to manage resources like creating

offers, plans, quotas, and alerts. This topic helps you configure the operator

environment.

Run the following prerequisites either from the Azure Stack Development Kit (ASDK) or

from a Windows-based external client if you're connected to the ASDK through VPN.

Install Azure Stack Hub-compatible Azure PowerShell modules.

Download the tools required to work with Azure Stack Hub.

To configure the Azure Stack Hub operator environment with PowerShell, run one of the

scripts below. Replace the Azure Active Directory (Azure AD) tenantName and Azure

Resource Manager endpoint values with your own environment configuration.

PowerShell

Prerequisites

Connect with Azure AD

Az modules

７ Note

If your session expires, your password has changed, or you simply wish to

switch accounts, run the following cmdlet before you sign in using ConnectAzAccount: Remove-AzAccount -Scope Process

# Register an Azure Resource Manager environment that targets your

Azure Stack Hub instance. Get your Azure Resource Manager endpoint value

from your service provider.

Add-AzEnvironment -Name "AzureStackAdmin" -ArmEndpoint

"https://adminmanagement.local.azurestack.external" `

-AzureKeyVaultDnsSuffix adminvault.local.azurestack.external `

-AzureKeyVaultServiceEndpointResourceId

https://adminvault.local.azurestack.external

Connect to the Azure Stack Hub operator environment with PowerShell with Azure

Active Directory Federated Services (Azure AD FS). For the ASDK, this Azure Resource

Manager endpoint is set to https://adminmanagement.local.azurestack.external . To get

the Azure Resource Manager endpoint for Azure Stack Hub integrated systems, contact

your service provider.

PowerShell

# Set your tenant name.

$AuthEndpoint = (Get-AzEnvironment -Name

"AzureStackAdmin").ActiveDirectoryAuthority.TrimEnd('/')

$AADTenantName = "<myDirectoryTenantName>.onmicrosoft.com"

$TenantId = (invoke-restmethod

"$($AuthEndpoint)/$($AADTenantName)/.well-known/openidconfiguration").issuer.TrimEnd('/').Split('/')[-1]

# After signing in to your environment, Azure Stack Hub cmdlets

# can be easily targeted at your Azure Stack Hub instance.

Connect-AzAccount -EnvironmentName "AzureStackAdmin" -TenantId

$TenantId

Connect with AD FS

Az modules

# Register an Azure Resource Manager environment that targets your Azure

Stack Hub instance. Get your Azure Resource Manager endpoint value from

your service provider.

Add-AzEnvironment -Name "AzureStackAdmin" -ArmEndpoint

"https://adminmanagement.local.azurestack.external" `

-AzureKeyVaultDnsSuffix adminvault.local.azurestack.external `

-AzureKeyVaultServiceEndpointResourceId

https://adminvault.local.azurestack.external

# Sign in to your environment.

Connect-AzAccount -EnvironmentName "AzureStackAdmin"

７ Note

AD FS only supports interactive authentication with user identities. If a credential

object is required, you must use a service principal (SPN). For more information on

setting up a service principal with Azure Stack Hub and AD FS as your identity

management service, see Manage an AD FS app identity.

Now that you've got everything set-up, use PowerShell to create resources within Azure

Stack Hub. For example, you can create a resource group for an app and add a virtual

machine. Use the following command to create a resource group named

MyResourceGroup.

PowerShell

Use PowerShell to manage subscriptions, plans, and offers in Azure Stack Hub

Develop templates for Azure Stack Hub.

Deploy templates with PowerShell.

Azure Stack Hub Module Reference.

Test the connectivity

Az modules

New-AzResourceGroup -Name "MyResourceGroup" -Location "Local"

Next steps

Use the privileged endpoint in Azure

Stack Hub

Article • 07/29/2022

As an Azure Stack Hub operator, you should use the administrator portal, PowerShell, or

Azure Resource Manager APIs for most day-to-day management tasks. However, for

some less common operations, you need to use the privileged endpoint (PEP). The PEP is

a pre-configured remote PowerShell console that provides you with just enough

capabilities to help you do a required task. The endpoint uses PowerShell JEA (Just

Enough Administration) to expose only a restricted set of cmdlets. To access the PEP and

invoke the restricted set of cmdlets, a low-privileged account is used. No admin

accounts are required. For additional security, scripting isn't allowed.

You can use the PEP to perform these tasks:

Low-level tasks, such as collecting diagnostic logs.

Many post-deployment datacenter integration tasks for integrated systems, such

as adding Domain Name System (DNS) forwarders after deployment, setting up

Microsoft Graph integration, Active Directory Federation Services (AD FS)

integration, certificate rotation, and so on.

To work with support to obtain temporary, high-level access for in-depth

troubleshooting of an integrated system.

The PEP logs every action (and its corresponding output) that you perform in the

PowerShell session. This provides full transparency and complete auditing of operations.

You can keep these log files for future audits.

７ Note

In the Azure Stack Development Kit (ASDK), you can run some of the commands

available in the PEP directly from a PowerShell session on the development kit host.

However, you may want to test some operations using the PEP, such as log

collection, because this is the only method available to perform certain operations

in an integrated systems environment.

７ Note

You can also use the The Operator Access Workstation (OAW) to access the

privileged endpoint (PEP), the Administrator portal for support scenarios, and Azure

You access the PEP through a remote PowerShell session on the virtual machine (VM)

that hosts the PEP. In the ASDK, this VM is named AzS-ERCS01. If you're using an

integrated system, there are three instances of the PEP, each running inside a VM

(Prefix-ERCS01, Prefix-ERCS02, or Prefix-ERCS03) on different hosts for resiliency.

Before you begin this procedure for an integrated system, make sure you can access the

PEP either by IP address or through DNS. After the initial deployment of Azure Stack

Hub, you can access the PEP only by IP address because DNS integration isn't set up yet.

Your OEM hardware vendor will provide you with a JSON file named

AzureStackStampDeploymentInfo that contains the PEP IP addresses.

You may also find the IP address in the Azure Stack Hub administrator portal. Open the

portal, for example, https://adminportal.local.azurestack.external . Select Region

Management > Properties.

You will need set your current culture setting to en-US when running the privileged

endpoint, otherwise cmdlets such as Test-AzureStack or Get-AzureStackLog will not

work as expected.

1. Establish the trust.

On an integrated system, run the following command from an elevated

Windows PowerShell session to add the PEP as a trusted host on the

hardened VM running on the hardware lifecycle host or the Privileged Access

Workstation.

PowerShell

Stack Hub GitHub Tools. For more information see Azure Stack Hub Operator

Access Workstation.

Access the privileged endpoint

７ Note

For security reasons, we require that you connect to the PEP only from a hardened

VM running on top of the hardware lifecycle host, or from a dedicated and secure

computer, such as a Privileged Access Workstation . The original configuration of

the hardware lifecycle host must not be modified from its original configuration

(including installing new software) or used to connect to the PEP.

If you're running the ASDK, sign in to the development kit host.

2. On the hardened VM running on the hardware lifecycle host or the Privileged

Access Workstation, open a Windows PowerShell session. Run the following

commands to establish a remote session on the VM that hosts the PEP:

On an integrated system:

PowerShell

The ComputerName parameter can be either the IP address or the DNS name of

one of the VMs that hosts the PEP.

If you're running the ASDK:

PowerShell

When prompted, use the following credentials:

User name: Specify the CloudAdmin account, in the format <Azure Stack

Hub domain>\cloudadmin. (For ASDK, the user name is

Set-Item WSMan:\localhost\Client\TrustedHosts -Value '<IP Address

of Privileged Endpoint>' -Concatenate

$cred = Get-Credential

$pep = New-PSSession -ComputerName <IP\_address\_of\_ERCS> -

ConfigurationName PrivilegedEndpoint -Credential $cred -

SessionOption (New-PSSessionOption -Culture en-US -UICulture enUS)

Enter-PSSession $pep

７ Note

Azure Stack Hub doesn't make a remote call when validating the PEP

credential. It relies on a locally-stored RSA public key to do that.

$cred = Get-Credential

$pep = New-PSSession -ComputerName azs-ercs01 -ConfigurationName

PrivilegedEndpoint -Credential $cred -SessionOption (NewPSSessionOption -Culture en-US -UICulture en-US)

Enter-PSSession $pep

azurestack\cloudadmin)

Password: Enter the same password that was provided during installation for

the AzureStackAdmin domain administrator account.

3. After you connect, the prompt will change to [IP address or ERCS VM name]: PS>

or to [azs-ercs01]: PS>, depending on the environment. From here, run GetCommand to view the list of available cmdlets.

You can find a reference for cmdlets in at Azure Stack Hub privileged endpoint

reference

Many of these cmdlets are intended only for integrated system environments (such

as the cmdlets related to datacenter integration). In the ASDK, the following

cmdlets have been validated:

Clear-Host

Close-PrivilegedEndpoint

Exit-PSSession

Get-AzureStackLog

Get-AzureStackStampInformation

Get-Command

Get-FormatData

Get-Help

Get-ThirdPartyNotices

Measure-Object

７ Note

If you're unable to connect to the ERCS endpoint, retry steps one and two

with another ERCS VM IP address.

２ Warning

By default your Azure Stack Hub stamp is configured with only one

CloudAdmin account. There are no recovery options if the account

credentials are lost, compromised, or locked. You will lose access to the

privileged endpoint and other resources.

It is highly recommended that you create additional CloudAdmin accounts,

to avoid redeployment of your stamp at your own expense. Make sure you

document these credentials based on your company's guidelines.

New-CloudAdminUser

Out-Default

Remove-CloudAdminUser

Select-Object

Set-CloudAdminUserPassword

Test-AzureStack

Stop-AzureStack

Get-ClusterLog

As mentioned above, the PEP is a PowerShell JEA endpoint. While providing a strong

security layer, a JEA endpoint reduces some of the basic PowerShell capabilities, such as

scripting or tab completion. If you try any type of script operation, the operation fails

with the error ScriptsNotAllowed. This failure is expected behavior.

For instance, to get the list of parameters for a given cmdlet, run the following

command:

PowerShell

Alternatively, you can use the Import-PSSession cmdlet to import all the PEP cmdlets

into the current session on your local machine. The cmdlets and functions of the PEP are

now available on your local machine, together with tab completion and, more in

general, scripting. You can also run the Get-Help module to review cmdlet instructions.

To import the PEP session on your local machine, do the following steps:

1. Establish the trust.

On an integrated system, run the following command from an elevated

Windows PowerShell session to add the PEP as a trusted host on the

hardened VM running on the hardware lifecycle host or the Privileged Access

Workstation.

PowerShell

If you're running the ASDK, sign in to the development kit host.

How to use the privileged endpoint

Get-Command <cmdlet\_name> -Syntax

winrm s winrm/config/client '@{TrustedHosts="<IP Address of

Privileged Endpoint>"}'

2. On the hardened VM running on the hardware lifecycle host or the Privileged

Access Workstation, open a Windows PowerShell session. Run the following

commands to establish a remote session on the virtual machine that hosts the PEP:

On an integrated system:

PowerShell

The ComputerName parameter can be either the IP address or the DNS name of

one of the VMs that hosts the PEP.

If you're running the ASDK:

PowerShell

When prompted, use the following credentials:

User name: Specify the CloudAdmin account, in the format <Azure Stack

Hub domain>\cloudadmin. (For ASDK, the user name is

azurestack\cloudadmin.)

Password: Enter the same password that was provided during installation for

the AzureStackAdmin domain administrator account.

3. Import the PEP session into your local machine:

PowerShell

4. Now, you can use tab-completion and do scripting as usual on your local

PowerShell session with all the functions and cmdlets of the PEP, without

$cred = Get-Credential

$session = New-PSSession -ComputerName <IP\_address\_of\_ERCS> `

-ConfigurationName PrivilegedEndpoint -Credential $cred `

-SessionOption (New-PSSessionOption -Culture en-US -UICulture

en-US)

$cred = Get-Credential

$session = New-PSSession -ComputerName azs-ercs01 `

-ConfigurationName PrivilegedEndpoint -Credential $cred `

-SessionOption (New-PSSessionOption -Culture en-US -UICulture

en-US)

Import-PSSession $session

decreasing the security posture of Azure Stack Hub. Enjoy!

As mentioned earlier, the PEP logs every action (and its corresponding output) that you

do in the PowerShell session. You must close the session by using the ClosePrivilegedEndpoint cmdlet. This cmdlet correctly closes the endpoint, and transfers the

log files to an external file share for retention.

To close the endpoint session:

1. Create an external file share that's accessible by the PEP. In a development kit

environment, you can just create a file share on the development kit host.

2. Run the following cmdlet:

PowerShell

The cmdlet uses the parameters in the following table:

Parameter Description Type Required

TranscriptsPathDestination Path to the external file share

defined as

"fileshareIP\sharefoldername"

String Yes

Credential Credentials to access the file share SecureString Yes

After the transcript log files are successfully transferred to the file share, they're

automatically deleted from the PEP.

Close the privileged endpoint session

Close-PrivilegedEndpoint -TranscriptsPathDestination

"\\fileshareIP\SharedFolder" -Credential Get-Credential

７ Note

If you close the PEP session by using the cmdlets Exit-PSSession or Exit , or you

just close the PowerShell console, the transcript logs don't transfer to a file share.

They remain in the PEP. The next time you run Close-PrivilegedEndpoint and

include a file share, the transcript logs from the previous session(s) will also

transfer. Don't use Exit-PSSession or Exit to close the PEP session; use ClosePrivilegedEndpoint instead.

During a support scenario, the Microsoft support engineer might need to elevate the

privileged endpoint PowerShell session to access the internals of the Azure Stack Hub

infrastructure. This process is sometimes informally referred to as "break the glass" or

"unlock the PEP". The PEP session elevation process is a two step, two people, two

organization authentication process. The unlock procedure is initiated by the Azure

Stack Hub operator, who retains control of their environment at all times. The operator

accesses the PEP and executes this cmdlet:

PowerShell

The cmdlet returns the support session request token, a very long alphanumeric string.

The operator then passes the request token to the Microsoft support engineer via a

medium of their choice (e.g., chat, email). The Microsoft support engineer uses the

request token to generate, if valid, a support session authorization token and sends it

back to the Azure Stack Hub operator. On the same PEP PowerShell session, the

operator then passes the authorization token as input to this cmdlet:

PowerShell

If the authorization token is valid, the PEP PowerShell session is elevated by providing

full admin capabilities and full reachability into the infrastructure.

Once the support session is terminated, it is very important to close back the elevated

PEP session by using the Close-PrivilegedEndpoint cmdlet as explained in the section

Unlocking the privileged endpoint for support

scenarios

Get-SupportSessionToken

unlock-supportsession

cmdlet Unlock-SupportSession at command pipeline position 1

Supply values for the following parameters:

ResponseToken:

７ Note

All the operations and cmdlets executed in an elevated PEP session must be

performed under strict supervision of the Microsoft support engineer. Failure to do

so could result in serious downtime, data loss and could require a full

redeployment of the Azure Stack Hub environment.

above. One the PEP session is terminated, the unlock token is no longer valid and

cannot be reused to unlock the PEP session again. An elevated PEP session has a validity

of 8 hours, after which, if not terminated, the elevated PEP session will automatically lock

back to a regular PEP session.

The PEP support session request and authorization tokens leverage cryptography to

protect access and ensure that only authorized tokens can unlock the PEP session. The

tokens are designed to cryptographically guarantee that a response token can only be

accepted by the PEP session that generated the request token. PEP tokens do not

contain any kind of information that could uniquely identify an Azure Stack Hub

environment or a customer. They are completely anonymous. Below the details of the

content of each token are provided.

The PEP support session request token is composed of three objects:

A randomly generated Session ID.

A self-signed certificate, generated for the purpose of having a one-time

public/private key pair. The certificate does not contain any information on the

environment.

A time stamp that indicates the request token expiration.

The request token is then encrypted with the public key of the Azure cloud against

which the Azure Stack Hub environment is registered to.

The PEP support authorization response token is composed of two objects:

The randomly generated session ID extracted from the request token.

A time stamp that indicates the response token expiration.

The response token is then encrypted with the self-signed certificate contained in the

request token. The self-signed certificate was decrypted with the private key associated

with the Azure cloud against which the Azure Stack Hub environment is registered to.

Content of the privileged endpoint tokens

Support session request token

Support session authorization response token

Next steps

Azure Stack Hub diagnostic tools

Azure Stack Hub privileged endpoint reference

Monitor health and alerts in Azure Stack

Hub

Article • 07/29/2022

Azure Stack Hub includes infrastructure monitoring capabilities that help you view

health and alerts for an Azure Stack Hub region. The Region management tile lists all

the deployed regions of Azure Stack Hub. It's pinned by default in the administrator

portal for the Default Provider Subscription. The tile shows the number of active critical

and warning alerts for each region. The tile is your entry point into the health and alert

functionality of Azure Stack Hub.

The health resource provider manages health and alerts. Azure Stack Hub infrastructure

components register with the health resource provider during Azure Stack Hub

deployment and configuration. This registration enables the display of health and alerts

for each component. Health in Azure Stack Hub is a simple concept. If alerts for a

registered instance of a component exist, the health state of that component reflects the

worst active alert severity: warning or critical.

Azure Stack Hub raises alerts with only two severities: warning and critical.

Warning

An operator can address the warning alert in a scheduled manner. The alert

Understand health in Azure Stack Hub

Alert severity definition

typically doesn't impact user workloads.

Critical

An operator should address the critical alert with urgency. These alerts indicate

issues that currently impact or will soon impact Azure Stack Hub users.

You can view the health state of components in the administrator portal and through

REST API and PowerShell.

To view the health state in the portal, click the region that you want to view in the

Region management tile. You can view the health state of infrastructure roles and of

resource providers.

You can click a resource provider or infrastructure role to view more detailed

information.

View and manage component health state

２ Warning

If you click an infrastructure role, and then click the role instance, there are options

to Start, Restart, or Shutdown. Don't use these actions when you apply updates to

an integrated system. Also, do not use these options in an Azure Stack

Development Kit (ASDK) environment. These options are only designed for an

integrated systems environment, where there's more than one role instance per

infrastructure role. Restarting a role instance (especially AzS-Xrp01) in the ASDK

causes system instability. For troubleshooting assistance, post your issue to the

Azure Stack Hub forum .

The list of active alerts for each Azure Stack Hub region is available directly from the

Region management blade. The first tile in the default configuration is the Alerts tile,

which displays a summary of the critical and warning alerts for the region. You can pin

the Alerts tile, like any other tile on this blade, to the dashboard for quick access.

To view a list of all active alerts for the region, select the top part of the Alerts tile. To

view a filtered list of alerts (Critical or Warning), select either the Critical or Warning line

item within the tile.

The Alerts blade supports the ability to filter both on status (Active or Closed) and

severity (Critical or Warning). The default view displays all active alerts. All closed alerts

are removed from the system after seven days.

View alerts

７ Note

If an alert remains active but hasn't been updated in over a day, you can run TestAzureStack and close the alert if no problems are reported.

The View API action displays the REST API that was used to generate the list view. This

action provides a quick way to become familiar with the REST API syntax that you can

use to query alerts. You can use this API in automation or for integration with your

existing datacenter monitoring, reporting, and ticketing solutions.

You can click a specific alert to view the alert details. The alert details show all fields that

are associated with the alert and enable quick navigation to the affected component

and source of the alert. For example, the following alert occurs if one of the

infrastructure role instances goes offline or isn't accessible.

Some alerts support a Repair option, as shown in the previous image. When selected,

the Repair action performs steps specific to the alert to attempt to resolve the issue.

Once selected, the status of the Repair action is available as a portal notification.

Alert remediation

Automated remediation

The Repair action will report successful completion or failure to complete the action in

the same portal notification blade. If a Repair action fails for an alert, you may rerun the

Repair action from the alert detail. If the Repair action successfully completes, do not

rerun the Repair action. After the infrastructure role instance is back online, this alert

automatically closes.

Manual remediation

If the Repair option is not supported, be sure to follow the complete set of remediation

instructions provided in the alert. As an example, the internal certificate expiration

remediation steps will guide you through the process of secret rotation:

Many, but not every alert, will automatically close when the underlying issue is resolved.

Alerts that provide a Repair action button will close automatically if Azure Stack Hub

Alert closure

resolves the issue. For all other alerts, select Close Alert after you do the remediation

steps. If the issue persists, Azure Stack Hub generates a new alert. If you resolve the

issue, the alert remains closed and requires no more steps.

Manage updates in Azure Stack Hub

Region management in Azure Stack Hub

Next steps

Monitor Azure Stack Hub hardware

components

Article • 02/08/2021

The Azure Stack Hub health and monitoring system monitors the status of the storage

subsystem and raises alerts as needed. The health and monitoring system can also raise

alerts for the following hardware components:

System fans

System temperature

Power supply

CPUs

Memory

Boot drives

An SNMP v3 listener is running on all three ERCS instances on TCP port 162. The BMC

must be configured to send SNMP traps to the Azure Stack Hub listener. You can get the

three PEP IPs from the administrator portal by opening the region properties view.

Sending traps to the listener requires authentication and must use the same credential

as accessing base BMC itself.

When an SNMP trap is received on any of the three ERCS instances on TCP port 162, the

OID is matched internally and an alert is raised. The Azure Stack Hub health and

monitoring system only accepts OIDs defined by the hardware partner. If an OID is

unknown to Azure Stack Hub, it won't match it to an alert.

Once a faulty component is replaced, an event is sent from the BMC to the SNMP

listener that indicates the state change. The alert then closes automatically in Azure

７ Note

Before you enable this feature, you must validate with your hardware partner that

they're ready. Your hardware partner will also provide the detailed steps for

enabling this feature in the baseboard management controller (BMC). The user

encryption in the base board management controller must be set to AES for build

2005 and later.

SNMP listener scenario

Stack Hub.

Firewall integration

７ Note

Existing alerts do not close automatically when the entire node or motherboard is

replaced. The same applies when the BMC loses its configuration; for example, due

to a factory reset.

Next steps

Manage network resources in Azure

Stack Hub

Article • 07/29/2022

Azure Stack Hub uses a static MAC address pool to automatically generate and assign

MAC address to virtual machines (VMs). This MAC address pool is automatically

generated during deployment and uses the following range:

StartMacAddress: 00-1D-D8-B7-00-00

EndMacAddress: 00-1D-D8-F4-FF-FF

Depending on how the virtual networks connect with existing corporate networks, you

may expect duplicated MAC addresses of VMs.

More information can be found about MAC address pool utilization using the cmdlet

Get-AzsMacAddressPool in the Azure Stack Hub administrator PowerShell module.

As a cloud administrator, you can view:

The number of public IP addresses that have been allocated to tenants.

The number of public IP addresses that are still available for allocation.

The percentage of public IP addresses that have been allocated in that location.

The Public IP pools usage tile shows the number of public IP addresses consumed

across public IP address pools. For each IP address, the tile shows usage for tenant IaaS

VM instances, fabric infrastructure services, and public IP address resources that were

explicitly created by tenants.

MAC address pool

７ Note

This MAC address pool is the same across each Azure Stack Hub system and is not

configurable.

View public IP address consumption in Azure

Stack Hub

The purpose of the tile is to give Azure Stack Hub operators a sense of the number of

public IP addresses used in this location. The number helps administrators determine

whether they're running low on this resource.

The Public IP addresses menu item under Tenant Resources lists only those public IP

addresses that have been explicitly created by tenants. You can find the menu item on

the Resource providers -> Network pane. The number of Used public IP addresses on

the Public IP pools usage tile is always different from (larger than) the number on the

Public IP Addresses tile under Tenant Resources.

To view the total number of public IP addresses that have been consumed in the region:

1. In the Azure Stack Hub administrator portal, select All services. Then, under the

ADMINISTRATION category, select Network.

2. The Network pane displays the Public IP pools usage tile in the Overview section.

The Used number represents the number of assigned public IP addresses from public IP

address pools. The Free number represents the number of public IP addresses from

public IP address pools that haven't been assigned and are still available. The % Used

number represents the number of used or assigned addresses as a percentage of the

total number of public IP addresses in public IP address pools in that location.

View the public IP address usage information

Select Public IP addresses under Tenant Resources. Review the list of public IP

addresses explicitly created by tenant subscriptions in a specific region.

You might notice that some public IP addresses that have been dynamically allocated

appear in the list. However, an address hasn't been associated with them yet. The

address resource has been created in the Network Resource Provider, but not yet in the

Network Controller.

The Network Controller doesn't assign an address to the resource until it binds to an

interface, a network interface card (NIC), a load balancer, or a virtual network gateway.

When the public IP address binds to an interface, the Network Controller allocates an IP

address. The address appears in the Address field.

In different cases, public IP addresses are assigned that determine whether the address

appears in one list or another.

Public IP address assignment case Appears

in usage

summary

Appears

in tenant

public IP

addresses

list

Unassigned dynamic public IP address (temporary). No Yes

Dynamic public IP address assigned to a NIC or load balancer. Yes Yes

Static public IP address assigned to a tenant NIC or load balancer. Yes Yes

View the public IP addresses that were created by tenant

subscriptions

View the public IP address information summary table

Public IP address assignment case Appears

in usage

summary

Appears

in tenant

public IP

addresses

list

Static public IP address assigned to a fabric infrastructure service

endpoint.

Yes No

Public IP address implicitly created for the virtual network. This public IP

is created only after the first standalone VM (VM without public IP or

load balancer assigned) is connected to the virtual network. This NAT IP

address ensures the outbound connectivity for any standalone VM

connected to the virtual network. To release this public IP usage from

the pool is necessary to disconnect all the VMs from the virtual network

and remove the virtual network.

Yes No

Manage Storage Accounts in Azure Stack Hub

Next steps

Change the billing owner for an Azure

Stack Hub user subscription

Article • 07/29/2022

Azure Stack Hub operators can use PowerShell to change the billing owner for a user

subscription. One reason to change the owner, for example, is to replace a user that

leaves your organization.

There are two types of Owners that are assigned to a subscription:

Billing owner: By default, the billing owner is the user account that gets the

subscription from an offer and then owns the billing relationship for that

subscription. This account is also an administrator of the subscription. Only one

user account can have this designation on a subscription. A billing owner is often

an organization or team lead.

You can use the PowerShell cmdlet Set-AzsUserSubscription to change the billing

owner.

Owners added through RBAC roles - Additional users can be granted the Owner

role using role-based access control (RBAC). Any number of additional user

accounts can be added as owners to compliment the billing owner. Additional

owners are also administrators of the subscription and have all privileges for the

subscription, except permission to delete the billing owner.

You can use PowerShell to manage additional owners. For more information, see

this article.

Run the following script to change the billing owner of a user subscription. The

computer that you use to run the script must connect to Azure Stack Hub and run the

Azure Stack Hub PowerShell module 1.3.0 or later. For more information, see Install

Azure Stack Hub PowerShell.

Change the billing owner

７ Note

In a multi-tenant Azure Stack Hub, the new owner must be in the same directory as

the existing owner. Before you can provide ownership of the subscription to a user

Replace the following values in the script before it runs:

$ArmEndpoint: The Resource Manager endpoint for your environment.

$TenantId: Your Tenant ID.

$SubscriptionId: Your subscription ID.

$OwnerUpn: An account, for example user@example.com, to add as the new

billing owner.

PowerShell

Manage Role-Based Access Control

that's in another directory, you must first invite that user as a guest into your

directory.

Az modules

# Set up Azure Stack Hub admin environment

Add-AzEnvironment -ARMEndpoint $ArmEndpoint -Name AzureStack-admin

Connect-AzAccount -Environment AzureStack-admin -TenantId $TenantId

# Select admin subscription

$providerSubscriptionId = (Get-AzSubscription -SubscriptionName "Default

Provider Subscription").Id

Write-Output "Setting context to the Default Provider Subscription:

$providerSubscriptionId"

Set-AzContext -Subscription $providerSubscriptionId

# Change user subscription owner

$subscription = Get-AzsUserSubscription -SubscriptionId $SubscriptionId

$Subscription.Owner = $OwnerUpn

$Subscription | Set-AzsUserSubscription | fl \*

７ Note

If your session expires, your password has changed, or you simply wish to

switch accounts, run the following cmdlet before you sign in using ConnectAzAccount: Remove-AzAccount -Scope Process

Next steps

Start and stop Azure Stack Hub

Article • 07/29/2022

Follow the procedures in this article to properly shut down and restart Azure Stack Hub

services. Stop physically shuts down and powers off the entire Azure Stack Hub

environment. Start powers on all infrastructure roles and returns tenant resources to the

power state they were in before shutdown.

Stop or shut down Azure Stack Hub with the following steps:

1. Prepare all workloads running on your Azure Stack Hub environment's tenant

resources for the upcoming shutdown.

2. Open a privileged endpoint session (PEP) from a machine with network access to

the Azure Stack Hub ERCS VMs. For instructions, see Using the privileged endpoint

in Azure Stack Hub.

3. From the PEP, run:

PowerShell

4. Wait for all physical Azure Stack Hub nodes to power off.

７ Note

The maximum supported time an Azure Stack Hub system can be turned off is 180

days. If it's turned off for a longer period of time, a re-deployment is required.

Please contact your hardware solution partner.

Stop Azure Stack Hub

Stop-AzureStack

７ Note

You can verify the power status of a physical node by following the

instructions from the original equipment manufacturer (OEM) who supplied

your Azure Stack Hub hardware.

5. (Optional) If the stop operation times out, you can monitor its progress using the

following PowerShell cmdlet:

PowerShell

Start Azure Stack Hub with the following steps. Follow these steps regardless of how

Azure Stack Hub stopped.

1. Power on each of the physical nodes in your Azure Stack Hub environment. Verify

the power on instructions for the physical nodes by following the instructions from

the OEM who supplied the hardware for your Azure Stack Hub.

2. Wait until the Azure Stack Hub infrastructure services starts. Azure Stack Hub

infrastructure services can require two hours to finish the start process. You can

verify the start status of Azure Stack Hub with the Get-ActionStatus cmdlet.

3. Ensure that all of your tenant resources have returned to the state they were in

before shutdown. Workloads running on tenant resources may need to be

reconfigured after startup by the workload manager.

Get the startup for the Azure Stack Hub startup routine with the following steps:

1. Open a privileged endpoint session from a machine with network access to the

Azure Stack Hub ERCS VMs.

2. From the PEP, run:

PowerShell

Get-ActionStatus Stop-AzureStack

Start Azure Stack Hub

Get the startup status for Azure Stack Hub

Get-ActionStatus Start-AzureStack

Troubleshoot startup and shutdown of Azure

Stack Hub

Take the following steps if the infrastructure and tenant services don't successfully start

two hours after you power on your Azure Stack Hub environment.

1. Open a privileged endpoint session from a machine with network access to the

Azure Stack Hub ERCS VMs.

2. Run:

PowerShell

3. Review the output and resolve any health errors. For more information, see Run a

validation test of Azure Stack Hub.

4. Run:

PowerShell

5. If running Start-AzureStack results in a failure, contact Microsoft Support.

Learn more about Azure Stack Hub diagnostic tools

Test-AzureStack

Start-AzureStack

Next steps

Decommission an Azure Stack Hub

system

Article • 04/28/2023

This article describes how to properly decommission an Azure Stack Hub system. Prior

to reclaiming the system hardware, follow this procedure to ensure tenant workloads

are secured, sensitive information is removed, and the system is unregistered with

Azure.

Before you begin, ensure that the following prerequisites are met:

Ensure that all workloads have been removed from the system with appropriate

backups.

It's not necessary that you fully stop or remove all resources (VMs, web apps, etc.)

from the system. However, you can stop or remove these resources to manage

usage and costs during the decommission process.

Once the system is permanently shut down, no further usage information is

reported.

Follow these steps in a connected (Azure AD) environment:

1. Disable multi-tenancy by removing secondary directories: Unregister a guest

directory.

2. Verify any additional guest directories have been removed: Retrieve identity health

report.

3. Remove any tenant registrations for usage billing: Remove a tenant mapping.

4. Remove Azure Stack Hub registration and prevent usage data being pushed to

Azure billing.

a. Follow the steps from Register Azure Stack Hub to import the

RegisterWithAzure.psm1 module.

b. Use the following script to remove the registration resource.

PowerShell

Prerequisites

Connected (Azure AD) scenarios

5. Remove Azure AD app registrations for Azure Stack Hub:

a. Connect to your Azure Stack environment with Azure PowerShell.

b. In the same PowerShell instance as the previous step, run the following script to

export a list of all app registration IDs.

PowerShell

# Select the subscription used during the registration (shown in

portal)

Select-AzSubscription -Subscription '<Registration subscription ID from

portal>'

# Unregister using the parameter values from portal

Remove-AzsRegistration -PrivilegedEndpointCredential

$YourCloudAdminCredential -PrivilegedEndpoint $YourPrivilegedEndpoint -

RegistrationName '<Registration name from portal>' -ResourceGroupName

'<Registration resource group from portal>'

$context = Get-AzContext

if (!$context.Subscription){

@"

# Connect To Azure Stack Admin Azure Resource Manager endpoint first

https://learn.microsoft.com/azure-stack/operator/azure-stackpowershell-configure-admin#connect-with-azure-ad

"@ | Write-Host -ForegroundColor:Red

}

"Getting access token for tenant {0}" -f

$context.Subscription.TenantID | Write-Host -ForegroundColor Green

$azureRmProfile =

[Microsoft.Azure.Commands.Common.Authentication.Abstractions.AzureRm

ProfileProvider]::Instance.Profile

$profileClient = New-Object

Microsoft.Azure.Commands.ResourceManager.Common.RMProfileClient($azu

reRmProfile)

$newtoken =

$profileClient.AcquireAccessToken($context.Subscription.TenantID)

$armEndpoint = $context.Environment.ResourceManagerUrl

$applicationRegistrationParams = @{

Method = [Microsoft.PowerShell.Commands.WebRequestMethod]::Get

Headers = @{ Authorization = "Bearer " + $newtoken.AccessToken }

Uri =

"$($armEndpoint.ToString().TrimEnd('/'))/applicationRegistrations?

api-version=2014-04-01-preview"

}

$applicationRegistrations = Invoke-RestMethod

@applicationRegistrationParams | Select-Object -ExpandProperty value

c. Work with your Azure AD administrator to remove the app registrations in the

previously generated list.

For disconnected environments, follow the Remove the activation resource from Azure

Stack Hub procedure.

There are two options to shut down your Azure Stack Hub system. Both commands

require the cloud administrator to connect to the Privileged Endpoint:

1. Shut down Azure Stack Hub (recoverable): run the Stop-AzureStack PowerShell

cmdlet from the Privileged Endpoint.

2. Shut down Azure Stack Hub (non-recoverable, data is wiped): run the StartAzsCryptoWipe cmdlet from the Privileged Endpoint.

Learn about Azure Stack Hub diagnostic tools

Stop-AzureStack

Start-AzsCryptoWipe

"[{0}] App Registrations were found for {1}" -f

$applicationRegistrations.appId.Count, $context.Environment.Name |

Write-Host -ForegroundColor Green

$applicationRegistrations.appId | Write-Host

７ Note

Proceed with app registration cleanup with caution. Outside of the

Privileged Endpoint (PEP), your Azure Stack Hub system becomes unusable

once these are removed. The app registrations cannot be restored, and

your system will not function without being redeployed.

Disconnected scenarios

Shut down Azure Stack Hub

） Important

After this command is executed, the stamp is not recoverable.

Next steps

Azure Site Recovery failback tool

Article • 07/27/2021

In a connected environment, you can use Azure Site Recovery to protect virtual

machines (VMs) running on Azure Stack Hub. This article describes how to set up the

environment, and how Site Recovery helps contribute to the overall business continuity

and disaster recovery strategy for these workloads.

In the event of an outage, the Azure Stack Hub operator goes through the failover

procedure; once Azure Stack Hub is up and running again, they go through a failback

process. The failover process is described in this Site Recovery article, but the failback

process involves several manual steps:

1. Stop the VM running in Azure.

2. Download the VHDs.

3. Upload the VHDs to Azure Stack Hub.

4. Recreate the VMs.

5. Finally, start that VM running on Azure Stack Hub.

As this process can be error prone and time consuming, we've built scripts to help

accelerate and automate this process.

The automated failback process contains three main parts:

Copy-AzSiteRecoveryVmVHD:

Shuts down the Azure VM.

Prepares the disk export.

Copies the disk either through AzCopy or StorageBlobCopy.

Uploads the disk to an Azure Stack Hub storage account.

７ Note

The Azure Site Recovery tool requires the Azure Stack Hub Az modules. If you are

running the Azure Stack Hub AzureRM modules, you must upgrade your

workstation or use the Azure Site Recovery failback tool in an isolated environment

with the Az modules. For more information, see Install PowerShell Az module for

Azure Stack Hub.

Failback procedure

Once the disk is copied, there are two scenarios covered by PrepareAzSiteRecoveryVMFailBack:

The original Azure Stack Hub has recovered. The original VM still exists, and you

only need to change its VHDs.

In the case of a disaster, if the original VMs are lost, you must rebuild the entire

VM.

This procedure covers both scenarios by creating the template and the parameter

file required.

The actual deployment of the Azure Resource Manager template using the

parameter file, and deploy/create the VM on Azure Stack Hub.

The following prerequisites are required to perform the failback procedure:

Copy the Azure Site Recovery failback tool .

Import the FailbackTool.psm1 module in PowerShell.

Follow the procedure in this article to install the Az module for Azure Stack Hub.

(optional) Download AzCopy version 10.

Copying the blob using AzCopy is faster, but requires extra local disk space to

temporarily store the blob file.

If AzCopy is not used, the VHD copy is done using AzStorageBlobCopy. This

means no local storage is required, but the process takes longer.

Access to the resources on the Azure portal, and access to create these resources

on Azure Stack Hub.

Call the Copy-AzSiteRecoveryVmVHD PowerShell cmdlet to stop the Azure VM,

download the VHDs from Azure, and upload them to Azure Stack Hub. For example:

PowerShell

Prerequisites

Step 1: Copy blob from Azure to Azure Stack

Hub

$uris = Copy-AzSiteRecoveryVmVHD `

-SourceVM $vmOnAzure `

-TargetStorageAccountName "targetaccountName" `

-TargetStorageEndpoint "redmond.ext-v.masd.stbtest.microsoft.com" `

Note the following considerations:

This example uses $uris to hold the SourceDiskVhdUris value used in step 2.

The -SourceVM parameter is a VM object retrieved by Get-AzVM .

This is the protected VM from Azure Stack Hub that was failed over on Azure.

It doesn't matter if the VM is running, as the script shuts down the VM.

However, it is recommended that you explicitly shut it down and stop the

services inside the VM accordingly.

You can provide either an account key (using TargetStorageAccountKey ) or the SAS

token (using TargetStorageAccountSasToken ) of the storage account on the Azure

Stack Hub side. The SAS token must be created at the storage account level, with

at least the following permissions:

You can provide either the storage endpoint, which includes the region and FQDN;

for example, regionname.azurestack.microsoft.com , or the environment name of

the Azure Stack Hub, such as AzureStackTenant . If the environment name is used, it

should be listed using Get-AzEnvironment.

You can choose to use AzCopy or AzStorageBlobCopy to copy the VHD from

Azure to Azure Stack Hub. AzCopy is faster, but it must download VHD files to a

local folder first:

To use AzCopy, provide the parameters -AzCopyPath and -VhdLocalFolder (the

path where the VHDs will be copied).

If there is not enough space locally, you can choose to copy the VHD directly,

without AzCopy, by omitting the parameters -AzCopyPath and -VhdLocalFolder .

By default, this command uses AzStorageBlobCopy to copy directly to the

Azure Stack Hub storage account.

-TargetStorageAccountKey $accountKey `

-AzCopyPath "C:\azcopy\_v10\azcopy.exe" `

-VhdLocalFolder "C:\tempfolder"

After the disk is copied, use the Prepare-AzSiteRecoveryVMFailBack cmdlet to create

the $templateFile and $parameterFile required to deploy the VM on Azure Stack Hub:

PowerShell

Note the following considerations:

This example uses -SourceDiskVhdUris as a return value from step 1 (using $uris ).

This cmdlet supports two scenarios:

By specifying -TargetVM , you assume that the VM is active on the Azure Stack

Hub side, and you want to replace its disks with the latest ones copied from

Azure.

The script generates a Resource Manager template to deploy this VM, and

deletes the existing VM from Azure Stack Hub.

By not providing the -TargetVM parameter, the script assumes that the VM no

longer exists on the Azure Stack Hub side, so the script creates a Resource

Manager template to deploy a completely new VM.

The generated Resource Manager template files are placed under -

ArmTemplateDestinationPath , and the full path of the template file or parameter file

is returned.

Step 2: Generate Resource Manager templates

$templateFile, $parameterFile = Prepare-AzSiteRecoveryVMFailBack `

-SourceContextName "PublicAzure" `

-SourceVM $vmOnAzure `

-SourceDiskVhdUris $uris `

-TargetResourceLocation "redmond" `

-ArmTemplateDestinationPath

"C:\ARMtemplates" `

-TargetVM $vmOnHub `

-TargetContextName "AzureStack"

７ Note

Deleting the Azure Stack Hub VM itself doesn't remove the other objects

(such as VNET, resource group, NSGs). It only removes the VM resource itself,

and then the template is deployed with the -incremental parameter.

If the -TargetVM parameter is provided, the cmdlet deletes the VM, so you can

continue with the following steps.

At this point, the VHD is uploaded to Azure Stack Hub, and the Resource Manager

template and respective parameter files are created. All that's left is to deploy the VM on

Azure Stack Hub.

In some scenarios, you might want to edit this template and add, remove, or change

some names or resources. This is permitted, as you can edit and adjust the template as

needed.

When ready, and after confirming the resources in the Resource Manager template are

as expected, you can call the New-AzResourceGroupDeployment cmdlet to deploy the

resources. For example:

PowerShell

Note the following considerations:

The -ResourceGroupName parameter should be an existing resource group.

The -TemplateFile and -TemplateParameterFile parameters come from the return

values in step 2.

Azure Stack Hub VM features

Add and remove a custom VM image to Azure Stack Hub

Create a Windows VM with PowerShell in Azure Stack Hub

Step 3: Deploy the Resource Manager template

New-AzResourceGroupDeployment `

-Name "Failback" `

-ResourceGroupName "failbackrg" `

-TemplateFile $templateFile `

-TemplateParameterFile $parameterFile `

-Mode Incremental

Next steps

Manage Azure Stack Hub storage

accounts

Article • 07/29/2022

Learn how to manage Azure Stack Hub storage accounts. Find, recover, and reclaim

storage capacity based on business needs.

The list of storage accounts in the region can be viewed in Azure Stack Hub by following

these steps:

1. Sign in to the administrator portal

https://adminportal.local.azurestack.external .

2. Select All services > Storage > Storage accounts.

By default, the first 10 accounts are displayed. You can choose to fetch more by clicking

the Load more link at the bottom of the list.

OR

If you're interested in a particular storage account - you can filter and fetch the relevant

accounts only.

To filter for accounts:

1. Select Filter at the top of the pane.

Find a storage account

2. On the Filter pane, it allows you to specify account name, subscription ID, or

status to fine-tune the list of storage accounts to be displayed. Use them as

appropriate.

3. As you type, the list will automatically apply the filter.

4. To reset the filter: select Filter, clear out the selections and update.

The search text box (on the top of the storage accounts list pane) lets you highlight the

selected text in the list of accounts. You can use this when the full name or ID isn't easily

available.

You can use free text here to help find the account you're interested in.

Once you've located the accounts you're interested in viewing, you can select the

particular account to view certain details. A new pane opens with the account details.

These details include the kind of account, creation time, location, and so on.

Look at account details

You may be in a situation where you need to recover a deleted account.

In Azure Stack Hub, there's a simple way to do that:

1. Browse to the storage accounts list. For more information, see Find a storage

account at the top of this article.

2. Locate that particular account in the list. You may need to filter.

3. Check the state of the account. It should say Deleted.

4. Select the account, which opens the account details pane.

5. On top of this pane, locate the Recover button and select it.

6. Select Yes to confirm.

Recover a deleted account

7. The recovery is now in process. Wait for an indication that it was successful. You

can also select the "bell" icon at the top of the portal to view progress indications.

Once the recovered account is successfully synchronized, it can be used again.

Your deleted account shows state as out of retention.

Out of retention means that the deleted account has exceeded the retention

period and may not be recoverable.

Your deleted account doesn't show in the accounts list.

You account may not show in the account list when the deleted account has

already been garbage collected. In this case, it can't be recovered. For more

information, see Reclaim capacity in this article.

The retention period setting allows a cloud operator to specify a time period in days

(between 0 and 9999 days) during which any deleted account can potentially be

recovered. The default retention period is set to 0 days. Setting the value to "0" means

Some Gotchas

Set the retention period

that any deleted account is immediately out of retention and marked for periodic

garbage collection.

To change the retention period:

1. Sign in to the administrator portal

https://adminportal.local.azurestack.external .

2. Select All services > Region management under Administration.

3. Select Resources providers > Storage > Settings. Your path is Home > region -

Resource providers > Storage.

4. Select Configuration then edit the retention period value.

Set the number of days and then save it.

This value is immediately effective and is set for your entire region.

One of the side effects of having a retention period is that a deleted account continues

to consume capacity until it comes out of the retention period. As a cloud operator, you

may need a way to reclaim the deleted account space even though the retention period

hasn't yet expired.

You can reclaim capacity using either the portal or PowerShell.

To reclaim capacity using the portal:

1. Navigate to the storage accounts pane. See Find a storage account.

Reclaim capacity

2. Select Reclaim space at the top of the pane.

3. Read the message and then select OK.

4. Wait for success notification. See the bell icon on the portal.

5. Refresh the Storage accounts page. The deleted accounts are no longer shown in

the list because they've been purged.

You can also use PowerShell to explicitly override the retention period and immediately

reclaim capacity.

To reclaim capacity using PowerShell:

1. Confirm that you have Azure PowerShell installed and configured. If not, use the

following instructions:

To install the latest Azure PowerShell version and associate it with your Azure

subscription, see How to install and configure Azure PowerShell. For more

information about Azure Resource Manager cmdlets, see Using Azure

PowerShell with Azure Resource Manager.

2. Run the following cmdlets:

PowerShell

For more information, see Azure Stack Hub PowerShell documentation.

For information on managing permissions, see Set access permissions using rolebased access control.

For information on managing storage capacity for Azure Stack Hub, see Manage

storage capacity for Azure Stack Hub.

７ Note

If you run these cmdlets, you permanently delete the account and its contents. It's

not recoverable. Use this with care.

$farm\_name = (Get-AzsStorageFarm)[0].name

Start-AzsReclaimStorageCapacity -FarmName $farm\_name

Next steps

Manage storage capacity for Azure

Stack Hub

Article • 07/29/2022

You can use this article as an Azure Stack Hub cloud operator to learn how to monitor

and manage the storage capacity of your Azure Stack Hub deployment. You can use the

guidance to understand the memory available for your user's VMs. The Azure Stack Hub

storage infrastructure allocates a subset of the total storage capacity of the Azure Stack

Hub deployment as storage services. Storage services store a tenant's data in shares on

volumes that correspond to the nodes of the deployment.

As a cloud operator, you have a limited amount of storage to work with. The amount of

storage is defined by the solution you implement. The solution is provided by your OEM

vendor when you use a multinode solution, or it's provided by the hardware on which

you install the Azure Stack Development Kit (ASDK).

Azure Stack Hub only supports the expansion of storage capacity by adding extra scale

unit nodes. For more information, see add scale unit nodes in Azure Stack Hub. Adding

physical disks to the nodes won't expand the storage capacity.

It's important to monitor the available storage to ensure that efficient operations are

maintained. When the remaining free capacity of a volume becomes limited, plan to

manage the available space to prevent the shares from running out of capacity.

Your options for managing capacity include:

Reclaiming capacity.

Migrating storage objects.

When an object store volume is 100% utilized, the storage service no longer functions

for that volume. To get assistance in restoring operations for the volume, contact

Microsoft support.

Tenant user creates disks, blobs, tables, and queues in Azure Stack Hub storage services.

These tenant data are put on volumes on top of the available storage.

Understand disks, containers, and volumes

Disks

VM store and manipulate data on virtual disks. Each VM starts with an OS disk, created

from a marketplace image or private image. The VM can attach zero or more data disks.

There are two types of disks offered in Azure Stack:

Managed disks simplify disk management for Azure IaaS VMs by managing the storage

accounts associated with the VM disks. You only have to specify the size of disk you

need, and Azure Stack Hub creates and manages the disk for you. For more information,

see Managed Disks Overview.

Unmanaged disks are VHD files that are stored as page blobs in storage containers in

Azure Stack storage accounts. The page blobs created by tenants are referred to as VM

disks and are stored in containers in the storage accounts. We recommend you use

unmanaged disks only for VMs that need to be compatible with third-party tools, which

only support Azure unmanaged disks.

The guidance to tenants is to place each disk into a separate container to improve

performance of the VM.

Each container that holds a disk, or page blob, from a VM is considered an

attached container to the VM that owns the disk.

A container that doesn't hold any disks from a VM is considered a free container.

The options to free up space on an attached container are limited. To learn more, see

Distribute unmanaged disks.

） Important

We recommended that you use only Managed disks in VMs for easier

management. You don't have to prepare storage accounts and containers before

using Managed disks. Managed disks provide equivalent or better functionality and

performance compared to unmanaged disks. There are no advantages to use

unmanaged disks and they are only provided for backward compatibility.

Managed disks are optimized for better placement in the storage infrastructure and

have significantly reduced management overhead. But due to Managed disks are

thin provisioned and the final utilization is unpredictable in creation, there are

opportunities of volume being over-utilized caused by unbalanced disk placement.

Operators are responsible for monitoring the storage capacity usage and avoid

such issue.

For users that use ARM templates to provision new virtual machines, use the

following document to understand how to modify your templates to use managed

disks: Use VM managed disks templates.

VM disks are stored as sparse files on storage infrastructure. Disks have provisioned size

that the user requests at the time the disk is created. However only the non-zero pages

written to the disk occupy space on the underlying storage infrastructure.

Disks are often created by copying from platform images, managed images, snapshots,

or other disks. And snapshots are taken from disks. To increase utilization of storage

capacity and reduce copy operation time the system uses block cloning in ReFS. Blob

cloning is a low-cost metadata operation rather than a full byte-by-byte copy between

files. The source file and target file can share the same extents, identical data isn't

physically stored multiple times, improving storage capacity.

The capacity usage grows only when the disks are written, and identical data reduces.

When an image or a disk is deleted, the space may not be freed immediately because

there could be disks or snapshots created from it still keep the identical data and occupy

space. Only if all the related entities are removed, the space becomes available.

Tenant users store massive amounts of unstructured data with Azure Blob. Azure Stack

Hub supports three types of Blobs: Block Blobs, Append Blobs and Page Blobs. For more

information about the different types of blobs, see Understanding Block Blobs, Append

Blobs, and Page Blobs.

Tenant users create containers that are then used to store blob data. Although users

decide in which container to place blobs, the storage service uses an algorithm to

determine on which volume to put the container. The algorithm typically chooses the

volume with the most available space.

After a blob is placed in a container, the blob can grow to use more space. As you add

new blobs and existing blobs grow, the available space in the volume that holds the

container shrinks.

Containers aren't limited to a single volume. When the combined blob data in a

container grows to use 80% or more of the available space, the container enters

overflow mode. When in overflow mode, any new blobs that are created in that

container are allocated to a different volume that has sufficient space. Over time, a

container in overflow mode can have blobs that are distributed across multiple volumes.

When 90% (and then 95%) of the available space in a volume is used, the system raises

alerts in the Azure Stack Hub administrator portal. Cloud operators should review

available storage capacity and plan to rebalance the content. The storage service stops

working when a disk is 100% used and no additional alerts are raised.

The storage service partitions the available storage into separate volumes that are

allocated to hold system and tenant data. Volumes combine the drives in the storage

pool to introduce the fault tolerance, scalability, and performance benefits of Storage

Spaces Direct. For more information about volumes in Azure Stack Hub, see Manage

storage infrastructure for Azure Stack Hub.

Blobs and containers

Volumes

Object store volumes hold tenant data. Tenant data includes page blobs, block blobs,

append blobs, tables, queues, databases, and related metadata stores. The number of

object store volumes is equal to the number of nodes in the Azure Stack Hub

deployment:

On a four-node deployment, there are four object store volumes. On a multinode

deployment, the number of volumes isn't reduced if a node is removed or

malfunctioning.

If you use the ASDK, there's a single volume with a single share.

The object store volumes are for the exclusive use of storage services. You must not

directly modify, add, or remove any files on the volumes. Only storage services should

work on the files stored in these volumes.

Because the storage objects (blobs, and so on) are individually contained within a single

volume, the maximum size of each object can't exceed the size of a volume. The

maximum size of new objects depends on the capacity that remains in a volume as

unused space when that new object is created.

When an object store volume is low on free space and actions to reclaim space aren't

successful or available, Azure Stack Hub cloud operators can migrate storage objects

from one volume to another.

For information about how tenant users work with blob storage in Azure Stack Hub, see

Azure Stack Hub Storage services.

Use Azure PowerShell or the administrator portal to monitor provisioned and used

capacity and plan for migration to ensure continuous normal operation of the system.

There are three tools for monitoring volume capacity:

Portal and PowerShell of for current volume capacity.

Storage space alerts.

Volume capacity metrics.

In this section, we will introduce how to use these tools to monitor the capacity of the

system.

Monitor storage

Use PowerShell

As a cloud operator, you can monitor the storage capacity of a volume using the

PowerShell Get-AzsVolume cmdlet. The cmdlet returns the total and free space in

gigabyte (GB) on each of the volumes.

Total capacity: The total space in GB that's available on the share. This space is

used for data and metadata that's maintained by the storage services.

Remaining capacity: The amount of space in GB that's free to store the tenant data

and associated metadata.

As a cloud operator, you can use the administrator portal to view the storage capacity of

all volumes.

1. Sign in to the Azure Stack Hub administrator portal

( https://adminportal.local.azurestack.external ).

2. Select All services > Storage > Volumes to open the volume list where you can

view the usage information.

Use the administrator portal

Total: The total space available on the volume. This space is used for data and

metadata that's maintained by the storage services.

Used: The amount of data that's used by the all the extents from the files that

store the tenant data and associated metadata.

When you use the administrator portal, you receive alerts about volumes that are low on

space.

Warning: When a file share is over 90% utilized, you receive a Warning alert in the

administrator portal:

Critical: When a file share is over 95% utilized, you receive a Critical alert in the

administrator portal:

Storage space alerts

） Important

As a cloud operator, you should prevent shares from reaching full usage. When a

share is 100% utilized, the storage service no longer functions for that share. To

recover free space and restore operations on a share that's 100% utilized, you must

contact Microsoft support.



View details: In the administrator portal, you can open an alert's details to view

your mitigation options:

Volume capacity metrics give you more detailed information about provisioned capacity

and used capacity for different types of objects. The metrics data are preserved for 30

days. Background monitoring service refreshes the volume capacity metrics data hourly.

It is necessary to understand the resource usage of a volume by proactively checking

the capacity metric report. The cloud operator can analyze the resource type distribution

when a volume is approaching full to decide the corresponding action to free space. The

operator can also prevent the volume being overused when the disk provisioned size

indicates the volume has been over-provisioned too much.

Azure Monitor provides following metrics to show volume capacity utilization:





Volume capacity metrics

Volume Total Capacity shows the total storage capacity of the volume.

Volume Remaining Capacity shows the remaining storage capacity of the volume.

Volume VM Disk Used Capacity shows the total spaces occupied by VM disk

related objects (including page blobs, managed disks/snapshot, managed images,

and platform images). The underlying VHD file of VM disks can share the same

extent (refer to Disks) with images, snapshots or other disks. This number could be

smaller than sum of the used capacity of all individual VM disk related object.

Volume Other Used Capacity is the total used size of objects other than disks –

including block blobs, append blobs, tables, queues, and blob metadata.

Volume VM Disk Provisioned Capacity is total provisioned size of page blobs and

managed disks/snapshots. This size is the maximum value of total disk capacity of

all managed disks and page blobs on the specific volume can grow to.

To view volume capacity metrics in Azure Monitor:

1. Confirm that you have Azure PowerShell installed and configured. For instructions

on configuring the PowerShell environment, see Install PowerShell for Azure Stack

Hub. To sign in to Azure Stack Hub, see Configure the operator environment and

sign in to Azure Stack Hub.

2. Download Azure Stack Hub tools from GitHub repository . For detailed steps, see

Download Azure Stack Hub tools from GitHub.

3. Generate the Capacity Dashboard json by running the DashboardGenerator under

CapacityManagement.

PowerShell

.\CapacityManagement\DashboardGenerator\Create-AzSStorageDashboard.ps1

-capacityOnly $true -volumeType object

There would be a json file named starts with DashboardVolumeObjStore under the

folder of DashboardGenerator.

4. Sign in to the Azure Stack Hub administrator portal

( https://adminportal.local.azurestack.external ).

5. In Dashboard page, click Upload, and select the json file generated in Step 3.

6. Once the json is uploaded, you would be directed to the new capacity dashboard.

Each volume has a corresponding chart in the dashboard. The number of charts

equals to the count of volumes:

7. By clicking one of the volumes, you can check five capacity metrics of the specific

volume in the detailed chart:

By checking the volume capacity metrics, the cloud operator understands how much a

volume’s capacity is utilized, and which resource type is taking most of the space usage.

The space usage pattern could be grouped to following types, which operator should

take different action for each of the types:

Under-provisioned, spare capacity: there’s enough available capacity on the volume,

and the total provisioned capacity of all disks located on this volume is smaller than the

total available capacity. The volume is available for more storage objects, including both

disks and other objects (block/append blobs, tables and queues). You don’t need to take

any action to operate the volume.

Volume usage patterns

Over-provisioned, spare capacity: the remaining capacity of the volume is high, but the

VM disk provisioned capacity is already above volume total capacity. This volume still

has room for more storage objects now. However it has potential to be filled with the

data in the VM disks located on this volume. You should closely monitor the usage trend

of this volume. If it changes to over-provisioned, low capacity pattern, you may need to

take action to free the space.

Over-provisioned, low capacity: the remaining capacity of the volume is low, and both

of the VM disk provisioned capacity and VM disk used capacity is high.

The low remaining capacity indicates the volume is reaching full usage. Operators need

to take immediate action to free space to prevent the volume being 100% utilized which

would block the storage service. The high VM disk used capacity shows the majority of

the volume usage is VM disks. You should refer instruction of Migrate disk to move disks

from the full volume to other available volumes to free space.

Under-provisioned, low capacity, high block blobs: the remaining capacity of the

volume is low, and both of the VM disk provisioned capacity and VM disk used capacity

is low, but the other used capacity is high.

The volume has the risk of being fully utilized that operator should take immediate

action to free space. The high other used capacity indicates most of the volume capacity

is taken by block/append blobs or table/queue. When the volume’s available capacity is

less than 20%, container overflow would be enabled, and new blob object won’t be

placed on this almost full volume. But the existing blobs may still grow. To prevent the

continuous growing blobs overuse the capacity, you can contact Microsoft Support to

query the containers occupying space on the specific volume, and decide whether

cleanup of those containers needs to be done by tenants to free up some space.

Over-provisioned, low capacity, high block blobs: the remaining capacity of the volume

is low, and both the disk used/provisioned capacity and other used capacity is high. This

volume has high space utilization by both disks and other storage objects. You should

free space of it to avoid volume being totally full. It is recommended to firstly following

instruction of Migrate disk to move disks from the full volume to other available

volumes. In other case, you can contact Microsoft Support to query the containers

occupying space on the specific volume, and decide whether cleanup of those

containers needs to be done by tenants to free up some space.

When it's necessary to free space on a volume, use the least invasive methods first. For

example, try to reclaim space before you choose to migrate a managed disk.

Manage available space

You can reclaim the capacity that's used by tenant accounts that have been deleted. This

capacity is automatically reclaimed when the data retention period is reached, or you

can act to reclaim it immediately.

For more information, see the "Reclaim capacity" section of Manage Azure Stack Hub

storage accounts.

This option applies only to Azure Stack Hub integrated systems.

Because of tenant usage patterns, some tenant volumes use more space than others.

The result can be a volume that runs low on space before other volumes that are

relatively unused.

You can free up space on an overused volume by manually migrating some managed

disks to a different volume. You can migrate several managed disks to a single volume

that has capacity to hold them all. Use migration to move offline managed disks. Offline

managed disks are disks that aren't attached to a VM.

1. Confirm that you have Azure PowerShell installed and configured. For instructions

on configuring the PowerShell environment, see Install PowerShell for Azure Stack

Hub. To sign in to Azure Stack Hub, see Configure the operator environment and

sign in to Azure Stack Hub.

Reclaim capacity

Migrate a managed disk between volumes

） Important

Migration of managed disks is an offline operation that requires the use of

PowerShell. You must deallocate the owner VMs of the candidate disk, or detach

the candidate disks for migration from their owner VM before starting migration

job (once the migration job is done, you can reallocate the VMs or reattach the

disks). Until migration completes, all managed disks you are migrating must remain

reserved or offline status and can't be used, otherwise the migration job would

abort and all unmigrated disks are still on their original volumes. You should also

avoid upgrading Azure Stack Hub until all ongoing migration completes.

To migrate managed disks using PowerShell

2. Examine the managed disks to understand what disks are on the volume that you

plan to migrate. To identify the best candidate disks for migration in a volume, use

the Get-AzsDisk cmdlet:

PowerShell

Then examine $disks:

PowerShell

3. Identify the best destination volume to hold the disks you migrate:

$ScaleUnit = (Get-AzsScaleUnit)[0]

$StorageSubSystem = (Get-AzsStorageSubSystem -ScaleUnit

$ScaleUnit.Name)[0]

$Volumes = (Get-AzsVolume -ScaleUnit $ScaleUnit.Name -StorageSubSystem

$StorageSubSystem.Name | Where-Object {$\_.VolumeLabel -Like

"ObjStore\_\*"})

$SourceVolume = ($Volumes | Sort-Object RemainingCapacityGB)[0]

$VolumeName = $SourceVolume.Name.Split("/")[2]

$VolumeName = $VolumeName.Substring($VolumeName.IndexOf(".")+1)

$MigrationSource =

"\\SU1FileServer."+$VolumeName+"\SU1\_"+$SourceVolume.VolumeLabel

$Disks = Get-AzsDisk -Status OfflineMigration -SharePath

$MigrationSource | Select-Object -First 10

$Disks

PowerShell

4. Start migration for managed disks. Migration is asynchronous. If you start

migration of other disks before the first migration completes, use the job name to

track the status of each.

PowerShell

5. Use the job name to check on the status of the migration job. When the disk

migration is complete, MigrationStatus is set to Complete.

PowerShell

If you are migrating multiple managed disks in one migration job, you can also

check the sub tasks of the job.

PowerShell

$DestinationVolume = ($Volumes | Sort-Object RemainingCapacityGB -

Descending)[0]

$VolumeName = $DestinationVolume.Name.Split("/")[2]

$VolumeName = $VolumeName.Substring($VolumeName.IndexOf(".")+1)

$MigrationTarget =

"\\SU1FileServer."+$VolumeName+"\SU1\_"+$DestinationVolume.VolumeLabel

$jobName = "MigratingDisk"

Start-AzsDiskMigrationJob -Disks $Disks -TargetShare $MigrationTarget -

Name $jobName

$job = Get-AzsDiskMigrationJob -Name $jobName

$job.Subtasks

6. You can cancel an in-progress migration job. Canceled migration jobs are

processed asynchronously. You can track cancellation by using job name until the

status confirms the migration job is Canceled:

PowerShell

This option applies only to Azure Stack Hub integrated systems.

The most extreme method for managing space involves moving unmanaged disks. If the

tenant adds numbers of unmanaged disks to one container, the total used capacity of

the container could grow beyond the available capacity of the volume that holds it

before the container entering overflow mode. To avoid single container exhaust the

space of a volume, the tenant could distribute the existing unmanaged disks of one

container to different containers. Because distributing an attached container (one that

contains a VM disk) is complex, contact Microsoft Support to accomplish this action.

Stop-AzsDiskMigrationJob -Name $jobName

Distribute unmanaged disks

Memory available for VMs

Azure Stack Hub is built as a hyper-converged cluster of compute and storage. The

convergence allows for the sharing of the hardware, referred to as a scale unit. In Azure

Stack Hub, a scale unit provides the availability and scalability of resources. A scale unit

consists of a set of Azure Stack Hub servers, referred to as hosts or nodes. The

infrastructure software is hosted within a set of VMs and shares the same physical

servers as the tenant VMs. All Azure Stack Hub VMs are then managed by the scale

unit's Windows Server clustering technologies and individual Hyper-V instances. The

scale unit simplifies the acquisition and management Azure Stack Hub. The scale unit

also allows for the movement and scalability of all services across Azure Stack Hub,

tenant and infrastructure.

You can review a pie chart in the administration portal that shows the free and used

memory in Azure Stack Hub like below:

The following components consume the memory in the used section of the pie chart:

Host OS usage or reserve This is the memory used by the operating system (OS)

on the host, virtual memory page tables, processes that are running on the host

OS, and the spaces direct memory cache. Since this value is dependent on the

memory used by the different Hyper-V processes running on the host, it can

fluctuate.

Infrastructure services These are the infrastructure VMs that make up Azure Stack

Hub. This entails approximately 31 VMs that take up 242 GB + (4 GB x number of

nodes) of memory. The memory utilization of the infrastructure services

component may change as we work on making our infrastructure services more

scalable and resilient.

Resiliency reserve Azure Stack Hub reserves a portion of the memory to allow for

tenant availability during a single host failure and during patch and update to

allow for successful live migration of VMs.

Tenant VMs These are the VMs created by Azure Stack Hub users. In addition to

running VMs, memory is consumed by any VMs that have landed on the fabric.

This means that VMs in Creating or Failed state, or VMs shut down from within the

guest, will consume memory. However, VMs that have been deallocated using the

stop deallocated option from Azure Stack Hub user portal, PowerShell, and Azure

CLI will not consume memory from Azure Stack Hub.

Add-on Resource Providers VMs deployed for the add-on resource providers such

as SQL, MySQL, and App Service.

As a cloud operator for Azure Stack Hub, there isn't an automated way to check the

allocated memory for each VM. You can have access to your user VMs, and calculate the

allocated memory manually. However, the allocated memory will not reflect the real use.

This value can be lower than the allocated value.

To workout available memory for VMs the following formula is used:

Available Memory for VM placement = Total Host Memory--Resiliency Reserve--

Memory used by running tenant VMs - Azure Stack Hub Infrastructure Overhead

Resiliency reserve = H + R \* ((N-1) \* H) + V \* (N-2)

Where:

H = Size of single host memory

N = Size of scale unit (number of hosts)

R = Operating system reserve/memory used by the Host OS, which is .15 in this formula

V = Largest VM (memory wise) in the scale unit

Azure Stack Hub Infrastructure Overhead = 242 GB + (4 GB x # of nodes). This

accounts for the approximately 31 VMs are used to host Azure Stack Hub's

Available Memory for VM placement

infrastructure.

Memory used by the Host OS = 15 percent (0.15) of host memory. The operating

system reserve value is an estimate and will vary based on the physical memory capacity

of the host and general operating system overhead.

The value V, largest VM in the scale unit, is dynamically based on the largest tenant VM

deployed. For example, the largest VM value could be 7 GB or 112 GB or any other

supported VM memory size in the Azure Stack Hub solution. We pick the size of the

largest VM here to have enough memory reserved so a live migration of this large VM

would not fail. Changing the largest VM on the Azure Stack Hub fabric will result in an

increase in the resiliency reserve in addition to the increase in the memory of the VM

itself.

For example, with a 12 node scale unit:

Stamp details Values

sts (N) 12

Memory per Host (H) 384

Total Memory of Scale Unit 4608

OS reserve (R) 15%

Largest VM (V) 112

Resiliency Reserve = H + R \* ((N-1) \* H) + V \* (N-2)

Resiliency Reserve = 2137.6

So with the above information, you can calculate that an Azure Stack with 12 nodes of

384 GB per host (Total 4,608 GB) has 2,137 GB reserved for resiliency if the largest VM

has 112-GB memory.

When you consult the Capacity blade for the Physical memory as per below, the Used

value includes the Resiliency Reserve. The graph is from a four node Azure Stack Hub

instance.

Keep these considerations in mind while planning the capacity for Azure Stack Hub. In

addition, you can use the Azure Stack Hub Capacity Planner.

To learn more about offering VMs to users, see Manage storage capacity for Azure Stack

Hub.

Next steps

Manage storage infrastructure for Azure

Stack Hub

Article • 07/29/2022

This article describes the health and operational status of Azure Stack Hub storage

infrastructure resources. These resources include storage drives and volumes. The

information in this topic helps you troubleshoot various issues, like when a drive can't

be added to a pool.

To find out what state volumes are in, use the following PowerShell commands:

PowerShell

Here's an example of output showing a detached volume and a degraded/incomplete

volume:

VolumeLabel HealthStatus OperationalStatus

ObjStore\_1 Unknown Detached

ObjStore\_2 Warning {Degraded, Incomplete}

The following sections list the health and operational states:

Operational

state

Description

OK The volume is healthy.

Volume states

$scaleunit\_name = (Get-AzsScaleUnit)[0].name

$subsystem\_name = (Get-AzsStorageSubSystem -ScaleUnit $scaleunit\_name)

[0].name

Get-AzsVolume -ScaleUnit $scaleunit\_name -StorageSubSystem $subsystem\_name |

Select-Object VolumeLabel, HealthStatus, OperationalStatus, RepairStatus,

Description, Action, TotalCapacityGB, RemainingCapacityGB

Volume health state: Healthy

Operational

state

Description

Suboptimal Data isn't written evenly across drives.

Action: Contact Support to optimize drive usage in the storage pool. Before you

do, start the log file collection process using the guidance from

https://aka.ms/azurestacklogfiles . You may have to restore from backup after the

failed connection is restored.

When the volume is in a Warning health state, it means that one or more copies of your

data are unavailable but Azure Stack Hub can still read at least one copy of your data.

Operational

state

Description

In service Azure Stack Hub is repairing the volume, like after adding or removing a drive.

When the repair is complete, the volume should return to the OK health state.

Action: Wait for Azure Stack Hub to finish repairing the volume and check the

status afterward.

Incomplete The resilience of the volume is reduced because one or more drives failed or are

missing. However, the missing drives contain up-to-date copies of your data.

Action: Reconnect any missing drives, replace any failed drives, and bring online

any servers that are offline.

Degraded The resilience of the volume is reduced because of one or more failed or missing

drives as well as outdated copies of data on the drives.

Action: Reconnect any missing drives, replace any failed drives, and bring online

any servers that are offline.

When a volume is in an Unhealthy health state, some or all of the data on the volume is

currently inaccessible.

Operational

state

Description

Volume health state: Warning

Volume health state: Unhealthy

Operational

state

Description

No

redundancy

The volume has lost data because too many drives failed.

Action: Contact Support. Before you do, start the log file collection process using

the guidance from https://aka.ms/azurestacklogfiles .

The volume can also be in the Unknown health state if the virtual disk has become

detached.

Operational

state

Description

Detached A storage device failure occurred which may cause the volume to be inaccessible.

Some data may be lost.

Action:

1. Check the physical and network connectivity of all storage devices.

2. If all devices are connected correctly, contact Support. Before you do, start the

log file collection process using the guidance from

https://aka.ms/azurestacklogfiles . You may have to restore from backup after the

failed connection is restored.

Use the following PowerShell commands to monitor the state of drives:

PowerShell

The following sections describe the health states a drive can be in:

Volume health state: Unknown

Drive states

$scaleunit\_name = (Get-AzsScaleUnit)[0].name

$subsystem\_name = (Get-AzsStorageSubSystem -ScaleUnit $scaleunit\_name)

[0].name

Get-AzsDrive -ScaleUnit $scaleunit\_name -StorageSubSystem $subsystem\_name |

Select-Object StorageNode, PhysicalLocation, HealthStatus,

OperationalStatus, Description, Action, Usage, CanPool, CannotPoolReason,

SerialNumber, Model, MediaType, CapacityGB

Drive health state: Healthy

Operational

state

Description

OK The volume is healthy.

In service The drive is doing some internal housekeeping operations. When the action is

complete, the drive should return to the OK health state.

A drive in the Warning state can read and write data successfully but has an issue.

Operational

state

Description

Lost

communication

Connectivity has been lost to the drive.

Action: Bring all servers back online. If that doesn't fix it, reconnect the drive. If

this state persists, replace the drive to ensure full resiliency.

Predictive

failure

A failure of the drive is predicted to occur soon.

Action: Replace the drive as soon as possible to ensure full resiliency.

IO error There was a temporary error accessing the drive.

Action: If this state persists, replace the drive to ensure full resiliency.

Transient error There was a temporary error with the drive. This error usually means the drive

was unresponsive, but it could also mean that the Storage Spaces Direct

protective partition was inappropriately removed from the drive.

Action: If this state persists, replace the drive to ensure full resiliency.

Abnormal

latency

The drive is sometimes unresponsive and is showing signs of failure.

Action: If this state persists, replace the drive to ensure full resiliency.

Removing from

pool

Azure Stack Hub is in the process of removing the drive from its storage pool.

Action: Wait for Azure Stack Hub to finish removing the drive, and check the

status afterward.

If the status remains, contact Support. Before you do, start the log file collection

process using the guidance from https://aka.ms/azurestacklogfiles .

Drive health state: Warning

Operational

state

Description

Starting

maintenance

mode

Azure Stack Hub is in the process of putting the drive in maintenance mode.

This state is temporary--the drive should soon be in the In maintenance mode

state.

Action: Wait for Azure Stack Hub to finish the process and check the status

afterward.

In maintenance

mode

The drive is in maintenance mode, halting reads and writes from the drive. This

state usually means Azure Stack Hub administration tasks such as PNU or FRU

are operating the drive. But the admin could also place the drive in

maintenance mode.

Action: Wait for Hub Azure Stack Hub to finish the administration task, and

check the status afterward.

If the status remains, contact Support. Before you do, start the log file collection

process using the guidance from https://aka.ms/azurestacklogfiles .

Stopping

maintenance

mode

Azure Stack Hub is in the process of bringing the drive back online. This state is

temporary - the drive should soon be in another state, ideally Healthy.

Action: Wait for Azure Stack Hub to finish the process and check the status

afterward.

A drive in the Unhealthy state can't currently be written to or accessed.

Operational

state

Description

Split The drive has become separated from the pool.

Action: Replace the drive with a new disk. If you must use this disk, remove the

disk from the system, make sure there's no useful data on the disk, erase the disk,

and then reseat the disk.

Not usable The physical disk is quarantined because it's not supported by your solution

vendor. Only disks that are approved for the solution and have the correct disk

firmware are supported.

Action: Replace the drive with a disk that has an approved manufacturer and

model number for the solution.

Drive health state: Unhealthy

Operational

state

Description

Stale

metadata

The replacement disk was previously used and may contain data from an

unknown storage system. The disk is quarantined.

Action: Replace the drive with a new disk. If you must use this disk, remove the

disk from the system, make sure there's no useful data on the disk, erase the disk,

and then reseat the disk.

Unrecognized

metadata

Unrecognized metadata found on the drive, which usually means that the drive

has metadata from a different pool on it.

Action: Replace the drive with a new disk. If you must use this disk, remove the

disk from the system, make sure there's no useful data on the disk, erase the disk,

and then reseat the disk.

Failed media The drive failed and won't be used by Storage Spaces anymore.

Action: Replace the drive as soon as possible to ensure full resiliency.

Device

hardware

failure

There was a hardware failure on this drive.

Action: Replace the drive as soon as possible to ensure full resiliency.

Updating

firmware

Azure Stack Hub is updating the firmware on the drive. This state is temporary

and usually lasts less than a minute and during which time other drives in the

pool handle all reads and writes.

Action: Wait for Azure Stack Hub to finish the updating and check the status

afterward.

Starting The drive is getting ready for operation. This state should be temporary--once

complete, the drive should transition to a different operational state.

Action: Wait for Azure Stack Hub to finish the operation and check the status

afterward.

Some drives just aren't ready to be in Azure Stack Hub storage pool. You can find out

why a drive isn't eligible for pooling by looking at the CannotPoolReason property of a

drive. The following table gives a little more detail on each of the reasons.

Reason Description

Reasons a drive can't be pooled

Reason Description

Hardware

not

compliant

The drive isn't in the list of approved storage models specified by using the Health

Service.

Action: Replace the drive with a new disk.

Firmware

not

compliant

The firmware on the physical drive isn't in the list of approved firmware revisions by

using the Health Service.

Action: Replace the drive with a new disk.

In use by

cluster

The drive is currently used by a Failover Cluster.

Action: Replace the drive with a new disk.

Removable

media

The drive is classified as a removable drive.

Action: Replace the drive with a new disk.

Not

healthy

The drive isn't in a healthy state and might need to be replaced.

Action: Replace the drive with a new disk.

Insufficient

capacity

There are partitions taking up the free space on the drive.

Action: Replace the drive with a new disk. If you must use this disk, remove the disk

from the system, make sure there's no useful data on the disk, erase the disk, and

then reseat the disk.

Verification

in progress

The Health Service is checking to see if the drive or firmware on the drive is

approved for use.

Action: Wait for Azure Stack Hub to finish the process, and check the status

afterward.

Verification

failed

The Health Service couldn't check to see if the drive or firmware on the drive is

approved for use.

Action: Contact Support. Before you do, start the log file collection process using

the guidance from https://aka.ms/azurestacklogfiles .

Offline The drive is offline.

Action: Contact Support. Before you do, start the log file collection process using

the guidance from https://aka.ms/azurestacklogfiles .

Manage physical memory capacity in

Azure Stack Hub

Article • 07/29/2022

To increase the total available memory capacity in Azure Stack Hub, you can add more

memory. In Azure Stack Hub, your physical server is also referred to as a scale unit node.

All scale unit nodes that are members of a single scale unit must have the same amount

of memory.

The following flow diagram shows the general process to add memory to each scale unit

node.

The following steps provide a high-level overview of the process to add memory.

７ Note

Before you continue, consult your hardware manufacturer's documentation to see if

your manufacturer supports a physical memory upgrade. Your OEM hardware

vendor support contract may require that the vendor perform the physical server

rack placement and the device firmware update.

Add memory to an existing node

２ Warning

Don't follow these steps without referring to your OEM-provided documentation.

２ Warning

The entire scale unit must be shut down as a rolling memory upgrade isn't

supported.

1. Stop Azure Stack Hub using the steps documented in the Start and stop Azure

Stack Hub article.

2. Upgrade the memory on each physical computer using your hardware

manufacturer's documentation.

3. Start Azure Stack Hub using the steps in the Start and stop Azure Stack Hub article.

To learn how to manage storage accounts in Azure Stack Hub, see Manage storage

accounts in Azure Stack Hub.

To learn how to monitor and manage the storage capacity of your Azure Stack Hub

deployment, see Manage storage capacity for Azure Stack Hub.

Next steps

Manage GPU capacity

Article • 04/29/2022

Azure Stack Hub supports adding graphics processing units (GPUs) to an existing Azure

Stack Hub system. You must consult with your hardware partner to verify that your

system was validated and can support GPUs.

In Azure Stack Hub, the physical server is also referred to as a scale unit node. All scale

unit nodes that are members of a single scale unit must have the same type and number

of GPUs.

The following flow shows the general process to add memory to each scale unit node:

The following section provides a high-level overview of the process to add a GPU.

1. The entire scale unit must be shut down, as a rolling GPU upgrade isn't supported.

Stop Azure Stack Hub using the steps documented in the Start and stop Azure

Stack Hub article.

７ Note

Before you continue, consult your hardware manufacturer's documentation to see if

your manufacturer supports GPUs with your system, and how you can order. Your

OEM hardware vendor support contract might require that the vendor performs the

installation.

Overview

Upgrade GPUs or add to an existing node

２ Warning

Do not follow these steps without referring to your OEM-provided documentation.

2. Add or upgrade the memory on each physical computer using your hardware

manufacturer's documentation.

3. Start Azure Stack Hub using the steps in Start and stop Azure Stack Hub.

Azure Stack Hub supports GPU partitioning for the AMD MI25. With GPU partitioning,

you can increase the density of virtual machines using a virtual GPU instance. You can

change the partition size to meet specific workload requirements. By default, Azure

Stack Hub uses the largest partition size (1/8) to provide the highest possible density

with a 2 GB frame buffer. This is useful for workloads that require accelerated graphics

applications and virtual desktops.

To change the partition size, do the following:

1. Deallocate all VMs that are currently using a GPU.

2. Ensure that the PowerShell Az module for Azure Stack Hub is installed.

3. Connect PowerShell to the admin Azure Resource Manager endpoint.

4. Run the following PowerShell cmdlets:

First determine the name of the scale unit to be updated:

PowerShell

Update the following $partitionSize and $scaleUnitName variables using the

"name" value returned in the previous step, then run the following to update the

scale unit partition size:

PowerShell

Supported values for $partitionSize are:

Change GPU partition size

Get-AzsScaleUnit # Returns a list of information

about scale units in your stamp

$partitionSize = 4 # Specify the partition size (1, 2,

4, 8)

$scaleUnitName = "contoso/cluster" # Specify the scale unit name

Set-AzsScaleUnit -Name $scaleUnitName -NumberOfGPUPartition

$partitionSize

Value Description

8 (default) 1/8 of a physical GPU.

4 1/4 of a physical GPU.

2 1/2 of a physical GPU.

1 Entire physical GPU.

Manage storage accounts in Azure Stack Hub.

Monitor and manage the storage capacity of your Azure Stack Hub deployment.

Next steps

Add scale unit nodes in Azure Stack Hub

Article • 07/29/2022

You can increase the overall capacity of an existing scale unit by adding another physical

computer. The physical computer is also referred to as a scale unit node. Each new node

must have the same CPU type, memory, disk number, and size as the nodes already

present in the scale unit. Azure Stack Hub doesn't support removing scale unit nodes for

scaling down because of architectural limitations. It's only possible to expand capacity

by adding nodes. The maximum size of a scale unit is 4-16 nodes.

To add a scale unit node, you'll need administrator privileges to access to your Azure

Stack Hub instance, and tools from your hardware equipment manufacturer (OEM). The

OEM tool runs on the hardware lifecycle host (HLH) to make sure the new physical

computer matches the same firmware level as existing nodes.

The following flow diagram shows the general process to add a scale unit node:

Whether your OEM hardware vendor enacts the physical server rack placement and

updates the firmware varies based on your support contract.

Take into consideration the following limitations when adding a new node:

The operation to add another scale unit Node includes two distinct phases:

compute and storage.

During the compute expansion phase, your Azure Stack Hub will show a state of

Expanding. After the compute expansion completes, and the storage expansion is

running, the stamp will show a state of Configuring Storage. Let your Azure Stack

Overview

２ Warning

Azure Stack Hub requires that the configuration of all servers in the solution have

the same configuration, including for example CPU (model, cores), memory

quantity, NIC and link speeds, and storage devices. Azure Stack Hub does not

support a change in CPU models during hardware replacement or when adding a

scale unit node. A change in CPU, such as an upgrade, will require uniform CPUs in

each scale unit node and a redeployment of Azure Stack Hub.

Hub return to the Running state before adding another node. This means when

adding multiple nodes you will need to add a node and wait for the state to return

to Running before adding the next node.

The following steps are a high-level overview of how to add a node. Don't follow these

steps without first referring to your OEM-provided capacity expansion documentation.

1. Make sure the new node is configured with the BMC credentials that are already

configured within Azure Stack Hub. For instructions on updating the BMC

credentials in Azure Stack Hub, refer to Update the BMC credential.

2. Place the new physical server in the rack and cable it appropriately.

3. Enable physical switch ports and adjust access control lists (ACLs) if applicable.

4. Configure the correct IP address in the baseboard management controller (BMC)

and apply all BIOS settings per your OEM-provided documentation.

5. Apply the current firmware baseline to all components by using the tools that are

provided by the hardware manufacturer that run on the HLH.

） Important

The storage expansion phase can run up to multiple days before completion,

as spaces are rebalanced in a pool to disks with capacity. There isn't an impact

to running workloads on the system while another scale unit node is added.

２ Warning

Do not attempt any of the following operations while an add scale unit node

operation is already in progress:

Update Azure Stack Hub

Rotate certificates

Stop Azure Stack Hub

Repair scale unit node

Add another node (the previous add-node action failure is also considered

in progress)

Add scale unit nodes

6. Run the add node operation. You can use the Administrator portal or PowerShell to

add new nodes. The add node operation first adds the new scale unit node as

available compute capacity and then automatically extends the storage capacity.

The capacity expands automatically because Azure Stack Hub is a hyperconverged

system where compute and storage scale together.

a. Sign in to the Azure Stack Hub administrator portal as an Azure Stack Hub

operator.

b. Navigate to + Create a resource > Capacity > Scale Unit Node.

c. On the Add node pane, select the Region, and then select the Scale unit

that you want to add the node to. Also specify the BMC IP ADDRESS for the

scale unit node you're adding. You can only add one node at a time.

7. Verify whether the add node operation succeeded by checking the status, which

should be "running". Refer to the Status for the add node operation section that

follows for more details.

Administrator portal

Use the administrator portal or PowerShell to get the status of the add node operation.

Add node operations can take several hours to days to complete.

To monitor the addition of a new node, review the scale unit or scale unit node objects

in the administrator portal. To do so, go to Region management > Scale units. Next,

select the scale unit or scale unit node you want to review.

The status for scale unit and scale unit nodes can be retrieved using PowerShell as

follows:

PowerShell

To validate that the add node operation succeeded, check the Status of the Scale Unit.

For a scale unit:

Status Description

Running All nodes are actively participating in the scale unit.

Stopped The scale unit node is either down or unreachable.

Expanding One or more scale unit nodes are currently being added as compute

capacity.

Configuring

Storage

The compute capacity has been expanded and the storage configuration is

running.

Requires

Remediation

An error has been detected that requires one or more scale unit nodes to be

repaired.

For a scale unit node:

Monitor add node operations

Use the administrator portal

Use PowerShell

#Retrieve Status for the Scale Unit

Get-AzsScaleUnit|select name,state

#Retrieve Status for each Scale Unit Node

Get-AzsScaleUnitNode |Select Name, ScaleUnitNodeStatus

Status for the add node operation

Status Description

Running The node is actively participating in the scale unit.

Stopped The node is unavailable.

Adding The node is actively being added to the scale unit.

Repairing The node is actively being repaired.

Maintenance The node is paused, and no active user workload is running.

Requires Remediation An error has been detected that requires the node to be repaired.

The following are common issues seen when adding a node.

Scenario 1: The add scale unit node operation fails but one or more of the nodes are

listed with a status of Stopped.

Remediation: Use the regular operation to repair one or more nodes. Only a single

repair operation can be run at one time.

Scenario 2: One or more scale unit nodes have been added but the storage expansion

failed. In this scenario, the scale unit node object reports a status of Running but the

Configuring Storage task isn't started.

Remediation: Use the privileged endpoint to review the storage health by running

the following PowerShell cmdlet:

Azure PowerShell

Scenario 3: You received an alert that indicates the storage scale-out job failed.

Remediation: In this case, the storage configuration task has failed. This problem

requires you to contact support.

Add public IP addresses

Troubleshooting

Get-VirtualDisk -CimSession s-Cluster | Get-StorageJob

Next steps

Add public IP addresses

Article • 11/09/2022

In this article, we refer to external addresses as public IP addresses. In the context of

Azure Stack Hub, a public IP address is an IP address that's accessible from outside of

Azure Stack Hub. Whether that external network is public internet routable or is on an

intranet and uses private address space doesn't matter for the purposes of this article,

the steps are the same.

While you can set up multiple IP pools, you won't be able to select which pool is used to

allocate Public IP addresses. Azure Stack Hub treats all IP pools as one. IP addresses

from any additional pools are allocated only after the IP addresses in existing pool(s)

have been exhausted. When you create a network resource, you cannot pick a specific

Public IP for assignment, but once assigned it can be made static.

You can add public IP addresses to your Azure Stack Hub system at any time after the

initial deployment of the Azure Stack Hub system. The network size on this subnet for

the new Public IP Pool can range from a minimum of /26 (64 hosts) to a maximum of

/22 (1022 hosts). We recommend that you plan for a /24 network. Check out how to

View public IP address consumption to see what the current usage and public IP address

availability is on your Azure Stack Hub.

At a high level, the process of adding a new public IP address block to Azure Stack Hub

looks like this:

） Important

The steps in this article apply only to systems that were deployed using the partner

toolkit version 1809 or later. Systems that were deployed before version 1809

require the top-of-rack (TOR) switch access control lists (ACLs) to be updated to

PERMIT the new public VIP pool range. If you are running older switch

configurations, work with your OEM to either add the appropriate PERMIT ACLs for

the new public IP pool or reconfigure your switch using the latest partner toolkit to

prevent the new public IP addresses from being blocked.

Add a public IP address pool

The first thing you'll need to do is to obtain the address block you want to add to Azure

Stack Hub. Depending on where you obtain your address block from, consider what the

lead time is and manage this against the rate at which you're consuming public IP

addresses in Azure Stack Hub.

1. In a browser, go to your administrator portal dashboard. For this example, we'll use

https://adminportal.local.azurestack.external .

2. Sign in to the Azure Stack Hub administrator portal as a cloud operator.

3. On the default dashboard, find the Region management list and select the region

you want to manage. For this example, we use local.

4. Find the Resource providers tile and click on the network resource provider.

5. Click on the Public IP pools usage tile.

6. Click on the Add IP pool button.

7. Provide a name for the IP pool. The name you choose helps you easily identify the

IP pool. You can't use a special character like "/" in this field. It's a good practice to

make the name the same as the address range, but that isn't required.

8. Enter the address block you want to add in CIDR notation. For example:

192.168.203.0/24

9. When you provide a valid CIDR range in the Address range (CIDR block) field the

Start IP address, End IP address and Available IP addresses fields will automatically

populate. They're read-only and automatically generated so you can't change

these fields without modifying the value in the Address range field.

Obtain the address block from your provider

） Important

Azure Stack Hub will accept any address block that you provide if it's a valid

address block and doesn't overlap with an existing address range in Azure Stack

Hub. Please make sure you obtain a valid address block that's routable and nonoverlapping with the external network to which Azure Stack Hub is connected. After

you add the range to Azure Stack Hub, you cannot remove it without the assistance

of Microsoft Support. Only IP pools specified post deployment can be removed.

The IP pool range specified during deployment cannot be modified or removed; a

redeployment of the stamp is required if the original IP pool range needs to be

changed.

Add the IP address range to Azure Stack Hub

10. After you review the info on the blade and confirm that everything looks correct,

select Ok to commit the change and add the address range to Azure Stack Hub.

Review scale unit node actions.

Next steps

Scale unit node actions in Azure Stack

Hub

Article • 07/29/2022

This article describes how to view the status of a scale unit. You can view the unit's

nodes. You can run node actions like power on, power off, shut down, drain, resume,

and repair. Typically, you use these node actions during field replacement of parts, or to

help recover a node.

In the administrator portal, you can view the status of a scale unit and its associated

nodes.

To view the status of a scale unit:

1. On the Region management tile, select the region.

2. On the left, under Infrastructure resources, select Scale units.

3. In the results, select the scale unit.

4. On the left, under General, select Nodes.

View the following information:

The list of individual nodes.

Operational Status (see list below).

Power Status (running or stopped).

Server model.

IP address of the baseboard management controller (BMC).

Total number of cores.

Total amount of memory.

Node actions can also raise expected alerts in the administrator portal.

） Important

All node actions described in this article should target one node at a time.

View the node status

Status Description

Running The node is actively participating in the scale unit.

Stopped The node is unavailable.

Adding The node is actively being added to the scale unit.

Repairing The node is actively being repaired.

Maintenance The node is paused, and no active user workload is running.

Requires Remediation An error has been detected that requires the node to be repaired.

Azure Stack Hub may show the operational node status as Adding after an operation

like drain, resume, repair, shutdown or start was executed. This can happen when the

Fabric Resource Provider Role cache did not refresh after an operation.

Before applying the following steps ensure that no operation is currently in progress.

Update the endpoint to match your environment.

1. Open PowerShell and add your Azure Stack Hub environment. This requires

Azure Stack Hub PowerShell to be installed on your computer.

PowerShell

Node operational states

Azure Stack Hub shows Adding status after an operation

Az modules

Add-AzEnvironment -Name AzureStack -ARMEndpoint

https://adminmanagement.local.azurestack.external

Connect-AzAccount -Environment AzureStack

2. Run the following command to restart the Fabric Resource Provider Role.

PowerShell

3. Validate the operational status of the impacted scale unit node changed to

Running. You can use the Administrator portal or the following PowerShell

command:

PowerShell

4. If the node operational status is still shown as Adding continue to open a

support incident.

When you view information about a scale unit node, you can also perform node actions

like:

Start and stop (depending on current power status).

Disable and resume (depending on operations status).

Repair.

Shutdown.

The operational state of the node determines which options are available.

You need to install Azure Stack Hub PowerShell modules. These cmdlets are in the

Azs.Fabric.Admin module. To install or verify your installation of PowerShell for Azure

Stack Hub, see Install PowerShell for Azure Stack Hub.

The Stop action turns off the node. It's the same as pressing the power button. It

doesn't send a shutdown signal to the operating system. For planned stop operations,

always try the shutdown operation first.

This action is typically used when a node no longer responds to requests.

Restart-AzsInfrastructureRole -Name FabricResourceProvider

Get-AzsScaleUnitNode |ft name,scaleunitnodestatus,powerstate

Scale unit node actions

Stop

To run the stop action, open an elevated PowerShell prompt, and run the following

cmdlet:

PowerShell

In the unlikely case that the stop action doesn't work, retry the operation and if it fails a

second time use the BMC web interface instead.

For more information, see Stop-AzsScaleUnitNode.

The start action turns on the node. It's the same as if you press the power button.

To run the start action, open an elevated PowerShell prompt, and run the following

cmdlet:

PowerShell

In the unlikely case that the start action doesn't work, retry the operation. If it fails a

second time, use the BMC web interface instead.

For more information, see Start-AzsScaleUnitNode.

The drain action moves all active workloads to the remaining nodes in that particular

scale unit.

This action is typically used during field replacement of parts, like the replacement of an

entire node.

Stop-AzsScaleUnitNode -Location <RegionName> -Name <NodeName>

Start

Start-AzsScaleUnitNode -Location <RegionName> -Name <NodeName>

Drain

） Important

Make sure you use a drain operation on a node during a planned maintenance

window, where users have been notified. Under some conditions, active workloads

can experience interruptions.

To run the drain action, open an elevated PowerShell prompt, and run the following

cmdlet:

PowerShell

For more information, see Disable-AzsScaleUnitNode.

The resume action resumes a disabled node and marks it active for workload placement.

Earlier workloads that were running on the node don't fail back. (If you use a drain

operation on a node be sure to power off. When you power the node back on it's not

marked as active for workload placement. When ready, you must use the resume action

to mark the node as active.)

To run the resume action, open an elevated PowerShell prompt, and run the following

cmdlet:

PowerShell

For more information, see Enable-AzsScaleUnitNode.

Disable-AzsScaleUnitNode -Location <RegionName> -Name <NodeName>

Resume

Enable-AzsScaleUnitNode -Location <RegionName> -Name <NodeName>

Repair

Ｕ Caution

Firmware leveling is critical for the success of the operation described in this article.

Missing this step can lead to system instability, a decrease in performance, security

threats, or failure when Azure Stack Hub automation deploys the operating system.

Always consult your hardware partner's documentation when replacing hardware to

ensure the applied firmware matches the OEM Version displayed in the Azure Stack

Hub administrator portal.

For more information and links to partner documentation, see Replace a hardware

component.

Hardware

Partner

Hardware Region URL

Partner

Region URL

Cisco All Cisco Integrated System for Microsoft Azure Stack Hub Operations

Guide

Release Notes for Cisco Integrated System for Microsoft Azure Stack

Hub

Dell EMC All Cloud for Microsoft Azure Stack Hub 14G (account and login

required)

Cloud for Microsoft Azure Stack Hub 13G (account and login

required)

Fujitsu JAPAN Fujitsu managed service support desk (account and login

required)

EMEA Fujitsu support IT products and systems

Fujitsu MySupport (account and login required)

HPE All HPE ProLiant for Microsoft Azure Stack Hub

Lenovo All ThinkAgile SXM Best Recipes

The repair action repairs a node. Use it only for either of the following scenarios:

Full node replacement (with or without new data disks).

After hardware component failure and replacement (if advised in the field

replaceable unit [FRU] documentation).

When you run the repair action, you need to specify the BMC IP address.

To run the repair action, open an elevated PowerShell prompt, and run the following

cmdlet:

PowerShell

） Important

See your OEM hardware vendor's FRU documentation for exact steps when you

need to replace a node or individual hardware components. The FRU

documentation will specify whether you need to run the repair action after

replacing a hardware component.

The shutdown action first moves all active workloads to the remaining nodes in the

same scale unit. Then the action gracefully shuts down the scale unit node.

After you start a node that was shut down, you need to run the resume action. Earlier

workloads that were running on the node don't fail back.

If the shutdown operation fails, attempt the drain operation followed by the shutdown

operation.

To run the shutdown action, open an elevated PowerShell prompt, and run the following

cmdlet:

PowerShell

Install Azure Stack PowerShell

Learn about the Azure Stack Hub Fabric operator module

Monitor Add node operations

Repair-AzsScaleUnitNode -Location <RegionName> -Name <NodeName> -

BMCIPv4Address <BMCIPv4Address>

Shutdown

Stop-AzsScaleUnitNode -Location <RegionName> -Name <NodeName> -Shutdown

Next steps

Replace a scale unit node on an Azure

Stack Hub integrated system

Article • 07/29/2022

This article describes the general process to replace a physical computer (also referred

to as a scale unit node) on an Azure Stack Hub integrated system. Actual scale unit node

replacement steps will vary based on your original equipment manufacturer (OEM)

hardware vendor. See your vendor's field replaceable unit (FRU) documentation for

detailed steps that are specific to your system.

The following flow diagram shows the general FRU process to replace an entire scale

unit node.

\*This action may not be required based on the physical condition of the hardware.

Ｕ Caution

Firmware leveling is critical for the success of the operation described in this article.

Missing this step can lead to system instability, performance decrease, security

threads, or prevent Azure Stack Hub automation from deploying the operating

system. Always consult your hardware partner's documentation when replacing

hardware to ensure the applied firmware matches the OEM Version displayed in the

Azure Stack Hub administrator portal. For more information and links to partner

documentation, see Replace a hardware component.

７ Note

If a scale unit node is down, you'll receive the following critical alerts:

Node not connected to network controller

Node inaccessible for virtual machine placement

Scale unit node is offline

If you open the Scale unit node is offline alert, the alert description contains the scale

unit node that's inaccessible. You may also receive additional alerts in the OEM-specific

monitoring solution that's running on the hardware lifecycle host.

If the shutdown operation does fail, it's recommended to use the drain operation

followed by the stop operation. For more information, see Scale unit node actions

in Azure Stack Hub.

Review alert information

The following steps are provided as a high-level overview of the scale unit node

replacement process. See your OEM hardware vendor's FRU documentation for detailed

steps that are specific to your system. Don't follow these steps without referring to your

OEM-provided documentation.

1. Use the Shutdown action to gracefully shut down the scale unit node. This action

may not be required based on the physical condition of the hardware.

2. In the unlikely case the shutdown action fails, use the Drain action to put the scale

unit node into maintenance mode. This action may not be required based on the

physical condition of the hardware.

Scale unit node replacement process

７ Note

In any case, only one node can be disabled and powered off at the same time

without breaking the S2D (Storage Spaces Direct).

3. After the scale unit node is in maintenance mode, use the Stop action. This action

may not be required based on the physical condition of the hardware.

4. Replace the physical computer. Typically, this replacement is done by your OEM

hardware vendor.

5. Use the Repair action to add the new physical computer to the scale unit.

6. Use the privileged endpoint to check the status of virtual disk repair. With new

data drives, a full storage repair job can take multiple hours depending on system

load and consumed space.

7. After the repair action has finished, validate that all active alerts have been

automatically closed.

For information about replacing a physical disk while the system is powered on,

see Replace a disk.

For information about replacing a hardware component that requires the system

to be powered off, see Replace a hardware component.

７ Note

In the unlikely case that the Power off action doesn't work, use the baseboard

management controller (BMC) web interface instead.

Next steps

Replace a physical disk in Azure Stack

Hub

Article • 07/29/2022

This article describes the general process to replace a physical disk in Azure Stack Hub. If

a physical disk fails, you should replace it as soon as possible.

You can use this procedure for deployments that have hot-swappable disks.

Actual disk replacement steps will vary based on your original equipment manufacturer

(OEM) hardware vendor. See your vendor's field replaceable unit (FRU) documentation

for detailed steps that are specific to your system.

When a disk fails, you receive an alert that tells you that connectivity has been lost to a

physical disk.

If you open the alert, the alert description contains the scale unit node and the exact

physical slot location for the disk that you must replace. Azure Stack Hub further helps

you to identify the failed disk by using LED indicator capabilities.

７ Note

Replacing a physical data drive does not require the scale unit node to be put into

maintenance mode (drain) upfront. Also after the physical drive has been replaced

the scale unit node doesn't need to be repaired using the Azure Stack Hub

administrator portal. The following article has more information when a repair is

required Replace a hardware component on an Azure Stack Hub scale unit node.

Review disk alert information

Follow your OEM hardware vendor's FRU instructions for actual disk replacement.

To prevent the use of an unsupported disk in an integrated system, the system blocks

disks that aren't supported by your vendor. If you try to use an unsupported disk, a new

alert tells you a disk has been quarantined because of an unsupported model or

firmware.

After you replace the disk, Azure Stack Hub automatically discovers the new disk and

starts the virtual disk repair process.

After you replace the disk, you can monitor the virtual disk health status and repair job

progress by using Azure Stack Hub PowerShell.

1. Check that you have Azure Stack Hub PowerShell installed. For more information,

see Install PowerShell for Azure Stack Hub.

2. Connect to Azure Stack Hub with PowerShell as an operator. For more information,

see Connect to Azure Stack Hub with PowerShell as an operator.

3. Run the following cmdlets to verify the virtual disk health and repair status:

PowerShell

Replace the physical disk

７ Note

Replace disks for one scale unit node at a time. Wait for the virtual disk repair jobs

to complete before moving on to the next scale unit node.

Check the status of virtual disk repair using

Azure Stack Hub PowerShell

$scaleunit=Get-AzsScaleUnit

$StorageSubSystem=Get-AzsStorageSubSystem -ScaleUnit $scaleunit.Name

Get-AzsVolume -StorageSubSystem $StorageSubSystem.Name -ScaleUnit

$scaleunit.name | Select-Object VolumeLabel, OperationalStatus,

RepairStatus

4. Validate Azure Stack Hub system state. For instructions, see Validate Azure Stack

Hub system state.

5. Optionally, you can run the following command to verify the status of the replaced

physical disk.

PowerShell

After you replace the disk, you can monitor the virtual disk health status and repair job

progress by using the privileged endpoint. Follow these steps from any computer that

has network connectivity to the privileged endpoint.

1. Open a Windows PowerShell session and connect to the privileged endpoint.

PowerShell

$scaleunit=Get-AzsScaleUnit

$StorageSubSystem=Get-AzsStorageSubSystem -ScaleUnit $scaleunit.Name

Get-AzsDrive -StorageSubSystem $StorageSubSystem.Name -ScaleUnit

$scaleunit.name | Sort-Object StorageNode,MediaType,PhysicalLocation |

Format-Table Storagenode, Healthstatus, PhysicalLocation, Model,

MediaType, CapacityGB, CanPool, CannotPoolReason

Check the status of virtual disk repair using the

privileged endpoint

2. Run the following command to view virtual disk health:

PowerShell

3. Run the following command to view current storage job status:

PowerShell

4. Validate the Azure Stack Hub system state. For instructions, see Validate Azure

Stack Hub system state.

If the virtual disk repair job appears stuck, run the following command to restart the job:

PowerShell

$cred = Get-Credential

Enter-PSSession -ComputerName <IP\_address\_of\_ERCS>`

-ConfigurationName PrivilegedEndpoint -Credential $cred

Get-VirtualDisk -CimSession s-cluster

Get-VirtualDisk -CimSession s-cluster | Get-StorageJob

Troubleshoot virtual disk repair using the

privileged endpoint

Get-VirtualDisk -CimSession s-cluster | Repair-VirtualDisk

Replace a hardware component on an

Azure Stack Hub scale unit node

Article • 07/29/2022

This article describes the general process to replace hardware components that are non

hot-swappable. Actual replacement steps vary based on your original equipment

manufacturer (OEM) hardware vendor. See your vendor's field replaceable unit (FRU)

documentation for detailed steps that are specific to your Azure Stack Hub integrated

system.

Hardware

Partner

Region URL

Cisco All Cisco Integrated System for Microsoft Azure Stack Hub Operations

Guide

Release Notes for Cisco Integrated System for Microsoft Azure Stack

Hub

Ｕ Caution

Firmware leveling is critical for the success of the operation described in this article.

Missing this step can lead to system instability, performance decrease, security

threats, or prevent Azure Stack Hub automation from deploying the operating

system. Always consult your hardware partner's documentation when replacing

hardware to ensure the applied firmware matches the OEM Version displayed in the

Azure Stack Hub administrator portal.

２ Warning

Azure Stack Hub requires that the configuration of all servers in the solution have

the same configuration, including for example CPU (model, cores), memory

quantity, NIC and link speeds, and storage devices. Azure Stack Hub does not

support a change in CPU models during hardware replacement or when adding a

scale unit node. A change in CPU, such as an upgrade, will require uniform CPUs in

each scale unit node and a redeployment of Azure Stack Hub.

Hardware

Partner

Region URL

Dell EMC All Cloud for Microsoft Azure Stack Hub 14G (account and sign in

required)

Cloud for Microsoft Azure Stack Hub 13G (account and sign in

required)

Fujitsu JAPAN Fujitsu managed service support desk (account and sign in

required)

EMEA Fujitsu support IT products and systems

EU Fujitsu MySupport (account and sign in required)

HPE All HPE ProLiant for Microsoft Azure Stack Hub

Lenovo All ThinkAgile SXM Best Recipes

Wortmann OEM/firmware package

terra Azure Stack Hub documentation (including FRU)

Non hot-swappable components include the following items:

CPU (must be of the same type (model, cores)\*

Memory\*

Motherboard/baseboard management controller (BMC)/video card

Disk controller/host bus adapter (HBA)/backplane

Network adapter (NIC)

Graphics processing unit (GPU)

Operating system disk\*

Data drives (drives that don't support hot swap, for example PCI-e add-in cards)\*

\*These components may support hot swap, but can vary based on vendor

implementation. See your OEM vendor's FRU documentation for detailed steps.

The following flow diagram shows the general FRU process to replace a non hotswappable hardware component.

This action may not be required based on the physical condition of the hardware.

\*\* Whether your OEM hardware vendor does the component replacement and updates

the firmware could vary based on your support contract.

The Azure Stack Hub health and monitoring system tracks the health of network

adapters and data drives controlled by Storage Spaces Direct. It doesn't track other

hardware components. For all other hardware components, alerts are raised in the

vendor-specific hardware monitoring solution that runs on the hardware lifecycle host.

The following steps provide a high-level overview of the component replacement

process. Don't follow these steps without referring to your OEM-provided FRU

documentation.

1. Use the Shutdown action to gracefully shut down the scale unit node. This action

may not be required based on the physical condition of the hardware.

2. In an unlikely case the shutdown action does fail, use the Drain action to put the

scale unit node into maintenance mode. This action may not be required based on

the physical condition of the hardware.

3. After the scale unit node is in maintenance mode, use the Power off action. This

action may not be required based on the physical condition of the hardware.

Review alert information

Component replacement process

７ Note

In any case, only one node can be disabled and powered off at the same time

without breaking the S2D (Storage Spaces Direct).

4. Replace the damaged hardware component. Whether your OEM hardware vendor

does the component replacement could vary based on your support contract.

5. Update the firmware. Follow your vendor-specific firmware update process using

the hardware lifecycle host to make sure the replaced hardware component has

the approved firmware level applied. Whether your OEM hardware vendor does

this step could vary based on your support contract.

6. Use the Repair action to bring the scale unit node back into the scale unit.

7. Use the privileged endpoint to check the status of virtual disk repair. With new

data drives, a full storage repair job can take multiple hours depending on system

load and consumed space.

8. After the repair action has finished, validate that all active alerts have been

automatically closed.

For information about replacing a hot-swappable physical disk, see Replace a disk.

For information about replacing a physical node, see Replace a scale unit node.

７ Note

In the unlikely case that the power off action doesn't work, use the baseboard

management controller (BMC) web interface instead.

Next steps

Azure Stack Hub infrastructure security

controls

Article • 07/29/2022

Security considerations and compliance regulations are among the main drivers for

using hybrid clouds. Azure Stack Hub is designed for these scenarios. This article

explains the security controls in place for Azure Stack Hub.

Two security posture layers coexist in Azure Stack Hub. The first layer is the Azure Stack

Hub infrastructure, which includes the hardware components up to the Azure Resource

Manager. The first layer includes the administrator and the user portals. The second

layer consists of the workloads created, deployed, and managed by tenants. The second

layer includes items like virtual machines and App Services web sites.

The security posture for Azure Stack Hub is designed to defend against modern threats

and was built to meet the requirements from the major compliance standards. As a

result, the security posture of the Azure Stack Hub infrastructure is built on two pillars:

Assume Breach

Starting from the assumption that the system has already been breached, focus on

detecting and limiting the impact of breaches versus only trying to prevent attacks.

Hardened by Default

Since the infrastructure runs on well-defined hardware and software, Azure Stack

Hub enables, configures, and validates all the security features by default.

Because Azure Stack Hub is delivered as an integrated system, the security posture of

the Azure Stack Hub infrastructure is defined by Microsoft. Just like in Azure, tenants are

responsible for defining the security posture of their tenant workloads. This document

provides foundational knowledge on the security posture of the Azure Stack Hub

infrastructure.

All Azure Stack Hub infrastructure and tenant data are encrypted at rest using BitLocker.

This encryption protects against physical loss or theft of Azure Stack Hub storage

components. For more information, see data at rest encryption in Azure Stack Hub.

Security approach

Data at rest encryption

The Azure Stack Hub infrastructure components communicate using channels encrypted

with TLS 1.2. Encryption certificates are self-managed by the infrastructure.

All external infrastructure endpoints, like the REST endpoints or the Azure Stack Hub

portal, support TLS 1.2 for secure communications. Encryption certificates, either from a

third party or your enterprise Certificate Authority, must be provided for those

endpoints.

While self-signed certificates can be used for these external endpoints, Microsoft

strongly advises against using them. For more information on how to enforce TLS 1.2 on

the external endpoints of Azure Stack Hub, see Configure Azure Stack Hub security

controls.

Azure Stack Hub infrastructure uses a multitude of secrets, like passwords and

certificates, to function. Most of the passwords associated with the internal service

accounts are automatically rotated every 24 hours because they're group Managed

Service Accounts (gMSA), a type of domain account managed directly by the internal

domain controller.

Azure Stack Hub infrastructure uses 4096-bit RSA keys for all its internal certificates.

Same key-length certificates can also be used for the external endpoints. For more

information on secrets and certificate rotation, please refer to Rotate secrets in Azure

Stack Hub.

Azure Stack Hub makes use of the latest Windows Server security features. One of them

is Windows Defender Application Control (WDAC, formerly known as Code Integrity),

which provides executables filtering and ensures that only authorized code runs within

the Azure Stack Hub infrastructure.

Authorized code is signed by either Microsoft or the OEM partner. The signed

authorized code is included in the list of allowed software specified in a policy defined

by Microsoft. In other words, only software that has been approved to run in the Azure

Stack Hub infrastructure can be executed. Any attempt to execute unauthorized code is

blocked and an alert is generated. Azure Stack Hub enforces both User Mode Code

Integrity (UMCI) and Hypervisor Code Integrity (HVCI).

Data in transit encryption

Secret management

Windows Defender Application Control

The WDAC policy also prevents third-party agents or software from running in the Azure

Stack Hub infrastructure. For more information on WDAC, please refer to Windows

Defender Application Control and virtualization-based protection of code integrity.

Every component in Azure Stack Hub (both Hyper-V hosts and virtual machines) is

protected with Windows Defender Antivirus.

In connected scenarios, antivirus definition and engine updates are applied multiple

times a day. In disconnected scenarios, antimalware updates are applied as part of

monthly Azure Stack Hub updates. In case a more frequent update to the Windows

Defender's definitions is required in disconnected scenarios, Azure Stack Hub also

support importing Windows Defender updates. For more information, see update

Windows Defender Antivirus on Azure Stack Hub.

Azure Stack Hub enforces Secure Boot on all the Hyper-V hosts and infrastructure virtual

machines.

Administration in Azure Stack Hub is controlled through three entry points, each with a

specific purpose:

The administrator portal provides a point-and-click experience for daily

management operations.

Azure Resource Manager exposes all the management operations of the

administrator portal via a REST API, used by PowerShell and Azure CLI.

For specific low-level operations (for example, datacenter integration or support

scenarios), Azure Stack Hub exposes a PowerShell endpoint called privileged

endpoint. This endpoint exposes only an allowed set of cmdlets and it's heavily

audited.

Azure Stack Hub infrastructure comes with multiple layers of network Access Control List

(ACL). The ACLs prevent unauthorized access to the infrastructure components and limit

infrastructure communications to only the paths that are required for its functioning.

Antimalware

Secure Boot

Constrained administration model

Network controls

Network ACLs are enforced in three layers:

Layer 1: Top of Rack switches

Layer 2: Software Defined Network

Layer 3: Host and VM operating system firewalls

Azure Stack Hub has gone through a formal capability assessment by a third partyindependent auditing firm. As a result, documentation on how the Azure Stack Hub

infrastructure meets the applicable controls from several major compliance standards is

available. The documentation isn't a certification of Azure Stack Hub because the

standards include several personnel-related and process-related controls. Rather,

customers can use this documentation to jump-start their certification process.

The assessments include the following standards:

PCI-DSS addresses the payment card industry.

CSA Cloud Control Matrix is a comprehensive mapping across multiple

standards, including FedRAMP Moderate, ISO27001, HIPAA, HITRUST, ITAR, NIST

SP800-53, and others.

FedRAMP High for government customers.

The compliance documentation can be found on the Microsoft Service Trust Portal .

The compliance guides are a protected resource and require you to sign in with your

Azure cloud service credentials.

Configure Azure Stack Hub security controls

Learn how to rotate your secrets in Azure Stack Hub

PCI-DSS and the CSA-CCM documents for Azure Stack Hub

Regulatory compliance

Next steps

Configure Azure Stack Hub security

controls

Article • 07/29/2022

This article explains the security controls that can be changed in Azure Stack Hub and

highlights the tradeoffs where applicable.

Azure Stack Hub architecture is built on two security principle pillars: assume breach and

hardened by default. For more information on Azure Stack Hub security, see Azure Stack

Hub infrastructure security posture. While the default security posture of Azure Stack

Hub is production-ready, there are some deployment scenarios that require additional

hardening.

The Transport Layer Security (TLS) protocol is a widely adopted cryptographic protocol

to establish encrypted communication over the network. TLS has evolved over time and

multiple versions have been released. Azure Stack Hub infrastructure exclusively uses

TLS 1.2 for all its communications. For external interfaces, Azure Stack Hub currently

defaults to use TLS 1.2. However, for backwards compatibility, it also supports

negotiating down to TLS 1.1. and 1.0. When a TLS client requests to communicate over

TLS 1.1 or TLS 1.0, Azure Stack Hub honors the request by negotiating to a lower TLS

version. If the client requests TLS 1.2, Azure Stack Hub will establish a TLS connection

using TLS 1.2.

Since TLS 1.0 and 1.1 are incrementally being deprecated or banned by organizations

and compliance standards you can now configure the TLS policy in Azure Stack Hub. You

can enforce a TLS 1.2 only policy where any attempt of establishing a TLS session with a

version lower than 1.2 isn't permitted and is rejected.

Use the privileged endpoint (PEP) to view the TLS policy for all Azure Stack Hub

endpoints:

TLS version policy

） Important

Microsoft recommends using TLS 1.2 only policy for Azure Stack Hub production

environments.

Get TLS policy

PowerShell

Example output:

PowerShell

Use the privileged endpoint (PEP) to set the TLS policy for all Azure Stack Hub

endpoints:

PowerShell

Parameters for Set-TLSPolicy cmdlet:

Parameter Description Type Required

Version Allowed version(s) of TLS in Azure Stack Hub String yes

Use one of the following values to configure the permitted TLS versions for all Azure

Stack Hub endpoints:

Version

value

Description

TLS\_All Azure Stack Hub TLS endpoints support TLS 1.2, but down negotiation to TLS 1.1

and TLS 1.0 is allowed.

TLS\_1.2 Azure Stack Hub TLS endpoints support TLS 1.2 only.

Updating the TLS policy takes a few minutes to complete.

This example sets your TLS policy to enforce TLS 1.2 only.

PowerShell

Get-TLSPolicy

TLS\_1.2

Set TLS policy

Set-TLSPolicy -Version <String>

Enforce TLS 1.2 configuration example

Example output:

PowerShell

This example sets your TLS policy to allow all versions of TLS (1.2, 1.1, and 1.0).

PowerShell

Example output:

PowerShell

Set-TLSPolicy -Version TLS\_1.2

VERBOSE: Successfully setting enforce TLS 1.2 to True

VERBOSE: Invoking action plan to update GPOs

VERBOSE: Create Client for execution of action plan

VERBOSE: Start action plan

<...>

VERBOSE: Verifying TLS policy

VERBOSE: Get GPO TLS protocols registry 'enabled' values

VERBOSE: GPO TLS applied with the following preferences:

VERBOSE: TLS protocol SSL 2.0 enabled value: 0

VERBOSE: TLS protocol SSL 3.0 enabled value: 0

VERBOSE: TLS protocol TLS 1.0 enabled value: 0

VERBOSE: TLS protocol TLS 1.1 enabled value: 0

VERBOSE: TLS protocol TLS 1.2 enabled value: 1

VERBOSE: TLS 1.2 is enforced

Allow all versions of TLS (1.2, 1.1, and 1.0) configuration example

Set-TLSPolicy -Version TLS\_All

VERBOSE: Successfully setting enforce TLS 1.2 to False

VERBOSE: Invoking action plan to update GPOs

VERBOSE: Create Client for execution of action plan

VERBOSE: Start action plan

<...>

VERBOSE: Verifying TLS policy

VERBOSE: Get GPO TLS protocols registry 'enabled' values

VERBOSE: GPO TLS applied with the following preferences:

VERBOSE: TLS protocol SSL 2.0 enabled value: 0

VERBOSE: TLS protocol SSL 3.0 enabled value: 0

VERBOSE: TLS protocol TLS 1.0 enabled value: 1

VERBOSE: TLS protocol TLS 1.1 enabled value: 1

VERBOSE: TLS protocol TLS 1.2 enabled value: 1

VERBOSE: TLS 1.2 is not enforced

There are scenarios where it's useful to display a legal notice, upon login to a privileged

endpoint (PEP) session. The Set-AzSLegalNotice and Get-AzSLegalNotice cmdlets are

used to manage the caption and body of such legal notice text.

To set the legal notice caption and text, see the Set-AzSLegalNotice cmdlet. If the legal

notice caption and text have previously been set, you can review them by using the GetAzSLegalNotice cmdlet.

Learn about Azure Stack Hub infrastructure security posture.

Learn how to rotate your secrets in Azure Stack Hub.

Update Windows Defender Antivirus on Azure Stack Hub.

Legal notice for PEP sessions

Next steps

Overview of identity providers for Azure

Stack Hub

Article • 06/26/2023

Azure Stack Hub requires Azure Active Directory (Azure AD) or Active Directory

Federation Services (AD FS), backed by Active Directory as an identity provider. The

choice of a provider is a one-time decision that you make when you first deploy Azure

Stack Hub. The concepts and authorization details in this article can help you choose

between identity providers.

Your choice of either Azure AD or AD FS is determined by the mode in which you deploy

Azure Stack Hub:

When you deploy it in a connected mode, you can use either Azure AD or AD FS.

When you deploy it in a disconnected mode, without a connection to the internet,

only AD FS is supported.

For more information about your options, which depend on your Azure Stack Hub

environment, see the following articles:

Azure Stack Hub development kit: Identity considerations.

Azure Stack Hub integrated systems: Deployment planning decisions for Azure

Stack Hub integrated systems.

The next sections discuss common concepts about identity providers and their use in

Azure Stack Hub.

） Important

Azure AD Graph is being deprecated, and will be retired on June 30, 2022. For more

information, see this section.

Common concepts for identity providers

A directory is a container that holds information about users, applications, groups, and

service principals.

A directory tenant is an organization, such as Microsoft or your own company.

Azure AD supports multiple tenants, and it can support multiple organizations,

each in its own directory. If you use Azure AD and have multiple tenants, you can

grant apps and users from one tenant access to other tenants of that same

directory.

AD FS supports only a single tenant and, therefore, only a single organization.

User accounts (identities) are standard accounts that authenticate individuals by using a

user ID and password. Groups can include users or other groups.

How you create and manage users and groups depends on the identity solution you

use.

In Azure Stack Hub, user accounts:

Are created in the username@domain format. Although AD FS maps user accounts

to an Active Directory instance, AD FS doesn't support the use of the \<domain>\

<alias> format.

Can be set up to use multi-factor authentication.

Are restricted to the directory where they first register, which is their organization's

directory.

Can be imported from your on-premises directories. For more information, see

Integrate your on-premises directories with Azure Active Directory.

