Azure VMware Solution documentation

Learn to use Azure VMware Solution to deploy a VMware Software-defined Data Center (SDDC) private cloud to Azure.

OVERVIEW
What's Azure VMware Solution?

GET STARTED
Architecture and design

HOW-TO GUIDE
Networking

HOW-TO GUIDE
Security

HOW-TO GUIDE
Disaster recovery

HOW-TO GUIDE
Migrate

CONCEPT
Well-Architected Framework (WAF)

CONCEPT
Cloud Adoption Framework (CAF)

Learn about Azure VMware Solution

Overview

- What's Azure VMware Solution?
- What's new?
- Known issues
- FAQ

Quickstart

- Plan the deployment
- Deploy Azure VMware Solution
- Connect to on-premises environment
- Install VMware HCX Connector
- Configure on-premises VMware HCX Connector

Tutorials

- Network planning checklist
- Create a private cloud
- Configure networking
- Access a private cloud
- Create an NSX network segment

Design Azure VMware Solution

Architecture and design

- Private clouds and clusters
- Hub and spoke
- Internet connectivity design considerations
- Network design considerations
- Migrate

Well Architected Framework (WAF)

- Azure VMware Solution design principles
- Infrastructure and provisioning considerations
- Application considerations
- Networking considerations
- Monitoring considerations

Cloud Adoption Framework (CAF)

- Enterprise-Scale for Azure VMware Solution
- Network topology and connectivity
- Management and monitoring
- Enterprise-scale business continuity and disaster recovery
- Enterprise-scale security, governance, and compliance

Build and operate Azure VMware Solution

Private cloud infrastructure

- Create an Azure VMware Solution assessment
- Request host quota for Azure VMware Solution
- Plan the deployment
- Deploy Azure VMware Solution
- Deploy vSAN stretched clusters

Security

- Security solutions for Azure VMware Solution
- Security recommendations
- Security baseline
- Vulnerability Management
- Rotate cloudadmin credentials

Networking

- Connect to on-premises environment
- Connect multiple private clouds in same region
- Configure DHCP server or relay
- Configure DHCP on L2 stretched networks
- Configure DNS forwarder

Backup and recovery

- Backup solutions for VMs
- Set up Azure Backup Server for Azure VMware Solution
- Backup private cloud VMs with Backup Server

Disaster recovery

- Disaster recovery solutions for VMs
- Deploy VMware HCX for disaster recovery
- Deploy VMware SRM for disaster recovery
- Deploy Zerto disaster recovery
- Deploy disaster recovery using JetStream DR software

Virtual machines

- Operating system support for VMs
- Configure Windows Server Failover Cluster
- Deploy VMs from the content library

Migrate

- Migration solutions for VMs
- Install and activate VMware HCX in Azure VMware Solution
- Configure on-premises VMware HCX Connector
- Configure VMware HCX network extension
- VMware HCX Mobility Optimized Networking (MON) guidance

Operate and monitor

- Run Command
- Configure VMware Syslogs
- Configure Alerts
- Arc-enabled Azure VMware Solution

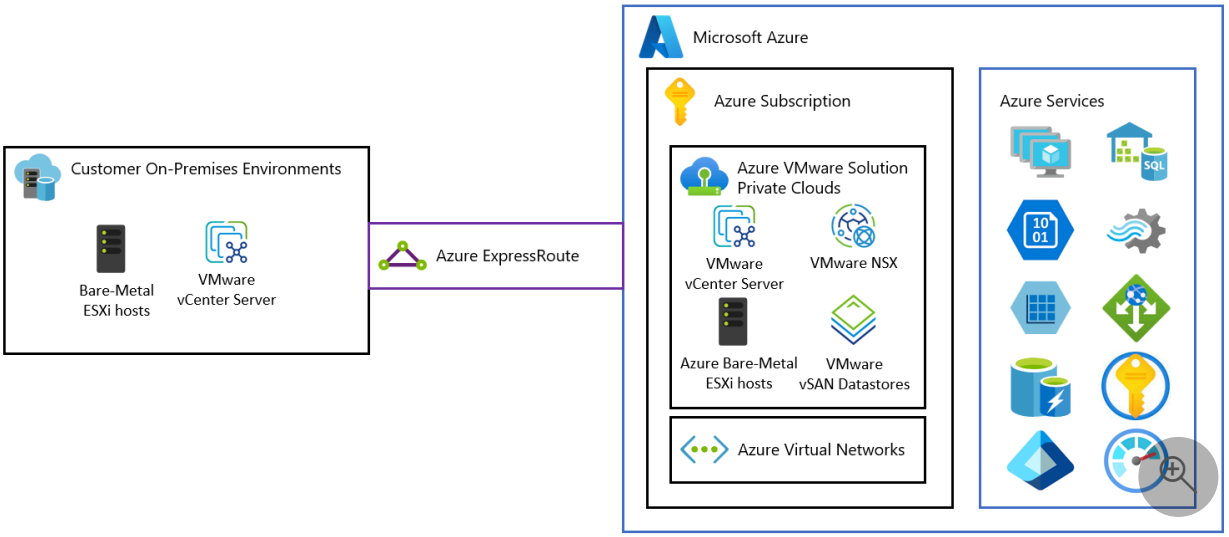
What is Azure VMware Solution?

Article • 09/16/2024

Azure VMware Solution provides private clouds that contain VMware vSphere clusters built from dedicated bare-metal Azure infrastructure. Azure VMware Solution is available in Azure Commercial and Azure Government. The minimum initial deployment is three hosts, with the option to add more hosts, up to a maximum of 16 hosts per cluster. All provisioned private clouds have VMware vCenter Server, VMware vSAN, VMware vSphere, and VMware NSX. As a result, you can migrate workloads from your on-premises environments, deploy new virtual machines (VMs), and consume Azure services from your private clouds. For information about the SLA, see the Azure service-level agreements page.

Azure VMware Solution is a VMware validated solution with ongoing validation and testing of enhancements and upgrades. Microsoft manages and maintains the private cloud infrastructure and software, allowing you to focus on developing and running workloads in your private clouds to deliver business value.

The diagram shows the adjacency between private clouds and VNets in Azure, Azure services, and on-premises environments. Network access from private clouds to Azure services or VNets provides SLA-driven integration of Azure service endpoints. ExpressRoute Global Reach connects your on-premises environment to your Azure VMware Solution private cloud.



Hosts, clusters, and private clouds

Azure VMware Solution clusters are based upon hyper-converged infrastructure. The following table shows the CPU, memory, disk and network specifications of the host.

Expand table

Host Type	CPU (Cores/GHz)	RAM (GB)	vSAN Cache Tier (TB, raw***)	vSAN Capacity Tier (TB, raw***)	Regional availability
AV36	Dual Intel Xeon Gold 6140 CPUs (Skylake microarchitecture) with 18 cores/CPU @ 2.3 GHz, Total 36 physical cores (72 logical cores with hyperthreading)	576	3.2 (NVMe)	15.20 (SSD)	Selected regions (*)
AV36P	Dual Intel Xeon Gold 6240 CPUs (Cascade Lake microarchitecture) with 18 cores/CPU @ 2.6 GHz / 3.9 GHz Turbo, Total 36 physical cores (72 logical cores with hyperthreading)	768	1.5 (Intel Cache)	19.20 (NVMe)	Selected regions (*)
AV52	Dual Intel Xeon Platinum 8270 CPUs (Cascade Lake microarchitecture) with 26 cores/CPU @ 2.7 GHz / 4.0 GHz Turbo, Total 52 physical cores (104 logical cores with hyperthreading)	1,536	1.5 (Intel Cache)	38.40 (NVMe)	Selected regions (*)
AV64	Dual Intel Xeon Platinum 8370C CPUs (Ice Lake microarchitecture) with 32 cores/CPU @ 2.8 GHz / 3.5 GHz Turbo, Total 64 physical cores (128 logical cores with hyperthreading)	1,024	3.84 (NVMe)	15.36 (NVMe)	Selected regions (**)

An Azure VMware Solution cluster requires a minimum number of three hosts. You can only use hosts of the same type in a single Azure VMware Solution private cloud. Hosts used to build or scale clusters come from an isolated pool of hosts. Those hosts passed hardware tests and had all data securely deleted before being added to a cluster.

All the above Host Types have 100 Gbps network interface throughput.

(*) details available via the Azure pricing calculator.

(**) AV64 Prerequisite: An Azure VMware Solution private cloud deployed with AV36, AV36P, or AV52 is required prior to adding AV64.

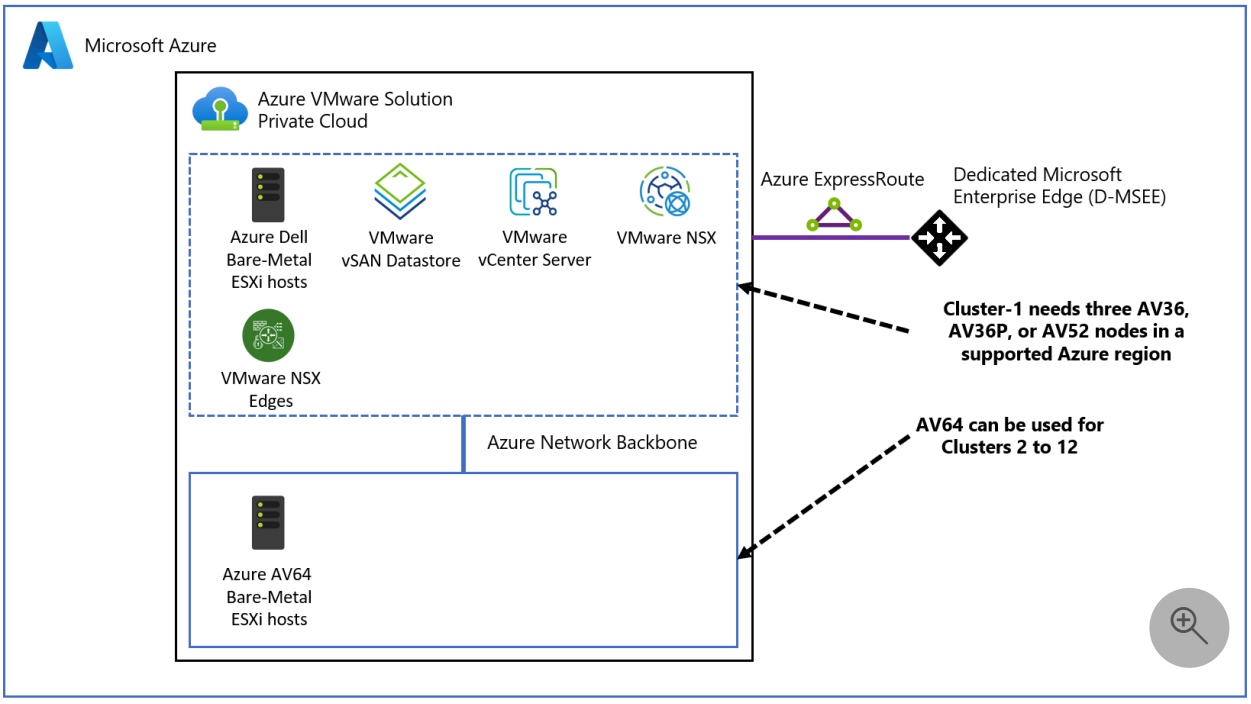
(***) Raw is based upon International Standard of Units (SI) reported by disk manufacturer. Example: 1 TB Raw = 1000000000000 bytes, space calculated by

computer in binary (1TB binary = 1099511627776 bytes binary) would equal 931.3 Gigabytes converted from raw decimal.

You can deploy new or scale existing private clouds through the Azure portal or Azure CLI.

Azure VMware Solution private cloud extension with AV64 node size

The AV64 is a new Azure VMware Solution host SKU, which is available to expand (not to create) the Azure VMware Solution private cloud built with the existing AV36, AV36P, or AV52 SKU. Use the Microsoft documentation to check for availability of the AV64 SKU in the region.



Prerequisite for AV64 usage

See the following prerequisites for AV64 cluster deployment.

- An Azure VMware solution private cloud is created using AV36, AV36P, or AV52 in AV64 supported region/AZ.
- You need one /23 or three (contiguous or noncontiguous) /25 address blocks for AV64 cluster management.

Supportability for customer scenarios

Customer with existing Azure VMware Solution private cloud: When a customer has a deployed Azure VMware Solution private cloud, they can scale the private cloud by adding a separate AV64 vCenter node cluster to that private cloud. In this scenario, customers should use the following steps:

1. Get an AV64 quota approval from Microsoft with the minimum of three nodes. Add other details on the Azure VMware Solution private cloud that you plan to extend using AV64.
2. For RAID-6 FTT2 or RAID-1 FTT3 support, ask Microsoft support to provide you with a feature flag to consume seven Fault Domains per AV64 cluster.
3. Use an existing Azure VMware Solution add-cluster workflow with AV64 hosts to expand.

Customer plans to create a new Azure VMware Solution private cloud: When a customer wants a new Azure VMware Solution private cloud that can use AV64 SKU but only for expansion. In this case, the customer meets the prerequisite of having an Azure VMware Solution private cloud built with AV36, AV36P, or AV52 SKU. The customer needs to buy a minimum of three nodes of AV36, AV36P, or AV52 SKU before expanding using AV64. For this scenario, use the following steps:

1. Get AV36, AV36P, or AV52, and AV64 quota approval from Microsoft with a minimum of three nodes each.
2. Create an Azure VMware Solution private cloud using AV36, AV36P, or AV52 SKU.
3. For RAID-6 FTT2 or RAID-1 FTT3 support, ask Microsoft support to provide you with a feature flag to consume seven Fault Domains per AV64 cluster.
4. Use an existing Azure VMware Solution add-cluster workflow with AV64 hosts to expand.

Azure VMware Solution stretched clusters private cloud: The AV64 SKU isn't supported with Azure VMware Solution stretched clusters private cloud. This means that an AV64-based expansion isn't possible for an Azure VMware Solution stretched clusters private cloud.

AV64 Cluster vSAN fault domain (FD) design and recommendations

The traditional Azure VMware Solution host clusters don't have explicit vSAN FD configuration. The reasoning is the host allocation logic ensures, within clusters, that no two hosts reside in the same physical fault domain within an Azure region. This feature inherently brings resilience and high availability for storage, which the vSAN FD configuration is supposed to bring. More information on vSAN FD can be found in the VMware documentation.

The Azure VMware Solution AV64 host clusters have an explicit vSAN fault domain (FD) configuration. Azure VMware Solution control plane configures seven vSAN fault domains (FDs) for AV64 clusters. Hosts are balanced evenly across the seven FDs as users scale up the hosts in a cluster from three nodes to 16 nodes. Some Azure regions still support a maximum of five FDs as part of the initial release of the AV64 SKU. Refer to the Azure Region Availability Zone (AZ) to SKU mapping table for more information.

Cluster size recommendation

The Azure VMware Solution minimum vSphere node cluster size supported is three. The vSAN data redundancy is handled by ensuring the minimum cluster size of three hosts are in different vSAN FDs. In a vSAN cluster with three hosts, each in a different FD, should an FD fail (for example, the top of rack switch fails), the vSAN data would be protected. Operations such as object creation (new VM, VMDK, and others) would fail. The same is true of any maintenance activities where an ESXi host is placed into maintenance mode and/or rebooted. To avoid scenarios such as these, the recommendation is to deploy vSAN clusters with a minimum of four ESXi hosts.

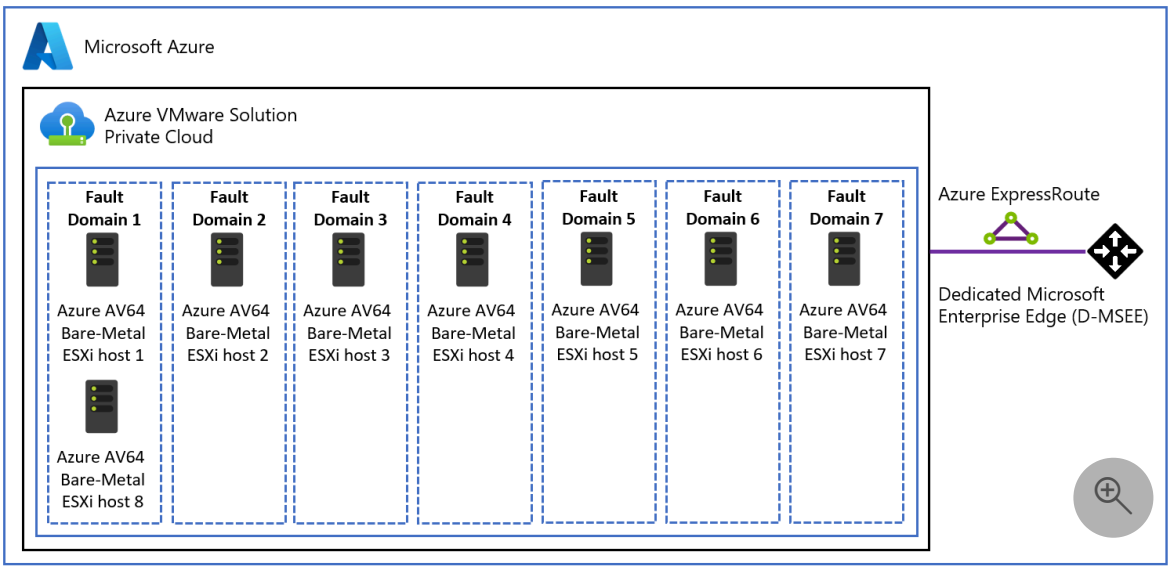
AV64 host removal workflow and best practices

Because of the AV64 cluster vSAN fault domain (FD) configuration and need for hosts balanced across all FDs, the host removal from AV64 cluster differs from traditional Azure VMware Solution host clusters with other SKUs.

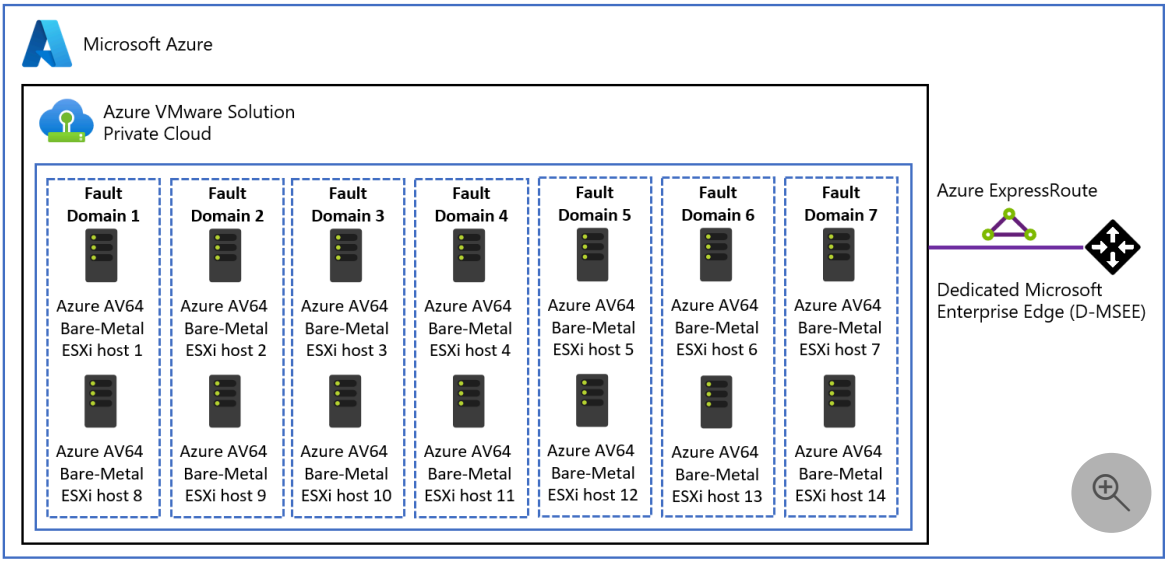
Currently, a user can select one or more hosts to be removed from the cluster using portal or API. One condition is that a cluster should have a minimum of three hosts. However, an AV64 cluster behaves differently in certain scenarios when AV64 uses vSAN FDs. Any host removal request is checked against potential vSAN FD imbalance. If a host removal request creates an imbalance, the request is rejected with the http 409-Conflict response. The http 409-Conflict response status code indicates a request conflict with the current state of the target resource (hosts).

The following three scenarios show examples of instances that normally error out and demonstrate different methods that can be used to remove hosts without creating a vSAN fault domain (FD) imbalance.

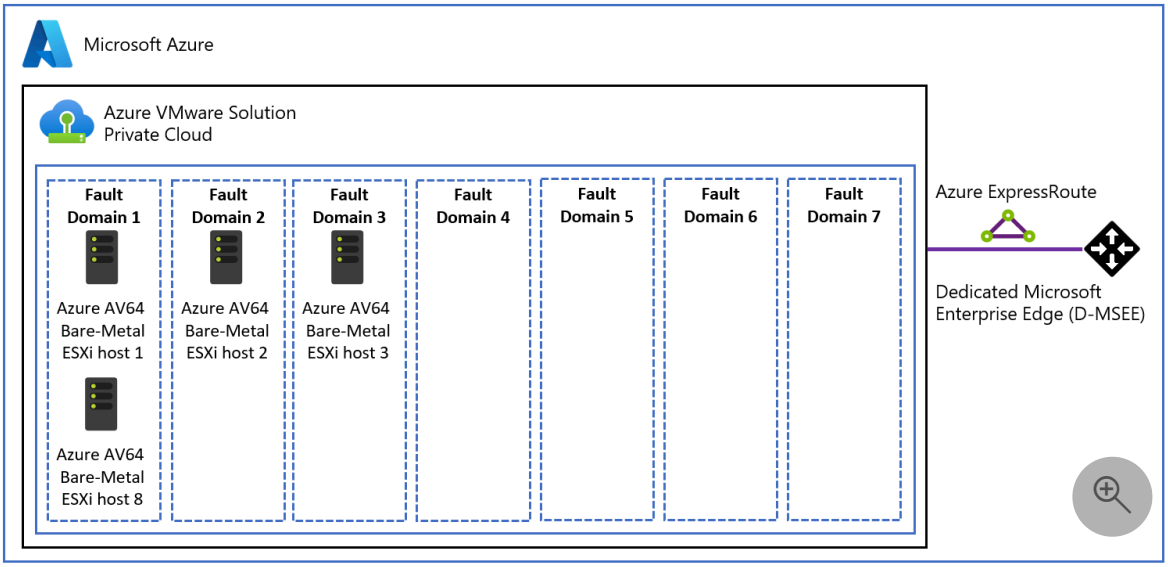
- Removing a host creates a vSAN FD imbalance with a difference of hosts between most and least populated FD to be more than one. In the following example users, need to remove one of the hosts from FD 1 before removing hosts from other FDs.



- Multiple host removal requests are made at the same time and certain host removals create an imbalance. In this scenario, the Azure VMware Solution control plane removes only hosts, which don't create imbalance. In the following example users can't take both of the hosts from the same FDs unless they're reducing the cluster size to four or lower.



- A selected host removal causes less than three active vSAN FDs. This scenario isn't expected to occur given that all AV64 regions have five or seven FDs. While adding hosts, the Azure VMware Solution control plane takes care of adding hosts from all seven FDs evenly. In the following example, users can remove one of the hosts from FD 1, but not from FD 2 or 3.



How to identify the host that can be removed without causing a vSAN FD imbalance: A user can go to the vSphere Client interface to get the current state of vSAN FDs and hosts associated with each of them. This helps to identify hosts (based on the previous examples) that can be removed without affecting the vSAN FD balance and avoid any errors in the removal operation.

AV64 supported RAID configuration

This table provides the list of RAID configuration supported and host requirements in AV64 clusters. The RAID-6 FTT2 and RAID-1 FTT3 policies are supported with the AV64 SKU in some regions. In Azure regions that are currently constrained to five FDs, Microsoft allows customers to use the RAID-5 FTT1 vSAN storage policy for AV64 clusters with six or more nodes to meet the service level agreement (SLA). Refer to the Azure Region Availability Zone (AZ) to SKU mapping table for more information.

Expand table

RAID configuration	Failures to tolerate (FTT)	Minimum hosts required
RAID-1 (Mirroring) Default setting.	1	3
RAID-5 (Erasure Coding)	1	4
RAID-1 (Mirroring)	2	5
RAID-6 (Erasure Coding)	2	6
RAID-1 (Mirroring)	3	7

Storage

Azure VMware Solution supports the expansion of datastore capacity beyond what is included with vSAN using Azure storage services, enabling you to expand datastore capacity without scaling the clusters. For more information, see Datastore capacity expansion options.

Networking

Azure VMware Solution offers a private cloud environment accessible from on-premises sites and Azure-based resources. Services such as Azure ExpressRoute, VPN connections, or Azure Virtual WAN deliver the connectivity. However, these services require specific network address ranges and firewall ports for enabling the services.

When you deploy a private cloud, private networks for management, provisioning, and vMotion get created. You use these private networks to access VMware vCenter Server and VMware NSX Manager and virtual machine vMotion or deployment.

ExpressRoute Global Reach is used to connect private clouds to on-premises environments. It connects circuits directly at the Microsoft Edge level. The connection requires a virtual network (vNet) with an ExpressRoute circuit to on-premises in your subscription. The reason is that vNet gateways (ExpressRoute Gateways) can't transit traffic, which means you can attach two circuits to the same gateway, but it doesn't send the traffic from one circuit to the other.

Each Azure VMware Solution environment is its own ExpressRoute region (its own virtual MSEE device), which lets you connect Global Reach to the 'local' peering location. It allows you to connect multiple Azure VMware Solution instances in one region to the same peering location.

> **Note**
>
> For locations where ExpressRoute Global Reach isn't enabled, for example, because of local regulations, you have to build a routing solution using Azure IaaS VMs. For some examples, see **Azure Cloud Adoption Framework - Network topology and connectivity for Azure VMware Solution**.

Virtual machines deployed on the private cloud are accessible to the internet through the Azure Virtual WAN public IP functionality. For new private clouds, internet access is disabled by default.

For more information, see Networking architecture.

Access and security

Azure VMware Solution private clouds use vSphere role-based access control for enhanced security. You can integrate vSphere SSO LDAP capabilities with Microsoft Entra ID. For more information, see the Access and identity architecture page.

vSAN data-at-rest encryption, by default, is enabled and is used to provide vSAN datastore security. For more information, see Storage architecture.

Data residency and customer data

Azure VMware Solution doesn't store customer data.

VMware software versions

The VMware solution software versions used in new deployments of Azure VMware Solution private clouds are:

Expand table

Software	Version
VMware vCenter Server	8.0 U2b
VMware ESXi	8.0 U2b
VMware vSAN	8.0 U2
VMware vSAN on-disk format	19
VMware vSAN storage architecture	OSA
VMware NSX	4.1.1
VMware HCX	4.9.1
VMware Site Recovery Manager	8.8.0.3
VMware vSphere Replication	8.8.0.3

The current running software version is applied to new clusters added to an existing private cloud, if the vCenter Server version supports it.

Host and software lifecycle maintenance

Regular upgrades of the Azure VMware Solution private cloud and VMware software ensure the latest security, stability, and feature sets are running in your private clouds. For more information, see Host maintenance and lifecycle management.

Monitoring your private cloud

Once you deployed Azure VMware Solution into your subscription, Azure Monitor logs are generated automatically.

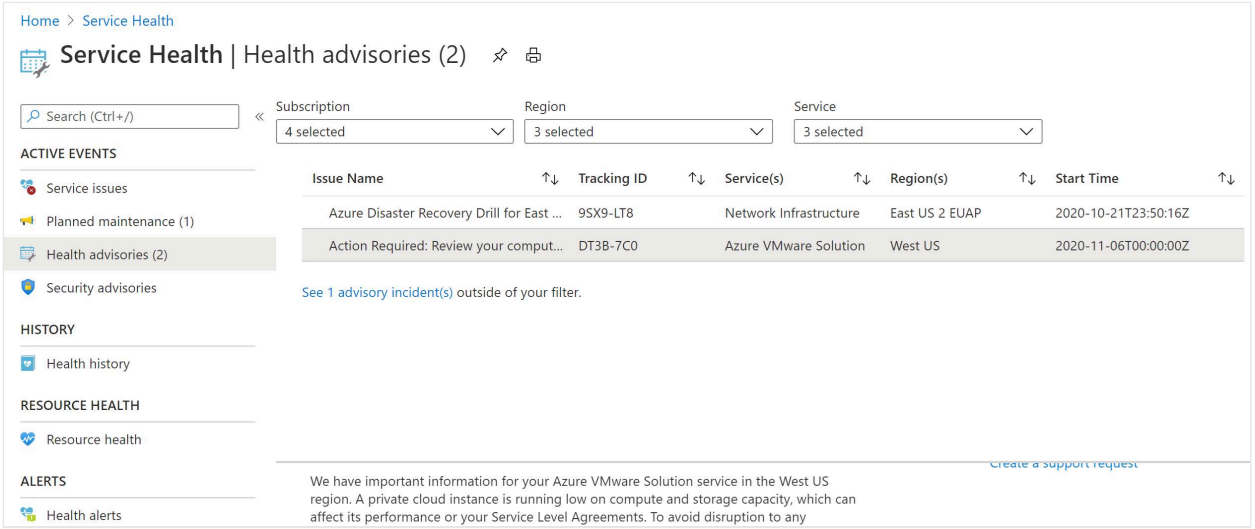
In your private cloud, you can:

- Collect logs on each of your VMs.
- Download and install the MMA agent on Linux and Windows VMs.
- Enable the Azure diagnostics extension.
- Create and run new queries.
- Run the same queries you usually run on your VMs.

Monitoring patterns inside the Azure VMware Solution are similar to Azure VMs within the IaaS platform. For more information and how-tos, see Monitoring Azure VMs with Azure Monitor.

Customer communication

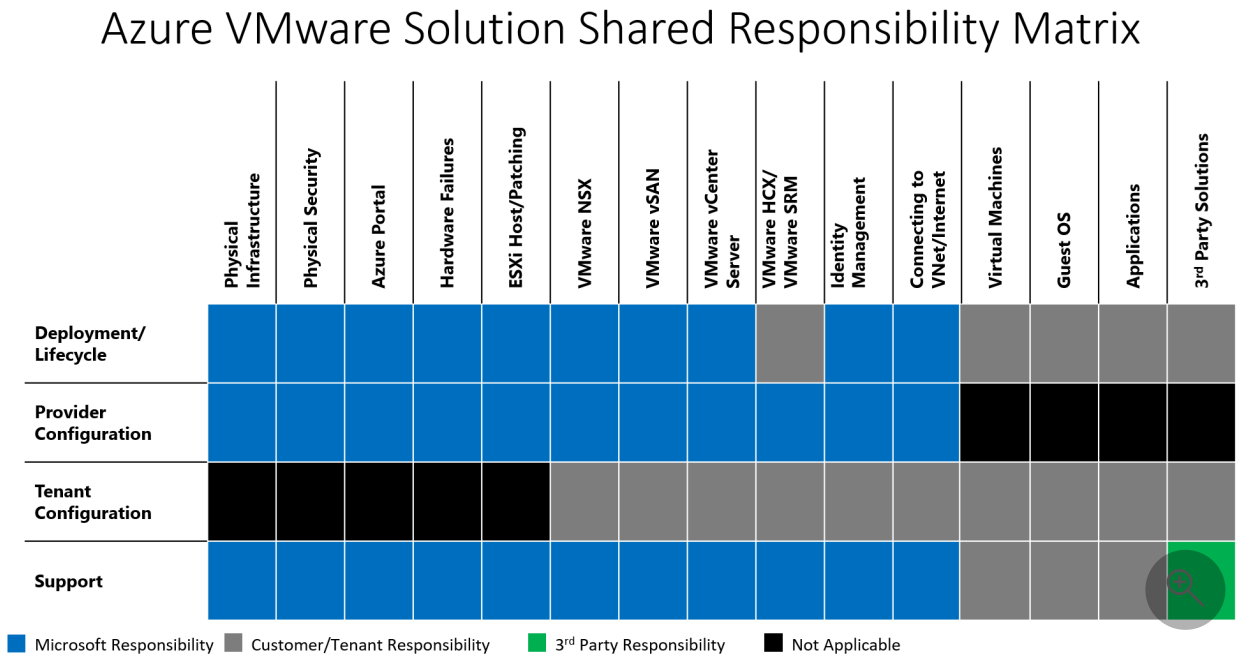
You can find service issues, planned maintenance, health advisories, and security advisories notifications published through **Service Health** in the Azure portal. You can take timely actions when you set up activity log alerts for these notifications. For more information, see Create Service Health alerts using the Azure portal.



Azure VMware Solution responsibility matrix - Microsoft vs customer

Azure VMware Solution implements a shared responsibility model that defines distinct roles and responsibilities of the two parties involved in the offering: customer and Microsoft. The shared role responsibilities are illustrated in more detail in the following two tables.

The shared responsibility matrix table outlines the main tasks that customers and Microsoft each handle in deploying and managing both the private cloud and customer application workloads.



The following table provides a detailed list of roles and responsibilities between the customer and Microsoft, which encompasses the most frequent tasks and definitions. For further questions, contact Microsoft.

Expand table

Role	Task/details
Microsoft - Azure VMware Solution	Physical infrastructure • Azure regions • Azure availability zones • Express Route/Global Reach Compute/Network/Storage • Rack and power Bare Metal hosts • Rack and power network equipment

Role	Task/details
	Private cloud deploy/lifecycle • VMware ESXi deploy, patch, and upgrade • VMware vCenter Servers deploy, patch, and upgrade • VMware NSX deploy, patch, and upgrade • VMware vSAN deploy, patch, and upgrade Private cloud Networking - VMware NSX provider config • Microsoft Edge node/cluster, VMware NSX host preparation • Provider Tier-0 and Tenant Tier-1 Gateway • Connectivity from Tier-0 (using BGP) to Azure Network via ExpressRoute Private cloud compute - VMware vCenter Server provider config • Create default cluster • Configure virtual networking for vMotion, Management, vSAN, and others Private cloud backup/restore • Back up and restore VMware vCenter Server • Back up and restore VMware NSX Manager Private cloud health monitoring and corrective actions, for example: replace failed hosts (optional) VMware HCX deploys with fully configured compute profile on cloud side as add-on (optional) VMware SRM deploys, upgrade, and scale up/down Support - Private cloud platforms and VMware HCX
Customer	Request Azure VMware Solution host quote with Microsoft Plan and create a request for private clouds on Azure portal with: • Host count • Management network range • Other information Configure private cloud network and security (VMware NSX) • Network segments to host applications • More Tier -1 routers • Firewall • VMware NSX LB • IPsec VPN • NAT

Role	Task/details

	• Public IP addresses
	• Distributed firewall/gateway firewall
	• Network extension using VMware HCX or VMware NSX
	• AD/LDAP config for RBAC
	
	Configure private cloud - VMware vCenter Server
	
	• AD/LDAP config for RBAC
	• Deploy and lifecycle management of Virtual Machines (VMs) and application
	  ◦ Install operating systems
	  ◦ Patch operating systems
	  ◦ Install antivirus software
	  ◦ Install backup software
	  ◦ Install configuration management software
	  ◦ Install application components
	  ◦ VM networking using VMware NSX segments
	• Migrate Virtual Machines (VMs)
	  ◦ VMware HCX configuration
	  ◦ Live vMotion
	  ◦ Cold migration
	  ◦ Content library sync
	
	Configure private cloud - vSAN
	
	• Define and maintain vSAN VM policies
	• Add hosts to maintain adequate 'slack space'
	
	Configure VMware HCX
	
	• Download and deploy HCA connector OVA in on-premises
	• Pairing on-premises VMware HCX connector
	• Configure the network profile, compute profile, and service mesh
	• Configure VMware HCX network extension/MON
	• Upgrade/updates
	
	Network configuration to connect to on-premises, virtual network, or internet
	
	Add or delete hosts requests to cluster from Portal
	
	Deploy/lifecycle management of partner (third party) solutions

Partner ecosystem	Support for their product/solution. For reference, the following are some of the supported Azure VMware Solution partner solution/product: • BCDR - VMware SRM, JetStream, Zerto, and others • Backup - Veeam, Commvault, Rubrik, and others • VDI - Horizon, Citrix • Multitenancy for enterprises - VMware Cloud Director Service (CDS), VMware vCloud Director Availability (VCDA)

Role	Task/details
	• Security solutions - BitDefender, TrendMicro, Checkpoint • Other VMware products - Aria Suite, NSX Advanced Load Balancer

Next steps

The next step is to learn key private cloud architecture concepts.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

What's new in Azure VMware Solution

Article • 08/20/2024

Microsoft regularly applies important updates to the Azure VMware Solution for new features and software lifecycle management. You should receive a notification through Azure Service Health that includes the timeline of the maintenance. For more information, see Host maintenance and lifecycle management.

August 2024

All new Azure VMware Solution private clouds are being deployed with VMware vSphere 8.0 version in Azure Commercial. Learn more

Azure VMware Solution was approved to be added as a service within the DoD SRG Impact Level 4 Provisional Authorization (PA) in Microsoft Azure Government.

May 2024

Azure VMware Solution is now generally available in the Central India, UAE North, and Italy North regions, increasing the total region count to 33. Learn more

VMware HCX 4.8.2 is now available. Learn more

April 2024

Azure VMware Solution Stretched Clusters is now generally available in the East US region. Learn more

March 2024

Pure Cloud Block Store for Azure VMware Solution is now generally available. Learn more

VMware vCenter Server 7.0 U3o and VMware ESXi 7.0 U3o are being rolled out. Learn more

February 2024

All new Azure VMware Solution private clouds are being deployed with VMware NSX version 4.1.1. Learn more

November 2023

VMware vSphere 8.0

VMware vSphere 8.0 is targeted for rollout to Azure VMware Solution by H2 2024.

AV64 SKU

Azure VMware Solution AV64 node size is now available in specific regions. The AV64 node is built on Intel Xeon Platinum 8370C CPUs with a total of 64 physical cores, 1 TB of memory and 15.4 TB of total storage. The AV64 SKU can be used for extending existing Azure VMware Solution private clouds built on AV36, AV36P, or AV52 node sizes. Learn more

Azure Elastic SAN (preview)

Azure Elastic SAN is a cloud-native managed SAN offering scalability, cost-efficiency, high performance, and security. It now supports snapshots, enhanced security, and integrates with Azure VMware Solution. Furthermore, as a VMware Certified datastore, Elastic SAN allows you to independently scale your storage and performance, optimizing your total cost of ownership and scalability. Learn more

Azure VMware Solution in Microsoft Azure Government

Azure VMware Solution was approved to be added as a service within the Azure Government Federal Risk and Authorization Management Program (FedRAMP) High Provisional Authorization to Operate (P-ATO). Azure VMware Solution is already available in Azure Commercial and included in the Azure Commercial FedRAMP High P-ATO. With this latest approval, customers and their partners who require the data sovereignty that Azure Government provides can now meet FedRAMP requirements with Azure VMware Solution in Azure Government. Learn more

Azure NetApp Files for Microsoft Azure Government

All Azure NetApp Files features available on Azure public cloud are also available on supported Azure Government regions. For Azure Government regions supported by Azure NetApp Files, see Products Available by Region.

Azure Arc-enabled VMware vSphere

Azure Arc-enabled VMware vSphere term refers to both vSphere on-premises and Azure VMware Solutions customer. Customers can start their onboarding with Azure Arc-enabled VMware vSphere, install agents at-scale, and enable Azure management, observability, and security solutions, while benefitting from the existing lifecycle management capabilities. Azure Arc-enabled VMware vSphere VMs now show up alongside other Azure Arc-enabled servers under 'Machines' view in the Azure portal. Learn more

Five-year Reserved Instance

A Five-year Reserved Instance promotion is available for Azure VMware Solution until March 31, 2024 for customers looking to lock-in their VMware solution costs for multiple years. Visit our pricing page .

August 2023

Available in 30 Azure Regions

Azure VMware Solution is now available in 30 Azure regions. Learn more

Pure Cloud Block Store (preview)

Pure Cloud Block Store for Azure VMware Solution is now in public preview. Now customers can use Pure Cloud Block Store from Pure Storage to scale compute and storage independently for storage heavy workloads. With Pure Cloud Block Store, customers can right size their storage and achieve sizeable savings in the process. Learn more

Azure Arc-enabled VMware vSphere (preview)

Azure Arc-enabled VMware vSphere has a new refresh for the public preview. Now customers can start their onboarding with Azure Arc-enabled VMware vSphere, install agents at-scale, and enable Azure management, observability, and security solutions, while benefitting from the existing lifecycle management capabilities. Azure Arc-enabled VMware vSphere VMs now show up alongside other Azure Arc-enabled servers under 'Machines' view in the Azure portal. Learn more

VMware Cloud Director Service

VMware Cloud Director service for Azure VMware Solution is now available for enterprise. VMware Cloud Director service provides a multicloud control plane for managing multi-tenancy on infrastructure ranging from on-premises customer data centers, managed service provider facilities, and in the cloud.

Well-Architected Assessment Tool

Azure VMware Solution Well-Architected Assessment Tool is now available. Based upon the Microsoft Azure Well-Architected Framework, the assessment tool methodically checks how your workloads align with best practices for resiliency, security, efficiency, and cost optimization. Learn more

VMware Cloud Universal

VMware Cloud Universal now includes Azure VMware Solution.

Updated cloudadmin Permissions

Customers using the cloudadmin@vsphere.local credentials with the vSphere Client now have read-only access to the Management Resource Pool that contains the management and control plane of Azure VMware Solution (vCenter Server, NSX-T Data Center, HCX Manager, SRM Manager).

June 2023

Stretched Clusters Generally Available

Stretched Clusters for Azure VMware Solution is now available and provides 99.99 percent uptime for mission critical applications that require the highest availability. In times of availability zone failure, your virtual machines (VMs) and applications automatically fail over to an unaffected availability zone with no application impact. Learn more

May 2023

Azure VMware Solution in Azure Gov

Azure VMware Service will become generally available on May 17, 2023, to US Federal and State and Local Government (US) customers and their partners, in the regions of Arizona and Virginia. With this release, we're combining world-class Azure infrastructure together with VMware technologies by offering Azure VMware Solutions on Azure Government, which is designed, built, and supported by Microsoft.

New Azure VMware Solution Region: Qatar

We're excited to announce that the Azure VMware Solution is now live in Qatar Central and available to customers.

With the introduction of AV36P in Qatar, customers receive access to 36 cores, 2.6-GHz clock speed, 768 GB of RAM, and 19.2 TB of SSD storage.

To learn more about available regions of Azure products, see Azure Products by Region.

April 2023

VMware HCX Run Commands

Introducing Run Commands for VMware HCX on Azure VMware Solution. You can use these run commands to restart VMware HCX Cloud Manager in your Azure VMware Solution private cloud. Additionally, you can also scale VMware HCX Cloud Manager using Run Commands. To learn how to use run commands for VMware HCX, see Use VMware HCX Run commands.

February 2023

All new Azure VMware Solution private clouds are being deployed with VMware NSX-T Data Center version 3.2.2. NSX-T Data Center versions in existing private clouds will be upgraded to NSX-T Data Center version 3.2.2 through April 2023.

VMware HCX Enterprise Edition - Default

VMware HCX Enterprise is now available and supported on Azure VMware Solution at no extra cost. VMware HCX Enterprise brings valuable services, like Replicated Assisted vMotion (RAV) and Mobility Optimized Networking (MON). VMware HCX Enterprise is now automatically installed for all new VMware HCX add-on requests, and existing VMware HCX Advanced customers can upgrade to VMware HCX Enterprise using the Azure portal. Learn more on how to Install and activate VMware HCX in Azure VMware Solution.

Azure Log Analytics - Monitor Azure VMware Solution

The data in Azure Log Analytics offer insights into issues by searching using Kusto Query Language.

New SKU availability - AV36P and AV52 nodes

The AV36P is now available in the West US Region. This node size is used for memory and storage workloads by offering increased Memory and NVME based SSDs.

AV52 is now available in the East US 2 Region. This node size is used for intensive workloads with higher physical core count, additional memory, and larger capacity

NVME based SSDs.

Customer-managed keys using Azure Key Vault

You can use customer-managed keys to bring and manage your master encryption keys to encrypt vSAN data. Azure Key Vault allows you to store your privately managed keys securely to access your Azure VMware Solution data.

Azure NetApp Files - more storage options available

You can use Azure NetApp Files volumes as a file share for Azure VMware Solution workloads using Network File System (NFS) or Server Message Block (SMB).

Stretched Clusters - increase uptime with Stretched Clusters (Preview)

Stretched clusters for Azure VMware Solution, provides 99.99% uptime for mission critical applications that require the highest availability.

For more information, see Azure Migration and Modernization blog.

January 2023

Starting January 2023, all new Azure VMware Solution private clouds are being deployed with Microsoft signed TLS certificate for vCenter Server and NSX.

November 2022

AV36P and AV52 node sizes available in Azure VMware Solution. The new node sizes increase memory and storage options to optimize your workloads. The gains in performance enable you to do more per server, break storage bottlenecks, and lower transaction costs of latency-sensitive workloads. The availability of the new nodes allows for large latency-sensitive services to be hosted efficiently on the Azure VMware Solution infrastructure.

For pricing and region availability, see the Azure VMware Solution pricing page and see the Products available by region page.

July 2022

VMware HCX Cloud Manager in Azure VMware Solution can now be accessible over a public IP address. You can pair VMware HCX sites and create a service mesh from on-premises to Azure VMware Solution private cloud using Public IP.

VMware HCX with public IP is especially useful in cases where On-premises sites aren't connected to Azure via ExpressRoute or VPN. VMware HCX service mesh appliances can be configured with public IPs to avoid lower tunnel MTUs due to double encapsulation if a VPN is used for on-premises to cloud connections. For more information, please see Enable VMware HCX over the internet

All new Azure VMware Solution private clouds are now deployed with VMware vCenter Server version 7.0 Update 3c and ESXi version 7.0 Update 3c.

Any existing private clouds will be upgraded to those versions. For more information, please see VMware ESXi 7.0 Update 3c Release Notes and VMware vCenter Server 7.0 Update 3c Release Notes.

You'll receive a notification through Azure Service Health that includes the timeline of the upgrade. You can reschedule an upgrade as needed. This notification also provides details on the upgraded component, its effect on workloads, private cloud access, and other Azure services.

June 2022

All new Azure VMware Solution private clouds in regions (East US2, Canada Central, North Europe, and Japan East), are now deployed in with VMware vCenter Server version 7.0 Update 3c and ESXi version 7.0 Update 3c.

Any existing private clouds in the above mentioned regions will also be upgraded to these versions. For more information, please see VMware ESXi 7.0 Update 3c Release Notes and VMware vCenter Server 7.0 Update 3c Release Notes.

May 2022

All new Azure VMware Solution private clouds in regions (Germany West Central, Australia East, Central US and UK West), are now deployed with VMware vCenter Server version 7.0 Update 3c and ESXi version 7.0 Update 3c.

Any existing private clouds in the previously mentioned regions will be upgraded to those versions. For more information, please see VMware ESXi 7.0 Update 3c Release Notes and VMware vCenter Server 7.0 Update 3c Release Notes.

You'll receive a notification through Azure Service Health that includes the timeline of the upgrade. You can reschedule an upgrade as needed. This notification also provides details on the upgraded component, its effect on workloads, private cloud access, and other Azure services.

All new Azure VMware Solution private clouds in regions (France Central, Brazil South, Japan West, Australia Southeast, Canada East, East Asia, and Southeast Asia), are now deployed with VMware vCenter Server version 7.0 Update 3c and ESXi version 7.0 Update 3c.

Any existing private clouds in the previously mentioned regions will be upgraded to those versions. For more information, please see VMware ESXi 7.0 Update 3c Release Notes and VMware vCenter Server 7.0 Update 3c Release Notes.

You'll receive a notification through Azure Service Health that includes the timeline of the upgrade. You can reschedule an upgrade as needed. This notification also provides details on the upgraded component, its effect on workloads, private cloud access, and other Azure services.

February 2022

Per VMware security advisory VMSA-2022-0004, multiple vulnerabilities in VMware ESXi have been reported to VMware.

To address the vulnerabilities (CVE-2021-22040 and CVE-2021-22041) reported in this VMware security advisory, ESXi hosts have been patched in all Azure VMware Solution private clouds to ESXi 6.7, Patch Release ESXi670-202111001. All new Azure VMware Solution private clouds are deployed with the same version.

For more information on this ESXi version, see VMware ESXi 6.7, Patch Release ESXi670-202111001.

No further action is required.

December 2021

Azure VMware Solution has completed maintenance activities to address critical vulnerabilities in Apache Log4j. The fixes documented in the VMware security advisory VMSA-2021-0028.6 to address CVE-2021-44228 and CVE-2021-45046 have been applied to these Azure VMware Solution managed VMware products: vCenter Server, NSX-T Data Center, SRM and HCX. We strongly encourage customers to apply the fixes to on-premises HCX connector appliances.

We also recommend customers to review the security advisory and apply the fixes for other affected VMware products or workloads.

If you need any assistance or have questions, contact us.

VMware has announced a security advisory VMSA-2021-0028, addressing a critical vulnerability in Apache Log4j identified by CVE-2021-44228. Azure VMware Solution is actively monitoring this issue. We're addressing this issue by applying VMware recommended workarounds or patches for Azure VMware Solution managed VMware components as they become available.

Note that you may experience intermittent connectivity to these components when we apply a fix. We strongly recommend that you read the advisory and patch or apply the recommended workarounds for other VMware products you may have deployed in Azure VMware Solution. If you need any assistance or have questions, contact us.

November 2021

Per VMware security advisory VMSA-2021-0027, multiple vulnerabilities in VMware vCenter Server have been reported to VMware.

To address the vulnerabilities (CVE-2021-21980 and CVE-2021-22049) reported in VMware security advisory, vCenter Server has been updated to 6.7 Update 3p release in all Azure VMware Solution private clouds.

For more information, see VMware vCenter Server 6.7 Update 3p Release Notes

No further action is required.

September 2021

Per VMware security advisory VMSA-2021-0020, multiple vulnerabilities in the VMware vCenter Server have been reported to VMware. To address the vulnerabilities (CVE-2021-21991, CVE-2021-21992, CVE-2021-21993, CVE-2021-22005, CVE-2021-22006, CVE-2021-22007, CVE-2021-22008, CVE-2021-22009, CVE-2021-22010, CVE-2021-22011, CVE-2021-22012,CVE-2021-22013, CVE-2021-22014, CVE-2021-22015, CVE-2021-22016, CVE-2021-22017, CVE-2021-22018, CVE-2021-22019, CVE-2021-22020) reported in VMware security advisory VMSA-2021-0020, vCenter Server has been updated to 6.7 Update 3o in all Azure VMware Solution private clouds. All new Azure VMware Solution private clouds are deployed with vCenter Server version 6.7 Update 3o. For more information, see VMware vCenter Server 6.7 Update 3o Release Notes. No further action is required.

All new Azure VMware Solution private clouds are now deployed with ESXi version ESXi670-202103001 (Build number: 17700523). ESXi hosts in existing private clouds have been patched to this version. For more information on this ESXi version, see VMware ESXi 6.7, Patch Release ESXi670-202103001.

July 2021

All new Azure VMware Solution private clouds are now deployed with NSX-T Data Center version 3.1.1. NSX-T Data Center version in existing private clouds will be upgraded through September 2021 to NSX-T Data Center 3.1.1 release.

You'll receive an email with the planned maintenance date and time. You can reschedule an upgrade. The email also provides details on the upgraded component, its effect on workloads, private cloud access, and other Azure services.

For more information on this NSX-T Data Center version, see VMware NSX-T Data Center 3.1.1 Release Notes.

May 2021

Per VMware security advisory VMSA-2021-0010, multiple vulnerabilities in VMware ESXi and vSphere Client (HTML5) have been reported to VMware. To address the vulnerabilities (CVE-2021-21985 and CVE-2021-21986) reported in VMware security advisory VMSA-2021-0010, vCenter Server has been updated in all Azure VMware Solution private clouds. No further action is required.

Azure VMware Solution service will do maintenance work through May 23, 2021, to apply important updates to the vCenter Server in your private cloud. You'll receive a notification through Azure Service Health that includes the timeline of the maintenance for your private cloud. During this time, VMware vCenter Server will be unavailable and you won't be able to manage VMs (stop, start, create, or delete). It's recommended that, during this time, you don't plan any other activities like scaling up private cloud, creating new networks, and so on, in your private cloud. There's no impact to workloads running in your private cloud.

April 2021

All new Azure VMware Solution private clouds are now deployed with VMware vCenter Server version 6.7U3l and NSX-T Data Center version 2.5.2. We're not using NSX-T Data Center 3.1.1 for new private clouds because of an identified issue in NSX-T Data Center 3.1.1 that impacts customer VM connectivity.

The VMware recommended mitigation was applied to all existing private clouds currently running NSX-T Data Center 3.1.1 on Azure VMware Solution. The workaround has been confirmed that there's no impact to customer VM connectivity.

March 2021

All new Azure VMware Solution private clouds are deployed with VMware vCenter Server version 6.7U3l and NSX-T Data Center version 3.1.1. Any existing private clouds will be updated and upgraded **through June 2021** to the releases mentioned above. You'll receive an email with the planned maintenance date and time. You can reschedule an upgrade. The email also provides details on the upgraded component, its effect on workloads, private cloud access, and other Azure services. An hour before the upgrade, you'll receive a notification and then again when it finishes.

Azure VMware Solution service will do maintenance work **through March 19, 2021,** to update the vCenter Server in your private cloud to vCenter Server 6.7 Update 3l version. VMware vCenter Server will be unavailable during this time, so you can't manage your VMs (stop, start, create, delete) or private cloud scaling (adding/removing servers and clusters). However, VMware High Availability (HA) will continue to operate to protect existing VMs.
For more information on this vCenter version, see VMware vCenter Server 6.7 Update 3l Release Notes.

Azure VMware Solution will apply the VMware ESXi 6.7, Patch Release ESXi670-202011002 to existing privates **through March 15, 2021**.

Documented workarounds for the vSphere stack, as per VMSA-2021-0002, will also be applied **through March 15, 2021**.

> **Note**
>
> This is non-disruptive and should not impact the Azure VMware Solution service or workloads. During maintenance, various VMware vSphere alerts, such as *Lost network connectivity on DVPorts* and *Lost uplink redundancy on DVPorts*, appear in vCenter Server and clear automatically as the maintenance progresses.

Post update

Once complete, newer versions of VMware solution components will appear. If you notice any issues or have any questions, contact our support team by opening a support ticket.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Known issues: Azure VMware Solution

Article • 09/19/2024

This article describes the currently known issues with Azure VMware Solution.

Refer to the table to find details about resolution dates or possible workarounds. For more information about the different feature enhancements and bug fixes in Azure VMware Solution, see What's New.

Expand table

Issue	Date discovered	Workaround	Date resolved
VMSA-2021-002 ESXiArgs OpenSLP vulnerability publicized in February 2023	2021	Disable OpenSLP service	February 2021 - Resolved in ESXi 7.0 U3c
After my private cloud NSX-T Data Center upgrade to version 3.2.2, the NSX-T Manager **DNS - Forwarder Upstream Server Timeout** alarm is raised	February 2023	Enable private cloud internet Access, alarm is raised because NSX-T Manager can't access the configured CloudFlare DNS server. Otherwise, change the default DNS zone to point to a valid and reachable DNS server.	February 2023
When first logging in to the vSphere Client, the **Cluster-n: vSAN health alarms are suppressed** alert is active in the vSphere Client	2021	The alert should be considered an informational message, since Microsoft manages the service. Select the **Reset to Green** link to clear it.	2021
When adding a cluster to my private cloud, the **Cluster-n: vSAN physical disk alarm 'Operation'** and **Cluster-n: vSAN cluster alarm 'vSAN Cluster Configuration Consistency'** alerts are active in the vSphere Client	2021	This alert should be considered an informational message, since Microsoft manages the service. Select the **Reset to Green** link to clear it.	2021

Issue	Date discovered	Workaround	Date resolved
After my private cloud NSX-T Data Center upgrade to version 3.2.2, the NSX-T Manager **Capacity - Maximum Capacity Threshold** alarm is raised	2023	Alarm raised because there are more than four clusters in the private cloud with the medium form factor for the NSX-T Data Center Unified Appliance. The form factor needs to be scaled up to large. This issue should get detected through Microsoft, however you can also open a support request.	2023
When I build a VMware HCX Service Mesh with the Enterprise license, the Replication Assisted vMotion Migration option isn't available.	2023	The default VMware HCX Compute Profile doesn't have the Replication Assisted vMotion Migration option enabled. From the Azure VMware Solution vSphere Client, select the VMware HCX option and edit the default Compute Profile to enable Replication Assisted vMotion Migration.	2023
VMSA-2023-023 VMware vCenter Server Out-of-Bounds Write Vulnerability (CVE-2023-34048) publicized in October 2023	October 2023	A risk assessment of CVE-2023-03048 was conducted and it was determined that sufficient controls are in place within Azure VMware Solution to reduce the risk of CVE-2023-03048 from a CVSS Base Score of 9.8 to an adjusted Environmental Score of 6.8 or lower. Adjustments from the base score were possible due to the network isolation of the Azure VMware Solution vCenter Server (ports 2012, 2014, and 2020 aren't exposed via any interactive network path) and multiple levels of authentication and authorization necessary to gain interactive access to the vCenter Server network segment. Azure VMware Solution is currently rolling out 7.0U3o to address this issue.	March 2024 - Resolved in ESXi 7.0U3o
The AV64 SKU currently supports RAID-1 FTT1, RAID-5 FTT1, and RAID-1 FTT2 vSAN storage policies. For more information, see AV64 supported RAID configuration	Nov 2023	The AV64 SKU now supports 7 Fault Domains and all vSAN storage policies. For more information, see AV64 supported Azure regions	June 2024

Issue	Date discovered	Workaround	Date resolved
VMware HCX version 4.8.0 Network Extension (NE) Appliance VMs running in High Availability (HA) mode may experience intermittent Standby to Active failover. For more information, see HCX - NE appliances in HA mode experience intermittent failover (96352)	Jan 2024	Avoid upgrading to VMware HCX 4.8.0 if you're using NE appliances in a HA configuration.	Feb 2024 - Resolved in VMware HCX 4.8.2
VMSA-2024-0006 ESXi Use-after-free and Out-of-bounds write vulnerability	March 2024	For ESXi 7.0, Microsoft worked with Broadcom on an AVS specific hotfix as part of the ESXi 7.0U3o rollout. For the 8.0 rollout, Azure VMware Solution is deploying vCenter Server 8.0 U2b & ESXi 8.0 U2b which is not vulnerable.	August 2024 - Resolved in ESXi 7.0U3o and vCenter Server 8.0 U2b & ESXi 8.0 U2b
When I run the VMware HCX Service Mesh Diagnostic wizard, all diagnostic tests will be passed (green check mark), yet failed probes will be reported. See HCX - Service Mesh diagnostics test returns 2 failed probes	2024	None, this will be fixed in 4.9+.	N/A
VMSA-2024-0011 Out-of-bounds read/write vulnerability (CVE-2024-22273)	June 2024	Microsoft has confirmed the applicability of the CVE-2024-22273 vulnerability and it will be addressed in the upcoming 8.0u2b Update.	July 2024
VMSA-2024-0012 Multiple Vulnerabilities in the DCERPC Protocol and Local Privilege Escalations	June 2024	Microsoft, working with Broadcom, adjudicated the risk of these vulnerabilities at an adjusted Environmental Score of 6.8 or lower. Adjustments from the base score were possible due to the network isolation of the Azure VMware Solution vCenter	N/A

Issue	Date discovered	Workaround	Date resolved
		Server (ports 2012, 2014, and 2020 aren't exposed via any interactive network path) and multiple levels of authentication and authorization necessary to gain interactive access to the vCenter Server network segment. A plan is being put in place to address these vulnerabilities at a future date TBD.	
Zerto DR isn't currently supported with the AV64 SKU. The AV64 SKU uses ESXi host secure boot and Zerto DR hasn't implemented a signed VIB for the ESXi install.	2024	Continue using the AV36, AV36P, and AV52 SKUs for Zerto DR.	N/A
VMSA-2024-0013 (CVE-2024-37085) VMware ESXi Active Directory Integration Authentication Bypass	July 2024	Azure VMware Solution does not provide Active Directory integration and isn't vulnerable to this attack.	N/A
AV36P SKU new private cloud deploys with vSphere 7, not vSphere 8.	September 2024	The AV36P SKU is waiting for a Hotfix to be deployed, which will resolve this issue.	N/A
VMSA-2024-0019 Vulnerability in the DCERPC Protocol and Local Privilege Escalations	September 2024	Microsoft, working with Broadcom, adjudicated the risk of CVE-2024-38812 at an adjusted Environmental Score of 6.8 and CVE-2024-38813 with an adjusted Environmental Score of 6.8. Adjustments from the base scores were possible due to the network isolation of the Azure VMware Solution vCenter Server DCERPC protocol access (ports 2012, 2014, and 2020 aren't exposed via any interactive network path) and multiple levels of authentication and authorization necessary to gain interactive access to the Azure VMware Solution vCenter Server. A plan is being put in place to address these vulnerabilities at a future date TBD.	N/A

In this article, you learned about the current known issues with the Azure VMware Solution.

For more information, see About Azure VMware Solution.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Plan the Azure VMware Solution deployment

Article • 02/05/2024

Planning your Azure VMware Solution deployment is crucial for creating a successful production-ready environment for virtual machines (VMs) and migration. During the planning process, you identify and gather the necessary information for your deployment. Be sure to document the information you collect for easy reference during the deployment. A successful deployment results in a production-ready environment for creating VMs and migration.

In this tutorial, learn how to complete the following tasks:

- ✓ Identify the Azure subscription, resource group, region, and resource name
- ✓ Identify the size hosts and determine the number of clusters and hosts
- ✓ Request a host quota for an eligible Azure plan
- ✓ Identify the /22 CIDR IP segment for private cloud management
- ✓ Identify a single network segment
- ✓ Define the virtual network gateway
- ✓ Define VMware HCX network segments

After you're finished, follow the recommended Next steps at the end of this article to continue with this getting started guide.

Identify the subscription

Identify the subscription you plan to use to deploy Azure VMware Solution. You can create a new subscription or use an existing one.

> ⓘ **Note**
>
> The subscription must be associated with a Microsoft Enterprise Agreement (EA), a Cloud Solution Provider (CSP) Azure plan, or a Microsoft Customer Agreement (MCA). For more information, see **Eligibility criteria**.

Identify the resource group

Identify the resource group you want to use for your Azure VMware Solution. Generally, a resource group is created specifically for Azure VMware Solution, but you can use an

existing resource group.

Identify the region or location

Identify the region you want Azure VMware Solution deployed.

Define the resource name

The resource name is a friendly and descriptive name for your Azure VMware Solution private cloud, for example, **MyPrivateCloud**.

> **Important**
>
> The name must not exceed 40 characters. If the name exceeds this limit, you won't be able to create public IP addresses for use with the private cloud.

Identify the size hosts

Identify the size hosts that you want to use when deploying Azure VMware Solution.

Azure VMware Solution clusters are based upon hyper-converged infrastructure. The following table shows the CPU, memory, disk and network specifications of the host.

Expand table

Host Type	CPU (Cores/GHz)	RAM (GB)	vSAN Cache Tier (TB, raw)	vSAN Capacity Tier (TB, raw)	Regional availability
AV36	Dual Intel Xeon Gold 6140 CPUs (Skylake microarchitecture) with 18 cores/CPU @ 2.3 GHz, Total 36 physical cores (72 logical cores with hyperthreading)	576	3.2 (NVMe)	15.20 (SSD)	Selected regions (*)
AV36P	Dual Intel Xeon Gold 6240 CPUs (Cascade Lake microarchitecture) with 18 cores/CPU @ 2.6 GHz / 3.9 GHz Turbo, Total 36 physical cores (72 logical cores with hyperthreading)	768	1.5 (Intel Cache)	19.20 (NVMe)	Selected regions (*)

Host Type	CPU (Cores/GHz)	RAM (GB)	vSAN Cache Tier (TB, raw)	vSAN Capacity Tier (TB, raw)	Regional availability
AV52	Dual Intel Xeon Platinum 8270 CPUs (Cascade Lake microarchitecture) with 26 cores/CPU @ 2.7 GHz / 4.0 GHz Turbo, Total 52 physical cores (104 logical cores with hyperthreading)	1,536	1.5 (Intel Cache)	38.40 (NVMe)	Selected regions (*)
AV64	Dual Intel Xeon Platinum 8370C CPUs (Ice Lake microarchitecture) with 32 cores/CPU @ 2.8 GHz / 3.5 GHz Turbo, Total 64 physical cores (128 logical cores with hyperthreading)	1,024	3.84 (NVMe)	15.36 (NVMe)	Selected regions (**)

An Azure VMware Solution cluster requires a minimum number of three hosts. You can only use hosts of the same type in a single Azure VMware Solution private cloud. Hosts used to build or scale clusters come from an isolated pool of hosts. Those hosts passed hardware tests and had all data securely deleted before being added to a cluster.

All the above Host Types have 100 Gbps network interface throughput.

(*) details available via the Azure pricing calculator.

(**) AV64 Prerequisite: An Azure VMware Solution private cloud deployed with AV36, AV36P, or AV52 is required prior to adding AV64.

Determine the number of clusters and hosts

The first Azure VMware Solution deployment you do consists of a private cloud containing a single cluster. You need to define the number of hosts you want to deploy to the first cluster for your deployment.

For each private cloud created, there's one vSAN cluster by default. You can add, delete, and scale clusters. The minimum number of hosts per cluster and the initial deployment is three.

You use vCenter Server and NSX-T Manager to manage most aspects of cluster configuration and operation. All local storage of each host in a cluster is under the control of VMware vSAN.

The Azure VMware Solution management and control plane have the following resource requirements that need to be accounted for during solution sizing of a **standard private cloud**.

Expand table

Area	Description	Provisioned vCPUs	Provisioned vRAM (GB)	Provisioned vDisk (GB)	Typical CPU Usage (GHz)	Typical vRAM Usage (GB)	Typical Raw vSAN Datastore Usage (GB)
VMware vSphere	vCenter Server	8	28	915	1.1	3.9	1,854
VMware vSphere	vSphere Cluster Service VM 1	1	0.1	2	0.1	0.1	5
VMware vSphere	vSphere Cluster Service VM 2	1	0.1	2	0.1	0.1	5
VMware vSphere	vSphere Cluster Service VM 3	1	0.1	2	0.1	0.1	5
VMware vSphere	ESXi node 1	N/A	N/A	N/A	5.1	0.2	N/A
VMware vSphere	ESXi node 2	N/A	N/A	N/A	5.1	0.2	N/A
VMware vSphere	ESXi node 3	N/A	N/A	N/A	5.1	0.2	N/A
VMware vSAN	vSAN System Usage	N/A	N/A	N/A	N/A	N/A	5,458
VMware NSX-T Data Center	NSX-T Unified Appliance Node 1	12	48	300	2.5	13.5	613

Area	Description	Provisioned vCPUs	Provisioned vRAM (GB)	Provisioned vDisk (GB)	Typical CPU Usage (GHz)	Typical vRAM Usage (GB)	Typical Raw vSAN Datastore Usage (GB)
VMware NSX-T Data Center	NSX-T Unified Appliance Node 2	12	48	300	2.5	13.5	613
VMware NSX-T Data Center	NSX-T Unified Appliance Node 3	12	48	300	2.5	13.5	613
VMware NSX-T Data Center	NSX-T Edge VM 1	8	32	200	1.3	0.6	409
VMware NSX-T Data Center	NSX-T Edge VM 2	8	32	200	1.3	0.6	409
VMware HCX (Optional Add-On)	HCX Manager	4	12	65	1	2.5	140
VMware Site Recovery Manager (Optional Add-On)	SRM Appliance	4	12	33	1	1	79
VMware vSphere (Optional Add-On)	vSphere Replication Manager Appliance	4	8	33	1	0.6	75
VMware vSphere (Optional Add-On)	vSphere Replication Server Appliance	2	1	33	1	0.3	68
	Total	77 vCPUs	269.3 GB	2,385 GB	30 GHz	50.4 GB	10,346 GB (9,032

Area	Description	Provisioned vCPUs	Provisioned vRAM (GB)	Provisioned vDisk (GB)	Typical CPU Usage (GHz)	Typical vRAM Usage (GB)	Typical Raw vSAN Datastore Usage (GB)

The Azure VMware Solution management and control plane have the following resource requirements that need to be accounted for during solution sizing of a **stretched clusters private cloud**. VMware SRM isn't included in the table since it currently isn't supported.

Expand table

Area	Description	Provisioned vCPUs	Provisioned vRAM (GB)	Provisioned vDisk (GB)	Typical CPU Usage (GHz)	Typical vRAM Usage (GB)	Typical Raw vSAN Datastore Usage (GB)
VMware vSphere	vCenter Server	8	28	915	1.1	3.9	3,708
VMware vSphere	vSphere Cluster Service VM 1	1	0.1	2	0.1	0.1	5
VMware vSphere	vSphere Cluster Service VM 2	1	0.1	2	0.1	0.1	5
VMware vSphere	vSphere Cluster Service VM 3	1	0.1	2	0.1	0.1	5
VMware vSphere	ESXi node 1	N/A	N/A	N/A	5.1	0.2	N/A
VMware vSphere	ESXi node 2	N/A	N/A	N/A	5.1	0.2	N/A
VMware vSphere	ESXi node 3	N/A	N/A	N/A	5.1	0.2	N/A
VMware vSphere	ESXi node 4	N/A	N/A	N/A	5.1	0.2	N/A

Area	Description	Provisioned vCPUs	Provisioned vRAM (GB)	Provisioned vDisk (GB)	Typical CPU Usage (GHz)	Typical vRAM Usage (GB)	Typical Raw vSAN Datastore Usage (GB)
VMware vSphere	ESXi node 5	N/A	N/A	N/A	5.1	0.2	N/A
VMware vSphere	ESXi node 6	N/A	N/A	N/A	5.1	0.2	N/A
VMware vSAN	vSAN System Usage	N/A	N/A	N/A	N/A	N/A	10,722
VMware NSX-T Data Center	NSX-T Unified Appliance Node 1	12	48	300	2.5	13.5	1,229
VMware NSX-T Data Center	NSX-T Unified Appliance Node 2	12	48	300	2.5	13.5	1,229
VMware NSX-T Data Center	NSX-T Unified Appliance Node 3	12	48	300	2.5	13.5	1,229
VMware NSX-T Data Center	NSX-T Edge VM 1	8	32	200	1.3	0.6	817
VMware NSX-T Data Center	NSX-T Edge VM 2	8	32	200	1.3	0.6	817
VMware HCX (Optional Add-On)	HCX Manager	4	12	65	1	2.5	270
	Total	67 vCPUs	248.3 GB	2,286 GB	42.3 GHz	49.1 GB	20,036 GB (17,173 GB with

Area	Description	Provisioned vCPUs	Provisioned vRAM (GB)	Provisioned vDisk (GB)	Typical CPU Usage (GHz)	Typical vRAM Usage (GB)	Typical Raw vSAN Datastore Usage (GB)
							expected 1.2x Data Reduction ratio)

These resource requirements only apply to the first cluster deployed in an Azure VMware Solution private cloud. Subsequent clusters only need to account for the vSphere Cluster Service, ESXi resource requirements and vSAN System Usage in solution sizing.

The virtual appliance **Typical Raw vSAN Datastore Usage** values account for the space occupied by virtual machine files, including configuration and log files, snapshots, virtual disks and swap files.

The VMware ESXi nodes have compute usage values that account for the vSphere VMkernel hypervisor overhead, vSAN overhead and NSX-T distributed router, firewall and bridging overhead. These are estimates for a standard three cluster configuration. The storage requirements are listed as not applicable (N/A) since a boot volume separate from the vSAN Datastore is used.

The VMware vSAN System Usage storage overhead accounts for vSAN performance management objects, vSAN file system overhead, vSAN checksum overhead and vSAN deduplication and compression overhead. To view this consumption, select the Monitor, vSAN Capacity object for the vSphere Cluster in the vSphere Client.

The VMware HCX and VMware Site Recovery Manager resource requirements are optional Add-ons to the Azure VMware Solution service. Discount these requirements in the solution sizing if they aren't being used.

The VMware Site Recovery Manager Add-On has the option of configuring multiple VMware vSphere Replication Server Appliances. The previous table assumes one vSphere Replication Server appliance is used.

Sizing an Azure VMware Solution is an estimate; the sizing calculations from the design phase should be validated during the testing phase of a project to ensure the Azure VMware Solution is sized correctly for the application workload.

> **Tip**

You can always extend the cluster and add additional clusters later if you need to go beyond the initial deployment number.

> **Note**
>
> To learn about the limits for the number of hosts per cluster, the number of clusters per private cloud, and the number of hosts per private cloud, check **Azure subscription and service limits, quotas, and constraints**.

Request a host quota

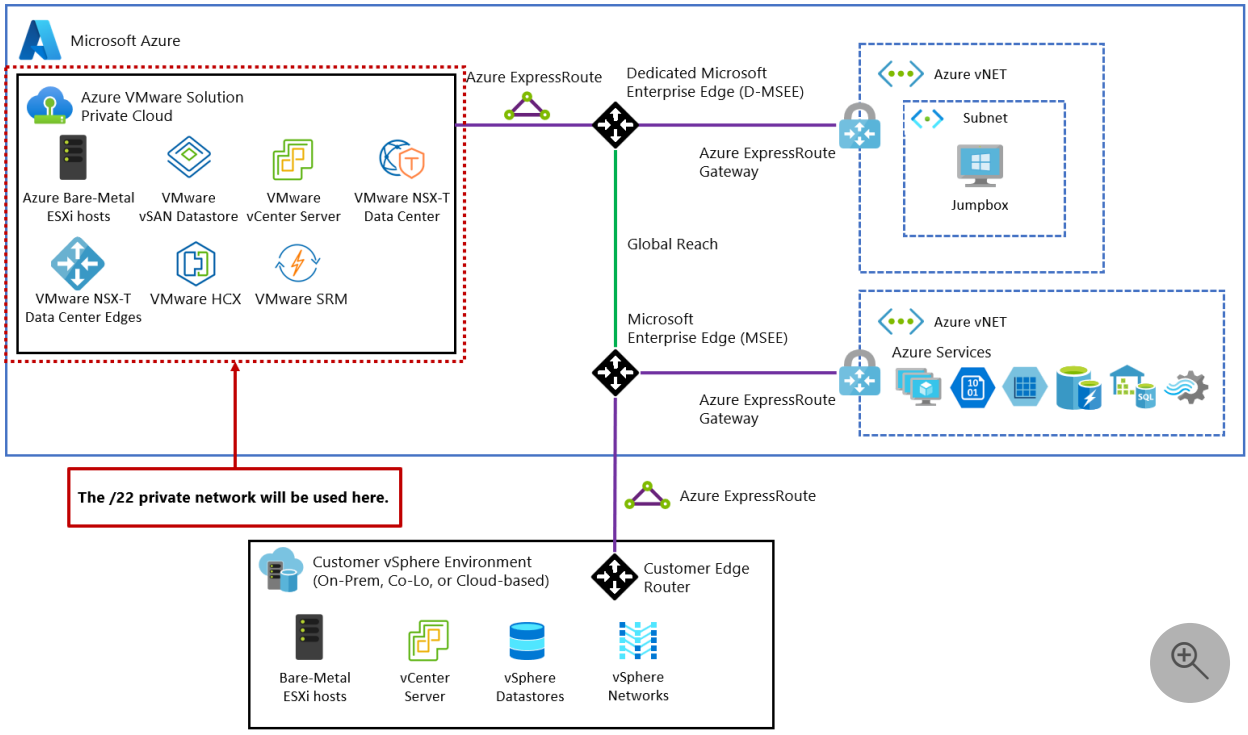
Request a host quota early in the planning process to ensure a smooth deployment of your Azure VMware Solution private cloud. Before making a request, identify the Azure subscription, resource group, and region. Determine the size of hosts, number of clusters, and hosts you need.

The support team takes up to five business days to confirm your request and allocate your hosts.

- EA customers
- CSP customers

Define the IP address segment for private cloud management

Azure VMware Solution requires a /22 CIDR network, such as `10.0.0.0/22`. This address space is divided into smaller network segments (subnets) for Azure VMware Solution management segments including vCenter Server, VMware HCX, NSX-T Data Center, and vMotion functionality. The following diagram shows Azure VMware Solution management IP address segments.

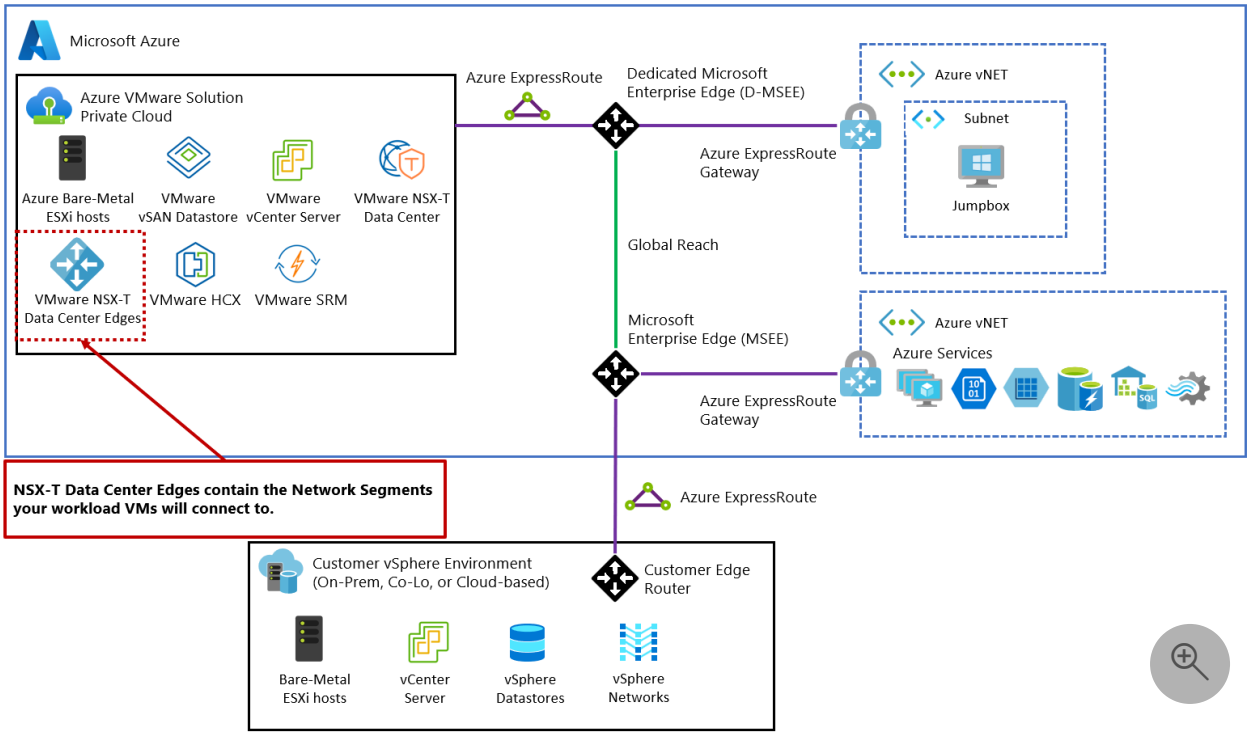


> **Important**
>
> The /22 CIDR network address block shouldn't overlap with any existing network segment you already have on-premises or in Azure. For details of how the /22 CIDR network is broken down per private cloud, see Routing and subnet considerations.

Define the IP address segment for VM workloads

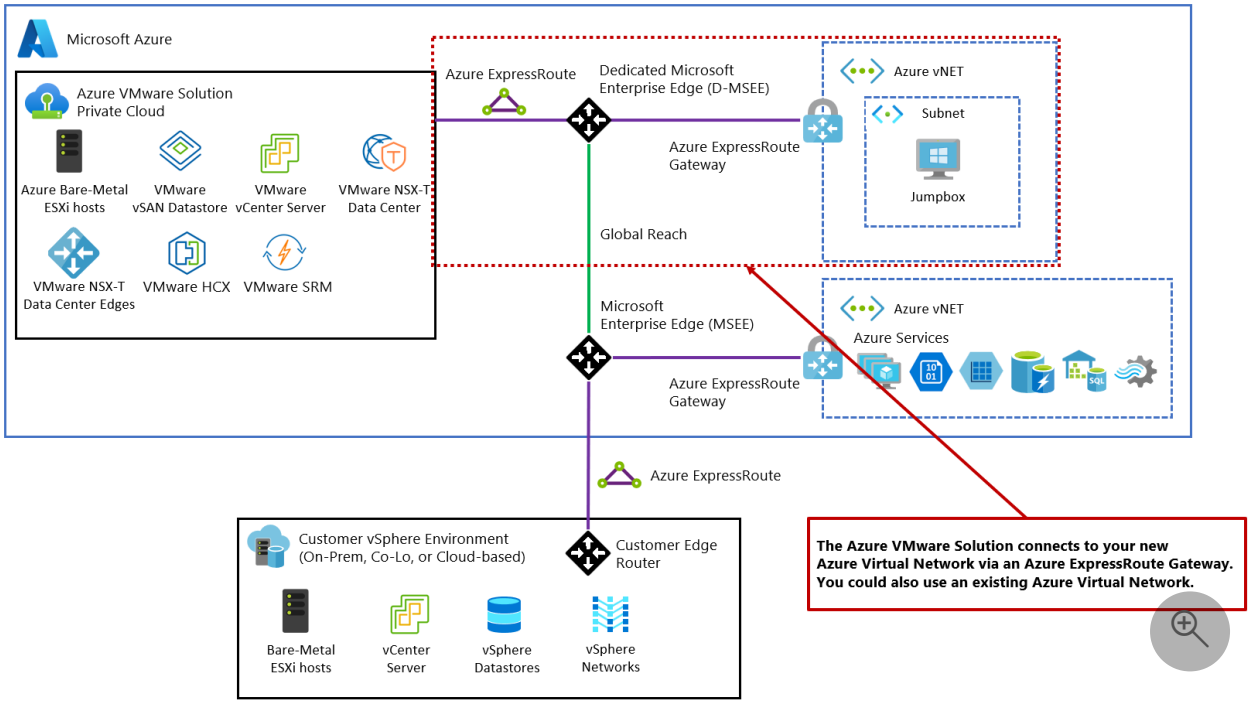
In a VMware vSphere environment, VMs must connect to a network segment. As Azure VMware Solution production deployment expands, you often see a combination of L2 extended segments from on-premises and local NSX-T Data Center network segments.

For the initial deployment, identify a single network segment (IP network), for example, `10.0.4.0/24`. This network segment is used primarily for testing purposes during the initial deployment. The address block shouldn't overlap with any network segments on-premises or within Azure and shouldn't be within the /22 network segment already defined.



Define the virtual network gateway

Azure VMware Solution requires an Azure Virtual Network and an ExpressRoute circuit. Decide whether to use an *existing* or *new* ExpressRoute virtual network gateway. If you choose a *new* virtual network gateway, create it after creating your private cloud. Using an existing ExpressRoute virtual network gateway is acceptable. For planning purposes, note which ExpressRoute virtual network gateway you use.



Important

You can connect to a virtual network gateway in an Azure Virtual WAN, but it is out of scope for this quick start.

Define VMware HCX network segments

VMware HCX is an application mobility platform that simplifies application migration, workload rebalancing, and business continuity across data centers and clouds. You can migrate your VMware vSphere workloads to Azure VMware Solution and other connected sites through various migration types.

VMware HCX Connector deploys a subset of virtual appliances (automated) that require multiple IP segments. When you create your network profiles, you use the IP segments. Identify the following listed items for the VMware HCX deployment, which supports a pilot or small product use case. Modify as necessary based on your migration needs.

- **Management network:** For on-premises VMware HCX deployment, identify a management network for VMware HCX. Typically, it's the same management network used by your on-premises VMware vSphere cluster. At a minimum, identify **two** IPs on this network segment for VMware HCX. You might need larger numbers, depending on the scale of your deployment beyond the pilot or small use case.

  > ⓘ **Note**
  >
  > For large environments, create a new /26 network and present it as a port group to your on-premises VMware vSphere cluster instead of using the existing management network. You can then create up to 10 service meshes and 60 network extenders (-1 per service mesh). You can stretch **eight** networks per network extender by using Azure VMware Solution private clouds.

- **Uplink network:** For on-premises VMware HCX deployment, identify an Uplink network for VMware HCX. Use the same network you plan to use for the Management network.

- **vMotion network:** For on-premises VMware HCX deployment, identify a vMotion network for VMware HCX. Typically, it's the same network used for vMotion by your on-premises VMware vSphere cluster. At a minimum, identify **two** IPs on this network segment for VMware HCX. You might need larger numbers, depending on the scale of your deployment beyond the pilot or small use case.

You must expose the vMotion network on a distributed virtual switch or vSwitch0. If it's not, modify the environment to accommodate.

> **Note**
>
> Many VMware vSphere environments use non-routed network segments for vMotion, which poses no problems.

- **Replication network:** For on-premises VMware HCX deployment, define a replication network. Use the same network you're using for your Management and Uplink networks. If the on-premises cluster hosts use a dedicated Replication VMkernel network, reserve **two** IP addresses in this network segment and use the Replication VMkernel network for the replication network.

Determine whether to extend your networks

Optionally, you can extend network segments from on-premises to Azure VMware Solution. If you extend network segments, identify those networks now following these guidelines:

- Networks must connect to a vSphere Distributed Switch (vDS) in your on-premises VMware environment.
- Networks that are on a vSphere Standard Switch can't be extended.

> **Important**
>
> These networks are extended as a final step of the configuration, not during deployment.

Next steps

Now that you gathered and documented the necessary information, continue to the next tutorial to create your Azure VMware Solution private cloud.

Deploy Azure VMware Solution

Deploy and configure Azure VMware Solution

Article • 05/15/2024

After you plan your deployment, deploy and configure your Azure VMware Solution private cloud.

In this tutorial, you'll:

- ✓ Register the resource provider and create a private cloud
- ✓ Connect to a new or existing ExpressRoute virtual network gateway
- ✓ Validate the network connection

Once you completed this section, follow the next steps provided at the end of this tutorial.

Register the Microsoft.AVS resource provider

To use Azure VMware Solution, you must first register the resource provider with your subscription. For more information about resource providers, see Azure resource providers and types.

Portal

1. Sign in to the Azure portal.

   > **Note**
   >
   > If you need access to the Azure US Gov portal, go to https://portal.azure.us/

2. On the Azure portal menu, select **All services**.
3. In the **All services** box, enter **subscription**, and then select **Subscriptions**.
4. Select the subscription from the subscription list to view.
5. Select **Resource providers** and enter **Microsoft.AVS** into the search.

6. If the resource provider isn't registered, select **Register**.

Create an Azure VMware Solution private cloud

You can create an Azure VMware Solution private cloud using the Azure portal or the Azure CLI.

Portal

1. Sign in to the Azure portal.

   > **Note**
   >
   > If you need access to the Azure US Gov portal, go to https://portal.azure.us/

2. Select **Create a resource**.

3. In the **Search services and marketplace** text box, type `Azure VMware Solution` and select it from the search results.

4. On the **Azure VMware Solution** window, select **Create**.

5. If you need more hosts, request a host quota increase.

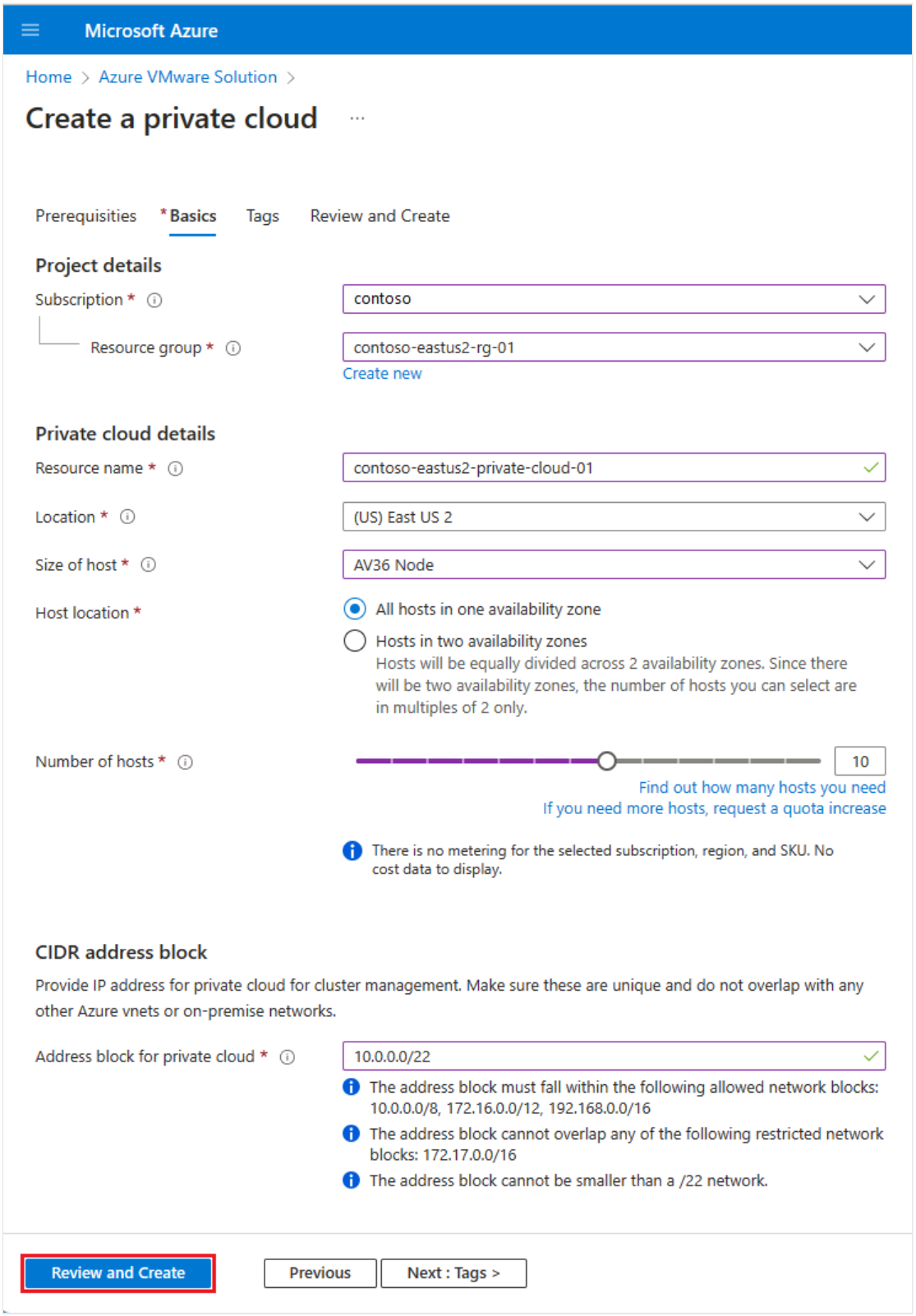
6. On the **Basics** tab, enter values for the fields and then select **Review + Create**.

   > **Tip**
   >
   > You gathered this information during the planning phase of this quick start.

Expand table

Field	Value
Subscription	Select the subscription you plan to use for the deployment. All resources in an Azure subscription are billed together.

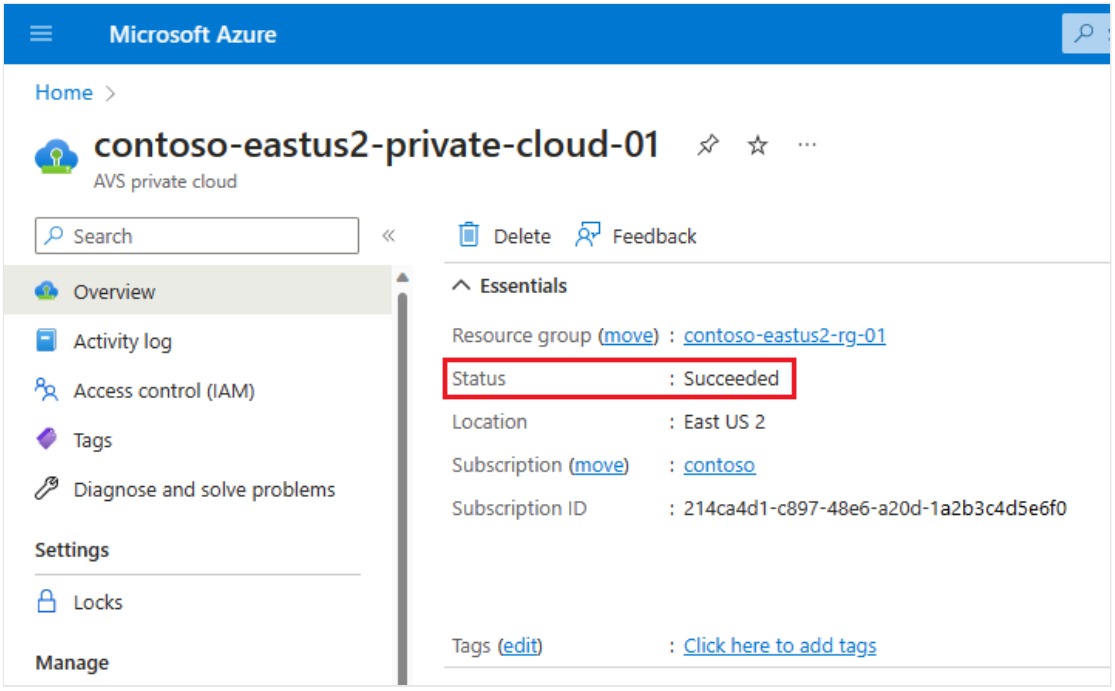
Field	Value
Resource group	Select the resource group for your private cloud. An Azure resource group is a logical container into which Azure resources are deployed and managed. Alternatively, you can create a new resource group for your private cloud.
Resource name	Provide the name of your Azure VMware Solution private cloud.
Location	Select a location, such as **(US) East US 2**. It's the *region* you defined during the planning phase.
Size of host	Select the **AV36**, **AV36P** or **AV52** SKU.
Host Location	Select **All hosts in one availability zone** for a standard private cloud or **Hosts in two availability zones** for stretched clusters.
Number of hosts	Number of hosts allocated for the private cloud cluster. The default value is 3, which you can increase or decrease after deployment. If these nodes aren't listed as available, contact support to request a quota increase. You can also select the link labeled **If you need more hosts, request a quota increase** in the Azure portal.
Address block for private cloud	Provide an IP address block for the private cloud. The CIDR represents the private cloud management network and is used for the cluster management services, such as vCenter Server and NSX-T Manager. Use /22 address space, for example, 10.175.0.0/22. The address should be unique and not overlap with other Azure Virtual Networks and with on-premises networks.



7. Verify the information entered, and if correct, select **Create**.

> **Note**
>
> This step takes roughly 3-4 hours. Adding a single host in an existing or the same cluster takes between 30 - 45 minutes.

8. Verify that the deployment was successful. Navigate to the resource group you created and select your private cloud. You see the status of **Succeeded** when the deployment is finished.



Connect to Azure Virtual Network with ExpressRoute

In the planning phase, you defined whether to use an *existing* or *new* ExpressRoute virtual network gateway.

> **ⓘ Important**
>
> If you plan to scale your Azure VMware Solution hosts using Azure NetApp Files datastores, deploying the vNet close to your hosts with an ExpressRoute virtual network gateway is crucial. The closer the storage is to your hosts, the better the performance.

Use a new ExpressRoute virtual network gateway

> **ⓘ Important**
>
> You must have a virtual network with a GatewaySubnet that **does not** already have a virtual network gateway.

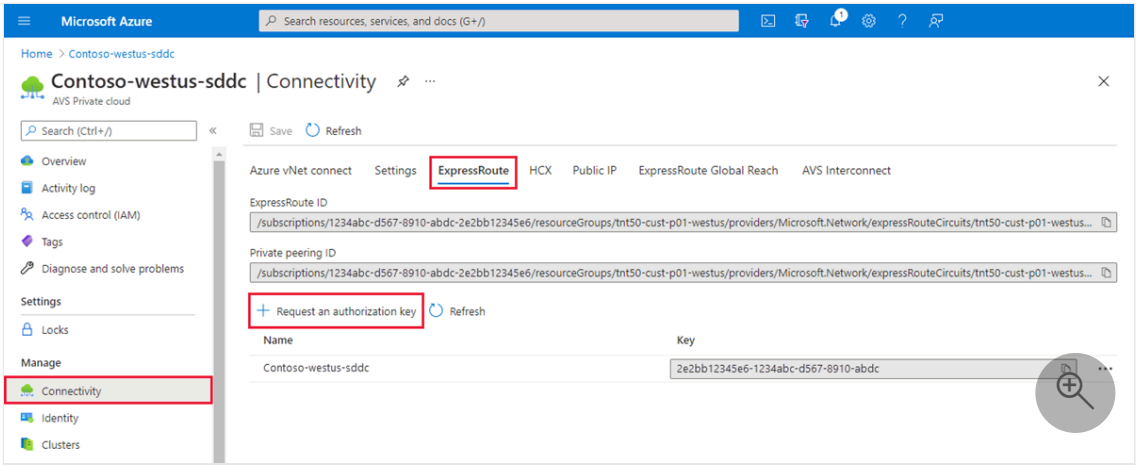
Expand table

If	Then
You don't already have a virtual network...	Create the following: 1. Virtual network 2. GatewaySubnet 3. Virtual network gateway 4. Connect ExpressRoute to the gateway
You already have a virtual network **without** a GatewaySubnet...	Create the following: 1. GatewaySubnet 2. Virtual network gateway 3. Connect ExpressRoute to the gateway
You already have a virtual network **with** a GatewaySubnet...	Create the following: 1. Virtual network gateway 2. Connect ExpressRoute to the gateway

Use an existing virtual network gateway

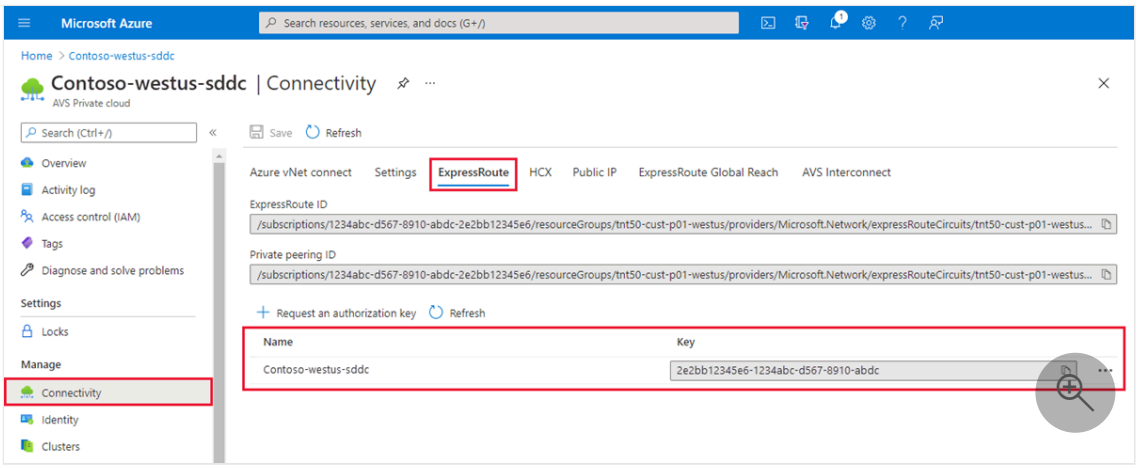
1. Request an ExpressRoute authorization key:

   a. In the Azure portal, navigate to the Azure VMware Solution private cloud. Select **Manage** > **Connectivity** > **ExpressRoute** and then select **+ Request an authorization key**.



   b. Provide a name for it and select **Create**.

It can take about 30 seconds to create the key. Once created, the new key appears in the list of authorization keys for the private cloud.



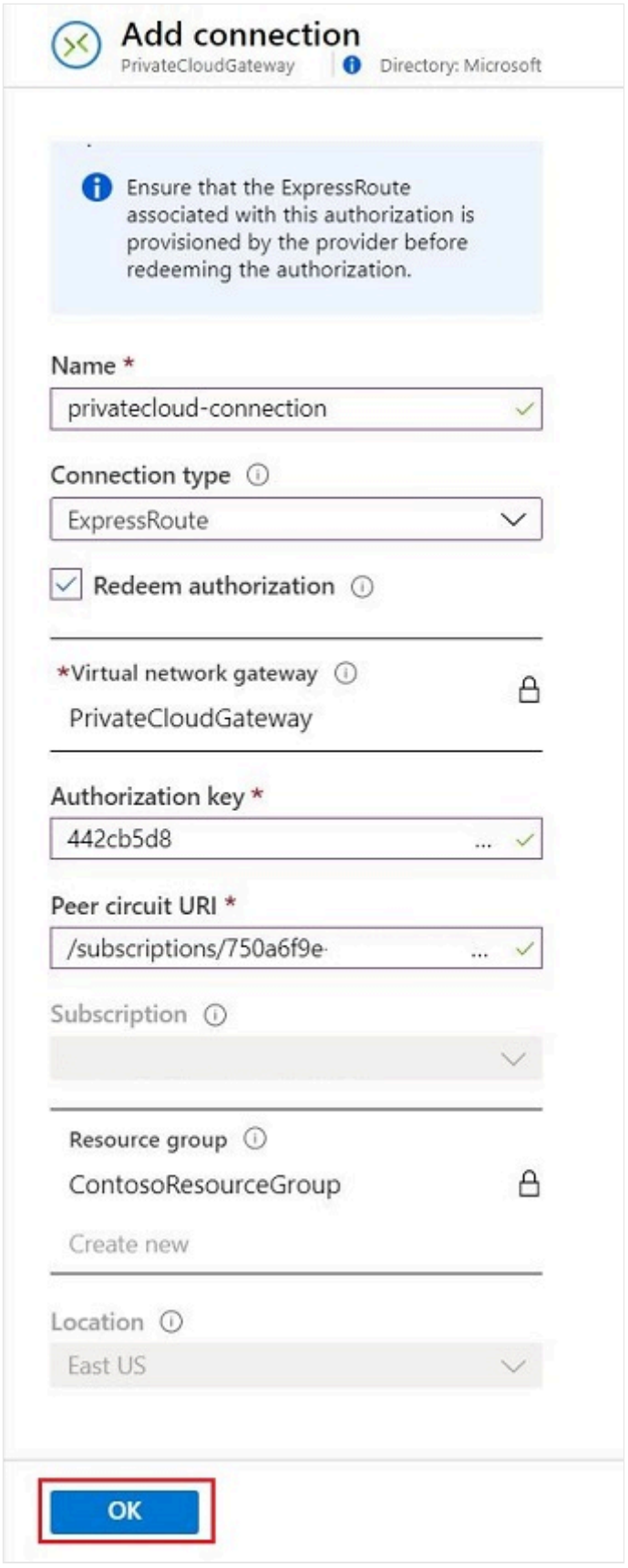
c. Copy the authorization key and ExpressRoute ID. You need them to complete the peering. The authorization key disappears after some time, so copy it as soon as it appears.

2. Navigate to the virtual network gateway you plan to use and select **Connections** > **+ Add**.

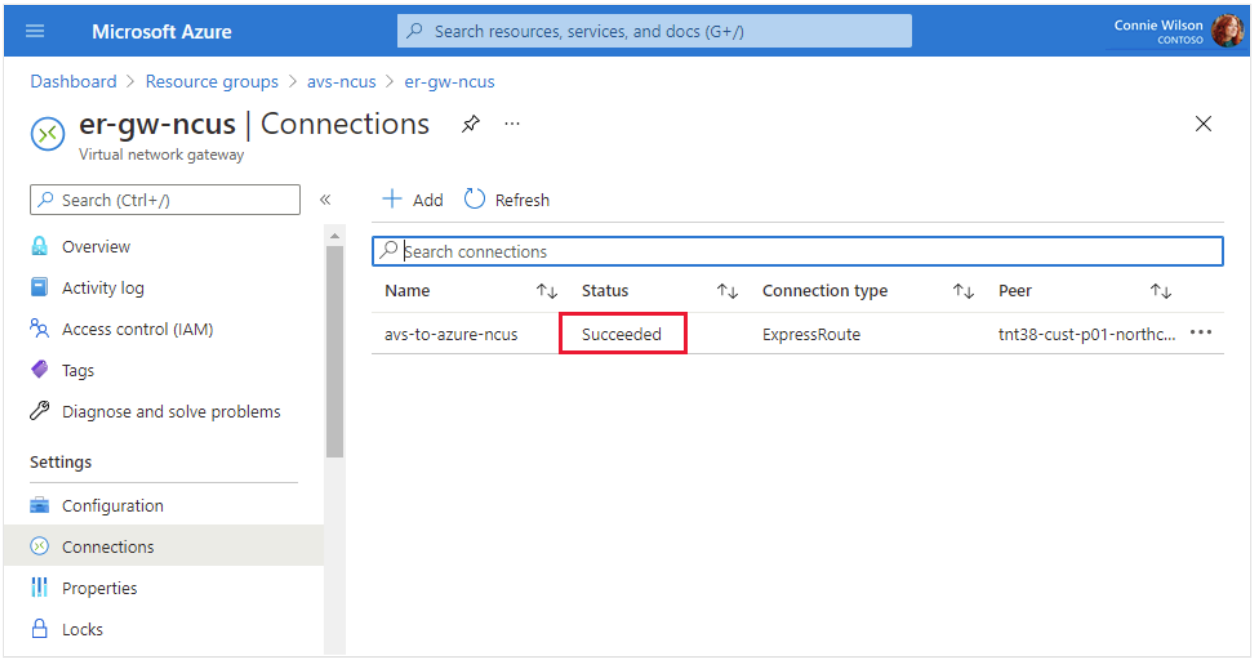
3. On the **Add connection** page, provide values for the fields, and select **OK**.

Expand table

Field	Value
Name	Enter a name for the connection.
Connection type	Select **ExpressRoute**.
Redeem authorization	Ensure this box is selected.
Virtual network gateway	The virtual network gateway you intend to use.
Authorization key	Paste the authorization key you copied earlier.
Peer circuit URI	Paste the ExpressRoute ID you copied earlier.



The connection between your ExpressRoute circuit and your Virtual Network is created.



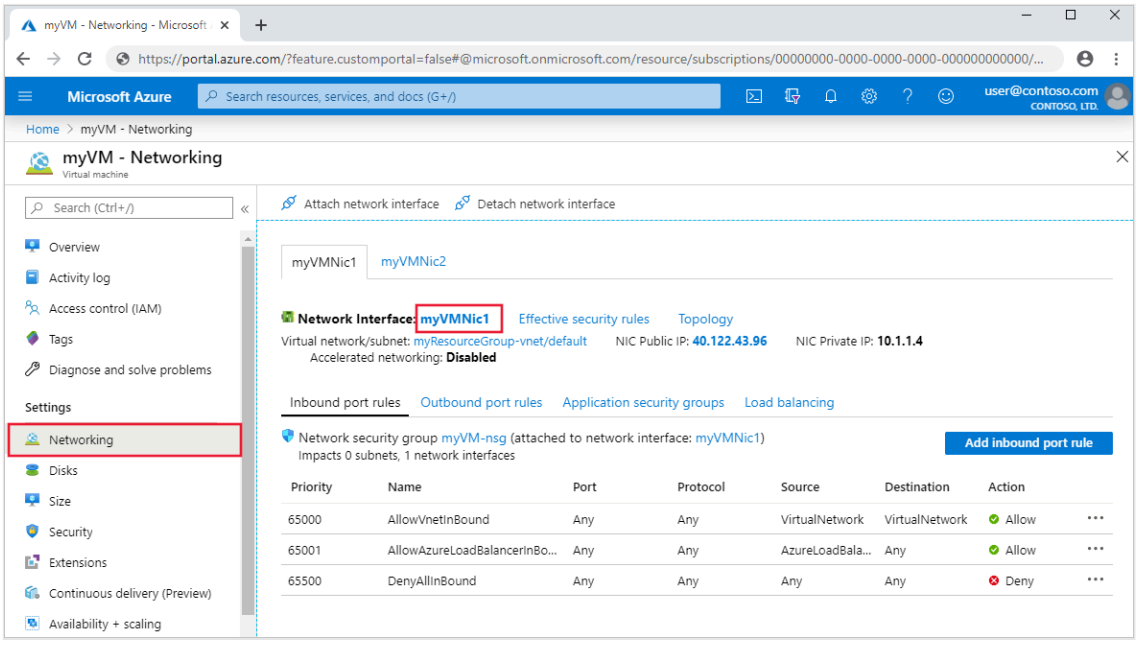
Validate the connection

Ensure connectivity between the Azure Virtual Network where the ExpressRoute terminates and the Azure VMware Solution private cloud.

1. Use a virtual machine within the Azure Virtual Network where the Azure VMware Solution ExpressRoute terminates. For more information, see Connect to Azure Virtual Network with ExpressRoute.

   a. Sign in to the Azure portal.