Directory tenants and organizations

Users and groups

When you sign in to your organization's user portal, you use the

https://portal.local.azurestack.external URL. When signing into the Azure Stack Hub

portal from domains other than the one used to register Azure Stack Hub, the domain

name used to register Azure Stack Hub must be appended to the portal url. For

example, if Azure Stack Hub has been registered with fabrikam.onmicrosoft.com and the

user account logging in is admin@contoso.com, the URL to use to log into the user

portal would be: https://portal.local.azurestack.external/fabrikam.onmicrosoft.com.

Guest users are user accounts from other directory tenants that have been granted

access to resources in your directory. To support guest users, you use Azure AD and

enable support for multi-tenancy. When support is enabled, you can invite guest users

to access resources in your directory tenant, which in turn enables their collaboration

with outside organizations.

To invite guest users, cloud operators and users can use Azure AD B2B collaboration.

Invited users get access to documents, resources, and apps from your directory, and you

maintain control over your own resources and data.

As a guest user, you can sign in to another organization's directory tenant. To do so, you

append that organization's directory name to the portal URL. For example, if you belong

to the Contoso organization and want to sign in to the Fabrikam directory, you use

https://portal.local.azurestack.external/fabrikam.onmicrosoft.com.

You can register apps to Azure AD or AD FS, and then offer the apps to users in your

organization.

Apps include:

Web apps: Examples include the Azure portal and Azure Resource Manager. They

support Web API calls.

Native client: Examples include Azure PowerShell, Visual Studio, and Azure CLI.

Apps can support two types of tenancy:

Single-tenant: Supports users and services only from the same directory where the

app is registered.

Guest users

Apps

７ Note

Multi-tenant: Supports use by users and services from both the directory where

the app is registered and additional tenant directories. With multi-tenant apps,

users of another tenant directory (another Azure AD tenant) can sign in to your

app.

For more information about multi-tenancy, see Enable multi-tenancy.

For more information about developing a multi-tenant app, see Multi-tenant apps.

When you register an app, you create two objects:

Application object: The global representation of the app across all tenants. This

relationship is one-to-one with the software app and exists only in the directory

where the app is first registered.

Service principal object: A credential that's created for an app in the directory

where the app is first registered. A service principal is also created in the directory

of each additional tenant where that app is used. This relationship can be one-tomany with the software app.

To learn more about app and service principal objects, see Application and service

principal objects in Azure Active Directory.

A service principal is a set of credentials for an app or service that grant access to

resources in Azure Stack Hub. The use of a service principal separates the app

permissions from the permissions of the user of the app.

A service principal is created in each tenant where the app is used. The service principal

establishes an identity for sign-in and access to resources (such as users) that are

secured by that tenant.

A single-tenant app has only one service principal, which is in the directory where

it's first created. This service principal is created and consents to being used during

registration of the app.

A multi-tenant web app or API has a service principal that's created in each tenant

where a user from that tenant consents to the use of the app.

Because AD FS supports only a single directory, apps you create in an AD FS

topology are, by design, single-tenant apps.

Service principals

Credentials for service principals can be either a key that's generated through the Azure

portal or a certificate. The use of a certificate is suited for automation because

certificates are considered more secure than keys.

To learn about service principals for Azure Stack Hub, see Create service principals.

Services in Azure Stack Hub that interact with the identity provider are registered as

apps with the identity provider. Like apps, registration enables a service to authenticate

with the identity system.

All Azure services use OpenID Connect protocols and JSON Web Tokens to establish

their identity. Because Azure AD and AD FS use protocols consistently, you can use the

Microsoft Authentication Library (MSAL) to obtain a security token to authenticate onpremises or to Azure (in a connected scenario). With MSAL, you can also use tools such

as Azure PowerShell and Azure CLI for cross-cloud and on-premises resource

management.

Identities for Azure Stack Hub include user accounts, groups, and service principals.

When you install Azure Stack Hub, several built-in apps and services automatically

register with your identity provider in the directory tenant. Some services that register

are used for administration. Other services are available for users. The default

registrations give core services identities that can interact both with each other and with

identities that you add later.

If you set up Azure AD with multi-tenancy, some apps propagate to the new directories.

７ Note

When you use AD FS with Azure Stack Hub, only the administrator can create

service principals. With AD FS, service principals require certificates and are created

through the privileged endpoint (PEP). For more information, see Use an app

identity to access resources.

Services

Identities and your identity system

Authentication and authorization

For apps and users, the architecture of Azure Stack Hub is described by four layers.

Interactions between each of these layers can use different types of authentication.

Layer Authentication between layers

Tools and

clients, such as

the

administrator

portal

To access or modify a resource in Azure Stack Hub, tools and clients use a JSON

Web Token to place a call to Azure Resource Manager.

Azure Resource Manager validates the JSON Web Token and peeks at the claims

in the issued token to estimate the level of authorization that user or service

principal has in Azure Stack Hub.

Azure

Resource

Manager and

its core

services

Azure Resource Manager communicates with resource providers to transfer

communication from users.

Transfers use direct imperative calls or declarative calls via Azure Resource

Manager templates.

Resource

providers

Calls passed to resource providers are secured with certificate-based

authentication.

Azure Resource Manager and the resource provider then stay in communication

through an API. For every call that's received from Azure Resource Manager, the

resource provider validates the call with that certificate.

Infrastructure

and business

logic

Resource providers communicate with business logic and infrastructure by using

an authentication mode of their choice. The default resource providers that ship

with Azure Stack Hub use Windows Authentication to secure this

communication.

Authentication by apps and users

To authenticate with the identity provider and receive a JSON Web Token, you must

have the following information:

1. URL for the identity system (Authority): The URL at which your identity provider

can be reached. For example, https://login.windows.net.

2. App ID URI for Azure Resource Manager: The unique identifier for Azure Resource

Manager that's registered with your identity provider. It's also unique to each

Azure Stack Hub installation.

3. Credentials: The credential you use to authenticate with the identity provider.

4. URL for Azure Resource Manager: The URL is the location of the Azure Resource

Manager service. For example, https://management.azure.com or

https://management.local.azurestack.external.

When a principal (a client, apps, or user) makes an authentication request to access a

resource, the request must include:

The principal's credentials.

The app ID URI of the resource that the principal wants to access.

The credentials are validated by the identity provider. The identity provider also

validates that the app ID URI is for a registered app, and that the principal has the

correct privileges to obtain a token for that resource. If the request is valid, a JSON Web

Token is granted.

The token must then pass in the header of a request to Azure Resource Manager. Azure

Resource Manager does the following, in no specific order:

Validates the issuer (iss) claim to confirm that the token is from the correct identity

provider.

Validates the audience (aud) claim to confirm that the token was issued to Azure

Resource Manager.

Authenticate to Azure Resource Manager

Validates that the JSON Web Token is signed with a certificate that's configured

through OpenID and known to Azure Resource Manager.

Review the issued at (iat) and expiration (exp) claims to confirm that the token is

active and can be accepted.

When all validations are complete, Azure Resource Manager uses the object id (oid) and

the groups claims to make a list of resources that the principal can access.

Role-Based Access Control (RBAC) in Azure Stack Hub is consistent with the

implementation in Microsoft Azure. You can manage access to resources by assigning

the appropriate RBAC role to users, groups, and apps. For information about how to use

RBAC with Azure Stack Hub, see the following articles:

Get started with Role-Based Access Control in the Azure portal.

Use Role-Based Access Control to manage access to your Azure subscription

resources.

Create custom roles for Azure Role-Based Access Control.

Manage Role-Based Access Control in Azure Stack Hub.

７ Note

After deployment, Azure Active Directory global administrator permission isn't

required. However, some operations may require the global admin credentials (for

example, a resource provider installer script or a new feature requiring a permission

to be granted). You can either temporarily re-instate the account's global admin

permissions or use a separate global admin account that's an owner of the default

provider subscription.

Use Role-Based Access Control

Details about using Azure PowerShell to authenticate with Azure Stack Hub can be

found at Configure the Azure Stack Hub user's PowerShell environment.

For information about using Azure PowerShell to authenticate with Azure Stack Hub, see

Install and configure Azure CLI for use with Azure Stack Hub.

Azure Policy helps to enforce organizational standards and to assess compliance atscale. Through its compliance dashboard, it provides an aggregated view to evaluate the

overall state of the environment, with the ability to drill down to per-resource, perpolicy granularity. It also helps to bring your resources to compliance through bulk

remediation for existing resources and automatic remediation for new resources.

Common use cases for Azure Policy include implementing governance for resource

consistency, regulatory compliance, security, cost, and management. Policy definitions

for these common use cases are already built in to your Azure environment to help you

get started.

Microsoft Azure has announced the deprecation of Azure AD Graph on June 30, 2020,

and its retirement date of June 30, 2023. Microsoft has informed customers via email

about this change. For more detailed information, see the Azure AD Graph Retirement

and Powershell Module Deprecation blog.

The following section describes how this deprecation affects Azure Stack Hub.

The Azure Stack Hub team is working closely with the Azure Graph team to ensure your

systems continue to work beyond June 30, 2023 if necessary, to ensure a smooth

transition. The most important action is to ensure you are compliant with the Azure

Stack Hub servicing policy. Customers will receive an alert in the administrator portal of

Authenticate with Azure PowerShell

Authenticate with Azure CLI

Azure Policy

７ Note

Azure Policy is currently not supported on Azure Stack Hub.

Azure AD Graph

Azure Stack Hub and will be required to update the home directory and all onboarded

guest directories.

The majority of the migration itself will be done by the integrated system update

experience; there will be a manual step required by customers to grant new permissions

to those applications, which will require global administrator permissions in each Azure

AD directory used with your Azure Stack Hub environments. After the update package

with these changes finishes installing, an alert is raised in the admin portal directing you

to complete this step using the multi-tenancy UI or PowerShell scripts. This is the same

operation you perform when onboarding additional directories or resource providers;

for more information, see Configure multi-tenancy in Azure Stack Hub.

If you use AD FS as your identity system with Azure Stack Hub, these Graph changes will

not impact your system directly. However, the latest versions of tools such as Azure CLI,

Azure PowerShell, etc., require the new Graph APIs, and they will not work. Ensure that

you only use the versions of these tools which are explicitly supported with your given

Azure Stack Hub build.

In addition to the alert in the admin portal, we will communicate changes via the update

release notes and will communicate which update package requires updating the home

directory and all onboarded guest directories.

Identity architecture

Datacenter integration - identity

Next steps

Identity architecture for Azure Stack

Hub

Article • 07/29/2022

When choosing an identity provider to use with Azure Stack Hub, you should

understand the important differences between the options of Azure Active Directory

(Azure AD) and Active Directory Federation Services (AD FS).

The identity provider that you choose can limit your options, including support for

multi-tenancy.

Capability or scenario Azure

AD

AD FS

Connected to the internet Yes Optional

Support for multi-tenancy Yes No

Offer items in the Marketplace Yes Yes (requires use of the offline Marketplace

Syndication tool)

Support for Active Directory Authentication

Library (ADAL)

Yes Yes

Support for tools such as Azure CLI, Visual

Studio, and PowerShell

Yes Yes

Create service principals through the Azure

portal

Yes No

Create service principals with certificates Yes Yes

Create service principals with secrets (keys) Yes Yes

Applications can use the Graph service Yes No

Applications can use identity provider for

sign-in

Yes Yes (requires apps to federate with onpremises AD FS instances)

Managed identities No No

Capabilities and limitations

Topologies

The following sections discuss the different identity topologies that you can use.

By default, when you install Azure Stack Hub and use Azure AD, Azure Stack Hub uses a

single-tenant topology.

A single-tenant topology is useful when:

All users are part of the same tenant.

A service provider hosts an Azure Stack Hub instance for an organization.

This topology features the following characteristics:

Azure Stack Hub registers all apps and services to the same Azure AD tenant

directory.

Azure Stack Hub authenticates only the users and apps from that directory,

including tokens.

Identities for administrators (cloud operators) and tenant users are in the same

directory tenant.

To enable a user from another directory to access this Azure Stack Hub

environment, you must invite the user as a guest to the tenant directory.

Azure AD: single-tenant topology

Azure AD: multi-tenant topology

Cloud operators can configure Azure Stack Hub to allow access to apps by tenants from

one or more organizations. Users access apps through the Azure Stack Hub user portal.

In this configuration, the administrator portal (used by the cloud operator) is limited to

users from a single directory.

A multi-tenant topology is useful when:

A service provider wants to allow users from multiple organizations to access

Azure Stack Hub.

This topology features the following characteristics:

Access to resources should be on a per-organization basis.

Users from one organization should be unable to grant access to resources to

users who are outside their organization.

Identities for administrators (cloud operators) can be in a separate directory tenant

from the identities for users. This separation provides account isolation at the

identity provider level.

The AD FS topology is required when either of the following conditions is true:

Azure Stack Hub doesn't connect to the internet.

Azure Stack Hub can connect to the internet, but you choose to use AD FS for your

identity provider.

AD FS

This topology features the following characteristics:

To support the use of this topology in production, you must integrate the built-in

Azure Stack Hub AD FS instance with an existing AD FS instance that's backed by

Active Directory, through a federation trust.

You can integrate the Graph service in Azure Stack Hub with your existing Active

Directory instance. You can also use the OData-based Graph API service that

supports APIs that are consistent with the Azure AD Graph API.

To interact with your Active Directory instance, the Graph API requires a user

credential with read-only permission to your Active Directory instance, and

accesses:

The built-in AD FS instance.

Your AD FS and Active Directory instances, which must be based on Windows

Server 2012 or later.

Between your Active Directory instance and the built-in AD FS instance,

interactions aren't restricted to OpenID Connect, and they can use any mutually

supported protocol.

User accounts are created and managed in your on-premises Active Directory

instance.

Service principals and registrations for apps are managed in the built-in Active

Directory instance.

Identity overview

Datacenter integration - identity

Next steps

Set access permissions using role-based

access control

Article • 07/29/2022

A user in Azure Stack Hub can be a reader, owner, or contributor for each instance of a

subscription, resource group, or service. For example, User A might have reader

permissions to Subscription One, but have owner permissions to Virtual Machine Seven.

Reader: User can view everything, but can't make any changes.

Contributor: User can manage everything except access to resources.

Owner: User can manage everything, including access to resources.

Custom: User has limited, specific access to resources.

For more information about creating a custom role, see Custom roles for Azure

resources.

1. Sign in with an account that has owner permissions to the resource you want to

manage.

2. In the blade for the resource, click the Access icon .

3. In the Users blade, click Roles.

4. In the Roles blade, click Add to add permissions for the user.

1. Sign in with an account that has owner permissions to the resource you want to

manage.

2. In the blade for the resource, click the Access icon .

3. In the Users blade, click Roles.

4. In the Roles blade, click Add to add permissions for the Universal Group Active

Directory Group.

Set access permissions for a user

Set access permissions for a universal group

７ Note

Applicable only to Active Directory Federated Services (AD FS).

Add an Azure Stack Hub tenant

Next steps

Add a new Azure Stack Hub user

account in Azure Active Directory (Azure

AD)

Article • 07/29/2022

Before you can test offers and plans and create resources, you'll need a user account for

the Azure Stack Hub user portal. You create a user account in your Azure AD tenant, by

using the Azure portal or PowerShell.

You must have an Azure subscription to use the Azure portal.

1. Sign in to the Azure portal .

2. Using the Directory + Subscription filter icon in the upper right, switch to the

Azure AD directory tenant you're using for Azure Stack Hub.

3. Using the search bar at the top, search for and select the Azure Active Directory

service.

4. In the left pane, select Users.

5. On the Users page, select + New user.

6. On the New user page, select Create user then fill in the required info:

Create user account using the Azure portal



User name (required): The identifier used for sign in. For example,

mary@contoso.com. The domain part of the user name must use either the

initial default domain name, <yourdomainname>.onmicrosoft.com, or a

custom domain name, such as contoso.com. For more info on how to create

a custom domain name, see How to add a custom domain name to Azure

AD.



Name (required): The first and last name of the new user. For example, Mary

Parker.

Show Password: Select the checkbox and copy the autogenerated password

provided in Initial password. You'll need this password for the initial sign-in

process.

Groups and roles: Make sure the User directory role is selected.

Settings and Job info: Optionally, you can add more info about the user. You

can also add user info later. For more details, see How to add or change user

profile information.

7. Select Create. You should see a "Successfully created user" notification in the

upper right.

8. Sign out and sign in to the Azure portal again, with the new account using the

password you saved. Change the password when prompted.

9. Sign in to the Azure Stack Hub user portal with the new account to see the user

portal.

If you don't have an Azure subscription, you can't use the Azure portal to add a tenant

user account. In this case, you can use the Azure AD Module for Windows PowerShell

instead.

1. Install the Microsoft Azure AD Module for Windows PowerShell with these steps:

Open an elevated Windows PowerShell command prompt (run Windows

PowerShell as admin).

Run the Install-Module AzureAD command.

If you're prompted to install the NuGet provider, select Y and Enter.

If you're prompted to install the module from PSGallery, select Y and Enter.

2. Run the following cmdlets to sign in and create the user account:

If your directory doesn't require multi-factor authentication, use this

sequence to authenticate:

PowerShell

Create a user account using PowerShell

# Wait for the prompt, then sign in using your Azure AD

credentials

$aadcred = get-credential

Connect-AzureAD -credential $aadcred

If your directory requires multi-factor authentication, use this sequence to

authenticate:

PowerShell

Now that you've authenticated, complete the sequence by adding the new

user:

PowerShell

3. Sign in to the Azure portal with the new user account. Change the password

when prompted.

4. Sign in to the Azure Stack Hub user portal with the new account to see the user

portal.

Learn how to create and test a subscription by subscribing to an offer

Add Azure Stack Hub users in AD FS

# Wait for the prompt, then sign in using your Azure AD

credentials and MFA code

Connect-AzureAD -Confirm

# Create the new user account (be sure to replace all

<placeholder> values first)

$passwordProfile = New-Object -TypeName

Microsoft.Open.AzureAD.Model.PasswordProfile

$passwordProfile.Password = "<Password>"

New-AzureADUser -DisplayName "<UserName>" -PasswordProfile

$passwordProfile -UserPrincipalName "<username>@<yourdomainname>"

-AccountEnabled $true -MailNickName "<MailNickName>"

Next steps

Add a new Azure Stack Hub user

account in Active Directory Federation

Services (AD FS)

Article • 07/29/2022

You can use the Active Directory Users and Computers snap-in to add additional users

to an Azure Stack Hub environment, using AD FS as its identity provider.

1. Sign in to a computer with an account that provides access to the Windows

Administrative Tools and open a new Microsoft Management Console (MMC).

2. Select File > Add or remove snap-in.

3. Select Active Directory Users and Computers > directory-domain > Users.

4. Select Action > New > User.

5. In New Object - User, provide user details. Select Next.

6. Provide and confirm a password.

7. Select Next to complete the values. Select Finish to create the user.

Create an app identity to access Azure Stack Hub resources

Add Windows Server Active Directory users

 Tip

Replace directory-domain with the domain that matches your directory.

Next steps

Give an app access to Azure Stack Hub

resources

Article • 03/09/2023

An application that deploys or configures resources through Azure Resource Manager must be

represented by its own identity, known as a security principal. Just as a user is represented by a user

principal, an app is represented by a service principal.

The identity can also be used to delegate only the necessary permissions to the user or app. For

example, a configuration management app might use Azure Resource Manager to inventory Azure

resources. The app would get registered in the directory, then added to the "reader" role at the

appropriate scope, limiting the app to read-only access.

Like a user, an app must present credentials during authentication, which requires two elements:

An Application ID, sometimes referred to as a Client ID. A GUID that uniquely identifies the

app's registration in your Active Directory tenant.

A secret. You can either generate a client secret string (similar to a password), or specify an

X509 certificate thumbprint (which uses its public key).

Running an app under its own identity is preferable to running it under the user's identity for the

following reasons:

Stronger credentials - an app can sign in using an X509 certificate, instead of a textual shared

secret/password.

More restrictive permissions can be assigned to an app. Typically, these permissions are

restricted to only what the app needs to do, known as the principle of least privilege.

Credentials and permissions don't change as frequently for an app as user credentials. For

example, when the user's responsibilities change, password requirements dictate a change, or

when a user leaves the company.

You start by creating a new app registration in your directory, which creates an associated service

principal object to represent the app's identity within the directory. The registration process varies

depending on the directory you chose for your Azure Stack Hub instance:

Azure Active Directory (Azure AD): Azure AD is a multi-tenant, cloud-based, directory and

identity management service. You can use Azure AD with a connected Azure Stack Hub

instance. The examples presented later will use the Azure portal for Azure AD app registration.

Active Directory Federation Services (AD FS): AD FS provides simplified, secured identity

federation, and web single sign-on (SSO) capabilities. You can use AD FS with both connected

and disconnected Azure Stack Hub instances. The examples presented later will use Azure

Stack Hub PowerShell for AD FS app registration.

After registering the app you learn how to assign it to a role, limiting its resource access.

Overview

If you deployed Azure Stack Hub with Azure AD as your identity management service, you create

and manage identities for apps just like you do for Azure. This section shows you how to perform

the steps using the Azure portal. Review Permissions required for registering an app before

beginning, to make sure you have sufficient permissions to register an app.

In this section, you register your app in your Azure AD tenant using the Azure portal. In following

example, you specify a client secret credential, but the portal also supports X509 certificate-based

credentials.

1. Sign in to the Azure portal using your Azure account.

2. Select Azure Active Directory > App registrations > New registration.

3. Provide a name for the app.

4. Select the appropriate Supported account types.

5. Under Redirect URI, select Web as the app type, and (optionally) specify a redirect URI if your

app requires it.

6. After setting the values, select Register. The app registration is created and the Overview

page displays.

7. Copy the Application ID for use in your app code. This value is also referred to as the Client

ID.

8. To generate a client secret, select the Certificates & secrets page. Select New client secret.

9. Provide a description for the secret, and an expires duration.

10. When done, select Add.

11. The value of the secret displays. Copy and save this value in another location, because you

can't retrieve it later. You provide the secret with the Application ID in your client app for signin.

Proceed to Assign a role to learn how to establish role-based access control for the app's identity.

Manage an Azure AD app

Create an app registration that uses a client secret credential

Additional Azure AD app management articles

See the following Azure articles for more details on managing Azure AD apps:

More details on registering an Azure AD app, including how to create an app registration that

uses a certificate credential.

How to Remove an app registration.

How to Restore or remove a recently deleted app registration.

If you deployed Azure Stack Hub with AD FS as your identity management service, you must use

PowerShell to manage your app's identity. The following examples demonstrate both an X509

certificate and a client secret credential.

The scripts must be run in an elevated ("Run as administrator") PowerShell console, which opens

another session to a VM that hosts a privileged endpoint for your Azure Stack Hub instance. Once

the privileged endpoint session has been established, additional cmdlets are used to create and

manage the app registration. For more information about the privileged endpoint, see Using the

privileged endpoint in Azure Stack Hub.

When creating a certificate credential, the following requirements must be met:

For production, the certificate must be issued from either an internal Certificate Authority or a

Public Certificate Authority. When using a public authority, you must include the authority in

the base operating system image as part of the Microsoft Trusted Root Authority Program. For

the full list, see List of Participants - Microsoft Trusted Root Program. An example of creating a

"self-signed" test certificate will also be shown later during Update a certificate credential.

The cryptographic provider must be specified as a Microsoft legacy Cryptographic Service

Provider (CSP) key provider.

The certificate format must be in PFX file, as both the public and private keys are required.

Windows servers use .pfx files that contain the public key file (TLS/SSL certificate file) and the

associated private key file.

Your Azure Stack Hub infrastructure must have network access to the certificate authority's

Certificate Revocation List (CRL) location published in the certificate. This CRL must be an

HTTP endpoint.

Once you have a certificate, use the PowerShell script below to register your app and sign in using

the app's identity. Substitute your own values for the following placeholders:

Placeholder Description Example

Manage an AD FS app

Create an app registration that uses a certificate credential

Placeholder Description Example

<PepVM> The name

of the

privileged

endpoint

VM on your

Azure Stack

Hub

instance.

"AzS-ERCS01"

<YourCertificateLocation> The location

of your

X509

certificate in

the local

certificate

store.

"Cert:\CurrentUser\My\AB5A8A3533CC7AA2025BF05120117E06DE407B34"

<YourAppName> A

descriptive

name for

the new

app

registration.

"My management tool"

1. Open an elevated Windows PowerShell session, and run the following script.

PowerShell

Az modules

# Sign in to PowerShell interactively, using credentials that have access to

the VM running the Privileged Endpoint (typically <domain>\cloudadmin)

$Creds = Get-Credential

# Create a PSSession to the Privileged Endpoint VM

$Session = New-PSSession -ComputerName "<PepVm>" -ConfigurationName

PrivilegedEndpoint -Credential $Creds -SessionOption (New-PSSessionOption -

Culture en-US -UICulture en-US)

# To use a managed certificate from the certificate store, use the Get-Item

cmdlet.

# To use a certificate file, use Get-Certificate for a .cer file, or GetPfxCertificate for a .pfx file.

# To use a test certificate, use the New-SelfSignedCertificate cmdlet

# See https://learn.microsoft.com/powershell/module/pki/newselfsignedcertificate for usage details, including using the -Provider

parameter

# $Cert = New-SelfSignedCertificate -CertStoreLocation

"cert:\CurrentUser\My" -Subject "CN=<YourAppName>" -KeySpec KeyExchange

$Cert = Get-Item "<YourCertificateLocation>"

# Use the privileged endpoint to create the new app registration

$SpObject = Invoke-Command -Session $Session -ScriptBlock {New-

2. After the script finishes, it displays the app registration info. The ClientID and

Thumbprint are authenticated, and later authorized for access to resources managed by

Azure Resource Manager.

shell

Keep your PowerShell console session open, as you use it with the ApplicationIdentifier

value in the next section.

Now that you registered the application, this section will show you how to:

1. Create a new self-signed X509 certificate for testing.

2. Update the application's credentials, by updating its Thumbprint property to match the new

certificate.

GraphApplication -Name "<YourAppName>" -ClientCertificates $using:cert}

$AzureStackInfo = Invoke-Command -Session $Session -ScriptBlock {GetAzureStackStampInformation}

$Session | Remove-PSSession

# Using the stamp info for your Azure Stack Hub instance, populate the

following variables:

# - Az endpoint used for Azure Resource Manager operations

# - Audience for acquiring an OAuth token used to access Graph API

# - GUID of the directory tenant

$ArmEndpoint = $AzureStackInfo.TenantExternalEndpoints.TenantResourceManager

$GraphAudience = "https://graph." + $AzureStackInfo.ExternalDomainFQDN + "/"

$TenantID = $AzureStackInfo.AADTenantID

# Register and set an Az environment that targets your Azure Stack Hub

instance

Add-AzEnvironment -Name "AzureStackUser" -ArmEndpoint $ArmEndpoint

# Sign in using the new service principal

$SpSignin = Connect-AzAccount -Environment "AzureStackUser" `

-ServicePrincipal `

-CertificateThumbprint $SpObject.Thumbprint `

-ApplicationId $SpObject.ClientId `

-TenantId $TenantID

# Output the service principal details

$SpObject

ApplicationIdentifier : S-1-5-21-1512385356-3796245103-1243299919-1356

ClientId : 3c87e710-9f91-420b-b009-31fa9e430145

Thumbprint : 30202C11BE6864437B64CE36C8D988442082A0F1

ApplicationName : Azurestack-MyApp-c30febe7-1311-4fd8-9077-3d869db28342

ClientSecret :

PSComputerName : azs-ercs01

RunspaceId : a78c76bb-8cae-4db4-a45a-c1420613e01b

Update a certificate credential

Update the certificate credential using PowerShell, substituting your own values for the following

placeholders:

Placeholder Description Example

<PepVM> The name

of the

privileged

endpoint

VM on your

Azure Stack

Hub

instance.

"AzS-ERCS01"

<YourAppName> A

descriptive

name for

the new

app

registration.

"My management tool"

<YourCertificateLocation> The location

of your

X509

certificate in

the local

certificate

store.

"Cert:\CurrentUser\My\AB5A8A3533CC7AA2025BF05120117E06DE407B34"

<AppIdentifier> The

identifier

assigned to

the

application

registration.

"S-1-5-21-1512385356-3796245103-1243299919-1356"

1. Using your elevated Windows PowerShell session, run the following cmdlets:

PowerShell

# Create a PSSession to the PrivilegedEndpoint VM

$Session = New-PSSession -ComputerName "<PepVM>" -ConfigurationName

PrivilegedEndpoint -Credential $Creds -SessionOption (New-PSSessionOption -

Culture en-US -UICulture en-US)

# Create a self-signed certificate for testing purposes, using the NewSelfSignedCertificate cmdlet

# See https://learn.microsoft.com/powershell/module/pki/new-selfsignedcertificate

for usage details, including using the -Provider parameter

$NewCert = New-SelfSignedCertificate -CertStoreLocation "cert:\CurrentUser\My" -

Subject "CN=<YourAppName>" -KeySpec KeyExchange

# In production, use Get-Item to retrieve a managed certificate from the

certificate store.

# Alteratively, use Get-Certificate for a .cer file, or Get-PfxCertificate for a

.pfx file.

# $Cert = Get-Item "<YourCertificateLocation>"

2. After the script finishes, it displays the updated app registration info, including the thumbprint

value for the new self-signed certificate.

Shell

Now you create another app registration, but this time specify a client secret credential. Unlike a

certificate credential, the directory has the ability to generate a client secret credential. Instead of

specifying the client secret, you use the -GenerateClientSecret switch to request that it be

generated. Substitute your own values for the following placeholders:

Placeholder Description Example

<PepVM> The name of the privileged endpoint VM on your Azure Stack Hub

instance.

"AzS-ERCS01"

<YourAppName> A descriptive name for the new app registration. "My management

tool"

1. Open an elevated Windows PowerShell session, and run the following cmdlets:

# Use the privileged endpoint to update the certificate thumbprint, used by

<AppIdentifier>

$SpObject = Invoke-Command -Session $Session -ScriptBlock {Set-GraphApplication -

ApplicationIdentifier "<AppIdentifier>" -ClientCertificates $using:NewCert}

$Session | Remove-PSSession

# Output the updated service principal details

$SpObject

ApplicationIdentifier : S-1-5-21-1512385356-3796245103-1243299919-1356

ClientId :

Thumbprint : AF22EE716909041055A01FE6C6F5C5CDE78948E9

ApplicationName : Azurestack-MyApp-c30febe7-1311-4fd8-9077-3d869db28342

ClientSecret :

PSComputerName : azs-ercs01

RunspaceId : a580f894-8f9b-40ee-aa10-77d4d142b4e5

Create an app registration that uses a client secret credential

２ Warning

Using a client secret is less secure than using an X509 certificate credential. Not only is the

authentication mechanism less secure, but it also typically requires embedding the secret in

the client app source code. As such, for production apps, you're strongly encouraged to use a

certificate credential.

Az modules

PowerShell

2. After the script finishes, it displays the app registration info. The ClientID and

ClientSecret are authenticated, and later authorized for access to resources managed by

Azure Resource Manager.

shell

# Sign in to PowerShell interactively, using credentials that have access to

the VM running the Privileged Endpoint (typically <domain>\cloudadmin)

$Creds = Get-Credential

# Create a PSSession to the Privileged Endpoint VM

$Session = New-PSSession -ComputerName "<PepVM>" -ConfigurationName

PrivilegedEndpoint -Credential $Creds -SessionOption (New-PSSessionOption -

Culture en-US -UICulture en-US)

# Use the privileged endpoint to create the new app registration

$SpObject = Invoke-Command -Session $Session -ScriptBlock {NewGraphApplication -Name "<YourAppName>" -GenerateClientSecret}

$AzureStackInfo = Invoke-Command -Session $Session -ScriptBlock {GetAzureStackStampInformation}

$Session | Remove-PSSession

# Using the stamp info for your Azure Stack Hub instance, populate the

following variables:

# - Az endpoint used for Azure Resource Manager operations

# - Audience for acquiring an OAuth token used to access Graph API

# - GUID of the directory tenant

$ArmEndpoint = $AzureStackInfo.TenantExternalEndpoints.TenantResourceManager

$GraphAudience = "https://graph." + $AzureStackInfo.ExternalDomainFQDN + "/"

$TenantID = $AzureStackInfo.AADTenantID

# Register and set an Az environment that targets your Azure Stack Hub

instance

Add-AzEnvironment -Name "AzureStackUser" -ArmEndpoint $ArmEndpoint

# Sign in using the new service principal

$securePassword = $SpObject.ClientSecret | ConvertTo-SecureString -

AsPlainText -Force

$credential = New-Object -TypeName System.Management.Automation.PSCredential

-ArgumentList $SpObject.ClientId, $securePassword

$SpSignin = Connect-AzAccount -Environment "AzureStackUser" -ServicePrincipal

-Credential $credential -TenantId $TenantID

# Output the service principal details

$SpObject

ApplicationIdentifier : S-1-5-21-1634563105-1224503876-2692824315-2623

ClientId : 8e0ffd12-26c8-4178-a74b-f26bd28db601

Thumbprint :

ApplicationName : Azurestack-YourApp-6967581b-497e-4f5a-87b5-

0c8d01a9f146

ClientSecret : 6RUWLRoBw3EebBLgaWGiowCkoko5\_j\_ujIPjA8dS

PSComputerName : azs-ercs01

RunspaceId : 286daaa1-c9a6-4176-a1a8-03f543f90998

Keep your PowerShell console session open, as you use it with the ApplicationIdentifier

value in the next section.

Update the client secret credential using PowerShell, using the ResetClientSecret parameter, which

immediately changes the client secret. Substitute your own values for the following placeholders:

Placeholder Description Example

<PepVM> The name of the privileged endpoint VM on your

Azure Stack Hub instance.

"AzS-ERCS01"

<AppIdentifier> The identifier assigned to the application

registration.

"S-1-5-21-1634563105-1224503876-

2692824315-2623"

1. Using your elevated Windows PowerShell session, run the following cmdlets:

PowerShell

2. After the script finishes, it displays the updated app registration info, including the newly

generated client secret.

shell

Now you'll see how to remove an app registration from your directory using PowerShell.

Update a client secret credential

# Create a PSSession to the PrivilegedEndpoint VM

$Session = New-PSSession -ComputerName "<PepVM>" -ConfigurationName

PrivilegedEndpoint -Credential $Creds -SessionOption (New-PSSessionOption -

Culture en-US -UICulture en-US)

# Use the privileged endpoint to update the client secret, used by

<AppIdentifier>

$SpObject = Invoke-Command -Session $Session -ScriptBlock {Set-GraphApplication -

ApplicationIdentifier "<AppIdentifier>" -ResetClientSecret}

$Session | Remove-PSSession

# Output the updated service principal details

$SpObject

ApplicationIdentifier : S-1-5-21-1634563105-1224503876-2692824315-2623

ClientId : 8e0ffd12-26c8-4178-a74b-f26bd28db601

Thumbprint :

ApplicationName : Azurestack-YourApp-6967581b-497e-4f5a-87b5-0c8d01a9f146

ClientSecret : MKUNzeL6PwmlhWdHB59c25WDDZlJ1A6IWzwgv\_Kn

PSComputerName : azs-ercs01

RunspaceId : 6ed9f903-f1be-44e3-9fef-e7e0e3f48564

Remove an app registration

Substitute your own values for the following placeholders:

Placeholder Description Example

<PepVM> The name of the privileged endpoint VM on your

Azure Stack Hub instance.

"AzS-ERCS01"

<AppIdentifier> The identifier assigned to the application

registration.

"S-1-5-21-1634563105-1224503876-

2692824315-2623"

PowerShell

There will be no output returned from calling the Remove-GraphApplication cmdlet on the

privileged endpoint, but you'll see verbatim confirmation output to the console during execution of

the cmdlet:

shell

Access to Azure resources by users and apps is authorized through Role-Based Access Control

(RBAC). To allow an app to access resources in your subscription, you must assign its service

principal to a role for a specific resource. First decide which role represents the right permissions for

the app. To learn about the available roles, see Built-in roles for Azure resources.

The type of resource you choose also establishes the access scope for the app. You can set the

access scope at the subscription, resource group, or resource level. Permissions are inherited to

# Sign in to PowerShell interactively, using credentials that have access to the VM

running the Privileged Endpoint (typically <domain>\cloudadmin)

$Creds = Get-Credential

# Create a PSSession to the PrivilegedEndpoint VM

$Session = New-PSSession -ComputerName "<PepVM>" -ConfigurationName PrivilegedEndpoint

-Credential $Creds -SessionOption (New-PSSessionOption -Culture en-US -UICulture enUS)

# OPTIONAL: Use the privileged endpoint to get a list of applications registered in AD

FS

$AppList = Invoke-Command -Session $Session -ScriptBlock {Get-GraphApplication}

# Use the privileged endpoint to remove application <AppIdentifier>

Invoke-Command -Session $Session -ScriptBlock {Remove-GraphApplication -

ApplicationIdentifier "<AppIdentifier>"}

VERBOSE: Deleting graph application with identifier S-1-5-21-1634563105-1224503876-

2692824315-2623.

VERBOSE: Remove-GraphApplication : BEGIN on AZS-ADFS01 on ADFSGraphEndpoint

VERBOSE: Application with identifier S-1-5-21-1634563105-1224503876-2692824315-2623

was deleted.

VERBOSE: Remove-GraphApplication : END on AZS-ADFS01 under ADFSGraphEndpoint

configuration

Assign a role

lower levels of scope. For example, adding an app to the "Reader" role for a resource group, means

it can read the resource group and any resources it contains.

1. Sign in to the appropriate portal, based on the directory you specified during Azure Stack Hub

installation (the Azure portal for Azure AD, or the Azure Stack Hub user portal for AD FS, for

example). In this example, we show a user signed in to the Azure Stack Hub user portal.

2. Navigate to the resource you wish to allow the app to access. In this example, assign the app

to a role at the subscription scope, by selecting Subscriptions, then a specific subscription.

You could instead select a resource group, or a specific resource like a virtual machine.

3. Select the Access Control (IAM) page, which is universal across all resources that support

RBAC.

4. Select + Add

5. Under Role, pick the role you wish to assign to the app.

6. Under Select, search for your app using a full or partial Application Name. During registration,

the Application Name is generated as Azurestack-<YourAppName>-<GUID>. For example, if

you used an application name of App2, and GUID 2bbe67d8-3fdb-4b62-87cf-cc41dd4344ff was

assigned during creation, the full name would be Azurestack-App2-2bbe67d8-3fdb-4b62-87cfcc41dd4344ff. You can search for either the exact string, or a portion, like Azurestack or

Azurestack-App2.

7. Once you find the app, select it and it will show under Selected members.

７ Note

To add role assignments for a given resource, your user account must belong to a role

that declares the Microsoft.Authorization/roleAssignments/write permission. For

example, either the Owner or User Access Administrator built-in roles.

8. Select Save to finish assigning the role.

9. When finished, the app will show in the list of principals assigned for the current scope, for the

given role.

Now that you've given your app an identity and authorized it for resource access, you can enable

your script or code to sign in and securely access Azure Stack Hub resources.

Manage user permissions

Azure Active Directory Documentation

Active Directory Federation Services





Next steps

Configure multi-tenancy in Azure Stack

Hub

Article • 07/29/2022

You can configure Azure Stack Hub to support sign-ins from users that reside in other

Azure Active Directory (Azure AD) directories, allowing them to use services in Azure

Stack Hub. These directories have a "guest" relationship with your Azure Stack Hub

directory, and are considered guest Azure AD tenants.

For example, consider this scenario:

You're the service administrator of contoso.onmicrosoft.com, the home Azure AD

tenant that provides identity and access management services to Azure Stack Hub.

Mary is the directory administrator of adatum.onmicrosoft.com, the guest Azure

AD tenant where guest users are located.

Mary's company (Adatum) uses IaaS and PaaS services from your company.

Adatum wants to allow users from the guest directory (adatum.onmicrosoft.com)

to sign in and use Azure Stack Hub resources secured by contoso.onmicrosoft.com.

This guide provides the steps required, in the context of this scenario, to enable or

disable multi-tenancy in Azure Stack Hub for a guest directory tenant. You and Mary

accomplish this process by registering or unregistering the guest directory tenant, which

enables or disables Azure Stack Hub sign-ins and service consumption by Adatum users.

If you're a Cloud Solution Provider (CSP), you have other ways to configure and manage

a multi-tenant Azure Stack Hub.

To register a guest directory for multi-tenancy, you need to configure both the home

Azure Stack Hub directory and the guest directory.

The first step is to make your Azure Stack Hub system aware of the guest directory. In

this example, the directory from Mary's company, Adatum, is called

adatum.onmicrosoft.com.

1. Sign in to the Azure Stack Hub administrator portal and go to All services -

Directories.

Register a guest directory

Configure Azure Stack Hub directory

2. Select Add to start the onboarding process. Enter the guest directory name

"adatum.onmicrosoft.com", and then select Add.

3. The guest directory appears in the list view, with a status of unregistered.

4. Only Mary has the credentials to authenticate to the guest directory, so you must

send her the link to complete the registration. Select the adatum.onmicrosoft.com

checkbox, and then select Register.

5. A new browser tab opens. Select Copy link at the bottom of the page, and provide

it to Mary.

6. If you have the credentials for the guest directory, you can complete the

registration yourself by selecting Sign in.









Mary received the email with the link to register the directory. She opens the link in a

browser and confirms the Azure Active Directory and the Azure Resource Manager

endpoint of your Azure Stack Hub system.

1. Mary signs in by using her global admin credentials for adatum.onmicrosoft.com.

2. Mary reviews the status for the directory and sees it isn't registered.



Configure guest directory

７ Note

Make sure pop-up blockers are disabled before signing in.



3. Mary selects Register to start the process.

4. After the registration process is finished, Mary can review all the applications that

were created in the directory, and check their status.



７ Note

Required objects for Visual Studio Code might not be able to be created, and

must use PowerShell.

5. Mary has successfully completed the registration process and can now direct

Adatum users with @adatum.onmicrosoft.com accounts to sign in by visiting the

Azure Stack Hub user portal. For multinode systems, the user portal URL is

formatted as https://portal.<region>.<FQDN> . For an ASDK deployment, the URL

is https://portal.local.azurestack.external .

Mary must also direct any foreign principals (users in the Adatum directory without the

suffix of adatum.onmicrosoft.com) to sign in using https://<user-portalurl>/adatum.onmicrosoft.com . If they don't specify the /adatum.onmicrosoft.com

directory tenant in the URL, they're sent to their default directory and receive an error

that says their administrator hasn't consented.

） Important

It can take up to one hour for the Azure Stack operator to see the directory status

updated in the admin portal.

Unregister a guest directory

If you no longer want to allow sign-ins to Azure Stack Hub services from a guest

directory tenant, you can unregister the directory. Again, both the home Azure Stack

Hub directory and guest directory need to be configured:

Mary no longer uses services on Azure Stack Hub and must remove the objects. She

opens the URL again that she received via email to unregister the directory. Before

starting this process, Mary removes all the resources from the Azure Stack Hub

subscription.

1. Mary signs in by using her global admin credentials for adatum.onmicrosoft.com.

2. Mary sees the status of the directory.

Configure guest directory

７ Note

Make sure pop-up blockers are disabled before signing in.



3. Mary selects Unregister to start the action.

4. When the process has finished, the status is shown as Not registered:

Mary has successfully unregistered the directory adatum.onmicrosoft.com.

As an Azure Stack Hub operator, you can remove the guest directory at any point, even

if Mary has not previously unregistered the directory.

1. Sign in to the Azure Stack Hub administrator portal and go to All services -

Directories.

2. Select the adatum.onmicrosoft.com directory checkbox, and then select Remove.



７ Note

It can take up to one hour to show the directory as not registered in the Azure

Stack admin portal.

Configure Azure Stack Hub directory



3. Confirm the delete action by typing yes and selecting Remove.

You have successfully removed the directory.

Azure Stack Hub updates can introduce support for new tools or services that might

require an update of the home or guest directory.

As an Azure Stack Hub operator, you get an alert in the admin portal that informs you

about a required directory update. You can also determine whether an update is

required for home or guest directories by viewing the directories pane in the admin

portal. Each directory listing shows the type of directory. The type can be a home or

guest directory, and its status is shown.

When an Azure Stack Hub directory update is required, a status of Update Required is

shown. For example:





Managing required updates

Update the Azure Stack Hub directories



To update the directory, select the Directory name checkbox, and then select Update.

An Azure Stack Hub operator should also inform the guest directory owner that they

need to update their directory by using the URL shared for registration. The operator

can resend the URL, but it doesn't change.

Mary, the owner of the guest directory, opens the URL that she received via email when

she registered the directory:

1. Mary signs in by using her global admin credentials for adatum.onmicrosoft.com.

Make sure pop-up blockers are disabled before signing in.

2. Mary sees the status of the directory saying an update is required.

3. The Update action is available for Mary to update the guest directory. It can take

up to one hour to show the directory as registered in the Azure Stack admin portal.

An Azure Stack Hub operator can view the subscriptions associated with a directory. In

addition, each directory has an action to manage the directory directly in the Azure

portal. To manage, the target directory must have manage permissions in the Azure

portal.

Manage delegated providers

Azure Stack Hub key concepts

Manage usage and billing for Azure Stack Hub as a Cloud Solution Provider

Add tenant for usage and billing to Azure Stack Hub

Update the guest directory



Additional capabilities

Next steps

Data at rest encryption in Azure Stack

Hub

Article • 07/29/2022

Azure Stack Hub protects user and infrastructure data at the storage subsystem level

using encryption at rest. By default, Azure Stack Hub's storage subsystem is encrypted

using BitLocker. Systems deployed before release 2002 use BitLocker with 128-bit AES

encryption; systems deployed starting with 2002, or newer, use BitLocker with AES-256

bit encryption. BitLocker keys are persisted in an internal secret store.

Data at rest encryption is a common requirement for many of the major compliance

standards (for example, PCI-DSS, FedRAMP, HIPAA). Azure Stack Hub enables you to

meet those requirements with no extra work or configurations required. For more

information on how Azure Stack Hub helps you meet compliance standards, see the

Microsoft Service Trust Portal .

Azure Stack Hub BitLocker keys for data at rest are internally managed. You aren't

required to provide them for regular operations or during system startup. However,

support scenarios may require BitLocker recovery keys to bring the system online.

Retrieving the BitLocker recovery keys requires access to the privileged endpoint (PEP).

From a PEP session, run the Get-AzsRecoveryKeys cmdlet.

７ Note

Data at rest encryption protects your data against being accessed by someone who

physically stole one or more hard drives. Data at rest encryption doesn't protect

against data being intercepted over the network (data in transit), data currently

being used (data in memory), or, more in general, data being exfiltrated while the

system is up and running.

Retrieving BitLocker recovery keys

２ Warning

Retrieve your BitLocker recovery keys and store them in a secure location outside of

Azure Stack Hub. Not having the recovery keys during certain support scenarios

may result in data loss and require a system restore from a backup image.

PowerShell

Parameters for Get-AzsRecoveryKeys cmdlet:

Parameter Description Type Required

raw Returns data mapping between recovery key, computer

name, and password id(s) of each encrypted volume.

Switch No, but

recommended

In extreme circumstances, a BitLocker unlock request could fail resulting in a specific

volume to not boot. Depending on the availability of some of the components of the

architecture, this failure could result in downtime and potential data loss if you don't

have your BitLocker recovery keys.

If you suspect your system is experiencing issues with BitLocker, such as Azure Stack

Hub failing to start, contact support. Support requires your BitLocker recovery keys. The

majority of the BitLocker related issues can be resolved with a FRU operation for that

specific VM/host/volume. For the other cases, a manual unlocking procedure using

BitLocker recovery keys can be done. If BitLocker recovery keys aren't available, the only

option is to restore from a backup image. Depending on when the last backup was

done, you may experience data loss.

Learn more about Azure Stack Hub security.

For more information on how BitLocker protects CSVs, see protecting cluster

shared volumes and storage area networks with BitLocker.

##This cmdlet retrieves the recovery keys for all the volumes that are

encrypted with BitLocker.

Get-AzsRecoveryKeys -raw

Troubleshoot issues

２ Warning

Retrieve your BitLocker recovery keys and store them in a secure location outside of

Azure Stack Hub. Not having the recovery keys during certain support scenarios

may result in data loss and require a system restore from a backup image.

Next steps

Rotate secrets in Azure Stack Hub

Article • 10/28/2022

This article provides guidance for performing secret rotation, to help maintain secure

communication with Azure Stack Hub infrastructure resources and services.

Azure Stack Hub uses secrets to maintain secure communication with infrastructure

resources and services. To maintain the integrity of the Azure Stack Hub infrastructure,

operators need the ability to rotate secrets at frequencies that are consistent with their

organization's security requirements.

When secrets are nearing expiration, the following alerts are generated in the

administrator portal. Completing secret rotation will resolve these alerts:

Pending service account password expiration

Pending internal certificate expiration

Pending external certificate expiration

For more information on alert monitoring and remediation, see Monitor health and

alerts in Azure Stack Hub.

1. It's highly recommended that you're running a supported version of Azure Stack

Hub and that you apply the latest available hotfix for the Azure Stack Hub version

your instance is running. For example, if you're running 2008, make sure you've

installed the latest hotfix available for 2008.

Overview

２ Warning

There are 2 phases of alerts triggered in the administrator portal prior to expiration:

90 days before expiration a warning alert is generated.

30 days before expiration a critical alert is generated.

It's critical that you complete secret rotation if you receive these notifications.

Failure to do so can cause the loss of workloads and possible Azure Stack Hub

redeployment at your own expense!

Prerequisites

2. Notify your users of planned maintenance operations. Schedule normal

maintenance windows, as much as possible, during non-business hours.

Maintenance operations may affect both user workloads and portal operations.

3. Generate certificate signing requests for Azure Stack Hub.

4. Prepare Azure Stack Hub PKI certificates.

5. During rotation of secrets, operators may notice alerts open and automatically

close. This behavior is expected and the alerts can be ignored. Operators can verify

the validity of these alerts using the Test-AzureStack PowerShell cmdlet. For

operators, using System Center Operations Manager to monitor Azure Stack Hub

systems, placing a system in maintenance mode will prevent these alerts from

reaching their ITSM systems. However, alerts will continue to come if the Azure

Stack Hub system becomes unreachable.

This section covers rotation of certificates used to secure external-facing services. These

certificates are provided by the Azure Stack Hub Operator, for the following services:

Administrator portal

Public portal

Rotate external secrets

） Important

External secret rotation for:

Non-certificate secrets such as secure keys and strings must be done

manually by the administrator. This includes user and administrator account

passwords, and network switch passwords.

Value-add resource provider (RP) secrets is covered under separate guidance:

App Service on Azure Stack Hub

Event Hubs on Azure Stack Hub

MySQL on Azure Stack Hub

SQL on Azure Stack Hub

Baseboard management controller (BMC) credentials is a manual process,

covered later in this article.

Azure Container Registry external certificates is a manual process, covered

later in this article.

Administrator Azure Resource Manager

Global Azure Resource Manager

Administrator Key Vault

Key Vault

Admin Extension Host

ACS (including blob, table, and queue storage)

ADFS

Graph

Container Registry

Applicable when using Active Directory Federated Services (ADFS).

Applicable when using Azure Container Registry (ACR).

Prior to rotation of external secrets:

1. Run the Test-AzureStack PowerShell cmdlet using the -group

SecretRotationReadiness parameter, to confirm all test outputs are healthy before

rotating secrets.

2. Prepare a new set of replacement external certificates:

The new set must match the certificate specifications outlined in the Azure

Stack Hub PKI certificate requirements.

Generate a certificate signing request (CSR) to submit to your Certificate

Authority (CA). Use the steps outlined in Generate certificate signing requests

and prepare them for use in your Azure Stack Hub environment using the

steps in Prepare PKI certificates. Azure Stack Hub supports secret rotation for

external certificates from a new Certificate Authority (CA) in the following

contexts:

Rotate from

CA

Rotate to

CA

Azure Stack Hub version support

Self-Signed Enterprise 1903 & later

Self-Signed SelfSigned

Not Supported

Self-Signed Public 1803 & later

1

1

2

1

2

Preparation

\*

Rotate from

CA

Rotate to

CA

Azure Stack Hub version support

Enterprise Enterprise 1803 & later; 1803-1903 if SAME enterprise CA as used

at deployment

Enterprise SelfSigned

Not Supported

Enterprise Public 1803 & later

Public Enterprise 1903 & later

Public SelfSigned

Not Supported

Public Public 1803 & later

Part of the Windows Trusted Root Program.

Be sure to validate the certificates you prepare with the steps outlined in

Validate PKI Certificates

Make sure there are no special characters in the password, like for example

$ , \* , # , @ , or )`.

Make sure the PFX encryption is TripleDES-SHA1. If you run into an issue, see

Fix common issues with Azure Stack Hub PKI certificates.

3. Store a backup to the certificates used for rotation in a secure backup location. If

your rotation runs and then fails, replace the certificates in the fileshare with the

backup copies before you rerun the rotation. Keep backup copies in the secure

backup location.

4. Create a fileshare you can access from the ERCS VMs. The fileshare must be

readable and writable for the CloudAdmin identity.

5. Open a PowerShell ISE console from a computer where you have access to the

fileshare. Navigate to your fileshare, where you create directories to place your

external certificates.

6. Create a folder in the file share named Certificates . Inside the certificates folder,

create a subfolder named AAD or ADFS , depending on the identity provider your

Hub uses. For example, .\Certificates\AAD or .\Certificates\ADFS. No other folders

besides the certificates folder and the identity provider subfolder should be

created here.

\*

\*

\*

\* \*

\*

7. Copy the new set of replacement external certificates created in step #2, to the

.\Certificates\<IdentityProvider> folder created in step #6. As mentioned above,

your identity provider subfolder must either be AAD or ADFS . Please ensure that the

subject alternative names (SANs) of your replacement external certificates follow

the cert.<regionName>.<externalFQDN> format specified in Azure Stack Hub public

key infrastructure (PKI) certificate requirements.

Here's an example of a folder structure for the Azure AD Identity Provider:

PowerShell

<ShareName>

│

└───Certificates

└───AAD

├───ACSBlob

│ <CertName>.pfx

│

├───ACSQueue

│ <CertName>.pfx

│

├───ACSTable

│ <CertName>.pfx

│

├───Admin Extension Host

│ <CertName>.pfx

│

├───Admin Portal

│ <CertName>.pfx

│

├───ARM Admin

│ <CertName>.pfx

│

├───ARM Public

│ <CertName>.pfx

│

├───Container Registry\*

│ <CertName>.pfx

│

├───KeyVault

│ <CertName>.pfx

│

├───KeyVaultInternal

│ <CertName>.pfx

│

├───Public Extension Host

│ <CertName>.pfx

│

└───Public Portal

<CertName>.pfx

Applicable when using Azure Container Registry (ACR) for AAD and ADFS.

Complete the following steps to rotate external secrets:

1. Use the following PowerShell script to rotate the secrets. The script requires access

to a Privileged EndPoint (PEP) session. The PEP is accessed through a remote

PowerShell session on the virtual machine (VM) that hosts the PEP. If you're using

an integrated system, there are three instances of the PEP, each running inside a

VM (Prefix-ERCS01, Prefix-ERCS02, or Prefix-ERCS03) on different hosts. The script

performs the following steps:

Creates a PowerShell Session with the Privileged endpoint using the

CloudAdmin account, and stores the session as a variable. This variable is

used as a parameter in the next step.

Runs Invoke-Command, passing the PEP session variable as the -Session

parameter.

Runs Start-SecretRotation in the PEP session, using the following

parameters. For more information, see the Start-SecretRotation reference:

Parameter

Variable Description

-PfxFilesPath $CertSharePath The network path to your certificates root

folder as discussed in step #6 of the

Preparation section, for example \\

<IPAddress>\<ShareName>\Certificates .

-

PathAccessCredential

$CertShareCreds The PSCredential object for credentials to

the share.

-

CertificatePassword

$CertPassword A secure string of the password used for

all of the pfx certificate files created.

PowerShell

\*

７ Note

If you are rotating external Container Registry certificates you must manually create

a Container Registry subfolder in the identity provider subfolder. Additionally, you

must store the corresponding .pfx certificate within this manually created subfolder.

Rotation

2. External secret rotation takes approximately one hour. After successful completion,

your console will display a ActionPlanInstanceID ... CurrentStatus: Completed

message, followed by Action plan finished with status: 'Completed' . Remove

your certificates from the share created in the Preparation section and store them

in their secure backup location.

3. Optionally, to confirm that all external certificates were rotated, run the TestAzureStack validation tool using the following script:

PowerShell

# Create a PEP session

winrm s winrm/config/client '@{TrustedHosts= "<IP\_address\_of\_ERCS>"}'

$PEPCreds = Get-Credential

$PEPSession = New-PSSession -ComputerName <IP\_address\_of\_ERCS\_Machine>

-Credential $PEPCreds -ConfigurationName "PrivilegedEndpoint" -

SessionOption (New-PSSessionOption -Culture en-US -UICulture en-US)

# Run secret rotation

$CertPassword = ConvertTo-SecureString '<Cert\_Password>' -AsPlainText -

Force

$CertShareCreds = Get-Credential

$CertSharePath = "<Network\_Path\_Of\_CertShare>"

Invoke-Command -Session $PEPsession -ScriptBlock {

param($CertSharePath, $CertPassword, $CertShareCreds )

Start-SecretRotation -PfxFilesPath $CertSharePath -

PathAccessCredential $CertShareCreds -CertificatePassword $CertPassword

} -ArgumentList ($CertSharePath, $CertPassword, $CertShareCreds)

Remove-PSSession -Session $PEPSession

７ Note

If secret rotation fails, follow the instructions in the error message and re-run

Start-SecretRotation with the -ReRun parameter.

PowerShell

Contact support if you experience repeated secret rotation failures.

Start-SecretRotation -ReRun

Test-AzureStack -Include AzsExternalCertificates -DetailedResults -

debug

Internal secrets include certificates, passwords, secure strings, and keys used by the

Azure Stack Hub infrastructure, without intervention of the Azure Stack Hub Operator.

Internal secret rotation is only required if you suspect one has been compromised, or

you've received an expiration alert.

Complete the following steps to rotate internal secrets:

1. Run the following PowerShell script. Notice for internal secret rotation, the "Run

Secret Rotation" section uses only the -Internal parameter to the StartSecretRotation cmdlet:

PowerShell

2. After successful completion, your console will display a ActionPlanInstanceID ...

CurrentStatus: Completed message, followed by Action plan finished with

status: 'Completed' .

Rotate internal secrets

# Create a PEP Session

winrm s winrm/config/client '@{TrustedHosts= "<IP\_address\_of\_ERCS>"}'

$PEPCreds = Get-Credential

$PEPSession = New-PSSession -ComputerName <IP\_address\_of\_ERCS\_Machine>

-Credential $PEPCreds -ConfigurationName "PrivilegedEndpoint" -

SessionOption (New-PSSessionOption -Culture en-US -UICulture en-US)

# Run Secret Rotation

Invoke-Command -Session $PEPSession -ScriptBlock {

Start-SecretRotation -Internal

}

Remove-PSSession -Session $PEPSession

７ Note

If secret rotation fails, follow the instructions in the error message and rerun

Start-SecretRotation with the -Internal and -ReRun parameters.

PowerShell

Contact support if you experience repeated secret rotation failures.

Start-SecretRotation -Internal -ReRun

The Azure Stack Hub root certificate is provisioned during deployment with an

expiration of five years. Starting with 2108, internal secret rotation also rotates the root

certificate. The standard secret expiration alert identifies the expiry of the root certificate

and generates alerts at both 90 (warning) and 30 (critical) days.

To rotate the root certificate, you must update your system to 2108 and perform internal

secret rotation.

The following code snippet uses the Privileged Endpoint to list the expiration date of the

root certificate:

PowerShell

The baseboard management controller monitors the physical state of your servers. Refer

to your original equipment manufacturer (OEM) hardware vendor for instructions to

update the user account name and password of the BMC.

1. It's no longer required that you first update the BMC credentials on the Azure

Stack Hub physical servers by following your OEM instructions. The user name and

password for each BMC in your environment must be the same, and can't exceed

16 characters.

Rotate Azure Stack Hub root certificate

$pep = New-PSSession -ComputerName <ip address> -ConfigurationName

PrivilegedEndpoint -Credential $cred -SessionOption (New-PSSessionOption -

Culture en-US -UICulture en-US)

$stampInfo = Invoke-Command -Session $pep -ScriptBlock { GetAzureStackStampInformation }

$rootCert = $stampInfo.RootCACertificates| Sort-Object -Property NotAfter |

Select-Object -Last 1

"The Azure Stack Hub Root Certificate expires on {0}" -f

$rootCert.NotAfter.ToString("D") | Write-Host -ForegroundColor Cyan

Update the BMC credential

７ Note

Your OEM may provide additional management apps. Updating the user name or

password for other management apps has no effect on the BMC user name or

password.

2. Open a privileged endpoint in Azure Stack Hub sessions. For instructions, see Using

the privileged endpoint in Azure Stack Hub.

3. After opening a privileged endpoint session, run one of the PowerShell scripts

below, which use Invoke-Command to run Set-BmcCredential. If you use the

optional -BypassBMCUpdate parameter with Set-BMCCredential, credentials in the

BMC aren't updated. Only the Azure Stack Hub internal datastore is updated. Pass

your privileged endpoint session variable as a parameter.

Here's an example PowerShell script that will prompt for user name and password:

PowerShell

You can also encode the user name and password in variables, which may be less

secure:

PowerShell

# Interactive Version

$PEPIp = "<Privileged Endpoint IP or Name>" # You can also use the

machine name instead of IP here.

$PEPCreds = Get-Credential "<Domain>\CloudAdmin" -Message "PEP

Credentials"

$NewBmcPwd = Read-Host -Prompt "Enter New BMC password" -AsSecureString

$NewBmcUser = Read-Host -Prompt "Enter New BMC user name"

$PEPSession = New-PSSession -ComputerName $PEPIp -Credential $PEPCreds

-ConfigurationName "PrivilegedEndpoint" -SessionOption (NewPSSessionOption -Culture en-US -UICulture en-US)

Invoke-Command -Session $PEPSession -ScriptBlock {

# Parameter BmcPassword is mandatory, while the BmcUser parameter

is optional.

Set-BmcCredential -BmcPassword $using:NewBmcPwd -BmcUser

$using:NewBmcUser

}

Remove-PSSession -Session $PEPSession

# Static Version

$PEPIp = "<Privileged Endpoint IP or Name>" # You can also use the

machine name instead of IP here.

$PEPUser = "<Privileged Endpoint user for example Domain\CloudAdmin>"

$PEPPwd = ConvertTo-SecureString '<Privileged Endpoint Password>' -

AsPlainText -Force

$PEPCreds = New-Object System.Management.Automation.PSCredential

($PEPUser, $PEPPwd)

$NewBmcPwd = ConvertTo-SecureString '<New BMC Password>' -AsPlainText -

Force

$NewBmcUser = "<New BMC User name>"

Start-SecretRotation cmdlet rotates the infrastructure secrets of an Azure Stack Hub

system. This cmdlet can only be executed against the Azure Stack Hub privileged

endpoint, by using an Invoke-Command script block passing the PEP session in the -

Session parameter. By default, it rotates only the certificates of all external network

infrastructure endpoints.

Parameter Type Required Position Default Description

PfxFilesPath String False Named None The fileshare path to the

\Certificates root folder

containing all external

network endpoint

certificates. Only required

when rotating external

secrets. Path must end with

\Certificates folder, for

example \\<IPAddress>\

<ShareName>\Certificates.

CertificatePassword SecureString False Named None The password for all

certificates provided in the

-PfXFilesPath. Required

value if PfxFilesPath is

provided when external

secrets are rotated.

Internal String False Named None Internal flag must be used

anytime an Azure Stack

Hub operator wishes to

rotate internal

infrastructure secrets.

$PEPSession = New-PSSession -ComputerName $PEPIp -Credential $PEPCreds

-ConfigurationName "PrivilegedEndpoint" -SessionOption (NewPSSessionOption -Culture en-US -UICulture en-US)

Invoke-Command -Session $PEPSession -ScriptBlock {

# Parameter BmcPassword is mandatory, while the BmcUser parameter

is optional.

Set-BmcCredential -BmcPassword $using:NewBmcPwd -BmcUser

$using:NewBmcUser

}

Remove-PSSession -Session $PEPSession

Reference: Start-SecretRotation cmdlet

Parameter Type Required Position Default Description

PathAccessCredential PSCredential False Named None The PowerShell credential

for the fileshare of the

\Certificates directory

containing all external

network endpoint

certificates. Only required

when rotating external

secrets.

ReRun SwitchParameter False Named None Must be used anytime

secret rotation is

reattempted after a failed

attempt.

PowerShell

PowerShell

PowerShell

PowerShell

Syntax

For external secret rotation

Start-SecretRotation [-PfxFilesPath <string>] [-PathAccessCredential

<PSCredential>] [-CertificatePassword <SecureString>]

For internal secret rotation

Start-SecretRotation [-Internal]

For external secret rotation rerun

Start-SecretRotation [-ReRun]

For internal secret rotation rerun

Start-SecretRotation [-ReRun] [-Internal]

This command must be run via your Azure Stack Hub environment's privileged endpoint.

PowerShell

This command rotates all of the infrastructure secrets exposed to the Azure Stack Hub

internal network.

PowerShell

This command rotates the TLS certificates used for Azure Stack Hub's external network

infrastructure endpoints.

Learn more about Azure Stack Hub security

Examples

Rotate only internal infrastructure secrets

PS C:\> Start-SecretRotation -Internal

Rotate only external infrastructure secrets

# Create a PEP Session

winrm s winrm/config/client '@{TrustedHosts= "<IP\_address\_of\_ERCS>"}'

$PEPCreds = Get-Credential

$PEPSession = New-PSSession -ComputerName <IP\_address\_of\_ERCS> -Credential

$PEPCreds -ConfigurationName "PrivilegedEndpoint" -SessionOption (NewPSSessionOption -Culture en-US -UICulture en-US)

# Create Credentials for the fileshare

$CertPassword = ConvertTo-SecureString '<CertPasswordHere>' -AsPlainText -

Force

$CertShareCreds = Get-Credential

$CertSharePath = "<NetworkPathOfCertShare>"

# Run Secret Rotation

Invoke-Command -Session $PEPsession -ScriptBlock {

param($CertSharePath, $CertPassword, $CertShareCreds )

Start-SecretRotation -PfxFilesPath $CertSharePath -PathAccessCredential

$CertShareCreds -CertificatePassword $CertPassword

} -ArgumentList ($CertSharePath, $CertPassword, $CertShareCreds)

Remove-PSSession -Session $PEPSession

Next steps

Update Microsoft Defender Antivirus on

Azure Stack Hub

Article • 07/29/2022

Microsoft Defender Antivirus is an antimalware solution that provides security and virus

protection. Every Azure Stack Hub infrastructure component (Hyper-V hosts and virtual

machines) is protected with Microsoft Defender Antivirus. For up-to-date protection,

you need periodic updates to Microsoft Defender Antivirus definitions, engine, and

platform. How updates are applied depends on your configuration.

The Azure Stack Hub update resource provider downloads antimalware definitions and

engine updates multiple times per day. Each Azure Stack Hub infrastructure component

gets the update from the update resource provider and applies the update

automatically.

For those Azure Stack Hub deployments that are connected to the public Internet, apply

the monthly Azure Stack Hub update. The monthly Azure Stack Hub update includes

Microsoft Defender Antivirus platform updates for the month.

For those Azure Stack Hub deployments that are not connected to the public Internet

(such as air-gapped datacenters) customers have the ability to apply the antimalware

definitions and engine updates as they are published.

To apply the updates to your Azure Stack Hub solution, you first have to download them

from the Microsoft site (links below) and subsequently, import them into a storage blob

container under your updateadminaccount. A scheduled task scans the blob container

every 30 minutes and, if new Defender definitions and engine updates are found, it

applies them to the Azure Stack Hub infrastructure.

For those disconnected deployments that don't have the ability to download Defender

definitions and engine updates on a daily basis, the monthly Azure Stack Hub update

includes Microsoft Defender Antivirus definitions, engine, and platform updates for the

month.

Connected scenario

Disconnected scenario

Set up Microsoft Defender for manual updates

You can use two new cmdlets in the privileged endpoint to configure Microsoft

Defender Antivirus manual update in Azure Stack Hub.

PowerShell

The following procedure shows how to setup Microsoft Defender Antivirus manual

update.

1. Connect to the privileged endpoint and run the following cmdlet to specify the

name of the storage blob container where the Defender updates will be uploaded.

PowerShell

2. Download the two Microsoft Defender Antivirus update packages and save them

on a location that is reachable from your Azure Stack Hub administration portal.

mpam-fe.exe from https://go.microsoft.com/fwlink/?

LinkId=121721&arch=x64

nis\_full.exe from https://go.microsoft.com/fwlink/?LinkId=197094

3. In the administration portal, select All services. Then, under the DATA + STORAGE

category, select Storage accounts. (Or, in the filter box, start typing storage

### cmdlet to configure the storage blob container for the Defender updates

Set-AzsDefenderManualUpdate [-Container <string>] [-Remove]

### cmdlet to retrieve the configuration of the Microsoft Defender Antivirus

manual update settings

Get-AzsDefenderManualUpdate

７ Note

The manual update process described below only works in disconnected

environments where access to "go.microsoft.com" is not allowed. Trying to run

the cmdlet Set-AzsDefenderManualUpdate in connected environments will

result in an error.

### Configure the storage blob container for the Defender updates

Set-AzsDefenderManualUpdate -Container <yourContainerName>

７ Note

You'll have to download these two files every time you want to update the

Defender signatures.

accounts, and select it.)

4. In the filter box, type update, and select the updateadminaccount storage

account.

5. In the storage account details, under Services, select Blobs.

6. Under Blob service, select + Container to create a container. Enter the name that

was specified with the Set-AzsDefenderManualUpdate (in this example

defenderupdates) and then select OK.

7. After the container is created, click the container name, and then click Upload to

upload the package files to the container.

8. Under Upload blob, click the folder icon, browse to the Microsoft Defender

Antivirus update mpam-fe.exe files and then click Open in the file explorer window.

9. Under Upload blob, click Upload.

10. Repeat steps 8 and 9 for the nis\_full.exe file.

A scheduled task scans the blob container every 30 minutes and applies any new

Microsoft Defender Antivirus package.

Learn more about Azure Stack Hub security

Next steps

Azure Stack Hub log and customer data

handling

Article • 04/19/2023

To the extent Microsoft is a processor or subprocessor of personal data in connection

with Azure Stack Hub, Microsoft makes to all customers, effective May 25, 2018, the

following commitments:

The "Processing of Personal Data; GDPR" provision in the "Data Protection Terms"

section of the Online Services Terms .

The European Union General Data Protection Regulation Terms in Attachment 4 of

the Online Services Terms .

As Azure Stack Hub resides in customer datacenters, Microsoft is the Data Controller

solely of the data that is shared with Microsoft through Diagnostics, Telemetry, and

Billing.

Microsoft employees, who are assigned to investigate a specific support case, will be

granted read-only access to the encrypted data. Microsoft employees also have access

to tools used to delete the data if needed. All access to the customer data is audited

and logged.

Data access controls:

Data is only kept for a maximum of 90 days after case close.

The customer always has the choice to have the data removed at any time in that

90-day period.

Microsoft employees are given access to the data on a case-by-case basis and only

as needed to help resolve the support issue.

In the event where Microsoft must share customer data with OEM partners,

customer consent is mandatory.

Microsoft supports on-demand data deletion per customer request. Customers can

request that one of our support engineers delete all their logs for a given case at any

time, before the data is permanently erased.

Data access controls

What Data Subject Requests (DSR) controls do customers

have?

For the automated data deletion action (90 days after case close), we don't proactively

contact customers and notify them about the deletion.

For the on-demand data deletion action, Microsoft support engineers have access to the

tool that lets them delete data on demand. They can provide confirmation on the phone

with the customer when it's done.

As part of the support process, Azure Stack Hub Operators can share diagnostic logs

with Azure Stack Hub support and engineering teams to help with troubleshooting.

Microsoft provides a tool and script for customers to collect and upload requested

diagnostic log files. Once collected, the log files are transferred over an HTTPS protected

encrypted connection to Microsoft. Because HTTPS provides the encryption over the

wire, there's no password needed for the encryption in transit. After they're received,

logs are encrypted and stored until they're automatically deleted 90 days after the

support case is closed.

Azure Stack Hub telemetry automatically uploads system data to Microsoft via the

Connected User Experience. Azure Stack Hub Operators have controls to customize

telemetry features and privacy settings at any time.

Microsoft doesn't intend to gather sensitive data, such as credit card numbers,

usernames and passwords, email addresses, and so on. If we determine that sensitive

information has been inadvertently received, we delete it.

Azure Stack Hub Billing leverages global Azure's Billing and Usage pipeline and is

therefore in alignment with Microsoft compliance guidelines.

Azure Stack Hub Operators can configure Azure Stack Hub to forward usage information

to Azure for billing. This configuration is required for Azure Stack Hub integrated

systems customers who choose the pay-as-you-use billing model. Usage reporting is

controlled independently from telemetry and isn't required for integrated systems

Does Microsoft notify customers when the data is

deleted?

Diagnostic data

Telemetry data

Billing data

customers who choose the capacity model or for Azure Stack Development Kit users. For

these scenarios, usage reporting can be turned off using the registration script.

Learn more about Azure Stack Hub security

Next steps

Azure Stack Hub Marketplace overview

Article • 06/09/2021

The Azure Stack Hub Marketplace is a collection of services, apps, and resources

customized for Azure Stack Hub. Resources include networks, virtual machines (VMs),

storage, and more. Use Azure Stack Hub Marketplace to create new resources and

deploy new apps or browse and choose the items you want to use. To use a marketplace

item, users must subscribe to an offer that grants them access to that item.

As an Azure Stack Hub operator, you decide which items to add (publish) to Azure Stack

Hub Marketplace. You can publish items such as databases, app services, and more.

Publishing makes items visible to all your users. You can publish custom items that you

create, or you can publish items from a growing list of Azure Marketplace items. When

you publish an item to Azure Stack Hub Marketplace, users can see it within five

minutes.

To open the Marketplace, in the administrator portal select + Create a resource.

Ｕ Caution

All gallery item artifacts, including images and JSON files, are accessible without

authentication after making them available in the Azure Stack Hub Marketplace. For

more considerations when publishing custom marketplace items, see Create and

publish a Marketplace item.

An Azure Stack Hub Marketplace item is a service, app, or resource that your users can

download and use. All Azure Stack Hub Marketplace items are visible to all your users,

including administrative items such as plans and offers. These administrative items don't

require a subscription to view, but are non-functional to users.

Every Marketplace item has the following:

An Azure Resource Manager template for resource provisioning.

Metadata, such as strings, icons, and other marketing collateral.

Formatting information to display the item in the portal.

Every item published to the Azure Stack Hub Marketplace uses the Azure Gallery

Package (.azpkg) format. Add deployment or runtime resources (code, .zip files with

software, or VM images) to Azure Stack Hub separately, not as part of the Marketplace

item.

Azure Stack Hub converts images to sparse files when they download from Azure, or

when you upload custom images. This process adds time when adding an image, but

saves space and speeds up the deployment of those images. Conversion only applies to

new images. Existing images are not changed.

Download existing marketplace items from Azure and publish to Azure Stack Hub

Create and publish a custom Azure Stack Hub Marketplace item

Marketplace items

Next steps

Azure Stack Hub Marketplace changes

Article • 03/03/2022

This article lists recent additions, updates, changes, and removals of Azure Stack Hub

Marketplace items. The information in this section is updated frequently, so check back

often for changes.

The Azure Stack Hub Marketplace items article always contains the most current list of

available Azure Stack Hub Marketplace items.

01/04/2021: Versa Operating System 21.1.1 - version 21.1.1

09/08/2020: Qualys Virtual Scanner Appliance

01/21/2020: Teradici Cloud Access Software

12/26/2019: CloudGuard IaaS High Availability

12/26/2019: Check Point CloudGuard IaaS Security Management

12/26/2019: Check Point CloudGuard IaaS Single Gateway

10/16/2019: SIOS DataKeeper Cluster Edition

08/19/2019: Iguazio Data Science Platform

08/09/2019: Oracle Linux

08/05/2019: Bitnami Drupal

08/05/2019: Bitnami etcd

08/05/2019: Bitnami Grafana

08/05/2019: Bitnami Neo4j

08/05/2019: Bitnami Parse Server

08/05/2019: Bitnami WordPress Multisite

08/05/2019: Bitnami ZooKeeper

08/05/2019: Bitnami TensorFlow Serving

08/05/2019: Bitnami NATS

08/05/2019: Bitnami Review Board

08/05/2019: Bitnami Composr

06/27/2019: SIOS Datakeeper Cluster Edition

７ Note

The catalog will be different based on the cloud environment your Azure Stack Hub

system is connected to. The cloud environment is determined by the Azure

subscription you use for registering your Azure Stack Hub.

New marketplace items

06/27/2019: Windows Server 2019 Datacenter Server Core With Containers Pay-asyou-use

06/27/2019: Windows Server 2019 Datacenter Server Core With Containers BYOL

06/27/2019: Windows Server 2019 Datacenter Pay-as-you-use

06/27/2019: Windows Server 2019 Datacenter BYOL

06/27/2019: Windows Server 2019 Datacenter Server Core Pay-as-you-use

06/27/2019: Windows Server 2019 Datacenter Server Core BYOL

06/27/2019: Windows Server 2019 Datacenter With Containers Pay-as-you-use

06/27/2019: Windows Server 2019 Datacenter With Containers BYOL

06/27/2019: Veeam Backup & Replication

03/01/2022: Horde Groupware Webmail

01/18/2022: eXo Platform

06/29/2021: Open Atrium

06/22/2021: SharePoint Server 2013 Trial

06/22/2021: SharePoint Server 2016 Trial

05/26/2021: CoreOS Linux (Stable) 64-bit

05/21/2021: Redmine+Agile

03/01/2021: SLES 15 (BYOS), SUSE Linux Enterprise Server 15

08/21/2020: Windows 10 Enterprise, Version 1903-Bring your own license - version

18362.959.2007101755

08/21/2020: Windows 10 Pro, Version 1903-Bring your own license - version

18362.959.2007101755

08/21/2020: Windows 10 Enterprise, Version 1909-Bring your own license - version

18363.959.2007101752

08/21/2020: Windows 10 Pro, Version 1909-Bring your own license - version

18363.959.2007101752

08/21/2020: Windows 10 Enterprise, Version 2004-Bring your own license - version

19041.388.2007101729

08/21/2020: Windows 10 Enterprise 2016 LTSB-Bring your own license - version

14393.3808.2007101707

08/21/2020: Windows 10 Enterprise 2019 LTSC-Bring your own license - version

17763.1339.2007101755

08/21/2020: Windows 10 Pro, Version 1809-Bring your own license - version

17763.1339.2007101755

08/21/2020: Windows Server 2008 R2 SP1-Pay as you go - version

7601.24557.2007101756

Deprecated marketplace items

08/21/2020: [smalldisk] Windows Server 2008 R2 SP1-Pay as you go - version

7601.24557.2007101756

08/21/2020: Windows Server 2012 Datacenter-Pay as you go - version

9200.23086.2007131700

08/21/2020: [smalldisk] Windows Server 2012 Datacenter-Pay as you go - version

9200.23086.2007131700

08/21/2020: Windows Server 2012 R2 Datacenter-Pay as you go - version

9600.19756.2007111612

08/21/2020: [smalldisk] Windows Server 2012 R2 Datacenter-Pay as you go -

version 9600.19756.2007111612

08/21/2020: Windows Server 2016 Datacenter-Pay as you go - version

14393.3808.2007101707

08/21/2020: Windows Server 2016 Datacenter - Server Core-Pay as you go -

version 14393.3808.2007101707

08/21/2020: [smalldisk] Windows Server 2016 Datacenter - Server Core-Pay as you

go - version 14393.3808.2007101707

08/21/2020: [smalldisk] Windows Server 2016 Datacenter-Pay as you go - version

14393.3808.2007101707

08/21/2020: Windows Server 2019 Datacenter Server Core-Pay as you go - version

17763.1339.2007101755

08/21/2020: [smalldisk] Windows Server 2019 Datacenter Server Core-Pay as you

go - version 17763.1339.2007101755

08/21/2020: Windows Server 2019 Datacenter Server Core with Containers-Pay as

you go - version 17763.1339.2007101755

08/21/2020: [smalldisk] Windows Server 2019 Datacenter Server Core with

Containers-Pay as you go - version 17763.1339.2007101755

08/21/2020: Windows Server 2019 Datacenter-Pay as you go - version

17763.1339.2007101755

08/21/2020: [smalldisk] Windows Server 2019 Datacenter-Pay as you go - version

17763.1339.2007101755

08/21/2020: Windows Server 2019 Datacenter with Containers-Pay as you go -

version 17763.1339.2007101755

08/21/2020: [smalldisk] Windows Server 2019 Datacenter with Containers-Pay as

you go - version 17763.1339.2007101755

08/21/2020: [smalldisk] Windows Server, version 1809 with Containers-Pay as you

go - version 17763.1339.2007101755

08/21/2020: [smalldisk] Windows Server, version 1903 with Containers-Pay as you

go - version 18362.959.2007101755

08/21/2020: [smalldisk] Windows Server, version 1909 with Containers-Pay as you

go - version 18363.959.2007101752

08/21/2020: [smalldisk] Windows Server, version 2004 with Containers-Pay as you

go - version 19041.388.2007101729

08/04/2020: Windows Server 2008 R2 SP1-Bring your own license - version

7601.24556.2006050139

08/04/2020: Windows Server 2008 R2 SP1-Pay as you go - version

7601.24556.2006050139

08/04/2020: [smalldisk] Windows Server 2008 R2 SP1-Bring your own license -

version 7601.24556.2006050139

08/04/2020: [smalldisk] Windows Server 2008 R2 SP1-Pay as you go - version

7601.24556.2006050139

08/04/2020: Windows Server 2012 Datacenter-Bring your own license - version

9200.23066.2006051749

08/04/2020: Windows Server 2012 Datacenter-Pay as you go - version

9200.23066.2006051749

08/04/2020: [smalldisk] Windows Server 2012 Datacenter-Bring your own license -

version 9200.23066.2006051749

08/04/2020: [smalldisk] Windows Server 2012 Datacenter-Pay as you go - version

9200.23066.2006051749

08/04/2020: Windows Server 2012 R2 Datacenter-Bring your own license - version

9600.19728.2006050139

08/04/2020: Windows Server 2012 R2 Datacenter-Pay as you go - version

9600.19728.2006050139

08/04/2020: [smalldisk] Windows Server 2012 R2 Datacenter-Bring your own

license - version 9600.19728.2006050139

08/04/2020: [smalldisk] Windows Server 2012 R2 Datacenter-Pay as you go -

version 9600.19728.2006050139

08/04/2020: Windows Server 2016 Datacenter-Bring your own license - version

14393.3750.2006031549

08/04/2020: Windows Server 2016 Datacenter-Pay as you go - version

14393.3750.2006031549

08/04/2020: Windows Server 2016 Datacenter - Server Core-Bring your own license

- version 14393.3750.2006031549

08/04/2020: Windows Server 2016 Datacenter - Server Core-Pay as you go -

version 14393.3750.2006031549

08/04/2020: [smalldisk] Windows Server 2016 Datacenter - Server Core-Bring your

own license - version 14393.3750.2006031549

08/04/2020: [smalldisk] Windows Server 2016 Datacenter - Server Core-Pay as you

go - version 14393.3750.2006031549

08/04/2020: [smalldisk] Windows Server 2016 Datacenter-Bring your own license -

version 14393.3750.2006031549

08/04/2020: [smalldisk] Windows Server 2016 Datacenter-Pay as you go - version

14393.3750.2006031549

08/04/2020: Windows Server 2019 Datacenter-Bring your own license - version

17763.1282.2006061952

08/04/2020: Windows Server 2019 Datacenter Server Core-Bring your own license -

version 17763.1282.2006061952

08/04/2020: Windows Server 2019 Datacenter Server Core-Pay as you go - version

17763.1282.2006061952

08/04/2020: [smalldisk] Windows Server 2019 Datacenter Server Core-Bring your

own license - version 17763.1282.2006061952

08/04/2020: [smalldisk] Windows Server 2019 Datacenter Server Core-Pay as you

go - version 17763.1282.2006061952

08/04/2020: Windows Server 2019 Datacenter Server Core with Containers-Bring

your own license - version 17763.1282.2006061952

08/04/2020: Windows Server 2019 Datacenter Server Core with Containers-Pay as

you go - version 17763.1282.2006061952

08/04/2020: [smalldisk] Windows Server 2019 Datacenter Server Core with

Containers-Bring your own license - version 17763.1282.2006061952

08/04/2020: [smalldisk] Windows Server 2019 Datacenter Server Core with

Containers-Pay as you go - version 17763.1282.2006061952

08/04/2020: Windows Server 2019 Datacenter-Pay as you go - version

17763.1282.2006061952

08/04/2020: [smalldisk] Windows Server 2019 Datacenter-Bring your own license -

version 17763.1282.2006061952

08/04/2020: [smalldisk] Windows Server 2019 Datacenter-Pay as you go - version

17763.1282.2006061952

08/04/2020: Windows Server 2019 Datacenter with Containers-Bring your own

license - version 17763.1282.2006061952

08/04/2020: Windows Server 2019 Datacenter with Containers-Pay as you go -

version 17763.1282.2006061952

08/04/2020: [smalldisk] Windows Server 2019 Datacenter with Containers-Bring

your own license - version 17763.1282.2006061952

08/04/2020: [smalldisk] Windows Server 2019 Datacenter with Containers-Pay as

you go - version 17763.1282.2006061952

08/04/2020: [smalldisk] Windows Server, version 1809 with Containers-Bring your

own license - version 17763.1282.2006061952

08/04/2020: [smalldisk] Windows Server, version 1809 with Containers-Pay as you

go - version 17763.1282.2006061952

08/04/2020: [smalldisk] Windows Server, version 1903 with Containers-Bring your

own license - version 18362.900.2006061800

08/04/2020: [smalldisk] Windows Server, version 1903 with Containers-Pay as you

go - version 18362.900.2006061800

08/04/2020: [smalldisk] Windows Server, version 2004 with Containers-Bring your

own license - version 19041.329.2006042019

08/04/2020: Windows 10 Enterprise 2016 LTSB-Bring your own license - version

14393.3750.2006031549

08/04/2020: Windows 10 Enterprise 2019 LTSC-Bring your own license - version

17763.1282.2006061952

08/04/2020: Windows 10 Enterprise, Version 1809-Bring your own license - version

17763.1282.2006061952

08/04/2020: Windows 10 Pro, Version 1809-Bring your own license - version

17763.1282.2006061952

08/04/2020: Windows 10 Enterprise, Version 1903-Bring your own license - version

18362.900.2006061800

08/04/2020: Windows 10 Pro, Version 1903-Bring your own license - version

18362.900.2006061800

08/04/2020: Windows 10 Enterprise, Version 1909-Bring your own license - version

18363.900.2006061800

08/04/2020: Windows 10 Pro, Version 1909-Bring your own license - version

18363.900.2006061800

08/04/2020: Windows 10 Enterprise, Version 2004-Bring your own license - version

19041.329.2006042019

05/21/2020: Windows Server 2008 R2 SP1 BYOL - version 7601.24552.2004101827

05/21/2020: Windows Server 2008 R2 SP1 Pay as you use - version

7601.24552.2004101827

05/21/2020: Windows Server 2012 Datacenter BYOL - version

9200.23016.2004101828

05/21/2020: Windows Server 2012 Datacenter Pay as you use - version

9200.23016.2004101828

05/21/2020: Windows Server 2012 R2 Datacenter BYOL - version

9600.19676.2004101829

05/21/2020: Windows Server 2012 R2 Datacenter Pay as you use - version

9600.19676.2004101829

05/21/2020: Windows Server 2016 Datacenter BYOL - version

14393.3630.2004101604

05/21/2020: Windows Server 2016 Datacenter Pay as you use - version

14393.3630.2004101604

05/21/2020: Windows Server 2016 Datacenter Server Core BYOL - version

14393.3630.2004101604

05/21/2020: Windows Server 2016 Datacenter Server Core Pay as you use - version

14393.3630.2004101604

05/21/2020: Windows Server 2019 Datacenter Server Core BYOL - version

17763.1158.2004131759

05/21/2020: Windows Server 2019 Datacenter Server Core Pay as you use - version

17763.1158.2004131759

05/21/2020: Windows Server 2019 Datacenter BYOL - version

17763.1158.2004131759

05/21/2020: Windows Server 2019 Datacenter Pay as you use - version

17763.1158.2004131759

05/21/2020: Windows Server 2019 Datacenter with Containers BYOL - version

17763.1158.2004131759

05/21/2020: Windows Server 2019 Datacenter with Containers Pay as you use -

version 17763.1158.2004131759

Bitnami Shopware

SQL Server 2017 Standard on SUSE Linux Enterprise Server (SLES) 12 SP2

Free License: SQL Server 2017 Developer on SUSE Linux Enterprise Server (SLES) 12

SP2

Free License: SQL Server 2017 Express on SUSE Linux Enterprise Server (SLES) 12

SP2

SQL Server 2017 Enterprise on SUSE Linux Enterprise Server (SLES) 12 SP2

SQL Server 2017 Web on SUSE Linux Enterprise Server (SLES) 12 SP2

Bitnami Codiad

Bitnami X2Engine Sales CRM

Bitnami SugarCRM

Bitnami Node.js High-Availability Cluster

Bitnami ProcessMaker Enterprise Edition

A10 vThunder: L4-L7 Application Delivery Controller, Global Server Load Balancing

(GSLB), SSL Insight

Check Point vSEC Security Management

06/23/2021: Free License: SQL Server 2016 SP2 Developer on Windows Server 2016

- Pay as you go - version 13.2.20210516

06/23/2021: Free License: SQL Server 2016 SP2 Developer on Windows Server 2016

- Bring your own license - version 13.2.20210516

06/23/2021: Free License: SQL Server 2016 SP2 Express on Windows Server 2016 -

Pay as you go - version 13.2.20210516

Updated marketplace items

06/23/2021: Free License: SQL Server 2016 SP2 Express on Windows Server 2016 -

Bring your own license - version 13.2.20210516

06/23/2021: Free SQL Server License: SQL Server 2017 Developer on Windows

Server 2016 - Pay as you go - version 14.0.20210516

06/23/2021: Free SQL Server License: SQL Server 2017 Developer on Windows

Server 2016 - Bring your own license - version 14.0.20210516

06/23/2021: Free SQL Server License: SQL Server 2017 Express on Windows Server

2016 - Pay as you go - version 14.0.20210516

06/23/2021: Free SQL Server License: SQL Server 2017 Express on Windows Server

2016 - Bring your own license - version 14.0.20210516

06/23/2021: SQL Server 2016 SP2 Enterprise on Windows Server 2016 - Pay as you

go - version 13.2.20210516

06/23/2021: SQL Server 2016 SP2 Enterprise on Windows Server 2016 - Bring your

own license - version 13.2.20210516

06/23/2021: SQL Server 2016 SP2 Standard on Windows Server 2016 - Pay as you

go - version 13.2.20210516

06/23/2021: SQL Server 2016 SP2 Standard on Windows Server 2016 - Bring your

own license - version 13.2.20210516

06/23/2021: SQL Server 2017 Enterprise Windows Server 2016 - Pay as you go -

version 14.0.20210516

06/23/2021: SQL Server 2017 Enterprise Windows Server 2016 - Bring your own

license - version 14.0.20210516

06/23/2021: SQL Server 2017 Standard on Windows Server 2016 - Pay as you go -

version 14.0.20210516

06/23/2021: SQL Server 2017 Standard on Windows Server 2016 - Bring your own

license - version 14.0.20210516

06/23/2021: SQL Server 2019 Enterprise on Windows Server 2019 - Pay as you go -

version 15.0.20210516

06/23/2021: SQL Server 2019 Enterprise on Windows Server 2019 - Bring your own

license - version 15.0.20210516

06/23/2021: Free SQL Server License: SQL 2019 Developer on Windows Server

2019 - Pay as you go - version 15.0.20210516

06/23/2021: Free SQL Server License: SQL 2019 Developer on Windows Server

2019 - Bring your own license - version 15.0.20210516

06/23/2021: SQL Server 2019 Standard on Windows Server 2019 - Pay as you go -

version 15.0.20210516

06/23/2021: SQL Server 2019 Standard on Windows Server 2019 - Bring your own

license - version 15.0.20210516

06/23/2021: SqlIaaSExtension - version 1.3.20680

06/15/2021: AKS Base Windows Image, May 20 2021 - version 17763.1935.210520

06/15/2021: AKS Base Ubuntu 18.04-LTS Image Distro, 2021 Q2 - version

2021.05.24

04/28/2021: Citrix ADC 13.0 VPX - Bring Your Own License - version 130.67.39

04/01/2021: Canonical Ubuntu Server 18.04 LTS - version 18.04.20210224

03/31/2021: SQL Server 2019 Enterprise on Windows Server 2019 - Pay as you go -

version 15.0.20210219

03/31/2021: SQL Server 2019 Enterprise on Windows Server 2019 - Bring your own

license - version 15.0.20210219

03/31/2021: Free SQL Server License: SQL 2019 Developer on Windows Server

2019 - Pay as you go - version 15.0.20210219

03/31/2021: Free SQL Server License: SQL 2019 Developer on Windows Server

2019 - Bring your own license - version 15.0.20210219

03/31/2021: SQL Server 2019 Standard on Windows Server 2019 - Pay as you go -

version 15.0.20210219

03/31/2021: SQL Server 2019 Standard on Windows Server 2019 - Bring your own

license - version 15.0.20210219

03/30/2021: Free License: SQL Server 2016 SP2 Developer on Windows Server 2016

- Pay as you go - version 13.2.20210219

03/30/2021: Free License: SQL Server 2016 SP2 Developer on Windows Server 2016

- Bring your own license - version 13.2.20210219

03/30/2021: Free License: SQL Server 2016 SP2 Express on Windows Server 2016 -

Pay as you go - version 13.2.20210219

03/30/2021: Free License: SQL Server 2016 SP2 Express on Windows Server 2016 -

Bring your own license - version 13.2.20210219

03/30/2021: Free SQL Server License: SQL Server 2017 Developer on Windows

Server 2016 - Pay as you go - version 14.0.20210219

03/30/2021: Free SQL Server License: SQL Server 2017 Developer on Windows

Server 2016 - Bring your own license - version 14.0.20210219

03/30/2021: Free SQL Server License: SQL Server 2017 Express on Windows Server

2016 - Pay as you go - version 14.0.20210219

03/30/2021: Free SQL Server License: SQL Server 2017 Express on Windows Server

2016 - Bring your own license - version 14.0.20210219

03/30/2021: SQL Server 2016 SP2 Enterprise on Windows Server 2016 - Pay as you

go - version 13.2.20210219

03/30/2021: SQL Server 2016 SP2 Enterprise on Windows Server 2016 - Bring your

own license - version 13.2.20210219

03/30/2021: SQL Server 2016 SP2 Standard on Windows Server 2016 - Pay as you

go - version 13.2.20210219

03/30/2021: SQL Server 2016 SP2 Standard on Windows Server 2016 - Bring your

own license - version 13.2.20210219

03/30/2021: SQL Server 2017 Enterprise Windows Server 2016 - Pay as you go -

version 14.0.20210219

03/30/2021: SQL Server 2017 Enterprise Windows Server 2016 - Bring your own

license - version 14.0.20210219

03/30/2021: SQL Server 2017 Standard on Windows Server 2016 - Pay as you go -

version 14.0.20210219

03/30/2021: SQL Server 2017 Standard on Windows Server 2016 - Bring your own

license - version 14.0.20210219

03/30/2021: SqlIaaSExtension - version 1.3.20590

03/11/2021: Data Box Gateway Virtual Device - version 1.0.2103

03/08/2021: AKS Base Ubuntu 16.04-LTS Image Distro, January 2021 - version

2021.01.28

03/08/2021: AKS Base Ubuntu 18.04-LTS Image Distro, 2021 Q1 - version

2021.01.28

03/08/2021: AKS Base Windows Image, January 28 2021 - version

17763.1697.210129

02/22/2021: F5 Networks, Inc. F5 BIG-IP VE - LTM/DNS (BYOL, 1 Boot Location) -

version 16.0.101000

02/22/2021: F5 Networks, Inc. F5 BIG-IP VE - ALL (BYOL, 1 Boot Location) - version

16.0.101000

02/22/2021: F5 Networks, Inc. F5 BIG-IP VE - LTM/DNS (BYOL, 2 Boot Locations) -

version 16.0.101000

02/22/2021: F5 Networks, Inc. F5 BIG-IP VE - ALL (BYOL, 2 Boot Locations) - version

16.0.101000

12/22/2020: Rogue Wave Software Centos 7.8 - version 7.8.2020062400

12/07/2020: Bitnami Elasticsearch Cluster - version 1.0.2

12/07/2020: Bitnami Cassandra Cluster - version 1.0.21

12/07/2020: Bitnami etcd Cluster - version 1.0.16

12/07/2020: Bitnami Jenkins Cluster - version 1.0.70

12/07/2020: Bitnami Kafka Cluster - version 1.0.2

12/07/2020: Bitnami MariaDB Galera Cluster - version 1.0.13

12/07/2020: Bitnami MariaDB with Replication - version 1.0.36

12/07/2020: Bitnami Memcached Multiple Instances - version 1.0.34

12/07/2020: Bitnami Moodle Multi-Tier - version 1.0.46

12/07/2020: Bitnami NATS Cluster - version 1.0.19

12/07/2020: Bitnami PostgreSQL with Replication - version 1.0.37

12/07/2020: Bitnami MySQL with Replication - version 1.0.37

12/07/2020: Bitnami ZooKeeper Cluster - version 1.0.18

12/07/2020: Bitnami Redis High Availability - version 1.0.27

12/07/2020: Bitnami WordPress Multi-Tier - version 1.0.56

12/07/2020: Bitnami RabbitMQ Cluster - version 1.0.38

11/17/2020: Azure Monitor, Update and Configuration Management - version

1.13.27

11/17/2020: Azure Monitor Dependency Agent - version 9.10.6.11730

11/17/2020: Azure Monitor Dependency Agent for Linux VMs - version

9.10.6.11730

11/17/2020: Azure Monitor, Update and Configuration Management - version

1.0.18053.0

11/04/2020: Teradici Cloud Access for Azure Stack nonGPU - version 1.0.2

10/29/2020: [smalldisk] Windows Server 2008 R2 SP1-Pay as you go - version

7601.24561.2010082056

10/29/2020: [smalldisk] Windows Server 2008 R2 SP1-Bring your own license -

version 7601.24561.2010082056

10/29/2020: Windows Server 2008 R2 SP1-Pay as you go - version

7601.24561.2010082056

10/29/2020: Windows Server 2008 R2 SP1-Bring your own license - version

7601.24561.2010082056

10/29/2020: Windows Server 2012 Datacenter-Pay as you go - version

9200.23179.2010090042

10/29/2020: Windows Server 2012 Datacenter-Bring your own license - version

9200.23179.2010090042

10/29/2020: [smalldisk] Windows Server 2012 Datacenter-Pay as you go - version

9200.23179.2010090042

10/29/2020: [smalldisk] Windows Server 2012 Datacenter-Bring your own license -

version 9200.23179.2010090042

10/29/2020: [smalldisk] Windows Server 2012 R2 Datacenter-Pay as you go -

version 9600.19847.2010090140

10/29/2020: [smalldisk] Windows Server 2012 R2 Datacenter-Bring your own

license - version 9600.19847.2010090140

10/29/2020: Windows Server 2012 R2 Datacenter-Pay as you go - version

9600.19847.2010090140

10/29/2020: Windows Server 2012 R2 Datacenter-Bring your own license - version

9600.19847.2010090140

10/29/2020: Windows 10 Enterprise 2016 LTSB-Bring your own license - version

14393.3986.2010070045

10/29/2020: Windows 10 Enterprise N 2016 LTSB-Bring your own license - version

14393.3986.2010070045

10/29/2020: Windows Server 2016 Datacenter-Pay as you go - version

14393.3986.2010070045

10/29/2020: Windows Server 2016 Datacenter-Bring your own license - version

14393.3986.2010070045

10/29/2020: Windows Server 2016 Datacenter - Server Core-Pay as you go -

version 14393.3986.2010070045

10/29/2020: Windows Server 2016 Datacenter - Server Core-Bring your own license

- version 14393.3986.2010070045

10/29/2020: [smalldisk] Windows Server 2016 Datacenter-Pay as you go - version

14393.3986.2010070045

10/29/2020: [smalldisk] Windows Server 2016 Datacenter-Bring your own license -

version 14393.3986.2010070045

10/29/2020: [smalldisk] Windows Server 2016 Datacenter - Server Core-Pay as you

go - version 14393.3986.2010070045

10/29/2020: [smalldisk] Windows Server 2016 Datacenter - Server Core-Bring your

own license - version 14393.3986.2010070045

10/29/2020: Windows Server 2019 Datacenter-Pay as you go - version

17763.1518.2010132039

10/29/2020: Windows Server 2019 Datacenter-Bring your own license - version

17763.1518.2010132039

10/29/2020: [smalldisk] Windows Server 2019 Datacenter Server Core-Pay as you

go - version 17763.1518.2010132039

10/29/2020: [smalldisk] Windows Server 2019 Datacenter Server Core-Bring your

own license - version 17763.1518.2010132039

10/29/2020: Windows Server 2019 Datacenter Server Core-Pay as you go - version

17763.1518.2010132039

10/29/2020: Windows Server 2019 Datacenter Server Core-Bring your own license -

version 17763.1518.2010132039

10/29/2020: Windows Server 2019 Datacenter with Containers-Pay as you go -

version 17763.1518.2010132039

10/29/2020: Windows Server 2019 Datacenter with Containers-Bring your own

license - version 17763.1518.2010132039

10/29/2020: [smalldisk] Windows Server 2019 Datacenter Server Core with

Containers-Pay as you go - version 17763.1518.2010132039

10/29/2020: [smalldisk] Windows Server 2019 Datacenter Server Core with

Containers-Bring your own license - version 17763.1518.2010132039

10/29/2020: [smalldisk] Windows Server 2019 Datacenter with Containers-Pay as

you go - version 17763.1518.2010132039

10/29/2020: [smalldisk] Windows Server 2019 Datacenter with Containers-Bring

your own license - version 17763.1518.2010132039

10/29/2020: [smalldisk] Windows Server 2019 Datacenter-Pay as you go - version

17763.1518.2010132039

10/29/2020: [smalldisk] Windows Server 2019 Datacenter-Bring your own license -

version 17763.1518.2010132039

10/29/2020: [smalldisk] Windows Server, version 1809 with Containers-Pay as you

go - version 17763.1518.2010132039

10/29/2020: [smalldisk] Windows Server, version 1809 with Containers-Bring your

own license - version 17763.1518.2010132039

10/29/2020: Windows Server 2019 Datacenter Server Core with Containers-Pay as

you go - version 17763.1518.2010132039

10/29/2020: Windows Server 2019 Datacenter Server Core with Containers-Bring

your own license - version 17763.1518.2010132039

10/29/2020: Windows 10 Pro, Version 1903-Bring your own license - version

18362.1139.2010070045

10/29/2020: Windows 10 Enterprise multi-session, Version 1903-Bring your own

license - version 18362.1139.2010070045

10/29/2020: Windows 10 Pro N, Version 1903-Bring your own license - version

18362.1139.2010070045

10/29/2020: Windows 10 Enterprise, Version 1903-Bring your own license - version

18362.1139.2010070045

10/29/2020: Windows 10 Enterprise N, Version 1903-Bring your own license -

version 18362.1139.2010070045

10/29/2020: [smalldisk] Windows Server, version 1903 with Containers-Pay as you

go - version 18362.1139.2010070045

10/29/2020: [smalldisk] Windows Server, version 1903 with Containers-Bring your

own license - version 18362.1139.2010070045

10/29/2020: Windows 10 Enterprise, Version 1909-Bring your own license - version

18363.1139.2010080514

10/29/2020: Windows 10 Pro N, Version 1909-Bring your own license - version

18363.1139.2010080514

10/29/2020: Windows 10 Pro, Version 1909-Bring your own license - version

18363.1139.2010080514

10/29/2020: Windows 10 Enterprise multi-session, Version 1909-Bring your own

license - version 18363.1139.2010080514

10/29/2020: Windows 10 Enterprise N, Version 1909-Bring your own license -

version 18363.1139.2010080514

10/29/2020: [smalldisk] Windows Server, version 1909 with Containers-Pay as you

go - version 18363.1139.2010080514

10/29/2020: [smalldisk] Windows Server, version 1909 with Containers-Bring your

own license - version 18363.1139.2010080514

10/29/2020: Windows 10 Enterprise, Version 2004-Bring your own license - version

19041.572.2010091946

10/29/2020: Windows 10 Enterprise multi-session, Version 2004-Bring your own

license - version 19041.572.2010091946

10/29/2020: [smalldisk] Windows Server, version 2004 with Containers-Pay as you

go - version 19041.572.2010091946

10/29/2020: [smalldisk] Windows Server, version 2004 with Containers-Bring your

own license - version 19041.572.2010091946

09/21/2020: Centos Application Connection Gateway - version 7.2.0

09/09/2020: FortiGate NGFW - Single VM Deployment (BYOL) - version 1.0.2

09/04/2020: CentOS-based 6.10 - version 6.10.2020042900

09/04/2020: CentOS-based 7.4 - version 7.4.20200220

09/04/2020: CentOS-based 7.5 - version 7.5.201808150

09/04/2020: CentOS-based 7.6 - version 7.6.201909120

09/04/2020: CentOS-based 7.7 - version 7.7.2020062400

09/04/2020: CentOS-based 8.0 - version 8.0.201912060

07/27/2020: Ubuntu Server 20.04 LTS - version 20.04.202007080

07/27/2020: Ubuntu Server 16.04 LTS - version 16.04.202007080

6/19/2020: Bitnami Gitlab CE - version 13.0.2006110322

6/16/2020: SQLIaaSExtension - version 1.3.20370

6/12/2020: Bitnami Grafana - version 6.7.2006040249

For more information about the Azure Stack Hub Marketplace, see the following articles:

Azure Marketplace overview

Azure Marketplace items available for Azure Stack Hub

Create and publish an Azure Stack Hub Marketplace item

Next steps

Azure Marketplace items available for

Azure Stack Hub

Article • 02/09/2023

This article describes the Azure Marketplace items that are available for Azure Stack

Hub.

Whenever there are updates to virtual machine (VM) extensions you use, you should

download them. Extensions shipped in the product don't update in the normal patch

and update process, so check for updates frequently. Other extensions are only available

through Marketplace Management.

Image Item name Description Publisher OS Type

SQL IaaS

Extension

(SqlIaasExtension)

Download this extension to deploy any

SQL Server on Windows Marketplace

item - this extension is required.

Microsoft Windows

Custom Script

Extension

Download this update to the in-box

version of the Custom Script Extension

for Windows.

Microsoft Windows

PowerShell DSC

Extension

Download this update to the in-box

version of the PowerShell DSC

Extension. Updated to support TLS v1.2.

Microsoft Windows

Microsoft

Antimalware

Extension

The Microsoft Antimalware for Azure is a

single-agent solution for apps and

tenant environments, designed to run in

the background without human

intervention. Download this update to

the in-box version of the Antimalware

Extension.

Microsoft Windows

７ Note

The catalog will be different based on the cloud environment your Azure Stack Hub

system is connected to. The cloud environment is determined by the Azure

subscription you use for registering your Azure Stack Hub.

Virtual Machine extensions

Image Item name Description Publisher OS Type

Microsoft Azure

Diagnostic

Extension

Microsoft Azure Diagnostics is the

capability within Azure that enables the

collection of diagnostic data on a

deployed app. Download this update to

the in-box version of the Diagnostic

Extension for Windows.

Microsoft Windows

Azure Monitor,

Update and

Configuration

Management

Extension

The Azure Monitor, Update and

Configuration Management Extension is

used with Log Analytics, Azure Security

Center, and Azure Sentinel to provide

VM monitoring capability. Download

this update to the in-box version of the

Monitoring Agent Extension for

Windows.

Microsoft Windows

- Custom Script

Extension

(version 1,

deprecated) -

Custom Script

Extension

(version 2)

Download this update to the in-box

version of the Custom Script Extension

for Linux. There are multiple versions of

this extension and you should

download both 1.5.2.1 and 2.0.x.

Microsoft Linux

VM Access for

Linux

Download this update to the in-box

version of the VMAccess for Linux

Extension. This update is important if

you plan to use Debian Linux VMs.

Microsoft Linux

Acronis Backup

Extension for

Linux

The Acronis Backup Extension for

Microsoft Azure is part of the Acronis

Backup family of data protection

products.

Acronis

International

GmbH.

Linux

Acronis Backup

Extension for

Windows

The Acronis Backup Extension for

Microsoft Azure is part of the Acronis

Backup family of data protection

products.

Acronis

International

GmbH.

Windows

CloudLink

SecureVM

Extension for

Linux

Control, monitor, and encrypt VMs with

ease and confidence.

Dell EMC Linux

CloudLink

SecureVM

Extension for

Windows

Control, monitor, and encrypt VMs with

ease and confidence.

Dell EMC Windows

Image Item name Description Publisher OS Type

Kaspersky Hybrid

Cloud Security

Agent for

Windows

With Kaspersky Hybrid Cloud Security,

you can provision cybersecurity

capabilities inside your cloud workloads

via Azure Extensions.

Kaspersky

Lab

Windows

Kaspersky Hybrid

Cloud Security

Agent for Linux

With Kaspersky Hybrid Cloud Security,

you can provision cybersecurity

capabilities right inside your cloud

workloads via Azure Extensions.

Kaspersky

Lab

Linux

Microsoft Azure Stack Hub supports the following Azure Marketplace VMs and solution

templates. Download any dependencies separately, as noted. Apps such as SQL Server

and Machine Learning Server require proper licensing, except where marked as Free or

Trial.

Image Item name Description Publisher

SQL Server 2014 SP3 on Windows

Server 2012 R2

SQL Server 2014 Service Pack 2.

Required download: SQL IaaS

Extension.

Microsoft

Microsoft Machine Learning

Server 9.3.0 on Windows Server

2016

Microsoft Machine Learning Server

9.3.0 on Windows Server 2016.

Microsoft

Microsoft Machine Learning

Server 9.3.0 on Ubuntu 18.04

Microsoft Machine Learning Server

9.3.0 on Ubuntu 16.04.

Microsoft +

Canonical

Microsoft Machine Learning

Server Windows Server

Microsoft Machine Learning Server

9.3.0 on CentOS Linux 7.2.

Microsoft +

Rogue

Wave

Image Item

name

Description Publisher

Clear

Linux

OS

A reference Linux distribution optimized for Intel Architecture. Clear Linux

Project

Microsoft VM images and solution templates

Linux distributions

Image Item

name

Description Publisher

Ubuntu

Server

Ubuntu Server is the world's most popular Linux for cloud

environments.

Canonical

Debian 8

"Jessie"

Debian GNU/Linux is one of the most popular Linux

distributions.

Debian

Oracle

Linux

The Oracle Linux operating system is engineered for open

cloud infrastructure. It delivers leading performance,

scalability, and reliability for enterprise SaaS and PaaS

workloads, as well as traditional enterprise apps.

Oracle

CentOSbased

7.6

This distribution of Linux is based on CentOS and is provided

by Rogue Wave Software.

Rogue

Wave

Software

(formerly

OpenLogic)

CentOSbased

7.5-

LVM

This distribution of Linux is based on CentOS and is provided

by Rogue Wave Software.

Rogue

Wave

Software

(formerly

OpenLogic)

CentOSbased

HPC

This distribution of Linux is based on CentOS and is provided

by Rogue Wave Software.

Rogue

Wave

Software

(formerly

OpenLogic)

SLES 11

SP4

(BYOS)

SUSE Linux Enterprise Server 11 SP4. SUSE

SLES 12

SP4

(BYOS)

SUSE Linux Enterprise Server 12 SP4. SUSE

Image Item name Description Publisher

Third-Party BYOL, free, trial images, and

solution templates

Image Item name Description Publisher

A10 vThunder

ADC

The A10 Networks vThunder ADC (Application Delivery

Controller) for Microsoft Azure is purpose-built for

high performance, flexibility, and easy-to-deploy app

delivery and server load balancing and optimized to

run natively within the Azure cloud.

A10

Networks

Arista vEOS

Router

The Arista vEOS Router is a feature-rich, multi-cloud,

and multi-hypervisor virtual router that empowers

enterprises and cloud providers to build consistent,

highly secure, and scalable hybrid networks.

Arista

Networks

Barracuda

Application

Security

Control

Center

Centrally manage multiple Barracuda Web Application

Firewalls (WAF).

Barracuda

Networks,

Inc.

Barracuda

Email Security

Gateway

Email security gateway to protect against inbound

email-borne threats.

Barracuda

Networks,

Inc.

Barracuda Web

Application

Firewall

(WAF)

Security and DDoS Protection Against Automated &

Targeted Attacks.

Barracuda

Networks,

Inc.

Barracuda

CloudGen

Firewall Control

Center

Centrally manage hundreds of Barracuda CloudGen

Firewalls regardless of their location and form factor.

Barracuda

Networks,

Inc.

Barracuda

CloudGen

Firewall for

Azure

Provides firewall protection where the app and data

reside, rather than solely where the connection

terminates.

Barracuda

Networks,

Inc.

CloudGuard

IaaS High

Availability

This solution deploys a 2 member Check Point

CloudGuard IaaS cluster. Each member has 2 network

interfaces.

Check Point

Check Point

CloudGuard

IaaS Security

Management

This solution deploys a single Check Point Security

Management Server with a single network interface.

Check Point

Check Point

CloudGuard

IaaS Single

Gateway

This solution deploys a single Check Point CloudGuard

IaaS security gateway with 2 network interfaces. After

deployment, you should set up User Defined Routes

(UDRs) to route traffic through the gateway.

Check Point

Image Item name Description Publisher

Chef

Automate

Build, deploy, and manage with Chef Automate, the

Continuous Automation Platform. Download both

Chef marketplace items.

Chef

Software, Inc

Commvault A comprehensive solution for backup and recovery,

app and VM migration to Azure Stack Hub, and

disaster recovery for Azure Stack Hub environments in

a single solution.

Commvault

CloudLink

SecureVM

Control, monitor, and encrypt VMs with ease and

confidence. Download all CloudLink SecureVM items.

Dell EMC

EventTracker

SIEM

EventTracker SIEM is a comprehensive security

platform that delivers advanced security tools with

audit-ready compliance capabilities.

EventTracker

Exivity - Hybrid

Cloud Billing

Solution

A billing tool that can satisfy the requirements of

virtually any IT service delivery model, whether

deployed within on-premises, public cloud, or hybrid

environments.

Exivity

f5 Big-IP Virtual

Edition

Advanced Load Balancing, GSLB, Network Firewall,

DNS, WAF, and App Access.

F5 Networks

FortiGate NextGeneration

Firewall

Firewall technology that delivers complete content

and network protection with a comprehensive suite of

powerful security features. App control, antivirus, IPS,

web filtering, and VPN along with advanced features

such as vulnerability management work in concert to

identify and mitigate the latest complex security

threats.

Fortinet

Kaspersky

Hybrid Cloud

Security

The Kaspersky Hybrid Cloud Security enables a

seamlessly orchestrated and adaptive cybersecurity

ecosystem.

Kaspersky

Lab

KEMP

LoadMaster

Load Balancer

ADC Content

Switch

Layer 4-7 Application Delivery Controller (ADC) Load

Balancer, Content Switch, and Traffic Manager.

KEMP

Technologies

Inc.

Kubernetes This solution deploys a Kubernetes cluster running as

a standalone cluster with templates generated using

AKS-Engine.

This solution template also requires Ubuntu Server

16.04 LTS and Custom Script for Linux 2.0.

Microsoft

Image Item name Description Publisher

Service Fabric

Cluster

This solution deploys Service Fabric running as a

standalone cluster on a Virtual Machine Scale Set.

This solution template requires you to also download

the Windows Server 2016 Datacenter

Microsoft

mPLAT Suite -

Multi-Cloud

Conductor

A Single Pane of Glass to monitor, configure,

provision, automate, and govern any workload or

cloud.

NRI

NooBaa Hybrid

AWS S3

compatible -

Community

Edition

S3-compatible storage service that spans public and

on-premises capacity resources.

NooBaa

NetFoundry

Gateway for

Multipoint,

Zero Trust

Azure Stack

Hub

Connections

Software-only, multi-point connectivity between Azure

Stack Hub and anywhere, over any network

connection, with industry leading Zero Trust security,

5x the throughput of VPN, and unlimited concurrent

users.

NetFoundry

Palo Alto VMSeries Next

Generation

Firewall

The VM-Series next-generation firewall allows

customers to securely migrate their apps and data to

Azure Stack Hub, protecting them from known and

unknown threats with app filtering and threat

prevention policies. This image requires a template to

deploy; see this article for important information.

Palo Alto

Networks,

Inc.

PT Application

Firewall

PT Application Firewall detects known & unknown

vulnerabilities and prevents attacks on web apps.

Download both PT Marketplace items.

Positive

Technologies

Puppet

Enterprise

Puppet Enterprise lets you automate the entire

lifecycle of your Azure Stack Hub infrastructure.

Download both Puppet Marketplace items.

Puppet

Qualys Virtual

Scanner

Appliance

The Virtual Scanner Appliance extends the Qualys

Cloud Platform's integrated suite of security and

compliance SaaS applications. Application modules

include Vulnerability Management, Policy Compliance,

and Web Application Scanning.

Qualys, Inc.

Quest Rapid

Recovery

Core

Rapid Recovery advanced data protection unifies

backup, replication, and recovery in one easy-to-use

software solution.

Quest

Software

Image Item name Description Publisher

SIOS

DataKeeper

Cluster

Edition

SIOS DataKeeper provides high availability (HA) and

disaster recovery (DR) in Azure Stack Hub. Simply add

SIOS DataKeeper software as an ingredient to your

Windows Server Failover Clustering (WSFC)

environment in an Azure Stack Hub deployment to

eliminate the need for shared storage.

SIOS

Technology

Corp.

SUSE Manager

3.1 Proxy

(BYOS)

Best-in-class open-source infrastructure management. SUSE

Teradici Cloud

Access

Software

Powered by PCoIP® technology, Cloud Access

Software delivers remote desktops and workstations

from Azure Stack to any device, anywhere. Consolidate

data storage, enhance collaboration, secure data,

streamline desktop management, and more.

Teradici

CipherTrust

Cloud Key

Manager

Leveraging Microsoft Azure and other cloud provider

Bring Your Own Key (BYOK) APIs, the CipherTrust

Cloud Key Manager reduces key management

complexity and operational costs by giving you

multicloud lifecycle control of encryption keys with

centralized management and visibility.

Thales

eSecurity

Veeam Backup

&

Replication

Veeam® Backup & Replication™ helps businesses

achieve comprehensive data protection for all

workloads -- virtual, physical, and cloud-based. With a

single console, you can achieve fast, flexible, and

reliable backup, recovery, and replication of all apps

and data.

Veeam

Software

Versa

Operating

System (VOS)

The Versa Operating System (VOS) is a comprehensive

and advanced next-generation virtual appliance that

brings the power of SD-WAN, SD-Routing and SDSecurity into the Microsoft Azure cloud.

Versa

Networks

ZeroDown

Software

Business

Continuity as a

Service

ZeroDown® Software technology provides businesses

with continuous access to their company data via their

Business Continuity as a Service (BCaaS)™ architecture,

protecting apps, and transactions, if network

interruptions occur that would normally hinder the

enterprise.

ZeroDown

Software

Download Marketplace items to Azure

Stack Hub

Article • 11/17/2022

As a cloud operator, you can download items to Azure Stack Hub from the Marketplace

and make them available to all users using the Azure Stack Hub environment. The items

you can choose are from a curated list of Azure Marketplace items that are pre-tested

and supported to work with Azure Stack Hub. Additional items are frequently added to

this list, so continue to check back for new content.

There are two scenarios for downloading Marketplace products:

Disconnected or partially connected scenario: Requires you to access the internet

using the Marketplace syndication tool to download Marketplace items. Then, you

transfer your downloads to your disconnected Azure Stack Hub installation. This

scenario uses PowerShell.

Connected scenario: Requires your Azure Stack Hub environment to be connected

to the internet. You use the Azure Stack Hub administrator portal to locate and

download items.

See Azure Marketplace items for Azure Stack Hub for a complete list of the marketplace

items you can download. See the Azure Stack Hub Marketplace changes article for a list

of recent additions, deletions, and updates to Azure Stack Hub Marketplace.

A connected deployment allows you to use the administrator portal to download

marketplace items.

７ Note

The catalog will be different based on the cloud your Azure Stack Hub system is

connected to. The cloud environment is determined by the Azure subscription you

use for registering your Azure Stack Hub.

７ Note

You can also use the The Operator Access Workstation (OAW) to access the

privileged endpoint (PEP), the Administrator portal for support scenarios, and Azure

Stack Hub GitHub Tools. For more information see Azure Stack Hub Operator

Access Workstation.

Your Azure Stack Hub deployment must have internet connectivity and be registered

with Azure.

1. Sign into the Azure Stack Hub administrator portal.

2. Review the available storage space before downloading marketplace items. Later,

when you select items for download, you can compare the download size to your

available storage capacity. If capacity is limited, consider options for managing

available space.