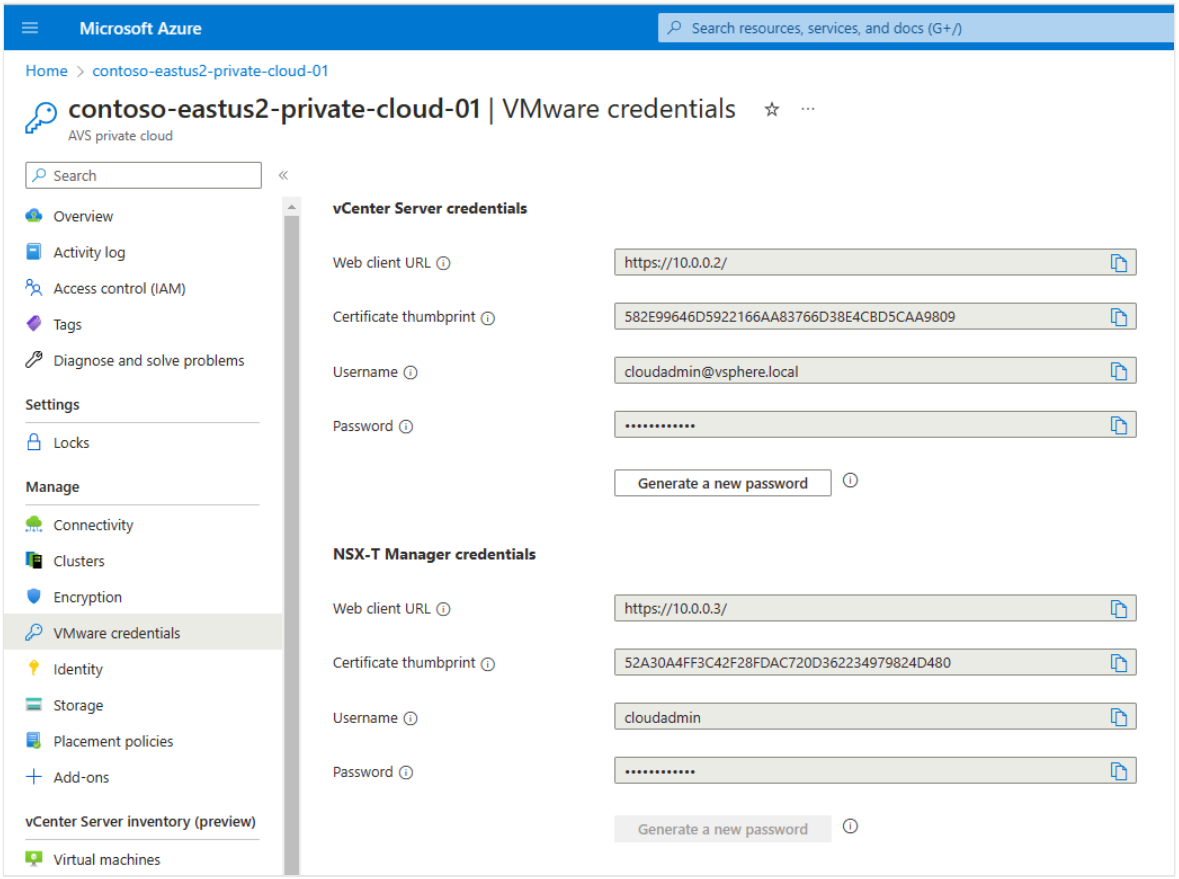
   b. Navigate to a running VM, and under **Settings**, select **Networking** and the network interface resource.



c. On the left, select **Effective routes**. A list of address prefixes that are contained within the `/22` CIDR block you entered during the deployment phase displays.

2. To sign in to both vCenter Server and NSX Manager, open a web browser and sign in to the same virtual machine used for network route validation.

   Find the vCenter Server and NSX Manager console's IP addresses and credentials in the Azure portal. Select your private cloud and then **Manage** > **VMware credentials**.



Next steps

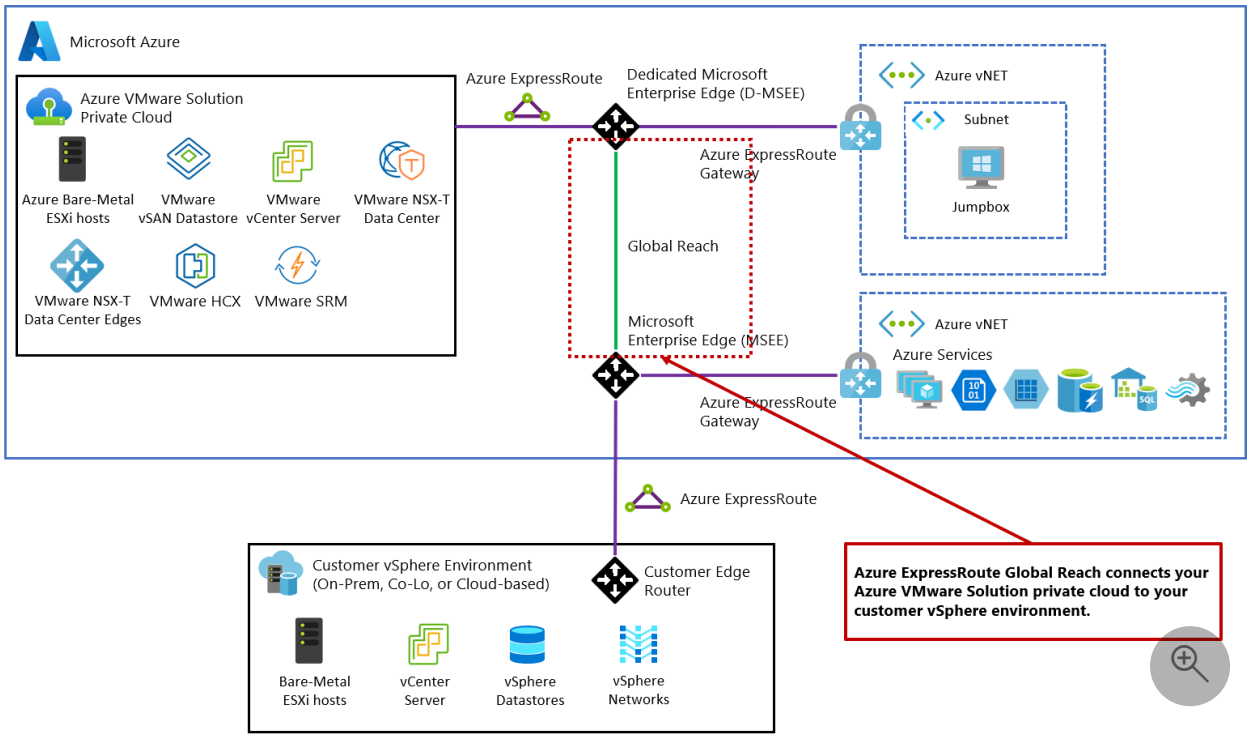
In the next tutorial, you'll connect Azure VMware Solution to your on-premises network through ExpressRoute.

Connect to your on-premises environment

Tutorial: Peer on-premises environments to Azure VMware Solution

Article • 12/20/2023

After you deploy your Azure VMware Solution private cloud, connect it to your on-premises environment. ExpressRoute Global Reach connects your on-premises environment to your Azure VMware Solution private cloud. The ExpressRoute Global Reach connection is established between the private cloud ExpressRoute circuit and an existing ExpressRoute connection to your on-premises environments.



> **Note**
>
> You can connect through VPN, but that's out of scope for this quick start guide.

In this article, you'll:

- ✓ Create an ExpressRoute auth key in the on-premises ExpressRoute circuit
- ✓ Peer the private cloud with your on-premises ExpressRoute circuit
- ✓ Verify on-premises network connectivity

Once you completed this section, follow the next steps provided at the end of this tutorial.

Prerequisites

- Review the documentation on how to enable connectivity in different Azure subscriptions.
- A separate, functioning ExpressRoute circuit for connecting on-premises environments to Azure, which is *circuit 1* for peering.
- Ensure that all gateways, including the ExpressRoute provider's service, support 4-byte Autonomous System Number (ASN). Azure VMware Solution uses 4-byte public ASNs for advertising routes.

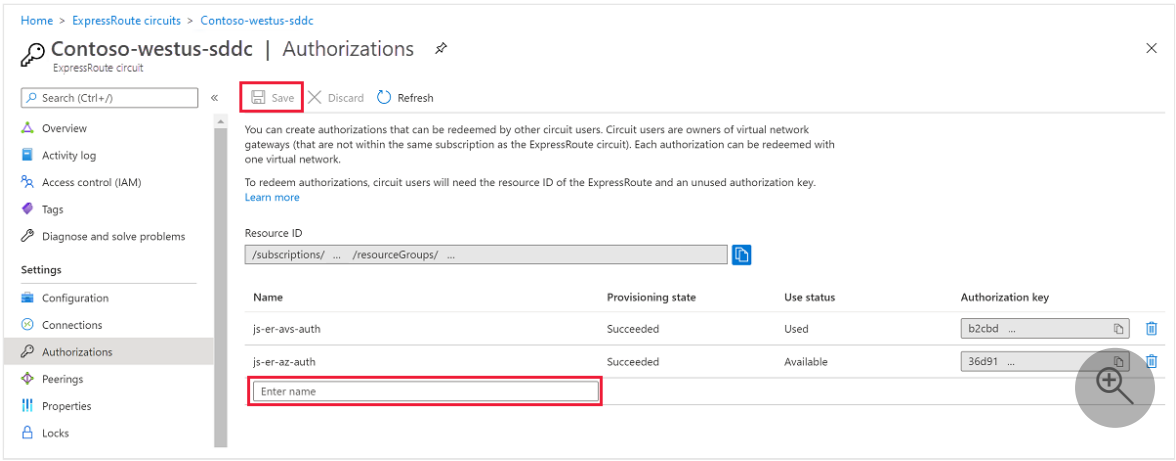
> **Note**
>
> If advertising a default route to Azure (0.0.0.0/0), ensure a more specific route containing your on-premises networks is advertised in addition to the default route to enable management access to Azure VMware Solution. A single 0.0.0.0/0 route will be discarded by Azure VMware Solution's management network to ensure successful operation of the service.

Create an ExpressRoute auth key in the on-premises ExpressRoute circuit

The circuit owner creates an authorization, which creates an authorization key to be used by a circuit user to connect their virtual network gateways to the ExpressRoute circuit. An authorization is valid for only one connection.

> **Note**
>
> Each connection requires a separate authorization.

1. From **ExpressRoute circuits** in the left navigation, under Settings, select **Authorizations**.
2. Enter the name for the authorization key and select **Save**.



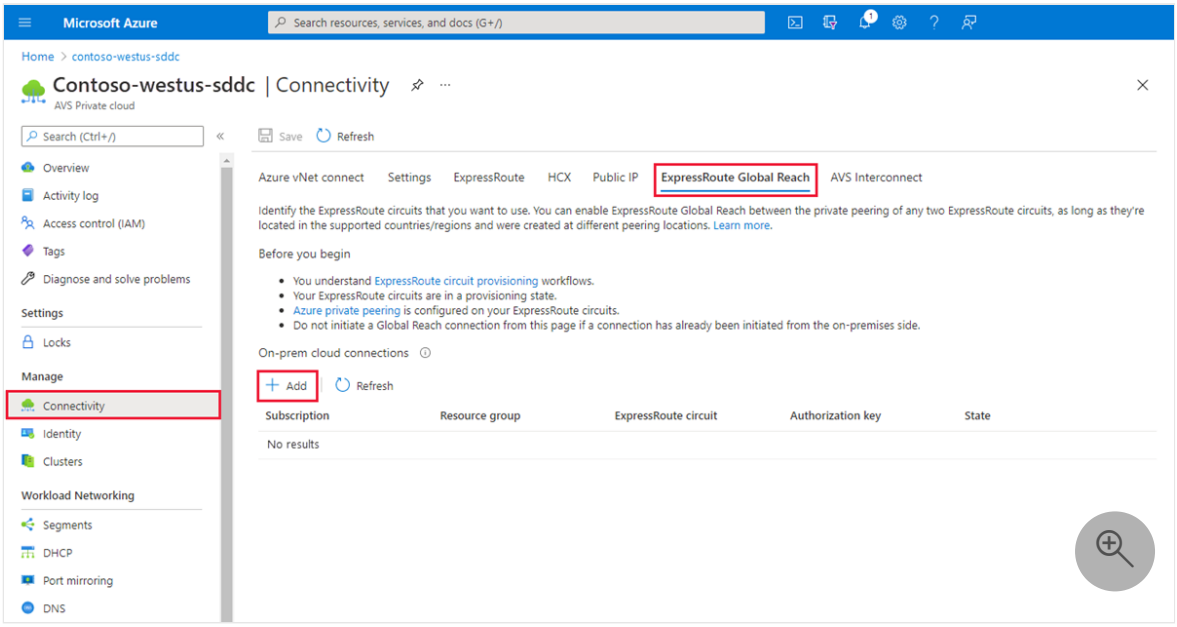
Once created, the new key appears in the list of authorization keys for the circuit.

3. Copy the authorization key and the ExpressRoute ID to use them in the next step to complete the peering.

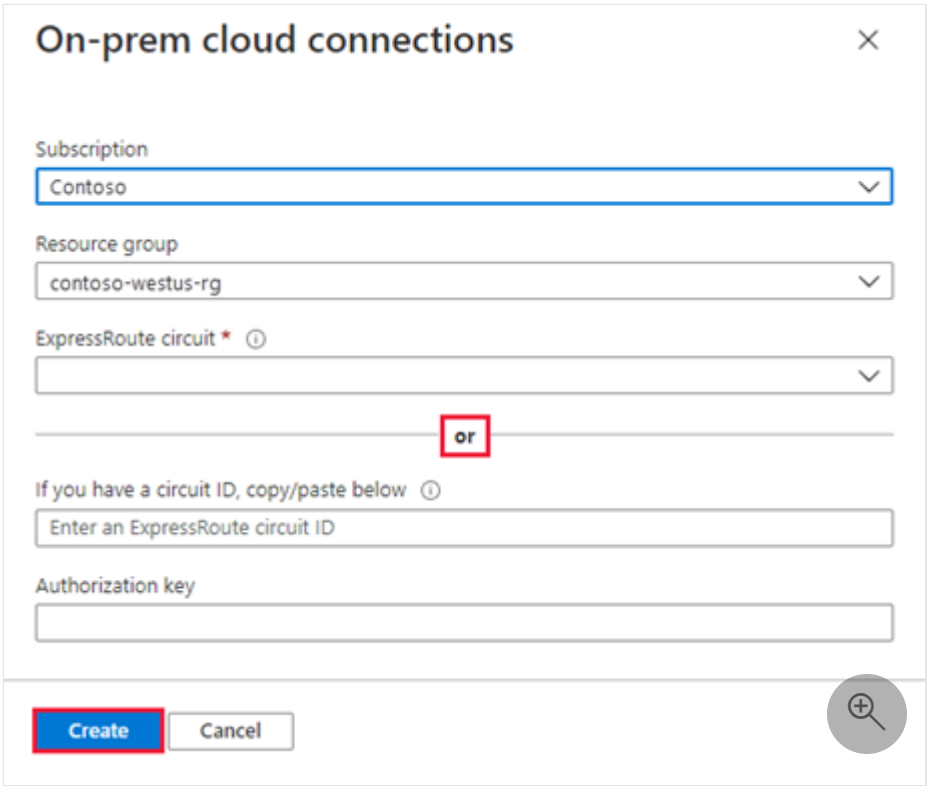
Peer private cloud to on-premises

Now that you created an authorization key for the private cloud ExpressRoute circuit, you can peer it with your on-premises ExpressRoute circuit. The peering is done from the on-premises ExpressRoute circuit in the **Azure portal**. You use the resource ID (ExpressRoute circuit ID) and authorization key of your private cloud ExpressRoute circuit to finish the peering.

1. From the private cloud, under Manage, select **Connectivity** > **ExpressRoute Global Reach** > **Add**.

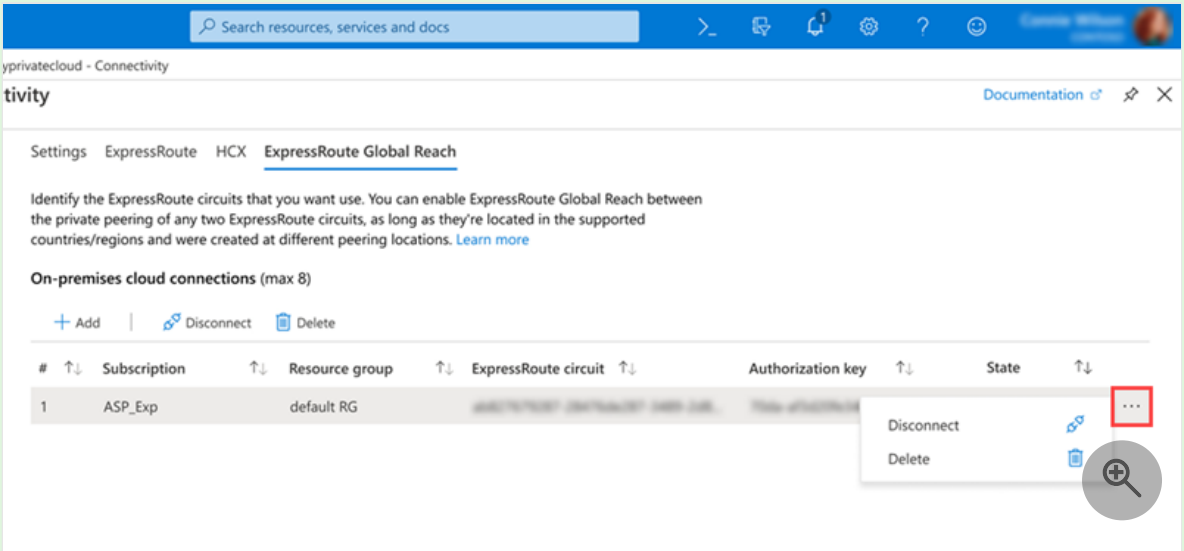


2. Enter the ExpressRoute ID and the authorization key created in the previous section.



3. Select **Create**. The new connection shows in the on-premises cloud connections list.

> **Tip**
>
> You can delete or disconnect a connection from the list by selecting **More**.



Verify on-premises network connectivity

In your **on-premises edge router**, you should now see where the ExpressRoute connects the NSX-T Data Center network segments and the Azure VMware Solution management segments.

> **Important**
>
> Everyone has a different environment, and some will need to allow these routes to propagate back into the on-premises network.

Next steps

Continue to the next tutorial to install VMware HCX add-on in your Azure VMware Solution private cloud.

Install VMware HCX

Install and activate VMware HCX in Azure VMware Solution

Article • 12/18/2023

VMware HCX is an application mobility platform designed for simplifying application migration, rebalancing workloads, and optimizing disaster recovery across data centers and clouds.

VMware HCX has two component services: **HCX Cloud Manager** and **HCX Connector**. These components work together for VMware HCX operations.

This article shows you how to install and activate the VMware HCX Cloud Manager and VMware HCX Connector components.

HCX Cloud manager is typically deployed as the destination (cloud side), but it can also be used as the source in cloud-to-cloud deployments. HCX Connector is deployed at the source (on-premises environment). A download link is provided for deploying HCX Connector appliance from within the HCX Cloud Manager.

This article also teaches you how to do the following tasks:

- Install VMware HCX Cloud through the Azure portal.
- Download and deploy the VMware HCX Connector in on-premises.
- Activate VMware HCX with a license key.

After HCX is deployed, follow the recommended Next steps.

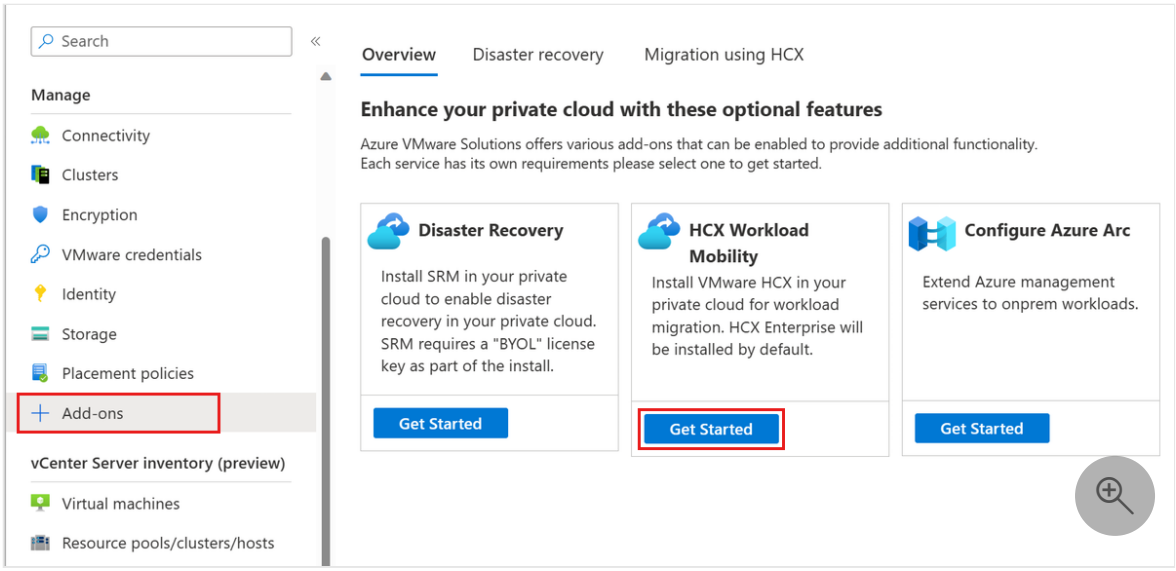
Prerequisite

- See Prepare for HCX installations

Install VMware HCX Cloud

1. In your Azure VMware Solution private cloud, select **Manage** > **Add-ons**.

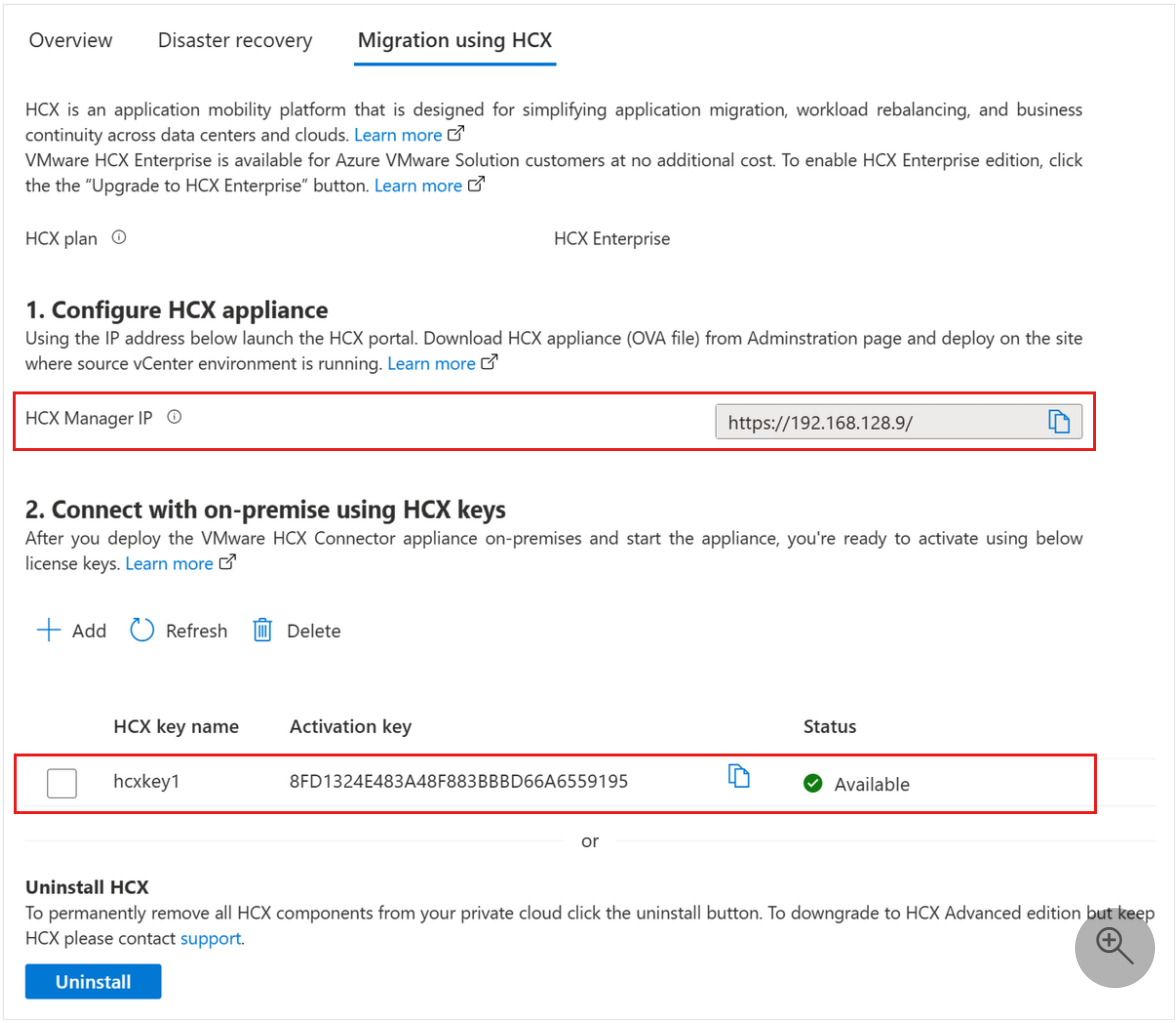
2. Select **Get started** for **HCX Workload Mobility**.



3. Select the **I agree with terms and conditions** checkbox and then select **Install**.

   Once installed, you should see the HCX Manager IP and the HCX keys required for the HCX on-premises connector site pairing on the **Migration using HCX** tab.

> **Important**
>
> If you don't see the HCX key after installing, click the **ADD** button to generate the key which you can then use for site pairing.



VMware HCX license edition

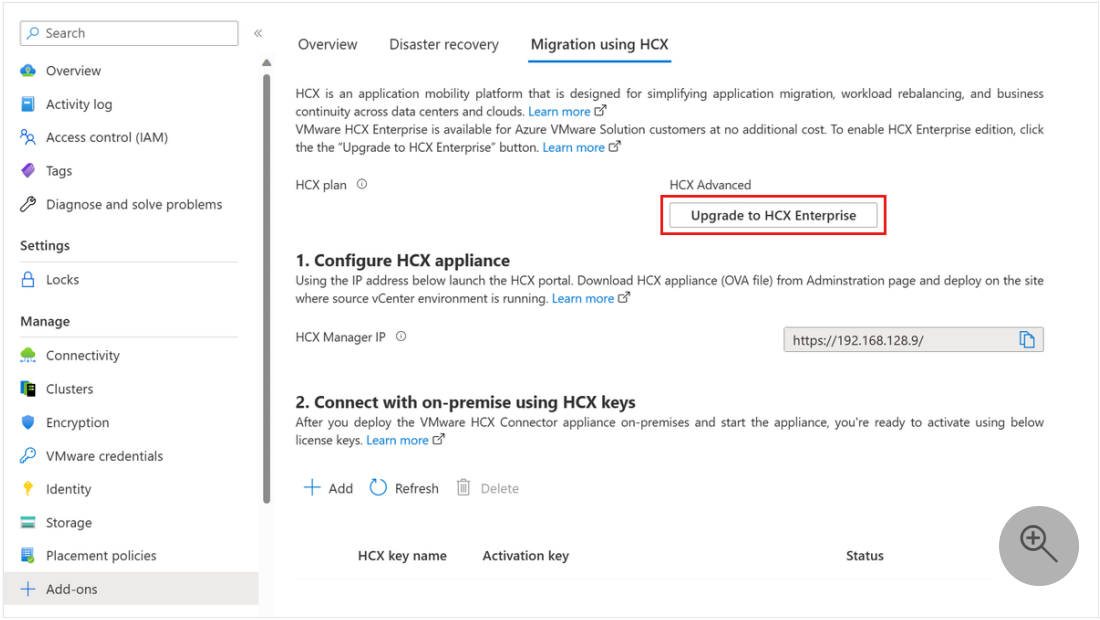
HCX offers various services based on the type of license installed with the system. Advanced delivers basic connectivity and mobility services to enable hybrid interconnect and migration services. HCX Enterprise offers more services than what standard licenses provide. Some of those services include; Mobility Groups, Replication assisted vMotion (RAV), Mobility Optimized Networking, Network Extension High availability, OS assisted Migration, and others.

> **Note**
>
> VMware HCX Enterprise is available for Azure VMware Solution customers at no additional cost.

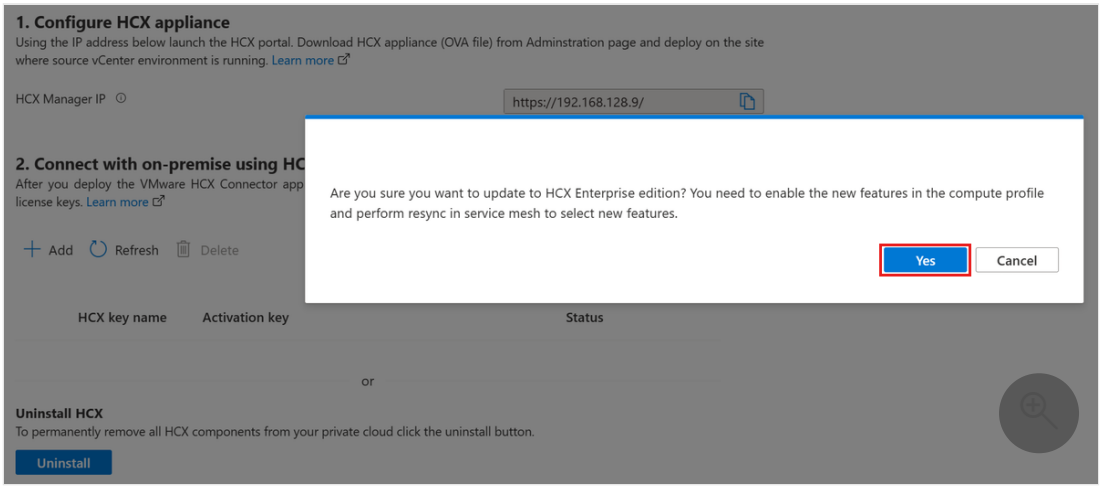
- HCX is now installed as Enterprise for all new HCX installations in Azure VMware solution.
- Existing HCX Advanced customers can upgrade to HCX Enterprise using the Azure portal. Use the following steps to upgrade to HCX Enterprise using Azure portal.

1. Under **Manage** in the left navigation, select **Add-ons**, then the **Migration using HCX** tab.

2. Select the **Upgrade to HCX Enterprise** button to enable HCX Enterprise edition.



3. Confirm the update to HCX Enterprise edition by selecting **Yes**.



> **ⓘ Important**
>
> If you upgraded VMware HCX from advanced to Enterprise, enable the new features in the compute profile and perform resync in service mesh to select a new feature like, Replication Assisted vMotion (RAV).

4. Change Compute profile after HCX upgrade to HCX Enterprise.
   a. On HCX UI, select **Infrastructure** > **Interconnect**, then select **Edit**.
   b. Select services you want activated like, Replication Assisted vMotion (RAV) and OS assisted Migration, which is available with VMware HCX Enterprise

only.

c. Select **Continue**, review the settings, then select **Finish** to create the Compute Profile.

5. If compute profile is being used in service mesh(es), resync service mesh.
   a. Go to **Interconnect** > **Service Mesh**.
   b. Select **Resync**, then verify that the changes appear in the Service Mesh configuration.

- Downgrading from HCX Enterprise Edition to HCX Advanced is possible without redeploying.

  1. Verify that you reverted to an HCX Advanced configuration state and you aren't using the Enterprise features.
  2. If you plan to downgrade, verify that no scheduled migrations, Enterprise services like RAV and HCX MON, etc. are in use. Open a support request to request downgrade.

Download and deploy the VMware HCX Connector on-premises

Use the following steps to download the VMware HCX Connector OVA file, and then deploy the VMware HCX Connector to your on-premises vCenter Server.

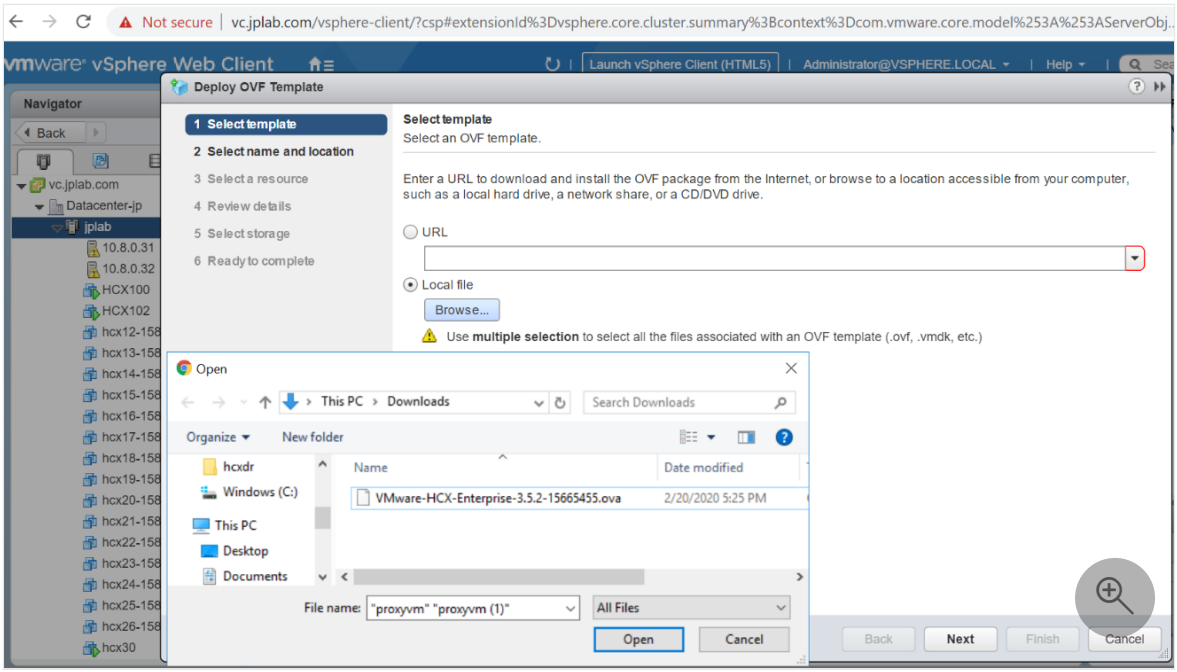
1. Open a browser window, sign in to the Azure VMware Solution HCX Manager on `https://x.x.x.9` port 443 with the **cloudadmin@vsphere.local** user credentials

2. Under **Administration** > **System Updates**, select **Request Download Link**. If the box is greyed, wait a few seconds for it to generate a link.

3. Either download or receive a link for the VMware HCX Connector OVA file you deploy on your local vCenter Server.

4. In your on-premises vCenter Server, select an OVF template to deploy the VMware HCX Connector to your on-premises vSphere cluster.

5. Navigate to and select the OVA file that you downloaded and then select **Open**.

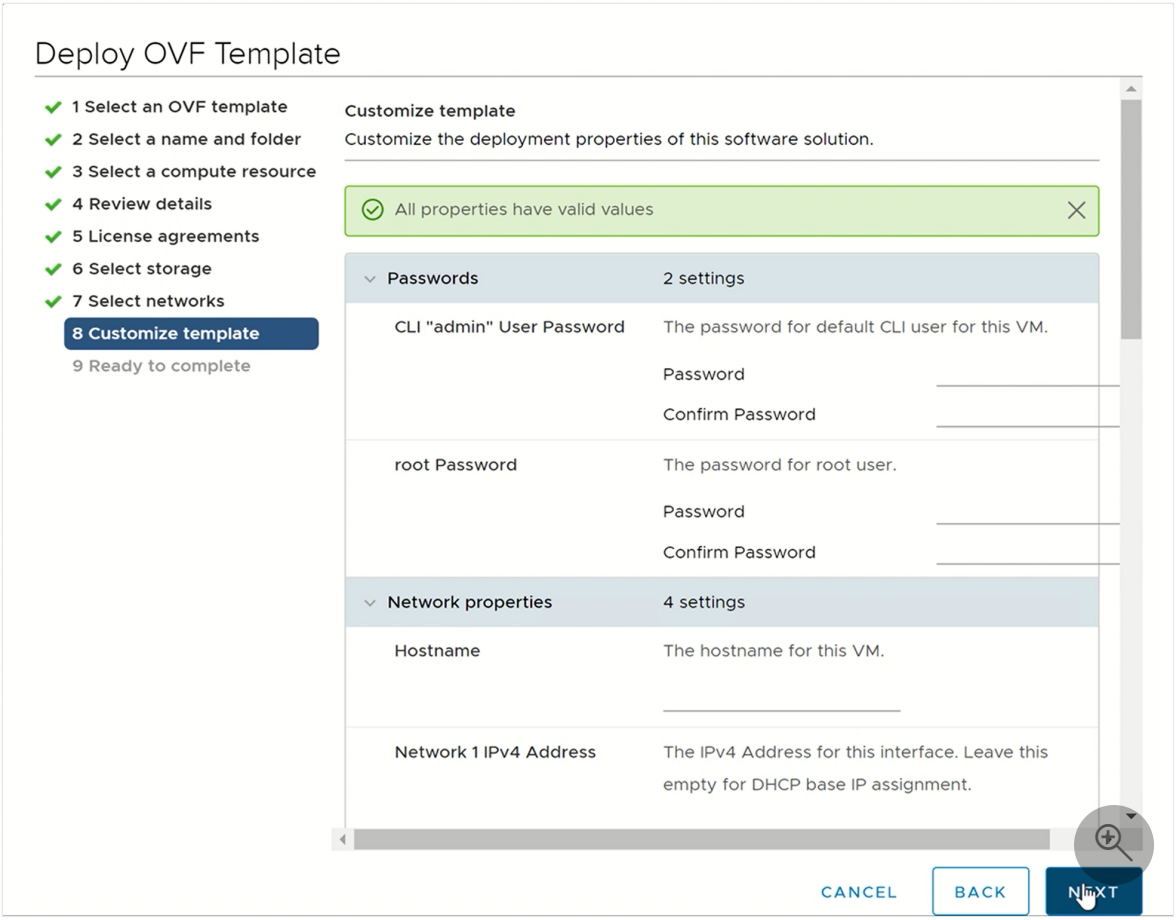


6. Select a name and location, and select a resource or cluster where you're deploying the VMware HCX Connector. Then review the details and required resources and select **Next**.

7. Review license terms, select the required storage and network, and then select **Next**.

8. Select the VMware HCX management network segment that you defined during the planning state. Then select **Next**.

9. In **Customize template**, enter all required information and then select **Next**.



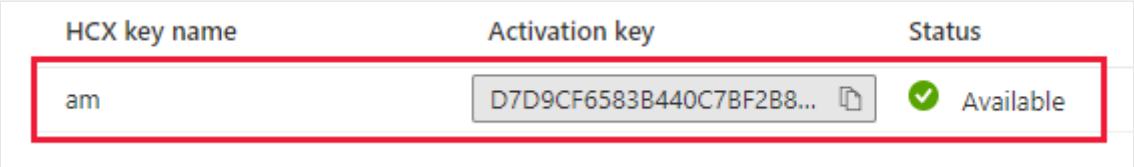
10. Verify and then select **Finish** to deploy the VMware HCX Connector OVA.

> **Important**
>
> You will need to turn on the virtual appliance manually. After powering on, wait 10-15 minutes before proceeding to the next step.

Activate VMware HCX

After deploying the VMware HCX Connector OVA on-premises and starting the appliance, you're ready to activate it. First, you need to get a license key from the Azure VMware Solution portal and activate it in VMware HCX Manager. Then you need a key for each on-premises HCX connector deployed.

1. In your Azure VMware Solution private cloud, select **Manage** > **Add-ons** > **Migration using HCX**. Then copy the **Activation key**.



2. Sign in to the on-premises VMware HCX Manager at `https://HCXManagerIP:9443` with the `admin` credentials. Make sure to include the `9443` port number with the VMware HCX Manager IP address.

   > **Tip**
   >
   > You defined the **admin** user password during the VMware HCX Manager OVA file deployment.

3. In **Licensing**, enter your key for **HCX Advanced Key** and select **Activate**.

   > **Important**
   >
   > VMware HCX Manager must have open internet access or a proxy configured.

4. In **Datacenter Location**, provide the nearest location for installing the VMware HCX Manager on-premises. Then select **Continue**.

5. In **System Name**, modify the name or accept the default and select **Continue**.

6. Select **Yes, Continue**.

7. In **Connect your vCenter**, provide the FQDN or IP address of your vCenter server and the appropriate credentials, and then select **Continue**.

   > **Tip**
   >
   > The vCenter Server is where you deployed the VMware HCX Connector in your datacenter.

8. In **Configure SSO/PSC**, provide your Platform Services Controller's FQDN or IP address, and select **Continue**.

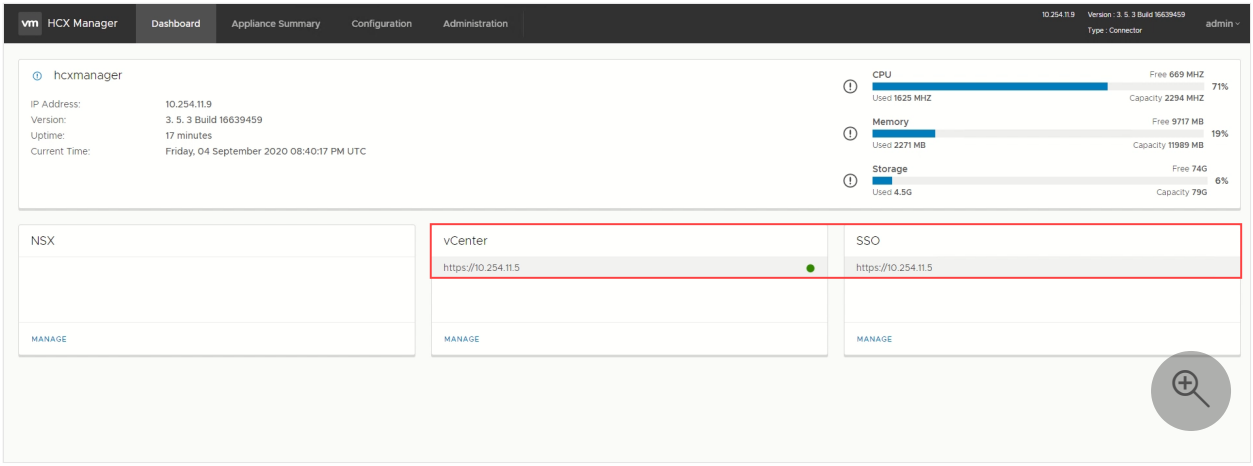
   > **Note**
   >
   > Typically, it's the same as your vCenter Server FQDN or IP address.

9. Verify that the information entered is correct and select **Restart**.

   > **Note**

> You'll experience a delay after restarting before being prompted for the next step.

After the services restart, you'll see vCenter Server displayed as green on the screen that appears. Both vCenter Server and SSO must have the appropriate configuration parameters, which should be the same as the previous screen.



Next steps

Continue to the next tutorial to configure the VMware HCX Connector. After you configured the VMware HCX Connector, you have a production-ready environment for creating virtual machines (VMs) and migration.

> Configure VMware HCX in Azure VMware Solution

> Understanding HCX Network Underlay Requirements

> VMware blog series - cloud migration

> Uninstall VMware HCX in Azure VMware Solution

Configure on-premises VMware HCX Connector

Article • 05/15/2024

After you install the VMware HCX add-on, configure the on-premises VMware HCX Connector for your Azure VMware Solution private cloud.

In this article, learn how to:

- ✓ Pair your on-premises VMware HCX Connector with your Azure VMware > Solution HCX Cloud Manager
- ✓ Configure the network profile, compute profile, and service mesh
- ✓ Check the appliance status and validate that migration is possible

After you complete these steps, you'll have a production-ready environment for creating virtual machines (VMs) and migration.

Prerequisites

- Install VMware HCX Connector.
- VMware HCX Enterprise is now available and supported on Azure VMware Solution at no extra cost. HCX Enterprise is automatically installed for all new HCX add-on requests, and existing HCX Advanced customers can upgrade to HCX Enterprise using the Azure portal.
- If you plan to enable VMware HCX MON, make sure you have:
  - VMware NSX or vSphere Distributed Switch (vDS) on-premises for HCX Network Extension (vSphere Standard Switch not supported).
  - One or more active stretched network segments.
- Meet the VMware software version requirements.
- Your on-premises vSphere environment (source environment) meets the minimum requirements.
- Azure ExpressRoute Global Reach is configured between on-premises and Azure VMware Solution private cloud ExpressRoute circuits.
- All required ports are open for communication between on-premises components and Azure VMware Solution private.

- Define VMware HCX network segments. The primary use cases for VMware HCX are workload migrations and disaster recovery.
- Review the VMware HCX Documentation for information on using HCX.

Add a site pairing

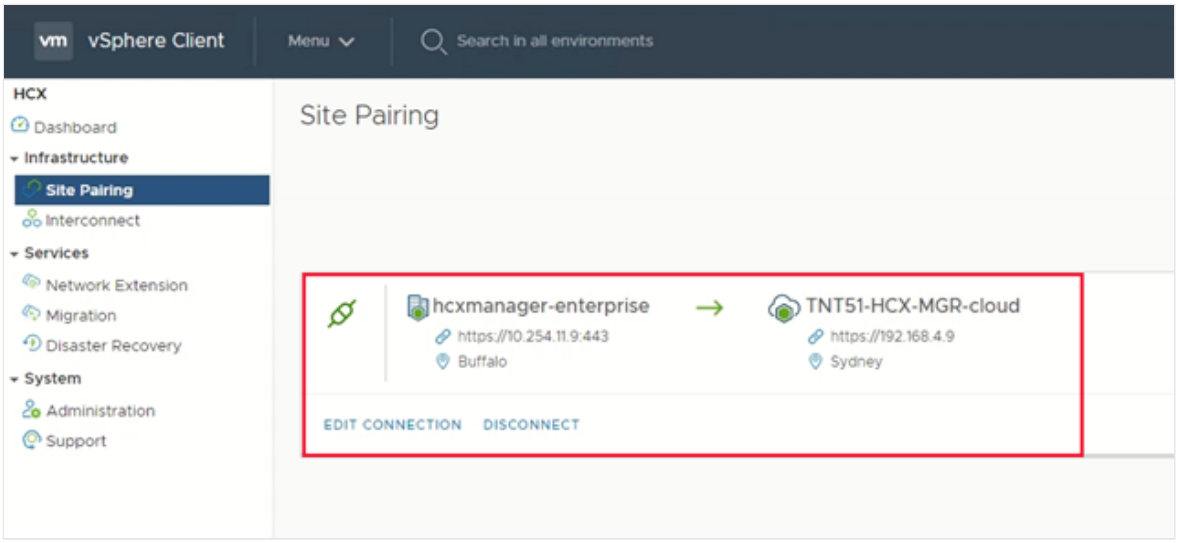
In your data center, connect or pair the VMware HCX Cloud Manager in Azure VMware Solution with the VMware HCX Connector.

> **Important**
>
> According to the Azure VMware Solution limits, a single HCX manager system can have a maximum of 25 site pairs and 10 service meshes, including inbound and outbound site pairings.

1. Sign in to your on-premises vCenter Server, and under **Home**, select **HCX**.
2. Under **Infrastructure**, select **Site Pairing** and choose the **Connect to Remote Site** option (in the middle of the screen).
3. Enter the Azure VMware Solution HCX Cloud Manager URL or IP address that you noted earlier `https://x.x.x.9` and the credentials for a user with the CloudAdmin role in your private cloud. Then select **Connect**.

   > **Note**
   >
   > To successfully establish a site pair:
   >
   > - Your VMware HCX Connector must be able to route to your HCX Cloud Manager IP over port 443.
   > - A service account from your external identity source, such as Active Directory, is recommended for site pairing connections. For more information about setting up separate accounts for connected services, see Access and identity architecture.

   A screen displays the connection (pairing) between your VMware HCX Cloud Manager in Azure VMware Solution and your on-premises VMware HCX Connector.



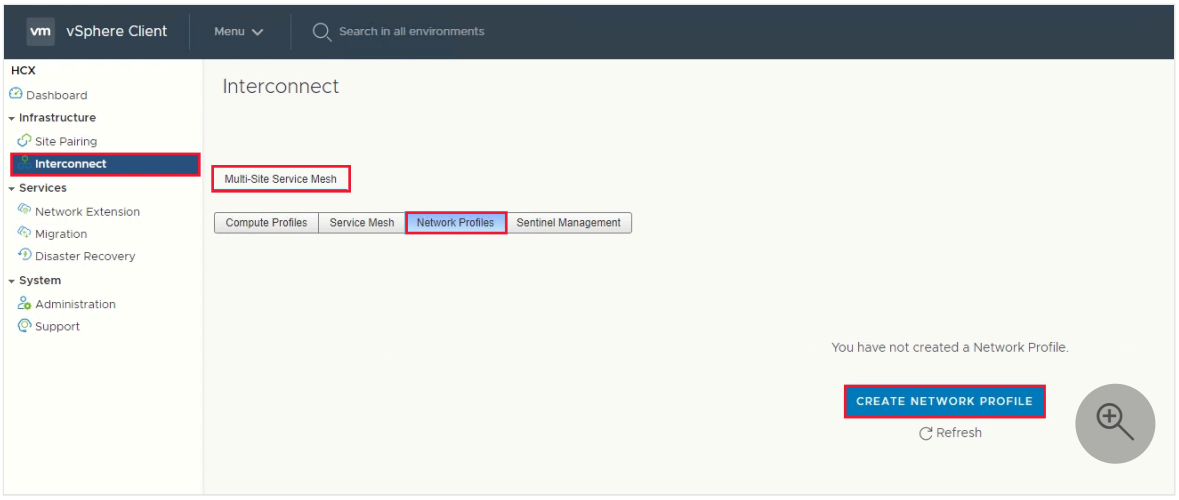
Create network profiles

VMware HCX Connector deploys a subset of virtual appliances (automated) that require multiple IP segments. Create your network profiles using the IP segments identified during the planning phase. Create four network profiles:

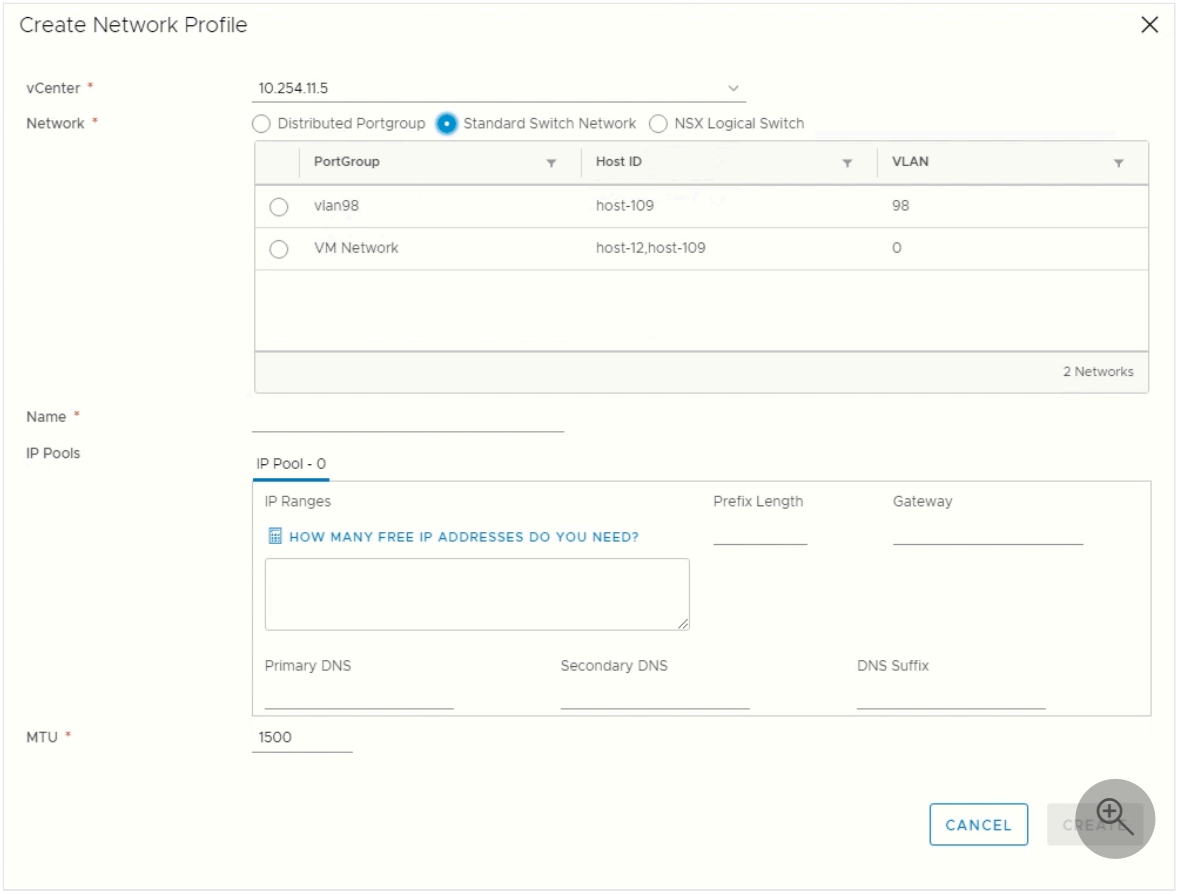
- Management
- vMotion
- Replication
- Uplink

> ⓘ **Note**
>
> - For Azure VMware Solution connected via VPN, set Uplink Network Profile MTU's to 1350 to account for IPSec overhead.
> - Azure VMware Solution defaults to 1500 MTU, which is sufficient for most ExpressRoute implementations.
>   - If your ExpressRoute provider does not support jumbo frames, you may need to lower the MTU in ExpressRoute setups as well.
>   - Adjust MTU settings on both HCX Connector (on-premises) and HCX Cloud Manager (Azure VMware Solution) network profiles.

1. Under **Infrastructure**, select **Interconnect** > **Multi-Site Service Mesh** > **Network Profiles** > **Create Network Profile**.



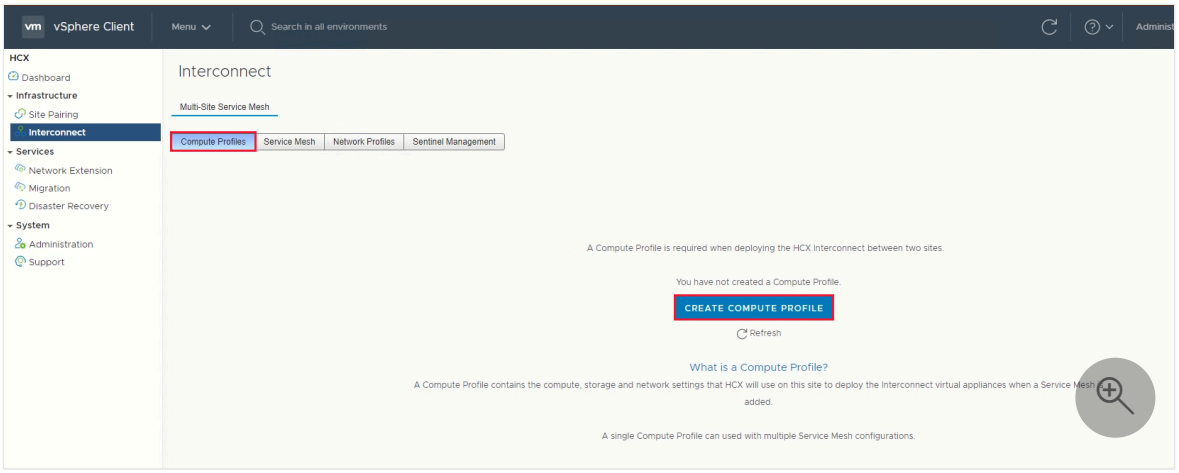
2. For each network profile, select the network and port group, provide a name, and create the segment's IP pool. Then select **Create**.



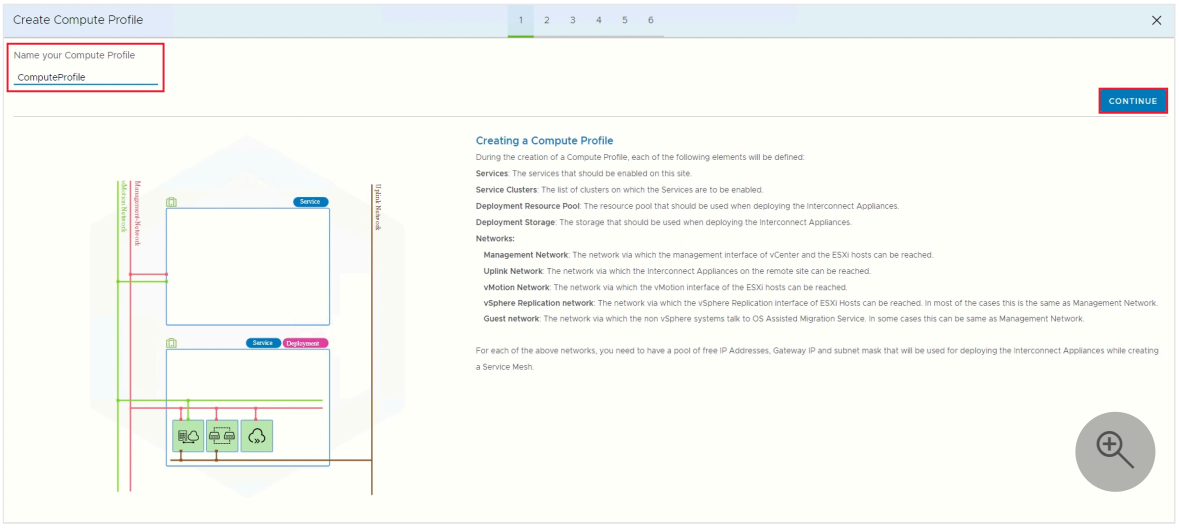
For an end-to-end overview of this procedure, watch the Azure VMware Solution: HCX Network Profile video.

Create a compute profile

1. Under **Infrastructure**, select **Interconnect** > **Compute Profiles** > **Create Compute Profile**.



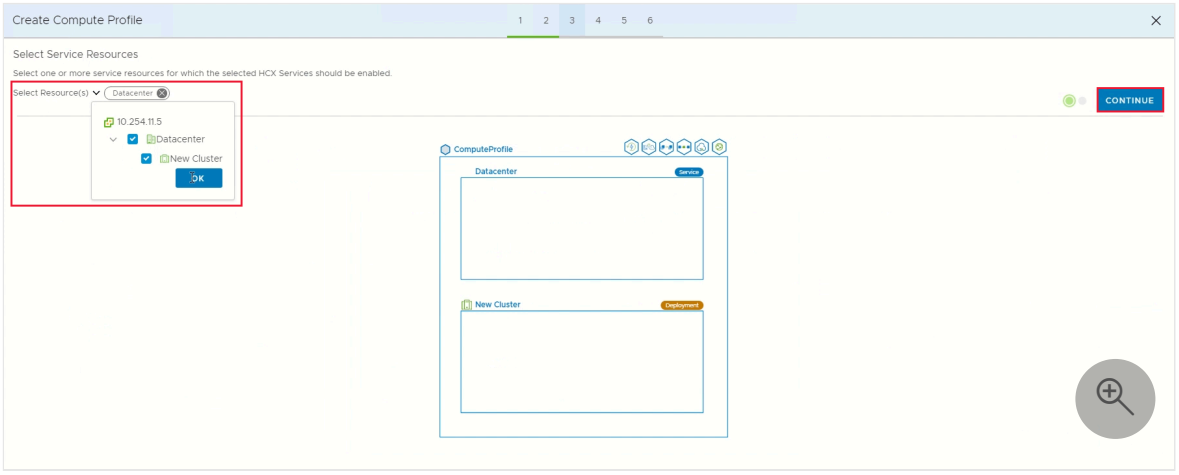
2. Enter a name for the profile and select **Continue**.



3. Select the services to enable, such as migration, network extension, or disaster recovery, and then select **Continue**.

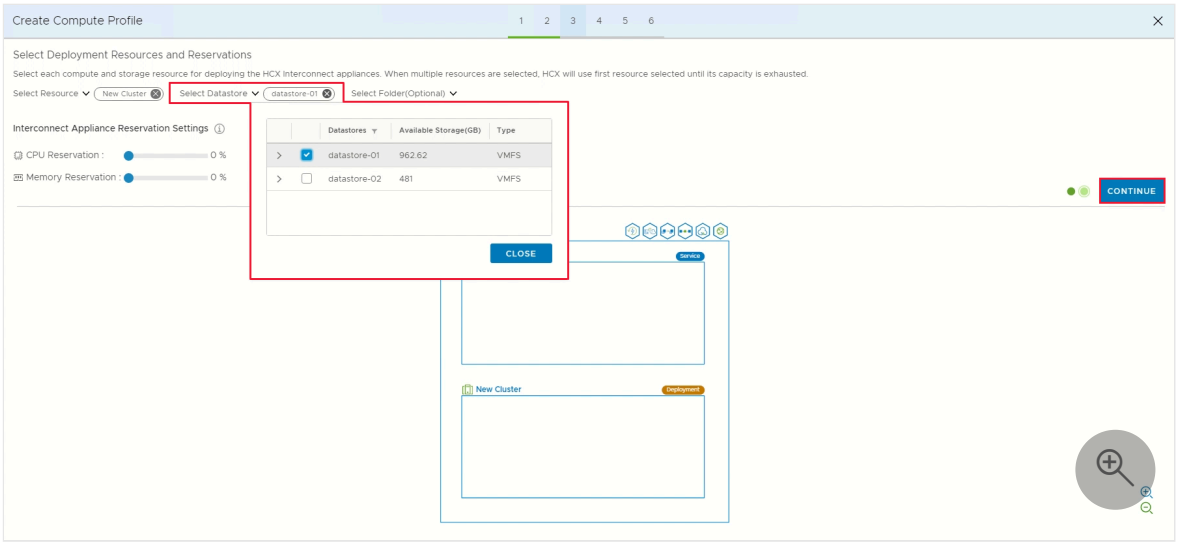
4. In **Select Service Resources**, select one or more service resources (clusters) to enable the selected VMware HCX services.

5. When you see the clusters in your on-premises datacenter, select **Continue**.

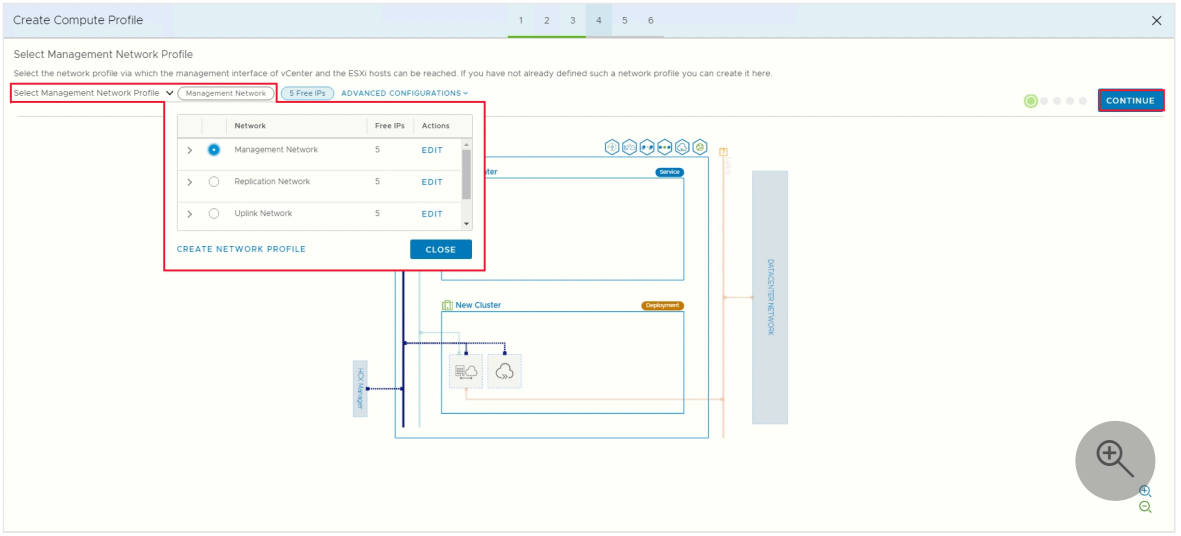


6. From **Select Datastore**, select the datastore storage resource for deploying the VMware HCX Interconnect appliances. Then select **Continue**.

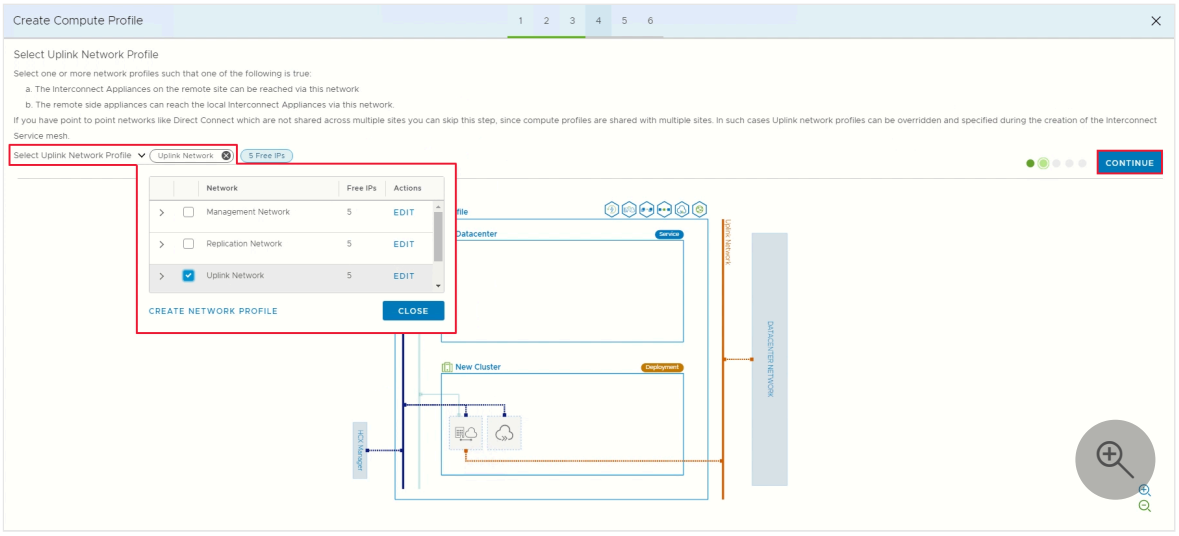
   When multiple resources are selected, VMware HCX uses the first resource selected until its capacity is exhausted.



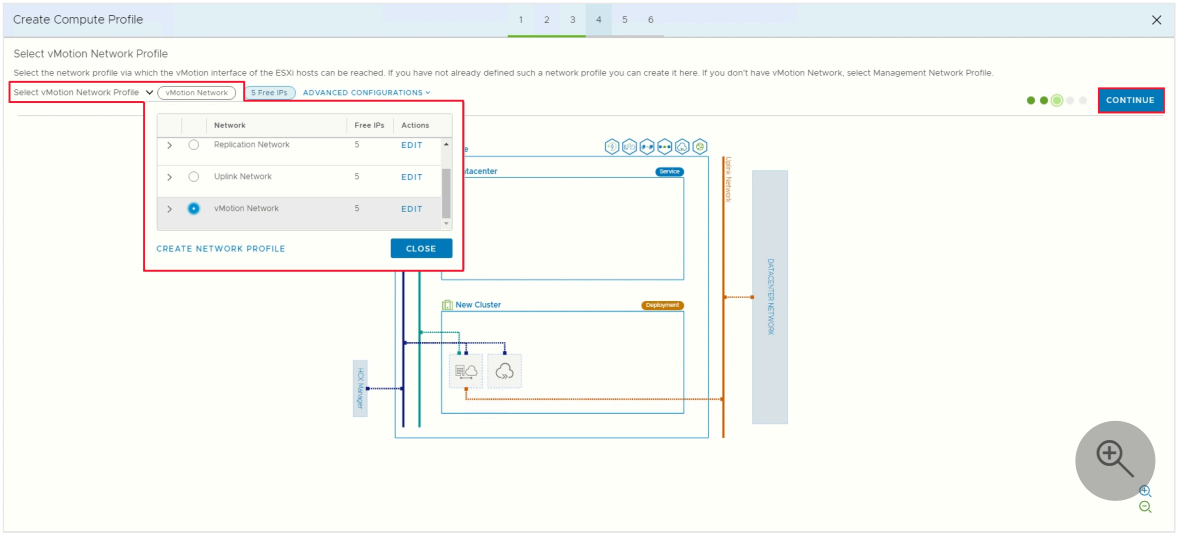
7. From **Select Management Network Profile**, select the management network profile that you created in previous steps. Then select **Continue**.



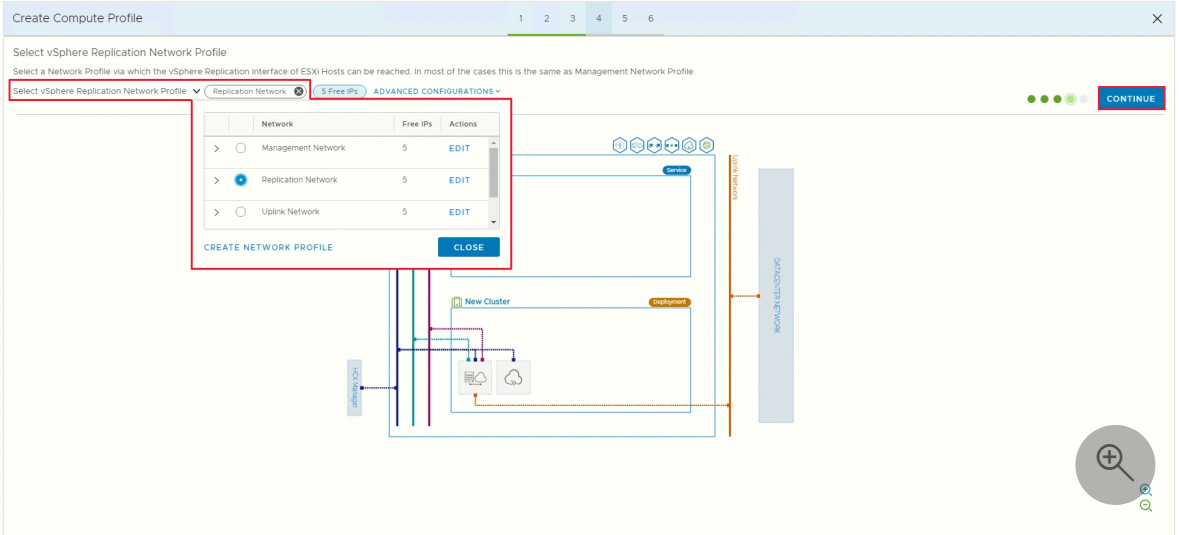
8. From **Select Uplink Network Profile**, select the uplink network profile you created in the previous procedure. Then select **Continue**.



9. From **Select vMotion Network Profile**, select the vMotion network profile that you created in previous steps. Then select **Continue**.



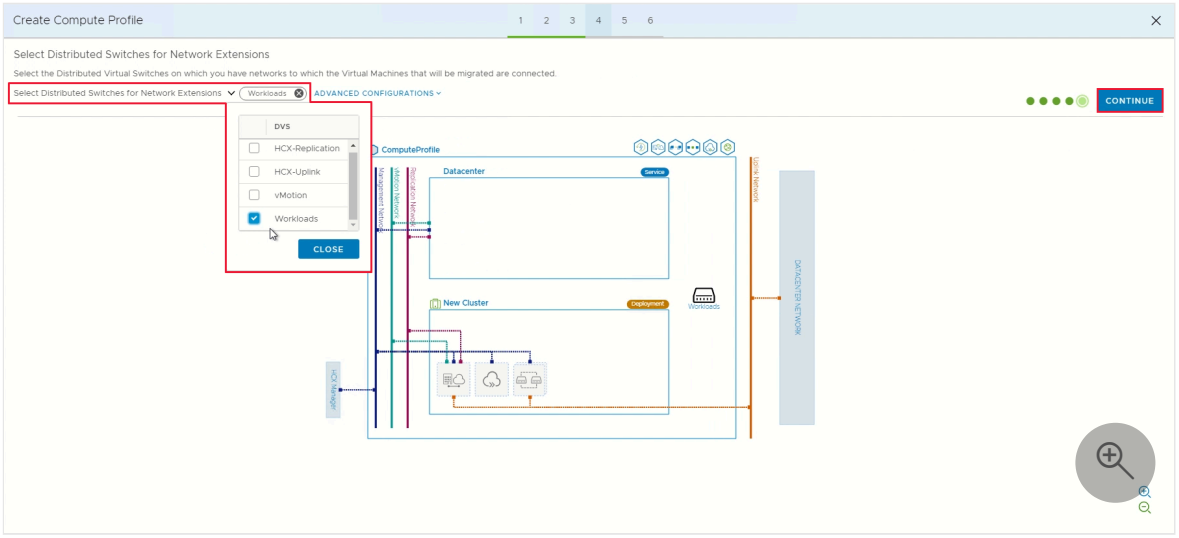
10. From **Select vSphere Replication Network Profile**, select the replication network profile that you created in previous steps. Then select **Continue**.



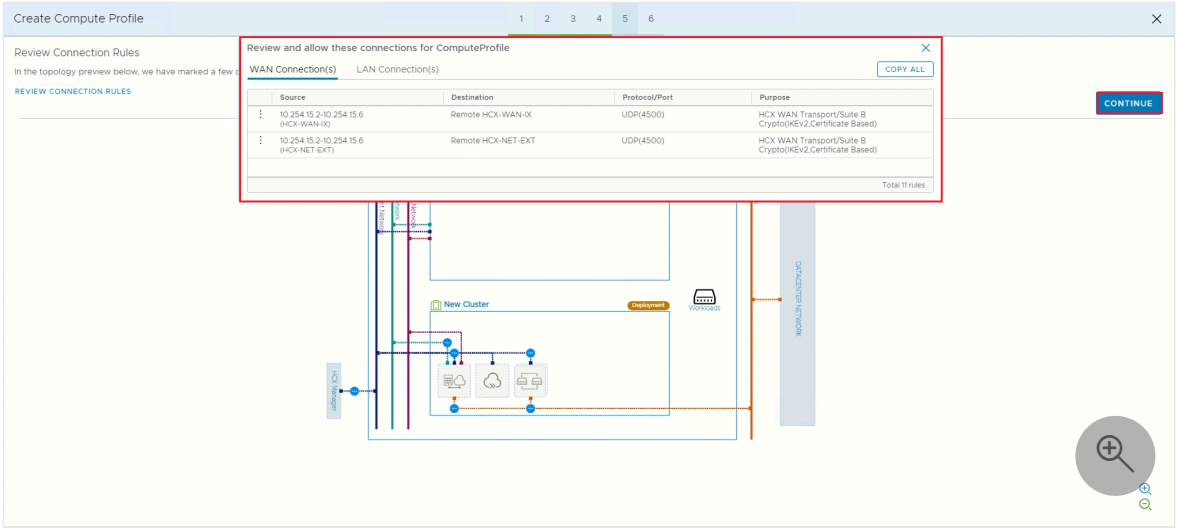
11. From **Select Distributed Switches for Network Extensions**, select the switches containing the virtual machines to be migrated to Azure VMware Solution on a

layer-2 extended network. Then select **Continue**.

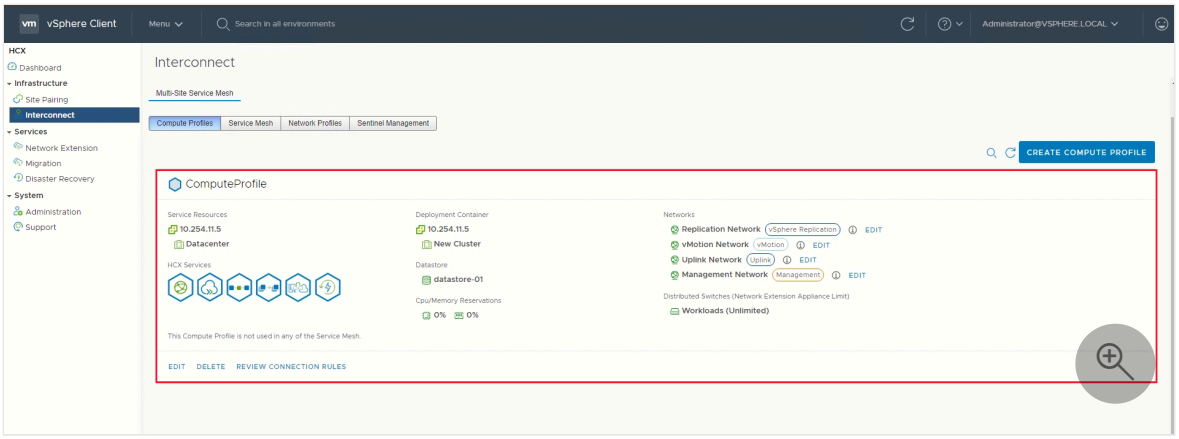
> **Note**
>
> If you're not migrating virtual machines on layer-2 (L2) extended networks, skip this step.



12. Review the connection rules and select **Continue**.



13. Select **Finish** to create the compute profile.

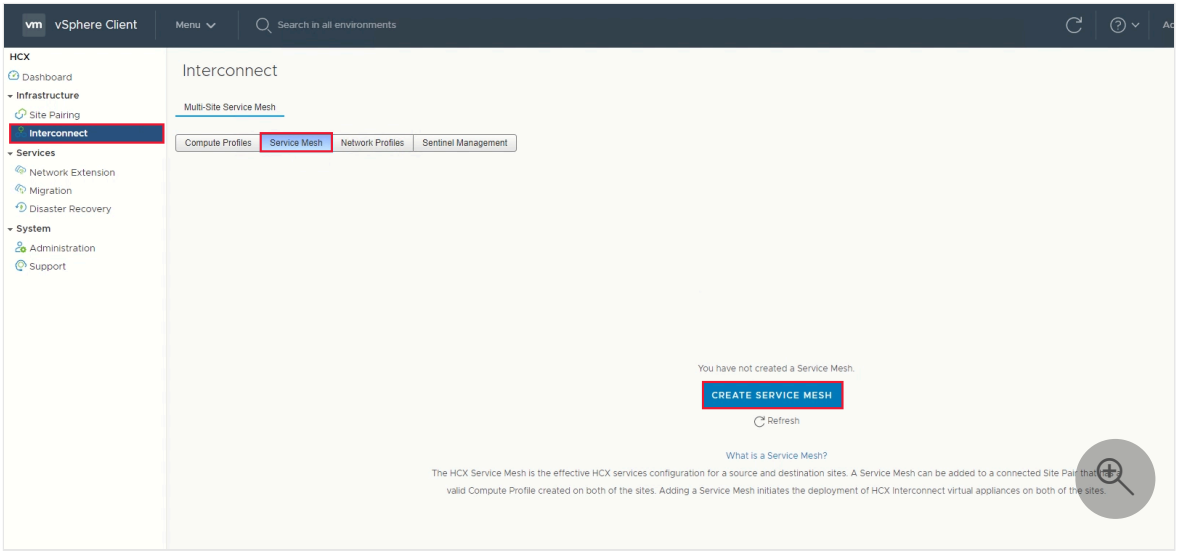


For an end-to-end overview of this procedure, view the Azure VMware Solution: Compute Profile video.

Create a service mesh

> **Important**
>
> Make sure port UDP 4500 is open between your on-premises VMware HCX Connector 'uplink' network profile addresses and the Azure VMware Solution HCX Cloud 'uplink' network profile addresses. (UDP 500 was required in legacy versions of HCX. See https://ports.vmware.com for the latest information.)

1. Under **Infrastructure**, select **Interconnect** > **Service Mesh** > **Create Service Mesh**.



2. Review the prepopulated sites, and then select **Continue**.

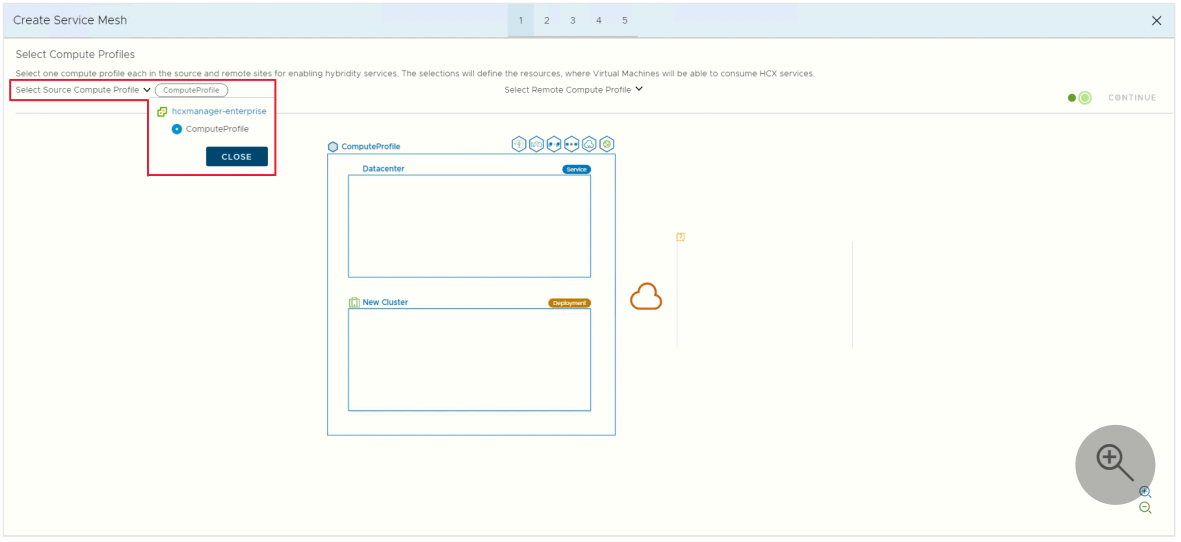
> **Note**

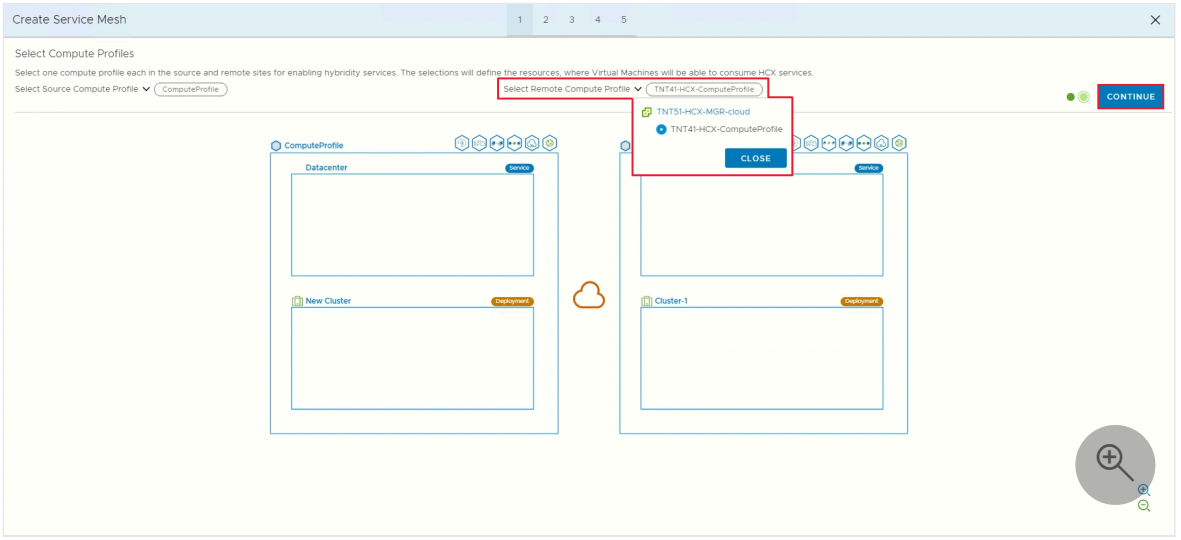
If this is your first service mesh configuration, you won't need to modify this screen.

3. Select the source and remote compute profiles from the drop-down lists, and then select **Continue**.

   The selections define the resources where VMs can consume VMware HCX services.

> **Note**
>
> In a mixed-mode SDDC with an AV64 cluster, deploying service mesh appliances on the AV64 cluster is not viable or supported. Nevertheless, this doesn't impede you from conducting HCX migration or network extension directly onto AV64 clusters. The deployment container can be cluster-1, hosting the HCX appliances.





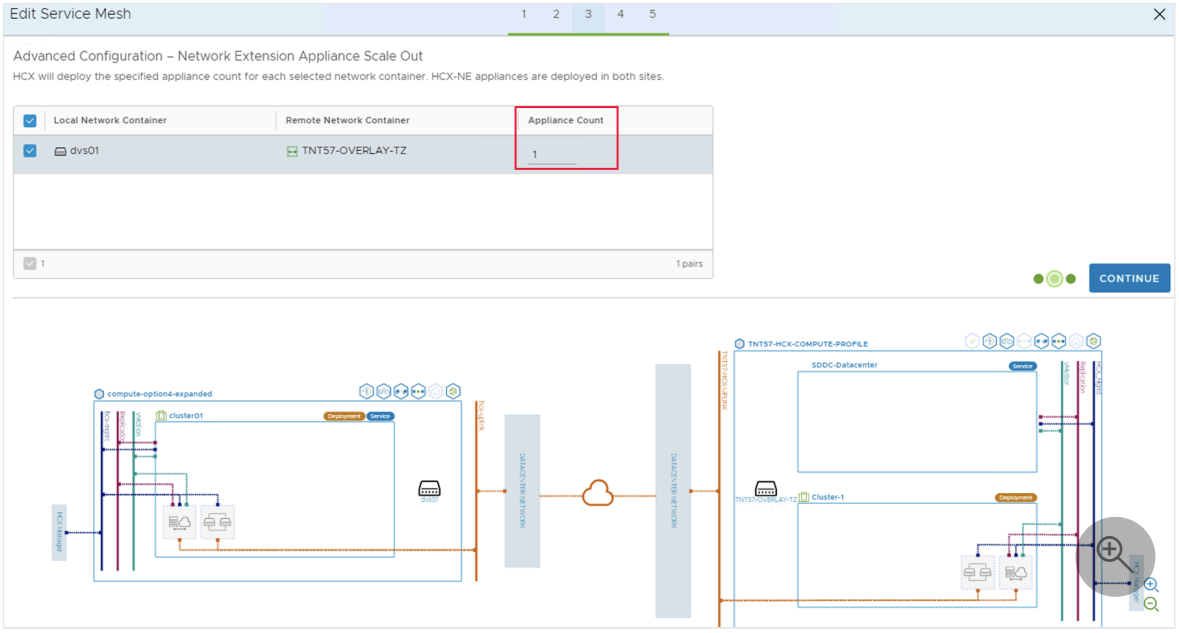
4. Review services to be enabled, and then select **Continue**.

5. In **Advanced Configuration - Override Uplink Network profiles**, select **Continue**.

   Uplink network profiles connect to the network through which the remote site's interconnect appliances can be reached.

6. In **Advanced Configuration - Network Extension Appliance Scale Out**, review and select **Continue**.

   You can have up to eight VLANs per appliance, but you can deploy another appliance to add another eight VLANs. You must also have IP space to account for the more appliances, and it's one IP per appliance. For more information, see VMware HCX Configuration Limits.

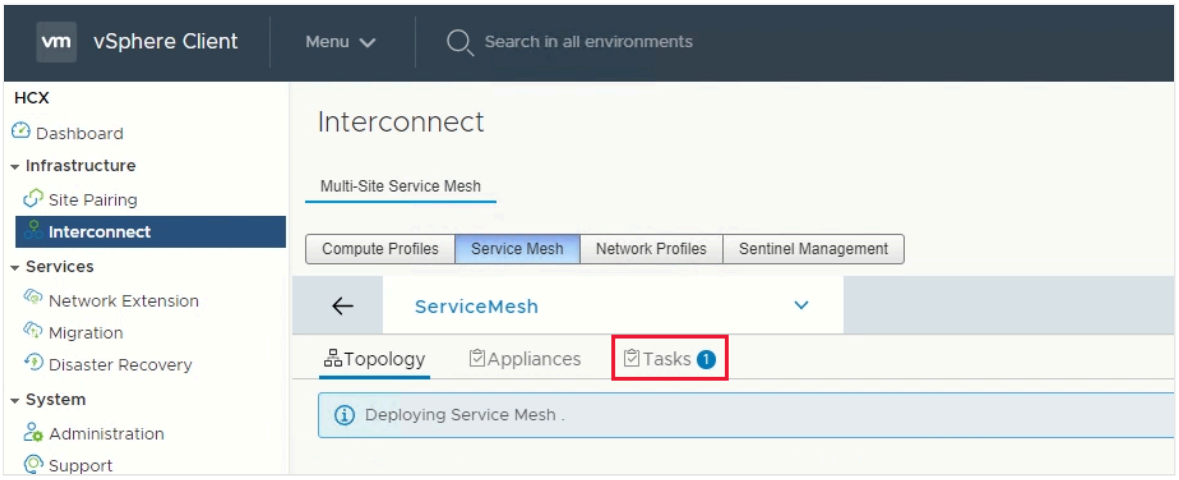


7. In **Advanced Configuration - Traffic Engineering**, review and make any modifications that you feel are necessary, and then select **Continue**.

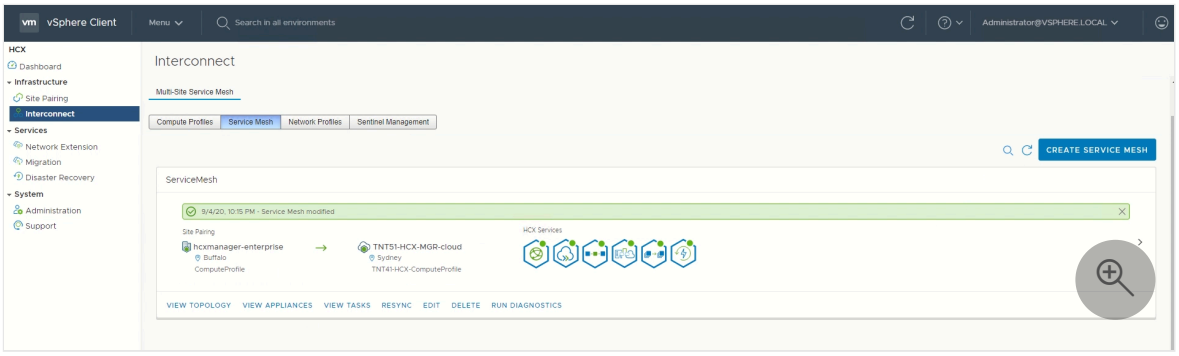
8. Review the topology preview and select **Continue**.

9. Enter a user-friendly name for this service mesh and select **Finish** to complete.

10. Select **View Tasks** to monitor the deployment.

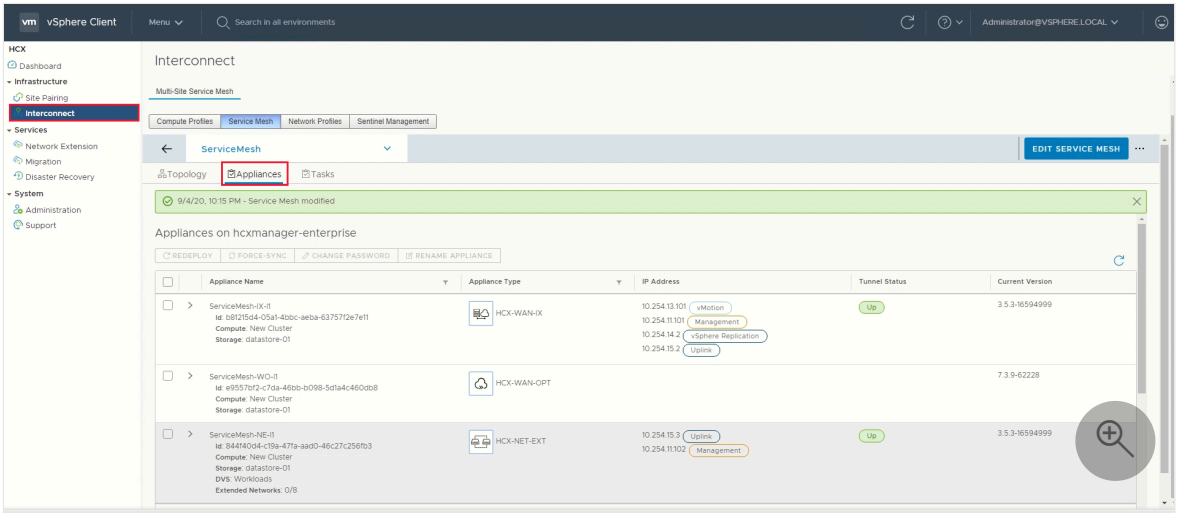


When the service mesh deployment finishes successfully, the services show as green.

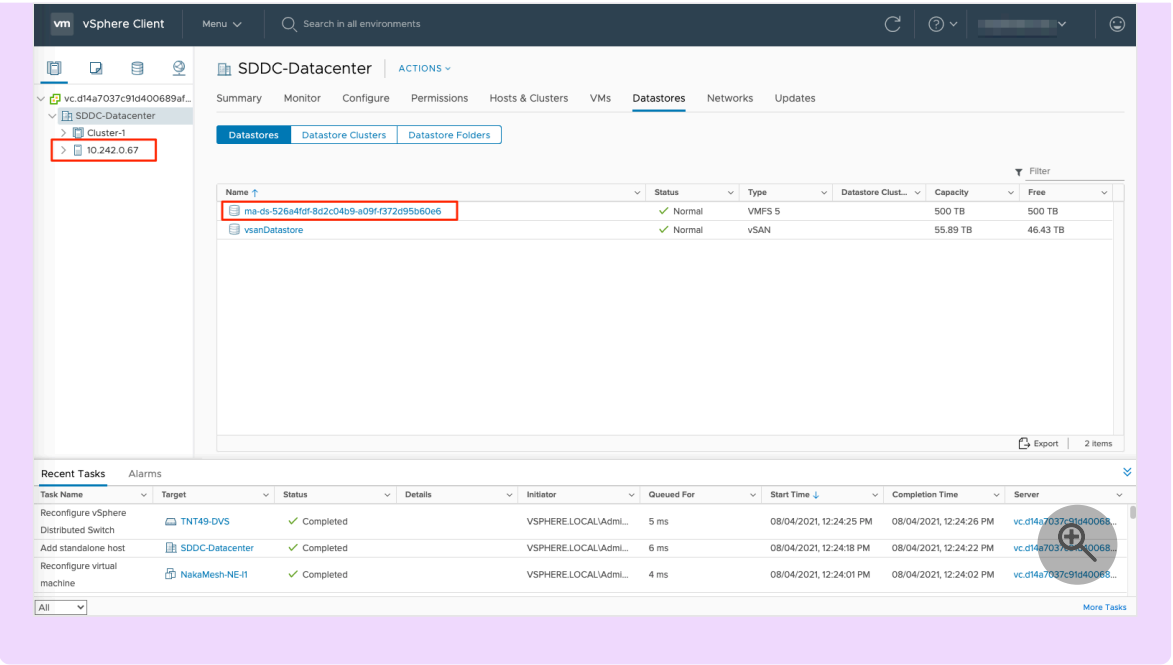


11. Verify the service mesh's health by checking the appliance status.

12. Select **Interconnect** > **Appliances**.



> **Note**
>
> After establishing the service mesh, you may notice a new datastore and a new host in your private cloud. This is normal behavior after establishing a service mesh.



The HCX interconnect tunnel status should display **UP** in green. Now you're ready to migrate and protect Azure VMware Solution VMs using VMware HCX. Azure VMware Solution supports workload migrations with or without a network extension that allow you to migrate workloads in your vSphere environment, create networks on-premises, and deploy VMs onto those networks. For more information, see the VMware HCX Documentation.

For an end-to-end overview of this procedure, watch the Azure VMware Solution: Service Mesh video.

Next steps

Now that you configured the HCX Connector, explore the following articles:

- Create an HCX network extension
- VMware HCX Mobility Optimized Networking (MON) guidance

Uninstall VMware HCX in Azure VMware Solution

Article • 12/20/2023

In this article, learn how to uninstall HCX in Azure VMware solution. You can uninstall HCX from the cloud side through the portal, which removes the existing pairing and software. Removing HCX returns the resources to your private cloud occupied by the HCX virtual appliances.

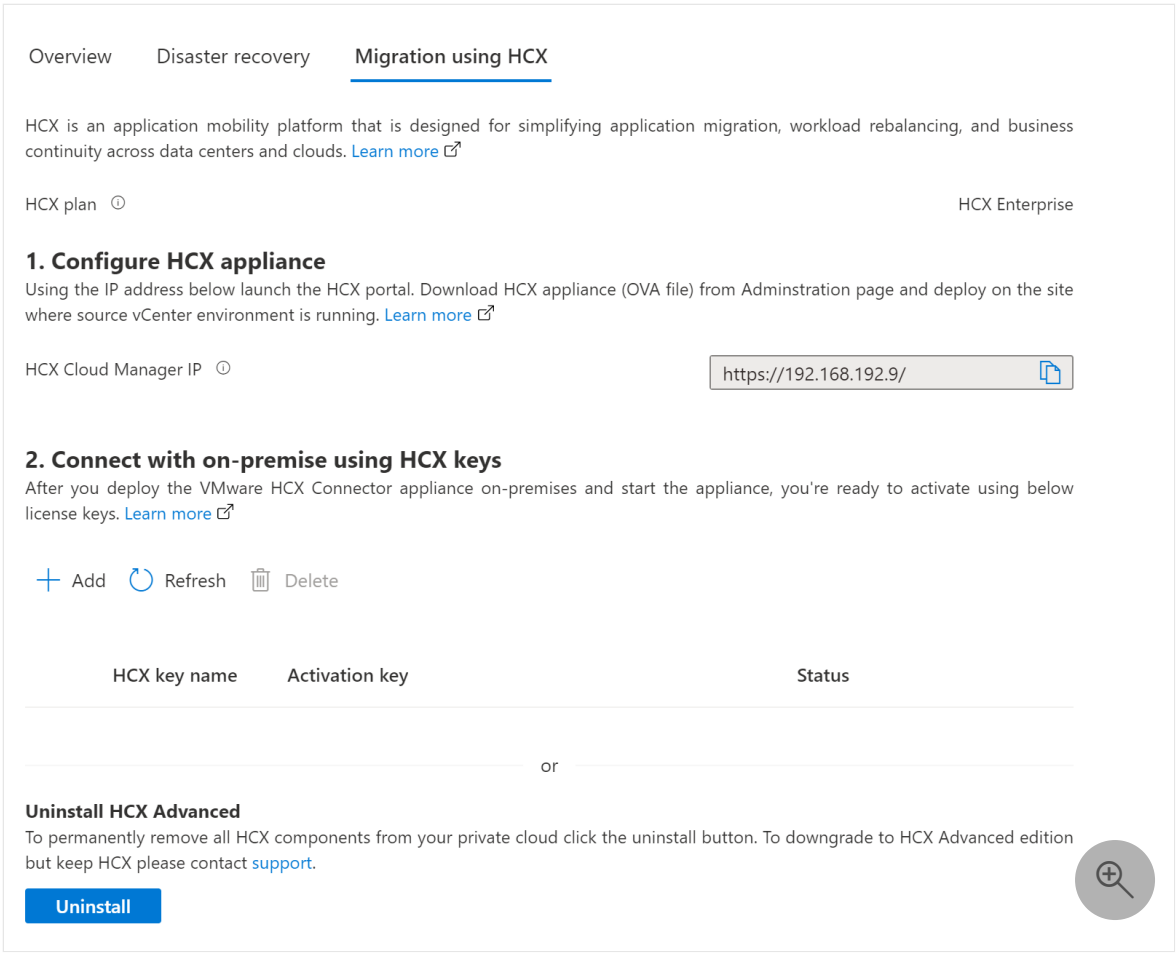
Generally, the workflow cleans up from the HCX on-premises side first, then clean up on the HCX Cloud side afterwards.

Prerequisites

- Make sure you don't have any active migrations in progress.
- Ensure that L2 extensions are no longer needed or the networks are `unstretched` to the destination.
- For workloads using MON, ensure that you removed the default gateways. Otherwise, it can result in workloads not being able to communicate or function.
- Uninstall HCX deployment from Connector on-premises.

Uninstall HCX

1. In your Azure VMware Solution private cloud, select **Manage** > **Add-ons**.
2. Select **Get started** for **HCX Workload Mobility**, then select **Uninstall**.
3. Enter **yes** to confirm the uninstall.



After you uninstall HCX, it no longer has the vCenter Server plugin. If necessary, you can reinstall it.

> Configure VMware HCX in Azure VMware Solution

> VMware blog series - cloud migration

> Install and activate VMware HCX in Azure VMware Solution

Networking planning checklist for Azure VMware Solution

Article • 05/15/2024

Azure VMware Solution provides a VMware private cloud environment accessible to users and applications from on-premises and Azure-based environments or resources. Connectivity is delivered through networking services such as Azure ExpressRoute and VPN connections. Specific network address ranges and firewall ports are required to enable these services. This article helps you configure your networking to work with Azure VMware Solution.

In this tutorial, learn about:

- ✓ Virtual network and ExpressRoute circuit considerations
- ✓ Routing and subnet requirements
- ✓ Required network ports to communicate with the services
- ✓ DHCP and DNS considerations in Azure VMware Solution

Prerequisites

Ensure all gateways, including the ExpressRoute provider's service, support 4-byte Autonomous System Number (ASN). Azure VMware Solution uses 4-byte public ASNs for advertising routes.

Virtual network and ExpressRoute circuit considerations

When you create a virtual network connection in your subscription, the ExpressRoute circuit is established through peering, using an authorization key and a peering ID you request in the Azure portal. The peering is a private, one-to-one connection between your private cloud and the virtual network.

> ⓘ **Note**
>
> The ExpressRoute circuit is not part of a private cloud deployment. The on-premises ExpressRoute circuit is beyond the scope of this document. If you require on-premises connectivity to your private cloud, use one of your existing ExpressRoute circuits or purchase one in the Azure portal.

When deploying a private cloud, you receive IP addresses for vCenter Server and NSX Manager. To access these management interfaces, create more resources in your subscription's virtual network. Find the procedures for creating those resources and establishing ExpressRoute private peering in the tutorials.

The private cloud logical networking includes a pre-provisioned NSX configuration. A Tier-0 gateway and Tier-1 gateway are pre-provisioned for you. You can create a segment and attach it to the existing Tier-1 gateway or attach it to a new Tier-1 gateway that you define. NSX logical networking components provide East-West connectivity between workloads and North-South connectivity to the internet and Azure services.

> **Important**
>
> If you plan to scale your Azure VMware Solution hosts using Azure NetApp Files datastores, deploying the vNet close to your hosts with an ExpressRoute virtual network gateway is crucial. The closer the storage is to your hosts, the better the performance.

Routing and subnet considerations

The Azure VMware Solution private cloud connects to your Azure virtual network using an Azure ExpressRoute connection. This high bandwidth, low latency connection allows you to access services running in your Azure subscription from your private cloud environment. The routing uses Border Gateway Protocol (BGP), is automatically provisioned, and enabled by default for each private cloud deployment.

Azure VMware Solution private clouds require a minimum `/22` CIDR network address block for subnets. This network complements your on-premises networks, so the address block shouldn't overlap with address blocks used in other virtual networks in your subscription and on-premises networks. Management, provisioning, and vMotion networks are provisioned automatically within this address block.

> **Note**
>
> Permitted ranges for your address block are the RFC 1918 private address spaces (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16), except for 172.17.0.0/16.

> **Important**
>
> Avoid using the following IP schemas reserved for NSX usage:

- 169.254.0.0/24 - used for internal transit network
- 169.254.2.0/23 - used for inter-VRF transit network
- 100.64.0.0/16 - used to connect T1 and T0 gateways internally

Example `/22` CIDR network address block: `10.10.0.0/22`

The subnets:

Expand table

Network usage	Description	Subnet	Example
Private cloud management	Management Network (such as vCenter, NSX)	`/26`	`10.10.0.0/26`
HCX Mgmt Migrations	Local connectivity for HCX appliances (downlinks)	`/26`	`10.10.0.64/26`
Global Reach Reserved	Outbound interface for ExpressRoute	`/26`	`10.10.0.128/26`
NSX DNS Service	Built-in NSX DNS Service	`/32`	`10.10.0.192/32`
Reserved	Reserved	`/32`	`10.10.0.193/32`
Reserved	Reserved	`/32`	`10.10.0.194/32`
Reserved	Reserved	`/32`	`10.10.0.195/32`
Reserved	Reserved	`/30`	`10.10.0.196/30`
Reserved	Reserved	`/29`	`10.10.0.200/29`
Reserved	Reserved	`/28`	`10.10.0.208/28`
ExpressRoute peering	ExpressRoute Peering	`/27`	`10.10.0.224/27`
ESXi Management	ESXi management VMkernel interfaces	`/25`	`10.10.1.0/25`
vMotion Network	vMotion VMkernel interfaces	`/25`	`10.10.1.128/25`
Replication Network	vSphere Replication interfaces	`/25`	`10.10.2.0/25`
vSAN	vSAN VMkernel interfaces and node communication	`/25`	`10.10.2.128/25`
HCX uplink	Uplinks for HCX IX and NE appliances to remote peers	`/26`	`10.10.3.0/26`
Reserved	Reserved	`/26`	`10.10.3.64/26`

Network usage	Description	Subnet	Example
Reserved	Reserved	`/26`	`10.10.3.128/26`
Reserved	Reserved	`/26`	`10.10.3.192/26`

Required network ports

Expand table

Source	Destination	Protocol	Port	Description
Private Cloud DNS server	On-premises DNS Server	UDP	53	DNS Client - Forward requests from Private Cloud vCenter Server for any on-premises DNS queries (see DNS section).
On-premises DNS Server	Private Cloud DNS server	UDP	53	DNS Client - Forward requests from on-premises services to Private Cloud DNS servers (see DNS section)
On-premises network	Private Cloud vCenter Server	TCP (HTTP)	80	vCenter Server requires port 80 for direct HTTP connections. Port 80 redirects requests to HTTPS port 443. This redirection helps if you use `http://server` instead of `https://server`.
Private Cloud management network	On-premises Active Directory	TCP	389/636	Enable Azure VMware Solutions vCenter Server to communicate with on-premises Active Directory/LDAP server(s). Optional for configuring on-premises AD as an identity source on the Private Cloud vCenter. Port 636 is

Source	Destination	Protocol	Port	Description
				recommended for security purposes.
Private Cloud management network	On-premises Active Directory Global Catalog	TCP	3268/3269	Enable Azure VMware Solutions vCenter Server to communicate with on-premises Active Directory/LDAP global catalog server(s). Optional for configuring on-premises AD as an identity source on the Private Cloud vCenter Server. Use port 3269 for security.
On-premises network	Private Cloud vCenter Server	TCP (HTTPS)	443	Access vCenter Server from an on-premises network. Default port for vCenter Server to listen for vSphere Client connections. To enable the vCenter Server system to receive data from the vSphere Client, open port 443 in the firewall. The vCenter Server system also uses port 443 to monitor data transfer from SDK clients.
On-premises network	HCX Cloud Manager	TCP (HTTPS)	9443	HCX Cloud Manager virtual appliance management interface for HCX system configuration.
On-premises Admin Network	HCX Cloud Manager	SSH	22	Administrator SSH access to HCX Cloud Manager virtual appliance.
HCX Manager	Interconnect (HCX-IX)	TCP (HTTPS)	8123	HCX Bulk Migration Control.

Source	Destination	Protocol	Port	Description
HCX Manager	Interconnect (HCX-IX), Network Extension (HCX-NE)	TCP (HTTPS)	9443	Send management instructions to the local HCX Interconnect using the REST API.
Interconnect (HCX-IX)	L2C	TCP (HTTPS)	443	Send management instructions from Interconnect to L2C when L2C uses the same path as the Interconnect.
HCX Manager, Interconnect (HCX-IX)	ESXi Hosts	TCP	80,443,902	Management and OVF deployment.
Interconnect (HCX-IX), Network Extension (HCX-NE) at Source	Interconnect (HCX-IX), Network Extension (HCX-NE) at Destination	UDP	4500	Required for IPSEC Internet key exchange (IKEv2) to encapsulate workloads for the bidirectional tunnel. Supports Network Address Translation-Traversal (NAT-T).
On-premises Interconnect (HCX-IX)	Cloud Interconnect (HCX-IX)	UDP	4500	Required for IPSEC Internet Key Exchange (ISAKMP) for the bidirectional tunnel.
On-premises vCenter Server network	Private Cloud management network	TCP	8000	vMotion of VMs from on-premises vCenter Server to Private Cloud vCenter Server
HCX Connector	connect.hcx.vmware.com hybridity.depot.vmware.com	TCP	443	`connect` is needed to validate license key. `hybridity` is needed for updates.

This table presents common firewall rules for typical scenarios. However, you might need to consider more items when configuring firewall rules. Note when the source and destination say "on-premises," this information is only relevant if your datacenter has a firewall that inspects flows. If your on-premises components don't have a firewall for inspection, you can ignore those rules.

For more information, see the full list of VMware HCX port requirements.

DHCP and DNS resolution considerations

Applications and workloads running in a private cloud environment require name resolution and DHCP services for lookup and IP address assignments. A proper DHCP and DNS infrastructure are required to provide these services. You can configure a virtual machine to provide these services in your private cloud environment.

Use the DHCP service built-in to NSX-T Data Center or use a local DHCP server in the private cloud instead of routing broadcast DHCP traffic over the WAN back to on-premises.

> **Important**
>
> If you advertise a default route to the Azure VMware Solution, then you must allow the DNS forwarder to reach the configured DNS servers and they must support public name resolution.

Next steps

In this tutorial, you learned about the considerations and requirements for deploying an Azure VMware Solution private cloud. Once you have the proper networking in place, continue to the next tutorial to create your Azure VMware Solution private cloud.

Create an Azure VMware Solution private cloud

Tutorial: Deploy an Azure VMware Solution private cloud

Article • 12/19/2023

The Azure VMware Solution private gives you the ability to deploy a vSphere cluster in Azure. For each private cloud created, there's one vSAN cluster by default. You can add, delete, and scale clusters. The minimum number of hosts per cluster is three. More hosts can be added one at a time, up to a maximum of 16 hosts per cluster. The maximum number of clusters per private cloud is 12. The initial deployment of Azure VMware Solution has three hosts.

You use vCenter Server and NSX-T Manager to manage most other aspects of cluster configuration or operation. All local storage of each host in a cluster is under the control of vSAN.

> **Tip**
>
> You can always extend the cluster and add more clusters later if you need to go beyond the initial deployment number.

Because Azure VMware Solution doesn't allow you to manage your private cloud with your cloud vCenter Server at launch, you need to do more steps for the configuration. This tutorial covers these steps and related prerequisites.

In this tutorial, learn how to:

- ✓ Create an Azure VMware Solution private cloud
- ✓ Verify the private cloud deployed

Prerequisites

- Appropriate administrative rights and permission to create a private cloud. You must be at minimum contributor level in the subscription.
- Follow the information you gathered in the planning tutorial to deploy Azure VMware Solution.
- Ensure you have the appropriate networking configured as described in the Network planning checklist.
- Hosts provisioned and the Microsoft.AVS resource provider is registered.

Create a private cloud

You can create an Azure VMware Solution private cloud using the Azure portal or the Azure CLI.

Portal

1. Sign in to the Azure portal.

   > **Note**
   >
   > If you need access to the Azure US Gov portal, go to **https://portal.azure.us/**

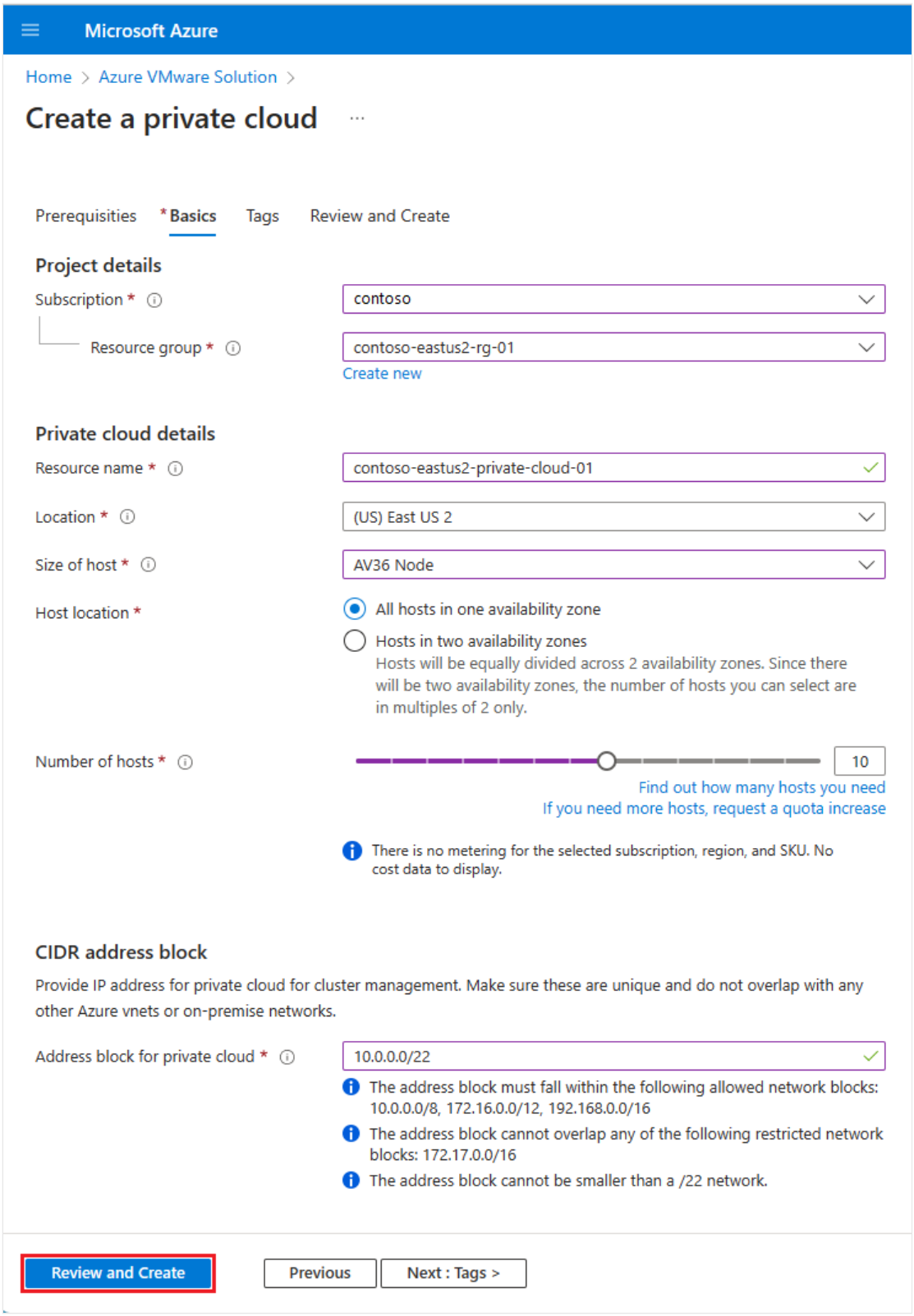
2. Select **Create a resource**.
3. In the **Search services and marketplace** text box, type `Azure VMware Solution` and select it from the search results.
4. On the **Azure VMware Solution** window, select **Create**.
5. If you need more hosts, request a host quota increase.
6. On the **Basics** tab, enter values for the fields and then select **Review + Create**.

   > **Tip**
   >
   > You gathered this information during the **planning phase** of this quick start.

Expand table

Field	Value
Subscription	Select the subscription you plan to use for the deployment. All resources in an Azure subscription are billed together.
Resource group	Select the resource group for your private cloud. An Azure resource group is a logical container into which Azure resources are deployed and managed. Alternatively, you can create a new resource group for your private cloud.
Resource name	Provide the name of your Azure VMware Solution private cloud.

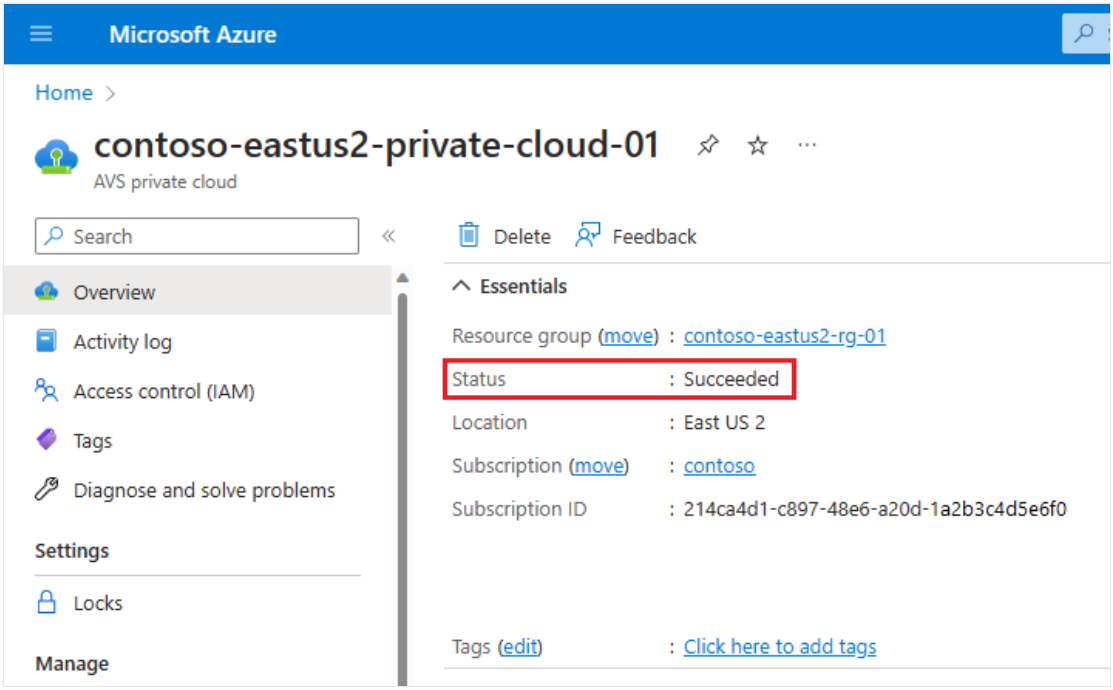
Field	Value
Location	Select a location, such as **(US) East US 2**. It's the *region* you defined during the planning phase.
Size of host	Select the **AV36**, **AV36P** or **AV52** SKU.
Host Location	Select **All hosts in one availability zone** for a standard private cloud or **Hosts in two availability zones** for stretched clusters.
Number of hosts	Number of hosts allocated for the private cloud cluster. The default value is 3, which you can increase or decrease after deployment. If these nodes are not listed as available, please contact support to request a quota increase. You can also click the link labeled **If you need more hosts, request a quota increase** in the Azure portal.
Address block for private cloud	Provide an IP address block for the private cloud. The CIDR represents the private cloud management network and is used for the cluster management services, such as vCenter Server and NSX-T Manager. Use /22 address space, for example, 10.175.0.0/22. The address should be unique and not overlap with other Azure Virtual Networks and with on-premises networks.



7. Verify the information entered, and if correct, select **Create**.

> **Note**
>
> This step takes roughly 3-4 hours. Adding a single host in an existing or the same cluster takes between 30 - 45 minutes.

8. Verify that the deployment was successful. Navigate to the resource group you created and select your private cloud. You'll see the status of **Succeeded** when the deployment has finished.



Next steps

In this tutorial, you learned how to:

- ✓ Create an Azure VMware Solution private cloud
- ✓ Verify the private cloud deployed
- ✓ Delete an Azure VMware Solution private cloud

Continue to the next tutorial to learn how to create a jump box. You use the jump box to connect to your environment to manage your private cloud locally.

Access an Azure VMware Solution private cloud

Tutorial: Configure networking for your VMware private cloud in Azure

Article • 06/21/2024

An Azure VMware Solution private cloud requires an Azure virtual network. Because Azure VMware Solution doesn't support an on-premises vCenter Server instance, you need to take extra steps to integrate with your on-premises environment. You also need to set up a virtual network gateway and an Azure ExpressRoute circuit.

If you plan to scale your Azure VMware Solution hosts by using Azure NetApp Files datastores, deploying the virtual network close to your hosts with an ExpressRoute virtual network gateway is crucial. The closer the storage is to your hosts, the better the performance.

In this tutorial, you learn how to:

- ✓ Create a virtual network.
- ✓ Create a virtual network gateway.
- ✓ Connect an ExpressRoute circuit to the gateway.

This tutorial assumes that you completed the previous tutorial about creating a private cloud.

> ⓘ **Note**
>
> Before you create a virtual network, evaluate whether you want to connect to Azure VMware Solution by using an existing virtual network or by creating a new one:
>
> - To use an existing virtual network in the same Azure subscription as Azure VMware Solution, use the **Azure VNet connect** tab on the **Connectivity** pane.
> - To use an existing virtual network in a different Azure subscription from Azure VMware Solution, use the guidance for **connecting to the private cloud manually**.
> - To create a new virtual network in the same Azure subscription as Azure VMware Solution, use the **Azure VNet connect** tab or create one **manually**.

Prerequisites

- Make sure that the virtual network that you use for this tutorial:

    - Contains a gateway subnet.
    - Is in the same region as the Azure VMware Solution private cloud.
    - Is in the same resource group as the Azure VMware Solution private cloud.
    - Contains an address space that doesn't overlap with CIDR in the Azure VMware Solution private cloud.

- Validate that your solution design is within the Azure VMware Solution limits.

Connect to the private cloud by using the Azure VNet connect feature

You can take advantage of the **Azure VNet connect** feature if you want to connect to Azure VMware Solution by using an existing virtual network or by creating a new virtual network.

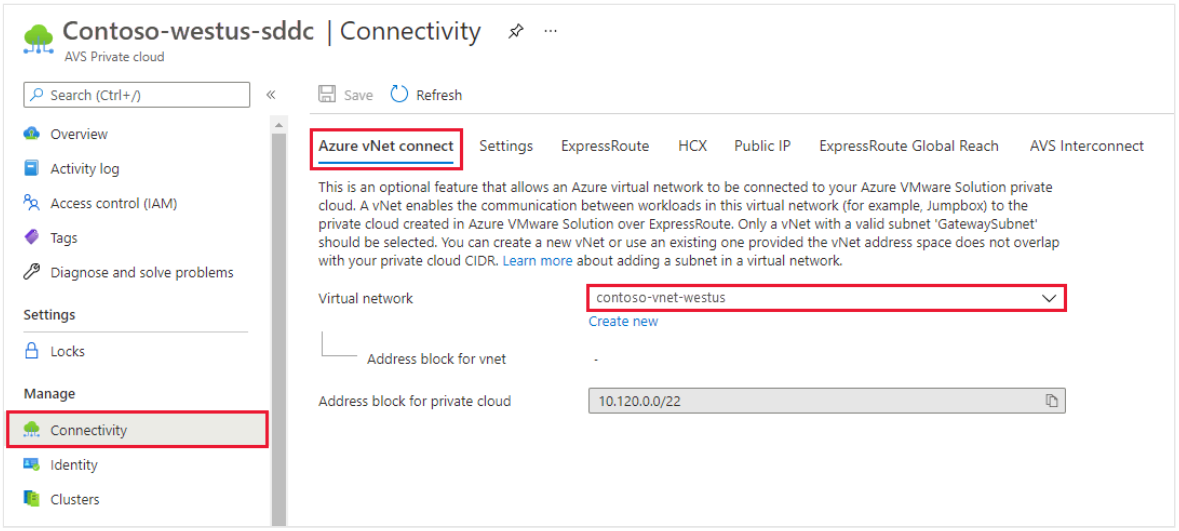
Azure VNet connect is a function to configure virtual network connectivity. It doesn't record configuration state. Browse through the Azure portal to check what settings are already configured.

Select an existing virtual network

When you select an existing virtual network, the Azure Resource Manager (ARM) template that creates the virtual network and other resources is redeployed. The resources, in this case, are the public IP address, gateway, gateway connection, and ExpressRoute authorization key.

If everything is set up, the deployment doesn't change anything. However, if anything is missing, it's created automatically. For example, if the gateway subnet is missing, it's added during the deployment.

1. In the Azure portal, go to the Azure VMware Solution private cloud.
2. Under **Manage**, select **Connectivity**.
3. Select the **Azure VNet connect** tab, and then select the existing virtual network.



4. Select **Save**.

At this point, the virtual network detects whether IP address spaces overlap between Azure VMware Solution and the virtual network. If overlapping IP address spaces are detected, change the network address of either the private cloud or the virtual network so they don't overlap.

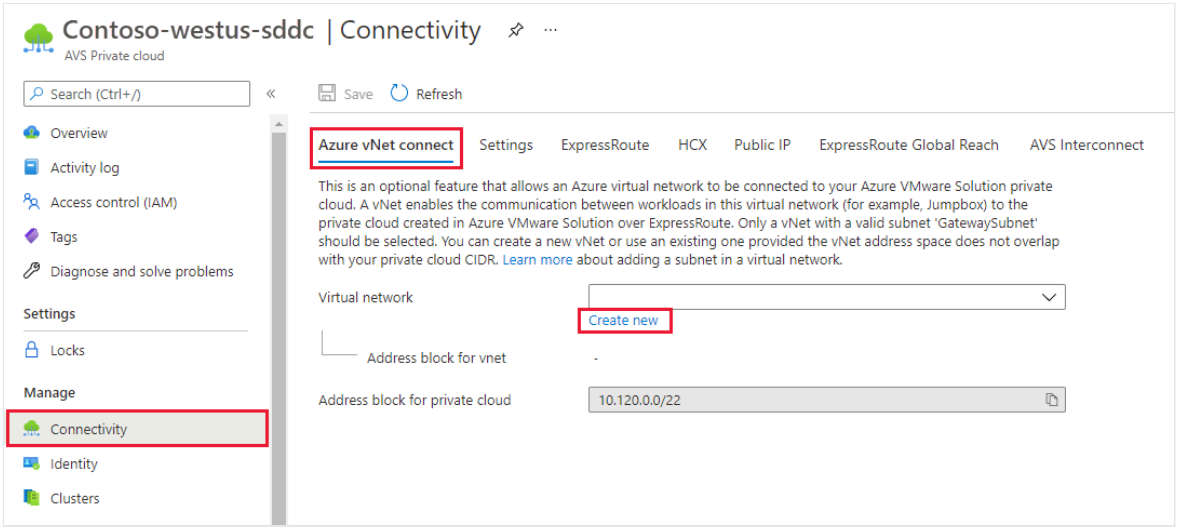
Create a new virtual network

When you create a virtual network, the required components to connect to Azure VMware Solution are automatically created.

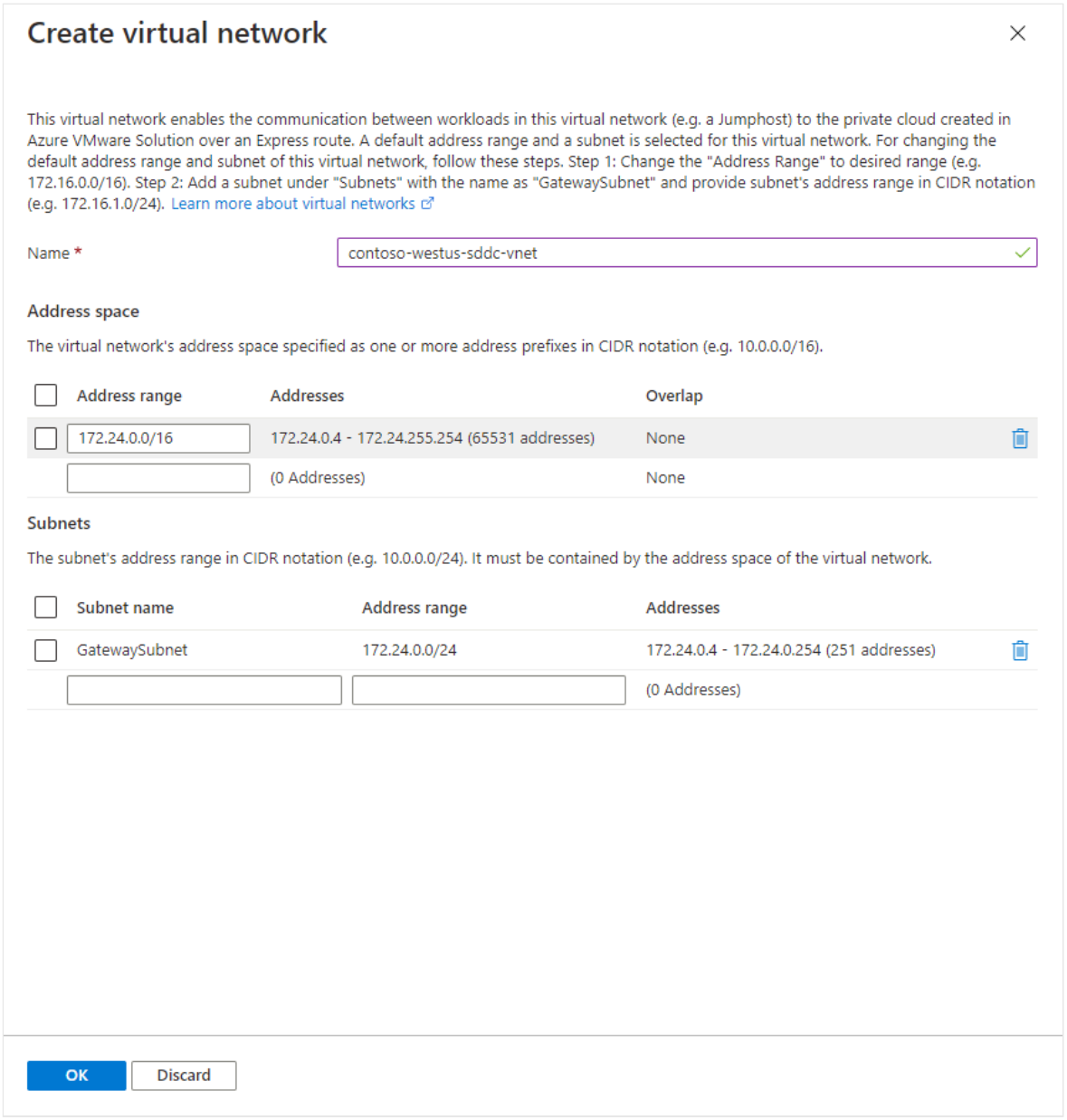
1. In the Azure portal, go to the Azure VMware Solution private cloud.

2. Under **Manage**, select **Connectivity**.

3. Select the **Azure VNet connect** tab, and then select **Create new**.



4. Provide or update the information for the new virtual network, and then select **OK**.



At this point, the virtual network detects whether IP address spaces overlap between Azure VMware Solution and the virtual network. If overlapping IP address spaces are detected, change the network address of either the private cloud or the virtual network so they don't overlap.

The virtual network with the provided address range and gateway subnet is created in your subscription and resource group.

Connect to the private cloud manually

Create a virtual network manually

1. Sign in to the Azure portal or, if necessary, the Azure Government portal.

2. Go to the resource group that you created in the tutorial for creating a private cloud, and then select + **Add** to define a new resource.

3. In the **Search the Marketplace** box, enter **virtual network**. Find the virtual network resource and select it.

4. On the **Virtual Network** page, select **Create** to set up your virtual network for your private cloud.

5. On the **Create virtual network** pane, enter the details for your virtual network:

   a. On the **Basics** tab, enter a name for the virtual network, select the appropriate region, and then select **Next : IP Addresses**.

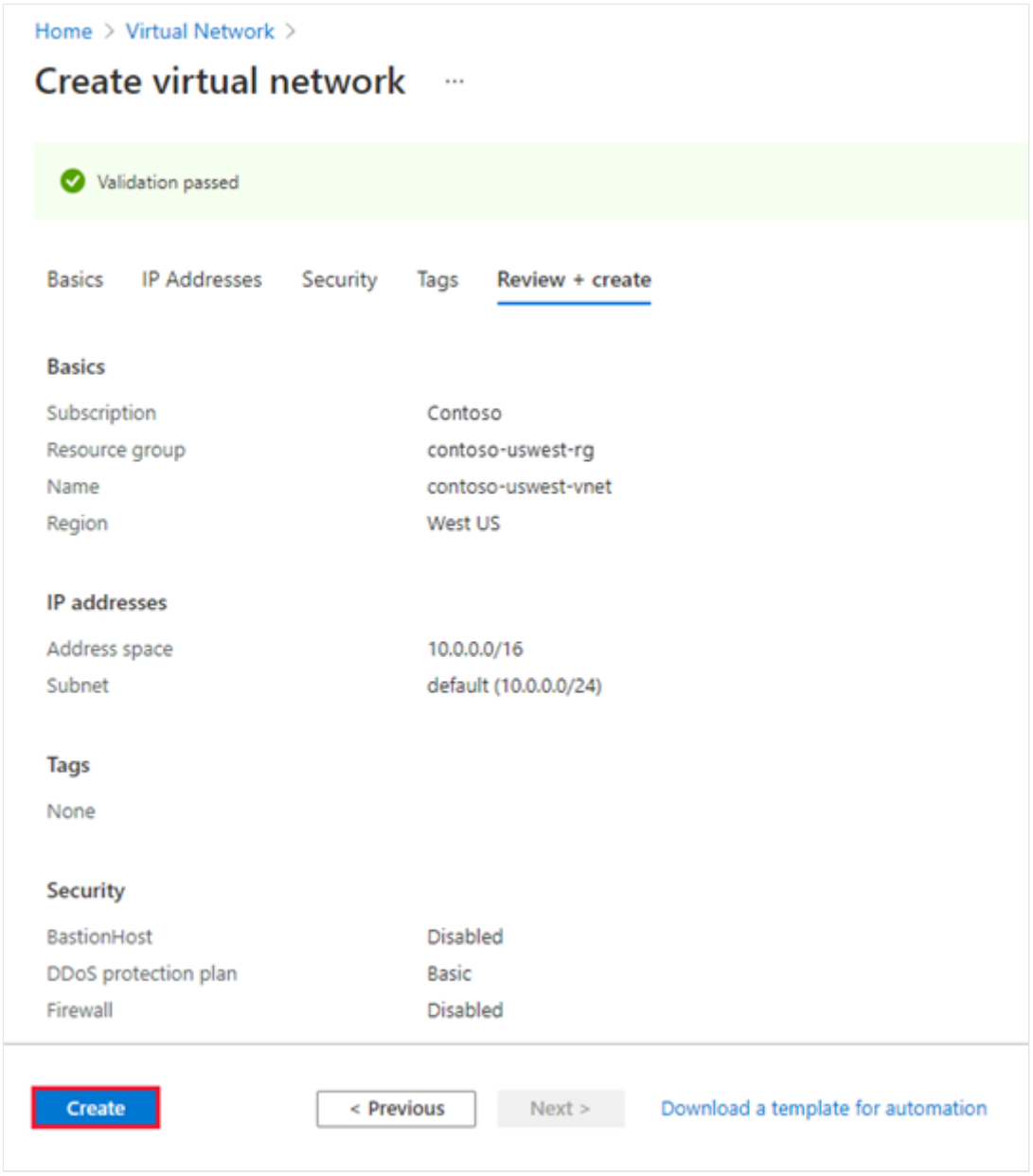
   b. On the **IP Addresses** tab, under **IPv4 address space**, enter the address space that you created in the previous tutorial.

   > **ⓘ Important**
   >
   > You must use an address space that doesn't overlap with the address space that you used when you created your private cloud in the preceding tutorial.

   c. Select **+ Add subnet**. On the **Add subnet** pane, give the subnet a name and an appropriate address range, and then select **Add**.

   d. Select **Review + create**.

   e. Verify the information and select **Create**.



After the deployment is complete, your virtual network appears in the resource group.

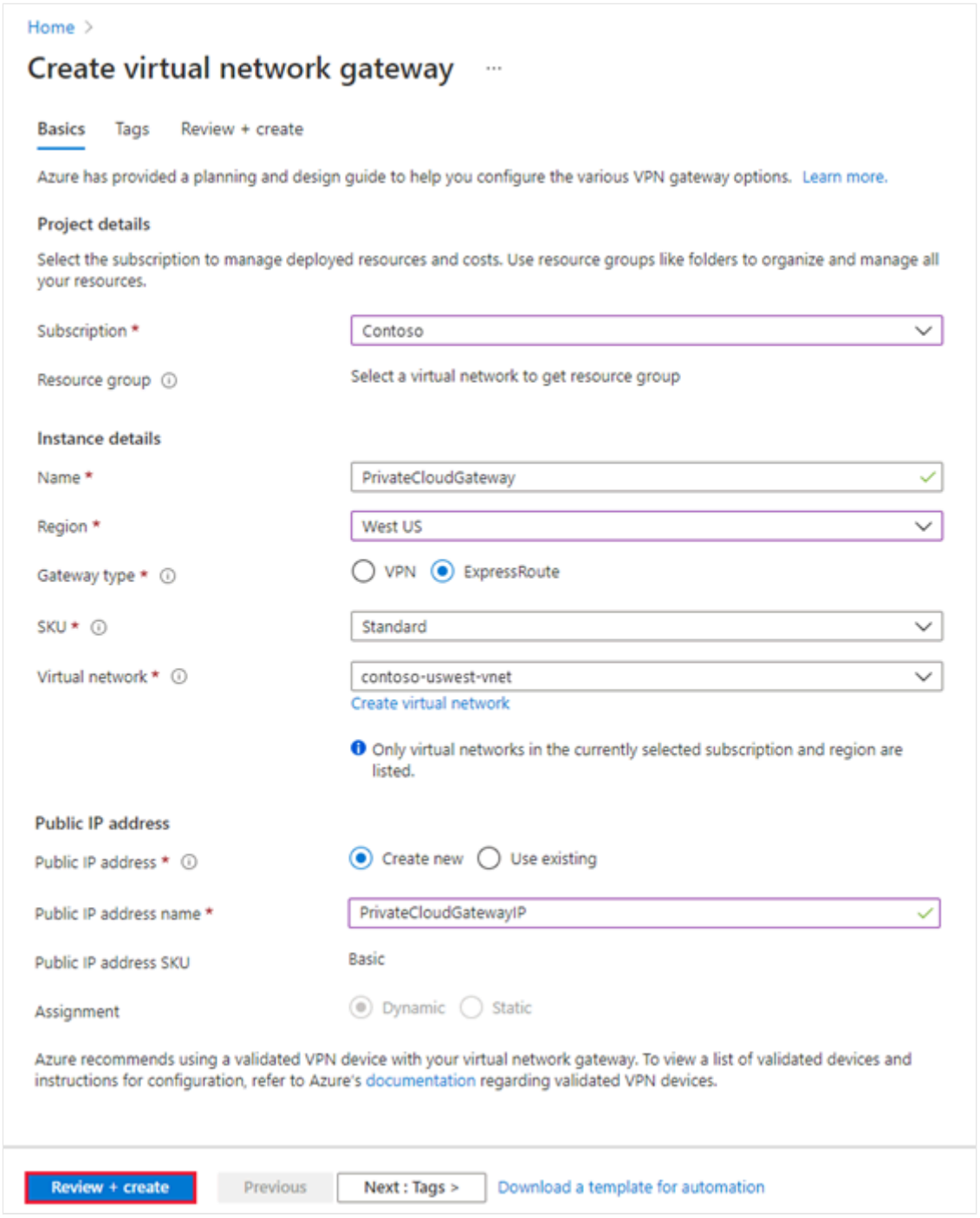
Create a virtual network gateway

Now that you've created a virtual network, create a virtual network gateway:

1. In your resource group, select + **Add** to add a new resource.
2. In the **Search the Marketplace** box, enter **virtual network gateway**. Find the virtual network resource and select it.
3. On the **Virtual Network gateway** page, select **Create**.
4. On the **Basics** tab of the **Create virtual network gateway** pane, provide the following values, and then select **Review + create**.

Expand table

Field	Value
Subscription	The value is prepopulated with the subscription to which the resource group belongs.
Resource group	The value is prepopulated for the current resource group. It should be the resource group that you created in a previous test.
Name	Enter a unique name for the virtual network gateway.
Region	Select the geographical location of the virtual network gateway.
Gateway type	Select **ExpressRoute**.
SKU	Select the gateway type that's appropriate for your workload. For Azure NetApp Files datastores, select **UltraPerformance** or **ErGw3Az**.
Virtual network	Select the virtual network that you created previously. If you don't see the virtual network, make sure the gateway's region matches the region of your virtual network.
Gateway subnet address range	The value is populated when you select the virtual network. Don't change the default value.
Public IP address	Select **Create new**.



5. Verify that the details are correct, and then select **Create** to start deployment of your virtual network gateway.

After the deployment finishes, move to the next section to connect ExpressRoute to the virtual network gateway that contains your Azure VMware Solution private cloud.

Connect ExpressRoute to the virtual network gateway

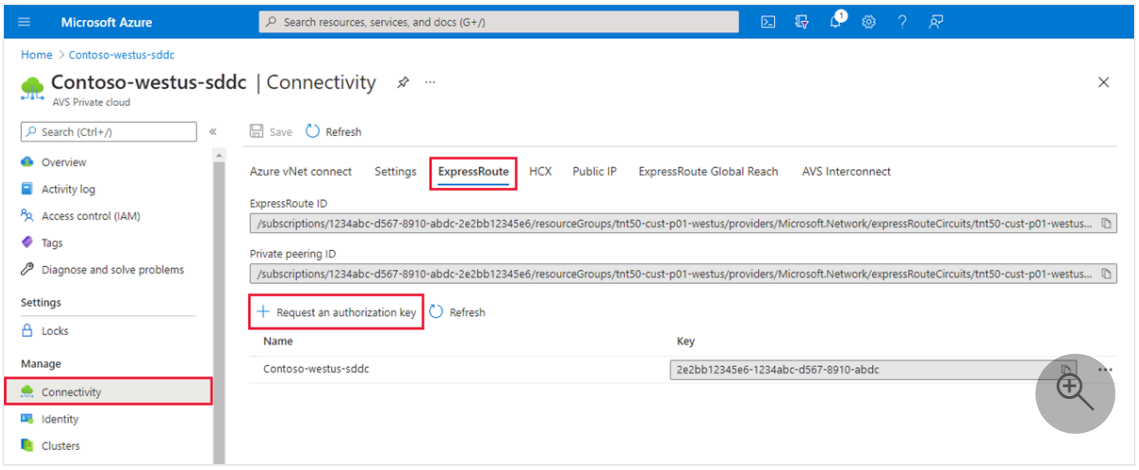
Now that you've deployed a virtual network gateway, add a connection between it and your Azure VMware Solution private cloud:

1. Request an ExpressRoute authorization key:

a. In the Azure portal, go to the Azure VMware Solution private cloud.

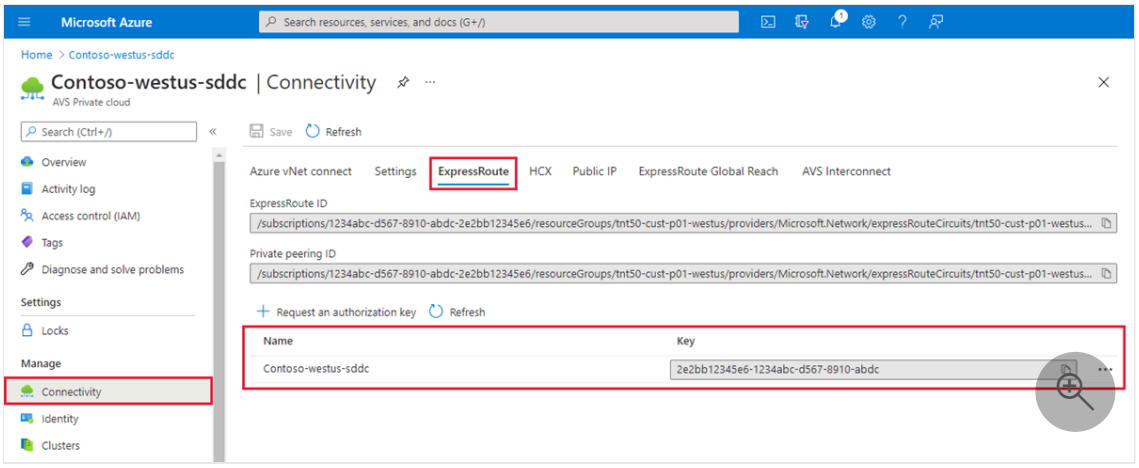
b. Under **Manage**, select **Connectivity**.

c. Select the **ExpressRoute** tab, and then select **+ Request an authorization key**.



d. Provide a name for the authorization key, and then select **Create**.

It can take about 30 seconds to create the key. After the key is created, it appears in the list of authorization keys for the private cloud.



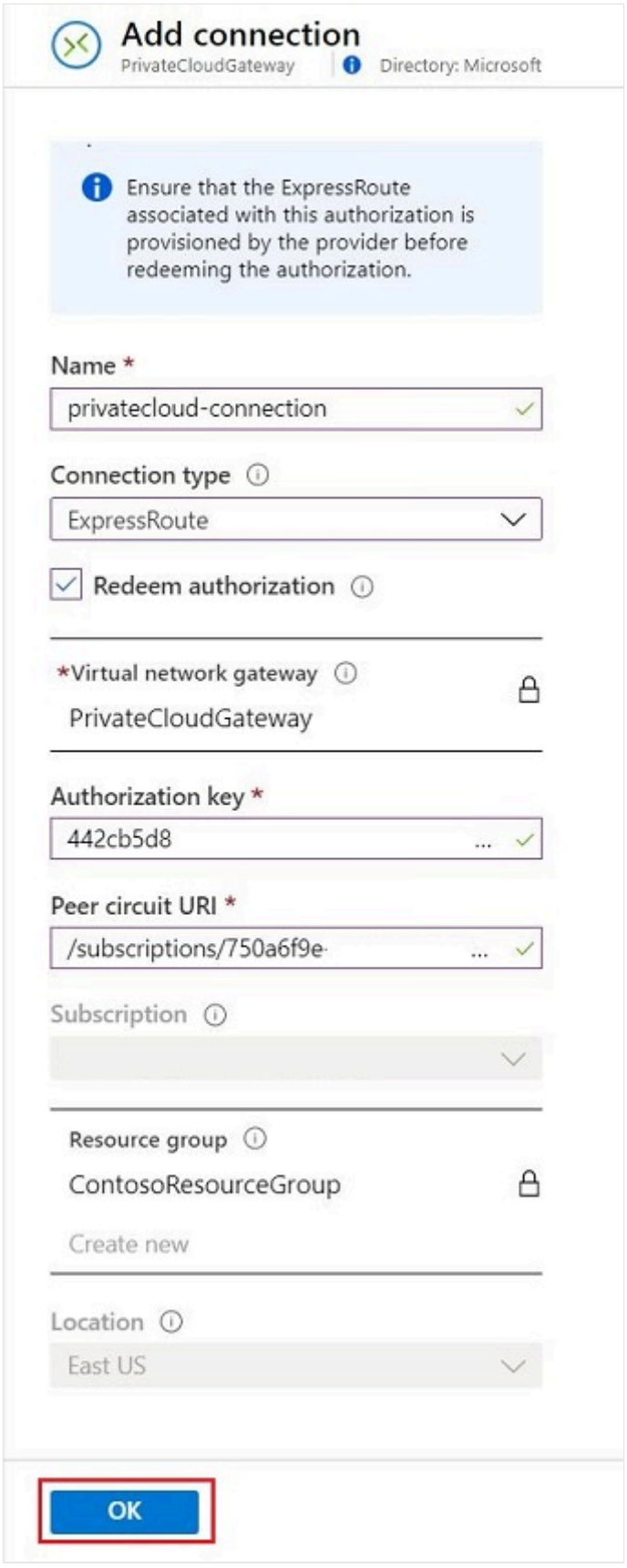
e. Copy the authorization key and the ExpressRoute ID. You need them to complete the peering. The authorization key disappears after some time, so copy it as soon as it appears.

2. Go to the virtual network gateway that you plan to use, and then select **Connections** > **+ Add**.

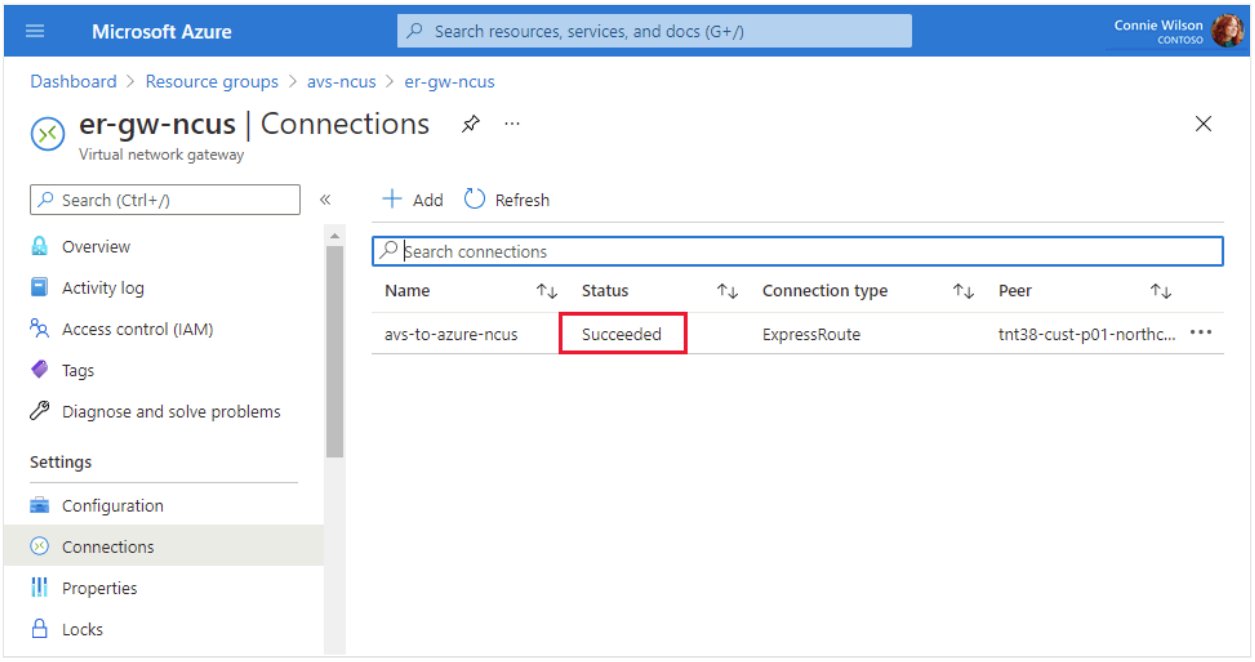
3. On the **Add connection** pane, provide the following values, and then select **OK**.

Expand table

Field	Value
Name	Enter a name for the connection.
Connection type	Select **ExpressRoute**.
Redeem authorization	Ensure that this checkbox is selected.
Virtual network gateway	The value is prepopulated with the virtual network gateway that you intend to use.
Authorization key	Paste the authorization key that you copied earlier.
Peer circuit URI	Paste the ExpressRoute ID that you copied earlier.



A status of **Succeeded** indicates that you finished creating the connection between your ExpressRoute circuit and your virtual network.



Next step

Continue to the next tutorial to learn how to create the NSX network segments for virtual machines in vCenter Server:

Create an NSX network segment

Feedback

Was this page helpful? Yes No

Provide product feedback

Tutorial: Access an Azure VMware Solution private cloud

Article • 04/01/2024

Azure VMware Solution doesn't allow you to manage your private cloud with your on-premises vCenter Server. Instead, you need to connect to the Azure VMware Solution vCenter Server instance through a jump box.

In this tutorial, learn how to create a jump box in the resource group that you created in the previous tutorial and sign in to the Azure VMware Solution vCenter Server. This jump box is a Windows virtual machine (VM) on the same virtual network you created. It provides access to both vCenter Server and the NSX Manager.

In this tutorial, you learn how to:

- ✓ Create a Windows VM to access the Azure VMware Solution vCenter Server
- ✓ Sign in to vCenter Server from this VM

Create a new Windows virtual machine

1. In the resource group, select **Add**, search for **Microsoft Windows 10**, and select it. Then select **Create**.

2. Enter the required information in the fields, and then select **Review + create**.

   For more information on the fields, see the following table.

Expand table

Field	Value
Subscription	Value is prepopulated with the Subscription belonging to the Resource Group.
Resource group	Value is prepopulated for the current Resource Group, which you created in the preceding tutorial.
Virtual machine name	Enter a unique name for the VM.
Region	Select the geographical location of the VM.
Availability options	Leave the default value selected.
Image	Select the VM image.
Size	Leave the default size value.
Authentication type	Select **Password**.
Username	Enter the user name for logging on to the VM.
Password	Enter the password for logging on to the VM.
Confirm password	Enter the password for logging on to the VM.
Public inbound ports	Select **None**. • To control access to the VM only when you want to access it, use JIT access. • To securely access the jump box server from the internet without exposing any network port, use an Azure Bastion.

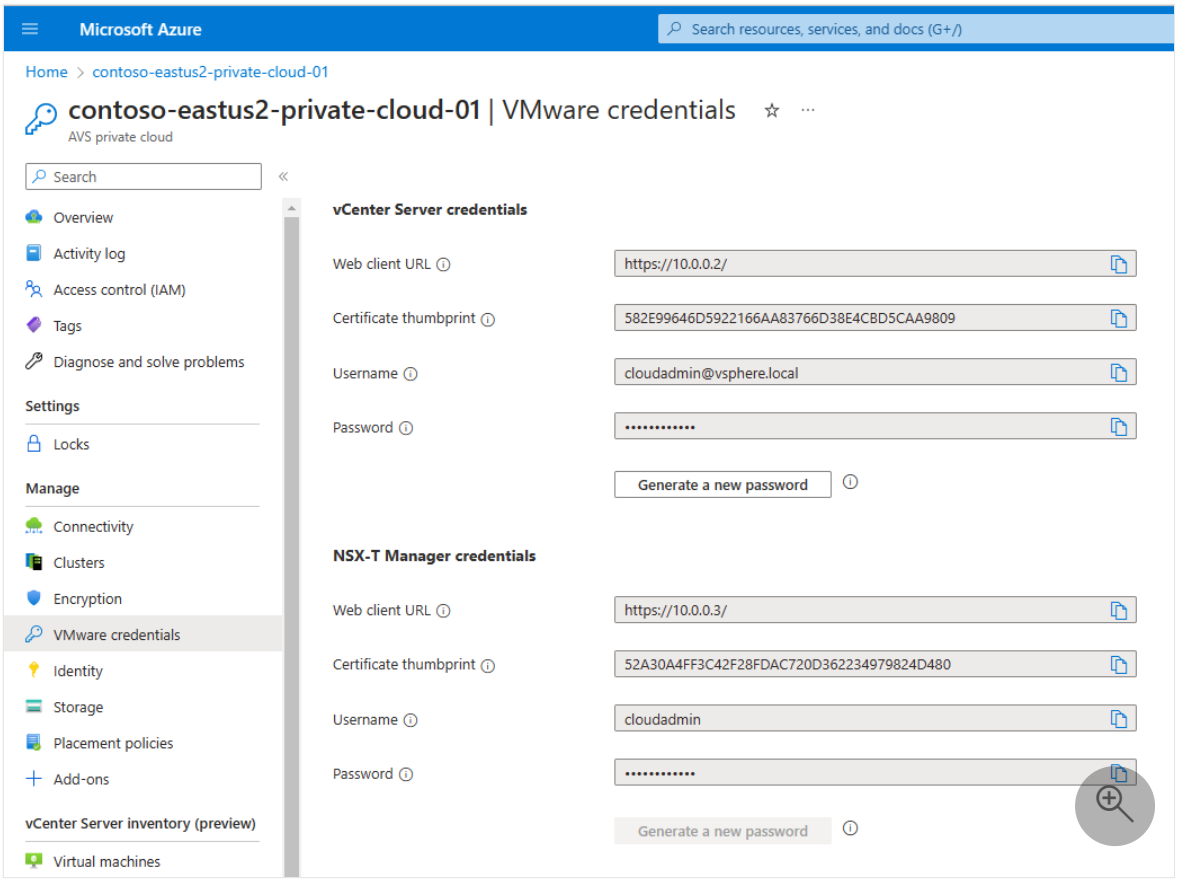
3. Once validation passes, select **Create** to start the virtual machine creation process.

Connect to the vCenter Server of your private cloud

1. From the jump box, sign in to vSphere Client with VMware vCenter Server SSO using a cloudadmin username and verify that the user interface displays successfully.

2. In the Azure portal, select your private cloud, and then **Manage** > **VMware credentials**.

   The URLs and user credentials for private cloud vCenter Server and NSX Manager are displayed.

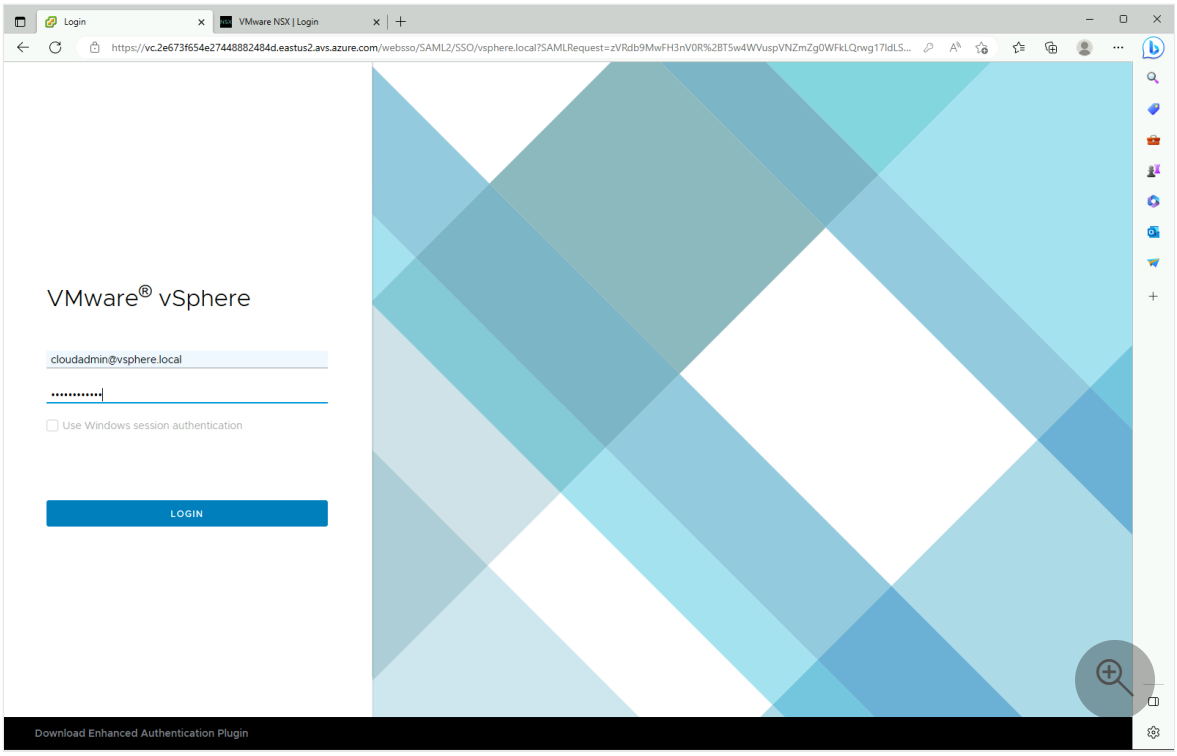


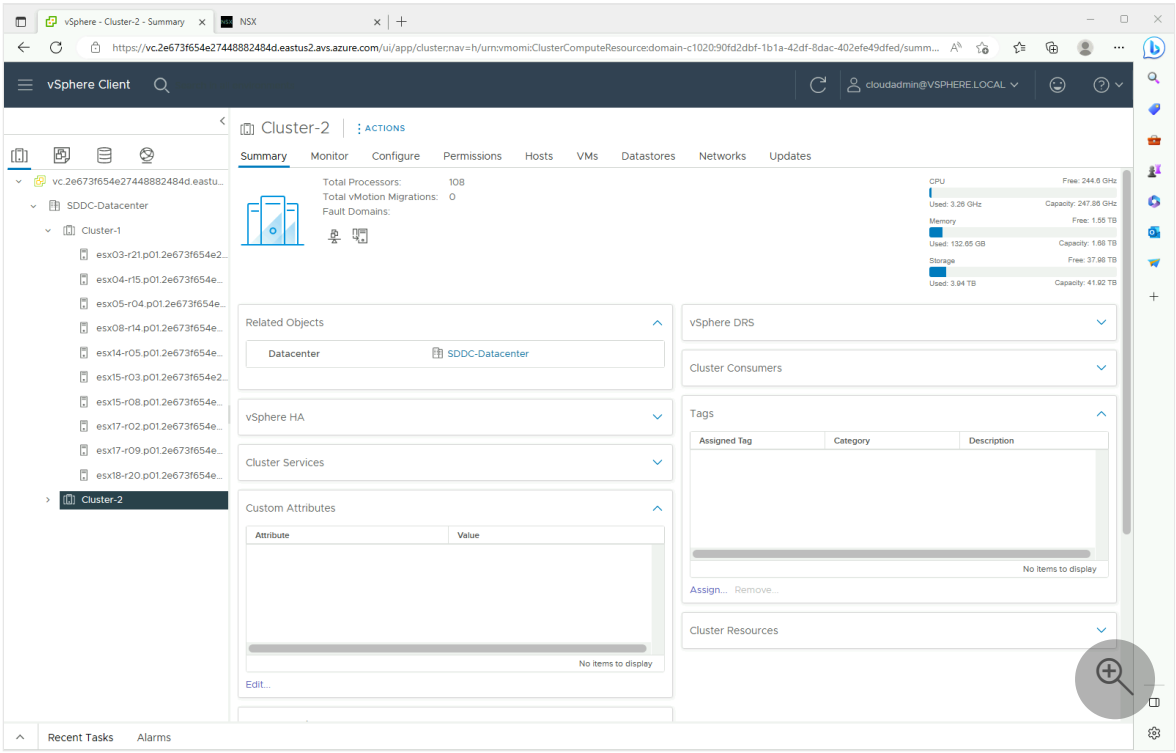
3. Navigate to the VM you created in the preceding step and connect to the virtual machine.

   If you need help with connecting to the VM, see connect to a virtual machine for details.

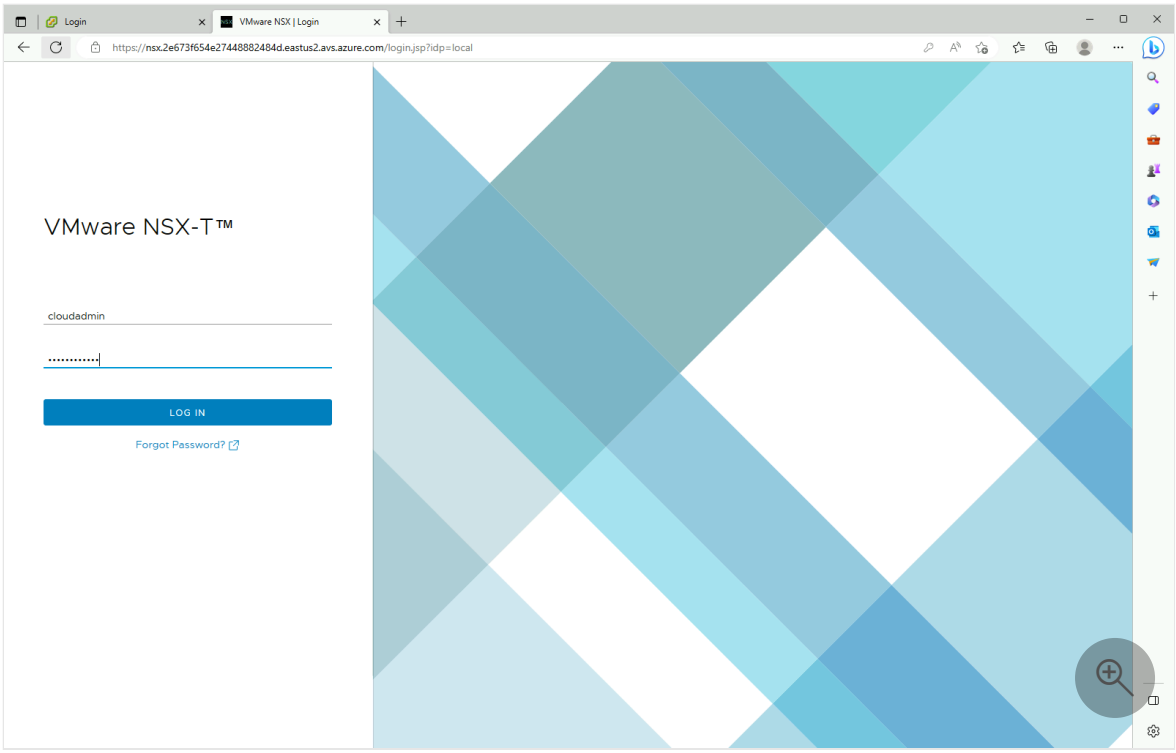
4. In the Windows VM, open a browser and navigate to the vCenter Server and NSX Manager URLs in two tabs.

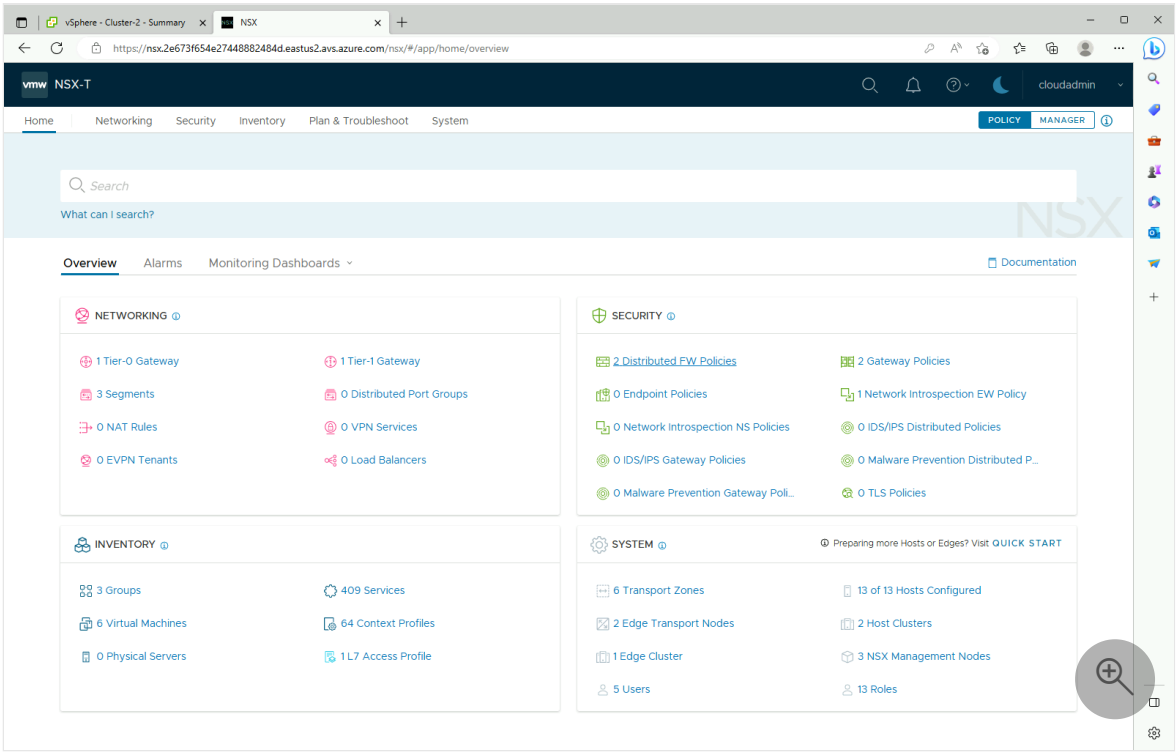
5. In the vSphere Client tab, enter the `cloudadmin@vsphere.local` user credentials from the previous step.





6. In the second tab of the browser, sign in to NSX Manager with the 'cloudadmin' user credentials from earlier.





Next steps

In this tutorial, you learned how to:

- ✓ Create a Windows VM to use to connect to vCenter Server
- ✓ Login to vCenter Server from your VM
- ✓ Login to NSX Manager from your VM

Continue to the next tutorial to learn how to create a virtual network to set up local management for your private cloud clusters.

Create a Virtual Network

Tutorial: Add an NSX network segment in Azure VMware Solution

Article • 06/12/2024

After deploying Azure VMware Solution, you can configure an NSX network segment from NSX Manager or the Azure portal. Once configured, the segments are visible in Azure VMware Solution, NSX Manager, and vCenter Server. NSX comes pre-provisioned by default with an NSX Tier-0 gateway in **Active/Active** mode and a default NSX Tier-1 gateway in **Active/Standby** mode. These gateways let you connect the segments (logical switches) and provide East-West and North-South connectivity.

> **Tip**
>
> The Azure portal presents a simplified view of NSX operations a VMware administrator needs regularly and targeted at users not familiar with NSX Manager.

In this tutorial, you learn how to:

- ✓ Add network segments using either NSX Manager or the Azure portal
- ✓ Verify the new network segment

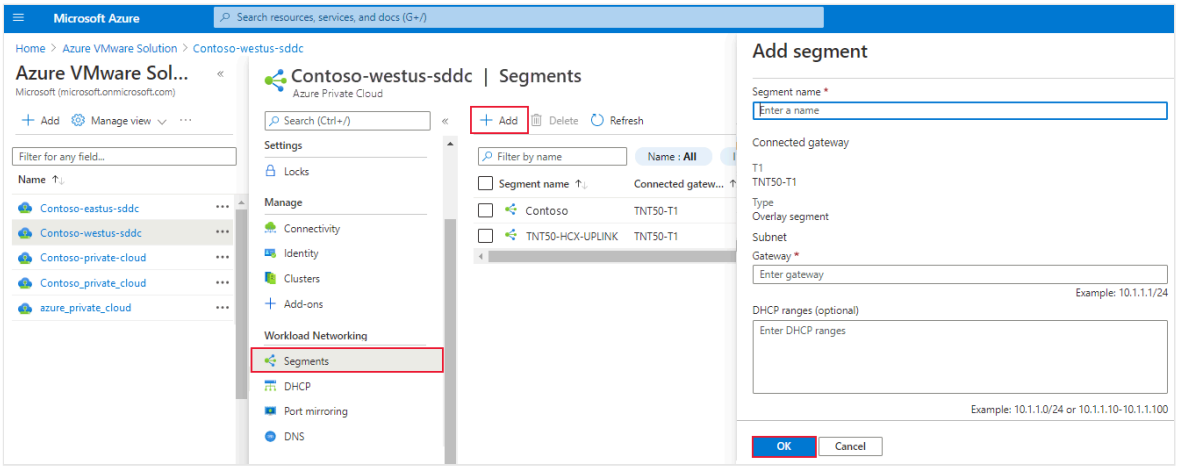
Prerequisites

An Azure VMware Solution private cloud with access to the vCenter Server and NSX Manager interfaces. For more information, see the Configure networking tutorial.

Use Azure portal to add an NSX network segment

> **Note**
>
> If you plan to use DHCP, you'll need to configure a DHCP server or DHCP relay before you can configure an NSX network segment.

1. In your Azure VMware Solution private cloud, under **Workload Networking**, select **Segments** > **Add**.
2. Provide the details for the new logical segment and select **OK**.



- **Segment name** - Name of the segment that is visible in vCenter Server.
- **Subnet gateway** - Gateway IP address for the segment's subnet with a subnet mask. VMs are attached to a logical segment, and all VMs connecting to this segment belong to the same subnet. Also, all VMs attached to this logical segment must carry an IP address from the same segment.
- **DHCP** (optional) - DHCP ranges for a logical segment. You must configure a DHCP server or DHCP relay to consume DHCP on Segments.

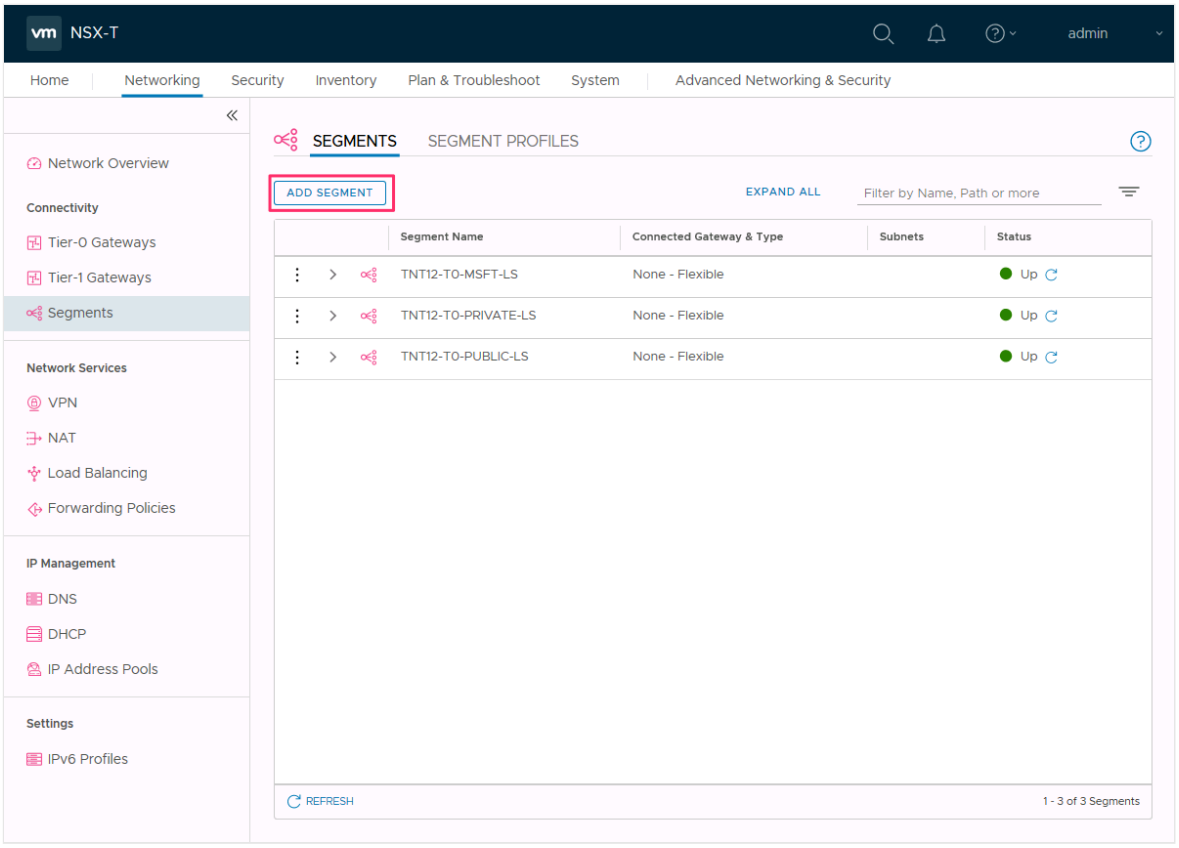
> **Note**
>
> The **Connected gateway** is selected by default and is read-only. It shows Tier-1 Gateway and type of segment information.
>
> - **T1** - Name of the Tier-1 Gateway in NSX Manager. A private cloud comes with an NSX Tier-0 Gateway in Active/Active mode and a default NSX Tier-1 Gateway in Active/Standby mode. Segments created through the Azure VMware Solution console only connect to the default Tier-1 Gateway, and the workloads of these segments get East-West and North-South connectivity. You can only create more Tier-1 Gateways through NSX Manager. Tier-1 Gateways created from the NSX Manager console are not visible in the Azure VMware Solution console.
> - **Type** - Overlay segment supported by Azure VMware Solution.

The segment is now visible in Azure VMware Solution, NSX Manager, and vCenter Server.

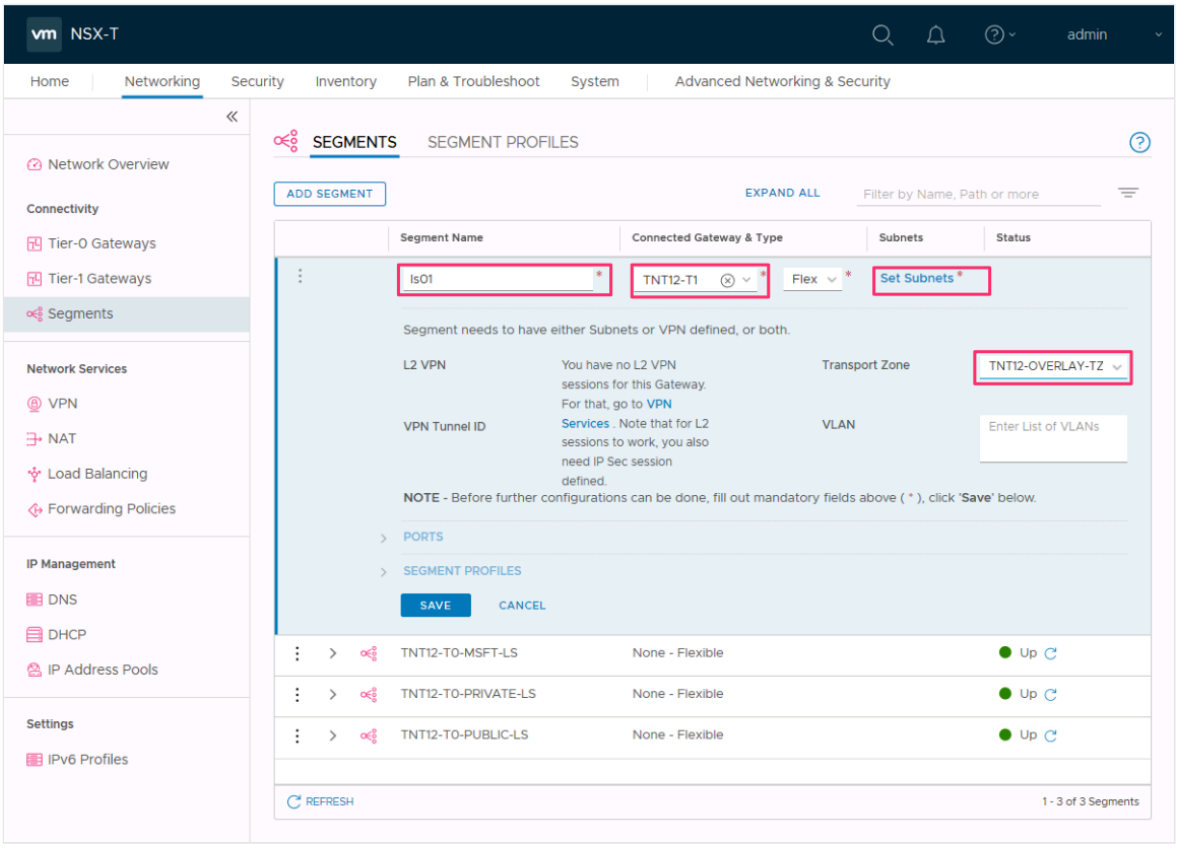
Use NSX Manager to add network segment

The virtual machines (VMs) created in vCenter Server are placed onto the network segments created in NSX and are visible in vCenter Server.

1. In NSX Manager, select **Networking** > **Segments**, and then select **Add Segment**.

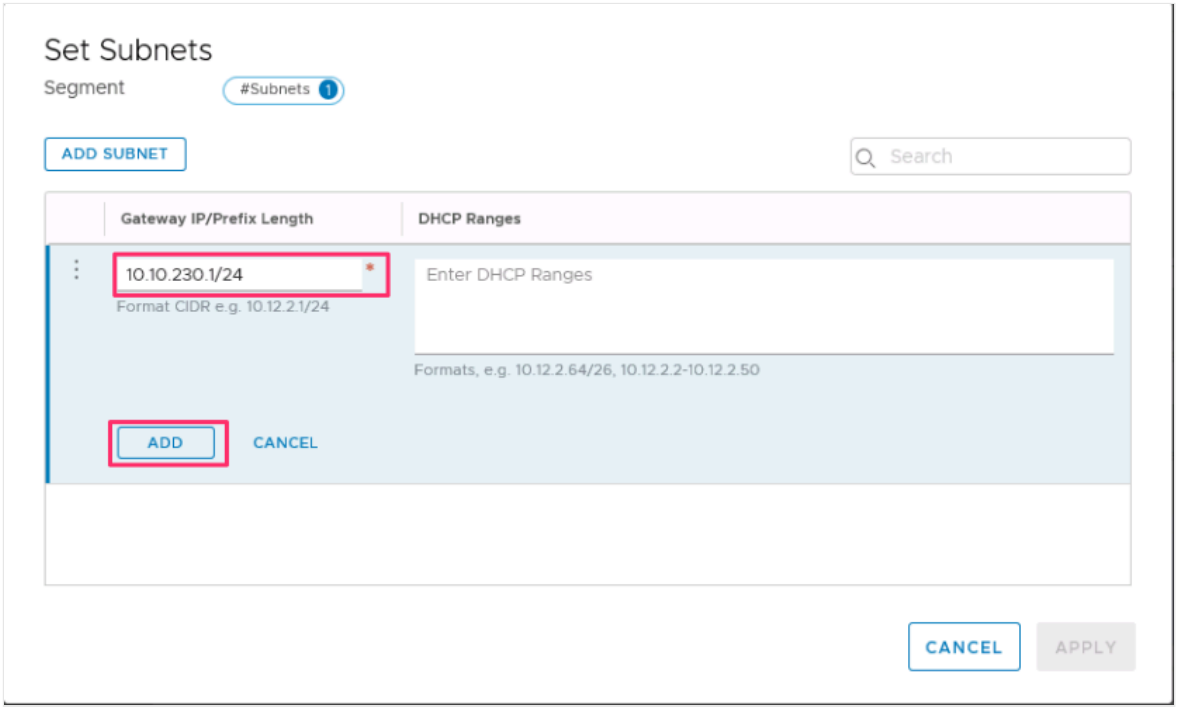


2. Enter a name for the segment.
3. Select the Tier-1 Gateway (TNTxx-T1) as the **Connected Gateway** and leave the **Type** as Flexible.
4. Select the preconfigured overlay **Transport Zone** (TNTxx-OVERLAY-TZ) and then select **Set Subnets**.



5. Enter the gateway IP address and then select **Add**.

> **Important**
>
> The IP address needs to be on a non-overlapping RFC1918 address block, which ensures connection to the VMs on the new segment.



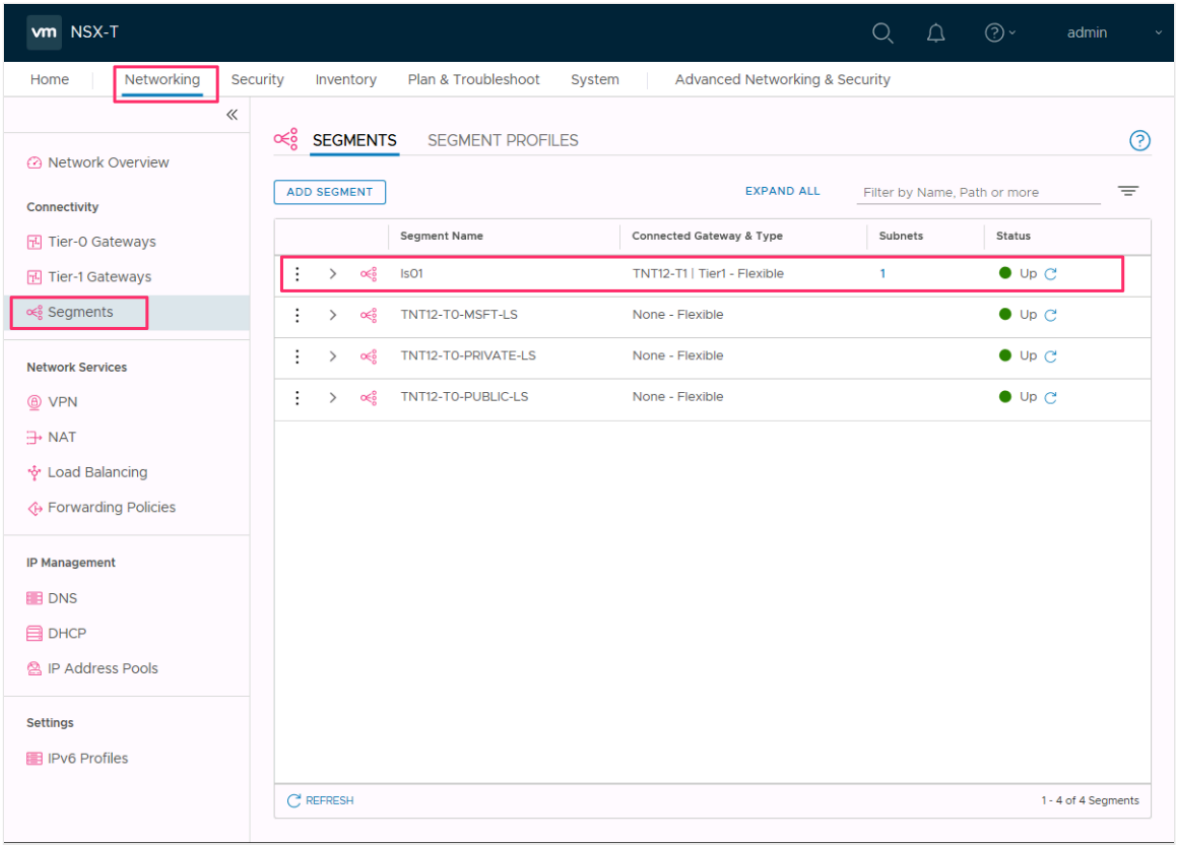
6. Select **Apply** and then **Save**.

7. Select **No** to decline the option to continue configuring the segment.

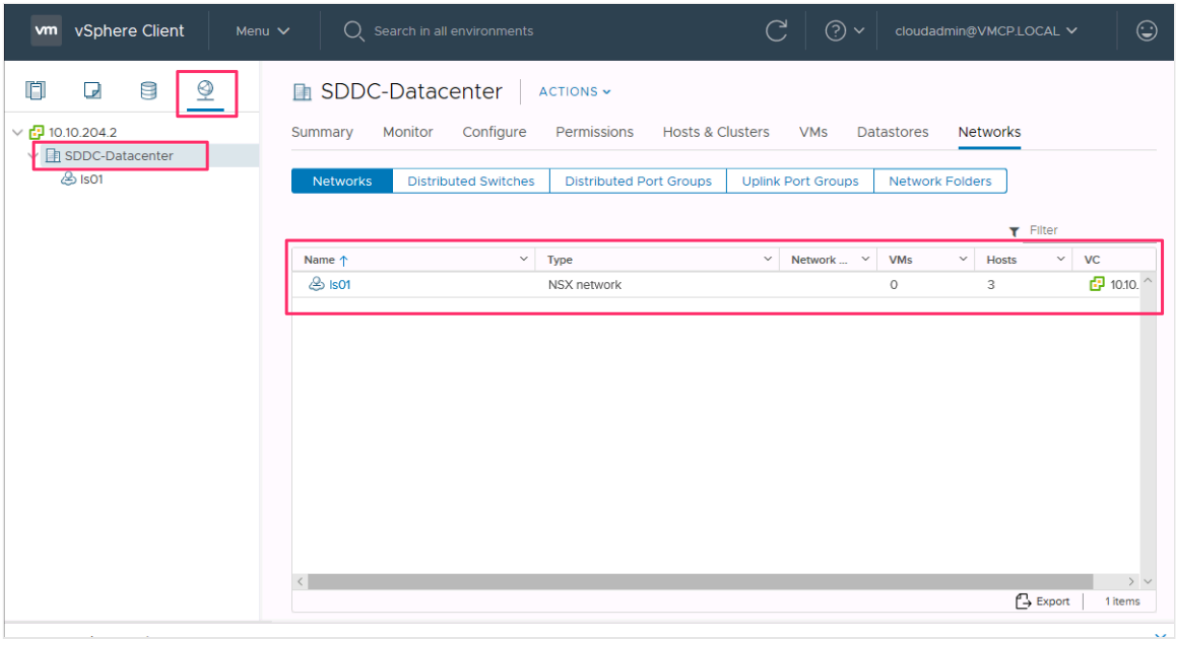
Verify the new network segment

Verify the presence of the new network segment. In this example, **ls01** is the new network segment.

1. In NSX Manager, select **Networking** > **Segments**.



2. In vCenter Server, select **Networking** > **SDDC-Datacenter**.



Next steps

In this tutorial, you created an NSX network segment to use for VMs in vCenter Server.

You can now:

- Configure and manage DHCP for Azure VMware Solution
- Create a Content Library to deploy VMs in Azure VMware Solution
- Peer on-premises environments to a private cloud

Feedback

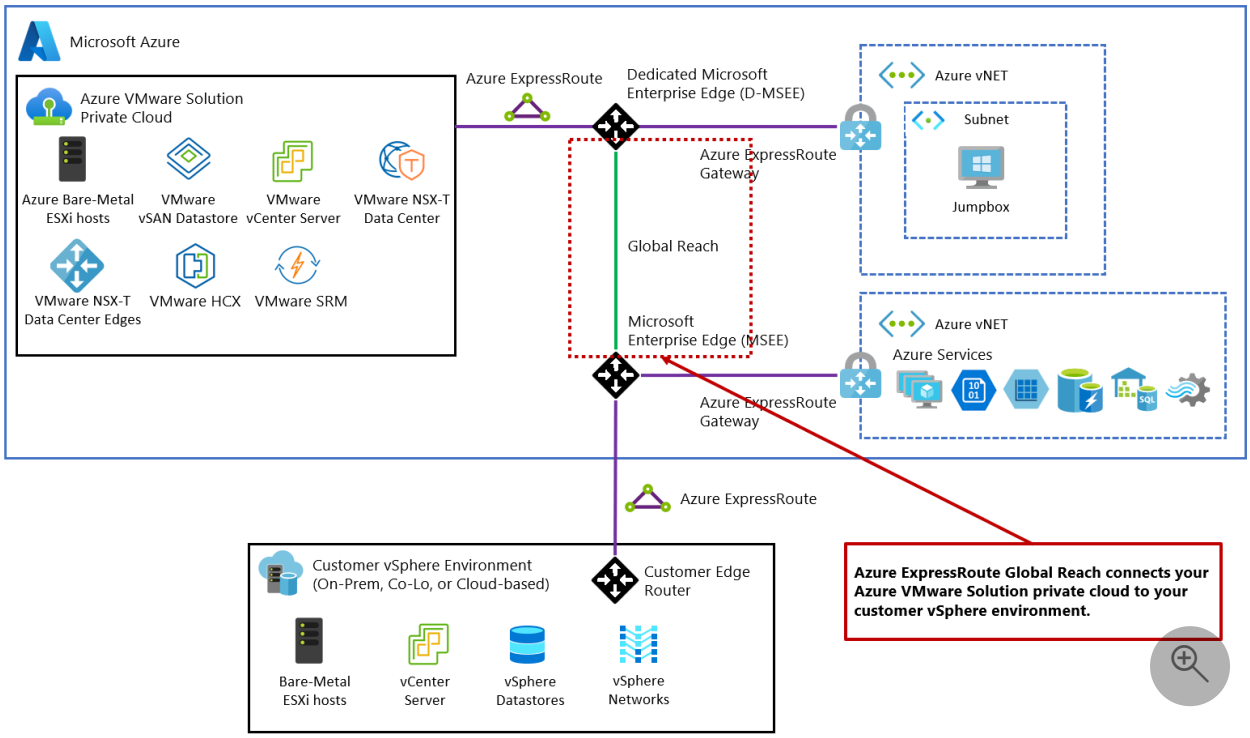
Was this page helpful? Yes No

Provide product feedback

Tutorial: Peer on-premises environments to Azure VMware Solution

Article • 12/20/2023

After you deploy your Azure VMware Solution private cloud, connect it to your on-premises environment. ExpressRoute Global Reach connects your on-premises environment to your Azure VMware Solution private cloud. The ExpressRoute Global Reach connection is established between the private cloud ExpressRoute circuit and an existing ExpressRoute connection to your on-premises environments.



> **Note**
>
> You can connect through VPN, but that's out of scope for this quick start guide.

In this article, you'll:

- ✓ Create an ExpressRoute auth key in the on-premises ExpressRoute circuit
- ✓ Peer the private cloud with your on-premises ExpressRoute circuit
- ✓ Verify on-premises network connectivity

Once you completed this section, follow the next steps provided at the end of this tutorial.

Prerequisites

- Review the documentation on how to enable connectivity in different Azure subscriptions.
- A separate, functioning ExpressRoute circuit for connecting on-premises environments to Azure, which is *circuit 1* for peering.
- Ensure that all gateways, including the ExpressRoute provider's service, support 4-byte Autonomous System Number (ASN). Azure VMware Solution uses 4-byte public ASNs for advertising routes.

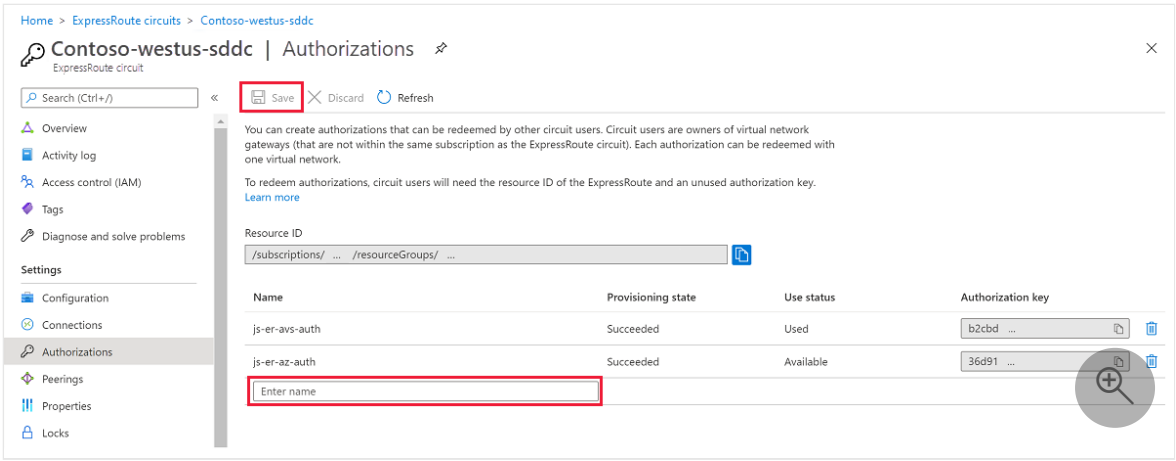
> **Note**
>
> If advertising a default route to Azure (0.0.0.0/0), ensure a more specific route containing your on-premises networks is advertised in addition to the default route to enable management access to Azure VMware Solution. A single 0.0.0.0/0 route will be discarded by Azure VMware Solution's management network to ensure successful operation of the service.

Create an ExpressRoute auth key in the on-premises ExpressRoute circuit

The circuit owner creates an authorization, which creates an authorization key to be used by a circuit user to connect their virtual network gateways to the ExpressRoute circuit. An authorization is valid for only one connection.

> **Note**
>
> Each connection requires a separate authorization.

1. From **ExpressRoute circuits** in the left navigation, under Settings, select **Authorizations**.
2. Enter the name for the authorization key and select **Save**.



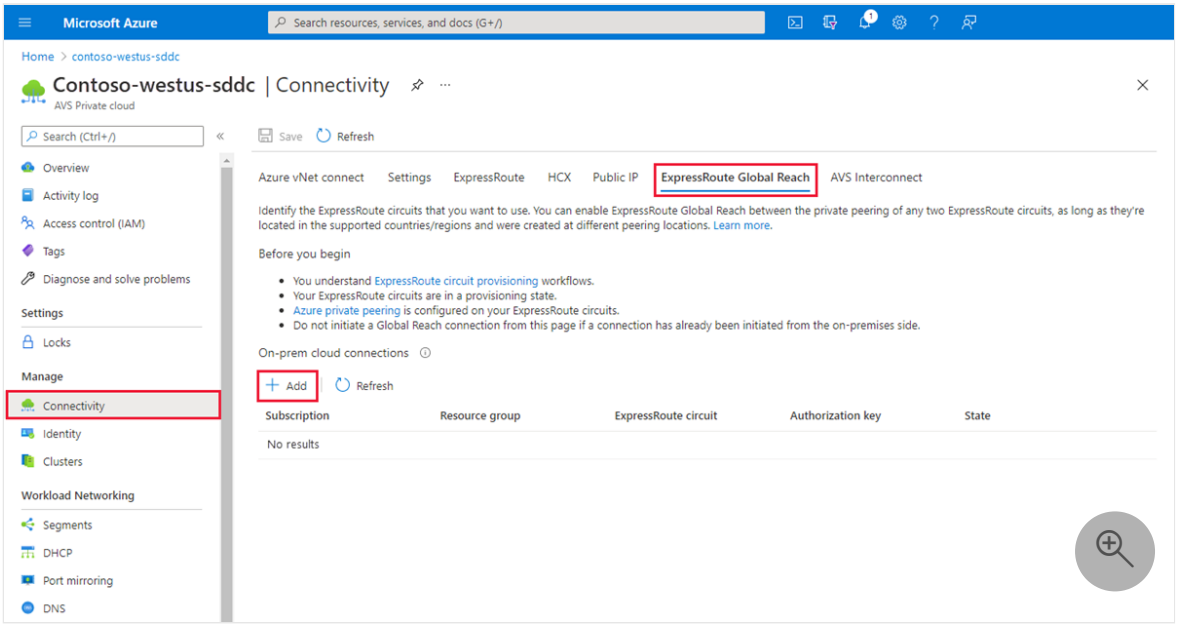
Once created, the new key appears in the list of authorization keys for the circuit.

3. Copy the authorization key and the ExpressRoute ID to use them in the next step to complete the peering.

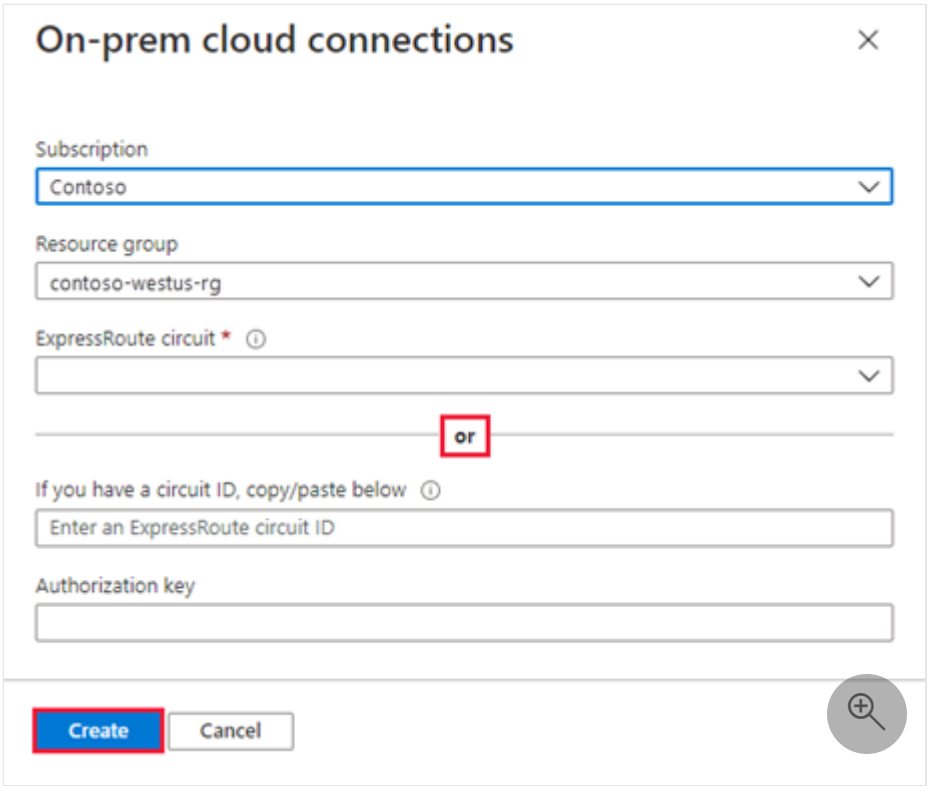
Peer private cloud to on-premises

Now that you created an authorization key for the private cloud ExpressRoute circuit, you can peer it with your on-premises ExpressRoute circuit. The peering is done from the on-premises ExpressRoute circuit in the **Azure portal**. You use the resource ID (ExpressRoute circuit ID) and authorization key of your private cloud ExpressRoute circuit to finish the peering.

1. From the private cloud, under Manage, select **Connectivity** > **ExpressRoute Global Reach** > **Add**.

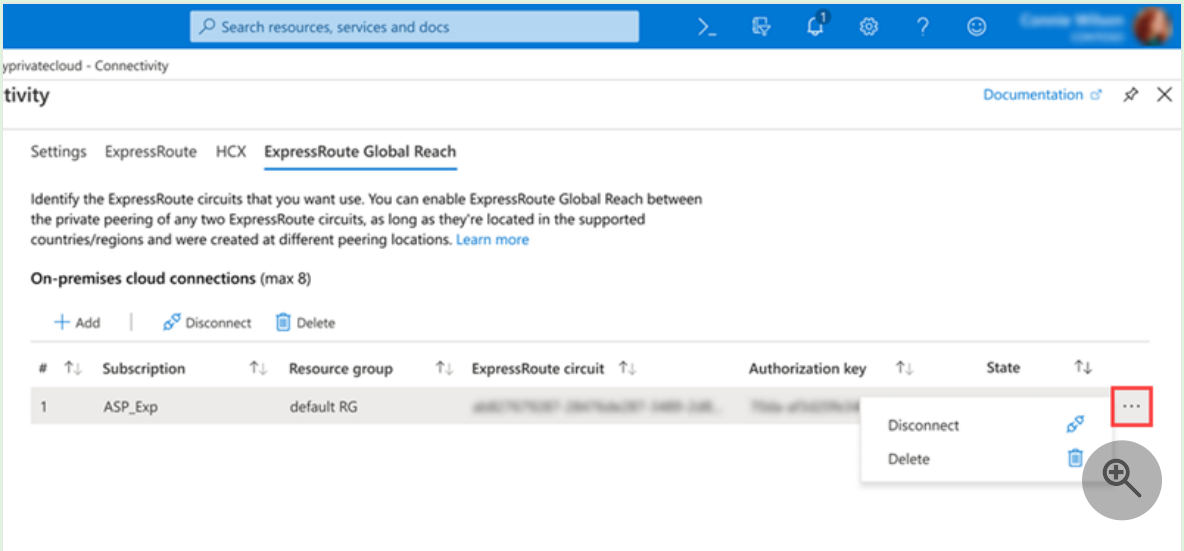


2. Enter the ExpressRoute ID and the authorization key created in the previous section.



3. Select **Create**. The new connection shows in the on-premises cloud connections list.

> **Tip**
>
> You can delete or disconnect a connection from the list by selecting **More**.



Verify on-premises network connectivity

In your **on-premises edge router**, you should now see where the ExpressRoute connects the NSX-T Data Center network segments and the Azure VMware Solution management segments.

> **Important**
>
> Everyone has a different environment, and some will need to allow these routes to propagate back into the on-premises network.

Next steps

Continue to the next tutorial to install VMware HCX add-on in your Azure VMware Solution private cloud.

Install VMware HCX

Tutorial: Scale clusters in a private cloud

Article • 06/07/2024

To get the most out of your Azure VMware Solution private cloud experience, scale the clusters and hosts to reflect what you need for planned workloads. You can scale the clusters and hosts in a private cloud as required for your application workload. You should address performance and availability limitations for specific services on a case-by-case basis.

The following table describes the maximum limits for Azure VMware Solution.

Expand table

Resource	Limit
vSphere clusters per private cloud	12
Minimum number of ESXi hosts per cluster	3 (hard-limit)
Maximum number of ESXi hosts per cluster	16 (hard-limit)
Maximum number of ESXi hosts per private cloud	96
Maximum number of vCenter Servers per private cloud	1 (hard-limit)
Maximum number of HCX site pairings	25 (any edition)
Maximum number of HCX service meshes	10 (any edition)
Maximum number of Azure VMware Solution ExpressRoute linked private clouds from a single location to a single Virtual Network Gateway	4 The virtual network gateway used determines the actual max linked private clouds. For more information, see About ExpressRoute virtual network gateways If you exceed this threshold use Azure VMware Solution Interconnect to aggregate private cloud connectivity within the Azure region.
Maximum Azure VMware Solution ExpressRoute port speed	10 Gbps (use Ultra Performance Gateway SKU with FastPath enabled) The virtual network gateway used determines the actual bandwidth. For more information, see About ExpressRoute virtual network gateways
Maximum number of Azure Public IPv4 addresses assigned to NSX	2,000

Resource	Limit
Maximum number of Azure VMware Solution Interconnects per private cloud	10
Maximum number of Azure ExpressRoute Global Reach connections per Azure VMware Solution private cloud	8
vSAN capacity limits	75% of total usable (keep 25% available for SLA)
VMware Site Recovery Manager - Maximum number of protected Virtual Machines	3,000
VMware Site Recovery Manager - Maximum number of Virtual Machines per recovery plan	2,000
VMware Site Recovery Manager - Maximum number of protection groups per recovery plan	250
VMware Site Recovery Manager - RPO Values	5 min or higher * (hard-limit)
VMware Site Recovery Manager - Maximum number of virtual machines per protection group	500
VMware Site Recovery Manager - Maximum number of recovery plans	250

* For information about Recovery Point Objective (RPO) lower than 15 minutes, see How the 5 Minute Recovery Point Objective Works in the *vSphere Replication Administration guide*.

For other VMware-specific limits, use the VMware configuration maximum tool.

In this tutorial, learn how to use the Azure portal to:

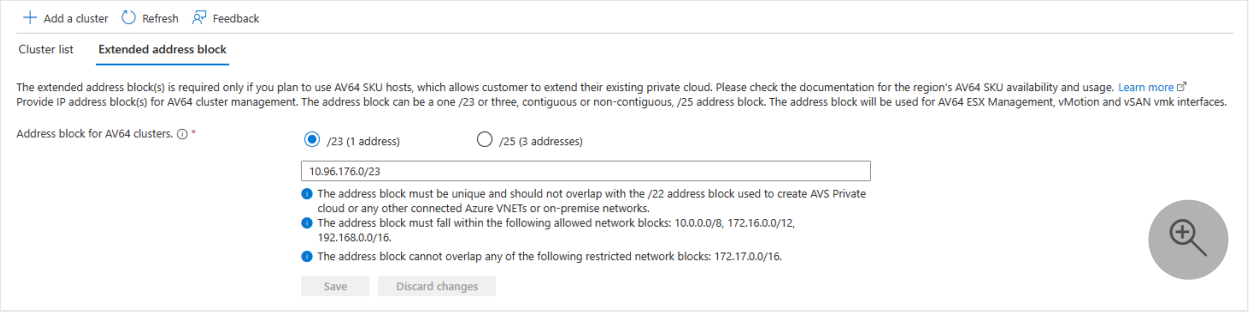
- ✓ Add a cluster to an existing private cloud
- ✓ Add hosts to an existing cluster

Prerequisites

You need an existing private cloud to complete this tutorial. If you don't already have a private cloud created, follow the create a private cloud tutorial to create one.

If you are planning on using the AV64 SKU, define a network for the management and control plane. In your Azure VMware Solution private cloud, under **Manage**, select

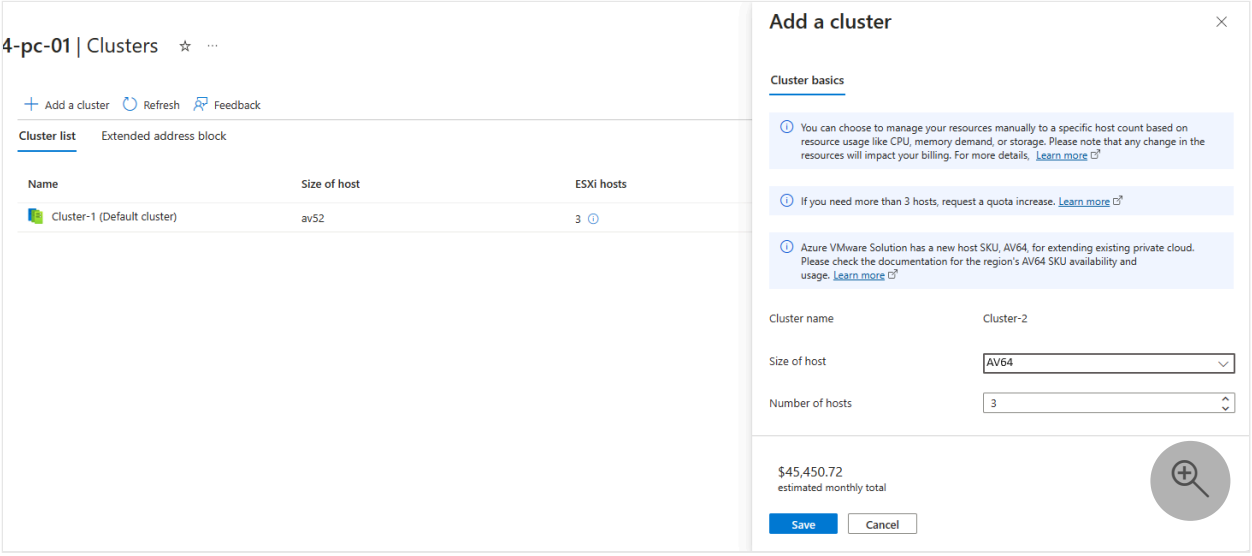
Clusters > **Add a cluster**. Then add the **Address block for AV64 clusters** (one /23 network or three /25 networks) under the **Extended address block** tab and select **Save**.



Add a new cluster

1. In your Azure VMware Solution private cloud, under **Manage**, select **Clusters** > **Add a cluster**. Then select the required SKU from **Size of host** and specify the **Number of hosts** for the cluster. **Prices listed in image are for illustration only.**

We do not allow the mixing of AV36, AV36P, or AV52 SKUs within the same cluster. We only allow the addition of AV64 clusters to existing private clouds that are built with the AV36, AV36P, or AV52 SKUs in certain regions. For more information.

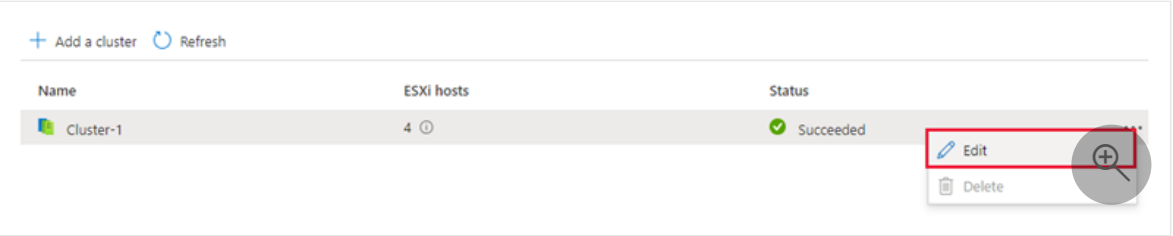


2. The deployment of the new cluster will begin.

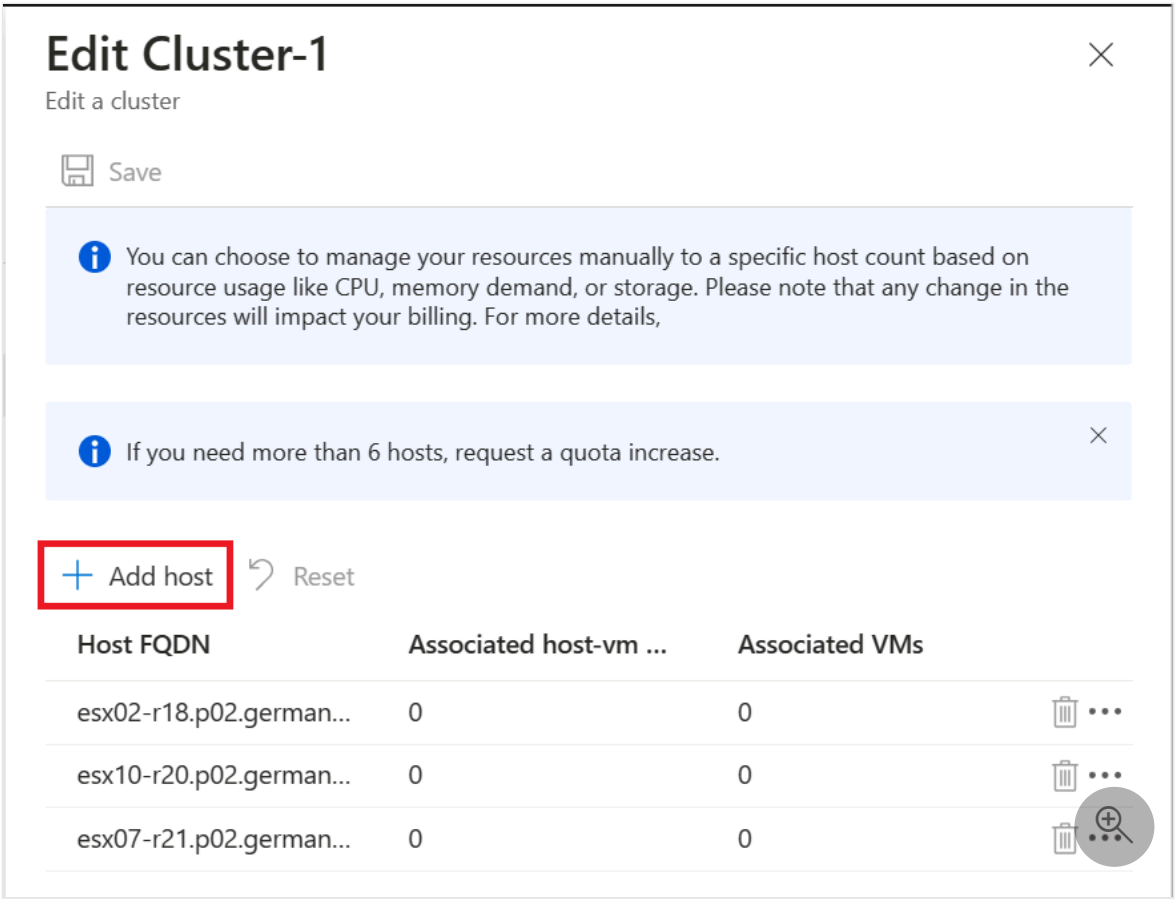
Scale a cluster

1. In your Azure VMware Solution private cloud, under **Manage**, select **Clusters**.

2. Select the cluster you want to scale, select **More** (...), then select **Edit**.



3. Select **Add Host** to add a host to the cluster. Repeat that to reach the desired number of hosts, and then select **Save**.



The addition of hosts to the cluster begins.

> **Note**
>
> The hosts will be added to the cluster in parallel.

Next steps

If you require another Azure VMware Solution private cloud, create another private cloud following the same networking prerequisites, cluster, and host limits.

Tutorial: Delete an Azure VMware Solution private cloud

Article • 02/21/2024

If you have an Azure VMware Solution private cloud that you no longer need, you can delete it. The private cloud includes:

- An isolated network domain
- One or more provisioned vSphere clusters on dedicated server hosts
- Several virtual machines (VMs)

When you delete a private cloud, all VMs, their data, clusters, and network address space provisioned get deleted. The dedicated Azure VMware Solution hosts are securely wiped and returned to the free pool.

> **⊗ Caution**
>
> Deleting the private cloud terminates all running workloads and components and is an irreversible operation. Once you delete the private cloud, you cannot recover the data.

Prerequisites

If you require the VMs and their data later, make sure to back up the data before you delete the private cloud. Unfortunately, there's no way to recover the VMs and their data.

Delete the private cloud

1. Access the Azure VMware Solutions console in the Azure portal.

   > **ⓘ Note**
   >
   > If you need access to the Azure US Gov portal, go to https://portal.azure.us/

2. Select the private cloud you want to delete.

3. Enter the name of the private cloud and select **Yes**.

> **Note**
>
> The deletion process takes a few hours to complete. The Delete icon is at the top of the Azure VMware Solution private cloud and Overview section in the portal. Selecting Delete requires you to add the private cloud name and reason to delete.

ESUs for SQL Server and Windows Server in Azure VMware Solution VMs

Article • 07/09/2024

This article describes how to enable Extended Security Updates (ESUs) and continue to run software that has reached its end-of-support lifecycle in Azure VMware Solution. ESUs allow older versions of software to run in a supported manner by continuing to receive security updates and critical patches. In Azure, which includes Azure VMware Solution, ESUs are free of charge for extra years after their end of support. For more information on timelines, see Extended Security Updates for SQL Server and Windows Server.

The following sections describe how to configure SQL Server and Windows Server virtual machines (VMs) for no-cost ESUs in Azure VMware Solution. The process is distinct to the Azure VMware Solution private cloud architecture.

Configure SQL Server and Windows Server for ESUs in Azure VMware Solution

In this section, you learn how to configure the VMs that run SQL Server and Windows Server for ESUs at no cost in Azure VMware Solution.

SQL Server

For SQL Server environments that run in a VM in Azure VMware Solution, you can use ESUs enabled by Azure Arc to configure ESUs and automate patching.

First, you need to Azure Arc-enable VMware vSphere for Azure VMware Solution. The Azure Extension for SQL Server must be installed on the VM.

1. Azure Arc-enable the VMware vSphere in Azure VMware Solution. Follow the steps in Deploy Azure Arc-enabled VMware vSphere for Azure VMware Solution private cloud.

2. Enable guest management for the individual VMs that run SQL Server. Make sure the Azure Extension for SQL Server is installed. To confirm that the extension is installed, see the section View ESU subscription status.

> ⚠ **Warning**

If you register SQL Server instances in a different manner from the preceding steps, the VM won't be registered as part of Azure VMware Solution. As a result, you will be billed for ESUs.

After you Azure Arc-enable the VMware vSphere in Azure VMware Solution and enable guest management, you can subscribe to ESUs by updating the SQL Server configuration on the Azure Arc-enabled VM.

To find the SQL Server configuration from the Azure portal:

1. In the Azure VMware Solution portal, go to **vCenter Server Inventory** and **Virtual Machines** by clicking through one of the Azure Arc-enabled VMs. The **Machine-Azure Arc (AVS)** page appears.
2. On the left pane, under **Operations**, select **SQL Server Configuration**.
3. Follow the steps in the section Configure SQL Server enabled by Azure Arc - Modify SQL Server configuration. This section also provides syntax to configure by using Azure PowerShell or the Azure CLI.