To review available space: in Region management, select the region you want to

explore and then go to Resource Providers > Storage:

3. Open Azure Stack Hub Marketplace and connect to Azure. To do so, select the

Marketplace management service, select Marketplace items, and then select Add

from Azure:

Prerequisites

Use the portal to download marketplace items

4. Each line item also shows the currently available version. If more than one version

of a Marketplace item is available, the Version column shows Multiple. You can

click on each item to view its description and additional information, including its

download size:

5. If the version of an item is shown as Multiple, you can select that item and then

choose a specific version from the resulting version selector dropdown. Note that

Microsoft now has the ability to add attributes that block administrators from

downloading marketplace products that are incompatible with their Azure Stack,

due to various properties, such as the Azure Stack version or billing model. Only

Microsoft can add these attributes:

6. Select the item you want, and then select Download. Download times vary and

depends on the network connectivity. After the download completes, you can

deploy the new marketplace item as either an Azure Stack Hub operator or a user.

7. To deploy the downloaded item, select + Create a resource, and then search

among the categories for the new marketplace item. Next, select the item to begin

the deployment process. The process varies for different marketplace items.

Connect to Azure Stack Hub with PowerShell



Next steps

Update Marketplace items in Azure Stack Hub

Article • 03/06/2023

As a cloud operator one of your responsibilities is to update the Azure Stack Hub Marketplace. When a

new version of a Marketplace item is available in Azure you can download the newer version to take

advantage of new features, security fixes and stability improvements.

There are four types of Marketplace items:

Virtual machine images

Extensions

Solution templates

Resource providers

New virtual machine (VM) images, extension and solution templates will be used automatically when

users deploy new resources. Resource providers use the Azure Stack Hub update experience and are not

covered by this article.

You can find more information about recent additions, updates, changes, and removals changes at

Azure Stack Hub Marketplace changes

Updating an extension within already deployed VMs require additional steps.

The process to download a new version of a Marketplace item is the same as the initial download of a

Marketplace item.

1. First check the version of an already downloaded Marketplace item in the Azure Stack Hub

Marketplace using the administrator portal.

2. Follow the instructions in Download Marketplace items to Azure Stack Hub for connected or

disconnected systems to download the new Marketplace item. Only download Marketplace items

that have a new version.

After the operator has downloaded a new version of an extension the user must take one of the

following two actions to ensure the new version is getting applied.

Retrieve the new version



Update already deployed extensions

1. Restart the VM. The extension gets updated automatically when starting the VM. This can be done

in the Azure Stack Hub user portal or PowerShell.

2. Use PowerShell to update the extension without a restart. This is helpful when scheduling a

downtime for a VM is not possible and an emergency update is required.

As a user you can use the following steps to query VMs and list the used extensions and update the

installed extension to the new version without restarting the VM.

Run the PowerShell cmdlets to list all the VMs and the installed extensions. Before running the cmdlets

make sure you have installed PowerShell for Azure Stack Hub.

PowerShell

If you want to list VMs that are running a specific extension you can use the following script.

PowerShell

Run PowerShell to update the extension to the latest version.

PowerShell

$VMs=Get-AzVM

Foreach($VM in $VMs)

{

Get-AzVMExtension -ResourceGroup $VM.ResourceGroupName -VMName $VM.name | ft VMName,

Name, TypeHandlerVersion, Publisher, ExtensionType, Location

}

$extensionname="SampleExtenionName"

$VMs=Get-AzVM

Foreach($VM in $VMs) {

$VMExtensions=Get-AzVMExtension -ResourceGroup $VM.ResourceGroupName -VMName $VM.name

$extensions=$VMExtensions.name

Foreach($Extension in $Extensions) {

if ($Extension -eq $extensionname)

{

write-host $VM.Name

}

}

}

Set-AzVMExtension -ResourceGroupName "SampleRG" -VMName "SampleVM" -Name "ExtensionName" -

Publisher "PublisherName" -typeHandlerVersion "NewExtensionVersion" -ExtensionType

SampleType -Location local

７ Note

It can take several minutes for the extension to be updated. You can safely run the first command

to check the version if it got updated.

Name Publisher TypeHandlerVersion ExtensionType

Microsoft.EnterpriseCloud.Monitoring Microsoft.EnterpriseCloud.Monitoring 1.14 OmsAgentForLinux

microsoft.linuxdiagnostic-3.1.135 Microsoft.Azure.Diagnostics 4.0 LinuxDiagnostic

For more information about the Azure Stack Hub Marketplace, see Azure Stack Hub Marketplace

overview.

List of recently updated extensions

７ Note

If you have installed any version of the following two extensions:

Azure Update and Configuration Management

Azure Update and Configuration Management for Linux

Ensure you replace them with the Azure Monitor, Update and Configuration Management for

Linux extension minimum version 1.14.02.

Next steps

Add and remove a custom VM image to

Azure Stack Hub

Article • 07/21/2021

In Azure Stack Hub, as an operator you can add your custom virtual machine (VM)

image to the marketplace and make it available to your users. You can add VM images

to the Azure Stack Hub Marketplace through the administrator portal or Windows

PowerShell. Use either an image from global Microsoft Azure Marketplace as a base for

your custom image, or create your own using Hyper-V.

You can find instructions for adding generalized and specialized images in the Compute

section of the user guide. You will want to create a generalized image before offering

the image to your users. For instructions, see Move a VM to Azure Stack Hub Overview.

When creating images available for your tenants, use the Azure Stack Hub

administrative portal or administrator endpoints rather than the user portal or tenant

directory endpoints.

You have two options for making an image available to your users:

Offer an image only accessible via Azure Resource Manager

If you add the image via the Azure Stack Hub administrative portal in Compute >

Images, all of your tenants can access the image. However your users will need to

use an Azure Resource Manager template to access it. It won't be visible in your

Azure Stack Hub Marketplace.

Offer an image through the Azure Stack Hub Marketplace

Once you have added your image through the Azure Stack Hub administrative

portal, you can then create a marketplace offering. For instructions, see Create and

publish a custom Azure Stack Hub Marketplace item.

７ Note

Blob access is required to allow the read access.

Add an image

Add a platform image

To add a platform image to Azure Stack Hub, use the Azure Stack Hub administrator

portal or endpoint using PowerShell. You must first create a generalized VHD. For more

information, see Move a VM to Azure Stack Hub Overview.

Add a VM image as an Azure Stack Hub operator using the portal.

1. Sign in to Azure Stack Hub as an operator. Select Dashboard from the lefthand navigation.

2. In the Resource providers list, select Compute.

3. Select VM images, then select Add.

4. Under Create image, enter the Publisher, Offer, SKU, Version, and OS disk

blob URI. Then, select Create to begin creating the VM image.

Portal





When the image is successfully created, the VM image status changes to

Succeeded.

5. When you add an image, it is only available for Azure Resource Managerbased templates and PowerShell deployments. To make an image available to

your users as a marketplace item, publish the marketplace item using the

steps in the article Create and publish a Marketplace item. Make sure you note

the Publisher, Offer, SKU, and Version values. You will need them when you

edit the Resource Manager template and Manifest.json in your custom .azpkg.

You can remove a platform image using the portal or PowerShell.

To remove the VM image as an Azure Stack Hub operator using the Azure Stack

Hub portal, follow these steps:

1. Open the Azure Stack Hub administrator portal .

2. If the VM image has an associated Marketplace item, select Marketplace

management, and then select the VM marketplace item you want to delete.

3. If the VM image does not have an associated Marketplace item, navigate to

All services > Compute > VM Images, and then select the ellipsis (...) next to

the VM image.

4. Select Delete.



Remove a platform image

Portal

Create and publish a custom Azure Stack Hub Marketplace item

Provision a virtual machine

Next steps

Create and publish a custom Azure

Stack Hub Marketplace item

Article • 10/11/2021

Every item published to the Azure Stack Hub Marketplace uses the Azure Gallery

Package (.azpkg) format. The Azure Gallery Packager tool enables you to create a

custom Azure Gallery package that you can upload to the Azure Stack Hub Marketplace,

which can then be downloaded by users. The deployment process uses an Azure

Resource Manager template.

The examples in this article show how to create a single VM Marketplace offer, of type

Windows or Linux.

Before creating the VM marketplace item, do the following:

1. Upload the custom VM image to the Azure Stack Hub portal, following the

instructions in Add a VM image to Azure Stack Hub.

2. Follow the instructions in this article to package the image (create an .azpkg) and

upload it to the Azure Stack Hub Marketplace.

To create a custom marketplace item, do the following:

1. Download the Azure Gallery Packager tool :

Marketplace items

Prerequisites

Create a Marketplace item

2. The tool includes sample packages that are in the .azpkg format, and must be

extracted first. You can rename the file extensions from ".azpkg" to ".zip," or use an

archiver tool of your choice:

3. Once extracted, the .zip file contains the Linux or Windows Azure Resource

Manager templates that are available. You can reuse the pre-made Resource

Manager templates, and modify the respective parameters with the product details

of the item that you will show on your Azure Stack Hub portal. Or, you can reuse

the .azpkg file and skip the following steps to customize your own gallery package.

4. Create an Azure Resource Manager template or use our sample templates for

Windows/Linux. These sample templates are provided in the packager tool .zip file

you downloaded in step 1. You can either use the template and change the text

fields, or you can download a pre-configured template from GitHub. For more

information about Azure Resource Manager templates, see Azure Resource

Manager templates.

5. The Gallery package should contain the following structure:

6. Replace the following highlighted values (those with numbers) in the Manifest.json

template with the value that you provided when uploading your custom image.

It's recommended that before publishing your own custom template, you try to

publish the sample as-is and make sure it works in your environment. Once you've

verified this step works, then delete the sample from gallery and make iterative

changes until you are satisfied with the result.

The following template is a sample of the Manifest.json file:

JSON

７ Note

Never hard code any secrets such as product keys, password, or any customer

identifiable information in the Azure Resource Manager template. Template

JSON files are accessible without the need for authentication once published

in the gallery. Store all secrets in Key Vault and call them from within the

template.

{

"$schema": "https://gallery.azure.com/schemas/2015-10-

01/manifest.json#",

"name": "Test", (1)

"publisher": "<Publisher name>", (2)

"version": "<Version number>", (3)

"displayName": "ms-resource:displayName", (4)

"publisherDisplayName": "ms-resource:publisherDisplayName", (5)

"publisherLegalName": "ms-resource:publisherDisplayName", (6)

"summary": "ms-resource:summary",

"longSummary": "ms-resource:longSummary",

"description": "ms-resource:description",

"longDescription": "ms-resource:description",

"links": [

{ "displayName": "ms-resource:documentationLink", "uri":

"http://go.microsoft.com/fwlink/?LinkId=532898" }

],

"artifacts": [

{

The following list explains the preceding numbered values in the example

template:

(1) - The name of the offer.

(2) - The name of the publisher, without a space.

(3) - The version of your template, without a space.

(4) - The name that customers see.

(5) - The publisher name that customers see.

(6) - The publisher legal name.

(7) - The path and name for each icon.

7. For all fields referring to ms-resource, you must change the appropriate values

inside the strings/resources.json file:

JSON

"isDefault": true

}

],

"images": [{

"context": "ibiza",

"items": [{

"id": "small",

"path": "icons\\Small.png", (7)

"type": "icon"

},

{

"id": "medium",

"path": "icons\\Medium.png",

"type": "icon"

},

{

"id": "large",

"path": "icons\\Large.png",

"type": "icon"

},

{

"id": "wide",

"path": "icons\\Wide.png",

"type": "icon"

}]

}]

}

{

"displayName": "<OfferName.PublisherName.Version>",

"publisherDisplayName": "<Publisher name>",

"summary": "Create a simple VM",

"longSummary": "Create a simple VM and use it",

"description": "<p>This is just a sample of the type of description you

8. The deployment templates file structure appears as follows:

Replace the values for the image in the createuidefinition.json file with the value

you provided when uploading your custom image.

9. To ensure that the resource can be deployed successfully, test the template with

the Azure Stack Hub APIs.

10. If your template relies on a virtual machine (VM) image, follow the instructions to

add a VM image to Azure Stack Hub.

11. Save your Azure Resource Manager template in the

/Contoso.TodoList/DeploymentTemplates/ folder.

12. Choose the icons and text for your Marketplace item. Add icons to the Icons

folder, and add text to the resources file in the Strings folder. Use the small,

medium, large, and wide naming convention for icons. See the Marketplace item

UI reference for a detailed description of these sizes.

13. For any further edits to Manifest.json, see Reference: Marketplace item

manifest.json.

14. When you finish modifying your files, convert it to an .azpkg file. You perform the

conversion using the AzureGallery.exe tool and the sample gallery package you

downloaded previously. Run the following command:

shell

could create for your gallery item!</p><p>This is a second paragraph.

</p>",

"documentationLink": "Documentation"

}

７ Note

All four icon sizes (small, medium, large, wide) are required for building the

Marketplace item correctly.

1. Use PowerShell or Azure Storage Explorer to upload your Marketplace item

(.azpkg) to Azure Blob storage. You can upload to local Azure Stack Hub

storage or upload to Azure Storage, which is a temporary location for the

package. Make sure that the blob is publicly accessible.

2. To import the gallery package into Azure Stack Hub, the first step is to

remotely connect (RDP) to the client VM, in order to copy the file you just

created to your Azure Stack Hub.

3. Add a context:

PowerShell

4. Run the following script to import the resource into your gallery:

PowerShell

.\AzureStackHubGallery.exe package -m c:\<path>\<gallery package

name>\manifest.json -o c:\Temp

７ Note

The output path can be any path you choose, and does not have to be under

the C: drive. However, the full path to both the manifest.json file, and the

output package, must exist. For example, if the output path is C:\

<path>\galleryPackageName.azpkg , the folder C:\<path> must exist.

Publish a Marketplace item

Az modules

$ArmEndpoint = "https://adminmanagement.local.azurestack.external"

Add-AzEnvironment -Name "AzureStackAdmin" -ArmEndpoint $ArmEndpoint

Connect-AzAccount -EnvironmentName "AzureStackAdmin"

Add-AzsGalleryItem -GalleryItemUri `

https://sample.blob.core.windows.net/<temporary blob

name>/<offerName.publisherName.version>.azpkg -Verbose

If you run into an error when running Add-AzsGalleryItem, you may have two

versions of the gallery.admin module installed. Remove all versions of the

module, and install the latest version. For steps on uninstalling your

PowerShell modules, see Uninstall existing versions of the Azure Stack Hub

PowerShell modules.

5. Verify that you have a valid Storage account that is available to store your

item. You can get the GalleryItemURI value from the Azure Stack Hub

administrator portal. Select Storage account -> Blob Properties -> URL, with

the extension .azpkg. The storage account is only for temporary use, in order

to publish to the marketplace.

After completing your gallery package and uploading it using AddAzsGalleryItem, your custom VM should now appear on the Marketplace as

well as in the Create a resource view. Note that the custom gallery package is

not visible in Marketplace Management.

6. Once your item has been successfully published to the marketplace, you can

delete the content from the storage account.

All default gallery artifacts and your custom gallery artifacts are now accessible

without authentication under the following URLs:

https://galleryartifacts.adminhosting.[Region].

[externalFQDN]/artifact/20161101/[TemplateName]/DeploymentTemplates/T

emplate.json



https://galleryartifacts.hosting.[Region].

[externalFQDN]/artifact/20161101/[TemplateName]/DeploymentTemplates/T

emplate.json

7. You can remove a Marketplace item by using the Remove-AzGalleryItem

cmdlet. For example:

PowerShell

Name Required Type Constraints Description

Name X String [A-Za-z0-9]+

Publisher X String [A-Za-z0-9]+

Version X String SemVer v2

Name Required Type Constraints Description

DisplayName X String Recommendation

of 80 characters

The portal might not display

your item name correctly if

it's longer than 80 characters.

PublisherDisplayName X String Recommendation

of 30 characters

The portal might not display

your publisher name

correctly if it's longer than 30

characters.

Remove-AzsGalleryItem -Name <Gallery package name> -Verbose

７ Note

The Marketplace UI may show an error after you remove an item. To fix the

error, click Settings in the portal. Then, select Discard modifications under

Portal customization.

Reference: Marketplace item manifest.json

Identity information

Metadata

Name Required Type Constraints Description

PublisherLegalName X String Maximum of 256

characters

Summary X String 60 to 100

characters

LongSummary X String 140 to 256

characters

Not yet applicable in Azure

Stack Hub.

Description X HTML 500 to 5,000

characters

The Marketplace uses the following icons:

Name Width Height Notes

Wide 255 px 115 px Always required

Large 115 px 115 px Always required

Medium 90 px 90 px Always required

Small 40 px 40 px Always required

Screenshot 533 px 324 px Optional

Each Marketplace item should be tagged with a category that identifies where the item

appears on the portal UI. You can choose one of the existing categories in Azure Stack

Hub (Compute, Data + Storage, and so on) or choose a new one.

Each Marketplace item can include various links to additional content. The links are

specified as a list of names and URIs:

Name Required Type Constraints Description

DisplayName X String Maximum of 64 characters.

Uri X URI

Images

Categories

Links

In addition to the preceding metadata, Marketplace authors can provide custom

key/value pair data in the following form:

Name Required Type Constraints Description

DisplayName X String Maximum of 25 characters.

Value X String Maximum of 30 characters.

For any field that allows HTML, the following elements and attributes are allowed :

h1, h2, h3, h4, h5, p, ol, ul, li, a[target|href], br, strong, em, b, i

Icons and text for Marketplace items as seen in the Azure Stack Hub portal are as

follows.

Additional properties

HTML sanitization

Reference: Marketplace item UI

Create blade

Marketplace item details blade

Azure Stack Hub Marketplace overview

Download Marketplace items

Format and structure of Azure Resource Manager templates

Next steps

Update solution templates to work with

new CreateUiDefinition changes

Article • 02/01/2023

This article describes how to prepare for the upcoming Azure Stack Hub update and its

changes to CreateUiDefinition.json. This JSON file is used to create the user experience

when deploying solution templates.

CreateUiDefinition.json will be updated to work with the UI changes in the upcoming

release. The changes provide a more complete user experience when deploying a

solution template. For more information about the new experience, see the

CreateUiDefinition overview.

However, we are aware of an issue in which certain solution templates are unable to

work with the new changes to the UI, unless the templates are updated. To ensure that

there are minimal disruptions, we have outlined a series of steps you can take to make

sure all your items are compatible with the latest update. The following images are a

side-by-side comparison between the old (bottom) and the new experience (top).

New:

Description of CreateUiDefinition issues

Old:

The first step is to determine which solution templates on your Azure Stack Hub

marketplace need to be updated. The following JavaScript snippet can help you find the

different items you may need to validate.

Run the script in the web console in which you are signed into the admin portal. The

console can usually be found in the web browser's development tools (can vary

depending on browser). Once the console is open, copy and paste the following script

into the console, and then hit Enter. The output is a list of solution templates from your

Azure Stack Hub marketplace that are not compatible with the new CreateUiDefinition

format:

JavaScript

Validation steps

uri = "/providers/Microsoft.Gallery/GalleryItems?api-version=2015-04-01"

let galleryItemsResult = await MsPortalFx.Base.Net2.ajax({uri: uri,

useFxArmEndpoint: true});

const result = [];

console.log("Checking....");

for (let i=0;i<galleryItemsResult.length;i++) {

const v = galleryItemsResult[i];

With the list of incompatible solution templates, use the following chart to determine

next steps:

If your solution template is downloaded with Marketplace management, update the

template to the latest version. Solution templates from marketplace management will be

updated in the coming months, so watch for the latest versions of your marketplace

items.

const uidef = await MsPortalFx.Base.Net2.ajax({uri: v.uiDefinitionUri,

useRawAjax: true});

const createBlade = uidef.createDefinition.createBlade;

if (createBlade.name === "CreateMultiVmWizardBlade" &&

createBlade.extension === "Microsoft\_Azure\_Compute") {

result.push(v);

}

}

if (result.length === 0) {

console.log("\n\n You don't have to update any item :)");

} else {

console.log("\n\nThese items need to be updated:");

result.forEach((v)=>{

console.log(v.itemDisplayName);

});

}

However, if your solution template is not from marketplace management or it's a

custom template that was created in-house, you may need to take additional steps to

ensure compatibility with the upcoming create UI. The following steps would need to be

completed before the new CreateUiDefinition experience is released (sometime in the

coming months) to ensure that your custom solution templates work with the new UX.

First, obtain the AZPKG file for the solution template. After extracting the .AZPKG file for

the template, follow these steps to update your solution templates.

1. Change the schema to the following code:

JSON

2. Change the "create blade" section to the following code:

JSON

1. Change the schema, handler, and version to the following code:

JSON

2. Go to https://<your portal

uri>/#blade/Microsoft\_Azure\_CreateUIDef/SandboxBlade , and follow the

instructions to test the modified CreateUiDefinition.json content. Address any

issues reported by the sandbox blade.

Step 1: modify UIDefinition.json file

"$schema": "https://gallery.azure.com/schemas/2018-02-

12/UIDefinition.json#",

"createBlade": {

"name": "CreateUIDefinitionBlade",

"extension": "Microsoft\_Azure\_CreateUIDef"

},

Step 2: modify CreateUiDefinition.json

"$schema": "https://schema.management.azure.com/schemas/0.1.2-

preview/CreateUIDefinition.MultiVm.json#",

"handler": "Microsoft.Azure.CreateUIDef",

"version": "0.1.2-preview",

1. Update the version property in the Manifest.json file to a newer version to allow

for publishing the updated template.

2. The final step is to create the new AZPKG using the Gallery Packager tool and to

run the packager command in PowerShell as follows:

PowerShell

This command creates a new AZPKG from the file that holds the different files

above. This AZPKG can then be used to publish the new solution template onto the

marketplace.

How to create and publish gallery item to the Azure Stack Hub marketplace

Createuidefinition.json official document

Step 3: update Manifest.json and create new AZPKG

AzureStackHubGallery.exe package -m <azpkg file\manifest.json> -o

<outfile path>

Next steps

Guest operating systems supported on

Azure Stack Hub

Article • 01/05/2023

Azure Stack Hub supports the Windows guest operating systems listed in the following

table:

Operating system Description Available in Azure Stack Hub

Marketplace

Windows Server 2022 64-bit Datacenter, Datacenter core

Windows Server,

version 1709

64-bit Core with containers

Windows Server 2019 64-bit Datacenter, Datacenter core, Datacenter

with containers

Windows Server 2016 64-bit Datacenter, Datacenter core, Datacenter

with containers

Windows Server 2012

R2

64-bit Datacenter

Windows Server 2012 64-bit Datacenter

Windows Server 2008

R2 SP1

64-bit Datacenter

Windows Server 2008

SP2

64-bit Bring your own image

Windows 10 (see note

1)

64-bit, Pro, and

Enterprise

Bring your own image

Windows

Azure Stack Hub 2108 or later

７ Note

To deploy Windows 10 client operating systems on Azure Stack Hub, you must have

Windows per-user licensing or purchase through a Qualified Multitenant

Marketplace images are available for pay-as-you-use or BYOL (EA/SPLA) licensing. Use

of both on a single Azure Stack Hub instance isn't supported. During deployment, Azure

Stack Hub injects a suitable version of the guest agent into the image.

Datacenter editions are available in Azure Stack Hub Marketplace for downloading;

customers can bring their own server images including other editions.

Linux distributions listed as available in Azure Stack Hub Marketplace include the

necessary Windows Azure Linux Agent (WALA). If you bring your own image to Azure

Stack, follow the guidelines in Add Linux images to Azure Stack.

Distribution Description Publisher Azure Stack Hub

Marketplace

CentOS-based 8.0 64-bit Rogue Wave Yes

CentOS-based 7.8 64-bit Rogue Wave Yes

CentOS-based 7.7 LVM 64-bit Rogue Wave Yes

CentOS-based 7.7 64-bit Rogue Wave Yes

CentOS-based 7.6 64-bit Rogue Wave Yes

CentOS-based 7.5 64-bit Rogue Wave Yes

CentOS-based 7.5 LVM 64-bit Rogue Wave Yes

CentOS-based 7.4 64-bit Rogue Wave Yes

CentOS-based 7.3 64-bit Rogue Wave Yes

CentOS-based 6.9 64-bit Rogue Wave Yes

Hoster (QMTH) .

Linux

７ Note

Custom images should be built with the latest public WALA version. For the

minimum supported Azure Linux agent see Minimum supported Azure Linux

Agent.

cloud-init is supported.

Distribution Description Publisher Azure Stack Hub

Marketplace

CentOS-based 6.10 64-bit Rogue Wave Yes

ClearLinux 64-bit ClearLinux.org Yes

Debian 8 "Jessie" 64-bit credativ Yes

Debian 9 "Stretch" 64-bit credativ Yes

Oracle Linux 64-bit Oracle Yes

Red Hat Enterprise Linux 7.1 (and

later)

64-bit Red Hat Bring your own image

SLES 11SP4 64-bit SUSE Yes

SLES 12SP3 64-bit SUSE Yes

Ubuntu 14.04-LTS 64-bit Canonical Yes

Ubuntu 16.04-LTS 64-bit Canonical Yes

Ubuntu 18.04-LTS 64-bit Canonical Yes

Ubuntu Server 20.04 LTS 64-bit Canonical Yes

For Red Hat Enterprise Linux support information, see Red Hat and Azure Stack Hub:

Frequently Asked Questions .

For more information about Azure Stack Hub Marketplace, see the following articles:

Download marketplace items

Create and publish a marketplace item

Next steps

Make virtual machine scale sets

available in Azure Stack Hub

Article • 04/11/2022

Virtual machine scale sets are an Azure Stack Hub compute resource. You can use scale

sets to deploy and manage a set of identical virtual machines (VMs). With all VMs

configured in the same way, scale sets do not require pre-provisioning of VMs. It's easier

to build large-scale services that target big compute, big data, and containerized

workloads.

This article guides you through the process of making scale sets available in the Azure

Stack Hub Marketplace. After you complete this procedure, your users can add virtual

machine scale sets to their subscriptions.

Virtual machine scale sets on Azure Stack Hub are similar to virtual machine scale sets

on Azure. For more information, see the following videos:

Mark Russinovich talks Azure scale sets

On Azure Stack Hub, virtual machine scale sets do not support autoscale. You can add

more instances to a scale set using Resource Manager templates, Azure CLI, or

PowerShell.

Azure Stack Hub Marketplace: Register Azure Stack Hub with global Azure to

enable the availability of items in the Azure Stack Hub Marketplace. Follow the

instructions in Register Azure Stack Hub with Azure.

Operating system image: Before a virtual machine scale set can be created, you

must download the VM images for use in the scale set from the Azure Stack Hub

Marketplace. The images must already be present before a user can create a new

scale set.

1. Sign in to the Azure Stack Hub portal. Then, go to All services, then Virtual

machine scale sets, and then under COMPUTE, select Virtual machine scale sets.

Prerequisites

Use the Azure Stack Hub portal

2. Select Add.

3. Fill in the empty fields, choose from the dropdowns for Operating system disk

image, Subscription, and Instance size. Select Yes for Use managed disks. Then,

select Create.





4. To see your new virtual machine scale set, go to All resources, search for the virtual

machine scale set name, and then select its name in the search.

After you create a virtual machine scale set, users can update images in the scale set

without the scale set having to be recreated. The process to update an image depends

on the following scenarios:

1. Virtual machine scale set deployment template specifies latest for version:

When the version is set to latest in the imageReference section of the template for

a scale set, scale-up operations on the scale set use the newest available version of

the image for the scale set instances. After a scale-up is complete, you can delete

older virtual machine scale sets instances. The values for publisher , offer , and

sku remain unchanged.

The following JSON example specifies latest :

JSON

2. Virtual machine scale set deployment template does not specify latest for version

and specifies a version number instead:

If the Azure Stack operator downloads an image with a newer version (and deletes

the older version), the scale set cannot scale up. This is by design, as the image

version specified in the scale set template must be available.



Update images in a virtual machine scale set

"imageReference": {

"publisher": "[parameters('osImagePublisher')]",

"offer": "[parameters('osImageOffer')]",

"sku": "[parameters('osImageSku')]",

"version": "latest"

}

For more information, see operating system disks and images.

You can change the size of a virtual machine scale set to make it larger or smaller.

1. In the portal, select your scale set and then select Scaling.

2. Use the slide bar to set the new level of scaling for this virtual machine scale set,

and then click Save.

Download marketplace items from Azure to Azure Stack Hub

Scale a virtual machine scale set



Next steps

Azure Stack Hub Marketplace FAQ

FAQ

This article answers some frequently asked questions about Marketplace items in the

Azure Stack Hub Marketplace.

Azure Marketplace support guidance extends to Azure Stack Hub Marketplace items as

well. Publishers are responsible for providing technical support for their products on the

Azure Stack Hub Marketplace. To learn more about support guidance for Azure

Marketplace items, see the support section in the Azure Marketplace FAQs article.

First, determine if any Azure Resource Manager templates refer to specific versions. If so,

update those templates, or keep older image versions. It's best to use version: latest.

Next, if any virtual machine scale sets refer to a specific version, you should think about

whether these will be scaled later, and decide whether to keep older versions. If neither

of these conditions apply, delete older images in Azure Stack Hub Marketplace before

downloading newer ones. Use Marketplace management to delete them if that's how

the original was downloaded. Then download the newer version.

Microsoft offers two versions of Windows Server images through Azure Stack Hub

Marketplace. Only one version of this image can be used in an Azure Stack Hub

environment.

Who should I contact for support issues

with Azure Stack Hub Marketplace

items?

How do I update to a newer Windows

image?

What are the licensing options for

Windows Server images on Azure Stack

Hub Marketplace?

Pay as you go (PAYG): These images run the full-price Windows meters. Who

should use this option: Enterprise Agreement (EA) customers who use the

Consumption billing model; CSPs who don't want to use SPLA licensing.

Bring Your Own License (BYOL): These images run basic meters. Who should use

this option: EA customers with a Windows Server license; CSPs who use SPLA

licensing.

Azure Hybrid Use Benefit (AHUB) is not supported on Azure Stack Hub. Customers who

license through the "Capacity" model must use the BYOL image. If you're testing with

the Azure Stack Development Kit (ASDK), you can use either of these options.

Delete the incorrect version first through marketplace management. Wait for it to

complete (look at the notifications for completion, not the Marketplace Management

blade). Then download the correct version.

If you download both versions of the image, only the latest version is visible to end

customers in Azure Stack Hub Marketplace.

You can change the license model attribute to switch from BYOL to the PAYG model by

running the following script:

powePowerShellrshell

What if I downloaded the wrong version

to offer my tenants/users?

What if my user incorrectly checked the

"I have a license" box in previous

Windows builds, and they don't have a

license?

Az modules

$vm= Get-Azvm -ResourceGroup "<your RG>" -Name "<your VM>"

$vm.LicenseType = "None"

Update-AzVM -ResourceGroupName "<your RG>" -VM $vm

You can change the license model attribute to the BYOL model by running the following

commands:

PowerShell

These images do apply the licenseType parameter, so they're PAYG. You can set this

parameter (see the previous FAQ answer). This only applies to the Windows Server

software, not to layered products such as SQL, which require you to bring your own

license. PAYG licensing doesn't apply to layered software products.

You can only change the licenseType property for SQL Server images from Azure Stack

Hub Marketplace if the version is XX.X.20190410 or higher. If you're running an older

version of the SQL Server images from Azure Stack Hub Marketplace, you can't change

the licenseType attribute and you must redeploy using the latest SQL Server images

from Azure Stack Hub Marketplace.

What if I have an older image and my

user forgot to check the "I have a

license" box, or we use our own images

and we do have Enterprise Agreement

entitlement?

Az modules

$vm= Get-Azvm -ResourceGroup "<your RG>" -Name "<your VM>"

$vm.LicenseType = "Windows\_Server"

Update-AzVM -ResourceGroupName "<your RG>" -VM $vm

What about other VMs that use

Windows Server, such as SQL or

Machine Learning Server?

I have an Enterprise Agreement (EA)

and will be using my EA Windows

You can add licenseType: Windows\_Server in an Azure Resource Manager template.

This setting must be added to each virtual machine (VM) resource block.

To activate a Windows Server VM on Azure Stack Hub, the following conditions must be

true:

The OEM has set the appropriate BIOS marker on every host system in Azure Stack

Hub.

Windows Server 2012 R2 and Windows Server 2016 must use Automatic VM

Activation. Key Management Service (KMS) and other activation services aren't

supported on Azure Stack Hub.

Run the following command from an elevated command prompt:

shell

If it's correctly activated, you'll see this clearly indicated and the host name displayed in

the slmgr output. Don't depend on watermarks on the display as they might not be up

to date, or are showing from a different VM behind yours.

Run the following command from an elevated command prompt:

shell

Server license; how do I make sure

images are billed correctly?

Activation

How can I verify that my VM is

activated?

slmgr /dlv

My VM isn't set up to use AVMA, how

can I fix it?

slmgr /ipk <AVMA key>

See the Automatic VM Activation article for the keys to use for your image.

It's recommended that you execute the slmgr /ipk command line with the appropriate

key before you run the sysprep command. Or, include the AVMA key in any

Unattend.exe setup file.

Run the slmgr /ipk command. Azure images may not correctly fall back to AVMA, but if

they can reach the Azure KMS system, they will activate. It's recommended that you

ensure these VMs are set to use AVMA.

Contact your hardware supplier to verify that the correct BIOS markers were installed.

Automatic VM Activation isn't supported in earlier versions of Windows Server. You must

activate the VMs manually.

For more information, see the following articles:

The Azure Stack Hub Marketplace overview

Download marketplace items from Azure to Azure Stack Hub

I create my own Windows Server

images, how can I make sure they use

AVMA?

I am trying to use my Windows Server

2016 image created on Azure and it's

not activating or using KMS activation

I have performed all of these steps but

my VMs are still not activating

What about earlier versions of Windows

Server?

Next steps

Add Linux images to the Azure Stack

Hub Marketplace

Article • 09/02/2022

You can deploy Linux virtual machines (VMs) on Azure Stack Hub by adding a Linuxbased image to the Azure Stack Hub Marketplace. The easiest way to add a Linux image

to Azure Stack Hub is through marketplace management. These images have been

prepared and tested for compatibility with Azure Stack Hub.

To download Linux images from Azure Marketplace, see Download marketplace items

from Azure to Azure Stack Hub. Select the Linux images that you want to offer users on

your Azure Stack Hub.

There are frequent updates to these images, so check back often to keep up to date.

Wherever possible, download the images available through marketplace management.

These images have been prepared and tested with Azure Stack Hub.

To get support for the Azure Linux Agent and extensions in Azure Stack Hub, the Linux

Agent version on the Linux virtual machine (VM) must be later than or equal to

version 2.2.10 and Azure Stack Hub must run a build that is within two releases of the

current release. For information about Azure Stack Hub updates, see Azure Stack Hub

release notes.

As of July 2020, the minimum supported version is 2.2.41 for the Linux Agent. If the

Linux Agent version is earlier than version 2.2.10, you must update the VM by using the

distribution package manager and by enabling auto-update.

If the distribution vendor doesn't have the minimum Linux Agent version in the

package repositories, the system is still in support. If the Linux Agent version is

later than version 2.1.7, you must enable the Agent auto-update feature. It will

retrieve the latest version of code for extension handling.

Marketplace management

Prepare your own image

Minimum supported Azure Linux Agent

If the Linux Agent version is earlier than version 2.2.10, or if the Linux system is

out-of-support, we may require you to update the agent before getting support.

If the Linux Agent version is customized by a publisher, Microsoft may direct you

to the publisher for support agent or extension-specific support because of the

customization. To upgrade the Linux Agent, see How to update the Azure Linux

Agent on a VM.

To check your Linux Agent Version, run:

Bash

For example, if you are running this command on Ubuntu 18.04, you'll see the output:

Bash

For more information about the agent, see the FAQ for WALinuxAgent .

You can prepare your own Linux image using the following instructions:

CentOS-based Distributions

Debian Linux

Red Hat Enterprise Linux

SLES & openSUSE

Ubuntu Server

You can use Cloud-init to customize your Linux VM, you can use the following

PowerShell instructions.

Check your Linux Agent Version

waagent --version

WALinuxAgent - 2.2.45

Python - 3.6.9

Goal State Agent - 2.2.48.1

Prepare your own Linux image

Cloud-init

Step 1: Create a cloud-init.txt file with your cloud-config

Create a file named cloud-init.txt and paste the following cloud configuration:

YAML

Upload the file to an Azure storage account, Azure Stack Hub storage account, or

GitHub repository reachable by your Azure Stack Hub Linux VM.

#cloud-config

package\_upgrade: true

packages:

- nginx

- nodejs

- npm

write\_files:

- owner: www-data:www-data

path: /etc/nginx/sites-available/default

content: |

server {

listen 80;

location / {

proxy\_pass http://localhost:3000;

proxy\_http\_version 1.1;

proxy\_set\_header Upgrade $http\_upgrade;

proxy\_set\_header Connection keep-alive;

proxy\_set\_header Host $host;

proxy\_cache\_bypass $http\_upgrade;

}

}

- owner: azureuser:azureuser

path: /home/azureuser/myapp/index.js

content: |

var express = require('express')

var app = express()

var os = require('os');

app.get('/', function (req, res) {

res.send('Hello World from host ' + os.hostname() + '!')

})

app.listen(3000, function () {

console.log('Hello world app listening on port 3000!')

})

runcmd:

- service nginx restart

- cd "/home/azureuser/myapp"

- npm init

- npm install express -y

- nodejs index.js

Step 2: Reference cloud-init.txt during the Linux VM

deployment

Currently, using cloud-init for VM deployment is only supported on REST, PowerShell,

and Azure CLI, and does not have an associated portal UI on Azure Stack Hub.

You can follow the Quickstart: Create a Linux server VM by using PowerShell in Azure

Stack Hub to create the Linux VM using PowerShell. Make sure to reference the cloudinit.txt as a part of the -CustomData flag:

PowerShell

Follow Add the image to the Marketplace. Make sure that the OSType parameter is set to

Linux .

After you've added the image to the Marketplace, a Marketplace item is created and

users can deploy a Linux VM.

Download marketplace items from Azure to Azure Stack Hub

Azure Stack Hub Marketplace overview

Az modules

$VirtualMachine =Set-AzVMOperatingSystem -VM $VirtualMachine `

-Linux `

-ComputerName "MainComputer" `

-Credential $cred -CustomData "#include

https://cloudinitstrg.blob.core.windows.net/strg/cloud-init.txt"

Add your image to Marketplace

Next steps

Offer a Red Hat-based virtual machine

for Azure Stack Hub

Article • 01/07/2022

This article describes how to prepare a Red Hat Enterprise Linux virtual machine (VM) for

use in Azure Stack Hub.

There are two ways that you can offer Red Hat-based VM in Azure Stack Hub:

You can add the virtual machine to the Azure Stack Hub Marketplace.

Get familiar with the Red Hat Cloud Access program terms. Enable your Red

Hat subscriptions for Cloud Access at Red Hat Subscription-Manager . To be

registered for Cloud Access, you must have on hand the Azure subscriptions

with which your Azure Stack Hub is registered.

Red Hat Enterprise Linux Images are a private offering on Azure Stack Hub. To

make this offering available to your Marketplace Management tab, you will

need to complete a survey . After you post the survey, it takes seven business

days to see it in your Add from Azure tab within Marketplace Management.

For more information, see the Azure Stack Hub Marketplace overview.

You can add your own custom image to your Azure Stack Hub, and then offer the

image in the Marketplace.

1. You must have Red Hat cloud access.

2. For instructions on preparing the image for Azure and Azure Stack Hub, see

Prepare a Red Hat-based virtual machine for Azure.

3. For instructions on offering your custom image in the Azure Stack Hub

Marketplace, see Create and publish a Marketplace item.

For more information about the hypervisors that are certified to run Red Hat Enterprise

Linux, see the Red Hat website .

Offer a Red Hat-based VM

Next steps

Add Commvault to Azure Stack Hub

Marketplace

Article • 07/29/2022

This article walks through offering Commvault Live Sync to update a recovery virtual

machine (VM) located on a separate Azure Stack Hub scale unit. You can download and

offer Commvault as a backup and replication solution for your users.

Your user needs to install the backup and replication software on a VM in their

source Azure Stack Hub subscription. Azure Site Recovery and Azure Backup can

offer an off-stack location to store your backups and recovery images. They both

require the creation of a Recovery Services Vault in Azure before downloading the

software images to be installed on your Azure Stack Hub. The software images can

be downloaded from: Azure Backup Server and Azure Site Recovery .

You may need licenses for third-party software (if chosen).

Your users may need assistance in connecting their source and target through a

VPN gateway or public IP on the backup and replication host.

Target Azure Cloud subscription or a subscription on a recovery target Azure Stack

Hub.

Target resource group and blob storage account on a recovery target Azure Stack

Hub.

Some solutions require that you create VMs in the target subscription that need to

run 24x7x365 in order to receive changes from the source server. In Back up your

VM on Azure Stack Hub with Commvault, Commvault Live Sync creates the target

recovery VMs during initial configuration and keeps them idle (not running, not

billable) until changes need to be applied during a replication cycle.

1. Open the Azure Stack Hub administrator portal.

2. Select Marketplace management > Add from Azure.

Notes for Commvault

Get Commvault for your marketplace

3. Enter commvault .

4. Select Commvault Trial. And then select Download.

Back up your VM on Azure Stack Hub with Commvault

Overview of offering services in Azure Stack Hub

Next steps

Azure Stack Hub services, plans, offers,

subscriptions overview

Article • 07/29/2022

Microsoft Azure Stack Hub is a hybrid cloud platform that lets you deliver services from

your datacenter. Services include virtual machines (VMs), SQL Server databases, and

even Azure Marketplace items. As a service provider, you can offer services to your

tenants. Within a business or government agency, you can offer on-premises services to

your employees.

As an Azure Stack Hub operator, you configure and deliver services by using offers,

plans, and subscriptions. Offers contain one or more plans, and each plan includes one

or more services, each configured with quotas. By creating plans and combining them

into different offers, users can subscribe to your offers and deploy resources. This

structure lets you manage:

Which services and resources your users can access.

The amount of resources that users can consume.

Which regions have access to the resources.

To deliver a service, follow these high-level steps:

1. Plan your service offering, using:

Foundational services, like compute, storage, networking, or Key Vault.

Value-add services, like Event Hubs, App Service, SQL Server, or MySQL

Server.

2. Create a plan that consists of one or more services. When creating a plan, select or

create quotas that define the resource limits of each service in the plan.

3. Create an offer that has one or more plans. The offer can include base plans and

optional add-on plans.

After you've created the offer, your users can subscribe to it to access the services and

deploy resources. Users can subscribe to as many offers as they want. The following

figure shows a simple example of a user who has subscribed to two offers. Each offer

has a plan or two, and each plan gives them access to specific services.

Overview

You can offer Infrastructure as a Service (IaaS) services that enable your users to build

an on-demand computing infrastructure, provisioned and managed from the Azure

Stack Hub user portal.

You can also deploy Platform as a Service (PaaS) services for Azure Stack Hub from

Microsoft and third-party providers. The PaaS services that you can deploy include, but

aren't limited to:

Event Hubs

App Service

SQL Server

MySQL Server

You can also combine services to integrate and build complex solutions for different

users.

To help manage your cloud capacity, you can use pre-configured quotas, or create a new

quota for each service in a plan. Quotas define the upper resource limits that a user

subscription can provision or consume. For example, a quota might allow a user to

create up to five VMs.

Services

Quotas

） Important

You can set up quotas by region. For example, a plan that provides compute services for

Region A could have a quota of two VMs.

Learn more about quota types in Azure Stack Hub.

Plans are groupings of one or more services. As an Azure Stack Hub operator, you create

plans to offer to your users. In turn, your users subscribe to your offers to use the plans

and services they include. When creating plans, make sure to set your quotas, define

your base plans, and consider including optional add-on plans.

When creating an offer, the service administrator can include a base plan. These base

plans are included by default when a user subscribes to that offer. When a user

subscribes, they have access to all the resource providers specified in those base plans

(with the corresponding quotas).

Add-on plans are optional plans you add to an offer. Add-on plans aren't included by

default in the subscription. Add-on plans are additional plans (with quotas) available in

an offer that a subscriber can add to their subscriptions. For example, you can offer a

base plan with limited resources for a trial, and an add-on plan with more substantial

resources to customers who decide to adopt the service.

It can take up to two hours for new quotas to be available in the user portal or

before a changed quota is enforced.

７ Note

In the Azure Stack Development Kit (ASDK), only one region (named local) is

available.

Plans

Base plan

７ Note

If an offer has multiple base plans, the combined storage capacity of the plans

cannot exceed the storage quota.

Add-on plans

Offers are groups of one or more plans that you create so that users can subscribe to

them. For example: Offer Alpha can contain Plan A, which provides a set of compute

services, and Plan B, which provides a set of storage and network services.

When you create an offer, you must include at least one base plan, but you can also

create add-on plans that users can add to their subscription.

When you're planning your offers, keep the following points in mind:

Trial offers: You use trial offers to attract new users, who can then upgrade to additional

services. To create a trial offer, create a small base plan with an optional larger add-on

plan. Alternatively, you can create a trial offer consisting of a small base plan, and a

separate offer with a larger "pay as you go" plan.

Capacity planning: You might be concerned about users who grab large amounts of

resources and clog the system for all users. To help performance, you can configure your

plans with quotas to cap usage.

Delegated providers: You can grant others the ability to create offers in your

environment. For example, if you're a service provider, you can delegate this ability to

your resellers. Or, if you're an organization, you can delegate to other

divisions/subsidiaries.

Subscriptions let users access your offers. If you're an Azure Stack Hub operator for a

service provider, your users (tenants) buy your services by subscribing to your offers. If

you're an Azure Stack Hub operator at an organization, your users (employees) can

subscribe to the services you offer without paying.

Users create new subscriptions and get access to existing subscriptions by signing in to

Azure Stack Hub. Each subscription represents an association with a single offer. The

offer (and its plans and quotas) assigned to one subscription can't be shared with other

subscriptions. Each resource that a user creates is associated with one subscription.

As an Azure Stack Hub operator, you can see information about tenant subscriptions,

but you can't access the contents of those subscriptions unless you are explicitly added

through RBAC by a tenant administrator of that subscription. This allows tenants to

enforce separation of power and responsibilities between Azure Stack Hub operator and

tenant spaces.

Offers

Subscriptions

The exception to this case is a situation in which the subscription owner is unable to

provide the operator with access to the subscription, which requires the administrator to

take ownership of the subscription as discussed in Change the billing owner for an

Azure Stack Hub user subscription.

If your Azure Stack Hub instance is disconnected and you have two different domains

where users in domain 1 create subscriptions that users in domain 2 consume, some

subscriptions may appear in the admin portal but not appear in the user portal. To fix

this, have the users in domain 1 set the correct RBAC for the subscriptions in domain 2.

The default provider subscription is automatically created when you deploy the ASDK.

This subscription can be used to manage Azure Stack Hub, deploy additional resource

providers, and create plans and offers for users. For security and licensing reasons, it

shouldn't be used to run customer workloads and apps. The quota of the default

provider subscription can't be changed.

To learn more about creating plans, offers, and subscriptions, start with Create a plan.

Default provider subscription

Next steps

Create a plan in Azure Stack Hub

Article • 07/29/2022

Azure Stack Hub plans are groupings of one or more services and their quotas. As a

provider, you can create plans to offer to your users. In turn your users subscribe to your

offers to use the plans, services, and quotas they include. This example shows you how

to create a plan that includes the compute, network, and storage resource providers.

This plan gives subscribers the ability to provision virtual machines.

1. Sign in to the Azure Stack Hub administrator portal

https://adminportal.local.azurestack.external .

2. To create a plan and offer that users can subscribe to, select + Create a resource,

then Offers + Plans, then Plan.

3. A tabbed user interface appears that enables you to specify the plan name, add

services, and define quotas for each of the selected services. Most importantly, you

can review the details of the offer you create before you decide to create it.

Under the Basics tab of the New plan window, enter a Display name and a

Resource name. The display name is the plan's friendly name that operators can

see. In the administrator portal, plan details are only visible to operators.

Create a plan (1902 and later)

4. Create a new Resource Group, or select an existing one, as a container for the

plan.

5. Select the Services tab, or click the Next : Services > button, and then select the

checkbox for Microsoft.Compute, Microsoft.Network, and Microsoft.Storage.

6. Select the Quotas tab, or click the Next : Quotas > button. Next to

Microsoft.Storage, choose either the default quota from the dropdown box, or

select Create New to create a customized quota.

7. If you're creating a new quota, enter a Name for the quota, and then specify the

quota values. Select OK to create the quota.

8. Repeat steps 6 and 7 to create and assign quotas for Microsoft.Network and

Microsoft.Compute. When all three services have quotas assigned, they'll look like

the next example.

７ Note

Once a quota has been created and used, its name cannot be changed.

9. Select Review + create to review the plan. Review all values and quotas to ensure

they're correct. The interface enables you to expand the quotas in the chosen plans

one at a time to view the details of each quota in a plan. You can also go back to

make any necessary edits.

10. When you're ready, select Create to create the plan.

11. To see the new plan, on the left-hand side click All services, select Plans, and then

search for the plan and select its name. If your list of resources is long, use Search

to locate your plan by name.

Create an offer

Next steps

Create an offer in Azure Stack Hub

Article • 07/29/2022

Offers are groups of one or more plans that providers present to users, which those

users can buy or subscribe to. This article describes how to create an offer that includes

the plan that you created. This offer gives subscribers the ability to set up virtual

machines (VMs).

1. Sign in to the Azure Stack Hub administrator portal

https://adminportal.local.azurestack.external and select + Create a resource,

then Offers + Plans, and then Offer.

2. A tabbed user interface appears that enables you to define the offer name. You can

also add existing or create new base plans and add-on plans. Most importantly,

you can review the details of the offer you create before you decide to create it.

In the Basics tab, enter a Display Name and a Resource Name, and then under

Resource Group, select Create new or Use existing. The display name is the

friendly name for the offer. This friendly name is the only information about the

offer that users see when they subscribe to an offer in the user portal. Use an

intuitive name that helps users understand what comes with the offer. Only the

Create an offer (1902 and later)

admin can see the resource name. It's the name that admins use to work with the

offer as an Azure Resource Manager resource. In this tab, you can also choose to

make this offer public or keep it private. The default setting is private. You can

change the public or private state of the offer at any time.

3. Select the Base plans tab or click the Next : Base plans > button. Select the plan(s)

you want to include in the offer.

4. At this point you can create an add-on plan to modify the base plan, but this is

optional. You have the opportunity to create an add-on plan in the next article,

Azure Stack Hub add-on plans.

5. Select the Review + create tab. Review the offer summary to ensure that all values

are correct. The interface enables you to expand the quotas in the chosen plans

one at a time to view the details of each quota in a plan. You can also go back to

make any necessary edits.

6. Select Create to create the offer.

Change the state of an offer

After creating the offer, you can change its state. Offers must be made Public for users

to get the full view when they subscribe. Offers can be:

Public: Visible to users.

Private: Only visible to cloud administrators. This setting is useful while drafting the

plan or offer, or if the cloud administrator wants to create each subscription for

users.

Decommissioned: Closed to new subscribers. The cloud administrator can

decommission offers to prevent future subscriptions, but leave current subscribers

unaffected.

There are two ways to change the state of an offer:

1. In All resources, select the name of the offer. On the Overview screen for the offer,

select Change state. Choose the state you want to use (for example, Public).

 Tip

Changes to the offer aren't immediately visible to the user. To see the

changes, users might have to sign out and sign in again to the user portal to

see the new offer.

2. Select Offer settings. Choose the state you want to use (for example, Public), then

select Save.

To learn how to modify an offer and provide your users with an add-on plan,

continue with Create an add-on plan (optional)

Otherwise, jump to Subscribe to an offer

Next steps

Create add-on plans in Azure Stack Hub

Article • 07/29/2022

As an Azure Stack Hub operator, you create add-on plans to modify a base plan when

you want to offer additional services or extend computer, storage, or network quotas

beyond the base plan initial offer. Add-on plans modify the base plan and are optional

extensions that users can choose to enable in their subscription.

There are times when combining everything in a single plan is optimal. Other times you

might want to have a base plan and then offer the additional services by using add-on

plans. For instance, you could decide to offer IaaS services as part of a base plan with all

PaaS services treated as add-on plans.

Another reason to use add-on plans is to help monitor resource usage. To do so, you

could start with a base plan that includes relatively small quotas (depending on the

services required). Then, as users reach capacity, they would be alerted that they've

consumed the allocation of resources based on their assigned plan. From there, the

users can select an add-on plan that provides the additional resources.

Add-on plans are created the same way as a base plan. The difference between the two

is determined when the plan is added to an offer. It's designated as either a base plan or

add-on plan. When you add an add-on plan to an existing offer, the additional

resources can take up to an hour to appear in the subscription.

1. Sign in to the Azure Stack Hub administrator portal as a cloud administrator.

2. Follow the same steps used to create a new base plan to create a new plan offering

services that weren't previously offered.

3. In the administrator portal, select Offers and then select the offer to be updated

with an add-on plan.

７ Note

When you don't want to use an add-on plan to extend a quota, you can also

choose to edit the original configuration of the quota.

Create an add-on plan (1902 and later)

4. At the bottom of the offer properties, select Add-on plans. Select Add.

5. Select the plan to add. In this example, the plan is called 20-storageaccounts. After

selecting the plan, click Select to add the plan to the offer. You should receive a

notification that the plan was added to the offer successfully.

6. Review the list of add-on plans included with the offer to verify that the new addon plan is listed.

Create an offer



N

e

xt

s

t

e

p

s

Create subscriptions to offers in Azure

Stack Hub

Article • 07/29/2022

After you create an offer, users need a subscription to that offer before they can use it.

There are two ways that users can subscribe to an offer:

As a cloud operator, you can create a subscription for a user from within the

administrator portal. Subscriptions you create can be for both public and private

offers.

As a tenant user, you can subscribe to a public offer when you use the user portal.

Cloud operators use the administrator portal to create a subscription to an offer for a

user. Subscriptions can be created for members of your own directory tenant. When

multi-tenancy is enabled, you can also create subscriptions for users in additional

directory tenants.

If you don't want your tenants to create their own subscriptions, make your offers

private, and then create subscriptions for your tenants. This approach is common when

integrating Azure Stack Hub with external billing or service catalog systems.

After you create a subscription for a user, they can sign in to the user portal and see that

they're subscribed to the offer.

1. In the administrator portal, go to User subscriptions.

2. Select Add. Under New user subscription, enter the following information:

Display name - A friendly name for identifying the subscription that appears

as the User subscription name.

User - Specify a user from an available directory tenant for this subscription.

The user name appears as Owner. The format of the user name depends on

your identity solution. For example:

Azure AD: <user1>@<contoso.onmicrosoft.com>

Create a subscription as a cloud operator

To create a subscription for a user

AD FS: <user1>@<azurestack.local>

Directory tenant - Select the directory tenant where the user account

belongs. If you haven't enabled multi-tenancy, only your local directory

tenant is available.

3. Select Offer. Under Offers, choose an Offer for this subscription. Because you're

creating the subscription for a user, select Private as the accessibility state.

4. Select Create to create the subscription. The new subscription appears under User

subscription. When the user signs in to the user portal, they can see the

subscription details.

A cloud operator can add a plan to a previously created subscription at any time:

1. In the administrator portal, select All Services and then under the

ADMINISTRATIVE RESOURCES category, select User subscriptions. Select the

subscription you want to change.

2. Select Add-ons and then select +Add.

3. Under Add plan, select the plan you want as an add-on.

As a user, you can sign in to the user portal to locate and subscribe to public offers and

add-on plans for your directory tenant (organization).

1. Sign in to the Azure Stack Hub user portal and select Get a Subscription.

To make an add-on plan available

Create a subscription as a user

７ Note

If your Azure Stack Hub environment supports multi-tenancy, you can also

subscribe to offers from a remote directory tenant.

To subscribe to an offer

2. Under Get a subscription, enter the friendly name of the subscription in Display

Name. Select Offer and under Choose an offer, pick an offer. Select Create to

create the subscription.

3. After you subscribe to an offer, refresh the portal to see which services are part of

the new subscription.

4. To see the subscription you created, select All services and then under the

GENERAL category select Subscriptions. Select the subscription to see the

subscription details.

If the offer you subscribe to has an add-on plan, you can add that plan to your

subscription at any time.

1. In the user portal, select All services. Next, under the GENERAL category, select

Subscriptions, and then select the subscription that you want change. If there are

add-on plans available, + Add plan is active and shows a tile for Add-on plans.

If + Add plan isn't active, then there are no add-on plans for the offer associated

with that subscription.

2. Select + Add plan or the Add-on plans tile. Under Add-on plans, select the plan

you want to add.

Learn more about how a user can now deploy resources into their subscription:

Several user quickstarts show how to provision Windows and Linux virtual

machines using PowerShell, Azure CLI, and the user portal.

A tutorial that uses an Azure Resource Manager template shows how to deploy an

Ubuntu 16.04 virtual machine running Minikube to manage Kubernetes cluster.

To enable an add-on plan in your subscription

Next steps

Delete quotas, plans, offers, and

subscriptions

Article • 07/29/2022

This article describes how to delete quotas, plans, offers, and subscriptions that you no

longer need. As a general principle, you can delete only what isn't in use. For example,

deleting an offer is only possible if there are no subscriptions that belong to that offer.

Subscriptions are the exception to this general principle: you can delete subscriptions

that contain resources and the resources will be deleted along with the subscription.

If you want to delete a quota, you must work back through any plans and offers that use

that quota. Starting with the offers, ensure they have no subscriptions, delete each offer,

then delete the plans that use the quota, and so on.

To delete a subscription, select All services, then User subscriptions, to display a list of

all subscriptions on the system. If you're working on an offer, you can also select

Subscriptions from there.

You can delete subscriptions from this list, or you can use PowerShell to write a script

that deletes all subscriptions for you. These commands are documented in the

Subscriptions - Delete reference.

To delete an offer, in the administrator portal, go to All services, then Offers. Select the

offer you want to delete, then select Delete.

Delete a subscription

Ｕ Caution

Deleting a subscription also deletes any data and resources it contains.

Delete an offer

You can only delete an offer when there are no subscriptions using it. If subscriptions

exist based on the offer, the Delete option isn't available. In this case, see the Delete a

subscription section.

To delete a plan, in the administrator portal go to All services, then Plans. Select the

plan you want to delete, then select Delete.

You can only delete a plan when there are no offers or subscriptions using it. If there are

offers that use the plan, delete the plan, allow it to fail, and you'll receive an error

Delete a plan

message. You can select Parent offers to display a list of offers that use the plan. For

more information about deleting offers, see Delete an offer.

Plans might have been added directly to a subscription as add-on plans, even if they're

not part of the offer. In this case, they must be removed from the subscriptions that use

them before the plan can be deleted.

Also, a plan can't be removed from a subscription if it's the only source of a given

resource for that subscription. For example, if Plan A has been added to Subscription 1,

and it's the only plan providing a network quota to the subscription, it can't be removed

from the subscription. Therefore, it can't be deleted.

You can view and edit existing quotas using the administrator portal: select Region

Management, then select the relevant resource provider, and then select Quotas. You

can also delete quotas for certain resource providers.

You can also delete some quotas using these REST APIs:

Compute

Network

Storage

Create subscriptions

Provision a virtual machine

Edit and delete a quota

７ Note

You can't delete a quota if there are any current plans that use it. You must first

delete the plan that references the quota.

Next steps

Delegate offers in Azure Stack Hub

Article • 10/11/2021

As an Azure Stack Hub operator, you might want to put other people in charge of

signing up users and creating subscriptions. For example, if you're a service provider,

you might want resellers to sign up customers and manage them on your behalf. Or, if

you're part of a central IT group in an enterprise, you might want to delegate user signup to other IT staff.

Delegation makes it easier to reach and manage more users than you can by yourself, as

shown in the following figure:

With delegation, the delegated provider manages an offer (called a delegated offer), and

end customers obtain subscriptions under that offer without involvement from the

system admin.

The following roles are part of delegation:

The Azure Stack Hub operator manages the Azure Stack Hub infrastructure and

creates an offer template. The operator delegates others to provide offers to their

tenant.

The delegated Azure Stack Hub operators are users with Owner or Contributor

rights in the subscriptions called delegated providers. They can belong to other

Delegation roles

organizations, such as other Azure Active Directory (Azure AD) tenants.

Users sign up for the offers and use them for managing their workloads, creating

VMs, storing data, and so on.

There are two steps to setting up delegation:

1. Create a delegated provider subscription: Subscribe a user to an offer containing

only the subscription service. Users who subscribe to this offer can then extend the

delegated offers to other users by signing them up for those offers.

2. Delegate an offer to the delegated provider: This offer enables the delegated

provider to create subscriptions or to extend the offer to their users. The delegated

provider can now take the offer and extend it to other users.

The following figure shows the steps for setting up delegation:

To act as a delegated provider, a user establishes a relationship with the main provider

by creating a subscription. This subscription identifies the delegated provider as having

the right to present the delegated offers on behalf of the main provider.

After this relationship is established, the Azure Stack Hub operator can delegate an offer

to the delegated provider. The delegated provider can take the offer, rename it (but not

Delegation steps

Delegated provider requirements

change its substance), and offer it to its customers.

The following sections describe the steps to set up a delegated provider, delegate an

offer, and verify that users can sign up for the delegated offer.

To use this walkthrough, you need two Azure AD accounts in addition to your Azure

Stack Hub operator account. If you don't have these two accounts, you must create

them. The accounts can belong to any Azure AD user and are referred to as the

delegated provider and the user.

Role Organizational rights

Delegated provider User

User User

1. Sign in to the administrator portal as an Azure Stack Hub operator.

2. To create an offer that enables a user to become a delegated provider:

a. Create a plan. This plan should include only the subscription service. This article

uses a plan named PlanForDelegation as an example.

b. Create an offer based on this plan. This article uses an offer named OfferToDP as

an example.

c. Add the delegated provider as a subscriber to this offer by selecting

Subscriptions, then Add, then New Tenant Subscription.

Delegation walkthrough

Set up roles

７ Note

In the case of a CSP-reseller, creating this delegated provider requires that these

users are in the tenant directory (the user Azure AD). The Azure Stack Hub operator

must first onboard that tenant Azure AD, and then set up usage and billing by

following these steps.

Identify the delegated provider

The next step is to create the plan and offer that you're going to delegate, and that your

users will use. It's a good idea to define this offer as you want users to see it because the

delegated provider can't change the plans and quotas it includes.

1. As an Azure Stack Hub operator, create a plan and an offer based on the plan. This

article uses an offer named DelegatedOffer as an example.

2. Delegate the offer. Go to DelegatedOffer. Under Settings, select Delegated

Providers, then select Add.

3. Select the subscription for the delegated provider from the drop-down list, and

then select Delegate.

７ Note

As with all Azure Stack Hub offers, you have the option of making the offer

public and letting users sign up for it, or keeping it private and letting the

Azure Stack Hub operator manage the sign-up. Delegated providers are

usually a small group. You want to control who is admitted to it, so keeping

this offer private makes sense in most cases.

Azure Stack Hub operator creates the delegated offer

７ Note

This offer doesn't have to be public, but you can make it public. However, in

most cases, you only want delegated providers to have access to the offer.

After you delegate a private offer as described in the following steps, the

delegated provider has access to it.

Sign in to the user portal as the delegated provider and then create a new offer by using

the delegated offer as a template.

1. Select + Create a resource, then Tenant Offers + Plans, then select Offer.

2. Assign a name to the offer. This example uses ResellerOffer. Select the delegated

offer on which to base it, and then select Create.

Delegated provider customizes the offer

3. The delegated provider can make these offers public through their own portal URL.

To make the offer public, select Browse, and then Offers. Select the offer, and then

select Change State.

4. The public delegated offers are now visible only through the delegated portal. To

find and change this URL:

a. Select Browse, then All services, and then under the GENERAL category, select

Subscriptions. Select the delegated provider subscription (for example,

DPSubscription), then Properties.

b. Copy the portal URL to a separate location, such as Notepad.

） Important

Delegated providers can only choose offers that are delegated to them. They

cannot make changes to those offers; only an Azure Stack Hub operator can

change these offers. For example, only an operator can change their plans and

quotas. A delegated provider does not construct an offer from base plans and

add-on plans.

You've finished creating a delegated offer as a delegated provider. Sign out as the

delegated provider and close the browser window.

1. In a new browser window, go to the delegated portal URL that you saved in the

previous step. Sign in to the portal as a user.

2. In the dashboard, select Get a subscription. You'll see that only the delegated

offers that were created by the delegated provider are presented to the user.

The process of delegating an offer is finished. Now a user can sign up for this offer by

getting a subscription to it.

Sign up for the offer

７ Note

The delegated offers are not visible unless you use the delegated portal.

Move subscriptions between delegated

providers

If needed, a subscription can be moved between new or existing delegated provider

subscriptions that belong to the same directory tenant. You can move them using the

PowerShell cmdlet Move-AzsSubscription.

Moving subscriptions is useful when:

You onboard a new team member that will take on the delegated provider role and

you want to assign to this team member user subscriptions that were previously

created in the default provider subscription.

You have multiple delegated providers subscriptions in the same directory tenant

(Azure AD) and need to move user subscriptions between them. This scenario

could occur when a team member moves between teams and their subscription

must be allocated to the new team.

Provision a VM

Next steps

Quota types in Azure Stack Hub

Article • 05/27/2021

Quotas define the limits of resources that a user subscription can provision or consume.

For example, a quota might allow a user to create up to five virtual machines (VMs).

Each resource can have its own types of quotas.

Type Default

value

Description

Maximum

number of VMs

50 The maximum number of VMs that a subscription can create in this

location.

Maximum

number of VM

cores

100 The maximum number of cores that a subscription can create in

this location (for example, an A3 VM has four cores).

Maximum

number of

availability sets

10 The maximum number of availability sets that can be created in this

location.

Maximum

number of virtual

machine scale

sets

100 The maximum number of scale sets that can be created in this

location.

Maximum

capacity (in GB)

of standard

managed disk

2048 The maximum capacity of standard managed disks that can be

created in this location. This value is a total of the allocation size of

all standard managed disks and the used size of all standard

snapshots.

Maximum

capacity (in GB)

of premium

managed disk

2048 The maximum capacity of premium managed disks that can be

created in this location. This value is a total of the allocation size of

all premium managed disks and the used size of all premium

snapshots.

） Important

It can take up to two hours for new quotas to be available in the user portal or

before a changed quota is enforced.

Compute quota types

７ Note

Item Default

value

Description

Maximum

capacity

(GB)

2048 Total storage capacity that can be consumed by a subscription in this

location. This value is a total of the used size of all blobs (including

unmanaged disks) and all associated snapshots, tables, queues.

Total

number of

storage

accounts

20 The maximum number of storage accounts that a subscription can create

in this location.

Item Default

value

Description

Maximum

virtual

networks

50 The maximum number of virtual networks that a subscription can

create in this location.

Maximum

virtual network

gateways

1 The maximum number of virtual network gateways (VPN gateways)

that a subscription can create in this location.

The maximum capacity of unmanaged disks (page blobs) is separate from the

managed disk quota. You can set this value in Maximum capacity (GB) in Storage

quotas.

Storage quota types

７ Note

When the Maximum capacity (GB) of a subscription is exceeded, you can't create a

new storage resource in the subscription. Although you can still create VMs with

unmanaged disks, doing so may cause your total used capacity to exceed the quota

limit.

The maximum capacity of managed disks is separate from the total storage quota.

You can set the total storage quota in Compute quotas.

Network quota types

Item Default

value

Description

Maximum

network

connections

2 The maximum number of network connections (point-to-point or siteto-site) that a subscription can create across all virtual network

gateways in this location.

Maximum

public IPs

50 The maximum number of public IP addresses that a subscription can

create in this location.

Maximum

NICs

100 The maximum number of network interfaces that a subscription can

create in this location.

Maximum load

balancers

50 The maximum number of load balancers that a subscription can

create in this location.

Maximum

network

security

groups

50 The maximum number of network security groups that a subscription

can create in this location.

Type Default

value

Description

Maximum

number of VM

cores

10 The maximum number of cores that a subscription can create in this

location (for example, an A3 VM has four cores).

There are two different ways to view an existing quota:

1. In the left navigation pane of the administrator portal, select Plans.

2. Select the plan you want to view details for by clicking on its name.

3. In the blade that opens, select Services and quotas.

4. Select the quota you want to see by clicking it in the Name column.

Event Hubs quota types

View an existing quota

Plans

1. On the default dashboard of the administrator portal, find the Resource providers

tile.

2. Select the service with the quota that you want to view, like Compute, Network, or

Storage.

3. Select Quotas, and then select the quota you want to view.

There are two different ways to edit a quota:

1. In the left navigation pane of the administrator portal, select Plans.

2. Select the plan for which you want to edit a quota by clicking on its name.

3. In the blade that opens, select Services and quotas.

4. Select the quota you want to edit by clicking it in the Name column.

5. In the blade that opens, select Edit in Compute, Edit in Network, or Edit in

Storage.



Resource providers

Edit a quota

Edit a plan



Alternatively, you can follow this procedure to edit a quota:

1. On the default dashboard of the administrator portal, find the Resource providers

tile.

2. Select the service with the quota that you want to modify, like Compute, Network,

or Storage.

3. Next, select Quotas, and then select the quota you want to change.

4. On the Set Storage quotas, Set Compute quotas, or Set Network quotas pane

(depending on the type of quota you've chosen to edit), edit the values, and then

select Save.

You can choose to edit the original configuration of a quota instead of using an add-on

plan. When you edit a quota, the new configuration automatically applies globally to all

plans that use that quota and all existing subscriptions that use those plans. The editing

of a quota is different than when you use an add-on plan to provide a modified quota,

which a user chooses to subscribe to.

The new values for the quota apply globally to all plans that use the modified quota and

to all existing subscriptions that use those plans.

Edit original configuration

７ Note

A quota change in a base plan does not impact already-deployed resources.

Therefore, a subscription will not be in violation.

Next steps

Learn more about services, plans, offers, and quotas.

Create quotas while creating a plan.

Use PowerShell to manage

subscriptions, plans, and offers in Azure

Stack Hub

Article • 07/29/2022

You can use PowerShell to configure and deliver services by using offers, plans, and

subscriptions. For instructions on getting set up with PowerShell on Azure Stack Hub,

see Install PowerShell Az module for Azure Stack Hub. For information on connecting to

Azure Stack Hub using PowerShell, see Connect to Azure Stack Hub with PowerShell.

Before you begin, verify the Azure Stack Hub PowerShell module is loaded. In a

PowerShell console, type Import-Module AzureStack .

Quotas are required when creating a plan. You can use an existing quotas or create new

quotas. For example, to create a storage, compute and network quota, you can use the

New-AzsStorageQuota, New-AzsComputeQuota, and New-AzsNetworkQuota cmdlets:

PowerShell

To create or update a base or add-on plan, use New-AzsPlan.

PowerShell

To create an offer, use New-AzsOffer.

Create a plan

$serviceQuotas = @()

$serviceQuotas += (New-AzsStorageQuota -Name "Example storage quota with

defaults").Id

$serviceQuotas += (New-AzsComputeQuota -Name "Example compute quota with

defaults").Id

$serviceQuotas += (New-AzsNetworkQuota -Name "Example network quota with

defaults").Id

$testPlan = New-AzsPlan -Name "testplan" -ResourceGroupName "testrg" -

QuotaIds $serviceQuotas -Description "Test plan"

Create an offer

PowerShell

Once you have an offer, you can add plans to the offer. Use Add-AzsPlanToOffer. The -

PlanLinkType parameter distinguishes the plan type.

PowerShell

If you want to change the state of an offer, use the Set-AzsOffer cmdlet.

PowerShell

After you create an offer, users need a subscription to that offer before they can use it.

There are two ways that users can subscribe to an offer:

As a cloud operator, you can create a subscription for a user. Subscriptions you

create can be for both public and private offers.

As a user, you can subscribe to a public offer.

To create a subscription for a user as a cloud operator, use New-AzsUserSubscription.

PowerShell

To subscribe to a public offer as a user, use New-AzsSubscription. New-AzsSubscription

requires connection to the user Azure Resource Manager environment. Use the steps in

Connect to Azure Stack Hub with PowerShell but use the user Azure Resource Manager

New-AzsOffer -Name "testoffer" -ResourceGroupName "testrg" -BasePlanIds

@($testPlan.Id)

Add-AzsPlanToOffer -PlanName "addonplan" -PlanLinkType Addon -OfferName

"testoffer" -ResourceGroupName "testrg" -MaxAcquisitionCount 18

$offer = Get-AzsAdminManagedOffer -Name "testoffer" -ResourceGroupName

"testrg"

$offer.state = "Public"

$offer | Set-AzsOffer -Confirm:$false

Create subscription to an offer

New-AzsUserSubscription -Owner "user@contoso.com" -DisplayName "User

subscription" -OfferId "/subscriptions/<Subscription

ID>/resourceGroups/testrg/providers/Microsoft.Subscriptions.Admin/offers/tes

toffer"

endpoint. For example, Add-AzEnvironment -Name "AzureStackUser" -ArmEndpoint

"https://management.local.azurestack.external" .

PowerShell

There are companion PowerShell cmdlets to delete Azure Stack Hub quotas, plans,

offers, and subscriptions. The following show examples for each.

Use Remove-AzsUserSubscription to remove a subscription from an offer.

PowerShell

To remove a plan from an offer, use Remove-AzsPlanFromOffer.

PowerShell

Use Remove-AzsPlan to remove a plan.

PowerShell

Use Remove-AzsOffer to remove an offer.

PowerShell

To remove quotas, use Remove-AzsStorageQuota, Remove-AzsComputeQuota, RemoveAzsNetworkQuota .

$testOffer = Get-AzsOffer | Where-Object Name -eq "testoffer"

New-AzsSubscription -OfferId $testOffer.Id -DisplayName "My subscription"

Delete quotas, plans, offers, and subscriptions

Remove-AzsUserSubscription -TargetSubscriptionId "c90173b1-de7a-4b1d-8600-

b8325ca1eab1e"

Remove-AzsPlanFromOffer -PlanName "addonplan" -PlanLinkType Addon -OfferName

"testoffer" -ResourceGroupName "testrg"

Remove-AzsPlanFromOffer -PlanName "testplan" -PlanLinkType Base -OfferName

"testoffer" -ResourceGroupName "testrg"

Remove-AzsPlan -Name "testplan" -ResourceGroupName "testrg"

Remove-AzsOffer -Name "testoffer" -ResourceGroupName "testrg"

PowerShell

Managing updates in Azure Stack Hub

Remove-AzsStorageQuota -Name "Example storage quota with defaults"

Remove-AzsComputeQuota -Name "Example compute quota with defaults"

Remove-AzsNetworkQuota -Name "Example network quota with defaults"

Next steps

Offer a network solution in Azure Stack

Hub with Fortinet FortiGate

Article • 07/29/2022

You can add FortiGate Next-Generation Firewall (NGFW) to your Azure Stack Hub

Marketplace. FortiGate lets your users create network solutions such as a virtual private

network (VPN) to Azure Stack Hub and VNET peering. A network virtual appliance (NVA)

controls the flow of network traffic from a perimeter network to other networks or

subnets.

1. Open the Azure Stack Hub administrator portal.

2. Select Marketplace management and select Add from Azure.

3. Type Forti in the search box, and double-click > select Download to get the latest

available versions of the following items:

Fortinet FortiGate-VM For Azure BYOL

FortiGate NGFW - Single VM Deployment (BYOL)

4. Wait until your marketplace items have a status of Downloaded. The items may

take several minutes to download.

Setup VPN for Azure Stack Hub using FortiGate NVA

How to connect two VNETs through peering

How to establish a VNET to VNET connection with Fortinet FortiGate NVA

Download the required Azure Stack Hub

Marketplace items

Next steps

Azure App Service and Azure Functions

on Azure Stack Hub overview

Article • 07/29/2022

Azure App Service on Azure Stack Hub is a platform-as-a-service (PaaS) offering from

Microsoft Azure available on Azure Stack Hub. The service enables your internal or

external customers to create Web and Azure Functions apps for any platform or device.

They can integrate your apps with on-premises apps and automate their business

processes. Azure Stack Hub cloud operators can run customer apps on fully managed

virtual machines (VMs) with their choice of shared VM resources or dedicated VMs.

Azure App Service enables you to automate business processes and host cloud APIs. As

a single integrated service, Azure App Service lets you combine various components

(like websites, REST APIs, and business processes) into a single solution.

Here are some key features and capabilities of Azure App Service:

Multiple languages and frameworks: Azure App Service has first-class support for

ASP.NET, Node.js, Java, PHP, and Python. You can also run Windows PowerShell

and other scripts or executables on App Service VMs.

DevOps optimization: Set up continuous integration and deployment with GitHub,

local Git, or BitBucket. Promote updates through test and staging environments,

and manage your apps in App Service by using Azure PowerShell or the crossplatform command-line interface (Azure CLI).

Visual Studio integration: Dedicated tools in Visual Studio streamline the work of

creating and deploying apps.

App Service offers several app types, each of which is intended to host a specific

workload:

Web Apps for hosting websites, web apps and REST APIs.

Azure Functions v1 for hosting event driven, serverless workloads.

Why offer Azure App Service on Azure Stack

Hub?

App types in App Service

The word app refers to the hosting resources dedicated to running a workload. Taking

web app as an example, you're probably accustomed to thinking of a web app as both

the compute resources and app code that together deliver functionality to a browser. In

Azure App Service, a web app is the compute resource that Azure Stack Hub provides

for hosting your app code.

Your app can be composed of multiple App Service apps of different kinds. For example,

if your app is composed of a web front end and a REST API back end, you can:

Deploy both (front end and API) to a single web app.

Deploy your front-end code to a web app and your back-end code to an API app.

The App Service resource provider uses the same code that Azure App Service uses, and

thus shares some common concepts. In App Service, the pricing container for apps is

called the App Service plan. It represents the set of dedicated VMs used to hold your

apps. Within a given subscription, you can have multiple App Service plans.

In Azure, there are shared and dedicated workers. A shared worker supports highdensity and multi-tenant app hosting, and there's only one set of shared workers.

Dedicated servers are used by only one tenant and come in three sizes: small, medium,

and large. The needs of on-premises customers can't always be described by using

those terms. In App Service on Azure Stack Hub, resource provider admins define the

worker tiers they want to make available. Based on your unique hosting needs, you can



What is an App Service plan?

define multiple sets of shared workers or different sets of dedicated workers. By using

those worker-tier definitions, they can then define their own pricing SKUs.

Azure App Service on Azure Stack Hub uses the same user interface that Azure App

Service uses. The same is true with the back end. However, some features are disabled in

Azure Stack Hub. The Azure-specific expectations or services that those features require

aren't currently available in Azure Stack Hub.

Prerequisites for deploying App Service on Azure Stack Hub

Install the Azure App Service resource provider

You can also try out other platform as a service (PaaS) services, such as the SQL Server

resource provider and the MySQL resource provider.

Portal features

Next steps

Capacity planning for App Service

server roles in Azure Stack Hub

Article • 07/29/2022

To set up a production-ready deployment of Azure App Service on Azure Stack Hub, you

must plan for the capacity you expect the system to support.

This article provides guidance for the minimum number of compute instances and

compute SKUs you should use for any production deployment.

You can plan your App Service capacity strategy using these guidelines.

App Service server role Minimum recommended number of

instances

Recommended

compute SKU

Controller 2 A4v2

Front End 2 A4\_v2

Management 2 D3\_v2

Publisher 2 A2\_v2

Web Workers - shared 2 A4\_v2

Web Workers - dedicated -

small

2 per tier A1\_v2

Web Workers - dedicated -

medium

2 per tier A2\_v2

Web Workers - dedicated -

large

2 per tier A4\_v2

Recommended minimum: Two instances of A4v2

７ Note

The guidance on recommended compute SKU for roles was updated with the

2020.Q2 release of Azure App Service on Azure Stack Hub to bring standard

deployments in line with Azure deployments.

Controller role

The Azure App Service controller typically experiences low consumption of CPU,

memory, and network resources. However, for high availability, you must have two

controllers. Two controllers are also the maximum number of controllers permitted. You

can create the second web sites controller direct from the installer during deployment.

Recommended minimum: Two instances of A4v\_2

The front-end routes requests to web workers depending on web worker availability. For

high availability, you should have more than one front end, and you can have more than

two. For capacity planning purposes, consider that each core can handle approximately

100 requests per second.

Recommended minimum: Two instances of D3v2

The Azure App classic deployment model role is responsible for the App Service Azure

Resource Manager and API endpoints, portal extensions (admin, tenant, Functions

portal), and the data service. The management server role typically requires only about

4-GB RAM in a production environment. However, it may experience high CPU levels

when many management tasks (such as web site creation) are performed. For high

availability, you should have more than one server assigned to this role, and at least two

cores per server.

Recommended minimum: Two instances of A2v2

If many users are publishing simultaneously, the publisher role may experience heavy

CPU usage. For high availability, make sure more than one publisher role is available.

The publisher only handles FTP/FTPS traffic.

Recommended minimum: Two instances of A4\_v2

For high availability, you should have at least four web worker roles: two for shared web

site mode and two for each dedicated worker tier you plan to offer. The shared and

Front-end role

Management role

Publisher role

Web worker role

dedicated compute modes provide different levels of service to tenants. You might need

more web workers if many of your customers are:

Using dedicated compute mode worker tiers (which are resource-intensive).

Running in shared compute mode.

After a user has created an App Service plan for a dedicated compute mode SKU, the

number of web worker(s) specified in that App Service plan is no longer available to

users.

To provide Azure Functions to users in the consumption plan model, you must deploy

shared web workers.

When deciding on the number of shared web worker roles to use, review these

considerations:

Memory: Memory is the most critical resource for a web worker role. Insufficient

memory impacts web site performance when virtual memory is swapped from disk.

Each server requires about 1.2 GB of RAM for the operating system. RAM above

this threshold can be used to run web sites.

Percentage of active web sites: Typically, about 5 percent of apps in an Azure App

Service on Azure Stack Hub deployment are active. However, the percentage of

apps that are active at any given moment can be higher or lower. With an active

app rate of 5 percent, the maximum number of apps to place in an Azure App

Service on Azure Stack Hub deployment should be less than 20 times the number

of active web sites (5 x 20 = 100).

Average memory footprint: The average memory footprint for apps observed in

production environments is about 70 MB. Using this footprint, the memory

allocated across all web worker role computers or VMs is calculated as follows:

Number of provisioned applications \* 70 MB \* 5% - (number of web worker roles

\* 1044 MB)

For example, if there are 5,000 apps on an environment running 10 web worker

roles, each web worker role VM should have 7060-MB RAM:

5,000 \* 70 \* 0.05 - (10 \* 1044) = 7060 (= about 7 GB)

For info on adding more worker instances, see Adding more worker roles.

Additional considerations for dedicated workers during

upgrade and maintenance

During upgrade and maintenance of workers, Azure App Service on Azure Stack Hub will

perform maintenance on 20% of each worker tier at any one time. Therefore, cloud

admins must always maintain a 20% pool of unallocated workers per worker tier to

ensure their tenants don't experience any loss of service during upgrade and

maintenance. For example, if you have 10 workers in a worker tier you should ensure

that 2 are unallocated to allow upgrade and maintenance. If the full 10 workers become

allocated, you should scale the worker tier up to maintain a pool of unallocated workers.

During upgrade and maintenance, Azure App Service will move workloads to

unallocated workers to ensure the workloads will continue to operate. However, if there

are no unallocated workers available during upgrade then there's potential for tenant

workload downtime. With regards to shared workers, customers don't need to provision

additional workers as the service will allocate tenant apps within available workers

automatically. For high availability, there's a minimum requirement of two workers in

this tier.

Cloud admins can monitor their worker tier allocation in the App Service admin area in

the Azure Stack Hub administrator portal. Navigate to App Service and then select

Worker Tiers in the left-hand pane. The Worker Tiers table shows worker tier name, size,

image used, number of available workers (unallocated), total number of workers in each

tier and the overall state of the worker tier.

For the file server role, you can use a standalone file server for development and testing.

For example, when deploying Azure App Service on the Azure Stack Development Kit

(ASDK) you can use this template . For production purposes, you should use a preconfigured Windows file server, or a pre-configured non-Windows file server.

File server role

In production environments, the file server role experiences intensive disk I/O. Because it

houses all of the content and app files for user web sites, you should preconfigure one

of the following resources for this role:

Windows file server

Windows file server cluster

Non-Windows file server

Non-Windows file server cluster

NAS (Network Attached Storage) device

For more information, see Provision a file server.

Prerequisites for deploying App Service on Azure Stack Hub

Next steps

Azure App Service on Azure Stack

Hub billing overview and FAQ

FAQ

This article shows how cloud operators are billed for offering Azure App Service on

Azure Stack Hub and how they can bill their tenants for using the service.

Azure Stack Hub cloud operators choose to deploy Azure App Service on Azure Stack

Hub onto their Azure Stack Hub stamp to offer the tenant capabilities of Azure App

Service and Azure Functions to their customers. The Azure App Service resource

provider consists of multiple types of roles that can be divided between infrastructure

and worker tiers.

Infrastructure roles aren't billed because they're required for the core operation of the

service. Infrastructure roles can be scaled out as required to support the demands of the

cloud operator's tenants. The infrastructure roles are as follows:

Controllers

Management roles

Publishers

Front ends

Worker tiers consist of two main types: shared and dedicated. Worker usage is billed to

the cloud operator's default provider subscription according to the following criteria.

Shared workers are multi-tenant and host free and shared App Service plans and

consumption-based Azure functions for many tenants. Shared workers emit usage

meters when marked as ready in the Azure App Service resource provider.

Dedicated workers are tied to the App Service plans that tenants create. For example, in

the S1 SKU, tenants can scale to 10 instances by default. When a tenant creates an S1

App Service plan, Azure App Service allocates one of the instances in the small worker

Billing overview

Shared workers

Dedicated workers

tier scale set to that tenant's App Service plan. The assigned worker is then no longer

available to be assigned to any other tenants. If the tenant chooses to scale the App

Service plan to 10 instances, nine more workers are removed from the available pool

and are assigned to the tenant's App Service plan.

Meters are emitted for dedicated workers when they're:

Marked as ready in the Azure App Service resource provider.

Assigned to an App Service plan.

This billing model lets cloud operators provision a pool of dedicated workers ready for

customers to use without paying for the workers until they're effectively reserved by

their tenant's App Service plan.

For example, say you have 20 workers in the small worker tier. Then if you have five

customers that create two S1 App Service plans each, and they each scale the App

Service plan up to two instances, you have no workers available. As a result, there's also

no capacity for any of your customers or new customers to scale out or create new App

Service plans.

Cloud operators can view the current number of available workers per worker tier by

looking at the worker tiers in the Azure App Service configuration on Azure Stack Hub

administration.

Cloud operators can query the Azure Stack Hub Tenant Resource Usage API to retrieve

usage information for their customers. You can find all of the individual meters that App

See customer usage by using the Azure Stack

Hub usage service

Service emits to describe tenant usage in the Usage FAQ. These meters then are used to

calculate the usage per customer subscription to calculate charges.

Licensing for SQL Server and file server infrastructure, required by the Azure App Service

resource provider, is covered here: Prerequisites for deploying App Service on Azure

Stack Hub.

As a cloud operator, you're free to apply your own pricing model to your customers. The

usage service provides the usage metering. You can then use the meter quantity to

charge your customers based on the pricing model you determine. The ability to set

pricing enables operators to differentiate from other Azure Stack Hub operators.

As a cloud operator, you incur costs for offering free and shared SKUs because they're

hosted in shared workers. To minimize that cost, you can choose to scale down the

shared worker tier to a bare minimum.

Frequently asked questions

How do I license the SQL Server and file

server infrastructure required in the

prerequisites?

The usage FAQ lists the tenant meters

but not the prices for those meters.

Where can I find them?

As a CSP, how can I offer free and

shared SKUs for customers to try out

the service?

） Important

The installer defaults for Shared Workers were changed in Azure App Service on

Azure Stack Hub 2020.Q2 for new installations. By default Shared Workers are

For example, to offer free and shared App Service plan SKUs and to offer consumptionbased functions, you need a minimum of one A1 instance available. Shared workers are

multi-tenant, so they can host multiple customer apps, each individually isolated and

protected by the App Service sandbox. By scaling the shared worker tier in this way, you

can limit your outlay to the cost of one vCPU per month.

You can then choose to create a quota for use in a plan, which only offers free and

shared SKUs and limits the number of free and shared App Service plans your customer

can create.

The Azure App Service team created sample PowerShell scripts to assist with querying

the Azure Stack Hub usage service. Cloud operators can use these sample scripts to

prepare their own billing for their tenants. The sample scripts are in the Azure Stack Hub

Tools repository in GitHub. The App Service scripts are in the AppService folder under

Usage .

The sample scripts available are:

Get-AppServiceBillingRecords : This sample fetches Azure App Service on Azure

Stack Hub billing records from the Azure Stack Hub Usage API.

Get-AppServiceSubscriptionUsage : This sample calculates Azure App Service on

Azure Stack Hub usage amounts per subscription. This script calculates usage

amounts based on data from the Usage API and the prices provided per meter by

the cloud operator.

Suspend-UserSubscriptions : This sample suspends or enables subscriptions

based on usage limits specified by the cloud operator.

Azure Stack Hub Tenant Resource Usage API

provisioned using the A4\_v2 compute SKU which can be changed by the operator

at installation time or post install.

Sample scripts to assist with billing

Next steps

Prerequisites for deploying App Service

on Azure Stack Hub

Article • 03/30/2023

Supported Azure Stack Hub version App Service RP version

2301 2302 Installer (release notes)

2206.2.52 2302 Installer (release notes)

2108.2.127 2302 Installer (release notes)

Before you deploy Azure App Service on Azure Stack Hub, you must complete the

prerequisite steps in this article.

This section lists the prerequisites for both integrated system and Azure Stack

Development Kit (ASDK) deployments.

If you've already installed a resource provider, you've likely completed the following

prerequisites, and can skip this section. Otherwise, complete these steps before

continuing:

1. Register your Azure Stack Hub instance with Azure, if you haven't done so. This

step is required as you'll be connecting to and downloading items to marketplace

from Azure.

2. If you're not familiar with the Marketplace Management feature of the Azure Stack

Hub administrator portal, review Download marketplace items from Azure and

） Important

Update Azure Stack Hub to a supported version (or deploy the latest Azure Stack

Development Kit) if necessary, before deploying or updating the App Service

resource provider (RP). Be sure to read the RP release notes to learn about new

functionality, fixes, and any known issues that could affect your deployment.

Before you get started

Resource provider prerequisites

publish to Azure Stack Hub. The article walks you through the process of

downloading items from Azure to the Azure Stack Hub marketplace. It covers both

connected and disconnected scenarios. If your Azure Stack Hub instance is

disconnected or partially connected, there are additional prerequisites to complete

in preparation for installation.

3. Update your Azure Active Directory (Azure AD) home directory. Starting with build

1910, a new application must be registered in your home directory tenant. This app

will enable Azure Stack Hub to successfully create and register newer resource

providers (like Event Hubs and others) with your Azure AD tenant. This is an onetime action that needs to be done after upgrading to build 1910 or newer. If this

step isn't completed, marketplace resource provider installations will fail.

After you've successfully updated your Azure Stack Hub instance to 1910 or

greater, follow the instructions for cloning/downloading the Azure Stack Hub

Tools repository.

Then, follow the instructions for Updating the Azure Stack Hub Azure AD

Home Directory (after installing updates or new Resource Providers) .

1. Download the App Service on Azure Stack Hub deployment helper scripts .

2. Download the App Service on Azure Stack Hub installer .

3. Extract the files from the helper scripts .zip file. The following files and folders are

extracted:

Common.ps1

Create-AADIdentityApp.ps1

Create-ADFSIdentityApp.ps1

Create-AppServiceCerts.ps1

Get-AzureStackRootCert.ps1

BCDR

ReACL.cmd

Modules folder

Installer and helper scripts

７ Note

The deployment helper scripts require the AzureRM PowerShell module. See

Install PowerShell AzureRM module for Azure Stack Hub for installation

details.

GraphAPI.psm1

This section lists the prerequisites for integrated system deployments.

To run the resource provider in production, you must provide the following certificates:

Default domain certificate

API certificate

Publishing certificate

Identity certificate

In addition to specific requirements listed in the following sections, you'll also use a tool

later to test for general requirements. See Validate Azure Stack Hub PKI certificates for

the complete list of validations, including:

File format of .PFX

Key usage set to server and client authentication

and several others

The default domain certificate is placed on the front-end role. User apps for wildcard or

default domain request to Azure App Service use this certificate. The certificate is also

used for source control operations (Kudu).

The certificate must be in .pfx format and should be a three-subject wildcard certificate.

This requirement allows one certificate to cover both the default domain and the SCM

endpoint for source control operations.

Format Example

\*.appservice.<region>.<DomainName>.

<extension>

\*.appservice.redmond.azurestack.external

\*.scm.appservice.<region>.<DomainName>.

<extension>

\*.scm.appservice.redmond.azurestack.external

Certificates and server configuration

(Integrated Systems)

Certificate requirements

Default domain certificate

Format Example

\*.sso.appservice.<region>.<DomainName>.

<extension>

\*.sso.appservice.redmond.azurestack.external

The API certificate is placed on the Management role. The resource provider uses it to

help secure API calls. The certificate for publishing must contain a subject that matches

the API DNS entry.

Format Example

api.appservice.<region>.<DomainName>.

<extension>

api.appservice.redmond.azurestack.external

The certificate for the Publisher role secures the FTPS traffic for app owners when they

upload content. The certificate for publishing must contain a subject that matches the

FTPS DNS entry.

Format Example

ftp.appservice.<region>.<DomainName>.

<extension>

ftp.appservice.redmond.azurestack.external

The certificate for the identity app enables:

Integration between the Azure Active Directory (Azure AD) or Active Directory

Federation Services (AD FS) directory, Azure Stack Hub, and App Service to support

integration with the compute resource provider.

Single sign-on scenarios for advanced developer tools within Azure App Service on

Azure Stack Hub.

The certificate for identity must contain a subject that matches the following format.

Format Example

sso.appservice.<region>.<DomainName>.

<extension>

sso.appservice.redmond.azurestack.external

API certificate

Publishing certificate

Identity certificate

Before deploying the App Service resource provider, you should validate the certificates

to be used by using the Azure Stack Hub Readiness Checker tool available from the

PowerShell Gallery . The Azure Stack Hub Readiness Checker Tool validates that the

generated PKI certificates are suitable for App Service deployment.

As a best practice, when working with any of the necessary Azure Stack Hub PKI

certificates, you should plan enough time to test and reissue certificates if necessary.

Azure App Service requires the use of a file server. For production deployments, the file

server must be configured to be highly available and capable of handling failures.

A reference architecture quickstart template is now available that will deploy a file

server and SQL Server. This template supports Active Directory infrastructure in a virtual

network configured to support a highly available deployment of Azure App Service on

Azure Stack Hub.

Validate certificates

Prepare the file server

Quickstart template for Highly Available file server and SQL Server

） Important

This template is offered as a reference or example of how you can deploy the

prerequisites. Because the Azure Stack Hub Operator manages these servers,

especially in production environments, you should configure the template as

needed or required by your organization.

７ Note

The integrated system instance must be able to download resources from GitHub

in order to complete the deployment.

Steps to deploy a custom file server

） Important

1. Create the following Active Directory global security groups:

FileShareOwners

FileShareUsers

2. Create the following Active Directory accounts as service accounts:

FileShareOwner

FileShareUser

As a security best practice, the users for these accounts (and for all web roles)

should be unique and have strong usernames and passwords. Set the passwords

with the following conditions:

Enable Password never expires.

Enable User cannot change password.

Disable User must change password at next logon.

3. Add the accounts to the group memberships as follows:

Add FileShareOwner to the FileShareOwners group.

Add FileShareUser to the FileShareUsers group.

If you choose to deploy App Service in an existing virtual network, the file server

should be deployed into a separate Subnet from App Service.

７ Note

If you have chosen to deploy a file server using either of the Quickstart templates

mentioned above, you can skip this section as the file servers are configured as part

of the template deployment.

Provision groups and accounts in Active Directory

Provision groups and accounts in a workgroup

７ Note

When you're configuring a file server, run all the following commands from an

Administrator Command Prompt.

Don't use PowerShell.

When you use the Azure Resource Manager template, the users are already created.

1. Run the following commands to create the FileShareOwner and FileShareUser

accounts. Replace <password> with your own values.

DOS

2. Set the passwords for the accounts to never expire by running the following WMIC

commands:

DOS

3. Create the local groups FileShareUsers and FileShareOwners, and add the accounts

in the first step to them:

DOS

The content share contains tenant website content. The procedure to provision the

content share on a single file server is the same for both Active Directory and

workgroup environments. But it's different for a failover cluster in Active Directory.

On a single file server, run the following commands at an elevated command prompt.

Replace the value for C:\WebSites with the corresponding paths in your environment.

DOS

net user FileShareOwner <password> /add /expires:never /passwordchg:no

net user FileShareUser <password> /add /expires:never /passwordchg:no

WMIC USERACCOUNT WHERE "Name='FileShareOwner'" SET

PasswordExpires=FALSE

WMIC USERACCOUNT WHERE "Name='FileShareUser'" SET PasswordExpires=FALSE

net localgroup FileShareUsers /add

net localgroup FileShareUsers FileShareUser /add

net localgroup FileShareOwners /add

net localgroup FileShareOwners FileShareOwner /add

Provision the content share

Provision the content share on a single file server (Active Directory

or workgroup)

Run the following commands at an elevated command prompt on the file server or on

the failover cluster node, which is the current cluster resource owner. Replace values in

italics with values that are specific to your environment.

DOS

DOS

set WEBSITES\_SHARE=WebSites

set WEBSITES\_FOLDER=C:\WebSites

md %WEBSITES\_FOLDER%

net share %WEBSITES\_SHARE% /delete

net share %WEBSITES\_SHARE%=%WEBSITES\_FOLDER% /grant:Everyone,full

Configure access control to the shares

Active Directory

set DOMAIN=<DOMAIN>

set WEBSITES\_FOLDER=C:\WebSites

icacls %WEBSITES\_FOLDER% /reset

icacls %WEBSITES\_FOLDER% /grant Administrators:(OI)(CI)(F)

icacls %WEBSITES\_FOLDER% /grant %DOMAIN%\FileShareOwners:(OI)(CI)(M)

icacls %WEBSITES\_FOLDER% /inheritance:r

icacls %WEBSITES\_FOLDER% /grant %DOMAIN%\FileShareUsers:(CI)(S,X,RA)

icacls %WEBSITES\_FOLDER% /grant \*S-1-1-0:(OI)(CI)(IO)(RA,REA,RD)

Workgroup

set WEBSITES\_FOLDER=C:\WebSites

icacls %WEBSITES\_FOLDER% /reset

icacls %WEBSITES\_FOLDER% /grant Administrators:(OI)(CI)(F)

icacls %WEBSITES\_FOLDER% /grant FileShareOwners:(OI)(CI)(M)

icacls %WEBSITES\_FOLDER% /inheritance:r

icacls %WEBSITES\_FOLDER% /grant FileShareUsers:(CI)(S,X,RA)

icacls %WEBSITES\_FOLDER% /grant \*S-1-1-0:(OI)(CI)(IO)(RA,REA,RD)

Prepare the SQL Server instance

７ Note

For the Azure App Service on Azure Stack Hub hosting and metering databases, you

must prepare a SQL Server instance to hold the App Service databases.

For production and high-availability purposes, you should use a full version of SQL

Server 2014 SP2 or later, enable mixed-mode authentication, and deploy in a highly

available configuration.

The SQL Server instance for Azure App Service on Azure Stack Hub must be accessible

from all App Service roles. You can deploy SQL Server within the Default Provider

Subscription in Azure Stack Hub. Or you can make use of the existing infrastructure

within your organization (as long as there's connectivity to Azure Stack Hub). If you're

using an Azure Marketplace image, remember to configure the firewall accordingly.

The App Service installer will check to ensure the SQL Server has database containment

enabled. To enable database containment on the SQL Server that will host the App

Service databases, run these SQL commands:

SQL

If you've chosen to deploy the Quickstart template for Highly Available File Server

and SQL Server, you can skip this section as the template deploys and configures

SQL Server in a HA configuration.

７ Note

A number of SQL IaaS VM images are available through the Marketplace

Management feature. Make sure you always download the latest version of the SQL

IaaS Extension before you deploy a VM using a Marketplace item. The SQL images

are the same as the SQL VMs that are available in Azure. For SQL VMs created from

these images, the IaaS extension and corresponding portal enhancements provide

features such as automatic patching and backup capabilities.

For any of the SQL Server roles, you can use a default instance or a named instance.

If you use a named instance, be sure to manually start the SQL Server Browser

service and open port 1434.

sp\_configure 'contained database authentication', 1;

GO

RECONFIGURE;

GO

This section lists the prerequisites for ASDK deployments.

The Create-AppServiceCerts.ps1 script works with the Azure Stack Hub certificate

authority to create the four certificates that App Service needs.

File name Use

\_.appservice.local.azurestack.external.pfx App Service default SSL certificate

api.appservice.local.azurestack.external.pfx App Service API SSL certificate

ftp.appservice.local.azurestack.external.pfx App Service publisher SSL certificate

sso.appservice.local.azurestack.external.pfx App Service identity application certificate

To create the certificates, follow these steps:

1. Sign in to the ASDK host using the AzureStack\AzureStackAdmin account.

2. Open an elevated PowerShell session.

3. Run the Create-AppServiceCerts.ps1 script from the folder where you extracted the

helper scripts. This script creates four certificates in the same folder as the script

that App Service needs for creating certificates.

4. Enter a password to secure the .pfx files, and make a note of it. You must enter it

later, in the App Service on Azure Stack Hub installer.

Parameter Required or

optional

Default value Description

pfxPassword Required Null Password that helps protect the

certificate private key

DomainName Required local.azurestack.external Azure Stack Hub region and

domain suffix

Certificates and server configuration (ASDK)

Certificates required for ASDK deployment of Azure App

Service

Create-AppServiceCerts.ps1 script parameters

Quickstart template for file server for deployments of

Azure App Service on ASDK.

For ASDK deployments only, you can use the example Azure Resource Manager

deployment template to deploy a configured single-node file server. The single-node

file server will be in a workgroup.

For the Azure App Service on Azure Stack Hub hosting and metering databases, you

must prepare a SQL Server instance to hold the App Service databases.

For ASDK deployments, you can use SQL Server Express 2014 SP2 or later. SQL Server

must be configured to support Mixed Mode authentication because App Service on

Azure Stack Hub DOES NOT support Windows Authentication.

The SQL Server instance for Azure App Service on Azure Stack Hub must be accessible

from all App Service roles. You can deploy SQL Server within the Default Provider

Subscription in Azure Stack Hub. Or you can make use of the existing infrastructure

within your organization (as long as there's connectivity to Azure Stack Hub). If you're

using an Azure Marketplace image, remember to configure the firewall accordingly.

The App Service installer will check to ensure the SQL Server has database containment

enabled. To enable database containment on the SQL Server that will host the App

Service databases, run these SQL commands:

７ Note

The ASDK instance must be able to download resources from GitHub in order to

complete the deployment.

SQL Server instance

７ Note

A number of SQL IaaS VM images are available through the Marketplace

Management feature. Make sure you always download the latest version of the SQL

IaaS Extension before you deploy a VM using a Marketplace item. The SQL images

are the same as the SQL VMs that are available in Azure. For SQL VMs created from

these images, the IaaS extension and corresponding portal enhancements provide

features such as automatic patching and backup capabilities.

For any of the SQL Server roles, you can use a default instance or a named instance.

If you use a named instance, be sure to manually start the SQL Server Browser

service and open port 1434.

SQL

Azure App Service on Azure Stack Hub requires a file server and SQL Server to operate.

You're free to use pre-existing resources located outside of your Azure Stack Hub

deployment or deploy resources within their Azure Stack Hub Default Provider

Subscription.

If you choose to deploy the resources within your Azure Stack Hub Default Provider

Subscription, the licenses for those resources (Windows Server Licenses and SQL Server

Licenses) are included in the cost of Azure App Service on Azure Stack Hub subject to

the following constraints:

the infrastructure is deployed into the Default Provider Subscription;

the infrastructure is exclusively used by the Azure App Service on Azure Stack Hub

resource provider. No other workloads, administrative (other resource providers,

for example: SQL-RP) or tenant (for example: tenant apps, which require a

database), are permitted to make use of this infrastructure.

Cloud operators are responsible for the maintenance and operation of the File Server

and SQL Server. The resource provider does not manage these resources. The cloud

operator is responsible for backing up the App Service databases and tenant content file

share.

Open an elevated PowerShell session on a computer that can reach the privileged

endpoint on the Azure Stack Hub Integrated System or ASDK Host.

sp\_configure 'contained database authentication', 1;

GO

RECONFIGURE;

GO

Licensing concerns for required file server and

SQL Server

Operational responsibility of file and sql servers

Retrieve the Azure Resource Manager root

certificate for Azure Stack Hub

Run the Get-AzureStackRootCert.ps1 script from the folder where you extracted the

helper scripts. The script creates a root certificate in the same folder as the script that

App Service needs for creating certificates.

When you run the following PowerShell command, you have to provide the privileged

endpoint and the credentials for the AzureStack\CloudAdmin.

PowerShell

Parameter Required or

optional

Default value Description

PrivilegedEndpoint Required AzS-ERCS01 Privileged endpoint

CloudAdminCredential Required AzureStack\CloudAdmin Domain account credential

for Azure Stack Hub cloud

admins

Azure App Service on Azure Stack Hub lets you deploy the resource provider to an

existing virtual network or lets you create a virtual network as part of the deployment.

Using an existing virtual network enables the use of internal IPs to connect to the file

server and SQL Server required by Azure App Service on Azure Stack Hub. The virtual

Get-AzureStackRootCert.ps1

Get-AzureStackRootCert.ps1 script parameters

Network and identity configuration

Virtual network

７ Note

The precreation of a custom virtual network is optional as the Azure App Service on

Azure Stack Hub can create the required virtual network but will then need to

communicate with SQL and File Server via public IP addresses. Should you use the

App Service HA File Server and SQL Server Quickstart template to deploy the prerequisite SQL and File Server resources, the template will also deploy a virtual

network.

network must be configured with the following address range and subnets before

installing Azure App Service on Azure Stack Hub:

Virtual network - /16

Subnets

ControllersSubnet /24

ManagementServersSubnet /24

FrontEndsSubnet /24

PublishersSubnet /24

WorkersSubnet /21

Azure App Service uses an Identity Application (Service Principal) to support the

following operations:

Virtual machine scale set integration on worker tiers.

SSO for the Azure Functions portal and advanced developer tools (Kudu).

Depending on which identity provider the Azure Stack Hub is using, Azure Active

Directory (Azure AD) or Active Directory Federation Services (ADFS) you must follow the

appropriate steps below to create the service principal for use by the Azure App Service

on Azure Stack Hub resource provider.

Follow these steps to create the service principal in your Azure AD tenant:

1. Open a PowerShell instance as azurestack\AzureStackAdmin.

2. Go to the location of the scripts that you downloaded and extracted in the

prerequisite step.

3. Install PowerShell for Azure Stack Hub.

4. Run the Create-AADIdentityApp.ps1 script. When you're prompted, enter the

Azure AD tenant ID that you're using for your Azure Stack Hub deployment. For

example, enter myazurestack.onmicrosoft.com.

） Important

If you choose to deploy App Service in an existing virtual network the SQL Server

should be deployed into a separate Subnet from App Service and the File Server.

Create an Identity Application to Enable SSO Scenarios

Create an Azure AD App

5. In the Credential window, enter your Azure AD service admin account and

password. Select OK.

6. Enter the certificate file path and certificate password for the certificate created

earlier. The certificate created for this step by default is

sso.appservice.local.azurestack.external.pfx.

7. Make note of the application ID that's returned in the PowerShell output. You use

the ID in the following steps to provide consent for the application's permissions,

and during installation.

8. Open a new browser window, and sign in to the Azure portal as the Azure Active

Directory service admin.

9. Open the Azure Active Directory service.

10. Select App Registrations in the left pane.

11. Search for the application ID you noted in step 7.

12. Select the App Service application registration from the list.

13. Select API permissions in the left pane.

14. Select Grant admin consent for <tenant>, where <tenant> is the name of your

Azure AD tenant. Confirm the consent grant by selecting Yes.

PowerShell

Parameter Required

or

optional

Default

value

Description

DirectoryTenantName Required Null Azure AD tenant ID. Provide the GUID or

string. An example is

myazureaaddirectory.onmicrosoft.com.

AdminArmEndpoint Required Null Admin Azure Resource Manager endpoint.

An example is

adminmanagement.local.azurestack.external.

TenantARMEndpoint Required Null Tenant Azure Resource Manager endpoint.

An example is

management.local.azurestack.external.

AzureStackAdminCredential Required Null Azure AD service admin credential.

CertificateFilePath Required Null Full path to the identity application

certificate file generated earlier.

CertificatePassword Required Null Password that helps protect the certificate

private key.

Create-AADIdentityApp.ps1

Parameter Required

or

optional

Default

value

Description

Environment Optional AzureCloud The name of the supported Cloud

Environment in which the target Azure

Active Directory Graph Service is available.

Allowed values: 'AzureCloud',

'AzureChinaCloud', 'AzureUSGovernment',

'AzureGermanCloud'.

1. Open a PowerShell instance as azurestack\AzureStackAdmin.

2. Go to the location of the scripts that you downloaded and extracted in the

prerequisite step.

3. Install PowerShell for Azure Stack Hub.

4. Run the Create-ADFSIdentityApp.ps1 script.

5. In the Credential window, enter your AD FS cloud admin account and password.

Select OK.

6. Provide the certificate file path and certificate password for the certificate created

earlier. The certificate created for this step by default is

sso.appservice.local.azurestack.external.pfx.

PowerShell

Parameter Required

or

optional

Default

value

Description

AdminArmEndpoint Required Null Admin Azure Resource Manager endpoint. An

example is

adminmanagement.local.azurestack.external.

PrivilegedEndpoint Required Null Privileged endpoint. An example is AzS-ERCS01.

CloudAdminCredential Required Null Domain account credential for Azure Stack Hub

cloud admins. An example is

Azurestack\CloudAdmin.

CertificateFilePath Required Null Full path to the identity application's certificate

PFX file.

Create an ADFS app

Create-ADFSIdentityApp.ps1

Parameter Required

or

optional

Default

value

Description

CertificatePassword Required Null Password that helps protect the certificate private

key.

Azure App Service on Azure Stack Hub requires items to be downloaded from the Azure

Marketplace, making them available in the Azure Stack Hub Marketplace. These items

must be downloaded before you start the deployment or upgrade of Azure App Service

on Azure Stack Hub:

1. The latest version of Windows Server 2022 Datacenter VM image.

2. Custom Script Extension v1.9.1 or greater. This item is a VM extension.

Install the App Service resource provider

Download items from the Azure Marketplace

） Important

Windows Server Core is not a supported platform image for use with Azure App

Service on Azure Stack Hub.

Do not use evaluation images for production deployments.

Azure App Service on Azure Stack 2022 H1

Next steps

Deploy App Service in Azure Stack Hub

Article • 10/25/2022

Supported Azure Stack Hub version App Service RP version

2301 2302 Installer (release notes)

2206.2.52 2302 Installer (release notes)

2108.2.127 2302 Installer (release notes)

In this article you learn how to deploy App Service in Azure Stack Hub, which gives your

users the ability to create Web, API and Azure Functions applications. You need to:

Add the App Service resource provider to your Azure Stack Hub deployment using

the steps described in this article.

After you install the App Service resource provider, you can include it in your offers

and plans. Users can then subscribe to get the service and start creating apps.

Installing the App Service resource provider takes at least an hour. The length of

time needed depends on how many role instances you deploy. During the

） Important

Update Azure Stack Hub to a supported version (or deploy the latest Azure Stack

Development Kit) if necessary, before deploying or updating the App Service

resource provider (RP). Be sure to read the RP release notes to learn about new

functionality, fixes, and any known issues that could affect your deployment.

） Important

Before you run the resource provider installer, you must complete the steps in

Before you get started

Azure App Service on Azure Stack 2022 H1

Run the App Service resource provider

installer

deployment, the installer runs the following tasks:

Registers the required resource providers in the Default Provider Subscription

Grants contributor access to the App Service Identity application

Create Resource Group and Virtual network (if necessary)

Create Storage accounts and containers for App Service installation artifacts,

usage service, and resource hydration

Download App Service artifacts and upload them to the App Service storage

account

Deploy the App Service

Register the usage service

Create DNS Entries for App Service

Register the App Service admin and tenant resource providers

Register Gallery Items - Web, API, Function App, App Service Plan, WordPress,

DNN, Orchard, and Django applications

To deploy App Service resource provider, follow these steps:

1. Run appservice.exe as an admin from a computer that can access the Azure

Stack Hub Admin Azure Resource Management Endpoint.

2. Select Deploy App Service or upgrade to the latest version.

3. Review and accept the Microsoft Software License Terms and then select Next.

4. Review and accept the third-party license terms and then select Next.

5. Make sure that the App Service cloud configuration information is correct. If

you used the default settings during ASDK deployment, you can accept the

default values. But, if you customized the options when you deployed the

ASDK, or are deploying on an Azure Stack Hub integrated system, you must

edit the values in this window to reflect the differences.

For example, if you use the domain suffix mycloud.com, your Azure Stack Hub

Tenant Azure Resource Manager endpoint must change to management.

<region>.mycloud.com. Review these settings, and then select Next to save

the settings.

6. On the next App Service Installer page you will connect to your Azure Stack

Hub:

a. Select the connection method you wish to use - Credential or Service

Principal

Credential

If you're using Azure Active Directory (Azure AD), enter the Azure

AD admin account and password that you provided when you

deployed Azure Stack Hub. Select Connect.

If you're using Active Directory Federation Services (AD FS), provide

your admin account. For example, cloudadmin@azurestack.local.

Enter your password, and then select Connect.

Service Principal

The service principal that you use must have Owner rights on the

Default Provider Subscription

Provide the Service Principal ID, Certificate File, and Password and

select Connect.

b. In Azure Stack Hub Subscriptions, select the Default Provider

Subscription. Azure App Service on Azure Stack Hub must be deployed in

the Default Provider Subscription.

c. In the Azure Stack Hub Locations, select the location that corresponds to

the region you're deploying to. For example, select local if you're deploying

to the ASDK.

d. Administrators can specify a three character Deployment Prefix for the

individual instances in each Virtual Machine Scale Set that are deployed.

This is useful if managing multiple Azure Stack Hub instances.

7. Now you can deploy into an existing virtual network that you configured using

these steps, or let the App Service installer create a new virtual network and

subnets. To create a VNet, follow these steps:

a. Select Create VNet with default settings, accept the defaults, and then

select Next.

b. Alternatively, select Use existing VNet and Subnets. Complete the following

actions:

Select the Resource Group that contains your virtual network.

Choose the Virtual Network name that you want to deploy to.

Select the correct Subnet values for each of the required role subnets.

Select Next.

8. Enter the info for your file share and then select Next. The address of the file

share must use the Fully Qualified Domain Name (FQDN) or the IP address of

your File Server. For example,

\\appservicefileserver.local.cloudapp.azurestack.external\websites, or

\\10.0.0.1\websites. If you're using a file server, which is domain joined, you

must provide the full username including domain. For example,

myfileserverdomain\FileShareOwner.

７ Note

The installer tries to test connectivity to the file share before proceeding.

But, if you're deploying to an existing virtual network, this connectivity

test might fail. You're given a warning and a prompt to continue. If the

file share info is correct, continue the deployment.

9. On the next App Service Installer page, follow these steps:

a. In the Identity Application ID box, enter the GUID for the Identity

application you created as part of the pre-requisites.

b. In the Identity Application certificate file box, enter (or browse to) the

location of the certificate file.

c. In the Identity Application certificate password box, enter the password for

the certificate. This password is the one that you made note of when you used

the script to create the certificates.

d. In the Azure Resource Manager root certificate file box, enter (or browse

to) the location of the certificate file.

e. Select Next.

10. For each of the three certificate file boxes, select Browse and navigate to the

appropriate certificate file. You must provide the password for each certificate.

These certificates are the ones that you created in Prerequisites for deploying

App Service on Azure Stack Hub. Select Next after entering all the information.

Box Certificate file name example

App Service default SSL certificate file \_.appservice.local.AzureStack.external.pfx

App Service API SSL certificate file api.appservice.local.AzureStack.external.pfx

App Service Publisher SSL certificate file ftp.appservice.local.AzureStack.external.pfx

If you used a different domain suffix when you created the certificates, your

certificate file names don't use local.AzureStack.external. Instead, use your

custom domain info.

11. Enter the SQL Server details for the server instance used to host the App

Service resource provider database and then select Next. The installer

validates the SQL connection properties.

The App Service installer tries to test connectivity to the SQL Server before

proceeding. If you're deploying to an existing virtual network, this connectivity

test might fail. You're given a warning and a prompt to continue. If the SQL

Server info is correct, continue the deployment.

12. Review the role instance and SKU options. The defaults populate with the

minimum number of instances and the minimum SKU for each role in a

production deployment. For ASDK deployment, you can scale the instances

down to lower SKUs to reduce the core and memory commit but you will

experience a performance degradation. A summary of vCPU and memory

requirements is provided to help plan your deployment. After you make your

selections, select Next.

Role Minimum

instances

Minimum SKU Notes

Controller 2 Standard\_A4\_v2

- (4 cores, 8192

MB)

Manages and maintains the health of

the App Service cloud.

Management 1 Standard\_D3\_v2

- (4 cores,

14336 MB)

Manages the App Service Azure

Resource Manager and API endpoints,

portal extensions (admin, tenant,

Functions portal), and the data service.

To support failover, increase the

recommended instances to 2.

Publisher 1 Standard\_A2\_v2

- (2 cores, 4096

MB)

Publishes content via FTP and web

deployment.

FrontEnd 1 Standard\_A4\_v2

- (4 cores, 8192

MB)

Routes requests to App Service apps.

Shared

Worker

1 Standard\_A4\_v2

- (4 cores, 8192

MB)

Hosts web or API apps and Azure

Functions apps. You might want to add

more instances. As an operator, you

can define your offering and choose

any SKU tier. The tiers must have a

minimum of one vCPU.

７ Note

For production deployments, following the guidance in Capacity

planning for Azure App Service server roles in Azure Stack Hub.

13. In the Select Platform Image box, choose your deployment Windows Server

2022 virtual machine (VM) image from the images available in the compute

resource provider for the App Service cloud. Select Next.

14. On the next App Service Installer page, follow these steps:

a. Enter the Worker Role VM admin user name and password.

b. Enter the Other Roles VM admin user name and password.

c. Select Next.

７ Note

Windows Server 2022 Core isn't a supported platform image for use

with Azure App Service on Azure Stack Hub. Don't use evaluation

images for production deployments.

15. On the App Service Installer summary page, follow these steps:

a. Verify the selections you made. To make changes, use the Previous buttons

to visit previous pages.

b. If the configurations are correct, select the check box.

c. To start the deployment, select Next.

16. On the next App Service Installer page, follow these steps:

a. Track the installation progress. App Service on Azure Stack Hub can take up

to 240 minutes to deploy based on the default selections and age of the base

Windows 2016 Datacenter image.

b. After the installer successfully finishes, select Exit.

If you're deploying to an existing virtual network and using an internal IP address to

connect to your file server, you must add an outbound security rule. This rule

enables SMB traffic between the worker subnet and the file server. In the

administrator portal, go to the WorkersNsg Network Security Group and add an

outbound security rule with the following properties:

Source: Any

Source port range: \*

Destination: IP addresses

Destination IP address range: Range of IPs for your file server

Destination port range: 445

Protocol: TCP

Action: Allow

Post-deployment Steps

） Important

If you've provided the App Service RP with a SQL Always On Instance you must

add the appservice\_hosting and appservice\_metering databases to an

availability group and synchronize the databases to prevent any loss of service

in the event of a database failover.

Priority: 700

Name: Outbound\_Allow\_SMB445

To remove latency when workers are communicating with the file server we also

advise adding the following rule to the Worker NSG to allow outbound LDAP and

Kerberos traffic to your Active Directory Controllers if securing the file server using

Active Directory, for example if you have used the Quickstart template to deploy a

HA File Server and SQL Server.

Go to the WorkersNsg in the Admin Portal and add an outbound security rule with

the following properties:

Source: Any

Source port range: \*

Destination: IP Addresses

Destination IP address range: Range of IPs for your AD Servers, for example

with the Quickstart template 10.0.0.100, 10.0.0.101

Destination port range: 389,88

Protocol: Any

Action: Allow

Priority: 710

Name: Outbound\_Allow\_LDAP\_and\_Kerberos\_to\_Domain\_Controllers

1. In the Azure Stack Hub administrator portal, go to Administration - App

Service.

2. In the overview, under status, check to see that the Status displays All roles

are ready.

Validate the App Service on Azure Stack Hub

installation

After you deploy and register the App Service resource provider, test it to make

sure that users can deploy web and API apps.

To create a test web app, follow these steps:

Test drive App Service on Azure Stack Hub

７ Note

You need to create an offer that has the Microsoft.Web namespace in the plan.

You also need a tenant subscription that subscribes to the offer. For more info,

see Create offer and Create plan.

You must have a tenant subscription to create apps that use App Service on

Azure Stack Hub. The only tasks that a service admin can complete in the

administrator portal are related to the resource provider administration of App

Service. This includes adding capacity, configuring deployment sources, and

adding Worker tiers and SKUs.

To create web, API, and Azure Functions apps, you must use the user portal

and have a tenant subscription.

1. In the Azure Stack Hub user portal, select + Create a resource > Web +

Mobile > Web App.

2. Under Web App, enter a name in Web app.

3. Under Resource Group, select New. Enter a name for the Resource Group.

4. Select App Service plan/Location > Create New.

5. Under App Service plan, enter a name for the App Service plan.

6. Select Pricing tier > Free-Shared or Shared-Shared > Select > OK > Create.

7. A tile for the new web app appears on the dashboard. Select the tile.

8. On Web App, select Browse to view the default website for this app.

1. In the Azure Stack Hub user portal, select +, go to the Azure Marketplace,

deploy a Django website, and then wait for the deployment to finish. The

Django web platform uses a file system-based database. It doesn't require any

additional resource providers, such as SQL or MySQL.

2. If you also deployed a MySQL resource provider, you can deploy a WordPress

website from the Marketplace. When you're prompted for database

parameters, enter the user name as User1@Server1, with the user name and

server name of your choice.

3. If you also deployed a SQL Server resource provider, you can deploy a DNN

website from the Marketplace. When you're prompted for database

parameters, choose a database in the computer running SQL Server that's

connected to your resource provider.

Prepare for additional admin operations for App Service on Azure Stack Hub:

Capacity Planning

Configure Deployment Sources

Deploy a WordPress, DNN, or Django

website (optional)

Next steps

Update Azure App Service on Azure

Stack Hub

Article • 10/25/2022

Supported Azure Stack Hub version App Service RP version

2301 2302 Installer (release notes)

2206.2.52 2302 Installer (release notes)

2108.2.127 2302 Installer (release notes)

In this article, you learn how to upgrade the Azure App Service resource provider

deployed in an internet-connected Azure Stack Hub environment.

During this process, the upgrade will:

Detect prior deployment of Azure App Service.

Prepare all update packages and new versions of all OSS Libraries to be deployed.

Upload to storage.

Upgrade all Azure App Service roles (Controllers, Management, Front-End,

Publisher, and Worker roles).

Update Azure App Service scale set definitions.

） Important

Update Azure Stack Hub to a supported version (or deploy the latest Azure Stack

Development Kit) if necessary, before deploying or updating the App Service

resource provider (RP). Be sure to read the RP release notes to learn about new

functionality, fixes, and any known issues that could affect your deployment.

） Important

Prior to running the upgrade, you must complete deployment of Azure App

Service on Azure Stack Hub.

Run the Azure App Service resource provider

installer

Update Azure App Service resource provider manifest.

To upgrade your deployment of Azure App Service on Azure Stack Hub, follow these

steps:

1. Download the Azure App Service Installer .

2. Run appservice.exe as an admin.

3. Select Deploy Azure App Service or upgrade to the latest version.

4. Review and accept the Microsoft Software License Terms and then select Next.

5. Review and accept the third-party license terms and then select Next.

6. Make sure that the Azure Stack Hub Azure Resource Manager endpoint and

Active Directory Tenant info is correct. If you used the default settings during

ASDK deployment, you can accept the default values here. However, if you

customized the options when you deployed Azure Stack Hub, you must edit

the values in this window. For example, if you use the domain suffix

） Important

The Azure App Service installer must be run on a machine which can reach the

Azure Stack Hub admin Azure Resource Manager endpoint.

Azure App Service on Azure Stack 2022 H1

mycloud.com, your Azure Stack Hub Azure Resource Manager endpoint must

change to management.region.mycloud.com. After you confirm your info,

select Next.

7. On the next page:

a. Select the connection method you wish to use - Credential or Service

Principal

Credential

If you're using Azure Active Directory (Azure AD), enter the Azure

AD admin account, and password that you provided when you

deployed Azure Stack Hub. Select Connect.

If you're using Active Directory Federation Services (AD FS), provide

your admin account. For example, cloudadmin@azurestack.local.

Enter your password, and then select Connect.

Service Principal

The service principal that you use must have Owner rights on the

Default Provider Subscription

Provide the Service Principal ID, Certificate File, and Password and

select Connect.

b. In Azure Stack Hub Subscriptions, select the Default Provider

Subscription. Azure App Service on Azure Stack Hub must be deployed in

the Default Provider Subscription.

c. In the Azure Stack Hub Locations, select the location that corresponds to

the region you're deploying to. For example, select local if you're deploying

to the ASDK.

d. If an existing Azure App Service deployment is detected, then the resource

group and storage account are populated and unavailable.

e. NEW: Administrators can specify a three character Deployment Prefix for

the individual instances in each Virtual Machine Scale Set that are

deployed. This is useful if managing multiple Azure Stack Hub instances.

8. In the next screen, you'll see the results of a status check performed against

the App Service Resource Provider. This status check has been added to verify

the deployment is in the correct state to be upgraded. The status check

verifies that all roles are ready, all worker tiers are valid, all virtual machine

scale sets are healthy and verifies access to the App Service secrets.

9. The Platform Image and SKU screen gives Administrators the opportunity to

choose the correct Windows 2022 Platform image to be used to deploy the

new role instances.

a. Select the correct Platform Image

b. Over time the minimum recommended spec of VM/VM Scale Set instance

SKUs has changed and here you see the details of what is currently

deployed and the new recommended SKU.

10. On the summary page:

a. Verify the selections you made. To make changes, use the Previous buttons

to visit previous pages.

b. If the configurations are correct, select the check box.

c. To start the upgrade, select Next.

11. Upgrade progress page:

a. Track the upgrade progress. The duration of the upgrade of Azure App

Service on Azure Stack Hub varies depending on the number of role

instances deployed.

b. After the upgrade successfully completes, select Exit.

７ Note

Upgrading to 2022.H1 can take a considerable amount of time dependent on

the number of role instances deployed within the App Service on Azure Stack

Hub Resource Provider deployment.

Prepare for other admin operations for Azure App Service on Azure Stack Hub:

Plan for extra capacity

Add extra capacity

Next steps

Add workers and infrastructure in Azure

App Service on Azure Stack Hub

Article • 07/29/2022

This document provides instructions on how to scale infrastructure and worker roles in

Azure App Service on Azure Stack Hub. We'll cover all the steps necessary for creating

additional worker roles to support apps of any size.

Azure App Service on Azure Stack Hub supports free and shared worker tiers by default.

To add other worker tiers, you need to add more worker roles.

If you're not sure what was deployed with the default Azure App Service on Azure Stack

Hub installation, you can review additional info in the App Service on Azure Stack Hub

overview.

Azure App Service on Azure Stack Hub deploys all roles using Virtual Machine Scale Sets

and as such takes advantage of the scaling capabilities of this workload. Therefore, all

scaling of the worker tiers is done via the App Service Admin.

1. Set up the Azure Stack Hub admin environment in PowerShell

2. Use this example to scale out the scale set.

PowerShell

７ Note

If your Azure Stack Hub Environment doesn't have more than 96-GB RAM, you may

have difficulties adding additional capacity.

Add additional workers with PowerShell

Az modules

##### Scale out the AppService Role instances ######

# Set context to AzureStack admin.

Connect-AzAccount -EnvironmentName AzureStackAdmin

## Name of the Resource group where AppService is deployed.

3. Monitor the status of the new role instances in the App Service administration.

To check the status of an individual role instance, click the role type in the list.

1. Sign in to the Azure Stack Hub administrator portal as the service admin.

2. Browse to App Services.

$AppServiceResourceGroupName = "AppService.local"

## Name of the ScaleSet : e.g. FrontEndsScaleSet,

ManagementServersScaleSet, PublishersScaleSet ,

LargeWorkerTierScaleSet, MediumWorkerTierScaleSet,

SmallWorkerTierScaleSet, SharedWorkerTierScaleSet

$ScaleSetName = "SharedWorkerTierScaleSet"

## TotalCapacity is sum of the instances needed at the end of

operation.

## e.g. if your VMSS has 1 instance(s) currently and you need 1

more the TotalCapacity should be set to 2

$TotalCapacity = 2

# Get current scale set

$vmss = Get-AzVmss -ResourceGroupName $AppServiceResourceGroupName

-VMScaleSetName $ScaleSetName

# Set and update the capacity

$vmss.sku.capacity = $TotalCapacity

Update-AzVmss -ResourceGroupName $AppServiceResourceGroupName -Name

$ScaleSetName -VirtualMachineScaleSet $vmss

７ Note

This step can take a number of hours to complete depending on the type

of role and the number of instances.

Add additional workers using the administrator

portal

3. Click Roles. Here you see the breakdown of all App Service roles deployed.

4. Right click on the row of the type you want to scale and then click ScaleSet.

5. Click Scaling, select the number of instances you want to scale to, and then click

Save.

6. Azure App Service on Azure Stack Hub will now add the additional VMs, configure

them, install all the required software, and mark them as ready when this process is

complete. This process can take approximately 80 minutes.

7. You can monitor the progress of the readiness of the new roles by viewing the

workers in the Roles blade.

After they're fully deployed and ready, the workers become available for users to deploy

their workload onto them. The following screenshot shows an example of the multiple

pricing tiers available by default. If there are no available workers for a particular worker

tier, the option to choose the corresponding pricing tier is unavailable.

Result

Configure deployment sources

７ Note

To scale out Management, Front End, or Publisher roles, follow the same steps

selecting the appropriate role type. Controllers aren't deployed as Scale Sets and

therefore two should be deployed at installation time for all production

deployments.

Next steps

Configure deployment sources for App

Services on Azure Stack Hub

Article • 10/25/2022

App Service on Azure Stack Hub supports on-demand deployment from multiple source

control providers. This feature lets app developers deploy directly from their source

control repositories. If users want to configure App Service to connect to their

repositories, a cloud operator must first configure the integration between App Service

on Azure Stack Hub and the source control provider.

In addition to local Git, the following source control providers are supported:

GitHub

BitBucket

OneDrive

DropBox

1. Sign in to the Azure Stack Hub administrator portal as the service admin.

2. Browse to All Services and select the App Service.

3. Select Source control configuration. You can see the list of all configured

deployment sources.

View deployment sources in App Service

administration

You must have a GitHub account to complete this task. You might want to use an

account for your organization rather than a personal account.

1. Sign in to GitHub, go to https://www.github.com/settings/developers , and then

select Register a new application.

） Important

If you are reconfiguring existing applications after upgrading to Azure App Service

on Azure Stack Hub 2022 H1 you must revoke all tokens and your end users will

need to reauthorize with the providers on their applications to enable

synchronisation from source control providers

Configure GitHub

2. Enter an Application name. For example, App Service on Azure Stack Hub.

3. Enter the Homepage URL. The Homepage URL must be the Azure Stack Hub portal

address. For example, https://portal.<region>.<FQDN> . For more information on

the Azure Stack Hub fully qualified domain name (FQDN), see Azure Stack Hub

DNS namespace.

4. Enter an Application Description.

5. Enter the Authorization callback URL. In a default Azure Stack Hub deployment,

the URL is in the form https://api.appservice.<region>.

<FQDN>:44300/auth/github/callback .

6. Select Register application. A page is displayed listing the Client ID and Client

Secret for the app.

7. In a new browser tab or window, sign in to the Azure Stack Hub administrator

portal as the service admin.

8. Go to Resource Providers and select the App Service Resource Provider Admin.

9. Select Source control configuration.

10. Copy and paste the Client ID and Client Secret into the corresponding input boxes

for GitHub.

11. Select Save.

You must have a BitBucket account to complete this task. You might want to use an

account for your organization rather than a personal account.

1. Sign in to BitBucket and go to Integrations under your account.

2. Select OAuth under Access Management and Add consumer.

3. Enter a Name for the consumer. For example, App Service on Azure Stack Hub.

4. Enter a Description for the app.

Configure BitBucket

5. Enter the Callback URL. In a default Azure Stack Hub deployment, the callback URL

is in the form https://api.appservice.<region>.

<FQDN>:44300/auth/bitbucket/callback . For BitBucket integration to succeed, the

URL must follow the capitalization listed here.

6. Enter the URL. This URL should be the Azure Stack Hub portal URL. For example,

https://portal.<region>.<FQDN> .

7. Select the Permissions required:

Repositories: Read

Webhooks: Read and write

8. Select Save. You now see this new app, along with the Key and Secret, under

OAuth consumers.

9. In a new browser tab or window, sign in to the Azure Stack Hub administrator

portal as the service admin.

10. Go to Resource Providers and select the App Service Resource Provider Admin.

11. Select Source control configuration.

12. Copy and paste the Key into the Client ID input box and Secret into the Client

Secret input box for BitBucket.

13. Select Save.

You must have a Microsoft account linked to a OneDrive account to complete this task.

You might want to use an account for your organization rather than a personal account.

Configure OneDrive

７ Note

1. Go to

https://portal.azure.com/#view/Microsoft\_AAD\_RegisteredApps/ApplicationsListBla

de and sign in using your Microsoft account.

2. Under App registrations, select New registration.

3. Enter a Name for the new app registration: for example, enter App Service on

Azure Stack Hub.

4. Under Supported account types, select Personal Microsoft accounts only

5. Enter the Redirect URI. Choose platform - Web and in a default Azure Stack Hub

deployment, the redirect URI is in the form - https://api.appservice.<region>.

<FQDN>:44300/auth/onedrive/callback .

6. Select Register

7. The next screen lists the properties of your new app. Save the Application (client)

ID to a temporary location.

8. Under Certificates & secrets, choose Client Secrets and select New client secret.

Provide a description and choose the expiration length for the new secret and

select Add.

9. Make a note of the value of the new secret.

10. Under API Permissions, select Add a permission

11. Add the Microsoft Graph Permissions - Delegated Permissions.

Files.ReadWrite.AppFolder

User. Read

12. In a new browser tab or window, sign in to the Azure Stack Hub administrator

portal as the service admin.

13. Go to Resource Providers and select the App Service Resource Provider Admin.

14. Select Source control configuration.

15. Copy and paste the Application (client) ID into the Client ID input box and Secret

into the Client Secret input box for OneDrive.

16. Select Save.

OneDrive for business accounts are currently not supported.

1. Go to https://www.dropbox.com/developers/apps and sign in using your

DropBox account credentials.

2. Select Create app.

3. Select DropBox API.

4. Set the access level to App Folder.

5. Enter a Name for your app.

Configure DropBox

７ Note

You must have a DropBox account to complete this task. You might want to use an

account for your organization rather than a personal account.

6. Select Create App. You're presented with a page listing the settings for the app,

including App key and App secret.

7. Make sure that the App folder name is set to App Service on Azure Stack Hub.

8. Set the OAuth 2 Redirect URI and then select Add. In a default Azure Stack Hub

deployment, the redirect URI is in the form https://api.appservice.<region>.

<FQDN>:44300/auth/dropbox/callback .

9. In a new browser tab or window, sign in to the Azure Stack Hub administrator

portal as the service admin.

10. Go to Resource Providers and select the App Service Resource Provider Admin.

11. Select Source control configuration.

12. Copy and paste the Application Key into the Client ID input box and App secret

into the Client Secret input box for DropBox.

13. Select Save.

Next steps

Users can now use the deployment sources for things like continuous deployment, local

Git deployment, and cloud folder synchronization.

Rotate App Service on Azure Stack Hub

secrets and certificates

Article • 11/24/2021

These instructions only apply to Azure App Service on Azure Stack Hub. Rotation of

Azure App Service on Azure Stack Hub secrets is not included in the centralized secret

rotation procedure for Azure Stack Hub. Operators can monitor the validity of secrets

within the system, the date on which they were last updated, and the time remaining

until the secrets expire.

This document contains the procedure for rotating the following secrets:

Encryption keys used within Azure App Service on Azure Stack Hub.

Database connection credentials used by Azure App Service on Azure Stack Hub to

interact with the hosting and metering databases.

Certificates used by Azure App Service on Azure Stack Hub to secure endpoints

and rotation of identity application certificates in Azure Active Directory (Azure AD)

or Active Directory Federation Services (AD FS).

System credentials for Azure App Service on Azure Stack Hub infrastructure roles.

To rotate the encryption keys used within Azure App Service on Azure Stack Hub, take

the following steps:

1. Go to the App Service administration experience in the Azure Stack Hub

administrator portal.

2. Go to the Secrets menu option.

3. Select the Rotate button in the Encryption Keys section.

） Important

Operators won't receive alerts for secret expiration on the Azure Stack Hub

dashboard as Azure App Service on Azure Stack Hub is not integrated with the

Azure Stack Hub alerting service. Operators must regularly monitor their secrets

using the Azure App Service on Azure Stack Hub administration experience in the

Azure Stack Hub administrator portal.

Rotate encryption keys

4. Select OK to start the rotation procedure.

5. The encryption keys are rotated and all role instances are updated. Operators can

check the status of the procedure using the Status button.

To update the credentials for the database connection string for the App Service hosting

and metering databases, take the following steps:

1. Go to the App Service administration experience in the Azure Stack Hub

administrator portal.

2. Go to the Secrets menu option.

3. Select the Rotate button in the Connection Strings section.

4. Provide the SQL SA Username and Password and select OK to start the rotation

procedure.

5. The credentials are rotated throughout the Azure App Service role instances.

Operators can check the status of the procedure using the Status button.

To rotate the certificates used within Azure App Service on Azure Stack Hub, take the

following steps:

1. Go to the App Service administration experience in the Azure Stack Hub

administrator portal.

2. Go to the Secrets menu option.

3. Select the Rotate button in the Certificates section

4. Provide the certificate file and associated password for the certificates you wish to

rotate and select OK.

5. The certificates are rotated as required throughout the Azure App Service on Azure

Stack Hub role instances. Operators can check the status of the procedure using

the Status button.

When the identity application certificate is rotated, the corresponding app in Azure AD

or AD FS must also be updated with the new certificate.

Rotate connection strings

Rotate certificates

The identity application is created by the operator before deployment of Azure App

Service on Azure Stack Hub. If the application ID is unknown, follow these steps to

discover it:

1. Go to the Azure Stack Hub administrator portal.

2. Go to Subscriptions and select Default Provider Subscription.

3. Select Access Control (IAM) and select the App Service application.

4. Take a note of the APP ID, this value is the application ID of the identity application

that must be updated in Azure AD.

To rotate the certificate for the application in Azure AD, follow these steps:

1. Go to the Azure portal and sign in using the Global Admin used to deploy Azure

Stack Hub.

2. Go to Azure Active Directory and browse to App Registrations.

3. Search for the Application ID, then specify the identity Application ID.

4. Select the application and then go to Certificates & Secrets.

5. Select Upload certificate and upload the new certificate for the identity application

with one of the following file types: .cer, .pem, .crt.

6. Confirm the thumbprint matches that listed in the App Service administration

experience in the Azure Stack Hub administrator portal.

7. Delete the old certificate.

） Important

Failure to update the identity application with the new certificate after rotation will

break the user portal experience for Azure Functions, prevent users from being able

to use the KUDU developer tools, and prevent admins from managing worker tier

scale sets from the App Service administration experience.

Rotate credential for the Azure AD identity application

Rotate certificate for AD FS identity application

The identity application is created by the operator before deployment of Azure App

Service on Azure Stack Hub. If the application's object ID is unknown, follow these steps

to discover it:

1. Go to the Azure Stack Hub administrator portal.

2. Go to Subscriptions and select Default Provider Subscription.

3. Select Access Control (IAM) and select the AzureStack-AppService-<guid>

application.

4. Take a note of the Object ID, this value is the ID of the Service Principal that must

be updated in AD FS.

To rotate the certificate for the application in AD FS, you need to have access to the

privileged endpoint (PEP). Then you update the certificate credential using PowerShell,

replacing your own values for the following placeholders:

Placeholder Description Example

<PepVM> The name of the privileged endpoint

VM on your Azure Stack Hub instance.

"AzS-ERCS01"

<CertificateFileLocation> The location of your X509 certificate

on disk.

"d:\certs\sso.cer"

<ApplicationObjectId> The identifier assigned to the identity

application.

"S-1-5-21-401916501-

2345862468-1451220656-

1451"

1. Open an elevated Windows PowerShell session and run the following script:

PowerShell

# Sign in to PowerShell interactively, using credentials that have

access to the VM running the Privileged Endpoint

$Creds = Get-Credential

# Create a new Certificate object from the identity application

certificate exported as .cer file

$Cert = New-Object

System.Security.Cryptography.X509Certificates.X509Certificate2("

<CertificateFileLocation>")

# Create a new PSSession to the PrivelegedEndpoint VM

$Session = New-PSSession -ComputerName "<PepVm>" -ConfigurationName

PrivilegedEndpoint -Credential $Creds -SessionOption (NewPSSessionOption -Culture en-US -UICulture en-US)

2. After the script finishes, it displays the updated app registration info, including the

thumbprint value for the certificate.

shell

To rotate the system credentials used within Azure App Service on Azure Stack Hub, take

the following steps:

1. Go to the App Service administration experience in the Azure Stack Hub

administrator portal.

2. Go to the Secrets menu option.

3. Select the Rotate button in the System Credentials section.

4. Select the Scope of the System Credential you're rotating. Operators can choose to

rotate the system credentials for all roles or individual roles.

5. Specify a new Local Admin User Name and a new Password. Then confirm the

Password and select OK.

6. The credential(s) are rotated as required throughout the corresponding Azure App

Service on Azure Stack Hub role instance. Operators can check the status of the

procedure using the Status button.

# Use the privileged endpoint to update the certificate thumbprint,

used by the service principal associated with the App Service identity

application

$SpObject = Invoke-Command -Session $Session -ScriptBlock {SetGraphApplication -ApplicationIdentifier "<ApplicationObjectId>" -

ClientCertificates $using:Cert}

$Session | Remove-PSSession

# Output the updated service principal details

$SpObject

ApplicationIdentifier : S-1-5-21-401916501-2345862468-1451220656-1451

ClientId :

Thumbprint : FDAA679BF9EDDD0CBB581F978457A37BFD73CA3B

ApplicationName : Azurestack-AppService-d93601c2-1ec0-4cac-8d1c8ccde63ef308

ClientSecret :

PSComputerName : AzS-ERCS01

RunspaceId : cb471c79-a0d3-40ec-90ba-89087d104510

Rotate system credentials

Back up App Service on Azure Stack

Hub

Article • 07/29/2022

This document provides instructions on how to back up App Service on Azure Stack

Hub.

Azure App Service on Azure Stack Hub has four main components to consider when

planning for disaster recovery:

1. The resource provider infrastructure; server roles, worker tiers, and so on.

2. The App Service secrets.

3. The App Service SQL Server hosting and metering databases.

4. The App Service user workload content stored in the App Service file share.

When recovering App Service from backup, you need to provide the App Service keys

used by the initial deployment. This information should be saved as soon as App Service

is successfully deployed and stored in a safe location. The resource provider

infrastructure configuration is recreated from backup during recovery using App Service

recovery PowerShell cmdlets.

Use the administration portal to back up app service secrets by following these steps:

1. Sign in to the Azure Stack Hub administrator portal as the service admin.

2. Browse to App Service -> Secrets.

3. Select Download Secrets.

） Important

App Service on Azure Stack Hub isn't backed up as part of Azure Stack Hub

infrastructure backup. As an Azure Stack Hub Operator, you must take steps to

ensure App Service can be successfully recovered if necessary.

Back up App Service secrets

4. When secrets are ready for downloading, click Save and store the App Service

secrets (SystemSecrets.JSON) file in a safe location.

７ Note

Repeat these steps every time the App Service secrets are rotated.

To restore App Service, you need the Appservice\_hosting and Appservice\_metering

database backups. We recommend using SQL Server maintenance plans or Azure

Backup Server to ensure these databases are backed up and saved securely on a regular

basis. However, any method of ensuring regular SQL backups are created can be used.

To manually back up these databases while logged into the SQL Server, use the

following PowerShell commands:

PowerShell

After all databases have been successfully backed up, copy the .bak files to a safe

location along with the App Service secrets info.

App Service stores tenant app info in the file share. This file share must be backed up on

a regular basis along with the App Service databases so that as little data as possible is

lost if a restore is required.

To back up the App Service file share content, use Azure Backup Server or another

method to regularly copy the file share content to the location you've saved all previous

recovery info.

For example, you can use these steps to use Robocopy from a Windows PowerShell (not

PowerShell ISE) console session:

PowerShell

Back up the App Service databases

$s = "<SQL Server computer name>"

$u = "<SQL Server login>"

$p = read-host "Provide the SQL admin password"

sqlcmd -S $s -U $u -P $p -Q "BACKUP DATABASE appservice\_hosting TO DISK =

'<path>\hosting.bak'"

sqlcmd -S $s -U $u -P $p -Q "BACKUP DATABASE appservice\_metering TO DISK =

'<path>\metering.bak'"

７ Note

If you need to back up SQL AlwaysOn databases, follow these instructions.

Back up the App Service file share

Restore App Service on Azure Stack Hub

$source = "<file share location>"

$destination = "<remote backup storage share location>"

net use $destination /user:<account to use to connect to the remote share in

the format of domain\username> \*

robocopy $source $destination

net use $destination /delete

Next steps

App Service recovery on Azure Stack

Hub

Article • 07/29/2022

This topic provides instructions on what actions to take for App Service disaster

recovery.

The following actions must be taken to recover App Service on Azure Stack Hub from

backup:

1. Restore the App Service databases.

2. Restore the file server share content.

3. Restore App Service roles and services.

If Azure Stack Hub storage was used for Function Apps storage, then you must also take

steps to restore Function Apps.

The App Service SQL Server databases should be restored on a production ready SQL

Server instance.

After preparing the SQL Server instance to host the App Service databases, use these

steps to restore databases from backup:

1. Sign in to the SQL Server that will host the recovered App Service databases with

admin permissions.

2. Use the following commands to restore the App Service databases from a

command prompt running with admin permissions:

dos

3. Verify that both App Service databases have been successfully restored and exit

SQL Server Management Studio.

Restore the App Service databases

sqlcmd -U <SQL admin login> -P <SQL admin password> -Q "RESTORE

DATABASE appservice\_hosting FROM DISK='<full path to backup>' WITH

REPLACE"

sqlcmd -U <SQL admin login> -P <SQL admin password> -Q "RESTORE

DATABASE appservice\_metering FROM DISK='<full path to backup>' WITH

REPLACE"

After preparing the file server to host the App Service file share, you need to restore the

tenant file share content from backup. You can use whatever method you have available

to copy the files into the newly created App Service file share location. Running this

example on the file server will use PowerShell and robocopy to connect to a remote

share and copy the files to the share:

PowerShell

In addition to copying the file share contents, you must also reset permissions on the

file share itself. To reset permissions, open an admin command prompt on the file server

computer and run the ReACL.cmd file. The ReACL.cmd file is located in the App Service

installation files in the BCDR directory.

After the App Service databases and file share content are restored, you next need to

use PowerShell to restore the App Service roles and services. These steps will restore

App Service secrets and service configurations.

1. Log into the App Service controller CN0-VM VM as roleadmin using the password

you provided during App Service installation.

７ Note

To recover from a failover cluster instance failure, see Recover from Failover Cluster

Instance Failure.

Restore the App Service file share content

$source = "<remote backup storage share location>"

$destination = "<local file share location>"

net use $source /user:<account to use to connect to the remote share in the

format of domain\username> \*

robocopy /E $source $destination

net use $source /delete

Restore App Service roles and services

 Tip

You need to modify the VM's network security group to allow RDP

connections.

2. Copy the SystemSecrets.JSON file locally to the controller VM. You need to

provide the path to this file as the $pathToExportedSecretFile parameter in the

next step.

3. Use the following commands in an elevated PowerShell console window to restore

App Service roles and services:

PowerShell

# Stop App Service services on the primary controller VM

net stop WebFarmService

net stop ResourceMetering

net stop HostingVssService # This service was deprecated in the App

Service 1.5 release and is not required after the App Service 1.4

release.

# Restore App Service secrets. Provide the path to the App Service

secrets file copied from backup. For example,

C:\temp\SystemSecrets.json.

# Press ENTER when prompted to reconfigure App Service from backup

# If necessary, use -OverrideDatabaseServer <restored server> with

Restore-AppServiceStamp when the restored database server has a

different address than backed-up deployment.

# If necessary, use -OverrideContentShare <restored file share path>

with Restore-AppServiceStamp when the restored file share has a

different path from backed-up deployment.

Restore-AppServiceStamp -FilePath $pathToExportedSecretFile

# Restore App Service roles

Restore-AppServiceRoles

# Restart App Service services

net start WebFarmService

net start ResourceMetering

net start HostingVssService # This service was deprecated in the App

Service 1.5 release and is not required after the App Service 1.4

release.

# After App Service has successfully restarted, and at least one

management server is in ready state, synchronize App Service objects to

complete the restore

# Enter Y when prompted to get all sites and again for all ServerFarm

entities.

Get-AppServiceSite | Sync-AppServiceObject

Get-AppServiceServerFarm | Sync-AppServiceObject

 Tip

App Service for Azure Stack Hub doesn't support restoring tenant user apps or data

other than file share content. All other data must be backed up and recovered outside

of App Service backup and restore operations. If Azure Stack Hub storage was used for

Function Apps storage, the following steps should be taken to recover lost data:

1. Create a new storage account to be used by the Function App. This storage can be

Azure Stack Hub storage, Azure storage, or any compatible storage.

2. Retrieve the connection string for the storage.

3. Open the function portal and browse to the function app.

4. Browse to the Platform features tab and click Application Settings.

5. Change AzureWebJobsDashboard and AzureWebJobsStorage to the new

connection string and click Save.

6. Switch to Overview.

7. Restart the app. It might take several tries to clear all errors.

App Service on Azure Stack Hub overview

It's highly recommended to close this PowerShell session when the command

completes.

Restore Function Apps

Next steps

Remove Azure App Service from Azure

Stack Hub

Article • 04/17/2020

This article shows how to remove the Azure App Service resource provider and related

components, from Azure Stack Hub.

To remove Azure App Service from Azure Stack Hub, follow this one step:

1. Delete the Resource Group that holds the Azure App Service on Azure Stack Hub

Resources, for example AppService.local

You only need to follow this section if your SQL Server and/or File Server is deployed

off-stamp or in a different resource group, otherwise continue to the next section.

1. If using SQL Server Always On, remove the AppService\_Hosting and

AppService\_Metering databases from the Availability Group:

2. Execute the following SQL Script to remove the databases and logins

SQL

Remove resource provider

） Important

This operation will remove all tenant resources, remove the service and quotas

from all plans and remove the Azure App Service resource provider in it's entirety. If

you have deployed the App Service Highly Available File Server and SQL Server

Quickstart template, these resources will also be removed as they are deployed in

the same resource group as Azure App Service on Azure Stack Hub.

Remove databases and file share content

Remove databases and logins

--\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

/\*

Script to clean up App Service objects (databases and logins).

\*/

1. Remove the content fileshare from your file server.

To reinstall, return to the Prerequisites for deploying App Service on Azure Stack Hub

article.

USE [master]

GO

DROP DATABASE [appservice\_hosting]

GO

DROP DATABASE [appservice\_metering]

GO

DECLARE @sql NVARCHAR(MAX) = N'';

SELECT @sql += '

DROP LOGIN [' + name + '];'

from master.sys.sql\_logins

WHERE name LIKE '%\_hosting\_%' OR

name LIKE '%\_metering\_%' OR

name LIKE '%WebWorker\_%';

PRINT @sql;

EXEC sp\_executesql @sql;

PRINT 'Completed';

--\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Remove the application file content from the file server

Next steps

Migrate file share

Article • 10/25/2022

This article provides instructions on how to migrate to the new file server infrastructure

for hosting the Azure App Service on Azure Stack Hub Resource Provider content file

share.

When recovering App Service from backup, you need to provide the App Service keys

used by the initial deployment. This information should be saved as soon as App Service

is successfully deployed and stored in a safe location. The resource provider

infrastructure configuration is recreated from backup during recovery using App Service

recovery PowerShell cmdlets.

Use the admin portal to back up App Service secrets by following these steps:

1. Sign in to the Azure Stack Hub administrator portal as the service admin.

2. Browse to App Service -> Secrets.

3. Select Download Secrets.

Back up App Service secrets

4. When secrets are ready for downloading, click Save and store the App Service

secrets (SystemSecrets.JSON) file in a safe location.

App Service stores tenant app info in the file share. This file share must be backed up

regularly along with the App Service databases so that as little data as possible is lost if

a restore or migration is required.

To back up the App Service file share content, use Azure Backup Server or another

method to regularly copy the file share content to the location to which you've saved all

previous recovery info.

For example, you can use these steps to use Robocopy from a Windows PowerShell (not

PowerShell ISE) console session:

PowerShell

７ Note

Repeat these steps every time the App Service secrets are rotated.

Back up the existing App Service file share

$source = "<file share location>"

$destination = "<remote backup storage share location>"

After preparing the new file server to host the App Service file share, you need to

restore the tenant file share content from backup. You can use whatever method you

have available to copy the files into the newly created App Service file share location.

Running this example on the file server will use PowerShell and Robocopy to connect to

a remote share and copy the files to the share:

PowerShell

In addition to copying the file share contents, you must also reset permissions on the

file share itself. To reset permissions, open an admin command prompt on the file server

computer and run the ReACL.cmd file. The ReACL.cmd file is located in the App Service

installation files in the BCDR directory.

1. In the Azure Stack Hub admin portal, navigate to Network Security Groups and

view the ControllersNSG Network Security Group.

2. By default, remote desktop is disabled to all App Service infrastructure roles.

Modify the Inbound\_Rdp\_2289 rule action to Allow access.

3. Navigate to the resource group containing the App Service Resource Provider

deployment, by default the name is AppService.<region> and connect to CN0-

VM.

4. Open an Administrator PowerShell session and run net stop webfarmservice

5. Repeat step 3 and 4 for all other controllers.

net use $destination /user:<account to use to connect to the remote share in

the format of domain\username> \*

robocopy $source $destination

net use $destination /delete

Restore the App Service file share content to a

new File Server

$source = "<remote backup storage share location>"

$destination = "<local file share location>"

net use $source /user:<account to use to connect to the remote share in the

format of domain\username> \*

robocopy /E $source $destination

net use $source /delete

Migrate the file share

6. Return to the CN0-VM remote desktop session.

7. Copy the App Service secrets file to the controller.

8. In an Administrator PowerShell session run

PowerShell

a. A prompt will appear to confirm the key values, verify and press ENTER to

continue, or close the PowerShell session to cancel.

9. Once the cmdlet has finished, all worker instances from custom worker tiers will be

removed, and then added back via the next PowerShell script

10. In the same administrative PowerShell session or a new Administrative PowerShell

session, run:

PowerShell

This command will inspect the Virtual Machine Scale Sets associated and perform

corresponding actions, including adding back the instances of the custom worker

tiers

11. In the same, or a new, administrative PowerShell session, run the command net

start webfarmservice.

12. Repeat the previous step for all other controllers.

13. In the Azure Stack admin portal, navigate back to the ControllersNSG Network

Security Group.

14. Modify the Inbound\_Rdp\_3389 rule to deny access.

If the credentials have changed, you must update the file share credentials to connect to

the new file server (FileShareOwnerCredential and FileShareUserCredential).

Restore-AppServiceStamp -FilePath <local secrets file> -

OverrideContentShare <new file share location> -CoreBackupFilePath

<filepath>

Restore-AppServiceRoles

Update file server credentials

1. In the Azure Stack admin portal, navigate to the ControllersNSG Network Security

Group.

2. By default remote desktop access is disabled to all App Service infrastructure roles.

Modify the Inbound\_Rdp\_3389 rule action to Allow access.

3. Navigate to the resource group containing the App Service Resource Provider

Deployment, by default the resource group is named in with the format,

AppService.<region> and connect to CN0-VM.

4. Launch the Web Cloud Management Console.

5. Check in the Web Cloud Management Console -> Web Cloud, verify that both

Controllers are Ready.

6. Select Credentials <insert screenshot here>.

7. Next select the credential you wish to update – in this case the

FileShareOwnerCrdential or the FileShareUserCredential and select edit – either

from the menu bar or from the right click context menu. <screenshot>

8. Enter the new credential details and then click OK.

9. Repeat for the FileShareUserCredential if that has changed also.

10. Once you have completed updating the credentials, you must restart CN0-VM.

11. Wait for CN0-VM and verify the role is marked as Ready in the Admin Portal ->

App Service -> Roles

12. Restart CN1-VM and verify the role is marked as Ready

13. Once both controllers are marked as Ready, Repair all other Role instances.

Recommend working through each role type that is. Management, Front End etc.,

methodically one set at a time.

14. In the Azure Stack admin portal, navigate back to the ControllersNSG Network

Security Group.

15. Modify the Inbound\_Rdp\_3389 rule to deny access.

Backup App Service on Azure Stack Hub Restore App Service on Azure Stack Hub

Next steps

Migrate SQL server

Article • 10/25/2022

This article describes how to migrate to new SQL Server infrastructure for hosting the

Azure App Service on Azure Stack Hub Resource Provider databases -

appservice\_hosting and appservice\_metrics.

When preparing to migrate, you must back up the App Service keys used by the initial

deployment.

Use the administration portal to back up app service secrets by following these steps:

1. Sign in to the Azure Stack Hub administrator portal as the service admin.

2. Browse to App Service -> Secrets.

3. Select Download Secrets.

4. When secrets are ready for downloading, click Save and store the App Service

secrets (SystemSecrets.JSON) file in a safe location.

Back up App Service secrets

To restore App Service, you need the Appservice\_hosting and Appservice\_metering

database backups. We recommend using SQL Server maintenance plans or Azure

Backup Server to ensure these databases are backed up and saved securely regularly.

However, any methods of ensuring regular SQL database backups are created can be

used.

To manually back up these databases while logged into the SQL Server, use the

following PowerShell commands:

PowerShell

Back up the App Service databases from the

current server

$s = "<SQL Server computer name>"

$u = "<SQL Server login>"

$p = read-host "Provide the SQL admin password"

sqlcmd -S $s -U $u -P $p -Q "BACKUP DATABASE appservice\_hosting TO DISK =

'<path>\hosting.bak'"

sqlcmd -S $s -U $u -P $p -Q "BACKUP DATABASE appservice\_metering TO DISK =

'<path>\metering.bak'"

７ Note

After all databases have been successfully backed up, copy the .bak files to a safe

location along with the App Service secrets info.

The App Service SQL Server databases should be restored on a production ready SQL

Server instance.

After preparing the SQL Server instance to host the App Service databases, use these

steps to restore databases from backup:

1. Sign in to the SQL Server that will host the recovered App Service databases with

admin permissions.

2. Use the following commands to restore the App Service databases from a

command prompt running with admin permissions:

dos

3. Verify that both App Service databases have been successfully restored and exit

SQL Server Management Studio.

1. In the Azure Stack Hub admin portal, navigate to Network Security Groups and

view the ControllersNSG Network Security Group.

2. By default, remote desktop is disabled to all App Service infrastructure roles.

Modify the Inbound\_Rdp\_2289 rule action to Allow access.

3. Navigate to the resource group containing the App Service Resource Provider

Deployment, by default the resource group is named in with the format,

AppService.<region> and connect to CN0-VM.

If you need to back up SQL AlwaysOn databases, follow these instructions.

Restore the App Service databases on a new

production ready SQL Server instance

sqlcmd -U <SQL admin login> -P <SQL admin password> -Q "RESTORE

DATABASE appservice\_hosting FROM DISK='<full path to backup>' WITH

REPLACE"

sqlcmd -U <SQL admin login> -P <SQL admin password> -Q "RESTORE

DATABASE appservice\_metering FROM DISK='<full path to backup>' WITH

REPLACE"

Migrate the SQL Server

4. Open an Administrator PowerShell session and run net stop webfarmservice.

5. Repeat step 3 and 4 for all other controllers.

6. Return to CN0-VM's RDP session and copy the secrets file to the controller.

7. In an Administrator PowerShell session run

PowerShell

a. A prompt will appear to confirm the key values, press Enter to continue or close

the PowerShell session to cancel.

8. Once the cmdlet completes, all worker instances from the custom worker tiers will

be removed, and those instances will be added back by the next step

9. In the same PowerShell session or a new Administrative PowerShell session, run the

following PowerShell script. The script will inspect all the Virtual Machine Scale Sets

associated and perform corresponding actions including adding back the instances

of custom worker tiers:

PowerShell

10. In the same, or a new, administrative PowerShell session, run the command net

start webfarmservice.

11. Repeat the previous step for all other controllers.

12. In the Azure Stack admin portal, navigate back to the ControllersNSG Network

Security Group

13. Modify the Inbound\_Rdp\_3389 rule to deny access.

Backup App Service on Azure Stack Hub Restore App Service on Azure Stack Hub

Restore-AppServiceStamp -FilePath <local secrets file> -

OverrideDatabaseServer <new database server> -CoreBackupFilePath

<filepath>

Restore-AppServiceRoles

Next steps

App Service on Azure Stack Hub 2302

release notes

Article • 08/17/2023

These release notes describe the improvements and fixes in Azure App Service on Azure

Stack Hub 2302, and any known issues. Known issues are divided into issues directly

related to the deployment, update process, and issues with the build (post-installation).

Supported Azure Stack Hub version App Service RP version

2301 2302 Installer (release notes)

2206.2.52 2302 Installer (release notes)

2108.2.127 2302 Installer (release notes)

The App Service on Azure Stack Hub 2302 build number is 98.0.1.703

Azure App Service on Azure Stack Hub 2302 release replaces the 2022 H1 release and

includes fixes for the following issues:

CVE-2023-21703 Azure App Service on Azure Stack Hub Elevation of Privilege

Vulnerability .

Unable to open Virtual Machine Scale Sets User Experience from the App Service

Roles admin user experience in the Azure Stack Hub administration portal.

All other updates are documented in the Azure App Service on Azure Stack Hub

2022 H1 Update Release Notes.

） Important

Update Azure Stack Hub to a supported version (or deploy the latest Azure Stack

Development Kit) if necessary, before deploying or updating the App Service

resource provider (RP). Be sure to read the RP release notes to learn about new

functionality, fixes, and any known issues that could affect your deployment.

Build reference

What's new?

As of the Azure App Service on Azure Stack Hub 2022 H1 update, the letter K is

now a reserved SKU letter. If you have a custom SKU defined that uses the letter K,

contact support to assist with resolving this situation prior to upgrade.

Refer to the Before You Get Started documentation before beginning deployment.

Before you begin the upgrade of Azure App Service on Azure Stack Hub to 2302:

Ensure your Azure Stack Hub is updated to 1.2108.2.127 or 1.2206.2.52.

Ensure all roles are ready in the Azure App Service administration in the Azure

Stack Hub admin portal.

Back up App Service secrets using the App Service administration in the Azure

Stack Hub admin portal.

Back up the App Service and SQL Server master databases:

AppService\_Hosting;

AppService\_Metering;

Master

Back up the tenant app content file share.

Syndicate the Custom Script Extension version 1.9.3 from the Marketplace.

Prerequisites

） Important

Cloud operators are responsible for the maintenance and operation of the file

server and SQL Server. The resource provider does not manage these

resources. The cloud operator is responsible for backing up the App Service

databases and tenant content file share.

Pre-update steps

７ Note

If you have previously deployed Azure App Service on Azure Stack Hub 2022 H1 to

your Azure Stack Hub stamp, this release is a minor upgrade to 2022 H1 which

addresses two issues.

Azure App Service on Azure Stack Hub 2302 is a significant update that will take

multiple hours to complete. The whole deployment will be updated and all roles

recreated with the Windows Server 2022 Datacenter OS. Therefore, we recommend

informing end customers of a planned update before applying the update.

As of the Azure App Service on Azure Stack Hub 2022 H1 update, the letter K is

now a reserved SKU letter. If you have a custom SKU defined that uses the letter K,

contact support to assist with resolving this situation prior to upgrade.

Review the known issues for update and take any actions prescribed.

In situations where you have converted the appservice\_hosting and

appservice\_metering databases to contained databases, the upgrade may fail if

logins haven't been successfully migrated to contained users.

If you converted the appservice\_hosting and appservice\_metering databases to

contained database post deployment, and haven't successfully migrated the

database logins to contained users, you might experience upgrade failures.

You must execute the following script against the SQL Server hosting

appservice\_hosting and appservice\_metering before upgrading your Azure App

Service on Azure Stack Hub installation to 2020 Q3. This script is non-destructive

and will not cause downtime.

This script must be run under the following conditions:

By a user that has the system administrator privilege, for example the SQL SA

Account.

If using SQL Always on, ensure the script is run from the SQL instance that

contains all App Service logins in the form:

appservice\_hosting\_FileServer

Post-deployment steps

） Important

If you have provided the App Service resource provider with a SQL Always On

instance, you must add the appservice\_hosting and appservice\_metering

databases to an availability group and synchronize the databases to prevent any

loss of service in the event of a database failover.

Known issues (update)

appservice\_hosting\_HostingAdmin

appservice\_hosting\_LoadBalancer

appservice\_hosting\_Operations

appservice\_hosting\_Publisher

appservice\_hosting\_SecurePublisher

appservice\_hosting\_WebWorkerManager

appservice\_metering\_Common

appservice\_metering\_Operations

All WebWorker logins - which are in the form WebWorker\_<instance ip

address>

SQL

USE appservice\_hosting

IF EXISTS(SELECT \* FROM sys.databases WHERE Name=DB\_NAME() AND

containment = 1)

BEGIN

DECLARE @username sysname ;

DECLARE user\_cursor CURSOR

FOR

SELECT dp.name

FROM sys.database\_principals AS dp

JOIN sys.server\_principals AS sp

ON dp.sid = sp.sid

WHERE dp.authentication\_type = 1 AND dp.name NOT IN

('dbo','sys','guest','INFORMATION\_SCHEMA');

OPEN user\_cursor

FETCH NEXT FROM user\_cursor INTO @username

WHILE @@FETCH\_STATUS = 0

BEGIN

EXECUTE sp\_migrate\_user\_to\_contained

@username = @username,

@rename = N'copy\_login\_name',

@disablelogin = N'do\_not\_disable\_login';

FETCH NEXT FROM user\_cursor INTO @username

END

CLOSE user\_cursor ;

DEALLOCATE user\_cursor ;

END

GO

USE appservice\_metering

IF EXISTS(SELECT \* FROM sys.databases WHERE Name=DB\_NAME() AND

containment = 1)

BEGIN

DECLARE @username sysname ;

DECLARE user\_cursor CURSOR

FOR

SELECT dp.name

FROM sys.database\_principals AS dp

JOIN sys.server\_principals AS sp

Tenant Applications are unable to bind certificates to applications after upgrade.

The cause of this issue is due to a missing feature on front-ends after the upgrade

to Windows Server 2022. Operators must follow this procedure to resolve the

issue.

1. In the Azure Stack Hub admin portal, navigate to Network Security Groups

and view the ControllersNSG Network Security Group.

2. By default, remote desktop is disabled to all App Service infrastructure roles.

Modify the Inbound\_Rdp\_3389 rule action to Allow access.

3. Navigate to the resource group containing the App Service Resource Provider

deployment, by default the name is AppService.<region> and connect to

CN0-VM.

4. Return to the CN0-VM remote desktop session.

5. In an administrator PowerShell session run:

ON dp.sid = sp.sid

WHERE dp.authentication\_type = 1 AND dp.name NOT IN

('dbo','sys','guest','INFORMATION\_SCHEMA');

OPEN user\_cursor

FETCH NEXT FROM user\_cursor INTO @username

WHILE @@FETCH\_STATUS = 0

BEGIN

EXECUTE sp\_migrate\_user\_to\_contained

@username = @username,

@rename = N'copy\_login\_name',

@disablelogin = N'do\_not\_disable\_login';

FETCH NEXT FROM user\_cursor INTO @username

END

CLOSE user\_cursor ;

DEALLOCATE user\_cursor ;

END

GO

） Important

During the execution of this script there will be a pause for each instance

in the front end scaleset. If there is a message indicating the feature is

being installed, that instance will be rebooted. Use the pause in the

script to maintain front end availability. Operators must ensure at least

one front end instance is "Ready" at all times to ensure tenant

applications can receive traffic and not experience downtime.

PowerShell

6. In the Azure Stack admin portal, navigate back to the ControllersNSG

Network Security Group.

7. Modify the Inbound\_Rdp\_3389 rule to deny access.

Workers are unable to reach the file server when App Service is deployed in an

existing virtual network and the file server is only available on the private network,

as called out in the Azure App Service on Azure Stack deployment documentation.

If you chose to deploy into an existing virtual network and an internal IP address to

connect to your file server, you must add an outbound security rule, enabling SMB

traffic between the worker subnet and the file server. Go to the WorkersNsg in the

admin portal and add an outbound security rule with the following properties:

Source: Any

Source port range: \*

$c = Get-AppServiceConfig -Type Credential -CredentialName

FrontEndCredential

$spwd = ConvertTo-SecureString -String $c.Password -AsPlainText -

Force

$cred = New-Object System.Management.Automation.PsCredential

($c.UserName, $spwd)

Get-AppServiceServer -ServerType LoadBalancer | ForEach-Object {

$lb = $\_

$session = New-PSSession -ComputerName $lb.Name -Credential

$cred

Invoke-Command -Session $session {

$f = Get-WindowsFeature -Name Web-CertProvider

if (-not $f.Installed) {

Write-Host Install feature on $env:COMPUTERNAME

Install-WindowsFeature -Name Web-CertProvider

Shutdown /t 5 /r /f

}

}

}

Remove-PSSession -Session $session

Read-Host -Prompt "If installing the feature, the machine will

reboot, wait till there are enough frontend availability and press

ENTER to continue"

Known issues (post-installation)

Destination: IP Addresses

Destination IP address range: Range of IPs for your file server

Destination port range: 445

Protocol: TCP

Action: Allow

Priority: 700

Name: Outbound\_Allow\_SMB445

To remove latency when workers are communicating with the file server, we also

advise adding the following rule to the Worker NSG to allow outbound LDAP and

Kerberos traffic to your Active Directory controllers if securing the file server using

Active Directory; for example, if you've used the Quickstart template to deploy a

HA file server and SQL Server.

Go to the WorkersNsg in the admin portal and add an outbound security rule with

the following properties:

Source: Any

Source port range: \*

Destination: IP Addresses

Destination IP address range: Range of IPs for your AD Servers, for example with

the Quickstart template 10.0.0.100, 10.0.0.101

Destination port range: 389,88

Protocol: Any

Action: Allow

Priority: 710

Name: Outbound\_Allow\_LDAP\_and\_Kerberos\_to\_Domain\_Controllers

Tenant applications are unable to bind certificates to applications after upgrade.

The cause of this issue is due to a missing feature on front ends after the upgrade

to Windows Server 2022. Operators must follow this procedure to resolve the

issue:

1. In the Azure Stack Hub admin portal, navigate to Network Security Groups

and view the ControllersNSG Network Security Group.

2. By default, remote desktop is disabled to all App Service infrastructure roles.

Modify the Inbound\_Rdp\_3389 rule action to Allow access.

3. Navigate to the resource group containing the App Service Resource Provider

deployment, by default the name is AppService.<region> and connect to

CN0-VM.

4. Return to the CN0-VM remote desktop session.

5. In an administrator PowerShell session run:

PowerShell

6. In the Azure Stack admin portal, navigate back to the ControllersNSG

Network Security Group.

7. Modify the Inbound\_Rdp\_3389 rule to deny access.

） Important

During the execution of this script there will be a pause for each instance

in the front end scaleset. If there is a message indicating the feature is

being installed, that instance will be rebooted. Use the pause in the

script to maintain front end availability. Operators must ensure at least

one front end instance is "Ready" at all times to ensure tenant

applications can receive traffic and not experience downtime.

$c = Get-AppServiceConfig -Type Credential -CredentialName

FrontEndCredential

$spwd = ConvertTo-SecureString -String $c.Password -AsPlainText -

Force

$cred = New-Object System.Management.Automation.PsCredential

($c.UserName, $spwd)

Get-AppServiceServer -ServerType LoadBalancer | ForEach-Object {

$lb = $\_

$session = New-PSSession -ComputerName $lb.Name -Credential

$cred

Invoke-Command -Session $session {

$f = Get-WindowsFeature -Name Web-CertProvider

if (-not $f.Installed) {

Write-Host Install feature on $env:COMPUTERNAME

Install-WindowsFeature -Name Web-CertProvider

Shutdown /t 5 /r /f

}

}

}

Remove-PSSession -Session $session

Read-Host -Prompt "If installing the feature, the machine will

reboot, wait till there are enough frontend availability and press

ENTER to continue"

Custom domains aren't supported in disconnected environments.

App Service performs domain ownership verification against public DNS

endpoints. As a result, custom domains aren't supported in disconnected

scenarios.

Virtual Network integration for Web and Function apps is not supported.

The ability to add virtual network integration to Web and Function apps shows in

the Azure Stack Hub portal and if a tenant attempts to configure, they receive an

internal server error. This feature is not supported in Azure App Service on Azure

Stack Hub.

For an overview of Azure App Service, see Azure App Service on Azure Stack

overview.

For more information about how to prepare to deploy App Service on Azure Stack,

see Before you get started with App Service on Azure Stack.

Known issues for Cloud Admins operating Azure App

Service on Azure Stack

Next steps

App Service on Azure Stack Hub 2022

H1 release notes

Article • 05/16/2023

These release notes describe the improvements and fixes in Azure App Service on Azure

Stack Hub 2022 H1 release notes and any known issues. Known issues are divided into

issues directly related to the deployment, update process, and issues with the build

(post-installation).

Supported Azure Stack Hub version App Service RP version

2301 2302 Installer (release notes)

2206.2.52 2302 Installer (release notes)

2108.2.127 2302 Installer (release notes)

The App Service on Azure Stack Hub 2022 H1 build number is 98.0.1.699

Azure App Service on Azure Stack Hub 2022 H1 brings many new capabilities to Azure

Stack Hub.

All roles are now powered by Windows Server 2022 Datacenter.

Administrators can isolate the platform image for use by App Service on Azure

Stack Hub, by setting the SKU to AppService.

Network design update for all worker Virtual Machine Scale Sets, addressing

customers faced with SNAT port exhaustion issues.

） Important

Update Azure Stack Hub to a supported version (or deploy the latest Azure Stack

Development Kit) if necessary, before deploying or updating the App Service

resource provider (RP). Be sure to read the RP release notes to learn about new

functionality, fixes, and any known issues that could affect your deployment.

Build reference

What's new?

Increased number of outbound addresses for all applications. The updated list of

outbound addresses can be discovered in the properties of an application in the

Azure Stack Hub portal.

Administrators can set a three character deployment prefix for the individual

instances in each Virtual Machine Scale Set that are deployed, useful when

managing multiple Azure Stack Hub instances.

Deployment Center is now enabled for tenants, replacing the Deployment Options

experience. IMPORTANT: Operators will need to reconfigure their deployment

sources as the Redirect URLs have changed with this update, in addition tenants

will need to reconnect their apps to their source control providers.

As of this update, the letter K is now a reserved SKU Letter, if you have a custom

SKU defined utilizing the letter K, contact support to assist resolving this situation

prior to upgrade.

Refer to the Before You Get Started documentation before beginning deployment.

Before you begin the upgrade of Azure App Service on Azure Stack to 2022 H1:

Ensure your Azure Stack Hub is updated to 1.2108.2.127 or 1.2206.2.52.

Ensure all roles are Ready in the Azure App Service Administration in the Azure

Stack Hub Admin Portal.

Backup App Service Secrets using the App Service Administration in the Azure

Stack Hub Admin Portal.

Back up the App Service and SQL Server Master Databases:

AppService\_Hosting;

AppService\_Metering;

Master

Back up the Tenant App content file share.

Prerequisites

） Important

Cloud operators are responsible for the maintenance and operation of the File

Server and SQL Server. The resource provider does not manage these

resources. The cloud operator is responsible for backing up the App Service

databases and tenant content file share.

Syndicate the Custom Script Extension version 1.9.3 from the Marketplace.

Azure App Service on Azure Stack Update 2022 H1 includes the following improvements

and fixes:

Updates to App Service Tenant, Admin, Functions portals and Kudu tools.

Consistent with Azure Stack Portal SDK version.

Updates Azure Functions runtime to v1.0.13154.

Updates to core service to improve reliability and error messaging enabling easier

diagnosis of common issues.

Updates to the following application frameworks and tools:

2022-09 Cumulative Update for .NET Framework 3.5 and 4.8 for Microsoft server

operating system version 21H2 for x64 (KB5017028).

ASP.NET Core

3.1.18

3.1.23

6.0.2

6.0.3

Eclipse Temurin OpenJDK 8

8u302

8u312

8u322

Microsoft OpenJDK 11

11.0.12.7.1

11.0.13.8

11.0.14.1

17.0.1.12

17.0.2.8

MSBuild

16.7.0

17.1.0

MSDeploy 3.5.100608.567

NodeJS

14.18.1

16.9.1

16.13.0

npm

Updates

6.14.15

7.21.1

8.1.0

Tomcat

8.5.69

8.5.72

8.5.78

9.0.52

9.0.54

9.0.62

10.0.12

10.0.20

Updated Kudu to 97.40427.5713.

Updates to underlying operating system of all roles:

2022-09 Cumulative Update for Windows Server 2022 for x64-based Systems

(KB5017316) .

Defender Definition 1.373.353.0

Cumulative Updates for Windows Server are now applied to Controller roles as

part of deployment and upgrade.

Automatically clean up SiteDataRecord and TraceMessages tables within the App

Service Resource Provider database(s).

Private certificate now shows in sites with deployment slot(s).

Improved reliability of upgrade process, by verifying all roles are ready.

Azure App Service on Azure Stack Hub 2022 H1 is a significant update and as such can

take multiple hours to complete as the whole deployment is updated and all roles are

recreated with the Windows Server 2022 Datacenter OS. Therefore we recommend

informing end customers of planned update ahead of applying the update.

As of Azure App Service on Azure Stack Hub 2022 H1 Update, the letter K is now a

reserved SKU Letter, if you have a custom SKU defined utilizing the letter K, contact

support to assist resolving this situation prior to upgrade.

Review the known issues for update and take any action prescribed.

Issues fixed in this release

Pre-Update steps

In situations where a customer has converted the appservice\_hosting and

appservice\_metering databases to contained database, upgrade may fail if logins

haven't been successfully migrated to contained users.

Customers that have converted the appservice\_hosting and appservice\_metering

databases to contained database post deployment, and haven't successfully migrated

the database logins to contained users, may experience upgrade failures.

Customers must execute the following script against the SQL Server hosting

appservice\_hosting and appservice\_metering before upgrading your Azure App Service

on Azure Stack Hub installation to 2020 Q3. This script is non-destructive and will not

cause downtime.

This script must be run under the following conditions:

By a user that has the system administrator privilege, for example the SQL SA

Account;

If using SQL Always on, ensure the script is run from the SQL instance that contains

all App Service logins in the form:

appservice\_hosting\_FileServer

appservice\_hosting\_HostingAdmin

appservice\_hosting\_LoadBalancer

appservice\_hosting\_Operations

appservice\_hosting\_Publisher

appservice\_hosting\_SecurePublisher

appservice\_hosting\_WebWorkerManager

appservice\_metering\_Common

appservice\_metering\_Operations

Post-deployment steps

） Important

If you have provided the App Service resource provider with a SQL Always On

Instance you MUST add the appservice\_hosting and appservice\_metering

databases to an availability group and synchronize the databases to prevent any

loss of service in the event of a database failover.

Known issues (update)

All WebWorker logins - which are in the form WebWorker\_<instance ip

address>

SQL

USE appservice\_hosting

IF EXISTS(SELECT \* FROM sys.databases WHERE Name=DB\_NAME() AND

containment = 1)

BEGIN

DECLARE @username sysname ;

DECLARE user\_cursor CURSOR

FOR

SELECT dp.name

FROM sys.database\_principals AS dp

JOIN sys.server\_principals AS sp

ON dp.sid = sp.sid

WHERE dp.authentication\_type = 1 AND dp.name NOT IN

('dbo','sys','guest','INFORMATION\_SCHEMA');

OPEN user\_cursor

FETCH NEXT FROM user\_cursor INTO @username

WHILE @@FETCH\_STATUS = 0

BEGIN

EXECUTE sp\_migrate\_user\_to\_contained

@username = @username,

@rename = N'copy\_login\_name',

@disablelogin = N'do\_not\_disable\_login';

FETCH NEXT FROM user\_cursor INTO @username

END

CLOSE user\_cursor ;

DEALLOCATE user\_cursor ;

END

GO

USE appservice\_metering

IF EXISTS(SELECT \* FROM sys.databases WHERE Name=DB\_NAME() AND

containment = 1)

BEGIN

DECLARE @username sysname ;

DECLARE user\_cursor CURSOR

FOR

SELECT dp.name

FROM sys.database\_principals AS dp

JOIN sys.server\_principals AS sp

ON dp.sid = sp.sid

WHERE dp.authentication\_type = 1 AND dp.name NOT IN

('dbo','sys','guest','INFORMATION\_SCHEMA');

OPEN user\_cursor

FETCH NEXT FROM user\_cursor INTO @username

WHILE @@FETCH\_STATUS = 0

BEGIN

EXECUTE sp\_migrate\_user\_to\_contained

@username = @username,

@rename = N'copy\_login\_name',

@disablelogin = N'do\_not\_disable\_login';

Tenant Applications are unable to bind certificates to applications after upgrade.

The cause of this issue is due to a missing feature on Front-Ends after upgrade to

Windows Server 2022. Operators must follow this procedure to resolve the issue.

1. In the Azure Stack Hub admin portal, navigate to Network Security Groups

and view the ControllersNSG Network Security Group.

2. By default, remote desktop is disabled to all App Service infrastructure roles.

Modify the Inbound\_Rdp\_2289 rule action to Allow access.

3. Navigate to the resource group containing the App Service Resource Provider

deployment, by default the name is AppService.<region> and connect to

CN0-VM.

4. Return to the CN0-VM remote desktop session.

5. In an Administrator PowerShell session run:

PowerShell

FETCH NEXT FROM user\_cursor INTO @username

END

CLOSE user\_cursor ;

DEALLOCATE user\_cursor ;

END

GO

） Important

During the execution of this script there will be a pause for each instance

in the Front End scaleset. If there is a message indicating the feature is

being installed, that instance will be rebooted, use the pause in the script

to maintain Front End availability. Operators must ensure at least one

Front End instance is "Ready" at all times to ensure tenant applications

can receive traffic and not experience downtime.

$c = Get-AppServiceConfig -Type Credential -CredentialName

FrontEndCredential

$spwd = ConvertTo-SecureString -String $c.Password -AsPlainText -

Force

$cred = New-Object System.Management.Automation.PsCredential

($c.UserName, $spwd)

Get-AppServiceServer -ServerType LoadBalancer | ForEach-Object {

$lb = $\_

6. In the Azure Stack admin portal, navigate back to the ControllersNSG

Network Security Group.

7. Modify the Inbound\_Rdp\_3389 rule to deny access.

Workers are unable to reach file server when App Service is deployed in an existing

virtual network and the file server is only available on the private network, as called

out in the Azure App Service on Azure Stack deployment documentation.

If you chose to deploy into an existing virtual network and an internal IP address to

connect to your file server, you must add an outbound security rule, enabling SMB

traffic between the worker subnet and the file server. Go to the WorkersNsg in the

Admin Portal and add an outbound security rule with the following properties:

Source: Any

Source port range: \*

Destination: IP Addresses

Destination IP address range: Range of IPs for your file server

Destination port range: 445

Protocol: TCP

Action: Allow

Priority: 700

Name: Outbound\_Allow\_SMB445

To remove latency when workers are communicating with the file server we also

advise adding the following rule to the Worker NSG to allow outbound LDAP and

$session = New-PSSession -ComputerName $lb.Name -Credential

$cred

Invoke-Command -Session $session {

$f = Get-WindowsFeature -Name Web-CertProvider

if (-not $f.Installed) {

Write-Host Install feature on $env:COMPUTERNAME

Install-WindowsFeature -Name Web-CertProvider

Shutdown /t 5 /r /f

}

}

Remove-PSSession -Session $session

Read-Host -Prompt "If installing the feature, the machine will

reboot, wait till there are enough frontend availability and press

ENTER to continue"

Known issues (post-installation)

Kerberos traffic to your Active Directory Controllers if securing the file server using

Active Directory, for example if you've used the Quickstart template to deploy a HA

File Server and SQL Server.

Go to the WorkersNsg in the Admin Portal and add an outbound security rule with

the following properties:

Source: Any

Source port range: \*

Destination: IP Addresses

Destination IP address range: Range of IPs for your AD Servers, for example with

the Quickstart template 10.0.0.100, 10.0.0.101

Destination port range: 389,88

Protocol: Any

Action: Allow

Priority: 710

Name: Outbound\_Allow\_LDAP\_and\_Kerberos\_to\_Domain\_Controllers

Tenant Applications are unable to bind certificates to applications after upgrade.

The cause of this issue is due to a missing feature on Front-Ends after upgrade to

Windows Server 2022. Operators must follow this procedure to resolve the issue.

1. In the Azure Stack Hub admin portal, navigate to Network Security Groups

and view the ControllersNSG Network Security Group.

2. By default, remote desktop is disabled to all App Service infrastructure roles.

Modify the Inbound\_Rdp\_2289 rule action to Allow access.

3. Navigate to the resource group containing the App Service Resource Provider

deployment, by default the name is AppService.<region> and connect to

CN0-VM.

4. Return to the CN0-VM remote desktop session.

5. In an Administrator PowerShell session run:

） Important

During the execution of this script there will be a pause for each instance

in the Front End scaleset. If there is a message indicating the feature is

being installed, that instance will be rebooted, use the pause in the script

to maintain Front End availability. Operators must ensure at least one

Front End instance is "Ready" at all times to ensure tenant applications

can receive traffic and not experience downtime.

PowerShell

6. In the Azure Stack admin portal, navigate back to the ControllersNSG

Network Security Group.

7. Modify the Inbound\_Rdp\_3389 rule to deny access.

Custom domains aren't supported in disconnected environments.

App Service performs domain ownership verification against public DNS

endpoints. As a result, custom domains aren't supported in disconnected

scenarios.

Virtual Network integration for Web and Function Apps is not supported.

$c = Get-AppServiceConfig -Type Credential -CredentialName

FrontEndCredential

$spwd = ConvertTo-SecureString -String $c.Password -AsPlainText -

Force

$cred = New-Object System.Management.Automation.PsCredential

($c.UserName, $spwd)

Get-AppServiceServer -ServerType LoadBalancer | ForEach-Object {

$lb = $\_

$session = New-PSSession -ComputerName $lb.Name -Credential

$cred

Invoke-Command -Session $session {

$f = Get-WindowsFeature -Name Web-CertProvider

if (-not $f.Installed) {

Write-Host Install feature on $env:COMPUTERNAME

Install-WindowsFeature -Name Web-CertProvider

Shutdown /t 5 /r /f

}

}

Remove-PSSession -Session $session

Read-Host -Prompt "If installing the feature, the machine will

reboot, wait till there are enough frontend availability and press

ENTER to continue"

Known issues for Cloud Admins operating Azure App

Service on Azure Stack

The ability to add virtual network integration to Web and Function apps shows in

the Azure Stack Hub portal and if a tenant attempts to configure, they receive an

internal server error. This feature is not supported in Azure App Service on Azure

Stack Hub.

For an overview of Azure App Service, see Azure App Service on Azure Stack

overview.

For more information about how to prepare to deploy App Service on Azure Stack,

see Before you get started with App Service on Azure Stack.

Next steps

App Service on Azure Stack Hub 2021

Q3 release notes

Article • 12/10/2021

These release notes describe the improvements and fixes in Azure App Service on Azure

Stack Hub 2021 Q3 and any known issues. Known issues are divided into issues directly

related to the deployment, update process, and issues with the build (post-installation).

Supported Azure Stack Hub version App Service RP version

2301 2302 Installer (release notes)

2206.2.52 2302 Installer (release notes)

2108.2.127 2302 Installer (release notes)

The App Service on Azure Stack Hub 2021 Q3 build number is 95.1.1.539

Refer to the Before You Get Started documentation before beginning deployment.

Before you begin the upgrade of Azure App Service on Azure Stack to 2021 Q3:

Ensure your Azure Stack Hub is updated to 2108.

Ensure all roles are Ready in the Azure App Service Administration in the Azure

Stack Hub Admin Portal

Backup App Service Secrets using the App Service Administration in the Azure

Stack Hub Admin Portal

） Important

Update Azure Stack Hub to a supported version (or deploy the latest Azure Stack

Development Kit) if necessary, before deploying or updating the App Service

resource provider (RP). Be sure to read the RP release notes to learn about new

functionality, fixes, and any known issues that could affect your deployment.

Build reference

Prerequisites

Back up the App Service and SQL Server Master Databases:

AppService\_Hosting;

AppService\_Metering;

Master

Back up the Tenant App content file share

Syndicate the Custom Script Extension version 1.9.3 from the Marketplace

Azure App Service on Azure Stack Update 2021 Q3 includes the following improvements

and fixes:

Updates to App Service Tenant, Admin, Functions portals and Kudu tools.

Consistent with Azure Stack Portal SDK version.

Updates Azure Functions runtime to v1.0.13154.

Updates to core service to improve reliability and error messaging enabling easier

diagnosis of common issues.

Updates to the following application frameworks and tools:

ASP.NET Core

3.1.16

5.0.7

6.0.0

Azul OpenJDK

8.52.0.23

11.44.13

Git 2.33.1.1

MSBuild 16.8.3

MSDeploy 3.5.100419.17

NodeJS

10.15.2

） Important

Cloud operators are responsible for the maintenance and operation of the File

Server and SQL Server. The resource provider does not manage these

resources. The cloud operator is responsible for backing up the App Service

databases and tenant content file share.

Updates

10.16.3

10.19.0

12.21.0

14.15.1

14.16.0

NPM

6.14.11

PHP

7.2.34

7.3.27

7.4.15

Tomcat

8.5.58

9.0.38

Wordpress 4.9.18

Updated Kudu to 94.30524.5227

Updates to underlying operating system of all roles:

2021-11 Cumulative Update for Windows Server 2016 for x64-based Systems

(KB5007192)

2021-09 Servicing Stack Update for Windows Server 2016 for x64-based

Systems (KB5005698)

Defender Definition 1.353.743.0

Cumulative Updates for Windows Server are now applied to Controller roles as

part of deployment and upgrade

TLS Cipher Suites updated to maintain consistency with Azure Service.

Added support for 2020-09-01-hybrid profile

App Service can now be deployed when running the installer from a FIPSCompliant Client machine

App Service Role Health is now automatically checked before completing App

Service secret rotation procedures. If all roles not in ready state, secret rotation will

be blocked

Outbound IP Address for sites is now displayed in the properties and Custom

Domains blades within the tenant portal

Issues fixed in this release

Included further details on event of Custom Domain verification failure

Customers can successfully upload and delete private certificates in the tenant

portal

Issue resolved whereby FrontEnd role instances can remain in Auto Repair loop

because of a missing dependency in Functions scaling components

Resolved Single Sign On Failures to SCM Site because of changes in Azure AD

endpoints

Updated load balancer health probes on Front-End roles and Management roles to

be in alignment with Azure implementation. Traffic blocked from reaching FrontEnd role instance(s) when not in Ready state.

Aligned per site temporary directory quota size with Azure, limit on Dedicated

Workers is 10 GB, Shared Workers is 500 MB

Added algorithm to Log Scavenger routines to prevent workers entering repair

loop in event generated http logs exceed available space on worker.

Review the known issues for update and take any action prescribed.

In situations where a customer has converted the appservice\_hosting and

appservice\_metering databases to contained database, upgrade may fail if logins

have not been successfully migrated to contained users

Pre-Update steps

Post-deployment steps

） Important

If you have provided the App Service resource provider with a SQL Always On

Instance you MUST add the appservice\_hosting and appservice\_metering

databases to an availability group and synchronize the databases to prevent any

loss of service in the event of a database failover.

Known issues (update)

Customers that have converted the appservice\_hosting and appservice\_metering

databases to contained database post deployment, and have not successfully migrated

the database logins to contained users, may experience upgrade failures.

Customers must execute the following script against the SQL Server hosting

appservice\_hosting and appservice\_metering before upgrading your Azure App Service

on Azure Stack Hub installation to 2020 Q3. This script is non-destructive and will not

cause downtime.

This script must be run under the following conditions

By a user that has the system administrator privilege, for example the SQL SA

Account;

If using SQL Always on, ensure the script is run from the SQL instance that contains

all App Service logins in the form:

appservice\_hosting\_FileServer

appservice\_hosting\_HostingAdmin

appservice\_hosting\_LoadBalancer

appservice\_hosting\_Operations

appservice\_hosting\_Publisher

appservice\_hosting\_SecurePublisher

appservice\_hosting\_WebWorkerManager

appservice\_metering\_Common

appservice\_metering\_Operations

All WebWorker logins - which are in the form WebWorker\_<instance ip

address>

SQL

USE appservice\_hosting

IF EXISTS(SELECT \* FROM sys.databases WHERE Name=DB\_NAME() AND

containment = 1)

BEGIN

DECLARE @username sysname ;

DECLARE user\_cursor CURSOR

FOR

SELECT dp.name

FROM sys.database\_principals AS dp

JOIN sys.server\_principals AS sp

ON dp.sid = sp.sid

WHERE dp.authentication\_type = 1 AND dp.name NOT IN

('dbo','sys','guest','INFORMATION\_SCHEMA');

OPEN user\_cursor

FETCH NEXT FROM user\_cursor INTO @username

WHILE @@FETCH\_STATUS = 0

BEGIN

Workers are unable to reach file server when App Service is deployed in an existing

virtual network and the file server is only available on the private network, as called

out in the Azure App Service on Azure Stack deployment documentation.

If you chose to deploy into an existing virtual network and an internal IP address to

connect to your file server, you must add an outbound security rule, enabling SMB

traffic between the worker subnet and the file server. Go to the WorkersNsg in the

Admin Portal and add an outbound security rule with the following properties:

Source: Any

EXECUTE sp\_migrate\_user\_to\_contained

@username = @username,

@rename = N'copy\_login\_name',

@disablelogin = N'do\_not\_disable\_login';

FETCH NEXT FROM user\_cursor INTO @username

END

CLOSE user\_cursor ;

DEALLOCATE user\_cursor ;

END

GO

USE appservice\_metering

IF EXISTS(SELECT \* FROM sys.databases WHERE Name=DB\_NAME() AND

containment = 1)

BEGIN

DECLARE @username sysname ;

DECLARE user\_cursor CURSOR

FOR

SELECT dp.name

FROM sys.database\_principals AS dp

JOIN sys.server\_principals AS sp

ON dp.sid = sp.sid

WHERE dp.authentication\_type = 1 AND dp.name NOT IN

('dbo','sys','guest','INFORMATION\_SCHEMA');

OPEN user\_cursor

FETCH NEXT FROM user\_cursor INTO @username

WHILE @@FETCH\_STATUS = 0

BEGIN

EXECUTE sp\_migrate\_user\_to\_contained

@username = @username,

@rename = N'copy\_login\_name',

@disablelogin = N'do\_not\_disable\_login';

FETCH NEXT FROM user\_cursor INTO @username

END

CLOSE user\_cursor ;

DEALLOCATE user\_cursor ;

END

GO

Known issues (post-installation)

Source port range: \*

Destination: IP Addresses

Destination IP address range: Range of IPs for your file server

Destination port range: 445

Protocol: TCP

Action: Allow

Priority: 700

Name: Outbound\_Allow\_SMB445

To remove latency when workers are communicating with the file server we also

advise adding the following rule to the Worker NSG to allow outbound LDAP and

Kerberos traffic to your Active Directory Controllers if securing the file server using

Active Directory, for example if you have used the Quickstart template to deploy a

HA File Server and SQL Server.

Go to the WorkersNsg in the Admin Portal and add an outbound security rule with

the following properties:

Source: Any

Source port range: \*

Destination: IP Addresses

Destination IP address range: Range of IPs for your AD Servers, for example with

the Quickstart template 10.0.0.100, 10.0.0.101

Destination port range: 389,88

Protocol: Any

Action: Allow

Priority: 710

Name: Outbound\_Allow\_LDAP\_and\_Kerberos\_to\_Domain\_Controllers

Custom domains are not supported in disconnected environments

App Service performs domain ownership verification against public DNS endpoints, as a

result custom domains are not supported in disconnected scenarios.

For an overview of Azure App Service, see Azure App Service on Azure Stack

overview.

Known issues for Cloud Admins operating Azure App

Service on Azure Stack

Next steps

For more information about how to prepare to deploy App Service on Azure Stack,

see Before you get started with App Service on Azure Stack.

App Service on Azure Stack Hub 2021

Q1 release notes

Article • 12/10/2021

These release notes describe the improvements and fixes in Azure App Service on Azure

Stack Hub 2021 Q1 and any known issues. Known issues are divided into issues directly

related to the deployment, update process, and issues with the build (post-installation).

Supported Azure Stack Hub version App Service RP version

2301 2302 Installer (release notes)

2206.2.52 2302 Installer (release notes)

2108.2.127 2302 Installer (release notes)

The App Service on Azure Stack Hub 2021 Q1 build number is 91.0.2.20

Refer to the Before You Get Started documentation before beginning deployment.

Before you begin the upgrade of Azure App Service on Azure Stack to 2021 Q1:

Ensure your Azure Stack Hub is updated to 2102.

Ensure all roles are Ready in the Azure App Service Administration in the Azure

Stack Hub Admin Portal

Backup App Service Secrets using the App Service Administration in the Azure

Stack Hub Admin Portal

） Important

Update Azure Stack Hub to a supported version (or deploy the latest Azure Stack

Development Kit) if necessary, before deploying or updating the App Service

resource provider (RP). Be sure to read the RP release notes to learn about new

functionality, fixes, and any known issues that could affect your deployment.

Build reference

Prerequisites

Back up the App Service and SQL Server Master Databases:

AppService\_Hosting;

AppService\_Metering;

Master

Back up the Tenant App content file share

Syndicate the Custom Script Extension version 1.9.3 from the Marketplace

Azure App Service on Azure Stack Update 2021 Q1 includes the following improvements

and fixes:

Updates to App Service Tenant, Admin, Functions portals and Kudu tools.

Consistent with Azure Stack Portal SDK version.

Addition of Full Screen Create experience for Web and Function Apps

New Azure Functions Portal Experience to be consistent with Web Apps

Updates Azure Functions runtime to v1.0.13154.

Updates to core service to improve reliability and error messaging enabling easier

diagnosis of common issues.

Updates to the following application frameworks and tools:

ASP.NET Core 5.0.4

.NET Framework 4.8

NodeJS

14.15.0

NPM

1.1.37

1.2.30

1.3.11

Updated Kudu to 90.21106.4900

） Important

Cloud operators are responsible for the maintenance and operation of the File

Server and SQL Server. The resource provider does not manage these

resources. The cloud operator is responsible for backing up the App Service

databases and tenant content file share.

Updates

Updates to underlying operating system of all roles:

2021-06 Cumulative Update for Windows Server 2016 for x64-based Systems

(KB5003638)

2021-04 Servicing Stack Update for Windows Server 2016 for x64-based

Systems (KB5001402)

Defender Definition 1.341.322.0

Cumulative Updates for Windows Server are now applied to Controller roles as

part of deployment and upgrade

MMC-based management console replaced with WPF application for improved

accessibility

TLS Cipher Suites updated to maintain consistency with Azure Service. From this

release onwards, suites will be updated with each update

Custom Shared SKU tenant usage not showing in tenant usage reports

Unable to select subscription and location when using Service Principal to

deploy/upgrade

Log scavenger on infrastructure roles

Added step to wait for management

If generated storage account names exceed 24 characters, installation fails as

storage account names may not exceed 24 characters

Remote git push error: Invalid Version: transformer

Review the known issues for update and take any action prescribed.

Issues fixed in this release

Pre-Update steps

Post-deployment steps

） Important

If you have provided the App Service resource provider with a SQL Always On

Instance you MUST add the appservice\_hosting and appservice\_metering

In situations where a customer has converted the appservice\_hosting and

appservice\_metering databases to contained database, upgrade may fail if logins

have not been successfully migrated to contained users

Customers that have converted the appservice\_hosting and appservice\_metering

databases to contained database post deployment, and have not successfully migrated

the database logins to contained users, may experience upgrade failures.

Customers must execute the following script against the SQL Server hosting

appservice\_hosting and appservice\_metering before upgrading your Azure App Service

on Azure Stack Hub installation to 2020 Q3. This script is non-destructive and will not

cause downtime.

This script must be run under the following conditions

By a user that has the system administrator privilege, for example the SQL SA

Account;

If using SQL Always on, ensure the script is run from the SQL instance that contains

all App Service logins in the form:

appservice\_hosting\_FileServer

appservice\_hosting\_HostingAdmin

appservice\_hosting\_LoadBalancer

appservice\_hosting\_Operations

appservice\_hosting\_Publisher

appservice\_hosting\_SecurePublisher

appservice\_hosting\_WebWorkerManager

appservice\_metering\_Common

appservice\_metering\_Operations

All WebWorker logins - which are in the form WebWorker\_<instance ip

address>

SQL

databases to an availability group and synchronize the databases to prevent any

loss of service in the event of a database failover.

Known issues (update)

USE appservice\_hosting

IF EXISTS(SELECT \* FROM sys.databases WHERE Name=DB\_NAME() AND

containment = 1)

BEGIN

DECLARE @username sysname ;

DECLARE user\_cursor CURSOR

FOR

SELECT dp.name

FROM sys.database\_principals AS dp

JOIN sys.server\_principals AS sp

ON dp.sid = sp.sid

WHERE dp.authentication\_type = 1 AND dp.name NOT IN

('dbo','sys','guest','INFORMATION\_SCHEMA');

OPEN user\_cursor

FETCH NEXT FROM user\_cursor INTO @username

WHILE @@FETCH\_STATUS = 0

BEGIN

EXECUTE sp\_migrate\_user\_to\_contained

@username = @username,

@rename = N'copy\_login\_name',

@disablelogin = N'do\_not\_disable\_login';

FETCH NEXT FROM user\_cursor INTO @username

END

CLOSE user\_cursor ;

DEALLOCATE user\_cursor ;

END

GO

USE appservice\_metering

IF EXISTS(SELECT \* FROM sys.databases WHERE Name=DB\_NAME() AND

containment = 1)

BEGIN

DECLARE @username sysname ;

DECLARE user\_cursor CURSOR

FOR

SELECT dp.name

FROM sys.database\_principals AS dp

JOIN sys.server\_principals AS sp

ON dp.sid = sp.sid

WHERE dp.authentication\_type = 1 AND dp.name NOT IN

('dbo','sys','guest','INFORMATION\_SCHEMA');

OPEN user\_cursor

FETCH NEXT FROM user\_cursor INTO @username

WHILE @@FETCH\_STATUS = 0

BEGIN

EXECUTE sp\_migrate\_user\_to\_contained

@username = @username,

@rename = N'copy\_login\_name',

@disablelogin = N'do\_not\_disable\_login';

FETCH NEXT FROM user\_cursor INTO @username

END

CLOSE user\_cursor ;

DEALLOCATE user\_cursor ;

END

GO

Workers are unable to reach file server when App Service is deployed in an existing

virtual network and the file server is only available on the private network, as called

out in the Azure App Service on Azure Stack deployment documentation.

If you chose to deploy into an existing virtual network and an internal IP address to

connect to your file server, you must add an outbound security rule, enabling SMB

traffic between the worker subnet and the file server. Go to the WorkersNsg in the

Admin Portal and add an outbound security rule with the following properties:

Source: Any

Source port range: \*

Destination: IP Addresses

Destination IP address range: Range of IPs for your file server

Destination port range: 445

Protocol: TCP

Action: Allow

Priority: 700

Name: Outbound\_Allow\_SMB445

To remove latency when workers are communicating with the file server we also

advise adding the following rule to the Worker NSG to allow outbound LDAP and

Kerberos traffic to your Active Directory Controllers if securing the file server using

Active Directory, for example if you have used the Quickstart template to deploy a

HA File Server and SQL Server.

Go to the WorkersNsg in the Admin Portal and add an outbound security rule with

the following properties:

Source: Any

Source port range: \*

Destination: IP Addresses

Destination IP address range: Range of IPs for your AD Servers, for example with

the Quickstart template 10.0.0.100, 10.0.0.101

Destination port range: 389,88

Protocol: Any

Action: Allow

Priority: 710

Name: Outbound\_Allow\_LDAP\_and\_Kerberos\_to\_Domain\_Controllers

Known issues (post-installation)

Known issues for Cloud Admins operating Azure App

Service on Azure Stack

Custom domains are not supported in disconnected environments

App Service performs domain ownership verification against public DNS endpoints, as a

result custom domains are not supported in disconnected scenarios.

For an overview of Azure App Service, see Azure App Service on Azure Stack

overview.

For more information about how to prepare to deploy App Service on Azure Stack,

see Before you get started with App Service on Azure Stack.

Next steps

Azure Container Registry on Azure Stack

Hub overview

Article • 06/01/2022

Azure Container Registry (ACR) on Azure Stack Hub provides your users with the ability

to store and manage container images and artifacts. With the Public Preview release,

your users can create and manage container registries by using the Azure Stack Hub

user portal as well as commands in PowerShell, Azure CLI, and the Docker CLI.

ACR on Azure Stack Hub allows users to store and retrieve OCI images, assign rolebased access control (RBAC) permissions, and create webhooks.

While a public preview, the Azure Container Registry on Azure Stack Hub can be used

without charge.

A local container registry enables users to manage a local repository of images as part

of a continuous integration, continuous delivery (CI/CD) pipeline for deployment to AKS

or other supported container orchestrators on Azure Stack Hub.

Features included with ACR on Azure Stack Hub include:

OCI artifact repository for adding Helm charts, Singularity support, and new OCI

artifact-supported formats.

Integrated security with Azure Active Directory (Azure AD) authentication or Azure

Active Directory Federated Services (AD FS), and role-based access control.

Webhooks for triggering events when actions occur in one of your registry

repositories.

） Important

Azure Container Registry on Azure Stack Hub is currently in PREVIEW. See the

Supplemental Terms of Use for Microsoft Azure Previews for legal terms that

apply to Azure features that are in beta, preview, or otherwise not yet released into

general availability.

Why offer ACR on Azure Stack Hub?

ACR on Azure and ACR on Azure Stack Hub

Azure Stack Hub support for ACR compared to ACR on Azure:

Feature Azure Container Registry Azure Container Registry on Azure

Stack Hub

SKUs 3 skus (Basic, Standard,

Premium)

A single sku is available

Azure portal UX Available Available

PS/CLI Available Available

Webhooks Available Available

Geo-replication Available w/ Premium Not available

Additional Storage Available for additional

charge

Not available

Tasks Available Not available

Security Center

integration

Available Not available

Content Trust Available Not available

Private Networks Available Not available

The ACR service is an optional service that requires operators provide an additional

certificate to enable the service. For more information, see Install Azure Container

Registry on Azure Stack Hub

Add items to the Azure Stack Hub Marketplace

Next steps

Install Azure Container Registry on

Azure Stack Hub

Article • 09/22/2022

You can install the Azure Container Registry (ACR) on Azure Stack Hub and make it

available to your users so that they can host containers in your environment. To install

the ACR, you will need to generate and validate a certificate and install the ACR. You can

install through the Azure Stack Hub administrative portal.

Azure Stack Hub version

You can only enable the Microsoft Azure Container in an Azure Stack Hub

integrated system running the 2108 update and later releases. Install the Azure

Stack Hub update before you complete the steps in this article. The Azure

Container Registry (ACR) service is not supported on the Azure Stack Developer Kit

(ASDK) deployments.

Certificate requirements

The configuration of the ACR on your Azure Stack Hub system adds a new data

path that requires a certificate. The certificate must meet the same requirements as

the other certificates required to install and operate Azure Stack Hub. Additionally,

it must not be a Cyptography: Next Generation (CNG) certificate, as these are not

currently supported by the public preview of ACR on Azure Stack Hub. You can find

more information in the article, "Azure Stack Hub public key infrastructure (PKI)

certificate requirements."

The URI for this new certificate should have the following format:

\*.azsacr.<region>.<fqdn>

For example:

\*.azsacr.azurestack.contoso.com

） Important

Once installed, Azure Container Registry on Azure Stack Hub is considered a

foundational RP and cannot be uninstalled. Operators can still restrict user access

to the ACR service through offers, plans, and quotas.

Prerequisites

Azure Stack Hub state

Only after validating that your Azure Stack Hub is healthy should you install ACR.

You can do so by following the steps listed on "Validate Azure Stack Hub system

state."

You can use the following steps to generate an ACR certificate using The Azure Stack

Hub Readiness Checker tool. You must specific the version of the

Microsoft.AzureStack.ReadinessChecker module for the steps to work.

1. Open PowerShell with an elevated prompt.

2. Run the following cmdlets:

PowerShell

3. When the ReadinessChecker module creates the.req\*\* file, sub the file to your

Certificate Authority (CA) (either internal or public). The output directory of NewAzsCertificateSigningRequest contains the CSR(s) necessary to submit to a CA. For

your reference, the directory also contains a child directory containing the INF

file(s) used during certificate request generation.

Validate the ACR certificate adheres to Azure Stack Hub requirements.

1. Copy resulting certificate file (.cer) signed by the CA (supported extensions .cer,

.cert, .srt, .pfx) to $ENV:USERPROFILE\Documents\AzureStack .

2. Run the following PowerShell cmdlets from an elevated prompt:

Generate your certificate

Install-Module -Name Microsoft.AzureStack.ReadinessChecker

New-Item -ItemType Directory

"$ENV:USERPROFILE\Documents\AzsCertRequests"

$certificateRequestParams = @{

'regionName' = 'azurestack'

'externalFQDN' = 'contoso.com'

'subject' = "C=US,ST=Washington,L=Redmond,O=Microsoft,OU=Azure

Stack"

'OutputRequestPath' =

"$ENV:USERPROFILE\Documents\AzsCertRequests" }

New-AzsHubAzureContainerRegistryCertificateSigningRequest

@certificateRequestParams

Validate the ACR certificate

PowerShell

You can use these steps to install the ACR service in Azure Stack Hub.

You can use the Azure Stack Hub administration portal to import the certificate and

install the service.

1. Sign into the Azure Stack Hub administration portal.

2. Navigate to All Services > Container Registries.

3. Enter the full path to the SSL certificate.

4. Enter the password for the certificate.

5. Select Deploy.

Installation of the ACR service may take up to one hour.

Install-Module -Name Microsoft.AzureStack.ReadinessChecker

$Path = "$ENV:USERPROFILE\Documents\AzureStack"

$pfxPassword = Read-Host -AsSecureString -Prompt "PFX Password"

ConvertTo-AzsPFX -Path $Path -pfxPassword $pfxPassword -ExportPath

$Path

Installation steps

Portal

6. Once the install completes in the Azure Stack Hub administration portal, close and

reopen the Container Registries blade.

Once the installation is complete, you can review or update your capacity in quota in the

Azure Stack Hub administrative portal.

Azure Container Registries on Azure Stack Hub overview

Next steps

Manage capacity and quotas for Azure

Container Registry on Azure Stack Hub

Article • 06/01/2022

Unlike Azure, Azure Stack Hub resources have physical constraints for memory and

storage based on the configuration and number of available physical nodes. You have

several options for limiting the amount of storage consumed by your user's containers

and OCI artifacts.

You can manage your container registry in the Azure Stack Hub administrative portal.

1. Sign in to the Azure Stack Hub administrator portal.

2. Type Container Registry in the search.

3. Select Configure.

4. You can increase or decrease the capacity from the default of 2000 GB. Add your

number, and then select Configure.

You can view the current storage usage by container registries in the Azure Stack Hub

administrative portal. In the same view, you can compare utilized capacity to the

maximum allocated capacity for the ACR in your Azure Stack Hub.

1. Sign in to the Azure Stack Hub administrator portal.

Set storage capacity

View storage use

2. Type Container Registry in the search.

3. Select Overview.

Besides restricting overall storage capacity used by container registries, you can limit the

use of the container registry service with the following quotas:

Storage capacity per registry (GB)

The maximum amount of storage that can be used by any registry. Registries by

default are limited to a maximum of 100 GB of storage, but you can offer more

limited quotas based on user deployments and user requirements.

Maximum number of registries

You can limit the number of registries that can be created per subscription.

You can find more guidance on offers, plans, and quotas in the article, Azure Stack Hub

services, plans, offers, subscriptions overview

Azure Container Registries on Azure Stack Hub overview

Quota settings

Next steps

Troubleshoot Azure Container Registry

on Azure Stack Hub for cloud operators

Article • 06/06/2022

As an Azure Stack Hub cloud operator you may need to troubleshoot or raise support

issues with Microsoft during installation of Azure Container Registry (ACR), or due to

issues hit by users of ACR on Azure Stack Hub. This document provides guidance on

how to collect specific logs for ACR and collect other details required when raising

support requests.

Users of ACR on Azure Stack Hub have troubleshooting guidance available for self-help.

If they are unable to resolve an issue with their registry, they may need the operator's

help in creating a support request. When creating a support request for a user registry

issue the Resource ID will be required during case creation. Users have guidance to find

this, but Operators can also find this using the following steps.

1. Open the Azure Stack Hub administration portal, and then open Container

Registries.

2. Select Registries under User Resources.

3. Search for the name of the registry in the list view

Find the Resource ID for a registry



4. Select the registry to view the detail

5. Copy the Resource ID field.

ACR logs are collected when collecting logs from the Azure Stack Hub administration

portal or during a full run of Send-AzureStackDiagnosticLog. There may be

circumstances where you just want to collect logs specific to ACR, for example, if you are

collecting for more than a four-hour period.

To collect ACR logs for ACR issues including installation issues, run SendAzureStackDiagnosticLog with the following parameters:

PowerShell

To collect ACR logs for ACR issues, excluding installation issues, run SendAzureStackDiagnosticLog with the following parameters:

PowerShell



Collect logs for support

Collecting logs for ACR install issues

Send-AzureStackDiagnosticLog -FilterByResourceProvider ACR -FilterByRole

FabricRingServices,ECE,CLM

Collecting logs for all other ACR issues

Send-AzureStackDiagnosticLog -FilterByResourceProvider ACR -FilterByRole

FabricRingServices

Azure Container Registries on Azure Stack Hub overview

Next steps

Install and offer the Azure Kubernetes

Service on Azure Stack Hub

Article • 05/17/2023

Azure Kubernetes Service (AKS) enables your users to deploy Kubernetes clusters in

Azure Stack Hub. AKS reduces the complexity and operational overhead of managing

Kubernetes clusters. As a hosted Kubernetes service, Azure Stack Hub handles critical

tasks like health monitoring and facilitates maintenance of clusters. The Azure Stack Hub

team manages the image used for maintaining the clusters. The cluster tenant

administrator only needs to apply the updates as needed. The services come at no extra

cost. AKS is free: you only pay to use the virtual machines (VMs) master and agent

nodes within your clusters. You can install the Azure Kubernetes Service (AKS) resource

provider for the users of your Azure Stack Hub.

To install, you must have the VM extensions, the AKS base image, a plan and offer to

your users, and enable multi-tenancy for your Azure Stack Hub. AKS clusters can only be

created in the user environment.

Make sure that the following VM extensions are available in your Azure Stack Hub.

） Important

Azure Kubernetes Service on Azure Stack Hub, currently in preview, is being

discontinued and will not become GA. See AKS Engine for a Kubernetes solution on

Azure Stack Hub. See the Supplemental Terms of Use for Microsoft Azure

Previews for legal terms that apply to Azure features that are in beta, preview, or

otherwise not yet released into general availability.

７ Note

Azure Kubernetes Service on Azure Stack Hub doesn't support the creation of a

cluster in the administration environment. You can only create AKS clusters in the

user environment.

Download required VM extensions

Get the extensions from the portal

You can find the VM extensions in the Azure Stack Hub Marketplace. You can download

them from Azure if you need to add them to a disconnected environment. Follow the

instructions in Download Marketplace items to Azure Stack Hub (Disconnected):

Run command for Linux (latest version)

Custom script for Linux (version 2.0.6)

PowerShell provides a Get-AzsVMExtension cmdlet to view the VM extensions available

in your system. Run the following script to view the available extensions. Specify the

correct URL for your Azure Stack Hub Resource Manager endpoint:

View the extensions with PowerShell

PowerShell

For information about installing and using the AzureStack PowerShell module, see Install

PowerShell Az module for Azure Stack Hub.

The AKS Service needs a special VM image referred to as the AKS base image. The AKS

service doesn't work without the correct image version available in the local Azure Stack

Hub Marketplace. The image is meant to be used by the AKS service, not to be used by

tenants to create individual VMs. The image is not visible to tenants in the Marketplace.

This is a task that needs to be done along with every Azure Stack Hub update. Every

time there is a new update, there is a new AKS base image associated with the AKS

service. Here are the steps:

1. Using the administrator portal, go the Marketplace management blade and select

Add from Azure.

2. Type AKS in the search box. Locate and download both the Linux AKS Base

Ubuntu 18.04-LTS Image Distro, 2022 Q1 version 2022.01.21 and the AKS Base

Windows Image version 17763.2300.220121.

Linux base image:

Windows base image:

Add-AzureRMEnvironment -Name "AzureStackAdmin" -ArmEndpoint

"https://adminmanagement.<location>.<yourdomainname>/"

Login-AzureRMAccount -EnvironmentName "AzureStackAdmin"

Get-AzsVMExtension

Download AKS base image



3. If your instance is disconnected, follow the instructions in the article Download

Marketplace items to Azure Stack Hub to download the two specified items from

the marketplace in Azure, and upload them to your Azure Stack Hub instance.

To allow tenant users to use the AKS service, the operator must make it available

through a plan and an offer.

1. Create a plan with the Microsoft.Container service. There are no specific quotas

for this service; it uses the quotas available for the Compute, Network, and Storage

services:

2. Again, use the Azure Stack Hub administration portal to create an offer that

contains the plan created in the prior step:



Create plans and offers

You must configure Azure Stack Hub to support sign-ins from users that reside in other

Azure Active Directory (Azure AD) directories, allowing them to use services in Azure

Stack Hub.

For instructions, see Configure multi-tenancy in Azure Stack Hub

1. Using the administrative portal, you can access the Azure Kubernetes Service

under the Administration group.

2. Select the Alerts blade. Review the alerts:

Configure multi-tenancy

Monitor and act on alerts

3. Alerts appear in the Alerts blade, and you can take action on them if necessary:

Learn more about AKS on Azure Stack Hub

Next steps

Azure Site Recovery overview (preview)

Article • 06/19/2023

Azure Site Recovery on Azure Stack Hub helps ensure business continuity by keeping

business apps and workloads running during outages. Azure Site Recovery on Azure

Stack Hub replicates virtual machine (VM) workloads from a primary site to a secondary

location. When an outage occurs at your primary site, you fail over to a secondary

location, and access apps from there. After the primary location is running again, you

can fail back to it.

To enable replication of VMs across two Azure Stack Hub stamps, configure the

following environments:

Source environment is the Azure Stack Hub stamp where tenant VMs are running.

Azure Stack Hub Operator, download the Azure Site Recovery Appliance VM

and the Azure Site Recovery VM extensions in the Marketplace Management.

Azure Stack Users, in the user subscriptions, configure the connection to the

target vault in this source environment.

Target environment is where the Azure Site Recovery Resource Provider and

dependencies run.

Azure Stack Hub Operator, download the respective images.

Azure Stack Hub Users, configure the vault and prepare the prerequisites for

your replicated VMs.

） Important

During the public preview of Azure Site Recovery on Azure Stack Hub, updates

might require a complete re-installation (a complete removal and then re-add) of

the service.

Azure Site Recovery on Azure Stack Hub is available for both Azure Active Directory

(Azure AD) and Active Directory Federation Services (AD FS) type deployments of Azure

Stack Hub, which means it can run in disconnected environments.

Azure Site Recovery provides many features, as described in the following table.

Feature Details

BCDR

solution

Using Site Recovery, you can set up and manage replication, failover, and failback

from a single location in the Azure Stack Hub portal.

BCDR

integration

Site Recovery integrates with other BCDR technologies. For example, you can use

Site Recovery to protect the SQL Server backend of corporate workloads, with

native support for SQL Server Always On, to manage the failover of availability

groups.

Azure

Automation

integration

A rich Azure Automation library provides production-ready, application-specific

scripts that can be downloaded and integrated with Site Recovery.



What does Site Recovery provide?

Feature Details

RTO and

PRO targets

Keep recovery time objectives (RTO) and recovery point objectives (RPO) within

organizational limits. Site Recovery provides continuous replication for Azure Stack

Hub VMs.

Keep apps

consistent

over

failover

You can replicate using recovery points with application-consistent snapshots.

These snapshots capture disk data, all data in memory, and all transactions in

process.

Testing

without

disruption

You can easily run disaster recovery drills, without affecting ongoing replication.

Flexible

failovers

You can run planned failovers for expected outages with zero-data loss or

unplanned failovers with minimal data loss, depending on replication frequency, for

unexpected disasters. You can easily fail back to your primary site when it's

available again.

Customized

recovery

plans

Not currently available in public preview. Using recovery plans, you can customize

and sequence the failover and recovery of multi-tier applications running on

multiple VMs. You can group machines together in a recovery plan, and optionally

add scripts and manual actions.

Azure Site Recovery on Azure Stack Hub, with a required agent installed on each of the

protected VMs, enables the replication of VMs across two instances, or stamps, of Azure

Stack Hub. Azure Stack Hub uses a VM extension, available through the Azure Stack Hub

Marketplace, to install this agent.

We've tested and validated the following VM OSs and each has respective Azure Stack

Hub Marketplace images available for download:

Operating

system

Details

Windows

Server

2022

Supported.

What can I replicate?

Windows

Operating

system

Details

Windows

Server

2019

Supported for Server Core, Server with Desktop Experience.

Windows

Server

2016

Supported Server Core, Server with Desktop Experience.

Windows

Server

2012 R2

Supported.

Windows

Server

2012

Supported.

Windows

Server

2008 R2

with

SP1/SP2

Supported. From version 9.30 of the Mobility service extension for Azure

VMs, you need to install a Windows servicing stack update (SSU) and SHA-2

update on machines running Windows Server 2008 R2 SP1/SP2. SHA-1 isn't

supported from September 2019, and if SHA-2 code signing isn't enabled the

agent extension won't install or upgrade as expected. For more information,

see SHA-2 upgrade and requirements .

Windows

10 (x64)

Supported.

Windows

8.1 (x64)

Supported.

Windows

8 (x64)

Supported.

Windows

7 (x64)

with SP1

onwards

Supported. From version 9.30 of the mobility service extension for Azure

VMs, install a Windows servicing stack update (SSU) and SHA-2 update on

machines running Windows 7 with SP1. From September 2019, SHA-1 isn't

supported, and if SHA-2 code signing isn't enabled the agent extension

won't install or upgrade as expected. For more information, see SHA-2

upgrade and requirements .

Azure Site Recovery on Azure Stack Hub capacity planning

Next steps

Deployment overview (preview)

Article • 09/01/2023

To enable replication of virtual machines (VMs) across two Azure Stack Hub

environments, you must configure the following environments:

The source environment. The Azure Stack Hub environment in which user VMs (the

actual workloads you want to protect) are running.

The target environment. The environment in which the Azure Site Recovery

resource provider and dependencies run.

During the public preview, Microsoft will release several versions for both the service

RPs and the extensions. The following is the complete list of currently available images:

） Important

During the public preview of Azure Site Recovery on Azure Stack Hub, updates

might require a complete re-installation (a complete removal and then re-add) of

the service.



Service Image name Image version

[target] ASR RP Microsoft.SiteRecovery 1.2301.2216.2287

[target] ASR

DependencyService

microsoft.servicebus 1.2210.4.0

[source] Appliance VM microsoft.asrazsappliance 1.8.7

[source] Extension

(Windows)

microsoft.azure-recoveryservices-siterecoverywindows

1.1.31.388

[source] Extension (Linux

general)

microsoft.azure-recoveryservices-siterecoverylinux

1.0.31.559

[source] Extension (RHEL 6) microsoft.azure-recoveryservices-siterecoverylinuxRHEL6

1.0.31.559

[source] Extension (RHEL 7) microsoft.azure-recoveryservices-siterecoverylinuxRHEL7

1.0.31.559

[source] Extension (RHEL 8) microsoft.azure-recoveryservices-siterecoverylinuxRHEL8

1.0.31.559

[source] Extension (Debian

8)

microsoft.azure-recoveryservices-siterecoverylinuxdebian8

1.0.31.559

[source] Extension (Debian

9)

microsoft.azure-recoveryservices-siterecoverylinuxDEBIAN9

1.0.31.559

[source] Extension (Debian

10)

microsoft.azure-recoveryservices-siterecoverylinuxdebian10

1.0.31.559

[source] Extension (Debian

11)

microsoft.azure-recoveryservices-siterecoverylinuxdebian11

1.0.31.559

[source] Extension (Ubuntu

1604)

microsoft.azure-recoveryservices-siterecoverylinuxubuntu1604

1.0.31.559

[source] Extension (Ubuntu

1804)

microsoft.azure-recoveryservices-siterecoverylinuxUBUNTU1804

1.0.31.559

[source] Extension (Ubuntu

1404)

microsoft.azure-recoveryservices-siterecoverylinuxUBUNTU1404

1.0.31.559

[source] Extension (OL7) microsoft.azure-recoveryservices-siterecoverylinuxOL7

1.0.31.559

[source] Extension (OL8) microsoft.azure-recoveryservices-siterecoverylinuxOL8

1.0.31.559

Service Image name Image version

[source] Extension (SLES

12)

microsoft.azure-recoveryservices-siterecoverylinuxSLES12

1.0.31.559

[source] Extension (SLES

15)

microsoft.azure-recoveryservices-siterecoverylinuxSLES15

1.0.31.559

The process to install Azure Site Recovery includes actions from both the Azure Stack

Hub operator and the Azure Stack Hub user:

Operators must perform the following steps:

Ensure that required networking requirements are in place for both source and

target environments.

Source: prepare the environment.

Download the Azure Site Recovery appliance on AzureStack Hub VM image

and the respective Azure Site Recovery – extensions in the Azure Stack Hub

Marketplace Management.

Ensure that Azure Stack Hub users can deploy the ASR appliance on AzureStack

Hub VM image in their respective Azure Stack Hub user subscriptions (where

the VM workloads run).

Target: prepare the environment by installing Site Recovery services and

dependencies, ensuring the right quotas are assigned to the respective plans and

offers where Site Recovery will be used.

Users must perform the following steps:

Source:

Deploy the Azure Site Recovery appliance on AzureStack Hub VM image in the

Azure Stack Hub user subscription.

The user must have owner rights on each Azure Stack Hub user subscription in

which they protect VM workloads.

Target:

Deploy the Azure Site Recovery Vault.

Create the protection policies and enable the protection of the workloads.

Operators

Users

Because the source and target Azure Stack Hubs might be in different datacenters,

regions, or security boundaries, the Azure Stack Hub operator must make sure the

networking connectivity is in place and configured in order for the Azure Site Recovery

services to function:

Name resolution

The Azure Site Recovery appliance running on the source Azure Stack Hub

instance must be able to resolve the FQDN of the target Azure Stack Hub

instance.

The Azure Site Recovery appliance running on the source Azure Stack Hub instance

should be able to access the following ports on the source site:

(When in use) Azure AD: \*.microsoftonline.com:443

(When in use) AD FS: adfs.< external-FQDN >:443

Azure Resource Manager: management.< external-FQDN >:443

The Azure Site Recovery appliance must be able to access the following ports of

the target Azure Stack Hub instance:

(When in use) Azure AD: \*.microsoftonline.com:443

(When in use) AD FS: adfs.< external-FQDN >:443

Azure Resource Manager: management.< external-FQDN >:443

Blob: \*.blob.< external-FQDN >:443

Azure Site Recovery: rp.asr.< external-FQDN >:8478,8479,44307

For more information about configuring the source and target environments, see the

following articles:

Deploy for source environments

Deploy for target environments

Check the Known issues.

Networking requirements

Next steps

Deploy for source environments

(preview)

Article • 06/08/2023

This article describes the actions that are required to complete the installation of the

source environment.

As an Azure Stack Hub operator, download the ASR appliance on AzureStack Hub VM

image and the respective Azure Site Recovery – extensions in the Azure Stack Hub

Marketplace Management.

For a disconnected or partially connected scenario, download the packages to your local

machine then import them into your Azure Stack Hub Marketplace:

1. Follow the instructions in Download Marketplace items: disconnected or partially

connected scenario. Download and run the Marketplace Syndication tool, which

enables you to download resource provider packages.

2. After the Azure Marketplace Items syndication tool window opens, find and select

the name of the resource provider to download the required packages to your

local machine.

3. Once the download finishes, import the packages to your Azure Stack Hub

instance and publish to the Marketplace.

For a connected scenario, download the items from Azure Marketplace directly to the

Azure Stack Hub Marketplace:

1. Sign in to the Azure Stack Hub administrator portal.

2. Select Marketplace Management.

3. Select Marketplace Items.

4. Select + Add from Azure.

） Important

Azure Site Recovery on Azure Stack Hub requires the Azure Stack Hub 2301 update

build number to be at least 1.2301.2.58.

Prerequisites

5. Search for "Azure Site Recovery" using the search bar.

6. The ASR appliance on AzureStack Hub is the VM that you must download. Based

on the type of VMs you want to protect, select and download the respective

Virtual Machine Extensions for each of the VM types to be protected.

7. Once the downloads are complete, you are ready to deploy and configure the

appliance.

In the source environment, in the Azure Stack Hub user subscription, you must now

deploy the ASR appliance on AzureStack Hub. This is a VM that appears in the Azure

Stack Hub Marketplace. Following the template, it creates a VM that has the following

properties:



Installation

Size: standard DS4 v2 (8 vcpus, 28 GiB memory). This means that by default, the

VM can have 32 data disks attached. This is important when doing a "failback"

operation; for example, when having more than 31 disks from protected VMs

generates an error (in which case the appliance VM must have its size increased).

By default, the Site Recovery appliance itself consumes one disk, and each data

disk from a protected VM must be attached.

Uses a 610 Gib disk.

Uses a storage account. Appliance boot diagnostics data is stored here.

After the deployment of the VM completes, sign in through RDP on that VM. This

launches a set of PowerShell scripts that install all the requirements for the Site

Recovery appliance and prepares the VM to be configured.

To start this process, open the Microsoft Azure Appliance Configuration Manager from

the desktop of the Site Recovery appliance on Azure Stack Hub. Follow the wizard while

using all the data from the vault connection properties, and the appliance is then

configured.

７ Note

During the configuration of the appliance, you must provide a user (or SPN) which

the appliance then uses for discovery. This user (or SPN) must have owner rights on

these subscriptions, both to discover resources as well as delegate rights as

needed. The Site Recovery Vault discovers all the VMs this user (or SPN) has access

to, within the respective tenant.

Azure Site Recovery overview

Download Marketplace items - Disconnected or partially connected scenario



Next steps

Deploy for target environments

(preview)

Article • 08/11/2023

This article describes the actions that are required to complete the installation of the

target environment.

In the target environment, Azure Site Recovery requires the Azure Stack Hub operator to

install the Azure Site Recovery - dependency service. Once this service is installed, you

can install the Azure Site Recovery service itself.

For the installation of these services, you must obtain 2 public key infrastructure (PKI)

SSL certificates. The Subject Alternative Name (SAN) must adhere to the naming pattern

described in PKI certificate requirements. The following 2 certificates are required:

1. For Azure Site Recovery dependency service: \*.servicebus.<region>.<fqdn> .

2. For Azure Site Recovery service: rp.asr.<region>.<fqdn> or \*.asr.<region>.

<fqdn> .

） Important

Azure Site Recovery on Azure Stack Hub requires the Azure Stack Hub 2301 update

build number to be at least 1.2301.2.58.

Prerequisites

７ Note

With Microsoft.SiteRecovery-1.2301.2216.2287, Azure Site Recovery on Azure Stack

Hub does not require Event Hubs as a dependency.

Once these 2 certificates are ready, installation on the target requires that you download

each of these images from Marketplace Management, and start each respective

installation.

Before installing or updating a resource provider, you must download the required

packages to the Azure Stack Hub Marketplace Management. The download process

varies, depending on whether your Azure Stack Hub instance is connected to the

Internet, or disconnected.

First, install the Azure Site Recovery - dependency service - there is no special

configuration required.



Download and install packages

７ Note

The download process can take 30 minutes to 2 hours, depending on the network

latency and existing packages on your Azure Stack Hub instance.

Disconnected scenario

For a disconnected or partially connected scenario, download the packages to your local

machine, then import them into your Azure Stack Hub Marketplace:

1. Follow the instructions in Download Marketplace items - Disconnected or partially

connected scenario. Download and run the Marketplace Syndication tool, which

enables you to download resource provider packages.

2. After the Azure Marketplace Items syndication tool window opens, find and select

the name of the resource provider to download the required packages to your

local machine.

3. Once the download finishes, import the packages to your Azure Stack Hub

instance and publish to the Marketplace.

For a connected scenario, download the items from Azure Marketplace directly to the

Azure Stack Hub Marketplace:

1. Sign in to the Azure Stack Hub administrator portal.

2. Select Marketplace Management on the left-hand side.

3. Select Resource providers.

4. Select + Add from Azure.

5. Search for Azure Site Recovery – dependency service and the Azure Site recovery

resource provider using the search bar.

Connected scenario



6. Download both resource providers.

7. Once both resource providers are downloaded, select each of them and start the

installation of the prerequisites, and then the resource provider itself. You are

asked for the certificates you generated in the prerequisites section.

8. The installation of each resource provider (Azure Site Recovery - dependency

service and Azure Site Recovery) usually takes 1.5 hours to complete.





Create plans and offers

Once Azure Site Recovery on Azure Stack Hub and its dependencies are installed, the

next step is to ensure that users have the correct offers assigned to their respective

Azure Stack Hub user subscriptions.

The process is similar to Create an offer in Azure Stack Hub, and you must add the

respective Microsoft.DataReplication service to the plan you intend to use. This can be

either a plan to a new offer, or used as an add-on to an existing offer:

The Microsoft.DataReplication service does not enforce any quotas. Instead, you can

rely on the existing quotas (for VM, Compute, Storage, and so on) to ensure that users

can create whatever resources they are allowed to create, conforming with the capacity

planning in place.

After the installation of the Azure Site Recovery resource provider and the assignment of

the correct plans to the Azure Stack Hub user subscriptions, the owner of this user

subscription must do the following:

Make sure the subscription has the following namespaces registered:

Microsoft.DataReplication, Microsoft.Compute, Microsoft.Storage,

Microsoft.Network, Microsoft.KeyVault.



Azure Stack Hub user subscription

Once these are configured, the users of this subscription are ready to create an

Azure Site Recovery Vault and start protecting workloads.

In the target environment, in the Azure Stack Hub user subscription in which you plan to

protect workloads, the user must create a Site Recovery Vault. A vault is a storage entity

in the Azure Stack Hub target environment that contains data. The data are typically

copies of data, or configuration information for VMs.

To create a new vault, open the Azure Stack Hub user portal, select Create new resource,

and then select the Azure Site Recovery items in the Compute category:

Provide a resource group and a name for the new recovery vault. Once created, you can

open the vault to access the properties required in the Site Recovery VM appliance. In



Create the Site Recovery Vault



the recovery vault, you can either select Protect Workload or on the left-hand side,

select the Replicated items blade.

In the Replicated items blade, you can select Set up a new replication appliance. This

provides a registration key that you can use to configure the Site Recovery VM

appliance (in the source environment):

With this key you are ready to start the deployment source environment and configure

the Azure Site Recovery VM appliance.

Azure Site Recovery overview





Next steps

Enable VM protection in Azure Site

Recovery (preview)

Article • 05/17/2023

Once the target and the source environments are configured, you can start enabling the

protection of VMs (from the source to the target). All configuration is done on the target

environment, in the Site Recovery vault itself.

You can configure the replication policy for the respective VMs you want to protect in

the Site Recovery vault. These VMs are on the source environment, where they have

configured a specific resource group structure, virtual networks, public IPs, and NSGs.

Site Recovery helps replicate all the VM data itself, but before starting that, make sure

that the following prerequisites are met:

The target network connectivity is configured.

The target virtual networks are configured - where each of the protected VMs are

connected when a failover occurs.

These virtual networks can be configured in the same manner as the source

networks, or they can have a different design, depending on your disaster recovery

plan and goal.

Ensure that the new public and private IPs work as expected for the specific

workloads you are protecting (when failovers occur, the failed-over VMs have IPs

from the target environment).

The desired resource group configuration is created.

When configuring the replication, you can also create the resource groups, but for

a production environment, you should pre-create them according to your naming

policy and structure.

Ensure the right RBAC is assigned and the tagging is in place – all according to

your enterprise policy.

The "cache storage account" is created and available.

Prerequisites

The "cache storage account" is a temporary storage account used in the replication

process.

In the target environment, in the Azure Stack Hub user portal, open the Site Recovery

vault and select Protect workloads:

Select the appliance you have configured and check that it is healthy:

７ Note

The scope of this storage account is complex and the Plan capacity for

Hyper-V VM disaster recovery article clarifies these concepts. For Azure Site

Recovery on Azure Stack Hub, see the Capacity Planning article.

Enable replication



The blade then asks you to select the source environment and the source subscription.

You should see all the Azure Stack Hub User subscriptions to which the user (or SPN)

you have configured has access.

Select the subscription that contains the source workloads, and select the VMs for which

you plan to enable protection. You can protect up to 10 VMs at a time. We have made

PowerShell scripts available that can enable larger deployments.





Azure Site Recovery replicates all disks attached to the VM. In this version, all the disks

are protected.

In the next step, select the target environment configuration. This configuration includes

the networks the VMs connect to, and the cache storage account they use. You must use

PowerShell to configure the replication policy. We have provided scripts that help start

the customization process.



Review the selected configuration and enable the replication:



In the Site Recovery vault, in the Replicated Items blade, you can see each of the VMs

for which you enabled replication:

Selecting these items enables you to view the current state, edit the settings of that

protected item, or trigger actions such as a test failover:



Check replication progress and edit settings



Once a VM is protected and data replicated, there are further tasks you can perform:

Run a test failover:

You can run a test failover to validate your replication and disaster recovery

strategy, without any data loss or downtime. A test failover doesn't impact

ongoing replication, or your production environment. You can run a test failover

on a specific VM, or on a recovery plan containing multiple VMs.

A test failover simulates the failover of this VM (from the source to the target) by

creating the target VM. When doing a test failover, you can select:

The recovery point to fail over to:

Latest recovery point (lowest RPO): this option first processes all the data that

has been sent to the Site Recovery service, to create a recovery point for each

VM before failing over to it. This option provides the lowest RPO (Recovery

Point Objective), because the VM created after failover will have all the data

replicated to Site Recovery when the failover triggers.

Latest processed (lowest RTO): fails over all VMs in the plan to the latest

recovery point processed by Site Recovery. To see the latest recovery point

for a specific VM, check Latest Recovery Points in the VM settings. This

option provides a low RTO (Recovery Time Objective), because no time is

spent processing unprocessed data.

Latest app-consistent: fails over all the VMs in the plan to the latest

application-consistent recovery point processed by Site Recovery. To see the

latest recovery point for a specific VM, check Latest Recovery Points in the

VM settings.



Understand the different states for protected

VMs

Custom: use this option to fail over a specific VM to a particular recovery

point.

You cannot select the network at this point. The test failover network is

configured for each protected VM. If you need to change it, go back to the

properties of the protected VM, then select View or edit.

The test failover can help check the application behavior when failed over.

However, your source VM might still be running. You must consider this behavior

when doing a test failover.

When the test failover is complete, you can select Clean test failover. This option

deletes the test failover VM and all the test resources



７ Note

Azure Site Recovery replicates the VM completely when doing a test failover.

The VM runs on both source and target environments. You must take this into

account, as it might affect the behavior of your app.

Failover:

In the event of an issue on the source environment, you can choose to fail the

VMs over to the target environment.

When starting the failover process, you can Shut down machine before

beginning failover. Since this option moves the entire VM from the source to

the target, the source VM should be shut down before you select this option.

Once the failover process is complete, you must commit the changes in order to

fully complete the failover process. If you don't commit first, then try to re-





７ Note

If no test failover was done in the past 180 days, Site Recovery

recommends that you perform one before an actual failover. Skipping

validation of the replication via test failover can lead to data loss or

unpredictable downtime.

protect, the re-protect action first triggers a commit, and then continues with

the re-protect (therefore it takes longer because both operations are required).

After the source environment is healthy again, you can start a "failback" process.

This process is performed in two steps:

Run re-protect to start replicating the data back to the source.

Once data is fully replicated, run the planned failover to move the resource

back to the initial environment.

You can check the following section for a list of considerations needed during

each of these phases.

The following information is not necessary for normal operations. However, these notes

can help give you a better understanding of the processes that take place behind the

scenes.

For each of the states, there are several considerations:

Re-protect:

Ensure that the initial source subscription, the initial resource group, and the

virtual network/subnet of the initial primary NIC still exist on the primary stamp.

You can retrieve this information from the protected item using PowerShell:

PowerShell

The following image shows example output from this command:

７ Note

At this time we don't support re-enabling protection (after a failback process).

You must disable protection, remove the agent, and then enable protection

again for this VM. This process can be automated and we provide scripts to

help you get started.

Considerations

Get-AzResource -ResourceID

"/subscriptions/<subID>/resourceGroups/<RGname>/providers/Microsoft.

DataReplication/replicationVaults/<vaultName>/protectedItems/<vmName

>"

Before running re-protect for Linux VMs, ensure that the certificate of the Site

Recovery service is trusted on the Linux VMs that you want to re-protect. This

trust unblocks the VM registration with the Site Recovery service, which reprotection requires.

For Ubuntu/Debian VMs:

shell

For Red Hat VMs:

shell

Ensure that the Site Recovery appliance VM has enough data disk slots

available. The replica disks for re-protection are attached to the

appliance (check the Capacity Planning for more information).

During the re-protection process, the source VM (which would have the

sourceAzStackVirtualMachineId on the source stamp) is shut down once the

re-protect is triggered, and the OS disk and data disks attached to it are

detached and attached to the appliance as replica disks if they are the old ones.