View ESU subscription status

For machines that run SQL Server where guest management is enabled, the Azure Extension for SQL Server must be registered. You can confirm that the extension is installed by using the Azure portal or Azure Resource Graph queries.

- Use the Azure portal:

    1. In the Azure VMware Solution portal, go to **vCenter Server Inventory** and **Virtual Machines** by clicking through one of the Azure Arc-enabled VMs. The **Machine-Azure Arc (AVS)** page appears.
    2. As part of the **Overview** section on the left pane, the **Properties/Extensions** view lists the `WindowsAgent.SqlServer` (*Microsoft.HybridCompute/machines/extensions*), if installed. Alternatively, you can expand **Settings** on the left pane and select **Extensions**. The `WindowsAgent.SqlServer` name and type appear, if installed.

    If you don't see the extension installed you can manually install by choosing **Extensions**, the Add button, and Azure Extension for SQL Server.

- Use Azure Resource Graph queries:
    - You can use the query VM ESU subscription status as an example to show that you can view eligible SQL Server ESU instances and their ESU subscription status.

Windows Server

To enable ESUs for Windows Server environments that run in VMs in Azure VMware Solution, contact Microsoft Support for configuration assistance.

When you contact Support, raise the ticket under the Azure VMware Solution category. Your ticket requires the following information:

- Customer name and tenant ID
- Number of VMs you want to register
- OS versions
- ESU year of coverage (for example, Year 1, Year 2, or Year 3). See ESU Availability and End Dates for ESU End Date and Year. The support ticket provides you with ESU keys for one year. You'll need to raise a new support request for other years. It's recommended to raise a new request as your current ESU End Date Year date is approaching.

> ⚠ **Warning**
>
> If you create ESU licenses for Windows through Azure Arc, you're charged for the ESUs.

Related content

- What are Extended Security Updates - SQL Server
- Extend Security Updates for Windows Server overview
- Plan your Windows Server and SQL Server end of support

Feedback

Was this page helpful? Yes No

Provide product feedback

License SQL Server, Windows Server, and Linux in Azure VMware Solution

Article • 05/29/2024

This article provides licensing considerations and tooling integration for running SQL Server, Windows Server, and Linux within Azure VMware Solution.

Included in the pricing of Azure VMware Solution is infrastructure, hosts, storage, and many VMware licensing components. These components include NSX-T, vSphere, vSAN, and HCX Advanced. There's no added charge in the pricing for any software running in your guest virtual machines (VMs).

To remain compliant, you need to license the software running in the VMs. For SQL Server, Windows Server, and Linux subscriptions, you can use your existing licenses and apply them in Azure VMware Solution.

With Software Assurance or an active Linux subscription, you can also take advantage of Azure Hybrid Benefit for other benefits around migration and unlimited virtualization.

> **Note**
>
> If you don't have Software Assurance, you need to apply the terms for licensing that are provided in Updated Microsoft licensing terms for dedicated hosted cloud services. These terms limit the licenses that can be applied based on terms applied after October 1, 2019, and other migration and virtualization benefits.

The remainder of this article discusses SQL Server and Windows Server licensing considerations in Azure VMware Solution with Software Assurance and Azure Hybrid Benefit applied.

> **Important**
>
> The Microsoft Product Terms for specific programs and software take precedence over this article and might contain more content specific to that product. For more information, select your specific program under:
>
> -SQL Server Product Terms
>
> -Windows Server Product Terms

-Azure Product Terms

Type of licenses

You can use the following licenses for SQL Server and Windows Server to apply to software running in Azure VMware Solution:

- **Windows Server**: Standard or Datacenter core licenses or Standard/Datacenter processor licenses, where each processor license is equivalent to 16 core licenses.
- **SQL Server**: Standard or Enterprise core licenses.

Dual-use rights for Azure Migration

Migration to Azure VMware Solution is usually executed over an extended time-frame instead of at a single point in time. To give you flexibility around your migration timelines, you can continue to use your licenses outside of Azure for 180 days from the time when the licenses are allocated within Azure VMware Solution. This dual-use rights benefit applies to SQL Server and Windows Server.

For more information and other considerations for dual-use rights outside of migration, see Azure Product Terms .

License the host physical cores by using unlimited virtualization rights

Unlimited virtualization allows you to license the physical cores on the host and run as many VMs with Windows Server or SQL Server as you can. You're limited only by host capacity. Unlimited virtualization can provide licensing cost optimization for the following scenarios:

- The host contains a high density of VMs.
- The host contains dynamic provisioning or deprovisioning of VMs.

By applying existing SQL Server Enterprise or Windows Server Datacenter licenses to cover the physical cores of any host, you can achieve unlimited virtualization of that host. Each host is required to have licenses applied to all the physical cores.

Standard licenses for SQL Server and Windows Server can't be used for unlimited virtualization, but they can be applied to license an individual VM. This use is discussed in the next section.

License a virtual machine based on virtual cores

You need to license each machine individually by applying licenses based on the number of virtual cores associated with the VM.

Either Enterprise or Standard licenses can be applied for SQL Server. Standard and Datacenter licenses can be applied for Windows.

Applying licenses at the VM scope could meet your needs for the following scenarios:

- The hosts aren't densely packed with VMs running the respective software. The overall licensing cost in this case could be more cost effective than licensing an entire host.
- You're running Standard editions of SQL Server or Windows Server, so you have these existing licenses to apply.

Each VM requires a minimum number of licenses to be applied:

- **Windows Server**: You need a minimum of 8 core licenses (Datacenter or Standard) per VM. For example, 8 core licenses are still required if you run a 4-core VM. You might also run VMs larger than 8 cores by allocating licenses equal to the core size of the VM. For example, 12 core licenses are required for a 12-core VM.
- **SQL Server**: A minimum of 4 core licenses (Enterprise or Standard) per VM.

Register licenses in Azure VMware Solution

Register your licenses in Azure VMware Solution.

SQL Server

You can register and manage your licenses with SQL Server.

License the host by using unlimited virtualization

You can enable Azure Hybrid Benefit for SQL Server and achieve unlimited virtualization through an Azure VMware Solution placement policy. For information on how to create the VM-Host placement policy, see Enable unlimited virtualization with Azure Hybrid Benefit for SQL Server in Azure VMware Solution.

License a virtual machine

You can register SQL Server licenses and apply them to VMs running SQL Server in Azure VMware Solution by registering through Azure Arc:

1. Azure VMware Solution must be Azure Arc-enabled. For more information, see Deploy Azure Arc-enabled VMware vSphere for Azure VMware Solution. You can Azure Arc-enable the VMs and install extensions to that VM by following the steps provided in the section titled "Enable guest management and extension installation."

2. When **Guest Management** is configured, the Azure Extension for SQL Server should be installed on that VM. The extension installation enables you to configure the license type for the SQL Server instance running in the VM.

3. Now you can configure the license type and other SQL Server configuration settings by using the Azure portal, PowerShell, or the Azure CLI for a specific Azure Arc-enabled server. To configure from the Azure portal with VMware vSphere in the Azure VMware Solution experience, follow these steps:
   a. In the Azure VMware Solution portal, go to **vCenter Server Inventory** and **Virtual Machines** by clicking through one of the Azure Arc-enabled VMs. The **Machine-Azure Arc (AVS)** page appears.
   b. On the left pane, under **Operations**, select **SQL Server Configuration**.
   c. You can now apply and save your license type for the VM along with other server configurations.

You can also configure these settings within the Azure Arc portal experience and by using PowerShell or the Azure CLI. To access the Azure Arc portal experience and code to update the configuration values, see Configure SQL Server enabled by Azure Arc.

For available license types, see License types.

> **Note**
>
> At this time, Azure VMware Solution doesn't have support for the new `SQLServerLicense` resource type.

Manage the environment

After the Azure Extension for SQL Server is installed, you can query the SQL Server configuration settings and track your SQL Server license inventory for each VM. For sample queries, see Query SQL Server configuration.

Windows Server

Currently, there's no way to register your Windows licenses in Azure VMware Solution.

Other cost savings for SQL Server and Windows Server

For more cost savings with Azure VMware Solution, see:

- Extended Security Updates (ESUs) for Windows Server and SQL Server - Azure VMware Solution
- Save costs with a reserved instance

Related content

- Azure Hybrid Benefit
- Azure VMware Solution pricing

Enable unlimited virtualization with Azure Hybrid Benefit for SQL Server in Azure VMware Solution

Article • 05/23/2024

In this article, you learn how to enable unlimited virtualization through Azure Hybrid Benefit for SQL Server in an Azure VMware Solution private cloud. You can register the licenses by configuring a placement policy. The placement policy defines the hosts and the virtual machines (VMs) on the hosts that are running SQL Server.

> **Important**
>
> SQL Server licenses are applied at the host level and must cover all the physical cores on a host. For example, if each host in Azure VMware Solution has 36 cores and you intend to have 2 hosts run SQL Server, the Azure Hybrid Benefit applies to 72 cores. This amount is regardless of the number of SQL Server instances or other VMs that are on that host.

View a video tutorial for configuring Azure Hybrid Benefit for SQL Server in Azure VMware Solution.

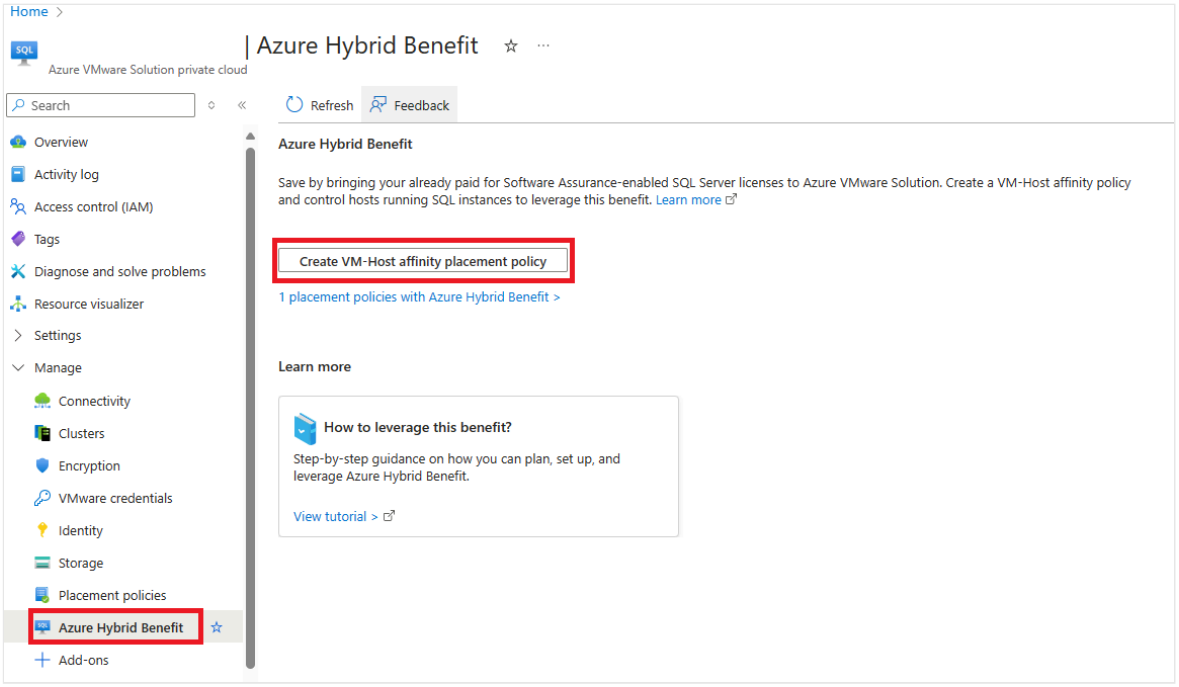
Configure VM-Host placement policy

You can configure the VM-Host placement policy to enable Azure Hybrid Benefit for SQL Server by using the Azure CLI or the Azure portal.

To enable by using the Azure CLI, see az vmware placement-policy vm-host.

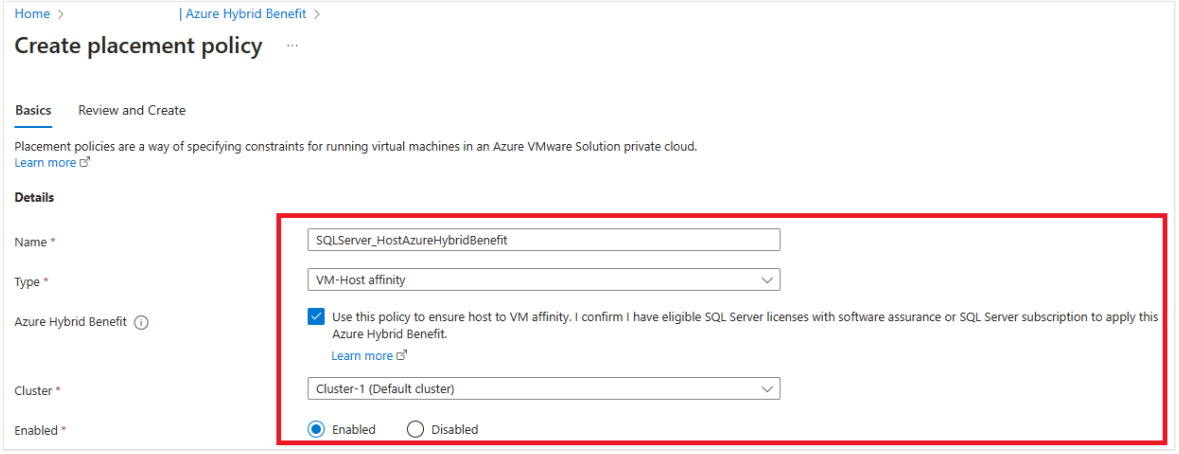
To use the Azure portal:

1. From your Azure VMware Solution private cloud, select **Azure Hybrid Benefit** > **Create VM-Host affinity placement policy**.



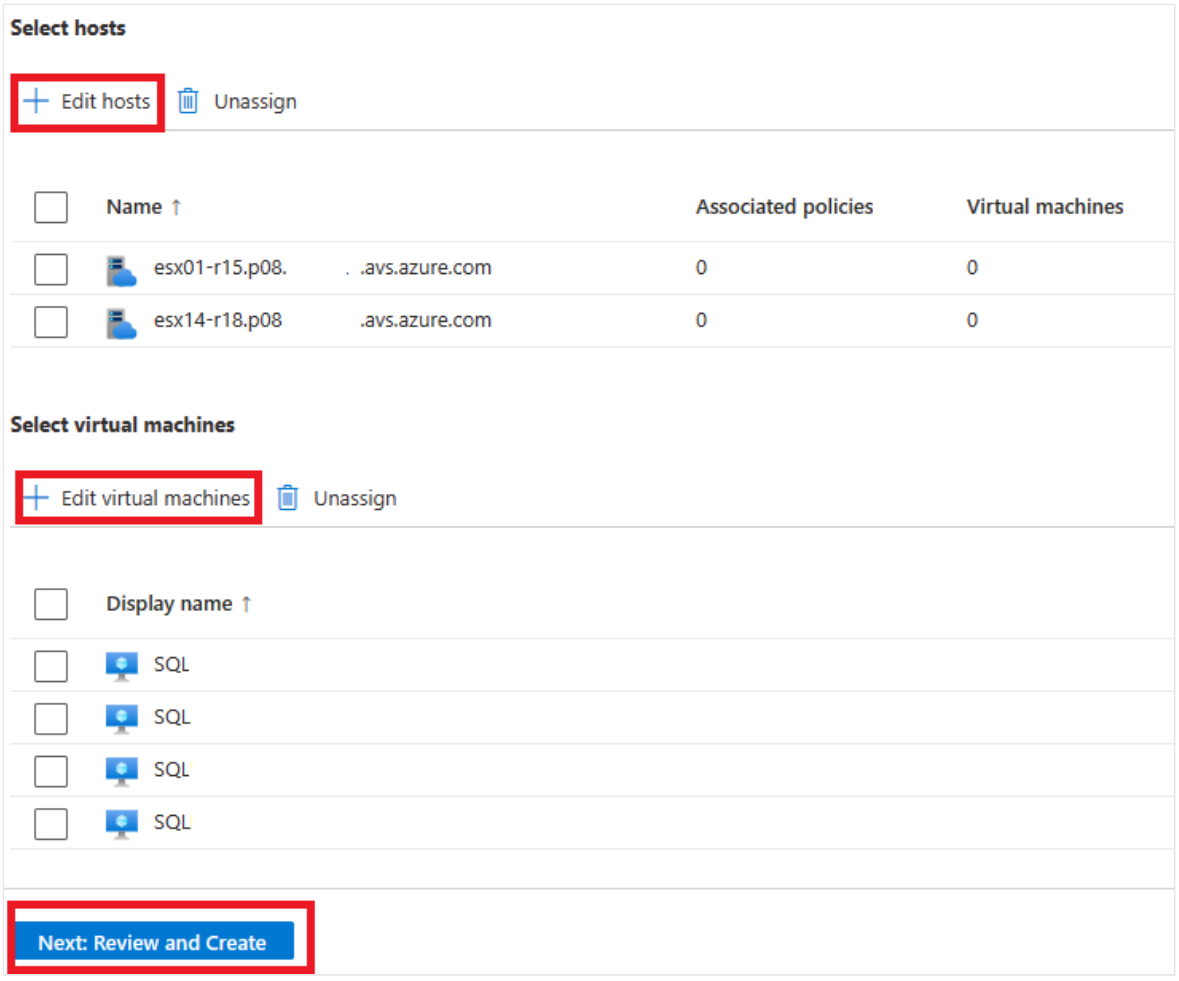
2. Fill in the required fields for creating the placement policy:

- **Name**: Select the name that identifies this policy.
- **Type**: Select the type of policy. This type must be a VM-Host affinity rule only.
- **Azure Hybrid Benefit**: Select the checkbox to apply Azure Hybrid Benefit for SQL Server.
- **Cluster**: Select the correct cluster. The policy is scoped to host in this cluster only.
- **Enabled**: Select **Enabled** to apply the policy immediately after creation.



3. Select the hosts and VMs to be applied to the VM-Host affinity policy:

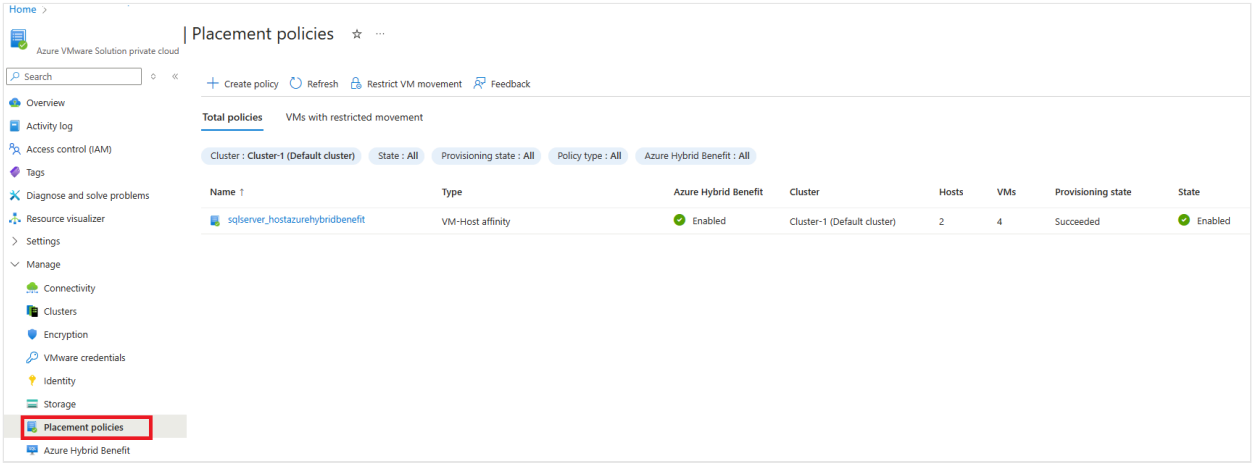
- **Select hosts**: Select the hosts to run SQL Server. When hosts are replaced, policies are re-created on the new hosts automatically.
- **Select virtual machines**: Select the VMs that should run on the selected hosts.
- **Review and Create**: Select to create the policy.



Manage placement policies

After you create the placement policy, you can review, manage, or edit the policy by using options on the **Placement policies** menu in the Azure VMware Solution private cloud.

When you select the Azure Hybrid Benefit checkbox in the configuration setting, you can enable existing VM-Host affinity policies with Azure Hybrid Benefit for SQL Server.



Related content

- Azure Hybrid Benefit
- az vmware placement-policy vm-host

Save costs with reserved instances in Azure VMware Solution

Article • 05/23/2024

When you commit to a reserved instance of Azure VMware Solution, you save money. The reservation discount automatically applies to the running Azure VMware Solution hosts that match the reservation scope and attributes. In addition, a reserved instance purchase covers only the compute part of your usage and includes software licensing costs.

Purchase restriction considerations

Reserved instances are available with some exceptions:

- **Clouds**: Reservations are available only in the regions listed on the Products available by region page.
- **Insufficient quota**: A reservation scoped to a single or shared subscription must have hosts quota available in the subscription for the new reserved instance. You can create a quota increase request to resolve this issue.
- **Offer eligibility**: You need an Azure Enterprise Agreement (EA) with Microsoft.
- **Capacity restrictions**: In rare circumstances, Azure limits the purchase of new reservations for Azure VMware Solution host SKUs because of low capacity in a region.

Buy a reservation

You can buy a reserved instance of an Azure VMware Solution host instance in the Azure portal.

You can pay for the reservation upfront or with monthly payments.

These requirements apply to buying a reserved dedicated host instance:

- To buy a reservation, you must have the owner role or reservation purchaser role on an Azure subscription.
- For EA subscriptions, you must enable the **Add Reserved Instances** option in the EA portal. If disabled, you must be an EA Admin for the subscription to enable it.
- For a subscription under a Cloud Solution Provider (CSP) Azure plan, the partner must purchase the customer's reserved instances in the Azure portal.

Buy reserved instances for an EA subscription

1. Sign in to the Azure portal.
2. Select **All services** > **Reservations**.
3. Select **Purchase Now**, and then select **Azure VMware Solution**.
4. Enter the required fields. The selected attributes that match running Azure VMware Solution hosts qualify for the reservation discount. Attributes include the SKU, regions (where applicable), and scope. Reservation scope selects where the reservation savings apply.

   If you have an EA agreement, you can use the **Add more option** to add instances quickly. The option isn't available for other subscription types.

Expand table

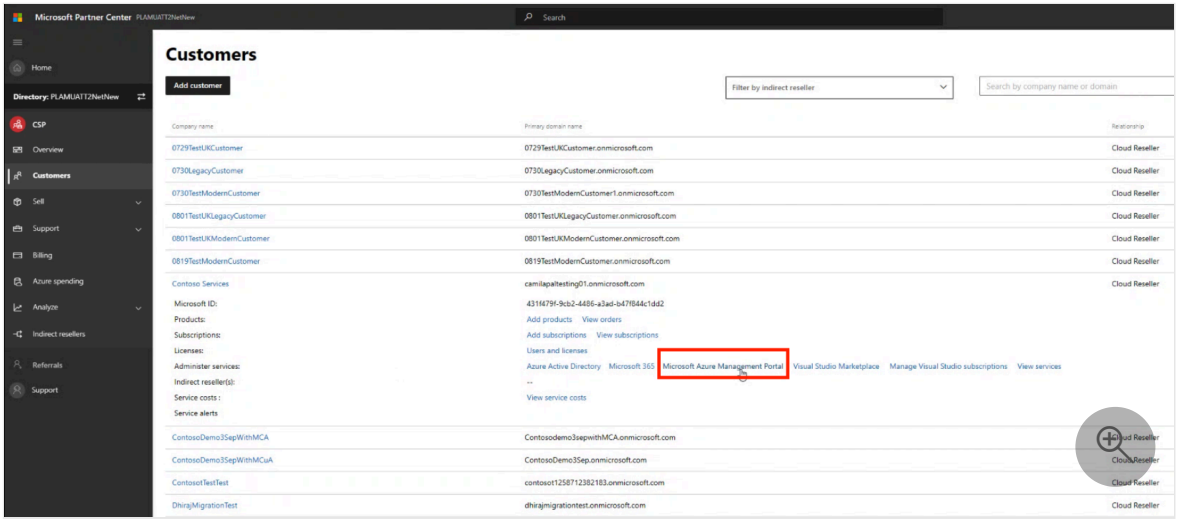
Field	Description
Subscription	The subscription used to pay for the reservation. The payment method on the subscription is charged the costs for the reservation. The subscription type must be an EA (offer numbers MS-AZR-0017P or MS-AZR-0148P), Microsoft Customer Agreement, or an individual subscription with pay-as-you-go rates (offer numbers MS-AZR-0003P or MS-AZR-0023P). The charges are deducted from the Azure Prepayment (previously called monetary commitment) balance, if available, or charged as overage. For a subscription with pay-as-you-go rates, the charges are billed to the subscription's credit card or an invoice payment method.
Scope	The reservation's scope can cover one subscription or multiple subscriptions (shared scope). If you select: • **Single resource group scope**: Applies the reservation discount to the matching resources in the selected resource group only. • **Single subscription scope**: Applies the reservation discount to the matching resources in the selected subscription. • **Shared scope**: Applies the reservation discount to matching resources in eligible subscriptions that are in the billing context. For EA customers, the billing context is the enrollment. Therefore, the billing scope is all eligible subscriptions created by the account administrator for individual subscriptions with pay-as-you-go rates. • **Management group**: Applies the reservation discount to the matching resource in the list of subscriptions that are a part of both the management group and billing scope.
Region	The Azure region covered by the reservation.

Field	Description
Host size	AV36
Term	One year or three years.
Quantity	The number of instances to purchase within the reservation. The quantity is the number of running Azure VMware Solution hosts that can get the billing discount.

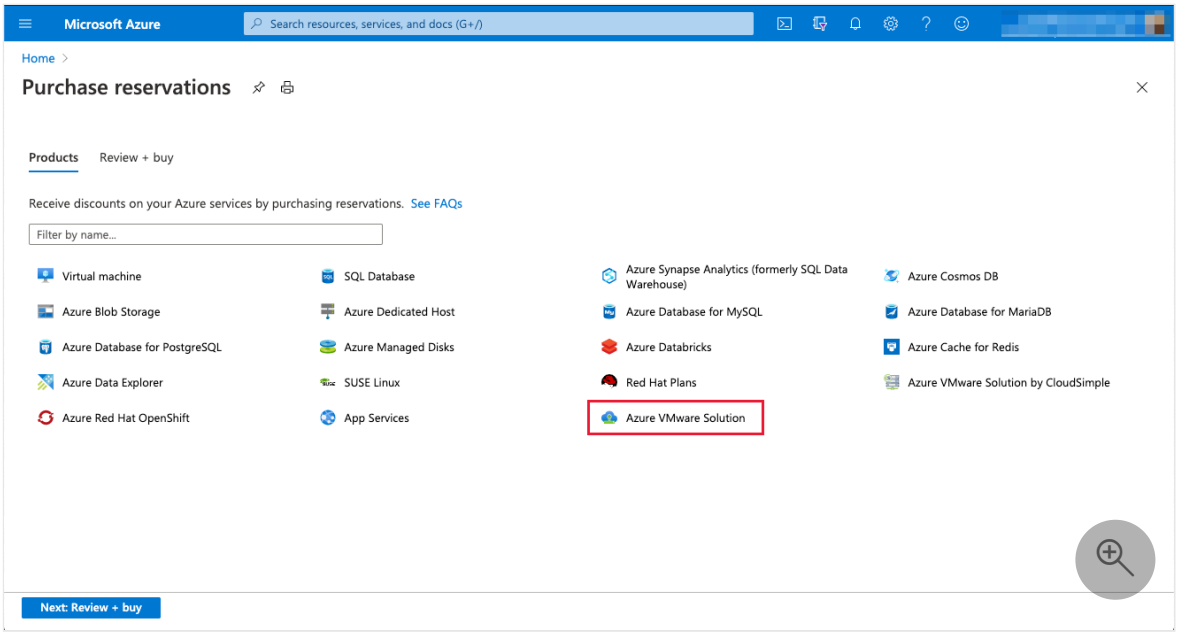
Buy reserved instances for a CSP subscription

CSPs that want to purchase reserved instances for their customers must use the **Admin On Behalf Of** procedure from the Partner Center documentation. For more information, view the Admin On Behalf Of video.

1. Sign in to Partner Center.
2. Select **CSP** to access the **Customers** pane.
3. Expand customer details and select **Microsoft Azure Management Portal**.



4. In the Azure portal, select **All services** > **Reservations**.
5. Select **Purchase Now** and then select **Azure VMware Solution**.



6. Enter the required fields. The selected attributes that match running Azure VMware Solution hosts qualify for the reservation discount. Attributes include the SKU, regions (where applicable), and scope. Reservation scope selects where the reservation savings apply.

Expand table

Field	Description
Subscription	The subscription that funds the reservation. The payment method on the subscription is charged the costs for the reservation. The subscription type must be an eligible one, which in this case is a CSP subscription.
Scope	The reservation's scope can cover one subscription or multiple subscriptions (shared scope). If you select: • **Single resource group scope**: Applies the reservation discount to the matching resources in the selected resource group only. • **Single subscription scope**: Applies the reservation discount to the matching resources in the selected subscription. • **Shared scope**: Applies the reservation discount to matching resources in eligible subscriptions that are in the billing context. For EA customers, the billing context is the enrollment. Therefore, the billing scope is all eligible subscriptions created by the account administrator for individual subscriptions with pay-as-you-go rates. • **Management group**: Applies the reservation discount to the matching resource in the list of subscriptions that are a part of both the management group and billing scope.
Region	The Azure region covered by the reservation.
Host size	AV36

Field	Description
Term	One year or three years.
Quantity	The number of instances to purchase within the reservation. The quantity is the number of running Azure VMware Solution hosts that can get the billing discount.

To learn more about viewing the purchased reservations for your customer, see View Azure reservations as a Cloud Solution Provider (CSP).

Usage data and reservation usage

Your usage that gets a reservation discount has an effective price of zero. You can see which Azure VMware Solution instance received the reservation discount for each reservation.

For more information about how reservation discounts appear in usage data:

- For EA customers, see Understand Azure reservation usage for your EA enrollment.
- For individual subscriptions, see Understand Azure reservation usage for your pay-as-you-go subscription.

Change a reservation after purchase

You can make these changes to a reservation after purchase:

- Update reservation scope
- Instance size flexibility (if applicable)
- Ownership

You can also split a reservation into smaller chunks or merge reservations. None of the changes causes a new commercial transaction or changes the end date of the reservation.

For more information about CSP-managed reservations, see Sell Azure reservations to customers by using Partner Center, the Azure portal, or APIs.

> **Note**
>
> After you purchase your reservation, you won't be able to make these types of changes directly:

- An existing reservation's region
- SKU
- Quantity
- Duration

However, you can *exchange* a reservation if you want to make changes.

Cancel, exchange, or refund reservations

You can cancel, exchange, or refund reservations with certain limitations. For more information, see Self-service exchanges and refunds for Azure reservations. *Azure VMware Solution reservations don't fall into this category, so the new exchange rules don't apply.*

CSPs can cancel, exchange, or refund reservations, with certain limitations, purchased for their customer. For more information, see Manage, cancel, exchange, or refund Azure reservations for customers.

Related content

Now that you covered reserved instances of Azure VMware Solution, learn how to:

- Create an Azure VMware Solution assessment
- Configure DHCP for Azure VMware Solution
- Integrate Azure native services in Azure VMware Solution

Azure Hybrid Benefit for Windows Server, SQL Server, and Linux subscriptions

Article • 12/20/2023

Azure Hybrid Benefit is a cost-saving offering from Microsoft you can use to save on cost while optimizing your hybrid environment by applying your existing Windows Server, SQL Server licenses, and Linux subscriptions.

- Save up to 85% over standard pay-as-you-go rate using Windows Server and SQL Server licenses with Azure Hybrid Benefit.
- Use Azure Hybrid Benefit in Azure SQL platform as a service (PaaS) environment.
- Apply to SQL Server one to four vCPUs exchange: For every one core of SQL Server Enterprise Edition, you get four vCPUs of Azure SQL Managed Instance or Azure SQL Database general purpose and Hyperscale tiers, or 4 vCPUs of SQL Server Standard edition on Azure VMs.
- Use existing SQL Server licensing to adopt Azure Arc–enabled SQL Server Managed Instance.
- Help meet compliance requirements with unlimited virtualization on Azure Dedicated Host and the Azure VMware Solution.
- Get 180 days of dual-use rights between on-premises and Azure.

Microsoft SQL Server

Microsoft SQL Server is a core component of many business-critical applications currently running on VMware vSphere. It's one of the most widely used database platforms in the market with customers running hundreds of SQL Server instances with VMware vSphere on-premises.

Azure VMware Solution is an ideal solution for customers looking to migrate and modernize their vSphere-based applications to the cloud, including their SQL Server databases.

Microsoft SQL Server Enterprise licenses are required for each Azure VMware Solution ESXi host core that is used by SQL Server workloads running in a cluster. This can be further reduced by configuring the Azure Hybrid Benefit feature within Azure VMware Solution, using placement policies to limit the scope of ESXi host cores that need to be licensed within a cluster.

Next steps

Now that you learned Azure Hybrid benefit, consider learning more about:

- Migrate Microsoft SQL Server Standalone to Azure VMware Solution
- Migrate SQL Server failover cluster to Azure VMware Solution
- Migrate Microsoft SQL Server Always-On Availability Group to Azure VMware Solution
- Enable SQL Azure hybrid benefit for Azure VMware Solution
- Configure Windows Server Failover Cluster on Azure VMware Solution vSAN

Use VMware Cloud Foundations (VCF) license portability on Azure VMware Solution

Article • 10/02/2024

This article discusses how to modernize your VMware workloads by bringing your VMware Cloud Foundations (VCF) entitlements to Azure VMware Solutions and take advantage of incredible cost savings as you modernize your VMware workloads. With Azure VMware Solution, you access both the physical infrastructure and the licensing entitlements for the entire VMware software-defined datacenter (SDDC) stack, including vSphere, ESXi, NSX networking, NSX Firewall, and HCX. With the new VCF license portability option, you can apply your on-premises VCF entitlements, purchased from Broadcom, directly to the Azure VMware Solution infrastructure. This flexibility means you can seamlessly integrate your VMware assets into a fully managed, state-of-the-art Azure environment, maximizing efficiency and cutting costs. Upgrade with confidence and experience the power and flexibility of Azure VMware Solution today!

What's changing?

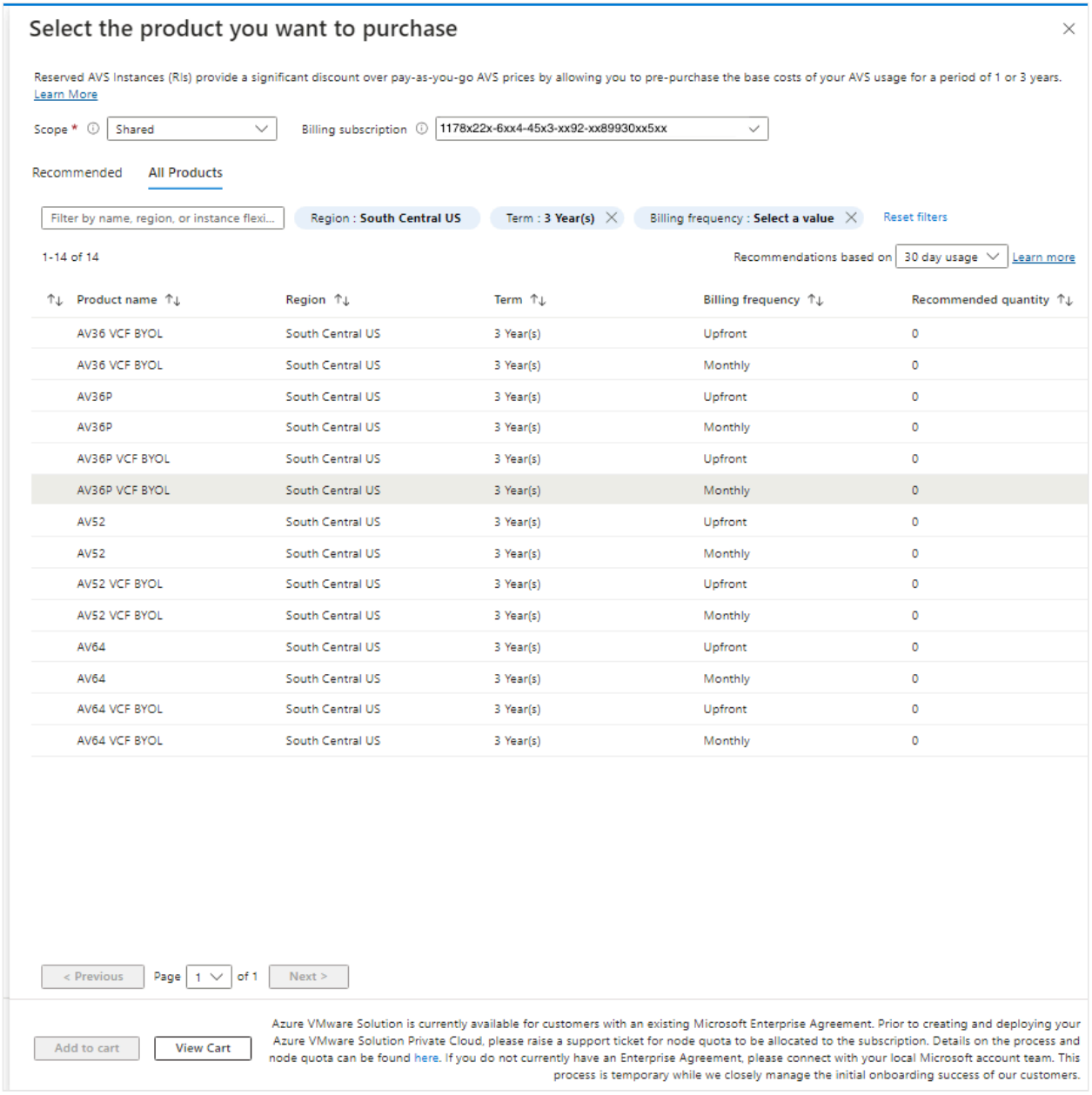
Private Cloud on the VCF license portability offering, must have prepurchase Firewall add-on from Broadcom along with the VCF subscription to use the vDefend Firewall on Azure VMware Solution. Prior to using the vDefend Firewall software on Azure VMware Solution ensure you register your Firewall add-on with Microsoft. For detailed instructions on how to register your VCF license, see "Register your VCF license with Azure VMware Solution" later in this article.

> **ⓘ Important**
>
> VCF portable licenses are applied at the host level and must cover all the physical cores on a host. For example, if each host in Azure VMware Solution has 36 cores and you intend to have a Private Cloud with 3 nodes, the VCF portable license must cover 108 (3*36) cores. In the current version, if you want to use your own license on an Azure subscription for the Azure VMware Solution workloads, all the nodes (cores) in that subscription including multiple Private Clouds need to be purchased through Broadcom and covered under your Broadcom VCF license portability contract. At the moment, you're required to bring VCF license entitlements that cover cores for all the nodes deployed within your Azure Subscription.

Purchasing VCF license portability offering on Azure VMware Solution

We offer three flexible commitments and pricing options for using your own VCF license on Azure VMware Solution. You can choose from pay-as-you-go, 1-year Reserved Instance (RI), and 3-year RI options.

To take advantage of the Reserved Instance (RI) pricing for the VCF license portability offering, purchase an RI under the Product Name- VCF BYOL. For example, if your private cloud uses AV36P nodes, you must purchase the Reserved Instance for the Product Name- AV36P VCF BYOL. To use the pay-as-you-go pricing for the VCF license portability offering, you only need to register your VCF license.



Request host quota with VCF license portability

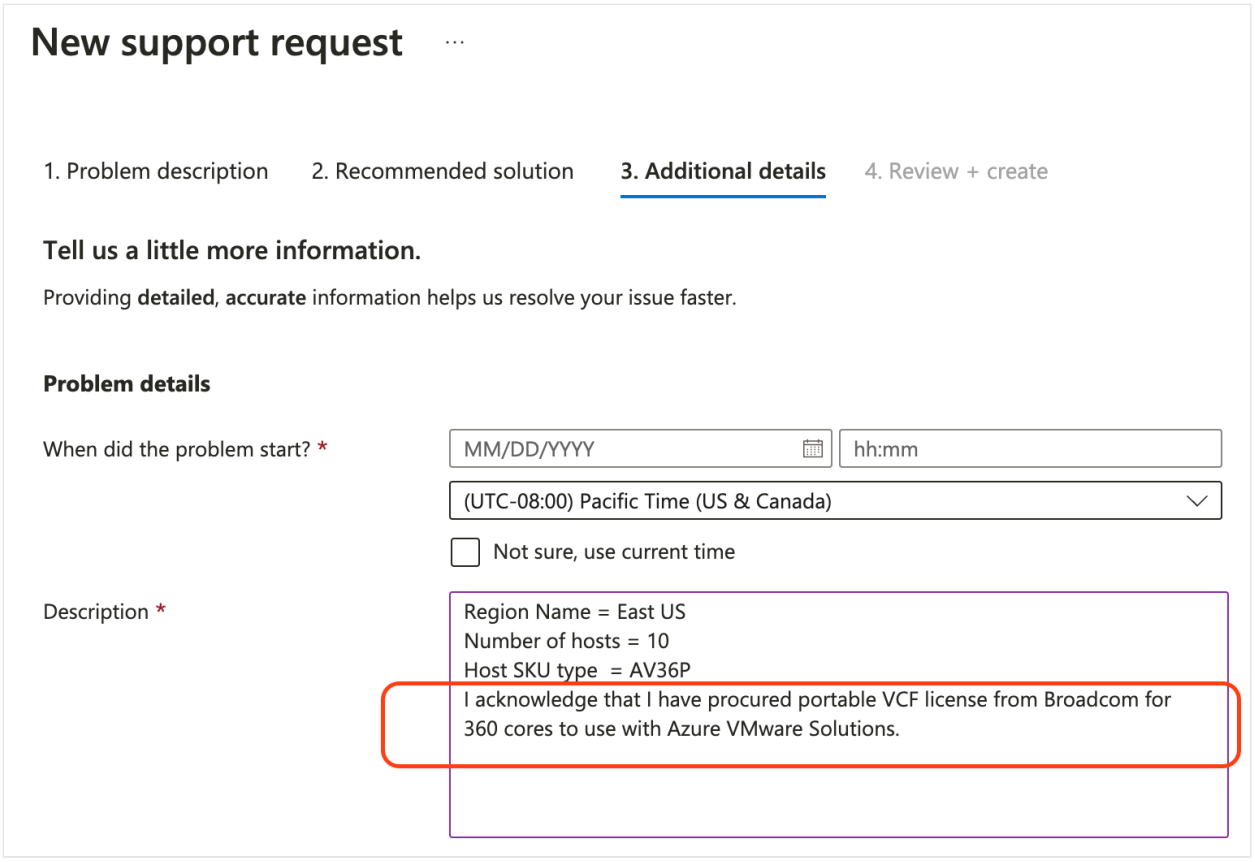
Existing:

1. In the Azure portal under **Help + Support**, create a New support request and provide the following information:
    - Issue type: Technical
    - Subscription: Select your subscription
    - Service: All services > Azure VMware Solution
    - Resource: General question
    - Summary: Need capacity
    - Problem type: AVS Quota Request
2. In the **Description** of the support ticket, on the **Details** tab, provide information for:
    - Region Name
    - Number of hosts
    - Host SKU type
    - Any other details

    Note: Azure VMware Solution requires a minimum of three hosts and recommends redundancy of N+1 hosts.
3. Select **Review + Create** to submit the request.

To request quota for VCF license portability offering, provide the following additional information in the **Description** of the support ticket:

- Region Name
- Number of hosts
- Host SKU type
- Add the following statement as is, by replacing "N" with the "Number of VCF BYOL cores" you purchased from Broadcom for license portability to Azure VMware Solutions:
  "I acknowledge that I have procured portable VCF license from Broadcom for "N" cores to use with Azure VMware Solutions."
- Any other details, including Availability Zone requirements for integrating with other Azure services; for example, Azure NetApp Files, Azure Blob Storage



> **Note**
>
> VCF portable license is applied at the host level and must cover all the physical cores on a host. Hence, quota will be approved only for the maximum number of nodes which the VCF portable license covers. For example, if you have purchased 1000 cores for portability and requesting for AV36P, you can get a maximum of 27 nodes quota approved for your subscription.
>
> That is, 36 physical CPU cores per AV36P node. 27 nodes = 27*36 = 972 cores. 28 nodes = 28*36 = 1008 cores. If you have purchased 1000 cores for portability, you can only use up to 27 AV36P nodes under your portable VCF.

Register your VCF license with Azure VMware Solution

To get your quota request approved, you must first register the VCF portable license details with Microsoft. Quota will be approved only after the entitlements are provided. Expect to receive a response in 1 to 2 business days.

How to register the VCF license keys

- Email your VCF license entitlements (and VMware vDefender Firewall license entitlements if to enable vDefender Firewall on Azure VMware Solution) to the following email address: registeravsvcfbyol@microsoft.com.
- VCF entitlement sample:

Line #	SKU/ Covered Products	Product Description	Qty	Start Date / End Date	Install – At Customer Number
1	VCF-CLD-FND-5	VMware Cloud Foundations	400	05-JUN-24/ 04-JUN-27	XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

> ⓘ **Note**
>
> The "Qty" represents the number of cores eligible for VCF license portability. Your quota request should not surpass the number of nodes equivalent to your entitled cores from Broadcom. If your quota request exceeds the approved cores, the quota request will be granted only for the number of nodes that are fully covered by the entitled cores.

- VCF with VMware vDefend entitlement sample:

Line #	SKU/ Covered Products	Product Description	Qty	Start Date / End Date	Install – At Customer Number
1	VCF-CLD-FND-5	VMware Cloud Foundations	400	05-JUN-24/ 04-JUN-27	XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
2	ANS-VMW-FW-B	VMware vDefend Firewall	400**	05-JUN-24/ 04-JUN-27	XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

Sample Email to register portable VCF entitlements:

Subject: VCF BYOL registration - <Your-Azure-Subscription-ID>

Aptos 11

Subscription ID: <Your-Azure-Subscription-ID>
Number of cores: 16
License entitlement: XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

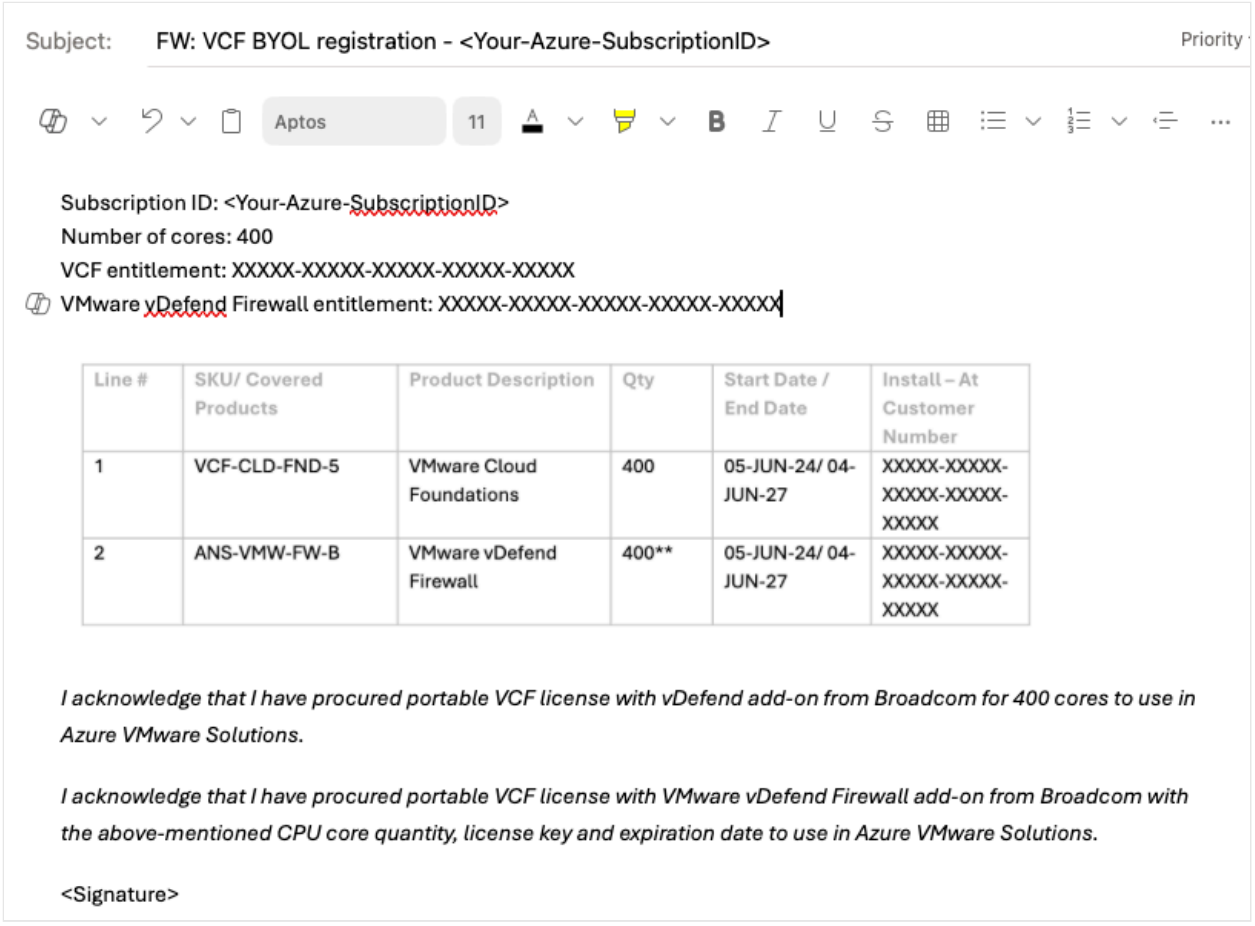
Line #	SKU/ Covered Products	Product Description	Qty	Start Date / End Date	Install – At Customer Number
1	VCF-CLD-FND-5	VMware Cloud Foundations	400	05-JUN-24/ 04-JUN-27	XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

I acknowledge that I have procured portable VCF license from Broadcom for 16 cores to use in Azure VMware Solutions.

<Signature>

The VMware vDefend Firewall add-on CPU cores required on Azure VMware Solution depend on the planned feature usage:

- For NSX Distributed Firewall: same core count as VCF core count.
- For NSX Gateway Firewall, it would be 64 cores (with default NSX Edges).
- For both NSX Distributed and Gateway firewall, it should be combined core count of both.



Subject: FW: VCF BYOL registration - <Your-Azure-SubscriptionID> Priority

Aptos 11

Subscription ID: <Your-Azure-SubscriptionID>
Number of cores: 400
VCF entitlement: XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
VMware vDefend Firewall entitlement: XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

Line #	SKU/ Covered Products	Product Description	Qty	Start Date / End Date	Install – At Customer Number
1	VCF-CLD-FND-5	VMware Cloud Foundations	400	05-JUN-24/ 04-JUN-27	XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
2	ANS-VMW-FW-B	VMware vDefend Firewall	400**	05-JUN-24/ 04-JUN-27	XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

I acknowledge that I have procured portable VCF license with vDefend add-on from Broadcom for 400 cores to use in Azure VMware Solutions.

I acknowledge that I have procured portable VCF license with VMware vDefend Firewall add-on from Broadcom with the above-mentioned CPU core quantity, license key and expiration date to use in Azure VMware Solutions.

<Signature>

> **Note**
>
> The VCF license entitlements submitted to Microsoft will be securely retained for our reporting purpose. You can request the permanent deletion of this data from Microsoft's systems at any time. Once the automated validation process is in place, your data will be automatically deleted from all Microsoft systems, which may take up to 120 days. Additionally, all your VCF entitlement data will be permanently deleted within 120 days any time you migrate to an Azure VMware Solution-owned VCF solution.

Creating/scaling a Private Cloud

You can create your Azure VMware Solution Private Cloud the same way as today regardless of your licensing method, that is, whether you bring your own VCF portable license or use the Azure VMware Solution-owned VCF license. Learn more. Your decision of licensing is a cost optimization choice and doesn't affect your deployment workflow.

For example, you want to deploy 10 nodes of AV36P node type.

Scenario 1: "I want to purchase my VCF subscription from Broadcom and use the license portability offering on Azure VMware Solution."

1. Create quota request for AV36P nodes. Declare your own VCF portable license intent and the number of cores you're entitled for portability.
2. Register your VCF entitlements via email to Microsoft.
3. Optional- to use the Reserved Instance pricing purchase AV36P VCF BYOL Reserved Instance. You can skip this step to use the pay-as-you-go pricing for the VCF license portability.
4. Create your Private Cloud with AV36P nodes.

Scenario 2: "I want to let Azure VMware Solution manage my license for all my Azure VMware Solution private cloud."

1. Create quota request for AV36P node type.
2. Optional- Purchase AV36P Reserved Instance.
3. Create your Private Cloud with AV36P nodes.

Moving between the two VCF licensing methods

If you're currently managing your own VCF licensing for Azure VMware Solution and wish to transition to Azure VMware Solution-owned licensing, you can easily make the switch without any changes to your Private Cloud.

Steps:

1. Create a support request to inform us of your intent to convert.
2. Exchange RI- If you have any active RI with VCF BYOL, exchange them for non-VCF BYOL RI. For instance, you can exchange your AV36P VCF BYOL RI for an AV36P.

If you're an existing Azure VMware Solution customer using Azure VMware Solution-owned licensing deployments and wish to transition to the license portability (VCF BYOL) offering, you can also easily make the switch without any changes to your Private Cloud deployments by registering your VCF entitlements with Microsoft.

> **Note**
>
> You need to purchase the VCF entitlements from Broadcom for all cores that match your current Azure VMware Solution deployment. For instance, if your Azure subscription has a Private Cloud with 100 AV36P nodes, you must purchase VCF subscription for atleast 3600 cores from Broadcom to convert to VCF BYOL offering.

Feedback

Azure VMware Solution private cloud and cluster concepts

Article • 09/20/2024

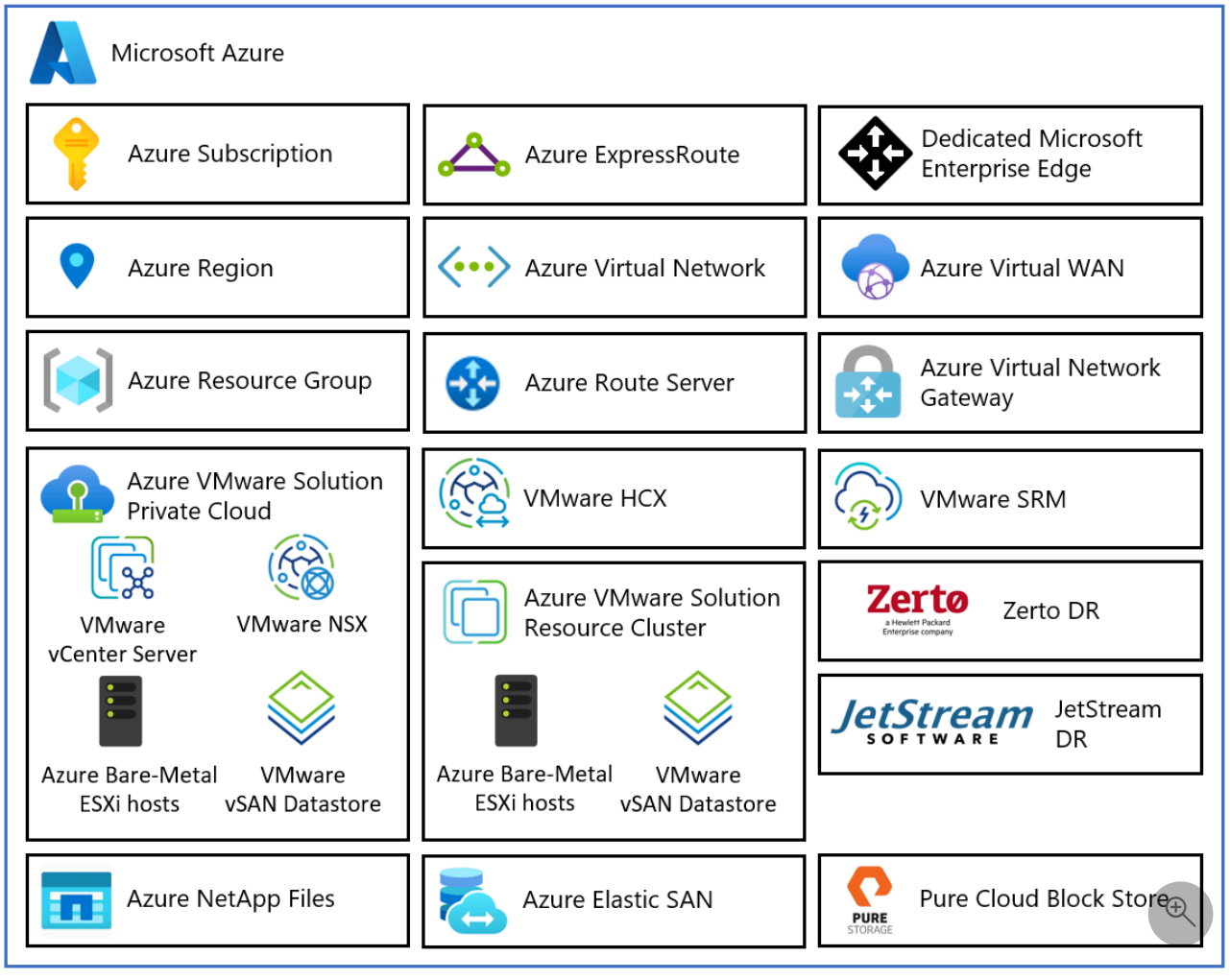
Azure VMware Solution provides VMware-based private clouds in Azure. The private cloud hardware and software deployments are fully integrated and automated in Azure. Deploy and manage the private cloud through the Azure portal, CLI, or PowerShell.

A private cloud includes clusters with:

- Dedicated bare-metal server hosts provisioned with VMware ESXi hypervisor
- VMware vCenter Server for managing ESXi and vSAN
- VMware NSX software-defined networking for vSphere workload VMs
- VMware vSAN datastore for vSphere workload VMs
- VMware HCX for workload mobility
- Resources in the Azure underlay (required for connectivity and to operate the private cloud)

Private clouds are installed and managed within an Azure subscription. The number of private clouds within a subscription is scalable. Initially, there's a limit of one private cloud per subscription. There's a logical relationship between Azure subscriptions, Azure VMware Solution private clouds, vSAN clusters, and hosts.

The following diagram describes the architectural components of the Azure VMware Solution.



Each Azure VMware Solution architectural component has the following function:

- Azure Subscription: Provides controlled access, budget, and quota management for the Azure VMware Solution.
- Azure Region: Groups data centers into Availability Zones (AZs) and then groups AZs into regions.
- Azure Resource Group: Places Azure services and resources into logical groups.
- Azure VMware Solution Private Cloud: Offers compute, networking, and storage resources using VMware software, including vCenter Server, NSX software-defined networking, vSAN software-defined storage, and Azure bare-metal ESXi hosts. Azure NetApp Files, Azure Elastic SAN, and Pure Cloud Block Store are also supported.
- Azure VMware Solution Resource Cluster: Provides compute, networking, and storage resources for customer workloads by scaling out the Azure VMware Solution private cloud using VMware software, including vSAN software-defined storage and Azure bare-metal ESXi hosts. Azure NetApp Files, Azure Elastic SAN, and Pure Cloud Block Store are also supported.
- VMware HCX: Delivers mobility, migration, and network extension services.
- VMware Site Recovery: Automates disaster recovery and storage replication services with VMware vSphere Replication. Third-party disaster recovery solutions Zerto Disaster Recovery and JetStream Software Disaster Recovery are also supported.
- Dedicated Microsoft Enterprise Edge (D-MSEE): Router that connects Azure cloud and the Azure VMware Solution private cloud instance.
- Azure Virtual Network (VNet): Connects Azure services and resources together.
- Azure Route Server: Exchanges dynamic route information with Azure networks.
- Azure Virtual Network Gateway: Connects Azure services and resources to other private networks using IPSec VPN, ExpressRoute, and VNet to VNet.
- Azure ExpressRoute: Provides high-speed private connections between Azure data centers and on-premises or colocation infrastructure.
- Azure Virtual WAN (vWAN): Combines networking, security, and routing functions into a single unified Wide Area Network (WAN).

Hosts

Azure VMware Solution clusters are based upon hyper-converged infrastructure. The following table shows the CPU, memory, disk and network specifications of the host.

Expand table

Host Type	CPU (Cores/GHz)	RAM (GB)	vSAN Cache Tier (TB, raw***)	vSAN Capacity Tier (TB, raw***)	Regional availability
AV36	Dual Intel Xeon Gold 6140 CPUs (Skylake microarchitecture) with 18 cores/CPU @ 2.3 GHz, Total 36 physical cores (72 logical cores with hyperthreading)	576	3.2 (NVMe)	15.20 (SSD)	Selected regions (*)
AV36P	Dual Intel Xeon Gold 6240 CPUs (Cascade Lake microarchitecture) with 18 cores/CPU @ 2.6 GHz / 3.9 GHz Turbo, Total 36 physical cores (72 logical cores with hyperthreading)	768	1.5 (Intel Cache)	19.20 (NVMe)	Selected regions (*)

Host Type	CPU (Cores/GHz)	RAM (GB)	vSAN Cache Tier (TB, raw***)	vSAN Capacity Tier (TB, raw***)	Regional availability
AV52	Dual Intel Xeon Platinum 8270 CPUs (Cascade Lake microarchitecture) with 26 cores/CPU @ 2.7 GHz / 4.0 GHz Turbo, Total 52 physical cores (104 logical cores with hyperthreading)	1,536	1.5 (Intel Cache)	38.40 (NVMe)	Selected regions (*)
AV64	Dual Intel Xeon Platinum 8370C CPUs (Ice Lake microarchitecture) with 32 cores/CPU @ 2.8 GHz / 3.5 GHz Turbo, Total 64 physical cores (128 logical cores with hyperthreading)	1,024	3.84 (NVMe)	15.36 (NVMe)	Selected regions (**)

An Azure VMware Solution cluster requires a minimum number of three hosts. You can only use hosts of the same type in a single Azure VMware Solution private cloud. Hosts used to build or scale clusters come from an isolated pool of hosts. Those hosts passed hardware tests and had all data securely deleted before being added to a cluster.

All the above Host Types have 100 Gbps network interface throughput.

(*) details available via the Azure pricing calculator.

(**) AV64 Prerequisite: An Azure VMware Solution private cloud deployed with AV36, AV36P, or AV52 is required prior to adding AV64.

(***) Raw is based upon International Standard of Units (SI) reported by disk manufacturer. Example: 1 TB Raw = 1000000000000 bytes, space calculated by computer in binary (1TB binary = 1099511627776 bytes binary) would equal 931.3 Gigabytes converted from raw decimal.

Azure Region Availability Zone (AZ) to SKU mapping table

When planning your Azure VMware Solution design, use the following table to understand what SKUs are available in each physical Availability Zone of an Azure region.

> **Important**
>
> This mapping is important for placing your private clouds in close proximity to your Azure native workloads, including integrated services such as Azure NetApp Files and Pure Cloud Block Store (CBS).

The Multi-AZ capability for Azure VMware Solution Stretched Clusters is also tagged in the following table. Customer quota for Azure VMware Solution is assigned by Azure region, and you aren't able to specify the Availability Zone during private cloud provisioning. An auto selection algorithm is used to balance deployments across the Azure region. If you have a particular Availability Zone you want to deploy to, open a Service Request with Microsoft requesting a "special placement policy" for your subscription, Azure region, Availability Zone, and SKU type. This policy remains in place until you request it be removed or changed.

SKUs marked in **bold** are of limited availability due to customer consumption and quota may not be available upon request. The AV64 SKU should be used instead when AV36, AV36P, or AV52 SKUs are limited.

AV64 SKUs are available per Availability Zone, the table below lists the Azure regions that support this SKU. For RAID-6 FTT2 and RAID-1 FTT3 storage policies, six and seven Fault Domains (FDs) are needed respectively, the FD count for each Azure region is listed in the "AV64 FDs Supported" column.

Expand table

Azure region	Availability Zone	SKU	Multi-AZ SDDC	AV64 FDs Supported
Australia East	AZ01	AV36P, AV64	Yes	7
Australia East	AZ02	AV36, AV64	No	7
Australia East	AZ03	AV36P, AV64	Yes	7
Australia Southeast	AZ01	AV36	No	N/A
Brazil South	AZ02	**AV36**	No	N/A
Canada Central	AZ02	AV36 **AV36P,** AV64	No	7
Canada East	N/A	AV36	No	N/A
Central India	AZ03	AV36P (AV64 Planned H2 2024)	No	N/A (7 Planned H2 2024)
Central US	AZ01	AV36P (AV64 Planned H2 2024)	No	N/A (7 Planned H2 2024)
Central US	AZ02	**AV36** (AV64 Planned H2 2024)	No	N/A (7 Planned H2 2024)
Central US	AZ03	AV36P, AV64	No	7
East Asia	AZ01	AV36 (AV64 Planned H2 2024)	No	N/A (7 Planned H2 2024)
East US	AZ01	**AV36P**, AV64	Yes	7
East US	AZ02	**AV36P**, AV64	Yes	7
East US	AZ03	**AV36**, **AV36P**, AV64	Yes	7
East US 2	AZ01	**AV36**, AV64	No	7
East US 2	AZ02	AV36P, **AV52**, AV64	No	7
France Central	AZ01	**AV36** (AV64 Planned H2 2024)	No	N/A (7 Planned H2 2024)
Germany West Central	AZ01	AV36P (AV64 Planned H2 2024)	Yes	N/A (7 Planned H2 2024)
Germany West Central	AZ02	**AV36** (AV64 Planned H2 2024)	Yes	N/A (7 Planned H2 2024)

Azure region	Availability Zone	SKU	Multi-AZ SDDC	AV64 FDs Supported
Germany West Central	AZ03	AV36, **AV36P**, AV64	Yes	7
Italy North	AZ03	AV36P (AV64 Planned H2 2024)	No	N/A (7 Planned H2 2024)
Japan East	AZ02	**AV36** (AV64 Planned H2 2024)	No	N/A (7 Planned H2 2024)
Japan West	AZ01	**AV36** (AV64 Planned H2 2024)	No	N/A (7 Planned H2 2024)
North Central US	AZ01	**AV36**, AV64	No	7
North Central US	AZ02	AV36P, AV64	No	7
North Europe	AZ02	AV36, AV64	No	7
Qatar Central	AZ03	AV36P (AV64 Planned H2 2024)	No	N/A (7 Planned H2 2024)
South Africa North	AZ03	AV36 (AV64 Planned H2 2024)	No	N/A (7 Planned H2 2024)
South Central US	AZ01	AV36, AV64	No	7
South Central US	AZ02	**AV36P**, AV52, AV64	No	7
Southeast Asia	AZ02	**AV36**	No	N/A
Sweden Central	AZ01	AV36 (AV64 Planned H2 2024)	No	N/A (7 Planned H2 2024)
Switzerland North	AZ01	**AV36**, AV64	No	7
Switzerland North	AZ03	AV36P (AV64 Planned H2 2024)	No	N/A (7 Planned H2 2024)
Switzerland West	AZ01	**AV36**, AV64	No	7
UAE North	AZ03	AV36P	No	N/A
UK South	AZ01	AV36, AV36P, AV52, AV64	Yes	7
UK South	AZ02	**AV36**, AV64	Yes	7
UK South	AZ03	AV36P, AV64	Yes	7
UK West	AZ01	AV36	No	N/A
West Europe	AZ01	**AV36**, AV36P, AV52, AV64	Yes	7
West Europe	AZ02	**AV36**, AV64	Yes	7
West Europe	AZ03	AV36P, AV64	Yes	7
West US	AZ01	AV36, AV36P	No	N/A
West US 2	AZ01	AV36	No	N/A

Azure region	Availability Zone	SKU	Multi-AZ SDDC	AV64 FDs Supported
West US 2	AZ02	AV36P	No	N/A
West US 3	AZ01	**AV36P**	No	N/A
US Gov Arizona	AZ02	AV36P	No	N/A
US Gov Virginia	AZ03	AV36	No	N/A

Clusters

For each private cloud created, there's one vSAN cluster by default. You can add, delete, and scale clusters. The minimum number of hosts per cluster and the initial deployment is three.

You use vCenter Server and NSX Manager to manage most aspects of cluster configuration and operation. All local storage of each host in a cluster is under the control of VMware vSAN.

The Azure VMware Solution management and control plane have the following resource requirements that need to be accounted for during solution sizing of a **standard private cloud**.

Expand table

Area	Description	Provisioned vCPUs	Provisioned vRAM (GB)	Provisioned vDisk (GB)	Typical CPU Usage (GHz)	Typical vRAM Usage (GB)	Typical Raw vSAN Datastore Usage (GB)
VMware vSphere	vCenter Server	8	28	915	1.1	3.9	1,854
VMware vSphere	vSphere Cluster Service VM 1	1	0.1	2	0.1	0.1	5
VMware vSphere	vSphere Cluster Service VM 2	1	0.1	2	0.1	0.1	5
VMware vSphere	vSphere Cluster Service VM 3	1	0.1	2	0.1	0.1	5
VMware vSphere	ESXi node 1	N/A	N/A	N/A	5.1	0.2	N/A
VMware vSphere	ESXi node 2	N/A	N/A	N/A	5.1	0.2	N/A
VMware vSphere	ESXi node 3	N/A	N/A	N/A	5.1	0.2	N/A
VMware vSAN	vSAN System Usage	N/A	N/A	N/A	N/A	N/A	5,458
VMware NSX	NSX Unified Appliance	12	48	300	2.5	13.5	613

Area	Description	Provisioned vCPUs	Provisioned vRAM (GB)	Provisioned vDisk (GB)	Typical CPU Usage (GHz)	Typical vRAM Usage (GB)	Typical Raw vSAN Datastore Usage (GB)
	Node 1						
VMware NSX	NSX Unified Appliance Node 2	12	48	300	2.5	13.5	613
VMware NSX	NSX Unified Appliance Node 3	12	48	300	2.5	13.5	613
VMware NSX	NSX Edge VM 1	8	32	200	1.3	0.6	409
VMware NSX	NSX Edge VM 2	8	32	200	1.3	0.6	409
VMware HCX (Optional Add-On)	HCX Manager	4	12	65	1	2.5	140
VMware Site Recovery Manager (Optional Add-On)	SRM Appliance	4	12	33	1	1	79
VMware vSphere (Optional Add-On)	vSphere Replication Manager Appliance	4	8	33	1	0.6	75
VMware vSphere (Optional Add-On)	vSphere Replication Server Appliance	2	1	33	1	0.3	68
	Total	77 vCPUs	269.3 GB	2,385 GB	30 GHz	50.4 GB	10,346 GB (9,032 GB with expected 1.2x Data Reduction ratio)

The Azure VMware Solution management and control plane have the following resource requirements that need to be accounted for during solution sizing of a **stretched clusters private cloud**. VMware SRM isn't included in the table since it currently isn't supported.

Expand table

Area	Description	Provisioned vCPUs	Provisioned vRAM (GB)	Provisioned vDisk (GB)	Typical CPU Usage (GHz)	Typical vRAM Usage (GB)	Typical Raw vSAN Datastore Usage (GB)
VMware vSphere	vCenter Server	8	28	915	1.1	3.9	3,708
VMware vSphere	vSphere Cluster Service VM 1	1	0.1	2	0.1	0.1	5
VMware vSphere	vSphere Cluster Service VM 2	1	0.1	2	0.1	0.1	5
VMware vSphere	vSphere Cluster Service VM 3	1	0.1	2	0.1	0.1	5
VMware vSphere	ESXi node 1	N/A	N/A	N/A	5.1	0.2	N/A
VMware vSphere	ESXi node 2	N/A	N/A	N/A	5.1	0.2	N/A
VMware vSphere	ESXi node 3	N/A	N/A	N/A	5.1	0.2	N/A
VMware vSphere	ESXi node 4	N/A	N/A	N/A	5.1	0.2	N/A
VMware vSphere	ESXi node 5	N/A	N/A	N/A	5.1	0.2	N/A
VMware vSphere	ESXi node 6	N/A	N/A	N/A	5.1	0.2	N/A
VMware vSAN	vSAN System Usage	N/A	N/A	N/A	N/A	N/A	10,722
VMware NSX	NSX Unified Appliance Node 1	12	48	300	2.5	13.5	1,229
VMware NSX	NSX Unified Appliance Node 2	12	48	300	2.5	13.5	1,229
VMware NSX	NSX Unified Appliance Node 3	12	48	300	2.5	13.5	1,229
VMware NSX	NSX Edge VM 1	8	32	200	1.3	0.6	817
VMware NSX	NSX Edge VM 2	8	32	200	1.3	0.6	817
VMware HCX	HCX Manager	4	12	65	1	2.5	270

Area	Description	Provisioned vCPUs	Provisioned vRAM (GB)	Provisioned vDisk (GB)	Typical CPU Usage (GHz)	Typical vRAM Usage (GB)	Typical Raw vSAN Datastore Usage (GB)
(Optional Add-On)							
	Total	67 vCPUs	248.3 GB	2,286 GB	42.3 GHz	49.1 GB	20,036 GB (17,173 GB with expected 1.2x Data Reduction ratio)

These resource requirements only apply to the first cluster deployed in an Azure VMware Solution private cloud. Subsequent clusters only need to account for the vSphere Cluster Service, ESXi resource requirements and vSAN System Usage in solution sizing.

The virtual appliance **Typical Raw vSAN Datastore Usage** values account for the space occupied by virtual machine files, including configuration and log files, snapshots, virtual disks and swap files.

The VMware ESXi nodes have compute usage values that account for the vSphere VMkernel hypervisor overhead, vSAN overhead and NSX distributed router, firewall and bridging overhead. These are estimates for a standard three cluster configuration. The storage requirements are listed as not applicable (N/A) since a boot volume separate from the vSAN Datastore is used.

The VMware vSAN System Usage storage overhead accounts for vSAN performance management objects, vSAN file system overhead, vSAN checksum overhead and vSAN deduplication and compression overhead. To view this consumption, select the Monitor, vSAN Capacity object for the vSphere Cluster in the vSphere Client.

The VMware HCX and VMware Site Recovery Manager resource requirements are optional Add-ons to the Azure VMware Solution service. Discount these requirements in the solution sizing if they aren't being used.

The VMware Site Recovery Manager Add-On has the option of configuring multiple VMware vSphere Replication Server Appliances. The previous table assumes one vSphere Replication Server appliance is used.

Sizing an Azure VMware Solution is an estimate; the sizing calculations from the design phase should be validated during the testing phase of a project to ensure the Azure VMware Solution is sized correctly for the application workload.

> **Tip**
>
> You can always extend the cluster and add additional clusters later if you need to go beyond the initial deployment number.

The following table describes the maximum limits for Azure VMware Solution.

Expand table

Resource	Limit
vSphere clusters per private cloud	12
Minimum number of ESXi hosts per cluster	3 (hard-limit)
Maximum number of ESXi hosts per cluster	16 (hard-limit)
Maximum number of ESXi hosts per private cloud	96
Maximum number of vCenter Servers per private cloud	1 (hard-limit)
Maximum number of HCX site pairings	25 (any edition)
Maximum number of HCX service meshes	10 (any edition)
Maximum number of Azure VMware Solution ExpressRoute linked private clouds from a single location to a single Virtual Network Gateway	4 The virtual network gateway used determines the actual max linked private clouds. For more information, see About ExpressRoute virtual network gateways If you exceed this threshold use Azure VMware Solution Interconnect to aggregate private cloud connectivity within the Azure region.
Maximum Azure VMware Solution ExpressRoute port speed	10 Gbps (use Ultra Performance Gateway SKU with FastPath enabled) The virtual network gateway used determines the actual bandwidth. For more information, see About ExpressRoute virtual network gateways
Maximum number of Azure Public IPv4 addresses assigned to NSX	2,000
Maximum number of Azure VMware Solution Interconnects per private cloud	10
Maximum number of Azure ExpressRoute Global Reach connections per Azure VMware Solution private cloud	8
vSAN capacity limits	75% of total usable (keep 25% available for SLA)
VMware Site Recovery Manager - Maximum number of protected Virtual Machines	3,000
VMware Site Recovery Manager - Maximum number of Virtual Machines per recovery plan	2,000
VMware Site Recovery Manager - Maximum number of protection groups per recovery plan	250
VMware Site Recovery Manager - RPO Values	5 min or higher * (hard-limit)
VMware Site Recovery Manager - Maximum number of virtual machines per protection group	500
VMware Site Recovery Manager - Maximum number of recovery plans	250

* For information about Recovery Point Objective (RPO) lower than 15 minutes, see How the 5 Minute Recovery Point Objective Works in the *vSphere Replication Administration guide*.

For other VMware-specific limits, use the VMware configuration maximum tool.

VMware software versions

Microsoft is a member of the VMware Metal-as-a-Service (MaaS) program and uses the VMware Cloud Provider Stack (VCPS) for Azure VMware Solution upgrade planning.

The VMware solution software versions used in new deployments of Azure VMware Solution private clouds are:

Expand table

Software	Version
VMware vCenter Server	8.0 U2b
VMware ESXi	8.0 U2b
VMware vSAN	8.0 U2
VMware vSAN on-disk format	19
VMware vSAN storage architecture	OSA
VMware NSX	4.1.1
VMware HCX	4.9.1
VMware Site Recovery Manager	8.8.0.3
VMware vSphere Replication	8.8.0.3

The current running software version is applied to new clusters added to an existing private cloud, if the vCenter Server version supports it.

Host maintenance and lifecycle management

One benefit of Azure VMware Solution private clouds is that the platform is maintained for you. Microsoft is responsible for the lifecycle management of VMware software (ESXi, vCenter Server, and vSAN) and NSX appliances. Microsoft is also responsible for bootstrapping the network configuration, like creating the Tier-0 gateway and enabling North-South routing. You're responsible for the NSX SDN configuration: network segments, distributed firewall rules, Tier 1 gateways, and load balancers.

> **Note**
>
> A T0 gateway is created and configured as part of a private cloud deployment. Any modification to that logical router or the NSX edge node VMs could affect connectivity to your private cloud and should be avoided.

Microsoft is responsible for applying any patches, updates, or upgrades to ESXi, vCenter Server, vSAN, and NSX in your private cloud. The impact of patches, updates, and upgrades on ESXi, vCenter Server, and NSX has the following considerations:

- **ESXi** - There's no impact to workloads running in your private cloud. Access to vCenter Server and NSX isn't blocked during this time. During this time, we recommend you don't plan other activities like: scaling up private cloud, scheduling or initiating active HCX migrations, making HCX configuration changes, and so on, in your private cloud.
- **vCenter Server** - There's no impact to workloads running in your private cloud. During this time, vCenter Server is unavailable and you can't manage VMs (stop, start, create, or delete). We recommend you don't plan other activities like scaling up private cloud, creating new networks, and so on, in your private cloud. When you use VMware Site Recovery Manager or vSphere Replication user interfaces, we recommend you don't do either of the actions: configure vSphere Replication, and configure or execute site recovery plans during the vCenter Server upgrade.
- **NSX** - The workload is impacted. When a particular host is being upgraded, the VMs on that host might lose connectivity from 2 seconds to 1 minute with any of the following symptoms:
  - Ping errors
  - Packet loss
  - Error messages (for example, *Destination Host Unreachable* and *Net unreachable*)

  During this upgrade window, all access to the NSX management plane is blocked. You can't make configuration changes to the NSX environment for the duration. Your workloads continue to run as normal, subject to the upgrade impact previously detailed.

  During the upgrade time, we recommend you don't plan other activities like, scaling up private cloud, and so on, in your private cloud. Other activities can prevent the upgrade from starting or could have adverse impacts on the upgrade and the environment.

You're notified through Azure Service Health that includes the timeline of the upgrade. This notification also provides details on the upgraded component, its effect on workloads, private cloud access, and other Azure services. You can reschedule an upgrade as needed.

Software updates include:

- **Patches** - Security patches or bug fixes released by VMware
- **Updates** - Minor version change of a VMware stack component
- **Upgrades** - Major version change of a VMware stack component

> ⓘ **Note**
>
> Microsoft tests a critical security patch as soon as it becomes available from VMware.

Documented VMware workarounds are implemented in lieu of installing a corresponding patch until the next scheduled updates are deployed.

Host monitoring and remediation

Azure VMware Solution continuously monitors the health of both the VMware components and underlay. When Azure VMware Solution detects a failure, it takes action to repair the failed components. When Azure

VMware Solution detects a degradation or failure on an Azure VMware Solution node, it triggers the host remediation process.

Host remediation involves replacing the faulty node with a new healthy node in the cluster. Then, when possible, the faulty host is placed in VMware vSphere maintenance mode. VMware vSphere vMotion moves the VMs off the faulty host to other available servers in the cluster, potentially allowing zero downtime for live migration of workloads. If the faulty host can't be placed in maintenance mode, the host is removed from the cluster. Before the faulty host is removed, the customer workloads are migrated to a newly added host.

> **Tip**
>
> **Customer communication:** An email is sent to the customer's email address before the replacement is initiated and again after the replacement is successful.
>
> To receive emails related to host replacement, you need to be added to any of the following Azure RBAC roles in the subscription: 'ServiceAdmin', 'CoAdmin', 'Owner', 'Contributor'.

Azure VMware Solution monitors the following conditions on the host:

- Processor status
- Memory status
- Connection and power state
- Hardware fan status
- Network connectivity loss
- Hardware system board status
- Errors occurred on the disk(s) of a vSAN host
- Hardware voltage
- Hardware temperature status
- Hardware power status
- Storage status
- Connection failure

Alert Codes and Remediation Table

Expand table

Error Code	Error Details	Recommended Action
EPC_SCSIDEVICE_SHARINGMODE	This error is encountered when a Virtual Machine is configured to use a device that prevents a maintenance operation: A	Follow the KB article for the removal of any SCSI controller engaged in bus-sharing attached to VMs https://knowledge.broadcom.com/external/article?legacyId=79910

Error Code	Error Details	Recommended Action
	device that is a SCSI controller which is engaged in bus-sharing	
EPC_CDROM_EMULATEMODE	This error is encountered when CD-ROM on the Virtual Machine uses emulate mode, whose ISO image is not accessible	Follow the KB article for the removal of any CDROM mounted on customer's workload Virtual Machines in emulate mode or detach ISO. It is recommended to use Passthrough mode for mounting any CD-ROM. https://knowledge.broadcom.com/external/article?legacyId=79306
EPC_DATASTORE_INACCESSIBLE	This error is encountered when any external Datastore attached to AVS Private Cloud becomes inaccessible	Follow the KB article for the removal of any stale Datastore attached to cluster /azure/azure-vmware/attach-azure-netapp-files-to-azure-vmware-solution-hosts?tabs=azure-portal#performance-best-practices
EPC_NWADAPTER_STALE	This error is encountered when connected Network interface on the Vitual Machine uses network adapter which becomes inaccessible	Follow the KB article for the removal of any stale N/W adapters attached to Virtual Machines https://knowledge.broadcom.com/external/article/318738/troubleshooting-the-migration-compatibil.html

Note

Azure VMware Solution tenant admins must not edit or delete the previously defined VMware vCenter Server alarms because they are managed by the Azure VMware Solution control plane on vCenter Server. These alarms are used by Azure VMware Solution monitoring to trigger the Azure VMware Solution host remediation process.

Backup and restore

Azure VMware Solution private cloud vCenter Server and HCX Manager (if enabled) configurations are on a daily backup schedule and NSX configuration has an hourly backup schedule. The backups are retained for a minimum of three days. Open a support request in the Azure portal to request restoration.

> **Note**
>
> Restorations are intended for catastrophic situations only.

Azure VMware Solution continuously monitors the health of both the physical underlay and the VMware Solution components. When Azure VMware Solution detects a failure, it takes action to repair the failed components.

Next steps

Now that you've covered Azure VMware Solution private cloud concepts, you might want to learn about:

- Azure VMware Solution networking and interconnectivity concepts
- Azure VMware Solution storage concepts
- How to enable Azure VMware Solution resource

Feedback

Design vSAN stretched clusters

Article • 06/04/2024

In this article, learn how to design a vSAN stretched cluster for an Azure VMware Solution private cloud.

Background

Azure's global infrastructure is broken up into Regions. Each region supports the services for a given geography. Within each region, Azure builds isolated, and redundant islands of infrastructure called availability zones (AZ). An AZ acts as a boundary for resource management. The compute and other resources available to an AZ are finite and can become exhausted by customer demands. An AZ is built to be independently resilient, meaning failures in one AZ doesn't affect other AZs.

With Azure VMware Solution, ESXi hosts deployed in a standard vSphere cluster traditionally reside in a single Azure Availability Zone (AZ) and are protected by vSphere high availability (HA). However, it doesn't protect the workloads against an Azure AZ failure. To protect against an AZ failure, a single vSAN cluster can be enabled to span two separate availability zones, called a vSAN stretched cluster.

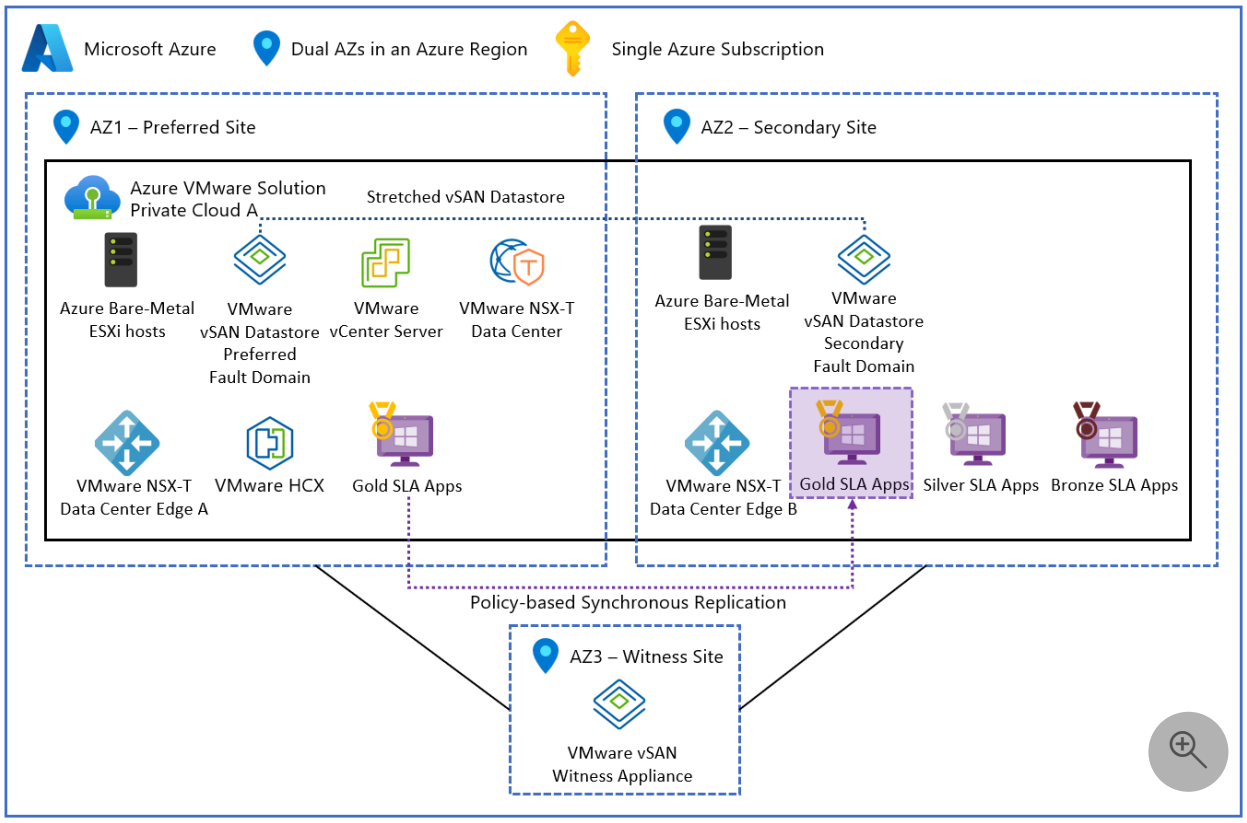
Stretched clusters allow the configuration of vSAN Fault Domains across two AZs to notify vCenter Server that hosts reside in each Availability Zone (AZ). Each fault domain is named after the AZ it resides within to increase clarity. When you stretch a vSAN cluster across two AZs within a region, should an AZ go down, it's treated as a vSphere HA event and the virtual machine is restarted in the other AZ.

Stretched cluster benefits:

- Improve application availability.
- Provide a zero recovery point objective (RPO) capability for enterprise applications without needing to redesign them, or deploy expensive disaster recovery (DR) solutions.
- A private cloud with stretched clusters is designed to provide 99.99% availability due to its resilience to AZ failures.
- Enable customers to focus on core application requirements and features, instead of infrastructure availability.

To protect against split-brain scenarios and help measure site health, a managed vSAN Witness is created in a third AZ. With a copy of the data in each AZ, vSphere HA attempts to recover from any failure using a simple restart of the virtual machine.

The following diagram depicts a vSAN cluster stretched across two AZs.



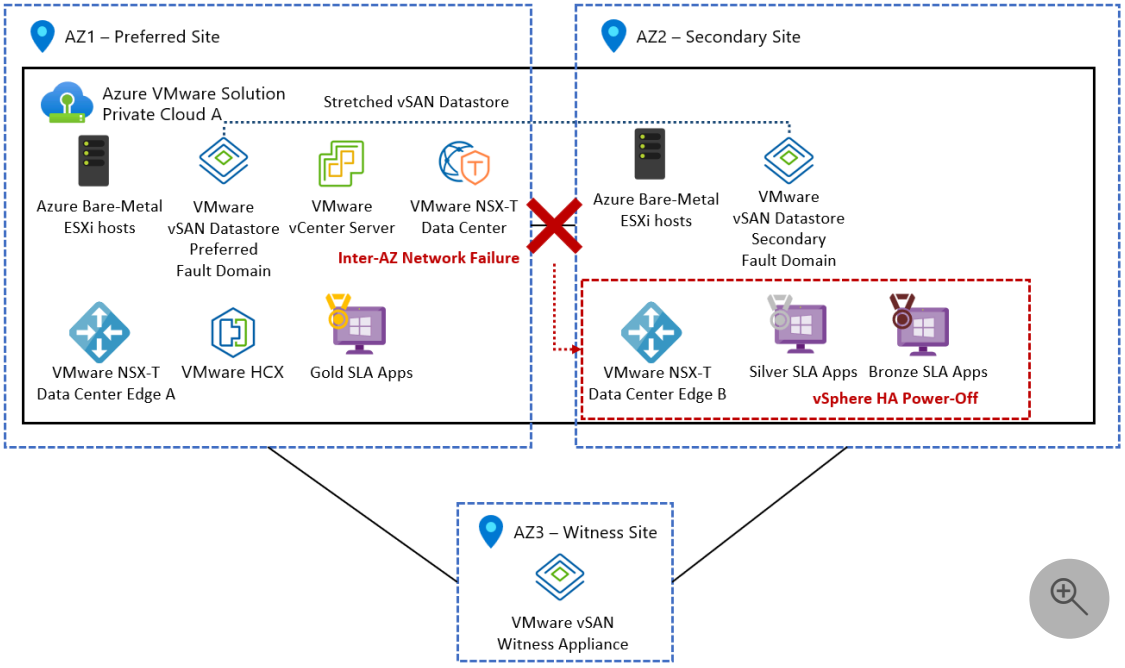
In summary, stretched clusters simplify protection needs by providing the same trusted controls and capabilities in addition to the scale and flexibility of the Azure infrastructure.

It's important to understand that stretched cluster private clouds only offer an extra layer of resiliency, and they don't address all failure scenarios. For example, stretched cluster private clouds:

- Don't protect against region-level failures within Azure or data loss scenarios caused by application issues or poorly planned storage policies.
- Provides protection against a single zone failure but aren't designed to provide protection against double or progressive failures. For example:

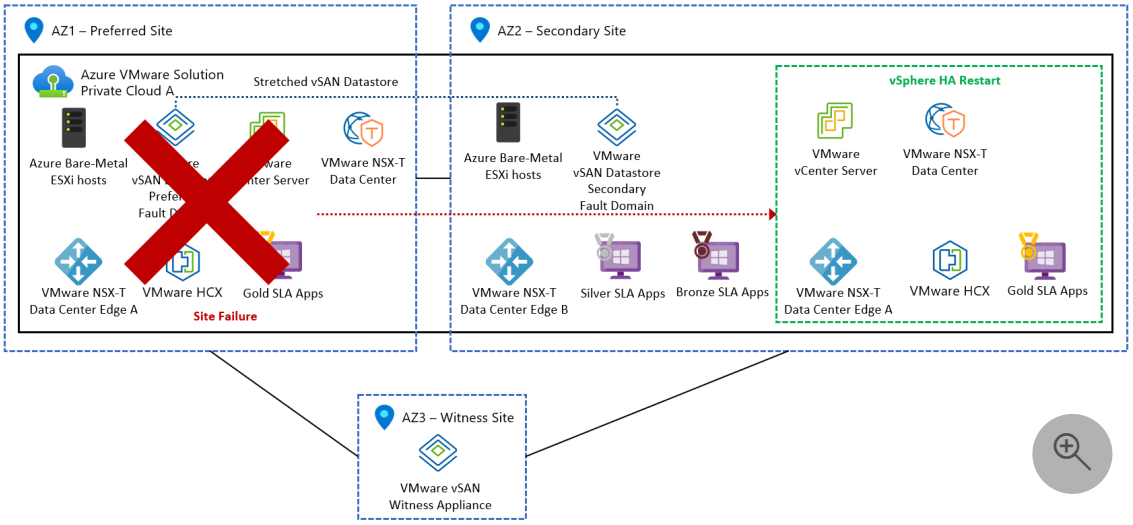
    - Despite various layers of redundancy built into the fabric, if an inter-AZ failure results in the partitioning of the secondary site, vSphere HA starts powering off the workload VMs on the secondary site.

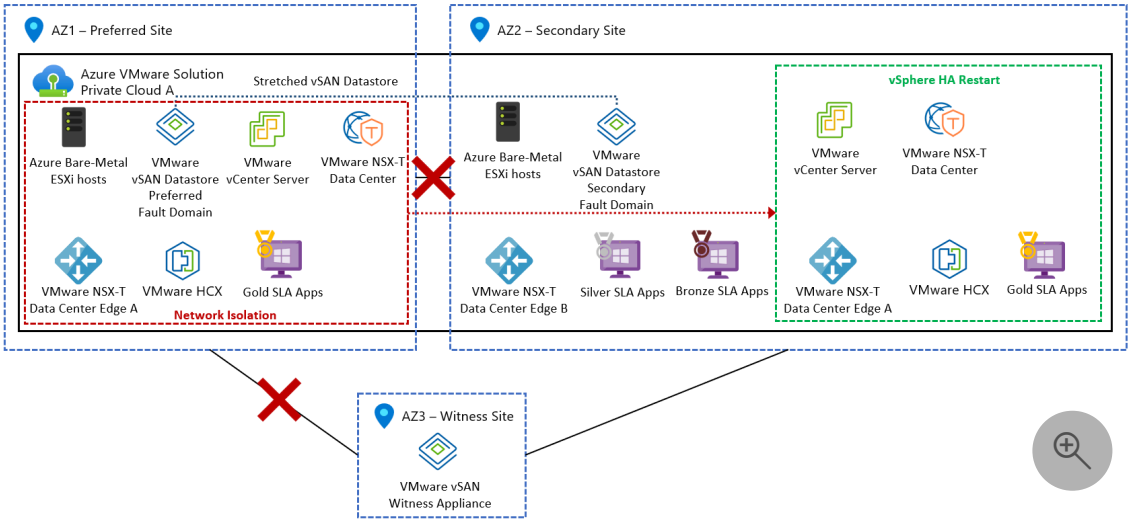
      The following diagram shows the secondary site partitioning scenario.



- If the secondary site partitioning progressed into the failure of the primary site instead, or resulted in a complete partitioning, vSphere HA would attempt to restart the workload VMs on the secondary site. If vSphere HA attempted to restart the workload VMs on the secondary site, it would put the workload VMs in an unsteady state.

  The following diagrams show the preferred site failure and complete network partitioning scenarios.





It should be noted that these types of failures, although rare, fall outside the scope of the protection offered by a stretched cluster private cloud. Because of those types of rare failures, a stretched cluster solution should be regarded as a multi-AZ high availability solution reliant upon vSphere HA. It's important you understand that a stretched cluster solution isn't meant to replace a comprehensive multi-region Disaster Recovery strategy that can be employed to ensure application availability. The reason is because a Disaster Recovery solution typically has separate management and control planes in separate Azure regions. Azure VMware Solution stretched clusters have a single management and control plane stretched across two availability zones within the same Azure region. For example, one vCenter Server, one NSX Manager cluster, one NSX Edge VM pair.

Stretched clusters region availability

Azure VMware Solution stretched clusters are available in the following regions:

- UK South (on AV36, and AV36P)
- West Europe (on AV36, and AV36P)
- Germany West Central (on AV36, and AV36P)
- Australia East (on AV36P)
- East US (on AV36P)

Storage policies supported

The following SPBM policies are supported with a PFTT of "Dual Site Mirroring" and SFTT of "RAID 1 (Mirroring)" enabled as the default policies for the cluster:

- Site disaster tolerance settings (PFTT):
  - Dual site mirroring

    - None - keep data on preferred
    - None - keep data on nonpreferred
- Local failures to tolerate (SFTT):
    - 1 failure – RAID 1 (Mirroring)
    - 1 failure – RAID 5 (Erasure coding), requires a minimum of four hosts in each AZ
    - 2 failures – RAID 1 (Mirroring)
    - 2 failures – RAID 6 (Erasure coding), requires a minimum of six hosts in each AZ
    - 3 failures – RAID 1 (Mirroring)

FAQ

Are any other regions planned?

Currently, there are five regions supported for stretched clusters.

What kind of SLA does Azure VMware Solution provide with the stretched clusters?

A private cloud created with a vSAN stretched cluster is designed to offer a 99.99% infrastructure availability commitment when the following conditions exist:

- A minimum of six nodes are deployed in the cluster (3 in each availability zone).
- When a VM storage policy of PFTT of "Dual-Site Mirroring" and an SFTT of 1 is used by the workload VMs.
- Compliance with the **Additional Requirements** captured in the SLA details of Azure VMware Solution is required to achieve the availability goals.

Do I get to choose the availability zone in which a private cloud is deployed?

No. A stretched cluster is created between two availability zones, while the third zone is used for deploying the witness node. Because all of the zones are effectively used for deploying a stretched cluster environment, a choice isn't provided to the customer. Instead, the customer chooses to deploy hosts in multiple AZs at the time of private cloud creation.

What are the limitations I should be aware of?

- Once a private cloud is created with a stretched cluster, it can't be changed to a standard cluster private cloud. Similarly, a standard cluster private cloud can't be changed to a stretched cluster private cloud after creation.
- Scale out and scale-in of stretched clusters can only happen in pairs. A minimum of six nodes and a maximum of 16 nodes are supported in a stretched cluster environment. For more information, see Azure subscription and service limits, quotas, and constraints.
- Customer workload VMs are restarted with a medium vSphere HA priority. Management VMs have the highest restart priority.
- The solution relies on vSphere HA and vSAN for restarts and replication. Recovery time objective (RTO) is determined by the amount of time it takes vSphere HA to restart a VM on the surviving AZ after the failure of a single AZ.
- Currently not supported in a stretched cluster environment:
  - Recently released features like Public IP down to NSX Edge and external storage, like ANF datastores.
  - Disaster recovery addons like VMware SRM, Zerto, and JetStream.
- Open a support ticket from the Azure portal for the following scenarios (be sure to select **Stretched Clusters** as a **Problem Type**):
  - Connect a private cloud to a stretched cluster private cloud.
  - Connect two stretched cluster private clouds in a single region.

What kind of latencies should I expect between the availability zones (AZs)?

vSAN stretched clusters operate within a 5-milliseconds round trip time (RTT) and 10 Gb/s or greater bandwidth between the AZs that host the workload VMs. The Azure VMware Solution stretched cluster deployment follows that guiding principle. Consider that information when deploying applications (with SFTT of dual site mirroring, which uses synchronous writes) that have stringent latency requirements.

Can I mix stretched and standard clusters in my private cloud?

No. A mix of stretched and standard clusters aren't supported within the same private cloud. A stretched or standard cluster environment is selected when you create the private cloud. Once a private cloud gets created with a stretched cluster, the assumption is that all clusters created within that private cloud are stretched in nature.

How much does the solution cost?

Customers are charged based on the number of nodes deployed within the private cloud.

Am I charged for the witness node and for inter-AZ traffic?

No. Customers don't see a charge for the witness node and the inter-AZ traffic. The witness node is entirely service managed, and Azure VMware Solution provides the required lifecycle management of the witness node. As the entire solution is service managed, the customer only needs to identify the appropriate SPBM policy to set for the workload virtual machines. The rest is managed through Microsoft.

Azure VMware Solution identity concepts

Article • 03/24/2024

Azure VMware Solution private clouds are provisioned with a vCenter Server and NSX Manager. You use vCenter Server to manage virtual machine (VM) workloads and NSX Manager to manage and extend the private cloud. The CloudAdmin role is used for vCenter Server and the CloudAdmin role (with restricted permissions) is used for NSX Manager.

vCenter Server access and identity

In Azure VMware Solution, VMware vCenter Server has a built-in local user account called *CloudAdmin* that's assigned the CloudAdmin role. You can configure users and groups in Windows Server Active Directory with the CloudAdmin role for your private cloud. In general, the CloudAdmin role creates and manages workloads in your private cloud. But in Azure VMware Solution, the CloudAdmin role has vCenter Server privileges that are different from other VMware cloud solutions and on-premises deployments.

> **ⓘ Important**
>
> The local CloudAdmin user account should be used as an emergency access account for "break glass" scenarios in your private cloud. It's not intended to be used for daily administrative activities or for integration with other services.

- In a vCenter Server and ESXi on-premises deployment, the administrator has access to the vCenter Server administrator@vsphere.local account and the ESXi root account. The administrator might also be assigned to more Windows Server Active Directory users and groups.

- In an Azure VMware Solution deployment, the administrator doesn't have access to the Administrator user account or the ESXi root account. But the administrator can assign Windows Server Active Directory users and groups the CloudAdmin role in vCenter Server. The CloudAdmin role doesn't have permissions to add an identity source like an on-premises Lightweight Directory Access Protocol (LDAP) or Secure LDAP (LDAPS) server to vCenter Server. However, you can use Run commands to add an identity source and assign the CloudAdmin role to users and groups.

A user account in a private cloud can't access or manage specific management components that Microsoft supports and manages. Examples include clusters, hosts, datastores, and distributed virtual switches.

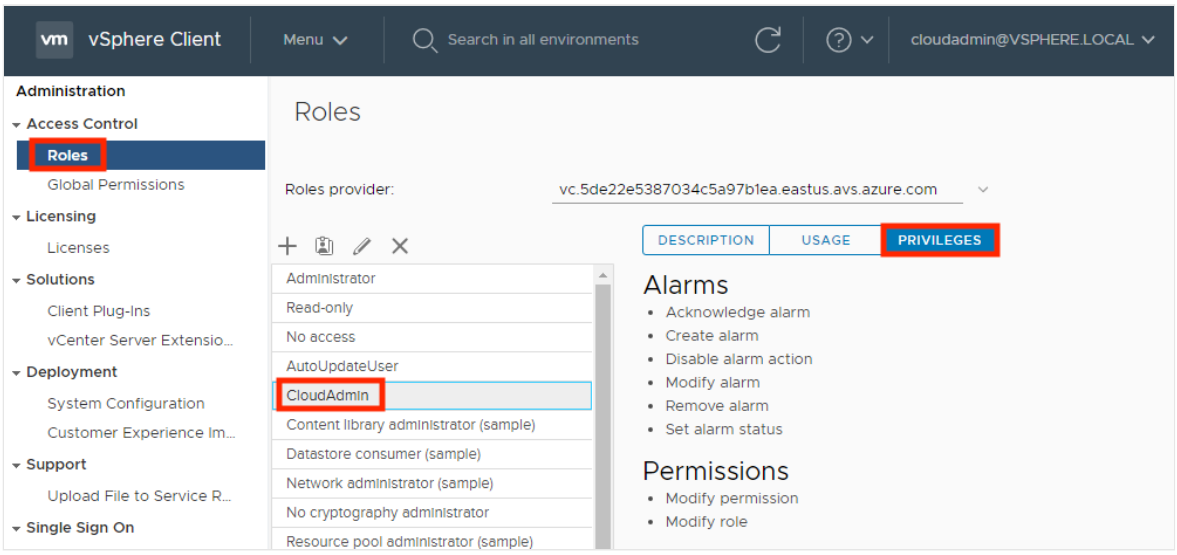
> **Note**
>
> In Azure VMware Solution, the vsphere.local single sign-on (SSO) domain is provided as a managed resource to support platform operations. You can't use it to create or manage local groups and users except for the ones that are provided by default with your private cloud.

> **Important**
>
> Azure VMware Solution offers custom roles on vCenter Server but currently doesn't offer them on the Azure VMware Solution portal. For more information, see the Create custom roles on vCenter Server section later in this article.

View the vCenter Server privileges

Use the following steps to view the privileges granted to the Azure VMware Solution CloudAdmin role on your Azure VMware Solution private cloud vCenter.

1. Sign in to the vSphere Client and go to **Menu** > **Administration**.
2. Under **Access Control**, select **Roles**.
3. From the list of roles, select **CloudAdmin** and then select **Privileges**.



The CloudAdmin role in Azure VMware Solution has the following privileges on vCenter Server. For more information, see the VMware product documentation.

Expand table

Privilege	Description
Alarms	Acknowledge alarm Create alarm Disable alarm action Modify alarm Remove alarm Set alarm status
Content Library	Add library item Add root certificate to trust store Check in a template Check out a template Create a subscription for a published library Create local library Create or delete a Harbor registry Create subscribed library Create, delete or purge a Harbor registry project Delete library item Delete local library Delete root certificate from trust store Delete subscribed library Delete subscription of a published library Download files Evict library items Evict subscribed library Import storage Manage Harbor registry resources on specified compute resource Probe subscription information Publish a library item to its subscribers Publish a library to its subscribers Read storage Sync library item Sync subscribed library Type introspection Update configuration settings Update files Update library Update library item Update local library Update subscribed library Update subscription of a published library View configuration settings

Privilege	Description
Cryptographic operations	Direct access
Datastore	Allocate space Browse datastore Configure datastore Low-level file operations Remove files Update virtual machine metadata
Folder	Create folder Delete folder Move folder Rename folder
Global	Cancel task Global tag Health Log event Manage custom attributes Service managers Set custom attribute System tag
Host	vSphere Replication Manage replication
Network	Assign network
Permissions	Modify permissions Modify role
Profile Driven Storage	Profile driven storage view
Resource	Apply recommendation Assign vApp to resource pool Assign virtual machine to resource pool Create resource pool Migrate powered off virtual machine Migrate powered on virtual machine Modify resource pool Move resource pool Query vMotion Remove resource pool Rename resource pool
Scheduled task	Create task Modify task Remove task Run task

Privilege	Description
Sessions	Message Validate session
Storage view	View
vApp	Add virtual machine Assign resource pool Assign vApp Clone Create Delete Export Import Move Power off Power on Rename Suspend Unregister View OVF environment vApp application configuration vApp instance configuration vApp managedBy configuration vApp resource configuration
Virtual machine	Change Configuration Acquire disk lease Add existing disk Add new disk Add or remove device Advanced configuration Change CPU count Change memory Change settings Change swapfile placement Change resource Configure host USB device Configure raw device Configure managedBy Display connection settings Extend virtual disk Modify device settings Query fault tolerance compatibility Query unowned files Reload from paths Remove disk Rename Reset guest information

Privilege	Description
	Set annotation Toggle disk change tracking Toggle fork parent Upgrade virtual machine compatibility Edit inventory Create from existing Create new Move Register Remove Unregister Guest operations Guest operation alias modification Guest operation alias query Guest operation modifications Guest operation program execution Guest operation queries Interaction Answer question Back up operation on virtual machine Configure CD media Configure floppy media Connect devices Console interaction Create screenshot Defragment all disks Drag and drop Guest operating system management by VIX API Inject USB HID scan codes Install VMware tools Pause or Unpause Wipe or shrink operations Power off Power on Record session on virtual machine Replay session on virtual machine Reset Resume Fault Tolerance Suspend Suspend fault tolerance Test failover Test restart secondary VM Turn off fault tolerance Turn on fault tolerance Provisioning Allow disk access Allow file access Allow read-only disk access

Privilege	Description
	Allow virtual machine download Clone template Clone virtual machine Create template from virtual machine Customize guest Deploy template Mark as template Modify customization specification Promote disks Read customization specifications Service configuration Allow notifications Allow polling of global event notifications Manage service configuration Modify service configuration Query service configurations Read service configuration Snapshot management Create snapshot Remove snapshot Rename snapshot Revert snapshot vSphere Replication Configure replication Manage replication Monitor replication
vService	Create dependency Destroy dependency Reconfigure dependency configuration Update dependency
vSphere tagging	Assign and unassign vSphere tag Create vSphere tag Create vSphere tag category Delete vSphere tag Delete vSphere tag category Edit vSphere tag Edit vSphere tag category Modify UsedBy field for category Modify UsedBy field for tag

Create custom roles on vCenter Server

Azure VMware Solution supports the use of custom roles with equal or lesser privileges than the CloudAdmin role. Use the CloudAdmin role to create, modify, or delete custom

roles with privileges less than or equal to their current role.