The OS disk is replaced with a temporary OS disk of size 1GB.

Even if a disk can be re-used as replica in re-protect, but it is in a different

subscription from the appliance VM, a new disk is created from it in the same



sudo cp /var/lib/waagent/Certificates.pem /usr/local/share/cacertificates/Certificates.crt

sudo update-ca-certificates

sudo update-ca-trust force-enable

sudo cp /var/lib/waagent/Certificates.pem /etc/pki/catrust/source/anchors/

sudo update-ca-trust extract

subscription and resource group as the appliance, so that the new disk can be

attached to the appliance.

The attached data disks of the appliance should not be

modified/attached/detached/changed manually, as a re-protect manual resync

is not supported in public preview (see the known issues article). The reprotection cannot be recovered if the replica disks are removed.

Failback (planned failover): fail back a re-protected item from the target stamp to

the source stamp:

Ensure that the initial source subscription, the initial resource group, and the

virtual network/subnet of the initial primary NIC still exist on the source stamp.

You can retrieve this information from the protected item using PowerShell.

The VM with the sourceAzStackVirtualMachineId on the source stamp is

created with the replica disks and newly-created NICs if it does not exist; or it is

replaced with a replica OS disk and data disks if it exists.

If the VM with the sourceAzStackVirtualMachineId on the primary stamp exists,

all the disks attached to it are detached but not deleted, and the NICs remain

the same.

If the VM with the sourceAzStackVirtualMachineId on the primary stamp exists,

and if it is in a different subscription from the appliance VM, new disks are

created in the same subscription and resource group as the failback VM from

the replica ones detached from the appliance, so that the new disks can be

attached to the failback VM.

Commit that the failover/failback is done. The failed-over VM on the recovery

stamp is deleted after failback is committed.

Azure Site Recovery overview

Next steps

Capacity planning using Azure Site

Recovery (preview)

Article • 06/19/2023

As an organization, it's imperative to adopt a business continuity and disaster recovery

(BCDR) strategy that keeps your data safe, apps available, and workloads online during

planned and unplanned outages.

Through the replication of virtual machines (VMs) workloads from a primary site to a

secondary location, Azure Site Recovery on Azure Stack Hub provides services that can

support the safety of organizational data, application availability, and workloads during

outages. For example, when an outage occurs at your primary site, you fail over to a

secondary location to access your apps. As soon as the primary site is running again,

you can fail back to it. For more information, see About Site Recovery.

To enable replication of VMs across two Azure Stack Hub stamps, you configure two

environments:

Source environment:

The Azure Stack Hub stamp where tenant VMs are running.

Target environment:

Where the Azure Site Recovery Resource Provider and dependencies run.

An essential component for the success of a business continuity and disaster recovery

plan is capacity planning. During capacity planning, there are a few factors to consider:

Recovery time objectives (RTO) and recovery point objectives (RPO) for the specific

workloads that you want to protect.

Workloads and the application characteristics:

How often the data changes within the respective VM.

How much data is generated or removed?

How the application design looks and more?

VM sizes, the number of disks, and how each VM is tied to other VMs.

For solutions that require several VMs, understand in what order those VMs

need to be started.

Network bandwidth between the source and target environments. This component

can affect RPOs.

Each of these points is important and have broad implications when building a BCDR

plan.



The following sections list the main points to consider from an Azure Site Recovery

perspective. Each BCDR plan is different and is based on the specifics of the workloads

you plan to protect. Therefore, this list isn't comprehensive.

In the source environment, Azure Stack Hub runs the Azure Site Recovery VM appliance.

The VM is a Standard\_DS4\_v2 (8 vCPUs, 28-Gb memory, 32 data disks) VM that runs in

the Azure Stack Hub user subscription.

On the source environment, consider the following areas:

Quota:

You should have sufficient quota for creating the Azure Site Recovery VM

appliance. You need one or more, depending on the overall plan.

Storage for the Azure Site Recovery VM appliance:

The Azure Site Recovery VM appliance itself has the data requirements defined

by its VM size.

When planning for capacity, make sure the appliance VM has enough storage to

exercise the fail-back and re-protect mechanisms.

Bandwidth:

The initial replication generates high bandwidth usage.

Changes on each VM are replicated, depending on the replication policies and

each type of application.

In the target environment, there are two pieces to consider for capacity planning:

The Azure Site Recovery service requirements: how much is consumed to run Azure

Site Recovery, without necessarily protecting any workloads.

Source considerations

７ Note

If there are storage limitations, the fail-back and re-protect can fail with an

error An internal error occurred message. Users should check the event

logs on the appliance to confirm the actual Azure Resource Manager error.

For more information, see Known issues for Azure Site Recovery.

Target considerations

The protected workloads requirements.

The target environment requires one Azure Site Recovery vault to be created for each

Site Recovery appliance, to protect VMs from the source (one appliance per vault).

Although this isn't a limitation from a capacity perspective, it should be taken into

consideration when planning the design of the overall environment.

Installing Azure Site Recovery on Azure Stack Hub involves adding two dependencies as

well as the Azure Site Recovery Resource Provider (RP) itself:

Event Hubs on Azure Stack Hub

Azure Site Recovery dependency service

Azure Site Recovery

These three services are created on the Azure Stack Hub admin subscription and

managed by Azure Stack Hub itself, therefore there's no configuration required.

However, as with any service, these resources consume memory, storage, and have

certain vCPUs allocated:

Service vCore Memory Disk Size

Event Hubs 16 91 GB 800 GB

Dependency Service 12 42 GB 600 GB

Azure Site Recovery 12 42 GB 300 GB

Total 40 175 GB 1700 GB

Azure Site Recovery RP resources



７ Note

When creating the BCDR plan, consider all aspects of the protected workloads. The

following list isn't complete and should be treated as a starting point:

VM size, number of disks, disk size, IOPS, data churn, and new data created.

Network bandwidth considerations:

The network bandwidth that's required for delta replication.

The amount of throughput, on the target environment, that Azure Site Recovery

can get from source environment.

The number of VMs to batch at a time. This number is based on the estimated

bandwidth to complete initial replication in a given amount of time.

The RPO that can be achieved for a given bandwidth.

The effect on the desired RPO if lower bandwidth is provisioned.

Storage considerations:

How much data is required for the initial replication.

How many recovery points are held and how data increases, for each protected

VM, during these intervals.

How many quotas need to be assigned to the target Azure Stack Hub user

subscriptions, so that users have sufficient allocation.

The cache storage account for replication.

Compute considerations:

When failover occurs, the VMs are started on the target Azure Stack Hub user

subscriptions. Enough quota allocation must be in place to be able to start

these VM resources.

During the protection of the VM, when the protected VM is active on the source

environment, no VM-related-resources like vCPU, memory, etc. are consumed

on the target environment. These resources become relevant only during a

failover process such as test failover.

For the scope of Azure Site Recovery on Azure Stack Hub, here's a starting point for

calculations, especially for the cache storage account used:

1. If there's a failover, during normal operations, multiply the number of disks

replicated by the average RPO. For example, you might have (2MB \* 250s). The

cache storage account is normally a few KB to 500 MB per disk.

These resources are Azure Stack Hub services on the administration side of Azure

Stack Hub. Once installed, the platform manages these resources.

Protected workloads

2. If there's a failover, given a worst case scenario, multiply the number of disks

replicated by the average RPO over a full day.

3. Failback to the new VM. Calculate the sum of the disks size of each batch.

The entire disk must be copied to the cache storage account for the target

VM to apply, since the target is an empty disk.

The associated data is deleted once copied, but it's likely to see peak usage

with the sum of all disk sizes.

Create the BDCR plan based on the specifics of the solution you're trying to protect.

The following table is an example of tests run in our environments. You can use this

insight to get a baseline for your own application, but each workload differs:

Block size Throughput/disk

2 MB 2 MB/s

64 KB 2 MB/s

8 KB 1 MB/s

8 KB 2 MB/s

Number of disks

supported

Total

throughput

Total

OPS

Bottleneck

68 136 MB/s 68 storage

60 120 MB/s 2048 storage

28 28 MB/s 3584 Azure Site Recovery CPU and

memory

） Important

If some parts of Azure Site Recovery aren't working, but others are working,

there can be at most one day of difflog in the storage account before Azure

Site Recovery decides to time out.

Configuration

Result

Number of disks

supported

Total

throughput

Total

OPS

Bottleneck

16 32 MB/s 4096

To test further, we generated a consistent type of workload; for example, consistent

storage changes in blocks of 8 Kb that total up to 1 MB/s per disk. This scenario isn't

likely in a real workload, given that changes can happen at various times of the day, or

in spikes of various sizes.

To replicate these random patterns, we've also tested scenarios with:

120 VMs (80 Windows, 40 Linux) protected through the same Azure Site Recovery

VM appliance.

Each VM generating at random intervals, at least twice per hour, random blocks

totaling 5 Gb of data across five files.

Replication succeeded across all 120 VMs with a low-to-medium load on the

Azure Site Recovery services.

Applications and solution workloads have certain recovery time objective (RTO) and

recovery point objective (RPO) requirements. Effective business continuity and disaster

recovery (BCDR) design take advantage of both the platform-level capabilities that meet

these requirements, as we use the solution specific mechanisms. To design BCDR

capabilities, capture platform disaster recovery (DR) requirements and consider all these

factors in your design:

７ Note

8Kb is the smallest block size of data Azure Site Recovery supports. Any changes

less than 8Kb are treated as 8Kb.

７ Note

These numbers should be used as a baseline only. They don't necessarily

scale linearly. Adding another batch of the same number of VMs might

have less impact than the initial one. The results are highly dependent on

the type of workloads used.

How should you plan and test

Application and data availability requirements:

RTO and RPO requirements for each workload.

Support for active-active and active-passive availability patterns.

Support for multi-region deployments for failover, with component proximity for

performance. You might experience application operations with reduced

functionality or degraded performance during an outage.

Avoid using overlapping IP address ranges in production and DR networks.

Production and DR networks that have overlapping IP addresses require a

failover process that can complicate and delay application failover. When

possible, plan for a BCDR network architecture that provides concurrent

connectivity to all sites.

Sizing your target environments:

If you're using the source and target in a 1:1 manner, allocate slightly more

storage on your target environment. This is due to the way the history of the

disk bookmarks happen. This allocation isn't a 2x increase, since it only includes

changes to the data. Depending on the type of data and the changes expected,

and replication policies having a 1.5x to 2x more storage on the target ensure

that failover processes introduce no concerns.

You might consider having the target Azure Stack Hub environment as the

target for multiple Azure Stack Hub sources. In this case, you're lowering the

overall cost, but must plan for what happens when certain workloads go down;

for example, which source must be prioritized.

If your target environment is used for running other workloads, the BCDR plan

must include the behavior of these workloads. For example, you can run the

Dev/Test VMs on the target environment, and if an issue occurs with your

source environment, you can turn off all the VMs on the target to ensure

sufficient resources are available to start the protected VMs.

７ Note

The application might know natively to run on, or have certain components

that are able to run across multiple Azure Stack Hub environments. In that

case, you can use Azure Site Recovery to replicate only the VMs with the

components that don't have this functionality; for example, a front-end or

back-end type solution, in which you can deploy the front-ends across Azure

Stack Hub environments.

You should test the BCDR and validate regularly. You can do this by using test failover

processes, or by moving the entire workloads to validate the flows end-to-end.

Azure Site Recovery on Azure Stack Hub

Next steps

Known issues - Azure Site Recovery on

Azure Stack Hub (preview)

Article • 06/19/2023

This article describes known issues for Azure Site Recovery on Azure Stack Hub. Use the

following sections for details about the current known issues and limitations in Azure

Site Recovery on Azure Stack Hub.

1. Ensure the appliance VM has enough data disk slots, as the replica disks for reprotection are attached to the appliance.

2. The initial allowed number of disks being re-protected at the same time is 31. The

default size of the appliance created from the marketplace item is

Standard\_DS4\_v2, which supports up to 32 data disks, and the appliance itself uses

one data disk.

3. If the sum of the protected VMs is greater than 31, perform one of the following

actions:

Split the VMs that require re-protection into smaller groups to ensure that

the number of disks re-protected at the same time doesn't exceed the

maximum number of data disks the appliance supports.

Increase the size of the Azure Site Recovery appliance VM.

4. If you're trying to re-protect a VM, but there aren't enough slots on the appliance

to hold the replication disks, the error message An internal error occurred

displays. You can check the number of the data disks currently on the appliance, or

sign in to the appliance, go to Event Viewer, and open logs for Azure Site

Recovery under Applications and Services Logs:

Re-protection: available data disk slots on

appliance

７ Note

We do not test and validate large VM SKUs for the appliance VM.

Find the latest warning to identify the issue.





Linux VM kernel version not supported

1. Check your kernel version by running the command uname -r .

For more information about supported Linux kernel versions, see Azure to Azure

support matrix.

2. With a supported kernel version, the failover, which causes the VM to perform a

restart, can cause the failed-over VM to be updated to a newer kernel version that

may not be supported. To avoid an update due to a failover VM restart, run the

command sudo apt-mark hold linux-image-azure linux-headers-azure so that the

kernel version update can proceed.

3. For an unsupported kernel version, check for an older kernel version to which you

can roll back, by running the appropriate command for your VM:

Debian/Ubuntu: dpkg --list | grep linux-image

RedHat/CentOS/RHEL: rpm -qa kernel

The following image shows an example in an Ubuntu VM on version 5.4.0-1103-

azure, which is unsupported. After the command runs, you can see a supported

version, 5.4.0-1077-azure, which is already installed on the VM. With this

information, you can roll back to the supported version.

4. Roll back to a supported kernel version using these steps:

a. First, make a copy of /etc/default/grub in case there's an error; for example,

sudo cp /etc/default/grub /etc/default/grub.bak .

b. Then, modify /etc/default/grub to set GRUB\_DEFAULT to the previous version

that you want to use. You might have something similar to

GRUB\_DEFAULT="Advanced options for Ubuntu>Ubuntu, with Linux 5.4.0-

1077-azure".





c. Select Save to save the file, then select Exit.

d. Run sudo update-grub to update the grub.

e. Finally, reboot the VM and continue with the rollback to a supported kernel

version.

5. If you don't have an old kernel version to which you can roll back, wait for the

mobility agent update so that your kernel can be supported. The update is

completed automatically, if it's ready, and you can check the version on the portal

to confirm:





Re-protect manual resync isn't supported yet

After the re-protect job is complete, the replication is started in sequence. During

replication, there may be cases that require a resync, which means a new initial

replication is triggered to synchronize all the changes.

There are two types of resync:

Automatic resync. Requires no user action and is done automatically. Users can see

some events shown on the portal:

Manual resync. Requires user action to trigger the resync manually and is needed

in the following instances:

The storage account chosen for the reprotect is missing.

The replication disk on the appliance is missing.

The replication write exceeds the capacity of the replication disk on the

appliance.

If you leave $failbackPolicyName and $failbackExtensionName empty or null, the

re-protect can fail. See the following examples:



 Tip

You can also find the manual resync reasons in the events blade to help

you decide whether a manual resync is required.

Known issues in PowerShell automation

Always specify the $failbackPolicyName and $failbackExtensionName , as shown in

the following example:

PowerShell





$failbackPolicyName = "failback-default-replication-policy"

$failbackExtensionName = "default-failback-extension"

$parameters = @{

"properties" = @{

"customProperties" = @{

"instanceType" = "AzStackToAzStackFailback"

"applianceId" = $applianceId

"logStorageAccountId" = $LogStorageAccount.Id

"policyName" = $failbackPolicyName

"replicationExtensionName" = $failbackExtensionName

}

}

}

When replicating multiple VMs, you might see the Protected item health changed to

Warning error in the Site Recovery jobs.

This error message should only be a warning and is not a blocking issue for the actual

replication or failover processes.

Azure Site Recovery on Azure Stack Hub

Azure Site Recovery on Azure Stack Hub capacity planning

$result = Invoke-AzureRmResourceAction -Action "reprotect" ` -

ResourceId $protectedItemId ` -Force -Parameters $parameters

Mobility service agent warning



 Tip

You can check the the state of the respective VM to ensure it's healthy.

Next steps

Event Hubs on Azure Stack Hub

operator overview

Article • 07/29/2022

Event Hubs on Azure Stack Hub allows you to realize hybrid cloud scenarios. Streaming

and event-based solutions are supported, for both on-premises and Azure cloud

processing. Whether your scenario is hybrid (connected), or disconnected, your solution

can support processing of events/streams at large scale. Your scenario is bound only by

cluster size, which you can provision according to your needs.

See the Azure Stack Hub User documentation for a feature comparison, between Event

Hubs on Azure Stack vs. Azure Event Hubs.

To learn more about the Event Hubs user experience, refer to the Azure Event Hubs

documentation. This documentation applies to both editions of Event Hubs, and

contains topics such as:

Details on Event Hubs concepts

How to create an Event Hubs cluster and namespace

How to create an event hub

How to stream using the Kafka protocol

Review Capacity planning for Event Hubs on Azure Stack Hub, before beginning the

installation process. Understanding capacity planning will help you ensure your users

have the capacity they require.

Features

Feature documentation

Next steps

How to do capacity planning for Event

Hubs on Azure Stack Hub

Article • 07/29/2022

As an Operator you manage your Azure Stack Hub capacity using quotas on resources.

You control Event Hubs resource consumption by setting quotas on the maximum

number of cores use by Event Hubs clusters. Event Hubs clusters are created by users

when they deploy an Event Hubs resource. There are also various resource consumption

requirements for the resource provider, which are covered in this article.

To understand capacity consumption of Event Hubs deployments, it's important to note

that users create Event Hubs clusters based on Capacity Units (CUs). They don't specify a

CPU core count when creating an Event Hubs cluster. However, every CU directly maps

to a specific number of cores consumed.

Your users will need to create Event Hubs clusters with CUs that meet their business

requirements. To inform your decision on quota configuration, the following table

shows:

The total cores used by a 1 CU Event Hubs cluster.

The approximate capacity required for consumption of other resources, including

VM storage, memory, and storage accounts.

VM

Type

Cluster

Nodes

Cores per

VM/node

Total

Cores

VM

Storage

Memory Storage

Accounts

Public

IPs

1 CU

Event

Hubs

cluster

D11\_V2 5 2 10 500 GiB 70 GiB 4 1

All Event Hubs clusters use a D11\_V2 VM type for their nodes. A D11\_V2 VM type

consists of 2 cores. So 1 CU Event Hubs cluster uses 5 D11\_V2 VMs, which translates into

10 cores used. In determining the number of cores to configure for a quota, use a

multiple of the total cores used by 1 CU. This calculation reflects the maximum CU count

you'll allow your users to use, when creating Event Hubs clusters. For example, to

configure a quota that allows users to create a cluster with 2 CUs of capacity, set your

quota at 20 cores.

Cluster resource consumption

The resource consumption by the Event Hubs resource provider is constant, and

independent of the number or sizes of clusters created by users. The following table

shows the core utilization by the Event Hubs resource provider on Azure Stack Hub, and

the approximate resource consumption by other resources. The Event Hubs resource

provider uses a D2\_V2 VM type for its deployment.

VM

Type

Cluster

Nodes

Cores VM

Storage

Memory Storage

Accounts

Public

IPs

Event Hubs resource

provider

D2\_V2 3 6 300 GiB 21 GiB 2 1

The total capacity consumed by the Event Hubs service includes resource consumption

by the resource provider, and consumption by user-created clusters.

The following table shows the total Event Hubs consumption under various

configurations, regardless if they're managed by quota. These numbers are based on the

resource provider and Event Hubs cluster consumptions presented above. You can easily

calculate your total Azure Stack Hub usage for other deployment sizes, using these

examples.

） Important

For production deployments requiring high availability (HA), we recommend a 2 CU

cluster. For non-HA and development/test, you can start with 1 CU.

CU scale-out (smaller-to-larger) is supported via the Create Event Hubs Cluster

blade. Scale-in (larger-to-smaller) is not supported.

Resource provider resource consumption

） Important

Resource provider consumption is not something that is controlled by quotas. You

do not need to accommodate the cores used by the resource provider in your

quota configurations. Resource providers are installed using an administrator

subscription. The subscription does not impose resource consumption limits on

operators, when installing their required resource providers.

Total resource consumption

Cores VM

Storage

Memory Storage

Accounts

Total

Storage\*

Public

IPs\*\*

Cores VM

Storage

Memory Storage

Accounts

Total

Storage\*

Public

IPs\*\*

1-CU cluster + resource

provider

16 800 GiB 91 GiB 6 variable 2

2-CU cluster + resource

provider

26 1.3 TB 161 GiB 10 variable 2

4-CU cluster + resource

provider

46 2.3 TB 301 GiB 18 variable 2

\* The ingress data block (message/event) rate and message retention are two important

factors that contribute to the storage used by Event Hubs clusters. For example, if

message retention is set to 7 days when creating an event hub, and messages are

ingested at a rate of 1MB/s, the approximate storage used is 604 GB (1 MB x 60 seconds

x 60 minutes x 24 hours X 7 days). If messages are sent at a rate of 20MB/s with a 7 days

retention, the approximate storage consumption is 12TB. Be sure to consider ingress

data rate and retention time to fully understand storage capacity consumption.

\*\* Public IP addresses are consumed from the network quota provided as part of your

subscription.

Complete the Prerequisites for installing Event Hubs on Azure Stack Hub, before

beginning the installation process.

Next steps

Prerequisites for installing Event Hubs

on Azure Stack Hub

Article • 07/29/2022

The following prerequisites must be completed before you can install Event Hubs on

Azure Stack Hub. Several days or weeks of lead time may be required to complete all

steps.

If you've already installed a resource provider, you've likely completed the following

prerequisites, and can skip this section. Otherwise, complete these steps before

continuing:

1. Register your Azure Stack Hub instance with Azure, if you haven't done so. This

step is required as you'll be connecting to and downloading items to marketplace

from Azure.

2. If you're not familiar with the Marketplace Management feature of the Azure Stack

Hub administrator portal, review Download marketplace items from Azure and

publish to Azure Stack Hub. The article walks you through the process of

downloading items from Azure to the Azure Stack Hub marketplace. It covers both

connected and disconnected scenarios. If your Azure Stack Hub instance is

disconnected or partially connected, there are additional prerequisites to complete

in preparation for installation.

） Important

These prerequisites assume that you've already deployed at least a 4-node Azure

Stack Hub integrated system. The Event Hubs resource provider is not supported

on the Azure Stack Development Kit (ASDK).

） Important

Azure Stack Hub 2005 build version or higher is required by Event Hubs. Please

note that Azure Stack Hub builds are incremental. For example, if you have version

1910 installed, you must first upgrade to 2002, then to 2005. That is, you cannot

skip builds in-between.

Common prerequisites

3. Update your Azure Active Directory (Azure AD) home directory. Starting with build

1910, a new application must be registered in your home directory tenant. This app

will enable Azure Stack Hub to successfully create and register newer resource

providers (like Event Hubs and others) with your Azure AD tenant. This is an onetime action that needs to be done after upgrading to build 1910 or newer. If this

step isn't completed, marketplace resource provider installations will fail.

After you've successfully updated your Azure Stack Hub instance to 1910 or

greater, follow the instructions for cloning/downloading the Azure Stack Hub

Tools repository.

Then, follow the instructions for Updating the Azure Stack Hub Azure AD

Home Directory (after installing updates or new Resource Providers) .

1. Procure public key infrastructure (PKI) SSL certificates for Event Hubs. The Subject

Alternative Name (SAN) must adhere to the following naming pattern:

CN=\*.eventhub.<region>.<fqdn> . Subject Name may be specified, but it's not used

by Event Hubs when handling certificates. Only the Subject Alternative Name is

used. See PKI certificate requirements for the full list of detailed requirements.

Event Hubs prerequisites

2. Be sure to review Validate your certificate. The article shows you how to prepare

and validate the certificates you use for the Event Hubs resource provider.

Next, install the Event Hubs resource provider.

７ Note

PFX files must be password protected. The password will be requested later

during installation.

Next steps

How to install Event Hubs on Azure

Stack Hub

Article • 05/17/2023

This article shows you how to download and install the Event Hubs resource provider,

making it available to offer to customers for subscription. You must also complete the

Event Hubs install prerequisites before continuing.

Before installing or updating a resource provider, you must download the required

packages to the Azure Stack Hub marketplace. The download process varies, depending

on whether your Azure Stack Hub instance is connected to the Internet, or disconnected.

For a connected scenario, you download the items from Azure Marketplace directly to

Azure Stack Hub Marketplace:

1. Sign in to the Azure Stack Hub administrator portal.

2. Select Marketplace Management on the left.

3. Select Resource providers.

4. Select + Add from Azure.

5. Search for "Event Hubs" using the search bar.

6. Select the "Event Hubs" row on the search results.

7. On the "Event Hubs" download page, select the Event Hubs version you wish to

install, then select Download at the bottom of the page.

） Important

Starting from Azure Stack Hub build 2301, the Event Hubs resource provider is

offered to subscriptions that have been granted access. If you want to start using

this feature, or if you need to upgrade from a previous version, open a support

case and our support engineers will guide you through the deployment or upgrade

process.

Download packages

７ Note

The download process can take 30 minutes to 2 hours, depending on the network

latency and existing packages on your Azure Stack Hub instance.

Notice that additional software packages are downloaded along with Event Hubs,

including:

Microsoft Azure Stack Hub Add-On RP Windows Server INTERNAL ONLY

PowerShell Desired State Configuration

1. If you haven't already, sign in to the Azure Stack Hub administrator portal, select

Marketplace Management on the left, select Resource providers.

2. Once Event Hubs and other required software have been downloaded,

Marketplace Management shows the "Event Hubs" packages with a status of "Not

Installed". There may be other packages that show a status of "Downloaded".

Select the "Event Hubs" row you wish to install.



Installation



3. The Event Hubs install package page shows a blue banner across the top. Select

the banner to start the installation of Event Hubs.

1. Next you're transferred to the install page. Select Install Prerequisites to begin the

installation process.

2. Wait until the installation of prerequisites succeeds. You should see a green

checkmark next to Install prerequisites before proceeding to the next step.



Install prerequisites

1. Under the 2. Prepare secrets step, select Add certificate, and the Add a certificate

panel will appear.

2. Select the browse button on Add a certificate, just to the right of the certificate

filename field.

3. Select the .pfx certificate file you procured when completing the prerequisites. For

more information, see the installation Prerequisites.

4. Enter the password you provided to create a secure string for Event Hubs SSL

Certificate. Then select Add.

Prepare secrets

1. When the installation of the certificate succeeds, you should see a green

checkmark next to Prepare secrets before proceeding to the next step. Now select

the Install button next to 3 Install resource provider.

2. Next you'll see the following page, which indicates that Event Hubs resource

provider is being installed.

Install resource provider

3. Wait for the installation complete notification. This process usually takes one or

more hours, depending on your Azure Stack Hub type.

4. Verify that the installation of Event Hubs has succeeded, by returning to the

Marketplace Management, Resource Providers page. The status of Event Hubs





should show "Installed".

Before users can deploy Event Hubs resources, you must create one or more plans,

offers, and subscriptions.

If this is the first time you're offering a service, start with the Offer services to users

tutorial. Then continue with the next tutorial, Test a service offering.

Once you're familiar with the concept of offering a service, create an offer and plan

that includes the Event Hubs resource provider. Then create a subscription for your

users, or give them the offer information so they can create their own. For

reference, you can also follow the series of articles under the Service, plan, offer,

subscription overview.

To check for updates, How to update Event Hubs on Azure Stack Hub.

If you need to remove the resource provider, see Remove the Event Hubs resource

provider

To learn more about the user experience, visit the Event Hubs on Azure Stack Hub

overview in the User documents.

Next steps

How to update an Azure Stack Hub

resource provider

Article • 07/29/2022

Resource providers that are installed from Marketplace will require regular servicing.

Servicing is done by applying service updates, provided by Microsoft on a regular basis.

Updates can include both new features and fixes.

Resource providers are updated using the same update feature that is used to apply

Azure Stack Hub updates.

1. Sign in to the Azure Stack Hub administrator portal.

2. Select the All services link on the left, then under the Administration section select

Updates.

3. On the Updates page, you find updates for the resource providers under the

Resource provider section, with State showing "Available".

） Important

Before continuing, be sure to review the resource provider's latest release notes to

learn about new functionality, fixes, and any known issues that could affect your

deployment. The release notes may also specify the minimum Azure Stack Hub

version required for the resource provider. If you've never installed the resource

provider previously, refer to the resource provider's prerequisites and initial install

instructions instead.

Check for updates



Before installing or updating a resource provider, you must download the required

packages to the Azure Stack Hub marketplace. The download process varies, depending

on whether your Azure Stack Hub instance is connected to the Internet, or disconnected.

For a connected scenario, you download the update directly from Azure Marketplace:

1. From the Resource provider section of the Updates page, select the row of the

resource provider you want to update. Notice the Download link at the top of the

page becomes enabled.



Download package

７ Note

The download process can take 30 minutes to 2 hours, depending on the network

latency and existing packages on your Azure Stack Hub instance.



2. Click the Download link to begin the download of the resource provider install

package. Notice the State column for the resource provider row change from

"Available" to "Downloading".

3. When the State changes to "Ready to install", the download is complete.

Once the resource provider package has been downloaded, return to the Resource

provider section of the Updates page:

1. Select the row of the resource provider you want to update. The State will now

show "Ready to install", and the Install now link at the top of the page becomes

enabled.

2. Select the Install now link and you're taken to the Install page for the resource

provider.

3. Select the Install button to begin the installation.

4. An "Installation in progress" notification will be shown in the upper right, and you

return to the Updates page. The resource provider row Status column also

changes to "Installing".

5. When installation is complete, another notification will indicate success or failure. A

successful installation will also update the Version on the Marketplace

management - Resource providers page.

Learn more about the administrator dashboard updates feature.

Apply an update

Next steps

Enable backup for Azure Stack Hub

from the administrator portal

Article • 07/29/2022

You can enable the Infrastructure Backup Service from the administrator portal so that

Azure Stack Hub can generate infrastructure backups. The hardware partner can use

these backups to restore your environment using cloud recovery in the event of a

catastrophic failure. The purpose of cloud recovery is to ensure that your operators and

users can log back into the portal after recovery is complete. Users will have their

subscriptions restored, including:

Role-based access permissions and roles.

Original plans and offers.

Previously defined compute, storage, and network quotas.

Key Vault secrets.

However, the Infrastructure Backup Service doesn't back up IaaS VMs, network

configurations, and storage resources such as storage accounts, blobs, tables, and so on.

Users logging in after cloud recovery won't see any of these previously existing

resources. Platform as a Service (PaaS) resources and data are also not backed up by the

service.

Admins and users are responsible for backing up and restoring IaaS and PaaS resources

separately from the infrastructure backup processes. For info on backing up IaaS and

PaaS resources, see the following links:

Protect VMs deployed on Azure Stack Hub

Back up your app in Azure

What is SQL Server on Azure VMs? (Windows)

1. Open the Azure Stack Hub administrator portal.

2. Select All services, and then under the ADMINISTRATION category select

Infrastructure backup. Choose Configuration in the Infrastructure backup blade.

3. Type the path to the Backup storage location. Use a Universal Naming Convention

(UNC) string for the path to a file share hosted on a separate device. A UNC string

specifies the location of resources such as shared files or devices. For the service,

Enable or reconfigure backup

you can use an IP address. To ensure availability of the backup data after a disaster,

the device should be in a separate location.

4. Type the Username using the domain and username with sufficient access to read

and write files. For example, Contoso\backupshareuser .

5. Type the Password for the user.

6. Type the password again to Confirm Password.

7. The frequency in hours determines how often backups are created. The default

value is 12. Scheduler supports a maximum of 12 and a minimum of 4.

8. The retention period in days determines how many days of backups are preserved

on the external location. The default value is 7. Scheduler supports a maximum of

14 and a minimum of 2. Backups older than the retention period are automatically

deleted from the external location.

9. In Encryption Settings, provide a certificate in the Certificate .cer file box. The

certificate key length must be 2048 bytes. Backup files are encrypted using this

public key in the certificate. Provide a certificate that only contains the public key

portion when you configure backup settings. Once you set this certificate for the

first time or rotate the certificate in the future, you can only view the thumbprint of

the certificate. You can't download or view the uploaded certificate file. To create

the certificate file, run the following PowerShell command to create a self-signed

certificate with the public and private keys and export a certificate with only the

public key portion. You can save the certificate anywhere that can be accessed

from admin portal.

７ Note

If your environment supports name resolution from the Azure Stack Hub

infrastructure network to your enterprise environment, you can use a Fully

Qualified Domain Name (FQDN) rather than the IP.

７ Note

If you want to archive backups older than the retention period, make sure to

back up the files before the scheduler deletes the backups. If you reduce the

backup retention period (e.g. from 7 days to 5 days), the scheduler will delete

all backups older than the new retention period. Make sure you're OK with the

backups getting deleted before you update this value.

PowerShell

10. Select OK to save your backup controller settings.

To start a backup, click on Backup now to start an on-demand backup. An on-demand

backup won't modify the time for the next scheduled backup. After the task completes,

$cert = New-SelfSignedCertificate `

-DnsName "www.contoso.com" `

-CertStoreLocation "cert:\LocalMachine\My"

New-Item -Path "C:\" -Name "Certs" -ItemType "Directory"

Export-Certificate `

-Cert $cert `

-FilePath c:\certs\AzSIBCCert.cer

７ Note

Azure Stack Hub accepts a certificate to encrypt infrastructure backup data.

Make sure to store the certificate with the public and private key in a secure

location. For security reasons, it's not recommended that you use the

certificate with the public and private keys to configure backup settings. For

more info on how to manage the lifecycle of this certificate, see Infrastructure

Backup Service best practices.

Start backup

you can confirm the settings in Essentials:

You can also run the PowerShell cmdlet Start-AzsBackup on your Azure Stack Hub

admin computer. For more info, see Back up Azure Stack Hub.

Backups are automatically scheduled when you enable backup. You can check the next

schedule backup time in Essentials.

If you need to disable future scheduled backups, click on Disable Automatic Backups.

Disabling automatic backups keeps backup settings configured and retains the backup

schedule. This action simply tells the scheduler to skip future backups.

Confirm that future scheduled backups have been disabled in Essentials:

Enable or disable automatic backups

Click on Enable Automatic Backups to inform the scheduler to start future backups at

the scheduled time.

As of 1901, support for encryption key is deprecated. If you're configuring backup for

the first time in 1901, you must use a certificate. Azure Stack Hub supports encryption

key only if the key is configured before updating to 1901. Backward compatibility mode

will continue for three releases. After that, encryption keys will no longer be supported.

In encryption settings, if you're configuring infrastructure backup for the first time after

installing or updating to 1901, you must configure backup with a certificate. Using an

encryption key is no longer supported.

To update the certificate used to encrypt backup data, upload a new .CER file with the

public key portion and select OK to save settings.

７ Note

If you configured infrastructure backup before updating to 1807, automatic

backups will be disabled. This way the backups started by Azure Stack Hub don't

conflict with backups started by an external task scheduling engine. Once you

disable any external task scheduler, click on Enable Automatic Backups.

Update backup settings

Default mode

New backups will start to use the public key in the new certificate. There's no impact to

all existing backups created with the previous certificate. Make sure to keep the older

certificate around in a secure location in case you need it for cloud recovery.

If you configured backup before updating to 1901, the settings are carried over with no

change in behavior. In this case, the encryption key is supported for backwards

compatibility. You can update the encryption key or switch to use a certificate. You have

at least three releases to continue updating the encryption key. Use this time to

transition to a certificate. To create a new encryption key, use NewAzsEncryptionKeyBase64.

Backwards compatibility mode

７ Note

Updating from encryption key to certificate is a one-way operation. After making

this change, you can't switch back to encryption key. All existing backups will

remain encrypted with the previous encryption key.

Learn to run a backup. See Back up Azure Stack Hub.

Learn to verify that your backup ran. See Confirm backup completed in administrator

portal.

Next steps

Diagnostic log collection

Article • 06/01/2023

You can share diagnostic logs created by Azure Stack Hub. The Windows components

and on-premises Azure services create these logs. Microsoft Support can use the logs to

fix or identify issues with your Azure Stack Hub instance.

To get started with Azure Stack Hub diagnostic log collection, you have to register your

instance. If you haven't registered Azure Stack Hub, use the privileged endpoint (PEP) to

share logs.

You have multiple ways to send diagnostic logs to Microsoft Support. Depending on

your connectivity to Azure, your options include:

Send logs proactively (recommended)

Send logs now

Save logs locally

The flowchart shows which option to use for sending diagnostic logs. If Azure Stack Hub

connects to Azure, enable Proactive log collection. Proactive log collection

automatically uploads diagnostic logs to a Microsoft-controlled storage blob in Azure

when a critical alert gets raised. You can also collect logs on-demand by using Send logs

now. For an Azure Stack Hub that runs in a disconnected environment, or if you're

having connectivity issues, choose to Save logs locally.

Send logs proactively

Proactive log collection automatically collects and sends diagnostic logs from Azure

Stack Hub to Microsoft before you open a support case. Only when a system health alert

is raise are these logs collected. Microsoft Support only accesses these logs in the

context of a support case.

Beginning with Azure Stack Hub version 2008, proactive log collection uses an improved

algorithm to capture logs even during error conditions that aren't visible to an operator.

This improvement helps ensure that the right diagnostic info is collected at the right

time without needing any operator interaction. Microsoft support can begin

troubleshooting and resolve problems sooner in some cases. Initial algorithm

improvements focus on patch and update operations.

When an event triggers these alerts, Azure Stack Hub proactively sends the logs to

Microsoft. In addition, Azure Stack Hub sends logs to Microsoft triggered by other

failure events. These events are not visible to the operator.

Enabling proactive log collection is highly recommended. It allows the product team to

diagnose problems due to failure events and improve the quality of the product.

Azure Stack Hub proactively collects logs for:

Alert Fault ID type

Update needs attention Urp.UpdateWarning

Update failed Urp.UpdateFailure

Proactive log collection can be disabled and re-enabled anytime. Follow these steps to

set up proactive log collection.

1. Sign in to the Azure Stack Hub administrator portal.

2. Open Help + support Overview.

3. If the banner appears, select Enable proactive log collection. Or you can select

Settings and set Proactive log collection to Enable, then select Save.

７ Note

If proactive log collection is enabled and you renew or change your Azure Stack

Hub registration, as described in Renew or change registration, you must reenable proactive log collection.

７ Note

You agree to periodic automatic log collections by Microsoft based only on Azure Stack

Hub system health alerts. You also acknowledge and consent to the upload and

retention of those logs in an Azure storage account managed and controlled by

Microsoft.

The data is used for troubleshooting system health alerts and isn't used for marketing,

advertising, or any other commercial purposes without your consent. The data can be

retained for up to 90 days and Microsoft handles any data collected following our

standard privacy practices .

The revocation of your permission doesn't affect any data previously collected with your

consent.

Logs collected using Proactive log collection are uploaded to an Azure storage account

managed and controlled by Microsoft. Microsoft might access these logs in the context

of a support case and to improve the health of Azure Stack Hub.

Send logs now is an option where you manually collect and uploads your diagnostic

logs from Azure Stack Hub, usually before opening a support case.

There are two ways you can manually send diagnostic logs to Microsoft Support:

Administrator portal (recommended)

PowerShell

If Azure Stack Hub is connected to Azure, we recommend using the administrator portal

because it's the simplest way to send the logs directly to Microsoft. If the portal is

unavailable, you should send logs using PowerShell.

If log location settings are configured for a local file share, make sure lifecycle

management policies will prevent share storage from reaching its size quota. Azure

Stack Hub does not monitor local file share or enforce any retention policies.

How the data is handled

Send logs now

 Tip

Save time by using Send logs proactively instead of Send logs now.

To send logs now using the administrator portal:

1. Open Help + support > Log Collection > Send logs now.

2. Specify the start time and end time for log collection.

3. Choose the local time zone.

4. Select Collect and Upload.

If you're disconnected from the internet or want to only save logs locally, use the GetAzureStackLog method to send logs.

If you're using the Send logs now method and want to use PowerShell instead of the

administrator portal, you can use the Send-AzureStackDiagnosticLog cmdlet to collect

and send specific logs.

The FromDate and ToDate parameters can be used to collect logs for a particular

time period. If these parameters aren't specified, logs are collected for the past

four hours by default.

Use the FilterByNode parameter to filter logs by computer name. For example:

PowerShell

Use the FilterByLogType parameter to filter logs by type. You can choose to filter

by File, Share, or WindowsEvent. For example:

PowerShell

Use the FilterByResourceProvider parameter to send diagnostic logs for value-add

Resource Providers (RPs). The general syntax is:

７ Note

If you send logs using the administrator portal or PowerShell cmdlet, TestAzureStack runs automatically in the background to collect diagnostic information.

Send logs now with the administrator portal

Send logs now with PowerShell

Send-AzureStackDiagnosticLog -FilterByNode azs-xrp01

Send-AzureStackDiagnosticLog -FilterByLogType File

PowerShell

To send diagnostic logs for SQL RP:

PowerShell

To send diagnostic logs for MySQL RP:

PowerShell

To send diagnostic logs for Event Hubs:

PowerShell

To send diagnostic logs for Azure Stack Edge:

PowerShell

Use the FilterByRole parameter to send diagnostic logs from VirtualMachines and

BareMetal roles:

PowerShell

To send diagnostic logs from VirtualMachines and BareMetal roles, with date

filtering for log files for the past 8 hours:

PowerShell

Send-AzureStackDiagnosticLog -FilterByResourceProvider <<value-add RP

name>>

Send-AzureStackDiagnosticLog -FilterByResourceProvider SQLAdapter

Send-AzureStackDiagnosticLog -FilterByResourceProvider MySQLAdapter

Send-AzureStackDiagnosticLog -FilterByResourceProvider eventhub

Send-AzureStackDiagnosticLog -FilterByResourceProvide databoxedge

Send-AzureStackDiagnosticLog -FilterByRole VirtualMachines,BareMetal

$fromDate = (Get-Date).AddHours(-8)

Invoke-Command -Session $pepsession -ScriptBlock {Send-

To send diagnostic logs from VirtualMachines and BareMetal roles, with date

filtering for log files for the time period between 8 hours ago and 2 hours ago:

PowerShell

By initiating diagnostic log collection from Azure Stack Hub, you acknowledge and

consent to uploading those logs and retaining them in an Azure storage account

managed and controlled by Microsoft. Microsoft Support can access these logs right

away with the support case without having to engage with the customer for log

collection.

You can save logs to a local Server Message Block (SMB) share when Azure Stack Hub is

disconnected from Azure. You may, for example, run a disconnected environment. If

you're normally connected but are experiencing connectivity issues, you can save logs

locally to help with troubleshooting.

In the Settings blade, enter the path and a username and password with permission to

write to the share. During a support case, Microsoft Support works to provide detailed

steps on how to get these local logs transferred. If the Administrator portal is

unavailable, you can use Get-AzureStackLog to save logs locally.

AzureStackDiagnosticLog -FilterByRole VirtualMachines,BareMetal -

FromDate $using:fromDate}

$fromDate = (Get-Date).AddHours(-8)

$toDate = (Get-Date).AddHours(-2)

Invoke-Command -Session $pepsession -ScriptBlock {SendAzureStackDiagnosticLog -FilterByRole VirtualMachines,BareMetal -

FromDate $using:fromDate -ToDate $using:toDate}

７ Note

If you're disconnected from the internet or want to only save logs locally, use GetAzureStackLog method to send logs.

How the data is handled

Save logs locally

The average size of diagnostic log collection varies based on whether it runs proactively

or manually. The average size for Proactive log collection is around 2 GB. The collection

size for Send logs now depends on how many hours (up to 4 hours) are being collected

and the number of physical nodes in the Azure Stack Hub scale unit (4 to 16 nodes).

The following table lists considerations for environments with limited or metered

connections to Azure.

Network connection Impact

Low-bandwidth/high-latency

connection

Log upload takes an extended amount of time to complete.

Shared connection The upload may also affect other apps/users sharing the

network connection.

Bandwidth considerations

Network connection Impact

Metered connection There may be another charge from your ISP for the extra

network usage.

For example, if the internet connection or link speed from Azure Stack Hub is 5

Megabits/second (low-bandwidth), it would take approximately 57 minutes to upload 2

GB of diagnostic log data to Microsoft support. For an 8 GB manual log collection using

a 5 Megabits/second link speed, it would take approx. 3 hours and 49 minutes to upload

the data. This extended length of time to upload diagnostic data could delay or affect

the support experience.

The history of logs collected from Azure Stack Hub appears on the Log collection page

in Help + support, with the following dates and times:

Time Collected: When the log collection operation began.

Status: Either in progress or complete.

Logs start: Start of the time period for which you want to collect.

Logs end: End of the time period.

Type: If it's a manual or proactive log collection.

Azure Stack Hub log and customer data handling

View log collection

See also

Monitor health and alerts in Azure Stack

Hub

Article • 07/29/2022

Azure Stack Hub includes infrastructure monitoring capabilities that help you view

health and alerts for an Azure Stack Hub region. The Region management tile lists all

the deployed regions of Azure Stack Hub. It's pinned by default in the administrator

portal for the Default Provider Subscription. The tile shows the number of active critical

and warning alerts for each region. The tile is your entry point into the health and alert

functionality of Azure Stack Hub.

The health resource provider manages health and alerts. Azure Stack Hub infrastructure

components register with the health resource provider during Azure Stack Hub

deployment and configuration. This registration enables the display of health and alerts

for each component. Health in Azure Stack Hub is a simple concept. If alerts for a

registered instance of a component exist, the health state of that component reflects the

worst active alert severity: warning or critical.

Azure Stack Hub raises alerts with only two severities: warning and critical.

Warning

An operator can address the warning alert in a scheduled manner. The alert

Understand health in Azure Stack Hub

Alert severity definition

typically doesn't impact user workloads.

Critical

An operator should address the critical alert with urgency. These alerts indicate

issues that currently impact or will soon impact Azure Stack Hub users.

You can view the health state of components in the administrator portal and through

REST API and PowerShell.

To view the health state in the portal, click the region that you want to view in the

Region management tile. You can view the health state of infrastructure roles and of

resource providers.

You can click a resource provider or infrastructure role to view more detailed

information.

View and manage component health state

２ Warning

If you click an infrastructure role, and then click the role instance, there are options

to Start, Restart, or Shutdown. Don't use these actions when you apply updates to

an integrated system. Also, do not use these options in an Azure Stack

Development Kit (ASDK) environment. These options are only designed for an

integrated systems environment, where there's more than one role instance per

infrastructure role. Restarting a role instance (especially AzS-Xrp01) in the ASDK

causes system instability. For troubleshooting assistance, post your issue to the

Azure Stack Hub forum .

The list of active alerts for each Azure Stack Hub region is available directly from the

Region management blade. The first tile in the default configuration is the Alerts tile,

which displays a summary of the critical and warning alerts for the region. You can pin

the Alerts tile, like any other tile on this blade, to the dashboard for quick access.

To view a list of all active alerts for the region, select the top part of the Alerts tile. To

view a filtered list of alerts (Critical or Warning), select either the Critical or Warning line

item within the tile.

The Alerts blade supports the ability to filter both on status (Active or Closed) and

severity (Critical or Warning). The default view displays all active alerts. All closed alerts

are removed from the system after seven days.

View alerts

７ Note

If an alert remains active but hasn't been updated in over a day, you can run TestAzureStack and close the alert if no problems are reported.

The View API action displays the REST API that was used to generate the list view. This

action provides a quick way to become familiar with the REST API syntax that you can

use to query alerts. You can use this API in automation or for integration with your

existing datacenter monitoring, reporting, and ticketing solutions.

You can click a specific alert to view the alert details. The alert details show all fields that

are associated with the alert and enable quick navigation to the affected component

and source of the alert. For example, the following alert occurs if one of the

infrastructure role instances goes offline or isn't accessible.

Some alerts support a Repair option, as shown in the previous image. When selected,

the Repair action performs steps specific to the alert to attempt to resolve the issue.

Once selected, the status of the Repair action is available as a portal notification.

Alert remediation

Automated remediation

The Repair action will report successful completion or failure to complete the action in

the same portal notification blade. If a Repair action fails for an alert, you may rerun the

Repair action from the alert detail. If the Repair action successfully completes, do not

rerun the Repair action. After the infrastructure role instance is back online, this alert

automatically closes.

Manual remediation

If the Repair option is not supported, be sure to follow the complete set of remediation

instructions provided in the alert. As an example, the internal certificate expiration

remediation steps will guide you through the process of secret rotation:

Many, but not every alert, will automatically close when the underlying issue is resolved.

Alerts that provide a Repair action button will close automatically if Azure Stack Hub

Alert closure

resolves the issue. For all other alerts, select Close Alert after you do the remediation

steps. If the issue persists, Azure Stack Hub generates a new alert. If you resolve the

issue, the alert remains closed and requires no more steps.

Manage updates in Azure Stack Hub

Region management in Azure Stack Hub

Next steps

How to manage Event Hubs on Azure

Stack Hub

Article • 07/29/2022

The Event Hubs management experience allows you to control the service and visualize

its status and alerts.

Use the following steps to access the Event Hubs management page:

1. Sign in to the Azure Stack Hub administrator portal.

2. Select All Services from the pane on the left.

3. Search for "Event Hubs" and select the service. If you can't find the Event Hubs

service, the resource provider must first be installed.

4. The Event Hubs management overview page display. You'll find four sections in the

left pane:

Overview: provides a general view and access to specific management areas.

Alerts: displays all critical and warning alerts for Event Hubs. See the Alerts

section section for details.

Quotas: allows you to create, update, and delete quotas. See the Quotas

section section for details.

Event Hubs clusters: displays a list of all clusters configured. See the Event

Hubs clusters section for details.

Overview

Selecting Quotas on the main page displays the list of quotas in use, including the

associated plans that specify the quotas.

For more information on quota types defined for Event Hubs, see Quota Types



Quotas



The Event Hubs resource provider supports the following alerts:

Category Alert Type Condition

Performance

EventHub-CpuUsage Warning The average of % CPU usage of Event

Hubs cluster in the last 6 hours is larger

than 50%.

EventHub-MemoryUsage Warning The average of % free memory space of

Event Hubs cluster in the last 6 hours is

smaller than 50%.

EventHub-DiskUsage Warning The average of % Data Disk(E:) usage of

Event Hubs cluster in the last 6 hours is

larger than 50%.

Usage/Quota

EventHub-QuotaExceeded Warning A quota exceeded error occurred within

the last six hours.

EventHubNamespaceCreditUsage

Warning The sum of namespace credit usages in

the last six hours is larger than 10000.0.

Service

degraded

EventHubInternalServerError

Warning An internal server error occurred within

the last six hours.

EventHub-ServerBusy Warning A server busy error occurred in the last

six hours.

Client

EventHub-ClientError Warning A client error occurred in the last six

hours.

Resource

EventHubPendingDeletingResources

Warning The sum of pending deleting resources in

the last six hours is larger than 100.

EventHubProvisioningQueueLength

Warning The average of provisioning queue

length in the last six hours is larger than

30.

Alerts

Selecting Alerts on the main page displays the list of alerts issued:

Selecting an alert from the list, displays the Alert details panel on the right:

For more information on Azure Stack Hub monitoring capability, including alerting, see

Monitor Health and Alerts. For details on collecting logs, see Overview of Azure Stack

diagnostic log collection.

Selecting Event Hubs clusters on the main page displays a list of available user clusters.

The list includes the following for each cluster:

High-level configuration information.

Service health.

Backup status.





Event Hubs clusters

Selecting a link under Health or Backup will display detailed information on the state of

Event Hubs health and backup status, respectively. The link under Name displays more

details for the cluster, including:

Status and configuration information.

A list of service limits for the cluster.

Service limits are configuration parameters that define the operational boundaries of

Event Hubs. The service limits available are similar to the ones offered for Azure Event

Hubs Dedicated. By selecting the link(s) under Config value, you can change the

assigned value.





） Important

You should spend time analyzing the full implications before changing service

limits. Service limit changes may impact the behavior of your solution that

For more information on:

The quota types defined for Event Hubs, consult Quota Types.

Azure Stack Hub monitoring capabilities, including alerting, refer to Monitor Health

and Alerts.

Azure Stack Hub log collection, see Overview of Azure Stack diagnostic log

collection.

consumes and produces events. Changes may also impact the resource

consumption from your Azure Stack capacity.

Next steps

How to rotate secrets for Event Hubs on

Azure Stack Hub

Article • 07/29/2022

This article will show you how to rotate the secrets used by the Event Hubs resource

provider.

Like the Azure Stack Hub infrastructure, value-add resource providers use both internal

and external secrets. Secrets can take multiple forms, including passwords and the

encryption keys maintained by X509 certificates. As an operator, you're responsible for:

Providing updated external secrets, such as a new TLS certificate used to secure

resource provider endpoints.

Managing resource provider secret rotation on a regular basis.

In preparation for the rotation process:

1. Review Azure Stack Hub public key infrastructure (PKI) certificate requirements for

important prerequisite information before acquiring/renewing your X509

certificate, including details on the required PFX format. Also review the

requirements specified in the Optional PaaS certificates section, for your specific

value-add resource provider.

2. If you haven't already, Install PowerShell Az module for Azure Stack Hub before

continuing. Version 2.0.2-preview or later is required for Azure Stack Hub secret

rotation. For more information, see Migrate from AzureRM to Azure PowerShell Az

in Azure Stack Hub.

Overview and prerequisites

７ Note

Secret rotation for value-add resource providers (RPs) is currently only supported

via PowerShell. Also, you must proactively rotate secrets for value-add RPs on a

regular basis, as administrative alerts are currently not generated.

Prepare a new TLS certificate

Next, create or renew your TLS certificate for securing the value-add resource provider

endpoints:

1. Complete the steps in Generate certificate signing requests (CSRs) for certificate

renewal for your resource provider. Here you use the Azure Stack Hub Readiness

Checker tool to create the CSR. Be sure to run the correct cmdlet for your resource

provider, in the step "Generate certificate requests for other Azure Stack Hub

services". For example New-AzsHubEventHubsCertificateSigningRequest is used for

Event Hubs. When finished, you submit the generated .REQ file to your Certificate

Authority (CA) for the new certificate.

2. Once you've received your certificate file from the CA, complete the steps in

Prepare certificates for deployment or rotation. You use the Readiness Checker tool

again, to process the file returned from the CA.

3. Finally, complete the steps in Validate Azure Stack Hub PKI certificates. You use the

Readiness Checker tool once more, to perform validation tests on your new

certificate.

Finally, determine the resource provider's latest deployment properties and use them to

complete the secret rotation process.

Resource providers are deployed into your Azure Stack Hub environment as a versioned

product package. Packages are assigned a unique package ID, in the format '<productid>.<installed-version>' . Where <product-id> is a unique string representing the

resource provider, and <installed-version> represents a specific version. The secrets

associated with each package are stored in the Azure Stack Hub Key Vault service.

Open an elevated PowerShell console and complete the following steps to determine

the properties required to rotate the resource provider's secrets:

1. Sign in to your Azure Stack Hub environment using your operator credentials. See

Connect to Azure Stack Hub with PowerShell for PowerShell sign-in script. Be sure

to use the PowerShell Az cmdlets (instead of AzureRM), and replace all placeholder

values, such as endpoint URLs and directory tenant name.

2. Run the Get-AzsProductDeployment cmdlet to retrieve a list of the latest resource

provider deployments. The returned "value" collection contains an element for

Rotate secrets

Determine deployment properties

each deployed resource provider. Find the resource provider of interest and make

note of the values for these properties:

"name" - contains the resource provider product ID in the second segment of

the value.

"properties"."deployment"."version" - contains the currently deployed

version number.

In the following example, notice the Event Hubs RP deployment in the first element

in the collection, which has a product ID of "microsoft.eventhub" , and version

"1.2003.0.0" :

PowerShell

PS C:\WINDOWS\system32> Get-AzsProductDeployment -AsJson

VERBOSE: GET

https://adminmanagement.myregion.mycompany.com/subscriptions/ze22ca96-

z546-zbc6-z566-

z35f68799816/providers/Microsoft.Deployment.Admin/locations/global/prod

uctDeployments?api-version=2019-01-01 with 0-char payload

VERBOSE: Received 2656-char response, StatusCode = OK

{

"value": [

{

"id": "/subscriptions/ze22ca96-z546-zbc6-z566-

z35f68799816/providers/Microsoft.Deployment.Admin/locations/global/prod

uctDeployments/microsoft.eventhub",

"name": "global/microsoft.eventhub",

"type":

"Microsoft.Deployment.Admin/locations/productDeployments",

"properties": {

"status":

"DeploymentSucceeded",

"subscriptionId": "b37ae55aa6c6-4474-ba97-81519412adf5",

"deployment": {

"version":

"1.2003.0.0",

"actionPlanInstanceResourceId":"/subscriptions/ze22ca96-z546-zbc6-z566-

z35f68799816/providers/Microsoft.Deployment.Admin/locations/global/acti

onplans/abcdfcd3-fef0-z1a3-z85d-z6ceb0f31e36",

"parameters": {

}

},

"lastSuccessfulDeployment": {

"version": "1.2003.0.0",

3. Build the resource provider's package ID, by concatenating the resource provider

product ID and version. For example, using the values derived in the previous step,

the Event Hubs RP package ID is microsoft.eventhub.1.2003.0.0 .

4. Using the package ID derived in the previous step, run Get-AzsProductSecret -

PackageId to retrieve the list of secret types being used by the resource provider.

In the returned value collection, find the element containing a value of

"Certificate" for the "properties"."secretKind" property. This element contains

properties for the RP's certificate secret. Make note of the name assigned to this

certificate secret, which is identified by the last segment of the "name" property,

just above "properties" .

In the following example, the secrets collection returned for the Event Hubs RP

contains a "Certificate" secret named aseh-ssl-gateway-pfx .

PowerShell

"actionPlanInstanceResourceId":"/subscriptions/ze22ca96-z546-zbc6-z566-

z35f68799816/providers/Microsoft.Deployment.Admin/locations/global/acti

onplans/abcdfcd3-fef0-z1a3-z85d-z6ceb0f31e36",

"parameters": {

}

},

"provisioningState":

"Succeeded"

}

},

{

...

}

]

}

PS C:\WINDOWS\system32> Get-AzsProductSecret -PackageId

'microsoft.eventhub.1.2003.0.0' -AsJson

VERBOSE: GET

https://adminmanagement.myregion.mycompany.com/subscriptions/ze22ca96-

z546-zbc6-z566-

z35f68799816/providers/Microsoft.Deployment.Admin/locations/global/prod

uctPackages/microsoft.eventhub.1.2003.0.0/secrets?api-version=2019-01-

01 with 0-char payload

VERBOSE: Received 617-char response, StatusCode = OK

{

"value": [

1. Use the Set-AzsProductSecret cmdlet to import your new certificate to Key Vault,

which will be used by the rotation process. Replace the variable placeholder values

accordingly before running the script:

Placeholder Description Example value

<product-id> The product ID of the latest resource provider

deployment.

microsoft.eventhub

<installedversion>

The version of the latest resource provider

deployment.

1.2003.0.0

<cert-secretname>

The name under which the certificate secret is

stored.

aseh-ssl-gatewaypfx

{

"id": "/subscriptions/ze22ca96-z546-zbc6-z566-

z35f68799816/providers/Microsoft.Deployment.Admin/locations/global/prod

uctPackages/microsoft.eventhub.1.2003.0.0/secrets/aseh-ssl-gatewaypfx",

"name":

"global/microsoft.eventhub.1.2003.0.0/aseh-ssl-gateway-pfx",

"type":

"Microsoft.Deployment.Admin/locations/productPackages/secrets",

"properties": {

"secretKind": "Certificate",

"description": "Event Hubs

gateway SSL certificate.",

"expiresAfter": "P730D",

"secretDescriptor": {

},

"secretState": {

"status":

"Deployed",

"rotationStatus": "None",

"expirationDate": "2022-03-31T00:16:05.3068718Z"

},

"provisioningState":

"Succeeded"

}

},

...

]

}

Rotate the secrets

Placeholder Description Example value

<cert-pfx-filepath>

The path to your certificate PFX file. C:\dir\eh-certfile.pfx

<pfx-password> The password assigned to your certificate .PFX

file.

strong@CertSecret6

PowerShell

2. Finally, use the Invoke-AzsProductRotateSecretsAction cmdlet to rotate the

internal and external secrets:

PowerShell

You can monitor secret rotation progress in either the PowerShell console, or in the

administrator portal by selecting the resource provider in the Marketplace service:

$productId = '<product-id>'

$packageId = $productId + '.' + '<installed-version>'

$certSecretName = '<cert-secret-name>'

$pfxFilePath = '<cert-pfx-file-path>'

$pfxPassword = ConvertTo-SecureString '<pfx-password>' -AsPlainText -

Force

Set-AzsProductSecret -PackageId $packageId -SecretName $certSecretName

-PfxFileName $pfxFilePath -PfxPassword $pfxPassword -Force

７ Note

It takes approximately 3.5 - 4 hours to complete the rotation process.

Invoke-AzsProductRotateSecretsAction -ProductId $productId



Troubleshooting

Secret rotation should complete successfully without errors. If you experience any of the

following conditions in the administrator portal, open a support request for assistance:

Authentication issues, including problems connecting to the Event Hubs resource

provider.

Unable to upgrade resource provider, or edit configuration parameters.

Usage metrics aren't showing.

Bills aren't being generated.

Backups aren't occurring.

For details on rotating your Azure Stack Hub infrastructure secrets, visit Rotate secrets in

Azure Stack Hub.

Next steps

Event Hubs on Azure Stack Hub

1.2102.3.0 release notes

Article • 01/06/2023

These release notes describe improvements and fixes in Event Hubs on Azure Stack Hub

version 1.2102.3.0, and any known issues.

） Important

Before deploying or updating the Event Hubs resource provider (RP), you may need

to update Azure Stack Hub to a supported version (or deploy the latest Azure Stack

Development Kit). Be sure to read the RP release notes first, to learn about new

functionality, fixes, and any known issues that could affect your deployment.

Supported Azure Stack Hub version(s) Event Hubs RP release

2206 and higher 1.2102.3.0 Install | Update | Release notes

2206 and higher 1.2102.2.0 Install | Update | Release notes

2108 and higher 1.2102.2.0 Install | Update | Release notes

2102 and higher 1.2102.2.0 Install | Update | Release notes

2102 and higher 1.2102.1.0 Install | Update | Release notes

2102 and higher 1.2102.0.0 Install | Update | Release notes

If you've installed a preview version not listed above, upgrading to one of the

versions above is also recommended.

２ Warning

Failure to rotate secrets on a regular basis can result in your data plane clusters

entering an unhealthy state, and possibly redeployment of the Event Hubs on

Azure Stack Hub resource provider. As such, it is critical that you proactively rotate

the secrets used by Event Hubs on Azure Stack Hub. Secrets should be rotated

after completing an install/update to a new release, and on a regular basis,

ideally every 6 months. Proactive rotation is required as secret expiration does not

trigger administrative alerts.

This release includes the following updates:

Minimum Azure Stack Hub version is 1.2102: this release cannot be downloaded or

installed on Azure Stack Hub versions lower than 1.2102.

Upgrade path for this version of Event Hubs On Azure Stack Hub:

1.2102.1.0 -> 1.2102.3.0

1.2012.2.0 -> 1.2102.3.0

This release includes the following fixes:

In some scenarios, a VM rejoining the cluster and certificate download to individual

VMs during secret rotation can fail due to a path issue with common PowerShell

modules.

Applicable: This issue applies to all supported releases of Event Hubs on Azure

Stack Hub.

Cause: Administrative alerts aren't currently integrated.

Remediation: Complete the process in How to rotate secrets for Event Hubs on

Azure Stack Hubs regularly, ideally every six months.

Applicable: This issue applies to all supported releases of Event Hubs on Azure

Stack Hub.

Cause: Internal infrastructure secrets may be nearing expiration.

Remediation: Update to the latest Event Hubs on Azure Stack Hub release, then

complete the process in How to rotate secrets for Event Hubs on Azure Stack Hubs.

Updates in this release

Issues fixed in this release

Known issues

Secret expiration doesn't trigger an alert

Data plane clusters are in an unhealthy state with all

nodes in warning state

Data plane clusters' health isn't getting updated in admin

portal or scale-out of clusters results in access denied

Applicable: This issue applies to all supported releases of Event Hubs on Azure

Stack Hub.

Cause: Internal components haven't refreshed their cache with new secrets, after

secret rotation is completed.

Remediation: Open a support request to receive assistance.

Applicable: This issue applies to all supported releases of Event Hubs on Azure

Stack Hub.

Cause: Internal infrastructure secrets may have expired.

Remediation: Open a support request to receive assistance.

Applicable: This issue applies to release 1.2102.0.0 of Event Hubs on Azure Stack

Hub.

Cause: A known internal limitation.

Remediation: None at this time. A fix is being worked on to increase the limit.

Applicable: This issue applies to all supported releases of Event Hubs on Azure

Stack Hub.

Cause: A known design gap in the SDK modules.

Remediation: Other methods for namespace creation can be used, including an

Azure Resource Manager (ARM) template or REST API.

For more information, start with the Event Hubs on Azure Stack Hub operator

overview.

Azure Stack Hub backup fails

Limit on namespace-level authorization rule is 12 even if

portal allows more

Namespace creation using PowerShell and CLI modules

fails with error

Next steps

Event Hubs on Azure Stack Hub

1.2102.2.0 release notes

Article • 07/29/2022

These release notes describe improvements and fixes in Event Hubs on Azure Stack Hub

version 1.2102.2.0, and any known issues.

） Important

Before deploying or updating the Event Hubs resource provider (RP), you may need

to update Azure Stack Hub to a supported version (or deploy the latest Azure Stack

Development Kit). Be sure to read the RP release notes first, to learn about new

functionality, fixes, and any known issues that could affect your deployment.

Supported Azure Stack Hub version(s) Event Hubs RP release

2206 and higher 1.2102.3.0 Install | Update | Release notes

2206 and higher 1.2102.2.0 Install | Update | Release notes

2108 and higher 1.2102.2.0 Install | Update | Release notes

2102 and higher 1.2102.2.0 Install | Update | Release notes

2102 and higher 1.2102.1.0 Install | Update | Release notes

2102 and higher 1.2102.0.0 Install | Update | Release notes

If you've installed a preview version not listed above, upgrading to one of the

versions above is also recommended.

２ Warning

Failure to rotate secrets on a regular basis can result in your data plane clusters

entering an unhealthy state, and possibly redeployment of the Event Hubs on

Azure Stack Hub resource provider. As such, it is critical that you proactively rotate

the secrets used by Event Hubs on Azure Stack Hub. Secrets should be rotated

after completing an install/update to a new release, and on a regular basis,

ideally every 6 months. Proactive rotation is required as secret expiration does not

trigger administrative alerts.

This release includes the following updates:

Support for 2020-09-01 API Profile.

This release includes the following fixes:

Initial VM provisioning failures in environments with slow networking.

VM rejoining the cluster after a reboot fails sometimes.

Applicable: This issue applies to all supported releases of Event Hubs on Azure

Stack Hub.

Cause: Administrative alerts aren't currently integrated.

Remediation: Complete the process in How to rotate secrets for Event Hubs on

Azure Stack Hubs regularly, ideally every six months.

Applicable: This issue applies to all supported releases of Event Hubs on Azure

Stack Hub.

Cause: Internal infrastructure secrets may be nearing expiration.

Remediation: Update to the latest Event Hubs on Azure Stack Hub release, then

complete the process in How to rotate secrets for Event Hubs on Azure Stack Hubs.

Applicable: This issue applies to all supported releases of Event Hubs on Azure

Stack Hub.

Cause: Internal components haven't refreshed their cache with new secrets, after

secret rotation is completed.

Updates in this release

Issues fixed in this release

Known issues

Secret expiration doesn't trigger an alert

Data plane clusters are in an unhealthy state with all

nodes in warning state

Data plane clusters' health isn't getting updated in admin

portal or scale-out of clusters results in access denied

Remediation: Open a support request to receive assistance.

Applicable: This issue applies to all supported releases of Event Hubs on Azure

Stack Hub.

Cause: Internal infrastructure secrets may have expired.

Remediation: Open a support request to receive assistance.

Applicable: This issue applies to release 1.2102.0.0 of Event Hubs on Azure Stack

Hub.

Cause: A known internal limitation.

Remediation: None at this time. A fix is being worked on to increase the limit.

Applicable: This issue applies to all supported releases of Event Hubs on Azure

Stack Hub.

Cause: A known design gap in the SDK modules.

Remediation: Other methods for namespace creation can be used, including an

Azure Resource Manager (ARM) template or REST API.

For more information, start with the Event Hubs on Azure Stack Hub operator

overview.

Azure Stack Hub backup fails

Limit on namespace-level authorization rule is 12 even if

portal allows more

Namespace creation using PowerShell and CLI modules

fails with error

Next steps

Event Hubs on Azure Stack Hub

1.2102.1.0 release notes

Article • 07/29/2022

These release notes describe improvements and fixes in Event Hubs on Azure Stack Hub

version 1.2102.1.0, and any known issues.

） Important

Before deploying or updating the Event Hubs resource provider (RP), you may need

to update Azure Stack Hub to a supported version (or deploy the latest Azure Stack

Development Kit). Be sure to read the RP release notes first, to learn about new

functionality, fixes, and any known issues that could affect your deployment.

Supported Azure Stack Hub version(s) Event Hubs RP release

2206 and higher 1.2102.3.0 Install | Update | Release notes

2206 and higher 1.2102.2.0 Install | Update | Release notes

2108 and higher 1.2102.2.0 Install | Update | Release notes

2102 and higher 1.2102.2.0 Install | Update | Release notes

2102 and higher 1.2102.1.0 Install | Update | Release notes

2102 and higher 1.2102.0.0 Install | Update | Release notes

If you've installed a preview version not listed above, upgrading to one of the

versions above is also recommended.

２ Warning

Failure to rotate secrets on a regular basis can result in your data plane clusters

entering an unhealthy state, and possibly redeployment of the Event Hubs on

Azure Stack Hub resource provider. As such, it is critical that you proactively rotate

the secrets used by Event Hubs on Azure Stack Hub. Secrets should be rotated

after completing an install/update to a new release, and on a regular basis,

ideally every 6 months. Proactive rotation is required as secret expiration does not

trigger administrative alerts.

This release includes the following updates:

Previous releases had a limit on the throughput units in a namespace, which has

been removed in this release. Users can update the throughput unit of a

namespace to any number, as long as the cluster allows it.

There are no fixes in this release.

Applicable: This issue applies to all supported releases of Event Hubs on Azure

Stack Hub.

Cause: Administrative alerts aren't currently integrated.

Remediation: Complete the process in How to rotate secrets for Event Hubs on

Azure Stack Hubs regularly, ideally every six months.

Applicable: This issue applies to all supported releases of Event Hubs on Azure

Stack Hub.

Cause: Internal infrastructure secrets may be nearing expiration.

Remediation: Update to the latest Event Hubs on Azure Stack Hub release, then

complete the process in How to rotate secrets for Event Hubs on Azure Stack Hubs.

Applicable: This issue applies to all supported releases of Event Hubs on Azure

Stack Hub.

Cause: Internal components haven't refreshed their cache with new secrets, after

secret rotation is completed.

Remediation: Open a support request to receive assistance.

Updates in this release

Issues fixed in this release

Known issues

Secret expiration doesn't trigger an alert

Data plane clusters are in an unhealthy state with all

nodes in warning state

Data plane clusters' health isn't getting updated in admin

portal or scale-out of clusters results in access denied

Applicable: This issue applies to all supported releases of Event Hubs on Azure

Stack Hub.

Cause: Internal infrastructure secrets may have expired.

Remediation: Open a support request to receive assistance.

Applicable: This issue applies to release 1.2102.0.0 of Event Hubs on Azure Stack

Hub.

Cause: A known internal limitation.

Remediation: None at this time. A fix is being worked on to increase the limit.

Applicable: This issue applies to all supported releases of Event Hubs on Azure

Stack Hub.

Cause: A known design gap in the SDK modules.

Remediation: Other methods for namespace creation can be used, including an

Azure Resource Manager (ARM) template or REST API.

For more information, start with the Event Hubs on Azure Stack Hub operator

overview.

Azure Stack Hub backup fails

Limit on namespace-level authorization rule is 12 even if

portal allows more

Namespace creation using PowerShell and CLI modules

fails with error

Next steps

Event Hubs on Azure Stack Hub

1.2102.0.0 release notes

Article • 07/29/2022

These release notes describe improvements and fixes in Event Hubs on Azure Stack Hub

version 1.2102.0.0, and any known issues. If you're upgrading from a prior version of

Event Hubs on Azure Stack Hub, you must be at version 1.2012.1.0 or higher to upgrade

to this release.

） Important

Before deploying or updating the Event Hubs resource provider (RP), you may need

to update Azure Stack Hub to a supported version (or deploy the latest Azure Stack

Development Kit). Be sure to read the RP release notes first, to learn about new

functionality, fixes, and any known issues that could affect your deployment.

Supported Azure Stack Hub version(s) Event Hubs RP release

2206 and higher 1.2102.3.0 Install | Update | Release notes

2206 and higher 1.2102.2.0 Install | Update | Release notes

2108 and higher 1.2102.2.0 Install | Update | Release notes

2102 and higher 1.2102.2.0 Install | Update | Release notes

2102 and higher 1.2102.1.0 Install | Update | Release notes

2102 and higher 1.2102.0.0 Install | Update | Release notes

If you've installed a preview version not listed above, upgrading to one of the

versions above is also recommended.

２ Warning

Failure to rotate secrets on a regular basis can result in your data plane clusters

entering an unhealthy state, and possibly redeployment of the Event Hubs on

Azure Stack Hub resource provider. As such, it is critical that you proactively rotate

the secrets used by Event Hubs on Azure Stack Hub. Secrets should be rotated

after completing an install/update to a new release, and on a regular basis,

ideally every 6 months. Proactive rotation is required as secret expiration does not

trigger administrative alerts.

This release includes the following updates:

For Azure portal SDK developers, portal version 6.509.0.5 is now supported.

90-day message retention is now supported.

There are no fixes in this release.

Applicable: This issue applies to all supported releases of Event Hubs on Azure

Stack Hub.

Cause: Administrative alerts aren't currently integrated.

Remediation: Complete the process in How to rotate secrets for Event Hubs on

Azure Stack Hubs regularly, ideally every six months.

Applicable: This issue applies to all supported releases of Event Hubs on Azure

Stack Hub.

Cause: Internal infrastructure secrets may be nearing expiration.

Remediation: Update to the latest Event Hubs on Azure Stack Hub release, then

complete the process in How to rotate secrets for Event Hubs on Azure Stack Hubs.

Applicable: This issue applies to all supported releases of Event Hubs on Azure

Stack Hub.

Cause: Internal components haven't refreshed their cache with new secrets, after

secret rotation is completed.

Updates in this release

Issues fixed in this release

Known issues

Secret expiration doesn't trigger an alert

Data plane clusters are in an unhealthy state with all

nodes in warning state

Data plane clusters' health isn't getting updated in admin

portal or scale-out of clusters results in access denied

Remediation: Open a support request to receive assistance.

Applicable: This issue applies to all supported releases of Event Hubs on Azure

Stack Hub.

Cause: Internal infrastructure secrets may have expired.

Remediation: Open a support request to receive assistance.

Applicable: This issue applies to release 1.2102.0.0 of Event Hubs on Azure Stack

Hub.

Cause: A known internal limitation.

Remediation: None at this time. A fix is being worked on to increase the limit.

Applicable: This issue applies to all supported releases of Event Hubs on Azure

Stack Hub.

Cause: A known design gap in the SDK modules.

Remediation: Other methods for namespace creation can be used, including an

Azure Resource Manager (ARM) template or REST API.

For more information, start with the Event Hubs on Azure Stack Hub operator

overview.

Azure Stack Hub backup fails

Limit on namespace-level authorization rule is 12 even if

portal allows more

Namespace creation using PowerShell and CLI modules

fails with error

Next steps

Event Hubs on Azure Stack Hub

1.2012.2.0 release notes

Article • 07/29/2022

These release notes describe improvements and fixes in Event Hubs on Azure Stack Hub

version 1.2012.2.0, and any known issues.

） Important

Before deploying or updating the Event Hubs resource provider (RP), you may need

to update Azure Stack Hub to a supported version (or deploy the latest Azure Stack

Development Kit). Be sure to read the RP release notes first, to learn about new

functionality, fixes, and any known issues that could affect your deployment.

Supported Azure Stack Hub version(s) Event Hubs RP release

2206 and higher 1.2102.3.0 Install | Update | Release notes

2206 and higher 1.2102.2.0 Install | Update | Release notes

2108 and higher 1.2102.2.0 Install | Update | Release notes

2102 and higher 1.2102.2.0 Install | Update | Release notes

2102 and higher 1.2102.1.0 Install | Update | Release notes

2102 and higher 1.2102.0.0 Install | Update | Release notes

If you've installed a preview version not listed above, upgrading to one of the

versions above is also recommended.

２ Warning

Failure to rotate secrets on a regular basis can result in your data plane clusters

entering an unhealthy state, and possibly redeployment of the Event Hubs on

Azure Stack Hub resource provider. As such, it is critical that you proactively rotate

the secrets used by Event Hubs on Azure Stack Hub. Secrets should be rotated

after completing an install/update to a new release, and on a regular basis,

ideally every 6 months. Proactive rotation is required as secret expiration does not

trigger administrative alerts.

This release includes the following updates:

Upgraded the infrastructure service fabric runtime to version 7.2.477.9590

This release includes the following fixes:

Service fabric runtime version display issue in Event Hubs management, whenever

an upgrade finishes.

HTTP port of an infrastructure service whose access wasn't removed when

reassigned, caused requests to error with "service unavailable".

Internal cluster certificate secret rotation issue that rendered clusters unresponsive

when rotating the cluster certificates.

Applicable: This issue applies to all supported releases of Event Hubs on Azure

Stack Hub.

Cause: Administrative alerts aren't currently integrated.

Remediation: Complete the process in How to rotate secrets for Event Hubs on

Azure Stack Hubs regularly, ideally every six months.

Applicable: This issue applies to all supported releases of Event Hubs on Azure

Stack Hub.

Cause: Internal infrastructure secrets may be nearing expiration.

Remediation: Update to the latest Event Hubs on Azure Stack Hub release, then

complete the process in How to rotate secrets for Event Hubs on Azure Stack Hubs.

Updates in this release

Issues fixed in this release

Known issues

Secret expiration doesn't trigger an alert

Data plane clusters are in an unhealthy state with all

nodes in warning state

Data plane clusters' health isn't getting updated in admin

portal or scale-out of clusters results in access denied

Applicable: This issue applies to all supported releases of Event Hubs on Azure

Stack Hub.

Cause: Internal components haven't refreshed their cache with new secrets, after

secret rotation is completed.

Remediation: Open a support request to receive assistance.

Applicable: This issue applies to all supported releases of Event Hubs on Azure

Stack Hub.

Cause: Internal infrastructure secrets may have expired.

Remediation: Open a support request to receive assistance.

For more information, start with the Event Hubs on Azure Stack Hub operator

overview.

Azure Stack Hub backup fails

Next steps

Event Hubs on Azure Stack Hub

1.2012.1.0 release notes

Article • 07/29/2022

These release notes describe improvements and fixes in Event Hubs on Azure Stack Hub

version 1.2012.1.0, and any known issues.

） Important

Before deploying or updating the Event Hubs resource provider (RP), you may need

to update Azure Stack Hub to a supported version (or deploy the latest Azure Stack

Development Kit). Be sure to read the RP release notes first, to learn about new

functionality, fixes, and any known issues that could affect your deployment.

Supported Azure Stack Hub version(s) Event Hubs RP release

2206 and higher 1.2102.3.0 Install | Update | Release notes

2206 and higher 1.2102.2.0 Install | Update | Release notes

2108 and higher 1.2102.2.0 Install | Update | Release notes

2102 and higher 1.2102.2.0 Install | Update | Release notes

2102 and higher 1.2102.1.0 Install | Update | Release notes

2102 and higher 1.2102.0.0 Install | Update | Release notes

If you've installed a preview version not listed above, upgrading to one of the

versions above is also recommended.

２ Warning

Failure to rotate secrets on a regular basis can result in your data plane clusters

entering an unhealthy state, and possibly redeployment of the Event Hubs on

Azure Stack Hub resource provider. As such, it is critical that you proactively rotate

the secrets used by Event Hubs on Azure Stack Hub. Secrets should be rotated

after completing an install/update to a new release, and on a regular basis,

ideally every 6 months. Proactive rotation is required as secret expiration does not

trigger administrative alerts.

This release includes the following updates:

For Azure portal SDK developers, portal version 5.0.303.7361 is now supported.

Internal logging improvements for Event Hubs clusters.

This release includes the following fixes:

A fix to the upgrade order for Event Hubs clusters, to address an upgrade issue.

The cluster health and backup health check for Event Hubs clusters were not

running when clusters were in "Upgrading" or "Upgrade Failed" state. The issue has

been fixed in this release.

Fixed a bug causing usage records to contain the wrong quantity. Instead of cores,

we were emitting capacity units (CU). Previously, a 1CU cluster would show 1 core

in hourly usage. Users will now see the correct quantity of 10 cores for a 1 CU

cluster in their hourly usage.

Applicable: This issue applies to all supported releases of Event Hubs on Azure

Stack Hub.

Cause: Administrative alerts aren't currently integrated.

Remediation: Complete the process in How to rotate secrets for Event Hubs on

Azure Stack Hubs regularly, ideally every six months.

Applicable: This issue applies to all supported releases of Event Hubs on Azure

Stack Hub.

Cause: Internal infrastructure secrets may be nearing expiration.

Remediation: Update to the latest Event Hubs on Azure Stack Hub release, then

complete the process in How to rotate secrets for Event Hubs on Azure Stack Hubs.

Updates in this release

Issues fixed in this release

Known issues

Secret expiration doesn't trigger an alert

Data plane clusters are in an unhealthy state with all

nodes in warning state

Applicable: This issue applies to all supported releases of Event Hubs on Azure

Stack Hub.

Cause: Internal components haven't refreshed their cache with new secrets, after

secret rotation is completed.

Remediation: Open a support request to receive assistance.

Applicable: This issue applies to all supported releases of Event Hubs on Azure

Stack Hub.

Cause: Internal infrastructure secrets may have expired.

Remediation: Open a support request to receive assistance.

For more information, start with the Event Hubs on Azure Stack Hub operator

overview.

Data plane clusters' health isn't getting updated in admin

portal or scale-out of clusters results in access denied

Azure Stack Hub backup fails

Next steps

How to uninstall Azure Stack Hub Event

Hubs resources

Article • 07/29/2022

This sequence of steps will delete all Azure Stack Hub Event Hubs resources, including

clusters, namespaces, event hubs, and the resource provider:

1. Sign in to the Azure Stack Hub administrator portal.

2. Select Marketplace management on the left.

3. Select Resource providers.

4. Select Event Hubs from the list of resource providers. You may want to filter the list

by entering "Event Hubs" in the search text box provided.

２ Warning

Uninstalling Azure Stack Hub Event Hubs resources will remove (erase) the resource

provider, and all user-created Event Hubs clusters, namespaces, and event hubs

resources. It will also remove their associated event data.

Please proceed with extreme caution before deciding to uninstall Event Hubs on

Azure Stack Hub. Uninstalling Event Hubs does not delete the packages used to

install Event Hubs on Azure Stack Hub. To achieve that, please refer to Delete Event

Hubs packages.

Uninstall Azure Stack Hub Event Hubs

resources

5. Select Uninstall from the options provided across the top of the page.

6. Enter the name of the resource provider, then select Uninstall. This action confirms

your desire to uninstall:

The Event Hubs resource provider.

All user-created clusters, namespaces, event hubs, and event data.





Use the Delete option after uninstalling Event Hubs on Azure Stack Hub, if you would

also like to remove the related installation packages.

To reinstall, return to the Install the Event Hubs resource provider article.





） Important

You must wait at least 10 minutes after Event Hubs has been removed

successfully before installing Event Hubs again. This is due to the fact that

cleanup activities might still be running, which may conflict with any new

installation.

Delete Event Hubs packages

Next steps

How to remove IoT Hub on Azure Stack

Hub

Article • 07/29/2022

This article provides instructions on how to remove IoT Hub resource provider on Azure

Stack Hub. This process takes around 37 minutes.

1. Go to Marketplace management. IoT Hub will be in the list and marked as

installed. Click on IoT Hub.

2. Click Uninstall under IoT Hub, provide the resource provider name

microsoft.iothub, then click Uninstall button under it.

） Important

The public preview of the IoT Hub on Azure Stack Hub resource provider is now

closed. For more detail see IoT Hub on Azure Stack Hub public preview will be

retired on 30 September 2022

Uninstalling IoT Hub

２ Warning

Once IoT Hub is uninstalled, all devices and data will be deleted. The operation is

NOT recoverable.



3. Wait for the uninstall to complete. A "Resource Provider installation has been

completed successfully" banner will show at the top of the page.

For more information on Azure IoT Hub, see the Azure IoT Hub Documentation.



） Important

The dependencies (eg. Event Hub) will NOT be uninstalled. Should you want to

uninstall/ remove any of the dependencies from marketplace, you will need to do it

separately.

Next steps

Add the Azure Kubernetes Services

(AKS) engine prerequisites to the Azure

Stack Hub Marketplace

Article • 10/06/2022

You can set up the Azure Kubernetes Services (AKS) Engine for your users. Add the items

described in this article to your Azure Stack Hub. Your users can then deploy a

Kubernetes cluster in a single, coordinated operation. This article walks you through the

steps you need to make the AKS engine available to your users in both connected and

disconnected environments. The AKS engine depends on a service principle identity. The

AKS engine also will need to have in the marketplace: a Custom Script extension, and

the AKS Base Image. The AKS engine requires that you're running Azure Stack Hub 1910

or greater.

Your users will need a plan, offer, and subscription to Azure Stack Hub with enough

space. Users will often want to deploy clusters of up to six virtual machines, made of

three masters and three worker nodes. You'll want to make sure they have a large

enough quota.

If you need more information about planning and setting up a service offering, see

Overview of offering services in Azure Stack Hub

The Kubernetes cluster will need service principal (SPN) and role-based permissions in

Azure Stack Hub.

Create an SPN in Azure AD

If you use Azure Active Directory (Azure AD) for your identity management service,

you'll need to create an SPN for users deploying a Kubernetes cluster. Create an

７ Note

You can find the mapping of Azure Stack Hub to AKS engine version number in the

AKS engine release notes.

Check your user's service offering

Create a service principal and credentials

SPN using a client secret.

For instructions using the Administrative portal, see Create an app registration.

For instructions, see Create an app registration that uses a client secret credential.

Create an SPN in AD FS

If you use Active Directory Federated Services (AD FS) for your identity

management service, you'll need to create an SPN for users deploying a

Kubernetes cluster. Create an SPN using a client secret.

For instructions using PowerShell, see Create an app registration that uses a client

secret credential.

Assign a role

The SPN will need access to resources in the user subscription using the SPN. The

SPN will need Contributor access. For instructions on assigning a role, see Assign a

role.

You can add an AKS Base Image to the marketplace by getting the item from Azure.

However, if your Azure Stack Hub is disconnected, use these instructions Download

marketplace items from Azure to add the item. Add the item specified in step 5.

Add the following item to the marketplace:

1. Sign in to the Administration portal

https://adminportal.local.azurestack.external .

2. Select All services, and then under the ADMINISTRATION category, select

Marketplace management.

3. Select + Add from Azure.

4. Enter AKS Base .

5. Select the image version that matches the version of the AKS engine. You can find

listing of AKS Base Image to AKS engine version at Supported Kubernetes Versions.

6. Select Download.

Add an AKS Base Image

Add a custom script extension

You can add the custom script to the marketplace by getting the item from Azure.

However, if your Azure Stack Hub is disconnected, use the instructions Download

marketplace items from Azure to add the item. Add the item specified in step 5.

1. Open the Administration portal https://adminportal.local.azurestack.external .

2. Select ALL services and then under the ADMINISTRATION category, select

Marketplace Management.

3. Select + Add from Azure.

4. Enter Custom Script for Linux .

5. Select the script with the following profile:

Offer: Custom Script for Linux 2.0

Version: 2.0.6 (or latest version)

Publisher: Microsoft Corp

6. Select Download.

What is the AKS engine on Azure Stack Hub?

Overview of offering services in Azure Stack Hub

７ Note

More than one version of the Custom Script for Linux may be listed. You

will need to add the last version of the item.

Next steps

Add Kubernetes to Azure Stack Hub

Marketplace

Article • 06/01/2022

You can offer Kubernetes as a marketplace item to your users. Your users can then

deploy Kubernetes in a single, coordinated operation.

This article looks at using an Azure Resource Manager template to deploy and provision

the resources for a standalone Kubernetes cluster. Before you start, check your Azure

Stack Hub and global Azure tenant settings. Collect the required information about your

Azure Stack Hub. Add necessary resources to your tenant and to Azure Stack Hub

Marketplace. The cluster depends on an Ubuntu server, custom script, and the

Kubernetes Cluster marketplace item to be in Azure Stack Hub Marketplace.

Create a plan, an offer, and a subscription for the Kubernetes marketplace item. You can

also use an existing plan and offer.

1. Sign in to the administrator portal

https://adminportal.local.azurestack.external .

2. Create a plan as the base plan. For instructions, see Create a plan in Azure Stack

Hub.

3. Create an offer. For instructions, see Create an offer in Azure Stack Hub.

4. Select Offers, and find the offer you created.

5. Select Overview in the Offer blade.

6. Select Change state. Select Public.

7. Select + Create a resource > Offers and Plans > Subscription to create a

subscription.

７ Note

Only use the Kubernetes Azure Stack Hub Marketplace item to deploy clusters as a

proof-of-concept. For supported Kubernetes clusters on Azure Stack Hub, use the

AKS engine.

Create a plan, an offer, and a subscription

a. Enter a Display Name.

b. Enter a User. Use the Azure AD account associated with your tenant.

c. Provider Description

d. Set the Directory tenant to the Azure AD tenant for your Azure Stack Hub.

e. Select Offer. Select the name of the offer that you created. Make note of the

Subscription ID.

If you use Active Directory Federated Services (AD FS) for your identity management

service, you need to create a service principal for users deploying a Kubernetes cluster.

Create service principal using a client secret. For instructions, see Create an app

registration that uses a client secret credential.

Add the following Ubuntu Server image to Azure Stack Hub Marketplace:

1. Sign in to the administrator portal

https://adminportal.local.azurestack.external .

2. Select All services, and then under the ADMINISTRATION category, select

Marketplace management.

3. Select + Add from Azure.

4. Enter Ubuntu Server .

5. Select the newest version of the server. Check the full version and ensure that you

have the newest version:

Publisher: Canonical

Offer: UbuntuServer

Version: 16.04.201806120 (or latest version)

SKU: 16.04-LTS

6. Select Download.

Create a service principal and credentials in AD

FS

Add an Ubuntu server image

Add the Kubernetes from Azure Stack Hub Marketplace:

1. Open the administrator portal https://adminportal.local.azurestack.external .

2. Select ALL services and then under the ADMINISTRATION category, select

Marketplace Management.

3. Select + Add from Azure.

4. Enter Custom Script for Linux .

5. Select the script with the following profile:

Offer: Custom Script for Linux 2.0

Version: 2.0.6 (or latest version)

Publisher: Microsoft Corp

6. Select Download.

1. Open the administrator portal https://adminportal.local.azurestack.external .

2. Select All services and then under the ADMINISTRATION category, select

Marketplace Management.

3. Select + Add from Azure.

4. Enter Kubernetes .

5. Select Kubernetes Cluster .

6. Select Download.

Add a custom script for Linux

７ Note

More than one version of Custom Script for Linux may be listed. You

need to add the last version of the item.

Add Kubernetes to the marketplace

７ Note

When updating the Kubernetes item, you remove the previous item in Azure Stack Hub

Marketplace. Follow the instruction below to add the Kubernetes update to Azure Stack

Hub Marketplace.

To remove the Kubernetes item:

1. Connect to Azure Stack Hub with PowerShell as an operator. For instruction, see

Connect to Azure Stack Hub with PowerShell as an operator.

2. Find the current Kubernetes Cluster item in the gallery.

PowerShell

It may take five minutes for the marketplace item to appear in Azure Stack

Hub Marketplace.

Update or remove the Kubernetes

Get-AzsGalleryItem | Select Name

3. Note name of the current item, such as

Microsoft.AzureStackKubernetesCluster.0.3.0 .

4. Use the following PowerShell cmdlet to remove the item:

PowerShell

Deploy a Kubernetes to Azure Stack Hub

Overview of offering services in Azure Stack Hub

$Itemname="Microsoft.AzureStackKubernetesCluster.0.3.0"

Remove-AzsGalleryItem -Name $Itemname

Next steps

Use MySQL databases on Microsoft

Azure Stack Hub

Article • 07/29/2022

Use the MySQL resource provider to offer MySQL databases on Azure Stack Hub. After

you deploy the resource provider and connect it to one or more MySQL server

instances, you can create:

MySQL databases for cloud-native apps.

MySQL databases for web applications.

There are several limitations to consider, before installing the MySQL resource provider:

Users can only create and manage individual databases. Database Server instance

is not accessible to end users. This may limit compatibility with on-premises

database applications that need access to master, Temp DB, or to dynamically

manage databases.

Your Azure Stack Hub operator is responsible for deploying, updating, securing,

configuring and maintaining the MySQL database servers and hosts. The RP service

does not provide any host and database server instance management

functionality.

Databases from different users in different subscriptions may be located on the

same database server instance. The RP does not provide any mechanism for

isolating databases on different hosts or database server instances.

The RP does not provide any reporting on tenant usage of databases.

The RP doesn't monitor the MySQL Server's health.

The resource provider has the following components:

） Important

Starting from Azure Stack Hub build 2108, the SQL and MySQL resource providers

are offered to subscriptions that have been granted access. If you want to start

using this feature, or if you need to upgrade from a previous version, open a

support case and our support engineers will guide you through the deployment or

upgrade process.

MySQL resource provider adapter architecture

The MySQL resource provider adapter virtual machine (VM), which is a Windows

Server VM that's running the provider services.

The resource provider, which processes requests and accesses database resources.

Servers that host MySQL Server, which provide capacity for databases that are

called hosting servers. You can create MySQL instances yourself, or provide access

to external MySQL instances. The Azure Stack Hub Quickstart Gallery has an

example template that you can use to:

Create a MySQL server for you.

Download and deploy a MySQL Server from Azure Marketplace.

The system account must have the following privileges:

Database: create, drop

Login: create, set, drop, grant, revoke

Deploy the MySQL resource provider

７ Note

Hosting servers that are installed on Azure Stack Hub integrated systems must be

created from a tenant subscription. They can't be created from the default provider

subscription. They must be created from the user portal or from a PowerShell

session with an appropriate sign-in. All hosting servers are billable VMs and must

have licenses. The service administrator can be the owner of the tenant

subscription.

Required privileges

Next steps

Deploy the MySQL resource provider on

Azure Stack Hub

Article • 05/22/2023

Use the MySQL Server resource provider to expose MySQL databases as an Azure Stack

Hub service.

The MySQL resource provider runs as a service on a special Add-on RP Windows Server.

If you've already installed a resource provider, you've likely completed the following

prerequisites, and can skip this section. Otherwise, complete these steps before

continuing:

1. Register your Azure Stack Hub instance with Azure, if you haven't done so. This

step is required as you'll be connecting to and downloading items to marketplace

from Azure.

2. If you're not familiar with the Marketplace Management feature of the Azure Stack

Hub administrator portal, review Download marketplace items from Azure and

publish to Azure Stack Hub. The article walks you through the process of

downloading items from Azure to the Azure Stack Hub marketplace. It covers both

connected and disconnected scenarios. If your Azure Stack Hub instance is

） Important

Starting from Azure Stack Hub build 2108, the SQL and MySQL resource providers

are offered to subscriptions that have been granted access. If you want to start

using this feature, or if you need to upgrade from a previous version, open a

support case and our support engineers will guide you through the deployment or

upgrade process.

） Important

Only the resource provider should create items on servers that host SQL or MySQL.

Items created on a host server that aren't created by the resource provider are

unsupported, and may result in a mismatched state.

Prerequisites

disconnected or partially connected, there are additional prerequisites to complete

in preparation for installation.

3. Update your Azure Active Directory (Azure AD) home directory. Starting with build

1910, a new application must be registered in your home directory tenant. This app

will enable Azure Stack Hub to successfully create and register newer resource

providers (like Event Hubs and others) with your Azure AD tenant. This is an onetime action that needs to be done after upgrading to build 1910 or newer. If this

step isn't completed, marketplace resource provider installations will fail.

After you've successfully updated your Azure Stack Hub instance to 1910 or

greater, follow the instructions for cloning/downloading the Azure Stack Hub

Tools repository.

Then, follow the instructions for Updating the Azure Stack Hub Azure AD

Home Directory (after installing updates or new Resource Providers) .

You'll need a computer and account that can access:

the Azure Stack Hub administrator portal.

the privileged endpoint (needed only when you're deploying MySQL Server

resource provider V1 or upgrading from MySQL Server resource provider V1 to

MySQL Server resource provider V2).

the Azure Resource Manager admin endpoint, https://adminmanagement.region.

<fqdn> , where <fqdn> is your fully qualified domain name.

the Internet, if your Azure Stack Hub was deployed to use Azure Active

Directory (Azure AD) as your identity provider.

Download the supported version of MySQL resource provider binary according to

the version mapping table below. For V2 MySQL resource provider, download the

marketplace item to Azure Stack Hub.

Supported Azure Stack

Hub version

MySQL RP version Windows Server that RP service is

running on

2206, 2301 MySQL RP version

2.0.13.x

Microsoft AzureStack Add-on RP

Windows Server 1.2009.0

2108,2206 MySQL RP version

2.0.6.x

Microsoft AzureStack Add-on RP

Windows Server 1.2009.0

2108, 2102, 2008, 2005 MySQL RP version

1.1.93.5

Microsoft AzureStack Add-on RP

Windows Server

MySQL Server resource provider prerequisites

Make sure that the required Windows Server VM is downloaded to Azure Stack

Hub Marketplace. Manually download the image according to the version

mapping table above if needed.

Ensure datacenter integration prerequisites are met:R

Prerequisite Reference

Conditional DNS

forwarding is set

correctly.

Azure Stack Hub datacenter integration - DNS

Inbound ports for

resource providers are

open.

Azure Stack Hub datacenter integration - Publish endpoints

PKI certificate subject

and SAN are set

correctly.

Azure Stack Hub deployment mandatory PKI prerequisitesAzure

Stack Hub deployment PaaS certificate prerequisites

Prepare the certificate. (For integrated systems installations only.)

You must provide the SQL PaaS PKI certificate described in the optional PaaS

certificates section of Azure Stack Hub deployment PKI requirements. The

Subject Alternative Name (SAN) must adhere to the following naming pattern:

CN=\*.dbadapter.<region>.<fqdn>, with password protected.

When deploying MySQL Server resource provider V1, place the .pfx file in the

location specified by the DependencyFilesLocalPath parameter. Don't provide a

certificate for ASDK systems.

When deploying MySQL Server resource provider V2, prepare the certificate for

the following installation steps.

Disconnected scenario

When deploying MySQL Server resource provider V2 in a disconnected scenario, follow

the download marketplace items to Azure Stack Hub instruction to download the

MySQL Server resource provider item and Add-on RP Windows Server item to your

Azure Stack Hub environment.

When deploying MySQL Server resource provider V1 in a disconnected scenario,

complete the following steps to download the required PowerShell modules and

register the repository manually.

1. Sign in to a computer with internet connectivity and use the following scripts to

download the PowerShell modules.

PowerShell

2. Depending on the version of resource provider that you are deploying, run one of

the scripts.

PowerShell

PowerShell

3. Then you copy the downloaded packages to a USB device.

4. Sign in to the disconnected workstation and copy the packages from the USB

device to a location on the workstation.

Import-Module -Name PowerShellGet -ErrorAction Stop

Import-Module -Name PackageManagement -ErrorAction Stop

# path to save the packages, c:\temp\azs1.6.0 as an example here

$Path = "c:\temp\azs1.6.0"

# for resource provider version >= 1.1.93.0

Save-Package -ProviderName NuGet -Source

https://www.powershellgallery.com/api/v2 -Name AzureRM -Path $Path -

Force -RequiredVersion 2.5.0

Save-Package -ProviderName NuGet -Source

https://www.powershellgallery.com/api/v2 -Name AzureStack -Path $Path -

Force -RequiredVersion 1.8.2

# for resource provider version <= 1.1.47.0

Save-Package -ProviderName NuGet -Source

https://www.powershellgallery.com/api/v2 -Name AzureRM -Path $Path -

Force -RequiredVersion 2.3.0

Save-Package -ProviderName NuGet -Source

https://www.powershellgallery.com/api/v2 -Name AzureStack -Path $Path -

Force -RequiredVersion 1.6.0

5. Register this location as a local repository.

PowerShell

If you are upgrading from a V1 version, refer to the doc Update the MySQL Server

resource provider.

1. If you haven't already, sign in to the Azure Stack Hub administrator portal, select

Marketplace Management on the left, select Resource providers.

2. Once MySQL resource provider and other required software have been

downloaded, Marketplace Management shows the "MySQL Server resource

provider" packages with a status of "Not Installed". There may be other packages

that show a status of "Downloaded".

3. Select the row you wish to install. The MySQL Server resource provider install

package page shows a blue banner across the top. Select the banner to start the

# requires -Version 5

# requires -RunAsAdministrator

# requires -Module PowerShellGet

# requires -Module PackageManagement

$SourceLocation = "C:\temp\azs1.6.0"

$RepoName = "azs1.6.0"

Register-PSRepository -Name $RepoName -SourceLocation $SourceLocation -

InstallationPolicy Trusted

New-Item -Path $env:ProgramFiles -name "SqlMySqlPsh" -ItemType

"Directory"

Deploy the MySQL resource provider V2

Start installation

installation.

1. Next you're transferred to the install page. Select Install Prerequisites to begin the

installation process.

2. Wait until the installation of prerequisites succeeds. You should see a green

checkmark next to Install prerequisites before proceeding to the next step.

Install prerequisites

1. Under the 2. Prepare secrets step, select Add certificate, and the Add a certificate

panel will appear.

2. Select the browse button on Add a certificate, just to the right of the certificate

filename field. Select the .pfx certificate file you procured when completing the

prerequisites.

3. Enter the password you provided to create a secure string for SQL Server resource

provider SSL Certificate. Then select Add.

Prepare secrets

1. When the installation of the certificate succeeds, you should see a green

checkmark next to Prepare secrets before proceeding to the next step. Now select

the Configure + Install button next to 3 Install resource provider.

2. Next you'll need to provide an Azure Stack Hub Blob URI for MySQL Connector.

Review the GPL license of MySQL Connector here and download version

8.0.21 to a local folder.

Create a storage account with your default operator subscription, and create

a container with the access level "Blob" or "Container".

Configure and install resource provider

Upload the mysql-connector-net-8.0.21.msi file from your local folder to the

newly created storage container.

Copy the blob URI.

Go back to the MySQL RP configuration page. Paste the blob URI (e.g.

https://<storageAccountName>.blob.<region>.

<FQDN>/<containerName>/mysql-connector-net-8.0.21.msi) to the textbox

） Important

Make sure the version of the MySQL Connector is 8.0.21.

and click OK.

3. Next you'll see the following page, which indicates that MySQL resource provider is

being installed.

4. Wait for the installation complete notification. This process usually takes one or

more hours, depending on your Azure Stack Hub type.

5. Verify that the installation of MySQL Server resource provider has succeeded, by

returning to the Marketplace Management, Resource Providers page. The status

of MySQL Server resource provider should show "Installed".

After you've completed all of the prerequisites, run the self-extractor to extract the

downloaded installation package to a temporary directory. Run the

DeployMySqlProvider.ps1 script from a computer that can access both the Azure Stack

Hub Azure Resource Manager admin endpoint and the privileged endpoint, to deploy

the MySQL resource provider. The DeployMySqlProvider.ps1 script is extracted as part of

the MySQL resource provider installation files that you downloaded for your version of

Azure Stack Hub.

To deploy the MySQL resource provider, open a new elevated PowerShell window (not

PowerShell ISE) and change to the directory where you extracted the MySQL resource

Deploy the SQL resource provider V1

） Important

Before deploying the resource provider, review the release notes to learn about

new functionality, fixes, and any known issues that could affect your deployment.

provider binary files.

Run the DeployMySqlProvider.ps1 script, which completes the following tasks:

Uploads the certificates and other artifacts to a storage account on Azure Stack

Hub.

Publishes gallery packages so that you can deploy MySQL databases using the

gallery.

Publishes a gallery package for deploying hosting servers.

Deploys a VM using the Windows Server 2016 core image or Microsoft AzureStack

Add-on RP Windows Server image you downloaded, and then installs the MySQL

resource provider.

Registers a local DNS record that maps to your resource provider VM.

Registers your resource provider with the local Azure Resource Manager for the

operator account.

You can specify these parameters from the command line. If you don't, or if any

parameter validation fails, you're prompted to provide the required parameters.

） Important

We strongly recommend using Clear-AzureRmContext -Scope CurrentUser and

Clear-AzureRmContext -Scope Process to clear the cache before running the

deployment or update script.

７ Note

If you're deploying MySQL Server resource provider V1 in a disconnected

environment, copy the mysql-connector-net-6.10.5.msi file to a local path.

Provide the path name using the DependencyFilesLocalPath parameter.

７ Note

When the MySQL resource provider deployment starts, the

system.local.mysqladapter resource group is created. It may take up to 75 minutes

to finish the deployments required to this resource group. You should not place any

other resources in the system.local.mysqladapter resource group.

DeployMySqlProvider.ps1 parameters

Parameter name Description Comment or

default value

Parameter name Description Comment or

default value

CloudAdminCredential The credential for the cloud administrator,

necessary for accessing the privileged

endpoint.

Required

AzCredential The credentials for the Azure Stack Hub service

admin account. Use the same credentials that

you used for deploying Azure Stack Hub. The

script will fail if the account you use with

AzCredential requires multi-factor

authentication (MFA).

Required

VMLocalCredential The credentials for the local administrator

account of the MySQL resource provider VM.

Required

PrivilegedEndpoint The IP address or DNS name of the privileged

endpoint.

Required

AzureEnvironment The Azure environment of the service admin

account used for deploying Azure Stack Hub.

Required only for Azure AD deployments.

Supported environment names are

AzureCloud, AzureUSGovernment, or if using

a China Azure AD, AzureChinaCloud.

AzureCloud

DependencyFilesLocalPath For integrated systems only, your certificate

.pfx file must be placed in this directory. For

disconnected environments, download mysqlconnector-net-6.10.5.msi to this directory.

You can optionally copy one Windows Update

MSU package here.

Optional

(mandatory

for integrated

systems or

disconnected

environments)

DefaultSSLCertificatePassword The password for the .pfx certificate. Required

MaxRetryCount The number of times you want to retry each

operation if there's a failure.

2

RetryDuration The timeout interval between retries, in

seconds.

120

Uninstall Removes the resource provider and all

associated resources (see the following notes).

No

DebugMode Prevents automatic cleanup on failure. No

AcceptLicense Skips the prompt to accept the GPL license.

https://www.gnu.org/licenses/old-licenses/gpl2.0.html

If you are deploying the MySQL resource provider version 1.1.47.0 or later, the

deployment script will automatically download and install the necessary PowerShell

modules for you to path C:\Program Files\SqlMySqlPsh.

PowerShell

To eliminate any manual configuration when deploying the resource provider, you can

customize the following script. Change the default account information and passwords

as needed for your Azure Stack Hub deployment.

PowerShell

Deploy the MySQL resource provider using a

custom script

# Install the AzureRM.Bootstrapper module, set the profile and install the

AzureStack module

# Note that this might not be the most currently available version of Azure

Stack Hub PowerShell

Install-Module -Name AzureRm.BootStrapper -Force

Use-AzureRmProfile -Profile 2018-03-01-hybrid -Force

Install-Module -Name AzureStack -RequiredVersion 1.6.0

７ Note

In disconnected scenario, you need to download the required PowerShell modules

and register the repository manually as a prerequisite.

# Use the NetBIOS name for the Azure Stack Hub domain. On the Azure Stack

Hub SDK, the default is AzureStack but could have been changed at install

time.

$domain = "AzureStack"

# For integrated systems, use the IP address of one of the ERCS VMs.

$privilegedEndpoint = "AzS-ERCS01"

# Provide the Azure environment used for deploying Azure Stack Hub. Required

only for Azure AD deployments. Supported environment names are AzureCloud,

AzureUSGovernment, or AzureChinaCloud.

$AzureEnvironment = "<EnvironmentName>"

# Point to the directory where the resource provider installation files were

extracted.

$tempDir = 'C:\TEMP\MYSQLRP'

# The service admin account (can be Azure Active Directory or Active

Directory Federation Services).

When the resource provider installation script finishes, refresh your browser to make

sure you can see the latest updates and close the current PowerShell session.

1. Sign in to the administrator portal as the service admin.

2. Select Resource Groups.

3. Select the system.<location>.mysqladapter resource group.

4. On the summary page for Resource group Overview, there should be no failed

deployments.

$serviceAdmin = "admin@mydomain.onmicrosoft.com"

$AdminPass = ConvertTo-SecureString 'P@ssw0rd1' -AsPlainText -Force

$AdminCreds = New-Object System.Management.Automation.PSCredential

($serviceAdmin, $AdminPass)

# Set the credentials for the new resource provider VM local admin account

$vmLocalAdminPass = ConvertTo-SecureString 'P@ssw0rd1' -AsPlainText -Force

$vmLocalAdminCreds = New-Object System.Management.Automation.PSCredential

("mysqlrpadmin", $vmLocalAdminPass)

# And the cloudadmin credential required for privileged endpoint access.

$CloudAdminPass = ConvertTo-SecureString 'P@ssw0rd1' -AsPlainText -Force

$CloudAdminCreds = New-Object System.Management.Automation.PSCredential

("$domain\cloudadmin", $CloudAdminPass)

# Change the following as appropriate.

$PfxPass = ConvertTo-SecureString 'P@ssw0rd1' -AsPlainText -Force

# For version 1.1.47.0 or later, the PowerShell modules used by the RP

deployment are placed in C:\Program Files\SqlMySqlPsh,

# The deployment script adds this path to the system $env:PSModulePath to

ensure correct modules are used.

$rpModulePath = Join-Path -Path $env:ProgramFiles -ChildPath 'SqlMySqlPsh'

$env:PSModulePath = $env:PSModulePath + ";" + $rpModulePath

# Change to the directory folder where you extracted the installation files.

Don't provide a certificate on ASDK!

. $tempDir\DeployMySQLProvider.ps1 `

-AzCredential $AdminCreds `

-VMLocalCredential $vmLocalAdminCreds `

-CloudAdminCredential $cloudAdminCreds `

-PrivilegedEndpoint $privilegedEndpoint `

-AzureEnvironment $AzureEnvironment `

-DefaultSSLCertificatePassword $PfxPass `

-DependencyFilesLocalPath $tempDir\cert `

-AcceptLicense

Verify the V1 deployment by using the Azure Stack Hub

portal

5. Finally, select Virtual machines in the administrator portal to verify that the MySQL

resource provider VM was successfully created and is running.

If your Azure Stack Hub is using Azure AD as an identity provider, make sure the VM

that has installed MySQL Server resource provider has outbound internet connectivity.

Add hosting servers

Important configuration for Azure AD

Next steps

Add MySQL hosting servers in Azure

Stack Hub

Article • 02/20/2023

You can host a MySQL hosting server instance on a virtual machine (VM) in Azure Stack

Hub, or on a VM outside your Azure Stack Hub environment, as long as the MySQL

resource provider can connect to the instance.

MySQL versions 5.6, 5.7 and 8.0 may be used for your hosting servers. The MySQL RP

doesn't support caching\_sha2\_password authentication. MySQL 8.0 servers must be

configured to use mysql\_native\_password.

By default, no public access is configured for MySQL into the host VM. For the Azure

Stack Hub MySQL resource provider to connect and manage the MySQL server, an

inbound network security group (NSG) rule needs to be created.

1. In the administrator portal, go to the resource group created when deploying the

MySQL server and select the network security group (default-subnet-sg):

） Important

Starting from Azure Stack Hub build 2108, the SQL and MySQL resource providers

are offered to subscriptions that have been granted access. If you want to start

using this feature, or if you need to upgrade from a previous version, open a

support case and our support engineers will guide you through the deployment or

upgrade process.

７ Note

The MySQL resource provider should be created in the default provider

subscription while MySQL hosting servers should be created in billable, user

subscriptions. The resource provider server shouldn't be used to host user

databases.

Prepare a MySQL hosting server

Create a network security group rule

2. Select Inbound security rules and then select Add.

Enter 3306 in the Destination port range and optionally provide a description in

the Name and Description fields.

3. Select Add to close the inbound security rule dialog.

Configure external access to the MySQL hosting server

Before the MySQL server can be added as an Azure Stack Hub MySQL Server host,

external access must be enabled. Take Bitnami MySQL, which is available in Azure Stack

Hub marketplace as an example, you can take the following steps to configure the

external access.

1. Using an SSH client (this example uses PuTTY ) log in to the MySQL server from a

computer that can access the public IP.

Use the public IP and log in to the VM with the username and the application

password you created earlier without special characters.

2. In the SSH client window, use the following command to ensure the bitnami

service is active and running. Provide the bitnami password again when prompted:

sudo service bitnami status

3. If the MySQL hosting server is version 8.0 or above, you need to change the

authentication method to mysql\_native\_password. If the MySQL version is below

8.0, this step can be skipped.

Take Bitnami MySQL as example, the configuration file is under

/opt/bitnami/mysql/conf/my.cnf. Set the property default\_authentication\_plugin

with value mysql\_native\_password.

Restart the Bitnami service and make sure it's running properly, but before you

must delete the ib\_logfile0 file before starting the Bitnami service.

Console

4. Create a remote access user account to be used by the Azure Stack Hub MySQL

Hosting Server to connect to MySQL.

Run the following commands to log in to MySQL as root, using the root password

which is recorded in ~/bitnami\_credentials. Create a new admin user and replace

[mysqld]

default\_authentication\_plugin=mysql\_native\_password

sudo service bitnami stop

sudo rm /bitnami/mysql/data/ib\_logfile0

sudo service bitnami start

sudo service bitnami status

<username> and <password> as required for your environment. In this example,

the created user is named sqlsa and a strong password is used:

SQL

5. Make sure the plugin of the created sql user sqlsa is mysql\_native\_password and

then exit the SSH client.

SQL

6. Record the new MySQL user information.

This username and password will be used while Azure Stack Hub operator creates a

MySQL hosting server using this MySQL server.

Make sure you have the credentials for an account with system admin privileges.

mysql -u root -p

create user <username>@'%' identified by '<password>';

grant all privileges on \*.\* to <username>@'%' with grant option;

flush privileges;

SELECT user,host,plugin from mysql.user;

Connect to a MySQL hosting server

７ Note

To add a hosting server, follow these steps:

1. Sign in to the Azure Stack Hub administrator portal as a service admin.

2. Select All services.

3. Under the ADMINISTRATIVE RESOURCES category, select MySQL Hosting Servers

> +Add. The Add a MySQL Hosting Server dialog will open, shown in the

following screen capture.

For MySQL 8.0 and above versions, the remote access isn't enabled by default. You

need to create a new user account and grant the privilege of remote access to this

user account before adding it as a hosting server.

4. Provide the connection details of your MySQL Server instance.

For MySQL Hosting Server Name, provide the fully qualified domain name

(FQDN) or a valid IPv4 address. Don't use the short VM name.

The default admin Username for the Bitnami MySQL images available in

Azure Stack Hub Marketplace is root.

If you don't know the root Password, see the Bitnami documentation to

learn how to get it.

A default MySQL instance isn't provided, so you have to specify the Size of

Hosting Server in GB. Enter a size that's close to the capacity of the database

server.

Keep the default setting for Subscription.

For Resource group, create a new one, or use an existing group.

） Important

Do not choose Resource group system.<region>.sqladapter , which was

created by the MySQL resource provider installer during deployment. You

must provide a different resource group for the hosting server.

７ Note

If the MySQL instance can be accessed by the tenant and the admin Azure

Resource Manager, you can put it under the control of the resource provider.

But, the MySQL instance must be allocated exclusively to the resource

provider.

5. Select SKUs to open the Create SKU dialog.

The SKU Name should reflect the properties of the SKU so users can deploy their

databases to the appropriate SKU.

6. Select OK to create the SKU.

7. Under Add a MySQL Hosting Server, select Create.

As you add servers, assign them to a new or existing SKU to differentiate service

offerings. For example, you can have a MySQL enterprise instance that provides

increased database and automatic backups. You can reserve this high-performance

server for different departments in your organization.

The following information applies to the RP and MySQL hosting servers:

Ensure that all hosting servers are configured for communication using TLS 1.1. See

Configuring MySQL to Use Encrypted Connections .

Employ Transparent Data Encryption .

The MySQL RP doesn't support caching\_sha2\_password authentication.

You can increase backend database capacity by deploying more MySQL servers in the

Azure Stack Hub portal. Add these servers to a new or existing SKU. If you add a server

to an existing SKU, make sure the server characteristics are the same as the other servers

in the SKU.

Use a SKU name that describes the capabilities of the servers in the SKU, such as

capacity and performance. The name serves as an aid to help users deploy their

７ Note

SKUs can take up to an hour to be visible in the portal. You can't create a

database until the SKU is deployed and running.

Security considerations for MySQL

Increase backend database capacity

SKU notes

databases to the appropriate SKU. For example, you can use SKU names to differentiate

service offerings by the following characteristics:

high capacity

high performance

high availability

As a best practice, all the hosting servers in a SKU should have the same resource and

performance characteristics.

SKUs cannot be hidden from certain tenants, nor can it be dedicated to certain tenants.

To edit a SKU, go to All services > MySQL Adapter > SKUs. Select the SKU to modify,

make any necessary changes, and click Save to save changes.

To delete a SKU that's no longer needed, go to All services > MySQL Adapter > SKUs.

Right-click the SKU name and select Delete to delete it.

Create plans and offers to make MySQL database servers available to users. Add the

Microsoft.MySqlAdapter service to the plan and create a new quota. MySQL doesn't

allow limiting the size of databases.

） Important

It can take up to an hour for new SKUs to be available in the user portal.

Make MySQL database servers available to your

users

） Important

It can take up to two hours for new quotas to be available in the user portal or

before a changed quota is enforced.

７ Note

You can't delete a quota if there are any current plans that use it. You must first

delete the plan that references the quota.

Create a MySQL database

Next steps

Create MySQL databases in Azure Stack

Hub

Article • 07/29/2022

An Azure Stack Hub user that's subscribed to an offer that includes the MySQL database

service can create and manage self-service MySQL databases in the user portal.

1. Sign in to the Azure Stack Hub user portal.

2. Select + Create a resource > Data + Storage > MySQL Database > Add.

3. Under Create MySQL Database, enter the Database Name, and configure the other

settings as required for your environment.

） Important

Starting from Azure Stack Hub build 2108, the SQL and MySQL resource providers

are offered to subscriptions that have been granted access. If you want to start

using this feature, or if you need to upgrade from a previous version, open a

support case and our support engineers will guide you through the deployment or

upgrade process.

Create a MySQL database

4. Under Create Database, select SKU. Under Select a MySQL SKU, pick the SKU for

your database.

5. Under Login, select Configure required settings.

6. Under Select a Login, you can choose an existing login or select + Create a new

login to set up a new login. Enter a Database login name and Password, and then

select OK.

７ Note

As hosting servers are added to Azure Stack Hub, they're assigned a SKU.

Databases are created in the pool of hosting servers in a SKU.

7. Select Create to finish setting up the database.

After the database is deployed, take note of the Connection String under Essentials.

You can use this string in any application that needs to access the MySQL database.

７ Note

The length of the Database login name can't exceed 32 characters in MySQL

5.7. In earlier editions, it can't exceed 16 characters.

You can modify the password by changing it on the MySQL server instance.

1. Select ADMINISTRATIVE RESOURCES > MySQL Hosting Servers. Select the

hosting server.

2. Under Settings, select Password.

3. Under Password, enter the new password and then select Save.

Learn how to offer highly available MySQL databases.

Update the administrative password

Next steps

Create highly available MySQL

databases

Article • 01/09/2023

As an Azure Stack Hub operator, you can configure server virtual machines (VMs) to host

MySQL Server databases. After a MySQL cluster is successfully created and managed by

Azure Stack Hub, users who have subscribed to MySQL services can easily create highly

available MySQL databases.

This article shows how to use Azure Stack Marketplace items to create a MySQL with

replication cluster . This solution uses multiple VMs to replicate the databases from the

control plane node to a configurable number of replicas. Once created, the cluster can

then be added as an Azure Stack Hub MySQL Hosting Server, and then users can create

highly available MySQL databases.

What you'll learn:

A three-VM MySQL Server cluster will be created and configured using available Azure

Stack Marketplace items.

Before starting, ensure that the MySQL Server resource provider has been successfully

installed and that the following items are available in Azure Stack Marketplace:

） Important

Starting from Azure Stack Hub build 2108, the SQL and MySQL resource providers

are offered to subscriptions that have been granted access. If you want to start

using this feature, or if you need to upgrade from a previous version, open a

support case and our support engineers will guide you through the deployment or

upgrade process.

） Important

The MySQL with replication Azure Stack Marketplace item might not be available

for all Azure cloud subscription environments. Verify that the marketplace item is

available in your subscription before attempting to follow the rest of this tutorial.