> ⓘ **Note**
>
> You can create roles with privileges greater than CloudAdmin. However, you can't assign the role to any users or groups or delete the role. Roles that have privileges greater than that of CloudAdmin is unsupported.

To prevent creating roles that can't be assigned or deleted, clone the CloudAdmin role as the basis for creating new custom roles.

Create a custom role

1. Sign in to vCenter Server with cloudadmin@vsphere.local or a user with the CloudAdmin role.
2. Navigate to the **Roles** configuration section and select **Menu** > **Administration** > **Access Control** > **Roles**.
3. Select the **CloudAdmin** role and select the **Clone role action** icon.

   > ⓘ **Note**
   >
   > Don't clone the **Administrator** role because you can't use it. Also, the custom role created can't be deleted by cloudadmin@vsphere.local.

4. Provide the name you want for the cloned role.
5. Remove privileges for the role and select **OK**. The cloned role is visible in the **Roles** list.

Apply a custom role

1. Navigate to the object that requires the added permission. For example, to apply permission to a folder, navigate to **Menu** > **VMs and Templates** > **Folder Name**.
2. Right-click the object and select **Add Permission**.
3. Select the Identity Source in the **User** drop-down where the group or user can be found.

4. Search for the user or group after selecting the Identity Source under the **User** section.

5. Select the role that you want to apply to the user or group.

   > ⓘ **Note**
   >
   > Attempting to apply a user or group to a role that has privileges greater than that of CloudAdmin will result in errors.

6. Check the **Propagate to children** if needed, and select **OK**. The added permission displays in the **Permissions** section.

VMware NSX Manager access and identity

When a private cloud is provisioned using Azure portal, software-defined data center (SDDC) management components like vCenter Server and VMware NSX Manager are provisioned for customers.

Microsoft is responsible for the lifecycle management of NSX appliances like, VMware NSX Manager and VMware NSX Edge appliances. They're responsible for bootstrapping network configuration, like creating the Tier-0 gateway.

You're responsible for VMware NSX software-defined networking (SDN) configuration, for example:

- Network segments
- Other Tier-1 gateways
- Distributed firewall rules
- Stateful services like gateway firewall
- Load balancer on Tier-1 gateways

You can access VMware NSX Manager using the built-in local user "cloudadmin" assigned to a custom role that gives limited privileges to a user to manage VMware NSX. While Microsoft manages the lifecycle of VMware NSX, certain operations aren't allowed by a user. Operations not allowed include editing the configuration of host and edge transport nodes or starting an upgrade. For new users, Azure VMware Solution deploys them with a specific set of permissions needed by that user. The purpose is to provide a clear separation of control between the Azure VMware Solution control plane configuration and Azure VMware Solution private cloud user.

For new private cloud deployments, VMware NSX access is provided with a built-in local user cloudadmin assigned to the **cloudadmin** role with a specific set of permissions to use VMware NSX functionality for workloads.

VMware NSX cloudadmin user permissions

The following permissions are assigned to the **cloudadmin** user in Azure VMware Solution NSX.

> **Note**
>
> **VMware NSX cloudadmin user** on Azure VMware Solution is not the same as the **cloudadmin user** mentioned in the VMware product documentation. The following permissions apply to the VMware NSX Policy API. Manager API functionality may be limited.

Expand table

Category	Type	Operation	Permission
Networking	Connectivity	Tier-0 Gateways Tier-1 Gateways Segments	Read-only Full Access Full Access
Networking	Network Services	VPN NAT Load Balancing Forwarding Policy Statistics	Full Access Full Access Full Access Read-only Full Access
Networking	IP Management	DNS DHCP IP Address Pools	Full Access Full Access Full Access
Networking	Profiles		Full Access
Security	East West Security	Distributed Firewall Distributed IDS and IPS Identity Firewall	Full Access Full Access Full Access
Security	North South Security	Gateway Firewall URL Analysis	Full Access Full Access
Security	Network Introspection		Read-only

Category	Type	Operation	Permission
Security	Endpoint Protection		Read-only
Security	Settings		Full Access
Inventory			Full Access
Troubleshooting	IPFIX		Full Access
Troubleshooting	Port Mirroring		Full Access
Troubleshooting	Traceflow		Full Access
System	Configuration Settings Settings Settings	Identity firewall Users and Roles Certificate Management (Service Certificate only) User Interface Settings	Full Access Full Access Full Access Full Access
System	All other		Read-only

You can view the permissions granted to the Azure VMware Solution cloudadmin role on your Azure VMware Solution private cloud VMware NSX.

1. Sign in to the NSX Manager.
2. Navigate to **Systems** and locate **Users and Roles**.
3. Select and expand the **cloudadmin** role, found under **Roles**.
4. Select a category like, Networking or Security, to view the specific permissions.

> **Note**
>
> **Private clouds created before June 2022** will switch from **admin** role to **cloudadmin** role. You'll receive a notification through Azure Service Health that includes the timeline of this change so you can change the NSX credentials you've used for other integration.

NSX LDAP integration for role-based access control (RBAC)

In an Azure VMware Solution deployment, the VMware NSX can be integrated with external LDAP directory service to add remote directory users or group, and assign them a VMware NSX RBAC role, like on-premises deployment. For more information on how to enable VMware NSX LDAP integration, see the VMware product documentation.

Unlike on-premises deployment, not all predefined NSX RBAC roles are supported with Azure VMware solution to keep Azure VMware Solution IaaS control plane config management separate from tenant network and security configuration. For more information, see the next section, Supported NSX RBAC roles.

> ⓘ **Note**
>
> VMware NSX LDAP Integration is supported only with SDDC's with VMware NSX "cloudadmin" user.

Supported and unsupported NSX RBAC roles

In an Azure VMware Solution deployment, the following VMware NSX predefined RBAC roles are supported with LDAP integration:

- Auditor
- Cloudadmin
- LB Admin
- LB Operator
- VPN Admin
- Network Operator

In an Azure VMware Solution deployment, the following VMware NSX predefined RBAC roles aren't supported with LDAP integration:

- Enterprise Admin
- Network Admin
- Security Admin
- NetX Partner Admin
- GI Partner Admin

You can create custom roles in NSX with permissions lesser than or equal to CloudAdmin role created by Microsoft. Following are examples on how to create a supported "Network Admin" and "Security Admin" role.

> ⓘ **Note**
>
> Custom role creation will fail if you assign a permission not allowed by CloudAdmin role.

Create “AVS network admin” role

Use the following steps to create this custom role.

1. Navigate to **System** > **Users and Roles** > **Roles**.
2. Clone **Network Admin** and provide the name, **AVS Network Admin**.
3. **Modify** the following permissions to "Read Only" or "None" as seen in the **Permission** column in the following table.

Expand table

Category	Subcategory	Feature	Permission
Networking	Connectivity	Tier-0 Gateways	Read-only
		Tier-0 Gateways > OSPF	None
	Network Services	Forwarding Policy	None

4. **Apply** the changes and **Save** the Role.

Create “AVS security admin” role

Use the following steps to create this custom role.

1. Navigate to **System** > **Users and Roles** > **Roles**.
2. Clone **Security Admin** and provide the name, “AVS Security Admin”.
3. **Modify** the following permissions to "Read Only" or "None" as seen in the **Permission** column in the following table.

Expand table

Category	Subcategory	Feature	Permission
Networking	Network Services	Forwarding Policy	None
Security	Network Introspection		None
	Endpoint Protection		None
	Settings	Service profiles	None

4. **Apply** the changes and **Save** the Role.

> **Note**

The VMware NSX **System** > **Identity Firewall AD** configuration option isn't supported by the NSX custom role. The recommendation is to assign the **Security Operator** role to the user with the custom role to allow managing the Identity Firewall (IDFW) feature for that user.

> **Note**
>
> The VMware NSX Traceflow feature isn't supported by the VMware NSX custom role. The recommendation is to assign the **Auditor** role to the user along with the custom role to enable Traceflow feature for that user.

> **Note**
>
> VMware Aria Operations Automation integration with the NSX component of the Azure VMware Solution requires the “auditor” role to be added to the user with the NSX Manager cloudadmin role.

Next steps

Now that you've covered Azure VMware Solution access and identity concepts, you may want to learn about:

- How to configure external identity source for vCenter
- How to enable Azure VMware Solution resource
- Details of each privilege
- How Azure VMware Solution monitors and repairs private clouds

Publish and protect APIs running on Azure VMware Solution VMs

Article • 03/24/2024

Microsoft Azure API Management lets you securely publish to external or internal consumers. Only the Developer (development) and Premium (production) SKUs allow Azure Virtual Network integration to publish APIs that run on Azure VMware Solution workloads. In addition, both SKUs enable the connectivity between the API Management service and the backend.

The API Management configuration is the same for backend services that run on Azure VMware Solution virtual machines (VMs) and on-premises. API Management also configures the virtual IP on the load balancer as the backend endpoint for both deployments when the backend server is placed behind an NSX Load Balancer on Azure VMware Solution.

External deployment

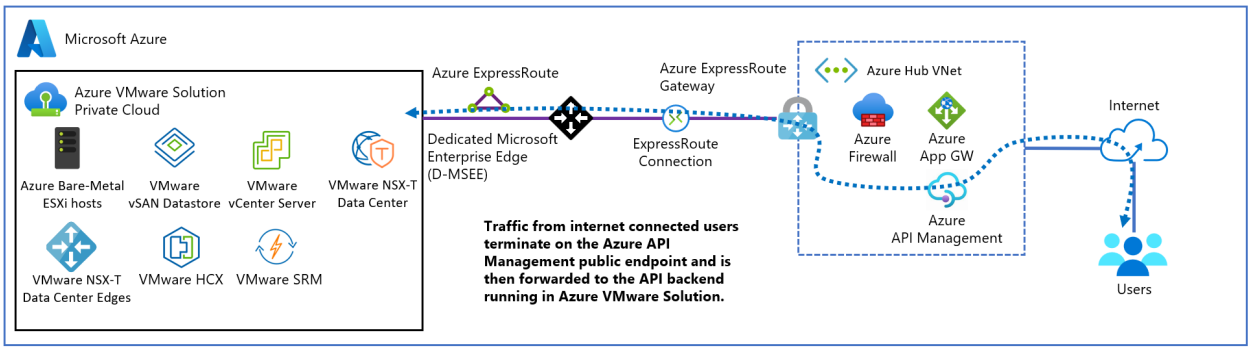
An external deployment publishes APIs consumed by external users that use a public endpoint. Developers and DevOps engineers can manage APIs through the Azure portal or PowerShell and the API Management developer portal.

The external deployment diagram shows the entire process and the actors involved (shown at the top). The actors are:

- **Administrator(s):** Represents the admin or DevOps team, which manages the Azure VMware Solution through the Azure portal and automation mechanisms like PowerShell or Azure DevOps.
- **Users:** Represents the exposed APIs' consumers and represents both users and services consuming the APIs.

The traffic flow goes through the API Management instance, which abstracts the backend services, plugged into the Hub virtual network. The ExpressRoute Gateway routes the traffic to the ExpressRoute Global Reach connection and reaches an NSX Load Balancer distributing the incoming traffic to the different backend service instances.

API Management has an Azure Public API, and activating Azure DDoS Protection Service is recommended.



Internal deployment

An internal deployment publishes APIs consumed by internal users or systems. DevOps teams and API developers use the same management tools and developer portal as in the external deployment.

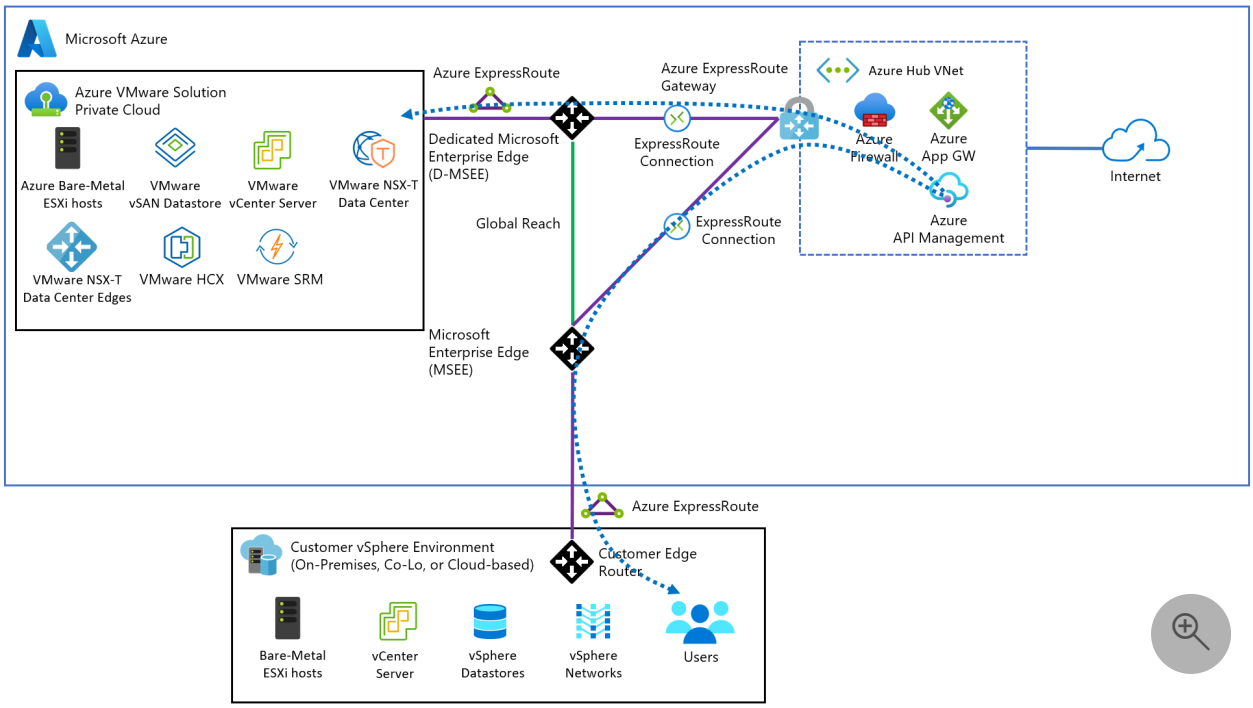
Use Azure Application Gateway for internal deployments to create a public and secure endpoint for the API. The gateway's capabilities are used to create a hybrid deployment that enables different scenarios.

- Use the same API Management resource for consumption by both internal and external consumers.
- Have a single API Management resource with a subset of APIs defined and available for external consumers.
- Provide an easy way to switch access to API Management from the public internet on and off.

The following deployment diagram shows consumers that can be internal or external, with each type accessing the same or different APIs.

In an internal deployment, APIs get exposed to the same API Management instance. In front of API Management, Application Gateway gets deployed with Azure Web Application Firewall (WAF) capability activated. Also deployed, a set of HTTP listeners and rules to filter the traffic, exposing only a subset of the backend services running on Azure VMware Solution.

- Internal traffic routes through ExpressRoute Gateway to Azure Firewall and then to API Management, directly or through traffic rules.
- External traffic enters Azure through Application Gateway, which uses the external protection layer for API Management.


Microsoft Azure
Azure VMware Solution
Private Cloud
Azure Bare-Metal
ESXi hosts
VMware
vSAN Datastore
VMware
vCenter Server
VMware NSX-T
Data Center
VMware NSX-T
Data Center Edges
VMware HCX
VMware SRM
Azure ExpressRoute
Dedicated Microsoft
Enterprise Edge
(D-MSEE)
Global Reach
Microsoft
Enterprise Edge
(MSEE)
Azure ExpressRoute
Gateway
ExpressRoute
Connection
ExpressRoute
Connection
Azure Hub VNet
Azure
Firewall
Azure
App GW
Azure
API Management
Internet

Azure ExpressRoute
Customer vSphere Environment
(On-Premises, Co-Lo, or Cloud-based)
Customer Edge
Routers
Bare-Metal
ESXi hosts
vCenter
Server
vSphere
Datastores
vSphere
Networks
Users

Integrate Azure VMware Solution in a hub and spoke architecture

Article • 04/12/2024

This article provides recommendations for integrating an Azure VMware Solution deployment in an existing or a new Hub and Spoke architecture on Azure.

The Hub and Spoke scenario assume a hybrid cloud environment with workloads on:

- Native Azure using IaaS or PaaS services
- Azure VMware Solution
- vSphere on-premises

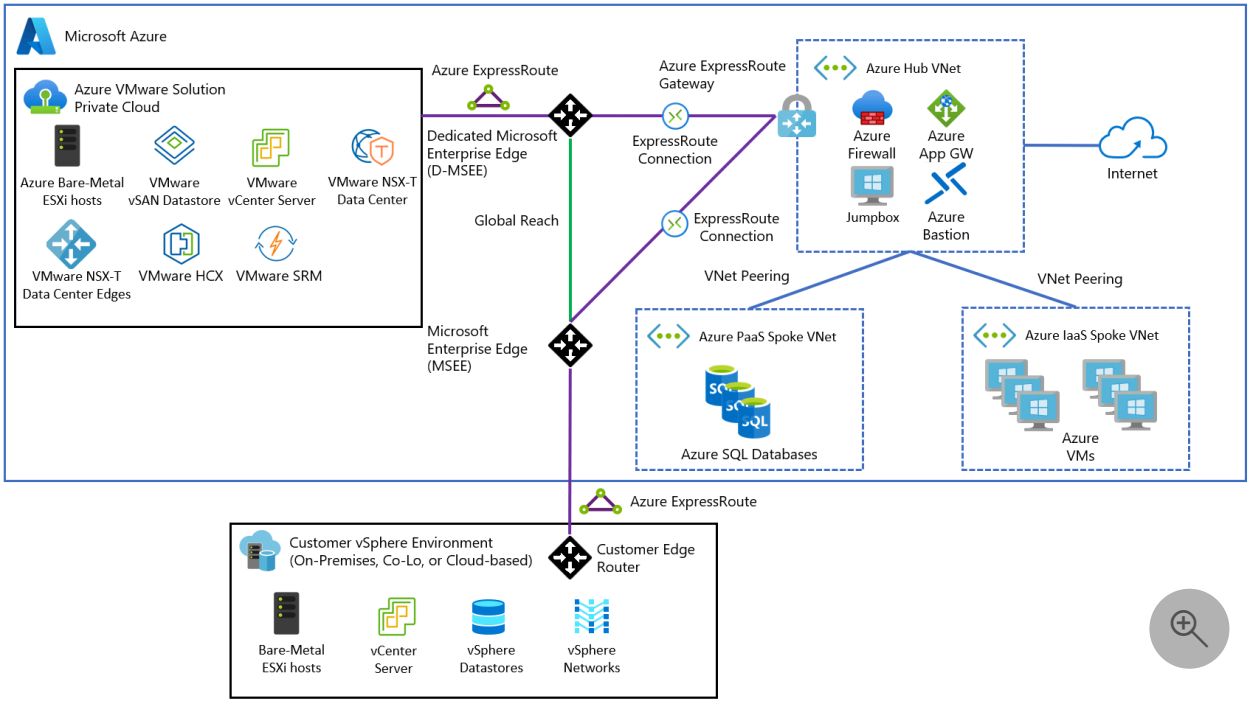
Architecture

The *Hub* is an Azure Virtual Network that acts as a central point of connectivity to your on-premises and Azure VMware Solution private cloud. The *Spokes* are virtual networks peered with the Hub to enable cross-virtual network communication.

Traffic between the on-premises datacenter, Azure VMware Solution private cloud, and the Hub goes through Azure ExpressRoute connections. Spoke virtual networks usually contain IaaS based workloads but can have PaaS services like App Service Environment, which has direct integration with Virtual Network, or other PaaS services with Azure Private Link enabled.

> **ⓘ Important**
>
> You can use an existing ExpressRoute Gateway to connect to Azure VMware Solution as long as it does not exceed the limit of four ExpressRoute circuits per virtual network. However, to access Azure VMware Solution from on-premises through ExpressRoute, you must have ExpressRoute Global Reach since the ExpressRoute gateway does not provide transitive routing between its connected circuits.

The diagram shows an example of a Hub and Spoke deployment in Azure connected to on-premises and Azure VMware Solution through ExpressRoute Global Reach.



The architecture has the following main components:

- **On-premises site:** Customer on-premises datacenter(s) connected to Azure through an ExpressRoute connection.
- **Azure VMware Solution private cloud:** Azure VMware Solution Software-Defined Data Center formed by one or more vSphere clusters, each one with a maximum of 16 hosts.
- **ExpressRoute gateway:** Enables the communication between Azure VMware Solution private cloud, shared services on Hub virtual network, and workloads running on Spoke virtual networks via an ExpressRoute Connection.
- **ExpressRoute Global Reach:** Enables the connectivity between on-premises and Azure VMware Solution private cloud. The connectivity between Azure VMware Solution and the Azure fabric is through ExpressRoute Global Reach only.
- **S2S VPN considerations:** Connectivity to Azure VMware Solution private cloud using Azure S2S VPN is supported as long as it meets the minimum network requirements for VMware HCX.
- **Hub virtual network:** Acts as the central point of connectivity to your on-premises network and Azure VMware Solution private cloud.
- **Spoke virtual network**
    - **IaaS Spoke:** Hosts Azure IaaS based workloads, including VM availability sets and Virtual Machine Scale Sets, and the corresponding network components.

- **PaaS Spoke:** Hosts Azure PaaS services using private addressing thanks to Private Endpoint and Private Link.

- **Azure Firewall:** Acts as the central piece to segment traffic between the Spokes and Azure VMware Solution.

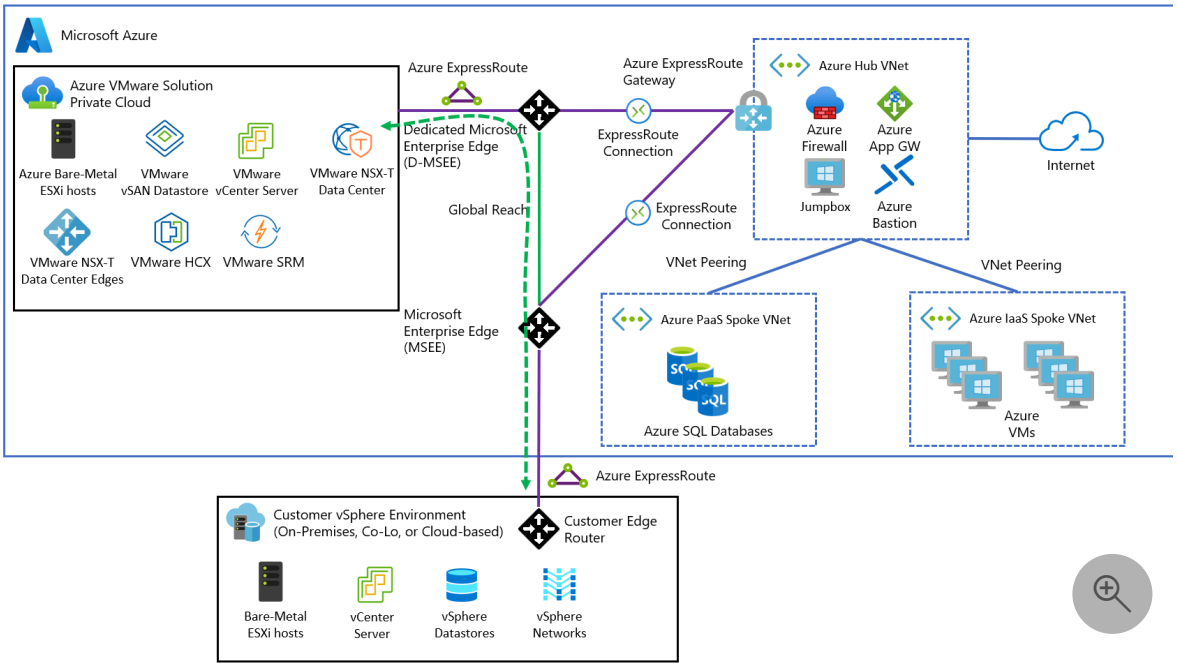
- **Application Gateway:** Exposes and protects web apps that run either on Azure IaaS/PaaS or Azure VMware Solution virtual machines (VMs). It integrates with other services like API Management.

Network and security considerations

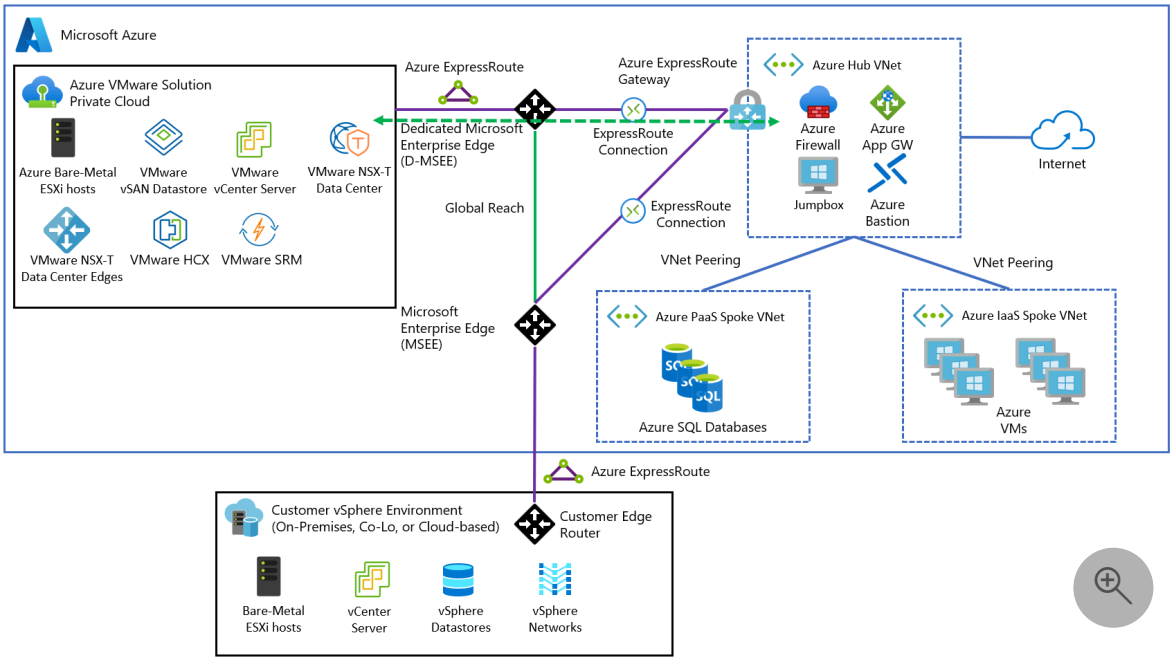
ExpressRoute connections enable traffic to flow between on-premises, Azure VMware Solution, and the Azure network fabric. Azure VMware Solution uses ExpressRoute Global Reach to implement this connectivity.

Because an ExpressRoute gateway doesn't provide transitive routing between its connected circuits, on-premises connectivity also must use ExpressRoute Global Reach to communicate between the on-premises vSphere environment and Azure VMware Solution.

- **On-premises to Azure VMware Solution traffic flow**



- **Azure VMware Solution to Hub VNet traffic flow**

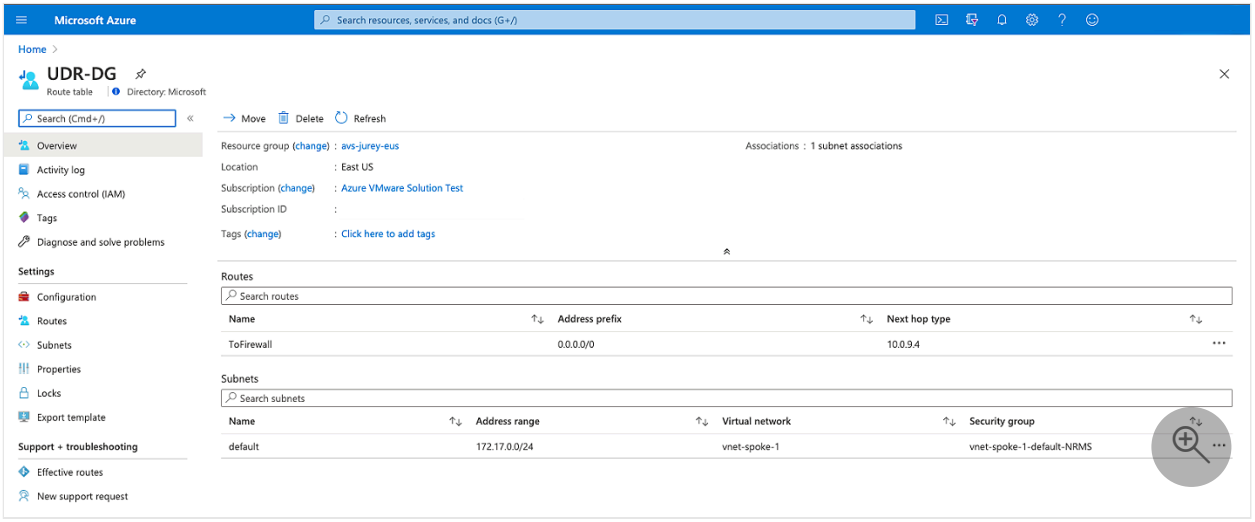


For more information on Azure VMware Solution networking and connectivity concepts, see the Azure VMware Solution product documentation.

Traffic segmentation

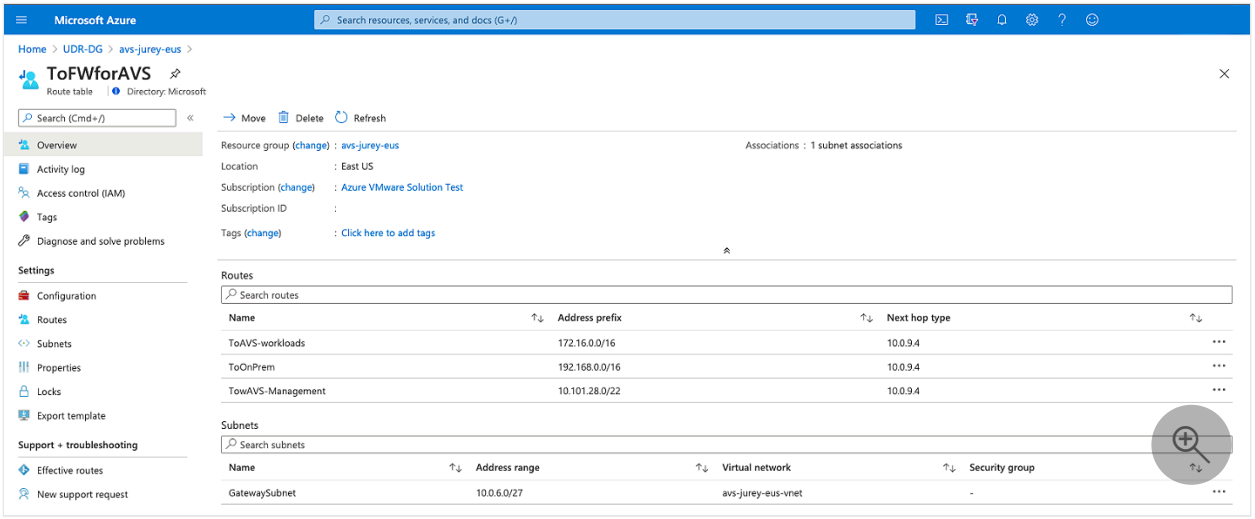
Azure Firewall is the Hub and Spoke topology's central piece, deployed on the Hub virtual network. Use Azure Firewall, or another Azure supported network virtual appliance (NVA) to establish traffic rules and segment the communication between the different spokes and Azure VMware Solution workloads.

Create route tables to direct the traffic to Azure Firewall. For the Spoke virtual networks, create a route that sets the default route to the internal interface of the Azure Firewall. This way, when a workload in the Virtual Network needs to reach the Azure VMware Solution address space, the firewall can evaluate it and apply the corresponding traffic rule to either allow or deny it.



> **Important**
>
> A route with address prefix 0.0.0.0/0 on the **GatewaySubnet** setting is not supported.

Set routes for specific networks on the corresponding route table. For example, routes to reach Azure VMware Solution management and workloads IP prefixes from the spoke workloads and the other way around.



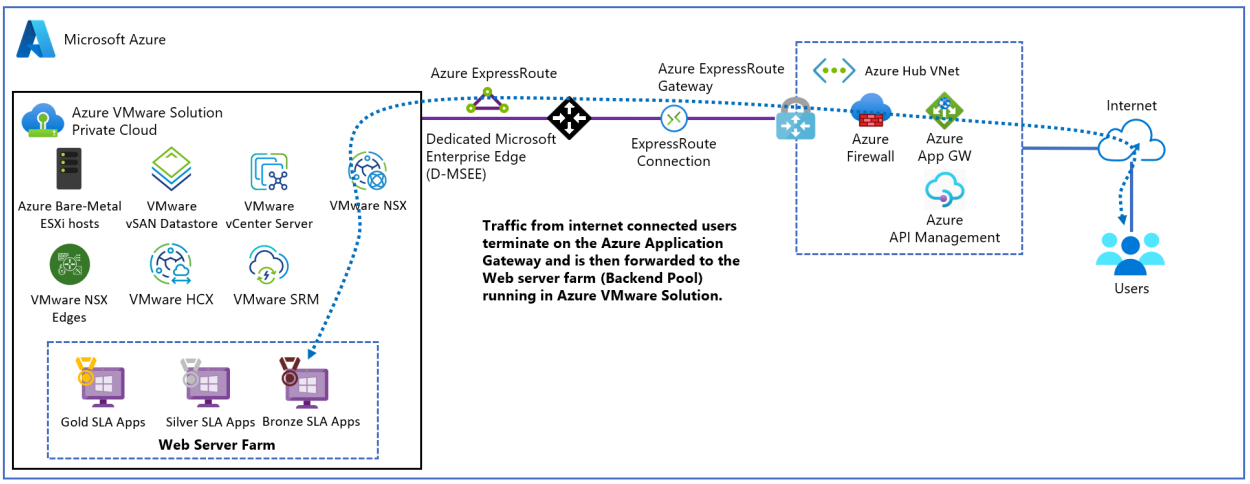
A second level of traffic segmentation using the network security groups within the Spokes and the Hub to create a more granular traffic policy.

> **Note**
>
> **Traffic from on-premises to Azure VMware Solution:** Traffic between on-premises workloads, either vSphere-based or others, are enabled by Global Reach, but the traffic doesn't go through Azure Firewall on the hub. In this scenario, you must implement traffic segmentation mechanisms, either on-premises or in Azure VMware Solution.

Application Gateway

Azure Application Gateway V1 and V2 were tested with web apps that run on Azure VMware Solution VMs as a backend pool. Application Gateway is currently the only supported method to expose web apps running on Azure VMware Solution VMs to the internet. It can also expose the apps to internal users securely.

For more information, see the Azure VMware Solution-specific article on Application Gateway.



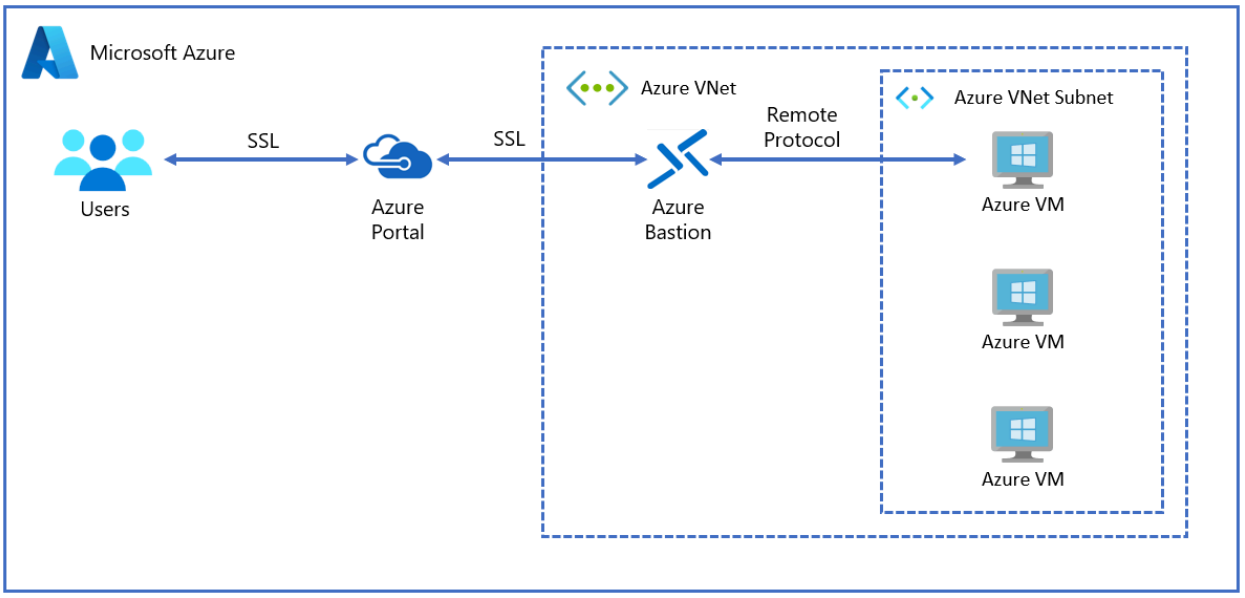
Jump box and Azure Bastion

Access Azure VMware Solution environment with a jump box, which is a Windows 10 or Windows Server VM deployed in the shared service subnet within the Hub virtual network.

> **ⓘ Important**
>
> Azure Bastion is the service recommended to connect to the jump box to prevent exposing Azure VMware Solution to the internet. You cannot use Azure Bastion to connect to Azure VMware Solution VMs since they are not Azure IaaS objects.

As a security best practice, deploy Microsoft Azure Bastion service within the Hub virtual network. Azure Bastion provides seamless RDP and SSH access to VMs deployed on Azure without providing public IP addresses to those resources. Once you provision the Azure Bastion service, you can access the selected VM from the Azure portal. After establishing the connection, a new tab opens, showing the jump box desktop, and from that desktop, you can access the Azure VMware Solution private cloud management plane.

> **ⓘ Important**
>
> Do not give a public IP address to the jump box VM or expose 3389/TCP port to the public internet.



Azure DNS resolution considerations

For Azure DNS resolution, there are two options available:

- Use the domain controllers deployed on the Hub (described in Identity considerations) as name servers.
- Deploy and configure an Azure DNS private zone.

The best approach is to combine both to provide reliable name resolution for Azure VMware Solution, on-premises, and Azure.

A general design recommendation: use the existing Active Directory-integrated DNS deployed onto at least two Azure VMs in the Hub virtual network and configured in the Spoke virtual networks to use those Azure DNS servers in the DNS settings.

You can use Azure Private DNS, where the Azure Private DNS zone links to the virtual network. The DNS servers are used as hybrid resolvers with conditional forwarding to on-premises or Azure VMware Solution running DNS using customer Azure Private DNS infrastructure.

To automatically manage the DNS records' lifecycle for the VMs deployed within the Spoke virtual networks, enable autoregistration. When enabled, the maximum number of private DNS zones is only one. If disabled, then the maximum number is 1000.

On-premises and Azure VMware Solution servers can be configured with conditional forwarders to resolver VMs in Azure for the Azure Private DNS zone.

Identity considerations

For identity purposes, the best approach is to deploy at least one domain controller on the Hub. Use two shared service subnets in zone-distributed fashion or a VM availability set. For more information on extending your on-premises Active Directory (AD) domain to Azure, see Azure Architecture Center.

Additionally, deploy another domain controller on the Azure VMware Solution side to act as identity and DNS source within the vSphere environment.

As a recommended best practice, integrate AD domain with Microsoft Entra ID.

Internet connectivity design considerations

Article • 03/24/2024

There are three primary patterns to create outbound access to the Internet from Azure VMware Solution and to enable inbound Internet access to resources on your Azure VMware Solution private cloud.

- Internet Service hosted in Azure
- Azure VMware Solution Managed SNAT
- Azure Public IPv4 address to NSX Data Center Edge

Your requirements for security controls, visibility, capacity, and operations drive the selection of the appropriate method for delivery of Internet access to the Azure VMware Solution private cloud.

Internet Service hosted in Azure

There are multiple ways to generate a default route in Azure and send it towards your Azure VMware Solution private cloud or on-premises. The options are as follows:

- An Azure firewall in a Virtual WAN Hub.
- A third-party Network Virtual Appliance in a Virtual WAN Hub Spoke Virtual Network.
- A third-party Network Virtual Appliance in a Native Azure Virtual Network using Azure Route Server.
- A default route from on-premises transferred to Azure VMware Solution over Global Reach.

Use any of these patterns to provide an outbound SNAT service with the ability to control what sources are allowed out, to view the connection logs, and for some services, do further traffic inspection.

The same service can also consume an Azure Public IP and create an inbound DNAT from the Internet towards targets in Azure VMware Solution.

An environment can also be built that utilizes multiple paths for Internet traffic. One for outbound SNAT (for example, a third-party security NVA), and another for inbound DNAT (like a third party Load balancer NVA using SNAT pools for return traffic).

Azure VMware Solution Managed SNAT

A Managed SNAT service provides a simple method for outbound internet access from an Azure VMware Solution private cloud. Features of this service include the following.

- Easily enabled – select the radio button on the Internet Connectivity tab and all workload networks have immediate outbound access to the Internet through a SNAT gateway.
- No control over SNAT rules, all sources that reach the SNAT service are allowed.
- No visibility into connection logs.
- Two Public IPs are used and rotated to support up to 128k simultaneous outbound connections.
- No inbound DNAT capability is available with the Azure VMware Solution Managed SNAT.

Azure Public IPv4 address to NSX Edge

This option brings an allocated Azure Public IPv4 address directly to the NSX Edge for consumption. It allows the Azure VMware Solution private cloud to directly consume and apply public network addresses in NSX as required. These addresses are used for the following types of connections:

- Outbound SNAT
- Inbound DNAT
- Load balancing using VMware NSX Advanced Load Balancer and other third-party Network Virtual Appliances
- Applications directly connected to a workload VM interface.

This option also lets you configure the public address on a third-party Network Virtual Appliance to create a DMZ within the Azure VMware Solution private cloud.

Features include:

- Scale – you can request to increase the soft limit of 64 Azure Public IPv4 addresses to 1,000 s of Azure Public IPs allocated if an application requires it.
- Flexibility – an Azure Public IPv4 address can be applied anywhere in the NSX ecosystem. It can be used to provide SNAT or DNAT, on load balancers like VMware's NSX Advanced Load Balancer, or third-party Network Virtual Appliances. It can also be used on third-party Network Virtual Security Appliances on VMware segments or directly on VMs.
- Regionality – the Azure Public IPv4 address to NSX Edge is unique to the local SDDC. For "multi private cloud in distributed regions," with local exit to Internet

intentions, it's easier to direct traffic locally versus trying to control default route propagation for a security or SNAT service hosted in Azure. If you have two or more Azure VMware Solution private clouds connected with a Public IP configured, they can both have a local exit.

Considerations for selecting an option

The option that you select depends on the following factors:

- To add an Azure VMware private cloud to a security inspection point provisioned in Azure native that inspects all Internet traffic from Azure native endpoints, use an Azure native construct and leak a default route from Azure to your Azure VMware Solution private cloud.
- If you need to run a third-party Network Virtual Appliance to conform to existing standards for security inspection or streamlined operating expenses, you have two options. You can run your Azure Public IPv4 address in Azure native with the default route method or run it in Azure VMware Solution using Azure Public IPv4 address to NSX Edge.
- There are scale limits on how many Azure Public IPv4 addresses can be allocated to a Network Virtual Appliance running in native Azure or provisioned on Azure Firewall. The Azure Public IPv4 address to NSX Edge option allows for higher allocations (1,000 s versus 100 s).
- Use an Azure Public IPv4 address to the NSX Edge for a localized exit to the internet from each private cloud in its local region. Using multiple Azure VMware Solution private clouds in several Azure regions that need to communicate with each other and the internet, it can be challenging to match an Azure VMware Solution private cloud with a security service in Azure. The difficulty is due to the way a default route from Azure works.

> **ⓘ Important**
>
> By design, Public IPv4 Address with NSX does not allow the exchange of Azure/Microsoft owned Public IP Addresses over ExpressRoute Private Peering connections. This means you cannot advertise the Public IPv4 addresses to your customer VNet or on-premises network via ExpressRoute. All Public IPv4 Addresses with NSX traffic must take the internet path even if the Azure VMware Solution private cloud is connected via ExpressRoute. For more information, visit ExpressRoute Circuit Peering.

Next Steps

Enable Managed SNAT for Azure VMware Solution Workloads

Enable Public IP to the NSX Edge for Azure VMware Solution

Disable Internet access or enable a default route

Azure VMware Solution network design considerations

Article • 03/24/2024

Azure VMware Solution offers a VMware private cloud environment that users and applications can access from on-premises and Azure-based environments or resources. Networking services such as Azure ExpressRoute and virtual private network (VPN) connections deliver the connectivity.

There are several networking considerations to review before you set up your Azure VMware Solution environment. This article provides solutions for use cases that you might encounter when you're using Azure VMware Solution to configure your networks.

Azure VMware Solution compatibility with AS-Path Prepend

Azure VMware Solution has considerations relating to the use of AS-Path Prepend for redundant ExpressRoute configurations. If you're running two or more ExpressRoute paths between on-premises and Azure, consider the following guidance for influencing traffic out of Azure VMware Solution towards your on-premises location via ExpressRoute GlobalReach.

Due to asymmetric routing, connectivity issues can occur when Azure VMware Solution doesn't observe AS-Path Prepend and therefore uses equal-cost multipath (ECMP) routing to send traffic toward your environment over both ExpressRoute circuits. This behavior can cause problems with stateful firewall inspection devices placed behind existing ExpressRoute circuits.

Prerequisites

For AS-Path Prepend, consider the following prerequisites:

- ✓ The key point is that you must prepend **Public** ASN numbers to influence how Azure VMware Solution routes traffic back to on-premises. If you prepend using *Private* ASN, Azure VMware Solution will ignore the prepend, and the ECMP behavior mentioned previously will occur. Even if you operate a Private BGP ASN on-premises, it's still possible to configure your on-premises devices to utilize a Public ASN when prepending routes outbound, to ensure compatibility with Azure VMware Solution.

- ✓ Design your traffic path for private ASNs after the public ASN to be honored by Azure VMware Solution. The Azure VMware Solution ExpressRoute circuit doesn't strip any private ASNs that exist in the path after the public ASN is processed.
- ✓ Both or all circuits are connected to Azure VMware Solution through Azure ExpressRoute Global Reach.
- ✓ The same netblocks are being advertised from two or more circuits.
- ✓ You wish to use AS-Path Prepend to force Azure VMware solution to prefer one circuit over another.
- ✓ Use either 2-byte or 4-byte public ASN numbers.

Management VMs and default routes from on-premises

> **ⓘ Important**
>
> Azure VMware Solution management virtual machines (VMs) won't honor a default route from on-premises for RFC1918 destinations.

If you're routing back to your on-premises networks by using only a default route advertised toward Azure, traffic from vCenter Server and NSX Manager VMs being used towards on-premises destinations with private IP addresses won't follow that route.

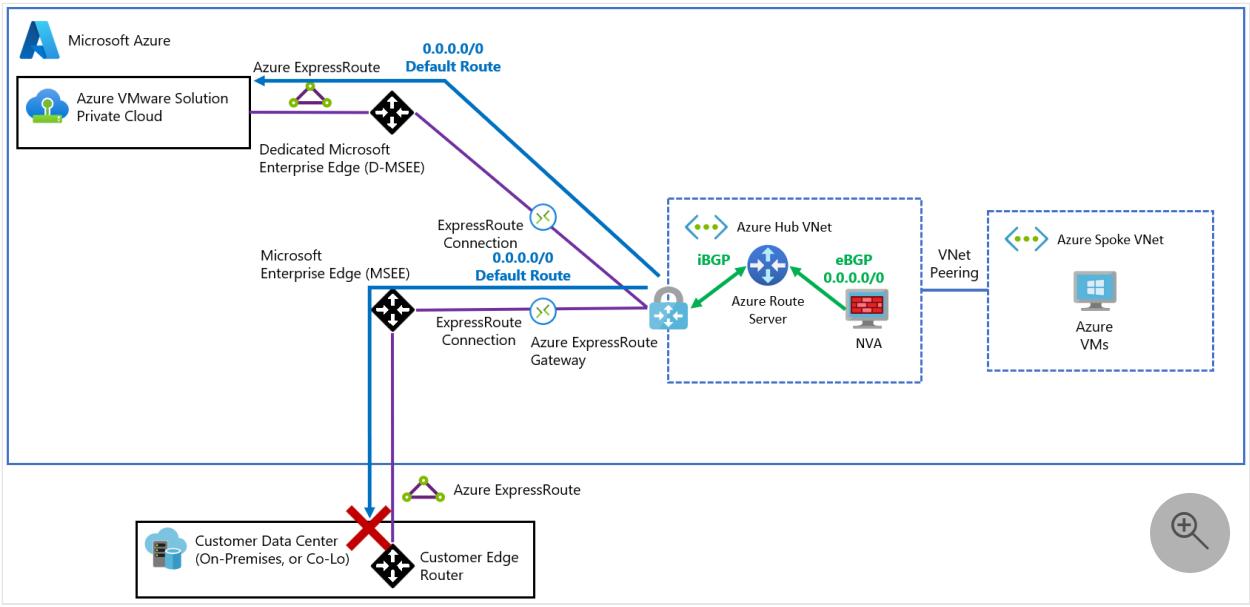
To reach vCenter Server and NSX Manager from on-premises, provide specific routes to allow traffic to have a return path to those networks. For example, advertise the RFC1918 summaries (10.0.0.0/8, 172.16.0.0/12 and 192.168.0.0/16).

Default route to Azure VMware Solution for internet traffic inspection

Certain deployments require inspecting all egress traffic from Azure VMware Solution toward the internet. Although it's possible to create network virtual appliances (NVAs) in Azure VMware Solution, there are use cases where these appliances already exist in Azure and can be applied to inspect internet traffic from Azure VMware Solution. In this case, a default route can be injected from the NVA in Azure to attract traffic from Azure VMware Solution and inspect the traffic before it goes out to the public internet.

The following diagram describes a basic hub-and-spoke topology connected to an Azure VMware Solution cloud and to an on-premises network through ExpressRoute. The diagram shows how the NVA in Azure originates the default route (`0.0.0.0/0`).

Azure Route Server propagates the route to Azure VMware Solution through ExpressRoute.



> **Important**
>
> The default route that the NVA advertises will be propagated to the on-premises network. You need to add user-defined routes (UDRs) to ensure that traffic from Azure VMware Solution is transiting through the NVA.

Communication between Azure VMware Solution and the on-premises network usually occurs over ExpressRoute Global Reach, as described in Peer on-premises environments to Azure VMware Solution.

Connectivity between Azure VMware Solution and an on-premises network

There are two main scenarios for connectivity between Azure VMware Solution and an on-premises network via a third-party NVA:

- Organizations have a requirement to send traffic between Azure VMware Solution and the on-premises network through an NVA (typically a firewall).
- ExpressRoute Global Reach isn't available in a particular region to interconnect the ExpressRoute circuits of Azure VMware Solution and the on-premises network.

There are two topologies that you can apply to meet all requirements for those scenarios: supernet and transit spoke virtual network.

> **Important**
>
> The preferred option to connect Azure VMware Solution and on-premises environments is a direct ExpressRoute Global Reach connection. The patterns described in this article add complexity to the environment.

Supernet design topology

If both ExpressRoute circuits (to Azure VMware Solution and to on-premises) are terminated in the same ExpressRoute gateway, you can assume that the gateway is going to route packets across them. However, an ExpressRoute gateway isn't designed to do that. You need to hairpin the traffic to an NVA that can route the traffic.

There are two requirements to hairpin network traffic to an NVA:

- The NVA should advertise a supernet for the Azure VMware Solution and on-premises prefixes.

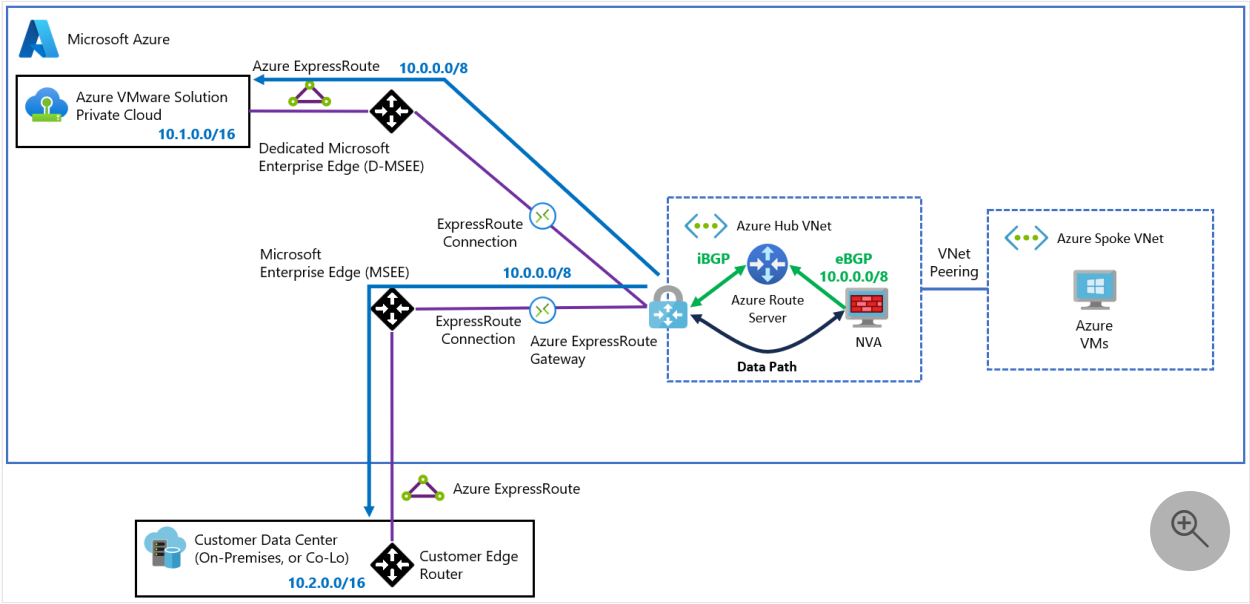
  You could use a supernet that includes both Azure VMware Solution and on-premises prefixes. Or you could use individual prefixes for Azure VMware Solution and on-premises (always less specific than the actual prefixes advertised over ExpressRoute). Keep in mind that all supernet prefixes advertised to Route Server get propagated to both Azure VMware Solution and on-premises.

- UDRs in the gateway subnet, that exactly match the prefixes advertised from Azure VMware Solution and on-premises, cause hairpin traffic from the gateway subnet to the NVA.

This topology results in high management overhead for large networks that change over time. Consider these limitations:

- Anytime a workload segment is created in Azure VMware Solution, UDRs might need to be added to ensure that traffic from Azure VMware Solution is transiting through the NVA.
- If your on-premises environment has a large number of routes that change, Border Gateway Protocol (BGP) and UDR configuration in the supernet might need to be updated.
- Because a single ExpressRoute gateway processes network traffic in both directions, performance might be limited.
- There's an Azure Virtual Network limit of 400 UDRs.

The following diagram demonstrates how the NVA needs to advertise prefixes that are more generic (less specific) and that include the networks from on-premises and Azure VMware Solution. Be careful with this approach. The NVA could potentially attract traffic that it shouldn't, because it's advertising wider ranges (for example, the whole `10.0.0.0/8` network).

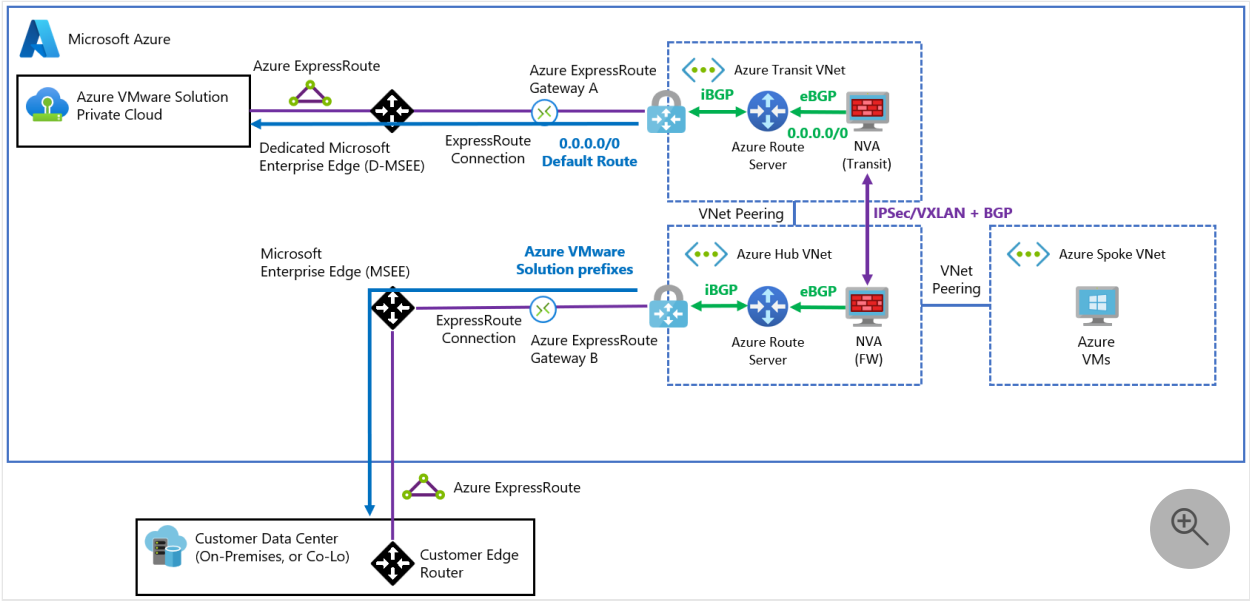


Transit spoke virtual network topology

> **Note**
>
> If advertising prefixes that are less specific isn't possible because of the previously described limits, you can implement an alternative design that uses two separate virtual networks.

In this topology, instead of propagating routes that are less specific to attract traffic to the ExpressRoute gateway, two different NVAs in separate virtual networks can exchange routes between each other. The virtual networks can propagate these routes to their respective ExpressRoute circuits via BGP and Azure Route Server. Each NVA has full control over which prefixes are propagated to each ExpressRoute circuit.

The following diagram demonstrates how a single `0.0.0.0/0` route is advertised to Azure VMware Solution. It also shows how the individual Azure VMware Solution prefixes are propagated to the on-premises network.



> **Important**
>
> An encapsulation protocol such as VXLAN or IPsec is required between the NVAs. Encapsulation is needed because the NVA network adapter (NIC) would learn the routes from Azure Route Server with the NVA as the next hop and create a routing loop.

There's an alternative to using an overlay. Apply secondary NICs in the NVA that don't learn the routes from Azure Route Server. Then, configure UDRs so that Azure can route traffic to the remote environment over those NICs. You can find more details in Enterprise-scale network topology and connectivity for Azure VMware Solution.

This topology requires a complex initial setup. The topology then works as expected with minimal management overhead. Setup complexities include:

- There's an extra cost to add another transit virtual network that includes Azure Route Server, an ExpressRoute gateway, and another NVA. The NVAs might also need to use large VM sizes to meet throughput requirements.
- IPsec or VXLAN tunneling is required between the two NVAs, which means that the NVAs are also in the datapath. Depending on the type of NVA that you're using, it can result in custom and complex configuration on those NVAs.

Next steps

After learning about network design considerations for Azure VMware Solution, consider exploring the following articles:

- Azure VMware Solution networking and interconnectivity concepts

- Plan the Azure VMware Solution deployment
- Tutorial: Networking planning checklist for Azure VMware Solution

Azure VMware Solution networking and interconnectivity concepts

Article • 03/24/2024

Azure VMware Solution offers a private cloud environment accessible from on-premises sites and Azure-based resources. Services such as Azure ExpressRoute, VPN connections, or Azure Virtual WAN deliver the connectivity. However, these services require specific network address ranges and firewall ports for enabling the services.

When you deploy a private cloud, private networks for management, provisioning, and vMotion get created. You use these private networks to access VMware vCenter Server and VMware NSX-T Data Center NSX-T Manager and virtual machine vMotion or deployment.

ExpressRoute Global Reach is used to connect private clouds to on-premises environments. It connects circuits directly at the Microsoft Edge level. The connection requires a virtual network (vNet) with an ExpressRoute circuit to on-premises in your subscription. The reason is that vNet gateways (ExpressRoute Gateways) can't transit traffic, which means you can attach two circuits to the same gateway, but it doesn't send the traffic from one circuit to the other.

Each Azure VMware Solution environment is its own ExpressRoute region (its own virtual MSEE device), which lets you connect Global Reach to the 'local' peering location. It allows you to connect multiple Azure VMware Solution instances in one region to the same peering location.

> **Note**
>
> For locations where ExpressRoute Global Reach isn't enabled, for example, because of local regulations, you have to build a routing solution using Azure IaaS VMs. For some examples, see Azure Cloud Adoption Framework - Network topology and connectivity for Azure VMware Solution.

Virtual machines deployed on the private cloud are accessible to the internet through the Azure Virtual WAN public IP functionality. For new private clouds, internet access is disabled by default.

Azure VMware Solution private cloud offers two types of interconnectivity:

- **Basic Azure-only interconnectivity** allows you to manage and use your private cloud with a single virtual network in Azure. This setup is ideal for evaluations or implementations that don't require access from on-premises environments.
- **Full on-premises to private cloud interconnectivity** extends the basic Azure-only implementation to include interconnectivity between on-premises and Azure VMware Solution private clouds.

This article explains key networking and interconnectivity concepts, including requirements and limitations. It also provides the information you need to configure your networking with Azure VMware Solution.

Azure VMware Solution private cloud use cases

The use cases for Azure VMware Solution private clouds include:

- New VMware vSphere VM workloads in the cloud
- VM workload bursting to the cloud (on-premises to Azure VMware Solution only)
- VM workload migration to the cloud (on-premises to Azure VMware Solution only)
- Disaster recovery (Azure VMware Solution to Azure VMware Solution or on-premises to Azure VMware Solution)
- Consumption of Azure services

> **Tip**
>
> All use cases for the Azure VMware Solution service are enabled with on-premises to private cloud connectivity.

Azure virtual network interconnectivity

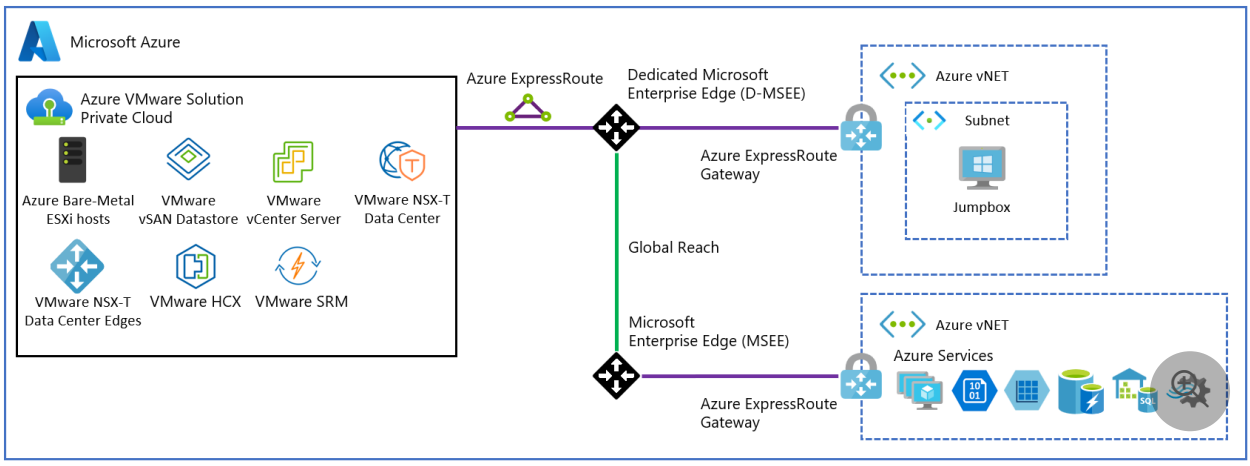
You can interconnect your Azure virtual network with the Azure VMware Solution private cloud implementation. This connection allows you to manage your Azure VMware Solution private cloud, consume workloads in your private cloud, and access other Azure services.

The following diagram illustrates the basic network interconnectivity established during a private cloud deployment. It shows the logical networking between a virtual network in Azure and a private cloud. This connectivity is established via a backend ExpressRoute that is part of the Azure VMware Solution service. The interconnectivity supports the following primary use cases:

- Inbound access to vCenter Server and NSX Manager from VMs in your Azure subscription.
- Outbound access from VMs on the private cloud to Azure services.
- Inbound access to workloads running in the private cloud.

> **Important**
>
> When connecting **production** Azure VMware Solution private clouds to an Azure virtual network, use an ExpressRoute virtual network gateway with the Ultra Performance Gateway SKU and enable FastPath to achieve 10Gbps connectivity. For less critical environments, use the Standard or High Performance Gateway SKUs for slower network performance.

> **Note**
>
> If you need to connect more than four Azure VMware Solution private clouds in the same Azure region to the same Azure virtual network, use AVS Interconnect to aggregate private cloud connectivity within the Azure region.



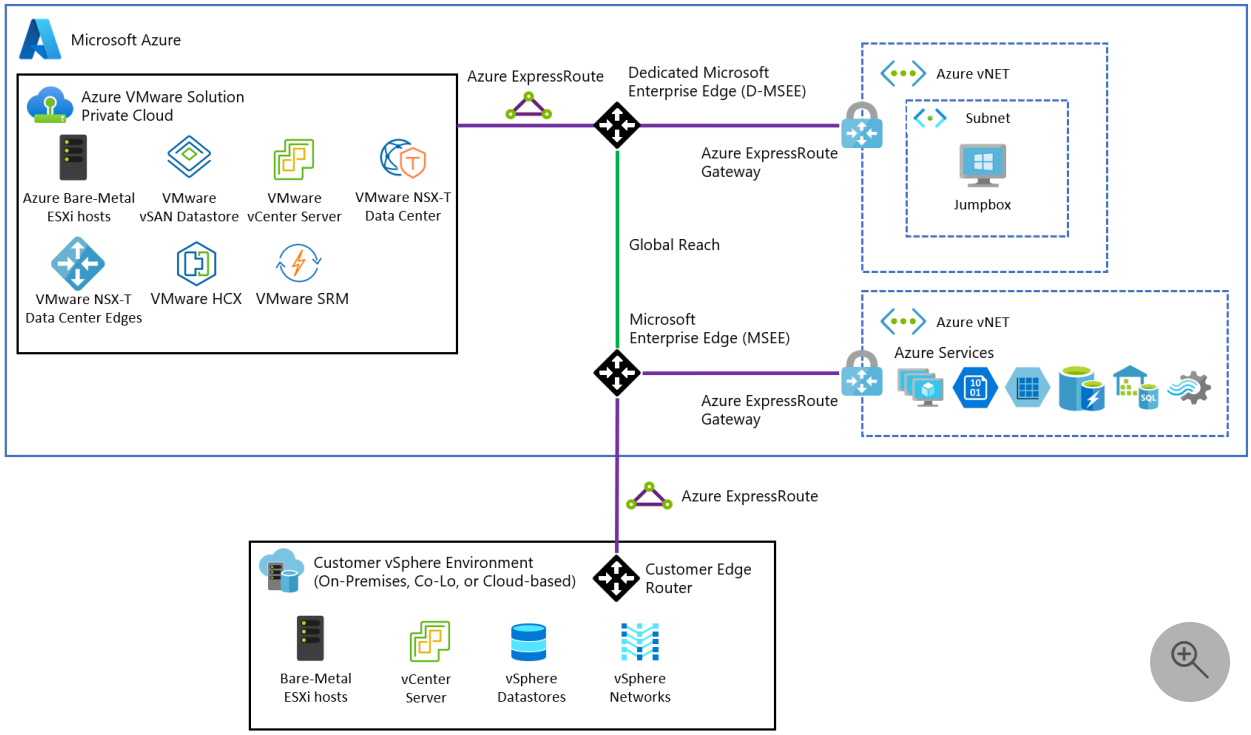
On-premises interconnectivity

In the fully interconnected scenario, you can access the Azure VMware Solution from your Azure virtual network(s) and on-premises. This implementation extends the basic implementation described in the previous section. An ExpressRoute circuit is required to connect from on-premises to your Azure VMware Solution private cloud in Azure.

The following diagram shows the on-premises to private cloud interconnectivity, which enables the following use cases:

- Hot/Cold vSphere vMotion between on-premises and Azure VMware Solution.

- On-premises to Azure VMware Solution private cloud management access.



For full interconnectivity to your private cloud, enable ExpressRoute Global Reach and then request an authorization key and private peering ID for Global Reach in the Azure portal. Use the authorization key and peering ID to establish Global Reach between an ExpressRoute circuit in your subscription and the ExpressRoute circuit for your private cloud. Once linked, the two ExpressRoute circuits route network traffic between your on-premises environments and your private cloud. For more information on the procedures, see the tutorial for creating an ExpressRoute Global Reach peering to a private cloud.

> **Important**
>
> Don't advertise bogon routes over ExpressRoute from on-premises or your Azure VNet. Examples of bogon routes include 0.0.0.0/5 or 192.0.0.0/3.

Route advertisement guidelines to Azure VMware Solution

Follow these guidelines when advertising routes from your on-premises and Azure virtual network to Azure VMware Solution over ExpressRoute:

Expand table

Supported	Not supported
Default route – 0.0.0.0/0*	Bogon routes. For example: `0.0.0.0/1, 128.0.0.0/1 0.0.0.0/5`, or `192.0.0.0/3.`
RFC-1918 address blocks. For example: (`10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16`) or its subnets (`10.1.0.0/16, 172.24.0.0/16, 192.168.1.0/24`).	Special address block reserved by IANA. For example, `RFC 6598-100.64.0.0/10` and its subnets.
Customer owned public-IP CIDR block or its subnets.	

> **Note**
>
> The customer-advertised default route to Azure VMware Solution can't be used to route back the traffic when the customer accesses Azure VMware Solution management appliances (vCenter Server, NSX Manager, HCX Manager). The customer needs to advertise a more specific route to Azure VMware Solution for that traffic to be routed back.

Limitations

The following table describes the maximum limits for Azure VMware Solution.

Expand table

Resource	Limit
vSphere clusters per private cloud	12
Minimum number of ESXi hosts per cluster	3 (hard-limit)
Maximum number of ESXi hosts per cluster	16 (hard-limit)
Maximum number of ESXi hosts per private cloud	96
Maximum number of vCenter Servers per private cloud	1 (hard-limit)
Maximum number of HCX site pairings	25 (any edition)
Maximum number of HCX service meshes	10 (any edition)
Maximum number of Azure VMware Solution ExpressRoute linked private clouds from a	4 The virtual network gateway used determines the

Resource	Limit
single location to a single Virtual Network Gateway	actual max linked private clouds. For more information, see About ExpressRoute virtual network gateways If you exceed this threshold use Azure VMware Solution Interconnect to aggregate private cloud connectivity within the Azure region.
Maximum Azure VMware Solution ExpressRoute port speed	10 Gbps (use Ultra Performance Gateway SKU with FastPath enabled) The virtual network gateway used determines the actual bandwidth. For more information, see About ExpressRoute virtual network gateways
Maximum number of Azure Public IPv4 addresses assigned to NSX-T Data Center	2,000
Maximum number of Azure VMware Solution Interconnects per private cloud	10
vSAN capacity limits	75% of total usable (keep 25% available for SLA)
VMware Site Recovery Manager - Maximum number of protected Virtual Machines	3,000
VMware Site Recovery Manager - Maximum number of Virtual Machines per recovery plan	2,000
VMware Site Recovery Manager - Maximum number of protection groups per recovery plan	250
VMware Site Recovery Manager - RPO Values	5 min or higher * (hard-limit)
VMware Site Recovery Manager - Maximum number of virtual machines per protection group	500
VMware Site Recovery Manager - Maximum number of recovery plans	250

* For information about Recovery Point Objective (RPO) lower than 15 minutes, see How the 5 Minute Recovery Point Objective Works in the *vSphere Replication Administration guide*.

For other VMware-specific limits, use the VMware configuration maximum tool.

Next steps

Now that you understand Azure VMware Solution network and interconnectivity concepts, consider learning about:

- Azure VMware Solution storage concepts
- Azure VMware Solution identity concepts
- Enabling the Azure VMware Solution resource provider

Azure VMware Solution storage concepts

Article • 03/24/2024

Azure VMware Solution private clouds provide native, cluster-wide storage with VMware vSAN. Local storage from each host in a cluster is used in a vSAN datastore, and data-at-rest encryption is available and enabled by default. You can use Azure Storage resources to extend storage capabilities of your private clouds.

vSAN clusters

Local storage in each cluster host is claimed as part of a vSAN datastore. For the AV36 SKU, all diskgroups use an NVMe cache tier of 1.6 TB with the raw, per host, SSD-based capacity of 15.4 TB. The size of the raw capacity tier of a cluster is the per host capacity times the number of hosts. For example, a four host cluster provides 61.6-TB raw capacity in the vSAN capacity tier. Check the hardware specification for the AV36P, AV52, and AV64 SKU storage device details.

Local storage in cluster hosts is used in the cluster-wide vSAN datastore. All datastores are created as part of private cloud deployment and are available for use immediately. The **cloudadmin** user and all users assigned to the CloudAdmin role can manage datastores with these vSAN privileges:

- Datastore.AllocateSpace
- Datastore.Browse
- Datastore.Config
- Datastore.DeleteFile
- Datastore.FileManagement
- Datastore.UpdateVirtualMachineMetadata

> **Important**
>
> You can't change the name of datastores or clusters. Azure CLI and PowerShell support changing the name of the resource clusters (Cluster-2 to Cluster-12), however this should not be used, because it creates a meta-data mismatch between the Azure portal resource cluster name and the vSphere cluster name.

Storage policies and fault tolerance

The default storage policy is set to **RAID-1 FTT-1**, with Object Space Reservation set to Thin provisioning. Unless you adjust the storage policy or apply a new policy, the cluster grows with this configuration. The default storage policy is the one that will be applied to the workload VMs. To set a different storage policy, see Configure storage policy.

In a three-host cluster, FTT-1 accommodates a single host's failure. Microsoft governs failures regularly and replaces the hardware when events are detected from an operations perspective.

> **Note**
>
> When you log on to the vSphere Client, you may notice a VM Storage Policy called **vSAN Default Storage Policy** with **Object Space Reservation** set to **Thick** provisioning. Please note that this is not the default storage policy applied to the cluster. This policy exists for historical purposes and will eventually be modified to **Thin** provisioning.

> **Note**
>
> All of the software-defined data center (SDDC) management VMs (vCenter Server, NSX Manager, NSX Edges, and others) use the **Microsoft vSAN Management Storage Policy**, with **Object Space Reservation** set to **Thin** provisioning.

> **Tip**
>
> If you're unsure if the cluster will grow to four or more, then deploy using the default policy. If you're sure your cluster will grow, then instead of expanding the cluster after your initial deployment, we recommend deploying the extra hosts during deployment. As the VMs are deployed to the cluster, change the disk's storage policy in the VM settings to either RAID-5 FTT-1 or RAID-6 FTT-2. In reference to **SLA for Azure VMware Solution**, note that more than 6 hosts should be configured in the cluster to use an FTT-2 policy (RAID-1, or RAID-6). Also note that the storage policy is not automatically updated based on cluster size. Similarly, changing the default does not automatically update the running VM policies.

Data-at-rest encryption

vSAN datastores use data-at-rest encryption by default using keys stored in Azure Key Vault. The encryption solution is KMS-based and supports vCenter Server operations for key management. When a host is removed from a cluster, all data on SSDs is invalidated immediately.

Datastore capacity expansion options

The existing cluster vSAN storage capacity can be expanded by connecting Azure storage resources including Azure NetApp Files or Azure Elastic SAN. Virtual machines can be migrated between vSAN datastores and other datastores non-disruptively using storage vMotion. Expanding datastore capacity using Azure storage resources allows increased datastore capacity without scaling the clusters.

Azure NetApp Files

Azure NetApp Files is an enterprise-class, high-performance, metered file storage service. The service supports the demanding enterprise file-workloads in the cloud: databases, SAP, and high-performance computing applications, with no code changes.

You can create Network File System (NFS) datastores with Azure NetApp Files volumes and attach them to clusters of your choice. By using NFS datastores backed by Azure NetApp Files, you can expand your storage instead of scaling the clusters. Azure NetApp Files is available in Ultra, Premium and Standard performance tiers to allow for adjusting performance and cost to the requirements of the workloads.

For more information, see Attach Azure NetApp Files datastores to Azure VMware Solution hosts.

Azure Elastic SAN

Azure Elastic storage area network (SAN) is Microsoft's answer to the problem of workload optimization and integration between your large-scale databases and performance-intensive mission-critical applications.

Azure VMware Solution supports attaching iSCSI datastores as a persistent storage option. You can create Virtual Machine File System (VMFS) datastores with Azure Elastic SAN volumes and attach them to clusters of your choice. By using VMFS datastores backed by Azure Elastic SAN, you can expand your storage instead of scaling the clusters.

For more information, see Use Azure VMware Solution with Azure Elastic SAN.

Azure storage integration

You can use Azure storage services in workloads running in your private cloud. The Azure storage services include Storage Accounts, Table Storage, Blob Storage, and file storage (Azure Files and Azure NetApp Files). The connection of workloads to Azure storage services doesn't traverse the internet. This connectivity provides more security and enables you to use SLA-based Azure storage services in your private cloud workloads.

Alerts and monitoring

Microsoft provides alerts when capacity consumption exceeds 75%. In addition, you can monitor capacity consumption metrics that are integrated into Azure Monitor. For more information, see Configure Azure Alerts in Azure VMware Solution.

Next steps

Now that you've covered Azure VMware Solution storage concepts, you may want to learn about:

- Configure storage policy - Each VM deployed to a vSAN datastore is assigned at least one VM storage policy. You can assign a VM storage policy in an initial deployment of a VM or when you perform other VM operations, such as cloning or migrating.
- Scale clusters in the private cloud - You can scale the clusters and hosts in a private cloud as required for your application workload. Performance and availability limitations for specific services should be addressed on a case by case basis.
- Azure NetApp Files with Azure VMware Solution - You can use Azure NetApp Files to migrate and run the most demanding enterprise file-workloads in the cloud: databases, and general purpose computing applications, with no code changes. Azure NetApp Files volumes can be attached to virtual machines, and as datastores to extend the vSAN datastore capacity without adding more nodes.
- vSphere role-based access control for Azure VMware Solution - You use vCenter Server to manage VM workloads and NSX Manager to manage and extend the private cloud. Access and identity management use the CloudAdmin role for vCenter Server and restricted administrator rights for NSX Manager.

VMware HCX migration considerations

Article • 03/24/2024

VMware HCX offers five options with the HCX Enterprise Edition license when migrating VMware vSphere virtual machines to the Azure VMware Solution:

- Cold Migration
- HCX vMotion
- Bulk Migration
- Replication Assisted vMotion
- OS Assisted Migration

The cost of the VMware HCX Enterprise Edition license is included in the cost of the Azure VMware Solution service.

VMware HCX migration options

Each of these options has different advantages and disadvantages when used. You need to select the best options for your migration plan.

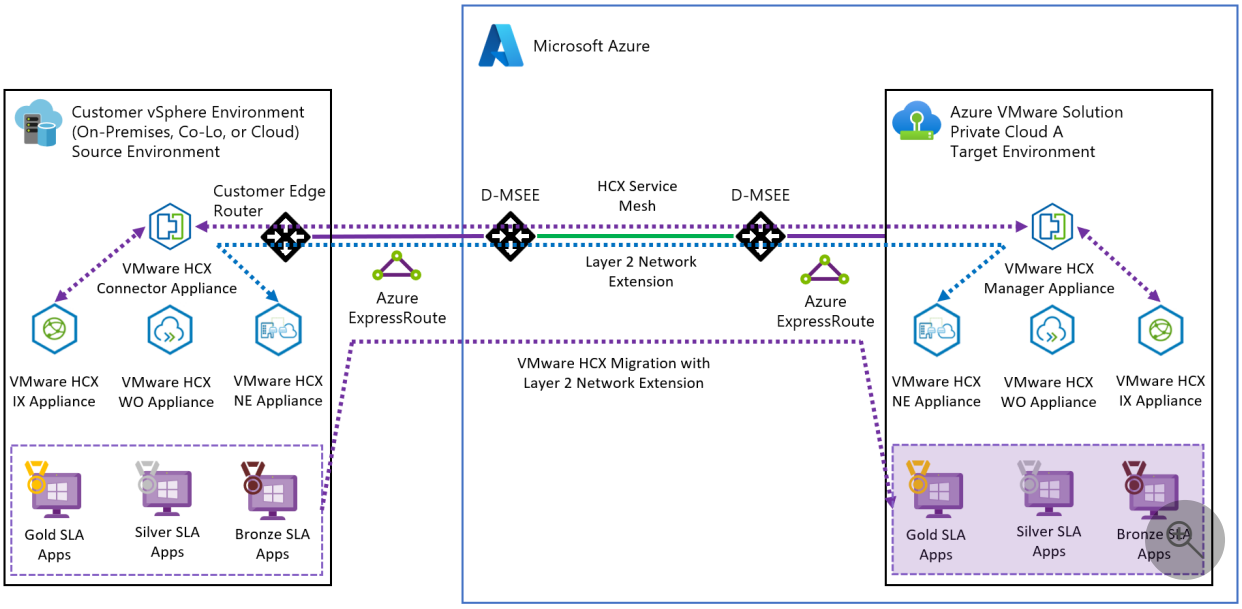
Expand table

Migration Method	Migration Downtime	Scale
Cold Migration	Long downtime	VM copy with Network File Copy (NFC) protocol, small scale
HCX vMotion	None	Serial migrations, small scale
Bulk Migration	Minimal downtime	VM shutdown (source site)/VM power-on (destination site), Parallel migrations, largest scale
Replication Assisted vMotion (RAV)	None	Parallel migrations, larger scale
OS Assisted Migration (OSAM)	Conversion downtime	Hyper-V and KVM workload migrations

VMware HCX architecture

The Azure VMware Solution deploys VMware HCX as an Add-On. A VMware HCX Service Mesh is used to connect two sites together, including a Layer 2 network

extension. This allows VMware vSphere virtual machines to be migrated from the on-premises site to the Azure VMware Solution private cloud.



Next Steps

After learning about the VMware HCX migration considerations of the Azure VMware Solution, consider exploring the following articles:

- Create an HCX network extension
- HCX Network extension high availability (HA)
- Enable HCX access over the internet
- Upgrade HCX on Azure VMware Solution
- Use VMware HCX Run Commands
- Migrate a SQL Server standalone instance to Azure VMware Solution
- Migrate a SQL Server Always On Failover Cluster Instance to Azure VMware Solution
- Migrate a SQL Server Always On Availability Group to Azure VMware Solution

Azure VMware Solution workload documentation

Relocate legacy application virtual machines to Azure VMware Solution as a staging area for the first phase of your migration and modernization strategy.

Get started

OVERVIEW

What is an Azure VMware Solution workload?

CONCEPT

Design principles

Integration with Azure landing zones

Design areas

CONCEPT

Infrastructure

Applications

Networking

Monitoring

Security

Operations

Reference examples

ARCHITECTURE

Baseline Azure VMware Solution reference architecture

Azure VMware Solution landing zone accelerator

Reference implementations

DEPLOY

Azure VMware Solution implementation options

Learn

TRAINING

Introduction to Azure VMware Solution

Migrate VMware resources on-premises to Azure VMware Solution

Run VMware resources on Azure VMware Solution

Assessment

HOW-TO GUIDE

Azure VMware Solution assessment tool

Create an Azure VMware Solution assessment

Article • 05/09/2024

This article describes how to create an Azure VMware Solution assessment for on-premises VMs in a VMware vSphere environment with Azure Migrate: Discovery and assessment.

Azure Migrate helps you to migrate to Azure. Azure Migrate provides a centralized hub to track discovery, assessment, and migration of on-premises infrastructure, applications, and data to Azure. The hub provides Azure tools for assessment and migration, as well as third-party independent software vendor (ISV) offerings.

Before you start

- Make sure you've created an Azure Migrate project.
- If you've already created a project, make sure you've added the Azure Migrate: Discovery and assessment tool.
- To create an assessment, you need to set up an Azure Migrate appliance for VMware vSphere, which discovers the on-premises servers, and sends metadata and performance data to Azure Migrate: Discovery and assessment. Learn more.
- You could also import the server metadata in comma-separated values (CSV) format or import your RVTools XLSX file.

Azure VMware Solution (AVS) Assessment overview

There are four types of assessments you can create using Azure Migrate: Discovery and assessment.

Expand table

Assessment Type	Details
Azure VM	Assessments to migrate your on-premises servers to Azure virtual machines. You can assess your on-premises VMs in VMware vSphere and Hyper-V environment, and physical servers for migration to Azure VMs using this assessment type.

Assessment Type	Details
Azure SQL	Assessments to migrate your on-premises SQL servers from your VMware environment to Azure SQL Database or Azure SQL Managed Instance.
Azure App Service	Assessments to migrate your on-premises ASP.NET/Java web apps, running on IIS web servers, from your VMware vSphere environment to Azure App Service.
Azure VMware Solution (AVS)	Assessments to migrate your on-premises servers to Azure VMware Solution (AVS). You can assess your on-premises VMs in VMware vSphere environment for migration to Azure VMware Solution (AVS) using this assessment type. Learn more

> **Note**
>
> Azure VMware Solution (AVS) assessment can be created for virtual machines in VMware vSphere environment only.

There are two types of sizing criteria that you can use to create Azure VMware Solution (AVS) assessments:

Expand table

Assessment	Details	Data
Performance-based	For RVTools & CSV file-based assessments and performance-based assessment will consider the "In Use MiB" & "Storage In Use" respectively for storage configuration of each VM. For appliance-based assessments and performance-based assessments will consider the collected CPU & memory performance data of on-premises servers.	**Recommended Node size**: Based on CPU and memory utilization data along with node type, storage type, and FTT setting that you select for the assessment.
As on-premises	Assessments based on on-premises sizing.	**Recommended Node size**: Based on the on-premises server size along with the node type, storage type, and FTT setting that you select for the assessment.

Run an Azure VMware Solution (AVS) assessment

1. On the **Overview** page > **Servers, databases and web apps**, click **Assess and migrate servers**.

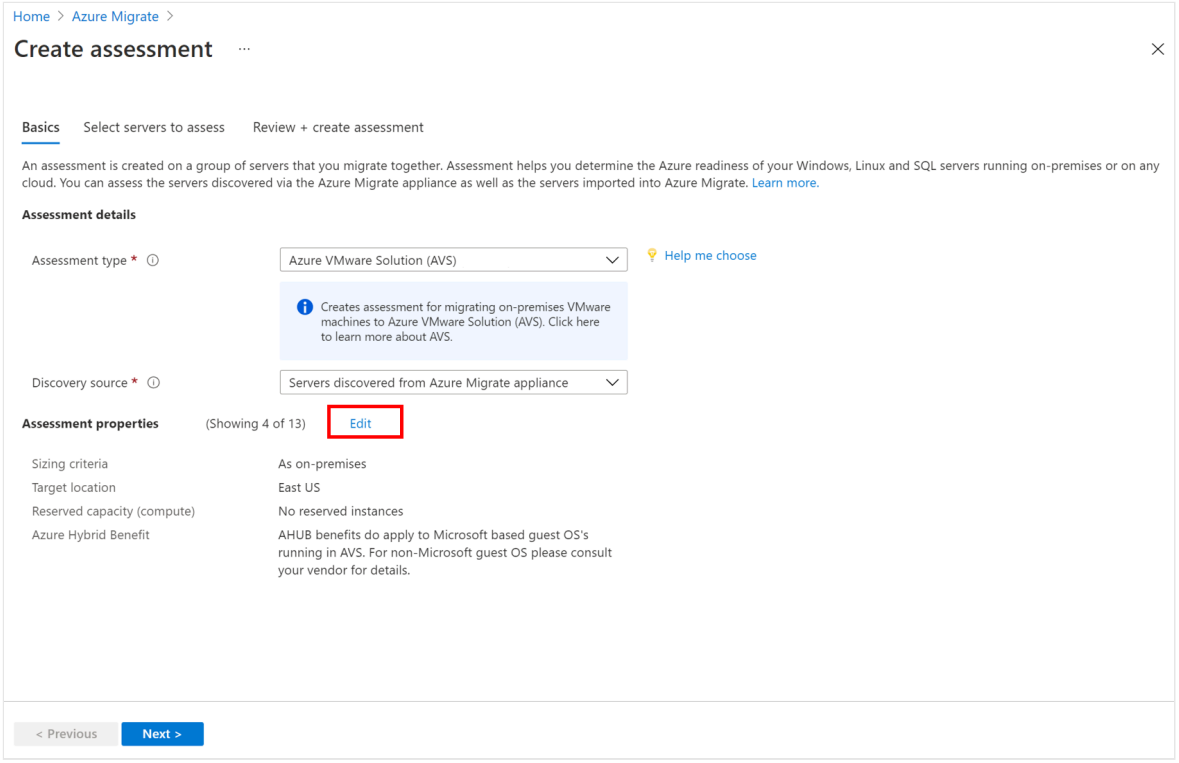
2. In **Azure Migrate: Discovery and assessment**, click **Assess**.

3. In **Assess servers** > **Assessment type**, select **Azure VMware Solution (AVS)**.

4. In **Discovery source**:

    - If you discovered servers using the appliance, select **Servers discovered from Azure Migrate appliance**.
    - If you discovered servers using an imported CSV or RVTools file, select **Imported servers**.

5. Click **Edit** to review the assessment properties.



6. In **Assessment properties** > **Target Properties**:

    - In **Target location**, specify the Azure region to which you want to migrate.
        - Size and cost recommendations are based on the location that you specify.
    - The **Storage type** is defaulted to **vSAN**. This is the default storage type for an Azure VMware Solution private cloud.
    - In **Reserved Instances**, specify whether you want to use reserve instances for Azure VMware Solution nodes when you migrate your VMs.
    - If you select to use a reserved instance, you can't specify '**Discount (%)**
    - Learn more

7. In **VM Size**:

- The **Node type** is defaulted to **AV36**. Azure Migrate recommends the number of nodes needed to migrate the servers to Azure VMware Solution.
- In **FTT setting, RAID level**, select the Failure to Tolerate and RAID combination. The selected FTT option, combined with the on-premises server disk requirement, determines the total vSAN storage required in AVS.
- In **CPU Oversubscription**, specify the ratio of virtual cores associated with one physical core in the AVS node. Oversubscription of greater than 4:1 might cause performance degradation, but can be used for web server type workloads.
- In **Memory overcommit factor**, specify the ratio of memory over commit on the cluster. A value of 1 represents 100% memory use, 0.5 for example is 50%, and 2 would be using 200% of available memory. You can only add values from 0.5 to 10 up to one decimal place.
- In **Dedupe and compression factor**, specify the anticipated deduplication and compression factor for your workloads. Actual value can be obtained from on-premises vSAN or storage config and this may vary by workload. A value of 3 would mean 3x so for 300GB disk only 100GB storage would be used. A value of 1 would mean no dedupe or compression. You can only add values from 1 to 10 up to one decimal place.

8. In **Node Size**:

- In **Sizing criterion**, select if you want to base the assessment on static metadata, or on performance-based data. If you use performance data:
  - In **Performance history**, indicate the data duration on which you want to base the assessment
  - In **Percentile utilization**, specify the percentile value you want to use for the performance sample.

- In **Comfort factor**, indicate the buffer you want to use during assessment. This accounts for issues like seasonal usage, short performance history, and likely increases in future usage. For example, if you use a comfort factor of two:

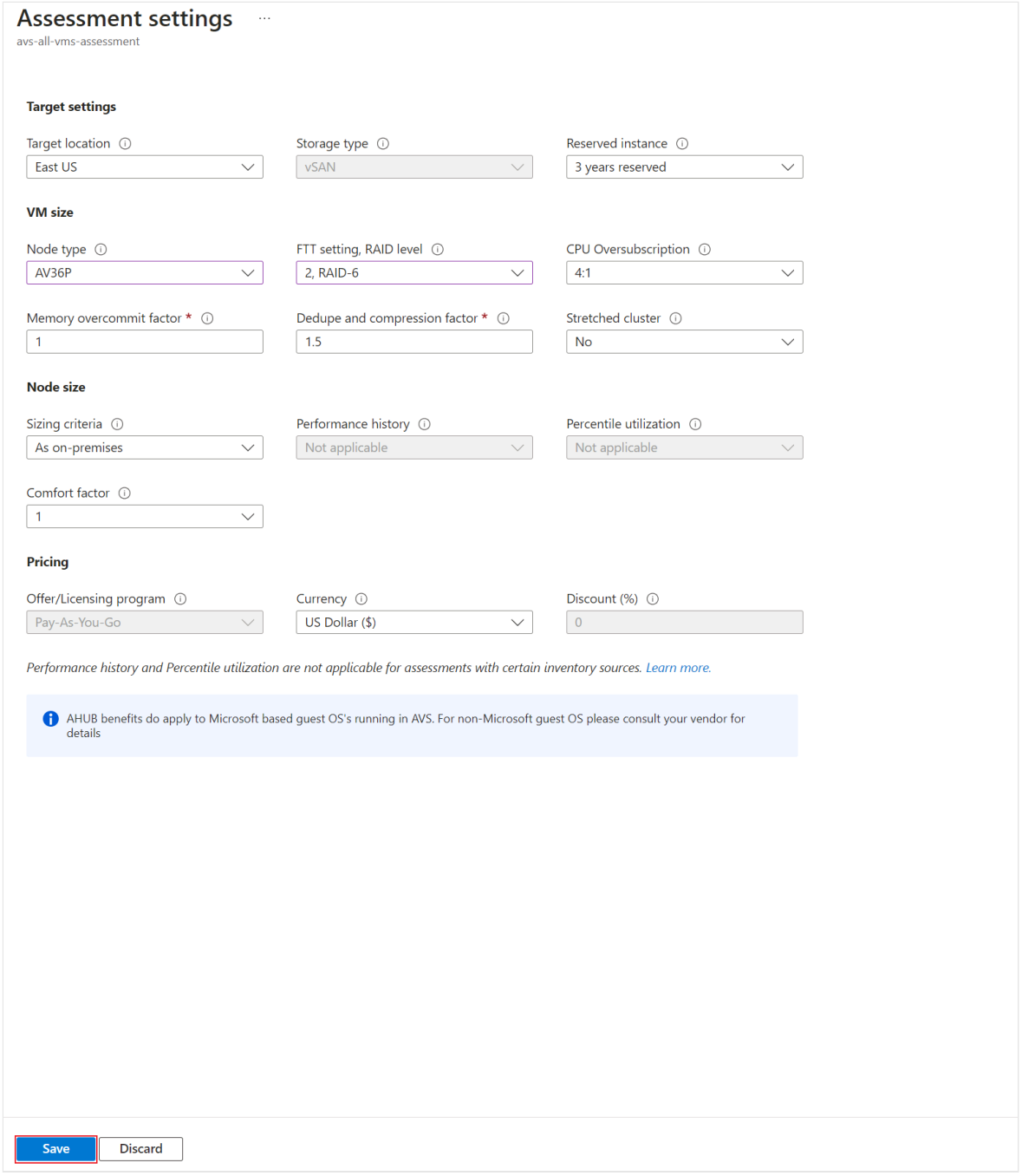
Expand table

Component	Effective utilization	Add comfort factor (2.0)
Cores	2	4
Memory	8 GB	16 GB

9. In **Pricing**:

- In **Offer**, Azure offer you're enrolled in is displayed. The Assessment estimates the cost for that offer.
- In **Currency**, select the billing currency for your account.
- In **Discount (%)**, add any subscription-specific discounts you receive on top of the Azure offer. The default setting is 0%.

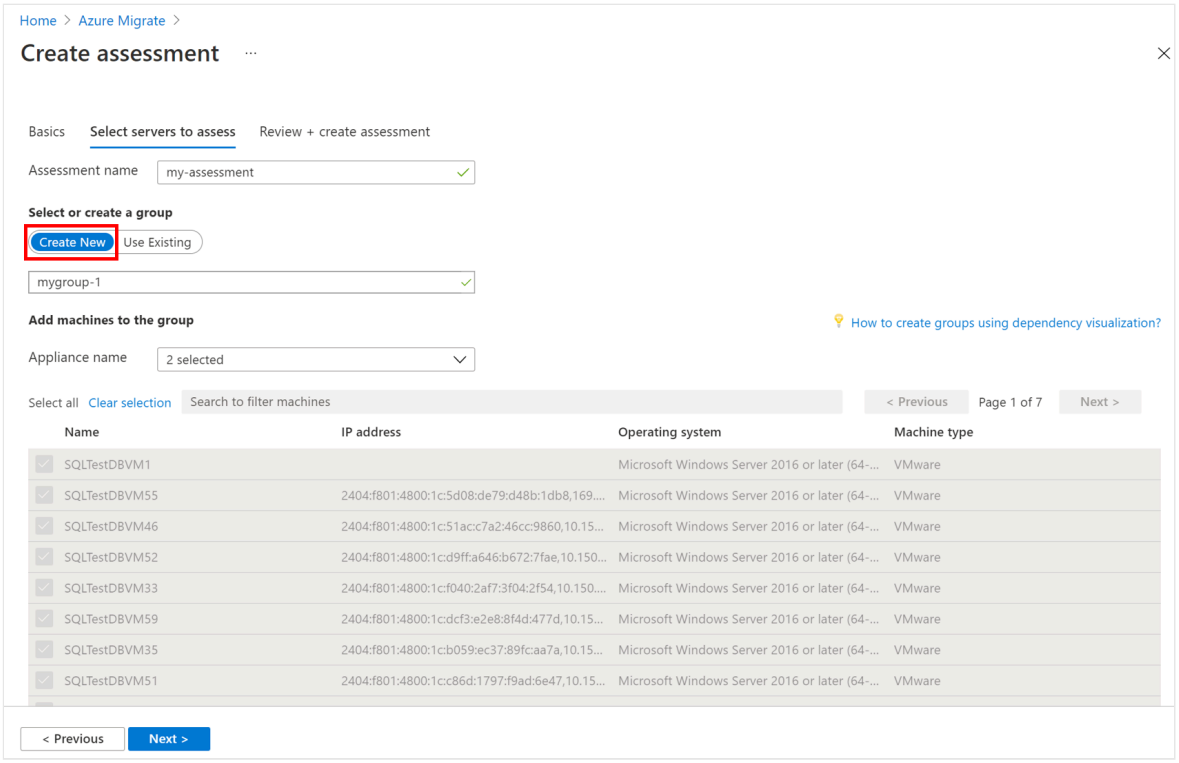
10. Click **Save** if you make changes.



11. In **Assess Servers**, click **Next**.

12. In **Select servers to assess** > **Assessment name** > specify a name for the assessment.

13. In **Select or create a group** > select **Create New** and specify a group name.



14. Select the appliance, and select the servers you want to add to the group. Then click **Next**.

15. In **Review + create assessment**, review the assessment details, and click **Create Assessment** to create the group and run the assessment.

> **Note**
>
> For performance-based assessments, we recommend that you wait at least a day after starting discovery before you create an assessment. This provides time to collect performance data with higher confidence. Ideally, after you start discovery, wait for the performance duration you specify (day/week/month) for a high-confidence rating.

Review an Azure VMware Solution (AVS) assessment

An Azure VMware Solution (AVS) assessment describes:

- **Azure VMware Solution (AVS) readiness**: Whether the on-premises VMs are suitable for migration to Azure VMware Solution (AVS).
- **Number of Azure VMware Solution nodes**: Estimated number of Azure VMware Solution nodes required to run the servers.

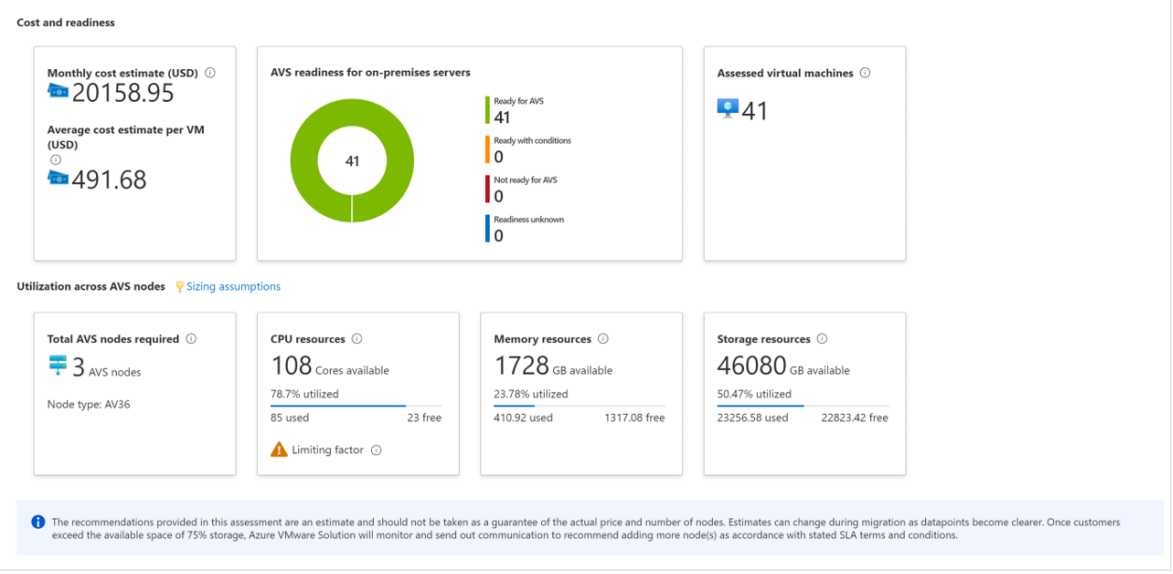
- **Utilization across AVS nodes**: Projected CPU, memory, and storage utilization across all nodes.
  - Utilization includes up front factoring in the following cluster management overheads such as the vCenter Server, NSX Manager (large), NSX Edge, if HCX is deployed also the HCX Manager and IX appliance consuming ~ 44vCPU (11 CPU), 75GB of RAM and 722GB of storage before compression and deduplication.
  - Limiting factor determines the number of hosts/nodes required to accommodate the resources.
- **Monthly cost estimation**: The estimated monthly costs for all Azure VMware Solution (AVS) nodes running the on-premises VMs.

You can click on **Sizing assumptions** to understand the assumptions that went in node sizing and resource utilization calculations. You can also edit the assessment properties, or recalculate the assessment.

View an assessment

1. In **Windows, Linux and SQL Server** > **Azure Migrate: Discovery and assessment**, click the number next to **Azure VMware Solution**.

2. In **Assessments**, select an assessment to open it. As an example (estimations and costs for example only):



3. Review the assessment summary. You can click on **Sizing assumptions** to understand the assumptions that went in node sizing and resource utilization calculations. You can also edit the assessment properties, or recalculate the assessment.

Review Azure VMware Solution (AVS) readiness

1. In **Azure readiness**, verify whether servers are ready for migration to AVS.

2. Review the server status:

    - **Ready for AVS**: The server can be migrated as-is to Azure (AVS) without any changes. It will start in AVS with full AVS support.
    - **Ready with conditions**: There might be some compatibility issues example internet protocol or deprecated OS in VMware and need to be remediated before migrating to Azure VMware Solution. To fix any readiness problems, follow the remediation guidance the assessment suggests.
    - **Not ready for AVS**: The VM will not start in AVS. For example, if the on-premises VMware VM has an external device attached such as a cd-rom the VMware vMotion operation will fail (if using VMware vMotion).
    - **Readiness unknown**: Azure Migrate couldn't determine the readiness of the server because of insufficient metadata collected from the on-premises environment.

3. Review the Suggested tool:

    - **VMware HCX Advanced or Enterprise**: For VMware vSphere VMs, VMware Hybrid Cloud Extension (HCX) solution is the suggested migration tool to migrate your on-premises workload to your Azure VMware Solution (AVS) private cloud. Learn More.
    - **Unknown**: For servers imported via a CSV or RVTools file, the default migration tool is unknown. Though for VMware vSphere VMs, it is suggested to use the VMware Hybrid Cloud Extension (HCX) solution.

4. Click on an **AVS readiness** status. You can view VM readiness details, and drill down to see VM details, including compute, storage, and network settings.

Review cost details

This view shows the estimated cost of running servers in Azure VMware Solution.

1. Review the monthly total costs. Costs are aggregated for all servers in the assessed group.

    - Cost estimates are based on the number of AVS nodes required considering the resource requirements of all the servers in total.
    - As the pricing for Azure VMware Solution is per node, the total cost does not have compute cost and storage cost distribution.

- The cost estimation is for running the on-premises servers in AVS. AVS assessment doesn't consider PaaS or SaaS costs.

2. You can review monthly storage cost estimates. This view shows aggregated storage costs for the assessed group, split over different types of storage disks.

3. You can drill down to see details for specific servers.

Review confidence rating

When you run performance-based assessments, a confidence rating is assigned to the assessment.

- A rating from 1-star (lowest) to 5-star (highest) is awarded.
- The confidence rating helps you estimate the reliability of the size recommendations provided by the assessment.
- The confidence rating is based on the availability of data points needed to compute the assessment.
- For performance-based sizing, AVS assessments need the utilization data for CPU and server memory. The following performance data is collected but not used in sizing recommendations for AVS assessments:
  - The disk IOPS and throughput data for every disk attached to the server.
  - The network I/O to handle performance-based sizing for each network adapter attached to a server.

Confidence ratings for an assessment are as follows.

Expand table

Data point availability	Confidence rating
0%-20%	1 Star
21%-40%	2 Star
41%-60%	3 Star
61%-80%	4 Star
81%-100%	5 Star

Learn more about performance data

Next steps

- Learn how to use dependency mapping to create high confidence groups.
- Learn more about how Azure VMware Solution assessments are calculated.

Request host quota for Azure VMware Solution

Article • 10/09/2024

In this article, learn how to request host quota/capacity for Azure VMware Solution. You learn how to submit a support ticket to have your hosts allocated whether it's for a new deployment or an existing one.

If you have an existing Azure VMware Solution private cloud and want more hosts allocated, follow the same process.

> **Important**
>
> It can take up to five business days to allocate the hosts, depending on the number requested. Therefore, request what you need for provisioning to avoid the delays associated with making additional quota increase requests.

Eligibility criteria

You need an Azure account in an Azure subscription that adheres to one of the following criteria:

- A subscription under an Azure Enterprise Agreement (EA) with Microsoft.
- A Cloud Solution Provider (CSP) managed subscription under an existing CSP Azure offers contract or an Azure plan.
- A Microsoft Customer Agreement (MCA) with Microsoft.

Request host quota for EA and MCA customers

1. In your Azure portal, under **Help + Support**, create a **New support request** and provide the following information:

    - **Issue type:** Technical
    - **Subscription:** Select your subscription
    - **Service:** All services > Azure VMware Solution
    - **Resource:** General question
    - **Summary:** Need capacity
    - **Problem type:** AVS Quota request

> ⓘ Note
>
> If the *Problem Type* is not is not visible from the short-list offered, select **None of the Above**. *AVS Quota requests* will be in the offered list of *Problem Types*.

2. In the **Description** of the support ticket, on the **Details** tab, provide information for:

   - Region Name
   - Number of hosts
   - Host SKU type
   - Any other details, including Stretched Cluster, Availability Zone requirements for integrating with other Azure services; for example, Azure NetApp Files, Azure Blob Storage.