＂ Create a MySQL Server cluster from marketplace items.

＂ Configure the MySQL Server cluster as an Azure Stack Hub MySQL Hosting Server.

＂ Create a highly available MySQL database.

MySQL with Replication : This is the Bitnami solution template that will be used

for the MySQL cluster deployment.

Debian 8 "Jessie" : Debian 8 "Jessie" with backports kernel for Microsoft Azure

provided by credativ. Debian GNU/Linux is one of the most popular Linux

distributions.

Custom script for linux 2.0 : Custom Script Extension is a tool to execute your VM

customization tasks post VM provision. When this Extension is added to a VM, it

can download scripts from Azure storage and run them on the VM. Custom Script

Extension tasks can also be automated using the Azure PowerShell cmdlets and

Azure Cross-Platform Command-Line Interface (xPlat CLI).

VM Access For Linux Extension 1.4.7: The VM Access extension enables you to reset

the password, SSH key, or the SSH configurations so you can regain access to your

VM. You can also add a new user with password or SSH key, or delete a user using

this extension. This extension targets Linux VMs.

To learn more about adding items to Azure Stack Marketplace, see the Azure Stack

Marketplace overview.

You'll also need an SSH client like PuTTY to log in to the Linux VMs after they're

deployed.

Use the steps in this section to deploy the MySQL Server cluster using the MySQL with

Replication marketplace item. This template deploys three MySQL Server instances

configured in a highly available MySQL cluster. By default, it creates the following

resources:

A virtual network

A network security group

A storage account

An availability set

Three network interfaces (one for each of the default VMs)

A public IP address (for the primary MySQL cluster VM)

Three Linux VMs to host the MySQL cluster

1. Sign in to the user portal:

） Important

All of the following are required to create the MySQL cluster.

Create a MySQL Server cluster

For an integrated system deployment, the portal address will vary based on

your solution's region and external domain name. It will be in the format of

https://portal.<region>.<FQDN> .

For the Azure Stack Development Kit (ASDK), the portal address is

https://portal.local.azurestack.external .

2. If no subscriptions were assigned yet, select Get a Subscription from the

Dashboard. In the blade, type a name for the subscription, and then select an offer.

It is recommended that you keep the MySQL cluster deployment in its own

subscription to prevent accidental removal.

3. Select + Create a resource > Compute, and then MySQL with Replication.

4. Provide basic deployment information on the Basics page. Review the default

values and change as needed and select OK.

At a minimum, provide the following info:

Deployment name (default is mymysql).

Application root password. Provide a 12 character alphanumeric password

with no special characters.

Application database name (default is bitnami).

Number of MySQL database replica VMs to create (default is 2).

Select the subscription to use.

Select the resource group to use or create a new one.

Select the location (default is local for ASDK before version 2107).

5. On the Environment Configuration page, provide the following information and

then select OK:

Password or SSH public key to use for secure shell (SSH) authentication. If

using a password, it must contain letters, numbers, and can contain special

characters.

VM size (default is Standard D1 v2 VMs).

Data disk size in GB

6. Review the deployment Summary. Optionally, you can download the customized

template and parameters and then select OK.

7. Select Create on the Buy page to start the deployment.

8. After all deployments have completed successfully, review the resource group

items and select the mysqlip Public IP address item. Record the public IP address

and full FQDN of the public IP for the cluster.

You'll need to provide this IP address to an Azure Stack Hub operator so they can

create a MySQL hosting server leveraging this MySQL cluster.

By default, no public access is configured for MySQL into the host VM. For the Azure

Stack Hub MySQL resource provider to connect and manage the MySQL cluster, an

inbound network security group (NSG) rule needs to be created.

７ Note

The deployment will take about an hour. Ensure that the deployment has

finished and the MySQL cluster has been completely configured before

continuing.

Create a network security group rule

1. In the administrator portal, go to the resource group created when deploying the

MySQL cluster and select the network security group (default-subnet-sg):

2. Select Inbound security rules and then select Add.

Enter 3306 in the Destination port range and optionally provide a description in

the Name and Description fields.

3. Select Add to close the inbound security rule dialog.

Before the MySQL cluster can be added as an Azure Stack Hub MySQL Server host,

external access must be enabled.

1. Using an SSH client (this example uses PuTTY ) log in to the primary MySQL

machine from a computer that can access the public IP. The primary MySQL VM

name usually ends with 0 and has a public IP assigned to it.

Use the public IP and log in to the VM with the username of bitnami and the

application password you created earlier without special characters.

2. In the SSH client window, use the following command to ensure the bitnami

service is active and running. Provide the bitnami password again when prompted:

sudo service bitnami status

Configure external access to the MySQL cluster

3. Create a remote access user account to be used by the Azure Stack Hub MySQL

Hosting Server to connect to MySQL and then exit the SSH client.

Run the following commands to log in to MySQL as root, using the root password

created earlier. Create a new admin user and replace <username> and <password>

as required for your environment. In this example, the created user is named sqlsa

and a strong password is used:

mysql

mysql -u root -p

create user <username>@'%' identified by '<password>';

grant all privileges on \*.\* to <username>@'%' with grant option;

flush privileges;

4. Record the new MySQL user information.

You'll need to provide this username and password, along with the public IP

address or full FQDN of the public IP for the cluster, to an Azure Stack Hub

operator so they can create a MySQL hosting server using this MySQL cluster.

After the MySQL Server cluster is created and properly configured, an Azure Stack Hub

operator must add it as an Azure Stack Hub MySQL Hosting Server.

Be sure to use the public IP or full FQDN for the public IP of the MySQL cluster primary

VM recorded previously when the MySQL cluster's resource group was created

(mysqlip). In addition, the operator needs to know the MySQL Server authentication

credentials you created to remotely access the MySQL cluster database.

Using the MySQL cluster's Public IP and MySQL authentication login information, an

Azure Stack Hub operator can now create a MySQL Hosting Server using the new

MySQL cluster.

Configure an Azure Stack Hub MySQL Hosting

Server

７ Note

This step must be run from the Azure Stack Hub administrator portal by an Azure

Stack Hub operator.

Also ensure that you've created plans and offers to make MySQL database creation

available for users. An operator will need to add the Microsoft.MySqlAdapter service to

a plan and create a new quota specifically for highly available databases. For more

information about creating plans, see Service, plan, offer, subscription overview.

After the MySQL cluster is created and configured, and added as an Azure Stack Hub

MySQL Hosting Server by an Azure Stack Hub operator, a tenant user with a

subscription including MySQL Server database capabilities can create highly available

MySQL databases by following the steps in this section.

1. Sign in to the user portal:

For an integrated system deployment, the portal address will vary based on

your solution's region and external domain name. It will be in the format of

https://portal.<region>.<FQDN> .

For the Azure Stack Development Kit (ASDK), the portal address is

https://portal.local.azurestack.external .

2. Select + Create a resource > Data + Storage, and then MySQL Database.

Provide the required database property information including name, collation, the

subscription to use, and location to use for the deployment.

 Tip

The Microsoft.MySqlAdapter service won't be available to add to plans until the

MySQL Server resource provider has been deployed.

Create a highly available MySQL database

７ Note

Run these steps from the Azure Stack Hub user portal as a tenant user with a

subscription providing MySQL Server capabilities (Microsoft.MySQLAdapter

service).

3. Select SKU and then choose the appropriate MySQL Hosting Server SKU to use. In

this example, the Azure Stack Hub operator has created the MySQL-HA SKU to

support high availability for MySQL cluster databases.

4. Select Login > Create a new login and then provide the MySQL authentication

credentials to be used for the new database. When finished, select OK and then

Create to begin the database deployment process.

5. When the MySQL database deployment completes successfully, review the

database properties to discover the connection string to use for connecting to the

new highly available database.

Update the MySQL resource provider

Next steps

Update the MySQL resource provider in

Azure Stack Hub

Article • 05/22/2023

When Azure Stack Hub releases a new build, we may release A new MySQL resource

provider adapter. While the existing adapter continues to work, we recommend

updating to the latest build as soon as possible.

Supported Azure Stack

Hub version

MySQL RP version Windows Server that RP service is

running on

2206, 2301 MySQL RP version

2.0.13.x

Microsoft AzureStack Add-on RP Windows

Server 1.2009.0

2108,2206 MySQL RP version

2.0.6.x

Microsoft AzureStack Add-on RP Windows

Server 1.2009.0

2108, 2102, 2008, 2005 MySQL RP version

1.1.93.5

Microsoft AzureStack Add-on RP Windows

Server

） Important

Starting from Azure Stack Hub build 2108, the SQL and MySQL resource providers

are offered to subscriptions that have been granted access. If you want to start

using this feature, or if you need to upgrade from a previous version, open a

support case and our support engineers will guide you through the deployment or

upgrade process.

） Important

Before updating the resource provider, review the release notes to learn about new

functionality, fixes, and any known issues that could affect your deployment. The

release notes also specify the minimum Azure Stack Hub version required for the

resource provider.

） Important

Updating the resource provider will NOT update the hosting MySQL Server.

Supported Azure Stack

Hub version

MySQL RP version Windows Server that RP service is

running on

2005, 2002, 1910 MySQL RP version

1.1.47.0

Windows Server 2016 Datacenter - Server

Core

1908 MySQL RP version

1.1.33.0

Windows Server 2016 Datacenter - Server

Core

If you have already deployed MySQL RP V2, and want to check for updates, check How

to apply updates to resource provider.

If you want to update from MySQL RP V1 to MySQL RP V2, make sure you have first

updated to MySQL RP V1.1.93.x, then apply the major version upgrade process to

upgrade from MySQl RP V1 to MySQL RP V2.

1. Make sure you have updated MySQL RP V1 to the latest 1.1.93.x. Under Default

Provider Subscription, find the RP resource group (naming format: system.

<region>.mysqladapter). Confirm the version tag and MySQL RP VM name in

resource group.

2. Open a support case to get the MajorVersionUpgrade package, and add your

subscription to the ASH marketplace allowlist for the future V2 version.

3. Download Microsoft AzureStack Add-On RP Windows Server 1.2009.0 to

marketplace.

4. Ensure your Azure Stack Hub meets the datacenter integration prerequisites.

Prerequisite Reference

Conditional DNS forwarding is set

correctly.

Azure Stack Hub datacenter integration - DNS

Update MySQL Server resource provider V2

Update from MySQL RP V1.1.93.x to MySQL RP

V2.0.6.0

Prerequisites

Prerequisite Reference

Inbound ports for resource

providers are open.

Azure Stack Hub datacenter integration - Ports and

protocols inbound

PKI certificate subject and SAN are

set correctly.

Azure Stack Hub deployment mandatory PKI

prerequisites

Azure Stack Hub deployment PaaS certificate

prerequisites

5. (for disconnected environment) Install the required PowerShell modules, similar to

the update process used to Deploy the MySQL resource provider.

6. Prepare the MySQL Connector Uri with the required version. For details, refer to

Deploy the MySQL resource provider. e.g. https://<storageAcountName>.blob.

<region>.<FQDN>/<containerName>/mysql-connector-net-8.0.21.msi

Run the following script from an elevated PowerShell console to perform major version

upgrade.

PowerShell

Trigger MajorVersionUpgrade

７ Note

Make sure the client machine that you run the script on is of OS version no older

than Windows 10 or Windows Server 2016, and the client machine has X64

Operating System Architecture.

） Important

We strongly recommend using Clear-AzureRmContext -Scope CurrentUser and

Clear-AzureRmContext -Scope Process to clear the cache before running the

deployment or update script.

# Check Operating System version

$osVersion = [environment]::OSVersion.Version

if ($osVersion.Build -lt 10240)

{

Write-Host "OS version is too old: $osVersion."

return

}

$osArch = (Get-WmiObject Win32\_OperatingSystem).OSArchitecture

if ($osArch -ne "64-bit")

{

Write-Host "OS Architecture is not 64 bit."

return

}

# Check LongPathsEnabled registry key

$regPath = 'HKLM:\SYSTEM\CurrentControlSet\Control\FileSystem'

$longPathsEnabled = 'LongPathsEnabled'

$property = Get-ItemProperty -Path $regPath -Name $longPathsEnabled -

ErrorAction Stop

if ($property.LongPathsEnabled -eq 0)

{

Write-Host "Detect LongPathsEnabled equals to 0, prepare to set the

property."

Set-ItemProperty -Path $regPath -Name $longPathsEnabled -Value 1 -

ErrorAction Stop

Write-Host "Set the long paths property, please restart the PowerShell."

return

}

# Use the NetBIOS name for the Azure Stack Hub domain.

$domain = "YouDomain"

# For integrated systems, use the IP address of one of the ERCS VMs

$privilegedEndpoint = "YouDomain-ERCS01"

# Provide the Azure environment used for deploying Azure Stack Hub. Required

only for Azure AD deployments. Supported values for the <environment name>

parameter are AzureCloud, AzureChinaCloud, or AzureUSGovernment depending

which Azure subscription you're using.

$AzureEnvironment = "AzureCloud"

# Point to the directory where the resource provider installation files were

extracted.

$tempDir = 'C:\extracted-folder\MajorVersionUpgrade-MySQLRP'

# The service admin account can be Azure Active Directory or Active

Directory Federation Services.

$serviceAdmin = "admin@mydomain.onmicrosoft.com"

$AdminPass = ConvertTo-SecureString 'xxxxxxxx' -AsPlainText -Force

$AdminCreds = New-Object System.Management.Automation.PSCredential

($serviceAdmin, $AdminPass)

# Add the cloudadmin credential that's required for privileged endpoint

access.

$CloudAdminPass = ConvertTo-SecureString 'xxxxxxxx' -AsPlainText -Force

$CloudAdminCreds = New-Object System.Management.Automation.PSCredential

("$domain\cloudadmin", $CloudAdminPass)

# Change the following as appropriate.

$PfxPass = ConvertTo-SecureString 'xxxxxxx' -AsPlainText -Force

# Provide the pfx file path

$PfxFilePath = "C:\tools\mysqlcert\SSL.pfx"

# Local blob uri where stores the required mysql connector

$MySQLConnector = "Provide the MySQL Connector Uri according to

Prerequisites step."

# PowerShell modules used by the RP MajorVersionUpgrade are placed in

C:\Program Files\SqlMySqlPsh

1. The MajorVersionUpgrade script executed without any errors.

2. Check the resource provider in marketplace and make sure that MySQL RP 2.0 has

been installed successfully.

3. The old system.<location>.mysqladapter resource group and system.

<location>.dbadapter.dns resource group in the default provider subscription will

not be automatically deleted by the script.

We recommend keeping the Storage Account and the Key Vault in the

mysqladapter resource group for some time. If after the upgrade, any tenant user

observes inconsistent database or login metadata, it is possible to get support to

restore the metadata from the resource group.

After verifying that the DNS Zone in the dbadapter.dns resource group is empty

with no DNS record, it is safe to delete the dbadapter.dns resource group.

[IMPORTANT] Do not use the V1 deploy script to uninstall the V1 version. After

upgrade completed and confirmation that the upgrade was successful, you can

manually delete the resource group from the provider subscription.

# The deployment script adds this path to the system $env:PSModulePath to

ensure correct modules are used.

$rpModulePath = Join-Path -Path $env:ProgramFiles -ChildPath 'SqlMySqlPsh'

$env:PSModulePath = $env:PSModulePath + ";" + $rpModulePath

. $tempDir\MajorVersionUpgradeMySQLProvider.ps1 -AzureEnvironment

$AzureEnvironment -AzCredential $AdminCreds -CloudAdminCredential

$CloudAdminCreds -Privilegedendpoint $privilegedEndpoint -PfxPassword

$PfxPass -PfxCert $PfxFilePath -MySQLConnector $MySQLConnector

７ Note

The DNS address and the corresponding IP address of MySQL RP V2 are different.

To get the new public IP, you can contact support to require a DRP break glass and

find the MySQLRPVM1130-PublicIP resource. You can also run "nslookup

mysqlrp.dbadapter.<fqdn>" from a client machine that already passed the

endpoint test to find out the public IP.

Validate the upgrade is successful

Update from MySQL RP V1 earlier version to

MySQL RP V1.1.93.x

MySQL resource provider V1 update is cumulative. You can directly update to the

1.1.93.x version.

To update the resource provider to 1.1.93.x, use the UpdateMySQLProvider.ps1 script.

Use your service account with local administrative rights and is an owner of the

subscription. This update script is included with the download of the resource provider.

To update the resource provider, you use the UpdateMySQLProvider.ps1 script. Use

your service account with local administrative rights and is an owner of the subscription.

The update script is included with the download of the resource provider.

The update process is similar to the process used to Deploy the resource provider. The

update script uses the same arguments as the DeployMySqlProvider.ps1 script, and

you'll need to provide certificate information.

The UpdateMySQLProvider.ps1 script creates a new virtual machine (VM) with the latest

OS image, deploy the latest resource provider code, and migrates the settings from the

old resource provider to the new resource provider.

After the UpdateMySQLProvider.ps1 script creates a new VM, the script migrates the

following settings from the old resource provider VM:

database information

hosting server information

required DNS record

Update script processes

７ Note

We recommend that you download the Microsoft AzureStack Add-on RP Windows

Server 1.2009.0 image from Marketplace Management. If you need to install an

update, you can place a single MSU package in the local dependency path. The

script will fail if there's more than one MSU file in this location.

） Important

We strongly recommend using Clear-AzureRmContext -Scope CurrentUser and

Clear-AzureRmContext -Scope Process to clear the cache before running the

deployment or update script.

Specify the following parameters from the command line when you run the

UpdateMySQLProvider.ps1 PowerShell script. If you don't, or if any parameter validation

fails, you're prompted to provide the required parameters.

Parameter Name Description Comment

or default

value

CloudAdminCredential The credential for the cloud admin, necessary for

accessing the privileged endpoint.

Required

AzCredential The credentials for the Azure Stack Hub service

admin account. Use the same credentials that you

used for deploying Azure Stack Hub. The script

will fail if the account you use with AzCredential

requires multi-factor authentication (MFA).

Required

VMLocalCredential The credentials for the local admin account of the

MySQL resource provider VM.

Required

PrivilegedEndpoint The IP address or DNS name of the privileged

endpoint.

Required

AzureEnvironment The Azure environment of the service admin

account used for deploying Azure Stack Hub.

Required only for Azure AD deployments.

Supported environment names are AzureCloud,

AzureUSGovernment, or if using a China Azure

AD, AzureChinaCloud.

AzureCloud

DependencyFilesLocalPath Your certificate .pfx file must be placed in this

directory as well.

Optional

(mandatory

for multinode)

DefaultSSLCertificatePassword The password for the .pfx certificate. Required

MaxRetryCount The number of times you want to retry each

operation if there's a failure.

2

RetryDuration The timeout interval between retries, in seconds. 120

Uninstall Remove the resource provider and all associated

resources (see the following notes).

No

DebugMode Prevents automatic cleanup on failure. No

Update script parameters

Parameter Name Description Comment

or default

value

AcceptLicense Skips the prompt to accept the GPL license.

(https://www.gnu.org/licenses/old-licenses/gpl2.0.html )

If you are updating the MySQL resource provider version to 1.1.33.0 or previous

versions, you need to install specific versions of AzureRm.BootStrapper and Azure Stack

Hub modules in PowerShell.

If you are updating the MySQL resource provider to version 1.1.47.0 or later, you can

skip this step. The deployment script will automatically download and install the

necessary PowerShell modules for you to path C:\Program Files\SqlMySqlPsh.

PowerShell

Update script example

７ Note

If folder C:\Program Files\SqlMySqlPsh already exists with PowerShell module

downloaded, it is recommended to clean up this folder before running the update

script. This is to make sure the right version of PowerShell module is downloaded

and used.

# Run the following scripts when updating to version 1.1.33.0 only.

# Install the AzureRM.Bootstrapper module, set the profile and install the

AzureStack module.

# Note that this might not be the most currently available version of Azure

Stack Hub PowerShell.

Install-Module -Name AzureRm.BootStrapper -Force

Use-AzureRmProfile -Profile 2018-03-01-hybrid -Force

Install-Module -Name AzureStack -RequiredVersion 1.6.0

７ Note

In disconnected scenario, you need to download the required PowerShell modules

and register the repository manually as a prerequisite. You can get more

information in Deploy MySQL resource provider

The following example shows the UpdateMySQLProvider.ps1 script that you can run from

an elevated PowerShell console. Be sure to change the variable information and

passwords as needed:

PowerShell

# Use the NetBIOS name for the Azure Stack Hub domain. On the Azure Stack

Hub SDK, the default is AzureStack but could have been changed at install

time.

$domain = "AzureStack"

# For integrated systems, use the IP address of one of the ERCS VMs.

$privilegedEndpoint = "AzS-ERCS01"

# Provide the Azure environment used for deploying Azure Stack Hub. Required

only for Azure AD deployments. Supported environment names are AzureCloud,

AzureUSGovernment, or AzureChinaCloud.

$AzureEnvironment = "<EnvironmentName>"

# Point to the directory where the resource provider installation files were

extracted.

$tempDir = 'C:\TEMP\MYSQLRP'

# The service admin account (can be Azure Active Directory or Active

Directory Federation Services).

$serviceAdmin = "admin@mydomain.onmicrosoft.com"

$AdminPass = ConvertTo-SecureString 'P@ssw0rd1' -AsPlainText -Force

$AdminCreds = New-Object System.Management.Automation.PSCredential

($serviceAdmin, $AdminPass)

# Set credentials for the new resource provider VM.

$vmLocalAdminPass = ConvertTo-SecureString 'P@ssw0rd1' -AsPlainText -Force

$vmLocalAdminCreds = New-Object System.Management.Automation.PSCredential

("mysqlrpadmin", $vmLocalAdminPass)

# And the cloudadmin credential required for privileged endpoint access.

$CloudAdminPass = ConvertTo-SecureString 'P@ssw0rd1' -AsPlainText -Force

$CloudAdminCreds = New-Object System.Management.Automation.PSCredential

("$domain\cloudadmin", $CloudAdminPass)

# Change the following as appropriate.

$PfxPass = ConvertTo-SecureString 'P@ssw0rd1' -AsPlainText -Force

# For version 1.1.47.0 or later, the PowerShell modules used by the RP

deployment are placed in C:\Program Files\SqlMySqlPsh

# The deployment script adds this path to the system $env:PSModulePath to

ensure correct modules are used.

$rpModulePath = Join-Path -Path $env:ProgramFiles -ChildPath 'SqlMySqlPsh'

$env:PSModulePath = $env:PSModulePath + ";" + $rpModulePath

# Change directory to the folder where you extracted the installation files.

# Then adjust the endpoints.

.$tempDir\UpdateMySQLProvider.ps1 -AzCredential $AdminCreds -

When the resource provider update script finishes, close the current PowerShell session.

Maintain MySQL resource provider

VMLocalCredential $vmLocalAdminCreds -CloudAdminCredential $cloudAdminCreds

-PrivilegedEndpoint $privilegedEndpoint -AzureEnvironment $AzureEnvironment

-DefaultSSLCertificatePassword $PfxPass -DependencyFilesLocalPath

$tempDir\cert -AcceptLicense

Next steps

MySQL resource provider maintenance

operations in Azure Stack Hub

Article • 07/29/2022

The MySQL resource provider runs on a locked down virtual machine (VM). To enable

maintenance operations, you need to update the VM's security. To do this using the

principle of least privilege (POLP), you can use PowerShell Just Enough Administration

(JEA) endpoint DBAdapterMaintenance. The resource provider installation package

includes a script for this operation.

The MySQL resource provider isn't serviced as part of Azure Stack Hub because it's an

add-on component. Microsoft provides updates to the MySQL resource provider as

necessary.

For MySQL RP V1, When an updated MySQL Server resource provider is released, a

script is provided to apply the update. This script creates a new resource provider VM,

migrating the state of the old provider VM to the new VM.

For MySQL RP V2, resource providers are updated using the same update feature that is

used to apply Azure Stack Hub updates.

For more information, see Update the MySQL resource provider.

MySQL RP V1 runs on a user VM, you need to apply the required patches and updates

when they're released. You can install a Windows Update package during the installation

of, or update to, the resource provider.

） Important

Starting from Azure Stack Hub build 2108, the SQL and MySQL resource providers

are offered to subscriptions that have been granted access. If you want to start

using this feature, or if you need to upgrade from a previous version, open a

support case and our support engineers will guide you through the deployment or

upgrade process.

Patching and updating

Update the provider VM

MySQL RP V2 runs on a managed Windows Server that is hidden. You don't need to

patch or update the resource provider VM. It will be updated automatically when you

update the RP.

These instructions only apply to SQL RP V1 running on Azure Stack Hub Integrated

Systems.

To update the Defender definitions, follow these steps:

1. Download the Windows Defender definitions update from Windows Defender

Definition .

On the definitions page, scroll down to "Manually download and install the

definitions". Download the "Windows Defender Antivirus for Windows 10 and

Windows 8.1" 64-bit file.

Alternatively, use this direct link to download/run the fpam-fe.exe file.

2. Open a PowerShell session to the MySQL resource provider adapter VM's

maintenance endpoint.

3. Copy the definitions update file to the resource provider adapter VM using the

maintenance endpoint session.

4. On the maintenance PowerShell session, run the UpdateDBAdapterWindowsDefenderDefinitions command.

5. After you install the definitions, we recommend that you delete the definitions

update file by using the Remove-ItemOnUserDrive) command.

PowerShell script example for updating definitions.

You can edit and run the following script to update the Defender definitions. Replace

values in the script with values from your environment.

PowerShell

Update the VM Windows Defender definitions

# Set credentials for the local admin on the resource provider VM.

$vmLocalAdminPass = ConvertTo-SecureString '<local admin user password>' -

AsPlainText -Force

$vmLocalAdminUser = "<local admin user name>"

$vmLocalAdminCreds = New-Object System.Management.Automation.PSCredential `

($vmLocalAdminUser, $vmLocalAdminPass)

These instructions only apply to SQL RP V1 running on Azure Stack Hub Integrated

Systems.

The Azure Diagnostics extension is installed on the MySQL resource provider adapter

VM by default. The following steps show how to customize the extension for gathering

the MySQL resource provider operational event logs and IIS logs for troubleshooting

and auditing purposes.

1. Sign in to the Azure Stack Hub administrator portal.

2. Select Virtual machines from the pane on the left, search for the MySQL resource

provider adapter VM and select the VM.

3. In the Diagnostics settings of the VM, go to the Logs tab and choose Custom to

customize event logs being collected.

# Provide the public IP address for the adapter VM.

$databaseRPMachine = "<RP VM IP address>"

$localPathToDefenderUpdate = "C:\DefenderUpdates\mpam-fe.exe"

# Download Windows Defender update definitions file from

https://www.microsoft.com/en-us/wdsi/definitions.

Invoke-WebRequest -Uri 'https://go.microsoft.com/fwlink/?

LinkID=121721&arch=x64' `

-Outfile $localPathToDefenderUpdate

# Create a session to the maintenance endpoint.

$session = New-PSSession -ComputerName $databaseRPMachine `

-Credential $vmLocalAdminCreds -ConfigurationName DBAdapterMaintenance `

-SessionOption (New-PSSessionOption -Culture en-US -UICulture en-US)

# Copy the defender update file to the adapter VM.

Copy-Item -ToSession $session -Path $localPathToDefenderUpdate `

-Destination "User:\"

# Install the update definitions.

Invoke-Command -Session $session -ScriptBlock `

{Update-AzSDBAdapterWindowsDefenderDefinition -

DefinitionsUpdatePackageFile "User:\mpam-fe.exe"}

# Cleanup the definitions package file and session.

Invoke-Command -Session $session -ScriptBlock `

{Remove-AzSItemOnUserDrive -ItemPath "User:\mpam-fe.exe"}

$session | Remove-PSSession

Configure Azure Diagnostics extension for

MySQL resource provider

4. Add Microsoft-AzureStack-DatabaseAdapter/Operational!\* to collect MySQL

resource provider operational event logs.

5. To enable the collection of IIS logs, check IIS logs and Failed request logs.

6. Finally, select Save to save all the diagnostics settings.

Once the event logs and IIS logs collection are configured for MySQL resource provider,

the logs can be found in a system storage account named mysqladapterdiagaccount.

To learn more about the Azure Diagnostics extension, see What is Azure Diagnostics

extension.

These instructions only apply to Azure Stack Hub Integrated Systems.

When using the SQL and MySQL resource providers with Azure Stack Hub integrated

systems, the Azure Stack Hub operator is responsible for rotating the following resource

provider infrastructure secrets to ensure that they don't expire:

External SSL Certificate provided during deployment.

The resource provider VM local administrator account password provided during

deployment.

Resource provider diagnostic user (dbadapterdiag) password.

(version >= 1.1.47.0) Key Vault certificate generated during deployment.

Change all the secrets at the same time:

PowerShell

Secrets rotation

PowerShell examples for rotating secrets

Change the diagnostic user password:

PowerShell

Change the VM local admin account password:

PowerShell

Rotate the SSL certificate

PowerShell

Rotate the Key Vault certificate

PowerShell

.\SecretRotationMySQLProvider.ps1 `

-Privilegedendpoint $Privilegedendpoint `

-CloudAdminCredential $cloudCreds `

-AzCredential $adminCreds `

-DiagnosticsUserPassword $passwd `

-DependencyFilesLocalPath $certPath `

-DefaultSSLCertificatePassword $certPasswd `

-VMLocalCredential $localCreds `

-KeyVaultPfxPassword $keyvaultCertPasswd

.\SecretRotationMySQLProvider.ps1 `

-Privilegedendpoint $Privilegedendpoint `

-CloudAdminCredential $cloudCreds `

-AzCredential $adminCreds `

-DiagnosticsUserPassword $passwd

.\SecretRotationMySQLProvider.ps1 `

-Privilegedendpoint $Privilegedendpoint `

-CloudAdminCredential $cloudCreds `

-AzCredential $adminCreds `

-VMLocalCredential $localCreds

.\SecretRotationMySQLProvider.ps1 `

-Privilegedendpoint $Privilegedendpoint `

-CloudAdminCredential $cloudCreds `

-AzCredential $adminCreds `

-DependencyFilesLocalPath $certPath `

-DefaultSSLCertificatePassword $certPasswd

.\SecretRotationSQLProvider.ps1 `

-Privilegedendpoint $Privilegedendpoint `

-CloudAdminCredential $cloudCreds `

Parameter Description Comment

AzureEnvironment The Azure environment of the service admin

account used for deploying Azure Stack Hub.

Required only for Azure AD deployments.

Supported environment names are AzureCloud,

AzureUSGovernment, or if using a China Azure

Active Directory, AzureChinaCloud.

Optional

AzCredential Azure Stack Hub service admin account credential.

The script will fail if the account you use with

AzCredential requires multi-factor authentication

(MFA).

Mandatory

CloudAdminCredential Azure Stack Hub cloud admin domain account

credential.

Mandatory

PrivilegedEndpoint Privileged Endpoint to access GetAzureStackStampInformation.

Mandatory

DiagnosticsUserPassword Diagnostics user account password. Optional

VMLocalCredential The local admin account on the MySQLAdapter VM. Optional

DefaultSSLCertificatePassword Default SSL Certificate (\*.pfx) password. Optional

DependencyFilesLocalPath Dependency files local path. Optional

KeyVaultPfxPassword The password used for generating the Key Vault

certificate for database adapter.

Optional

Azure Stack Hub has multiple ways to collect, save, and send diagnostic logs to

Microsoft Support. Starting from version 1.1.93, MySQL Resource Provider supports the

standard way of collecting logs from your Azure Stack Hub environment. For more

information, see Diagnostic log collection.

-AzCredential $adminCreds `

-KeyVaultPfxPassword $keyvaultCertPasswd

SecretRotationMySQLProvider.ps1 parameters

Collect diagnostic logs

Known limitations of MySQL Server resource provider

Version 1

Limitation:

When the deployment, upgrade, or secret rotation script failed, some logs cannot be

collected by the standard log collection mechanism.

Workaround:

Besides using the standard log collection mechanism, go to the Logs folder in the

extracted folder where the script locates, to find more logs.

Add MySQL Server hosting servers

Next steps

Remove the MySQL resource provider in

Azure Stack Hub

Article • 07/29/2022

Removing the MySQL resource provider will delete:

The MySQL resource provider.

The associated plans and quotas managed by operator.

The metadata in Azure Stack Hub for the hosting server, database, and logins.

Removing the SQL resource provider will not delete:

The tenant databases on the hosting servers.

The packages used to install MySQL RP.

1. Verify that you've removed all the existing MySQL resource provider dependencies.

2. Get a copy of the MySQL resource provider installation package and then run the

self-extractor to extract the contents to a temporary directory. You can find the

download links for the resource provider installers in Deploy the MySQL resource

provider prerequisites.

3. Open a new elevated PowerShell console window and change to the directory

where you extracted the MySQL resource provider installation files.

） Important

Starting from Azure Stack Hub build 2108, the SQL and MySQL resource providers

are offered to subscriptions that have been granted access. If you want to start

using this feature, or if you need to upgrade from a previous version, open a

support case and our support engineers will guide you through the deployment or

upgrade process.

To remove the MySQL resource provider V1

７ Note

Uninstalling the MySQL resource provider will proceed even if dependent

resources are currently using the resource provider.

4. Run the DeployMySqlProvider.ps1 script using the following parameters:

Uninstall: Removes the resource provider and all associated resources.

PrivilegedEndpoint: The IP address or DNS name of the privileged endpoint.

AzureEnvironment: The Azure environment used for deploying Azure Stack

Hub. Required only for Azure AD deployments.

CloudAdminCredential: The credential for the cloud administrator, necessary

to access the privileged endpoint.

AzCredential: The credential for the Azure Stack Hub service admin account.

Use the same credentials that you used for deploying Azure Stack Hub. The

script will fail if the account you use with AzCredential requires multi-factor

authentication (MFA).

1. Sign in to the Azure Stack Hub administrator portal.

2. Select Marketplace Management on the left, then select Resource providers.

3. Select MySQL resource provider from the list of resource providers. You may want

to filter the list by Entering “SQL Server resource provider” or “MySQL Server

resource provider” in the search text box provided.

） Important

We strongly recommend using Clear-AzureRmContext -Scope CurrentUser

and Clear-AzureRmContext -Scope Process to clear the cache before running

the script.

To remove the SQL resource provider V2

4. Select Uninstall from the options provided across the top the page.

5. Enter the name of the resource provider, then select Uninstall. This action confirms

your desire to uninstall:

The MySQL Server resource provider.

All admin/user created SKU/Quota/HostingServer/Database/Login metadata.

6. (Optional) If you want to delete the installation package, after uninstalling the

MySQL resource provider, select Delete from the MySQL resource provider page.

Offer App Services as PaaS

Next steps

MySQL resource provider 2.0.13.x

release notes

Article • 05/22/2023

These release notes describe the improvements and known issues in MySQL resource

provider version 2.0.13.x.

After release version 2.0, MySQL resource provider becomes a standard Azure Stack Hub

value-add RP. If you want to get access to the MySQL resource provider in Azure Stack

Hub marketplace, open a support case to add your subscription to the allowlist.

The resource provider has a minimum corresponding Azure Stack Hub build. It is

required that you apply the minimum supported Azure Stack Hub update to your Azure

Stack Hub integrated system before deploying the latest version of the MySQL resource

provider.

Supported Azure Stack Hub

version

MySQL resource provider

version

MySQL Connector

version

Version 2108,2206 MySQL RP version 2.0.6.0 mysql-connector-net8.0.21

Version 2206, 2301 MySQL RP version 2.0.13.0 mysql-connector-net8.0.21

This version of the Azure Stack Hub MySQL resource provider includes the following

improvements and fixes:

UI fixes to prevent future breaks when portal is upgraded.

Other bug fixes.

Build reference

） Important

It is strongly recommended to upgrade to 2.0.13.0 when your Azure Stack Hub

version is 2206.

New features and fixes

Learn more about the MySQL resource provider.

Prepare to deploy the MySQL resource provider.

Upgrade the MySQL resource provider from a previous version.

） Important

You may need to refresh the web browser cache for the new UI fixes to take effect.

Known issues

Next steps

MySQL resource provider 2.0.6.x release

notes

Article • 10/21/2022

These release notes describe the improvements and known issues in MySQL resource

provider version 2.0.6.x.

Starting from this release, MySQL resource provider becomes a standard Azure Stack

Hub value-add RP. If you want to get access to the MySQL resource provider in Azure

Stack Hub marketplace, open a support case to add your subscription to the allowlist.

The resource provider has a minimum corresponding Azure Stack Hub build. The

minimum Azure Stack Hub release version required to install this version of the MySQL

resource provider is listed below.

It is required that you apply the minimum supported Azure Stack Hub update to your

Azure Stack Hub integrated system before deploying the latest version of the MySQL

resource provider.

Supported Azure Stack Hub version MySQL resource provider version

Version 2108, 2206 MySQL RP version 2.0.6.x

This version of the Azure Stack Hub MySQL resource provider includes the following

improvements and fixes:

Installation and future version upgrade will be from the Azure Stack Hub

marketplace.

Build reference

） Important

If there is an existing version of MySQL resource provider running in your system,

make sure to update it to version 1.1.93.x, before upgrading to this lattest version.

New features and fixes

A specific version of Add-on RP Windows Server will be required. The correct

version of Microsoft AzureStack Add-On RP Windows Server will be automatically

downloaded if you install the resource provider in connected environment. In

disconnected environment, make sure the right version of Microsoft AzureStack

Add-On RP Windows Server image is downloaded before deploying or upgrading

to this version of the MySQL resource provider.

Receive alerts when certifications are about to expire. Check this document for

details.

Other bug fixes.

After deployment or upgrade, Azure Stack Hub Operators need to manually register

their default provider subscription to the tenant namespace (Microsoft.MySQLAdapter)

before they can create Login or Databases.

Learn more about the MySQL resource provider.

Prepare to deploy the MySQL resource provider.

Upgrade the MySQL resource provider from a previous version.

Known issues

Next steps

MySQL resource provider 1.1.93.x release

notes

Article • 04/01/2022

These release notes describe the improvements and known issues in MySQL resource

provider version 1.1.93.x.

Download the MySQL resource provider binary and then run the self-extractor to extract

the contents to a temporary directory. The resource provider has a minimum

corresponding Azure Stack Hub build. The minimum Azure Stack Hub release version

required to install this version of the MySQL resource provider is listed below:

Supported Azure Stack Hub version MySQL resource provider version

Version 2108, 2102, 2008, 2005 MySQL RP version 1.1.93.5

This version of the Azure Stack Hub MySQL resource provider includes the following

improvements and fixes:

Update the base VM to a specialized Windows Server. This Windows Server

version is specialize for Azure Stack Hub Add-On RP Infrastructure and it is not

visible to the tenant marketplace. Make sure to download the Microsoft

AzureStack Add-On RP Windows Server image before deploying or upgrading to

this version of the MySQL resource provider.

Support removing orphaned database metadata and hosting server metadata.

When a hosting server cannot be connected anymore, the tenant will have an

option to remove the orphaned database metadata from the portal. When there is

Build reference

） Important

Apply the minimum supported Azure Stack Hub update to your Azure Stack Hub

integrated system before deploying the latest version of the MySQL resource

provider.

New features and fixes

no orphaned database metadata linked to the hosting server, the operator will be

able to remove the orphaned hosting server metadata from the admin portal.

Make KeyVaultPfxPassword an optional argument when performing secrets

rotation. Check this document for details.

Other bug fixes.

It's recommended that you apply MySQL resource provider 1.1.93.5 after Azure Stack

Hub is upgraded to the 2005 release.

Deployment of 1.1.93.0 version may fail if the wrong AzureRmContext is used. It is

recommended to upgrade to 1.1.93.5 version directly.

When redeploying the MySQL resource provider while the same version had deployed

already (for example, when MySQL resource provider 1.1.93.5 is already deployed, and

the same version is deployed again), the VM that is hosting the MySQL resource

provider will be stopped. To fix this issue, go to the admin portal, locate and restart the

VM named mysqlvm<version> in the resource group named system.

<region>.mysqladapter.

Learn more about the MySQL resource provider.

Prepare to deploy the MySQL resource provider.

Upgrade the MySQL resource provider from a previous version.

Known issues

Next steps

MySQL resource provider 1.1.47.0

release notes

Article • 07/29/2022

These release notes describe the improvements and known issues in MySQL resource

provider version 1.1.47.0.

Download the MySQL resource provider binary and then run the self-extractor to extract

the contents to a temporary directory. The resource provider has a minimum

corresponding Azure Stack Hub build. The minimum Azure Stack Hub release version

required to install this version of the MySQL resource provider is listed below:

Minimum Azure Stack Hub version MySQL resource provider version

Version 1910 (1.1910.0.58) MySQL RP version 1.1.47.0

This version of the Azure Stack Hub MySQL resource provider is a hotfix release to make

the resource provider compatible with some of the latest portal changes in the 1910

update. There are no new features.

It also supports the latest Azure Stack Hub API version profile 2019-03-01-hybrid and

Azure Stack Hub PowerShell module 1.8.0. So during deployment and update, no

specific history versions of modules need to be installed.

It's recommended that you apply the MySQL resource provider hotfix 1.1.47.0 after

Azure Stack Hub is upgraded to the 1910 release.

Build reference

） Important

Apply the minimum supported Azure Stack Hub update to your Azure Stack Hub

integrated system or deploy the latest Azure Stack Development Kit (ASDK) before

deploying the latest version of the MySQL resource provider.

New features and fixes

When rotating certificate for Azure Stack Hub integrated systems, KeyVaultPfxPassword

argument is mendatory, even if there's no intention to update the Key Vault certificate

password.

Learn more about the MySQL resource provider.

Prepare to deploy the MySQL resource provider.

Upgrade the MySQL resource provider from a previous version.

Known issues

Next steps

Use SQL databases on Azure Stack Hub

Article • 08/02/2022

Use the SQL resource provider to offer SQL databases on Azure Stack Hub. After you

install the resource provider and connect it to one or more SQL Server instances, you

and your users can create:

SQL databases for cloud-native apps.

SQL databases for web applications.

Limitations to consider before installing the SQL resource provider:

Users can only create and manage individual databases. Database server instances

aren't accessible to end users. This may limit compatibility with on-premises

database apps that need access to master, Temp DB, or to dynamically manage

databases.

Your Azure Stack Hub operator is responsible for deploying, updating, securing,

configuring, and maintaining the SQL database servers and hosts. The RP service

doesn't provide any host and database server instance management functionality.

Databases from different users in different subscriptions may be located on the

same database server instance. The RP does not provide a mechanism for isolating

databases on different hosts or database server instances.

The RP doesn't provide any reporting on tenant usage of databases.

You can only move a SQL hosting server to another subscription in global Azure.

Azure Stack Hub does not support moving a SQL hosting server to another

subscription.

The RP doesn't monitor the SQL server's health.

There is no access control on SQL Server's system databases. If your SQL hosting

server is a standalone SQL server (not SQL HA), SQL RP uses SQL logins to control

users' access to their own databases. However, the SQL logins don't control users'

access to system databases. For example, a user trying to restore a database from

） Important

Starting from Azure Stack Hub build 2108, the SQL and MySQL resource providers

are offered to subscriptions that have been granted access. If you want to start

using this feature, or if you need to upgrade from a previous version, open a

support case and our support engineers will guide you through the deployment or

upgrade process.

one of the backups will be able to see all the backup histories on the same hosting

server, because the backup history is stored in the msdb database.

For traditional SQL Server workload on premises, a SQL Server virtual machine on Azure

Stack Hub is recommended.

The resource provider consists of the following components:

The SQL resource provider adapter virtual machine (VM), which is a Windows

Server VM that runs the provider services.

The resource provider, which processes requests and accesses database resources.

Servers that host SQL Server, which provide capacity for databases called hosting

servers.

You must create at least one instance of SQL Server or provide access to external SQL

Server instances.

Deploy the SQL Server resource provider

SQL resource provider adapter architecture

７ Note

Hosting servers that are installed on Azure Stack Hub integrated systems must be

created from a tenant subscription. They can't be created from the default provider

subscription. They must be created from the user portal or by using PowerShell

with the appropriate sign-in. All hosting servers are billable VMs and must have

licenses. The service admin can be the owner of the tenant subscription.

Next steps

Deploy the SQL Server resource

provider on Azure Stack Hub

Article • 05/22/2023

Use the Azure Stack Hub SQL Server resource provider to expose SQL databases as an

Azure Stack Hub service.

The SQL resource provider runs as a service on a special Add-on RP Windows Server.

If you've already installed a resource provider, you've likely completed the following

prerequisites, and can skip this section. Otherwise, complete these steps before

continuing:

1. Register your Azure Stack Hub instance with Azure, if you haven't done so. This

step is required as you'll be connecting to and downloading items to marketplace

） Important

Starting from Azure Stack Hub build 2108, the SQL and MySQL resource providers

are offered to subscriptions that have been granted access. If you want to start

using this feature, or if you need to upgrade from a previous version, open a

support case and our support engineers will guide you through the deployment or

upgrade process.

） Important

Only the resource provider should create items on servers that host SQL or MySQL.

Items created on a host server that aren't created by the resource provider are

unsupported, and may result in a mismatched state.

） Important

The V2.x SQL/MySQL resource provider uses the Deployment Resource Provider

(DRP) installation mechanism, which isn't supported on the ASDK. Therefore, the

V2.x SQL/MySQL resource provider isn't supported on the ASDK.

Prerequisites

from Azure.

2. If you're not familiar with the Marketplace Management feature of the Azure Stack

Hub administrator portal, review Download marketplace items from Azure and

publish to Azure Stack Hub. The article walks you through the process of

downloading items from Azure to the Azure Stack Hub marketplace. It covers both

connected and disconnected scenarios. If your Azure Stack Hub instance is

disconnected or partially connected, there are additional prerequisites to complete

in preparation for installation.

3. Update your Azure Active Directory (Azure AD) home directory. Starting with build

1910, a new application must be registered in your home directory tenant. This app

will enable Azure Stack Hub to successfully create and register newer resource

providers (like Event Hubs and others) with your Azure AD tenant. This is an onetime action that needs to be done after upgrading to build 1910 or newer. If this

step isn't completed, marketplace resource provider installations will fail.

After you've successfully updated your Azure Stack Hub instance to 1910 or

greater, follow the instructions for cloning/downloading the Azure Stack Hub

Tools repository.

Then, follow the instructions for Updating the Azure Stack Hub Azure AD

Home Directory (after installing updates or new Resource Providers) .

You'll need a computer and account that can access:

the Azure Stack Hub administrator portal.

the privileged endpoint (needed only when you're deploying SQL Server

resource provider V1 or upgrading from SQL Server resource provider V1 to

SQL Server resource provider V2).

the Azure Resource Manager admin endpoint, https://adminmanagement.region.

<fqdn> , where <fqdn> is your fully qualified domain name.

the Internet, if your Azure Stack Hub was deployed to use Azure Active

Directory (Azure AD) as your identity provider.

Download the supported version of SQL resource provider binary according to the

version mapping table below. For V2 SQL resource provider, download the

marketplace item to Azure Stack Hub.

Supported Azure Stack

Hub version

SQL RP version Windows Server that RP service is

running on

SQL Server resource provider prerequisites

Supported Azure Stack

Hub version

SQL RP version Windows Server that RP service is

running on

2206, 2301 SQL RP version

2.0.13.x

Microsoft AzureStack Add-on RP

Windows Server 1.2009.0

2108, 2206 SQL RP version

2.0.6.x

Microsoft AzureStack Add-on RP

Windows Server 1.2009.0

2108, 2102, 2008, 2005 SQL RP version

1.1.93.5

Microsoft AzureStack Add-on RP

Windows Server

Make sure that the required Windows Server VM is downloaded to Azure Stack

Hub Marketplace. Manually download the image according to the version

mapping table above if needed.

Ensure datacenter integration prerequisites are met:

Prerequisite Reference

Conditional DNS forwarding is set

correctly.

Azure Stack Hub datacenter integration - DNS

Inbound ports for resource

providers are open.

Azure Stack Hub datacenter integration - Ports and

protocols inbound

PKI certificate subject and SAN are

set correctly.

Azure Stack Hub deployment mandatory PKI

prerequisites

Azure Stack Hub deployment PaaS certificate

prerequisites

Prepare the certificate. (For integrated systems installations only.)

You must provide the SQL PaaS PKI certificate described in the optional PaaS

certificates section of Azure Stack Hub deployment PKI requirements. The

Subject Alternative Name (SAN) must adhere to the following naming pattern:

CN=\*.dbadapter.<region>.<fqdn>, with password protected.

When deploying SQL Server resource provider V1, place the .pfx file in the

location specified by the DependencyFilesLocalPath parameter. Don't provide a

certificate for ASDK systems.

When deploying SQL Server resource provider V2, prepare the certificate for the

following installation steps.

Disconnected scenario

When deploying SQL Server resource provider V2 in a disconnected scenario, follow the

download marketplace items to Azure Stack Hub instruction to download the SQL

Server resource provider item and Add-on RP Windows Server item to your Azure Stack

Hub environment.

When deploying SQL Server resource provider V1 in a disconnected scenario, complete

the following steps to download the required PowerShell modules and register the

repository manually.

1. Sign in to a computer with internet connectivity and use the following scripts to

download the PowerShell modules.

PowerShell

2. Depending on the version of resource provider that you are deploying, run one of

the scripts.

PowerShell

PowerShell

3. Then you copy the downloaded packages to a USB device.

4. Sign in to the disconnected workstation and copy the packages from the USB

device to a location on the workstation.

Import-Module -Name PowerShellGet -ErrorAction Stop

Import-Module -Name PackageManagement -ErrorAction Stop

# path to save the packages, c:\temp\azs1.6.0 as an example here

$Path = "c:\temp\azs1.6.0"

# for resource provider version >= 1.1.93.0

Save-Package -ProviderName NuGet -Source

https://www.powershellgallery.com/api/v2 -Name AzureRM -Path $Path -

Force -RequiredVersion 2.5.0

Save-Package -ProviderName NuGet -Source

https://www.powershellgallery.com/api/v2 -Name AzureStack -Path $Path -

Force -RequiredVersion 1.8.2

# for resource provider version <= 1.1.47.0

Save-Package -ProviderName NuGet -Source

https://www.powershellgallery.com/api/v2 -Name AzureRM -Path $Path -

Force -RequiredVersion 2.3.0

Save-Package -ProviderName NuGet -Source

https://www.powershellgallery.com/api/v2 -Name AzureStack -Path $Path -

Force -RequiredVersion 1.6.0

5. Register this location as a local repository.

PowerShell

If you are upgrading from a V1 version, refer to the doc Update the SQL Server resource

provider.

1. If you haven't already, sign in to the Azure Stack Hub administrator portal, select

Marketplace Management on the left, select Resource providers.

2. Once SQL resource provider and other required software have been downloaded,

Marketplace Management shows the "SQL Server resource provider" packages

with a status of "Not Installed". There may be other packages that show a status of

"Downloaded".

3. Select the row you wish to install. The SQL Server resource provider install package

page shows a blue banner across the top. Select the banner to start the

# requires -Version 5

# requires -RunAsAdministrator

# requires -Module PowerShellGet

# requires -Module PackageManagement

$SourceLocation = "C:\temp\azs1.6.0"

$RepoName = "azs1.6.0"

Register-PSRepository -Name $RepoName -SourceLocation $SourceLocation -

InstallationPolicy Trusted

New-Item -Path $env:ProgramFiles -name "SqlMySqlPsh" -ItemType

"Directory"

Deploy the SQL resource provider V2

Start installation

installation.

1. Next you're transferred to the install page. Select Install Prerequisites to begin the

installation process.

2. Wait until the installation of prerequisites succeeds. You should see a green

checkmark next to Install prerequisites before proceeding to the next step.

Install prerequisites

1. Under the 2. Prepare secrets step, select Add certificate, and the Add a certificate

panel will appear.

2. Select the browse button on Add a certificate, just to the right of the certificate

filename field. Select the .pfx certificate file you procured when completing the

prerequisites.

3. Enter the password you provided to create a secure string for SQL Server resource

provider SSL Certificate. Then select Add.

Prepare secrets

1. When the installation of the certificate succeeds, you should see a green

checkmark next to Prepare secrets before proceeding to the next step. Now select

the Install button next to 3 Install resource provider.

2. Next you'll see the following page, which indicates that SQL resource provider is

being installed.

Install resource provider

3. Wait for the installation complete notification. This process usually takes one or

more hours, depending on your Azure Stack Hub type.

4. Verify that the installation of SQL Server resource provider has succeeded, by

returning to the Marketplace Management, Resource Providers page. The status

of SQL Server resource provider should show "Installed".

Deploy the SQL resource provider V1

After you've completed all of the prerequisites, run the self-extractor to extract the

downloaded installation package to a temporary directory. run the

DeploySqlProvider.ps1 script from a computer that can access both the Azure Stack Hub

Azure Resource Manager admin endpoint and the privileged endpoint, to deploy the

SQL resource provider. The DeploySqlProvider.ps1 script is extracted as part of the SQL

resource provider binary that you downloaded for your version of Azure Stack Hub.

To deploy the SQL resource provider, open a new elevated PowerShell window (not

PowerShell ISE) and change to the directory where you extracted the SQL resource

provider binary files.

Run the DeploySqlProvider.ps1 script, which completes the following tasks:

Uploads the certificates and other artifacts to a storage account on Azure Stack

Hub.

Publishes gallery packages so you can deploy SQL databases using the gallery.

Publishes a gallery package for deploying hosting servers.

Deploys a VM using the Windows Server 2016 core image or Microsoft AzureStack

Add-on RP Windows Server image you downloaded, and then installs the SQL

resource provider.

Registers a local DNS record that maps to your resource provider VM.

Registers your resource provider with the local Azure Resource Manager for the

operator account.

） Important

Before deploying the resource provider, review the release notes to learn about

new functionality, fixes, and any known issues that could affect your deployment.

） Important

We strongly recommend using Clear-AzureRmContext -Scope CurrentUser and

Clear-AzureRmContext -Scope Process to clear the cache before running the

deploy or update script.

７ Note

When the SQL resource provider deployment starts, the system.local.sqladapter

resource group is created. It may take up to 75 minutes to finish the required

deployments to this resource group. You should not place any other resources in

the system.local.sqladapter resource group.

You can specify the following parameters from the command line. If you don't, or if any

parameter validation fails, you're prompted to provide the required parameters.

Parameter name Description Comment

or default

value

CloudAdminCredential The credential for the cloud admin, necessary for

accessing the privileged endpoint.

Required

AzCredential The credentials for the Azure Stack Hub service

admin account. Use the same credentials that you

used for deploying Azure Stack Hub. The script

will fail if the account you use with AzCredential

requires multi-factor authentication (MFA).

Required

VMLocalCredential The credentials for the local admin account of the

SQL resource provider VM.

Required

PrivilegedEndpoint The IP address or DNS name of the privileged

endpoint.

Required

AzureEnvironment The Azure environment of the service admin

account used for deploying Azure Stack Hub.

Required only for Azure AD deployments.

Supported environment names are AzureCloud,

AzureUSGovernment, or if using a China Azure

AD, AzureChinaCloud.

AzureCloud

DependencyFilesLocalPath For integrated systems only, your certificate .pfx

file must be placed in this directory. You can

optionally copy one Windows Update MSU

package here.

Optional

(mandatory

for

integrated

systems)

DefaultSSLCertificatePassword The password for the .pfx certificate. Required

MaxRetryCount The number of times you want to retry each

operation if there's a failure.

2

RetryDuration The timeout interval between retries, in seconds. 120

Uninstall Removes the resource provider and all associated

resources (see the following notes).

No

DebugMode Prevents automatic cleanup on failure. No

DeploySqlProvider.ps1 parameters

If you're deploying the SQL resource provider version 1.1.47.0 or later, the deployment

script will automatically download and install the necessary PowerShell modules for you

to path C:\Program Files\SqlMySqlPsh.

PowerShell

To eliminate any manual configuration when deploying the resource provider, you can

customize the following script. Change the default account information and passwords

as needed for your Azure Stack Hub deployment.

PowerShell

Deploy the SQL resource provider using a

custom script

# Install the AzureRM.Bootstrapper module, set the profile, and install the

AzureStack module

# Note that this might not be the most currently available version of Azure

Stack Hub PowerShell

Install-Module -Name AzureRm.BootStrapper -RequiredVersion 0.5.0 -Force

Use-AzureRmProfile -Profile 2018-03-01-hybrid -Force

Install-Module -Name AzureStack -RequiredVersion 1.6.0

７ Note

In disconnected scenario, you need to download the required PowerShell modules

and register the repository manually as a prerequisite.

# Use the NetBIOS name for the Azure Stack Hub domain. On the Azure Stack

Hub SDK, the default is AzureStack but could have been changed at install

time.

$domain = "AzureStack"

# For integrated systems, use the IP address of one of the ERCS VMs

$privilegedEndpoint = "AzS-ERCS01"

# Provide the Azure environment used for deploying Azure Stack Hub. Required

only for Azure AD deployments. Supported values for the <environment name>

parameter are AzureCloud, AzureChinaCloud, or AzureUSGovernment depending

which Azure subscription you're using.

$AzureEnvironment = "<EnvironmentName>"

# Point to the directory where the resource provider installation files were

extracted.

$tempDir = 'C:\TEMP\SQLRP'

# The service admin account can be Azure Active Directory or Active

When the resource provider installation script finishes, refresh your browser to make

sure you can see the latest updates and close the current PowerShell session.

1. Sign in to the administrator portal as the service admin.

2. Select Resource Groups.

3. Select the system.<location>.sqladapter resource group.

4. On the summary page for Resource group Overview, there should be no failed

deployments.

Directory Federation Services.

$serviceAdmin = "admin@mydomain.onmicrosoft.com"

$AdminPass = ConvertTo-SecureString 'P@ssw0rd1' -AsPlainText -Force

$AdminCreds = New-Object System.Management.Automation.PSCredential

($serviceAdmin, $AdminPass)

# Set credentials for the new resource provider VM local admin account.

$vmLocalAdminPass = ConvertTo-SecureString 'P@ssw0rd1' -AsPlainText -Force

$vmLocalAdminCreds = New-Object System.Management.Automation.PSCredential

("sqlrpadmin", $vmLocalAdminPass)

# Add the cloudadmin credential that's required for privileged endpoint

access.

$CloudAdminPass = ConvertTo-SecureString 'P@ssw0rd1' -AsPlainText -Force

$CloudAdminCreds = New-Object System.Management.Automation.PSCredential

("$domain\cloudadmin", $CloudAdminPass)

# Change the following as appropriate.

$PfxPass = ConvertTo-SecureString 'P@ssw0rd1' -AsPlainText -Force

# For version 1.1.47.0 or later, the PowerShell modules used by the RP

deployment are placed in C:\Program Files\SqlMySqlPsh

# The deployment script adds this path to the system $env:PSModulePath to

ensure correct modules are used.

$rpModulePath = Join-Path -Path $env:ProgramFiles -ChildPath 'SqlMySqlPsh'

$env:PSModulePath = $env:PSModulePath + ";" + $rpModulePath

# Change to the directory folder where you extracted the installation files.

Don't provide a certificate on ASDK!

. $tempDir\DeploySQLProvider.ps1 `

-AzCredential $AdminCreds `

-VMLocalCredential $vmLocalAdminCreds `

-CloudAdminCredential $cloudAdminCreds `

-PrivilegedEndpoint $privilegedEndpoint `

-AzureEnvironment $AzureEnvironment `

-DefaultSSLCertificatePassword $PfxPass `

-DependencyFilesLocalPath $tempDir\cert

Verify the V1 deployment using the Azure Stack Hub

portal

5. Finally, select Virtual machines in the administrator portal to verify that the SQL

resource provider VM was successfully created and is running.

If your Azure Stack Hub is using Azure AD as an identity provider, make sure the VM

that has installed SQL Server resource provider has outbound internet connectivity.

Add hosting servers

Important configuration for Azure AD

Next steps

Add hosting servers for the SQL

resource provider

Article • 02/20/2023

You can create SQL Server database hosting servers on a virtual machine (VM) in Azure

Stack Hub, or on a VM outside your Azure Stack Hub environment, as long as the SQL

resource provider can connect to the instance.

Before you add a SQL hosting server, review the following mandatory and general

requirements.

Enable SQL authentication on the SQL Server instance. Because the SQL resource

provider VM isn't domain-joined, it can only connect to a hosting server using SQL

authentication.

Configure the IP addresses for the SQL instances as Public when installed on Azure

Stack Hub. The resource provider and users, such as web apps, communicate over

the user network, so connectivity to the SQL instance on this network is required.

） Important

Starting from Azure Stack Hub build 2108, the SQL and MySQL resource providers

are offered to subscriptions that have been granted access. If you want to start

using this feature, or if you need to upgrade from a previous version, open a

support case and our support engineers will guide you through the deployment or

upgrade process.

７ Note

The SQL resource provider should be created in the default provider subscription

while SQL hosting servers should be created in a billable, user subscription. The

resource provider server shouldn't be used to host user databases.

Overview

Mandatory requirements

General requirements

Dedicate the SQL instance for use by the resource provider and user workloads.

You can't use a SQL instance that's being used by any other consumer. This

restriction also applies to App Services.

If you have multiple SQL Server instances on a single VM that you want to

configure as hosting servers, each of the SQL Server instance should have unique

IP or FQDN. It is not supported to configure multiple SQL Server instances that

share the same IP or FQDN as hosting servers.

Configure an account with the appropriate privilege levels for the resource

provider (described below).

You're responsible for managing the SQL instances and their hosts. For example,

the resource provider doesn't apply updates, handle backups, or handle credential

rotation.

SQL IaaS VM images are available through the Marketplace Management feature. These

images are the same as the SQL VMs that are available in Azure.

Make sure you always download the latest version of the SQL IaaS Extension before you

deploy a SQL VM using a Marketplace item. The IaaS extension and corresponding

portal enhancements provide additional features such as automatic patching and

backup. For more information about this extension, see Automate management tasks on

Azure VMs with the SQL Server Agent Extension.

There are other options for deploying SQL VMs, including templates in the Azure Stack

Hub Quickstart Gallery .

SQL Server VM images

７ Note

The SQL IaaS Extension is required for all SQL on Windows images in the

marketplace; the VM will fail to deploy if you didn't download the extension. It's not

used with Linux-based SQL VM images.

７ Note

Any hosting servers installed on a multi-node Azure Stack Hub must be created

from a user subscription and not the Default Provider Subscription. They must be

created from the user portal or from a PowerShell session with an appropriate

login. All hosting servers are billable VMs and must have appropriate SQL licenses.

The service admin can be the owner of that subscription.

You can create an admin user with lower privileges than a SQL sysadmin. The user only

needs permissions for the following operations:

Database: Create, Alter, With Containment (for Always On only), Drop, Backup

Availability Group: Alter, Join, Add/Remove Database

Login: Create, Select, Alter, Drop, Revoke

Select Operations: [master].[sys].[availability\_group\_listeners] (AlwaysOn),

sys.availability\_replicas (AlwaysOn), sys.databases, [master].[sys].

[dm\_os\_sys\_memory], SERVERPROPERTY, [master].[sys].[availability\_groups]

(AlwaysOn), sys.master\_files

The following information provides additional security guidance:

All Azure Stack Hub storage is encrypted using BitLocker, so any SQL instance on

Azure Stack Hub will use encrypted blob storage.

The SQL Resource Provider fully supports TLS 1.2. Ensure that any SQL Server that's

managed through the SQL RP is configured for TLS 1.2 only and the RP will default

to that. All supported versions of SQL Server support TLS 1.2. For more

information, see TLS 1.2 support for Microsoft SQL Server .

Use SQL Server Configuration Manager to set the ForceEncryption option to

ensure all communications to the SQL server are always encrypted. For more

information, see To configure the server to force encrypted connections.

Ensure any client app is also communicating over an encrypted connection.

The RP is configured to trust the certificates used by the SQL Server instances.

You can use standalone (non-HA) SQL servers using any edition of SQL Server 2014, SQL

Server 2016 or SQL Server 2019. Make sure you have the credentials for an account with

sysadmin privileges.

To add a standalone hosting server that's already set up, follow these steps:

1. Sign in to the Azure Stack Hub administrator portal as a service admin.

2. Select All services > ADMINISTRATIVE RESOURCES > SQL Hosting Servers.

Required Privileges

Additional Security Information

Provide capacity by connecting to a standalone

hosting SQL server

Under SQL Hosting Servers, you can connect the SQL resource provider to

instances of SQL Server that will serve as the resource provider's backend.

3. Click Add and then provide the connection details for your SQL Server instance on

the Add a SQL Hosting Server blade.

） Important

Do not choose Resource group system.<region>.sqladapter , which was

created by the SQL resource provider installer during deployment. You must

provide a different resource group for the standalone hosting server.

Optionally, provide an instance name, and specify a port number if the instance

isn't assigned to the default port of 1433.

4. As you add servers, you must assign them to an existing SKU or create a new SKU.

Under Add a Hosting Server, select SKUs.

To use an existing SKU, choose an available SKU and then select Create.

To create a SKU, select + Create new SKU. In Create SKU, enter the required

information, and then select OK.

７ Note

As long as the SQL instance can be accessed by the user and admin Azure

Resource Manager, it can be placed under control of the resource provider.

The SQL instance must be allocated exclusively to the resource provider.

Configuring SQL Always On instances requires additional steps and requires three VMs

(or physical machines.) This article assumes that you already have a solid understanding

of Always On availability groups. For more information, see the following articles:

Introducing SQL Server Always On availability groups on Azure virtual machines

Always On Availability Groups (SQL Server)

Provide high availability using SQL Always On

Availability Groups

You must enable Automatic Seeding on each availability group for each instance of SQL

Server.

To enable automatic seeding on all instances, edit and then run the following SQL

command on the primary replica for each secondary instance:

SQL

The availability group must be enclosed in square brackets.

On the secondary nodes, run the following SQL command:

SQL

Before adding a contained database to an availability group, ensure that the contained

database authentication server option is set to 1 on every server instance that hosts an

availability replica for the availability group. For more information, see contained

database authentication Server Configuration Option.

Use these commands to set the contained database authentication server option for

each instance:

SQL

７ Note

The SQL adapter resource provider only supports SQL 2016 SP1 Enterprise or later

instances for Always On Availability Groups. This adapter configuration requires

new SQL features such as automatic seeding.

Automatic seeding

ALTER AVAILABILITY GROUP [<availability\_group\_name>]

MODIFY REPLICA ON '<secondary\_node>'

WITH (SEEDING\_MODE = AUTOMATIC)

GO

ALTER AVAILABILITY GROUP [<availability\_group\_name>] GRANT CREATE ANY

DATABASE

GO

Configure contained database authentication

1. Sign in to the Azure Stack Hub administrator portal as a service admin.

2. Select Browse > ADMINISTRATIVE RESOURCES > SQL Hosting Servers > +Add.

Under SQL Hosting Servers, you can connect the SQL Server Resource Provider to

actual instances of SQL Server that serve as the resource provider's backend.

3. Fill out the form with the connection details for your SQL Server instance. Make

sure that you use the FQDN address of the Always On Listener (and optional port

number and instance name). Provide the information for the account you

configured with sysadmin privileges.

4. Check the Always On Availability Group box to enable support for SQL Always On

Availability Group instances.

5. Add the SQL Always On instance to a SKU.

EXEC sp\_configure 'contained database authentication', 1

GO

RECONFIGURE

GO

To add SQL Always On hosting servers

） Important

Do not choose Resource group system.<region>.sqladapter , which was

created by the SQL resource provider installer during deployment. You must

provide a different resource group for the standalone hosting server.

） Important

You can't mix standalone servers with Always On instances in the same SKU.

Attempting to mix types after adding the first hosting server results in an

error.

SKU notes

Use a SKU name that describes the capabilities of the servers in the SKU, such as

capacity and performance. The name serves as an aid to help users deploy their

databases to the appropriate SKU. For example, you can use SKU names to differentiate

service offerings by the following characteristics:

high capacity

high performance

high availability

As a best practice, all the hosting servers in a SKU should have the same resource and

performance characteristics.

SKUs cannot be hidden from certain tenants, nor can it be dedicated to certain tenants.

SKUs can take up to an hour to be visible in the portal. Users can't create a database

until the SKU is fully created.

To edit a SKU, go to All services > SQL Adapter > SKUs. Select the SKU to modify, make

any necessary changes, and click Save to save changes.

To delete a SKU that's no longer needed, go to All services > SQL Adapter > SKUs.

Right-click the SKU name and select Delete to delete it.

Create plans and offers to make SQL databases available for users. Add the

Microsoft.SqlAdapter service to the plan and create a new quota.

） Important

It can take up to an hour for new SKUs to be available in the user portal.

Make SQL databases available to users

） Important

It can take up to two hours for new quotas to be available in the user portal or

before a changed quota is enforced.

７ Note

You can't delete a quota if there are any current plans that use it. You must first

delete the plan that references the quota.

Add databases

Next steps

Create SQL databases

Article • 07/29/2022

You can create and manage self-service databases in the user portal. An Azure Stack

Hub user needs a subscription with an offer that includes the SQL database service.

1. Sign in to the Azure Stack Hub user portal.

2. Select + New >Data + Storage > SQL Server Database > Add.

3. Under Create Database, enter the required information, such as Database Name

and Max Size in MB.

Configure the other settings as required for your environment.

4. Under Create Database, select SKU. Under Select a SKU, select the SKU for your

database.

） Important

Starting from Azure Stack Hub build 2108, the SQL and MySQL resource providers

are offered to subscriptions that have been granted access. If you want to start

using this feature, or if you need to upgrade from a previous version, open a

support case and our support engineers will guide you through the deployment or

upgrade process.

７ Note

The database size must be at least 64 MB, which can be increased after you

deploy the database.

5. Select Login.

6. Under Select a Login, choose an existing login, or select + Create a new login.

7. Under New Login, enter a name for Database login and a Password.

７ Note

As hosting servers are added to Azure Stack Hub, they're assigned a SKU.

Databases are created in the pool of hosting servers in a SKU.

７ Note

These settings are the SQL authentication credential that's created for your

access to this database only. The login user name must be globally unique.

8. Select OK to finish deploying the database.

Under Essentials, which is shown after the database is deployed, take note of the

Connection string. You can use this string in any app that needs to access the SQL

Server database.

You can reuse login settings for other databases that use the same SKU.

By design, Always On databases are handled differently than in a standalone server

environment. For more information, see Introducing SQL Server Always On availability

groups on Azure virtual machines.

The following screen capture shows how you can use SQL Server Management Studio to

look at database status in SQL Always On.

SQL Always On databases

Verify SQL Always On databases

Always On databases should show as Synchronized and available on all the SQL

instances and appear in Availability Groups. In the previous screenshot, the database

example is newdb1 and its status is newdb1 (Synchronized).

Delete an Always On database

When you delete a SQL Always On database from the resource provider, SQL deletes the

database from the Primary replica and from the availability group.

SQL then puts the database into the Restoring state on the other replicas and doesn't

drop the database unless triggered. If the database isn't dropped, the secondary replicas

go into a Not Synchronizing state.

Learn how to offer highly available SQL databases

Next steps

Create highly available SQL databases

with Azure Stack Hub

Article • 07/29/2022

As an Azure Stack Hub Operator, you can configure server VMs to host SQL Server

databases. After a SQL hosting server is created and managed by Azure Stack Hub, users

who have subscribed to SQL services can easily create SQL databases.

This article shows how to use an Azure Stack Hub quickstart template to create a SQL

Server AlwaysOn availability group, add it as an Azure Stack Hub SQL Hosting Server,

and then create a highly available SQL database.

What you'll learn:

A two VM SQL Server AlwaysOn availability group will be created and configured using

available Azure Stack Marketplace items.

Before starting, ensure that the SQL Server resource provider has been successfully

installed and the following items are available in Azure Stack Marketplace:

Windows Server 2016 Datacenter.

） Important

Starting from Azure Stack Hub build 2108, the SQL and MySQL resource providers

are offered to subscriptions that have been granted access. If you want to start

using this feature, or if you need to upgrade from a previous version, open a

support case and our support engineers will guide you through the deployment or

upgrade process.

＂ Create a SQL Server AlwaysOn availability group from a template.

Configure the SQL Server AlwaysOn availability group as an Azure Stack Hub SQL

Hosting Server.

＂

＂ Create a highly available SQL database.

） Important

All of the following are required for the Azure Stack Hub quickstart template to be

used.

SQL Server 2016 SP1 or SP2 (Enterprise or Developer) on Windows Server 2016

server image.

SQL Server IaaS Extension version 1.3.20180 or higher. The SQL IaaS Extension

installs necessary components that are required by the Marketplace SQL Server

items for all Windows versions. It enables SQL-specific settings to be configured on

SQL virtual machines (VMs). If the extension isn't installed in the local marketplace,

provisioning of SQL will fail.

To learn more about adding items to Azure Stack Marketplace, see the Azure Stack Hub

Marketplace overview.

Use the steps in this section to deploy the SQL Server AlwaysOn availability group by

using the sql-2016-alwayson Azure Stack Hub quickstart template . This template

deploys two SQL Server Enterprise or Developer instances in an Always On Availability

Group. It creates the following resources:

A network security group.

A virtual network.

Four storage accounts (one for Active Directory (AD), one for SQL, one for file

share witness, and one for VM diagnostics).

Four public IP addresses (one for AD, two for each SQL VM, and one for public

load balancer bound to SQL AlwaysOn listener).

One external load balancer for SQL VMs with Public IP bound to the SQL AlwaysOn

listener.

One VM (Windows Server 2016) configured as Domain Controller for a new forest

with a single domain.

Two VMs (Windows Server 2016) configured with SQL Server 2016 SP1 or SP2

Enterprise or Developer Edition and clustered. These must be marketplace images.

One VM (Windows Server 2016) configured as the file share witness for the cluster.

７ Note

Standard version is not supported. When setting up the SQL Server AlwaysOn

availability group with SQL Server Standard version, only one database can be

created for one availability group. This limitation makes Standard version

unsuitable for our scenario. For more details, check the document here.

Create a SQL Server AlwaysOn availability

group

One availability set containing the SQL and file share witness VMs.

1. Sign in to the user portal:

For an integrated system deployment, the portal address will vary based on

your solution's region and external domain name. It will be in the format of

https://portal.<region>.<FQDN> .

For the Azure Stack Development Kit (ASDK), the portal address is

https://portal.local.azurestack.external .

2. Select + Create a resource > Custom, and then Template deployment.

3. On the Custom deployment blade, select Edit template > Quickstart template

and then use the drop-down list of available custom templates to select the sql2016-alwayson template. Select OK, then Save.

4. On the Custom deployment blade, select Edit parameters and review the default

values. Modify the values as necessary to provide all required parameter

information and then select OK.

At a minimum:

Provide complex passwords for the ADMINPASSWORD,

SQLSERVERSERVICEACCOUNTPASSWORD, and SQLAUTHPASSWORD

parameters.

Enter the DNS Suffix for reverse lookup in all lowercase letters for the

DNSSUFFIX parameter (azurestack.external for ASDK installations before

version 2107).



5. On the Custom deployment blade, choose the subscription to use and create a

new resource group or select an existing resource group for the custom

deployment.

Next, select the resource group location (local for ASDK installations before version

2107) and then click Create. The custom deployment settings will be validated and

then the deployment will start.



6. In the user portal, select Resource groups and then the name of the resource

group you created for the custom deployment (resource-group for this example).

View the status of the deployment to ensure all deployments have completed

successfully.

Next, review the resource group items and select the SQLPIPsql<resource group

name> public IP address item. Record the public IP address and full FQDN of the

load balancer public IP. You'll need to provide this to an Azure Stack Hub operator

so they can create a SQL hosting server leveraging this SQL AlwaysOn availability

group.



７ Note

The template deployment will take several hours to complete.

Enable automatic seeding

After the template has successfully deployed and configured the SQL AlwaysON

availability group, you must enable automatic seeding on each instance of SQL Server in

the availability group.

When you create an availability group with automatic seeding, SQL Server automatically

creates the secondary replicas for every database in the group without any other manual

intervention necessary. This measure ensures high availability of AlwaysOn databases.

Use these SQL commands to configure automatic seeding for the AlwaysOn availability

group. Replace <PrimaryInstanceName> with the primary instance SQL Server name,

<SecondaryInstanceName> with the secondary instance SQL Server name and

<availability\_group\_name> with the AlwaysOn availability group name as necessary.

On the primary SQL instance:

SQL

On secondary SQL instances:

SQL

ALTER AVAILABILITY GROUP [<availability\_group\_name>]

MODIFY REPLICA ON '<PrimaryInstanceName>'

WITH (SEEDING\_MODE = AUTOMATIC)

GO

ALTER AVAILABILITY GROUP [<availability\_group\_name>]

MODIFY REPLICA ON '<SecondaryInstanceName>'

WITH (SEEDING\_MODE = AUTOMATIC)

GO

ALTER AVAILABILITY GROUP [<availability\_group\_name>] GRANT CREATE ANY

DATABASE

Before adding a contained database to an availability group, ensure that the contained

database authentication server option is set to 1 on every server instance that hosts an

availability replica for the availability group. For more information, see contained

database authentication.

Use these commands to set the contained database authentication server option for

each SQL Server instance in the availability group:

SQL

GO

Configure contained database authentication

EXEC sp\_configure 'contained database authentication', 1

GO

RECONFIGURE

GO

After the SQL Server AlwayOn availability group has been created and properly

configured, an Azure Stack Hub operator has to configure it as an Azure Stack Hub SQL

Hosting Server.

Be sure to use the public IP or full FQDN for the public IP of the SQL load balancer

recorded previously when the SQL AlwaysOn availability group's resource group was

created (SQLPIPsql<resource group name>). In addition, you need to know the SQL

Server authentication credentials used to access the SQL instances in the AlwaysOn

availability group.

With the SQL AlwaysOn availability group's load balancer listener public IP and SQL

authentication login information, an Azure Stack Hub operator can create a SQL Hosting

Server using the SQL AlwaysOn availability group.

Also ensure that you have created plans and offers to make SQL AlwaysOn database

creation available for users. The operator will need to add the Microsoft.SqlAdapter

service to a plan and create a new quota specifically for highly available databases. For

more information about creating plans, see Service, plan, offer, subscription overview.

After the SQL AlwaysOn availability group has been created, configured, and added as

an Azure Stack Hub SQL Hosting Server by an Azure Stack Hub operator, a tenant user

with a subscription including SQL Server database capabilities can create SQL databases

supporting AlwaysOn functionality. They can create those databases by following the

steps in this section.

Configure an Azure Stack Hub SQL Hosting

Server

７ Note

This step must be run from the Azure Stack Hub administrator portal by an Azure

Stack Hub operator.

 Tip

The Microsoft.SqlAdapter service won't be available to add to plans until the SQL

Server resource provider has been deployed.

Create a highly available SQL database

1. Sign in to the user portal:

For an integrated system deployment, the portal address will vary based on

your solution's region and external domain name. It will be in the format of

https://portal.<region>.<FQDN> .

For the Azure Stack Development Kit (ASDK), the portal address is

https://portal.local.azurestack.external .

2. Select + Create a resource > Data + Storage, and then SQL Database.

Provide the required database property information. This info includes name,

collation, maximum size, and the subscription, resource group, and location to use

for the deployment.

3. Select SKU and then choose the appropriate SQL Hosting Server SKU to use. In this

example, the Azure Stack Hub operator has created the Enterprise-HA SKU to

support high availability for SQL AlwaysOn availability groups.

７ Note

Run these steps from the Azure Stack Hub user portal as a tenant user with a

subscription providing SQL Server capabilities (Microsoft.SQLAdapter service).

4. Select Login > Create a new login and then provide the SQL authentication

credentials to be used for the new database. When finished, select OK and then

Create to begin the database deployment process.

5. When the SQL database deployment completes successfully, review the database

properties to discover the connection string to use for connecting to the new

highly available database.

Update the SQL resource provider

Next steps

Update the SQL resource provider

Article • 05/22/2023

A new SQL resource provider might be released when Azure Stack Hub is updated to a

new build. Although the existing resource provider continues to work, we recommend

updating to the latest build as soon as possible.

Supported Azure Stack

Hub version

SQL RP version Windows Server that RP service is

running on

2206,2301 SQL RP version

2.0.13.x

Microsoft AzureStack Add-on RP Windows

Server 1.2009.0

2108,2206 SQL RP version

2.0.6.x

Microsoft AzureStack Add-on RP Windows

Server 1.2009.0

2108, 2102, 2008, 2005 SQL RP version

1.1.93.5

Microsoft AzureStack Add-on RP Windows

Server

2005, 2002, 1910 SQL RP version

1.1.47.0

Windows Server 2016 Datacenter - Server

Core

） Important

Starting from Azure Stack Hub build 2108, the SQL and MySQL resource providers

are offered to subscriptions that have been granted access. If you want to start

using this feature, or if you need to upgrade from a previous version, open a

support case and our support engineers will guide you through the deployment or

upgrade process.

） Important

Before updating the resource provider, review the release notes to learn about new

functionality, fixes, and any known issues that could affect your deployment. The

release notes also specify the minimum Azure Stack Hub version required for the

resource provider.

） Important

Updating the resource provider will NOT update the hosting SQL Server.

Supported Azure Stack

Hub version

SQL RP version Windows Server that RP service is

running on

1908 SQL RP version

1.1.33.0

Windows Server 2016 Datacenter - Server

Core

If you have already deployed SQL RP V2, and want to check for updates, check How to

apply updates to resource provider.

If you want to update from SQL RP V1 to SQL RP V2, make sure you have first updated

to SQL RP V1.1.93.x, then apply the major version upgrade process to upgrade from SQL

RP V1 to SQL RP V2.

1. Make sure you have updated SQL RP V1 to the latest 1.1.93.x. Under Default

Provider Subscription, find the RP resource group (naming format: system.

<region>.sqladapter). Confirm the version tag and SQL RP VM name in resource

group.

2. open a support case to get the MajorVersionUpgrade package, and add your

subscription to the ASH marketplace allowlist for the future V2 version.

3. Download Microsoft AzureStack Add-On RP Windows Server 1.2009.0 to

marketplace.

4. Ensure datacenter integration prerequisites are met.

Prerequisite Reference

Conditional DNS forwarding is set

correctly.

Azure Stack Hub datacenter integration - DNS

Inbound ports for resource providers

are open.

Azure Stack Hub datacenter integration - Ports and

protocols inbound

Update SQL Server resource provider V2

Update from SQL RP V1.1.93.x to SQL RP

V2.0.6.0

Prerequisites

Prerequisite Reference

PKI certificate subject and SAN are set

correctly.

Azure Stack Hub deployment mandatory PKI

prerequisites

Azure Stack Hub deployment PaaS certificate

prerequisites

5. (for disconnected environment) Install the required PowerShell modules, similar to

the update process used to Deploy the resource provider.

Run the following script from an elevated PowerShell console to perform major version

upgrade.

PowerShell

Trigger MajorVersionUpgrade

７ Note

Make sure the client machine that you run the script on is of OS version no older

than Windows 10 or Windows Server 2016, and the client machine has X64

Operating System Architecture.

） Important

We strongly recommend using Clear-AzureRmContext -Scope CurrentUser and

Clear-AzureRmContext -Scope Process to clear the cache before running the

deployment or update script.

# Check Operating System version

$osVersion = [environment]::OSVersion.Version

if ($osVersion.Build -lt 10240)

{

Write-Host "OS version is too old: $osVersion."

return

}

$osArch = (Get-WmiObject Win32\_OperatingSystem).OSArchitecture

if ($osArch -ne "64-bit")

{

Write-Host "OS Architecture is not 64 bit."

return

}

# Check LongPathsEnabled registry key

$regPath = 'HKLM:\SYSTEM\CurrentControlSet\Control\FileSystem'

$longPathsEnabled = 'LongPathsEnabled'

$property = Get-ItemProperty -Path $regPath -Name $longPathsEnabled -

ErrorAction Stop

if ($property.LongPathsEnabled -eq 0)

{

Write-Host "Detect LongPathsEnabled equals to 0, prepare to set the

property."

Set-ItemProperty -Path $regPath -Name $longPathsEnabled -Value 1 -

ErrorAction Stop

Write-Host "Set the long paths property, please restart the PowerShell."

return

}

# Use the NetBIOS name for the Azure Stack Hub domain.

$domain = "YouDomain"

# For integrated systems, use the IP address of one of the ERCS VMs

$privilegedEndpoint = "YouDomain-ERCS01"

# Provide the Azure environment used for deploying Azure Stack Hub. Required

only for Azure AD deployments. Supported values for the <environment name>

parameter are AzureCloud, AzureChinaCloud, or AzureUSGovernment depending

which Azure subscription you're using.

$AzureEnvironment = "AzureCloud"

# Point to the directory where the resource provider installation files were

extracted.

$tempDir = 'C:\extracted-folder\MajorVersionUpgrade-SQLRP'

# The service admin account can be Azure Active Directory or Active

Directory Federation Services.

$serviceAdmin = "admin@mydomain.onmicrosoft.com"

$AdminPass = ConvertTo-SecureString 'xxxxxxxx' -AsPlainText -Force

$AdminCreds = New-Object System.Management.Automation.PSCredential

($serviceAdmin, $AdminPass)

# Add the cloudadmin credential that's required for privileged endpoint

access.

$CloudAdminPass = ConvertTo-SecureString 'xxxxxxxx' -AsPlainText -Force

$CloudAdminCreds = New-Object System.Management.Automation.PSCredential

("$domain\cloudadmin", $CloudAdminPass)

# Change the following as appropriate.

$PfxPass = ConvertTo-SecureString 'xxxxxxx' -AsPlainText -Force

# Provide the pfx file path

$PfxFilePath = "C:\tools\sqlcert\SSL.pfx"

# PowerShell modules used by the RP MajorVersionUpgrade are placed in

C:\Program Files\SqlMySqlPsh

# The deployment script adds this path to the system $env:PSModulePath to

ensure correct modules are used.

$rpModulePath = Join-Path -Path $env:ProgramFiles -ChildPath 'SqlMySqlPsh'

1. The MajorVersionUpgrade script executed without any errors.

2. Check the resource provider in marketplace and make sure that SQL RP 2.0 has

been installed successfully.

3. The old system.<location>.sqladapter resource group and system.

<location>.dbadapter.dns resource group in the default provider subscription will

not be automatically deleted by the script.

We recommend keeping the Storage Account and the Key Vault in the sqladapter

resource group for some time. If after the upgrade, any tenant user observes

inconsistent database or login metadata, it is possible to get support to restore the

metadata from the resource group.

After verifying that the DNS Zone in the dbadapter.dns resource group is empty

with no DNS record, it is safe to delete the dbadapter.dns resource group.

[IMPORTANT] Do not use the V1 deploy script to uninstall the V1 version. After

upgrade completed and confirmation that the upgrade was successful, you can

manually delete the resource group from the provider subscription.

SQL resource provider V1 update is cumulative. You can directly update to the 1.1.93.x

version.

$env:PSModulePath = $env:PSModulePath + ";" + $rpModulePath

. $tempDir\MajorVersionUpgradeSQLProvider.ps1 -AzureEnvironment

$AzureEnvironment -AzCredential $AdminCreds -CloudAdminCredential

$CloudAdminCreds -Privilegedendpoint $privilegedEndpoint -PfxPassword

$PfxPass -PfxCert $PfxFilePath

７ Note

The DNS address and the corresponding IP address of SQL RP V2 are different. To

get the new public IP, you can contact support to require a DRP break glass and

find the SQLRPVM1130-PublicIP resource. You can also run "nslookup

sqlrp.dbadapter.<fqdn>" from a client machine that already passed the endpoint

test to find out the public IP.

Validate the upgrade is successful

Update from SQL RP V1 earlier version to SQL

RP V1.1.93.x

To update the resource provider to 1.1.93.x, use the UpdateSQLProvider.ps1 script. Use

your service account with local administrative rights and is an owner of the subscription.

This update script is included with the download of the resource provider.

The update process is similar to the process used to Deploy the resource provider. The

update script uses the same arguments as the DeploySqlProvider.ps1 script, and you'll

need to provide certificate information.

The UpdateSQLProvider.ps1 script creates a new virtual machine (VM) with the latest OS

image, deploy the latest resource provider code, and migrates the settings from the old

resource provider to the new resource provider.

After the UpdateSQLProvider.ps1 script creates a new VM, the script migrates the

following settings from the old resource provider VM:

database information

hosting server information

required DNS record

You can specify the following parameters from the command line when you run the

UpdateSQLProvider.ps1 PowerShell script. If you don't, or if any parameter validation

fails, you're prompted to provide the required parameters.

Update script processes

７ Note

We recommend that you download the Microsoft AzureStack Add-on RP Windows

Server 1.2009.0 image from Marketplace Management. If you need to install an

update, you can place a single MSU package in the local dependency path. The

script will fail if there's more than one MSU file in this location.

） Important

We strongly recommend using Clear-AzureRmContext -Scope CurrentUser and

Clear-AzureRmContext -Scope Process to clear the cache before running the

deployment or update script.

Update script parameters

Parameter name Description Comment

or default

value

Parameter name Description Comment

or default

value

CloudAdminCredential The credential for the cloud admin, necessary for

accessing the privileged endpoint.

Required

AzCredential The credentials for the Azure Stack Hub service

admin account. Use the same credentials that you

used for deploying Azure Stack Hub. The script

will fail if the account you use with AzCredential

requires multi-factor authentication (MFA).

Required

VMLocalCredential The credentials for the local admin account of the

SQL resource provider VM.

Required

PrivilegedEndpoint The IP address or DNS name of the privileged

endpoint.

Required

AzureEnvironment The Azure environment of the service admin

account which you used for deploying Azure

Stack Hub. Required only for Azure AD

deployments. Supported environment names are

AzureCloud, AzureUSGovernment, or if using a

China Azure AD, AzureChinaCloud.

AzureCloud

DependencyFilesLocalPath You must also put your certificate .pfx file in this

directory.

Optional

for single

node, but

mandatory

for multinode

DefaultSSLCertificatePassword The password for the .pfx certificate. Required

MaxRetryCount The number of times you want to retry each

operation if there's a failure.

2

RetryDuration The timeout interval between retries, in seconds. 120

Uninstall Removes the resource provider and all associated

resources.

No

DebugMode Prevents automatic cleanup on failure. No

If you are updating the SQL resource provider version to 1.1.33.0 or previous versions,

you need to install specific versions of AzureRm.BootStrapper and Azure Stack Hub

Update script PowerShell example

modules in PowerShell.

If you are updating the SQL resource provider to version 1.1.47.0 or later, you can skip

this step. The deployment script will automatically download and install the necessary

PowerShell modules for you to path C:\Program Files\SqlMySqlPsh.

PowerShell

The following is an example of using the UpdateSQLProvider.ps1 script that you can run

from an elevated PowerShell console. Be sure to change the variable information and

passwords as needed:

PowerShell

７ Note

If folder C:\Program Files\SqlMySqlPsh already exists with PowerShell module

downloaded, it is recommended to clean up this folder before running the update

script. This is to make sure the right version of PowerShell module is downloaded

and used.

# Run the following scripts when updating to version 1.1.33.0 only.

# Install the AzureRM.Bootstrapper module, set the profile, and install the

AzureStack module.

# Note that this might not be the most currently available version of Azure

Stack Hub PowerShell.

Install-Module -Name AzureRm.BootStrapper -Force

Use-AzureRmProfile -Profile 2018-03-01-hybrid -Force

Install-Module -Name AzureStack -RequiredVersion 1.6.0

７ Note

In disconnected scenario, you need to download the required PowerShell modules

and register the repository manually as a prerequisite. You can get more

information in Deploy SQL resource provider

# Use the NetBIOS name for the Azure Stack Hub domain. On the Azure Stack

Hub SDK, the default is AzureStack but this might have been changed at

installation.

$domain = "AzureStack"

# For integrated systems, use the IP address of one of the ERCS VMs.

$privilegedEndpoint = "AzS-ERCS01"

# Provide the Azure environment used for deploying Azure Stack Hub. Required

When the resource provider update script finishes, close the current PowerShell session.

Maintain the SQL resource provider

only for Azure AD deployments. Supported values for the <environment name>

parameter are AzureCloud, AzureChinaCloud, or AzureUSGovernment depending

which Azure subscription you're using.

$AzureEnvironment = "<EnvironmentName>"

# Point to the directory where the resource provider installation files were

extracted.

$tempDir = 'C:\TEMP\SQLRP'

# The service admin account (this can be Azure AD or AD FS).

$serviceAdmin = "admin@mydomain.onmicrosoft.com"

$AdminPass = ConvertTo-SecureString 'P@ssw0rd1' -AsPlainText -Force

$AdminCreds = New-Object System.Management.Automation.PSCredential

($serviceAdmin, $AdminPass)

# Set the credentials for the new resource provider VM.

$vmLocalAdminPass = ConvertTo-SecureString 'P@ssw0rd1' -AsPlainText -Force

$vmLocalAdminCreds = New-Object System.Management.Automation.PSCredential

("sqlrpadmin", $vmLocalAdminPass)

# Add the cloudadmin credential required for privileged endpoint access.

$CloudAdminPass = ConvertTo-SecureString 'P@ssw0rd1' -AsPlainText -Force

$CloudAdminCreds = New-Object System.Management.Automation.PSCredential

("$domain\cloudadmin", $CloudAdminPass)

# Change the following as appropriate.

$PfxPass = ConvertTo-SecureString 'P@ssw0rd1' -AsPlainText -Force

# For version 1.1.47.0 or later, the PowerShell modules used by the RP

deployment are placed in C:\Program Files\SqlMySqlPsh

# The deployment script adds this path to the system $env:PSModulePath to

ensure correct modules are used.

$rpModulePath = Join-Path -Path $env:ProgramFiles -ChildPath 'SqlMySqlPsh'

$env:PSModulePath = $env:PSModulePath + ";" + $rpModulePath

# Change directory to the folder where you extracted the installation files.

# Then adjust the endpoints.

. $tempDir\UpdateSQLProvider.ps1 -AzCredential $AdminCreds -

VMLocalCredential $vmLocalAdminCreds -CloudAdminCredential $cloudAdminCreds

-PrivilegedEndpoint $privilegedEndpoint -AzureEnvironment $AzureEnvironment

-DefaultSSLCertificatePassword $PfxPass -DependencyFilesLocalPath

$tempDir\cert

Next steps

SQL resource provider maintenance

operations

Article • 08/03/2022

The SQL resource provider runs on a locked down virtual machine (VM). To enable

maintenance operations, you need to update the VM's security. To do this using the

principle of Least Privilege, use PowerShell Just Enough Administration (JEA) endpoint

DBAdapterMaintenance. The resource provider installation package includes a script for

this action.

The SQL resource provider isn't serviced as part of Azure Stack Hub because it's an addon component. Microsoft provides updates to the SQL resource provider as necessary.

For SQL RP V1, When an updated SQL Server resource provider is released, a script is

provided to apply the update. This script creates a new resource provider VM, migrating

the state of the old provider VM to the new VM.

For SQL RP V2, resource providers are updated using the same update feature that is

used to apply Azure Stack Hub updates.

For more information, see Update the SQL resource provider.

SQL RP V1 runs on a user VM, you need to apply the required patches and updates

when they're released. You can install a Windows Update package during the installation

of, or update to, the resource provider.

） Important

Starting from Azure Stack Hub build 2108, the SQL and MySQL resource providers

are offered to subscriptions that have been granted access. If you want to start

using this feature, or if you need to upgrade from a previous version, open a

support case and our support engineers will guide you through the deployment or

upgrade process.

Patching and updating

Update the provider VM

SQL RP V2 runs on a managed Windows Server that is hidden. You don't need to patch

or update the resource provider VM. It will be updated automatically when you update

the RP.

These instructions only apply to SQL RP V1 running on Azure Stack Hub Integrated

Systems.

To update the Windows Defender definitions:

1. Download the Windows Defender definitions update from Security intelligence

updates for Windows Defender .

On the definitions update page, scroll down to "Manually download the update".

Download the "Windows Defender Antivirus for Windows 10 and Windows 8.1" 64-

bit file.

You can also use this direct link to download/run the fpam-fe.exe file.

2. Create a PowerShell session to the SQL resource provider adapter VM's

maintenance endpoint.

3. Copy the definitions update file to the VM using the maintenance endpoint

session.

4. On the maintenance PowerShell session, run the UpdateDBAdapterWindowsDefenderDefinitions command.

5. After you install the definitions, we recommend you delete the definitions update

file by using the Remove-ItemOnUserDrive command.

PowerShell script example for updating definitions

You can edit and run the following script to update the Defender definitions. Replace

values in the script with values from your environment.

PowerShell

Update the VM Windows Defender definitions

# Set credentials for local admin on the resource provider VM.

$vmLocalAdminPass = ConvertTo-SecureString '<local admin user password>' -

AsPlainText -Force

$vmLocalAdminUser = "<local admin user name>"

$vmLocalAdminCreds = New-Object System.Management.Automation.PSCredential `

($vmLocalAdminUser, $vmLocalAdminPass)

# Provide the public IP address for the adapter VM.

These instructions only apply to SQL RP V1 running on Azure Stack Hub Integrated

Systems.

Azure Diagnostics extension is installed on the SQL resource provider adapter VM by

default. The following steps show how to customize the extension for gathering the SQL

resource provider operational event logs and IIS logs for troubleshooting and auditing

purpose.

1. Sign in to the Azure Stack Hub administrator portal.

2. Select Virtual machines from the pane on the left, search for the SQL resource

provider adapter VM and select the VM.

3. In Diagnostics settings of the VM, go to the Logs tab and choose Custom to

customize event logs being collected.

$databaseRPMachine = "<RP VM IP address>"

$localPathToDefenderUpdate = "C:\DefenderUpdates\mpam-fe.exe"

# Download the Windows Defender update definitions file from

https://www.microsoft.com/wdsi/definitions.

Invoke-WebRequest -Uri 'https://go.microsoft.com/fwlink/?

LinkID=121721&arch=x64' `

-Outfile $localPathToDefenderUpdate

# Create a session to the maintenance endpoint.

$session = New-PSSession -ComputerName $databaseRPMachine `

-Credential $vmLocalAdminCreds -ConfigurationName DBAdapterMaintenance `

-SessionOption (New-PSSessionOption -Culture en-US -UICulture en-US)

# Copy the defender update file to the adapter VM.

Copy-Item -ToSession $session -Path $localPathToDefenderUpdate `

-Destination "User:\"

# Install the update definitions.

Invoke-Command -Session $session -ScriptBlock `

{Update-AzSDBAdapterWindowsDefenderDefinition -

DefinitionsUpdatePackageFile "User:\mpam-fe.exe"}

# Cleanup the definitions package file and session.

Invoke-Command -Session $session -ScriptBlock `

{Remove-AzSItemOnUserDrive -ItemPath "User:\mpam-fe.exe"}

$session | Remove-PSSession

Configure Azure Diagnostics extension for SQL resource

provider

4. Add Microsoft-AzureStack-DatabaseAdapter/Operational!\* to collect SQL

resource provider operational event logs.

5. To enable the collection of IIS logs, check IIS logs and Failed request logs.

6. Finally select Save to save all the Diagnostics settings.

Once the event logs and IIS logs collection are configured for SQL resource provider, the

logs can be found in a system storage account named sqladapterdiagaccount.

To learn more about Azure Diagnostics extension, please see What is Azure Diagnostics

extension.

You're responsible for creating and maintaining sysadmin accounts on your SQL servers.

The resource provider needs an account with these privileges to manage databases for

users, but it doesn't need access to the users' data. If you need to update the sysadmin

passwords on your SQL servers, you can use the resource provider's administrator

interface to change a stored password. These passwords are stored in a Key Vault on

your Azure Stack Hub instance.

To modify the settings, select Browse > ADMINISTRATIVE RESOURCES > SQL Hosting

Servers > SQL Logins and select a user name. The change must be made on the SQL

instance first (and any replicas, if necessary.) Under Settings, select Password.

Updating SQL credentials

These instructions only apply to SQL RP V1 running on Azure Stack Hub Integrated

Systems.

When using the SQL and MySQL resource providers with Azure Stack Hub integrated

systems, the Azure Stack Hub operator is responsible for rotating the following resource

provider infrastructure secrets to ensure that they don't expire:

External SSL certificate provided during deployment.

The resource provider VM local admin account password provided during

deployment.

Resource provider diagnostic user (dbadapterdiag) password.

(version >= 1.1.47.0) Key Vault certificate generated during deployment.

Change all the secrets at the same time.

PowerShell

Secrets rotation

PowerShell examples for rotating secrets

） Important

Successful secret rotation requires the removal of any existing versions of the

Azure Stack Hub PowerShell modules, prior to running the script below.

.\SecretRotationSQLProvider.ps1 `

-Privilegedendpoint $Privilegedendpoint `

-CloudAdminCredential $cloudCreds `

-AzCredential $adminCreds `

-DiagnosticsUserPassword $passwd `

Change the diagnostic user password.

PowerShell

Change the VM local admin account password.

PowerShell

Rotate the SSL certificate

PowerShell

Rotate the Key Vault certificate

PowerShell

-DependencyFilesLocalPath $certPath `

-DefaultSSLCertificatePassword $certPasswd `

-VMLocalCredential $localCreds `

-KeyVaultPfxPassword $keyvaultCertPasswd

.\SecretRotationSQLProvider.ps1 `

-Privilegedendpoint $Privilegedendpoint `

-CloudAdminCredential $cloudCreds `

-AzCredential $adminCreds `

-DiagnosticsUserPassword $passwd

.\SecretRotationSQLProvider.ps1 `

-Privilegedendpoint $Privilegedendpoint `

-CloudAdminCredential $cloudCreds `

-AzCredential $adminCreds `

-VMLocalCredential $localCreds

.\SecretRotationSQLProvider.ps1 `

-Privilegedendpoint $Privilegedendpoint `

-CloudAdminCredential $cloudCreds `

-AzCredential $adminCreds `

-DependencyFilesLocalPath $certPath `

-DefaultSSLCertificatePassword $certPasswd

.\SecretRotationSQLProvider.ps1 `

-Privilegedendpoint $Privilegedendpoint `

-CloudAdminCredential $cloudCreds `

-AzCredential $adminCreds `

-KeyVaultPfxPassword $keyvaultCertPasswd

Parameter Description Comment

AzureEnvironment The Azure environment of the service admin

account used for deploying Azure Stack Hub.

Required only for Azure AD deployments.

Supported environment names are AzureCloud,

AzureUSGovernment, or if using a China Azure

Active Directory, AzureChinaCloud.

Optional

AzCredential Azure Stack Hub service admin account credential.

The script will fail if the account you use with

AzCredential requires multi-factor authentication

(MFA).

Mandatory

CloudAdminCredential Azure Stack Hub cloud admin domain account

credential.

Mandatory

PrivilegedEndpoint Privileged Endpoint to access GetAzureStackStampInformation.

Mandatory

DiagnosticsUserPassword Diagnostics user account password. Optional

VMLocalCredential Local admin account on the MySQLAdapter VM. Optional

DefaultSSLCertificatePassword Default SSL certificate (\*.pfx) password. Optional

DependencyFilesLocalPath Dependency files local path. Optional

KeyVaultPfxPassword The password used for generating the Key Vault

certificate for database adapter.

Optional

Azure Stack Hub has multiple ways to collect, save, and send diagnostic logs to

Microsoft Support. Starting from version 1.1.93, SQL Resource Provider supports the

standard way of collecting logs from your Azure Stack Hub environment. For more

information, see Diagnostic log collection.

Limitation:

When the deployment, upgrade, or secret rotation script failed, some logs cannot be

SecretRotationSQLProvider.ps1 parameters

Collect diagnostic logs

Known limitations of SQL Server resource provider

Version 1

collected by the standard log collection mechanism.

Workaround:

Besides using the standard log collection mechanism, go to the Logs folder in the

extracted folder where the script locates, to find more logs.

Add SQL Server hosting servers

Next steps

Remove the SQL resource provider

Article • 07/29/2022

Removing the SQL resource provider will delete:

The SQL resource provider.

The associated plans and quotas managed by operator.

The metadata in Azure Stack Hub for the hosting server, database, and logins.

Removing the SQL resource provider will not delete:

The tenant databases on the hosting servers.

The packages used to install SQL RP.

1. Verify that you've removed all the existing SQL resource provider dependencies.

2. Get a copy of the SQL resource provider installation package and then run the selfextractor to extract the contents to a temporary directory. You can find the

download links for the resource provider installers in Deploy the resource provider

prerequisites.

3. Open a new elevated PowerShell console window and change to the directory

where you extracted the SQL resource provider installation files.

） Important

Starting from Azure Stack Hub build 2108, the SQL and MySQL resource providers

are offered to subscriptions that have been granted access. If you want to start

using this feature, or if you need to upgrade from a previous version, open a

support case and our support engineers will guide you through the deployment or

upgrade process.

To remove the SQL resource provider V1

７ Note

Uninstalling the SQL resource provider will proceed even if dependent

resources are currently using the resource provider.

） Important

4. Run the DeploySqlProvider.ps1 script using the following parameters:

Uninstall: Removes the resource provider and all associated resources.

PrivilegedEndpoint: The IP address or DNS name of the privileged endpoint.

AzureEnvironment: The Azure environment used for deploying Azure Stack

Hub. Required only for Azure AD deployments.

CloudAdminCredential: The credential for the cloud admin, necessary to

access the privileged endpoint.

AzCredential: The credential for the Azure Stack Hub service admin account.

Use the same credentials that you used for deploying Azure Stack Hub. The

script will fail if the account you use with AzCredential requires multi-factor

authentication (MFA).

1. Sign in to the Azure Stack Hub administrator portal.

2. Select Marketplace Management on the left, then select Resource providers.

3. Select SQL resource provider from the list of resource providers. You may want to

filter the list by Entering “SQL Server resource provider” or “MySQL Server resource

provider” in the search text box provided.

We strongly recommend using Clear-AzureRmContext -Scope CurrentUser and

Clear-AzureRmContext -Scope Process to clear the cache before running the

script.

To remove the SQL resource provider V2

4. Select Uninstall from the options provided across the top the page.

5. Enter the name of the resource provider, then select Uninstall. This action confirms

your desire to uninstall:

The SQL Server resource provider.

All admin/user created SKU/Quota/HostingServer/Database/Login metadata.

6. (Optional) If you want to delete the installation package, after uninstalling the SQL

resource provider, select Delete from the SQL resource provider page.

Offer App Services as PaaS

Next steps

SQL resource provider 2.0.13.x release

notes

Article • 05/22/2023

These release notes describe the improvements and known issues in SQL resource

provider version 2.0.13.x.

After release version 2.0, SQL resource provider becomes a standard Azure Stack Hub

value-add RP. If you want to get access to the SQL resource provider in Azure Stack Hub

marketplace, open a support case to add your subscription to the allowlist.

The resource provider has a minimum corresponding Azure Stack Hub build. It is

required that you apply the minimum supported Azure Stack Hub update to your Azure

Stack Hub integrated system before deploying the latest version of the SQL resource

provider.

Supported Azure Stack Hub version SQL resource provider version

Version 2108,2206 SQL RP version 2.0.6.0

Version 2206, 2301 SQL RP version 2.0.13.0

This version of the Azure Stack Hub SQL resource provider includes the following

improvements and fixes:

UI fixes to prevent future breaks when portal is upgraded.

Other bug fixes.

Build reference

） Important

It is strongly recommended to upgrade to 2.0.13.0 when your Azure Stack Hub

version is 2206.

New features and fixes

） Important

Learn more about the SQL resource provider.

Prepare to deploy the SQL resource provider.

Upgrade the SQL resource provider from a previous version.

You may need to refresh the web browser cache for the new UI fixes to take effect.

Known issues

Next steps

SQL resource provider 2.0.6.x release

notes

Article • 10/21/2022

These release notes describe the improvements and known issues in SQL resource

provider version 2.0.6.x.

Starting from this release, SQL resource provider becomes a standard Azure Stack Hub

value-add RP. If you want to get access to the SQL resource provider in Azure Stack Hub

marketplace, open a support case to add your subscription to the allowlist.

The resource provider has a minimum corresponding Azure Stack Hub build. The

minimum Azure Stack Hub release version required to install this version of the SQL

resource provider is listed below.

It is required that you apply the minimum supported Azure Stack Hub update to your

Azure Stack Hub integrated system before deploying the latest version of the SQL

resource provider.

Supported Azure Stack Hub version SQL resource provider version

Version 2108,2206 SQL RP version 2.0.6.0

This version of the Azure Stack Hub SQL resource provider includes the following

improvements and fixes:

Installation and future version upgrade will be from the Azure Stack Hub

marketplace.

Build reference

） Important

If there is an existing version of SQL resource provider running in your system,

make sure to update it to version 1.1.93.x, before upgrading to this lattest version.

New features and fixes

A specific version of Add-on RP Windows Server will be required. The correct

version of Microsoft AzureStack Add-On RP Windows Server will be automatically

downloaded if you install the resource provider in connected environment. In

disconnected environment, make sure the right version of Microsoft AzureStack

Add-On RP Windows Server image is downloaded before deploying or upgrading

to this version of the SQL resource provider.

Receive alerts when certifications are about to expire. Check this document for

details.

Other bug fixes.

After deployment or upgrade, Azure Stack Hub Operators need to manually register

their default provider subscription to the tenant namespace (Microsoft.SQLAdapter)

before they can create Login or Databases.

Learn more about the SQL resource provider.

Prepare to deploy the SQL resource provider.

Upgrade the SQL resource provider from a previous version.

Known issues

Next steps

SQL resource provider 1.1.93.x release

notes

Article • 04/01/2022

These release notes describe the improvements and known issues in SQL resource

provider version 1.1.93.x.

Download the SQL resource provider binary and then run the self-extractor to extract

the contents to a temporary directory. The resource provider has a minimum

corresponding Azure Stack Hub build. The minimum Azure Stack Hub release version

required to install this version of the SQL resource provider is listed below:

Supported Azure Stack Hub version SQL resource provider version

Version 2108\*， 2102, 2008, 2005 SQL RP version 1.1.93.5

This version of the Azure Stack Hub SQL resource provider includes the following

improvements and fixes:

Update the base VM to a specialized Windows Server. This Windows Server

version is specialize for Azure Stack Hub Add-On RP Infrastructure and it is not

Build reference

７ Note

It is supported to run SQL RP 1.1.93.x on Azure Stack 2108, however it is an known

issue that the monitoring panel cannot load.

） Important

Apply the minimum supported Azure Stack Hub update to your Azure Stack Hub

integrated system before deploying the latest version of the MySQL resource

provider.

New features and fixes

visible to the tenant marketplace. Make sure to download the Microsoft

AzureStack Add-On RP Windows Server image before deploying or upgrading to

this version of the SQL resource provider.

Support removing orphaned database metadata and hosting server metadata.

When a hosting server cannot be connected anymore, the tenant will have an

option to remove the orphaned database metadata from the portal. When there is

no orphaned database metadata linked to the hosting server, the operator will be

able to remove the orphaned hosting server metadata from the admin portal.

Make KeyVaultPfxPassword an optional argument when performing secrets

rotation. Check this document for details.

Other bug fixes.

It's recommended that you apply SQL resource provider 1.1.93.5 after Azure Stack Hub

is upgraded to the 2005 release.

Deployment of 1.1.93.0 version may fail if the wrong AzureRmContext is used. It is

recommended to upgrade to 1.1.93.5 version directly.

When redeploying the SQL resource provider while the same version had deployed

already (for example, when SQL resource provider 1.1.93.5 is already deployed, and the

same version is deployed again), the VM that is hosting the SQL resource provider will

be stopped. To fix this issue, go to the admin portal, locate and restart the VM named

sqlvm<version> in the resource group named system.<region>.sqladapter.

Learn more about the SQL resource provider.

Prepare to deploy the SQL resource provider.

Upgrade the SQL resource provider from a previous version.

Known issue

Next steps

SQL resource provider 1.1.47.0 release

notes

Article • 07/29/2022

These release notes describe the improvements and known issues in SQL resource

provider version 1.1.47.0.

Download the SQL resource provider binary and then run the self-extractor to extract

the contents to a temporary directory. The resource provider has a minimum

corresponding Azure Stack Hub build. The minimum Azure Stack Hub release version

required to install this version of the SQL resource provider is listed below:

Minimum Azure Stack Hub version SQL resource provider version

Version 1910 (1.1910.0.58) SQL RP version 1.1.47.0

This version of the Azure Stack Hub SQL resource provider is a hotfix release to make

the resource provider compatible with the latest portal changes in the 1910 update.

There are no new features.

It also supports the latest Azure Stack Hub API version profile 2019-03-01-hybrid and

Azure Stack Hub PowerShell module 1.8.0. So during deployment and update, no

specific history versions of modules need to be installed.

Follow the resource provider update process to apply the SQL resource provider hotfix

1.1.47.0 after Azure Stack Hub is upgraded to the 1910 update. It will help address a

known issue in the administrator portal where Capacity Monitoring in SQL resource

provider keeps loading.

Build reference

） Important

Apply the minimum supported Azure Stack Hub update to your Azure Stack Hub

integrated system before deploying the latest version of the SQL resource provider.

New features and fixes

When rotating certificate for Azure Stack Hub integrated systems, KeyVaultPfxPassword

argument is mendatory, even if there's no intention to update the Key Vault certificate

password.

Learn more about the SQL resource provider.

Prepare to deploy the SQL resource provider.

Upgrade the SQL resource provider from a previous version.

Known issues

Next steps

Usage and billing in Azure Stack Hub

Article • 12/16/2021

This article describes how Azure Stack Hub users are billed for resource usage, and how

the billing information is accessed for analytics and chargeback.

Azure Stack Hub collects and groups usage data for resources that are used, then

forwards this data to Azure Commerce. Azure Commerce bills you for Azure Stack Hub

usage in the same way it bills you for Azure usage.

You can also get usage data and export it to your own billing or chargeback system by

using a billing adapter, or export it to a business intelligence tool such as Microsoft

Power BI.

Each resource provider in Azure Stack Hub posts usage data per resource usage. The

usage service periodically (hourly and daily) aggregates usage data and stores it in the

usage database. Azure Stack Hub operators and users can access the stored usage data

through the Azure Stack Hub resource usage APIs.

If you've registered your Azure Stack Hub instance with Azure, Azure Stack Hub is

configured to send the usage data to Azure Commerce. After the data is uploaded to

Azure, you can access it through the billing portal or by using Azure resource usage

APIs. For more information about what usage data is reported to Azure, see Usage data

reporting.

The following figure shows the key components in the usage pipeline:

Usage pipeline

Azure Stack Hub resource providers (such as Compute, Storage, and Network) generate

usage data at hourly intervals for each subscription. The usage data contains

information about the resource used; such as resource name, subscription used, and

quantity used. To learn about the meters' ID resources, see the Usage API FAQ.

After the usage data has been collected, it is reported to Azure to generate a bill, which

can be viewed through the Azure billing portal.

The Azure billing portal shows usage data for the chargeable resources. In addition to

the chargeable resources, Azure Stack Hub captures usage data for a broader set of

resources, which you can access in your Azure Stack Hub environment through REST

APIs or PowerShell cmdlets. Azure Stack Hub operators can get the usage data for all

user subscriptions. Individual users can only get their own usage details.

A multi-tenant Cloud Solution Provider (CSP) using Azure Stack Hub might want to

report each customer usage separately, so that the provider can charge usage to

different Azure subscriptions.

Each customer has their identity represented by a different Azure Active Directory (Azure

AD) tenant. Azure Stack Hub supports assigning one CSP subscription to each Azure AD

tenant. You can add tenants and their subscriptions to the base Azure Stack Hub

registration. The base registration is done for all Azure Stack Hub instances. If a

subscription is not registered for a tenant, the user can still use Azure Stack Hub, and

their usage is sent to the subscription used for the base registration.

Register with Azure Stack Hub

What usage information can I find, and how?

７ Note

Usage data reporting is not required for the Azure Stack Development Kit (ASDK)

and for Azure Stack Hub integrated system users who license under the capacity

model. To learn more about licensing in Azure Stack Hub, see the packaging and

pricing data sheet .

Usage reporting for multi-tenant Cloud

Solution Providers

Next steps

Report Azure Stack Hub usage data to Azure

Provider Resource Usage API

Tenant Resource Usage API

Usage-related FAQ

Manage usage and billing for Azure

Stack Hub as a Cloud Solution Provider

Article • 10/11/2021

This article describes how to register Azure Stack Hub as a Cloud Solution Provider (CSP)

and how to add customers.

As a CSP, you work with diverse customers using your Azure Stack Hub. Each customer

has a CSP subscription in Azure. You must direct usage from your Azure Stack Hub to

each user subscription.

The following figure shows the required steps to choose your shared services account,

and to register the Azure account with the Azure Stack Hub account. Once registered,

you can onboard your end customers:

Choose the type of shared services account that you use for Azure Stack Hub. The types

of subscriptions that can be used for registration of a multi-tenant Azure Stack Hub are:

Cloud Solution Provider

Azure Partner Shared Services subscription

We've created a tutorial video to help you understand how to manage your multi-tenant

rights:

Create a CSP or APSS subscription

CSP subscription types

https://www.youtube-nocookie.com/embed/ZP6jkbLeS34

Azure Partner Shared Services

Azure Partner Shared Services (APSS) subscriptions are the preferred choice for

registration when a direct CSP or a CSP distributor operates Azure Stack Hub.

APSS subscriptions are associated with a shared-services tenant. When you register

Azure Stack Hub, you provide credentials for an account that's an owner of the

subscription. The account you use to register Azure Stack Hub can be different from the

admin account that you use for deployment. Furthermore, the two accounts do not

need to belong to the same domain; you can deploy using the tenant that you already

use. For example, you can use ContosoCSP.onmicrosoft.com , then register using a

different tenant; for example, IURContosoCSP.onmicrosoft.com . You must remember to

sign in using ContosoCSP.onmicrosoft.com when you perform daily Azure Stack Hub

administration. You sign in to Azure using IURContosoCSP.onmicrosoft.com when you

need to perform registration operations.

For a description of APSS subscriptions and how to create them, see Add Azure Partner

Shared Services.

CSP subscriptions are the preferred choice for registration when a CSP reseller or an end

customer operates Azure Stack Hub.

Use the APSS subscription created using the information in the preceding section to

register Azure Stack Hub with Azure. For more information, see Register Azure Stack

Hub with your Azure subscription.

To configure Azure Stack Hub so that a new tenant's resource usage is reported to their

CSP subscription, see Add tenant for usage and billing to Azure Stack Hub.

Azure Stack Hub uses a feature called registration. A registration is an object stored in

Azure. The registration object documents which Azure subscription(s) to use to charge

for a given Azure Stack Hub. This section addresses the importance of registration.

Using registration, Azure Stack Hub can:

CSP subscriptions

Register Azure Stack Hub

Add end customer

Charge the right subscriptions

Forward Azure Stack Hub usage data to Azure Commerce and bill an Azure

subscription.

Report each customer's usage on a different subscription with a multi-tenant Azure

Stack Hub deployment. Multi-tenancy enables Azure Stack Hub to support

different organizations on the same Azure Stack Hub instance.

For each Azure Stack Hub, there is one default subscription and many tenant

subscriptions. The default subscription is an Azure subscription that is charged if there's

no tenant-specific subscription. It must be the first subscription to be registered. For

multi-tenant usage reporting to work, the subscription must be a CSP or APSS

subscription.

Then, the registration is updated with an Azure subscription for each tenant that uses

Azure Stack Hub. Tenant subscriptions must be of the CSP type, and must roll up to the

partner who owns the default subscription. You cannot register someone else's

customers.

When Azure Stack Hub forwards usage info to global Azure, a service in Azure consults

the registration and maps each tenant's usage to the appropriate tenant subscription. If

a tenant has not been registered, that usage goes to the default subscription for the

Azure Stack Hub instance from which it originated.

Because tenant subscriptions are CSP subscriptions, their bill is sent to the CSP partner,

and usage info is not visible to the end customer.

To learn more about the CSP program, see Cloud Solution Provider program .

To learn more about how to retrieve resource usage info from Azure Stack Hub,

see Usage and billing in Azure Stack Hub.

Next steps

Add tenant for usage and billing to

Azure Stack Hub

Article • 10/11/2021

This article describes how to add a tenant to an Azure Stack Hub deployment managed

by a Cloud Solution Provider (CSP). When the new tenant uses resources, Azure Stack

Hub reports usage to their CSP subscription.

CSPs often offer services to multiple end customers (tenants) on their Azure Stack Hub

deployment. Adding tenants to the Azure Stack Hub registration ensures that each

tenant's usage is reported and billed to the corresponding CSP subscription. If you don't

complete the steps in this article, tenant usage is charged to the subscription used in the

initial registration of Azure Stack Hub. Before you can add an end customer to Azure

Stack Hub for usage tracking and to manage their tenant, you must configure Azure

Stack Hub as a CSP. For steps and resources, see Manage usage and billing for Azure

Stack Hub as a Cloud Solution Provider.

The following figure shows the steps that a CSP needs to follow to enable a new end

customer to use Azure Stack Hub, and to set up usage tracking for the customer. By

adding the end customer, you're also able to manage resources in Azure Stack Hub. You

have two options for managing their resources:

You can maintain the end customer and provide credentials for the local Azure

Stack Hub subscription to the end customer.

The end customer can work with their subscription locally and add the CSP as a

guest with owner permissions.

Before you add an end customer, you must enable multi-tenant billing on your

registration. In order to enable multi-tenant billing, send the registration subscription ID,

resource group name, and registration name to azstcsp@microsoft.com . It usually takes

1-2 business days to enable multi-tenancy.

Perform the following steps to add an end customer, as pictured in the following figure:

Add an end customer

In Partner Center, create a new Azure subscription for the customer. For instructions, see

Add a new customer.

After you've created a record of your customer in Partner Center, you can sell them

subscriptions to products in the catalog. For instructions, see Create, suspend, or cancel

customer subscriptions.