   > ⓘ Note
   >
   > - Azure VMware Solution requires a minimum of three hosts and recommends redundancy of N+1 hosts.
   > - Any unused quota expires after 30 days. A new request will need to be submitted for any additional quota.
   > - **NEW** If requesting quota to leverage Portable VMware Cloud Foundation (VCF) pricing, add the following statement as is, by replacing <N> with the Number of VCF cores you have purchased from Broadcom for license portability to Azure VMware Solution. "***I acknowledge that I have procured portable VCF license from Broadcom for <N> cores to use with Azure VMware Solution.***"

3. Select **Review + Create** to submit the request.

Request host quota for CSP customers

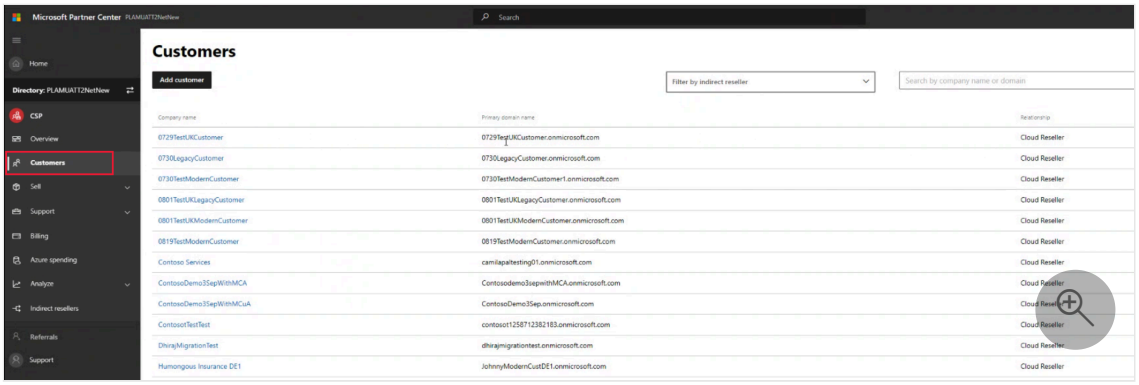
CSPs must use Microsoft Partner Center to enable Azure VMware Solution for their customers. This article uses CSP Azure plan as an example to illustrate the purchase procedure for partners.

Access the Azure portal using the **Admin On Behalf Of (AOBO)** procedure from Partner Center.

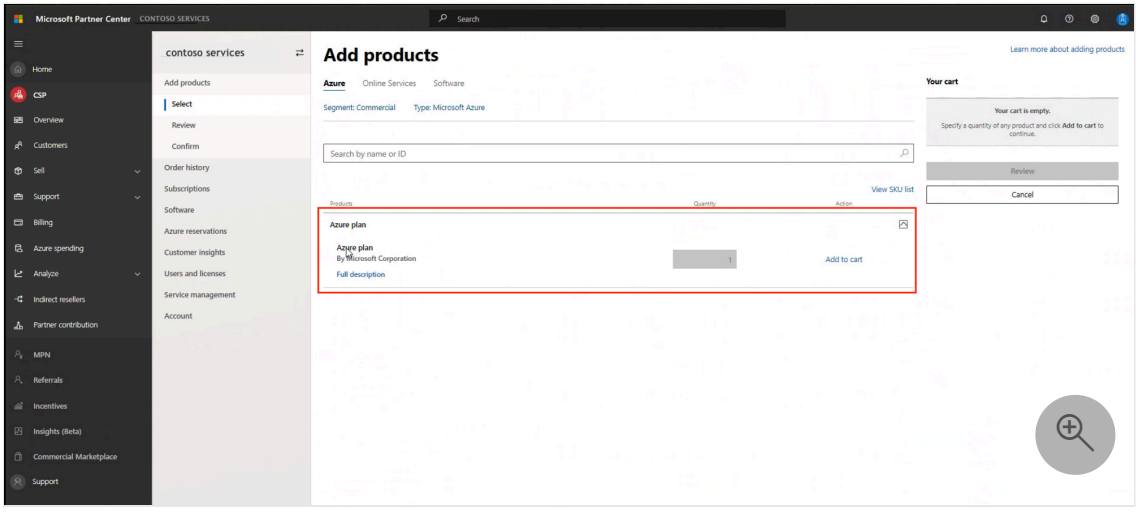
> **ⓘ Important**
>
> Azure VMware Solution service does not provide multi-tenancy support. Hosting partners requiring it are not supported.

1. Configure the CSP Azure plan:

   a. In **Partner Center**, select **CSP** to access the **Customers** area.



   b. Select your customer and then select **Add products**.



   c. Select **Azure plan** and then select **Add to cart**.

   d. Review and finish the general setup of the Azure plan subscription for your customer. For more information, see Microsoft Partner Center documentation.

2. After you configure the Azure plan and you have the needed Azure RBAC permissions in place for the subscription, you'll request the quota for your Azure plan subscription.

   a. Access Azure portal from Microsoft Partner Center using the **Admin On Behalf Of (AOBO)** procedure.

   b. Select **CSP** to access the **Customers** area.

c. Expand customer details and select **Microsoft Azure Management Portal**.

d. In the Azure portal, under **Help + Support**, create a New support request and provide the following information:

- **Issue type:** Technical
- **Subscription:** Select your subscription
- **Service:** All services > Azure VMware Solution
- **Resource:** General question
- **Summary:** Need capacity
- **Problem type:** Capacity Management Issues
- **Problem subtype:** Customer Request for more Host Quota/Capacity

e. In the **Description** of the support ticket, on the **Details** tab, provide information for:

- Region Name
- Number of hosts
- Host SKU type
- Any other details, including Availability Zone requirements for integrating with other Azure services; for example, Azure NetApp Files, Azure Blob Storage.
- Is intended to host multiple customers?

> **Note**
>
> - Azure VMware Solution requires a minimum of three hosts and recommends redundancy of N+1 hosts.
> - Any unused quota expires after 30 days. A new request will need to be submitted for any additional quota.
> - **NEW** If requesting quota to leverage Portable VMware Cloud Foundation (VCF) pricing, add the following statement as is, by replacing <N> with the Number of VCF cores you have purchased from Broadcom for license portability to Azure VMware Solution. ***"I acknowledge that I have procured portable VCF license from Broadcom for <N> cores to use with Azure VMware Solution."***

3. Select **Review + Create** to submit the request.

Next steps

Before deploying Azure VMware Solution, you must first register the resource provider with your subscription to enable the service.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Plan the Azure VMware Solution deployment

Article • 02/05/2024

Planning your Azure VMware Solution deployment is crucial for creating a successful production-ready environment for virtual machines (VMs) and migration. During the planning process, you identify and gather the necessary information for your deployment. Be sure to document the information you collect for easy reference during the deployment. A successful deployment results in a production-ready environment for creating VMs and migration.

In this tutorial, learn how to complete the following tasks:

- ✓ Identify the Azure subscription, resource group, region, and resource name
- ✓ Identify the size hosts and determine the number of clusters and hosts
- ✓ Request a host quota for an eligible Azure plan
- ✓ Identify the /22 CIDR IP segment for private cloud management
- ✓ Identify a single network segment
- ✓ Define the virtual network gateway
- ✓ Define VMware HCX network segments

After you're finished, follow the recommended Next steps at the end of this article to continue with this getting started guide.

Identify the subscription

Identify the subscription you plan to use to deploy Azure VMware Solution. You can create a new subscription or use an existing one.

> ⓘ **Note**
>
> The subscription must be associated with a Microsoft Enterprise Agreement (EA), a Cloud Solution Provider (CSP) Azure plan, or a Microsoft Customer Agreement (MCA). For more information, see **Eligibility criteria**.

Identify the resource group

Identify the resource group you want to use for your Azure VMware Solution. Generally, a resource group is created specifically for Azure VMware Solution, but you can use an

existing resource group.

Identify the region or location

Identify the region you want Azure VMware Solution deployed.

Define the resource name

The resource name is a friendly and descriptive name for your Azure VMware Solution private cloud, for example, **MyPrivateCloud**.

> **Important**
>
> The name must not exceed 40 characters. If the name exceeds this limit, you won't be able to create public IP addresses for use with the private cloud.

Identify the size hosts

Identify the size hosts that you want to use when deploying Azure VMware Solution.

Azure VMware Solution clusters are based upon hyper-converged infrastructure. The following table shows the CPU, memory, disk and network specifications of the host.

Expand table

Host Type	CPU (Cores/GHz)	RAM (GB)	vSAN Cache Tier (TB, raw)	vSAN Capacity Tier (TB, raw)	Regional availability
AV36	Dual Intel Xeon Gold 6140 CPUs (Skylake microarchitecture) with 18 cores/CPU @ 2.3 GHz, Total 36 physical cores (72 logical cores with hyperthreading)	576	3.2 (NVMe)	15.20 (SSD)	Selected regions (*)
AV36P	Dual Intel Xeon Gold 6240 CPUs (Cascade Lake microarchitecture) with 18 cores/CPU @ 2.6 GHz / 3.9 GHz Turbo, Total 36 physical cores (72 logical cores with hyperthreading)	768	1.5 (Intel Cache)	19.20 (NVMe)	Selected regions (*)

Host Type	CPU (Cores/GHz)	RAM (GB)	vSAN Cache Tier (TB, raw)	vSAN Capacity Tier (TB, raw)	Regional availability
AV52	Dual Intel Xeon Platinum 8270 CPUs (Cascade Lake microarchitecture) with 26 cores/CPU @ 2.7 GHz / 4.0 GHz Turbo, Total 52 physical cores (104 logical cores with hyperthreading)	1,536	1.5 (Intel Cache)	38.40 (NVMe)	Selected regions (*)
AV64	Dual Intel Xeon Platinum 8370C CPUs (Ice Lake microarchitecture) with 32 cores/CPU @ 2.8 GHz / 3.5 GHz Turbo, Total 64 physical cores (128 logical cores with hyperthreading)	1,024	3.84 (NVMe)	15.36 (NVMe)	Selected regions (**)

An Azure VMware Solution cluster requires a minimum number of three hosts. You can only use hosts of the same type in a single Azure VMware Solution private cloud. Hosts used to build or scale clusters come from an isolated pool of hosts. Those hosts passed hardware tests and had all data securely deleted before being added to a cluster.

All the above Host Types have 100 Gbps network interface throughput.

(*) details available via the Azure pricing calculator.

(**) AV64 Prerequisite: An Azure VMware Solution private cloud deployed with AV36, AV36P, or AV52 is required prior to adding AV64.

Determine the number of clusters and hosts

The first Azure VMware Solution deployment you do consists of a private cloud containing a single cluster. You need to define the number of hosts you want to deploy to the first cluster for your deployment.

For each private cloud created, there's one vSAN cluster by default. You can add, delete, and scale clusters. The minimum number of hosts per cluster and the initial deployment is three.

You use vCenter Server and NSX-T Manager to manage most aspects of cluster configuration and operation. All local storage of each host in a cluster is under the control of VMware vSAN.

The Azure VMware Solution management and control plane have the following resource requirements that need to be accounted for during solution sizing of a **standard private cloud**.

Expand table

Area	Description	Provisioned vCPUs	Provisioned vRAM (GB)	Provisioned vDisk (GB)	Typical CPU Usage (GHz)	Typical vRAM Usage (GB)	Typical Raw vSAN Datastore Usage (GB)
VMware vSphere	vCenter Server	8	28	915	1.1	3.9	1,854
VMware vSphere	vSphere Cluster Service VM 1	1	0.1	2	0.1	0.1	5
VMware vSphere	vSphere Cluster Service VM 2	1	0.1	2	0.1	0.1	5
VMware vSphere	vSphere Cluster Service VM 3	1	0.1	2	0.1	0.1	5
VMware vSphere	ESXi node 1	N/A	N/A	N/A	5.1	0.2	N/A
VMware vSphere	ESXi node 2	N/A	N/A	N/A	5.1	0.2	N/A
VMware vSphere	ESXi node 3	N/A	N/A	N/A	5.1	0.2	N/A
VMware vSAN	vSAN System Usage	N/A	N/A	N/A	N/A	N/A	5,458
VMware NSX-T Data Center	NSX-T Unified Appliance Node 1	12	48	300	2.5	13.5	613

Area	Description	Provisioned vCPUs	Provisioned vRAM (GB)	Provisioned vDisk (GB)	Typical CPU Usage (GHz)	Typical vRAM Usage (GB)	Typical Raw vSAN Datastore Usage (GB)
VMware NSX-T Data Center	NSX-T Unified Appliance Node 2	12	48	300	2.5	13.5	613
VMware NSX-T Data Center	NSX-T Unified Appliance Node 3	12	48	300	2.5	13.5	613
VMware NSX-T Data Center	NSX-T Edge VM 1	8	32	200	1.3	0.6	409
VMware NSX-T Data Center	NSX-T Edge VM 2	8	32	200	1.3	0.6	409
VMware HCX (Optional Add-On)	HCX Manager	4	12	65	1	2.5	140
VMware Site Recovery Manager (Optional Add-On)	SRM Appliance	4	12	33	1	1	79
VMware vSphere (Optional Add-On)	vSphere Replication Manager Appliance	4	8	33	1	0.6	75
VMware vSphere (Optional Add-On)	vSphere Replication Server Appliance	2	1	33	1	0.3	68
	Total	77 vCPUs	269.3 GB	2,385 GB	30 GHz	50.4 GB	10,346 GB (9,032

Area	Description	Provisioned vCPUs	Provisioned vRAM (GB)	Provisioned vDisk (GB)	Typical CPU Usage (GHz)	Typical vRAM Usage (GB)	Typical Raw vSAN Datastore Usage (GB)

The Azure VMware Solution management and control plane have the following resource requirements that need to be accounted for during solution sizing of a **stretched clusters private cloud**. VMware SRM isn't included in the table since it currently isn't supported.

Expand table

Area	Description	Provisioned vCPUs	Provisioned vRAM (GB)	Provisioned vDisk (GB)	Typical CPU Usage (GHz)	Typical vRAM Usage (GB)	Typical Raw vSAN Datastore Usage (GB)
VMware vSphere	vCenter Server	8	28	915	1.1	3.9	3,708
VMware vSphere	vSphere Cluster Service VM 1	1	0.1	2	0.1	0.1	5
VMware vSphere	vSphere Cluster Service VM 2	1	0.1	2	0.1	0.1	5
VMware vSphere	vSphere Cluster Service VM 3	1	0.1	2	0.1	0.1	5
VMware vSphere	ESXi node 1	N/A	N/A	N/A	5.1	0.2	N/A
VMware vSphere	ESXi node 2	N/A	N/A	N/A	5.1	0.2	N/A
VMware vSphere	ESXi node 3	N/A	N/A	N/A	5.1	0.2	N/A
VMware vSphere	ESXi node 4	N/A	N/A	N/A	5.1	0.2	N/A

Area	Description	Provisioned vCPUs	Provisioned vRAM (GB)	Provisioned vDisk (GB)	Typical CPU Usage (GHz)	Typical vRAM Usage (GB)	Typical Raw vSAN Datastore Usage (GB)
VMware vSphere	ESXi node 5	N/A	N/A	N/A	5.1	0.2	N/A
VMware vSphere	ESXi node 6	N/A	N/A	N/A	5.1	0.2	N/A
VMware vSAN	vSAN System Usage	N/A	N/A	N/A	N/A	N/A	10,722
VMware NSX-T Data Center	NSX-T Unified Appliance Node 1	12	48	300	2.5	13.5	1,229
VMware NSX-T Data Center	NSX-T Unified Appliance Node 2	12	48	300	2.5	13.5	1,229
VMware NSX-T Data Center	NSX-T Unified Appliance Node 3	12	48	300	2.5	13.5	1,229
VMware NSX-T Data Center	NSX-T Edge VM 1	8	32	200	1.3	0.6	817
VMware NSX-T Data Center	NSX-T Edge VM 2	8	32	200	1.3	0.6	817
VMware HCX (Optional Add-On)	HCX Manager	4	12	65	1	2.5	270
	Total	67 vCPUs	248.3 GB	2,286 GB	42.3 GHz	49.1 GB	20,036 GB (17,173 GB with

Area	Description	Provisioned vCPUs	Provisioned vRAM (GB)	Provisioned vDisk (GB)	Typical CPU Usage (GHz)	Typical vRAM Usage (GB)	Typical Raw vSAN Datastore Usage (GB)
							expected 1.2x Data Reduction ratio)

These resource requirements only apply to the first cluster deployed in an Azure VMware Solution private cloud. Subsequent clusters only need to account for the vSphere Cluster Service, ESXi resource requirements and vSAN System Usage in solution sizing.

The virtual appliance **Typical Raw vSAN Datastore Usage** values account for the space occupied by virtual machine files, including configuration and log files, snapshots, virtual disks and swap files.

The VMware ESXi nodes have compute usage values that account for the vSphere VMkernel hypervisor overhead, vSAN overhead and NSX-T distributed router, firewall and bridging overhead. These are estimates for a standard three cluster configuration. The storage requirements are listed as not applicable (N/A) since a boot volume separate from the vSAN Datastore is used.

The VMware vSAN System Usage storage overhead accounts for vSAN performance management objects, vSAN file system overhead, vSAN checksum overhead and vSAN deduplication and compression overhead. To view this consumption, select the Monitor, vSAN Capacity object for the vSphere Cluster in the vSphere Client.

The VMware HCX and VMware Site Recovery Manager resource requirements are optional Add-ons to the Azure VMware Solution service. Discount these requirements in the solution sizing if they aren't being used.

The VMware Site Recovery Manager Add-On has the option of configuring multiple VMware vSphere Replication Server Appliances. The previous table assumes one vSphere Replication Server appliance is used.

Sizing an Azure VMware Solution is an estimate; the sizing calculations from the design phase should be validated during the testing phase of a project to ensure the Azure VMware Solution is sized correctly for the application workload.

> **Tip**

You can always extend the cluster and add additional clusters later if you need to go beyond the initial deployment number.

> **Note**
>
> To learn about the limits for the number of hosts per cluster, the number of clusters per private cloud, and the number of hosts per private cloud, check **Azure subscription and service limits, quotas, and constraints**.

Request a host quota

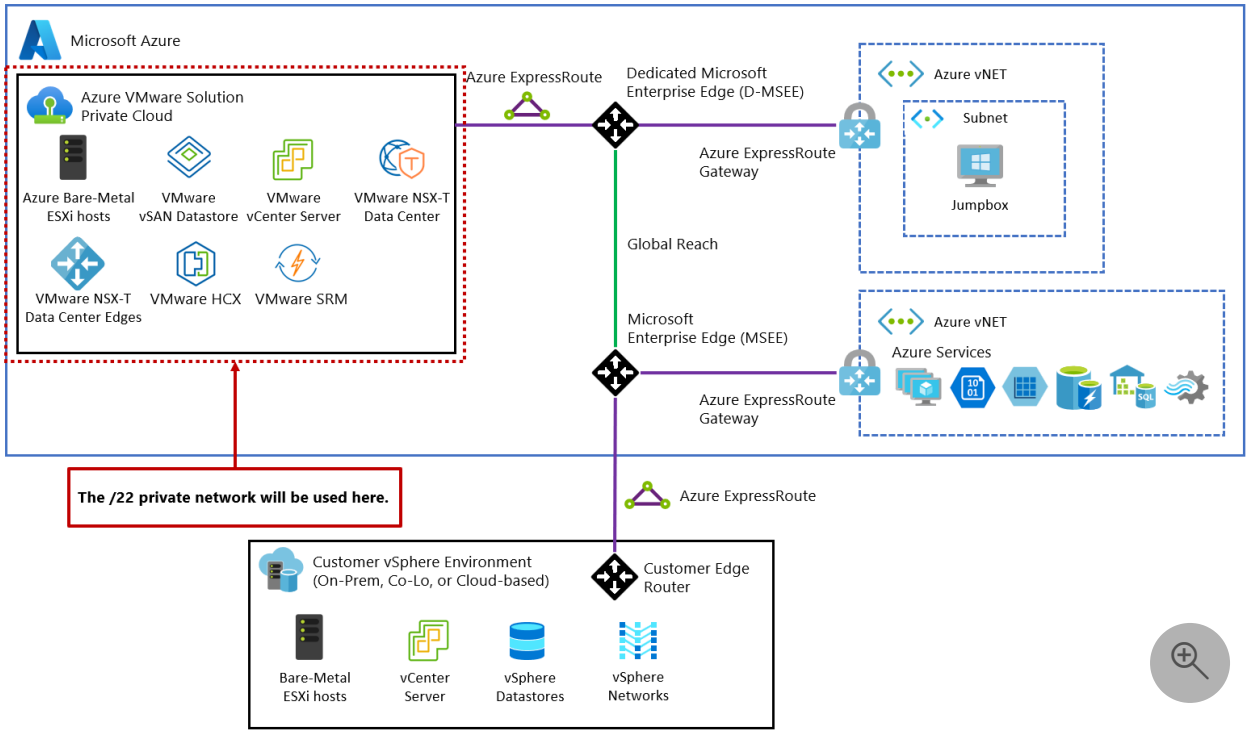
Request a host quota early in the planning process to ensure a smooth deployment of your Azure VMware Solution private cloud. Before making a request, identify the Azure subscription, resource group, and region. Determine the size of hosts, number of clusters, and hosts you need.

The support team takes up to five business days to confirm your request and allocate your hosts.

- EA customers
- CSP customers

Define the IP address segment for private cloud management

Azure VMware Solution requires a /22 CIDR network, such as `10.0.0.0/22`. This address space is divided into smaller network segments (subnets) for Azure VMware Solution management segments including vCenter Server, VMware HCX, NSX-T Data Center, and vMotion functionality. The following diagram shows Azure VMware Solution management IP address segments.

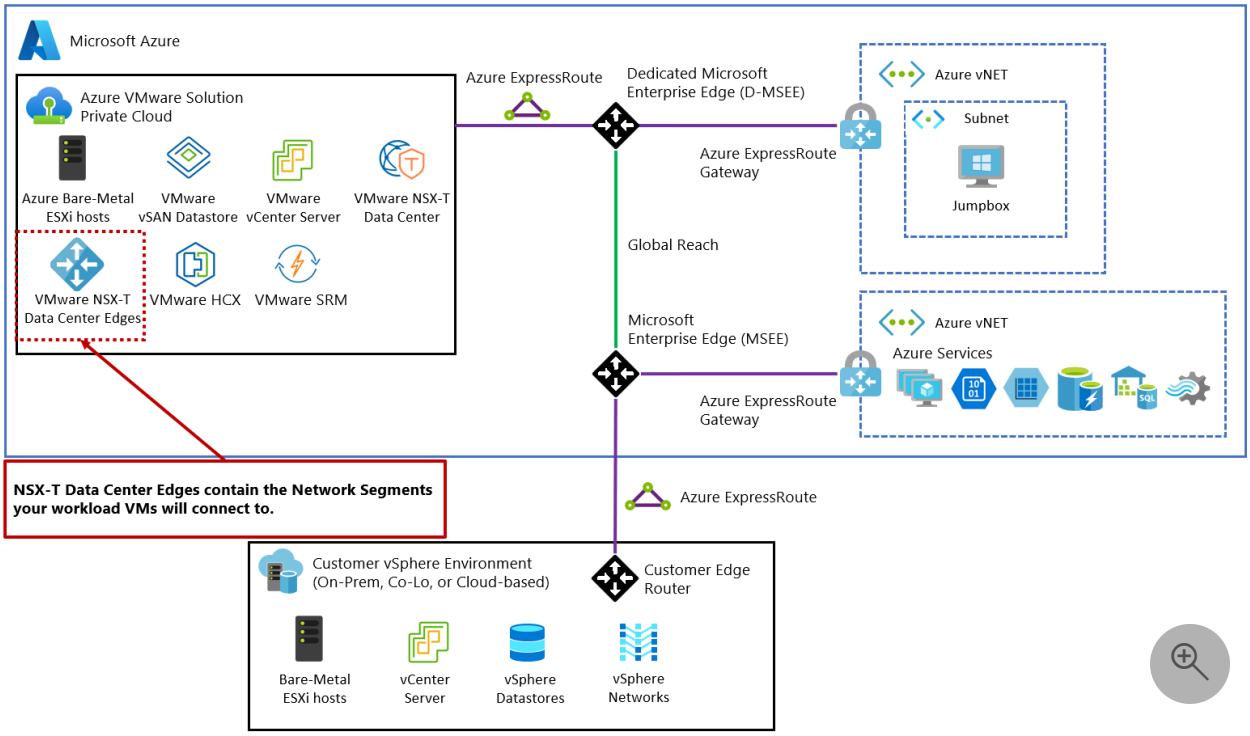


> **Important**
>
> The /22 CIDR network address block shouldn't overlap with any existing network segment you already have on-premises or in Azure. For details of how the /22 CIDR network is broken down per private cloud, see Routing and subnet considerations.

Define the IP address segment for VM workloads

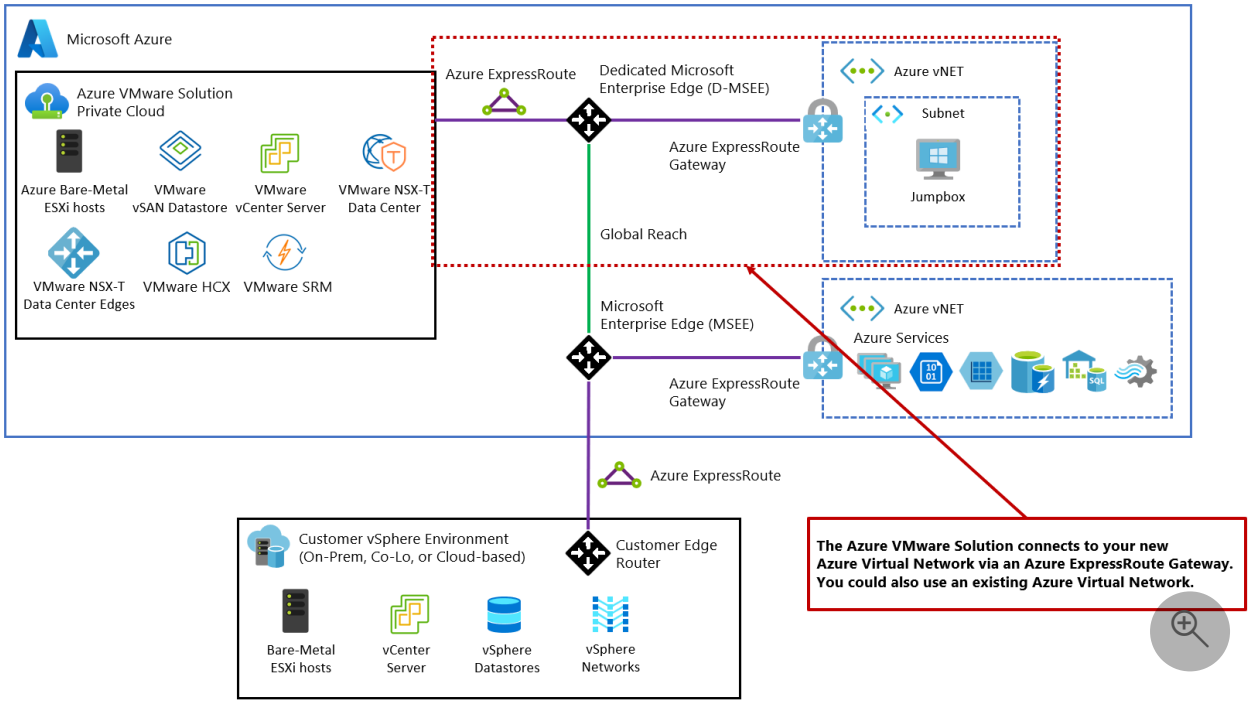
In a VMware vSphere environment, VMs must connect to a network segment. As Azure VMware Solution production deployment expands, you often see a combination of L2 extended segments from on-premises and local NSX-T Data Center network segments.

For the initial deployment, identify a single network segment (IP network), for example, `10.0.4.0/24`. This network segment is used primarily for testing purposes during the initial deployment. The address block shouldn't overlap with any network segments on-premises or within Azure and shouldn't be within the /22 network segment already defined.



Define the virtual network gateway

Azure VMware Solution requires an Azure Virtual Network and an ExpressRoute circuit. Decide whether to use an *existing* or *new* ExpressRoute virtual network gateway. If you choose a *new* virtual network gateway, create it after creating your private cloud. Using an existing ExpressRoute virtual network gateway is acceptable. For planning purposes, note which ExpressRoute virtual network gateway you use.



Important

You can connect to a virtual network gateway in an Azure Virtual WAN, but it is out of scope for this quick start.

Define VMware HCX network segments

VMware HCX is an application mobility platform that simplifies application migration, workload rebalancing, and business continuity across data centers and clouds. You can migrate your VMware vSphere workloads to Azure VMware Solution and other connected sites through various migration types.

VMware HCX Connector deploys a subset of virtual appliances (automated) that require multiple IP segments. When you create your network profiles, you use the IP segments. Identify the following listed items for the VMware HCX deployment, which supports a pilot or small product use case. Modify as necessary based on your migration needs.

- **Management network:** For on-premises VMware HCX deployment, identify a management network for VMware HCX. Typically, it's the same management network used by your on-premises VMware vSphere cluster. At a minimum, identify **two** IPs on this network segment for VMware HCX. You might need larger numbers, depending on the scale of your deployment beyond the pilot or small use case.

  > ⓘ **Note**
  >
  > For large environments, create a new /26 network and present it as a port group to your on-premises VMware vSphere cluster instead of using the existing management network. You can then create up to 10 service meshes and 60 network extenders (-1 per service mesh). You can stretch **eight** networks per network extender by using Azure VMware Solution private clouds.

- **Uplink network:** For on-premises VMware HCX deployment, identify an Uplink network for VMware HCX. Use the same network you plan to use for the Management network.

- **vMotion network:** For on-premises VMware HCX deployment, identify a vMotion network for VMware HCX. Typically, it's the same network used for vMotion by your on-premises VMware vSphere cluster. At a minimum, identify **two** IPs on this network segment for VMware HCX. You might need larger numbers, depending on the scale of your deployment beyond the pilot or small use case.

You must expose the vMotion network on a distributed virtual switch or vSwitch0. If it's not, modify the environment to accommodate.

> **Note**
>
> Many VMware vSphere environments use non-routed network segments for vMotion, which poses no problems.

- **Replication network:** For on-premises VMware HCX deployment, define a replication network. Use the same network you're using for your Management and Uplink networks. If the on-premises cluster hosts use a dedicated Replication VMkernel network, reserve **two** IP addresses in this network segment and use the Replication VMkernel network for the replication network.

Determine whether to extend your networks

Optionally, you can extend network segments from on-premises to Azure VMware Solution. If you extend network segments, identify those networks now following these guidelines:

- Networks must connect to a vSphere Distributed Switch (vDS) in your on-premises VMware environment.
- Networks that are on a vSphere Standard Switch can't be extended.

> **Important**
>
> These networks are extended as a final step of the configuration, not during deployment.

Next steps

Now that you gathered and documented the necessary information, continue to the next tutorial to create your Azure VMware Solution private cloud.

Deploy Azure VMware Solution

Deploy and configure Azure VMware Solution

Article • 05/15/2024

After you plan your deployment, deploy and configure your Azure VMware Solution private cloud.

In this tutorial, you'll:

- ✓ Register the resource provider and create a private cloud
- ✓ Connect to a new or existing ExpressRoute virtual network gateway
- ✓ Validate the network connection

Once you completed this section, follow the next steps provided at the end of this tutorial.

Register the Microsoft.AVS resource provider

To use Azure VMware Solution, you must first register the resource provider with your subscription. For more information about resource providers, see Azure resource providers and types.

Portal

1. Sign in to the Azure portal.

   > **Note**
   >
   > If you need access to the Azure US Gov portal, go to https://portal.azure.us/

2. On the Azure portal menu, select **All services**.
3. In the **All services** box, enter **subscription**, and then select **Subscriptions**.
4. Select the subscription from the subscription list to view.
5. Select **Resource providers** and enter **Microsoft.AVS** into the search.

6. If the resource provider isn't registered, select **Register**.

Create an Azure VMware Solution private cloud

You can create an Azure VMware Solution private cloud using the Azure portal or the Azure CLI.

Portal

1. Sign in to the Azure portal.

   > **Note**
   >
   > If you need access to the Azure US Gov portal, go to https://portal.azure.us/

2. Select **Create a resource**.

3. In the **Search services and marketplace** text box, type `Azure VMware Solution` and select it from the search results.

4. On the **Azure VMware Solution** window, select **Create**.

5. If you need more hosts, request a host quota increase.

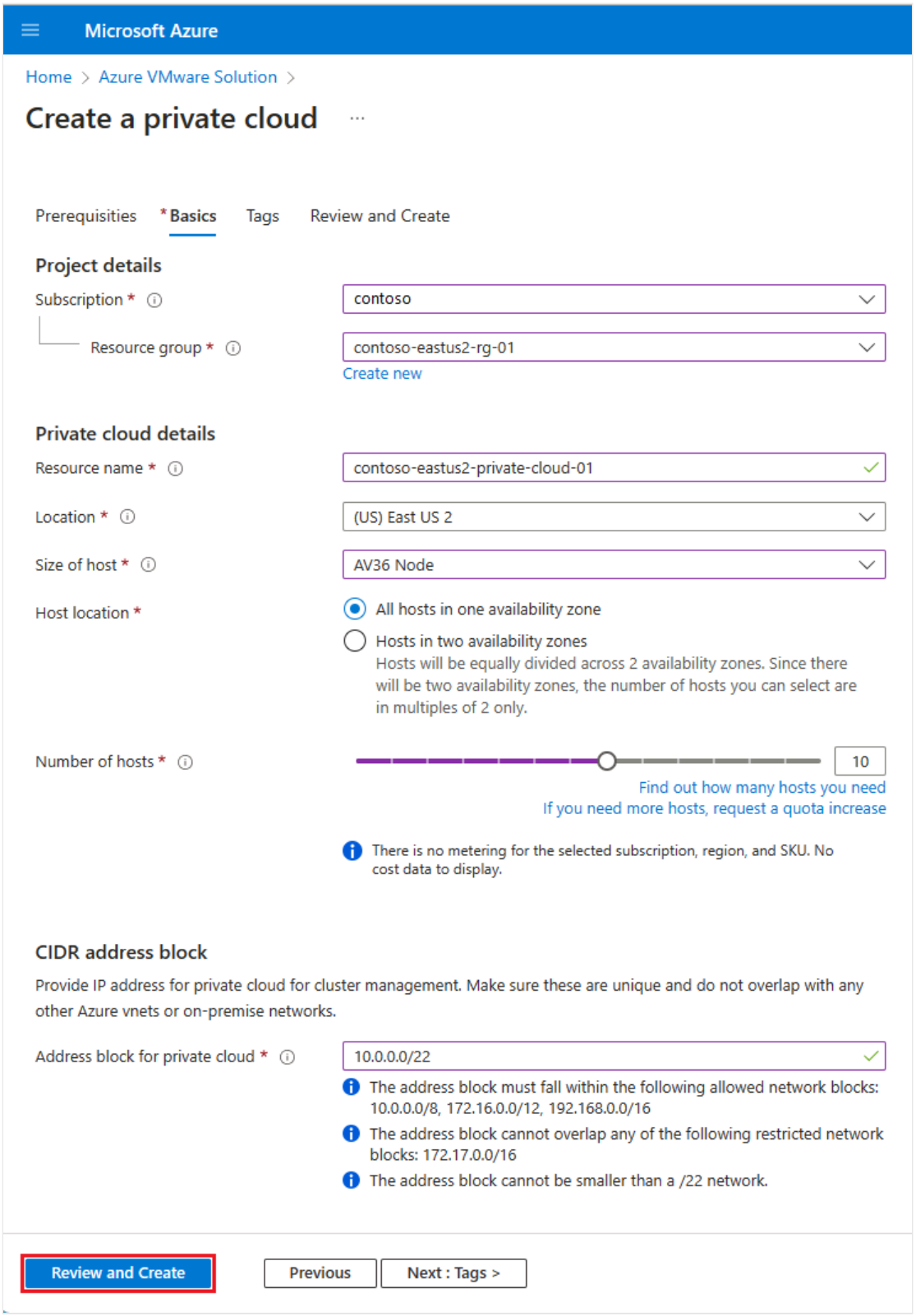
6. On the **Basics** tab, enter values for the fields and then select **Review + Create**.

   > **Tip**
   >
   > You gathered this information during the planning phase of this quick start.

Expand table

Field	Value
Subscription	Select the subscription you plan to use for the deployment. All resources in an Azure subscription are billed together.

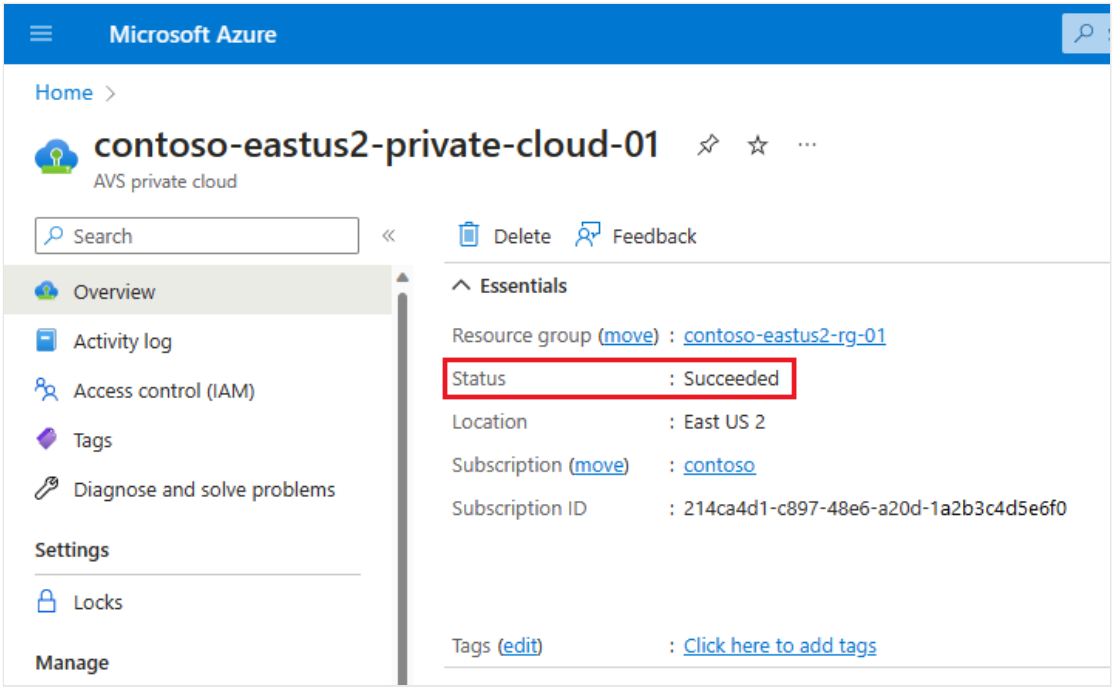
Field	Value
Resource group	Select the resource group for your private cloud. An Azure resource group is a logical container into which Azure resources are deployed and managed. Alternatively, you can create a new resource group for your private cloud.
Resource name	Provide the name of your Azure VMware Solution private cloud.
Location	Select a location, such as **(US) East US 2**. It's the *region* you defined during the planning phase.
Size of host	Select the **AV36**, **AV36P** or **AV52** SKU.
Host Location	Select **All hosts in one availability zone** for a standard private cloud or **Hosts in two availability zones** for stretched clusters.
Number of hosts	Number of hosts allocated for the private cloud cluster. The default value is 3, which you can increase or decrease after deployment. If these nodes aren't listed as available, contact support to request a quota increase. You can also select the link labeled **If you need more hosts, request a quota increase** in the Azure portal.
Address block for private cloud	Provide an IP address block for the private cloud. The CIDR represents the private cloud management network and is used for the cluster management services, such as vCenter Server and NSX-T Manager. Use /22 address space, for example, 10.175.0.0/22. The address should be unique and not overlap with other Azure Virtual Networks and with on-premises networks.



7. Verify the information entered, and if correct, select **Create**.

> **Note**
>
> This step takes roughly 3-4 hours. Adding a single host in an existing or the same cluster takes between 30 - 45 minutes.

8. Verify that the deployment was successful. Navigate to the resource group you created and select your private cloud. You see the status of **Succeeded** when the deployment is finished.



Connect to Azure Virtual Network with ExpressRoute

In the planning phase, you defined whether to use an *existing* or *new* ExpressRoute virtual network gateway.

> **ⓘ Important**
>
> If you plan to scale your Azure VMware Solution hosts using Azure NetApp Files datastores, deploying the vNet close to your hosts with an ExpressRoute virtual network gateway is crucial. The closer the storage is to your hosts, the better the performance.

Use a new ExpressRoute virtual network gateway

> **ⓘ Important**
>
> You must have a virtual network with a GatewaySubnet that **does not** already have a virtual network gateway.

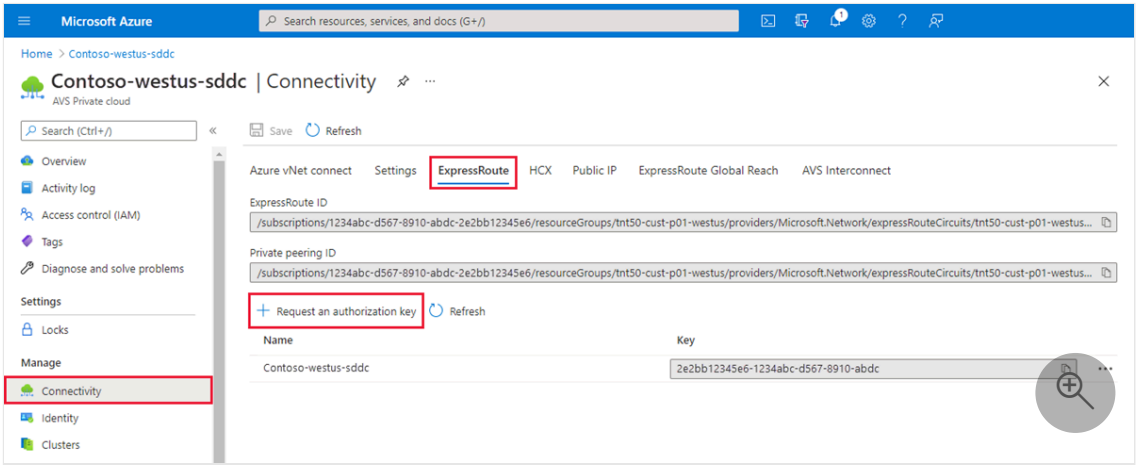
Expand table

If	Then
You don't already have a virtual network...	Create the following: 1. Virtual network 2. GatewaySubnet 3. Virtual network gateway 4. Connect ExpressRoute to the gateway
You already have a virtual network **without** a GatewaySubnet...	Create the following: 1. GatewaySubnet 2. Virtual network gateway 3. Connect ExpressRoute to the gateway
You already have a virtual network **with** a GatewaySubnet...	Create the following: 1. Virtual network gateway 2. Connect ExpressRoute to the gateway

Use an existing virtual network gateway

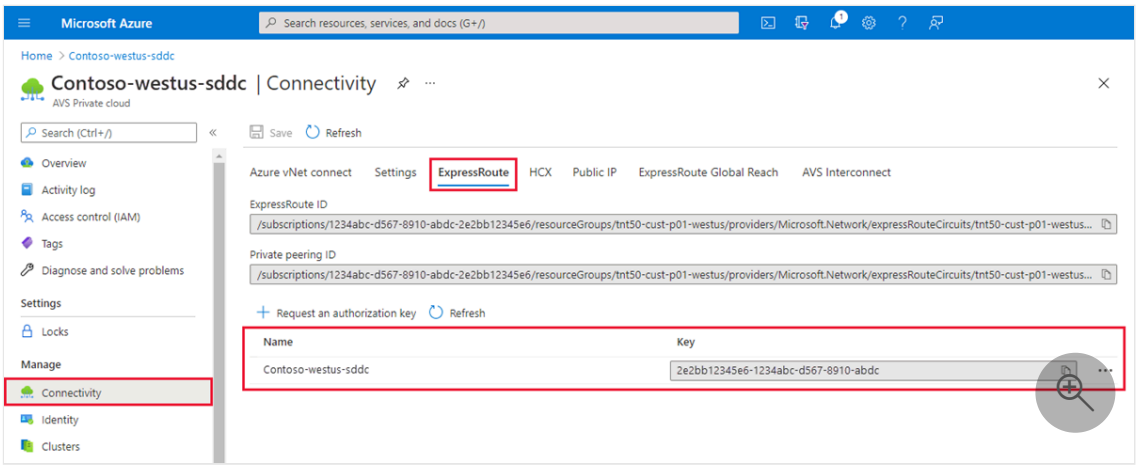
1. Request an ExpressRoute authorization key:

   a. In the Azure portal, navigate to the Azure VMware Solution private cloud. Select **Manage** > **Connectivity** > **ExpressRoute** and then select **+ Request an authorization key**.



   b. Provide a name for it and select **Create**.

It can take about 30 seconds to create the key. Once created, the new key appears in the list of authorization keys for the private cloud.



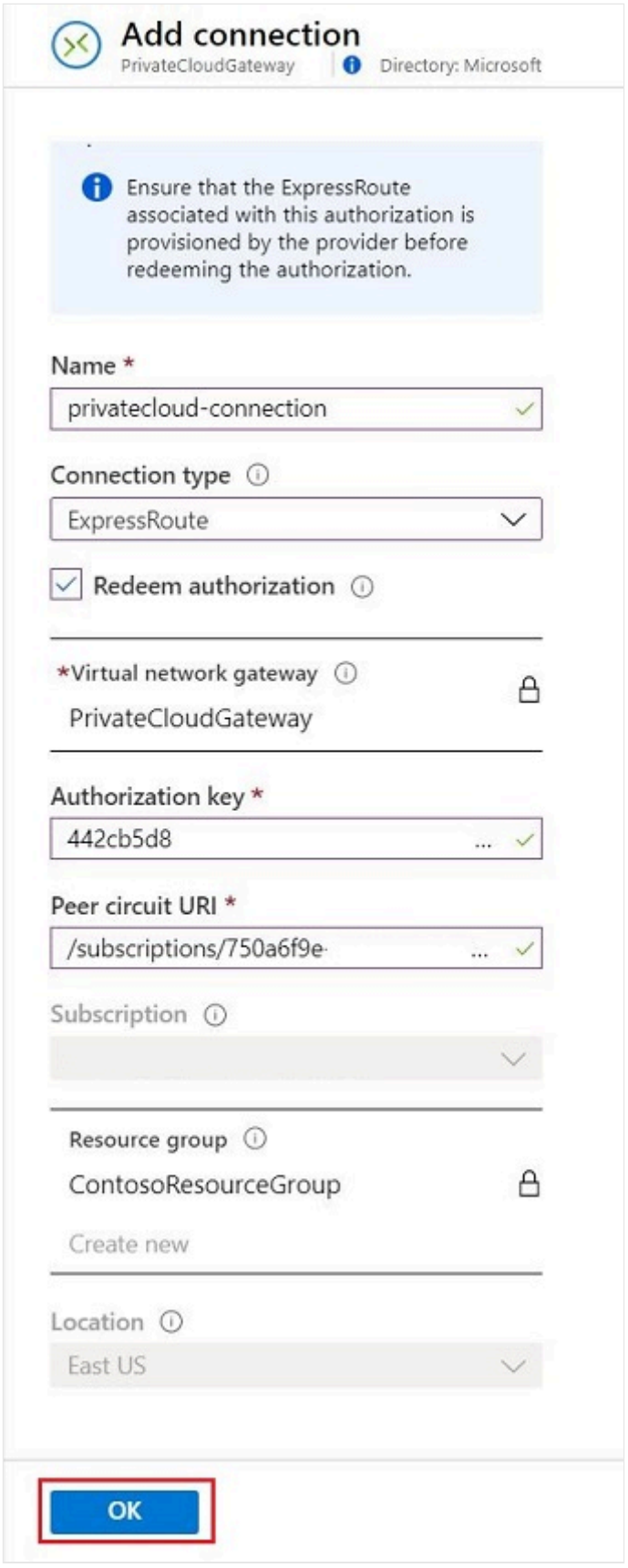
c. Copy the authorization key and ExpressRoute ID. You need them to complete the peering. The authorization key disappears after some time, so copy it as soon as it appears.

2. Navigate to the virtual network gateway you plan to use and select **Connections** > **+ Add**.

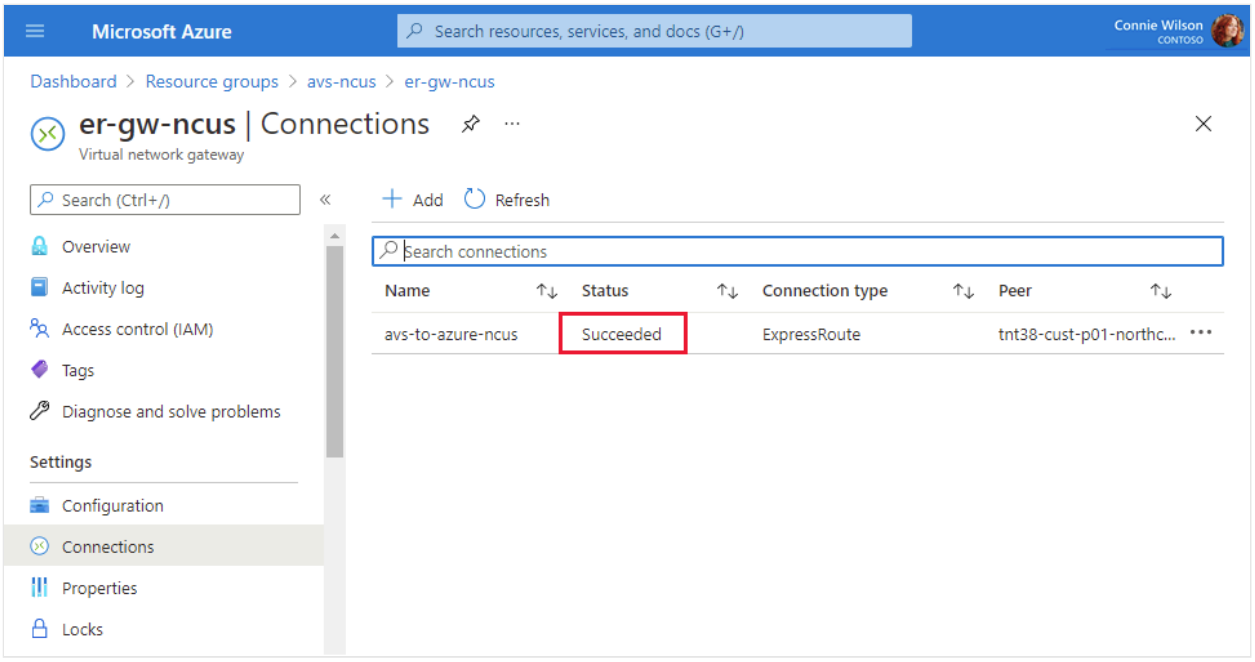
3. On the **Add connection** page, provide values for the fields, and select **OK**.

Expand table

Field	Value
Name	Enter a name for the connection.
Connection type	Select **ExpressRoute**.
Redeem authorization	Ensure this box is selected.
Virtual network gateway	The virtual network gateway you intend to use.
Authorization key	Paste the authorization key you copied earlier.
Peer circuit URI	Paste the ExpressRoute ID you copied earlier.



The connection between your ExpressRoute circuit and your Virtual Network is created.



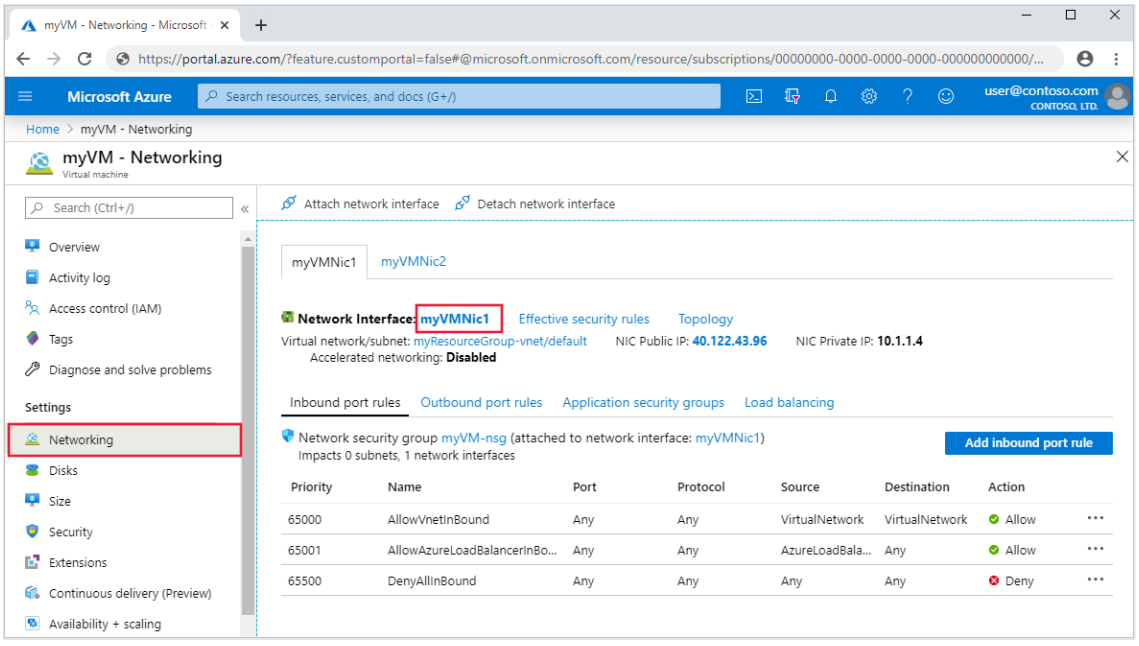
Validate the connection

Ensure connectivity between the Azure Virtual Network where the ExpressRoute terminates and the Azure VMware Solution private cloud.

1. Use a virtual machine within the Azure Virtual Network where the Azure VMware Solution ExpressRoute terminates. For more information, see Connect to Azure Virtual Network with ExpressRoute.

   a. Sign in to the Azure portal.

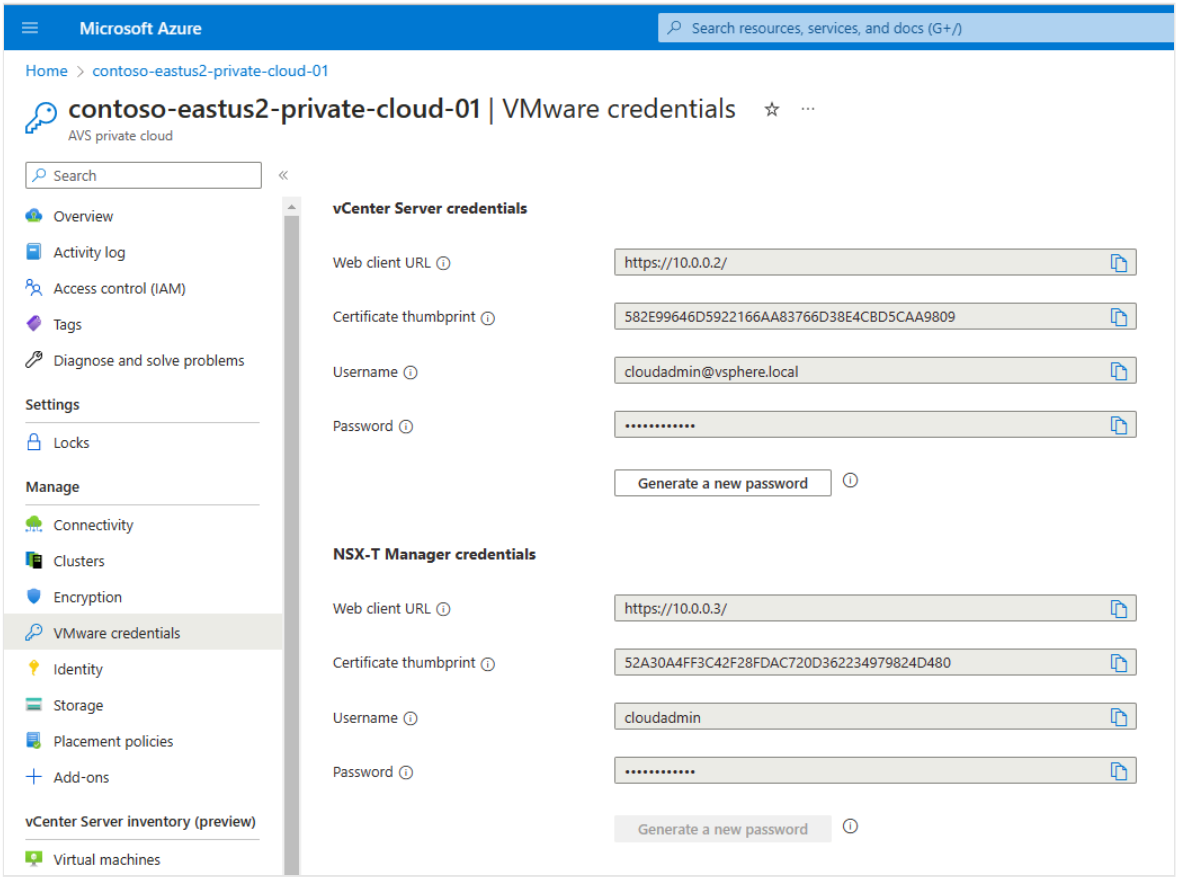
   b. Navigate to a running VM, and under **Settings**, select **Networking** and the network interface resource.



c. On the left, select **Effective routes**. A list of address prefixes that are contained within the `/22` CIDR block you entered during the deployment phase displays.

2. To sign in to both vCenter Server and NSX Manager, open a web browser and sign in to the same virtual machine used for network route validation.

   Find the vCenter Server and NSX Manager console's IP addresses and credentials in the Azure portal. Select your private cloud and then **Manage** > **VMware credentials**.



Next steps

In the next tutorial, you'll connect Azure VMware Solution to your on-premises network through ExpressRoute.

Connect to your on-premises environment

Deploy vSAN stretched clusters

Article • 03/28/2024

In this article, learn how to implement a vSAN stretched cluster for an Azure VMware Solution private cloud.

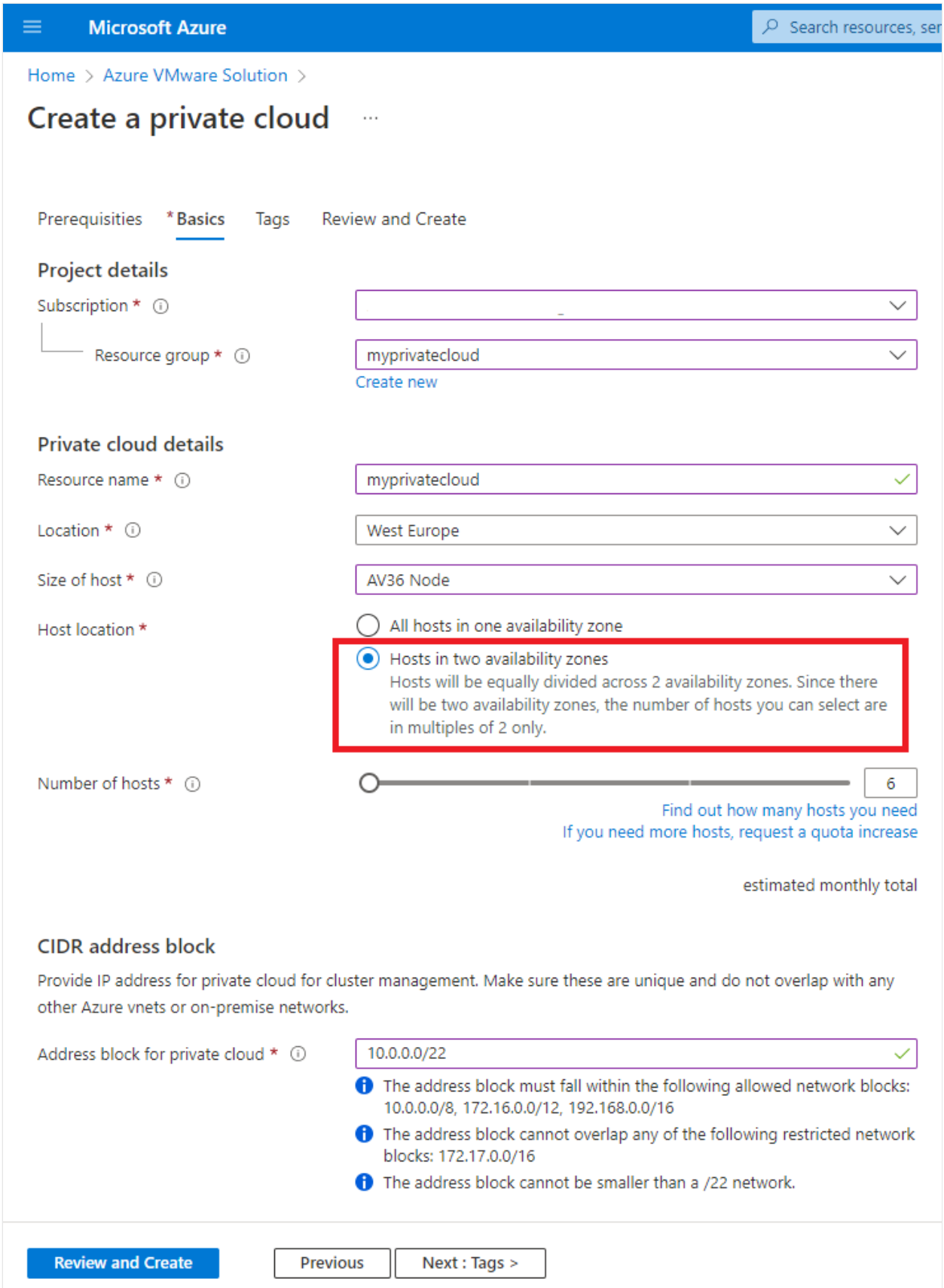
Prerequisites

Follow the Request Host Quota process to get the quota reserved for the required number of nodes. Provide the following details to facilitate the process:

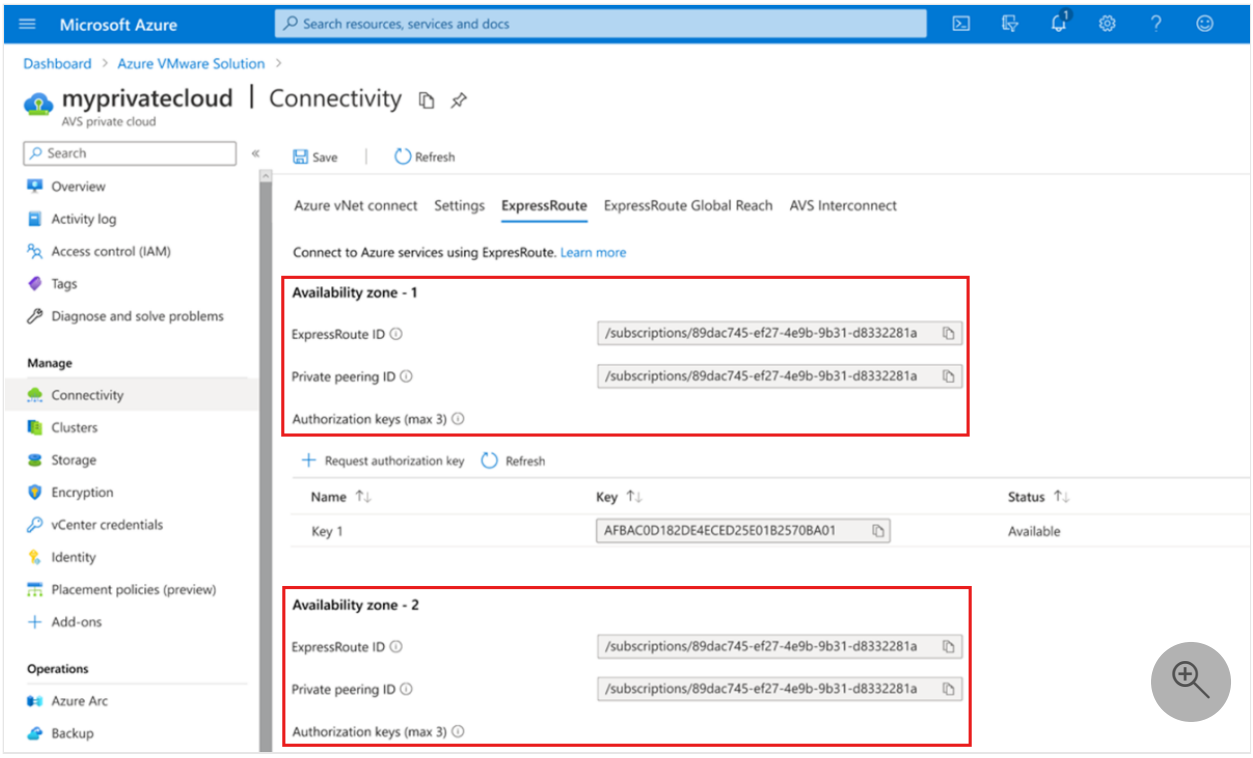
- Company name
- Point of contact: email
- Subscription ID: a new, separate subscription is required
- Type of private cloud: "Stretched Cluster"
- Region requested: UK South, West Europe, Germany West Central, or Australia East
- Number of nodes in first stretched cluster: minimum 6, maximum 16 - in multiples of two
- Estimated expansion plan

Deploy a stretched cluster private cloud

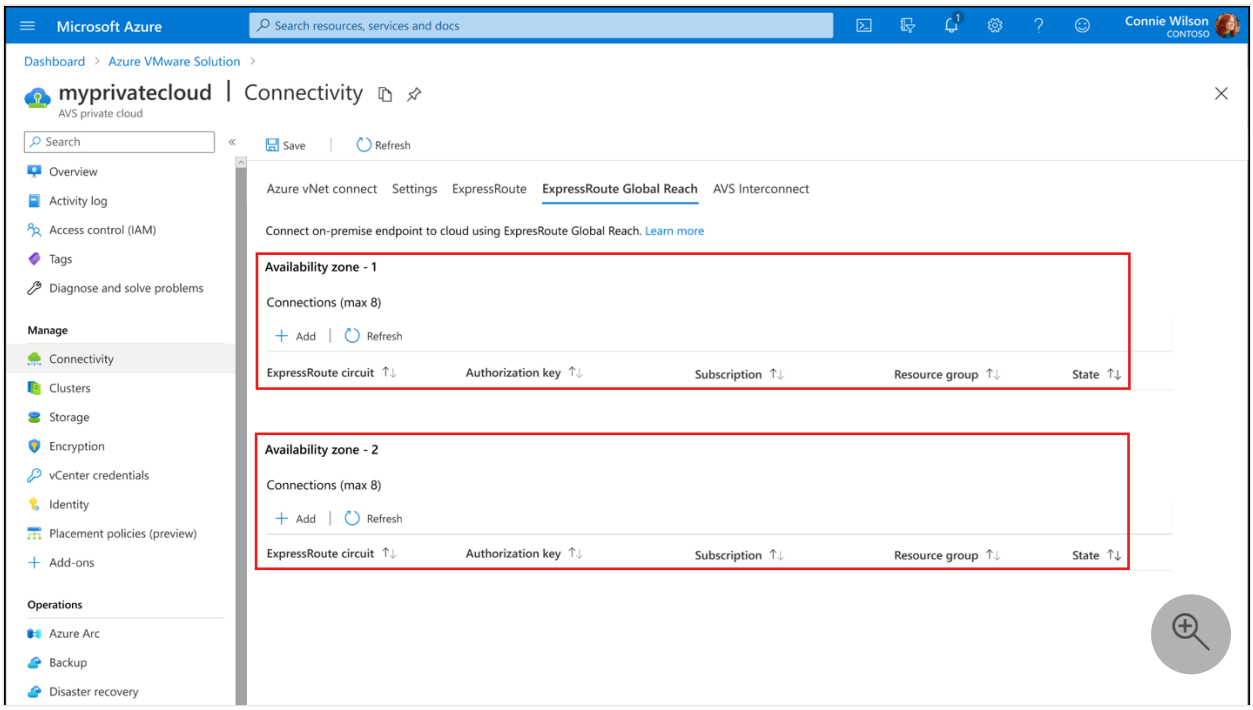
When the request support details are received, quota is reserved for a stretched cluster environment in the region requested. The subscription gets enabled to deploy a stretched cluster SDDC through the Azure portal. A confirmation email is sent to the designated point of contact within two business days upon which you should be able to self-deploy a stretched cluster private cloud via the Azure portal. Be sure to select **Hosts in two availability zones** to ensure that a stretched cluster gets deployed in the region of your choice.



Once the private cloud is created, you can peer both availability zones (AZs) to your on-premises ExpressRoute circuit with Global Reach that helps connect your on-premises data center to the private cloud. Peering both the AZs ensures that an AZ failure doesn't result in a loss of connectivity to your private cloud. Since an ExpressRoute Auth Key is valid for only one connection, repeat the Create an ExpressRoute auth key in the on-premises ExpressRoute circuit process to generate another authorization.



Next, repeat the process to peer ExpressRoute Global Reach two availability zones to the on-premises ExpressRoute circuit.



Storage policies supported

The following SPBM policies are supported with a Primary Failures To Tolerate (PFTT) of "Dual Site Mirroring" and Secondary Failures To Tolerate (SFTT) of "RAID 1 (Mirroring)" enabled as the default policies for the cluster:

- Site disaster tolerance settings (PFTT):

    - Dual site mirroring
    - None - keep data on preferred
    - None - keep data on nonpreferred
- Local failures to tolerate (SFTT):
    - 1 failure – RAID 1 (Mirroring)
    - 1 failure – RAID 5 (Erasure coding), requires a minimum of four hosts in each AZ
    - 2 failures – RAID 1 (Mirroring)
    - 2 failures – RAID 6 (Erasure coding), requires a minimum of six hosts in each AZ
    - 3 failures – RAID 1 (Mirroring)

Create a placement policy in Azure VMware Solution

Article • 03/22/2024

In Azure VMware Solution, clusters in a private cloud are a managed resource. As a result, the CloudAdmin role can't make certain changes to the cluster from the vSphere Client, including the management of Distributed Resource Scheduler (DRS) rules.

The placement policy feature is available in all Azure VMware Solution regions. Placement policies let you control the placement of virtual machines (VMs) on hosts within a cluster through the Azure portal. When you create a placement policy, it includes a DRS rule in the specified vSphere cluster. It also includes other logic for interoperability with Azure VMware Solution operations.

A placement policy has at least five required components:

- **Name** - Defines the name of the policy and is subject to the naming constraints of Azure Resources.
- **Type** - Defines the type of control you want to apply to the resources contained in the policy.
- **Cluster** - Defines the cluster for the policy. The scope of a placement policy is a vSphere cluster, so only resources from the same cluster can be part of the same placement policy.
- **State** - Defines if the policy is enabled or disabled. In certain scenarios, a policy might be disabled automatically when a conflicting rule gets created. For more information, see Considerations.
- **Virtual machine** - Defines the VMs and hosts for the policy. Depending on the type of rule you create, your policy might require you to specify some number of VMs and hosts. For more information, see Placement policy types.

Prerequisite

You must have *Contributor* level access to the private cloud to manage placement policies.

Placement policy types

VM-VM policies

VM-VM policies specify if selected VMs should run on the same host or must be kept on separate hosts. In addition to choosing a name and cluster for the policy, **VM-VM** policies require that you select at least two VMs to assign. The assignment of hosts isn't required or permitted for this policy type.

- **VM-VM Affinity** policies instruct DRS to try to keeping the specified VMs together on the same host. It's useful for performance reasons, for example.
- **VM-VM Anti-Affinity** policies instruct DRS to try keeping the specified VMs apart from each other on separate hosts. It's useful in availability scenarios where a problem with one host doesn't affect multiple VMs within the same policy.

VM-Host policies

VM-Host policies specify if selected VMs can run on selected hosts. To avoid interference with platform-managed operations such as host maintenance mode and host replacement, **VM-Host** policies in Azure VMware Solution are always preferential (also known as "should" rules). Accordingly, **VM-Host** policies may not be honored in certain scenarios. For more information, see Monitor the operation of a policy.

Certain platform operations dynamically update the list of hosts defined in **VM-Host** policies. For example, when you delete a host that is a member of a placement policy, the host is removed when more than one host is part of that policy. Also, if a host is part of a policy and needs to be replaced as part of a platform-managed operation, the policy is updated dynamically with the new host.

In addition to choosing a name and cluster for the policy, a **VM-Host** policy requires that you select at least one VM and one host to assign to the policy.

- **VM-Host Affinity** policies instruct DRS to try running the specified VMs on the hosts defined.
- **VM-Host Anti-Affinity** policies instruct DRS to try running the specified VMs on hosts other than the ones defined.

Considerations

Cluster scale-in

Azure VMware Solution attempts to prevent certain DRS rule violations from occurring when performing cluster scale-in operations.

You can't remove the last host from a VM-Host policy. However, if you need to remove the last host from the policy, you can remediate it by adding another host to the policy before removing the host from the cluster. Alternatively, you can delete the placement policy before removing the host.

You can't have a VM-VM Anti Affinity policy with more VMs than the number of hosts in a cluster. If removing a host results in fewer hosts in the cluster than VMs, you receive an error preventing the operation. You can remediate it by first removing VMs from the rule and then removing the host from the cluster.

Rule conflicts

If DRS rule conflicts are detected when you create a VM-VM policy, it results in that policy being created in a disabled state following standard VMware DRS Rule behavior. For more information on viewing rule conflicts, see Monitor the operation of a policy.

Create a placement policy

There's no defined limit to the number of policies that you create. However, the more placement constraints you create, the more challenging it is for vSphere DRS to effectively move virtual machines within the cluster and provide the resources needed by the workloads.

Make sure to review the requirements for the policy type.

1. In your Azure VMware Solution private cloud, under **Manage**, select **Placement policies** > + **Create**.

   > **Tip**
   >
   > You may also select the Cluster from the Placement Policy overview pane and then select **Create**.

2. Provide a descriptive name, select the policy type, and select the cluster where the policy is created. Then select **Enabled**.

   > **Warning**

If you disable the policy, then the policy and the underlying DRS rule are created, but the policy actions are ignored until you enable the policy.

3. If you selected **VM-Host affinity** or **VM-Host anti-affinity** as the type, select **+ Add hosts** and the hosts to include in the policy. You can select multiple hosts.

> **Note**
>
> The select hosts pane shows how many VM-Host policies are associated with the host and the total number of VMs contained in those associated policies.

4. Select **+ Add virtual machine** and the VMs to include in the policy. You can select multiple VMs.

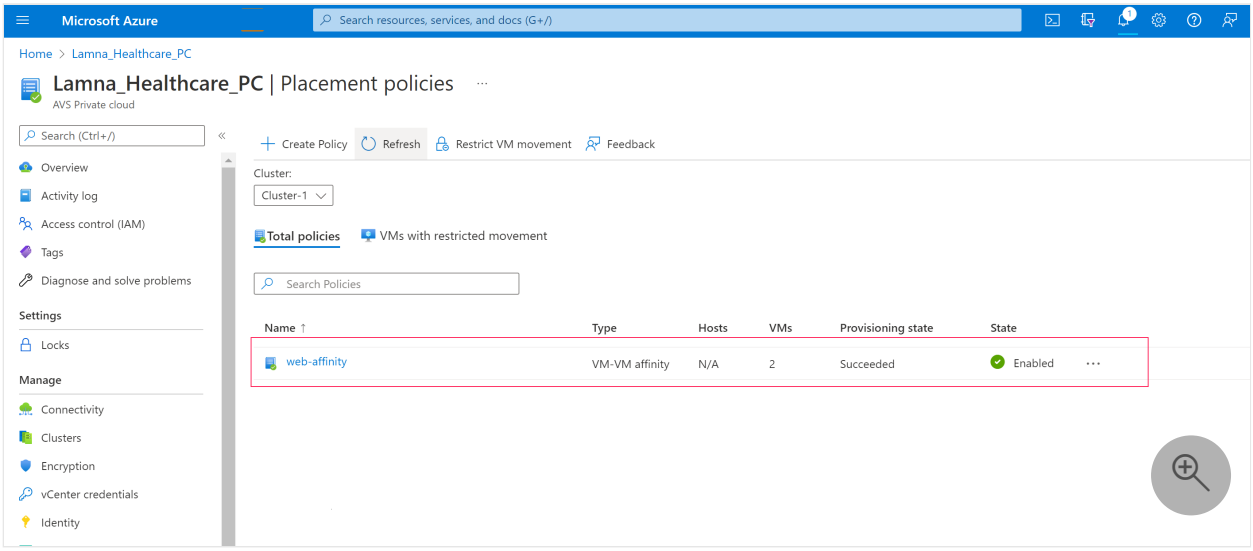
> **Note**
>
> The select hosts pane shows how many VM-Host policies are associated with the host and the total number of VMs contained in those associated policies.

5. Once you finish adding the VMs you want, select **Add virtual machines**.

6. Select **Next: Review and create** to review your policy.

7. Select **Create policy**. If you want to make changes, select **Back: Basics**.

8. After the placement policy gets created, select **Refresh** to see it in the list.



Edit a placement policy

You can change the state of a policy, add a new resource, or unassign an existing resource.

Change the policy state

You can change the state of a policy to **Enabled** or **Disabled**.

1. In your Azure VMware Solution private cloud, under **Manage**, select **Placement policies**.
2. For the policy you want to edit, select **More** (...) and then select **Edit**.

   > **Tip**
   >
   > You can disable a policy from the Placement policy overview by selecting **Disable** from the Settings drop-down. You can't enable a policy from the Settings drop-down.

3. If the policy is enabled but you want to disable it, select **Disabled** and then select **Disabled** on the confirmation message. Otherwise, if the policy is disabled and you want to enable it, select **Enable**.
4. Select **Review + update**.
5. Review the changes and select **Update policy**. If you want to make changes, select **Back: Basics**.

Update the resources in a policy

You can add new resources, such as a VM or a host, to a policy or remove existing ones.

1. In your Azure VMware Solution private cloud, under **Manage**, select **Placement policies**.
2. For the policy you want to edit, select **More** (...) and then **Edit**.
   To remove an existing resource, select one or more resources you want to remove and select **Unassign**.
   To add a new resource, select **Edit virtual machine** or **Edit host**, select the resource you'd like to add, and then select **Save**.
3. Select **Next : Review and update**.

4. Review the changes and select **Update policy**. If you want to make changes, select **Back : Basics**.

Delete a policy

You can delete a placement policy and its corresponding DRS rule.

1. In your Azure VMware Solution private cloud, under **Manage**, select **Placement policies**.
2. For the policy you want to edit, select **More** (...) and then select **Delete**.
3. Select **Delete** on the confirmation message.

Monitor the operation of a policy

Use the vSphere Client to monitor the operation of a placement policy's corresponding DRS rule.

As a holder of the CloudAdmin role, you can view, but not edit, the DRS rules created by a placement policy on the cluster's Configure tab under VM/Host Rules. It lets you view additional information, such as if the DRS rules are in a conflict state.

Additionally, you can monitor various DRS rule operations, such as recommendations and faults, from the cluster's Monitor tab.

Restrict VM Movement

For certain sensitive applications, vMotion can cause unexpected service interruptions or disruptions. For these types of applications, it might be preferred to restrict VM movement to manually initiated vMotion only. With the Restrict VM movement Placement Policy, DRS-initiated vMotions can be disabled. For most workloads, this isn't necessary and can cause unintended performance impacts due to noisy neighbors on the same host.

Enable Restrict VM movement for specific VMs

1. Navigate to Manage Placement policies and select Restrict VM movement.
2. Select the VM or VMs you want to restrict, then select Select.
3. The VM or VMS you selected appears in the VMs with restricted movement tab. In the vSphere Client, a VM override is created to set DRS to *partially automated*

for that VM.
DRS will no longer migrate the VM automatically.
Manual vMotion of the VM and automatic initial placement of the VM continues to function.

FAQs

Are placement policies the same as DRS affinity rules?

Yes, and no. While vSphere DRS implements the current set of policies, we simplified the experience. Modifying VM groups and Host groups are a cumbersome operation, especially as hosts are ephemeral in nature and could be replaced in a cloud environment. As hosts are replaced in the vSphere inventory in an on-premises environment, the vSphere admin must modify the host group to ensure that the desired VM-Host placement constraints remain in effect. Placement policies in Azure VMware Solution update the Host groups when a host is rotated or changed. Similarly, if you scale in a cluster, the Host Group is automatically updated, as applicable. The automatic update eliminates the overhead of managing the Host Groups for the customer.

As this is an existing functionality available in vCenter Server, why can't I use it directly?

Azure VMware Solution provides a private cloud in Azure. In this managed VMware solution infrastructure, Microsoft manages the clusters, hosts, datastores, and distributed virtual switches in the private cloud. At the same time, the tenant is responsible for managing the workloads deployed on the private cloud. As a result, the tenant administering the private cloud doesn't have the same set of privileges as available to the VMware solution administrator in an on-premises deployment.

Further, the lack of the desired granularity in the vSphere privileges presents some challenges when managing the placement of the workloads on the private cloud. For example, vSphere DRS rules commonly used on-premises to define affinity and anti-affinity rules can't be used as-is in an Azure VMware Solution environment, as some of those rules can block day-to-day operation the private cloud. Placement Policies provides a way to define those rules using the Azure portal, thereby circumventing the need to use DRS rules. Coupled with a simplified experience, Placement Policies ensure the rules don't impact the day-to-day infrastructure maintenance and operation activities.

What is the difference between the VM-Host affinity policy and Restrict VM movement?

A VM-Host affinity policy is used to restrict the movement of VMs to a group of hosts included in the VM-Host affinity policy. Thus, a VM can be vMotioned within the set of hosts selected in the VM-Host affinity policy. Alternatively, **Restrict VM movement** ensures that the selected VM remains on the host on which it currently resides.

What caveats should I know about?

The VM-Host **MUST** rules aren't supported because they block maintenance operations.

VM-Host **SHOULD** rules are preferential rules, where vSphere DRS tries to accommodate the rules to the extent possible. Occasionally, vSphere DRS may vMotion VMs subjected to the VM-Host **SHOULD** rules to ensure that the workloads get the resources they need. It's a standard vSphere DRS behavior, and the Placement policies feature doesn't change the underlying vSphere DRS behavior.

If you create conflicting rules, those conflicts can show up on the vCenter Server, and the newly defined rules might not take effect. It's a standard vSphere DRS behavior, the logs for which can be observed in the vCenter Server.

Monitor and protect VMs with Azure native services

Article • 03/21/2024

Microsoft Azure native services let you monitor, manage, and protect your virtual machines (VMs) in a hybrid environment (Azure, Azure VMware Solution, and on-premises). In this article, learn how to integrate Azure native services into your Azure VMware Solution private cloud and use the tools to manage your VMs throughout their lifecycle.

The Azure native services that you can integrate with Azure VMware Solution include:

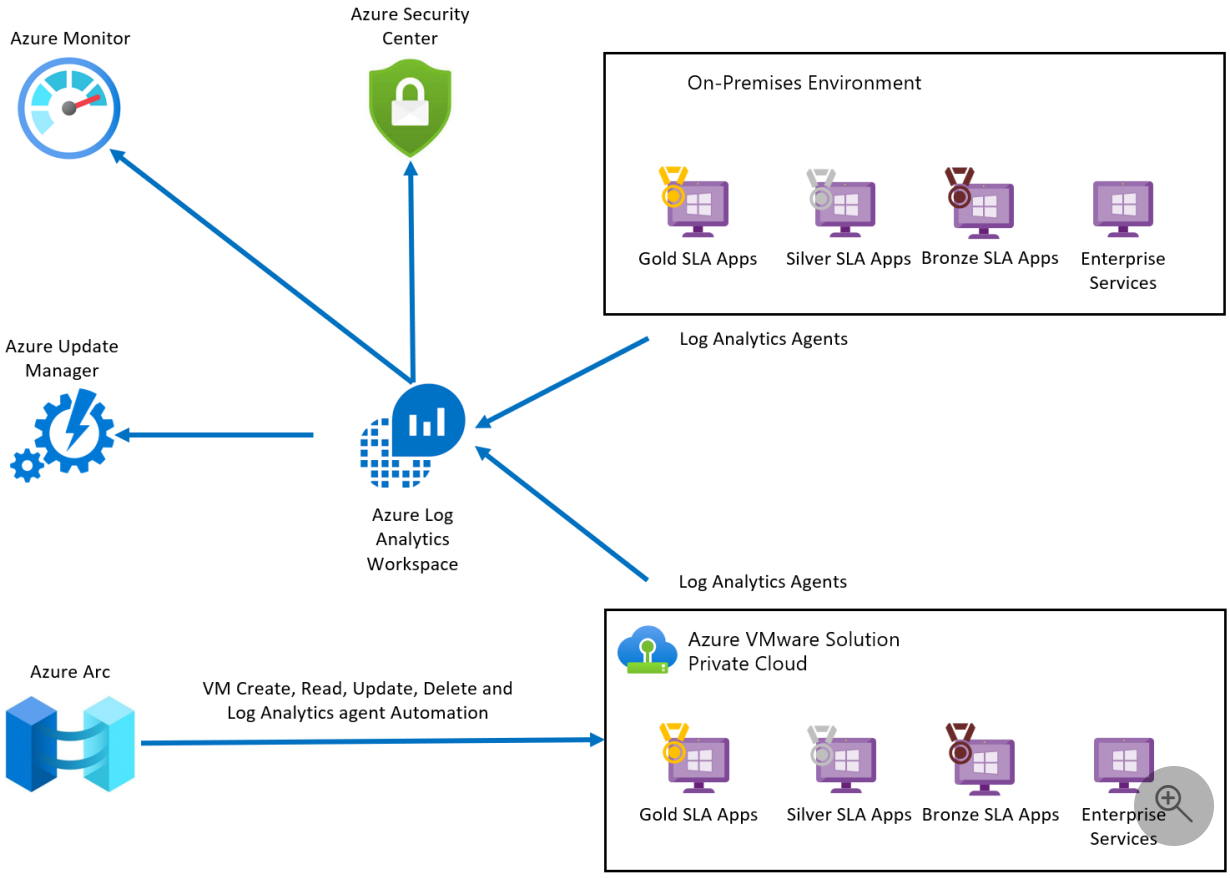
- Azure Arc extends Azure management to the Azure VMware Solution. After your Azure VMware Solution private cloud is deployed to Arc, you'll be ready to execute operations in Azure VMware Solution vCenter Server from the Azure portal. Operations are related to Create, Read, Update, and Delete (CRUD) virtual machines (VMs) in an Arc-enabled Azure VMware Solution private cloud. Users can also enable guest management and install Azure extensions after the private cloud is Arc-enabled.
- Azure Monitor collects, analyzes, and acts on data from your cloud and on-premises environments. Your Log Analytics workspace in Azure Monitor enables log collection and performance counter collection using the Log Analytics agent or extensions. You can send logs from your Azure VMware Solution private cloud to your Log Analytics workspace, allowing you to take advantage of the Log Analytics feature set, including:
    - system patches, security misconfigurations, and endpoint protection. You can also define security policies in Microsoft Defender for Cloud.
- Log Analytics workspace stores log data. Each workspace has its own data repository and configuration to store data. You can monitor Azure VMware Solution VMs through the Log Analytics agent. Machines connected to the Log Analytics Workspace use the Log Analytics agent to collect data about changes to installed software, Microsoft services, Windows registry and files, and Linux daemons on monitored servers. When data is available, the agent sends it to Azure Monitor Logs for processing. Azure Monitor Logs applies logic to the received data, records it, and makes it available for analysis.

Benefits

- Azure native services can be used to manage your VMs in a hybrid environment (Azure, Azure VMware Solution, and on-premises).
- Integrated monitoring and visibility of your Azure, Azure VMware Solution, and on-premises VMs.
  - Fileless security alerts
  - Operating system patch assessment
  - Security misconfigurations assessment
  - Endpoint protection assessment
- Easily deploy the Log Analytics extension after enabling guest management on VMware vSphere virtual machine (VM).
- Your Log Analytics workspace in Azure Monitor enables log collection and performance counter collection using the Log Analytics extensions. Collect data and logs to a single point and present that data to different Azure native services.
- Added benefits of Azure Monitor include:
  - Seamless monitoring
  - Better infrastructure visibility
  - Instant notifications
  - Automatic resolution
  - Cost efficiency

Topology

The diagram shows the integrated monitoring architecture for Azure VMware Solution VMs.



> **Note**
>
> If you're new to Azure or not familiar with the services previously mentioned, see Enable Azure Monitor for VMs overview for guidance.

Enable guest management and install extension

The guest management must be enabled on the VMware vSphere virtual machine (VM) before you can install an extension. Use the following prerequisite steps to enable guest management.

Prerequisites

- Navigate to Azure portal.
- Locate the VMware vSphere VM you want to check for guest management and install extensions on, select the name of the VM.
- Select **Configuration** from the left navigation for a VMware VM.
- Verify **Enable guest management** is checked.

The following conditions are necessary to enable guest management on a VM.

- The machine must be running a supported operating system.
- The machine needs to connect through the firewall to communicate over the internet. Make sure the URLs listed aren't blocked.
- The machine can't be behind a proxy, it isn't currently supported.
- If you're using Linux VM, the account must not prompt to sign in on pseudo commands.
- To avoid pseudo commands, follow these steps:

    1. Sign in to Linux VM.
    2. Open terminal and run the following command: sudo visudo.
    3. Add the line `username ALL=(ALL) NOPASSWD: ALL` at the end of the file.
    4. Replace username with the appropriate user-name. If your VM template already has these changes incorporated, you don't need to do the steps for the VM created from that template.

Install extensions

1. Sign in to the Azure portal.
2. Find the Arc-enabled Azure VMware Solution VM that you want to install an extension on and select the VM name.
3. Navigate to **Extensions** in the left navigation, select **Add**.
4. Select the extension you want to install.
   Based on the extension, you need to provide details.
   For example, workspace ID and key for Log Analytics extension.
5. When you're done, select **Review + create**.

When the extension installation steps are completed, they trigger deployment and install the selected extension on the VM.

Next steps

Now that you covered how to integrate services and monitor VMware Solution VMs, you can also learn about:

- Using the workload protection dashboard
- Advanced multistage attack detection in Microsoft Sentinel

Move Azure VMware Solution subscription to another subscription

Article • 12/19/2023

This article describes how to move an Azure VMware Solution subscription to another subscription. You might move your subscription for various reasons, like billing.

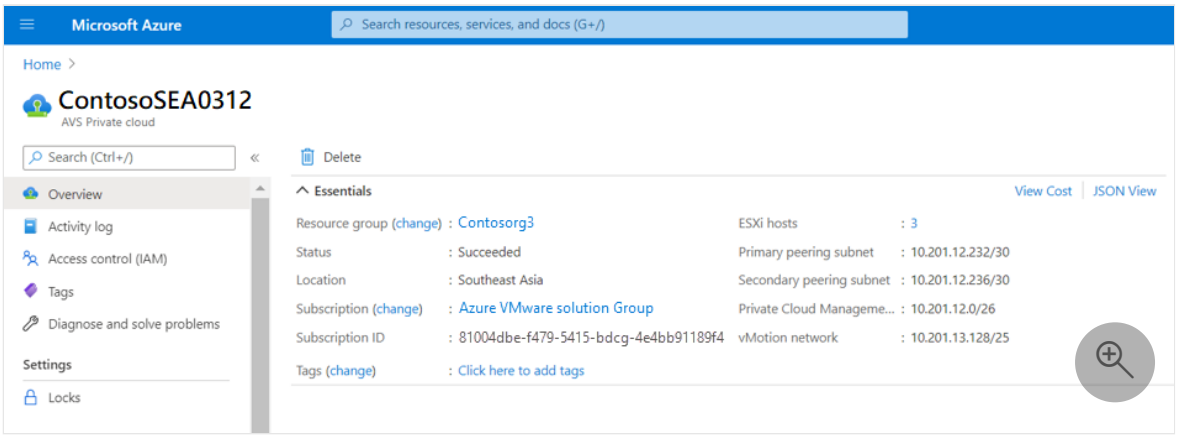
Prerequisites

You should have at least contributor rights on both **source** and **target** subscriptions.

> **Important**
>
> VNet and VNet gateway can't be moved from one subscription to another. Additionally, moving your subscriptions has no impact on the management and workloads, like the vCenter Server, NSX-T Data Center, vSAN, and workload virtual machines.

Prepare and move

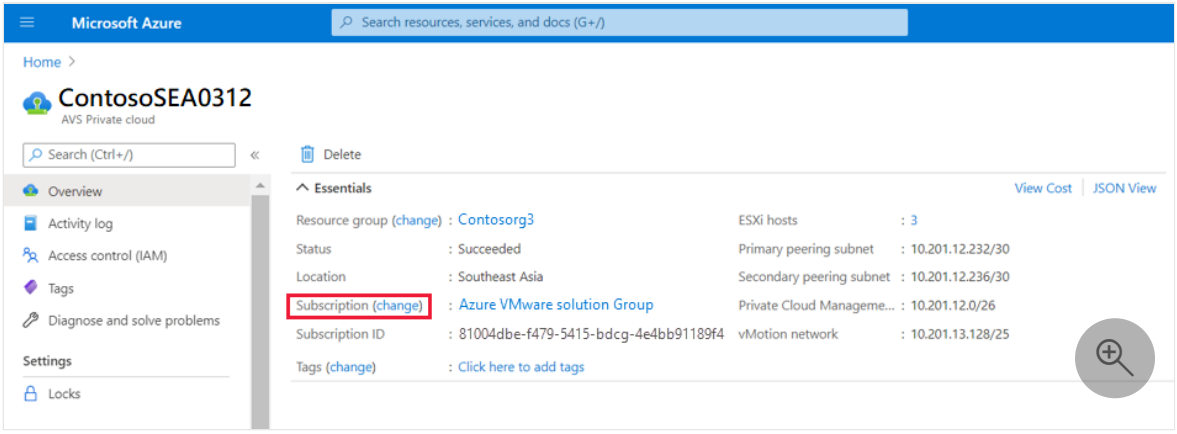
1. In the Azure portal, select the private cloud you want to move.



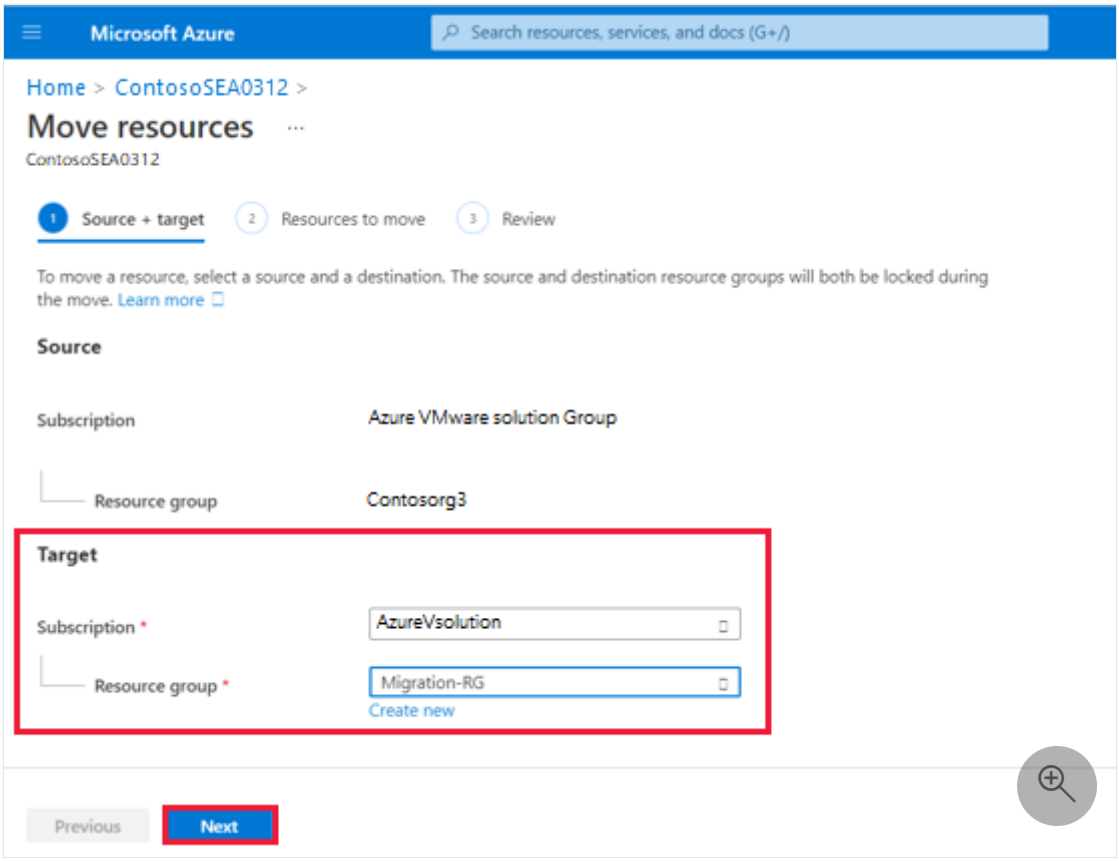
2. From a command prompt, ping the components and workloads to verify that they're pinging from the same subscription.

```
C:\Users\contosoad>ping 10.201.12.2

Pinging 10.201.12.2 with 32 bytes of data:
Reply from 10.201.12.2: bytes=32 time=222ms TTL=60
Reply from 10.201.12.2: bytes=32 time=222ms TTL=60
Reply from 10.201.12.2: bytes=32 time=222ms TTL=60
Reply from 10.201.12.2: bytes=32 time=221ms TTL=60

Ping statistics for 10.201.12.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 221ms, Maximum = 222ms, Average = 221ms

C:\Users\contosoad>ping 10.201.12.3

Pinging 10.201.12.3 with 32 bytes of data:
Reply from 10.201.12.3: bytes=32 time=224ms TTL=60
Reply from 10.201.12.3: bytes=32 time=224ms TTL=60
Reply from 10.201.12.3: bytes=32 time=223ms TTL=60
Reply from 10.201.12.3: bytes=32 time=223ms TTL=60

Ping statistics for 10.201.12.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 223ms, Maximum = 224ms, Average = 223ms

C:\Users\contosoad>ping 192.168.12.11

Pinging 192.168.12.11 with 32 bytes of data:
Reply from 192.168.12.11: bytes=32 time=227ms TTL=123
Reply from 192.168.12.11: bytes=32 time=231ms TTL=123
Reply from 192.168.12.11: bytes=32 time=227ms TTL=123
```

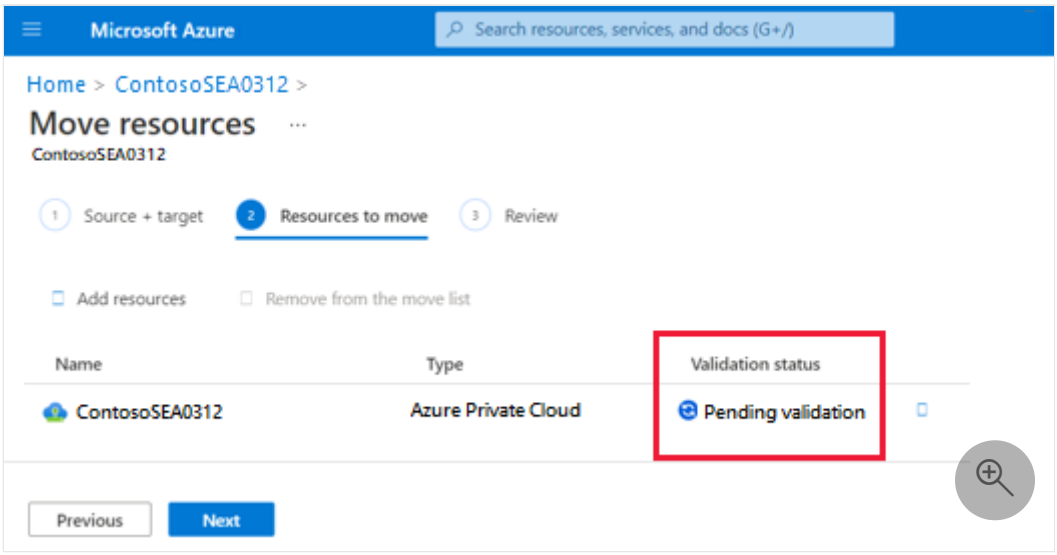
3. Select the **Subscription (change)** link.



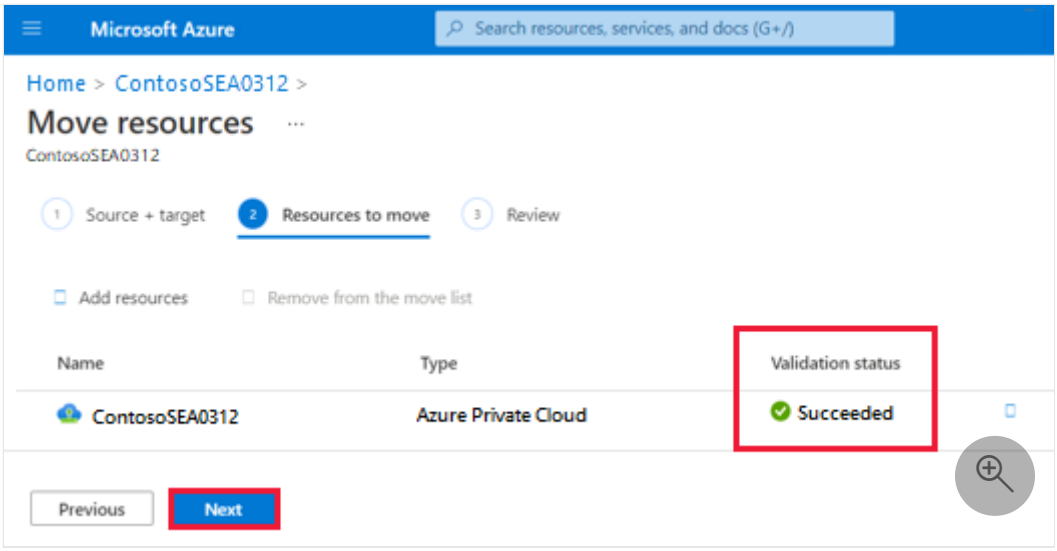
4. Provide the subscription details for **Target** and select **Next**.



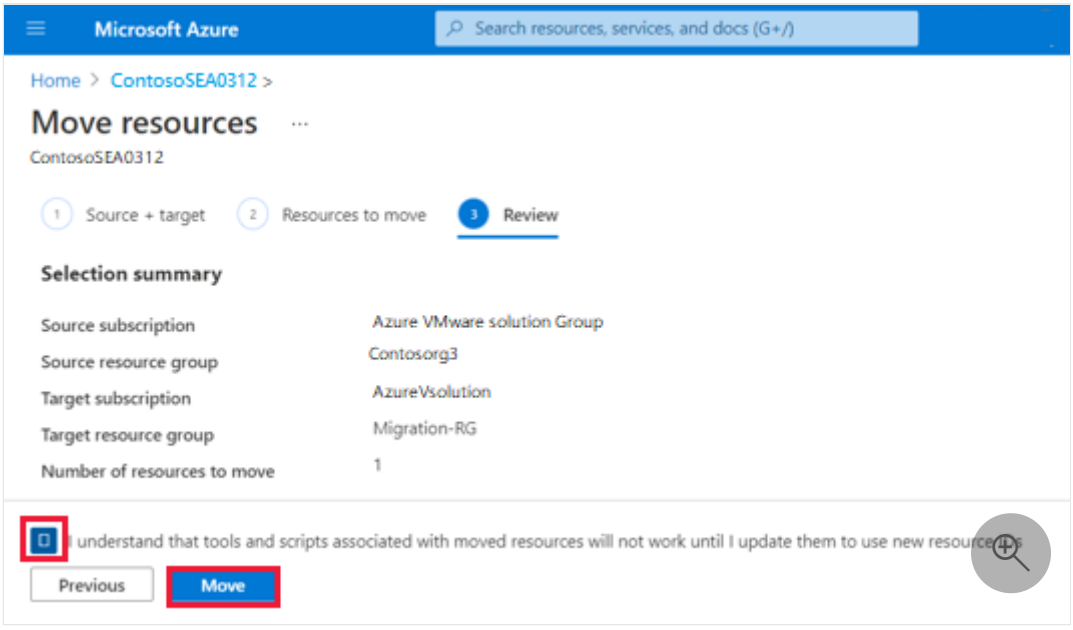
5. Confirm the validation of the resources you selected to move. During the validation, you see *Pending validation* under **Validation status**.



6. Once the validation is successful, select **Next** to start the migration of your private cloud.

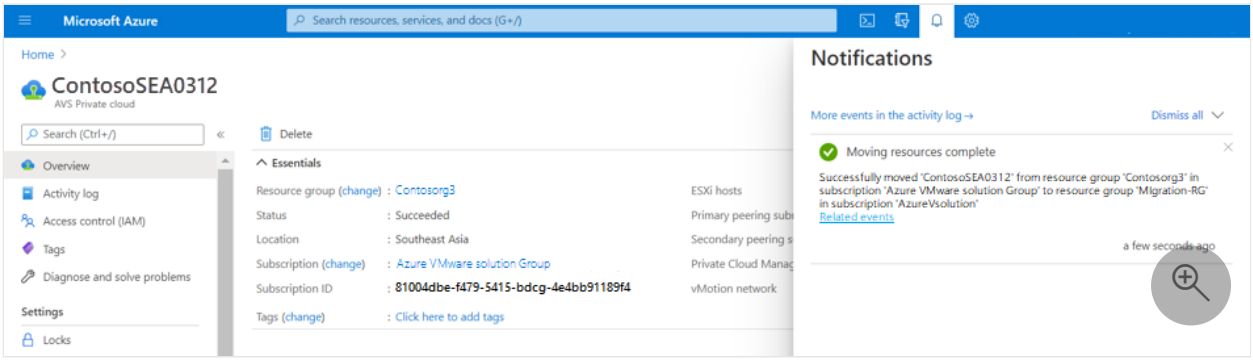


7. Select the check box indicating you understand that the tools and scripts associated don't work until you update them to use the new resource IDs. Then select **Move**.

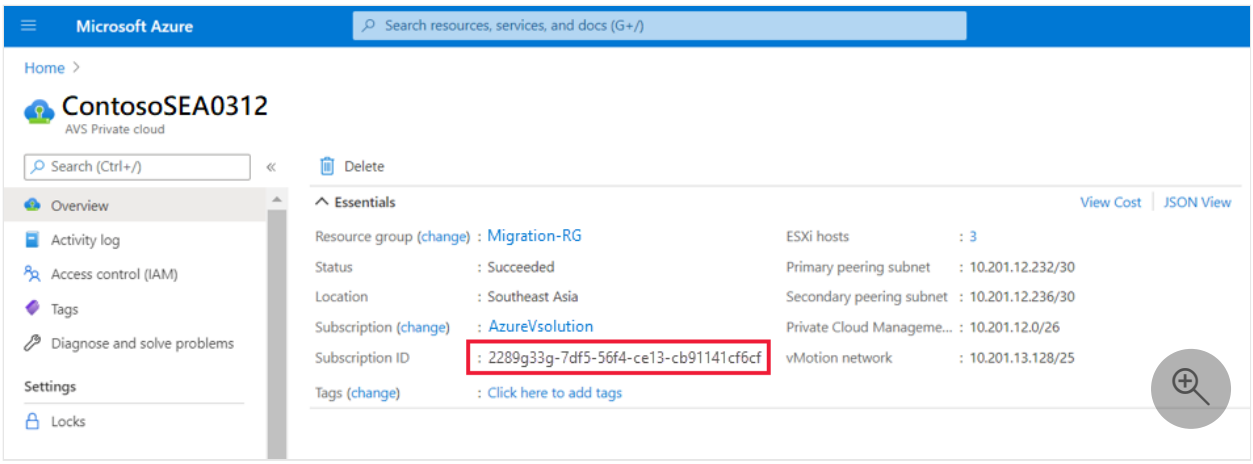


Verify the move

A notification appears once the resource move is complete.



The new subscription appears in the private cloud Overview.



Next steps

Learn more about:

- Move Azure VMware Solution across regions
- Move guidance for networking resources
- Move guidance for virtual machines
- Move guidance for App Service resources

Move Azure VMware Solution resources to another region

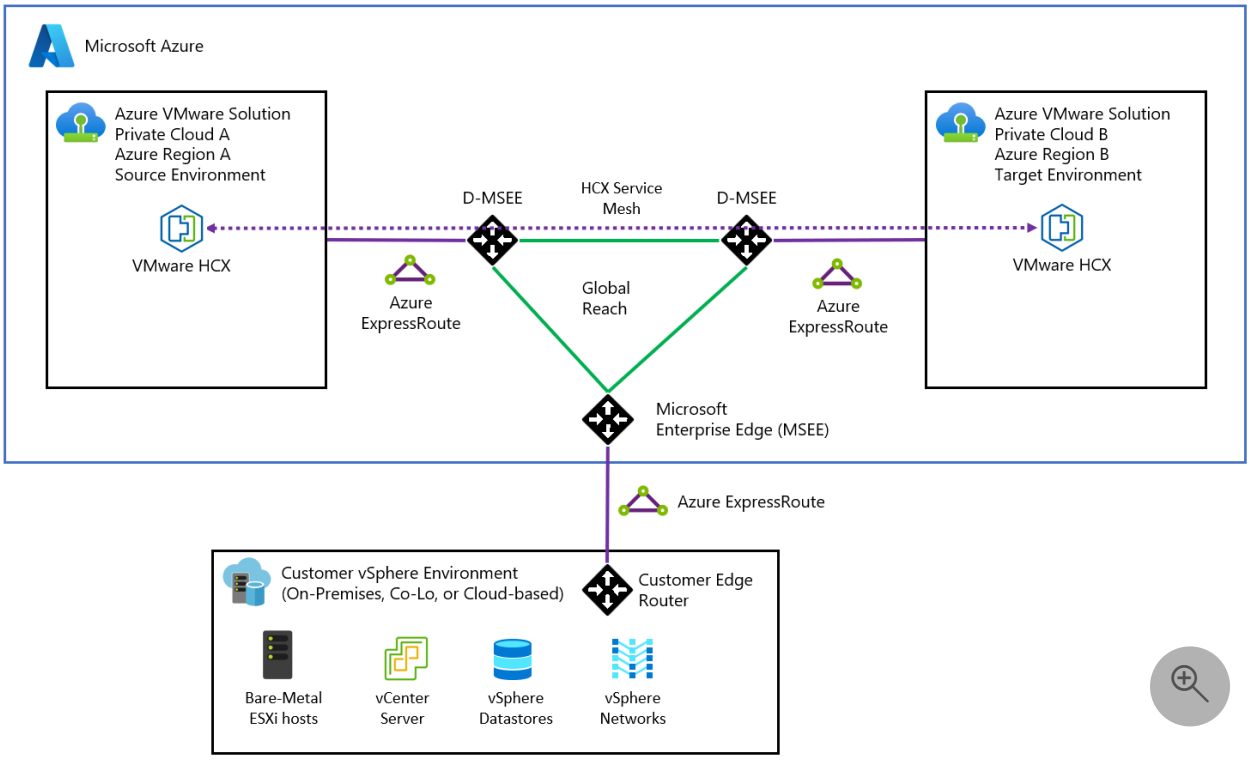
Article • 03/28/2024

> **Important**
>
> The steps in this article are strictly for moving Azure VMware Solution (source) in one region to Azure VMware Solution (target) in another region.

You can move Azure VMware Solution resources to a different region for several reasons. For example, deploy features or services available in specific regions only, meet policy and governance requirements, or respond to capacity planning requirements.

This article helps you plan and migrate Azure VMware Solution from one Azure region to another, such as Azure region A to Azure region B.

The diagram shows the recommended ExpressRoute connectivity between the two Azure VMware Solution environments. An HCX site pairing and service mesh are created between the two environments. The HCX migration traffic and Layer-2 extension moves (depicted by the purple line) between the two environments. For VMware recommended HCX planning, see Planning an HCX Migration.

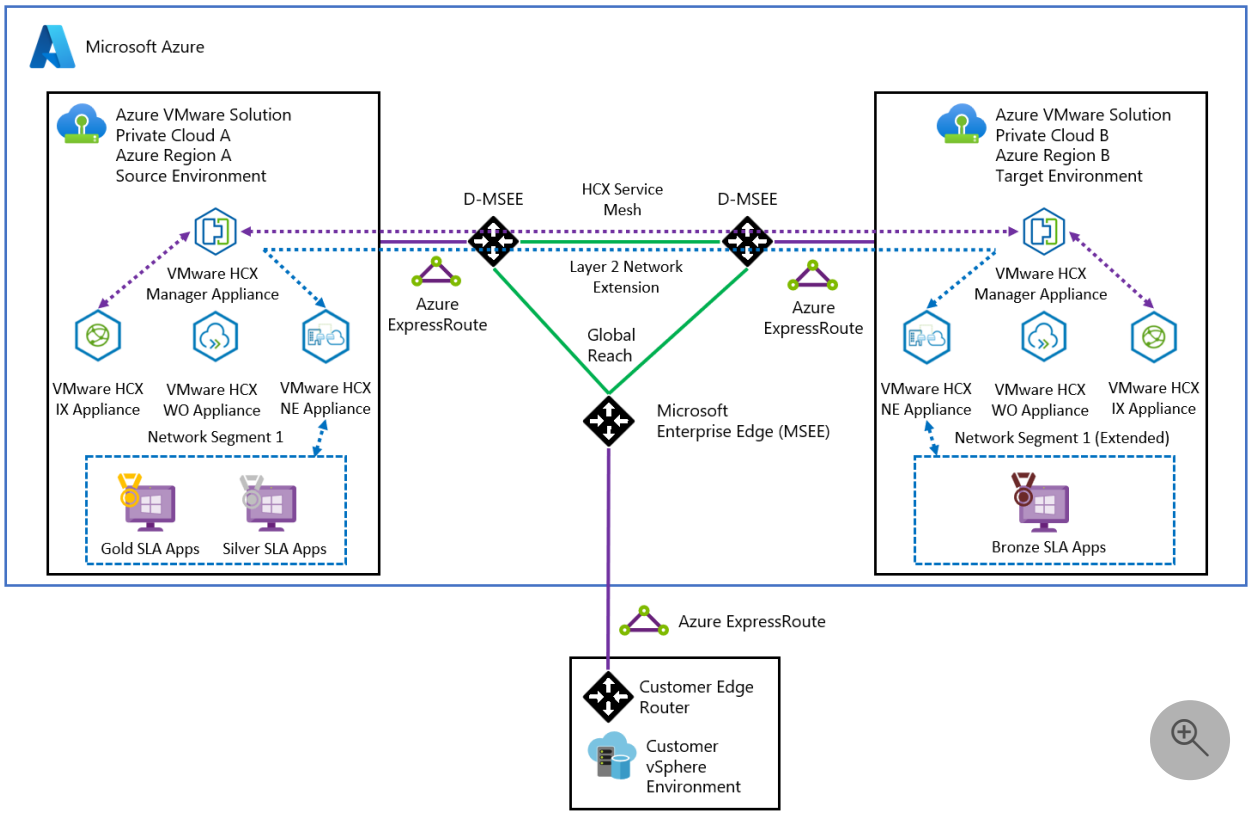


> **Note**

You don't need to migrate any workflow back to on-premises because the traffic will flow between the private clouds (source and target):

Azure VMware Solution private cloud (source) > ExpressRoute gateway (source) > Global Reach -> ExpressRoute gateway (target) > Azure VMware Solution private cloud (target)

The diagram shows the connectivity between both Azure VMware Solution environments.



In this article, walk through the steps to:

- ✓ Prepare and plan the move to another Azure region
- ✓ Establish network connectivity between the two Azure VMware Solution private clouds
- ✓ Export the configuration from the Azure VMware Solution source environment
- ✓ Reapply the supported configuration elements to the Azure VMware Solution target environment
- ✓ Migrate workloads using VMware HCX

Prerequisites

- VMware HCX appliance is upgraded to the latest patch to avoid migration issues if any.

- Source's local content library is a published content library.

Prepare

The following steps show how to prepare your Azure VMware Solution private cloud to move to another Azure VMware Solution private cloud.

Export the source configuration

1. From the source, export the extended segments, firewall rules, port details, and route tables.
2. Export the contents of an inventory list view to a CSV file.
3. Sort workloads into migration groups (migration wave).

Deploy the target environment

Before you can move the source configuration, you need to deploy the target environment.

Back up the source configuration

Back up the Azure VMware Solution (source) configuration that includes vCenter Server, NSX-T Data Center, and firewall policies and rules.

- **Compute:** Export existing inventory configuration. For Inventory backup, you can use RVTools (an open-source app).
- **Network and firewall policies and rules:** This is included as part of the VMware HCX Network Extension.

Azure VMware Solution supports all backup solutions. You need CloudAdmin privileges to install, backup data, and restore backups. For more information, see Backup solutions for Azure VMware Solution VMs.

- VM workload backup using the Commvault solution:
  - Create a VMware client from the Command center for Azure VMware Solution vCenter.
  - Create a VM group with the required VMs for backups.

- Run backups on VM groups.
- Restore VMs.

- VM workload backup using Veritas NetBackup solution.

> **Tip**
>
> You can use **Azure Resource Mover** to verify and migrate the list of supported resources to move across regions, which are dependent on Azure VMware Solution.

Locate the source ExpressRoute circuit ID

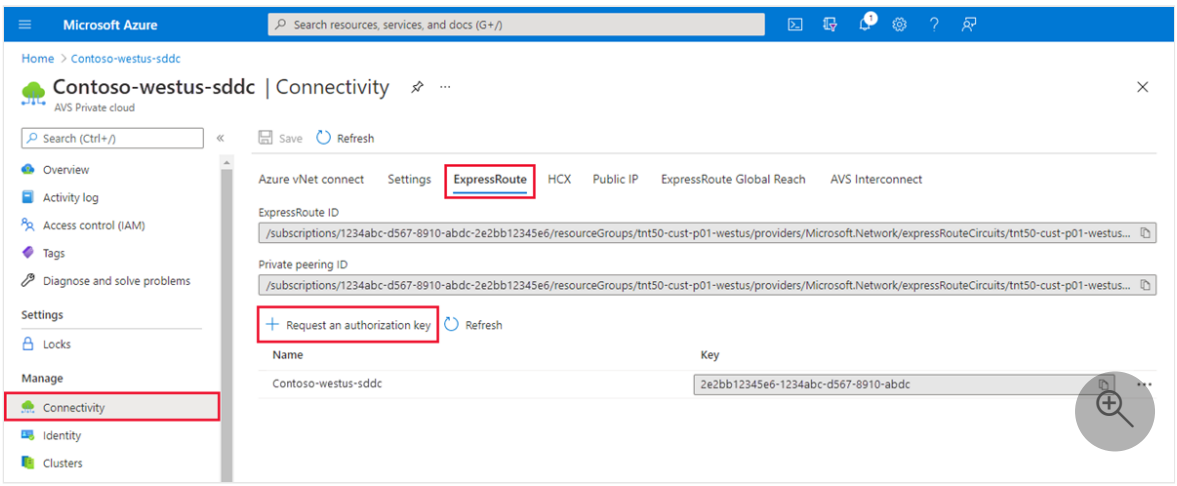
1. From the source, sign in to the Azure portal.
2. Select **Manage** > **Connectivity** > **ExpressRoute**.
3. Copy the source's **ExpressRoute ID**. You need it to peer between the private clouds.

Create the target's authorization key

1. From the target, sign in to the Azure portal.

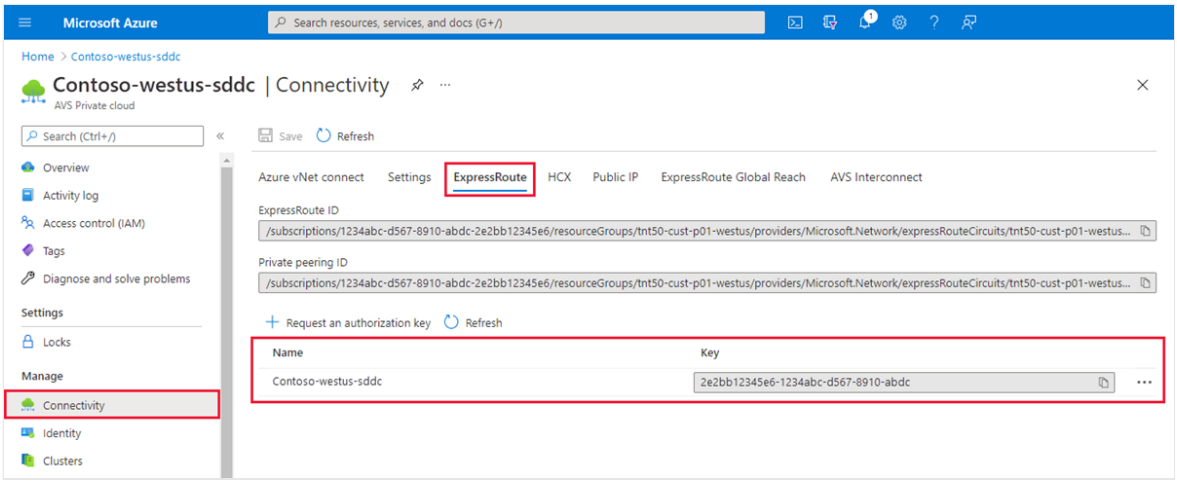
   > **Note**
   >
   > If you need access to the Azure US Gov portal, go to https://portal.azure.us/

2. Select **Manage** > **Connectivity** > **ExpressRoute**, then select **+ Request an authorization key**.



3. Provide a name for it and select **Create**.

   It can take about 30 seconds to create the key. Once created, the new key appears in the list of authorization keys for the private cloud.



4. Copy the authorization key and ExpressRoute ID. You need them to complete the peering. The authorization key disappears after some time, so copy it as soon as it appears.

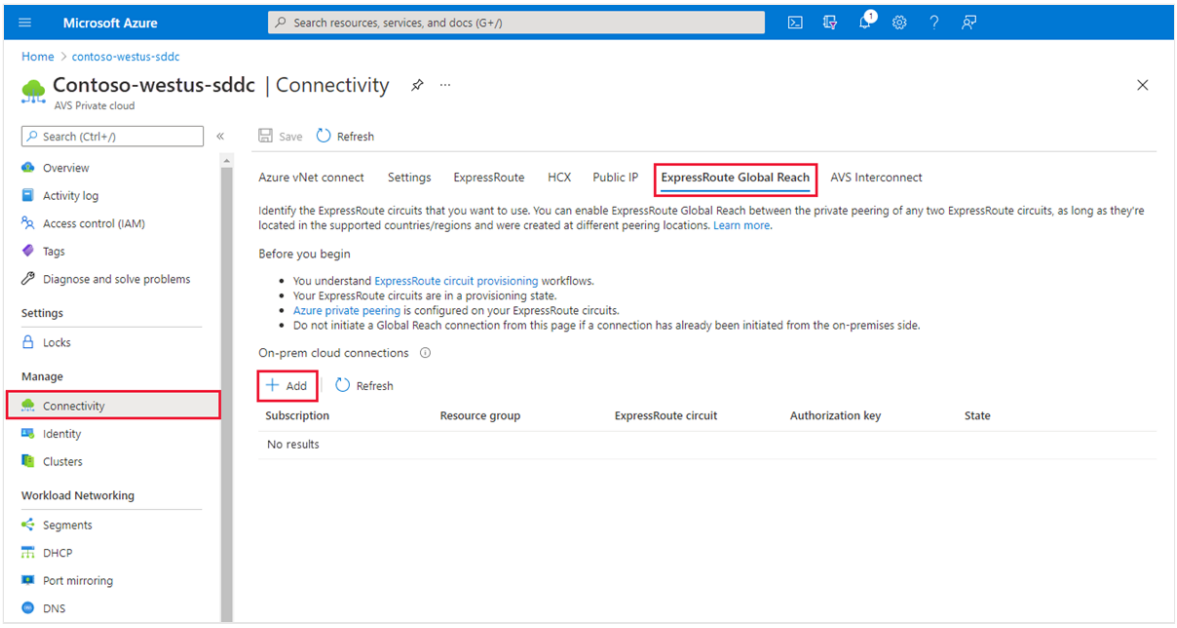
Peer between private clouds

Now that you have the ExpressRoute circuit IDs and authorization keys for both environments, you can peer the source to the target. You use the resource ID and authorization key of your private cloud ExpressRoute circuit to finish the peering.

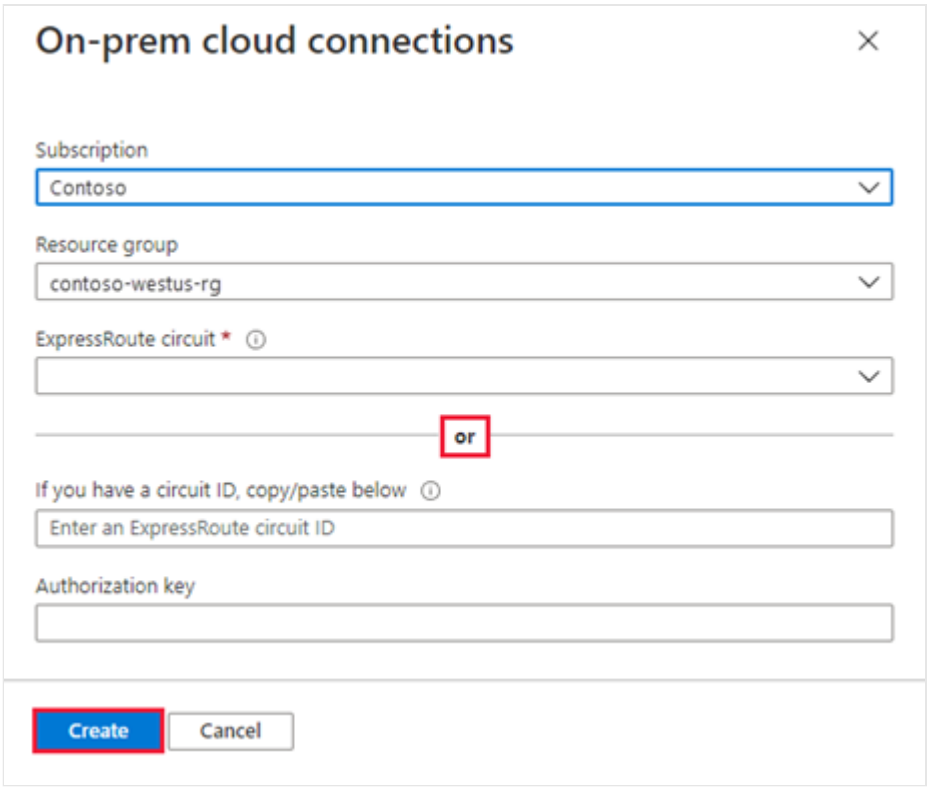
1. From the target, sign in to the Azure portal using the same subscription as the source's ExpressRoute circuit.

   > **Note**
   >
   > If you need access to the Azure US Gov portal, go to https://portal.azure.us/

2. Under Manage, select **Connectivity** > **ExpressRoute Global Reach** > **Add**.



3. Paste the ExpressRoute circuit ID and target's authorization key you created in the previous step. Then select **Create**:



Create a site pairing between private clouds

After you establish connectivity, you'll create a VMware HCX site pairing between the private clouds to facilitate the migration of your VMs. You can connect or pair the VMware HCX Cloud Manager in Azure VMware Solution with the VMware HCX Connector in your data center.

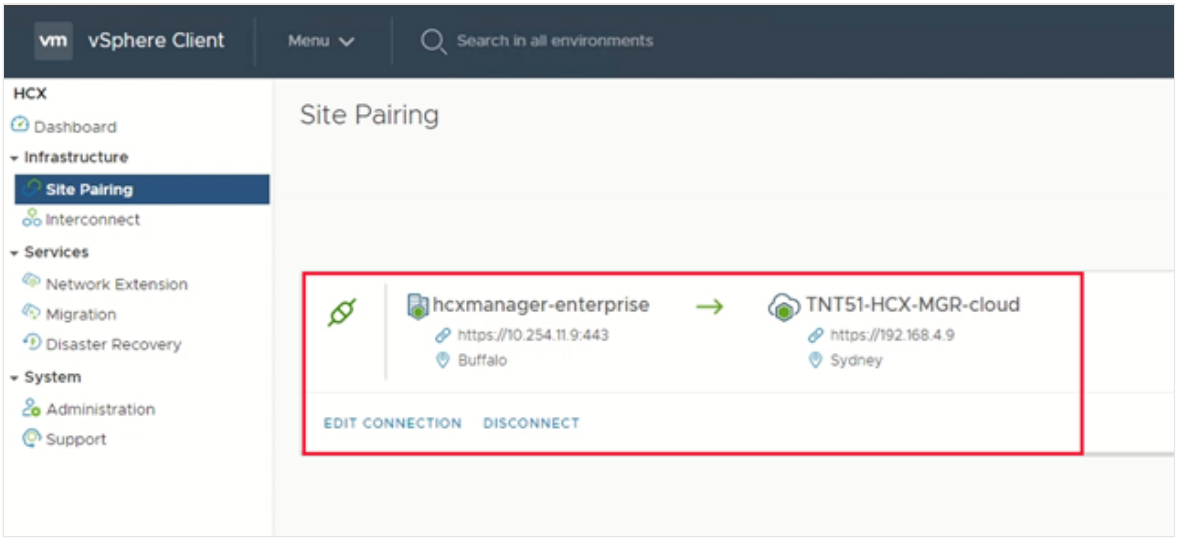
1. Sign in to your source's vCenter Server, and under **Home**, select **HCX**.

2. Under **Infrastructure**, select **Site Pairing** and select the **Connect To Remote Site** option (in the middle of the screen).

3. Enter the Azure VMware Solution HCX Cloud Manager URL or IP address you noted earlier `https://x.x.x.9`, the Azure VMware Solution cloudadmin@vsphere.local username, and the password. Then select **Connect**.

   > **Note**
   >
   > To successfully establish a site pair:
   >
   > - Your VMware HCX Connector must be able to route to your HCX Cloud Manager IP over port 443.
   > - Use the same password that you used to sign in to vCenter Server. You defined this password on the initial deployment screen.

   You see a screen showing that your VMware HCX Cloud Manager in Azure VMware Solution and your on-premises VMware HCX Connector are connected (paired).

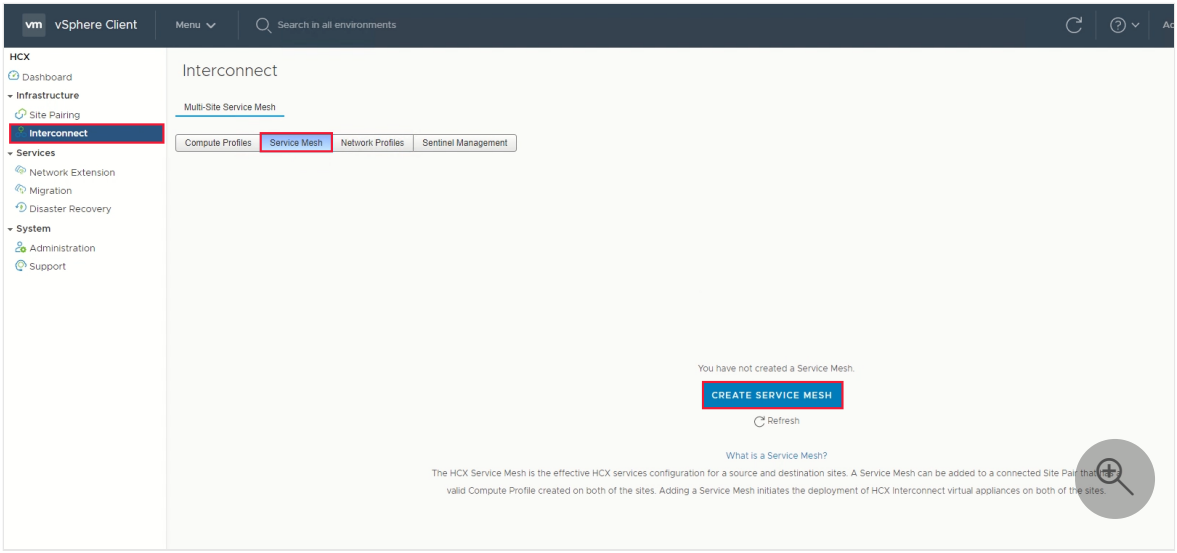


Create a service mesh between private clouds

> **Note**
>
> To successfully establish a service mesh with Azure VMware Solution:
>
> - Ports UDP 500/4500 are open between your on-premises VMware HCX Connector 'uplink' network profile addresses and the Azure VMware Solution HCX Cloud 'uplink' network profile addresses.

- Be sure to review the VMware HCX required ports.

1. Under **Infrastructure**, select **Interconnect** > **Service Mesh** > **Create Service Mesh**.

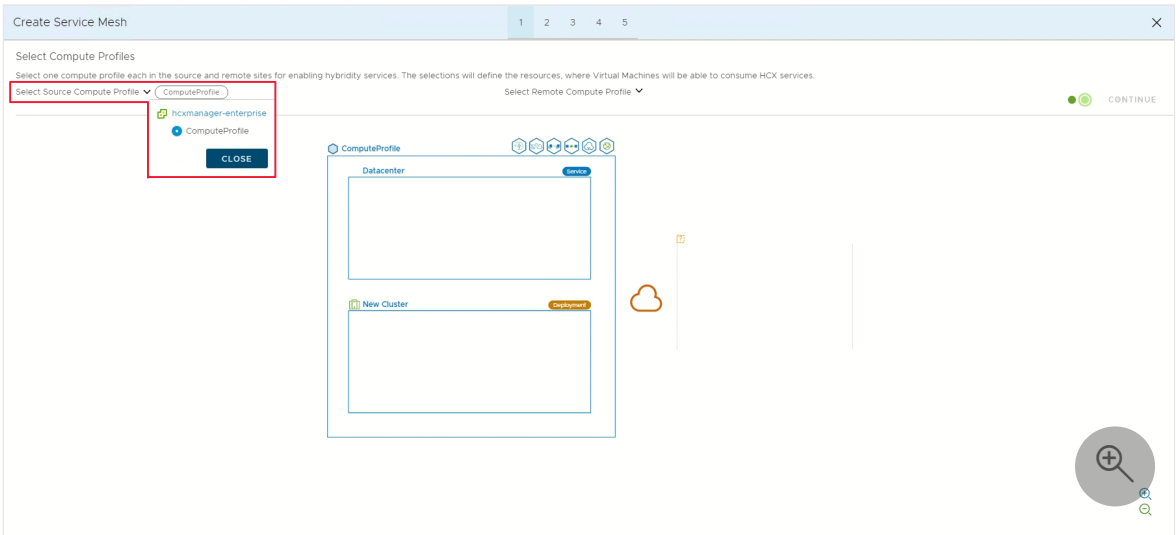


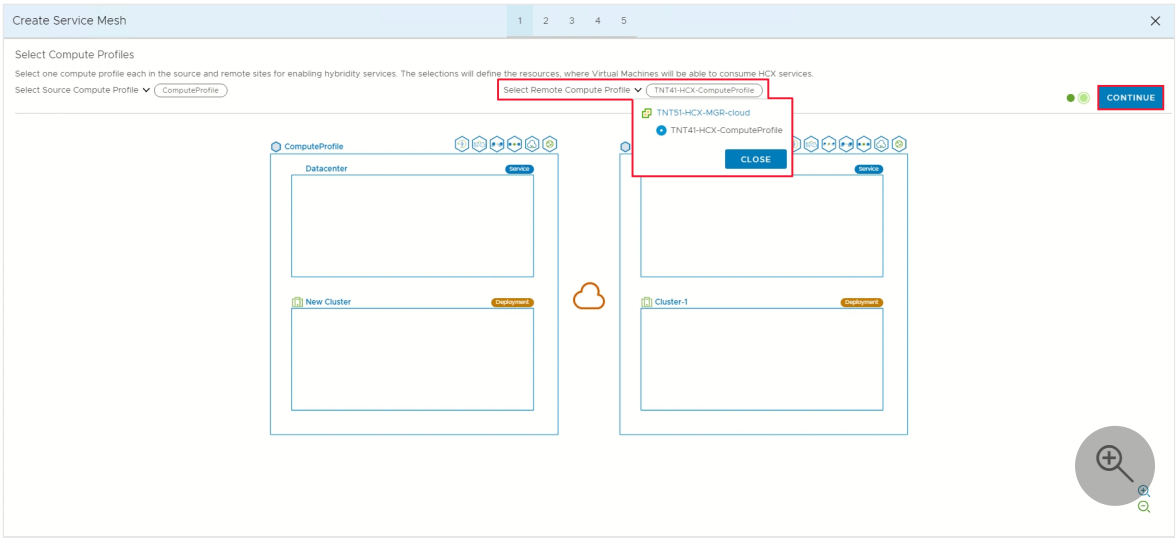
2. Review the prepopulated sites, and then select **Continue**.

> **Note**
>
> If this is your first service mesh configuration, you won't need to modify this screen.

3. Select the source and remote compute profiles from the drop-down lists, and then select **Continue**.

   The selections define the resources where VMs can consume VMware HCX services.

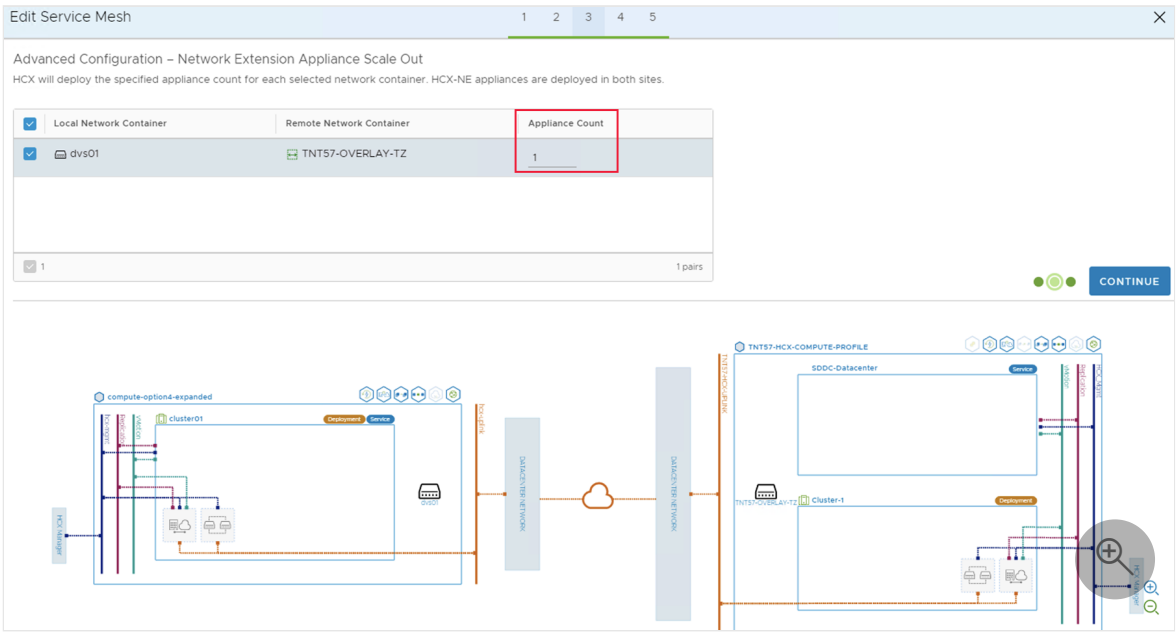




4. Review services that you want to be enabled, and then select **Continue**.
5. In **Advanced Configuration - Override Uplink Network profiles**, select **Continue**.

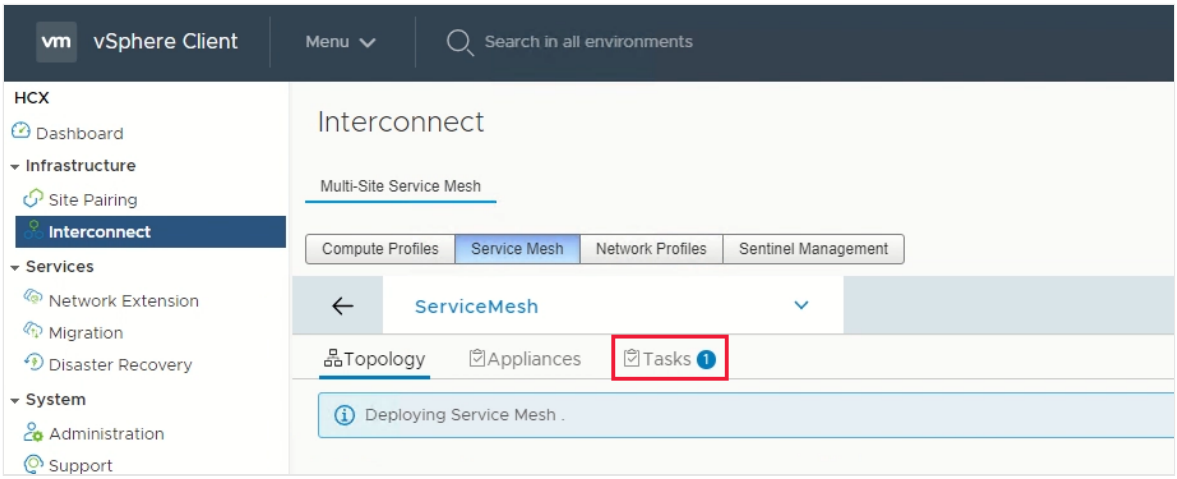
   Uplink network profiles connect to the network through which the remote site's interconnect appliances can be reached.
6. In **Advanced Configuration - Network Extension Appliance Scale Out**, review and select **Continue**.

   You can have up to eight Network Segments per appliance, but you can deploy another appliance to add another eight Network Segments. You must also have IP space to account for the more appliances, and it's one IP per appliance. For more information, see VMware HCX Configuration Limits.

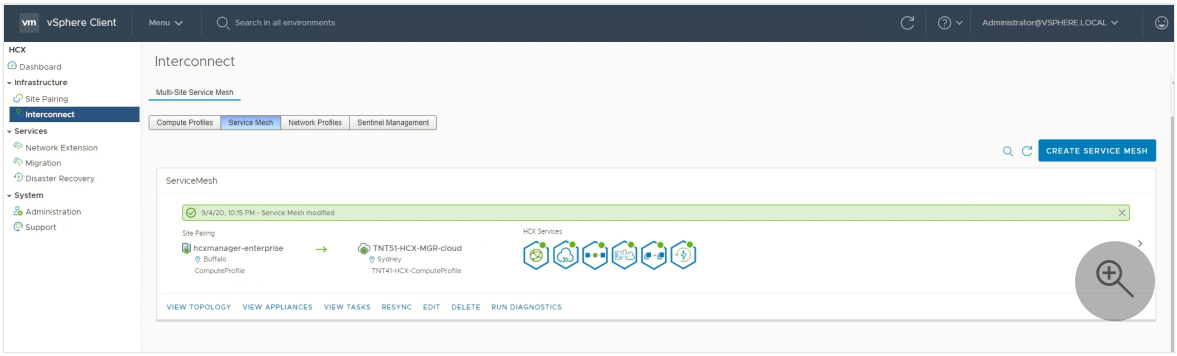


7. In **Advanced Configuration - Traffic Engineering**, review and make any modifications that you feel are necessary, and then select **Continue**.

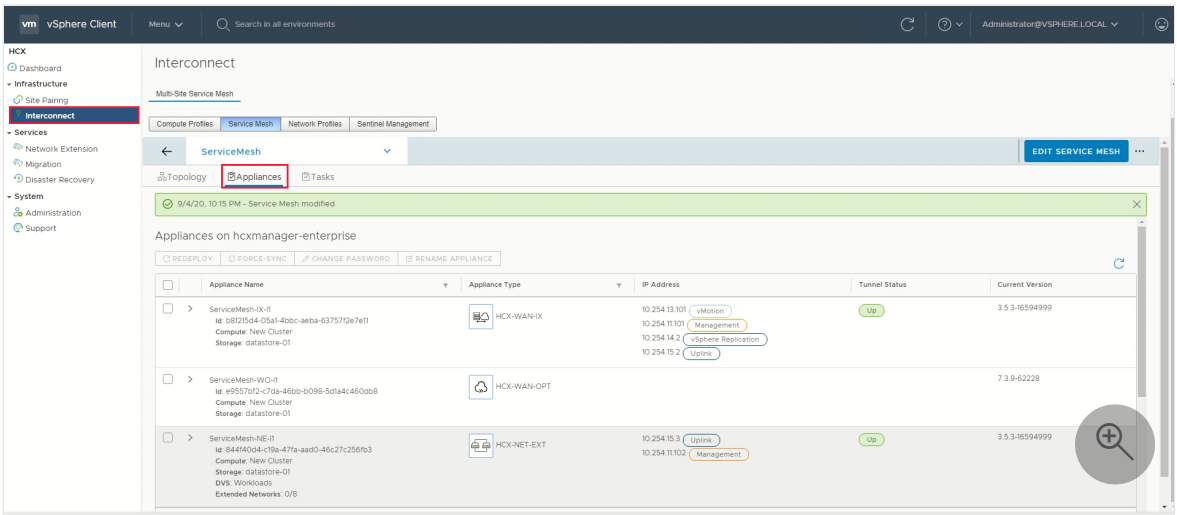
8. Review the topology preview and select **Continue**.
9. Enter a user-friendly name for this service mesh and select **Finish** to complete.
10. Select **View Tasks** to monitor the deployment.



When the service mesh deployment finishes successfully, you see the services as green.



11. Verify the service mesh's health by checking the appliance status.
12. Select **Interconnect** > **Appliances**.



Move

The following steps show how to move your Azure VMware Solution private cloud resources to another Azure VMware Solution private cloud in a different region.

In this section, you migrate the:

- Resource pool configuration and folder creation
- VM templates and the associated tags
- Logical segments deployment based on the source's port groups and associated VLANs
- Network security services and groups
- Gateway firewall policy and rules based on the source's firewall policies

Migrate the source vSphere configuration

In this step, copy the source vSphere configuration and move it to the target environment.

1. From the source vCenter Server, use the same resource pool configuration and create the same resource pool configuration on the target's vCenter Server.
2. From the source's vCenter Server, use the same VM folder name and create the same VM folder on the target's vCenter Server under **Folders**.
3. Use VMware HCX to migrate all VM templates from the source's vCenter Server to the target's vCenter Server.
    a. From the source, convert the existing templates to VMs and then migrate them to the target.
    b. From the target, convert the VMs to VM templates.
4. From the source environment, use the same VM Tags name and create them on the target's vCenter.
5. From the source's vCenter Server Content Library, use the subscribed library option to copy the ISO, OVF, OVA, and VM Templates to the target content library:
    a. If the content library isn't already published, select the **Enable publishing** option.

b. From the source's Content Library, copy the URL of the published library.

c. From the target, create a subscribed content library with the URL from the source's library.

d. Select **Sync Now**.

Configure the target NSX-T Data Center environment

In this step, use the source NSX-T Data Center configuration to configure the target NSX-T Data Center environment.

> **Note**
>
> You'll have multiple features configured on the source NSX-T Data Center, so you must copy or read from the source NSX-T Data Center and recreate it in the target private cloud. Use L2 Extension to keep same IP address and Mac Address of the VM while migrating Source to target Azure VMware Solution Private Cloud to avoid downtime due to IP change and related configuration.

1. Configure NSX-T Data Center network components required in the target environment under default Tier-1 gateway.
2. Create the security group configuration.
3. Create the distributed firewall policy and rules.
4. Create the gateway firewall policy and rules.
5. Create the DHCP server or DHCP relay service.
6. Configure port mirroring.
7. Configure DNS forwarder.
8. Configure a new Tier-1 gateway (other than default). This configuration is based on the NSX-T Data Center configured on the source.

Migrate the VMs from the source

In this step, use VMware HCX to migrate the VMs from the source to the target. You can opt to do a Layer-2 extension from the source and use HCX to vMotion the VMs from the source to the target with minimal interruption.

Besides vMotion, other methods, like Bulk and Cold vMotion, are also recommended. Learn more about:

- Plan an HCX Migration
- Migrate Virtual Machines with HCX

Cutover extended networks

In this step, perform a final gateway cutover to terminate the extended networks. Move (migrate) the gateways from the source Azure VMware Solution environment to the target environment.

> **Important**
>
> You must do the gateway cutover post VLAN workload migration to the target Azure VMware Solution environment. Also, there shouldn't be any VM dependency on the source and target environments.

Before the gateway cutover, verify all migrated workload services and performance. Once application and web service owners accept the performance (except for any latency issues), you can continue with the gateway cutover. Once the cutover is completed, you need to modify the public DNS A and PTR records.

For VMware recommendations, see Cutover of extended networks.

Public IP DNAT for migrated DMZ VMs

To this point, you migrated the workloads to the target environment. These application workloads must be reachable from the public internet. The target environment provides two ways of hosting any application. Applications can be:

- Hosted and published under the application gateway load balancer.
- Published through the public IP feature in vWAN.

Public IP is typically the destination NAT translated into the Azure firewall. With DNAT rules, firewall policy would translate the public IP address request to a private address (webserver) with a port. For more information, see How to use the public IP functionality in Azure Virtual WAN.

> **Note**

SNAT is by default configured in Azure VMware Solution, so you must enable SNAT from Azure VMware Solution private cloud connectivity settings under the Manage tab.

Decommission

For this last step, verify that all the VM workloads were migrated successfully, including the network configuration. If there's no dependency, you can disconnect the HCX service mesh, site pairing, and network connectivity from the source environment.

> **Note**
>
> Once you decommission the private cloud, you cannot undo it as the configuration and data will be lost.

Next steps

Learn more about:

- Move operation support for Microsoft.AVS
- Move guidance for networking resources
- Move guidance for virtual machines
- Move guidance for App Service resources

Security solutions for Azure VMware Solution

Article • 12/20/2023

A fundamental part of Azure VMware Solution is security. It allows customers to run their VMware-based workloads in a safe and trustable environment.

Our security partners have industry-leading solutions in VMware-based environments that cover many aspects of the security ecosystem like threat protection and security scanning. Our customers adopted many of these solutions integrated with VMware NSX-T Data Center for their on-premises deployments. As one of our key principles, we want to enable them to continue to use their investments and VMware solutions running on Azure. Many of these Independent Software Vendors (ISV) validated their solutions with Azure VMware Solution.

You can find more information about these solutions here:

- Bitdefender
- Trend Micro Deep Security
- Check Point

Security recommendations for Azure VMware Solution

Article • 04/04/2024

It's important to take proper measures to secure your Azure VMware Solution deployments. Use the information in this article as a high-level guide to achieve your security goals.

General

Use the following guidelines and links for general security recommendations for both Azure VMware Solution and VMware best practices.

Expand table

Recommendation	Comments
Review and follow VMware Security Best Practices.	It's important to stay updated on Azure security practices and VMware Security Best Practices.
Keep up to date on VMware Security Advisories.	Subscribe to VMware notifications in `my.vmware.com`. Regularly review and remediate any VMware Security Advisories.
Enable Microsoft Defender for Cloud.	Microsoft Defender for Cloud provides unified security management and advanced threat protection across hybrid cloud workloads.
Follow the Microsoft Security Response Center blog.	Microsoft Security Response Center
Review and implement recommendations within the Azure security baseline for Azure VMware Solution.	Azure security baseline for VMware Solution

Network

The following recommendations for network-related security apply to Azure VMware Solution.

Expand table

Recommendation	Comments
Only allow trusted networks.	Only allow access to your environments over Azure ExpressRoute or other secured networks. Avoid exposing your management services like vCenter Server, for example, on the internet.
Use Azure Firewall Premium.	If you must expose management services on the internet, use Azure Firewall Premium with both intrusion detection and detention system (IDPS) Alert and Deny mode along with Transport Layer Security (TLS) inspection for proactive threat detection.
Deploy and configure network security groups on a virtual network.	Ensure that any deployed virtual network has network security groups configured to control ingress and egress to your environment.
Review and implement recommendations within the Azure security baseline for Azure VMware Solution.	Azure security baseline for Azure VMware Solution

VMware HCX

See the following information for recommendations to secure your VMware HCX deployment.

Expand table

Recommendation	Comments
Stay current with VMware HCX service updates.	VMware HCX service updates can include new features, software fixes, and security patches. To apply service updates during a maintenance window where no new VMware HCX operations are queued up, follow these steps.

Azure security baseline for Azure VMware Solution

Article • 09/20/2023

This security baseline applies guidance from the Microsoft cloud security benchmark version 1.0 to Azure VMware Solution. The Microsoft cloud security benchmark provides recommendations on how you can secure your cloud solutions on Azure. The content is grouped by the security controls defined by the Microsoft cloud security benchmark and the related guidance applicable to Azure VMware Solution.

You can monitor this security baseline and its recommendations using Microsoft Defender for Cloud. Azure Policy definitions will be listed in the Regulatory Compliance section of the Microsoft Defender for Cloud portal page.

When a feature has relevant Azure Policy Definitions, they are listed in this baseline to help you measure compliance with the Microsoft cloud security benchmark controls and recommendations. Some recommendations may require a paid Microsoft Defender plan to enable certain security scenarios.

> ⓘ **Note**
>
> **Features** not applicable to Azure VMware Solution have been excluded. To see how Azure VMware Solution completely maps to the Microsoft cloud security benchmark, see the **full Azure VMware Solution security baseline mapping file**.

Security profile

The security profile summarizes high-impact behaviors of Azure VMware Solution, which may result in increased security considerations.

Service Behavior Attribute	Value
Product Category	Compute
Customer can access HOST / OS	No Access
Service can be deployed into customer's virtual network	True
Stores customer content at rest	True

Network security

For more information, see the Microsoft cloud security benchmark: Network security.

NS-1: Establish network segmentation boundaries

Features

Virtual Network Integration

Description: Service supports deployment into customer's private Virtual Network (VNet). Learn more.

Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

Configuration Guidance: Deploy the service into a virtual network. Assign private IPs to the resource (where applicable) unless there is a strong reason to assign public IPs directly to the resource.

Note: An Azure VMware Solution private cloud requires an Azure Virtual Network. Because Azure VMware Solution doesn't support your on-premises vCenter Server, you'll need to do additional steps to integrate with your on-premises environment. Setting up an ExpressRoute circuit and a virtual network gateway is also required.

Reference: Tutorial: Configure networking for your VMware private cloud in Azure

Network Security Group Support

Description: Service network traffic respects Network Security Groups rule assignment on its subnets. Learn more.

Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

Configuration Guidance: Although NSG is supported, consider ingress and egress your network connectivity to ExpressRoute or other secured networks. Avoid exposing your management services like vCenter Server, for example, on the internet.

NS-2: Secure cloud services with network controls

Features

Azure Private Link

Description: Service native IP filtering capability for filtering network traffic (not to be confused with NSG or Azure Firewall). Learn more.

Supported	Enabled By Default	Configuration Responsibility
False	Not Applicable	Not Applicable

Configuration Guidance: This feature is not supported to secure this service.

Disable Public Network Access

Description: Service supports disabling public network access either through using service-level IP ACL filtering rule (not NSG or Azure Firewall) or using a 'Disable Public Network Access' toggle switch. Learn more.

Supported	Enabled By Default	Configuration Responsibility
True	True	Microsoft

Configuration Guidance: No additional configurations are required as this is enabled on a default deployment.

Reference: Azure VMware Solution networking and interconnectivity concepts

Identity management

For more information, see the Microsoft cloud security benchmark: Identity management.

IM-1: Use centralized identity and authentication system

Features

Azure AD Authentication Required for Data Plane Access

Description: Service supports using Azure AD authentication for data plane access. Learn more.

Supported	Enabled By Default	Configuration Responsibility
False	Not Applicable	Not Applicable

Configuration Guidance: This feature is not supported to secure this service.

Local Authentication Methods for Data Plane Access

Description: Local authentications methods supported for data plane access, such as a local username and password. Learn more.

Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

Feature notes: Avoid the usage of local authentication methods or accounts, these should be disabled wherever possible. Instead use Azure AD to authenticate where possible.

Configuration Guidance: For configuration of the identity access management of the Azure VMware Solution, refer to the link below.

Reference: vCenter Server access and identity

IM-3: Manage application identities securely and automatically

Features

Managed Identities

Description: Data plane actions support authentication using managed identities. Learn more.

Supported	Enabled By Default	Configuration Responsibility
False	Not Applicable	Not Applicable

Configuration Guidance: This feature is not supported to secure this service.

Service Principals

Description: Data plane supports authentication using service principals. Learn more.

Supported	Enabled By Default	Configuration Responsibility
False	Not Applicable	Not Applicable

Configuration Guidance: This feature is not supported to secure this service.

IM-7: Restrict resource access based on conditions

Features

Conditional Access for Data Plane

Description: Data plane access can be controlled using Azure AD Conditional Access Policies. Learn more.

Supported	Enabled By Default	Configuration Responsibility
False	Not Applicable	Not Applicable

Feature notes: AVS access is controlled by VMware vSphere RBAC

Configuration Guidance: This feature is not supported to secure this service.

IM-8: Restrict the exposure of credential and secrets

Features

Service Credential and Secrets Support Integration and Storage in Azure Key Vault

Description: Data plane supports native use of Azure Key Vault for credential and secrets store. Learn more.

Supported	Enabled By Default	Configuration Responsibility
False	Not Applicable	Not Applicable

Configuration Guidance: This feature is not supported to secure this service.

Privileged access

For more information, see the Microsoft cloud security benchmark: Privileged access.

PA-1: Separate and limit highly privileged/administrative users

Features

Local Admin Accounts

Description: Service has the concept of a local administrative account. Learn more.

Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

Feature notes: Avoid the usage of local authentication methods or accounts, these should be disabled wherever possible. Instead use Azure AD to authenticate where possible.

Configuration Guidance: View the privileges granted to the Azure VMware Solution CloudAdmin role on your Azure VMware Solution private cloud vCenter. Refer to the link for details

Reference: vCenter Server access and identity

PA-7: Follow just enough administration (least privilege) principle

Features

Azure RBAC for Data Plane

Description: Azure Role-Based Access Control (Azure RBAC) can be used to managed access to service's data plane actions. Learn more.

Supported	Enabled By Default	Configuration Responsibility
False	Not Applicable	Not Applicable

Feature notes: Azure RBAC is not supported. Azure VMware solution makes use of vCenter RBAC roles which provides customers with the ability to integrate with Azure AD.

Configuration Guidance: This feature is not supported to secure this service.

PA-8: Determine access process for cloud provider support

Features

Customer Lockbox

Description: Customer Lockbox can be used for Microsoft support access. Learn more.

Supported	Enabled By Default	Configuration Responsibility
False	Not Applicable	Not Applicable

Configuration Guidance: This feature is not supported to secure this service.

Data protection

For more information, see the Microsoft cloud security benchmark: Data protection.

DP-3: Encrypt sensitive data in transit

Features

Data in Transit Encryption

Description: Service supports data in-transit encryption for data plane. Learn more.

Supported	Enabled By Default	Configuration Responsibility
True	True	Microsoft

Configuration Guidance: No additional configurations are required as this is enabled on a default deployment.

DP-4: Enable data at rest encryption by default

Features

Data at Rest Encryption Using Platform Keys

Description: Data at-rest encryption using platform keys is supported, any customer content at rest is encrypted with these Microsoft managed keys. Learn more.

Supported	Enabled By Default	Configuration Responsibility
True	True	Microsoft

Configuration Guidance: No additional configurations are required as this is enabled on a default deployment.

Reference: Data-at-rest encryption

DP-5: Use customer-managed key option in data at rest encryption when required

Features

Data at Rest Encryption Using CMK

Description: Data at-rest encryption using customer-managed keys is supported for customer content stored by the service. Learn more.

Supported	Enabled By Default	Configuration Responsibility
False	Not Applicable	Not Applicable

Feature notes: This feature is currently being worked on, but we do not have an ETA for private preview.

Configuration Guidance: This feature is not supported to secure this service.

DP-6: Use a secure key management process

Features

Key Management in Azure Key Vault

Description: The service supports Azure Key Vault integration for any customer keys, secrets, or certificates. Learn more.

Supported	Enabled By Default	Configuration Responsibility
False	Not Applicable	Not Applicable

Configuration Guidance: This feature is not supported to secure this service.

DP-7: Use a secure certificate management process

Features

Certificate Management in Azure Key Vault

Description: The service supports Azure Key Vault integration for any customer certificates. Learn more.

Supported	Enabled By Default	Configuration Responsibility
False	Not Applicable	Not Applicable

Feature notes: We will be adding specific features in the future that support this but for now we do not.

Configuration Guidance: This feature is not supported to secure this service.

Asset management

For more information, see the Microsoft cloud security benchmark: Asset management.

AM-2: Use only approved services

Features

Azure Policy Support

Description: Service configurations can be monitored and enforced via Azure Policy. Learn more.

Supported	Enabled By Default	Configuration Responsibility
False	Not Applicable	Not Applicable

Feature notes: Azure VMWare Solution currently does support Azure Policy to manage the workload VM resources. If you choose to deploy Azure Arc Server for VMWare Solution, it will come with Azure Policy support.

Configuration Guidance: This feature is not supported to secure this service.

Logging and threat detection

For more information, see the Microsoft cloud security benchmark: Logging and threat detection.

LT-1: Enable threat detection capabilities

Features

Microsoft Defender for Service / Product Offering

Description: Service has an offering-specific Microsoft Defender solution to monitor and alert on security issues. Learn more.

Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

Configuration Guidance: Use Azure Arc-enabled server for your VM on your VMware which allows Microsoft Defender for Cloud to provide the following features:

- File integrity monitoring
- Fileless attack detection
- Operating system patch assessment
- Security misconfigurations assessment
- Endpoint protection assessment

Reference: Integrate Microsoft Defender for Cloud with Azure VMware Solution

LT-4: Enable logging for security investigation

Features

Azure Resource Logs

Description: Service produces resource logs that can provide enhanced service-specific metrics and logging. The customer can configure these resource logs and send them to their own data sink like a storage account or log analytics workspace. Learn more.

Supported	Enabled By Default	Configuration Responsibility
False	Not Applicable	Not Applicable

Feature notes: For Azure VMware Solution logging. Enable configuration in VMware syslog. Refer to the link for more details: Configure VMware syslogs for Azure VMware Solution

Configuration Guidance: This feature is not supported to secure this service.

Backup and recovery

For more information, see the Microsoft cloud security benchmark: Backup and recovery.

BR-1: Ensure regular automated backups

Features

Azure Backup

Description: The service can be backed up by the Azure Backup service. Learn more.

Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

Configuration Guidance: Use Azure Backup Server (as part of Azure Backup) to perform the VM-level backup. Azure Backup Server can store backup data to: Disk: For short-term storage, Azure Backup Server backs up data to disk pools. Azure cloud: For both short-term and long-term storage off-premises, Azure Backup Server data stored in disk pools can be backed up to the Microsoft Azure cloud by using Azure Backup.

Reference: Set up Azure Backup Server for Azure VMware Solution

Service Native Backup Capability

Description: Service supports its own native backup capability (if not using Azure Backup). Learn more.

Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

Configuration Guidance: There is no current Microsoft guidance for this feature configuration. Please review and determine if your organization wants to configure this security feature.

Reference: Deploy disaster recovery with VMware Site Recovery Manager

Next steps

- See the Microsoft cloud security benchmark overview
- Learn more about Azure security baselines

Azure VMware Solution addresses vulnerabilities in the infrastructure

Article • 04/04/2024

At a high level, Azure VMware Solution is an Azure service, so it must follow all the same policies and requirements that Azure follows. Azure policies and procedures dictate that Azure VMware Solution must follow the Security Development Lifecycle (SDL) and must meet several regulatory requirements as promised by Azure.

Our approach to vulnerabilities

Azure VMware Solution takes an in-depth approach to vulnerability and risk management. We follow the SDL to ensure that we're building securely from the start. This focus on security includes working with any third-party solutions. Our services are continually assessed through automatic and manual reviews on a regular basis. We also partner with third-party partners on security hardening and early notifications of vulnerabilities within their solutions.

Vulnerability management

- Engineering and security teams triage any signal of vulnerabilities.
- Details within the signal are adjudicated and assigned a Common Vulnerability Scoring System (CVSS) score and risk rating according to compensating controls within the service.
- The risk rating is used against internal bug bars, internal policies, and regulations to establish a timeline for implementing a fix.
- Internal engineering teams partner with appropriate parties to qualify and roll out any fixes, patches, and other configuration updates necessary.
- Communications are drafted when necessary and published according to the risk rating assigned.

> **Tip**
>
> Communications are surfaced through **Azure Service Health portal**, **known issues**, or email.

Subset of regulations governing vulnerability and risk management

Azure VMware Solution is in scope for the following certifications and regulatory requirements. The regulations listed aren't a complete list of certifications that Azure VMware Solution holds. Instead, it's a list with specific requirements around vulnerability management. These regulations don't rely on other regulations for the same purpose. For example, certain regional certifications might point to ISO requirements for vulnerability management.

> **Note**
>
> You must be an active Microsoft customer to access the following audit reports hosted in the Service Trust Portal:

- ISO
- PCI: See the packages for DSS and 3DS for audit information.
- SOC
- NIST Cybersecurity Framework
- Cyber Essentials Plus

More information

- Azure VMware Solution security recommendations
- Azure VMware Solution security baseline
- Azure defense in-depth approach to cloud vulnerabilities
- Azure compliance offerings
- Azure Service Health portal

Rotate the cloudadmin credentials for Azure VMware Solution

Article • 04/04/2024

In this article, you learn how to rotate the cloudadmin credentials (vCenter Server and VMware NSX cloudadmin credentials) for your Azure VMware Solution private cloud. Although the password for this account doesn't expire, you can generate a new one at any time.

> **⊗ Caution**
>
> If you use your cloudadmin credentials to connect services to vCenter Server or NSX in your private cloud, those connections stop working after you rotate your password. Those connections also lock out the cloudadmin account unless you stop those services before you rotate the password.

Prerequisites

Consider and determine which services connect to vCenter Server as `cloudadmin@vsphere.local` or NSX as cloudadmin before you rotate the password. Services can include VMware services like HCX, vRealize Orchestrator, vRealize Operations Manager, VMware Horizon, or other non-Microsoft tools that are used for monitoring or provisioning.

One way to determine which services authenticate to vCenter Server with the cloudadmin user is to inspect vSphere events by using the vSphere Client for your private cloud. After you identify such services, and before you rotate the password, you must stop these services. Otherwise, the services won't work after you rotate the password. You can also experience temporary locks on your vCenter Server cloudadmin account. Locks occur because these services continuously attempt to authenticate by using a cached version of the old credentials.

Instead of using the cloudadmin user to connect services to vCenter Server or NSX, we recommend that you use individual accounts for each service. For more information about setting up separate accounts for connected services, see Access and identity architecture.

Reset your vCenter Server credentials

Portal

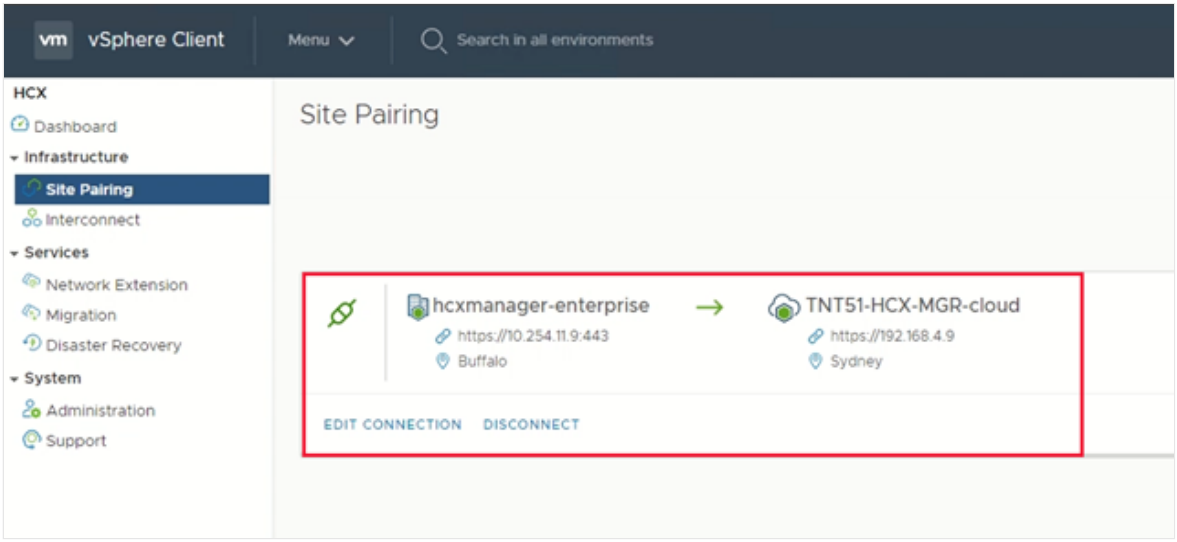
1. In your Azure VMware Solution private cloud, select **VMware credentials**.
2. Select **Generate new password** under vCenter Server credentials.
3. Select the confirmation checkbox and then select **Generate password**.

Update HCX Connector

1. Go to the on-premises HCX Connector and sign in by using the new credentials.

   Be sure to use port **443**.

2. On the VMware HCX dashboard, select **Site Pairing**.



3. Select the correct connection to Azure VMware Solution and select **Edit Connection**.

4. Provide the new vCenter Server user credentials. Select **Edit** to save the credentials. Save should show as successful.

Reset your NSX Manager credentials

1. In your Azure VMware Solution private cloud, select **VMware credentials**.
2. Under NSX Manager credentials, select **Generate new password**.
3. Select the confirmation checkbox and then select **Generate password**.

Next steps

Now that you've learned how to reset your vCenter Server and NSX Manager credentials for Azure VMware Solution, consider learning more about:

- Integrating Azure native services in Azure VMware Solution
- Deploying disaster recovery for Azure VMware Solution workloads using VMware HCX

Set an external identity source for vCenter Server

Article • 03/29/2024

In Azure VMware Solution, VMware vCenter Server has a built-in local user account called *CloudAdmin* that's assigned the CloudAdmin role. You can configure users and groups in Windows Server Active Directory with the CloudAdmin role for your private cloud. In general, the CloudAdmin role creates and manages workloads in your private cloud. But in Azure VMware Solution, the CloudAdmin role has vCenter Server privileges that are different from other VMware cloud solutions and on-premises deployments.

> **Important**
>
> The local CloudAdmin user account should be used as an emergency access account for "break glass" scenarios in your private cloud. It's not intended to be used for daily administrative activities or for integration with other services.

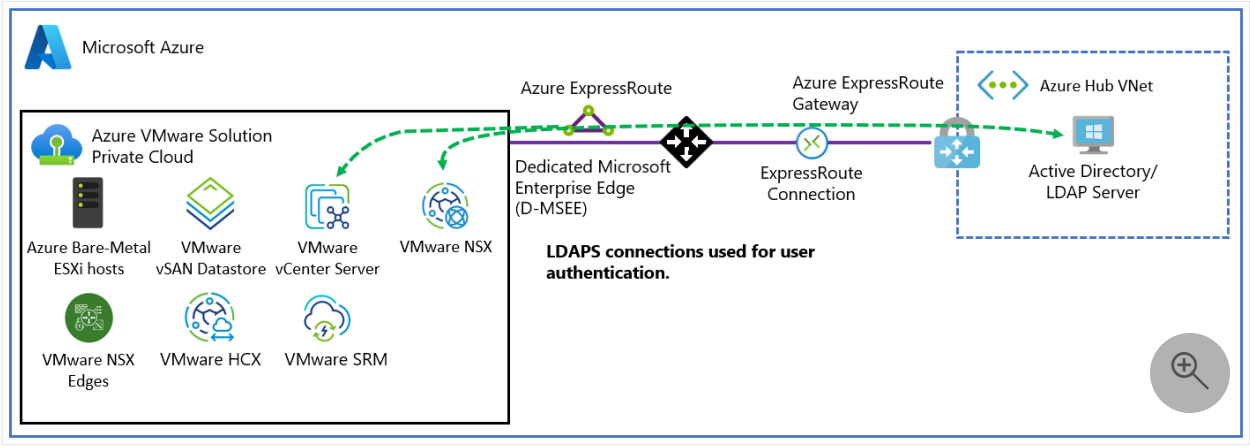
- In a vCenter Server and ESXi on-premises deployment, the administrator has access to the vCenter Server administrator@vsphere.local account and the ESXi root account. The administrator might also be assigned to more Windows Server Active Directory users and groups.
- In an Azure VMware Solution deployment, the administrator doesn't have access to the Administrator user account or the ESXi root account. But the administrator can assign Windows Server Active Directory users and groups the CloudAdmin role in vCenter Server. The CloudAdmin role doesn't have permissions to add an identity source like an on-premises Lightweight Directory Access Protocol (LDAP) or Secure LDAP (LDAPS) server to vCenter Server. However, you can use Run commands to add an identity source and assign the CloudAdmin role to users and groups.

A user account in a private cloud can't access or manage specific management components that Microsoft supports and manages. Examples include clusters, hosts, datastores, and distributed virtual switches.

> **Note**
>
> In Azure VMware Solution, the vsphere.local single sign-on (SSO) domain is provided as a managed resource to support platform operations. You can't use it to

create or manage local groups and users except for the ones that are provided by default with your private cloud.

You can set up vCenter Server to use an external Lightweight Directory Access Protocol (LDAP) directory service to authenticate users. A user can sign in by using their Windows Server Active Directory account credentials or credentials from a third-party LDAP server. Then, the account can be assigned a vCenter Server role, like in an on-premises environment, to provide role-based access for vCenter Server users.



In this article, you learn how to:

- ✓ Export a certificate for LDAPS authentication. (Optional)
- ✓ Upload the LDAPS certificate to blob storage and generate a shared access signature (SAS) URL. (Optional)
- ✓ Configure NSX DNS for resolution to your Windows Server Active Directory domain.
- ✓ Add Windows Server Active Directory by using LDAPS (secure) or LDAP (unsecured).
- ✓ Add an existing Windows Server Active Directory group to the CloudAdmin group.
- ✓ List all existing external identity sources that are integrated with vCenter Server SSO.
- ✓ Assign additional vCenter Server roles to Windows Server Active Directory identities.
- ✓ Remove a Windows Server Active Directory group from the CloudAdmin role.
- ✓ Remove all existing external identity sources.

ⓘ Note

- The steps to export the certificate for LDAPS authentication and upload the LDAPS certificate to blob storage and generate an SAS URL are optional. If the `SSLCertificatesSasUrl` parameter is not provided, the certificate is downloaded from the domain controller automatically through the `PrimaryUrl` or `SecondaryUrl` parameters. To manually export and upload the

certificate, you can provide the `SSLCertificatesSasUrl` parameter and complete the optional steps.

- Run commands one at a time in the order that's described in the article.

Prerequisites

- Ensure that your Windows Server Active Directory network is connected to your Azure VMware Solution private cloud.
- For Windows Server Active Directory authentication with LDAPS:
    1. Get access to the Windows Server Active Directory domain controller with Administrator permissions.
    2. Enable LDAPS on your Windows Server Active Directory domain controllers by using a valid certificate. You can obtain the certificate from an Active Directory Certificate Services Certificate Authority (CA) or a third-party or public CA.
    3. To obtain a valid certificate, complete the steps in Create a certificate for secure LDAP. Ensure that the certificate meets the listed requirements.

        > **Note**
        >
        > Avoid using self-signed certificates in production environments.

    4. Optional: If you don't provide the `SSLCertificatesSasUrl` parameter, the certificate is automatically downloaded from the domain controller via the `PrimaryUrl` or the `SecondaryUrl` parameters. Alternatively, you can manually export the certificate for LDAPS authentication and upload it to an Azure Storage account as blob storage. Then, grant access to Azure Storage resources by using an SAS.
- Configure DNS resolution for Azure VMware Solution to your on-premises Windows Server Active Directory. Set up a DNS forwarder in the Azure portal. For more information, see Configure a DNS forwarder for Azure VMware Solution.

> **Note**

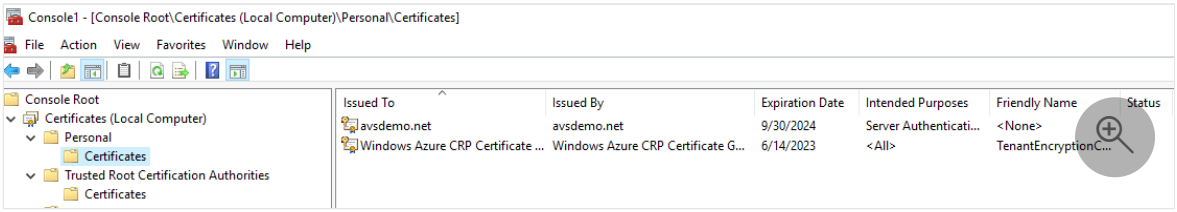
For more information about LDAPS and certificate issuance, contact your security team or your identity management team.

Export the certificate for LDAPS authentication (Optional)

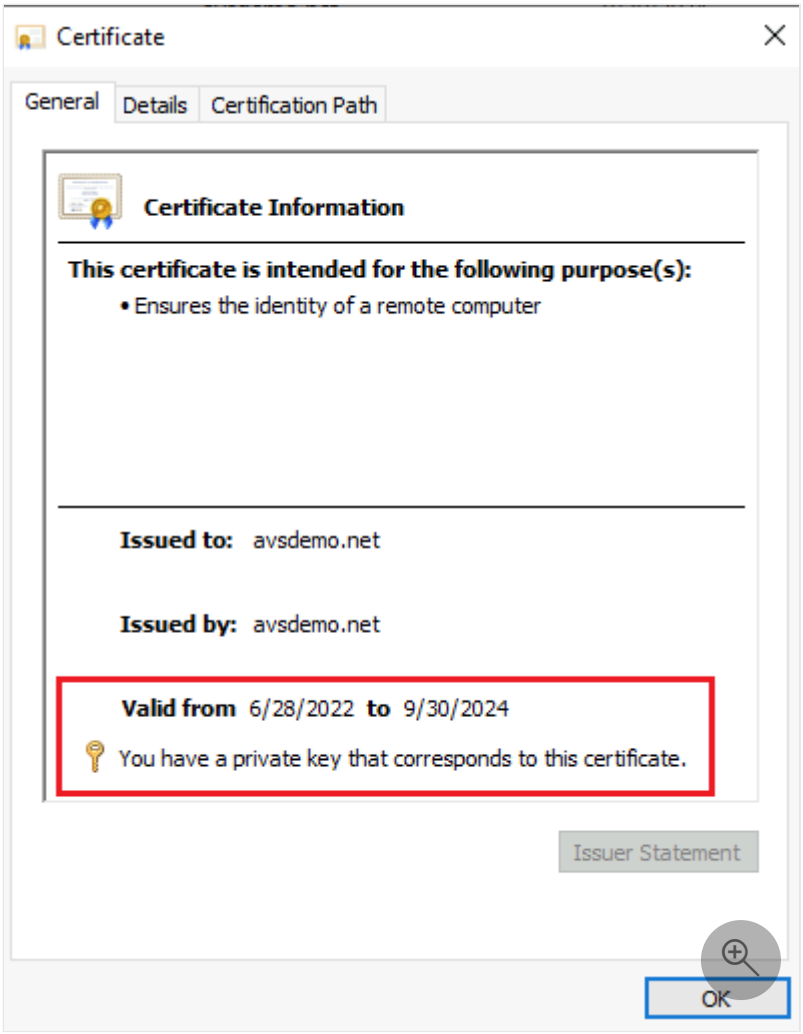
First, verify that the certificate that's used for LDAPS is valid. If you don't have a certificate, complete the steps to create a certificate for LDAPS before you continue.

To verify that the certificate is valid:

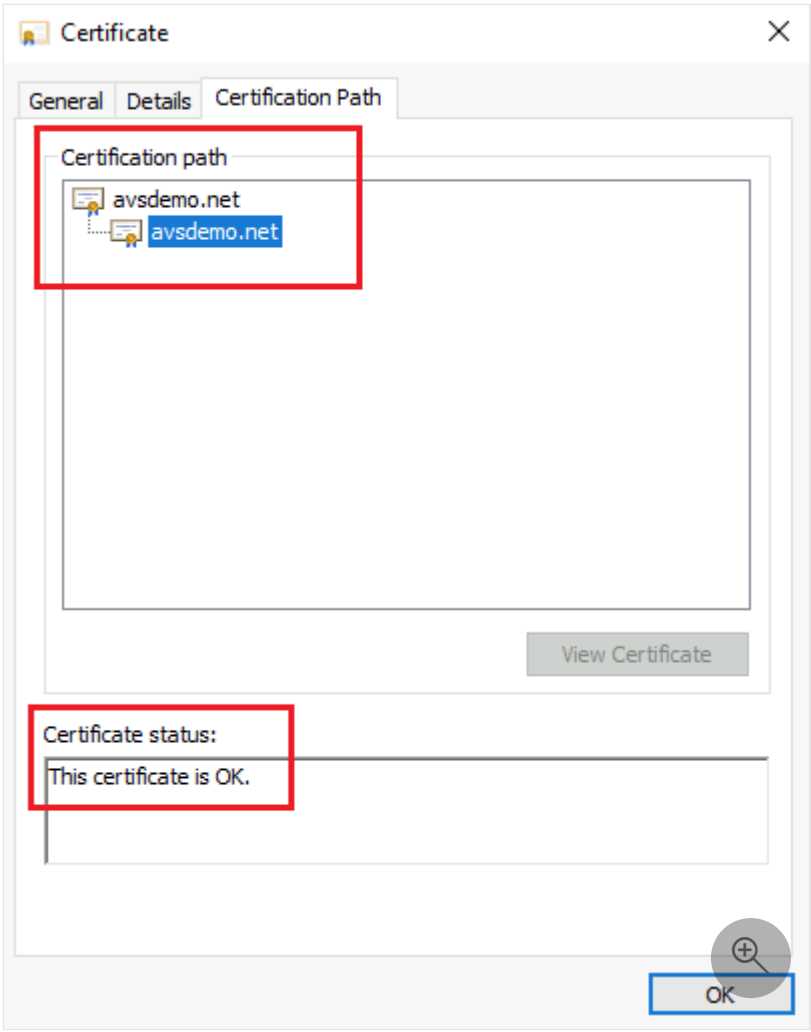
1. Sign in to a domain controller on which LDAPS is active by using Administrator permissions.
2. Open the **Run** tool, enter **mmc**, and then select **OK**.
3. Select **File** > **Add/Remove Snap-in**.
4. In the list of snap-ins, select **Certificates**, and then select **Add**.
5. In the **Certificates snap-in** pane, select **Computer account**, and then select **Next**.
6. Keep **Local computer** selected, select **Finish**, and then select **OK**.
7. In the **Certificates (Local Computer)** management console, expand the **Personal** folder and select the **Certificates** folder to view the installed certificates.



8. Double-click the certificate for LDAPS. Ensure that the certificate date **Valid from** and **Valid to** is current and that the certificate has a private key that corresponds to the certificate.



9. In the same dialog, select the **Certification Path** tab and verify that the value for **Certification path** is valid. It should include the certificate chain of root CA and optional intermediate certificates. Check that the **Certificate status** is **OK**.



10. Select **OK**.

To export the certificate:

1. In the Certificates console, right-click the LDAPS certificate and select **All Tasks** > **Export**. The Certificate Export Wizard opens. Select **Next**.
2. In the **Export Private Key** section, select **No, do not export the private key**, and then select **Next**.
3. In the **Export File Format** section, select **Base-64 encoded X.509(.CER)**, and then select **Next**.
4. In the **File to Export** section, select **Browse**. Select a folder location to export the certificate, and enter a name. Then select **Save**.

> ⓘ **Note**
>
> If more than one domain controller is set to use LDAPS, repeat the export procedure for each additional domain controller to export their corresponding certificates. Note that you can reference only two LDAPS servers in the `New-`

`LDAPSIdentitySource` Run tool. If the certificate is a wildcard certificate, such as `.avsdemo.net`, export the certificate from only one of the domain controllers.

Upload the LDAPS certificate to blob storage and generate an SAS URL (Optional)

Next, upload the certificate file (in *.cer* format) you exported to an Azure Storage account as blob storage. Then, grant access to Azure Storage resources by using an SAS.

If you need multiple certificates, upload each one individually and generate an SAS URL for each certificate.

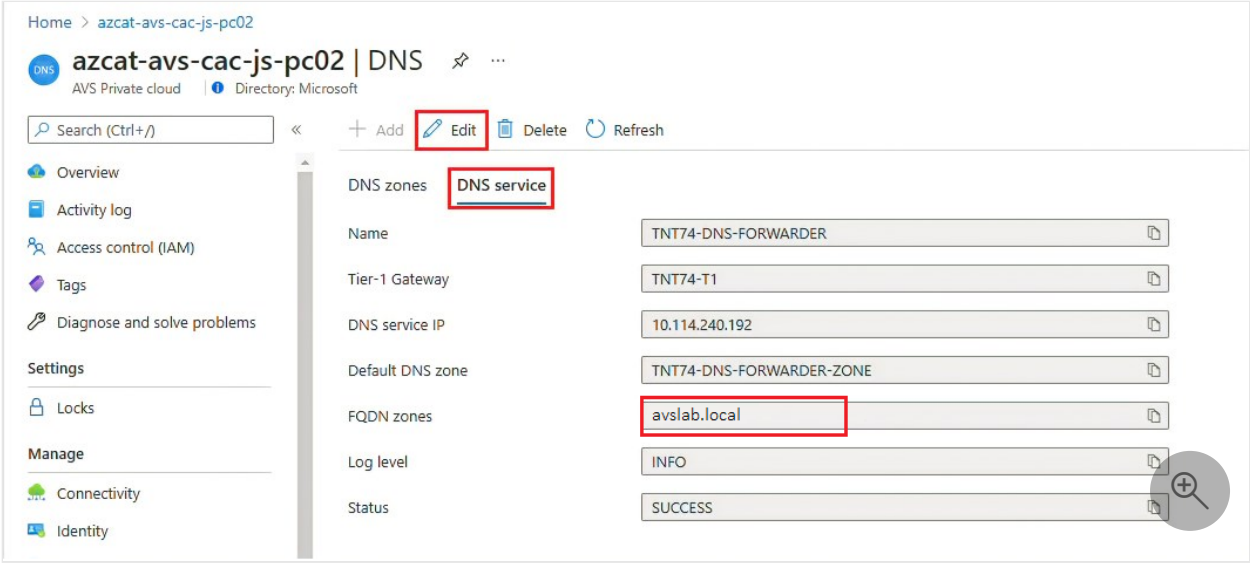
> **Important**
>
> Remember to copy all SAS URL strings. The strings aren't accessible after you leave the page.

> **Tip**
>
> An alternative method to consolidate certificates involves storing all the certificate chains in one file, as detailed in a VMware knowledge base article. Then, generate a single SAS URL for the file that contains all the certificates.

Set up NSX-T DNS for Windows Server Active Directory domain resolution

Create a DNS zone and add it to the DNS service. Complete the steps in Configure a DNS forwarder in the Azure portal.

After you complete these steps, verify that your DNS service includes your DNS zone.



Your Azure VMware Solution private cloud should now properly resolve your on-premises Windows Server Active Directory domain name.

Add Windows Server Active Directory by using LDAP via SSL

To add Windows Server Active Directory over LDAP with SSL as an external identity source to use with SSO to vCenter Server, run the New-LDAPSIdentitySource cmdlet.

1. Go to your Azure VMware Solution private cloud and select **Run command** > **Packages** > **New-LDAPSIdentitySource**.

2. Provide the required values or modify the default values, and then select **Run**.

Expand table

Name	Description
GroupName	The group in the external identity source that grants CloudAdmin access. For example, **avs-admins**.
SSLCertificatesSasUrl	The path to SAS strings that contain the certificates for authentication to the Windows Server Active Directory source. Separate multiple certificates with a comma. For example, **pathtocert1,pathtocert2**.
Credential	The domain username and password for authentication with the Windows Server Active Directory source (not CloudAdmin). Use the `<username@avslab.local>` format.
BaseDNGroups	The location to search for groups. For example, **CN=group1, DC=avsldap,DC=local**. Base DN is required for LDAP

Name	Description
	authentication.
BaseDNUsers	The location to search for valid users. For example, **CN=users,DC=avsldap,DC=local**. Base DN is required for LDAP authentication.
PrimaryUrl	The primary URL of the external identity source. For example, `ldaps://yourserver.avslab.local:636`.
SecondaryURL	The secondary fallback URL if the primary fails. For example, `ldaps://yourbackupldapserver.avslab.local:636`.
DomainAlias	For Windows Server Active Directory identity sources, the domain's NetBIOS name. Add the NetBIOS name of the Windows Server Active Directory domain as an alias of the identity source, typically in the **avsldap** format.
DomainName	The domain's fully qualified domain name (FQDN). For example, **avslab.local**.
Name	A name for the external identity source. For example, **avslab.local**.
Retain up to	The retention period of the cmdlet output. The default value is 60 days.
Specify name for execution	An alphanumeric name. For example, **addexternalIdentity**.
Timeout	The period after which a cmdlet exits if it isn't finished running.

3. To monitor progress and confirm successful completion, check **Notifications** or the **Run Execution Status** pane.

Add Windows Server Active Directory by using LDAP

> ⓘ **Note**
>
> We recommend that you use the method to add Windows Server Active Directory over LDAP by using SSL.

To add Windows Server Active Directory over LDAP as an external identity source to use with SSO to vCenter Server, run the New-LDAPIdentitySource cmdlet.

1. Select **Run command** > **Packages** > **New-LDAPIdentitySource**.

2. Provide the required values or modify the default values, and then select **Run**.

Expand table

Name	Description
Name	A name for the external identity source. For example, **avslab.local**. This name appears in vCenter Server.
DomainName	The domain's FQDN. For example, **avslab.local**.
DomainAlias	For Windows Server Active Directory identity sources, the domain's NetBIOS name. Add the Windows Server Active Directory domain's NetBIOS name as an alias of the identity source, typically in the **avsldap** format.
PrimaryUrl	The primary URL of the external identity source. For example, `ldap://yourserver.avslab.local:389`.
SecondaryURL	The secondary fallback URL if there's a primary failure.
BaseDNUsers	The location to search for valid users. For example, **CN=users,DC=avslab,DC=local**. Base DN is required for LDAP authentication.
BaseDNGroups	The location to search for groups. For example, **CN=group1, DC=avslab,DC=local**. Base DN is required for LDAP authentication.
Credential	The domain username and password for authentication with the Windows Server Active Directory source (not CloudAdmin). The user must be in the `<username@avslab.local>` format.
GroupName	The group in your external identity source that grants CloudAdmin access. For example, **avs-admins**.
Retain up to	The retention period for the cmdlet output. The default value is 60 days.
Specify name for execution	An alphanumeric name. For example, **addexternalIdentity**.
Timeout	The period after which a cmdlet exits if it isn't finished running.

3. To monitor the progress, check **Notifications** or the **Run Execution Status** pane.

Add an existing Windows Server Active Directory group to a CloudAdmin group

> **Important**
>
> Nested groups aren't supported. Using a nested group might cause loss of access.

Users in a CloudAdmin group have user rights that are equal to the CloudAdmin (`<cloudadmin@vsphere.local>`) role that's defined in vCenter Server SSO. To add an existing Windows Server Active Directory group to a CloudAdmin group, run the Add-GroupToCloudAdmins cmdlet.

1. Select **Run command** > **Packages** > **Add-GroupToCloudAdmins**.
2. Enter or select the required values, and then select **Run**.

Expand table

Name	Description
GroupName	The name of the group to add. For example, **VcAdminGroup**.
Retain up to	The retention period of the cmdlet output. The default value is 60 days.
Specify name for execution	An alphanumeric name. For example, **addADgroup**.
Timeout	The period after which a cmdlet exits if it isn't finished running.

3. Check **Notifications** or the **Run Execution Status** pane to see the progress.

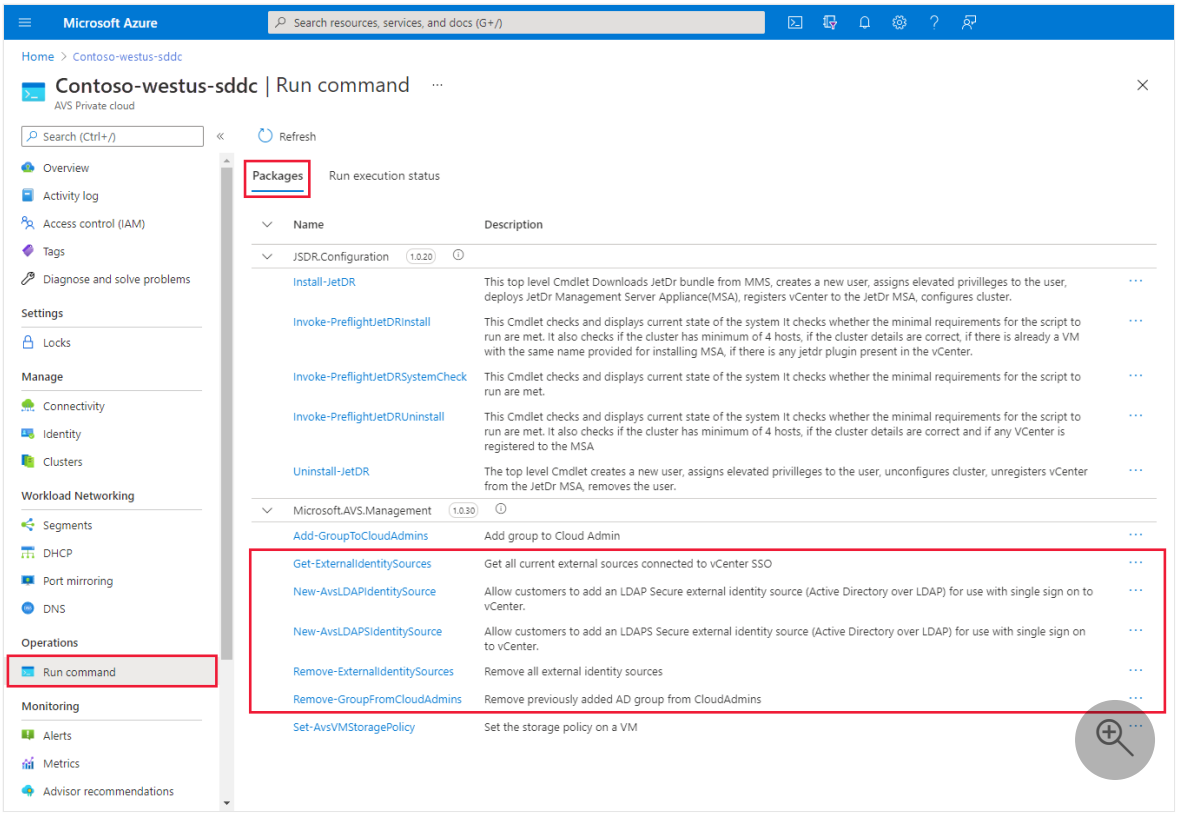
List external identity sources

To list all external identity sources that are already integrated with vCenter Server SSO, run the Get-ExternalIdentitySources cmdlet.

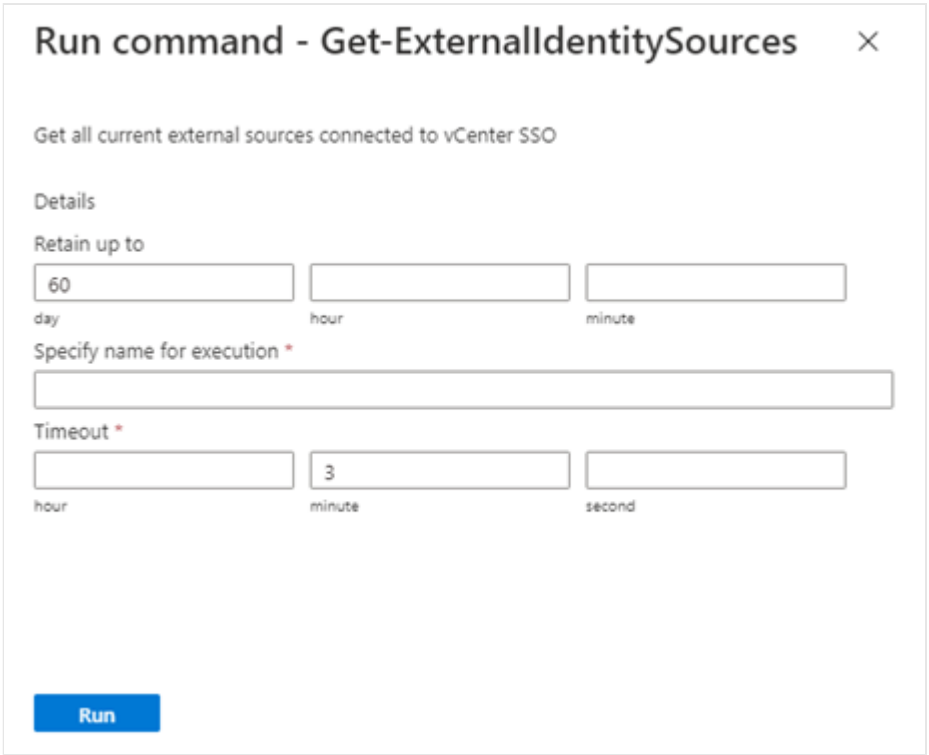
1. Sign in to the Azure portal.

> **Note**
>
> If you need access to the Azure for US Government portal, go to `<https://portal.azure.us/>`.

2. Select **Run command** > **Packages** > **Get-ExternalIdentitySources**.



3. Enter or select the required values, and then select **Run**.

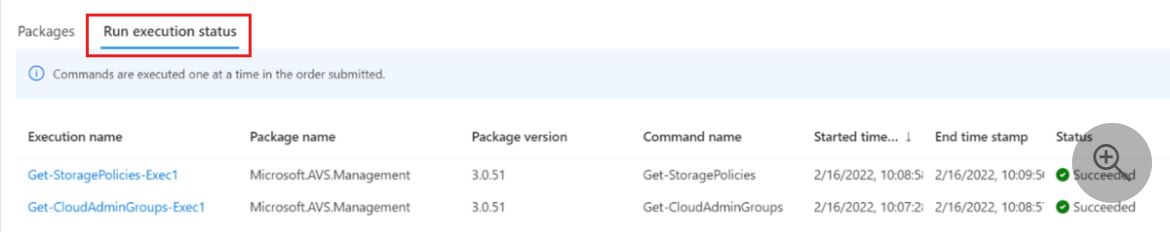


Expand table

Name	Description
Retain up to	The retention period of the cmdlet output. The default value is 60 days.

Name	Description
Specify name for execution	An alphanumeric name. For example, **getExternalIdentity**.
Timeout	The period after which a cmdlet exits if it isn't finished running.

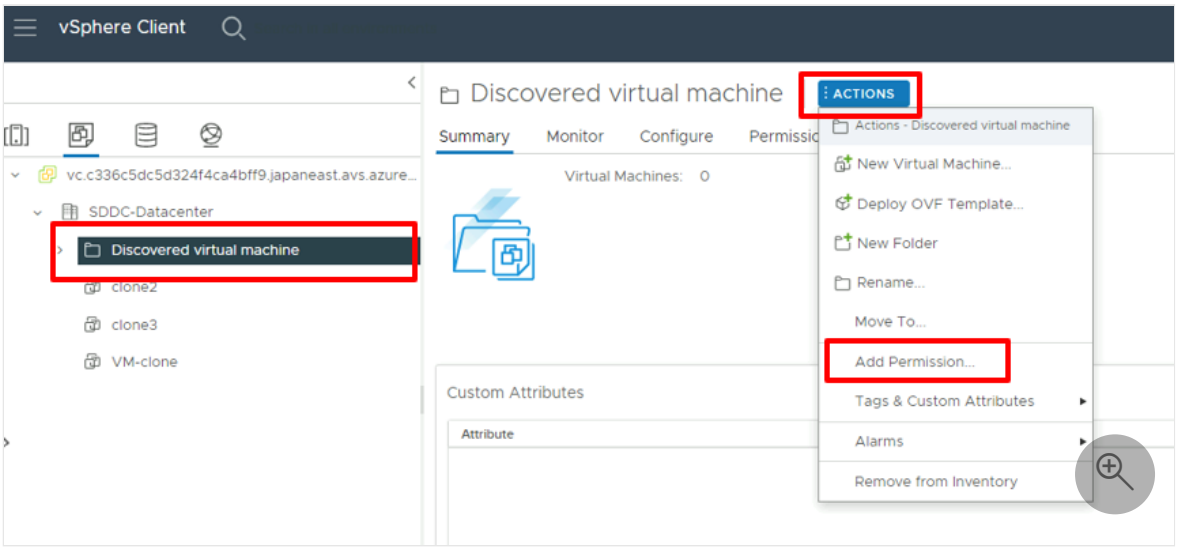
4. To see the progress, check **Notifications** or the **Run Execution Status** pane.



Assign more vCenter Server roles to Windows Server Active Directory identities

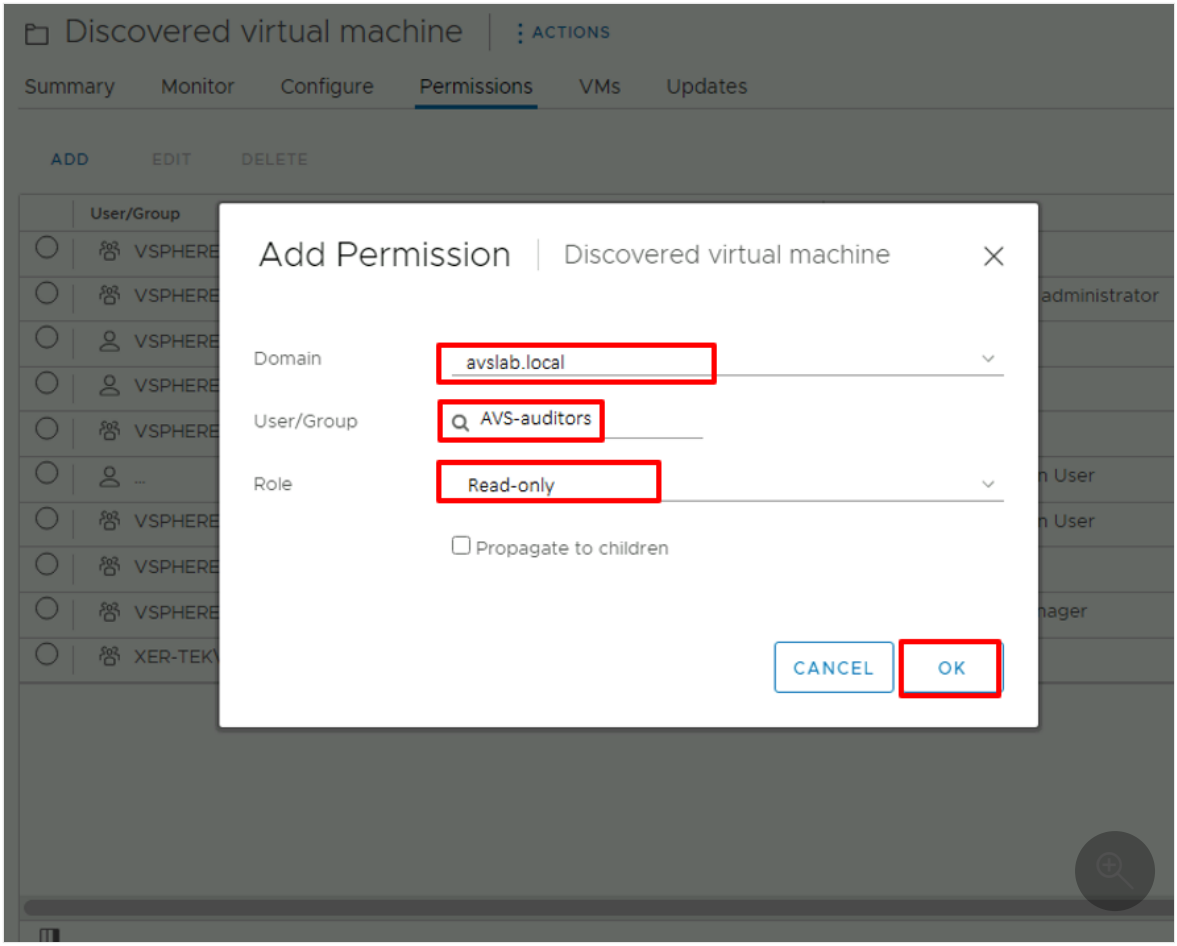
After you add an external identity over LDAP or LDAPS, you can assign vCenter Server roles to Windows Server Active Directory security groups based on your organization's security controls.

1. Sign in to vCenter Server as CloudAdmin, select an item from the inventory, select the **Actions** menu, and then select **Add Permission**.

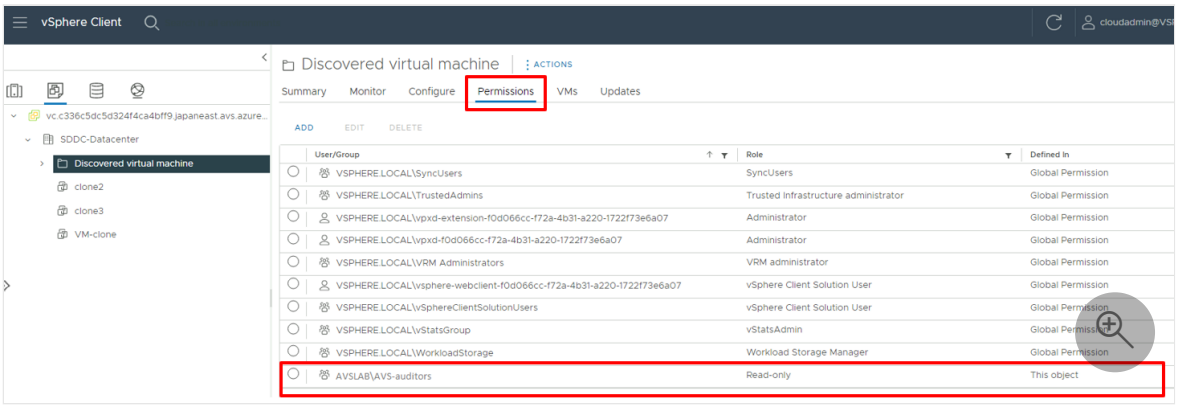


2. In the **Add Permission** dialog:
   a. **Domain**: Select the previously added instance of Windows Server Active Directory.
   b. **User/Group**: Enter the user or group name, search for it, and then select it.
   c. **Role**: Select the role to assign.

d. **Propagate to children**: Optionally, select the checkbox to propagate permissions to child resources.



3. Select the **Permissions** tab and verify that the permission assignment was added.



Users can now sign in to vCenter Server by using their Windows Server Active Directory credentials.

Remove a Windows Server Active Directory group from the CloudAdmin role

To remove a specific Windows Server Active Directory group from the CloudAdmin role, run the Remove-GroupFromCloudAdmins cmdlet.

1. Select **Run command** > **Packages** > **Remove-GroupFromCloudAdmins**.
2. Enter or select the required values, and then select **Run**.

Expand table

Name	Description
GroupName	The name of the group to remove. For example, **VcAdminGroup**.
Retain up to	The retention period of the cmdlet output. The default value is 60 days.
Specify name for execution	An alphanumeric name. For example, **removeADgroup**.
Timeout	The period after which a cmdlet exits if it isn't finished running.

3. To see the progress, check **Notifications** or the **Run Execution Status** pane.

Remove all existing external identity sources

To remove all existing external identity sources at once, run the Remove-ExternalIdentitySources cmdlet.

1. Select **Run command** > **Packages** > **Remove-ExternalIdentitySources**.
2. Enter or select the required values, and then select **Run**:

Expand table

Name	Description
Retain up to	The retention period of the cmdlet output. The default value is 60 days.
Specify name for execution	An alphanumeric name. For example, **remove_externalIdentity**.
Timeout	The period after which a cmdlet exits if it isn't finished running.

3. To see the progress, check **Notifications** or the **Run Execution Status** pane.

Rotate an existing external identity source account's username or password

1. Rotate the password of the account that's used for authentication with the Windows Server Active Directory source in the domain controller.
2. Select **Run command** > **Packages** > **Update-IdentitySourceCredential**.
3. Enter or select the required values, and then select **Run**.

Expand table

Name	Description
Credential	The domain username and password that are used for authentication with the Windows Server Active Directory source (not CloudAdmin). The user must be in the `<username@avslab.local>` format.
DomainName	The FQDN of the domain. For example, **avslab.local**.

4. To see the progress, check **Notifications** or the **Run Execution Status** pane.

> ⚠ **Warning**
>
> If you don't provide a value for **DomainName**, all external identity sources are removed. Run the cmdlet Update-IdentitySourceCredential only after the password is rotated in the domain controller.

Renew existing certificates for LDAPS identity source

1. Renew the existing certificates in your domain controllers.
2. Optional: If the certificates are stored in default domain controllers, this step is optional. Leave the SSLCertificatesSasUrl parameter blank and the new certificates will be downloaded from the default domain controllers and updated in vCenter automatically. If you choose to not use the default way, export the certificate for LDAPS authentication and upload the LDAPS certificate to blob storage and generate an SAS URL. Save the SAS URL for the next step.
3. Select **Run command** > **Packages** > **Update-IdentitySourceCertificates**.

4. Provide the required values and the new SAS URL (optional), and then select **Run**.

Expand table

Field	Value
DomainName*	The FQDN of the domain, for example **avslab.local**.
SSLCertificatesSasUrl (optional)	A comma-delimited list of SAS path URI to Certificates for authentication. Ensure permissions to read are included. To generate, place the certificates in any storage account blob and then right-click the cert and generate SAS. If the value of this field isn't provided by a user, the certificates will be downloaded from the default domain controllers.

5. Check **Notifications** or the **Run Execution Status** pane to see the progress.

Related content

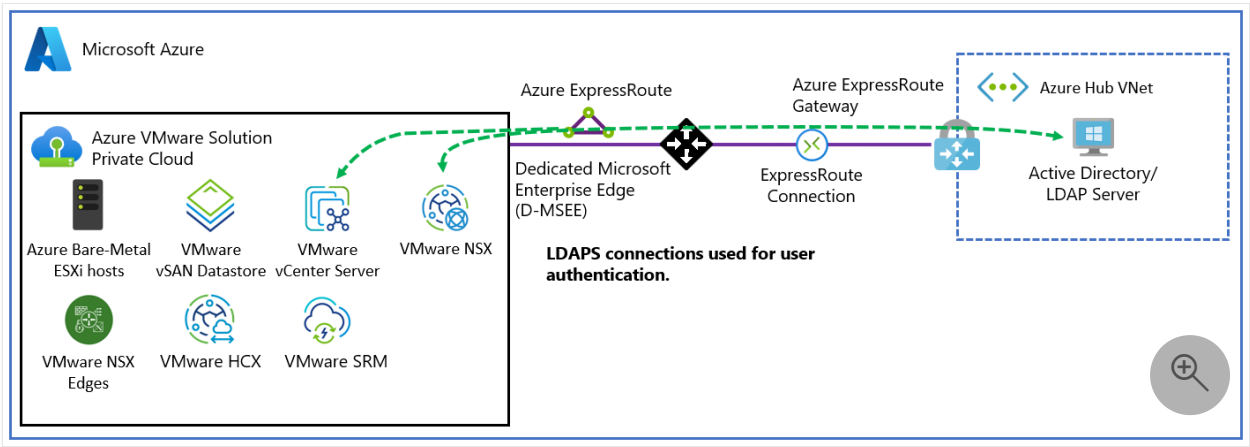
- Create a storage policy
- Azure VMware Solution identity architecture
- Set an external identity source for NSX
- VMware product documentation

Set an external identity source for VMware NSX

Article • 03/29/2024

In this article, learn how to set up an external identity source for VMware NSX in an instance of Azure VMware Solution.

You can set up NSX to use an external Lightweight Directory Access Protocol (LDAP) directory service to authenticate users. A user can sign in by using their Windows Server Active Directory account credentials or credentials from a third-party LDAP server. Then, the account can be assigned an NSX role, like in an on-premises environment, to provide role-based access for NSX users.



Prerequisites

- A working connection from your Windows Server Active Directory network to your Azure VMware Solution private cloud.
- A network path from your Windows Server Active Directory server to the management network of the instance of Azure VMware Solution in which NSX is deployed.
- A Windows Server Active Directory domain controller that has a valid certificate. The certificate can be issued by a Windows Server Active Directory Certificate Services Certificate Authority (CA) or by a third-party CA.

  We recommend that you use two domain controllers that are located in the same Azure region as the Azure VMware Solution software-defined datacenter.

  > **Note**

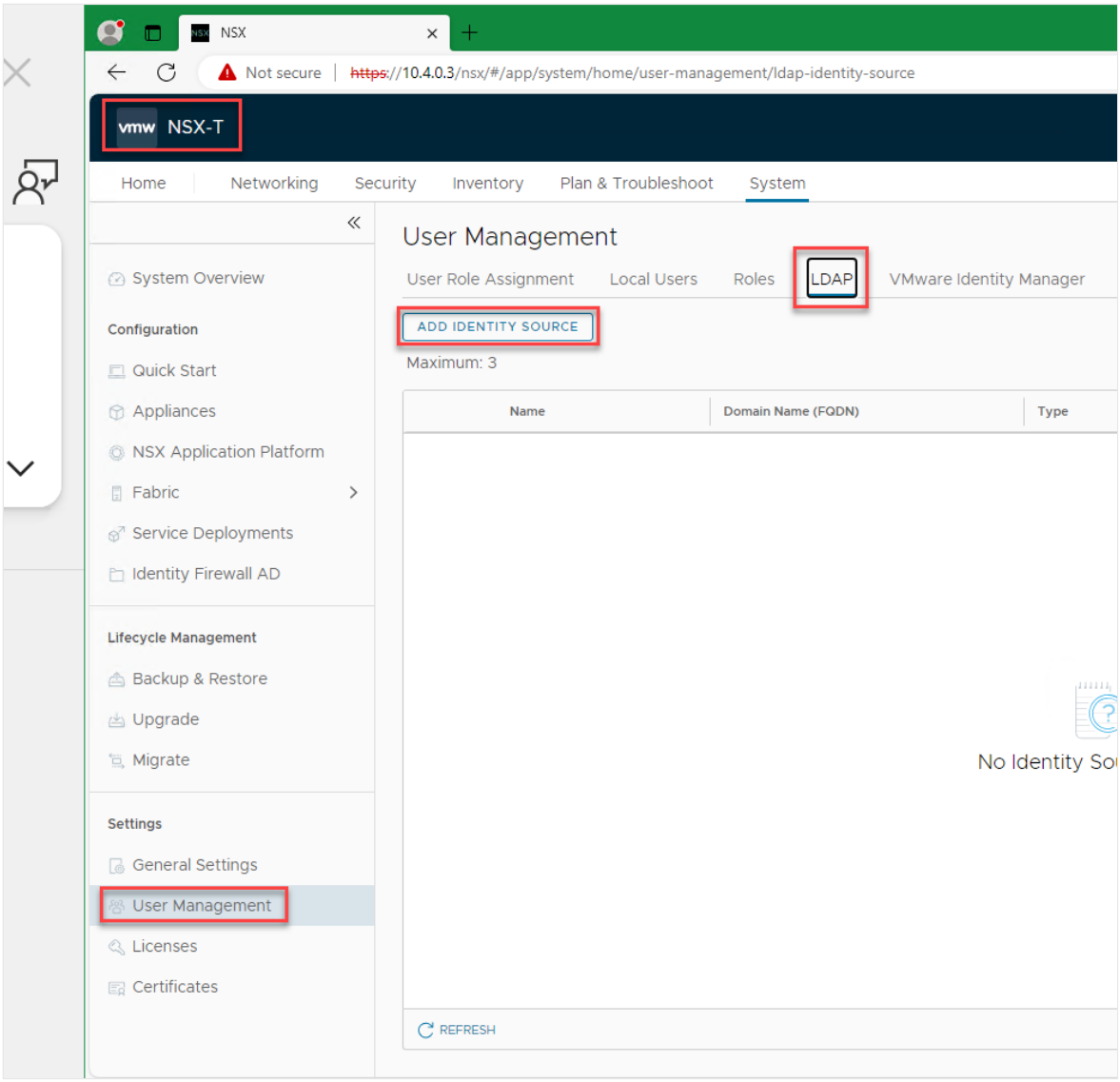
Self-signed certificates are not recommended for production environments.

- An account that has Administrator permissions.
- Azure VMware Solution DNS zones and DNS servers that are correctly configured. For more information, see Configure NSX DNS for resolution to your Windows Server Active Directory domain and set up DNS forwarder.

> **Note**
>
> For more information about Secure LDAP (LDAPS) and certificate issuance, contact your security team or your identity management team.

Use Windows Server Active Directory as an LDAPS identity source

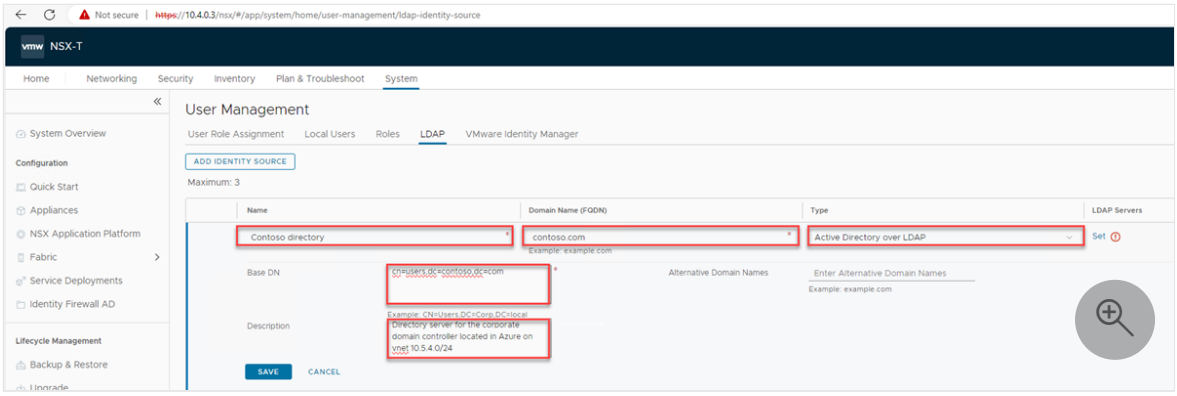
1. Sign in to NSX Manager, and then go to **System** > **User Management** > **LDAP** > **Add Identity Source**.



2. Enter values for **Name**, **Domain Name (FQDN)**, **Type**, and **Base DN**. You can add a description (optional).

   The base DN is the container where your user accounts are kept. The base DN is the starting point that an LDAP server uses when it searches for users in an authentication request. For example, **CN=users,dc=azfta,dc=com**.

> **Note**
>
> You can use more than one directory as an LDAP provider. An example is if you have multiple Windows Server Azure Directory domains, and you use Azure VMware Solution as a way to consolidate workloads.