By default, you, as the CSP, do not have access to the end customer's Azure Stack Hub

subscription. However, if your customer wants you to manage their resources, they can

then add your account as owner/contributor to their Azure Stack Hub subscription. In

order to do that, they must add your account as a guest user to their Azure AD tenant.

It's advised that you use a different account from your Azure CSP account to manage

your customer's Azure Stack Hub subscription to ensure you don't lose access to your

customer's Azure subscription.

Update your registration with the new customer subscription. Azure reports the

customer usage using the customer identity from Partner Center. This step ensures that

each customer's usage is reported under that customer's individual CSP subscription.

This makes tracking usage and billing easier. To perform this step, you must first register

Azure Stack Hub.

1. Open Windows PowerShell in an elevated prompt, and run:

PowerShell

Create a new customer in Partner Center

Create an Azure subscription for the end customer

Create a guest user in the end customer directory

Update the registration with the end customer

subscription

Az modules

Connect-AzAccount

７ Note

2. Type your Azure credentials.

3. In the PowerShell session, run:

PowerShell

The following section describes the parameters for the New-AzResource cmdlet:

Parameter Description

registrationSubscriptionID The Azure subscription that was used for the initial registration

of the Azure Stack Hub.

customerSubscriptionID The Azure subscription (not Azure Stack Hub) belonging to the

customer to be registered. Must be created in the CSP offer. In

practice, this means through Partner Center. If a customer has

more than one Azure Active Directory tenant, this subscription

must be created in the tenant that will be used to log into Azure

Stack Hub. The customer subscription ID is case sensitive.

resourceGroup The resource group in Azure in which your registration is stored.

registrationName The name of the registration of your Azure Stack Hub. It's an

object stored in Azure.

If your session expires, your password has changed, or you want to switch

accounts, run the following cmdlet before you sign in using ConnectAzAccount: Remove-AzAccount-Scope Process .

New-AzResource -ResourceId

"subscriptions/{registrationSubscriptionId}/resourceGroups/{resourc

eGroup}/providers/Microsoft.AzureStack/registrations/{registrationN

ame}/customerSubscriptions/{customerSubscriptionId}" -ApiVersion

2017-06-01

New-AzResource PowerShell parameters

７ Note

Tenants must be registered with each Azure Stack Hub they use. If you have two

Azure Stack Hub deployments, and a tenant uses both of them, you must update

the initial registrations of each deployment with the tenant subscription.

Configure Azure Stack Hub to support users from multiple Azure AD tenants to use

services in Azure Stack Hub. For instructions, see Enable multi-tenancy in Azure Stack

Hub.

Once you've added the new customer to Azure Stack Hub, or the end customer tenant

has enabled your guest account with owner privileges, verify that you can create a

resource in their tenant. For example, they can Create a Windows virtual machine with

the Azure Stack Hub portal.

To review error messages if they're triggered in your registration process, see

Tenant registration error messages.

To learn more about how to retrieve resource usage information from Azure Stack

Hub, see Usage and billing in Azure Stack Hub.

To review how an end customer may add you, the CSP, as the manager for their

Azure Stack Hub tenant, see Enable a Cloud Solution Provider to manage your

Azure Stack Hub subscription.

Onboard tenant to Azure Stack Hub

Create a local resource in the end customer tenant in

Azure Stack Hub

Next steps

Register tenants for usage tracking in

Azure Stack Hub

Article • 10/11/2021

This article contains details about registration operations. You can use these operations

to:

Manage tenant registrations.

Manage tenant usage tracking.

You can use this operation when you want to add a new tenant to your registration.

Tenant usage is reported under an Azure subscription connected with the Azure Active

Directory (Azure AD) tenant.

You can also use this operation to change the subscription associated with a tenant. Call

PUT or the New-AzResource PowerShell cmdlet to overwrite the previous mapping. If

you are using the AzureRM PowerShell module, use the New-AzureRMResource

PowerShell cmdlet.

You can associate a single Azure subscription with a tenant. If you try to add a second

subscription to an existing tenant, the first subscription is overwritten.

The following registration cmdlets require that you specify an API profile when running

PowerShell. API profiles represent a set of Azure resource providers and their API

versions. They help you use the right version of the API when interacting with multiple

Azure clouds. For example, if you work with multiple clouds when working with global

Azure and Azure Stack Hub, API profiles specify a name that matches their release date.

You use the 2017-09-03 profile.

For more information about Azure Stack Hub and API profiles, see Manage API version

profiles in Azure Stack Hub.

Parameter Description

Add tenant to registration

Use API profiles

Parameters

Parameter Description

registrationSubscriptionID The Azure subscription that was used for the initial registration.

customerSubscriptionID The Azure subscription (not Azure Stack Hub) belonging to the

customer to be registered. Must be created in the Cloud Solution

Provider (CSP) offer through the Partner Center. If a customer has

more than one tenant, create a subscription for the tenant to sign in

to Azure Stack Hub. The customer subscription ID is case sensitive.

resourceGroup The resource group in Azure in which your registration is stored.

registrationName The name of the registration of your Azure Stack Hub. It's an object

stored in Azure. The name is usually in the form azurestack-CloudID,

where CloudID is the cloud ID of your Azure Stack Hub deployment.

Use the New-AzResource cmdlet to add a tenant. Connect to Azure, and then from

an elevated prompt run the following command:

PowerShell

Operation: PUT

RequestURI:

subscriptions/{registrationSubscriptionId}/resourceGroups/{resourceGroup}/providers

/Microsoft.AzureStack/registrations/{registrationName}/customerSubscriptions/{custo

７ Note

Tenants must be registered with each Azure Stack Hub deployment that they use. If

a tenant uses more than one Azure Stack Hub, update the initial registrations of

each deployment with the tenant subscription.

PowerShell

Az modules

New-AzResource -ResourceId

"subscriptions/{registrationSubscriptionId}/resourceGroups/{resourceGrou

p}/providers/Microsoft.AzureStack/registrations/{registrationName}/custo

merSubscriptions/{customerSubscriptionId}" -ApiVersion 2017-06-01

API call

merSubscriptionId}?api-version=2017-06-01 HTTP/1.1

Response: 201 Created

Response Body: Empty

Get a list of all tenants that have been added to a registration.

Parameter Description

registrationSubscriptionId The Azure subscription that was used for the initial registration.

resourceGroup The resource group in Azure in which your registration is stored.

registrationName The name of the registration of your Azure Stack Hub deployment.

It's an object stored in Azure. The name is usually in the form of

azurestack-CloudID, where CloudID is the cloud ID of your Azure

Stack Hub deployment.

Use the Get-AzResource cmdlet to list all registered tenants. Connect to Azure

Stack Hub, and then from an elevated prompt run the following cmdlet:

PowerShell

List all registered tenants

７ Note

If no tenants have been registered, you won't receive a response.

Parameters

PowerShell

Az modules

Get-AzResource -ResourceId

"subscriptions/{registrationSubscriptionId}/resourceGroups/{resourceGrou

p}/providers/Microsoft.AzureStack/registrations/{registrationName}/custo

merSubscriptions" -ApiVersion 2017-06-01

API call

You can get a list of all tenant mappings using the GET operation.

Operation: GET

RequestURI:

subscriptions/{registrationSubscriptionId}/resourceGroups/{resourceGroup}/providers

/Microsoft.AzureStack/registrations/{registrationName}/customerSubscriptions?apiversion=2017-06-01 HTTP/1.1

Response: 200

Response Body:

JSON

You can remove a tenant that has been added to a registration. If that tenant is still

using resources on Azure Stack Hub, their usage is charged to the subscription used in

the initial Azure Stack Hub registration.

Parameter Description

registrationSubscriptionId Subscription ID for the registration.

{

"value": [{

"id": "

subscriptions/{subscriptionId}/resourceGroups/{resourceGroup}/providers/Micr

osoft.AzureStack/registrations/{registrationName}/customerSubscriptions/{

cspSubscriptionId 1}",

"name": " cspSubscriptionId 1",

"type": "Microsoft.AzureStack\customerSubscriptions",

"properties": { "tenantId": "tId1" }

},

{

"id": "

subscriptions/{subscriptionId}/resourceGroups/{resourceGroup}/providers/Micr

osoft.AzureStack/registrations/{registrationName}/customerSubscriptions/{

cspSubscriptionId 2}",

"name": " cspSubscriptionId2 ",

"type": "Microsoft.AzureStack\customerSubscriptions",

"properties": { "tenantId": "tId2" }

}

],

"nextLink": "{originalRequestUrl}?$skipToken={opaqueString}"

}

Remove a tenant mapping

Parameters

Parameter Description

resourceGroup The resource group for the registration.

registrationName The name of the registration.

customerSubscriptionId The customer subscription ID. The customer subscription ID is case

sensitive.

Use the Remove-AzResource cmdlet to remove a tenant. Connect to Azure Stack

Hub, and then from an elevated prompt run the following cmdlet:

PowerShell

You can remove tenant mappings using the DELETE operation.

Operation: DELETE

RequestURI:

subscriptions/{registrationSubscriptionId}/resourceGroups/{resourceGroup}/providers

/Microsoft.AzureStack/registrations/{registrationName}/customerSubscriptions/{custo

merSubscriptionId}?api-version=2017-06-01 HTTP/1.1

Response: 204 No Content

Response Body: Empty

How to retrieve resource usage information from Azure Stack Hub

PowerShell

Az modules

Remove-AzResource -ResourceId

"subscriptions/{registrationSubscriptionId}/resourceGroups/{resourceGrou

p}/providers/Microsoft.AzureStack/registrations/{registrationName}/custo

merSubscriptions/{customerSubscriptionId}" -ApiVersion 2017-06-01

API call

Next steps

Report Azure Stack Hub usage data to

Azure

Article • 11/10/2022

Usage data, also called consumption data, represents the amount of resources used.

Azure Stack Hub multi-node systems that use the consumption-based billing model

should report usage data to Azure for billing purposes. Azure Stack Hub operators

should configure their Azure Stack Hub instance to report usage data to Azure.

Usage data reporting is required for Azure Stack Hub multi-node users who license

under the pay-as-you-use model. It is optional for customers who license under the

capacity model (see How to buy ). For Azure Stack Development Kit (ASDK) users,

Azure Stack Hub operators can report usage data and test the feature. However, users

won't be charged for any usage they incur.

Usage data is sent from Azure Stack Hub to Azure through the Azure Bridge. In Azure,

the commerce system processes the usage data and generates the bill. After the bill is

generated, the Azure subscription owner can view and download it from the Azure

Account Center . To learn about how Azure Stack Hub is licensed, see Azure Stack Hub

packaging and pricing .

） Important

All workloads must be deployed under tenant subscriptions to comply with the

licensing terms of Azure Stack Hub.

To set up usage data reporting, you must register your Azure Stack Hub instance with

Azure. As part of the registration process, the Azure Bridge component of Azure Stack

Hub is configured. The Azure Bridge component is what connects Azure Stack Hub to

Azure. The following usage data is sent from Azure Stack Hub to Azure:

Meter ID - Unique ID for the resource that was consumed.

Quantity - Amount of resource usage.

Location - Location where the current Azure Stack Hub resource is deployed.

Resource URI - Fully qualified URI of the resource for which usage is being

reported.

Subscription ID - Subscription ID of the Azure Stack Hub user, which is the local

(Azure Stack Hub) subscription.

Time - Start and end time of the usage data. There is some delay between the time

when these resources are consumed in Azure Stack Hub and when the usage data

is reported to commerce. Azure Stack Hub aggregates usage data for every 24

hours, and reporting usage data to the commerce pipeline in Azure takes another

few hours. Therefore, usage that happens shortly before midnight can appear in

Azure the following day.

To test usage data reporting, create a few resources in Azure Stack Hub. For

example, you can create a storage account, Windows Server VM, and a Linux VM

with Basic and Standard SKUs to see how core usage is reported. The usage data

for different types of resources are reported under different meters.

Leave your resources running for a few hours. Usage information is collected

approximately once every hour. After collecting, this data is transmitted to Azure

and processed into the Azure commerce system. This process can take up to a few

hours.

If you registered your Azure Stack Hub using a CSP subscription, you can view your

usage and charges in the same way you view Azure consumption. Azure Stack Hub

usage is included in your invoice and in the reconciliation file, which is available through

the Partner Center . The reconciliation file is updated monthly. If you need to access

recent Azure Stack Hub usage information, you can use the Partner Center APIs.

Set up usage data reporting

Generate usage data reporting

View usage - CSP subscriptions

If you registered your Azure Stack Hub using an Enterprise Agreement subscription, you

can view your usage and charges in the Azure portal cost management and billing

overview blade .

If you registered your Azure Stack Hub using any other subscription type (for example, a

pay-as-you-go subscription), you can view usage and charges in the Azure Account

Center. Sign in to the Azure Account Center as the Azure account administrator and

select the Azure subscription that you used to register Azure Stack Hub. You can view

the Azure Stack Hub usage data and the amount charged for each of the used

resources, as shown in the following image:

View usage - Enterprise Agreement

subscriptions

View usage - other subscriptions

For the ASDK, Azure Stack Hub resources are not charged, so the price shown is $0.00.

Resource usage is free for the ASDK. Azure Stack Hub multi-node systems, workload

VMs, storage services, and App Services are charged.

No. Usage data for some Azure Stack Hub resource provider VMs are reported to Azure,

but there are no charges for these VMs, nor for the VMs created during deployment to

enable the Azure Stack Hub infrastructure.

Which Azure Stack Hub deployments are

charged?

Are users charged for the infrastructure VMs?

Users are only charged for VMs that run under tenant subscriptions. All workloads must

be deployed under tenant subscriptions to comply with the licensing terms of Azure

Stack Hub.

Using the existing licenses avoids generating usage meters. Existing Windows Server

licenses can be used in Azure Stack Hub. This process is described in the "Using existing

software with Azure Stack Hub" section of the Azure Stack Hub Licensing Guide . In

order to use their existing licenses, customers must deploy their Windows Server VMs as

described in Hybrid benefit for Windows Server license.

The subscription that's provided when registering Azure Stack Hub with Azure is

charged.

For Azure Stack Hub multi-node, Enterprise Agreement (EA) and CSP subscriptions are

supported. For the ASDK, Enterprise Agreement (EA), pay-as-you-go, CSP, and MSDN

subscriptions support usage data reporting.

In the ASDK, usage data reporting requires subscriptions that are created in the global

Azure system. Subscriptions created in one of the sovereign clouds (the Azure

Government, Azure Germany, and Azure China 21Vianet clouds) cannot be registered

with Azure, so they don't support usage data reporting.

I have a Windows Server license I want to use

on Azure Stack Hub, how do I do it?

Which subscription is charged for the resources

consumed?

What types of subscriptions are supported for

usage data reporting?

Does usage data reporting work in sovereign

clouds?

Why doesn't the usage reported in Azure Stack

Hub match the report generated from Azure

There is always a delay between the usage data reported by the Azure Stack Hub usage

APIs and the usage data reported in the Azure Account Center. This delay is the time

required to upload usage data from Azure Stack Hub to Azure commerce. Because of

this delay, usage that occurs shortly before midnight might appear in Azure the

following day. If you use the Azure Stack Hub usage APIs and compare the results to the

usage reported in the Azure billing portal, you can see a difference.

Provider usage API

Tenant usage API

Usage FAQ

Manage usage and billing as a Cloud Solution Provider

Account Center?

Next steps

Usage reporting infrastructure for Cloud

Solution Providers

Article • 10/11/2021

Azure Stack Hub includes the infrastructure needed to track usage as it occurs and

forwards it to Azure. In Azure, Azure Commerce processes the usage data and charges

usage to the appropriate Azure subscriptions. This process works in the same way as

usage tracking in the global Azure cloud.

Some concepts are consistent between global Azure and Azure Stack Hub. Azure Stack

Hub has local subscriptions, which fulfill a similar role to an Azure subscription. Local

subscriptions are only valid locally. Local subscriptions are mapped to Azure

subscriptions when usage is forwarded to Azure.

Azure Stack Hub has local usage meters. Local usage is mapped to the meters used in

Azure commerce. However, the meter IDs are different. There are more meters available

locally than the one Microsoft uses for billing.

There are some differences between how services are priced in Azure Stack Hub and

Azure. For example, in Azure Stack Hub, the charge for VMs is only based on

vcore/hours, with the same rate for all VM series, unlike Azure. The reason is that in

global Azure the different prices reflect different hardware. In Azure Stack Hub, the

customer provides the hardware, so there's no reason to charge different rates for

different VM classes.

You can find out about the Azure Stack Hub meters used in Commerce and their prices

in Partner Center. The process is the same as it is for Azure services:

1. In Partner Center, go to the Dashboard menu, then select Sell, then select Pricing

and offers.

2. Under Usage-based services, select Current.

3. Open the Azure in Global CSP price list spreadsheet.

4. Filter on Region = Azure Stack Hub.

The following terms and concepts are used for usage and billing in Azure Stack Hub:

Term Definition

Terms used for billing and usage

Term Definition

Direct

CSP

partner

A direct CSP partner receives an invoice directly from Microsoft for Azure and Azure

Stack Hub usage, and bills customers directly.

Indirect

CSP

Indirect resellers work with an indirect provider (also known as a distributor). The

resellers recruit end customers; the indirect provider holds the billing relationship with

Microsoft, manages customer billing, and provides additional services like product

support.

End

customer

End customers are the businesses and government agencies that own the apps and

other workloads that run on Azure Stack Hub.

To learn more about the CSP program, see the Microsoft Cloud Solution Provider

program information.

To learn more about how to retrieve resource usage information from Azure Stack

Hub, see Usage and billing in Azure Stack Hub.

Next steps

Provider resource usage API

Article • 10/11/2021

The term provider applies to the service administrator and to any delegated providers. Azure Stack Hub

operators and delegated providers can use the provider usage API to view the usage of their direct

tenants. For example, as shown in the following diagram, P0 can call the provider API to get direct

usage information on P1 and P2, and P1 can call for usage information on P3 and P4.

The request gets consumption details for the requested subscriptions and for the requested time

frame. There is no request body.

This usage API is a provider API, so the caller must be assigned an Owner, Contributor, or Reader role

in the provider's subscription.

Method Request URI

GET https://{armendpoint}/subscriptions/{subId}/providers/Microsoft.Commerce.Admin/subscriberUsageAggregates?

reportedStartTime={reportedStartTime}&reportedEndTime={reportedEndTime}&aggregationGranularity=

{granularity}&subscriberId={sub1.1}&api-version=2015-06-01-preview&continuationToken={token-value}

API call reference

Request

Arguments

Argument Description

armendpoint Azure Resource Manager endpoint of your Azure Stack Hub environment. The Azure

Stack Hub convention is that the name of the Azure Resource Manager endpoint is in

the format https://adminmanagement.{domain-name} . For example, for the Azure Stack

Development Kit (ASDK), if the domain name is local.azurestack.external, then the

Resource Manager endpoint is https://adminmanagement.local.azurestack.external .

subId Subscription ID of the user who makes the call.

reportedStartTime Start time of the query. The value for DateTime should be in Coordinated Universal Time

(UTC) and at the beginning of the hour; for example, 13:00. For daily aggregation, set

this value to UTC midnight. The format is escaped ISO 8601; for example, 2015-06-

16T18%3a53%3a11%2b00%3a00Z , where the colon is escaped to %3a and the plus is escaped

to %2b so that it's URI-friendly.

reportedEndTime End time of the query. The constraints that apply to reportedStartTime also apply to this

argument. The value for reportedEndTime can't be either in the future, or the current

date. If it is, the result is set to "processing not complete."

aggregationGranularity Optional parameter that has two discrete potential values: daily and hourly. As the

values suggest, one returns the data in daily granularity, and the other is an hourly

resolution. The daily option is the default.

subscriberId Subscription ID. To get filtered data, the subscription ID of a direct tenant of the

provider is required. If no subscription ID parameter is specified, the call returns usage

data for all the provider's direct tenants.

api-version Version of the protocol that's used to make this request. This value is set to 2015-06-01-

preview .

continuationToken Token retrieved from the last call to the usage API provider. This token is needed when a

response is greater than 1,000 lines. It acts as a bookmark for the progress. If the token

isn't present, the data is retrieved from the beginning of the day or hour, based on the

granularity passed in.

HTTP

JSON

Response

GET

/subscriptions/sub1/providers/Microsoft.Commerce.Admin/subscriberUsageAggregates?

reportedStartTime=reportedStartTime=2014-05-

01T00%3a00%3a00%2b00%3a00&reportedEndTime=2015-06-

01T00%3a00%3a00%2b00%3a00&aggregationGranularity=Daily&subscriberId=sub1.1&api-version=1.0

{

"value": [

{

"id":

"/subscriptions/sub1.1/providers/Microsoft.Commerce.Admin/UsageAggregate/sub1.1-

meterID1",

Argument Description

id Unique ID of the usage aggregate.

name Name of the usage aggregate.

type Resource definition.

subscriptionId Subscription identifier of the Azure Stack Hub user.

usageStartTime UTC start time of the usage bucket to which this usage aggregate belongs.

usageEndTime UTC end time of the usage bucket to which this usage aggregate belongs.

instanceData Key-value pairs of instance details (in a new format):

resourceUri : Fully qualified resource ID, which includes the resource groups and the instance

name.

location : Region in which this service was run.

tags : Resource tags that are specified by the user.

additionalInfo : More details about the resource that was consumed; for example, the OS

version or image type.

quantity Amount of resource consumption that occurred in this time frame.

meterId Unique ID for the resource that was consumed (also called ResourceID ).

To generate the usage data, you should have resources that are running and actively using the system;

for example, an active virtual machine (VM), or a storage account containing some data. If you're not

sure whether you have any resources running in the Azure Stack Hub Marketplace, deploy a VM, and

"name": "sub1.1-meterID1",

"type": "Microsoft.Commerce.Admin/UsageAggregate",

"properties": {

"subscriptionId":"sub1.1",

"usageStartTime": "2015-03-03T00:00:00+00:00",

"usageEndTime": "2015-03-04T00:00:00+00:00",

"instanceData":"{\"Microsoft.Resources\":

{\"resourceUri\":\"resourceUri1\",\"location\":\"Alaska\",\"tags\":null,\"additionalInfo\"

:null}}",

"quantity":2.4000000000,

"meterId":"meterID1"

}

},

. . .

Response details

Retrieve usage information

PowerShell

verify the VM monitoring blade to make sure it's running. Use the following PowerShell cmdlets to view

the usage data:

1. Install PowerShell for Azure Stack Hub.

2. Configure the Azure Stack Hub user or the Azure Stack Hub operator PowerShell environment.

3. To retrieve the usage data, call the Get-AzsSubscriberUsage PowerShell cmdlet:

PowerShell

You can collect usage information for deleted subscriptions by calling the Microsoft.Commerce.Admin

service.

Method Request URI

GET https://{armendpoint}/subscriptions/{subId}/providers/Microsoft.Commerce.Admin/subscriberUsageAggregates?

reportedStartTime={start-time}&reportedEndTime={end-endtime}&aggregationGranularity=Hourly&apiversion=2015-06-01-preview

Method Request URI

GET https://{armendpoint}/subscriptions/{subId}/providers/Microsoft.Commerce.Admin/subscriberUsageAggregates?

reportedStartTime={start-time}&reportedEndTime={end-endtime}&aggregationGranularity=Hourly&subscriberId=

{subscriber-id}&api-version=2015-06-01-preview

Tenant resource usage API reference

Usage-related FAQ

Get-AzsSubscriberUsage -ReportedStartTime "2017-09-06T00:00:00Z" -ReportedEndTime

"2017-09-07T00:00:00Z"

REST API

Return all tenant usage for deleted for active users

Return usage for deleted or active tenant

Next steps

Tenant resource usage API reference

Article • 07/21/2021

A tenant can use the tenant APIs to view the tenant's own resource usage data. These

APIs are consistent with the Azure usage APIs.

You can use the Windows PowerShell cmdlet Get-UsageAggregates to get usage data,

just like in Azure.

The request gets consumption details for the requested subscriptions and for the

requested time frame. There is no request body.

Method Request URI

GET https://{armendpoint}/subscriptions/{subId}/providers/Microsoft.Commerce/usageAggregates?

reportedStartTime={reportedStartTime}&reportedEndTime=

{reportedEndTime}&aggregationGranularity={granularity}&api-version=2015-06-01-

preview&continuationToken={token-value}

Parameter Description

Armendpoint Azure Resource Manager endpoint of your Azure Stack Hub

environment. The Azure Stack Hub convention is that the name of Azure

Resource Manager endpoint is in the format https://management.

{domain-name} . For example, for the development kit, the domain name

is local.azurestack.external, then the Resource Manager endpoint is

https://management.local.azurestack.external .

subId Subscription ID of the user who is making the call. You can use this API

only to query for a single subscription's usage. Providers can use the

provider resource usage API to query usage for all tenants.

reportedStartTime Start time of the query. The value for DateTime should be in UTC and at

the beginning of the hour; for example, 13:00. For daily aggregation, set

this value to UTC midnight. The format is escaped ISO 8601; for

example, 2015-06-16T18%3a53%3a11%2b00%3a00Z, where colon is

escaped to %3a and plus is escaped to %2b so that it's URI friendly.

API call

Request

Parameters

Parameter Description

reportedEndTime End time of the query. The constraints that apply to reportedStartTime

also apply to this parameter. The value for reportedEndTime can't be in

the future.

aggregationGranularity Optional parameter that has two discrete potential values: daily and

hourly. As the values suggest, one returns the data in daily granularity,

and the other is an hourly resolution. The daily option is the default.

api-version Version of the protocol that's used to make this request. You must use

2015-06-01-preview.

continuationToken Token retrieved from the last call to the usage API provider. This token

is needed when a response is greater than 1,000 lines. It acts as a

bookmark for progress. If not present, the data is retrieved from the

beginning of the day or hour, based on the granularity passed in.

HTML

JSON

Response

GET

/subscriptions/sub1/providers/Microsoft.Commerce/UsageAggregates?

reportedStartTime=reportedStartTime=2014-05-

01T00%3a00%3a00%2b00%3a00&reportedEndTime=2015-06-

01T00%3a00%3a00%2b00%3a00&aggregationGranularity=Daily&api-version=1.0

{

"value": [

{

"id":

"/subscriptions/sub1/providers/Microsoft.Commerce/UsageAggregate/sub1-

meterID1",

"name": "sub1-meterID1",

"type": "Microsoft.Commerce/UsageAggregate",

"properties": {

"subscriptionId":"sub1",

"usageStartTime": "2015-03-03T00:00:00+00:00",

"usageEndTime": "2015-03-04T00:00:00+00:00",

"instanceData":"{\"Microsoft.Resources\":

{\"resourceUri\":\"resourceUri1\",\"location\":\"Alaska\",\"tags\":null,\"ad

ditionalInfo\":null}}",

"quantity":2.4000000000,

"meterId":"meterID1"

Parameter Description

id Unique ID of the usage aggregate.

name Name of the usage aggregate.

type Resource definition.

subscriptionId Subscription identifier of the Azure user.

usageStartTime UTC start time of the usage bucket to which this usage aggregate belongs.

usageEndTime UTC end time of the usage bucket to which this usage aggregate belongs.

instanceData Key-value pairs of instance details (in a new format):

resourceUri: Fully qualified resource ID, including resource groups and instance

name.

location: Region in which this service was run.

tags: Resource tags that the user specifies.

additionalInfo: More details about the resource that was consumed. For

example, OS version or image type.

quantity Amount of resource consumption that occurred in this time frame.

meterId Unique ID for the resource that was consumed (also called ResourceID).

Provider resource usage API

Usage-related FAQ

}

},

...

Response details

Next steps

Frequently asked questions about

Azure Stack Hub usage

FAQ

This article answers some frequently asked questions about Azure Stack Hub usage and

the Azure Stack Hub usage API.

Usage is reported for the following resource providers:

Meter ID: F271A8A388C44D93956A063E1D2FA80B

Meter name: Static IP Address Usage

Unit: IP addresses

Notes: Count of IP addresses used. If you call the usage API with a daily granularity, the

meter returns IP address multiplied by the number of hours.

Meter ID: 9E2739BA86744796B465F64674B822BA

Meter name: Dynamic IP Address Usage

Unit: IP addresses

Notes: Count of IP addresses used. If you call the usage API with a daily granularity, the

meter returns IP address multiplied by the number of hours.

Meter ID: B4438D5D-453B-4EE1-B42A-DC72E377F1E4

Meter name: TableCapacity

Unit: GB\*hours

Notes: Total capacity consumed by tables.

Meter ID: B5C15376-6C94-4FDD-B655-1A69D138ACA3

Meter name: PageBlobCapacity

Unit: GB\*hours

Notes: Total capacity consumed by page blobs.

Meter ID: B03C6AE7-B080-4BFA-84A3-22C800F315C6

Meter name: QueueCapacity

What meter IDs can I see?

Network

Storage

Unit: GB\*hours

Notes: Total capacity consumed by queue.

Meter ID: 09F8879E-87E9-4305-A572-4B7BE209F857

Meter name: BlockBlobCapacity

Unit: GB\*hours

Notes: Total capacity consumed by block blobs.

Meter ID: B9FF3CD0-28AA-4762-84BB-FF8FBAEA6A90

Meter name: TableTransactions

Unit: Request count in 10,000s

Notes: Table service requests (in 10,000s).

Meter ID: 50A1AEAF-8ECA-48A0-8973-A5B3077FEE0D

Meter name: TableDataTransIn

Unit: Ingress data in GB

Notes: Table service data ingress in GB.

Meter ID: 1B8C1DEC-EE42-414B-AA36-6229CF199370

Meter name: TableDataTransOut

Unit: Egress in GB

Notes: Table service data egress in GB.

Meter ID: 43DAF82B-4618-444A-B994-40C23F7CD438

Meter name: BlobTransactions

Unit: Requests count in 10,000s

Notes: Blob service requests (in 10,000s).

Meter ID: 9764F92C-E44A-498E-8DC1-AAD66587A810

Meter name: BlobDataTransIn

Unit: Ingress data in GB

Notes: Blob service data ingress in GB.

Meter ID: 3023FEF4-ECA5-4D7B-87B3-CFBC061931E8

Meter name: BlobDataTransOut

Unit: Egress in GB

Notes: Blob service data egress in GB.

Meter ID: EB43DD12-1AA6-4C4B-872C-FAF15A6785EA

Meter name: QueueTransactions

Unit: Requests count in 10,000s

Notes: Queue service requests (in 10,000s).

Meter ID: E518E809-E369-4A45-9274-2017B29FFF25

Meter name: QueueDataTransIn

Unit: Ingress data in GB

Notes: Queue service data ingress in GB.

Meter ID: DD0A10BA-A5D6-4CB6-88C0-7D585CEF9FC2

Meter name: QueueDataTransOut

Unit: Egress in GB

Notes: Queue service data egress in GB.

Meter ID: FAB6EB84-500B-4A09-A8CA-7358F8BBAEA5

Meter name: Base VM Size Hours

Unit: Virtual core hours

Notes: Number of virtual cores multiplied by the hours the VM ran.

Meter ID: 9CD92D4C-BAFD-4492-B278-BEDC2DE8232A

Meter name: Windows VM Size Hours

Unit: Virtual core hours

Notes: Number of virtual cores multiplied by hours the VM ran.

Meter ID: 6DAB500F-A4FD-49C4-956D-229BB9C8C793

Meter name: VM size hours

Unit: VM hours

Notes: Captures both base and Windows VM. Doesn't adjust for cores.

Meter ID: 380874f9-300c-48e0-95a0-d2d9a21ade8f Meter name: S4 Unit: Count of

Disks\*month Notes: Standard Managed Disk - 32 GB

Meter ID: 1b77d90f-427b-4435-b4f1-d78adec53222 Meter name: S6 Unit: Count of

Disks\*month Notes: Standard Managed Disk - 64 GB

Meter ID: d5f7731b-f639-404a-89d0-e46186e22c8d Meter name: S10 Unit: Count of

Disks\*month Notes: Standard Managed Disk - 128 GB

Meter ID: ff85ef31-da5b-4eac-95dd-a69d6f97b18a Meter name: S15 Unit: Count of

Disks\*month Notes: Standard Managed Disk - 256 GB

Meter ID: 88ea9228-457a-4091-adc9-ad5194f30b6e Meter name: S20 Unit: Count of

Disks\*month Notes: Standard Managed Disk - 512 GB

Compute

Managed Disks

Meter ID: 5b1db88a-8596-4002-8052-347947c26940 Meter name: S30 Unit: Count of

Disks\*month Notes: Standard Managed Disk - 1024 GB

Meter ID: 7660b45b-b29d-49cb-b816-59f30fbab011 Meter name: P4 Unit: Count of

Disks\*month Notes: Premium Managed Disk - 32 GB

Meter ID: 817007fd-a077-477f-bc01-b876f27205fd Meter name: P6 Unit: Count of

Disks\*month Notes: Premium Managed Disk - 64 GB

Meter ID: e554b6bc-96cd-4938-a5b5-0da990278519 Meter name: P10 Unit: Count of

Disks\*month Notes: Premium Managed Disk - 128 GB

Meter ID: cdc0f53a-62a9-4472-a06c-e99a23b02907 Meter name: P15 Unit: Count of

Disks\*month Notes: Premium Managed Disk - 256 GB

Meter ID: b9cb2d1a-84c2-4275-aa8b-70d2145d59aa Meter name: P20 Unit: Count of

Disks\*month Notes: Premium Managed Disk - 512 GB

Meter ID: 06bde724-9f94-43c0-84c3-d0fc54538369 Meter name: P30 Unit: Count of

Disks\*month Notes: Premium Managed Disk - 1024 GB

Meter ID: 7ba084ec-ef9c-4d64-a179-7732c6cb5e28 Meter name:

ActualStandardDiskSize Unit: GB\*month Notes: The actual size on disk of standard

managed disk.

Meter ID: daef389a-06e5-4684-a7f7-8813d9f792d5

Meter name: ActualPremiumDiskSize Unit: GB\*month Notes: The actual size on disk of

premium managed disk.

Meter ID: 108fa95b-be0d-4cd9-96e8-5b0d59505df1

Meter name: ActualStandardSnapshotSize Unit: GB\*month Notes: The actual size on

disk of managed standard snapshot.

Meter ID: 578ae51d-4ef9-42f9-85ae-42b52d3d83ac Meter name:

ActualPremiumSnapshotSize Unit: GB\*month Notes: The actual size on disk of managed

premium snapshot.

Meter ID: 5d76e09f-4567-452a-94cc-7d1f097761f0 Meter name: S4 Unit: Count of

Disks\*hours Notes: Standard Managed Disk - 32 GB (Deprecated)

Meter ID: dc9fc6a9-0782-432a-b8dc-978130457494 Meter name: S6 Unit: Count of

Disks\*hours Notes: Standard Managed Disk - 64 GB (Deprecated)

Meter ID: e5572fce-9f58-49d7-840c-b168c0f01fff Meter name: S10 Unit: Count of

Disks\*hours Notes: Standard Managed Disk - 128 GB (Deprecated)

Meter ID: 9a8caedd-1195-4cd5-80b4-a4c22f9302b8 Meter name: S15 Unit: Count of

Disks\*hours Notes: Standard Managed Disk - 256 GB (Deprecated)

Meter ID: 5938f8da-0ecd-4c48-8d5a-c7c6c23546be Meter name: S20 Unit: Count of

Disks\*hours Notes: Standard Managed Disk - 512 GB (Deprecated)

Meter ID: 7705a158-bd8b-4b2b-b4c2-0782343b81e6 Meter name: S30 Unit: Count of

Disks\*hours Notes: Standard Managed Disk - 1024 GB (Deprecated)

Meter ID: 5c105f5f-cbdf-435c-b49b-3c7174856dcc Meter name: P4 Unit: Count of

Disks\*hours Notes: Premium Managed Disk - 32 GB (Deprecated)

Meter ID: 518b412b-1927-4f25-985f-4aea24e55c4f Meter name: P6 Unit: Count of

Disks\*hours Notes: Premium Managed Disk - 64 GB (Deprecated)

Meter ID: 5cfb1fed-0902-49e3-8217-9add946fd624 Meter name: P10 Unit: Count of

Disks\*hours Notes: Premium Managed Disk - 128 GB (Deprecated)

Meter ID: 8de91c94-f740-4d9a-b665-bd5974fa08d4 Meter name: P15

Unit: Count of Disks\*hours Notes: Premium Managed Disk - 256 GB (Deprecated)

Meter ID: c7e7839c-293b-4761-ae4c-848eda91130b Meter name: P20 Unit: Count of

Disks\*hours Notes: Premium Managed Disk - 512 GB (Deprecated)

Meter ID: 9f502103-adf4-4488-b494-456c95d23a9f Meter name: P30 Unit: Count of

Disks\*hours Notes: Premium Managed Disk - 1024 GB (Deprecated)

Meter ID: 8a409390-1913-40ae-917b-08d0f16f3c38 Meter name:

ActualStandardDiskSize Unit: Byte\*hours Notes: The actual size on disk of standard

managed disk (Deprecated).

Meter ID: 1273b16f-8458-4c34-8ce2-a515de551ef6

Meter name: ActualPremiumDiskSize Unit: Byte\*hours Notes: The actual size on disk of

premium managed disk (Deprecated).

Meter ID: 89009682-df7f-44fe-aeb1-63fba3ddbf4c

Meter name: ActualStandardSnapshotSize Unit: Byte\*hours Notes: The actual size on

disk of managed standard snapshot (Deprecated).

Meter ID: 95b0c03f-8a82-4524-8961-ccfbf575f536 Meter name:

ActualPremiumSnapshotSize Unit: Byte\*hours Notes: The actual size on disk of

managed premium snapshot (Deprecated).

Meter ID: 75d4b707-1027-4403-9986-6ec7c05579c8 Meter name:

ActualStandardSnapshotSize Unit: GB\*month Notes: The actual size on disk of managed

standard snapshot (Deprecated).

Meter ID: 5ca1cbb9-6f14-4e76-8be8-1ca91547965e Meter name:

ActualPremiumSnapshotSize Unit: GB\*month Notes: The actual size on disk of managed

premium snapshot (Deprecated).

Meter ID: CBCFEF9A-B91F-4597-A4D3-01FE334BED82

Meter name: DatabaseSizeHourSqlMeter

Unit: MB\*hours

Notes: Total DB capacity at creation. If you call the usage API with a daily granularity, the

meter returns MB multiplied by the number of hours.

Meter ID: E6D8CFCD-7734-495E-B1CC-5AB0B9C24BD3

Meter name: DatabaseSizeHourMySqlMeter

Unit: MB\*hours

Notes: Total DB capacity at creation. If you call the usage API with a daily granularity, the

meter returns MB multiplied by the number of hours.

Meter ID: CB6A35C5-FADE-406C-B14D-6DDB7C4CA3D5

Meter name: 1 Core

Unit: Core\*hours

Notes: Unit represents the number of cores per hour used by deployed Event Hubs

clusters. Numbers of cores are in multiples of 10 because each configured CU uses 10

cores.

Meter ID: EBF13B9F-B3EA-46FE-BF54-396E93D48AB4

Meter name: Key Vault transactions

Unit: Request count in 10,000s

Notes: Number of REST API requests received by Key Vault data plane.

Meter ID: 2C354225-B2FE-42E5-AD89-14F0EA302C87

Meter name: Advanced keys transactions

Sql RP

MySql RP

Event Hubs

Key Vault

Unit: 10K transactions

Notes: RSA 3K/4K, ECC key transactions (preview).

Meter ID: 190C935E-9ADA-48FF-9AB8-56EA1CF9ADAA

Meter name: App Service

Unit: Virtual core hours

Notes: Number of virtual cores used to run app service.

Meter ID: 67CC4AFC-0691-48E1-A4B8-D744D1FEDBDE

Meter name: Functions Requests

Unit: 10 Requests

Notes: Total number of requested executions (per 10 executions). Executions are

counted each time a function runs in response to an event, or is triggered by a binding.

Meter ID: D1D04836-075C-4F27-BF65-0A1130EC60ED

Meter name: Functions - Compute

Unit: GB-s

Notes: Resource consumption measured in gigabyte seconds (GB/s). Observed resource

consumption is calculated by multiplying average memory size in GB by the time in

milliseconds it takes to execute the function. Memory used by a function is measured by

rounding up to the nearest 128 MB, up to the maximum memory size of 1,536 MB, with

execution time calculated by rounding up to the nearest 1 ms. The minimum execution

time and memory for a single function execution is 100 ms and 128 mb respectively.

Meter ID: 957E9F36-2C14-45A1-B6A1-1723EF71A01D

Meter name: Shared App Service Hours

Unit: 1 hour Notes: Per hour usage of shard App Service Plan. Plans are metered on a

per App basis.

Meter ID: 539CDEC7-B4F5-49F6-AAC4-1F15CFF0EDA9

Meter name: Free App Service Hours

Unit: 1 hour Notes: Per hour usage of free App Service Plan. Plans are metered on a per

App basis.

App service

７ Note

Microsoft uses this meter to charge the App Service on Azure Stack Hub. Cloud

Solution Providers can use the other App Service meters (below) to calculate usage

for their tenants.

Meter ID: 88039D51-A206-3A89-E9DE-C5117E2D10A6

Meter name: Small Standard App Service Hours

Unit: 1 hour Notes: Calculated based on size and number of instances.

Meter ID: 83A2A13E-4788-78DD-5D55-2831B68ED825

Meter name: Medium Standard App Service Hours

Unit: 1 hour Notes: Calculated based on size and number of instances.

Meter ID: 1083B9DB-E9BB-24BE-A5E9-D6FDD0DDEFE6

Meter name: Large Standard App Service Hours

Unit: 1 hour Notes: Calculated based on size and number of instances.

Meter ID: Custom Worker Tiers Meter name: Custom Worker Tiers

Unit: Hours Notes: Deterministic meter ID is created based on SKU and custom worker

tier name. This meter ID is unique for each custom worker tier.

Meter ID: 264ACB47-AD38-47F8-ADD3-47F01DC4F473

Meter name: SNI SSL

Unit: Per SNI SSL Binding

Notes: App Service supports two types of SSL connections: Server Name Indication (SNI)

SSL Connections and IP Address SSL Connections. SNI-based SSL works on modern

browsers while IP-based SSL works on all browsers.

Meter ID: 60B42D72-DC1C-472C-9895-6C516277EDB4

Meter name: IP SSL Unit: Per IP Based SSL Binding Notes: App Service supports two

types of SSL connections: Server Name Indication (SNI) SSL Connections and IP Address

SSL Connections. SNI-based SSL works on modern browsers while IP-based SSL works

on all browsers.

Meter ID: 73215A6C-FA54-4284-B9C1-7E8EC871CC5B

Meter name: Web Process Unit:

Notes: Calculated per active site per hour.

Meter ID: 5887D39B-0253-4E12-83C7-03E1A93DFFD9

Meter name: External Egress Bandwidth

Unit: GB

Notes: Total incoming request response bytes + total outgoing request bytes + total

incoming FTP request response bytes + total incoming web deploy request response

bytes.

Custom Worker Tiers

The tenant usage API is consistent with the Azure API, with one exception: the

showDetails flag currently isn't supported in Azure Stack Hub.

The provider usage API applies only to Azure Stack Hub.

Currently, the RateCard API that is available in Azure isn't available in Azure Stack

Hub.

Usage data reports have two main time values:

Reported Time: The time when the usage event entered the usage system.

Usage Time: The time when the Azure Stack Hub resource was consumed.

You might see a discrepancy in values for usage time and reported time for a specific

usage event. The delay can be as long as several hours in any environment.

Currently, you can query only by Reported Time.

HTTP

status

code

Error code Description

400/Bad

Request

NoApiVersion The api-version query parameter is

missing.

400/Bad

Request

InvalidProperty A property is missing or has an invalid

value. The message in the error code

in the response body identifies the

missing property.

How do the Azure Stack Hub usage APIs

compare to the Azure usage API

(currently in public preview)?

What is the difference between usage

time and reported time?

What do these usage API error codes

mean?

HTTP

status

code

Error code Description

400/Bad

Request

RequestEndTimeIsInFuture The value for ReportedEndTime is in the

future. Values in the future are not

allowed for this argument.

400/Bad

Request

SubscriberIdIsNotDirectTenant A provider API call has used a

subscription ID that is not a valid

tenant of the caller.

400/Bad

Request

SubscriptionIdMissingInRequest The subscription ID of the caller is

missing.

400/Bad

Request

InvalidAggregationGranularity An invalid aggregation granularity was

requested. Valid values are daily and

hourly.

503 ServiceUnavailable A retryable error occurred because the

service is busy or the call is being

throttled.

Running and stopped VMs generate usage data. Consistent with Azure, deallocation is

needed to stop the emission of usage data. In the case in which the portal is unavailable

but the compute resource provider is still running, usage will be emitted.

The easiest way to extract usage data from local usage APIs on an Azure Stack Hub is by

using the usage summary script on GitHub . The script requires the start and end dates

as input parameters.

A common scenario is to retrieve detailed information about usage billed from Azure.

Detail can be found in your Azure bill. Also, you can access the Azure commerce APIs.

For more information about the Azure commerce APIs, see Getting started with Azure in

Cloud Solution Provider .

What is the policy for charging for VMs?

How do I extract usage data from the

Azure Stack Hub usage APIs?

Alternatively, you can use the REST APIs, as explained in the Provider resource usage API

and Tenant resource usage API articles.

The usage records include a property bag called additionalinfo, which includes the

Azure Stack Hub subscription ID. This ID is the user subscription emitting the

corresponding usage record.

Customer billing and chargeback in Azure Stack Hub

Provider Resource Usage API

Tenant Resource Usage API

How can I associate usage extracted

from Azure usage APIs to a specific

Azure Stack Hub user subscription?

Next steps

Usage connectivity errors

Article • 07/21/2021

Azure Stack Hub usage data is sent to Azure by the Azure Bridge component in Azure

Stack Hub. If the bridge within Azure Stack Hub is unable to connect to the Azure usage

service, the following error appears:

The window may provide more information about the error and resolution:

To mitigate the issue, try the following steps:

Verify that network configuration allows the Azure Bridge to connect to the remote

service.

Go to the Region Management > Properties blade to find the Azure subscription

ID used for the registration, resource group, and name of the registration resource.

Verify that the registration resource exists under the correct Azure subscription ID

in Azure portal. To do so, go to All resources created under the Azure subscription

ID, and check the Show hidden types box. If you can't find the registration

resource, follow the steps in Renew or change registration to re-register your

Azure Stack Hub.

Resolve connectivity issues

This section describes the usage error codes.

Error code Issue Remediation

NetworkError Azure Stack Hub bridge is

unable to send request to

usage service endpoint in

Azure.

Check if a proxy is blocking or

intercepting access to the usage

service endpoint.

RequestTimedOut Request was sent from the

Azure Bridge but the usage

service in Azure failed to

respond within the timeout

period.

Check if a proxy is blocking or

intercepting access to the usage

service endpoint.

LoginError Unable to authenticate with

Microsoft Azure Active

Directory.

Ensure the Azure AD login endpoint

is accessible from all XRP VMs in

Azure Stack Hub.

CertificateValidationError The Azure bridge is unable to

send the request because it is

unable to authenticate with

the Azure service.

Check if there is a proxy intercepting

HTTPS traffic between the Azure

Stack Hub XRP machine and the

usage gateway endpoint.

Unauthorized The Azure bridge is unable to

push data to the usage

service in Azure, because the

Azure service is unable to

authenticate the Azure Stack

Hub bridge.

Check if the registration resource has

been modified, and if so, re-register

Azure Stack Hub.

Sometimes, a time sync issue

between Azure Stack Hub and Azure

AD can cause this failure. In this case,

ensure the times on the XRP VMs on

Azure Stack Hub are in sync with

Azure AD.

Error codes

Additionally, you may be required to provide the log files for the Azure Bridge, WAS,

and WASPublic components.

Learn more about reporting Azure Stack Hub usage data to Azure.

To review error messages if they are triggered in your registration process, see

Tenant registration error messages.

Learn more about the Usage reporting infrastructure for Cloud Solution Providers.

Next steps

Usage and billing registration error

codes

Article • 10/13/2021

If you're a Cloud Solution Provider (CSP), the following error messages can appear when

adding tenants to a registration for reporting usage against the customer's Azure

subscription ID.

Error Details Comments

RegistrationNotFound The provided

registration was not

found. Make sure the

following information

was provided correctly:

1. Subscription identifier

(value provided:

subscription identifier),

2. Resource group

(value provided:

resource group),

3. Registration name

(value provided:

registration name).

This error usually happens when

the information pointing to the

initial registration isn't correct. If

you need to verify the resource

group and name of your

registration, you can find it in the

Azure portal, by listing all

resources. If you find more than

one registration resource, look at

the CloudDeploymentID in the

properties, and select the

registration whose

CloudDeploymentID matches

that of your cloud. To find the

CloudDeploymentID, you can

use this PowerShell command on

Azure Stack Hub:

$azureStackStampInfo = InvokeCommand -Session $session -

ScriptBlock { GetAzureStackStampInformation }

List of registration error codes

Error Details Comments

BadCustomerSubscriptionId The provided customer

subscription identifier

and the registration

name subscription

identifier are not owned

by the same Microsoft

CSP. Check that the

customer subscription

identifier is correct. The

customer subscription

ID is case sensitive. If

the problem persists,

contact support.

This error happens when the

customer subscription is a CSP

subscription, but it rolls up to a

CSP partner different from the

one to which the subscription

used in the initial registration

rolls up. This check is made to

prevent a situation that would

result in billing a CSP partner

who isn't responsible for the

Azure Stack Hub used.

InvalidCustomerSubscriptionId The customer

subscription identifier

is not valid. Make sure a

valid Azure subscription

is provided.

CustomerSubscriptionNotFound Customer subscription

identifier was not found

under registration

name. Make sure a valid

Azure subscription is

being used and that the

subscription ID was

added to the

registration using the

PUT operation.

This error happens when trying

to verity that a tenant has been

added to a subscription but the

customer subscription isn't found

to be associated with the

registration. The customer hasn't

been added to the registration,

or the subscription ID has been

written incorrectly.

UnauthorizedCspRegistration The provided

registration name is

not approved to use

multi-tenancy. Send an

email to

azstCSP@microsoft.com

and include your

registration name,

resource group, and the

subscription identifier

used in the registration.

A registration must be approved

for multi-tenancy by Microsoft

before you can start adding

tenants to it.

Error Details Comments

CustomerSubscriptionsNotAllowed Customer subscription

operations aren't

supported for

disconnected

customers. To use this

feature, re-register with

pay-as-you-use

licensing.

The registration to which you're

trying to add tenants is a

capacity registration. So when

the registration was created, the

parameter BillingModel

Capacity was used. Only pay-asyou-use registrations are allowed

to add tenants. You must reregister using the parameter

BillingModel PayAsYouUse .

InvalidCSPSubscription The provided customer

subscription identifier

is not a valid CSP

subscription. Make sure

a valid Azure

subscription is

provided.

This error is most likely due to

the customer subscription being

mistyped.

MetadataResolverBadGatewayError One of the upstream

servers returned an

unexpected error. Try

again later. If the

problem persists,

contact support.

Learn more about the Usage reporting infrastructure for Cloud Solution Providers.

To learn more about the CSP program, see Cloud Solutions .

To learn more about how to retrieve resource usage information from Azure Stack

Hub, see Usage and billing in Azure Stack Hub.

Next steps

Enable backup for Azure Stack Hub

from the administrator portal

Article • 07/29/2022

You can enable the Infrastructure Backup Service from the administrator portal so that

Azure Stack Hub can generate infrastructure backups. The hardware partner can use

these backups to restore your environment using cloud recovery in the event of a

catastrophic failure. The purpose of cloud recovery is to ensure that your operators and

users can log back into the portal after recovery is complete. Users will have their

subscriptions restored, including:

Role-based access permissions and roles.

Original plans and offers.

Previously defined compute, storage, and network quotas.

Key Vault secrets.

However, the Infrastructure Backup Service doesn't back up IaaS VMs, network

configurations, and storage resources such as storage accounts, blobs, tables, and so on.

Users logging in after cloud recovery won't see any of these previously existing

resources. Platform as a Service (PaaS) resources and data are also not backed up by the

service.

Admins and users are responsible for backing up and restoring IaaS and PaaS resources

separately from the infrastructure backup processes. For info on backing up IaaS and

PaaS resources, see the following links:

Protect VMs deployed on Azure Stack Hub

Back up your app in Azure

What is SQL Server on Azure VMs? (Windows)

1. Open the Azure Stack Hub administrator portal.

2. Select All services, and then under the ADMINISTRATION category select

Infrastructure backup. Choose Configuration in the Infrastructure backup blade.

3. Type the path to the Backup storage location. Use a Universal Naming Convention

(UNC) string for the path to a file share hosted on a separate device. A UNC string

specifies the location of resources such as shared files or devices. For the service,

Enable or reconfigure backup

you can use an IP address. To ensure availability of the backup data after a disaster,

the device should be in a separate location.

4. Type the Username using the domain and username with sufficient access to read

and write files. For example, Contoso\backupshareuser .

5. Type the Password for the user.

6. Type the password again to Confirm Password.

7. The frequency in hours determines how often backups are created. The default

value is 12. Scheduler supports a maximum of 12 and a minimum of 4.

8. The retention period in days determines how many days of backups are preserved

on the external location. The default value is 7. Scheduler supports a maximum of

14 and a minimum of 2. Backups older than the retention period are automatically

deleted from the external location.

9. In Encryption Settings, provide a certificate in the Certificate .cer file box. The

certificate key length must be 2048 bytes. Backup files are encrypted using this

public key in the certificate. Provide a certificate that only contains the public key

portion when you configure backup settings. Once you set this certificate for the

first time or rotate the certificate in the future, you can only view the thumbprint of

the certificate. You can't download or view the uploaded certificate file. To create

the certificate file, run the following PowerShell command to create a self-signed

certificate with the public and private keys and export a certificate with only the

public key portion. You can save the certificate anywhere that can be accessed

from admin portal.

７ Note

If your environment supports name resolution from the Azure Stack Hub

infrastructure network to your enterprise environment, you can use a Fully

Qualified Domain Name (FQDN) rather than the IP.

７ Note

If you want to archive backups older than the retention period, make sure to

back up the files before the scheduler deletes the backups. If you reduce the

backup retention period (e.g. from 7 days to 5 days), the scheduler will delete

all backups older than the new retention period. Make sure you're OK with the

backups getting deleted before you update this value.

PowerShell

10. Select OK to save your backup controller settings.

To start a backup, click on Backup now to start an on-demand backup. An on-demand

backup won't modify the time for the next scheduled backup. After the task completes,

$cert = New-SelfSignedCertificate `

-DnsName "www.contoso.com" `

-CertStoreLocation "cert:\LocalMachine\My"

New-Item -Path "C:\" -Name "Certs" -ItemType "Directory"

Export-Certificate `

-Cert $cert `

-FilePath c:\certs\AzSIBCCert.cer

７ Note

Azure Stack Hub accepts a certificate to encrypt infrastructure backup data.

Make sure to store the certificate with the public and private key in a secure

location. For security reasons, it's not recommended that you use the

certificate with the public and private keys to configure backup settings. For

more info on how to manage the lifecycle of this certificate, see Infrastructure

Backup Service best practices.

Start backup

you can confirm the settings in Essentials:

You can also run the PowerShell cmdlet Start-AzsBackup on your Azure Stack Hub

admin computer. For more info, see Back up Azure Stack Hub.

Backups are automatically scheduled when you enable backup. You can check the next

schedule backup time in Essentials.

If you need to disable future scheduled backups, click on Disable Automatic Backups.

Disabling automatic backups keeps backup settings configured and retains the backup

schedule. This action simply tells the scheduler to skip future backups.

Confirm that future scheduled backups have been disabled in Essentials:

Enable or disable automatic backups

Click on Enable Automatic Backups to inform the scheduler to start future backups at

the scheduled time.

As of 1901, support for encryption key is deprecated. If you're configuring backup for

the first time in 1901, you must use a certificate. Azure Stack Hub supports encryption

key only if the key is configured before updating to 1901. Backward compatibility mode

will continue for three releases. After that, encryption keys will no longer be supported.

In encryption settings, if you're configuring infrastructure backup for the first time after

installing or updating to 1901, you must configure backup with a certificate. Using an

encryption key is no longer supported.

To update the certificate used to encrypt backup data, upload a new .CER file with the

public key portion and select OK to save settings.

７ Note

If you configured infrastructure backup before updating to 1807, automatic

backups will be disabled. This way the backups started by Azure Stack Hub don't

conflict with backups started by an external task scheduling engine. Once you

disable any external task scheduler, click on Enable Automatic Backups.

Update backup settings

Default mode

New backups will start to use the public key in the new certificate. There's no impact to

all existing backups created with the previous certificate. Make sure to keep the older

certificate around in a secure location in case you need it for cloud recovery.

If you configured backup before updating to 1901, the settings are carried over with no

change in behavior. In this case, the encryption key is supported for backwards

compatibility. You can update the encryption key or switch to use a certificate. You have

at least three releases to continue updating the encryption key. Use this time to

transition to a certificate. To create a new encryption key, use NewAzsEncryptionKeyBase64.

Backwards compatibility mode

７ Note

Updating from encryption key to certificate is a one-way operation. After making

this change, you can't switch back to encryption key. All existing backups will

remain encrypted with the previous encryption key.

Learn to run a backup. See Back up Azure Stack Hub.

Learn to verify that your backup ran. See Confirm backup completed in administrator

portal.

Next steps

Enable Backup for Azure Stack Hub with

PowerShell

Article • 07/29/2022

Enable the Infrastructure Backup Service with Windows PowerShell to take periodic

backups of:

Internal identity service and root certificate.

User plans, offers, subscriptions.

Compute, storage, and network user quotas.

User Key Vault secrets.

User RBAC roles and policies.

User storage accounts.

You can access the PowerShell cmdlets to enable backup, start backup, and get backup

information via the operator management endpoint.

For instructions on configuring the PowerShell environment, see Install PowerShell for

Azure Stack Hub. To sign in to Azure Stack Hub, see Configure the operator environment

and sign in to Azure Stack Hub.

In the same PowerShell session, edit the following PowerShell script by adding the

variables for your environment. Run the updated script to provide the backup share,

credentials, and encryption key to the Infrastructure Backup Service.

Variable Description

$username Type the Username using the domain and username for the shared

drive location with sufficient access to read and write files. For example,

Contoso\backupshareuser .

$password Type the Password for the user.

Prepare PowerShell environment

Provide the backup share, credentials, and

encryption key to enable backup

Variable Description

$sharepath Type the path to the Backup storage location. You must use a

Universal Naming Convention (UNC) string for the path to a file share

hosted on a separate device. A UNC string specifies the location of

resources such as shared files or devices. To ensure availability of the

backup data, the device should be in a separate location.

$frequencyInHours The frequency in hours determines how often backups are created. The

default value is 12. Scheduler supports a maximum of 12 and a

minimum of 4.

$retentionPeriodInDays The retention period in days determines how many days of backups are

preserved on the external location. The default value is 7. Scheduler

supports a maximum of 14 and a minimum of 2. Backups older than

the retention period get automatically deleted from the external

location.

$encryptioncertpath Applies to 1901 and later. Parameter is available in Azure Stack Hub

Module version 1.7 and later. The encryption certificate path specifies

the file path to the .CER file with public key used for data encryption.

PowerShell

Enable backup using certificate

# Example username:

$username = "domain\backupadmin"

# Example share path:

$sharepath = "\\serverIP\AzSBackupStore\contoso.com\seattle"

$password = Read-Host -Prompt ("Password for: " + $username) -

AsSecureString

# Create a self-signed certificate using New-SelfSignedCertificate,

export the public key portion and save it locally.

$cert = New-SelfSignedCertificate `

-DnsName "www.contoso.com" `

-CertStoreLocation "cert:\LocalMachine\My"

New-Item -Path "C:\" -Name "Certs" -ItemType "Directory"

#make sure to export the PFX format of the certificate with the public

and private keys and then delete the certificate from the local certificate

store of the machine where you created the certificate

Export-Certificate `

-Cert $cert `

-FilePath c:\certs\AzSIBCCert.cer

In the same PowerShell session, run the following commands:

PowerShell

The result should look like the following example output:

PowerShell

In the same PowerShell session, you can update the default values for retention period

and frequency for backups.

PowerShell

The result should look like the following example output:

PowerShell

# Set the backup settings with the name, password, share, and CER

certificate file.

Set-AzsBackupConfiguration -Path $sharepath -Username $username -

Password $password -EncryptionCertPath "c:\temp\cert.cer"

Confirm backup settings

Get-AzsBackupConfiguration | Select-Object -Property Path, UserName

Path : \\serverIP\AzsBackupStore\contoso.com\seattle

UserName : domain\backupadmin

Update backup settings

#Set the backup frequency and retention period values.

$frequencyInHours = 10

$retentionPeriodInDays = 5

Set-AzsBackupConfiguration -BackupFrequencyInHours $frequencyInHours -

BackupRetentionPeriodInDays $retentionPeriodInDays

Get-AzsBackupConfiguration | Select-Object -Property Path, UserName,

AvailableCapacity, BackupFrequencyInHours, BackupRetentionPeriodInDays

Path : \\serverIP\AzsBackupStore\contoso.com\seattle

UserName : domain\backupadmin

AvailableCapacity : 60 GB

The PowerShell cmdlet to configure infrastructure backup is SetAzsBackupConfiguration. In previous releases, the cmdlet was Set-AzsBackupShare. This

cmdlet requires providing a certificate. If infrastructure backup is configured with an

encryption key, you can't update the encryption key or view the property. You need to

use version 1.6 of the Admin PowerShell.

If infrastructure backup was configured before updating to 1901, you can use version 1.6

of the admin PowerShell to set and view the encryption key. Version 1.6 won't allow you

to update from encryption key to a certificate file. Refer to Install Azure Stack Hub

PowerShell for more info on installing the correct version of the module.

Learn to run a backup, see Back up Azure Stack Hub.

Learn to verify that your backup ran, see Confirm backup completed in administration

portal.

BackupFrequencyInHours : 10

BackupRetentionPeriodInDays : 5

Azure Stack Hub PowerShell

Next steps

Back up Azure Stack Hub

Article • 07/29/2022

This article shows you how to do an on-demand backup on Azure Stack Hub. For

instructions on configuring the PowerShell environment, see Install PowerShell for Azure

Stack Hub. To sign in to Azure Stack Hub, see Using the administrator portal in Azure

Stack Hub.

Use Start-AzSBackup to start a new backup immediately with no job progress tracking.

PowerShell

Use Start-AzSBackup to start a new backup with the -AsJob parameter and save it as a

variable to track backup job progress.

PowerShell

Start Azure Stack Hub backup

Start a new backup without job progress tracking

Start-AzsBackup -Force

Start Azure Stack Hub backup with job progress tracking

７ Note

Your backup job appears as successfully completed in the portal about 10-15

minutes before the job finishes.

The actual status is better observed via the code below.

） Important

The initial 1 millisecond delay is introduced because the code is too quick to

register the job correctly and it comes back with no PSBeginTime and in turn with

no State of the job.

Use the following PowerShell commands to ensure the backup has completed

successfully:

PowerShell

$BackupJob = Start-AzsBackup -Force -AsJob

While (!$BackupJob.PSBeginTime) {

Start-Sleep -Milliseconds 1

}

Write-Host "Start time: $($BackupJob.PSBeginTime)"

While ($BackupJob.State -eq "Running") {

Write-Host "Job is currently: $($BackupJob.State) - Duration:

$((New-TimeSpan -Start ($BackupJob.PSBeginTime) -End (GetDate)).ToString().Split(".")[0])"

Start-Sleep -Seconds 30

}

If ($BackupJob.State -eq "Completed") {

Get-AzsBackup | Where-Object {$\_.BackupId -eq

$BackupJob.Output.BackupId}

$Duration = $BackupJob.Output.TimeTakenToCreate

$Pattern = '^P?T?((?<Years>\d+)Y)?((?<Months>\d+)M)?((?

<Weeks>\d+)W)?((?<Days>\d+)D)?(T((?<Hours>\d+)H)?((?<Minutes>\d+)M)?((?

<Seconds>\d\*(\.)?\d\*)S)?)$'

If ($Duration -match $Pattern) {

If (!$Matches.ContainsKey("Hours")) {

$Hours = ""

}

Else {

$Hours = ($Matches.Hours).ToString + 'h '

}

$Minutes = ($Matches.Minutes)

$Seconds = [math]::round(($Matches.Seconds))

$Runtime = '{0}{1:00}m {2:00}s' -f $Hours, $Minutes, $Seconds

}

Write-Host "BackupJob: $($BackupJob.Output.BackupId) - Completed

with Status: $($BackupJob.Output.Status) - It took: $($Runtime) to run" -

ForegroundColor Green

}

ElseIf ($BackupJob.State -ne "Completed") {

$BackupJob

$BackupJob.Output

}

Confirm backup has completed

Confirm backup has completed using PowerShell

Get-AzsBackup

The result should look like the following output:

PowerShell

Use the Azure Stack Hub administrator portal to verify that backup has completed

successfully by following these steps:

1. Open the Azure Stack Hub administrator portal.

2. Select All services, and then under the ADMINISTRATION category select >

Infrastructure backup. Choose Configuration in the Infrastructure backup blade.

3. Find the Name and Date Completed of the backup in Available backups list.

4. Verify the State is Succeeded.

Learn more about the workflow for recovering from a data loss event.

BackupDataVersion : 1.0.1

BackupId : <backup ID>

RoleStatus : {NRP, SRP, CRP, KeyVaultInternalControlPlane...}

Status : Succeeded

CreatedDateTime : 7/6/2018 6:46:24 AM

TimeTakenToCreate : PT20M32.364138S

DeploymentID : <deployment ID>

StampVersion : 1.1807.0.41

OemVersion :

Id : /subscriptions/<subscription

ID>/resourceGroups/System.local/providers/Microsoft.Backup.Admin/backupLocat

ions/local/backups/<backup ID>

Name : local/<local name>

Type : Microsoft.Backup.Admin/backupLocations/backups

Location : local

Tags : {}

Confirm backup has completed in the administrator

portal

Next steps

Recover data in Azure Stack Hub with

the Infrastructure Backup Service

Article • 07/29/2022

You can back up and restore configuration and service data using the Azure Stack Hub

Infrastructure Backup Service. Each Azure Stack Hub installation contains an instance of

the service. You can use backups created by the service for the redeployment of the

Azure Stack Hub cloud to restore identity, security, and Azure Resource Manager data.

Enable backup when you're ready to put your cloud into production. Don't enable

backup if you plan to perform testing and validation for a long period of time.

Before you enable your backup service, make sure you have the requirements in place.

The service contains the following features:

Feature Description

Backup Infrastructure

Services

Coordinate backup across a subset of infrastructure services in Azure

Stack Hub. If there's a disaster, the data can be restored as part of

redeployment.

Compression and

encryption of exported

backup data

Backup data is compressed and encrypted by the system before it's

exported to the external storage location provided by the admin.

Backup job monitoring System notifies you when backup jobs fail and how to fix the problem.

Backup management

experience

Backup RP supports enabling backup.

７ Note

The Infrastructure Backup Service doesn't include user data and apps. For more info

on how to protect IaaS VM-based apps, see protect VMs deployed on Azure Stack

Hub. For a comprehensive understanding of how to protect apps on Azure Stack

Hub, see the Azure Stack Hub considerations for business continuity and disaster

recovery whitepaper .

The Infrastructure Backup Service

Feature Description

Cloud recovery If there's a catastrophic data loss, backups can be used to restore core

Azure Stack Hub info as part of deployment.

Storage location

You need a file share accessible from Azure Stack Hub that can contain 14 backups.

Each backup is about 10 GB. Your file share should be able to store 140 GB of

backups. For more info on selecting a storage location for the Infrastructure

Backup Service, see Backup Controller requirements.

Credentials

You need a domain user account and credentials. For example, you can use your

Azure Stack Hub admin credentials.

Encryption certificate

Backup files are encrypted using the public key in the certificate. Make sure to

store this certificate in a secure location.

Learn how to Enable Backup for Azure Stack Hub from the administrator portal.

Learn how to Enable Backup for Azure Stack Hub with PowerShell.

Learn how to Back up Azure Stack Hub.

Learn how to Recover from catastrophic data loss.

Verify requirements for the Infrastructure

Backup Service

Next steps

Back up files and applications on Azure

Stack

Article • 02/02/2023

You can use Azure Backup to protect (or back up) files and applications on Azure Stack.

To back up files and applications, install Microsoft Azure Backup Server as a virtual

machine running on Azure Stack. You can protect the files on any Azure Stack server in

the same virtual network. Once you've installed Azure Backup Server, add Azure disks to

increase the local storage available for short-term backup data. Azure Backup Server

uses Azure storage for long-term retention.

This article doesn't cover installing Azure Backup Server in the Azure Stack environment.

To install Azure Backup Server on Azure Stack, see the article, Installing Azure Backup

Server.

To configure Azure Backup Server to protect Files in Azure Stack virtual machines, open

the Azure Backup Server console. You'll use the console to configure protection groups

and to protect the data on your virtual machines.

1. In the Azure Backup Server console, select Protection and in the toolbar, select

New to open the Create New Protection Group wizard.

７ Note

Though Azure Backup Server and System Center Data Protection Manager (DPM)

are similar, DPM isn't supported for use with Azure Stack.

Back up Files and Folders in Azure Stack VMs to

Azure

It may take a few seconds for the wizard to open. Once the wizard opens, select

Next to advance to the Select Protection Group Type screen.

2. On the Select Protection Group Type screen, choose Servers and select Next.

The Select Group Members screen opens.

3. In the Select Group Members screen, select + to expand the list of subitems. For

all items that you want to protect, select the check box. Once all items have been

selected, select Next.

Microsoft recommends putting all data that will share a protection policy, into one

protection group. For complete information about planning and deploying

protection groups, see the System Center DPM article, Deploy Protection Groups.

4. In the Select Data Protection Method screen, type a name for the protection

group. Select the checkbox for I want short-term protection using: and I want

online protection. Select Next.

To select I want online protection, you must first select I want short-term

protection using: Disk. Azure Backup Server doesn't protect to tape, so disk is the

only choice for short-term protection.

5. In the Specify Short-Term Goals screen, choose how long to retain the recovery

points saved to disk, and when to save incremental backups. Select Next.

） Important

You should not retain operational recovery (backup) data on Azure Backup

Server-attached disks for more than five days.

Instead of selecting an interval for incremental backups, to run an express full

backup just before each scheduled recovery point, select Just before a recovery

point. If you're protecting application workloads, Azure Backup Server creates

recovery points per the Synchronization frequency schedule (provided the

application supports incremental backups). If the application doesn't support

incremental backups, Azure Backup Server runs an express full backup.

For File recovery points, specify when to create recovery points. Select Modify to

set the times and days of the week when recovery points are created.

6. In the Review disk allocation screen, review the storage pool disk space allocated

for the protection group.

Total Data size is the size of the data you want to back up and Disk space to be

provisioned on Azure Backup Server is the recommended space for the protection

group. Azure Backup Server chooses the ideal backup volume, based on the

settings. However, you can edit the backup volume choices in the Disk allocation

details. For the workloads, select the preferred storage in the dropdown menu.

Your edits change the values for Total Storage and Free Storage in the Available

Disk Storage pane. Underprovisioned space is the amount of storage Azure Backup

Server suggests you add to the volume, to continue with backups smoothly in the

future.

7. In Choose replica creation method, select how you want to handle the initial full

data replication. If you decide to replicate over the network, Azure recommends

you choose an off-peak time. For large amounts of data or less than optimal

network conditions, consider replicating the data using removable media.

8. In Choose consistency check options, select how you want to automate

consistency checks. Enable consistency checks to run only when data replication

becomes inconsistent, or according to a schedule. If you don't want to configure

automatic consistency checking, run a manual check at any time by:

In the Protection area of the Azure Backup Server console, right-click the

protection group and select Perform Consistency Check.

9. If you choose to back up to Azure, on the Specify online protection data page

make sure the workloads you want to back up to Azure are selected.

10. In Specify online backup schedule, specify when incremental backups to Azure

should occur.

You can schedule backups to run every day/week/month/year and the time/date at

which they should run. Backups can occur up to twice a day. Each time a backup

job runs, a data recovery point is created in Azure from the copy of the backed-up

data stored on the Azure Backup Server disk.

11. In Specify online retention policy, specify how the recovery points created from

the daily/weekly/monthly/yearly backups are retained in Azure.

12. In Choose online replication, specify how the initial full replication of data occurs.

13. On Summary, review your settings. When you select Create Group, the initial data

replication occurs. When the data replication finishes, on the Status page, the

protection group status shows as OK. The initial backup job takes place in line with

the protection group settings.

Use Azure Backup Server console to recover data to your virtual machine.

1. In the Azure Backup Server console, on the navigation bar, select Recovery and

browse for the data you want to recover. In the results pane, select the data.

2. On the calendar in the recovery points section, dates in bold indicate recovery

points are available. Select the date to recover.

3. In the Recoverable item pane, select the item you want to recover.

4. In the Actions pane, select Recover to open the Recovery Wizard.

5. You can recover data as follows:

Recover to the original location - If the client computer is connected over

VPN, this option doesn't work. Instead use an alternate location, and then

copy data from that location.

Recover to an alternate location

6. Specify the recovery options:

For Existing version recovery behavior, select Create copy, Skip, or

Overwrite. Overwrite is available only when recovering to the original

location.

For Restore security, choose Apply settings of the destination computer or

Apply the security settings of the recovery point version.

For Network bandwidth usage throttling, select Modify to enable network

bandwidth usage throttling.

Recover file data

Notification Select Send an e-mail when the recovery completes, and

specify the recipients who will receive the notification. Separate the e-mail

addresses with commas.

After making the selections, select Next

7. Review your recovery settings, and select Recover.

If you're using Modern Backup Storage (MBS), File Server end-user recovery (EUR) isn't

supported. File Server EUR has a dependency on Volume Shadow Copy Service (VSS),

which Modern Backup Storage doesn't use. If EUR is enabled, use the following steps to

recover data:

1. Navigate to the protected files, and right-click the file name and select Properties.

2. On the Properties menu, select Previous Versions and choose the version you

want to recover.

To view Azure Backup Server entities in the Azure portal, you can follow the following

steps:

1. Open Recovery Services vault.

2. Select Backup Infrastructure.

3. View Backup Management Servers.

For information on using Azure Backup Server to protect other workloads, see one of

the following articles:

About Azure Backup service

About Azure AD

About Azure Recovery Services vault

About Azure Storage

About Azure Stack Hub

７ Note

While the recovery job is in progress, all synchronization jobs for the selected

recovery items are canceled.

View Azure Backup Server with a vault

Next steps

Back up SharePoint farm

Back up SQL server

Replicate Azure Stack VMs to Azure

Article • 01/31/2023

This article shows you how to set up disaster recovery Azure Stack VMs to Azure, using the

Azure Site Recovery service.

Site Recovery contributes to your business continuity and disaster recovery (BCDR) strategy.

The service ensures that your VM workloads remain available when expected and unexpected

outages occur.

Site Recovery orchestrates and manages replication of VMs to Azure storage.

When an outage occurs in your primary site, you use Site Recovery to fail over to Azure.

On failover, Azure VMs are created from the stored VM data, and users can continue

accessing workloads running on those Azure VMs.

When everything's up and running again, you can fail back Azure VMs to your primary

site, and start replicating to Azure storage again.

In this article, you learn how to:

With these steps complete, you can then run a full failover to Azure as and when you need to.

Step 1: Prepare Azure stack VMs for replication. Check that VMs comply with Site

Recovery requirements, and prepare for installation of the Site Recovery Mobility service.

This service is installed on each VM you want to replicate.

＂

Step 2: Set up a Recovery Services vault. Set up a vault for Site Recovery, and specify what

you want to replicate. Site Recovery components and actions are configured and managed

in the vault.

＂

Step 3: Set up the source replication environment. Set up a Site Recovery configuration

server. The configuration server is a single Azure Stack VM that runs all the components

needed by Site Recovery. After you've set up the configuration server, you register it in the

vault.

＂

Step 4: Set up the target replication environment. Select your Azure account, and the

Azure storage account and network that you want to use. During replication, VM data is

copied to Azure storage. After failover, Azure VMs are joined to the specified network.

＂

Step 5: Enable replication. Configure replication settings, and enable replication for VMs.

The Mobility service will be installed on a VM when replication is enabled. Site Recovery

performs an initial replication of the VM, and then ongoing replication begins.

＂

Step 6: Run a disaster recovery drill: After replication is up and running, you verify that

failover will work as expected by running a drill. To initiate the drill, you run a test failover

in Site Recovery. The test failover doesn't impact your production environment.

＂

Architecture

Location Component Details

Configuration

server

Runs on a single

Azure Stack VM.

In each subscription you set up a configuration server VM. This VM

runs the following Site Recovery components:

- Configuration server: Coordinates communications between onpremises and Azure, and manages data replication. - Process

server: Acts as a replication gateway. It receives replication data,

optimizes with caching, compression, and encryption; and sends it

to Azure storage.

If VMs you want to replicate exceed the limits stated below, you

can set up a separate standalone process server. Learn more.

Mobility

service

Installed on each

VM you want to

replicate.

In the steps in this article, we prepare an account so that the

Mobility service is installed automatically on a VM when replication

is enabled. If you don't want to install the service automatically,

there are a number of other methods you can use. Learn more.

Azure In Azure you need

a Recovery Services

vault, a storage

account, and a

virtual network.

Replicated data is stored in the storage account. Azure VMs are

added to the Azure network when failover occurs.

Replication works as follows:

1. In the vault, you specify the replication source and target, set up the configuration server,

create a replication policy, and enable replication.

2. The Mobility service is installed on the machine (if you've used push installation), and

machines begin replication in accordance with the replication policy.

3. An initial copy of the server data is replicated to Azure storage.

4. After initial replication finishes, replication of delta changes to Azure begins. Tracked

changes for a machine are held in a .hrl file.

5. The configuration server orchestrates replication management with Azure (port HTTPS

443 outbound).

6. The process server receives data from source machines, optimizes and encrypts it, and

sends it to Azure storage (port 443 outbound).

7. Replicated machines communicate with the configuration server (port HTTPS 443

inbound, for replication management. Machines send replication data to the process

server (port HTTPS 9443 inbound - can be modified).

8. Traffic is replicated to Azure storage public endpoints, over the internet. Alternately, you

can use Azure ExpressRoute public peering. Replicating traffic over a site-to-site VPN from

an on-premises site to Azure isn't supported.

Here's what you need to set up this scenario.

Requirement Details

Azure

subscription

account

If you don't have an Azure subscription, create a free account .

Azure account

permissions

The Azure account you use needs permissions to:

- Create a Recovery Service vault

- Create a virtual machine in the resource group and virtual network you use for the

scenario

- Write to the storage account you specify

Note that:

-If you create an account, you're the administrator of your subscription and can perform

all actions.

- If you use an existing subscription and you're not the administrator, you need to work

with the admin to assign you Owner or Contributor permissions.

- If you need more granular permissions, review this article.

Azure Stack

VM

You need an Azure Stack VM in the tenant subscription, that will be deployed as the Site

Recovery configuration server.

Configuration/Process server requirements for physical server replication

Prerequisites

Prerequisites for the configuration server

Component Requirement

HARDWARE

SETTINGS

CPU cores 8

RAM 16 GB

Number of

disks

3, including the OS disk, process server cache disk, and retention drive for failback

Free disk

space

(process

server

cache)

600 GB

Free disk

space

(retention

disk)

600 GB

SOFTWARE

SETTINGS

Operating

system

Windows Server 2012 R2

Windows Server 2016

Operating

system

locale

English (en-us)

Windows

Server roles

Don't enable these roles:

- Active Directory Domain Services

- Internet Information Services

- Hyper-V

Group

policies

Don't enable these group policies:

- Prevent access to the command prompt.

- Prevent access to registry editing tools.

- Trust logic for file attachments.

- Turn on Script Execution.

Learn more

IIS - No preexisting default website

- No preexisting website/application listening on port 443

- Enable anonymous authentication

- Enable FastCGI setting.

IP address

type

Static

Component Requirement

ACCESS

SETTINGS

MYSQL MySQL should be installed on the configuration server. You can install manually, or Site

Recovery can install it during deployment. For Site Recovery to install, check that the

machine can reach http://cdn.mysql.com/archives/mysql-5.5/mysql-5.5.37-win32.msi .

URLs The configuration server needs access to these URLs (directly or via proxy):

Azure AD: login.microsoftonline.com ; login.microsoftonline.us ;

\*.accesscontrol.windows.net

Replication data transfer: \*.backup.windowsazure.com ; \*.backup.windowsazure.us

Replication management: \*.hypervrecoverymanager.windowsazure.com ;

\*.hypervrecoverymanager.windowsazure.us ; https://management.azure.com ;

\*.services.visualstudio.com

Storage access: \*.blob.core.windows.net ; \*.blob.core.usgovcloudapi.net

Time synchronization: time.nist.gov ; time.windows.com

Telemetry (optional): dc.services.visualstudio.com

Firewall IP address-based firewall rules should allow communication to Azure URLs. To simplify and

limit the IP ranges, we recommend using URL filtering.

For commercial IPs:

- Allow the Azure Datacenter IP Ranges , and the HTTPS (443) port.

- Allow IP address ranges for the West US (used for Access Control and Identity

Management).

- Allow IP address ranges for the Azure region of your subscription, to support the URLs

needed for Azure Active Directory, backup, replication, and storage.

For government IPs:

- Allow the Azure Government Datacenter IP Ranges, and the HTTPS (443) port.

- Allow IP address ranges for all US Gov Regions (Virginia, Texas, Arizona, and Iowa), to

support the URLs needed for Azure Active Directory, backup, replication, and storage.

Ports Allow 443 (Control channel orchestration)

Allow 9443 (Data transport)

Configuration/Process server sizing requirements

CPU CPU Memor Memoryy Cache disk Cache disk Data change rat Data change ratee RReplicat eplicated machines ed machines

8 vCPUs

2 sockets \* 4 cores @ 2.5 GHz

16GB 300 GB 500 GB or less < 100 machines

12 vCPUs

2 socks \* 6 cores @ 2.5 GHz

18 GB 600 GB 500 GB-1 TB 100 to 150 machines

16 vCPUs

2 socks \* 8 cores @ 2.5 GHz

32 GB 1 TB 1-2 TB 150 -200 machines

Make sure that the VMs are running one of the operating systems summarized in the table.

Operating

system

Details

64-bit

Windows

Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server

2012, Windows Server 2008 R2 (from SP1)

CentOS 5.2 to 5.11, 6.1 to 6.9, 7.0 to 7.3

Ubuntu 14.04 LTS server, 16.04 LTS server. Review supported kernels

Every VM you want to replicate must have the Mobility service installed. In order for the

process server to install the service automatically on the VM when replication is enabled, verify

the VM settings.

You need network connectivity between the VM on which you want to enable replication,

and the machine running the process server (by default this is the configuration server

VM).

You need an account with admin rights (domain or local) on the machine for which you

enable replication.

You specify this account when you set up Site Recovery. Then the process server uses

this account to install the Mobility service when replication is enabled.

Step 1: Prepare Azure Stack VMs

Verify the operating system

Prepare for Mobility service installation

Windows machines

This account will only be used by Site Recovery for the push installation, and to update

the Mobility service.

If you're not using a domain account, you need to disable Remote User Access control

on the VM:

In the registry, create DWORD value LocalAccountTokenFilterPolicy under

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System.

Set the value to 1.

To do this at the command prompt, type the following: REG ADD

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

/v LocalAccountTokenFilterPolicy /t REG\_DWORD /d 1.

In the Windows Firewall on the VM you want to replicate, allow File and Printer Sharing,

and WMI.

To do this, run wf.msc to open the Windows Firewall console. Right click Inbound Rules

> New Rule. Select Predefined, and choose File and Printer sharing from the list.

Complete the wizard, select to allow the connection > Finish.

For domain computers, you can use a GPO to do this.

Ensure that there's network connectivity between the Linux computer and the process

server.

On the machine for which you enable replication, you need an account that's a root user

on the source Linux server:

You specify this account when you set up Site Recovery. Then the process server uses

this account to install the Mobility service when replication is enabled.

This account will only be used by Site Recovery for the push installation, and to update

the Mobility service.

Check that the /etc/hosts file on the source Linux server has entries that map the local

hostname to IP addresses associated with all network adapters.

Install the latest openssh, openssh-server, and openssl packages on the computer that

you want to replicate.

Ensure that Secure Shell (SSH) is enabled and running on port 22.

Enable SFTP subsystem and password authentication in the sshd\_config file:

1. To do this, sign in as root.

2. Find the line that begins with PasswordAuthentication, in the /etc/ssh/sshd\_config

file. Uncomment the line and change the value to yes.

3. Find the line that begins with Subsystem and uncomment the line.

4. Restart the sshd service.

Linux machines

For each machine you want to replicate, find the IP address:

1. In the Azure Stack Portal, click on the VM.

2. On the Resource menu, click Network Interfaces.

3. Note down the private IP address.

1. In the Azure portal, select Create a resource > Management Tools > Backup and Site

Recovery.

2. In Name, enter a friendly name to identify the vault.

3. In Resource group, create or select a resource group. We're using contosoRG.

4. In Location, enter the Azure region. We're using West Europe.

5. To quickly access the vault from the dashboard, select Pin to dashboard > Create.

Note the VM private IP address

Step 2: Create a vault and select a replication goal

The new vault appears on Dashboard > All resources, and on the main Recovery Services

vaults page.

1. In Recovery Services vaults > specify a vault name. We're using ContosoVMVault.

2. In Getting Started, select Site Recovery. Then select Prepare Infrastructure.

3. In Protection goal > Where are your machines located, select On-premises.

4. In Where do you want to replicate your machines, select To Azure.

5. In Are your machines virtualized, select Not virtualized/Other. Then select OK.

Select a replication goal

Set up the configuration server machine, register it in the vault, and discover machines you

want to replicate.

1. Click Prepare Infrastructure > Source.

2. In Prepare source, click +Configuration server.

Step 3: Set up the source environment

3. In Add Server, check that Configuration Server appears in Server type.

4. Download the Site Recovery Unified Setup installation file.

5. Download the vault registration key. You need the registration key when you run Unified

Setup. The key is valid for five days after you generate it.

To install and register the configuration server, do an RDP connection to the VM you want to

use for the configuration server, and run Unified Setup.

Before you start, make sure that the clock is synchronized with a time server on the VM before

you start. Installation fails if the time is more than five minutes off local time.

Now install the configuration server:

1. Run the Unified Setup installation file.

2. In Before You Begin, select Install the configuration server and process server.

Run Azure Site Recovery Unified Setup

3. In Third Party Software License, click I Accept to download and install MySQL.

4. In Registration, select the registration key you downloaded from the vault.

5. In Internet Settings, specify how the Provider running on the configuration server

connects to Azure Site Recovery over the Internet. Make sure you've allowed the required

URLs.

If you want to connect with the proxy that's currently set up on the machine, select

Connect to Azure Site Recovery using a proxy server.

If you want the Provider to connect directly, select Connect directly to Azure Site

Recovery without a proxy server.

If the existing proxy requires authentication, or if you want to use a custom proxy for

the Provider connection, select Connect with custom proxy settings, and specify the

address, port, and credentials.

6. In Prerequisites Check, Setup runs a check to make sure that installation can run. If a

warning appears about the Global time sync check, verify that the time on the system

clock (Date and Time settings) is the same as the time zone.

7. In MySQL Configuration, create credentials for logging on to the MySQL server instance

that is installed.

8. In Environment Details, select No if you're replicating Azure Stack VMs or physical

servers.

9. In Install Location, select where you want to install the binaries and store the cache. The

drive you select must have at least 5 GB of disk space available, but we recommend a

cache drive with at least 600 GB of free space.

10. In Network Selection, first select the NIC that the in-built process server uses for

discovery and push installation of mobility service on source machines, and then select

the NIC that Configuration Server uses for connectivity with Azure. Port 9443 is the default

port used for sending and receiving replication traffic, but you can modify this port

number to suit your environment's requirements. In addition to the port 9443, we also

open port 443, which is used by a web server to orchestrate replication operations. Do not

use port 443 for sending or receiving replication traffic.

11. In Summary, review the information and click Install. When installation finishes, a

passphrase is generated. You will need this when you enable replication, so copy it and

keep it in a secure location.

After registration finishes, the server is displayed on the Settings > Servers blade in the vault.

Select and verify target resources.

1. In Prepare infrastructure > Target, select the Azure subscription you want to use.

2. Specify the target deployment model.

3. Site Recovery checks that you have one or more compatible Azure storage accounts and

networks. If it doesn't find them, you need to create at least one storage account and

virtual network, in order to complete the wizard.

７ Note

The configuration server can also be installed from the command line. Learn more.

It can take 15 minutes or more for the account name to appear in the portal. To update

immediately, select Configuration Servers > server name > Refresh Server.

Step 4: Set up the target environment

Step 5: Enable replication

Create a replication policy

1. Click Prepare Infrastructure > Replication Settings.

2. In Create replication policy, specify a policy name.

3. In RPO threshold, specify the recovery point objective (RPO) limit.

Recovery points for replicated data are created in accordance with the time set.

This setting does not affect replication, which is continuous. It simply issues an alert

if the threshold limit is reached without a recovery point being created.

4. In Recovery point retention, specify how long each recovery point is kept. Replicated VMs

can be recovered to any point in the specified time window.

5. In App-consistent snapshot frequency, specify how often application-consistent

snapshots are created.

An app-consistent snapshot is a point-in-time snapshot of the app data inside the

VM.

Volume Shadow Copy Service (VSS) ensures that apps on the VM are in a consistent

state when the snapshot is taken.

6. Select OK to create the policy.

You can skip this step right now. In Deployment Planning dropdown list, click Yes, I have done

it.

Make sure you've completed all the tasks in Step 1: Prepare machine. Then enable replication

as follows:

1. Select Replicate application > Source.

2. In Source, select the configuration server.

3. In Machine type, select Physical machines.

4. Select the process server (configuration server). Then click OK.

5. In Target, select the subscription and the resource group in which you want to create the

VMs after failover. Choose the deployment model that you want to use for the failed-over

VMs.

6. Select the Azure storage account in which you want to store the replicated data.

Confirm deployment planning

Enable replication

7. Select the Azure network and subnet to which Azure VMs connect when they're created

after failover.

8. Select Configure now for selected machines to apply the network setting to all machines

you select for protection. Select Configure later if you want to select the Azure network

separately for each machine.

9. In Physical Machines, click +Physical machine. Specify the name, IP address and OS type

of each machine you want to replicate.

Use the internal IP address of the machine.

If you specify the public IP address, replication may not work as expected.

10. In Properties > Configure properties, select the account that the process server will use

to automatically install Mobility Service on the machine.

11. In Replication settings > Configure replication settings, check that the correct replication

policy is selected.

12. Click Enable Replication.

13. Track progress of the Enable Protection job in Settings > Jobs > Site Recovery Jobs.

After the Finalize Protection job runs, the machine is ready for failover.

You run a test failover to Azure to make sure that everything's working as expected. This

failover won't affect your production environment.

Before you run a test failover, verify the machine properties, and make sure that they comply

with Azure requirements. You can view and modify properties as follows:

1. In Protected Items, click Replicated Items > VM.

７ Note

Site Recovery installs Mobility Service when replication is enabled for a VM.

It can take 15 minutes or longer for changes to take effect and appear in the portal.

To monitor VMs you add, check the last discovered time for VMs in Configuration Servers

> Last Contact At. To add VMs without waiting for the scheduled discovery, highlight the

configuration server (don't select it) and select Refresh.

Step 6: Run a disaster recovery drill

Verify machine properties

2. In the Replicated item pane, there's a summary of VM information, health status, and the

latest available recovery points. Click Properties to view more details.

3. In Compute and Network settings, modify settings as needed.

You can modify the Azure VM name, resource group, target size, availability set, and

managed disk settings.

You can also view and modify network settings. These include the network/subnet to

which the Azure VM is joined after failover, and the IP address that will be assigned

to the VM.

4. In Disks, view information about the operating system and data disks on the VM.

When you run a test failover, the following happens:

1. A prerequisites check runs to make sure all of the conditions required for failover are in

place.

2. Failover processes the data using the specified recovery point:

Latest processed: The machine fails over to the latest recovery point processed by

Site Recovery. The time stamp is shown. With this option, no time is spent

processing data, so it provides a low RTO (recovery time objective).

Latest app-consistent: The machine fails over to the latest app-consistent recovery

point.

Custom: Select the recovery point used for failover.

3. An Azure VM is created using the processed data.

4. Test failover can automatically clean up Azure VMs created during the drill.

Run a test failover for a VM as follows:

1. In Settings > Replicated Items, click the VM > +Test Failover.

2. For this walkthrough, we'll select to use the Latest processed recovery point.

3. In Test Failover, select the target Azure network.

4. Click OK to begin the failover.

5. Track progress by clicking on the VM to open its properties. Or, click the Test Failover job

in vault name > Settings > Jobs >Site Recovery jobs.

6. After the failover finishes, the replica Azure VM appears in the Azure portal > Virtual

Machines. Check that the VM is the appropriate size, connected to the right network, and

running.

7. You should now be able to connect to the replicated VM in Azure. Learn more.

8. To delete Azure VMs created during the test failover, click Cleanup test failover on the

VM. In Notes, save any observations associated with the test failover.

Run a test failover

After you've set up replication, and run a drill to make sure everything's working, you can fail

machines over to Azure as required.

Before you run a failover, if you want to connect to the machine in Azure after the failover, then

prepare to connect before you start.

Then run a failover as follows:

1. In Settings > Replicated Items, click the machine > Failover.

2. Select the recovery point that you want to use.

3. In Test Failover, select the target Azure network.

4. Select Shut down machine before beginning failover. With this setting, Site Recovery

tries to shut down the source machine before starting the failover. However failover

continues even if shutdown fails.

5. Click OK to begin the failover. You can follow the failover progress on the Jobs page.

6. After the failover finishes, the replica Azure VM appears in the Azure portal > Virtual

Machines. If you prepared to connect after failover, check that the VM is the appropriate

size, connected to the right network, and running.

7. After verifying the VM, click Commit to finish the failover. This deletes all available

recovery points.

When your primary site is up and running again, you can fail back from Azure to Azure Stack.

To do this, follow the steps listed out here.

In this article we replicated Azure Stack VMs to Azure. With replication in place, we ran a

disaster recovery drill to make sure failover to Azure worked as expected. The article also

included steps for running a full failover to Azure, and failing back to Azure Stack.

After failing back, you can reprotect the VM and start replicating it to Azure again To do this,

repeat the steps in this article.

Fail over and fail back

２ Warning

Don't cancel a failover in progress: Before failover is started, VM replication is stopped. If

you cancel a failover in progress, failover stops, but the VM won't replicate again.

Fail back to Azure Stack

Conclusion

Next steps

Recover from catastrophic data loss

Article • 07/29/2022

Azure Stack Hub runs Azure services in your datacenter and can run on environments as

small as four nodes installed in a single rack. In contrast, Azure runs in more than 40

regions in multiple datacenters and multiple zones in each region. User resources can

span multiple servers, racks, datacenters, and regions. With Azure Stack Hub, you

currently only have the choice to deploy your entire cloud to a single rack. This

limitation exposes your cloud to the risk of catastrophic events at your datacenter or

failures due to major product bugs. When a disaster strikes, the Azure Stack Hub

instance goes offline. All of the data is potentially unrecoverable.

Depending on the root cause of the data loss, you may need to repair a single

infrastructure service or restore the entire Azure Stack Hub instance. You may even need

to restore to different hardware in the same location or in a different location.

This scenario addresses recovering your entire installation if there's a failure and the

redeployment of the private cloud.

Scenario Data Loss Considerations

Recover from catastrophic data loss

due to disaster or product bug.

All infrastructure

and user and app

data.

Can restore to different OEM.

Can restore to different generation

of hardware.

Can restore to different count of

scale-unit nodes.

User app and data are protected

separately from infrastructure data.

The journey of protecting Azure Stack Hub starts with backing up the infrastructure and

app/tenant data separately. This document covers how to protect the infrastructure.

Workflows

In worst case scenarios where all data is lost, recovering Azure Stack Hub is the process

of restoring the infrastructure data unique to that deployment of Azure Stack Hub and

all user data.

If there's catastrophic data loss but the hardware is still usable, redeployment of Azure

Stack Hub is required. During redeployment, you can specify the storage location and

credentials required to access backups. In this mode, there's no need to specify the

services that need to be restored. Infrastructure Backup Controller injects control plane

state as part of the deployment workflow.

If there's a disaster that renders the hardware unusable, redeployment is only possible

on new hardware. Redeployment can take several weeks while replacement hardware is

ordered and arrives in the datacenter. Restore of control plane data is possible at any

time. However, restore isn't supported if the version of the redeployed instance is more

than one version greater than the version used in the last backup.

Deployment

mode

Starting

point

End point

Clean install Baseline

build

OEM deploys Azure Stack Hub and updates to the latest supported

version.

Recovery

mode

Baseline

build

OEM deploys Azure Stack Hub in recovery mode and handles the

version matching requirements based on the latest backup available.

The OEM completes the deployment by updating to latest supported

version.

Azure Stack Hub supports a type of deployment called cloud recovery mode. This mode

is used only if you choose to recover Azure Stack Hub after a disaster or product bug

rendered the solution unrecoverable. This deployment mode doesn't recover any of the

Restore

Data in backups

user data stored in the solution. The scope of this deployment mode is limited to

restoring the following data:

Deployment inputs

Internal identity service data

Federated identify configuration (ADFS deployments).

Root certificates used by internal certificate authority.

Azure Resource Manager configuration user data, such as subscriptions, plans,

offers, resource groups, tags, storage quotas, network quotas, and compute

resources.

Key Vault secrets and vaults.

RBAC policy assignments and role assignments.

None of the user Infrastructure as a Service (IaaS) or Platform as a Service (PaaS)

resources are recovered during deployment. These losses include IaaS VMs, storage

accounts, blobs, tables, network configuration, and so on. The purpose of cloud recovery

is to ensure your operators and users can sign back in to the portal after deployment is

complete. Users signing back in won't see any of their resources. Users have their

subscriptions restored and along with that the original plans, offers, and policies defined

by the admin. Users signing back in to the system operate under the same constraints

imposed by the original solution before the disaster. After cloud recovery completes, the

operator can manually restore value-add and third-party RPs and associated data.

You can use ASDK to test a backup to confirm that the data is valid and usable. For more

information, see Use the ASDK to validate an Azure Stack backup.

Learn about the best practices for using the Infrastructure Backup Service.

Validate backups

Next steps

Infrastructure Backup Service best

practices

Article • 07/29/2022

Follow these best practices when you deploy and manage Azure Stack Hub to help

mitigate data loss if there's a catastrophic failure.

Review the best practices regularly to verify that your installation is still in compliance

when changes are made to the operation flow. If you come across any issues while

implementing these best practices, contact Microsoft Support for help.

Enable Infrastructure Backup after deployment of each Azure Stack Hub Cloud. Using

Azure Stack Hub PowerShell, you can schedule backups from any client/server with

access to the operator management API endpoint.

The Universal Naming Convention (UNC) string for the path must use a fully qualified

domain name (FQDN). IP address can be used if name resolution isn't possible. A UNC

string specifies the location of resources such as shared files or devices.

The encryption certificate is used to encrypt backup data that gets exported to external

storage. The certificate can be a self-signed certificate since the certificate is only used

to transport keys. Refer to New-SelfSignedCertificate for more info on how to create a

certificate.

The key must be stored in a secure location (for example, global Azure Key Vault

certificate). The CER format of the certificate is used to encrypt data. The PFX format

must be used during cloud recovery deployment of Azure Stack Hub to decrypt backup

data.

Configuration best practices

Deployment

Networking

Encryption

Backup jobs execute while the system is running so there's no downtime to the

management experiences or user apps. Expect the backup jobs to take 20-40

minutes for a solution that's under reasonable load.

Automatic backups will not start during patch and update and FRU operations.

Scheduled backups jobs will get skipped by default. On-demand requests for

backups are blocked as well during these operations.

Using OEM provided instructions, manually backed up network switches and the

hardware lifecycle host (HLH) should be stored on the same backup share where

the Infrastructure Backup Controller stores control plane backup data. Consider

storing switch and HLH configurations in the region folder. If you have multiple

Azure Stack Hub instances in the same region, consider using an identifier for each

configuration that belongs to a scale unit.

Infrastructure creates MASBACKUP folder automatically. This is a Microsoftmanaged share. You can create shares at the same level as MASBACKUP. It's not

recommended to create folders or storage data inside of MASBACKUP that Azure

Stack Hub doesn't create.

User FQDN and region in your folder name to differentiate backup data from

different clouds. The FQDN of your Azure Stack Hub deployment and endpoints is

Operational best practices

Backups

Folder Names

the combination of the Region parameter and the External Domain Name

parameter. For more info, see Azure Stack Hub datacenter integration - DNS.

For example, the backup share is AzSBackups hosted on fileserver01.contoso.com. In

that file share there may be a folder per Azure Stack Hub deployment using the external

domain name and a subfolder that uses the region name.

FQDN: contoso.com

Region: nyc

Console

MASBackup folder is where Azure Stack Hub stores its backup data. Don't use this folder

to store your own data. OEMs shouldn't use this folder to store any backup data either.

OEMs are encouraged to store backup data for their components under the region

folder. Each network switch, hardware lifecycle host (HLH), and so on, may be stored in

its own subfolder. For example:

Console

The following alerts are supported by the system:

Alert Description Remediation

Backup failed

because the file

share is out of

capacity.

File share is out of capacity

and backup controller can't

export backup files to the

location.

Add more storage capacity and try back up

again. Delete existing backups (starting from

oldest first) to free up space.

\\fileserver01.contoso.com\AzSBackups

\\fileserver01.contoso.com\AzSBackups\contoso.com

\\fileserver01.contoso.com\AzSBackups\contoso.com\nyc

\\fileserver01.contoso.com\AzSBackups\contoso.com\nyc\MASBackup

\\fileserver01.contoso.com\AzSBackups\contoso.com\nyc\HLH

\\fileserver01.contoso.com\AzSBackups\contoso.com\nyc\Switches

\\fileserver01.contoso.com\AzSBackups\contoso.com\nyc\DeploymentData

\\fileserver01.contoso.com\AzSBackups\contoso.com\nyc\Registration

Monitoring

Alert Description Remediation

Backup failed

due to

connectivity

problems.

Network between Azure Stack

Hub and the file share is

experiencing issues.

Address the network issue and try backup

again.

Backup failed

due to a fault in

the path.

The file share path can't be

resolved.

Map the share from a different computer to

ensure the share is accessible. You may need

to update the path if it's no longer valid.

Backup failed

due to

authentication

issue.

There might be an issue with

the credentials or a network

issue that impacts

authentication.

Map the share from a different computer to

ensure the share is accessible. You may need

to update credentials if they're no longer

valid.

Backup failed

due to a general

fault.

The failed request could be

due to an intermittent issue.

Try to back up again.

Call support.

Review the reference material for the Infrastructure Backup Service.

Enable the Infrastructure Backup Service.

Next steps

Infrastructure Backup Service reference

Article • 07/29/2022

Azure Stack Hub consists of many services that comprise the portal (Azure Resource

Manager) and the overall infrastructure management experience. The app-like

management experience of Azure Stack Hub focuses on reducing the complexity

exposed to the operator of the solution.

Infrastructure Backup Service is designed to internalize the complexity of backing up

and restoring data for infrastructure services, ensuring operators can focus on managing

the solution and maintaining an SLA to users.

Exporting the backup data to an external share is required to avoid storing backups on

the same system. Requiring an external share gives the admin the flexibility to determine

where to store the data based on existing company BC/DR policies.

Infrastructure Backup Service includes the following components:

Infrastructure Backup Controller

The Infrastructure Backup Controller is instantiated with and resides in every Azure

Stack Hub Cloud.

Backup Resource Provider

The Backup Resource Provider (Backup RP) is composed of the user interface and

APIs exposing basic backup functionality for Azure Stack Hub infrastructure.

The Infrastructure Backup Controller is a Service Fabric service that gets instantiated for

an Azure Stack Hub Cloud. Backup resources are created at a regional level and capture

region-specific service data from AD, CA, Azure Resource Manager, CRP, SRP, NRP, Key

Vault, RBAC.

The Backup Resource Provider presents a user interface in the Azure Stack Hub portal

for basic configuration and listing of backup resources. Operators can do the following

Azure backup infrastructure

Infrastructure Backup Service components

Infrastructure Backup Controller

Backup Resource Provider

actions in the user interface:

Enable backup for the first time by providing external storage location, credentials,

and encryption key.

View completed created backup resources and status resources under creation.

Modify the storage location where Backup Controller places backup data.

Modify the credentials that Backup Controller uses to access external storage

location.

Modify the encryption key that Backup Controller uses to encrypt backups.

This section describes the important requirements for Infrastructure Backup Service. We

recommend you review the info carefully before you enable backup for your Azure Stack

Hub instance, and then refer back to it as necessary during deployment and subsequent

operation.

The requirements include:

Software requirements - describes supported storage locations and sizing

guidance.

Network requirements - describes network requirements for different storage

locations.

Storage location Details

SMB file share hosted on a

storage device within the

trusted network environment.

SMB share in the same datacenter where Azure Stack Hub is

deployed or in a different datacenter. Multiple Azure Stack Hub

instances can use the same file share.

SMB file share on Azure. Not currently supported.

Blob storage on Azure. Not currently supported.

SMB Version

Backup Controller requirements

Software requirements

Supported storage locations

Supported SMB versions

SMB Version

SMB 3.x

Infrastructure Backup Service supports transferring backup data to an external storage

location with SMB encryption enabled on the server side. If the server doesn't support

SMB Encryption or doesn't have the feature enabled, Infrastructure Backup Service will

fall back to unencrypted data transfer. Backup data placed on the external storage

location is always encrypted at rest and isn't dependent on SMB encryption.

We recommend you back up at last two times a day and keep at most seven days of

backups. This is the default behavior when you enable infrastructure backups on Azure

Stack Hub.

Environment Scale Projected size of backup Total amount of space required

4-16 nodes 20 GB 280 GB

ASDK 10 GB 140 GB

Storage location Details

SMB file share hosted on a

storage device within the

trusted network

environment.

Port 445 is required if the Azure Stack Hub instance resides in a

firewalled environment. Infrastructure Backup Controller will

initiate a connection to the SMB file server over port 445.

To use FQDN of file server,

the name must be resolvable

from the PEP.

Make sure to setup firewall rules to allow connectivity between ERCS VMs to the

external storage location.

SMB encryption

Storage location sizing

Network requirements

Firewall rules

Sour Sourcece TTar arget get Pr Prot otocol/P ocol/Por ortt

ERCS VM 1 Storage location 445/SMB

ERCS VM 2 Storage location 445/SMB

ERCS VM 3 Storage location 445/SMB

The Infrastructure Backup Service will use a certificate with a public key (.CER) to encrypt

backup data and a certificate with the private key (.PFX) to decrypt backup data during

cloud recovery. The certificate key length must be 2048 bytes.

The certificate is used for transport of keys and isn't used to establish secure

authenticated communication. For this reason, the certificate can be a self-signed

certificate. Azure Stack Hub doesn't need to verify root or trust for this certificate

so external internet access isn't required.

The self-signed certificate comes in two parts, one with the public key and one with the

private key:

Encrypt backup data: Certificate with the public key (exported to .CER file) is used

to encrypt backup data.

Decrypt backup data: Certificate with the private key (exported to .PFX file) is used

to decrypt backup data.

The certificate with the public key (.CER) isn't managed by internal secret rotation. To

rotate the certificate, you need to create a new self-signed certificate and update

backup settings with the new file (.CER).

All existing backups remain encrypted using the previous public key. New backups

use the new public key.

The certificate used during cloud recovery with the private key (.PFX) is not persisted by

Azure Stack Hub for security reasons. This file will need to be provided explicitly during

cloud recovery.

７ Note

No inbound ports need to be opened.

Encryption Requirements

Consider these limits as you plan, deploy, and operate your Microsoft Azure Stack Hub

instances. The following table describes these limits.

Limit identifier Limit Comments

Backup type Full only Infrastructure Backup Controller only supports full

backups. Incremental backups aren't supported.

Scheduled backups Scheduled

and

manual

Backup controller supports scheduled and on-demand

backups.

Maximum concurrent

backup jobs

1 Only one active backup job is supported per instance of

Backup Controller.

Network switch

configuration

Not in

scope

Admin must back up network switch configuration using

OEM tools. Refer to documentation for Azure Stack Hub

provided by each OEM vendor.

Hardware Lifecycle Host Not in

scope

Admin must back up Hardware Lifecycle Host using

OEM tools. Refer to documentation for Azure Stack Hub

provided by each OEM vendor.

Maximum number of file

shares

1 Only one file share can be used to store backup data.

Backup App Services,

Function, SQL, mysql

resource provider data

Not in

scope

Refer to guidance published for deploying and

managing value-add RPs created by Microsoft.

Backup third-party

resource providers

Not in

scope

Refer to guidance published for deploying and

managing value-add RPs created by third-party vendors.

To learn more about the Infrastructure Backup Service, see Backup and data

recovery for Azure Stack Hub with the Infrastructure Backup Service.

Infrastructure Backup Limits

Infrastructure Backup limits

Next steps

Azure Stack Hub Operator Access

Workstation

Article • 07/29/2022

The Operator Access Workstation (OAW) is used to deploy a virtual machine (VM) on an

Azure Stack Hub's--Hardware Lifecycle Host (HLH) or any other machine that runs

Microsoft Hyper-V. It does require network connectivity to the Azure Stack Hub

endpoints to be used for operator or user scenarios.

The OAW VM is an optional virtual machine that isn't required by Azure Stack Hub to

function. Its purpose is to provide the latest tools to operators or user as they interact

with Azure Stack Hub.

The following tables list common scenarios for the OAW. Use Remote Desktop to

connect to the OAW.

Scenario Description

Access the

Administration portal

Perform administrative operations.

Access PEP Log collection and upload:

-Create an SMB share on the HLH for file transfer from Azure Stack Hub.

-Use Azure Storage Explorer to upload logs saved to the SMB share.

Register Azure Stack

Hub

For re-registration, get previous Registration Name and Resource Group

from the Administration portal.

Marketplace

syndication

Create an SMB share on the HLH to store the downloaded image or

extension.

Create Virtual

Machines

Create virtual machines using Azure CLI.

Manage AKS Manage AKS clusters, for example, scale or upgrade.

The following table lists the pre-installed software on the OAW VM.

OAW scenarios

Pre-installed software

Software Name Location

Microsoft Edge for Business [SystemDrive]\Program Files (x86)\Microsoft\Edge\Application

Az Modules [SystemDrive]\ProgramFiles\WindowsPowerShell\Modules

PowerShell 7 [SystemDrive]\Program Files\PowerShell\7

Azure Command-Line Interface

(CLI)

[SystemDrive]\Program Files (x86)\Microsoft SDKs\Azure\CLI2

Microsoft Azure Storage

Explorer

[SystemDrive]\Program Files (x86)\Microsoft Azure Storage

Explorer

AzCopy [SystemDrive]\VMSoftware\azcopy\_windows\_amd64\_\*

AzureStack-Tools [SystemDrive]\VMSoftware\AzureStack-Tools

To get the files to create the OAW VM, download here . Be sure to review the Microsoft

Privacy Statement and Legal Terms before you download.

Because of the stateless nature of the solution, there are no updates for the OAW VM.

For each milestone, a new version of the VM image file is released. Use the latest version

to create a new OAW VM. The image file is based on the latest Windows Server 2019

version. After installation, you can apply updates, including any critical updates, using

Windows Update.

Validate the hash of the downloaded OAW.zip file to make sure it hasn't been modified

before using it to create the OAW VM. Run the following PowerShell script. If the return

value is True, you can use the downloaded OAW.zip:

PowerShell

Download files

７ Note

Unblock the script files after extracting the download.

param(

[Parameter(Mandatory=$True)]

[ValidateNotNullOrEmpty()]

[ValidateScript({Test-Path $\_ -PathType Leaf})]

[string]

$DownloadedOAWZipFilePath

)

Another way to copy this script to your environment is to use the Test-FileHash cmdlet

that's offered in AzureStack-Tools to verify the hash of the OAW.zip file:

1. Download the Test-FileHash.psm1 file from GitHub, and then run:

PowerShell

2. After you import the Test-FileHash module, verify the hash of the OAW.zip file:

PowerShell

1. Sign in to the HLH with your credentials.

2. Open PowerShell ISE and run the following script:

PowerShell

$expectedHash =

'2F6242F122532E176A5FACD694C132D3DAFD50D0F17F5F23F26A8102C7BA6157'

$actualHash = (Get-FileHash -Path $DownloadedOAWZipFilePath).Hash

Write-Host "Expected hash: $expectedHash"

if ($expectedHash -eq $actualHash)

{

Write-Host 'SUCCESS: OAW.zip file hash matches.'

}

else

{

Write-Error "ERROR: OAW.zip file hash does not match! It isn't safe to

use it, please download it again. Actual hash: $actualHash"

}

Import-Module .\Test-FileHash.psm1 -Force -Verbose

Test-FileHash -ExpectedHash

"2F6242F122532E176A5FACD694C132D3DAFD50D0F17F5F23F26A8102C7BA6157" -

FilePath "<path to the OAW.zip file>"

Check HLH version

７ Note

This step is important to determine if you deploy the OAW on a HLH that was

deployed using a Microsoft image or an OEM image. This PowerShell cmdlet is not

present on a HLH that was deployed using an OEM image. If you deploy the OAW

on a general Microsoft Hyper-V, you can skip this step.

For example:

The following script prepares the virtual machine as the Operator Access Workstation

(OAW), which is used to access Microsoft Azure Stack Hub.

1. Sign in to the HLH with your credentials.

2. Download OAW.zip and extract the files.

3. Open an elevated PowerShell session.

4. Navigate to the extracted contents of the OAW.zip file.

5. Run the New-OAW.ps1 script.

PowerShell

PowerShell

C:\Version\Get-Version.ps1

Create the OAW VM using a script

Example: Deploy on HLH using a Microsoft Image

$oawRootPath = "D:\oawtest"

$securePassword = Read-Host -Prompt "Enter password for Azure Stack OAW's

local administrator" -AsSecureString

if (Get-ChildItem -Path $oawRootPath -Recurse | Get-Item -Stream Zone\* -

ErrorAction SilentlyContinue | Select-Object FileName)

{ Write-Host "Execution failed, unblock the script files first" }

else { .\New-OAW.ps1 -LocalAdministratorPassword $securePassword }

Example: Deploy on HLH using an OEM Image

If the AzureStackStampInformation.json file includes the naming prefix for OAW VM, that

value will be used for the VirtualMachineName parameter. Otherwise, the default name is

AzSOAW or whatever name specified is by the user. The AzureStackStampInformation.json

can be re-created using the privileged endpoint in case it is not present on the HLH.

The machine running Microsoft Hyper-V does requires four (4) cores and two (2) GB of

available memory. The PowerShell cmdlets will create the OAW VM without applying an

IP configuration to the guest network interface. If you use the example to provision the

OAW on a HLH you must configure the IP Address originally used by the Deployment

VM (DVM), which is typically the second to last IP of the BMC Network.

Examples IPs

BMC Network 10.26.5.192/26

First Host IP 10.26.5.193

Last Host IP 10.26.5.254

DVM/OAW IP 10.26.5.253

Subnet Mask 255.255.255.192

$oawRootPath = "D:\oawtest"

$securePassword = Read-Host -Prompt "Enter password for Azure Stack OAW's

local administrator" -AsSecureString

if (Get-ChildItem -Path $oawRootPath -Recurse | Get-Item -Stream Zone\* -

ErrorAction SilentlyContinue | Select-Object FileName)

{ Write-Host "Execution failed, unblock the script files first" }

else { .\New-OAW.ps1 -LocalAdministratorPassword $securePassword -

AzureStackCertificatePath 'F:\certroot.cer' -DeploymentDataFilePath

'F:\DeploymentData.json' -AzSStampInfoFilePath

'F:\AzureStackStampInformation.json' }

７ Note

The parameter AzureStackCertificatePath should only be used when Azure Stack

Hub was deployed using certificates issued from an enterprise certificate authority.

If the DeploymentData.json is not available, reach out to your hardware partner to

retrieve it or continue with the example deploy on Microsoft Hyper-V.

Example: Deploy on Microsoft Hyper-V

Examples IPs

Default Gateway 10.26.5.193

PowerShell

The following user account policy is applied to the OAW VM:

Built-in Administrator username: AdminUser

MinimumPasswordLength = 14

PasswordComplexity is enabled

MinimumPasswordAge = 1 (day)

MaximumPasswordAge = 42 (days)

NewGuestName = GUser (disabled by default)

Two parameter sets are available for New-OAW. Optional parameters are shown in

brackets.

PowerShell

$oawRootPath = "D:\oawtest"

$securePassword = Read-Host -Prompt "Enter password for Azure Stack OAW's

local administrator" -AsSecureString

if (Get-ChildItem -Path $oawRootPath -Recurse | Get-Item -Stream Zone\* -

ErrorAction SilentlyContinue | Select-Object FileName)

{ Write-Host "Execution failed, unblock the script files first" }

else { .\New-OAW.ps1 -LocalAdministratorPassword $securePassword -

AzureStackCertificatePath 'F:\certroot.cer' `-SkipNetworkConfiguration -

VirtualSwitchName Example }

７ Note

The parameter AzureStackCertificatePath should only be used when Azure Stack

Hub was deployed using certificates issued from an enterprise certificate authority.

The OAW virtual machine will be deployed without a network configuration. You

can configure a static IP address or retrieve an IP address via DHCP.

User account policy

New-OAW cmdlet parameters

PowerShell

New-OAW

-LocalAdministratorPassword <Security.SecureString> `

[-AzureStackCertificatePath <String>] `

[-AzSStampInfoFilePath <String>] `

[-CertificatePassword <Security.SecureString>] `

[-ERCSVMIP <String[]>] `

[-DNS <String[]>] `

[-DeploymentDataFilePath <String>] `

[-SkipNetworkConfiguration] `

[-ImageFilePath <String>] `

[-VirtualMachineName <String>] `

[-VirtualMachineMemory <int64>] `

[-VirtualProcessorCount <int>] `

[-VirtualMachineDiffDiskPath <String>] `

[-PhysicalAdapterMACAddress <String>] `

[-VirtualSwitchName <String>] `

[-ReCreate] `

[-AsJob] `

[-Passthru] `

[-WhatIf] `

[-Confirm] `

[<CommonParameters>]

New-OAW

-LocalAdministratorPassword <Security.SecureString> `

-IPAddress <String> `

-SubnetMask <String> `

-DefaultGateway <String> `

-DNS <String[]> `

-TimeServer<String> `

[-AzureStackCertificatePath <String>] `

[-AzSStampInfoFilePath <String>] `

[-CertificatePassword <Security.SecureString>] `

[-ERCSVMIP <String[]>] `

[-ImageFilePath <String>] `

[-VirtualMachineName <String>] `

[-VirtualMachineMemory <int64>] `

[-VirtualProcessorCount <int>] `

[-VirtualMachineDiffDiskPath <String>] `

[-PhysicalAdapterMACAddress <String>] `

[-VirtualSwitchName <String>] `

[-ReCreate] `

[-AsJob] `

[-Passthru] `

[-WhatIf] `

[-Confirm] `

[<CommonParameters>]

The following table lists the definition for each parameter.

Parameter Required/Optional Description

LocalAdministratorPassword Required Password for the virtual machine's local

administrator account AdminUser.

IPAddress Required The static IPv4 address to configure TCP/IP

on the virtual machine.

SubnetMask Required The IPv4 subnet mask to configure TCP/IP on

the virtual machine.

DefaultGateway Required IPv4 address of the default gateway to

configure TCP/IP on the virtual machine.

DNS Required DNS server(s) to configure TCP/IP on the

virtual machine.

TimeServer Required IP address of the time server that Azure

Stack Hub syncs from, which will be the time

source that OAW syncs from too. Check the

AzureStackStampInformation.json or ask

your admin for the IP of the time server that

Hub syncs from. In case of urgency and you

could not get the IP of the time server that

Hub syncs from, you could input the default

time server, 'time.windows.com,0x8' for this

parameter. Note that it is highly

recommended to make sure the time in

OAW and Hub is in sync to avoid potential

clock skew issues when working in an OAW

to interact with Hub.

ImageFilePath Optional Path of OAW.vhdx provided by Microsoft.

Default value is OAW.vhdx under the same

parent folder of this script.

VirtualMachineName Optional The name to be assigned to the virtual

machine. If the Naming Prefix can be found

in the DeploymentData.json file, it will be

used as the default name. Otherwise,

AzSOAWwill be used as the default name.

You can specify another name to overwrite

the default value.

VirtualMachineMemory Optional Memory to be assigned to the virtual

machine. Default value is 2 GB.

VirtualProcessorCount Optional Number of virtual processors to be assigned

to the virtual machine. Default value is 4.

Parameter Required/Optional Description

VirtualMachineDiffDiskPath Optional Path to store temporary diff disk files while

the management VM was active. Default

value is DiffDisks subdirectory under the

same parent folder of this script.

AzureStackCertificatePath Optional Path of certificates to be imported to the

virtual machine for Azure Stack Hub access.

AzSStampInfoFilePath Optional Path of AzureStackStampInformation.json file

where the script can retrieve the IPs of the

ERCS VM.

CertificatePassword Optional Password of certificate to be imported to the

virtual machine for Azure Stack Hub access.

ERCSVMIP Optional IP of Azure Stack Hub ERCS VM(s) to be

added to trusted host list of the virtual

machine. Won't take effect if -

SkipNetworkConfiguration is set.

SkipNetworkConfiguration Optional Skips network configuration for the virtual

machine so user can configure later.

DeploymentDataFilePath Optional Path of DeploymentData.json. Won't take

effect if -SkipNetworkConfiguration is set.

PhysicalAdapterMACAddress Optional The MAC address of the host's network

adapter that will be used to connect the

virtual machine to.

- If there's only one physical network

adapter, this parameter isn't needed and the

only network adapter will be used.

- If there's more than one physical network

adapter, this parameter is required to specify

which one to use.

VirtualSwitchName Optional The name of virtual switch that needs to be

configured in Hyper-V for the virtual

machine.

- If there's VMSwitch with the provided

name, such VMSwitch will be selected.

- If there's no VMSwitch with the provided

name, a VMSwitch will be created with the

provided name.

Re-Create Optional Removes and re-creates the virtual machine

if there's already an existed virtual machine

with the same name.

1. Sign into the OAW VM with your credentials.

2. Open PowerShell ISE and run the following script:

PowerShell

For example:

If you need to transfer files between the HLH and the OAW, create an SMB share by

using the New-SmbShare cmdlet. New-SmbShare exposes a file system folder to remote

clients as a Server Message Block (SMB) share. For example:

To delete a share that was created by this cmdlet, use the Remove-SmbShare cmdlet.

The following script removes the OAW VM, which is used to access Azure Stack Hub for

administration and diagnostics. This script also removes the disk files and the guardian

associated with the VM.

1. Sign into the HLH with your credentials.

2. Open an elevated PowerShell session.

3. Navigate to the extracted contents of the installed OAW.zip file.

4. Remove the VM by running the Remove-OAW.ps1 script:

PowerShell

Check the OAW VM version

C:\Version\Get-Version.ps1

Transfer files between the HLH and OAW

Remove the OAW VM

.\Remove-OAW.ps1 -VirtualMachineName \<name\>

Where <name> is the name of the virtual machine to be removed. By default, the

name is AzSOAW.

For example:

PowerShell

Azure Stack Management Tasks

.\Remove-OAW.ps1 -VirtualMachineName AzSOAW

Next steps

Azure Stack Hub help and support

Article • 07/29/2022

Azure Stack Hub operators can use Help + support to collect diagnostic logs and send

them to Microsoft for troubleshooting. Help + support in the Azure Stack Hub portal

can be accessed from the administrator portal. It has resources to help operators learn

more about Azure Stack, check their support options, and get expert help.

Operators can use Help + support to learn more about Azure Stack Hub, check their

support options, and get expert help.

At the top of Help + support are things you should try first, like read about new

concepts, learn how billing works, or see which support options are available.

Help resources

Things to try first

Documentation. Azure Stack Hub Operator Documentation includes concepts,

how-to instructions, and tutorials that show how to offer Azure Stack Hub services.

These services include virtual machines, SQL databases, web apps, and more.

Learn about billing. Get tips on usage and billing.

Support options. Azure Stack Hub operators can choose from a range of Azure

support options that can fit the needs of any enterprise.

For an integrated system, there's a coordinated escalation and resolution process

between Microsoft and our original equipment manufacturer (OEM) hardware partners.

If there's a cloud services issue, support is offered through Microsoft Support. You can

select Help (question mark) in the upper-right corner of the administrator portal and

then select Help + support to open Help + Support Overview and submit a new

support request. Creating a support request will preselect Azure Stack Hub service. We

highly recommend that customers use this experience to submit tickets rather than

using the Global Azure portal.

If there's an issue with deployment, patch and update, hardware (including field

replaceable units), and any hardware-branded software (like software running on the

hardware lifecycle host), contact your OEM hardware vendor first. For anything else,

contact Microsoft Support.

Get expert help

For the Azure Stack Development Kit (ASDK), you can ask support-related questions in

the Azure Stack Hub MSDN Forum .

Select Help (question mark) in the upper-right corner of the administrator portal and

then select Help + support to open Help + Support Overview, which has a link to the

forum. MSDN forums are regularly monitored. Because the ASDK is an evaluation

environment, there's no official support offered through Microsoft Support.

You can also reach out to the MSDN Forums to discuss an issue, or take online training

and improve your own skills.

To speed up your support experience, have the following information:

Are you an Azure Stack Hub hardware partner?

How many Azure Stack Hub nodes are you in your system?

What is the current patch level for your system?

What build number is your system currently running?

What is the name of your cloud's region?

Is a connected or disconnected system?

When did the problem start?

Can you provide the exact time when the last backup failed?

For what roles is the backup failing?

Did you perform any recent changes? For example, did you perform an update,

make a hardware change, or apply an OEM update?

Are you able to provide logs in order to investigate the issue?

This set of tutorials is customized depending on whether you're running the ASDK or

integrated systems so you can quickly get up to speed with your environment.

Information for a support request

Get up to speed with Azure Stack Hub

You can send diagnostic logs to Microsoft in two ways:

Send logs proactively: If enabled, log collection is triggered by specific health

alerts.

Send logs now: You can manually choose a specific sliding window as the time

frame for log collection.

Learn about diagnostic log collection.

Learn how to find your Cloud ID.

Learn about troubleshooting Azure Stack Hub.

Diagnostic log collection

Next steps

Find your Cloud ID

Article • 07/29/2022

This topic covers how to get your Cloud ID by using the Administrator portal or the

privileged endpoint (PEP). The Cloud ID is the unique ID for tracking support data

uploaded from a specific scale unit. When diagnostic logs are uploaded for support

analysis, the Cloud ID is how the logs are associated with that scale unit.

1. Open the Administrator portal.

2. Select Region management.

3. Select Properties and copy the Stamp Cloud ID.

Use the administrator portal

1. Open an elevated PowerShell session and run the following script. Replace the IP

address of the PEP VM and Cloud Admin credentials as needed for your

environment.

PowerShell

Send logs proactively

Send logs now

Use the privileged endpoint

$ipAddress = "<IP ADDRESS OF THE PEP VM>" # You can also use the

machine name instead of IP here.

$password = ConvertTo-SecureString "<CLOUD ADMIN PASSWORD>" -

AsPlainText -Force

$cred = New-Object -TypeName System.Management.Automation.PSCredential

("<DOMAIN NAME>\CloudAdmin", $password)

$session = New-PSSession -ComputerName $ipAddress -ConfigurationName

PrivilegedEndpoint -Credential $cred -SessionOption (NewPSSessionOption -Culture en-US -UICulture en-US)

$stampInfo = Invoke-Command -Session $session { GetAzureStackStampInformation }

if ($session) {

Remove-PSSession -Session $session

}

$stampInfo.CloudID

Next steps

Diagnostic log collection

Article • 06/01/2023

You can share diagnostic logs created by Azure Stack Hub. The Windows components

and on-premises Azure services create these logs. Microsoft Support can use the logs to

fix or identify issues with your Azure Stack Hub instance.

To get started with Azure Stack Hub diagnostic log collection, you have to register your

instance. If you haven't registered Azure Stack Hub, use the privileged endpoint (PEP) to

share logs.

You have multiple ways to send diagnostic logs to Microsoft Support. Depending on

your connectivity to Azure, your options include:

Send logs proactively (recommended)

Send logs now

Save logs locally

The flowchart shows which option to use for sending diagnostic logs. If Azure Stack Hub

connects to Azure, enable Proactive log collection. Proactive log collection

automatically uploads diagnostic logs to a Microsoft-controlled storage blob in Azure

when a critical alert gets raised. You can also collect logs on-demand by using Send logs

now. For an Azure Stack Hub that runs in a disconnected environment, or if you're

having connectivity issues, choose to Save logs locally.

Send logs proactively

Proactive log collection automatically collects and sends diagnostic logs from Azure

Stack Hub to Microsoft before you open a support case. Only when a system health alert

is raise are these logs collected. Microsoft Support only accesses these logs in the

context of a support case.

Beginning with Azure Stack Hub version 2008, proactive log collection uses an improved

algorithm to capture logs even during error conditions that aren't visible to an operator.

This improvement helps ensure that the right diagnostic info is collected at the right

time without needing any operator interaction. Microsoft support can begin

troubleshooting and resolve problems sooner in some cases. Initial algorithm

improvements focus on patch and update operations.

When an event triggers these alerts, Azure Stack Hub proactively sends the logs to

Microsoft. In addition, Azure Stack Hub sends logs to Microsoft triggered by other

failure events. These events are not visible to the operator.

Enabling proactive log collection is highly recommended. It allows the product team to

diagnose problems due to failure events and improve the quality of the product.

Azure Stack Hub proactively collects logs for:

Alert Fault ID type

Update needs attention Urp.UpdateWarning

Update failed Urp.UpdateFailure

Proactive log collection can be disabled and re-enabled anytime. Follow these steps to

set up proactive log collection.

1. Sign in to the Azure Stack Hub administrator portal.

2. Open Help + support Overview.

3. If the banner appears, select Enable proactive log collection. Or you can select

Settings and set Proactive log collection to Enable, then select Save.

７ Note

If proactive log collection is enabled and you renew or change your Azure Stack

Hub registration, as described in Renew or change registration, you must reenable proactive log collection.

７ Note

You agree to periodic automatic log collections by Microsoft based only on Azure Stack

Hub system health alerts. You also acknowledge and consent to the upload and

retention of those logs in an Azure storage account managed and controlled by

Microsoft.

The data is used for troubleshooting system health alerts and isn't used for marketing,

advertising, or any other commercial purposes without your consent. The data can be

retained for up to 90 days and Microsoft handles any data collected following our

standard privacy practices .

The revocation of your permission doesn't affect any data previously collected with your

consent.

Logs collected using Proactive log collection are uploaded to an Azure storage account

managed and controlled by Microsoft. Microsoft might access these logs in the context

of a support case and to improve the health of Azure Stack Hub.

Send logs now is an option where you manually collect and uploads your diagnostic

logs from Azure Stack Hub, usually before opening a support case.

There are two ways you can manually send diagnostic logs to Microsoft Support:

Administrator portal (recommended)

PowerShell

If Azure Stack Hub is connected to Azure, we recommend using the administrator portal

because it's the simplest way to send the logs directly to Microsoft. If the portal is

unavailable, you should send logs using PowerShell.

If log location settings are configured for a local file share, make sure lifecycle

management policies will prevent share storage from reaching its size quota. Azure

Stack Hub does not monitor local file share or enforce any retention policies.

How the data is handled

Send logs now

 Tip

Save time by using Send logs proactively instead of Send logs now.

To send logs now using the administrator portal:

1. Open Help + support > Log Collection > Send logs now.

2. Specify the start time and end time for log collection.

3. Choose the local time zone.

4. Select Collect and Upload.

If you're disconnected from the internet or want to only save logs locally, use the GetAzureStackLog method to send logs.

If you're using the Send logs now method and want to use PowerShell instead of the

administrator portal, you can use the Send-AzureStackDiagnosticLog cmdlet to collect

and send specific logs.

The FromDate and ToDate parameters can be used to collect logs for a particular

time period. If these parameters aren't specified, logs are collected for the past

four hours by default.

Use the FilterByNode parameter to filter logs by computer name. For example:

PowerShell

Use the FilterByLogType parameter to filter logs by type. You can choose to filter

by File, Share, or WindowsEvent. For example:

PowerShell

Use the FilterByResourceProvider parameter to send diagnostic logs for value-add

Resource Providers (RPs). The general syntax is:

７ Note

If you send logs using the administrator portal or PowerShell cmdlet, TestAzureStack runs automatically in the background to collect diagnostic information.

Send logs now with the administrator portal

Send logs now with PowerShell

Send-AzureStackDiagnosticLog -FilterByNode azs-xrp01

Send-AzureStackDiagnosticLog -FilterByLogType File

PowerShell

To send diagnostic logs for SQL RP:

PowerShell

To send diagnostic logs for MySQL RP:

PowerShell

To send diagnostic logs for Event Hubs:

PowerShell

To send diagnostic logs for Azure Stack Edge:

PowerShell

Use the FilterByRole parameter to send diagnostic logs from VirtualMachines and

BareMetal roles:

PowerShell

To send diagnostic logs from VirtualMachines and BareMetal roles, with date

filtering for log files for the past 8 hours:

PowerShell

Send-AzureStackDiagnosticLog -FilterByResourceProvider <<value-add RP

name>>

Send-AzureStackDiagnosticLog -FilterByResourceProvider SQLAdapter

Send-AzureStackDiagnosticLog -FilterByResourceProvider MySQLAdapter

Send-AzureStackDiagnosticLog -FilterByResourceProvider eventhub

Send-AzureStackDiagnosticLog -FilterByResourceProvide databoxedge

Send-AzureStackDiagnosticLog -FilterByRole VirtualMachines,BareMetal

$fromDate = (Get-Date).AddHours(-8)

Invoke-Command -Session $pepsession -ScriptBlock {Send-

To send diagnostic logs from VirtualMachines and BareMetal roles, with date

filtering for log files for the time period between 8 hours ago and 2 hours ago:

PowerShell

By initiating diagnostic log collection from Azure Stack Hub, you acknowledge and

consent to uploading those logs and retaining them in an Azure storage account

managed and controlled by Microsoft. Microsoft Support can access these logs right

away with the support case without having to engage with the customer for log

collection.

You can save logs to a local Server Message Block (SMB) share when Azure Stack Hub is

disconnected from Azure. You may, for example, run a disconnected environment. If

you're normally connected but are experiencing connectivity issues, you can save logs

locally to help with troubleshooting.

In the Settings blade, enter the path and a username and password with permission to

write to the share. During a support case, Microsoft Support works to provide detailed

steps on how to get these local logs transferred. If the Administrator portal is

unavailable, you can use Get-AzureStackLog to save logs locally.

AzureStackDiagnosticLog -FilterByRole VirtualMachines,BareMetal -

FromDate $using:fromDate}

$fromDate = (Get-Date).AddHours(-8)

$toDate = (Get-Date).AddHours(-2)

Invoke-Command -Session $pepsession -ScriptBlock {SendAzureStackDiagnosticLog -FilterByRole VirtualMachines,BareMetal -

FromDate $using:fromDate -ToDate $using:toDate}

７ Note

If you're disconnected from the internet or want to only save logs locally, use GetAzureStackLog method to send logs.

How the data is handled

Save logs locally

The average size of diagnostic log collection varies based on whether it runs proactively

or manually. The average size for Proactive log collection is around 2 GB. The collection

size for Send logs now depends on how many hours (up to 4 hours) are being collected

and the number of physical nodes in the Azure Stack Hub scale unit (4 to 16 nodes).

The following table lists considerations for environments with limited or metered

connections to Azure.

Network connection Impact

Low-bandwidth/high-latency

connection

Log upload takes an extended amount of time to complete.

Shared connection The upload may also affect other apps/users sharing the

network connection.

Bandwidth considerations

Network connection Impact

Metered connection There may be another charge from your ISP for the extra

network usage.

For example, if the internet connection or link speed from Azure Stack Hub is 5

Megabits/second (low-bandwidth), it would take approximately 57 minutes to upload 2

GB of diagnostic log data to Microsoft support. For an 8 GB manual log collection using

a 5 Megabits/second link speed, it would take approx. 3 hours and 49 minutes to upload

the data. This extended length of time to upload diagnostic data could delay or affect

the support experience.

The history of logs collected from Azure Stack Hub appears on the Log collection page

in Help + support, with the following dates and times:

Time Collected: When the log collection operation began.

Status: Either in progress or complete.

Logs start: Start of the time period for which you want to collect.

Logs end: End of the time period.

Type: If it's a manual or proactive log collection.

Azure Stack Hub log and customer data handling

View log collection

See also

Remote support for Azure Stack Hub

Article • 07/27/2023

Use remote support to allow a Microsoft support professional to diagnose and help

speed resolution of your support request by permitting remote access to your device for

limited troubleshooting and repair. You can enable this feature by granting consent for a

specific access level and duration. Support can only access your device after a support

request has been submitted.

Once enabled, Microsoft support gets just-in-time (JIT) limited time access to your

device over a secure, audited, and compliant channel. Remote support uses protocol

HTTPS over port 443. The traffic is encrypted with TLS 1.2. Operations performed are

restricted based on the access level granted using just enough administration (JEA).

For more information about cmdlets that Microsoft support can execute during a

remote support session, see the list of Microsoft Support operations section in this

article.

） Important

Remote support is only available in the following versions:

2206

2108

2102 with hotfix 1.2102.30.132 and later

Remote support gives you the ability to:

Improve the speed to resolution. After the initial scoping consultation with

Microsoft Support, you can enable remote support. At that point Microsoft

Support no longer needs to arrange meetings with you for further

troubleshooting.

Reduce the number of privileged endpoint (PEP) session elevation to resolve

issues.

View the detailed transcript of all executed operations at any time.

Grant just-in-time authenticated access on an incident-by-incident basis. You can

define the access level and duration for each incident.

You can revoke consent at any time which terminates the remote session. Access is

automatically disabled once the consent duration expires.

Remote support requires you to allow access to certain outbound ports and destination

URLs. For more information on required endpoints, see Ports and URLs (outbound).

Why use remote support?

Requirements

Consent

Before remote support is enabled, you must provide consent to authorize Microsoft

Support to execute diagnostic or repair commands. The following text includes the data

handling terms:

By approving this request, the Microsoft support organization or the Azure

engineering team supporting this feature ("Microsoft Support Engineer") will be

given direct access to your device for troubleshooting purposes and/or resolving

the technical issue described in the Microsoft support case.

During a remote support session, a Microsoft Support Engineer may need to collect

logs. By enabling remote support, you have agreed to a diagnostic logs collection

by Microsoft Support Engineer to address a support case You also acknowledge and

consent to the upload and retention of those logs in an Azure storage account

managed and controlled by Microsoft. These logs may be accessed by Microsoft in

the context of a support case and to improve the health of Azure Stack Hub.

The data will be used only to troubleshoot failures that are subject to a support

ticket, and will not be used for marketing, advertising, or any other commercial

purposes without your consent. The data may be retained for up to ninety (90) days

and will be handled following our standard privacy practices.

Any data previously collected with your consent will not be affected by the

revocation of your permission.

In Azure Stack Hub, remote support can be managed using privileged endpoint (PEP).

The following example scenarios show you how to perform various operations to enable

remote support access for Microsoft support.

In this example, you enable remote support access for diagnostic-related operations

only. The consent expires in 1,440 minutes (one day) after which remote access cannot

be established.

PowerShell

Use ExpireInMinutes parameter to set the duration of the session. In the example,

consent expires in 1,440 minutes (one day). After one day, remote access cannot be

Remote support examples

Enable remote support for diagnostics

Enable-RemoteSupport -AccessLevel Diagnostics -ExpireInMinutes 1440

established.

You can set ExpireInMinutes a minimum duration of 60 minutes (one hour) and a

maximum of 20,160 minutes (14 days).

If duration is not defined the remote session will expire in 480 (8 hours) by default.

In this example, you enable remote support access for diagnostic and repair related

operations only. Because expiration was not explicitly provided, it expires in eight hours

by default.

PowerShell

In this example, you retrieve any previously granted consent. The result includes expired

consent in the last 30 days.

PowerShell

In this example, you revoke remote access consent. Any existing sessions are terminated

and new sessions can no longer be established.

PowerShell

In this example, you list all the remote sessions that were made to the device since

FromDate.

PowerShell

Enable remote support for diagnostics and repair

Enable-RemoteSupport -AccessLevel DiagnosticsRepair

Retrieve existing consent grants

Get-RemoteSupportAccess -IncludeExpired

Revoke remote access consent

Disable-RemoteSupport

List existing remote sessions

In this example, you get the details for remote session with the ID SessionID.

PowerShell

The following sections list the allowed cmdlets that Microsoft support can execute

during a remote support session.

Name Description

Clear-AzsSupportParentWorkingDirectory Clears stale Azs.Support working directory

contents across all infrastructure nodes.

Clear-AzsSupportWorkingDirectory Clears the contents of the current working

directory.

Copy-AzsSupportFiles Copies files from the remote computer to the

local working directory file path location (GetAzsSupportWorkingDirectory).

Debug-AzsSupportStorageSubsystem Runs Debug-StorageSubSystem against

Storage Sub System Clustered Windows

Storage on \*.

Disable-AzsSupportNetshTrace Disables netsh tracing.

Enable-AzsSupportNetshTrace Enables netsh tracing.

Get-RemoteSupportSessionHistory -FromDate <Date>

Get details on a specific remote session

Get-RemoteSupportSessionHistory -SessionId <SessionId> -

IncludeSessionTranscript

７ Note

Session transcript details are retained for ninety days. You can retrieve detail for a

remote session within ninety days after the session.

List of Microsoft support operations

Access level: Diagnostics

Name Description

Get-AzsSupportActionPlanInstance Lists ECE Action plans and provides options for

filtering by name and status. This command

has two behaviors:

Default: Lists all action plan instances (backup

plans filtered out by default), their IDs, status,

and timestamps

ActionPlanInstanceId: Drills into a specified

action plan and lists the step, name, status,

and timestamps

Get-AzsSupportClusterLog Generates a failover cluster log for the

specified nodes and returns the file path to the

log. If no nodes are specified, generates cluster

log from all nodes.

Get-AzsSupportClusterResource Gets cluster resources, sorted by state.

Get-AzsSupportClusterSharedVolume Returns a list of all the cluster shared volumes,

sorted by state.

Get-AzsSupportCodeIntegrityEnforcementStatus Gets the kernel and user mode Code Integrity

status.

Get-AzsSupportComputerInformation Collects computer information from the

specified ComputerName such as Uptime,

Localtime, OSVersion, etc. This is a wrapper for

Get-ComputerInfo .

Get-AzsSupportDiskSpace Get available disk space on target computers.

Get-AzsSupportDscLogs Gets Desired State Configuration (DSC)

text/event logs from the specified

ComputerName.

Get-AzsSupportECECloudDefinitionXml Retrieves the Azure Stack cloud definition from

ECE and caches the data as an XmlDocument.

If ECE is unavailable, attempts to load ECE from

a well-known backup location.

Get-AzsSupportECEComputerRole Retrieves a specified ComputerName's role

from ECE.

Get-AzsSupportECERoleDefinition Retrieves role-specific information from ECE.

Get-AzsSupportECERoleNodes Retrieves nodes information from ECE for a

given role.

Get-AzsSupportECERoleProvisioningStatus Get the provisioning status for virtual

machines and physical nodes.

Name Description

Get-AzsSupportFolderSize Get the size of folders and files found in the

Path parameter on an infrastructure VM or

physical node.

Get-AzsSupportInfrastructureHost Gets physical host node information from

FailoverClustering.

Get-AzsSupportInfrastructureVM Gets Hyper-V VM objects for infrastructure

VMs such as ACS or SeedRingServices.

Get-AzsSupportInfrastructureVMHost Retrieves Hyper-V VM objects for

infrastructure VMs such as ACS or

SeedRingServices.

Get-AzsSupportManagedDiskBlobUriAndFilePath Gets the blob uri of a managed disk.

Get-AzsSupportPerformanceMetrics Calls Test-AzureStack -Include

AzsInfraPerformance -Debug and returns all

host and infrastructure VM performance

metrics.

Get-AzsSupportProcess Gets processes on a remote computer, and

sorts them by Name, ProcessID. Supports WMI,

WinRM, and Tasklist /SVC.

Get-AzsSupportRoutingInformation Gets detailed information for failed action

plans and provides guidance on which

engineering team owns the component.

Get-AzsSupportSClusterFileSize Gets file size in s-cluster from local file path.

Get-AzsSupportS2SConnectionInformation Gets the connections associated with a tenant

virtual network gateways.

Get-AzsSupportService Gets services on a specified ComputerName,

and sorts them by State, Name. Supports WMI,

and WinRM.

GetAzsSupportServiceFabricClusterConfiguration

Gets the Service Fabric cluster configuration

for a given ring.

Get-AzsSupportServiceFabricClusterHealth Gets the aggregated cluster health across a

specified ring. If no ring is specified, it checks

all Service Fabric rings.

Get-AzsSupportServiceFabricClusterManifest Gets the Service Fabric cluster manifest for a

given ring.

Get-AzsSupportServiceFabricClusterUpgrade Gets the Service Fabric cluster upgrade status

Name Description

for a given ring.

Get-AzsSupportServiceFabricNode Gets the Service Fabric cluster nodes for a

given ring.

Get-AzsSupportServiceFabricReplica Gets the replicas for a specified service fabric

service.

Get-AzsSupportServiceFabricRuntimeVersion Gets the Service Fabric runtime version across

all fabric cluster nodes in a specified ring. If no

ring is specified, it checks all Service Fabric

rings.

Get-AzsSupportServiceFabricService Gets service fabric services on the specified

ring.

GetAzsSupportServiceFabricServiceDockerImageName

Gets image name of a Service Fabric

application.

GetAzsSupportServiceFabricServiceDockerImageTag

Gets image tag of a Service Fabric application.

GetAzsSupportServiceFabricServiceManifestNames

Gets Service Fabric service manifest names.

Get-AzsSupportStampInformation Calls Get-StampInformation and caches the

data to allow faster retrieval.

Get-AzsSupportStampVersion Gets the minor version of the stamp version, or

the full version of the stamp if the parameter is

supplied.

Get-AzsSupportStorageAccountProperties Get properties for a specified storage account.

Get-AzsSupportStorageEventLogErrors Gets errors from event logs for a specified

node. If no node is specified, lists errors from

all nodes.

Get-AzsSupportStorageNode Gets specified storage node or all nodes if

none is provided.

Get-AzsSupportTenantVM Gets tenant VM information from CRP.

Get-AzsSupportTenantVMSS Gets tenant VMMS information from CRP.

Get-AzsSupportTraceEvent Gets the trace events from GetAzsSupportTraceFilePath .

Get-AzsSupportTraceFilePath Gets the logfile path that was generated by

New-AzsSupportTraceFilePath .

Name Description

Get-AzsSupportVirtualDisk Gets all virtual disks and their health states.

Get-AzsSupportVirtualDiskStorageJob Gets all active storage jobs for any virtual disk.

Get-AzsSupportVMReport Get Hyper-V VM objects for all VMs including

infrastructure VMs and tenant VMs from

infrastructure hosts.

Get-AzsSupportVolumeUtilization Reports the utilization for all Object Stores.

Get-AzsSupportWinEvent Gets a list of events from the specified

ComputerNames.

Get-AzsSupportWorkingDirectory Gets the file path used for the working

directory/staging area.

Get-AzsSupportWorkingDirectoryFiles Gets a list of all files that are present in the

working directory.

Invoke-AzsSupportGetNetView Invokes Get-Netview function on the specified

ComputerNames.

Invoke-AzsSupportProcDump Invokes ProcDump on the specified

ComputerName against a specified process ID.

Default arguments are procdump.exe -ma <pid>

"$(Get-AzsSupportWorkingDirectory)\dumps" .

Invoke-AzsSupportHandle Invokes Handle.exe on the specified

ComputerName. Defaults to listing all open

handles.

Invoke-AzsSupportWmiTracing Enables netsh ETL tracing for a series of WMI

providers on a specified computer name. Also

supports a series of procdumps of winmgt and

WmiPrvSE if specified.

Save-AzsSupportObjectToFile Save an object to a file in a consistent format

creating a file that contains the current time as

a timestamp in the file name.

Send-AzureStackDiagnosticLog Sends Azure Stack diagnostic logs to

Microsoft.

Start-AzsSupportSdnDiagnostic Automated network diagnostics and data

collection/tracing script.

Start-AzsSupportStorageDiagnostic Runs a series of storage specific diagnostic

tests and generates a storage report.

Name Description

Clear-AzSSupportDiskSpace Clear infra VM or host disk space.

Invoke-AzsSupportNrpResourceRequest Allows a user to perform GET or PUT requests to NRP

REST API endpoint.

Invoke-AzsSupportSdnResourceRequest Invokes a web request to SDN API for the requested

resource.

Invoke-AzsSupportSpaceDB Invokes spacedb.exe on the specified host. If no host

is provided, runs spacedb on the first node in the

cluster.

Invoke-AzsSupportSysinternalsDownload Downloads the Sysinternals suite from the internet,

or checks for a well-known location for disconnected

stamps.

Move-AzsSupportClusterGroup Moves a clustered role from one node to another in

a failover cluster.

Move-AzsSupportClusterSharedVolume Moves a Cluster Shared Volume (CSV) to ownership

by a different node in a failover cluster.

MoveAzsSupportServiceFabricPrimaryReplica

Moves the primary replica of the provided service to

an available node.

Move-AzsSupportVirtualMachine Moves a clustered Virtual Machine to a new scale

unit host.

Remove-AzsSupportItem Remove items from a specified path from an infra

VM or host.

Remove-AzsSupportItemByStopService Remove items from a specified path from an infra

VM or host, stopping the specified service prior to

removal.

Restart-AzsSupportComputerByRole Restarts all Azure Stack Hub infrastructure computers

in a given role using safe restart action plans. Only

supports virtual machine roles.

Restart-AzsSupportService Restart services on a specified ComputerName.

RestartAzsSupportServiceFabricPrimaryReplica

Restarts the primary replica of the provided service.

Only supports services that contain one primary

replica.

Start-AzsSupportContainerHotpatch Patches a docker image on fabric ring machines.

Access level: Diagnostics and Repair

Name Description

Start-AzsSupportService Start services on a specified ComputerName.

Stop-AzsSupportProcess Stops a process on a specified ComputerName.

Stop-AzsSupportService Stops a service on a specified ComputerName.

Test-AzsSupportKnownIssue Executes a suite of known issue and infrastructure

health checks.

Update-AzsSupportStorageHealthCache Refreshes the storage cache and health cluster

resources.

Learn about Azure Stack Hub help and support.

Next steps

Send Azure Stack Hub diagnostic logs

by using the privileged endpoint (PEP)

Article • 07/29/2022

To run Get-AzureStackLog on an integrated system, you need to have access to the

privileged endpoint (PEP). Here's an example script you can run using the PEP to collect

logs. If you are canceling a running log collection to start a new one, please wait 5

minutes Before starting new log collection and enter Remove-PSSession -Session

$session .

PowerShell

Collect all logs for all roles:

PowerShell

$ipAddress = "<IP ADDRESS OF THE PEP VM>" # You can also use the machine

name instead of IP here.

$password = ConvertTo-SecureString "<CLOUD ADMIN PASSWORD>" -AsPlainText -

Force

$cred = New-Object -TypeName System.Management.Automation.PSCredential ("

<DOMAIN NAME>\CloudAdmin", $password)

$shareCred = Get-Credential

$session = New-PSSession -ComputerName $ipAddress -ConfigurationName

PrivilegedEndpoint -Credential $cred -SessionOption (New-PSSessionOption -

Culture en-US -UICulture en-US)

$fromDate = (Get-Date).AddHours(-8)

$toDate = (Get-Date).AddHours(-2) # Provide the time that includes the

period for your issue

Invoke-Command -Session $session { Get-AzureStackLog -OutputSharePath "

<EXTERNAL SHARE ADDRESS>" -OutputShareCredential $using:shareCred -

FilterByRole Storage -FromDate $using:fromDate -ToDate $using:toDate}

if ($session) {

Remove-PSSession -Session $session

}

Examples

Get-AzureStackLog -OutputSharePath "<path>" -OutputShareCredential

$cred

Collect logs from VirtualMachines and BareMetal roles:

PowerShell

Collect logs from VirtualMachines and BareMetal roles, with date filtering for log

files for the past 8 hours:

PowerShell

Collect logs from VirtualMachines and BareMetal roles, with date filtering for log

files for the time period between 8 hours ago and 2 hours ago:

PowerShell

Collect logs from tenant deployments running self-managed Kubernetes clusters

(AKS engine) on Azure Stack. Kubernetes logs should be stored in a tenant storage

account in a format that will enable the collection time range to be applied to

them as well.

PowerShell

For example:

PowerShell

Get-AzureStackLog -OutputSharePath "<path>" -OutputShareCredential

$cred -FilterByRole VirtualMachines,BareMetal

Get-AzureStackLog -OutputSharePath "<path>" -OutputShareCredential

$cred -FilterByRole VirtualMachines,BareMetal -FromDate (GetDate).AddHours(-8)

Get-AzureStackLog -OutputSharePath "<path>" -OutputShareCredential

$cred -FilterByRole VirtualMachines,BareMetal -FromDate (GetDate).AddHours(-8) -ToDate (Get-Date).AddHours(-2)

Get-AzureStackLog -OutputPath <Path> -InputSasUri "<Blob Service Sas

URI>" -FromDate "<Beginning of the time range>" -ToDate "<End of the

time range>"

Get-AzureStackLog -OutputPath C:\KubernetesLogs -InputSasUri

"https://<storageAccountName>.blob.core.windows.net/<ContainerName><SAS

token>" -FromDate (Get-Date).AddHours(-8) -ToDate (GetDate).AddHours(-2)

Collect logs for the value-add RPs. The general syntax is:

PowerShell

To collect logs for SQL RP:

PowerShell

To collect logs for MySQL RP:

PowerShell

To collect logs for Event Hubs:

PowerShell

To collect logs for Azure Stack Edge:

PowerShell

Collect logs and store them in the specified Azure Storage blob container. The

general syntax for this operation is as follows:

PowerShell

For example:

PowerShell

Get-AzureStackLog -FilterByResourceProvider <<value-add RP name>>

Get-AzureStackLog -FilterByResourceProvider SQLAdapter

Get-AzureStackLog -FilterByResourceProvider MySQLAdapter

Get-AzureStackLog -FilterByResourceProvider eventhub

Get-AzureStackLog -FilterByResourceProvide databoxedge

Get-AzureStackLog -OutputSasUri "<Blob service SAS Uri>"

Get-AzureStackLog -OutputSasUri

"https://<storageAccountName>.blob.core.windows.net/<ContainerName><SAS

token>"

To generate the SAS token for the storage account, the following permissions are

required:

Access to the Blob Storage service.

Access to the container resource type.

To generate a SAS Uri value to be used for the -OutputSasUri parameter, follow

these steps:

1. Create a storage account, following the steps in this article.

2. Open an instance of the Azure Storage Explorer.

3. Connect to the storage account created in step 1.

4. Navigate to Blob Containers in Storage Services.

5. Select Create a new container.

6. Right-click the new container, then click Get Shared Access Signature.

7. Select a valid Start Time and End Time, depending on your requirements.

8. For the required permissions, select Read, Write, and List.

9. Select Create.

10. You'll get a Shared Access Signature. Copy the URL portion and provide it to

the -OutputSasUri parameter.

The parameters OutputSharePath and OutputShareCredential are used to store

logs in a user specified location.

The FromDate and ToDate parameters can be used to collect logs for a particular

time period. If these parameters aren't specified, logs are collected for the past

four hours by default.

Use the FilterByNode parameter to filter logs by computer name. For example:

PowerShell

７ Note

This procedure is useful for uploading logs. Even if you don't have an SMB

share accessible or internet access, you can create a blob storage account on

your Azure Stack Hub to transfer the logs, and then use your client to retrieve

those logs.

Parameter considerations

Use the FilterByLogType parameter to filter logs by type. You can choose to filter

by File, Share, or WindowsEvent. For example:

PowerShell

You can use the TimeOutInMinutes parameter to set the timeout for log

collection. It's set to 150 (2.5 hours) by default.

Dump file log collection is disabled by default. To enable it, use the

IncludeDumpFile switch parameter.

Currently, you can use the FilterByRole parameter to filter log collection by the

following roles:

ACS

ACSBlob

ACSDownloadService

ACSFabric

ACSFrontEnd

ACSMetrics

ACSMigrationService

ACSMonitoringService

ACSSettingsService

ACSTableMaster

ACSTableServer

ACSWac

ADFS

Get-AzureStackLog -OutputSharePath "<path>" -OutputShareCredential

$cred -FilterByNode azs-xrp01

Get-AzureStackLog -OutputSharePath "<path>" -OutputShareCredential

$cred -FilterByLogType File

ApplicationController

ASAppGateway

AzureBridge

AzureMonitor

BareMetal

BRP

CA

CacheService

Compute

CPI

CRP

DeploymentMachine

DiskRP

Domain

ECE

EventAdminRP

EventRP

ExternalDNS

FabricRing

FabricRingServices

FirstTierAggregationService

FRP

Gateway

HealthMonitoring

HintingServiceV2

HRP

IBC

InfraServiceController

KeyVaultAdminResourceProvider

KeyVaultControlPlane

KeyVaultDataPlane

KeyVaultInternalControlPlane

KeyVaultInternalDataPlane

KeyVaultNamingService

MDM

MetricsAdminRP

MetricsRP

MetricsServer

MetricsStoreService

MonAdminRP

MonRP

NC

NonPrivilegedAppGateway

NRP

OboService

OEM

OnboardRP

PXE

QueryServiceCoordinator

QueryServiceWorker

SeedRing

SeedRingServices

SLB

SQL

SRP

Storage

StorageController

URP

SupportBridgeController

SupportRing

SupportRingServices

SupportBridgeRP

UsageBridge

VirtualMachines

WAS

WASPUBLIC

The command takes some time to run based on which role(s) the logs are

collecting. Contributing factors also include the time duration specified for log

collection, and the numbers of nodes in the Azure Stack Hub environment.

As log collection runs, check the new folder created in the OutputSharePath

parameter specified in the command.

Each role has its logs inside individual zip files. Depending on the size of the

collected logs, a role may have its logs split into multiple zip files. For such a role, if

you want to have all the log files unzipped into a single folder, use a tool that can

unzip in bulk. Select all the zipped files for the role and select extract here. All the

log files for that role will be unzipped into a single merged folder.

Additional considerations on diagnostic logs

A file called Get-AzureStackLog\_Output.log is also created in the folder that

contains the zipped log files. This file is a log of the command output, which can

be used for troubleshooting problems during log collection. Sometimes the log file

includes PS>TerminatingError entries which can be safely ignored, unless expected

log files are missing after log collection runs.

To investigate a specific failure, logs may be needed from more than one

component.

System and event logs for all infrastructure VMs are collected in the

VirtualMachines role.

System and event logs for all hosts are collected in the BareMetal role.

Failover cluster and Hyper-V event logs are collected in the Storage role.

ACS logs are collected in the Storage and ACS roles.

You can use the Invoke-AzureStackOnDemandLog cmdlet to generate on-demand logs

for certain roles (see the list at the end of this section). The logs generated by this

cmdlet aren't present by default in the log bundle you receive when you execute the

Get-AzureStackLog cmdlet. Also, it's recommended that you collect these logs only

when requested by the Microsoft support team.

Currently, you can use the -FilterByRole parameter to filter log collection by the

following roles:

OEM

NC

SLB

Gateway

７ Note

Size and age limits are enforced on the logs collected as it's essential to ensure

efficient utilization of your storage space and to avoid getting flooded with logs.

However, when diagnosing a problem, you sometimes need logs that don't exist

anymore because of these limits. Thus, it's highly recommended that you offload

your logs to an external storage space (a storage account in Azure, an additional on

premises storage device, etc.) every 8 to 12 hours and keep them there for 1 - 3

months, depending on your requirements. You should also ensure this storage

location is encrypted.

Invoke-AzureStackOnDemandLog

PowerShell

Azure Stack Hub diagnostics tools help make log collection easy and efficient. The

following diagram shows how the diagnostics tools work:

Example of collecting on-demand diagnostic logs

$ipAddress = "<IP ADDRESS OF THE PEP VM>" # You can also use the machine

name instead of IP here.

$password = ConvertTo-SecureString "<CLOUD ADMIN PASSWORD>" -AsPlainText -

Force

$cred = New-Object -TypeName System.Management.Automation.PSCredential ("

<DOMAIN NAME>\CloudAdmin", $password)

$shareCred = Get-Credential

$session = New-PSSession -ComputerName $ipAddress -ConfigurationName

PrivilegedEndpoint -Credential $cred -SessionOption (New-PSSessionOption -

Culture en-US -UICulture en-US)

$fromDate = (Get-Date).AddHours(-8)

$toDate = (Get-Date).AddHours(-2) # Provide the time that includes the

period for your issue

Invoke-Command -Session $session {

Invoke-AzureStackOnDemandLog -Generate -FilterByRole "<on-demand role

name>" # Provide the supported on-demand role name e.g. OEM, NC, SLB,

Gateway

Get-AzureStackLog -OutputSharePath "<external share address>" -

OutputShareCredential $using:shareCred -FilterByRole Storage -FromDate

$using:fromDate -ToDate $using:toDate

}

if ($session) {

Remove-PSSession -Session $session

}

How diagnostic log collection using the PEP works

The Trace Collector is enabled by default and runs continuously in the background to

collect all Event Tracing for Windows (ETW) logs from Azure Stack Hub component

services. ETW logs are stored in a common local share with a five-day age limit. Once

this limit is reached, the oldest files are deleted as new ones are created. The default

maximum size allowed for each file is 200 MB. A size check happens every 2 minutes,

and if the current file is >= 200 MB, it's saved and a new file generates. There's also an 8

GB limit on the total file size generated per event session.

The PowerShell cmdlet Get-AzureStackLog can be used to collect logs from all the

components in an Azure Stack Hub environment. It saves them in zip files in a userdefined location. If the Azure Stack Hub technical support team needs your logs to help

troubleshoot an issue, they may ask you to run Get-AzureStackLog.

The following are some example log types that are collected:

Azure Stack Hub deployment logs

Windows event logs

Trace Collector

Get-AzureStackLog

Ｕ Caution

These log files may contain personally identifiable information (PII). Take this into

account before you publicly post any log files.

Panther logs

Cluster logs

Storage diagnostic logs

ETW logs

These files are collected and saved in a share by Trace Collector. Get-AzureStackLog can

then be used to collect them when necessary.

Validate Azure Stack Hub system state

Article • 07/29/2022

As an Azure Stack Hub operator, being able to determine the health and status of your

system on demand is essential. The Azure Stack Hub validation tool (Test-AzureStack)) is

a PowerShell cmdlet that lets you run a series of tests on your system to identify failures

if present. You'll typically be asked to run this tool through the privileged end point

(PEP) when you contact Microsoft Customer Services Support (Microsoft Support) with

an issue. With the system-wide health and status information at hand, Microsoft

Support can collect and analyze detailed logs, focus on the area where the error

occurred, and work with you to fix the issue.

You can use the PEP to run the validation tool. The tool can take a while to run. The

length of the time depends on the number of virtual machines in your system. Each test

returns a PASS/FAIL status in the PowerShell window.

Here's an outline of the end-to-end validation testing process:

1. Establish the trust. On an integrated system, run the following command from an

elevated Windows PowerShell session to add the PEP as a trusted host on the

hardened VM running on the hardware lifecycle host or the Privileged Access

Workstation.

PowerShell

If you're running the Azure Stack Development Kit (ASDK), sign in to the

development kit host.

2. Access the PEP. Run the following commands to establish a PEP session:

PowerShell

Running the validation tool and accessing

results

winrm s winrm/config/client '@{TrustedHosts="<IP Address of Privileged

Endpoint>"}'

Enter-PSSession -ComputerName "<ERCS VM-name/IP address>" -

ConfigurationName PrivilegedEndpoint -Credential $localcred

3. Once you're in the PEP, run:

PowerShell

For more information, see Parameter considerations and Use case examples.

4. If any tests report FAIL, run Get-AzureStackLog . For instructions on an integrated

system, see how to run Get-AzureStackLog on Azure Stack Hub integrated systems.

The cmdlet gathers logs generated by Test-AzureStack. We recommend you don't

collect logs and contact Microsoft Support instead if tests report WARN.

5. If you're instructed to run the validation tool by the Microsoft Support, the

Microsoft Support representative will request the logs you collected to continue

troubleshooting your issue.

The validation tool lets you run a series of system-level tests and basic cloud scenarios

that provide you with insight to the current state, allowing you to fix issues in your

system.

These low impact tests work on an infrastructure level and provide you with information

on various system components and functions. Currently, tests are grouped into the

following categories:

Test Category Argument for -Include and -

Ignore

Azure Stack Hub ACS Summary AzsAcsSummary

Azure Stack Hub Active Directory Summary AzsAdSummary

Azure Stack Hub Alert Summary AzsAlertSummary

 Tip

To access the PEP on an Azure Stack Development Kit (ASDK) host computer,

use AzS-ERCS01 for -ComputerName.

Test-AzureStack

Tests available

Cloud infrastructure tests

Test Category Argument for -Include and -

Ignore

Azure Stack Hub Application Crash Summary AzsApplicationCrashSummary

Azure Stack Hub Backup Share Accessibility Summary AzsBackupShareAccessibility

Azure Stack Hub BMC Summary AzsStampBMCSummary

Azure Stack Hub Cloud Hosting Infrastructure Summary AzsHostingInfraSummary

Azure Stack Hub Cloud Hosting Infrastructure Utilization AzsHostingInfraUtilization

Azure Stack Hub Control Plane Summary AzsControlPlane

Azure Stack Hub Defender Summary AzsDefenderSummary

Azure Stack Hub External Certificates Summary AzsExternalCertificates

Azure Stack Hub Hosting Infrastructure Firmware

Summary

AzsHostingInfraFWSummary

Azure Stack Hub Infrastructure Capacity AzsInfraCapacity

Azure Stack Hub Infrastructure Performance AzsInfraPerformance

Azure Stack Hub Infrastructure Role Summary AzsInfraRoleSummary

Azure Stack Hub Network Infra AzsNetworkInfra

Azure Stack Hub Portal and API Summary AzsPortalAPISummary

Azure Stack Hub Scale Unit VM Events AzsScaleUnitEvents

Azure Stack Hub Scale Unit VM Resources AzsScaleUnitResources

Azure Stack Hub Scenarios AzsScenarios

Azure Stack Hub SDN Validation Summary AzsSDNValidation

Azure Stack Hub Service Fabric Role Summary AzsSFRoleSummary

Azure Stack Hub Storage Data Plane AzsStorageDataPlane

Azure Stack Hub Storage Services Summary AzsStorageSvcsSummary

Azure Stack Hub SQL Store Summary AzsStoreSummary

Azure Stack Hub Update Summary AzsInfraUpdateSummary

Azure Stack Hub VM Placement Summary AzsVmPlacement

In addition to the infrastructure tests above, you can also run cloud scenario tests to

check functionality across infrastructure components. Cloud admin credentials are

required to run these tests because they involve resource deployment.

The following cloud scenarios are tested by the validation tool:

Resource group creation

Plan creation

Offer creation

Storage account creation

Virtual machine creation (VM)

Blob storage operation

Queue storage operation

Table storage operation

The parameter List can be used to display all available test categories.

The parameters Include and Ignore can be used to include or exclude test

categories. For more information about these arguments, see the following

section.

PowerShell

PowerShell

A tenant VM is deployed as part of the cloud scenario tests. You can use

DoNotDeployTenantVm to disable this VM deployment.

Cloud scenario tests

７ Note

Currently you can't run cloud scenario tests using Active Directory Federated

Services (AD FS) credentials.

Parameter considerations

Test-AzureStack -Include AzsSFRoleSummary, AzsInfraCapacity

Test-AzureStack -Ignore AzsInfraPerformance

You need to supply the ServiceAdminCredential parameter to run cloud scenario

tests as described in the Use case examples section.

BackupSharePath and BackupShareCredential are used when testing

infrastructure backup settings as shown in the Use case examples section.

DetailedResults can be used to get pass/fail/warning information for each test, as

well as the overall run. When not specified, Test-AzureStack returns $true if there

are no failures, and $false if there are failures.

TimeoutSeconds can be used to set a specific time for each group to complete.

The validation tool also supports common PowerShell parameters: Verbose, Debug,

ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer,

PipelineVariable, and OutVariable. For more information, see About Common

Parameters.

Run the validation tool without the ServiceAdminCredential parameter to skip running

cloud scenario tests:

PowerShell

Supplying the validation tool with the ServiceAdminCredentials parameter runs the

cloud scenario tests by default:

PowerShell

Use case examples

Run validation without cloud scenarios

New-PSSession -ComputerName "<ERCS VM-name/IP address>" -ConfigurationName

PrivilegedEndpoint -Credential $localcred -SessionOption (NewPSSessionOption -Culture en-US -UICulture en-US)

Test-AzureStack

Run validation with cloud scenarios

Enter-PSSession -ComputerName "<ERCS VM-name/IP address>" -ConfigurationName

PrivilegedEndpoint -Credential $localcred

Test-AzureStack -ServiceAdminCredential "<Cloud administrator user name>"

If you wish to run ONLY cloud scenarios without running the rest of the tests, you can

use the Include parameter to do so:

PowerShell

The cloud admin user name must be typed in the UPN format:

serviceadmin@contoso.onmicrosoft.com (Azure AD). When prompted, type the

password to the cloud admin account.

To improve the operator experience, a Group parameter has been enabled to run

multiple test categories at the same time. Currently, there are three groups defined:

Default, UpdateReadiness, and SecretRotationReadiness.

Default: Considered to be a standard run of Test-AzureStack. This group is run by

default if no other groups are selected.

UpdateReadiness: A check to see if the Azure Stack Hub instance can be updated.

When the UpdateReadiness group is run, warnings are displayed as errors in the

console output, and they should be considered as blockers for the update. The

following categories are part of the UpdateReadiness group:

AzsInfraFileValidation

AzsActionPlanStatus

AzsStampBMCSummary

SecretRotationReadiness: A check to see if the Azure Stack Hub instance is in a

state in which secret rotation can be run. When the SecretRotationReadiness

group is run, warnings are displayed as errors in the console output and they

should be considered as blockers for secret rotation. The following categories are

part of the SecretRotationReadiness Group:

AzsAcsSummary

AzsDefenderSummary

AzsHostingInfraSummary

AzsInfraCapacity

AzsInfraRoleSummary

AzsPortalAPISummary

AzsSFRoleSummary

Enter-PSSession -ComputerName "<ERCS VM-name/IP address>" -ConfigurationName

PrivilegedEndpoint -Credential $localcred

Test-AzureStack -ServiceAdminCredential "<Cloud administrator user name>" -

Include AzsScenarios

Groups

AzsStorageSvcsSummary

AzsStoreSummary

The following example runs Test-AzureStack to test system readiness before installing

an update or hotfix using Group. Before you start the installation of an update or hotfix,

run Test-AzureStack to check the status of your Azure Stack Hub:

PowerShell

Before configuring infrastructure backup, you can test the backup share path and

credential using the AzsBackupShareAccessibility test:

PowerShell

After configuring backup, you can run AzsBackupShareAccessibility to validate the

share is accessible from the ERCS:

PowerShell

To test new credentials with the configured backup share, run:

PowerShell

Group parameter example

Test-AzureStack -Group UpdateReadiness

Run validation tool to test infrastructure backup settings

Enter-PSSession -ComputerName "<ERCS VM-name/IP address>" -ConfigurationName

PrivilegedEndpoint -Credential $localcred

Test-AzureStack -Include AzsBackupShareAccessibility -BackupSharePath "\\

<fileserver>\<fileshare>" -BackupShareCredential $using:backupcred

Enter-PSSession -ComputerName "<ERCS VM-name/IP address>" -ConfigurationName

PrivilegedEndpoint -Credential $localcred

Test-AzureStack -Include AzsBackupShareAccessibility

Enter-PSSession -ComputerName "<ERCS VM-name/IP address>" -ConfigurationName

PrivilegedEndpoint -Credential $localcred

Test-AzureStack -Include AzsBackupShareAccessibility -BackupShareCredential

"<PSCredential for backup share>"

This test checks the connectivity of the network infrastructure bypassing the Azure Stack

Hub software defined network (SDN). It demonstrates connectivity from a Public VIP to

the configured DNS forwarders, NTP servers, and authentication endpoints. This includes

connectivity to Azure when using Azure AD as identity provider or the federated server

when using AD FS as identity provider.

Include the debug parameter to get a detailed output of the command:

PowerShell

To learn more about Azure Stack Hub diagnostics tools and issue logging, see Azure

Stack Hub Diagnostic log collection.

To learn more about troubleshooting, see Microsoft Azure Stack Hub troubleshooting.

Run validation tool to test network infrastructure

Test-AzureStack -Include AzsNetworkInfra -Debug

Next steps

Troubleshoot issues in Azure Stack Hub

Article • 07/29/2022

This document provides troubleshooting information for Azure Stack Hub integrated

environments. For help with the Azure Stack Development Kit, see ASDK

Troubleshooting or get help from experts on the Azure Stack Hub MSDN Forum .

These sections include links to docs that cover common questions sent to Microsoft

Support.

How to buy

Azure Stack Hub overview

How to use diagnostics tools in Azure Stack Hub

How to validate Azure Stack Hub system state

Update package release cadence

Verify and troubleshoot node status

Guest operating systems supported on Azure Stack Hub

VM sizes supported in Azure Stack Hub

Azure Marketplace items available for Azure Stack Hub

Frequently asked questions

Purchase considerations

Updates and diagnostics

Supported operating systems and sizes for guest VMs

Azure Marketplace

Manage capacity

Memory

To increase the total available memory capacity for Azure Stack Hub, you can add

additional memory. In Azure Stack Hub, your physical server is also referred to as a scale

unit node. All scale unit nodes that are members of a single scale unit must have the

same amount of memory.

The retention period setting lets a cloud operator to specify a time period in days

(between 0 and 9999 days) during which any deleted account can potentially be

recovered. The default retention period is set to 0 days. Setting the value to 0 means

that any deleted account is immediately out of retention and marked for periodic

garbage collection.

Set the retention period

A user in Azure Stack Hub can be a reader, owner, or contributor for each instance of a

subscription, resource group, or service.

Azure Stack Hub Manage RBAC

If the built-in roles for Azure resources don't meet the specific needs of your

organization, you can create your own custom roles. For this tutorial, you create a

custom role named Reader Support Tickets using Azure PowerShell.

Tutorial: Create a custom role for Azure resources using Azure PowerShell

Manage usage and billing as a CSP

Create a CSP or APSS subscription

Choose the type of shared services account that you use for Azure Stack Hub. The types

of subscriptions that can be used for registration of a multi-tenant Azure Stack Hub are:

Cloud Solution Provider

Partner Shared Services subscription

Retention period

Security, compliance, and identity

Manage RBAC

Manage usage and billing as a CSP

Get scale unit metrics

You can use PowerShell to get stamp utilization information without help from Microsoft

Support. To obtain stamp utilization:

1. Create a PEP session.

2. Run the following command:

3. Exit PEP session.

4. Run the following using an Invoke-Command call:

5. Extract the seedring .zip. You can obtain the validation report from the ERCS folder

where you ran Test-AzureStack .

For more information, see Azure Stack Hub Diagnostics.

If you forget the password for a Linux VM and the Reset password option is not working

due to issues with the VMAccess extension, you can perform a reset following these

steps:

1. Choose a Linux VM to use as a recovery VM.

2. Sign in to the User portal:

a. Make a note of the VM size, NIC, Public IP, NSG and data disks.

b. Stop the impacted VM.

c. Remove the impacted VM.

d. Attach the disk from the impacted VM as a data disk on the recovery VM (it may

take a couple of minutes for the disk to be available).

3. Sign in to the recovery VM and run the following command:

Test-AzureStack

Get-AzureStackLog -FilterByRole SeedRing

Troubleshoot virtual machines (VMs)

Reset Linux VM password

4. Sign in to the User portal:

a. Detach the disk from the Recovery VM.

b. Recreate the VM from the disk.

c. Be sure to transfer the Public IP from the previous VM, attach the data disks, etc.

You may also take a snapshot of the original disk and create a new disk from it rather

than perform the changes directly on the original disk. For more information, see these

topics:

Reset password

Create a disk from a snapshot

Changing and resetting the Root password

In this case, Windows will fail to activate and you will see a watermark on the bottomright corner of the screen. The WaSetup.xml logs located under C:\Windows\Panther

contains the following event:

XML

sudo su -

mkdir /tempmount

fdisk -l

mount /dev/sdc2 /tempmount /\*adjust /dev/sdc2 as necessary\*/

chroot /tempmount/

passwd root /\*substitute root with the user whose password you want to

reset\*/

rm -f /.autorelabel /\*Remove the .autorelabel file to prevent a time

consuming SELinux relabel of the disk\*/

exit /\*to exit the chroot environment\*/

umount /tempmount

License activation fails for Windows Server 2012 R2

during provisioning

<Event time="2019-05-16T21:32:58.660Z" category="ERROR" source="Unattend">

<UnhandledError>

<Message>InstrumentProcedure: Failed to execute 'Call

ConfigureLicensing()'. Will raise error to caller</Message>

<Number>-2147221500</Number>

<Description>Could not find the VOLUME\_KMSCLIENT

product</Description>

<Source>Licensing.wsf</Source>

</UnhandledError>

</Event>

To activate the license, copy the Automatic Virtual Machine Activation (AVMA) key for

the SKU you want to activate.

Edition AVMA Key

Datacenter Y4TGP-NPTV9-HTC2H-7MGQ3-DV4TW

Standard DBGBW-NPF86-BJVTX-K3WKJ-MTB6V

Essentials K2XGM-NMBT3-2R6Q8-WF2FK-P36R2

On the VM, run the following command:

PowerShell

For complete details, see VM Activation.

A Windows Server image and gallery item must be added before deploying VMs in

Azure Stack Hub.

This behavior is by design:

When you delete a VM, VHDs aren't deleted. Disks are separate resources in the

resource group.

When a storage account gets deleted, the deletion is visible immediately through

Azure Resource Manager. But the disks it may contain are still kept in storage until

garbage collection runs.

If you see "orphan" VHDs, it's important to know if they're part of the folder for a

storage account that was deleted. If the storage account wasn't deleted, it's normal that

they're still there.

You can read more about configuring the retention threshold and on-demand

reclamation in manage storage accounts.

slmgr /ipk <AVMA\_key>

Default image and gallery item

I've deleted some VMs, but still see the VHD files on disk

Troubleshoot storage

It may take up to 14 hours for reclaimed capacity to show up in the portal. Space

reclamation depends on different factors including usage percentage of internal

container files in block blob store. Therefore, depending on how much data is deleted,

there's no guarantee on the amount of space that could be reclaimed when garbage

collector runs.

If you're using an integrated system in a disconnected scenario, it's recommended to

use an Enterprise Certificate Authority (CA). Export the root certificate in a Base-64

format and then import it in Azure Storage Explorer. Make sure that you remove the

trailing slash ( / ) from the Resource Manager endpoint. For more information, see

Prepare for connecting to Azure Stack Hub.

If the Create-AADIdentityApp.ps1 script that's required for App Service fails, be sure to

include the required -AzureStackAdminCredential parameter when running the script.

For more information, see Prerequisites for deploying App Service on Azure Stack Hub.

The Azure Stack Hub patch and update process is designed to allow operators to apply

update packages in a consistent, streamlined way. While uncommon, issues can occur

during patch and update process. The following steps are recommended should you

encounter an issue during the patch and update process:

0. Prerequisites: Be sure that you have followed the Update Activity Checklist and

enable proactive log collection.

1. Follow the remediation steps in the failure alert created when your update failed.

2. If you have been unable to resolve your issue, create an Azure Stack Hub support

ticket. Be sure you have logs collected for the time span when the issue occurred. If

an update fails, either with a critical alert or a warning, it's important that you

review the failure and contact Microsoft Customer Support Services as directed in

Storage reclamation

Azure Storage Explorer not working with Azure Stack Hub

Troubleshoot App Service

Create-AADIdentityApp.ps1 script fails

Troubleshoot Azure Stack Hub updates

the alert so that your scale unit does not stay in a failed state for a long time.

Leaving a scale unit in a failed update state for an extended period of time can

cause additional issues that are more difficult to resolve later.

Applies to: Azure Stack Hub integrated systems

Applicable: This issue applies to all supported releases.

Cause: When attempting to install the Azure Stack Hub update, the status for the update

might fail and change state to PreparationFailed . For internet-connected systems this is

usually indicative of the update package being unable to download properly due to a

weak internet connection.

Remediation: You can work around this issue by clicking Install now again. If the

problem persists, we recommend manually uploading the update package by following

the Install updates section.

Occurrence: Common

Applicable: This issue applies to all supported releases.

Cause: The baseboard management controller (BMC) password is not set correctly.

Remediation: Update the BMC credential and resume the update.

Applicable: This issue applies to all supported releases.

Cause: When Azure Stack Hub update is in status In progress, warnings and errors may

be reported in the portal. Components may timeout waiting for other components

during upgrade resulting in an error. Azure Stack Hub has mechanism to retry or

remediate some of the tasks due to intermittent errors.

Common Azure Stack Hub patch and update

issues

PreparationFailed

Update failed: Check and Enforce external key protectors

on CSVs

Warnings and errors reported while update is in progress

Remediation: While the Azure Stack Hub update is in status In progress, warnings and

errors reported in the portal can be ignored.

Occurrence: Common

Azure Stack Hub Module 2.2.0

Article • 01/05/2022

Minimum supported Azure Stack Hub version is 2108.

Note: For earlier versions of Azure Stack check Install Azure Stack Powershell

For detailed install instructions please refer to Install Azure Stack Powershell Run the

following cmdlets from an elevated PowerShell session prompt:

PowerShell

Close your PowerShell session, then open a new PowerShell session so that update can

take effect. Run the following command from a PowerShell session:

PowerShell

Requirements:

Install

# Remove previous versions of AzureStack and AzureRM modules

Get-Module -Name Azure\* -ListAvailable | Uninstall-Module -Force -Verbose -

ErrorAction Continue

Get-Module -Name Azs.\* -ListAvailable | Uninstall-Module -Force -Verbose -

ErrorAction Continue

Get-Module -Name Az.\* -ListAvailable | Uninstall-Module -Force -Verbose -

ErrorAction Continue

[Net.ServicePointManager]::SecurityProtocol =

[Net.SecurityProtocolType]::Tls12

Install-Module PowerShellGet -MinimumVersion 2.2.3 -Force

[Net.ServicePointManager]::SecurityProtocol =

[Net.SecurityProtocolType]::Tls12

Install-Module -Name Az.BootStrapper -Force

# Install and import the API Version Modules required by Azure Stack into

the current PowerShell session.

Use-AzProfile -Profile 2020-09-01-hybrid -Force

# Install Azure Stack Admin Module

Install-Module -Name AzureStack -RequiredVersion 2.2.0 -AllowPrerelease

Supported with 2108 update.

This release 2.2.0 updates the capabilities in the Azs.Compute.Admin module. This

also adds new modules for working with Azure Container Registry on Azure Stack

Hub: Azs.ContainerRegistry.Admin and Azs.ContainerService.Admin. The Admin

modules now have a dependency on the Az.Resources module version 0.12.0. For

details on the changes in this update, see the AzureStack module change log

Release Notes

Azure Stack Hub privileged endpoint

reference

Article • 08/24/2023

The Azure Stack Hub privileged endpoint (PEP) is a pre-configured remote PowerShell

console that provides you with the capabilities to perform a required task. The endpoint

uses PowerShell JEA (Just Enough Administration) to expose only a restricted set of

cmdlets.

Cmdlet Description

Close-PrivilegedEndpoint No description.

Get-ActionStatus Gets the status of the latest action for the operation with

the specified function name.

Get-AzsDnsForwarder Get the DNS forwarder IP addresses used by Azure Stack

Hub

Get-AzSDnsServerSettings Get DNS server settings

Get-AzSLegalNotice Get legal notice caption and text

Get-AzureStackLog Get logs from various roles of AzureStack with timeout.

Get-AzureStackStampInformation Gets the stamp information.

Get-AzureStackSupportConfiguration Gets Support Service configuration settings.

GetCloudAdminPasswordRecoveryToken

No description.

Get-CloudAdminUserList No description.

Get-ClusterLog No description.

Get-GraphApplication Get-GraphApplication is a wrapper function to get the

Graph application information for the application Name

or Identifier specified.

Get-StorageJob No description.

Get-SupportSessionInfo No description.

Get-SupportSessionToken No description.

Privileged endpoint cmdlets

Cmdlet Description

Get-SyslogClient Gets the syslog Client settings.

Get-SyslogServer Gets the syslog server endpoint.

Get-ThirdPartyNotices No description.

Get-TLSPolicy No description.

Get-VirtualDisk No description.

Invoke-AzureStackOnDemandLog Generates on demand logs from AzureStack roles where

applicable.

New-AzureBridgeServicePrincipal Creates a new service principal in Azure Active Directory.

New-AzureStackActivation Activate Azure Stack.

New-CloudAdminUser No description.

New-GraphApplication New-GraphApplication is a wrapper function to call

ADFS Graph cmdlets on AD FS.

New-RegistrationToken Creates a new registration token

Register-CustomAdfs Script to register custom Active Directory Federation

Service (ADFS) as claims provider with Azure Stack AD

FS.

Register-CustomDnsServer Script to register custom DNS servers with Azure Stack

DNS.

Register-DirectoryService Script to register customer Active Directory with Graph

Service.

Remove-AzureStackActivation No description.

Remove-CloudAdminUser No description.

Remove-GraphApplication Remove-GraphApplication is a wrapper function to call

ADFS Graph cmdlets on AD FS.

Repair-VirtualDisk No description.

ResetDatacenterIntegrationConfiguration

Script to reset Datacenter Integration changes.

Send-AzureStackDiagnosticLog Sends Azure Stack Diagnostic Logs to Microsoft.

Set-AzSLegalNotice Set legal notice caption and text

Cmdlet Description

Set-AzsDnsForwarder Update the DNS forwarder IP addresses used by Azure

Stack Hub

Set-AzSDnsServerSettings Update DNS server settings

Set-CloudAdminUserPassword No description.

Set-GraphApplication Set-GraphApplication is a wrapper function to call ADFS

Graph cmdlets on AD FS.

Set-ServiceAdminOwner Script to update service administrator.

Set-SyslogClient Imports and applies syslog client endpoint certificate.

Set-SyslogServer Sets the syslog server endpoint.

Set-Telemetry Enables or disables the transfer of telemetry data to

Microsoft.

Set-TLSPolicy No description.

Start-AzsCryptoWipe Performs cryptographic wipe of Azure Stack Hub

infrastructure.

Start-AzureStack Starts all Azure Stack services.

Start-SecretRotation Triggers secret rotation on a stamp.

Stop-AzureStack Stops all Azure Stack services.

Test-AzureStack Validates the status of Azure Stack.

Unlock-SupportSession No description.

For more information about the Privileged Endpoint on Azure Stack Hub, see Using the

privileged endpoint in Azure Stack.

Next steps

Azure Stack Admin API reference

Article • 06/16/2020

Azure Stack Hub Admin APIs include interfaces for each resource provider. This reference

includes guidance for each available operation. You can use the APIs to work with:

Scale unit nodes

Alerts

Updates

Backup

Marketplace

Subscriptions

Offers

And others

Resource Provider Description

Health Resource Provider Provides operations for Alert management and list component health

Azure Bridge Provides operations to manage marketplace syndication

Backup Resource Provider Provides operations to manage backup & restore of Azure Stack

infrastructure

Commerce Provides operations to manage usage data in Azure Stack

Compute Resource Provider Provides operations to manage compute in Azure Stack

Fabric Resource Provider Provides operations to manage the underlying infrastructure of Azure Stack

Gallery Provides operations to manage the Marketplace in Azure Stack

Keyvault Provides operations to manage Quotas for Keyvault

Network Resource Provider Provides operations to manage network in Azure Stack

Update Resource Provider Provides operations to manage Updates in Azure Stack

Storage Resource Provider Provides operations to manage storage (Blobs, Queues, and Tables) in Azure

Stack

Subscription Resource

Provider

Provides operations to manage Offers, Plan, and Subscriptions in Azure

Stack

Resource providers

Azure Stack Admin API versioning, support, and

breaking changes for Azure Stack Hub

This section lists all of the Azure Stack Hub Admin resource providers and their supported

versions. The table reflects the current state of the APIs.

All APIs will follow the general Azure Stack Hub support policy that Azure Stack Hub support the

current version and two prior version releases.

Resource Provider API Version supported

Health Resource Provider 2016-05-01

Azure Bridge 2016-01-01

Backup Resource Provider 2018-09-01

Commerce 2015-06-01-preview

Compute Resource Provider 2015-12-01-preview, 2018-02-09, 2018-07-30-preview

Fabric Resource Provider 2016-05-01, 2018-10-01, 2019-05-01

Gallery 2015-04-01

Keyvault 2017-02-01-preview

Network Resource Provider 2015-06-15

Update Resource Provider 2016-05-01

Storage Resource Provider 2019-08-08

Subscription Resource Provider 2015-11-01

User Subscription Resource Provider 2015-11-01

Resource Provider Resource Version Announcement Release

Microsoft.Storage.Admin Farms 2015-

12-01-

preview

2020-02-20 2002

Microsoft.Storage.Admin arms/acquisitions 2015-

12-01-

preview

2020-02-20 2002

API contract

Versioning

Breaking changes

Deprecated APIs

Resource Provider Resource Version Announcement Release

Microsoft.Storage.Admin farms/shares 2015-

12-01-

preview

2020-02-20 2002

Microsoft.Storage.Admin farms/storageaccounts 2015-

12-01-

preview

2020-02-20 2002

Microsoft.Backup.Admin backupLocation 2016-

05-01

2020-02-20 2002

Microsoft.Backup.Admin backups 2016-

05-01

2020-02-20 2002

Microsoft.Backup.Admin operations 2016-

05-01

2020-02-20 2002

Microsoft.Fabric.Admin infraRoleInstances/{infraRoleInstance}/PowerOff 2016-

05-01

2020-6-11 NA

Microsoft.Fabric.Admin infraRoleInstances/{infraRoleInstance}/Shutdown 2016-

05-01

2020-6-11 NA

Microsoft.Fabric.Admin infraRoleInstances/{infraRoleInstance}/Reboot 2016-

05-01

2020-6-11 NA

Azure Stack Hub Admin API reference

MS policy

Service policy

Updates

See also

az

Reference

Name Description Type Status

az account Manage Azure subscription information. Core and

Extension

GA

az acr Manage private registries with Azure

Container Registries.

Core and

Extension

GA

az ad Manage Azure Active Directory Graph

entities needed for Role Based Access

Control.

Core and

Extension

GA

az adp Manage Azure Autonomous Development

Platform resources.

Extension GA

az advisor Manage Azure Advisor. Core GA

az afd Manage Azure Front Door

Standard/Premium. For classical Azure Front

Door, please refer

https://docs.microsoft.com/enus/cli/azure/network/front-door?

view=azure-cli-latest.

Core Preview

az ai-examples Add AI powered examples to help content. Extension Preview

az aks Manage Azure Kubernetes Services. Core and

Extension

GA

az alertsmanagement

Manage Azure Alerts Management Service

Resource.

Extension GA

az alias Manage Azure CLI Aliases. Extension GA

az amlfs Manage lustre file system. Extension GA

７ Note

This command group has commands that are defined in both Azure CLI and at least

one extension. Install each extension to benefit from its extended capabilities. Learn

more about extensions.

Commands

Name Description Type Status

az ams Manage Azure Media Services resources. Core GA

az apim Manage Azure API Management services. Core GA

az appconfig Manage App Configurations. Core GA

az appservice Manage App Service plans. Core and

Extension

GA

az arcappliance Commands to manage Arc resource bridge. Extension Preview

az arcdata Commands for using Azure Arc-enabled

data services.

Extension GA

az aro Manage Azure Red Hat OpenShift clusters. Core GA

az artifacts Manage Azure Artifacts. Extension GA

az attestation Manage Microsoft Azure Attestation (MAA). Extension Experimental

az automanage Manage Automanage. Extension GA

az automation Manage Automation Account. Extension GA

az azurestackhci Manage azurestackhci. Extension Experimental

az backup Manage Azure Backups. Core GA

az baremetalinstance (PREVIEW) Manage BareMetal Instances. Extension GA

az batch Manage Azure Batch. Core and

Extension

GA

az batchai Manage Batch AI resources. Core Deprecated

az bicep Bicep CLI command group. Core GA

az billing Manage Azure Billing. Core GA

az billing-benefits Azure billing benefits commands. Extension GA

az blockchain Manage blockchain. Extension GA

az blueprint Commands to manage blueprint. Extension GA

az boards Manage Azure Boards. Extension GA

az bot Manage Microsoft Azure Bot Service. Core GA

az cache Commands to manage CLI objects cached

using the --defer argument.

Core GA

Name Description Type Status

az capacity Manage capacity. Core GA

az cdn Manage Azure Content Delivery Networks

(CDNs).

Core GA

az change-analysis List changes for resources. Extension GA

az cli-translator Translate ARM template or REST API to CLI

scripts.

Extension Experimental

az cloud Manage registered Azure clouds. Core GA

az cloud-service Manage cloud service (extended support). Extension Experimental

az cognitiveservices Manage Azure Cognitive Services accounts. Core GA

az command-change Commands for CLI modules metadata

management.

Extension GA

az communication Manage communication service with

communication.

Extension GA

az confcom Commands to generate security policies for

confidential containers in Azure.

Extension GA

az confidentialledger Manage Confidential Ledger. Extension GA

az config Manage Azure CLI configuration. Core Experimental

az configure Manage Azure CLI configuration. This

command is interactive.

Core GA

az confluent Manage confluent resources. Extension Experimental

az connectedk8s Commands to manage connected

kubernetes clusters.

Extension GA

az connectedmachine Manage an Azure Arc-Enabled Server. Extension GA

az connectedvmware Commands to manage Connected VMware. Extension GA

az connection Commands to manage Service Connector

local connections which allow local

environment to connect Azure Resource. If

you want to manage connection for

compute service, please run 'az

webapp/containerapp/spring connection'.

Core and

Extension

GA

az consumption Manage consumption of Azure resources. Core Preview

Name Description Type Status

az container Manage Azure Container Instances. Core and

Extension

GA

az containerapp Manage Azure Container Apps. Core and

Extension

GA

az cosmosdb Manage Azure Cosmos DB database

accounts.

Core and

Extension

GA

az costmanagement Manage cost and billing in Azure. Extension GA

az csvmware Manage Azure VMware Solution by

CloudSimple.

Extension Preview

az custom-providers Commands to manage custom providers. Extension GA

az customlocation Commands to Create, Get, List and Delete

CustomLocations.

Extension GA

az databox Manage data box. Extension GA

az databoxedge Support data box edge device and

management.

Core Preview

az databricks Manage databricks workspaces. Extension GA

az datadog Manage datadog. Extension GA

az datafactory Manage Data Factory. Extension GA

az datamigration Manage Data Migration. Extension GA

az dataprotection Manage dataprotection. Extension Experimental

az datashare Manage Data Share. Extension Experimental

az dedicated-hsm Manage dedicated hsm with hardware

security modules.

Extension GA

az demo Demos for designing, developing and

demonstrating Azure CLI.

Core Deprecated

az deployment Manage Azure Resource Manager template

deployment at subscription scope.

Core GA

az deployment-scripts Manage deployment scripts at subscription

or resource group scope.

Core GA

az

desktopvirtualization

Manage desktop virtualization. Extension GA

Name Description Type Status

az devcenter Manage resources with devcenter. Extension GA

az devops Manage Azure DevOps organization level

operations.

Extension GA

az disk Manage Azure Managed Disks. Core GA

az disk-access Manage disk access resources. Core GA

az disk-encryption-set Disk Encryption Set resource. Core GA

az disk-pool Manage Azure disk pool. Extension GA

az dla Manage Data Lake Analytics accounts, jobs,

and catalogs.

Core Preview

az dls Manage Data Lake Store accounts and

filesystems.

Core Preview

az dms Manage Azure Data Migration Service

(classic) instances.

Core and

Extension

GA

az dnc Manage Delegated Network. Extension Preview

az dns-resolver Manage Dns Resolver. Extension GA

az dt Manage Azure Digital Twins solutions &

infrastructure.

Extension GA

az dynatrace Manage dynatrace. Extension GA

az edgeorder Manage Edge Order. Extension GA

az elastic Manage Microsoft Elastic. Extension GA

az elastic-san Manage Elastic SAN. Extension Preview

az eventgrid Manage Azure Event Grid topics, domains,

domain topics, system topics partner topics,

event subscriptions, system topic event

subscriptions and partner topic event

subscriptions.

Core and

Extension

GA

az eventhubs Eventhubs. Core GA

az extension Manage and update CLI extensions. Core GA

az feature Manage resource provider features. Core GA

az feedback Send feedback to the Azure CLI Team. Core GA

Name Description Type Status

az find I'm an AI robot, my advice is based on our

Azure documentation as well as the usage

patterns of Azure CLI and Azure ARM users.

Using me improves Azure products and

documentation.

Core GA

az fleet Commands to manage fleet. Extension Preview

az fluid-relay Manage Fluid Relay. Extension GA

az footprint Extension GA

az functionapp Manage function apps. To install the Azure

Functions Core tools see

https://github.com/Azure/azure-functionscore-tools .

Core and

Extension

GA

az fzf Commands to select active or default

objects via fzf.

Extension GA

az grafana Commands to manage Azure Grafana

instanced.

Extension GA

az graph Query the resources managed by Azure

Resource Manager.

Extension GA

az graph-services Make operations on

Microsoft.GraphServices resource types.

Extension GA

az group Manage resource groups and template

deployments.

Core GA

az guestconfig Manage Guest Configuration. Extension GA

az hack Commands to manage resources commonly

used for student hacks.

Extension GA

az hanainstance (PREVIEW) Manage Azure SAP HANA

Instance.

Extension GA

az hdinsight Manage HDInsight resources. Core GA

az healthbot Manage bot with healthbot. Extension Experimental

az healthcareapis Manage Healthcare Apis. Extension GA

az hpc-cache Commands to manage hpc cache. Extension GA

az hybridaks Manage hybridaks provisioned clusters. Extension Preview

Name Description Type Status

az identity Managed Identities. Core GA

az image Manage custom virtual machine images. Core and

Extension

GA

az import-export Manage Import Export. Extension Experimental

az init It's an effortless setting up tool for configs. Extension Experimental

az interactive Start interactive mode. Installs the

Interactive extension if not installed already.

Core Preview

az internet-analyzer Commands to manage internet analyzer. Extension GA

az iot Manage Internet of Things (IoT) assets. Core and

Extension

GA

az k8s-configuration Commands to manage resources from

Microsoft.KubernetesConfiguration.

Extension GA

az k8s-extension Commands to manage Kubernetes

Extensions.

Extension GA

az k8sconfiguration Commands to manage Kubernetes

configuration.

Extension Preview and

Deprecated

az keyvault Manage KeyVault keys, secrets, and

certificates.

Core GA

az kusto Manage Azure Kusto resources. Core and

Extension

GA

az lab Manage Azure DevTest Labs. Core Preview

az load Manage Azure Load Testing resources. Extension GA

az lock Manage Azure locks. Core GA

az logic Manage logic. Extension Preview

az logicapp Manage logic apps. Core GA

az login Log in to Azure. Core GA

az logout Log out to remove access to Azure

subscriptions.

Core GA

az logz Manage Microsoft Logz. Extension Experimental

az maintenance Manage Maintenance. Extension GA

Name Description Type Status

az managedcassandra

Azure Managed Cassandra. Core and

Extension

GA

az managedapp Manage template solutions provided and

maintained by Independent Software

Vendors (ISVs).

Core GA

az managedservices Manage the registration assignments and

definitions in Azure.

Core GA

az

managementpartner

Allows the partners to associate a Microsoft

Partner Network(MPN) ID to a user or

service principal in the customer's Azure

directory.

Extension GA

az maps Manage Azure Maps. Core GA

az mariadb Manage Azure Database for MariaDB

servers.

Core GA

az mesh (PREVIEW) Manage Azure Service Fabric

Mesh Resources.

Extension Preview

az ml Manage Azure Machine Learning resources

with the Azure CLI ML extension v2.

Extension GA

az ml Manage Azure Machine Learning resources

with the Azure CLI ML extension v1.

Extension GA

az mobile-network Manage mobile network. Extension GA

az monitor Manage the Azure Monitor Service. Core and

Extension

GA

az mysql Manage Azure Database for MySQL servers. Core and

Extension

GA

az netappfiles Manage Azure NetApp Files (ANF)

Resources.

Core and

Extension

GA

az network Manage Azure Network resources. Core and

Extension

GA

az network-function Manage network function. Extension GA

az networkcloud Manage Network Cloud resources. Extension GA

az networkfabric Manage Azure Network Fabric Management

Service API.

Extension GA

Name Description Type Status

az new-relic Manage Azure NewRelic resources. Extension GA

az next Recommend the possible next set of

commands to take.

Extension Experimental

az nginx Manage NGINX deployment resources. Extension GA

az notification-hub Manage notification hubs. Extension Experimental

az offazure Manage on-premise resources for migrate. Extension Experimental

az orbital Azure Orbital Ground Station as-a-Service

(GSaaS).

Extension GA

az palo-alto Manage palo-alto networks resource. Extension GA

az partnercenter Partner Center management. Extension GA

az peering Manage peering. Extension GA

az pipelines Manage Azure Pipelines. Extension GA

az policy Manage resource policies. Core GA

az portal Manage Portal. Extension Experimental

az postgres Manage Azure Database for PostgreSQL

servers.

Core and

Extension

GA

az powerbi Manage PowerBI resources. Extension Preview

az ppg Manage Proximity Placement Groups. Core GA

az private-link Private-link association CLI command group. Core GA

az provider Manage resource providers. Core GA

az providerhub Manage resources with ProviderHub. Extension GA

az purview Manage Purview. Extension Preview

az quantum Manage Azure Quantum Workspaces and

submit jobs to Azure Quantum Providers.

Extension Preview

az qumulo Manage qumulo. Extension GA

az quota Manage Azure Quota Extension API. Extension Experimental

az redis Manage dedicated Redis caches for your

Azure applications.

Core GA

Name Description Type Status

az redisenterprise Manage the redisenterprise cache. Extension GA

az relay Manage Azure Relay Service namespaces,

WCF relays, hybrid connections, and rules.

Core GA

az remote-renderingaccount

Manage remote rendering account with

mixed reality.

Extension GA

az repos Manage Azure Repos. Extension GA

az reservations Azure Reservations. Extension Preview

az resource Manage Azure resources. Core GA

az resource-mover Manage Resource Mover Service API. Extension Experimental

az

resourcemanagement

Resourcemanagement CLI command group. Core GA

az rest Invoke a custom request. Core GA

az restore-point Manage restore point with res. Core GA

az role Manage user roles for access control with

Azure Active Directory and service principals.

Core GA

az sapmonitor (PREVIEW) Manage Azure SAP Monitor. Extension GA

az scenario E2E Scenario Usage Guidance. Extension GA

az scvmm Commands for managing Arc for SCVMM

resources.

Extension Preview

az search Manage Azure Search services, admin keys

and query keys.

Core GA

az security Manage your security posture with

Microsoft Defender for Cloud.

Core GA

az self-help Azure SelfHelp will help you troubleshoot

issues with Azure resources.

Extension Preview

az self-test Runs a self-test of the CLI. Core Deprecated

az sentinel Manage Microsoft Sentinel. Extension GA

az serial-console Connect to the Serial Console of a

Linux/Windows Virtual Machine or VMSS

Instance.

Extension GA

az servicebus Servicebus. Core GA

Name Description Type Status

az sf Manage and administer Azure Service Fabric

clusters.

Core GA

az sig Manage shared image gallery. Core and

Extension

GA

az signalr Manage Azure SignalR Service. Core GA

az site-recovery Manage Site Recovery Service. Extension GA

az snapshot Manage point-in-time copies of managed

disks, native blobs, or other snapshots.

Core GA

az spatial-anchorsaccount

Manage spatial anchor account with mixed

reality.

Extension GA

az sphere Manage Azure Sphere. Extension GA

az spring Commands to manage Azure Spring Apps. Core and

Extension

GA

az spring-cloud Commands to manage Azure Spring Cloud. Core and

Extension

Deprecated

az sql Manage Azure SQL Databases and Data

Warehouses.

Core and

Extension

GA

az ssh SSH into resources (Azure VMs, Arc servers,

etc) using AAD issued openssh certificates.

Extension GA

az sshkey Manage ssh public key with vm. Core GA

az stack A deployment stack is a native Azure

resource type that enables you to perform

operations on a resource collection as an

atomic unit.

Core GA

az stack-hci Manage Azure Stack HCI. Extension GA

az staticwebapp Manage static apps. Core and

Extension

GA

az storage Manage Azure Cloud Storage resources. Core and

Extension

GA

az storage-mover Manage top-level Storage Mover resource. Extension GA

az storagesync Manage Azure File Sync. Extension GA

az stream-analytics Manage Stream Analytics. Extension Experimental

Name Description Type Status

az support Manage Azure support resource. Extension GA

az survey Take Azure CLI survey. Core GA

az synapse Manage and operate Synapse Workspace,

Spark Pool, SQL Pool.

Core GA

az tag Tag Management on a resource. Core GA

az term Manage marketplace agreement with

marketplaceordering.

Core Experimental

az ts Manage template specs at subscription or

resource group scope.

Core GA

az tsi Manage Azure Time Series Insights. Extension GA

az upgrade Upgrade Azure CLI and extensions. Core Preview

az version Show the versions of Azure CLI modules and

extensions in JSON format by default or

format configured by --output.

Core GA

az vm Manage Linux or Windows virtual machines. Core and

Extension

GA

az vmss Manage groupings of virtual machines in an

Azure Virtual Machine Scale Set (VMSS).

Core GA

az vmware Commands to manage Azure VMware

Solution.

Extension GA

az webapp Manage web apps. Core and

Extension

GA

az webpubsub Commands to manage Webpubsub. Extension GA

az workloads Manage workloads. Extension Preview

／ Edit

Manage Azure CLI configuration. This command is interactive.

For automation scenarios or to set all available options, use the new az config .

Azure CLI

az configure

Set default resource group, webapp and VM names.

Azure CLI

Clear default webapp and VM names.

Azure CLI

--defaults -d

Space-separated 'name=value' pairs for common argument defaults.

--list-defaults -l

List all applicable defaults.

accepted values: false, true

--scope

Scope of defaults. Using "local" for settings only effective under current folder.

accepted values: global, local

default value: global

Global Parameters

--debug

Increase logging verbosity to show all debug logs.

az configure [--defaults]

[--list-defaults {false, true}]

[--scope {global, local}]

Examples

az configure --defaults group=myRG web=myweb vm=myvm

az configure --defaults vm='' web=''

Optional Parameters

--help -h

Show this help message and exit.

--only-show-errors

Only show errors, suppressing warnings.

--output -o

Output format.

--query

JMESPath query string. See http://jmespath.org/ for more information and

examples.

--subscription

Name or ID of subscription. You can configure the default subscription using az

account set -s NAME\_OR\_ID .

--verbose

Increase logging verbosity. Use --debug for full debug logs.

／ Edit

Send feedback to the Azure CLI Team.

This command is interactive. If possible, it launches the default web browser to open

GitHub issue creation page with the body auto-generated and pre-filled. You will have a

chance to edit the issue body before submitting it.

Azure CLI

Global Parameters

--debug

az feedback

az feedback

Increase logging verbosity to show all debug logs.

--help -h

Show this help message and exit.

--only-show-errors

Only show errors, suppressing warnings.

--output -o

Output format.

--query

JMESPath query string. See http://jmespath.org/ for more information and

examples.

--subscription

Name or ID of subscription. You can configure the default subscription using az

account set -s NAME\_OR\_ID .

--verbose

Increase logging verbosity. Use --debug for full debug logs.

／ Edit

I'm an AI robot, my advice is based on our Azure documentation as well as the usage

patterns of Azure CLI and Azure ARM users. Using me improves Azure products and

documentation.

Azure CLI

az find

az find [<CLI\_TERM>]

Examples

Give me any Azure CLI group and I’ll show the most popular commands within the

group.

Azure CLI

Give me any Azure CLI command and I’ll show the most popular parameters and

subcommands.

Azure CLI

You can also enter a search term, and I'll try to help find the best commands.

Azure CLI

<CLI\_TERM>

An Azure CLI command or group for which you need an example.

Global Parameters

--debug

Increase logging verbosity to show all debug logs.

--help -h

Show this help message and exit.

--only-show-errors

Only show errors, suppressing warnings.

--output -o

az find "az storage"

az find "az monitor activity-log list"

az find "arm template"

Optional Parameters

Output format.

--query

JMESPath query string. See http://jmespath.org/ for more information and

examples.

--subscription

Name or ID of subscription. You can configure the default subscription using az

account set -s NAME\_OR\_ID .

--verbose

Increase logging verbosity. Use --debug for full debug logs.

It's an effortless setting up tool for configs.

Azure CLI

Global Parameters

--debug

Increase logging verbosity to show all debug logs.

--help -h

Show this help message and exit.

--only-show-errors

Only show errors, suppressing warnings.

--output -o

Output format.

az init

az init

--query

JMESPath query string. See http://jmespath.org/ for more information and

examples.

--subscription

Name or ID of subscription. You can configure the default subscription using az

account set -s NAME\_OR\_ID .

--verbose

Increase logging verbosity. Use --debug for full debug logs.

Start interactive mode. Installs the Interactive extension if not installed already.

For more information on interactive mode, see:

https://azure.microsoft.com/blog/welcome-to-azure-cli-shell/ .

Azure CLI

--style -s

The colors of the shell.

accepted values: bg, br, contrast, default, grey, halloween, neon, none, pastel, primary, purple,

quiet

--update

Update the Interactive extension to the latest available.

Global Parameters

az interactive

az interactive [--style {bg, br, contrast, default, grey, halloween, neon,

none, pastel, primary, purple, quiet}]

[--update]

Optional Parameters

--debug

Increase logging verbosity to show all debug logs.

--help -h

Show this help message and exit.

--only-show-errors

Only show errors, suppressing warnings.

--output -o

Output format.

--query

JMESPath query string. See http://jmespath.org/ for more information and

examples.

--subscription

Name or ID of subscription. You can configure the default subscription using az

account set -s NAME\_OR\_ID .

--verbose

Increase logging verbosity. Use --debug for full debug logs.

／ Edit

Log in to Azure.

By default, this command logs in with a user account. CLI will try to launch a web

browser to log in interactively. If a web browser is not available, CLI will fall back to

device code login. To login with a service principal, specify --service-principal.

Azure CLI

az login

az login [--allow-no-subscriptions]

[--federated-token]

Log in interactively.

Azure CLI

Log in with user name and password. This doesn't work with Microsoft accounts or

accounts that have two-factor authentication enabled. Use -p=secret if the first

character of the password is '-'.

Azure CLI

Log in with a service principal using client secret. Use -p=secret if the first character of

the password is '-'.

Azure CLI

Log in with a service principal using client certificate.

Azure CLI

Log in using a VM's system-assigned managed identity.

Azure CLI

[--identity]

[--password]

[--scope]

[--service-principal]

[--tenant]

[--use-cert-sn-issuer]

[--use-device-code]

[--username]

Examples

az login

az login -u johndoe@contoso.com -p VerySecret

az login --service-principal -u http://azure-cli-2016-08-05-14-31-15 -p

VerySecret --tenant contoso.onmicrosoft.com

az login --service-principal -u http://azure-cli-2016-08-05-14-31-15 -p

~/mycertfile.pem --tenant contoso.onmicrosoft.com

Log in using a VM's user-assigned managed identity. Client or object ids of the service

identity also work.

Azure CLI

--allow-no-subscriptions

Support access tenants without subscriptions. It's uncommon but useful to run

tenant level commands, such as 'az ad'.

default value: False

--federated-token

Federated token that can be used for OIDC token exchange.

--identity -i

Log in using the Virtual Machine's identity.

default value: False

--password -p

Credentials like user password, or for a service principal, provide client secret or a

pem file with key and public certificate. Will prompt if not given.

--scope

Used in the /authorize request. It can cover only one static resource.

--service-principal

The credential representing a service principal.

az login --identity

az login --identity -u

/subscriptions/<subscriptionId>/resourcegroups/myRG/providers/Microsoft.Mana

gedIdentity/userAssignedIdentities/myID

Optional Parameters

--tenant -t

The AAD tenant, must provide when using service principals.

--use-cert-sn-issuer

Used with a service principal configured with Subject Name and Issuer

Authentication in order to support automatic certificate rolls.

--use-device-code

Use CLI's old authentication flow based on device code. CLI will also use this if it

can't launch a browser in your behalf, e.g. in remote SSH or Cloud Shell.

default value: False

--username -u

User name, service principal, or managed service identity ID.

Global Parameters

--debug

Increase logging verbosity to show all debug logs.

--help -h

Show this help message and exit.

--only-show-errors

Only show errors, suppressing warnings.

--output -o

Output format.

--query

JMESPath query string. See http://jmespath.org/ for more information and

examples.

--subscription

Name or ID of subscription. You can configure the default subscription using az

account set -s NAME\_OR\_ID .

--verbose

Increase logging verbosity. Use --debug for full debug logs.

／ Edit

Log out to remove access to Azure subscriptions.

Azure CLI

--username

Account user, if missing, logout the current active account.

Global Parameters

--debug

Increase logging verbosity to show all debug logs.

--help -h

Show this help message and exit.

--only-show-errors

Only show errors, suppressing warnings.

--output -o

Output format.

--query

az logout

az logout [--username]

Optional Parameters

JMESPath query string. See http://jmespath.org/ for more information and

examples.

--subscription

Name or ID of subscription. You can configure the default subscription using az

account set -s NAME\_OR\_ID .

--verbose

Increase logging verbosity. Use --debug for full debug logs.

Recommend the possible next set of commands to take.

There are some custom configurations:

[1] az config set next.execute\_in\_prompt=True/False Turn on/off the step of executing

recommended commands in interactive mode. Turn on by default.

[2] az config set next.recommended\_type=all/scenario/command Set the default

recommended type. All is the default.

[3] az config set next.output=json/jsonc/none/table/tsv/yaml/yamlc/status Set default

output format. Status is the default.

[4] az config set next.command\_num\_limit={command\_amount\_limit} Set the limit of

recommended command items. 5 is the default.

[5] az config set next.scenario\_num\_limit={scenario\_amount\_limit} Set the limit of

recommended scenario items. 5 is the default.

[6] az config set next.show\_arguments=True/False Show/hide the arguments of

recommended items. False is the default.

[7] az config set next.print\_help=True/False Enable/disable whether to print help actively

before executing each command. False is the default.

Azure CLI

az next

az next [--command]

[--scenario]

--command -c

Specify this parameter will only recommend commands.

default value: False

--scenario -s

Specify this parameter will only recommend E2E scenarios.

default value: False

Global Parameters

--debug

Increase logging verbosity to show all debug logs.

--help -h

Show this help message and exit.

--only-show-errors

Only show errors, suppressing warnings.

--output -o

Output format.

--query

JMESPath query string. See http://jmespath.org/ for more information and

examples.

--subscription

Name or ID of subscription. You can configure the default subscription using az

account set -s NAME\_OR\_ID .

--verbose

Increase logging verbosity. Use --debug for full debug logs.

Optional Parameters

Invoke a custom request.

This command automatically authenticates using the logged-in credential: If

Authorization header is not set, it attaches header Authorization: Bearer <token> ,

where <token> is retrieved from AAD. The target resource of the token is derived from -

-url if --url starts with an endpoint from az cloud show --query endpoints . You may also

use --resource for a custom resource.

If Content-Type header is not set and --body is a valid JSON string, Content-Type

header will default to application/json.

For passing JSON in PowerShell, see https://github.com/Azure/azurecli/blob/dev/doc/quoting-issues-with-powershell.md .

Azure CLI

Get Audit log through Microsoft Graph

Azure CLI

Update a Azure Active Directory Graph User's display name

Azure CLI

az rest

az rest --uri

[--body]

[--headers]

[--method {delete, get, head, options, patch, post, put}]

[--output-file]

[--resource]

[--skip-authorization-header]

[--uri-parameters]

Examples

az rest --method get --url

https://graph.microsoft.com/beta/auditLogs/directoryAudits

(Bash or CMD)

az rest --method patch --url

"https://graph.microsoft.com/v1.0/users/johndoe@azuresdkteam.onmicrosoft.com

" --body "{\"displayName\": \"johndoe2\"}"

Get a virtual machine

Azure CLI

Create a public IP address from body.json file

Azure CLI

List the top three resources (Bash)

Azure CLI

--uri --url -u

Request URL. If it doesn't start with a host, CLI assumes it as an Azure resource ID

and prefixes it with the ARM endpoint of the current cloud shown by az cloud show

--query endpoints.resourceManager . Common token {subscriptionId} will be replaced

with the current subscription ID specified by az account set .

(Bash)

az rest --method patch --url

"https://graph.microsoft.com/v1.0/users/johndoe@azuresdkteam.onmicrosoft.com

" --body '{"displayName": "johndoe2"}'

(PowerShell)

az rest --method patch --url

"https://graph.microsoft.com/v1.0/users/johndoe@azuresdkteam.onmicrosoft.com

" --body '{\"displayName\": \"johndoe2\"}'

az rest --method get --uri

/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers

/Microsoft.Compute/virtualMachines/{vmName}?api-version=2019-03-01

az rest --method put --url

https://management.azure.com/subscriptions/{subscriptionId}/resourceGroups/{

resourceGroupName}/providers/Microsoft.Network/publicIPAddresses/{publicIpAd

dressName}?api-version=2019-09-01 --body @body.json

az rest --method get --url

https://management.azure.com/subscriptions/{subscriptionId}/resources?apiversion=2019-07-01 --url-parameters \$top=3

Required Parameters

--body -b

Request body. Use @{file} to load from a file. For quoting issues in different

terminals, see https://github.com/Azure/azurecli/blob/dev/doc/use\_cli\_effectively.md#quoting-issues .

--headers

Space-separated headers in KEY=VALUE format or JSON string. Use @{file} to load

from a file.

--method -m

HTTP request method.

accepted values: delete, get, head, options, patch, post, put

default value: get

--output-file

Save response payload to a file.

--resource

Resource url for which CLI should acquire a token from AAD in order to access the

service. The token will be placed in the Authorization header. By default, CLI can

figure this out based on --url argument, unless you use ones not in the list of "az

cloud show --query endpoints".

--skip-authorization-header

Do not auto-append Authorization header.

default value: False

--uri-parameters --url-parameters

Query parameters in the URL. Space-separated queries in KEY=VALUE format or

JSON string. Use @{file} to load from a file.

Global Parameters

Optional Parameters

--debug

Increase logging verbosity to show all debug logs.

--help -h

Show this help message and exit.

--only-show-errors

Only show errors, suppressing warnings.

--output -o

Output format.

--query

JMESPath query string. See http://jmespath.org/ for more information and

examples.

--subscription

Name or ID of subscription. You can configure the default subscription using az

account set -s NAME\_OR\_ID .

--verbose

Increase logging verbosity. Use --debug for full debug logs.

Runs a self-test of the CLI.

Azure CLI

Global Parameters

--debug

az self-test

az self-test

Increase logging verbosity to show all debug logs.

--help -h

Show this help message and exit.

--only-show-errors

Only show errors, suppressing warnings.

--output -o

Output format.

--query

JMESPath query string. See http://jmespath.org/ for more information and

examples.

--subscription

Name or ID of subscription. You can configure the default subscription using az

account set -s NAME\_OR\_ID .

--verbose

Increase logging verbosity. Use --debug for full debug logs.

Take Azure CLI survey.

Help us improve Azure CLI by sharing your experience. This survey should take about 3

minutes. Learn more at https://go.microsoft.com/fwlink/?linkid=2203309 .

Azure CLI

Global Parameters

--debug

az survey

az survey

Increase logging verbosity to show all debug logs.

--help -h

Show this help message and exit.

--only-show-errors

Only show errors, suppressing warnings.

--output -o

Output format.

--query

JMESPath query string. See http://jmespath.org/ for more information and

examples.

--subscription

Name or ID of subscription. You can configure the default subscription using az

account set -s NAME\_OR\_ID .

--verbose

Increase logging verbosity. Use --debug for full debug logs.

Upgrade Azure CLI and extensions.

Azure CLI

--all

az upgrade

az upgrade [--all {false, true}]

[--yes]

Optional Parameters

Enable updating extensions as well.

accepted values: false, true

default value: true

--yes -y

Do not prompt for checking release notes.

Global Parameters

--debug

Increase logging verbosity to show all debug logs.

--help -h

Show this help message and exit.

--only-show-errors

Only show errors, suppressing warnings.

--output -o

Output format.

--query

JMESPath query string. See http://jmespath.org/ for more information and

examples.

--subscription

Name or ID of subscription. You can configure the default subscription using az

account set -s NAME\_OR\_ID .

--verbose

Increase logging verbosity. Use --debug for full debug logs.

az version

Show the versions of Azure CLI modules and extensions in JSON format by default or

format configured by --output.

Azure CLI

Global Parameters

--debug

Increase logging verbosity to show all debug logs.

--help -h

Show this help message and exit.

--only-show-errors

Only show errors, suppressing warnings.

--output -o

Output format.

--query

JMESPath query string. See http://jmespath.org/ for more information and

examples.

--subscription

Name or ID of subscription. You can configure the default subscription using az

account set -s NAME\_OR\_ID .

--verbose

Increase logging verbosity. Use --debug for full debug logs.

az version

Azure Stack Hub user documentation

Azure Stack Hub is a hybrid cloud platform that lets you use Azure services from your

company's or service provider's datacenter.

About Azure Stack Hub

ｅ OVERVIEW

What is Azure Stack Hub?

Differences between Azure and Azure Stack Hub

Get started

ｂ GET STARTED

Create a Windows VM

Create a Linux VM

ｇ TUTORIAL

Create a VM from a template

Deploy a C# web app to a Windows VM

Deploy a Java web app

Deploy a Python web app

Configure your client

ｂ GET STARTED

Install Azure Stack Hub PowerShell

Install CLI for Azure Stack Hub

ｓ SAMPLE

Use Docker to run PowerShell

Use Visual Studio Code

Infrastructure-as-a-Service (IaaS) on Azure Stack Hub

ｆ QUICKSTART

Quickstart - Create a VM

ｃ HOW-TO GUIDE

Migrate VMs

Deploy a VM in IaaS with a template

Configure a virtual network

Host Apps written in your code

Deploy a GPU IoT module

Platform-as-a-Service (PaaS) on Azure Stack Hub

ｃ HOW-TO GUIDE

Deploy a Service Fabric cluster

Deploy a container to a Azure Stack Hub registry

Deploy an Azure Kubernetes Services (AKS) cluster

Azure Stack Development Kit

documentation

Learn how to deploy and use the Azure Stack Development Kit.

Deploy the ASDK

｀ DEPLOY

Deploy the ASDK

｀ DEPLOY

Release notes

Get started

ｂ GET STARTED

Add an Azure Stack Hub Marketplace item

ｇ TUTORIAL

Offer IaaS services

How to use

ｃ HOW-TO GUIDE

Subscribe to an offer

Create a virtual machine from a template

ｐ CONCEPT

Planning and requirements

Deployment architecture

Platforms used to build and operate hybrid and multicloud solutions.

Azure global

public/sovereign

cloud platform

Azure services

Private cloud

platforms for hosted,

on-prem, and mobile

data centers

Azure Modular Datacenter

Azure Stack HCI

Azure Stack Hub

Azure Stack Hub

Ruggedized

Intelligent edge

platforms for devices

Azure IoT Edge

Azure Sphere

Azure Stack Edge

Windows for IoT

V I D E O

Ignite 2023: Session catalog

V I D E O

Ignite 2022: post-event sessions

(Oct/Nov 2022)

V I D E O

Inspire 2023: Session catalog

V I D E O

Build 2023: post-event sessions

(May/June 2023)

Azure hybrid and multicloud platform

Azure hybrid and multicloud documentation

Resources for building and operating hybrid and multicloud solutions that span the global cloud,

datacenter, and edge.

Services and products for building and operating hybrid and multicloud solutions.

Hybrid and multicloud technologies

AI + Machine Learning

ｅ Azure Bot Service

ｅ Azure Cognitive Search

ｅ Azure Cognitive Services

ｅ Azure Machine Learning

Containers

ｅ Azure Arc-enabled

Kubernetes

ｅ Azure Container Instances

ｅ Azure Container Registry

ｅ Azure Kubernetes Services

on Azure

ｅ Azure Kubernetes Services

on Azure Stack Hub

ｅ Azure Kubernetes Services

on Azure Stack HCI/AKS

hybrid

ｅ Docker on Azure

ｅ IoT Edge on Kubernetes

Database

ｅ Azure Arc-enabled data

services

ｅ SQL Server on Azure Arcenabled servers (preview)

ｅ Azure SQL Edge

Development and

integration

ｅ App Service on Azure Stack

Hub

ｅ Azure App Service Hybrid

Connections

ｅ Azure DevOps for CI/CD

ｅ Azure Event Hubs

ｅ Azure Functions

ｅ Azure IoT Hub

ｅ Azure Logic Apps

ｅ Azure Monitor Application

Insights

ｅ Azure Service Fabric

ｅ Event Hubs on Azure Stack

Hub

ｅ IoT Hub on Azure Stack

Hub (preview)

Edge

ｅ Azure Databox Gateway

ｅ Azure IoT Edge

ｅ Azure IoT Edge on

Kubernetes

ｅ Azure Sphere

ｅ Azure Stack Edge

ｅ Azure SQL Edge

ｅ Windows for IoT

Identity and security

ｅ Azure AD hybrid identity

ｅ Microsoft Defender for

Cloud

ｅ Microsoft Sentinel

ｅ Hybrid Azure AD joined

devices

Guidance and examples to explore and reuse for your hybrid and multicloud projects.

Management

ｅ Azure Arc-enabled data

services

ｅ Azure Arc-enabled

Kubernetes

ｅ Azure Arc-enabled servers

ｅ SQL Server on Azure Arcenabled servers (preview)

ｅ Azure Automation

ｅ Azure Files

ｅ Azure Monitor

ｅ Azure Site Recovery

ｅ Azure Stack HCI hybrid

capabilities

ｅ Windows Admin Center

Azure hybrid services

Networking

ｅ Azure Edge Zones

ｅ Azure ExpressRoute

ｅ Azure Orbital (preview)

ｅ Azure Load Balancer

ｅ Azure Private Link

ｅ Azure Relay

ｅ Azure Traffic Manager

ｅ Azure Virtual Network

ｅ Azure VPN Gateway

Storage

ｅ Avere vFXT for Azure

ｅ Azure Backup

ｅ Azure Files

ｅ Azure Site Recovery

ｅ Azure FXT Edge Filer

Hybrid and multicloud solutions

App patterns and

solution examples

What are patterns and solution

examples?

App design considerations

Explore app patterns

Cross-cloud scaling

DevOps hybrid CI/CD

Footfall detection (retail)

Geo-distributed app

Highly available Kubernetes

cluster

Deploy app solution

examples

Cross-cloud scaling

DevOps hybrid CI/CD

Footfall detection (retail)

Geo-distributed app

Highly available Kubernetes

cluster

Evaluation and learning resources

Azure Stack

Azure Stack development kit

Azure Stack HCI evaluation

guide

Development and

integration

Azure Stack hybrid apps intro

Edge

Azure IoT Edge AI video

intelligence solution

accelerator

Azure Stack hybrid apps intro

Building modern hybrid

applications with Azure Arc

and Azure Stack

Dynamically scale from Azure

Stack Hub to Azure

Introducing the Azure Modular

Datacenter

What's new for Azure Stack

HCI

Build cloud-native applications

that run anywhere

Build consistent hybrid and

multicloud applications with

Azure Arc (Ask the Experts)

Dynamically scale from Azure

Stack Hub to Azure

Logic Apps - Powering the

future of Integration

The future of modern

application development with

.NET

Azure IoT Edge hands-on-labs

Azure IoT solution accelerators

Certified for Azure IoT Edge

devices

General

Align requirements with cloud

types and service models in

Azure

Azure hybrid architectures

Azure hybrid capabilities

Azure hybrid virtual event

Cloud Adoption Framework -

Hybrid and multicloud scenario

Introduction to Azure hybrid

cloud services

IT Ops Talks - All Things Hybrid

(featuring Mark Russinovich)

Microsoft Events Catalog

Microsoft Learn

Identity and security

Deploy Microsoft Sentinel and

connect data sources

Expose hybrid services securely

with Azure Relay

Implement and manage hybrid

identity

Implement hybrid identity with

Windows Server

Intro to Microsoft Sentinel

Windows Server hybrid cloud

management, monitoring, and

security

Management

Azure Arc jumpstart guides

Azure Arc Learn modules

Describe high availability and

disaster recovery strategies

Disaster recovery Learn

modules

High availability Learn modules

Introduction to Azure Arc

Monitor Windows Server IaaS

Virtual Machines and hybrid

instances

Windows Server hybrid cloud

management, monitoring, and

security

Networking

Design a hybrid network

architecture on Azure

Expose hybrid services securely

with Azure Relay

Implement hybrid network

infrastructure

Storage

Implement a hybrid file server

infrastructure

Implement hybrid backup and

recovery with Windows Server

IaaS

Windows Server

Implement a Windows Server

hybrid cloud infrastructure

Implement hybrid backup and

recovery with Windows Server

IaaS

Implement hybrid identity with

Windows Server

Monitor Windows Server IaaS

Virtual Machines and hybrid

instances

Windows Server hybrid cloud

management, monitoring, and

security

Additional resources

General

Azure hybrid blog

Azure hybrid capabilities

Customer Azure Stack Hub

solutions

Customer hybrid cloud stories

Support

Azure support

Azure user voice feedback

Microsoft Q&A forums

Stack Overflow

Technical

Azure developer docs and

tools

Azure IoT Tools for Visual

Studio Code

Code samples browser

Vision AI Developer Kit

Visual Studio Azure

development

Azure Stack Hub archived release notes

Article • 05/25/2023

This article describes the contents of Azure Stack Hub update packages. The update

includes improvements and fixes for this release of Azure Stack Hub.

To access release notes for a different archived version, use the version selector

dropdown above the table of contents on the left.

The latest Azure Stack Hub 2102 update build number is 1.2102.30.97. For updated build

and hotfix information, see the Hotfixes section.

The Azure Stack Hub 2102 update build type is Full.

The 2102 update has the following expected runtimes based on our internal testing:

4 nodes: 8-20 hours

8 nodes: 11-26 hours

12 nodes: 14-32 hours

16 nodes: 17-38 hours

Exact update durations typically depend on the capacity used on your system by tenant

workloads, your system network connectivity (if connected to the internet), and your

system hardware specifications. Durations that are shorter or longer than the expected

value are not uncommon and do not require action by Azure Stack Hub operators

unless the update fails. This runtime approximation is specific to the 2102 update and

should not be compared to other Azure Stack Hub updates.

For more information about update build types, see Manage updates in Azure Stack

Hub.

This release includes a public preview of remote support, which enables a

Microsoft support professional to solve your support case faster by permitting

access to your device remotely and performing limited troubleshooting and repair.

You can enable this feature by granting consent, while controlling the access level

2102 build reference

Update type

What's new

and duration of access. Support can only access your device after a support

request has been submitted. For more information, see Remote support for Azure

Stack Hub.

The Azure Stack Hub infrastructure backup service now supports progressive

backup. This feature helps reduce storage requirements on the external backup

location, and changes the way files are organized on the external backup store. It is

recommended that you do not manipulate files under the backup root directory.

Azure Stack Hub managed disks now support Azure Disk APIs version 2019-07-01,

with a subset of the available features.

Azure Stack Hub Storage now supports Azure Storage services management APIs

version 2019-06-01, with a subset of total available features.

The Azure Stack Hub administrator portal now shows GPU-related information,

including capacity data. This requires a GPU to be installed in the system.

Users can now deploy all supported VM sizes, using Nvidia T4 via the Azure Stack

Hub user portal.

Azure Stack Hub operators can now configure multi-tenancy in Azure Stack Hub

via the administrator portal. For more information, see Configure multi-tenancy.

Azure Stack Hub operators can now configure a legal notice using the privileged

endpoint. For more information, see Configure Azure Stack Hub security controls.

During the update process, Granular Bitmap Repair (GBR), an optimization in the

storage repair process, is introduced to repair out-of-sync data. Compared to the

previous process, smaller segments are repaired, which leads to less repair time

and a shorter overall update duration. GBR is enabled by default for all new

deployments of 2102. For an update to 2102 from an earlier version (2008), GBR is

enabled during the update. GBR requires that all physical disks are in a healthy

state, so an extra validation was added in the UpdateReadiness check. Patch &

update will fail at an early stage if the validation fails. At that point, a cloud admin

must take action to resolve the disk problem before resuming the update. To

follow up with the OEM, check the OEM contact information.

Azure Stack Hub now supports new Dv3, Ev3, and SQL-specific D-series VM sizes.

Azure Stack Hub now supports adding GPUs to any existing system. To add a GPU,

execute stop-azurestack, run through the process of stop-azurestack, add GPUs,

and then run start-azurestack until completion. If the system already had GPUs,

then any previously created GPU VMs must be stop-deallocated and then restarted.

Reduced OEM update time using the live update process.

The AKS engine on Azure Stack Hub added the following new features. For details,

see the release notes under the AKS engine documentation:

General availability of Ubuntu 18.04.

Support for Kubernetes 1.17.17 and 1.18.15.

Certificate rotation command public preview.

CSI Driver Azure Disks public preview.

CSI Driver NFS public preview.

CSI Driver for Azure Blobs private preview.

T4 Nvidia GPU support private preview.

Azure Active Directory integration private preview.

Increased the Network Controller log retention period, so the logs will be available

for longer to help engineers in effective troubleshooting, even after an issue has

been resolved.

Improvements to preserve the Network Controller, Gateway VM, Load Balancer,

and Host Agent logs during an update.

Improved the deletion logic for networking resources that are blocked by a failed

provisioning state.

Reduced the XRP memory to 14 GB per VM and WAS memory to 10 GB per VM. By

avoiding the increase in total VM memory footprint, more tenant VMs are

deployable.

The log collection HTML report, which gives a snapshot of the files on the stamp

and diagnostic share, now has a summarized view of the collected files, roles,

resource providers, and event information to better help understand the success

and failure rate of the log collection process.

Added PowerShell cmdlets Set-AzSLegalNotice and Get-AzSLegalNotice to the

privileged endpoint (PEP) to retrieve and update the content of the login banner

text after deployment.

Removed Active Directory Certificate Services (ADCS) and the CA VM entirely from

Azure Stack Hub. This reduces the infrastructure footprint and saves up to 2 hours

of update time.

Improvements

Changes

The Fabric Resource Provider APIs now expose information about GPUs if available

in the scale unit.

Azure Stack Hub operators can now change the GPU partitioning ratio via

PowerShell (AMD only). This requires all virtual machines to be deallocated.

This build includes a new version of Azure Resource Manager.

The Azure Stack Hub user portal now uses the full screen experience for load

balancers, Network Security Groups, DNS zones, and disk and VM creation.

In the 2102 release, the Windows Admin Center (WAC) is enabled on demand from

an unlocked PEP session. By default, WAC is not enabled. To enable it, specify the -

EnableWac flag; for example, unlock-supportsession -EnableWac .

Proactive log collection now uses an improved algorithm, which captures logs

during error conditions that aren't visible to an operator. This algorithm ensures

that the correct diagnostic info is collected at the right time, without requiring any

operator interaction. In some cases, Microsoft support can begin troubleshooting

and resolving problems sooner. Initial algorithm improvements focus on patch and

update operations. Enabling proactive log collections is recommended, as more

operations are optimized and the benefits increase.

There is a temporary increase of 10 GB of memory used by the Azure Stack Hub

infrastructure.

Fixed an issue in which internal DNS zones became out of sync during update, and

caused the update to fail. This fix has been backported to 2008 and 2005 via

hotfixes.

Fixed an issue in which disk space was exhausted by logs on physical hosts,

Network Controllers, Gateways and load balancers. This fix has been backported to

2008.

Fixed an issue in which deletion of resource groups or virtual networks failed due

to an orphaned resource in the Network Controller layer.

Removed the ND6s\_dev size from the VM size picker, as it is an unsupported VM

size.

Fixed an issue in which performing Stop-Deallocate on a VM results in an MTU

configuration on the VM to be removed. This behavior was inconsistent with Azure.

For information about security updates in this update of Azure Stack Hub, see Azure

Stack Hub security updates.

Fixes

Security updates

Azure Stack Hub releases hotfixes regularly. Starting with the 2005 release, when you

update to a new major version (for example, 1.2005.x to 1.2008.x), the latest hotfixes (if

any) in the new major version are installed automatically. From that point forward, if a

hotfix is released for your build, you should install it.

For more information, see our servicing policy.

Azure Stack Hub hotfixes are only applicable to Azure Stack Hub integrated systems; do

not attempt to install hotfixes on the ASDK.

The 2102 release of Azure Stack Hub must be applied on the 2008 release with the

following hotfixes:

Azure Stack Hub hotfix 1.2008.41.161

When you update to a new major version (for example, 1.2008.x to 1.2102.x), the latest

hotfixes (if any) in the new major version are installed automatically. From that point

forward, if a hotfix is released for your build, you should install it.

After the installation of 2102, if any hotfixes for 2102 are subsequently released, you

should install them:

Azure Stack Hub hotfix 1.2102.30.148

Hotfixes

７ Note

Azure Stack Hub hotfix releases are cumulative; you only need to install the latest

hotfix to get all fixes included in any previous hotfix releases for that version.

Hotfix prerequisites: before applying the 2102 update

After successfully applying the 2102 update

） Important

This update package is only for Azure Stack Hub integrated systems. Do not apply

this update package to the Azure Stack Development Kit (ASDK).

） Important

If your Azure Stack Hub instance is behind by more than two updates, it's

considered out of compliance. You must update to at least the minimum

supported version to receive support.

Azure Stack Hub archived known issues

Article • 05/25/2023

This article lists known issues in unsupported Azure Stack Hub releases. The list is

updated as new issues are identified.

To access known issues for a different archived version, use the version selector

dropdown above the table of contents on the left.

For known Azure Stack Hub update issues, see Troubleshooting Updates in Azure Stack

Hub.

Applicable: This issue applies to Azure Kubernetes Service (AKS) and Azure

Container Registry (ACR) private preview customers who plan to upgrade to 2102

or apply any hotfixes.

Remediation: Uninstall AKS and ACR prior to updating to 2102, or prior to applying

any hotfixes after updating to 2102. Restart the update after uninstalling these

services.

Occurrence: Any stamp that has ACR or AKS installed will experience this failure.

Applicable: This issue applies to all supported releases.

Cause: The two administrative subscription types Metering and Consumption have

been disabled and should not be used. If you have resources in them, an alert is

generated until those resources are removed.

Remediation: If you have resources running on these two subscriptions, recreate

them in user subscriptions.

Occurrence: Common

Update

Update to 2102 fails during pre-update checks for

AKS/ACR

Portal

Administrative subscriptions

Networking

Applicable: This issue applies to all supported releases.

Cause: The documentation links in the overview page of Virtual Network gateway

link to Azure-specific documentation instead of Azure Stack Hub. Use the following

links for the Azure Stack Hub documentation:

Gateway SKUs

Highly Available Connections

Configure BGP on Azure Stack Hub

ExpressRoute circuits

Specify custom IPsec/IKE policies

Applicable: This issue applies to all supported releases.

Cause: Updating/changing the load distribution property (session persistence) has

no effect and some virtual machines might not participate in the traffic load

distribution. For example, if you have 4 backend virtual machines and only 2 clients

connecting to the load balancer, and the load distribution is set to client IP, the

client sessions will always use the same backend virtual machines. Changing the

load distribution property to "none" to distribute the client connections across all

the backend virtual machines will have no effect.

Remediation: Recreating the load balancing rule will ensure the selected settings

are correctly configured to all backend VMs.

Occurrence: Common

Applicable: This issue applies to release 2008 and later.

Cause: IPv6 button is visible on the Add frontend IP address option on a load

balancer. These buttons are disabled and cannot be selected.

Occurrence: Common

Virtual network gateway

Documentation links are Azure-specific

Load balancer

Load Balancer rules

IPv6 button visible on "Add frontend IP address"

Backend and frontend ports when floating IP is enabled

Applicable: This issue applies to all supported releases.

Cause: Both the frontend port and backend port need to be the same in the load

balancing rule when floating IP is enabled. This behavior is by design.

Occurrence: Common

Applicable: This issue applies to release 2102 and earlier.

Cause: When you run the test-azurestack update readiness command the test

triggers the following two warnings:

PowerShell

Remediation: These warnings are to be expected since you don't have the Azure

Kubernetes Service (AKS) or Azure Container Registry (ACR) resource provider

installed.

Occurrence: Common

Applicable: This issue applies to release 2102.

Cause: The alert module for customers depending on Syslog for alerts has been

disabled in this release. For this release, the health and monitoring pipeline was

modified to reduce the number of dependencies and services requirements. As a

result, the new services will not emit alerts to the Syslog pipeline.

Remediation: None.

Occurrence: Common

Applicable: This issue applies to release 2102.

Health and alerts

Azure Kubernetes Service (AKS) or Azure Container

Registry (ACR) resource providers fail in test-azurestack

WARNING: Name resolution of containerservice.aks.azs failed

WARNING: Name resolution of containerregistry.acr.azs failed

No alerts in Syslog pipeline

Usage

Wrong status on infrastructure backup

Cause: The infrastructure backup job can display the wrong status (failed or

successful) while the status itself is refreshed. This does not impact the consistency

of the backup data, but can cause confusion if an actual failure occurred.

Remediation: The issue will be fixed in the next hotfix for 2102.

Known issues for supported versions of Azure Stack Hub can be found under Overview

> Release notes > Known issues

Known issues for supported versions

Azure Stack Hub training and

certification

Article • 07/29/2022

Applies to: Azure Stack Hub integrated systems

Want to learn about Azure Stack Hub and demonstrate your Azure Stack Hub

proficiency? Check out the following training and certification opportunities.

Microsoft IT training course:

Course 20537A: Configuring and Operating a Hybrid Cloud with Microsoft

Azure Stack Hub

Open edx:

edX: Configuring and Operating Microsoft Azure Stack Hub online course

Microsoft Learning Paths:

Job roles and learning paths

Configuring and Operating a Hybrid Cloud with Microsoft Azure Stack Hub certification,

Exam 70-537

Azure Stack Hub documentation

Training

Certification

Next steps