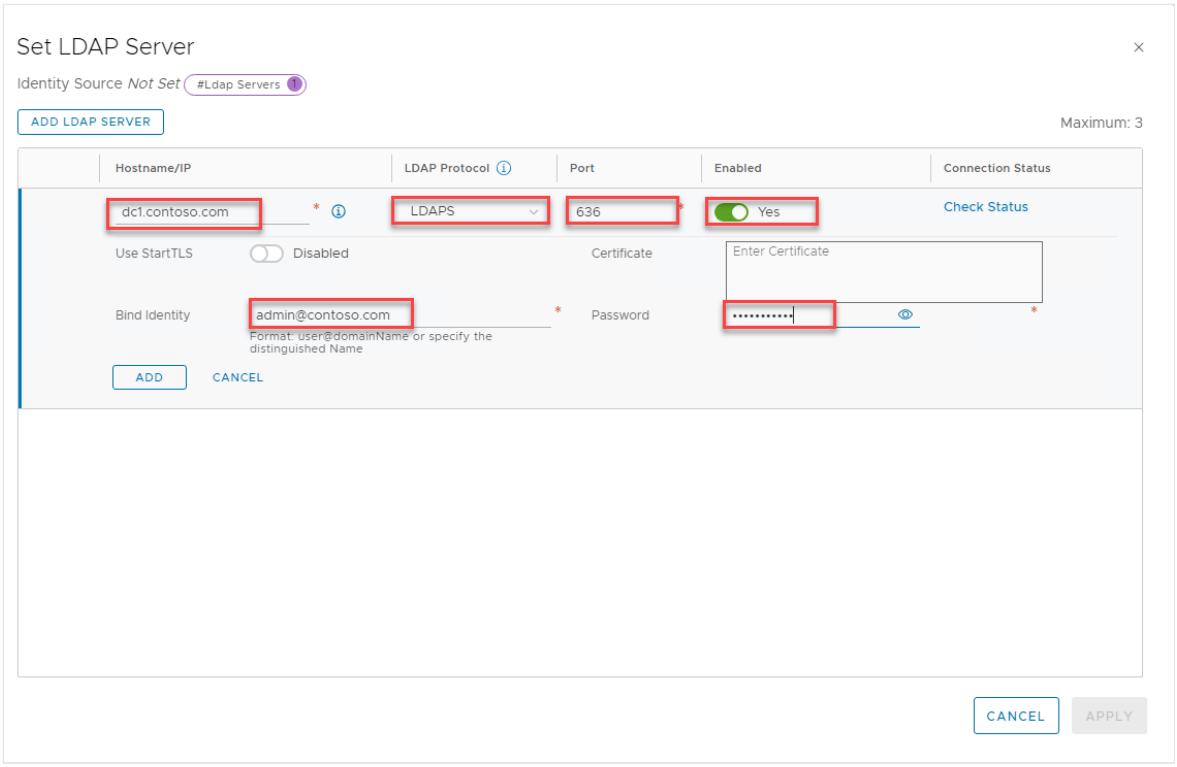


3. Next, under **LDAP Servers**, select **Set** as shown in the preceding screenshot.

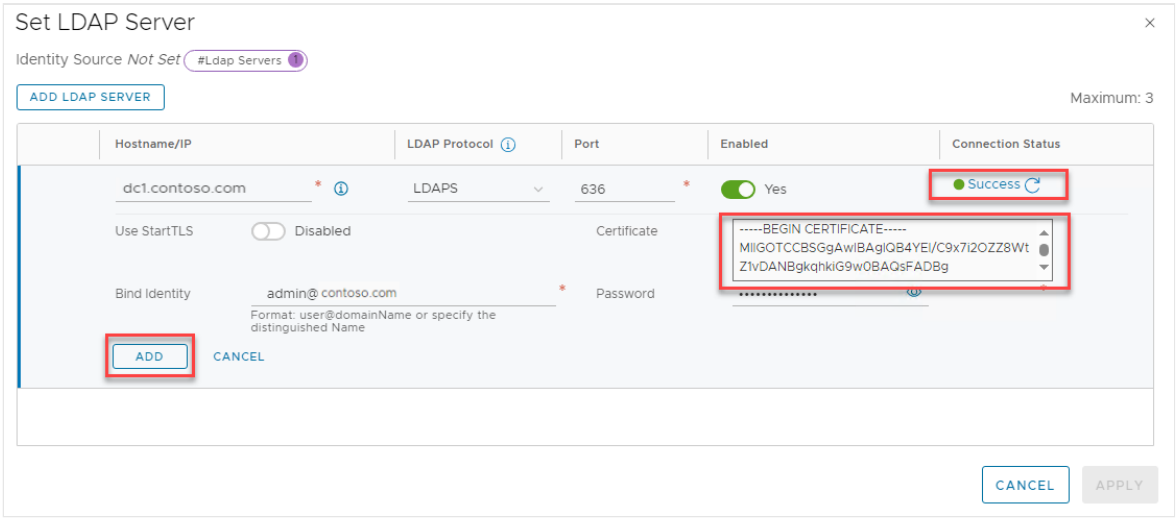
4. On **Set LDAP Server**, select **Add LDAP Server**, and then enter or select values for the following items:

Expand table

Name	Action
Hostname/IP	Enter the LDAP server's FQDN or IP address. For example, **azfta-dc01.azfta.com** or **10.5.4.4**.
LDAP Protocol	Select **LDAPS**.
Port	Leave the default secure LDAP port.
Enabled	Leave as **Yes**.
Use Start TLS	Required only if you use standard (unsecured) LDAP.
Bind Identity	Use your account that has domain Administrator permissions. For example, `<admin@contoso.com>`.
Password	Enter the password for the LDAP server. This password is the one that you use with the example `<admin@contoso.com>` account.
Certificate	Leave empty (see step 6).



5. After the page updates and displays a connection status, select **Add**, and then select **Apply**.



6. On **User Management**, select **Save** to complete the changes.

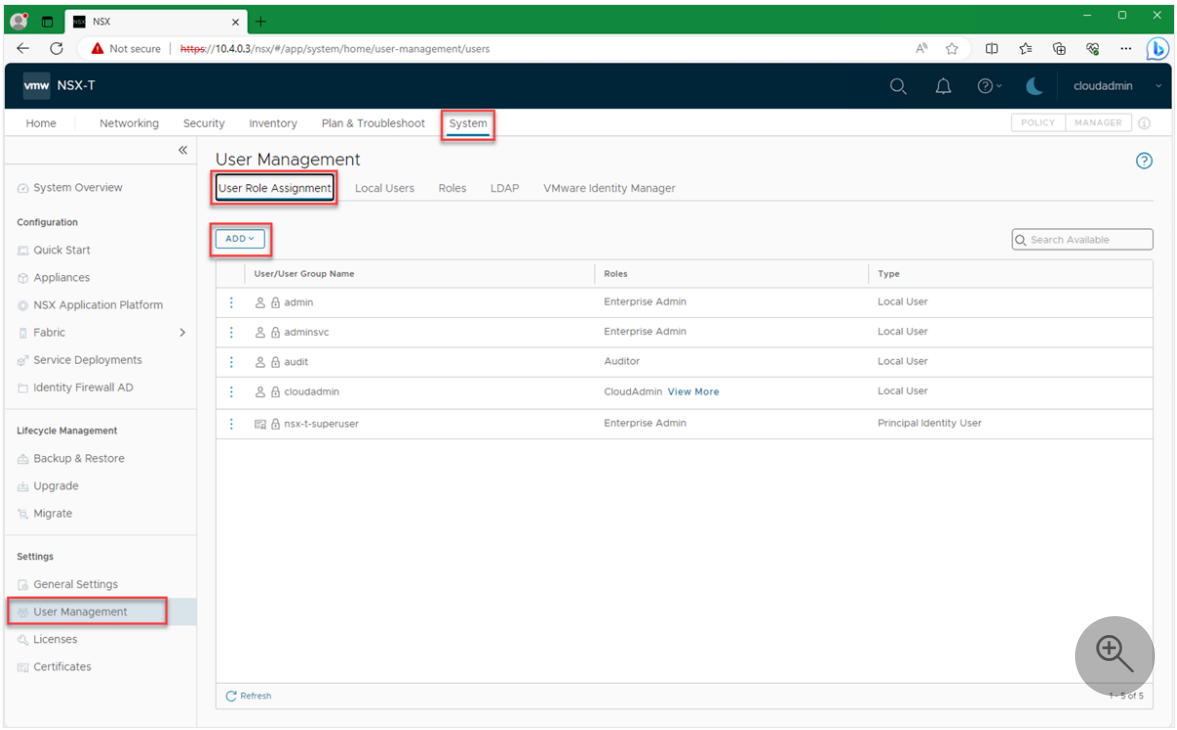
7. To add a second domain controller or another external identity provider, return to step 1.

> **Note**
>
> A recommended practice is to have two domain controllers to act as LDAP servers. You can also put the LDAP servers behind a load balancer.

Assign roles to Windows Server Active Directory identities

After you add an external identity, you can assign NSX roles to Windows Server Active Directory security groups based on your organization's security controls.

1. In NSX Manager, go to **System** > **User Management** > **User Role Assignment** > **Add**.



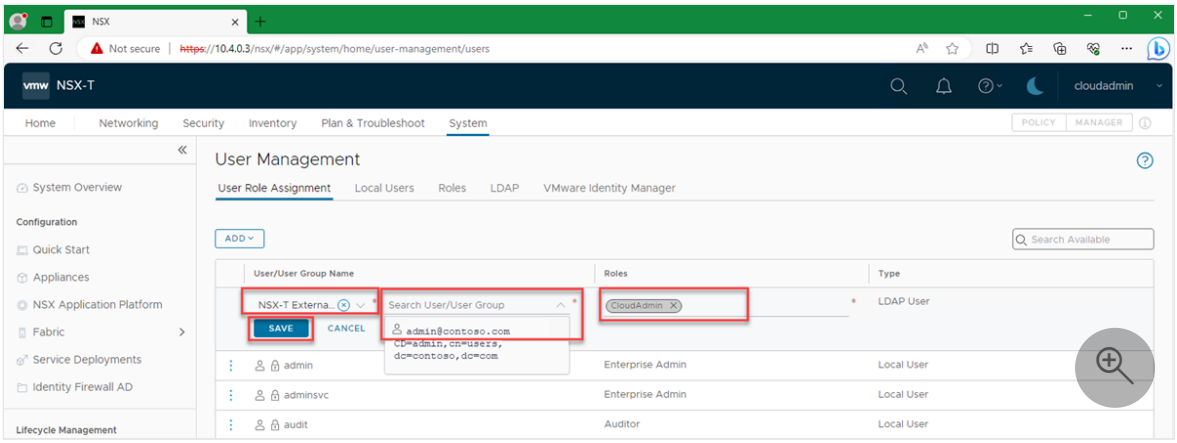
2. Select **Add** > **Role Assignment for LDAP**.

   a. Select the external identity provider that you selected in step 3 in the preceding section. For example, **NSX External Identity Provider**.

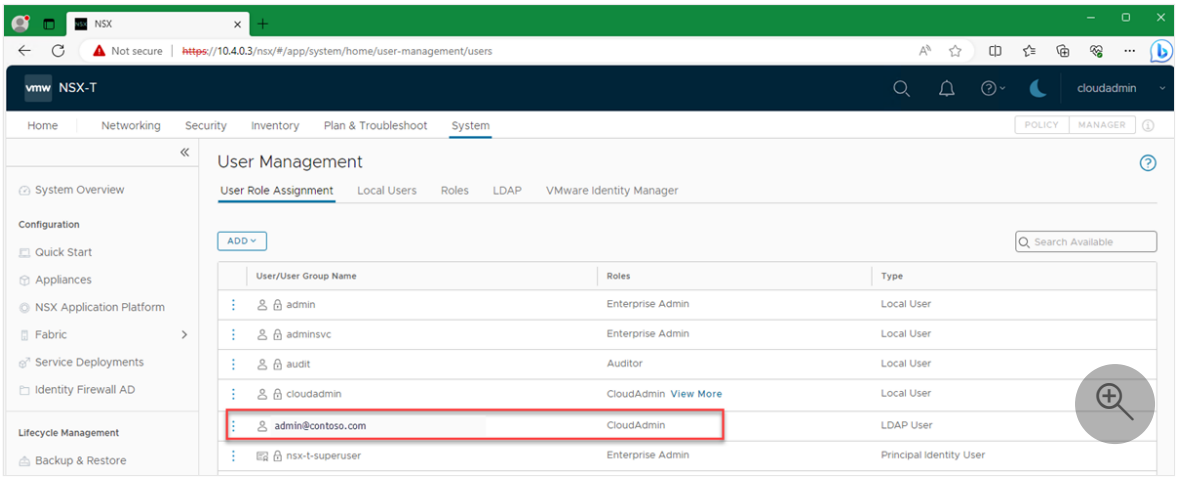
   b. Enter the first few characters of the user's name, the user's sign-in ID, or a group name to search the LDAP directory. Then select a user or group from the list of results.

   c. Select a role. In this example, assign the FTAdmin user the CloudAdmin role.

   d. Select **Save**.



3. Under **User Role Assignment**, verify that the permissions assignment appears.



Your users should now be able to sign in to NSX Manager by using their Windows Server Active Directory credentials.

Related content

- Azure VMware Solution identity architecture
- Set an external identity source for vCenter Server
- VMware product documentation

Integrate Microsoft Defender for Cloud with Azure VMware Solution

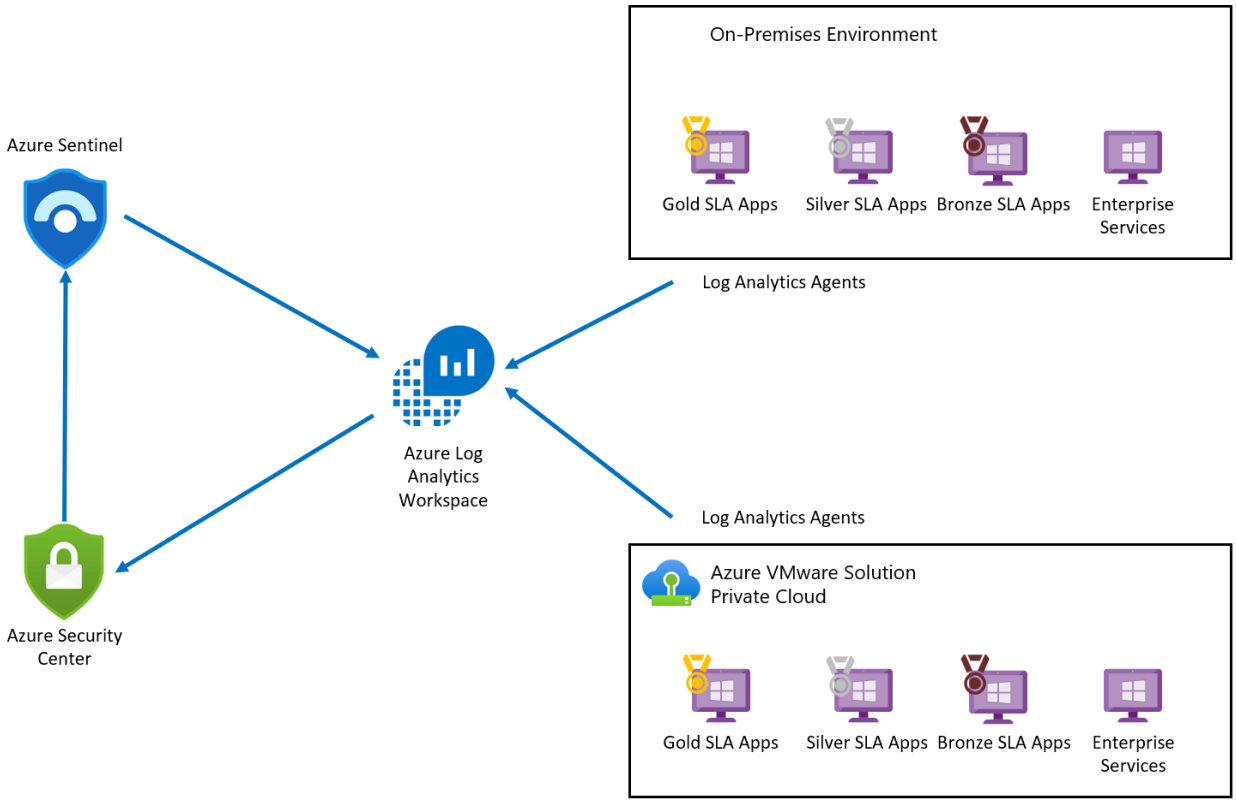
Article • 02/28/2024

Microsoft Defender for Cloud provides advanced threat protection across your Azure VMware Solution and on-premises virtual machines (VMs). It assesses the vulnerability of Azure VMware Solution VMs and raises alerts as needed. These security alerts can be forwarded to Azure Monitor for resolution. You can define security policies in Microsoft Defender for Cloud. For more information, see Working with security policies.

Microsoft Defender for Cloud offers many features, including:

- File integrity monitoring
- Fileless attack detection
- Operating system patch assessment
- Security misconfigurations assessment
- Endpoint protection assessment

The diagram shows the integrated monitoring architecture of integrated security for Azure VMware Solution VMs.



Log Analytics agent collects log data from Azure, Azure VMware Solution, and on-premises VMs. The log data is sent to Azure Monitor Logs and stored in a **Log Analytics Workspace**. Each workspace has its own data repository and configuration to store data.

Once the logs are collected, **Microsoft Defender for Cloud** assesses the vulnerability status of Azure VMware Solution VMs and raises an alert for any critical vulnerability. Once assessed, Microsoft Defender for Cloud forwards the vulnerability status to Microsoft Sentinel to create an incident and map with other threats. Microsoft Defender for Cloud is connected to Microsoft Sentinel using Microsoft Defender for Cloud Connector.

Prerequisites

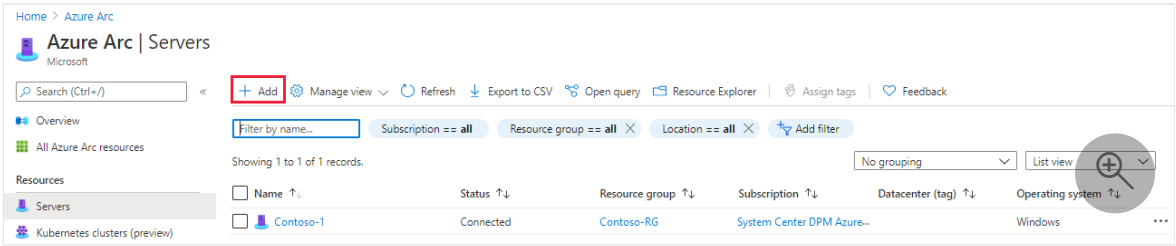
- Plan for optimized use of Defender for Cloud.
- Review the supported platforms in Defender for Cloud.
- Create a Log Analytics workspace to collect data from various sources.
- Enable Microsoft Defender for Cloud in your subscription.

  > **Note**
  >
  > Microsoft Defender for Cloud is a pre-configured tool that doesn't require deployment, but you'll need to enable it.

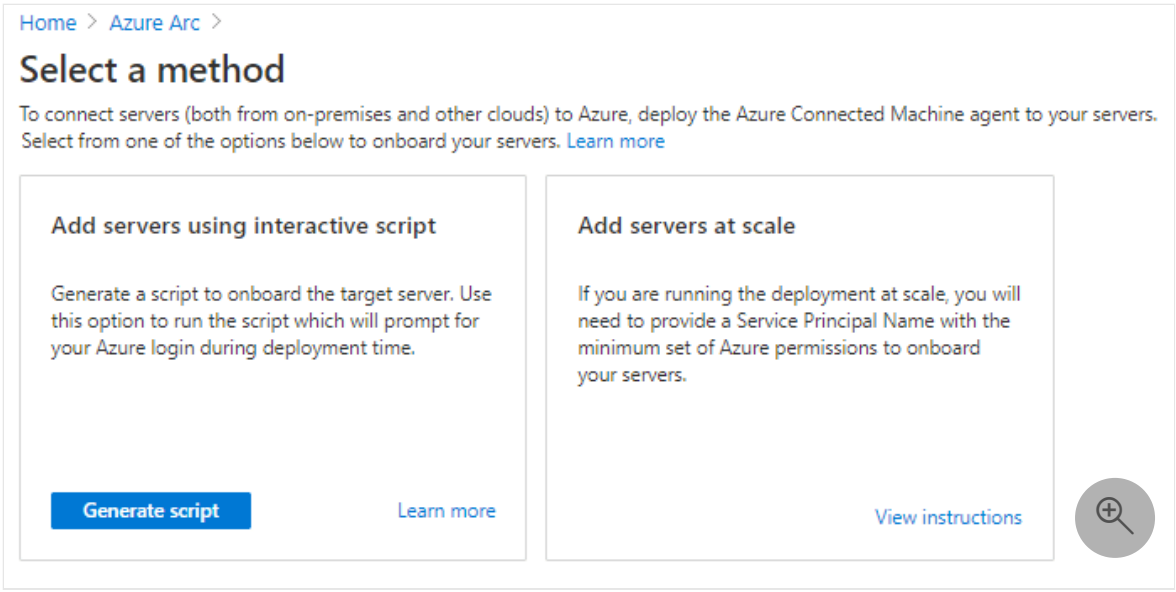
- Enable Microsoft Defender for Cloud.

Add Azure VMware Solution VMs to Defender for Cloud

1. In the Azure portal, search on **Azure Arc** and select it.
2. Under Resources, select **Servers** and then **+Add**.



3. Select **Generate script**.



4. On the **Prerequisites** tab, select **Next**.

5. On the **Resource details** tab, fill in the following details and then select **Next. Tags**:

    - Subscription
    - Resource group
    - Region
    - Operating system
    - Proxy Server details

6. On the **Tags** tab, select **Next**.

7. On the **Download and run script** tab, select **Download**.

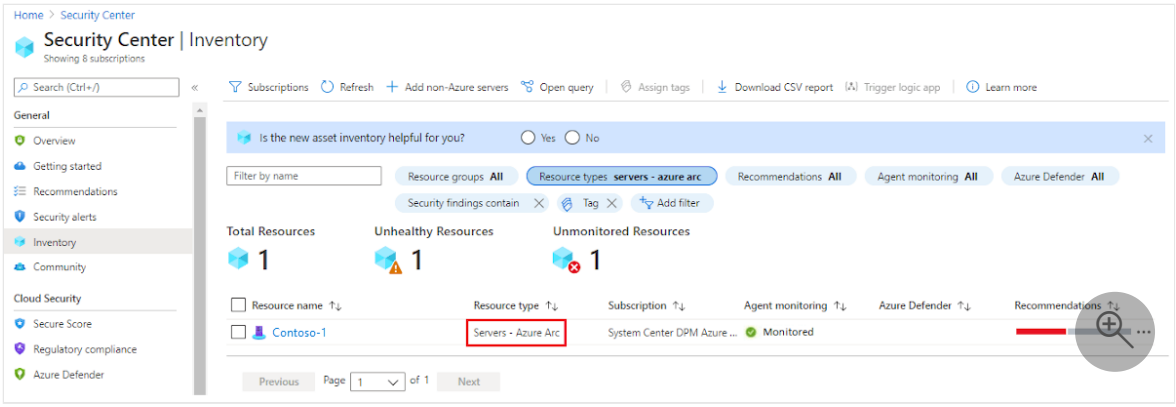
8. Specify your operating system and run the script on your Azure VMware Solution VM.

View recommendations and passed assessments

Recommendations and assessments provide you with the security health details of your resource.

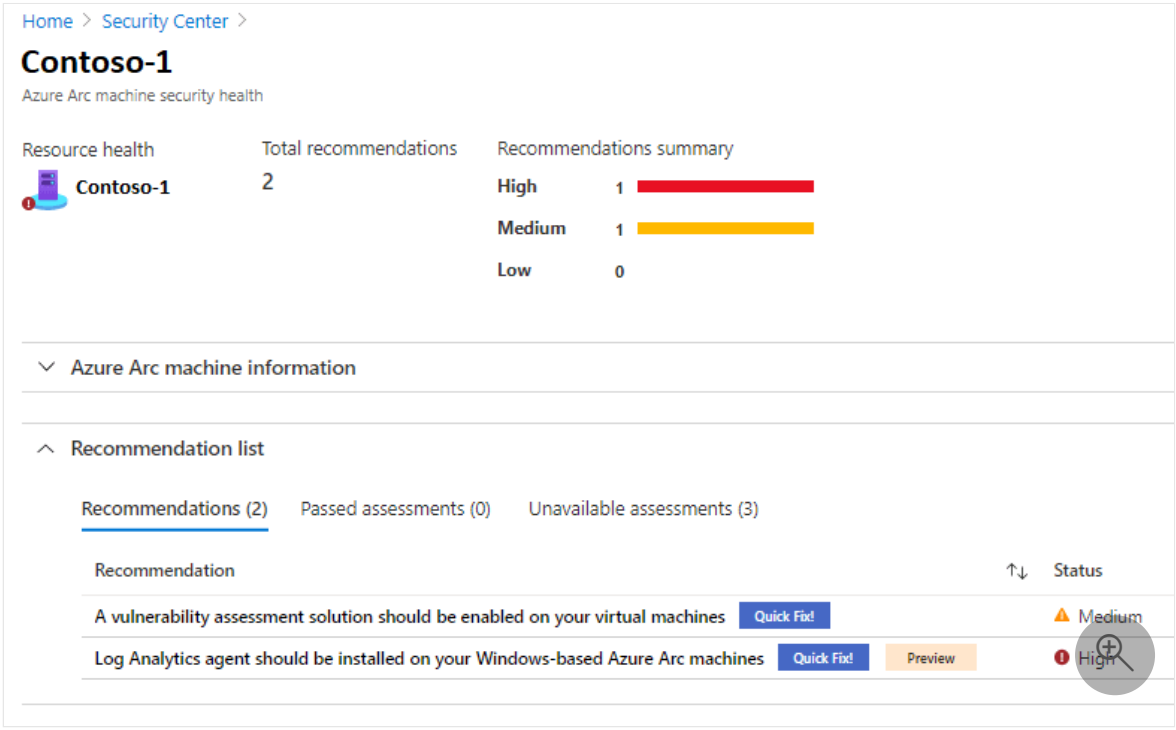
1. In Microsoft Defender for Cloud, select **Inventory** from the left pane.

2. For Resource type, select **Servers - Azure Arc**.



3. Select the name of your resource. A page opens showing the security health details of your resource.

4. Under **Recommendation list**, select the **Recommendations**, **Passed assessments**, and **Unavailable assessments** tabs to view these details.



Deploy a Microsoft Sentinel workspace

Microsoft Sentinel provides security analytics, alert detection, and automated threat response across an environment. It's a cloud-native, security information event management (SIEM) solution built on top of a Log Analytics workspace.

Since Microsoft Sentinel is built on top of a Log Analytics workspace, you only need to select the workspace you want to use.

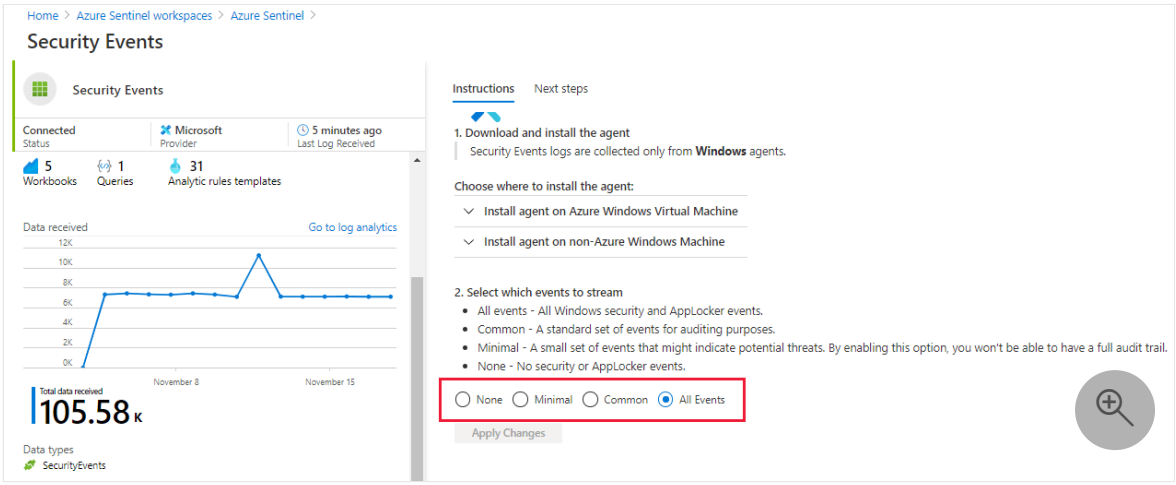
1. In the Azure portal, search for **Microsoft Sentinel**, and select it.

2. On the Microsoft Sentinel workspaces page, select **+Add**.

3. Select the Log Analytics workspace and select **Add**.

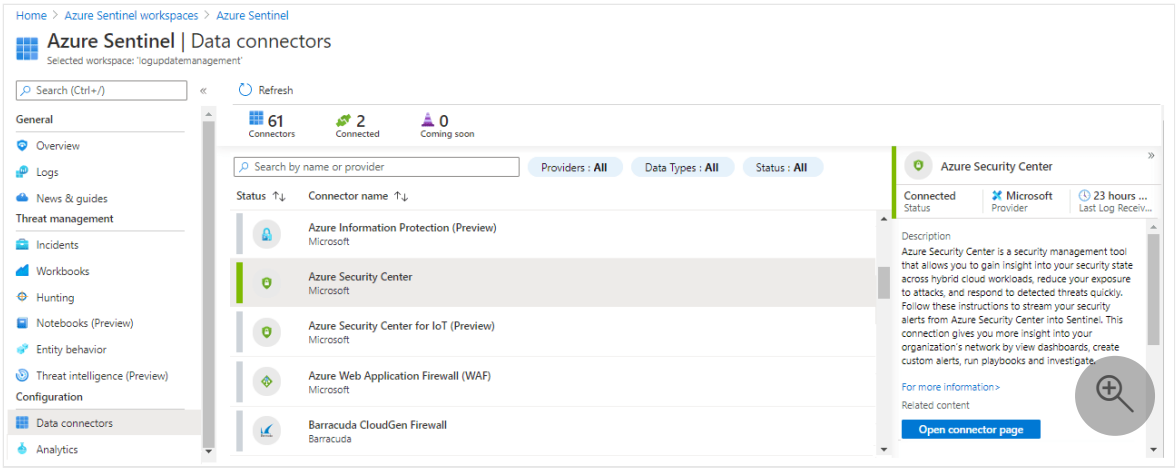
Enable data collector for security events

1. On the Microsoft Sentinel workspaces page, select the configured workspace.
2. Under Configuration, select **Data connectors**.
3. Under the Connector Name column, select **Security Events** from the list, then select **Open connector page**.
4. On the connector page, select the events you wish to stream, then select **Apply Changes**.



Connect Microsoft Sentinel with Microsoft Defender for Cloud

1. On the Microsoft Sentinel workspace page, select the configured workspace.
2. Under Configuration, select **Data connectors**.
3. Select **Microsoft Defender for Cloud** from the list, then select **Open connector page**.



4. Select **Connect** to connect the Microsoft Defender for Cloud with Microsoft Sentinel.

5. Enable **Create incident** to generate an incident for Microsoft Defender for Cloud.

Create rules to identify security threats

After connecting data sources to Microsoft Sentinel, you can create rules to generate alerts for detected threats. In the following example, we create a rule for attempts to sign in to Windows server with the wrong password.

1. On the Microsoft Sentinel overview page, under Configurations, select **Analytics**.

2. Under Configurations, select **Analytics**.

3. Select **+Create** and on the drop-down, select **Scheduled query rule**.

4. On the **General** tab, enter the required information and then select **Next: Set rule logic**.

    - Name
    - Description
    - Tactics
    - Severity
    - Status

5. On the **Set rule logic** tab, enter the required information, then select **Next**.

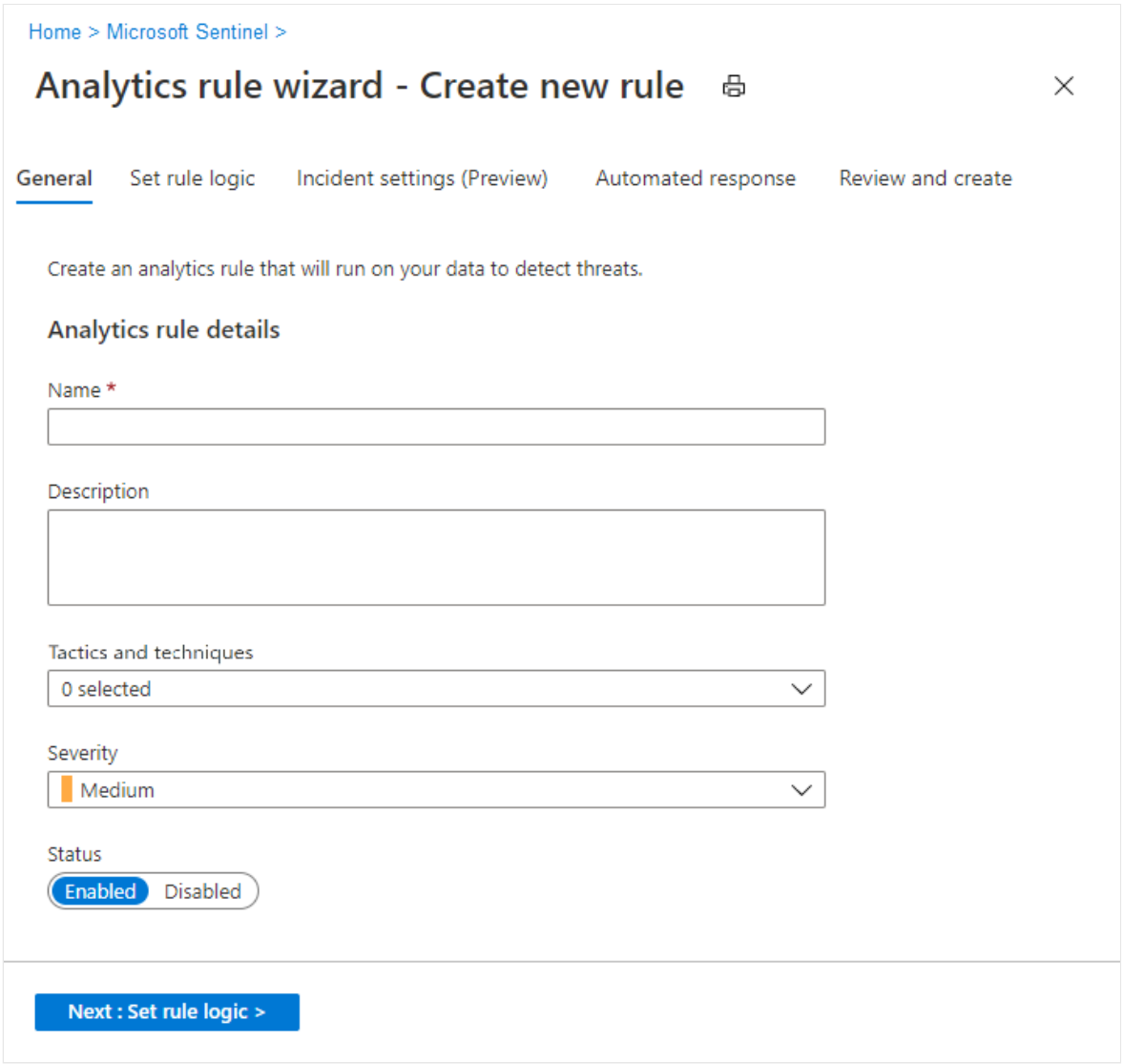
    - Rule query (here showing our example query)

```
SecurityEvent
|where Activity startswith '4625'
```

```
|summarize count () by IpAddress,Computer
|where count_ > 3
```

- Map entities
- Query scheduling
- Alert threshold
- Event grouping
- Suppression

6. On the **Incident settings** tab, enable **Create incidents from alerts triggered by this analytics rule** and select **Next: Automated response**.



7. Select **Next: Review**.

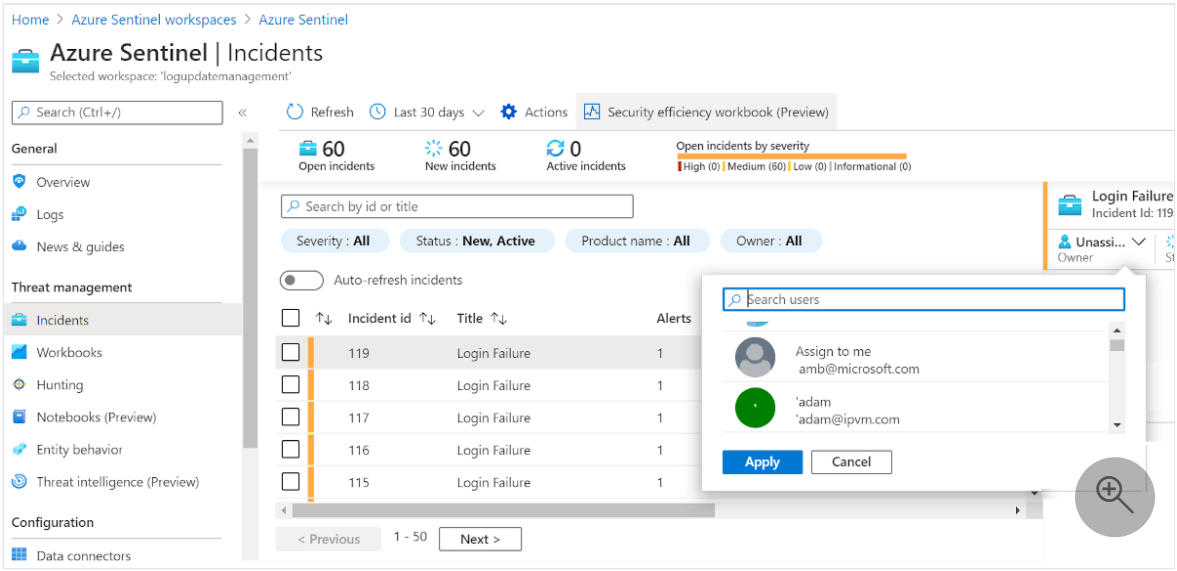
8. On the **Review and create** tab, review the information, and select **Create**.

> **Tip**
>
> After the third failed attempt to sign in to Windows server, the created rule triggers an incident for every unsuccessful attempt.

View alerts

You can view generated incidents with Microsoft Sentinel. You can also assign incidents and close them once they're resolved, all from within Microsoft Sentinel.

1. Go to the Microsoft Sentinel overview page.
2. Under Threat Management, select **Incidents**.
3. Select an incident and then assign it to a team for resolution.

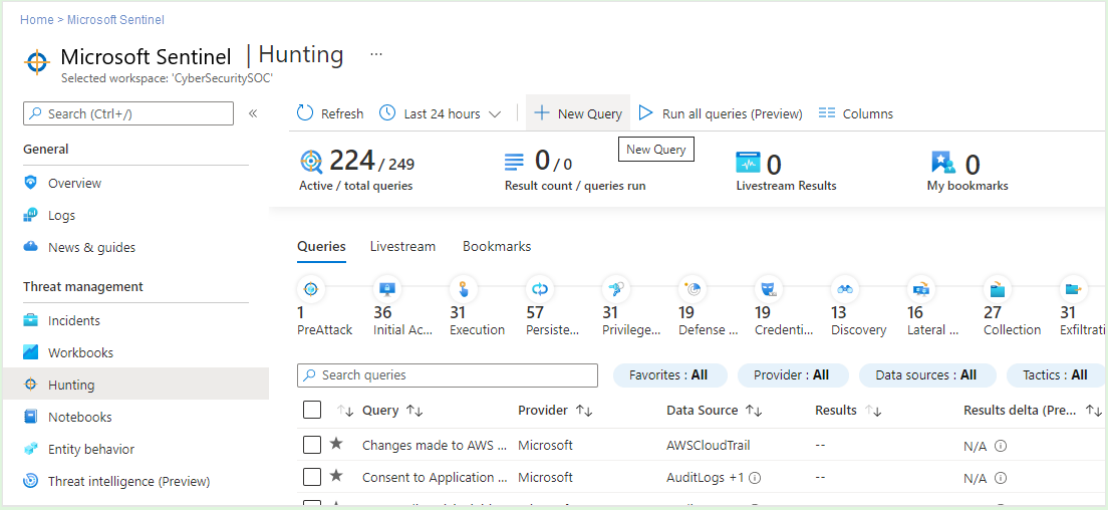


> **Tip**
>
> After resolving the issue, you can close it.

Hunt security threats with queries

You can create queries or use the available predefined query in Microsoft Sentinel to identify threats in your environment. The following steps run a predefined query.

1. On the Microsoft Sentinel overview page, under Threat management, select **Hunting**. A list of predefined queries is displayed.

> **Tip**
>
> You can also create a new query by selecting **New Query**.
>
> 
>

2. Select a query and then select **Run Query**.

3. Select **View Results** to check the results.

Next steps

Now that you covered how to protect your Azure VMware Solution VMs, you can learn more about:

- Using the workload protection dashboard
- Advanced multistage attack detection in Microsoft Sentinel
- Integrating Azure native services in Azure VMware Solution

Protect web apps on Azure VMware Solution with Azure Application Gateway

Article • 03/21/2024

Azure Application Gateway is a layer 7 web traffic load balancer that lets you manage traffic to your web applications, offered in both Azure VMware Solution v1.0 and v2.0. Both versions tested with web apps running on Azure VMware Solution.

The capabilities include:

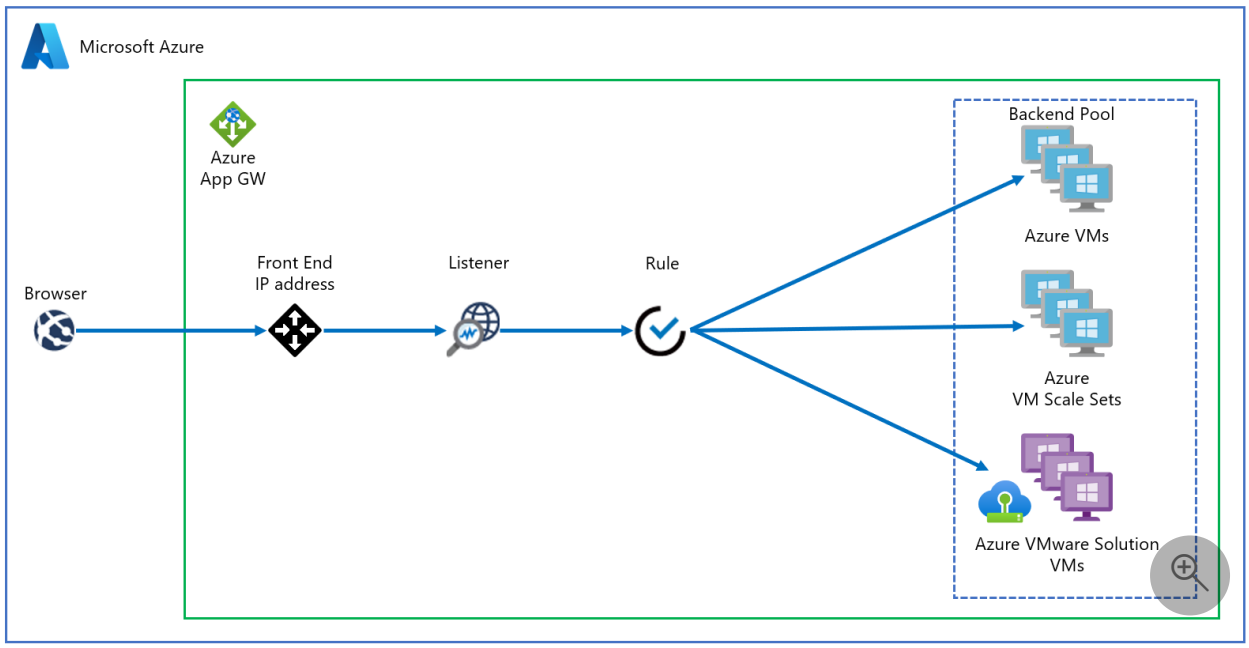
- Cookie-based session affinity
- URL-based routing
- Web Application Firewall (WAF)

For a complete list of features, see Azure Application Gateway features.

This article shows you how to use Application Gateway in front of a web server farm to protect a web app running on Azure VMware Solution.

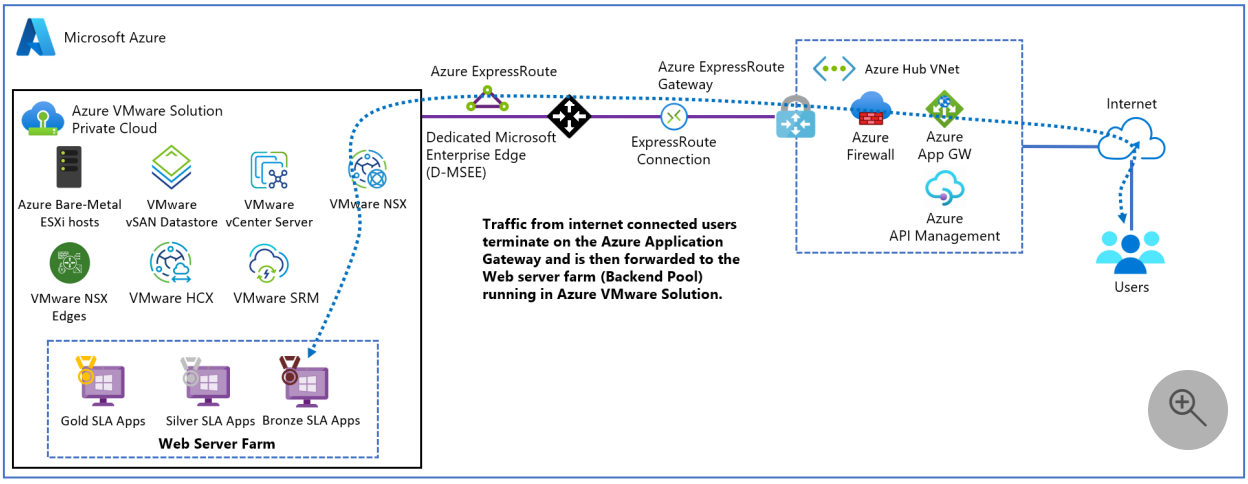
Topology

The diagram shows how Application Gateway is used to protect Azure IaaS virtual machines (VMs), Azure Virtual Machine Scale Sets, or on-premises servers. Application Gateway treats Azure VMware Solution VMs as on-premises servers.



> **Important**
>
> Azure Application Gateway is the preferred method to expose web apps running on Azure VMware Solution VMs.

The diagram shows the testing scenario used to validate the Application Gateway with Azure VMware Solution web applications.



The Application Gateway instance gets deployed on the hub in a dedicated subnet with an Azure public IP address. Activating the Azure DDoS Protection for the virtual network is recommended. The web server is hosted on an Azure VMware Solution private cloud behind NSX T0 and T1 Gateways. Additionally, Azure VMware Solution uses ExpressRoute Global Reach to enable communication with the hub and on-premises systems.

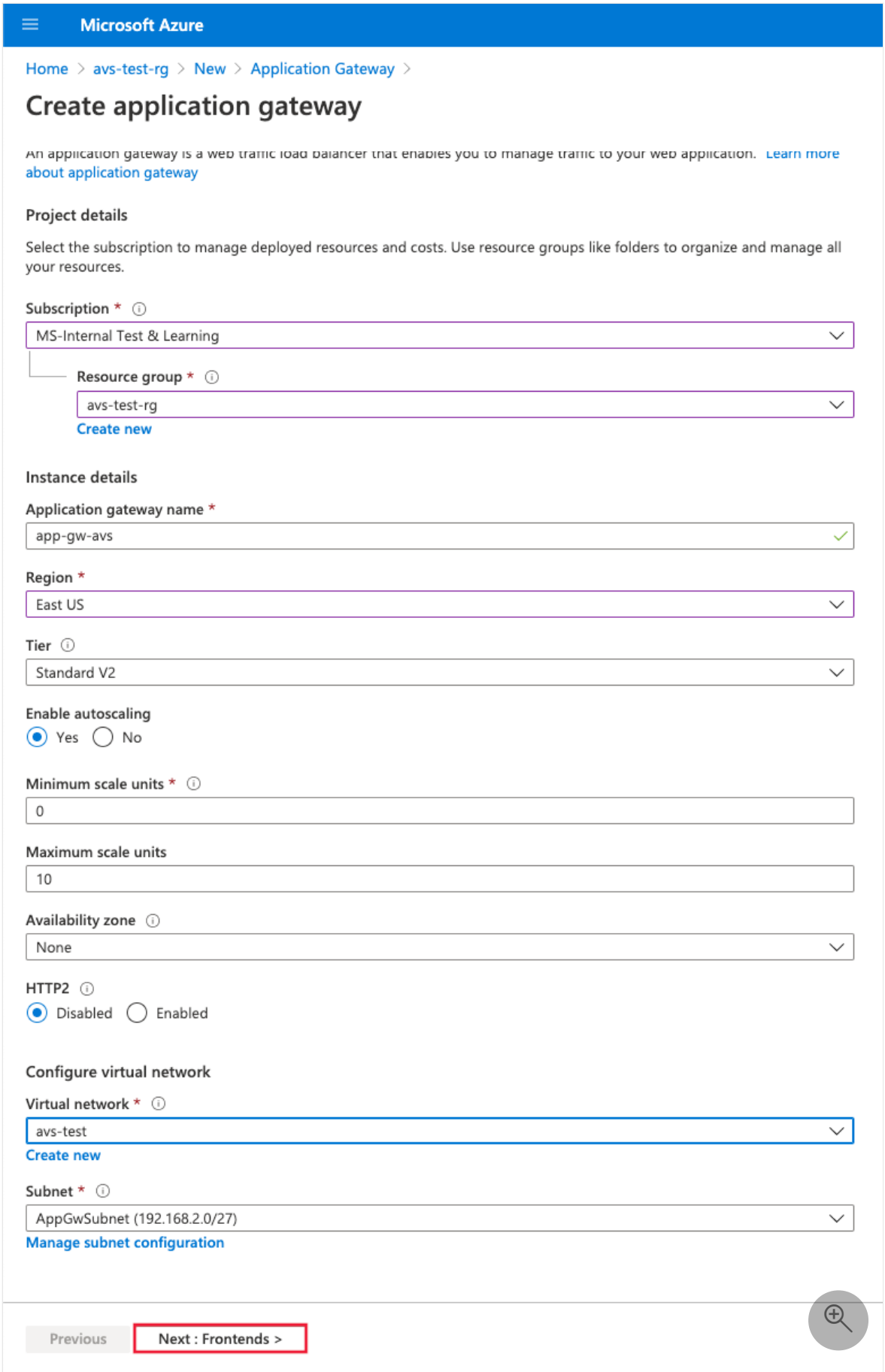
Prerequisites

- An Azure account with an active subscription.
- An Azure VMware Solution private cloud deployed and running.

Deployment and configuration

1. In the Azure portal, search for **Application Gateway** and select **Create application gateway**.

2. Provide the basic details as in the following figure; then select **Next: Frontends**>.



3. Choose the frontend IP address type. For public, choose an existing public IP address or create a new one. Select **Next: Backends>**.

> ⓘ Note

> Only standard and Web Application Firewall (WAF) SKUs are supported for private frontends.

4. Add a backend pool of the VMs that run on Azure VMware Solution infrastructure. Provide the details of web servers that run on the Azure VMware Solution private cloud and select **Add**. Then select **Next: Configuration>**.
5. On the **Configuration** tab, select **Add a routing rule**.
6. On the **Listener** tab, provide the details for the listener. If HTTPS is selected, you must provide a certificate, either from a PFX file or an existing Azure Key Vault certificate.
7. Select the **Backend targets** tab and select the backend pool previously created. For the **HTTP settings** field, select **Add new**.
8. Configure the parameters for the HTTP settings. Select **Add**.
9. If you want to configure path-based rules, select **Add multiple targets to create a path-based rule**.
10. Add a path-based rule and select **Add**. Repeat to add more path-based rules.
11. When you finish adding path-based rules, select **Add** again, then select **Next: Tags>**.
12. Add tags and then select **Next: Review + Create>**.
13. A validation runs on your Application Gateway. If it's successful, select **Create** to deploy.

Configuration examples

Now configure Application Gateway with Azure VMware Solution VMs as backend pools for the following use cases:

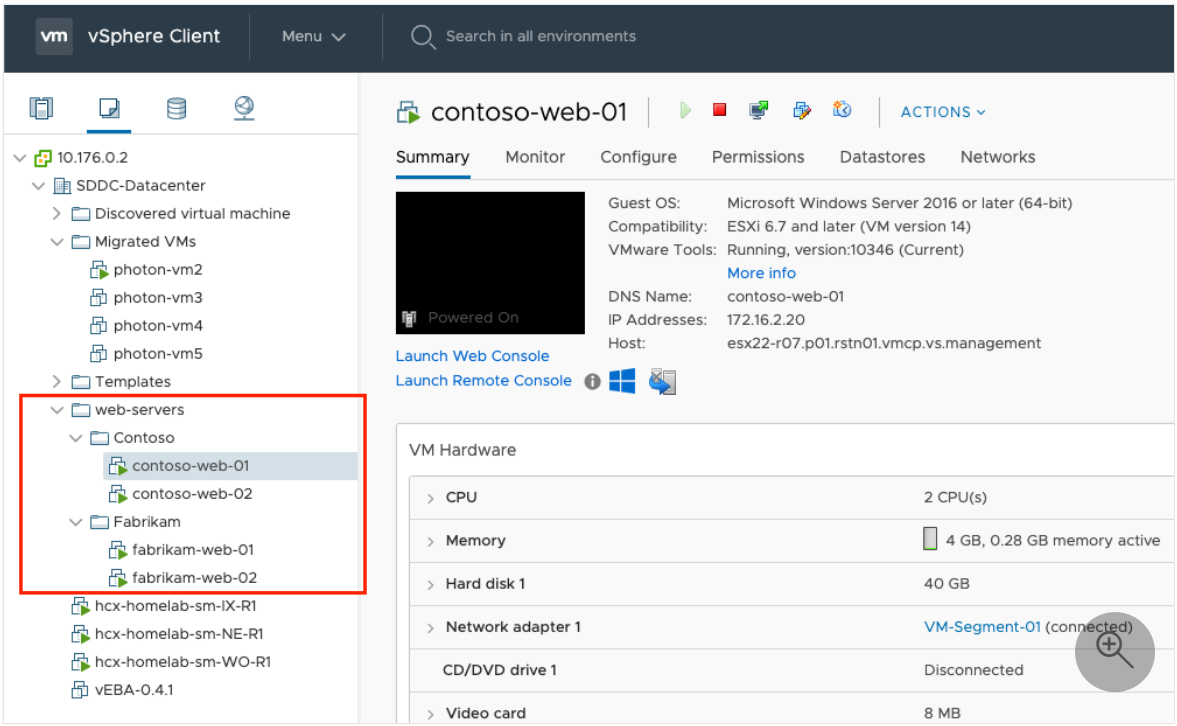
- Hosting multiple sites
- Routing by URL

Hosting multiple sites

This procedure shows you how to define backend address pools using VMs running on an Azure VMware Solution private cloud on an existing application gateway.

> **Note**
>
> This procedure assumes you have multiple domains, so we'll use examples of www.contoso.com and www.contoso2.com.

1. In your private cloud, create two different pools of VMs. One represents Contoso and the second contoso2.

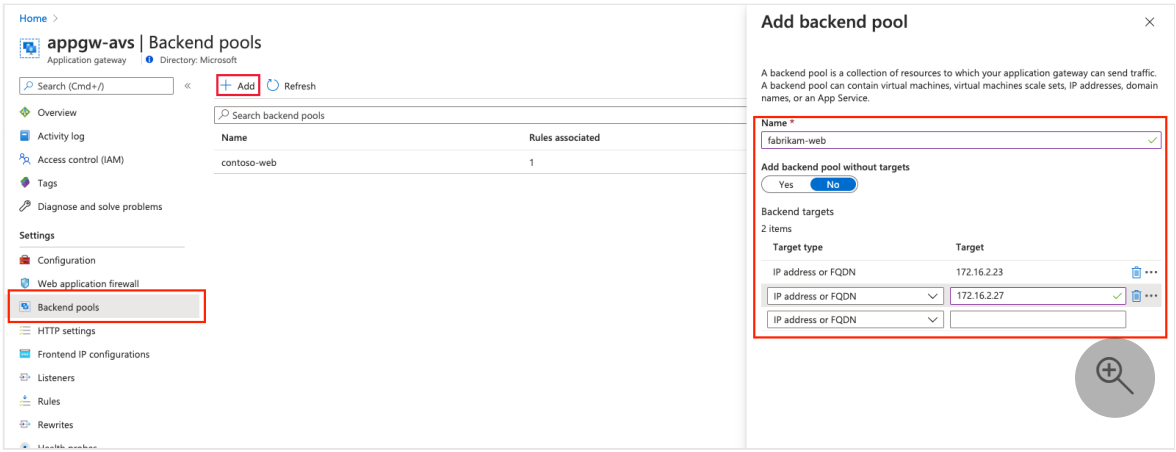


   We used Windows Server 2016 with the Internet Information Services (IIS) role installed. Once the VMs are installed, run the following PowerShell commands to configure IIS on each of the VMs.

   PowerShell

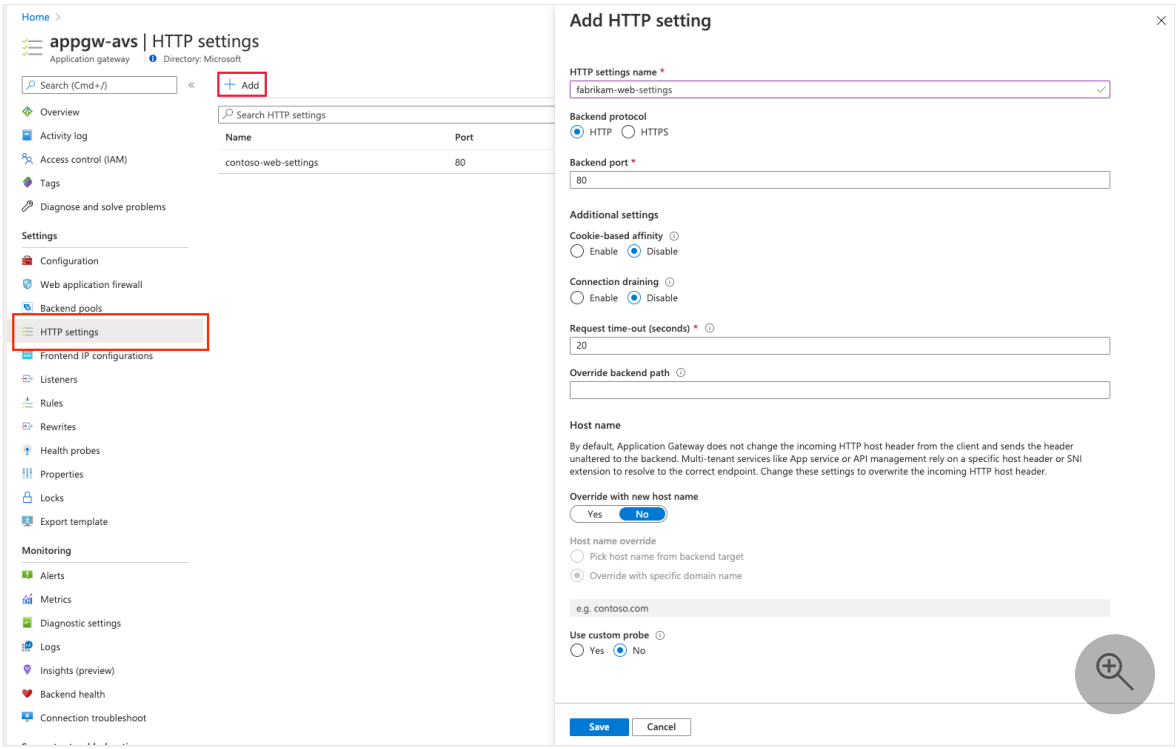
```
Install-WindowsFeature -Name Web-Server
Add-Content -Path C:\inetpub\wwwroot\Default.htm -Value
$($env:computername)
```

2. In an existing application gateway instance, select **Backend pools** from the left menu, select **Add**, and enter the new pools' details. Select **Add** in the right pane.



3. In the **Listeners** section, create a new listener for each website. Enter the details for each listener and select **Add**.

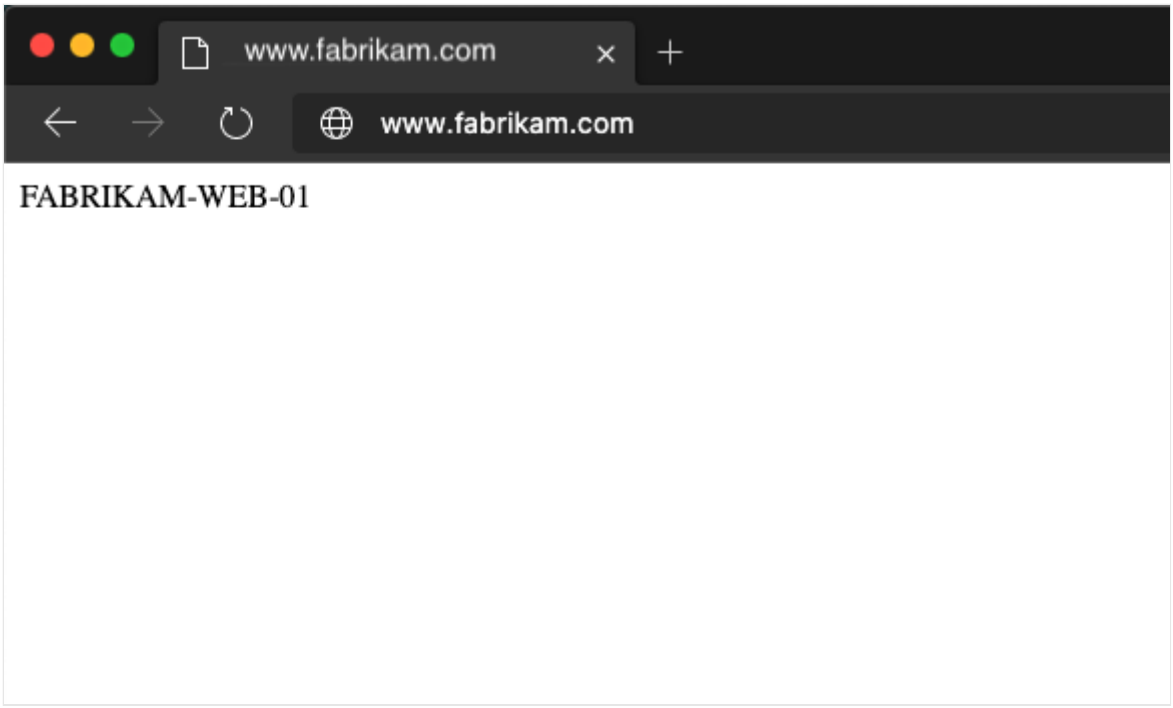
4. On the left, select **HTTP settings** and select **Add** in the left pane. Fill in the details to create a new HTTP setting and select **Save**.



5. Create the rules in the **Rules** section of the left menu. Associate each rule with the corresponding listener. Select **Add**.

6. Configure the corresponding backend pool and HTTP settings. Select **Add**.

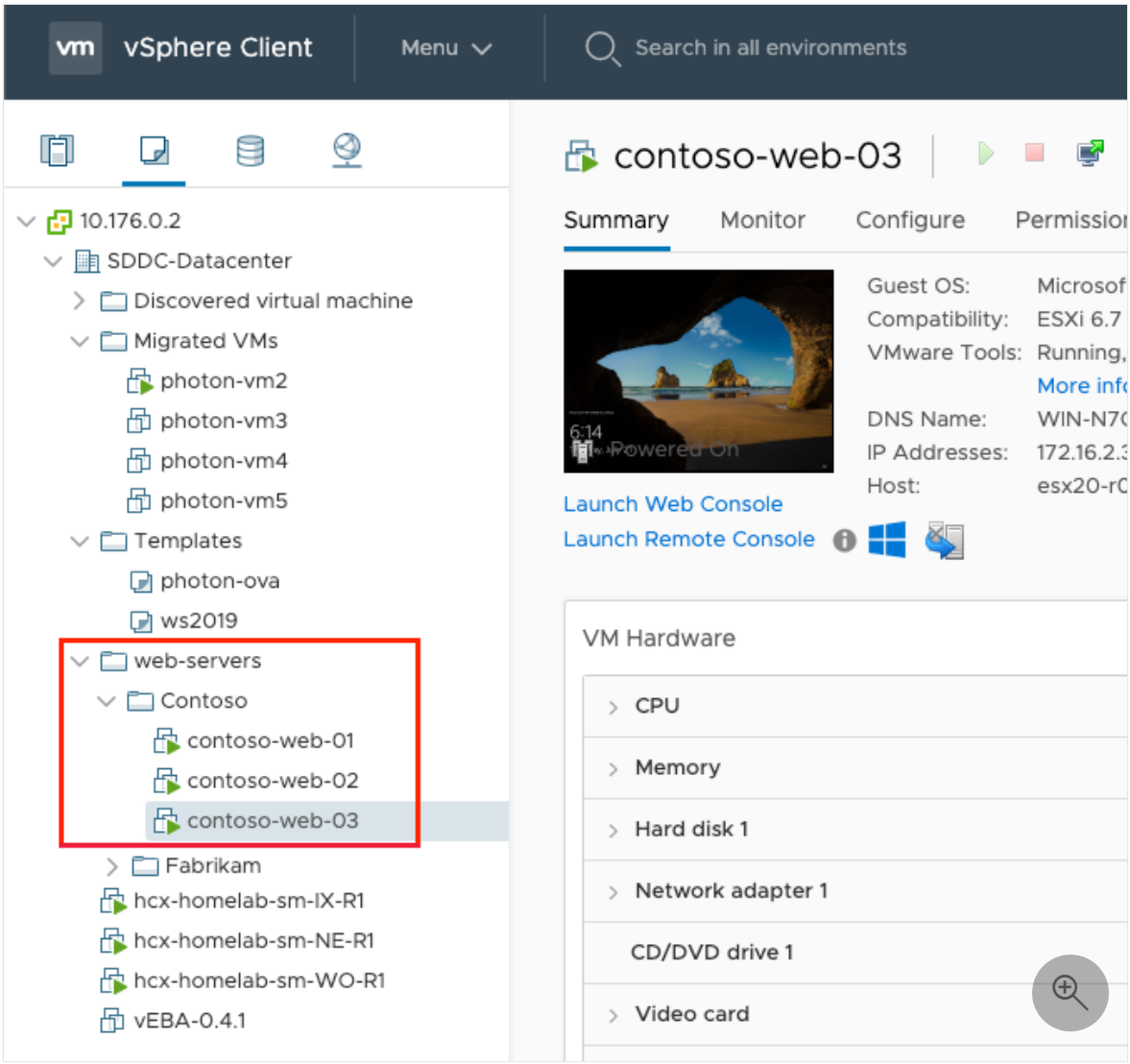
7. Test the connection. Open your preferred browser and navigate to the different websites hosted on your Azure VMware Solution environment.



Routing by URL

The following steps define backend address pools using VMs running on an Azure VMware Solution private cloud. The private cloud is on an existing application gateway. You then create routing rules that make sure web traffic arrives at the appropriate servers in the pools.

1. In your private cloud, create a virtual machine pool to represent the web farm.



Windows Server 2016 with IIS role installed was used to illustrate this tutorial. Once the VMs are installed, run the following PowerShell commands to configure IIS for each VM tutorial.

The first virtual machine, contoso-web-01, hosts the main website.

PowerShell

```
Install-WindowsFeature -Name Web-Server
Add-Content -Path C:\inetpub\wwwroot\Default.htm -Value
$($env:computername)
```

The second virtual machine, contoso-web-02, hosts the images site.

PowerShell

```
Install-WindowsFeature -Name Web-Server
New-Item -Path "C:\inetpub\wwwroot\" -Name "images" -ItemType
"directory"
```

```
Add-Content -Path C:\inetpub\wwwroot\images\test.htm -Value
$($env:computername)
```

The third virtual machine, contoso-web-03, hosts the video site.

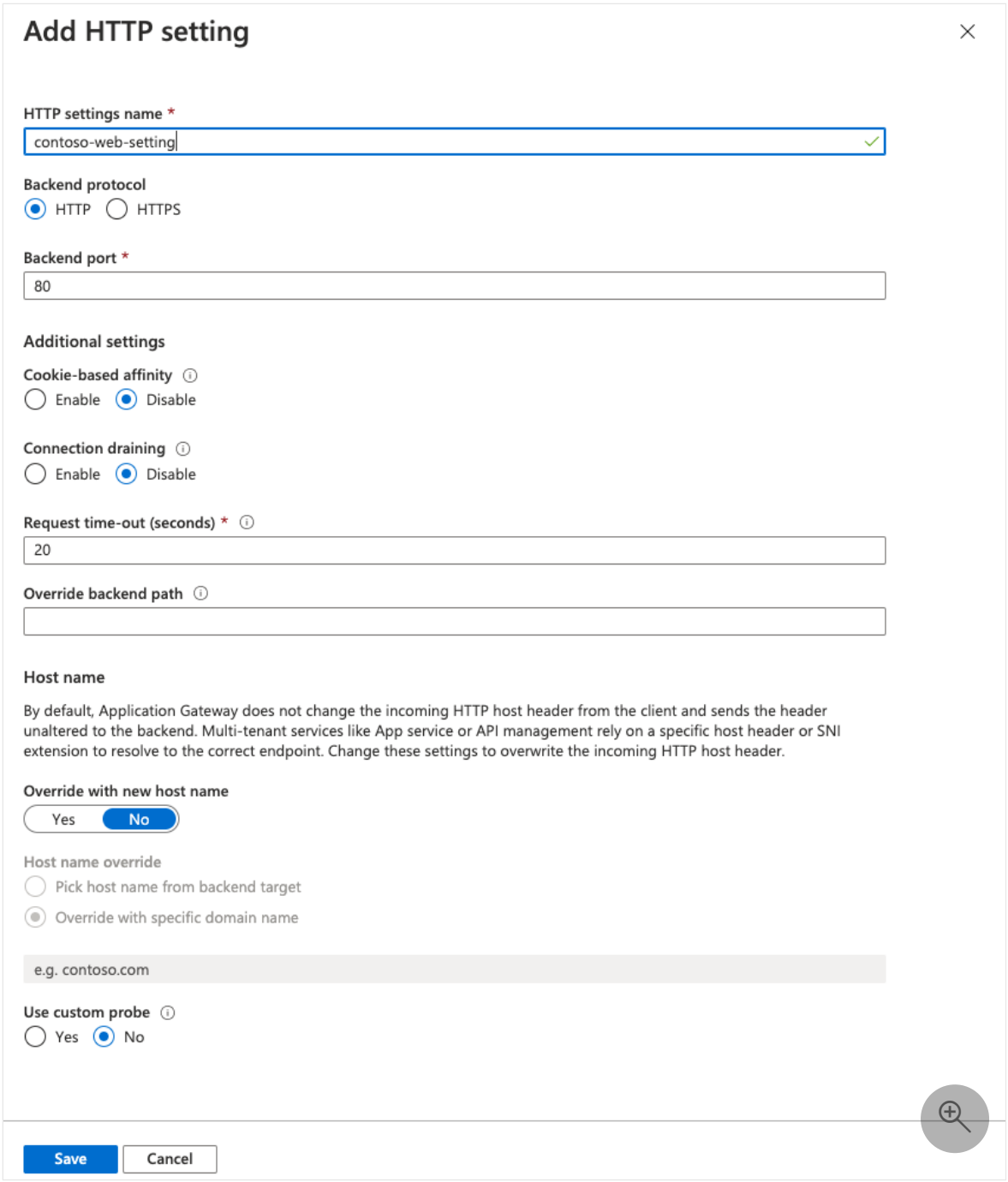
PowerShell

```
Install-WindowsFeature -Name Web-Server
New-Item -Path "C:\inetpub\wwwroot\" -Name "video" -ItemType
"directory"
Add-Content -Path C:\inetpub\wwwroot\video\test.htm -Value
$($env:computername)
```

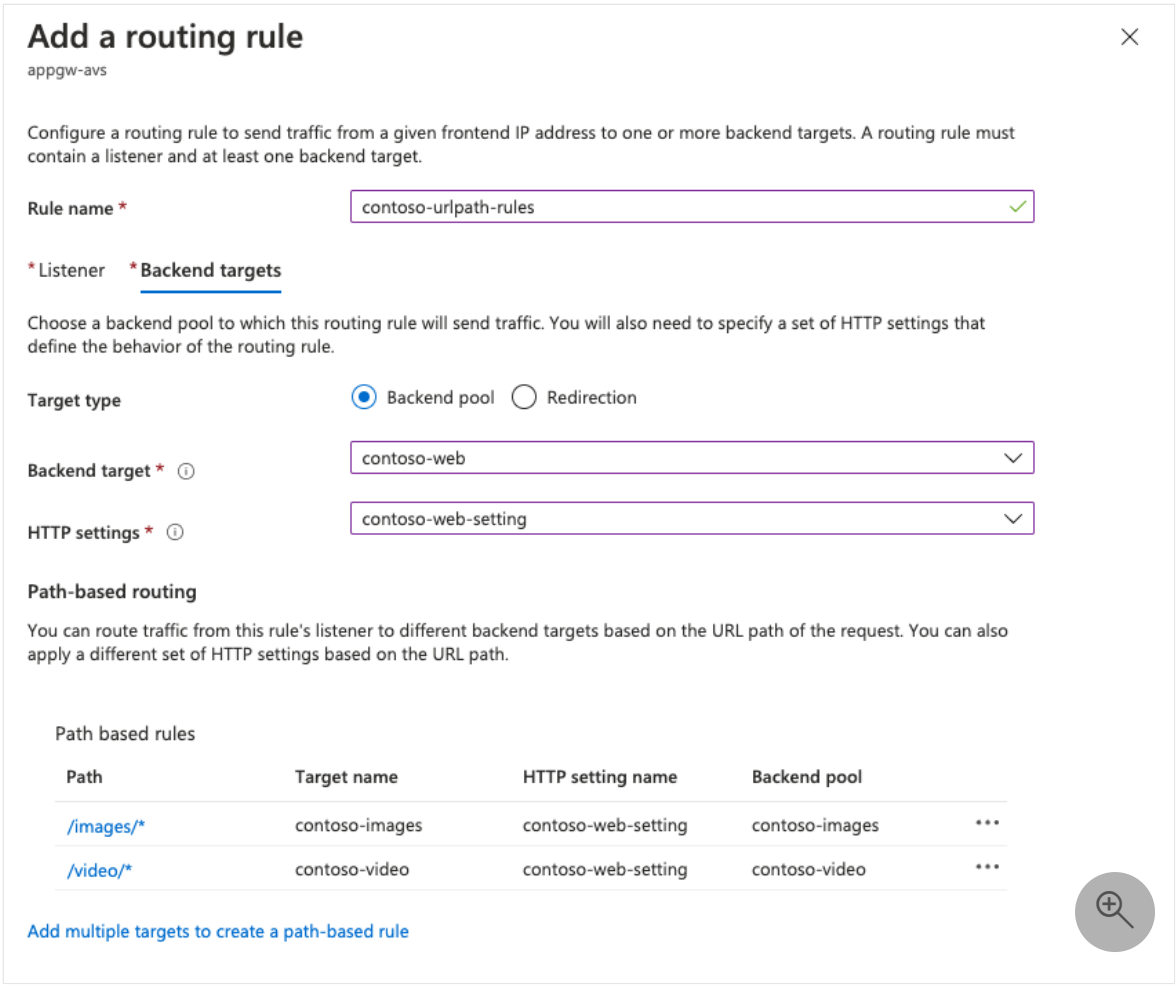
2. Add three new backend pools in an existing application gateway instance.
   a. Select **Backend pools** from the left menu.
   b. Select **Add** and enter the details of the first pool, **contoso-web**.
   c. Add one VM as the target.
   d. Select **Add**.
   e. Repeat this process for **contoso-images** and **contoso-video**, adding one unique VM as the target.

3. In the **Listeners** section, create a new listener of type Basic using port 8080.

4. On the left navigation, select **HTTP settings** and select **Add** in the left pane. Fill in the details to create a new HTTP setting and select **Save**.

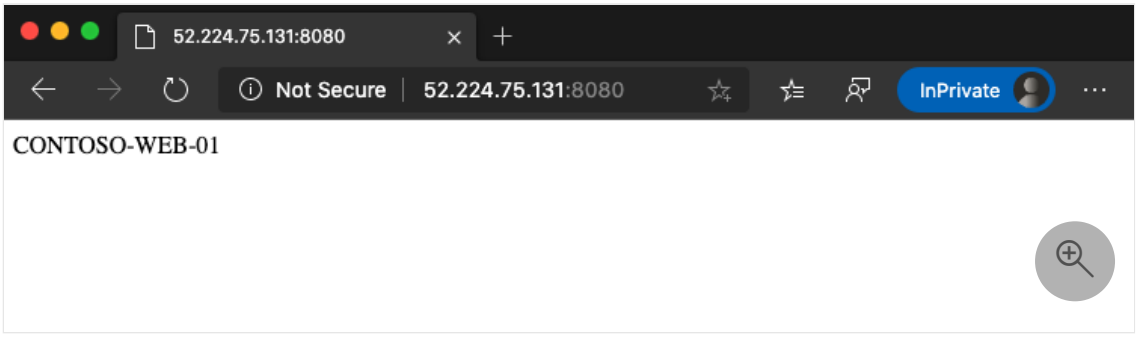


5. Create the rules in the **Rules** section of the left menu and associate each rule with the previously created listener. Then configure the main backend pool and HTTP settings, and then select **Add**.

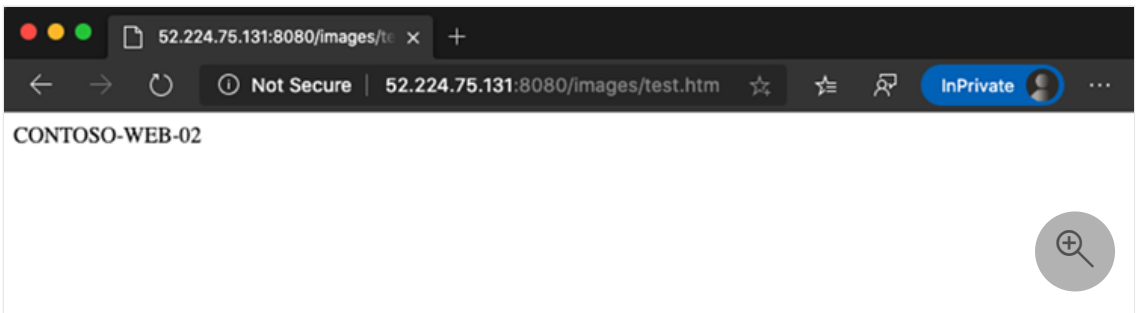


6. Test the configuration. Access the application gateway on the Azure portal and copy the public IP address in the **Overview** section.

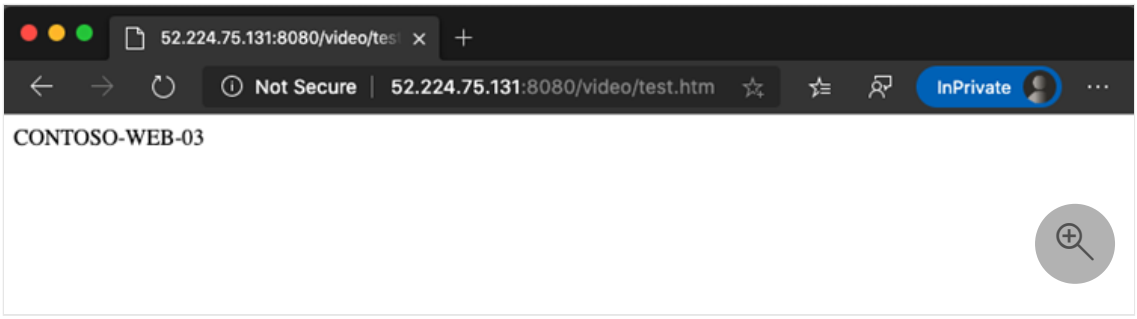
   a. Open a new browser window and enter the URL `http://<app-gw-ip-address>:8080`.



   b. Change the URL to `http://<app-gw-ip-address>:8080/images/test.htm`.



c. Change the URL again to `http://<app-gw-ip-address>:8080/video/test.htm`.



Next Steps

Now that you covered using Application Gateway to protect a web app running on Azure VMware Solution, learn more about:

- Configuring Azure Application Gateway for different scenarios.
- Deploying Traffic Manager to balance Azure VMware Solution workloads.
- Integrating Azure NetApp Files with Azure VMware Solution-based workloads.
- Protecting Azure resources in virtual networks.

Configure customer-managed key encryption at rest in Azure VMware Solution

Article • 04/12/2024

This article illustrates how to encrypt VMware vSAN key encryption keys (KEKs) with customer-managed keys (CMKs) managed by a customer-owned Azure Key Vault instance.

When CMK encryptions are enabled on your Azure VMware Solution private cloud, Azure VMware Solution uses the CMK from your key vault to encrypt the vSAN KEKs. Each ESXi host that participates in the vSAN cluster uses randomly generated disk encryption keys (DEKs) that ESXi uses to encrypt disk data at rest. vSAN encrypts all DEKs with a KEK provided by the Azure VMware Solution key management system. The Azure VMware Solution private cloud and the key vault don't need to be in the same subscription.

When you manage your own encryption keys, you can:

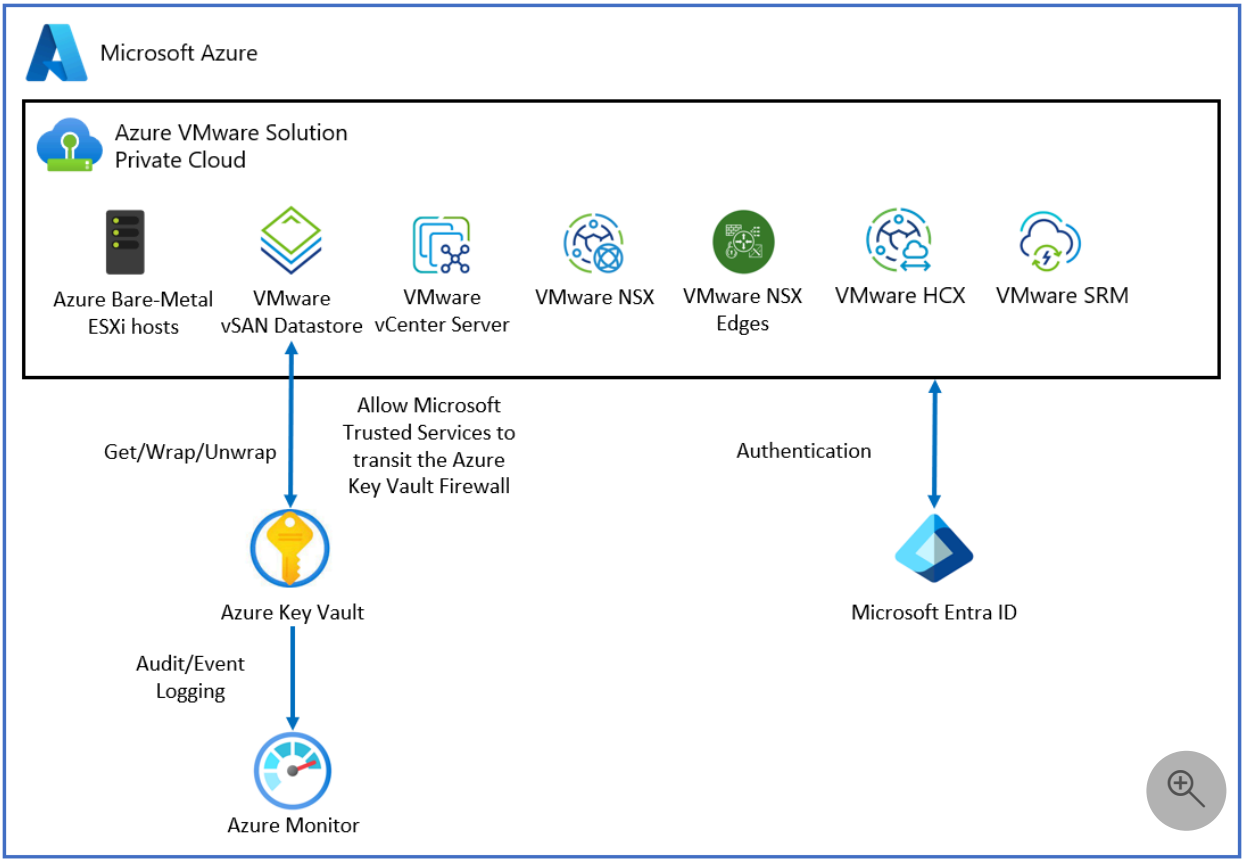
- Control Azure access to vSAN keys.
- Centrally manage the lifecycle of CMKs.
- Revoke Azure access to the KEK.

The CMKs feature supports the following key types and their key sizes:

- **RSA**: 2048, 3072, 4096
- **RSA-HSM**: 2048, 3072, 4096

Topology

The following diagram shows how Azure VMware Solution uses Microsoft Entra ID and a key vault to deliver the CMK.



Prerequisites

Before you begin to enable CMK functionality, ensure that the following requirements are met:

- You need a key vault to use CMK functionality. If you don't have a key vault, you can create one by using Quickstart: Create a key vault using the Azure portal.
- If you enabled restricted access to Key Vault, you need to allow Microsoft Trusted Services to bypass the Key Vault firewall. Go to Configure Azure Key Vault networking settings to learn more.

> **Note**
>
> After firewall rules are in effect, users can only perform Key Vault data plane operations when their requests originate from allowed VMs or IPv4 address ranges. This restriction also applies to accessing Key Vault from the Azure portal. It also affects the Key Vault Picker by Azure VMware Solution. Users might be able to see a list of key vaults, but not list keys, if firewall rules prevent their client machine or the user doesn't have list permission in Key Vault.

- Enable System Assigned identity on your Azure VMware Solution private cloud if you didn't enable it during software-defined datacenter (SDDC) provisioning.

  Portal

  To enable System Assigned identity:

  1. Sign in to the Azure portal.
  2. Go to **Azure VMware Solution** and locate your private cloud.
  3. On the leftmost pane, open **Manage** and select **Identity**.
  4. In **System Assigned**, select **Enable** > **Save**. **System Assigned identity** should now be enabled.

  After System Assigned identity is enabled, you see the tab for **Object ID**. Make a note of the Object ID for use later.

- Configure the key vault access policy to grant permissions to the managed identity. You use it to authorize access to the key vault.

  Portal

  1. Sign in to the Azure portal.
  2. Go to **Key vaults** and locate the key vault you want to use.
  3. On the leftmost pane, under **Settings**, select **Access policies**.
  4. In **Access policies**, select **Add Access Policy** and then:
     a. In the **Key Permissions** dropdown, choose **Select**, **Get**, **Wrap Key**, and **Unwrap Key**.
     b. Under **Select principal**, select **None selected**. A new **Principal** window with a search box opens.
     c. In the search box, paste the **Object ID** from the previous step. Or search for the private cloud name you want to use. Choose **Select** when you're finished.
     d. Select **ADD**.
     e. Verify that the new policy appears under the current policy's Application section.
     f. Select **Save** to commit changes.

Customer-managed key version lifecycle

You can change the CMK by creating a new version of the key. The creation of a new version doesn't interrupt the virtual machine (VM) workflow.

In Azure VMware Solution, CMK key version rotation depends on the key selection setting that you chose during CMK setup.

Key selection setting 1

A customer enables CMK encryption without supplying a specific key version for CMK. Azure VMware Solution selects the latest key version for CMK from the customer's key vault to encrypt the vSAN KEKs. Azure VMware Solution tracks the CMK for version rotation. When a new version of the CMK key in Key Vault is created, it gets captured by Azure VMware Solution automatically to encrypt vSAN KEKs.

> **Note**
>
> Azure VMware Solution can take up to 10 minutes to detect a new autorotated key version.

Key selection setting 2

A customer can enable CMK encryption for a specified CMK key version to supply the full key version URI under the **Enter Key from URI** option. When the customer's current key expires, they need to extend the CMK key expiration or disable CMK.

Enable CMK with system-assigned identity

System-assigned identity is restricted to one per resource and is tied to the lifecycle of the resource. You can grant permissions to the managed identity on Azure resource. The managed identity is authenticated with Microsoft Entra ID, so you don't have to store any credentials in code.

> **Important**
>
> Ensure that Key Vault is in the same region as the Azure VMware Solution private cloud.

Portal

Go to your Key Vault instance and provide access to the SDDC on Key Vault by using the principal ID captured on the **Enable MSI** tab.

1. From your Azure VMware Solution private cloud, under **Manage**, select **Encryption**. Then select **Customer-managed keys (CMKs)**.

2. CMK provides two options for **Key Selection** from Key Vault:

   Option 1:
   a. Under **Encryption key**, choose **select from Key Vault**.
   b. Select the encryption type. Then select the **Select Key Vault and key** option.
   c. Select the **Key Vault and key** from the dropdown. Then choose **Select**.

   Option 2:
   a. Under **Encryption key**, select **Enter key from URI**.
   b. Enter a specific Key URI in the **Key URI** box.

   > **Important**
   >
   > If you want to select a specific key version instead of the automatically selected latest version, you need to specify the Key URI with the key version. This choice affects the CMK key version lifecycle.

   The Key Vault Managed Hardware Security Module (HSM) option is only supported with the Key URI option.

3. Select **Save** to grant access to the resource.

Change from a customer-managed key to a Microsoft managed key

When a customer wants to change from a CMK to a Microsoft-managed key (MMK), the VM workload isn't interrupted. To make the change from a CMK to an MMK:

1. Under **Manage**, select **Encryption** from your Azure VMware Solution private cloud.
2. Select **Microsoft-managed keys (MMK)**.
3. Select **Save**.

Limitations

Key Vault must be configured as recoverable. You need to:

- Configure Key Vault with the **Soft Delete** option.
- Turn on **Purge Protection** to guard against force deletion of the secret vault, even after soft delete.

Updating CMK settings don't work if the key is expired or the Azure VMware Solution access key was revoked.

Troubleshooting and best practices

Here are troubleshooting tips for some common issues you might encounter and also best practices to follow.

Accidental deletion of a key

If you accidentally delete your key in the key vault, the private cloud can't perform some cluster modification operations. To avoid this scenario, we recommend that you keep soft deletes enabled in the key vault. This option ensures that if a key is deleted, it can be recovered within a 90-day period as part of the default soft-delete retention. If you're within the 90-day period, you can restore the key to resolve the issue.

Restore key vault permission

If you have a private cloud that has lost access to the CMK, check if Managed System Identity (MSI) requires permissions in the key vault. The error notification returned from Azure might not correctly indicate MSI requiring permissions in the key vault as the root cause. Remember, the required permissions are `get`, `wrapKey`, and `unwrapKey`. See step 4 in Prerequisites.

Fix an expired key

If you aren't using the autorotate function and the CMK expired in Key Vault, you can change the expiration date on the key.

Restore key vault access

Ensure that the MSI is used for providing private cloud access to the key vault.

Deletion of MSI

If you accidentally delete the MSI associated with a private cloud, you need to disable the CMK. Then follow the steps to enable the CMK from the start.

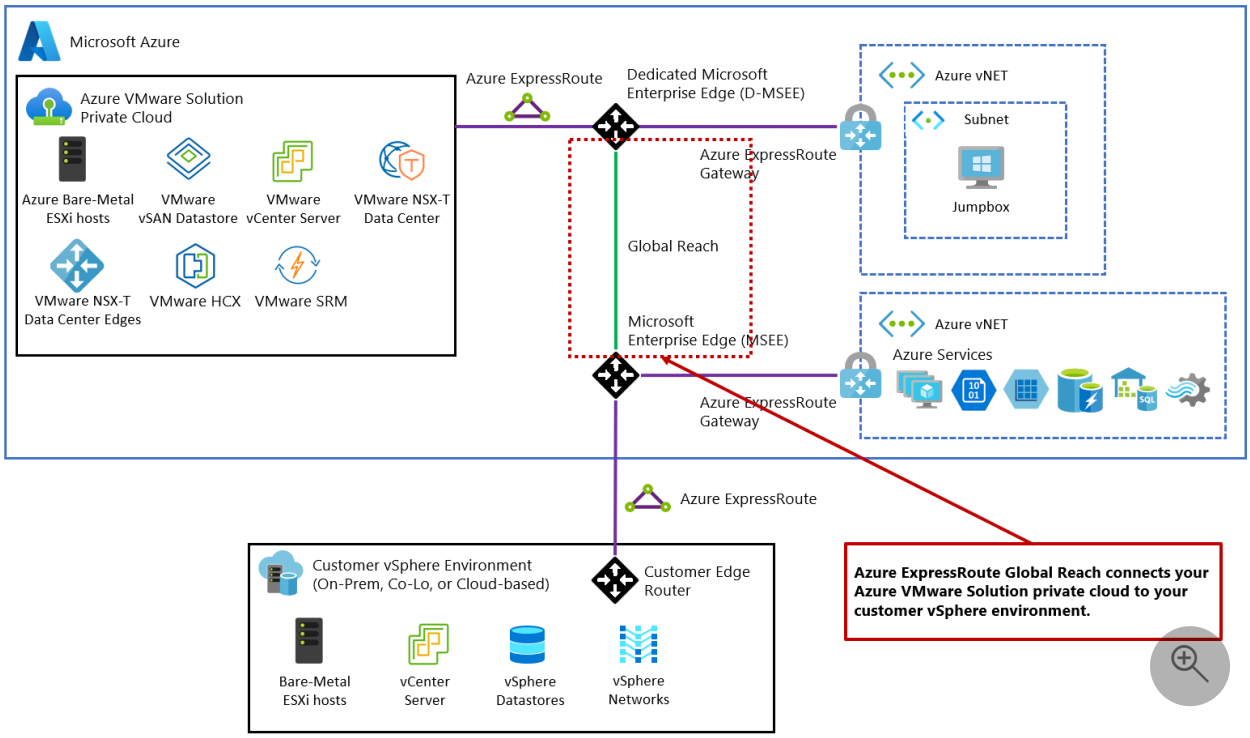
Next steps

- Learn about Azure Key Vault backup and restore.
- Learn about Azure Key Vault recovery.

Tutorial: Peer on-premises environments to Azure VMware Solution

Article • 12/20/2023

After you deploy your Azure VMware Solution private cloud, connect it to your on-premises environment. ExpressRoute Global Reach connects your on-premises environment to your Azure VMware Solution private cloud. The ExpressRoute Global Reach connection is established between the private cloud ExpressRoute circuit and an existing ExpressRoute connection to your on-premises environments.



> **Note**
>
> You can connect through VPN, but that's out of scope for this quick start guide.

In this article, you'll:

- ✓ Create an ExpressRoute auth key in the on-premises ExpressRoute circuit
- ✓ Peer the private cloud with your on-premises ExpressRoute circuit
- ✓ Verify on-premises network connectivity

Once you completed this section, follow the next steps provided at the end of this tutorial.

Prerequisites

- Review the documentation on how to enable connectivity in different Azure subscriptions.
- A separate, functioning ExpressRoute circuit for connecting on-premises environments to Azure, which is *circuit 1* for peering.
- Ensure that all gateways, including the ExpressRoute provider's service, support 4-byte Autonomous System Number (ASN). Azure VMware Solution uses 4-byte public ASNs for advertising routes.

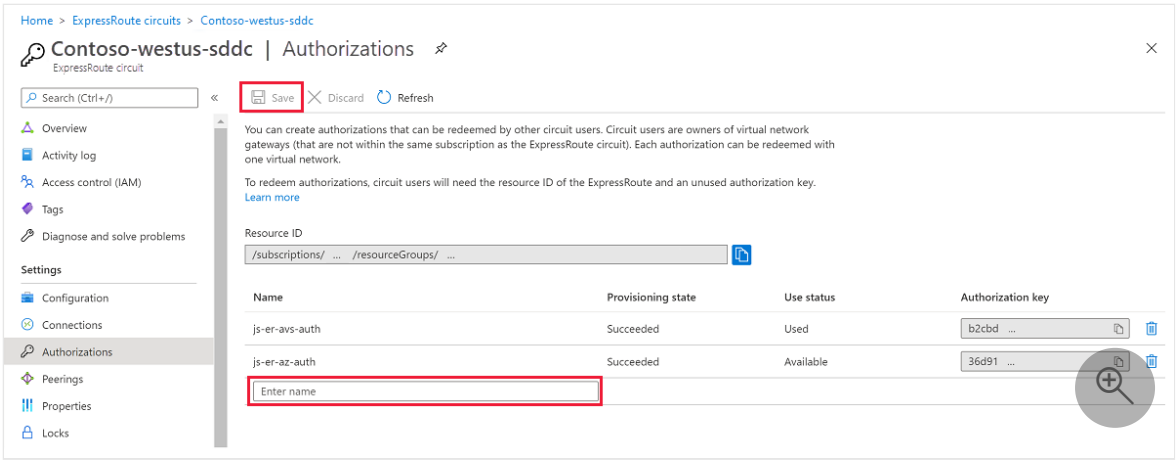
> **Note**
>
> If advertising a default route to Azure (0.0.0.0/0), ensure a more specific route containing your on-premises networks is advertised in addition to the default route to enable management access to Azure VMware Solution. A single 0.0.0.0/0 route will be discarded by Azure VMware Solution's management network to ensure successful operation of the service.

Create an ExpressRoute auth key in the on-premises ExpressRoute circuit

The circuit owner creates an authorization, which creates an authorization key to be used by a circuit user to connect their virtual network gateways to the ExpressRoute circuit. An authorization is valid for only one connection.

> **Note**
>
> Each connection requires a separate authorization.

1. From **ExpressRoute circuits** in the left navigation, under Settings, select **Authorizations**.
2. Enter the name for the authorization key and select **Save**.



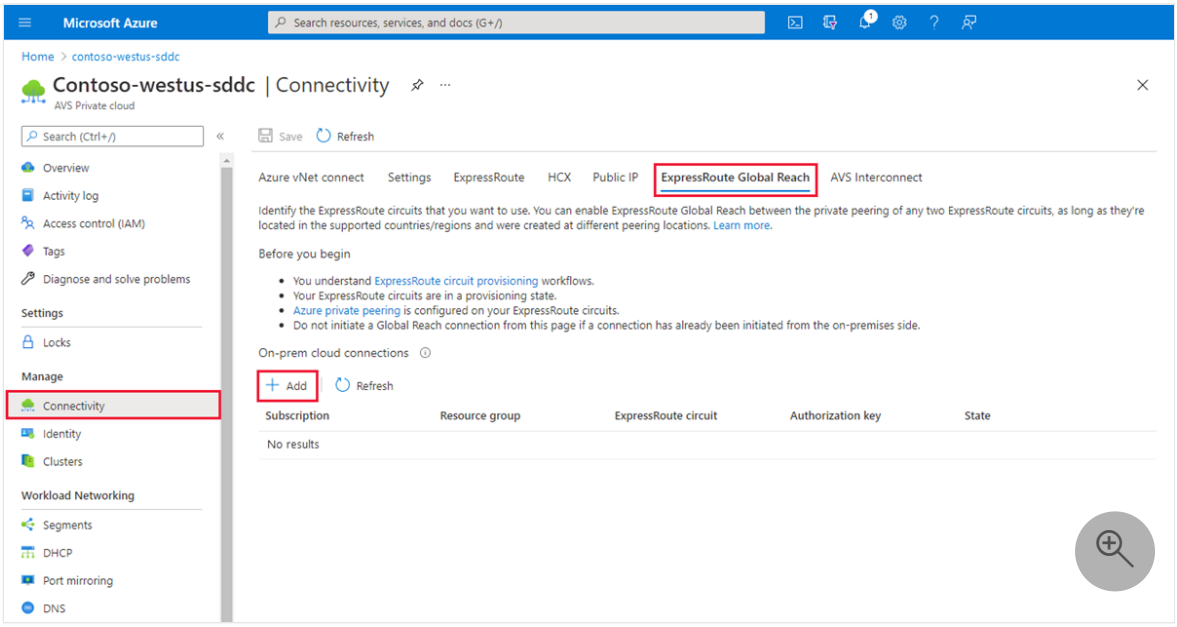
Once created, the new key appears in the list of authorization keys for the circuit.

3. Copy the authorization key and the ExpressRoute ID to use them in the next step to complete the peering.

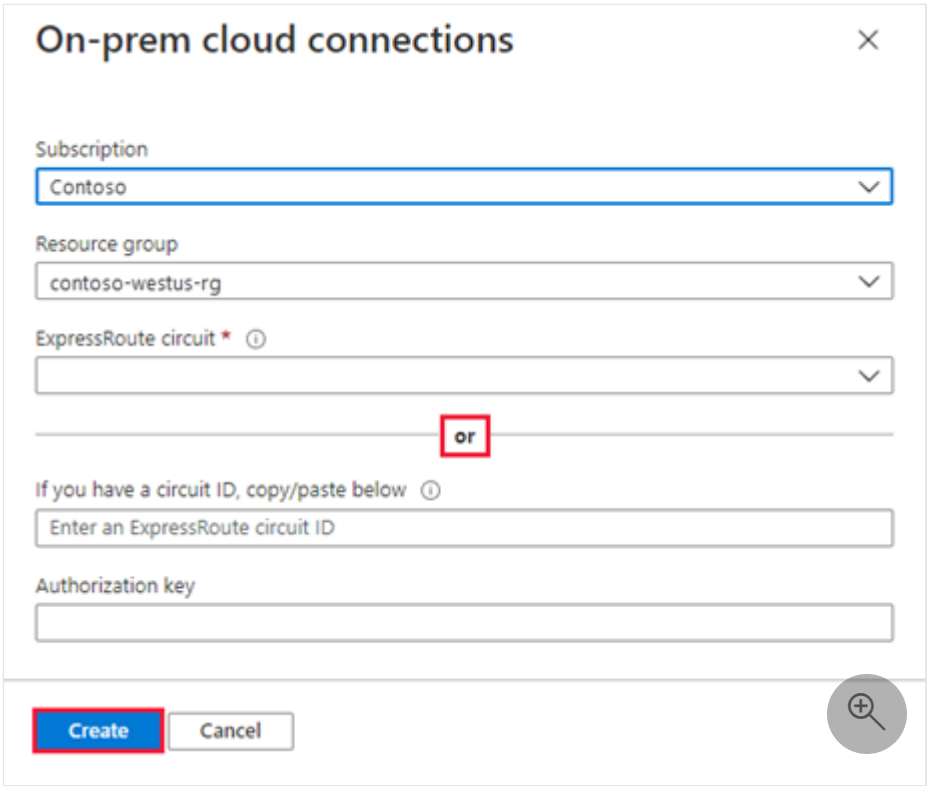
Peer private cloud to on-premises

Now that you created an authorization key for the private cloud ExpressRoute circuit, you can peer it with your on-premises ExpressRoute circuit. The peering is done from the on-premises ExpressRoute circuit in the **Azure portal**. You use the resource ID (ExpressRoute circuit ID) and authorization key of your private cloud ExpressRoute circuit to finish the peering.

1. From the private cloud, under Manage, select **Connectivity** > **ExpressRoute Global Reach** > **Add**.

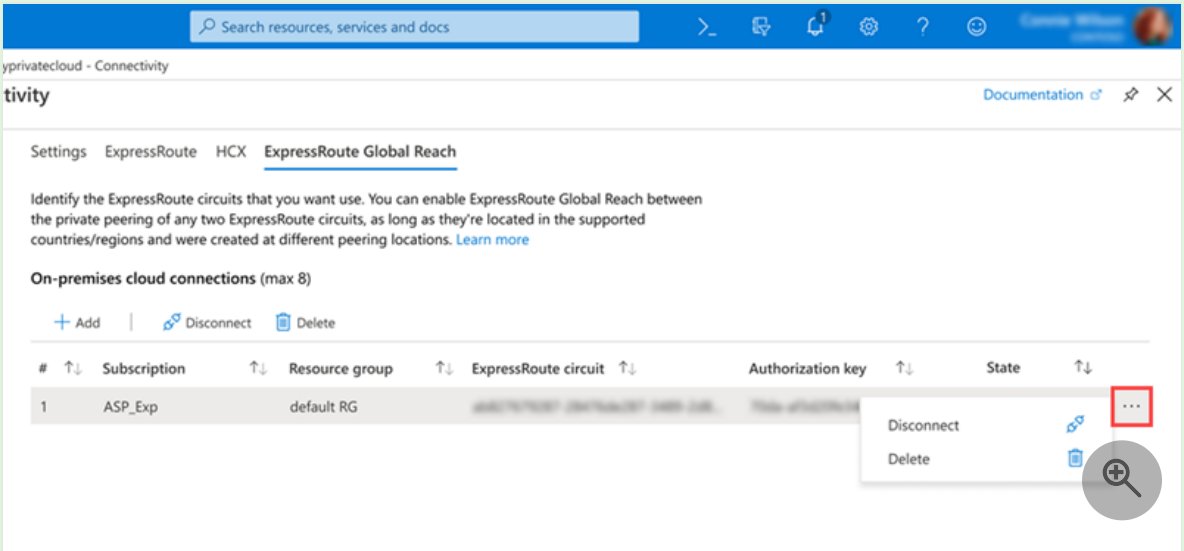


2. Enter the ExpressRoute ID and the authorization key created in the previous section.



3. Select **Create**. The new connection shows in the on-premises cloud connections list.

> **Tip**
>
> You can delete or disconnect a connection from the list by selecting **More**.



Verify on-premises network connectivity

In your **on-premises edge router**, you should now see where the ExpressRoute connects the NSX-T Data Center network segments and the Azure VMware Solution management segments.

> **Important**
>
> Everyone has a different environment, and some will need to allow these routes to propagate back into the on-premises network.

Next steps

Continue to the next tutorial to install VMware HCX add-on in your Azure VMware Solution private cloud.

Install VMware HCX

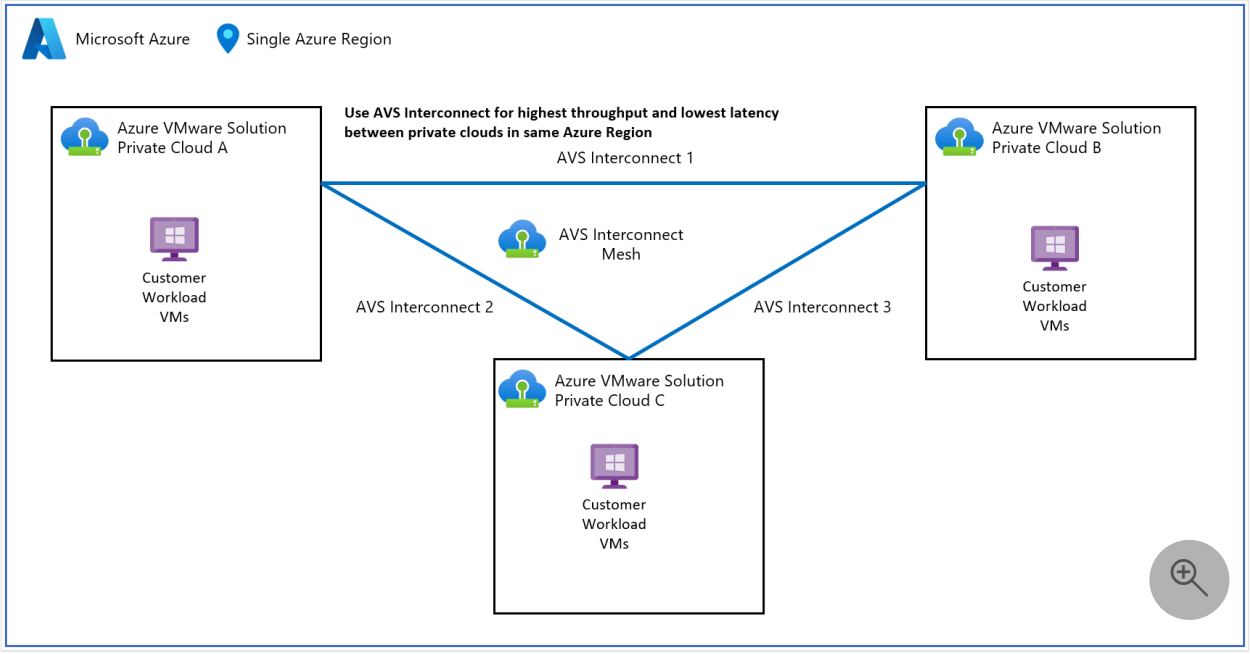
Connect multiple Azure VMware Solution private clouds in the same region

Article • 07/29/2024

The **AVS Interconnect** feature lets you create a network connection between two or more Azure VMware Solution private clouds located in the same region. It creates a routing link between the management and workload networks of the private clouds to enable network communication between the clouds.

You can connect a private cloud to multiple private clouds, and the connections are nontransitive. For example, if *private cloud A* is connected to *private cloud B*, and *private cloud B* is connected to *private cloud C*, private clouds A and B wouldn't communicate until they were directly connected.

You can only connect private clouds in the same region. To connect private clouds in different regions, use ExpressRoute Global Reach to connect them in the same way you connect your private cloud to your on-premises circuit.



> **Note**
>
> AVS Interconnect is based on Global Reach feature for both interconnection to same\different region. Please check the Global Reach availability for your AVS deployment

Supported regions

The Azure VMware Solution Interconnect feature is available in all regions.

Prerequisites

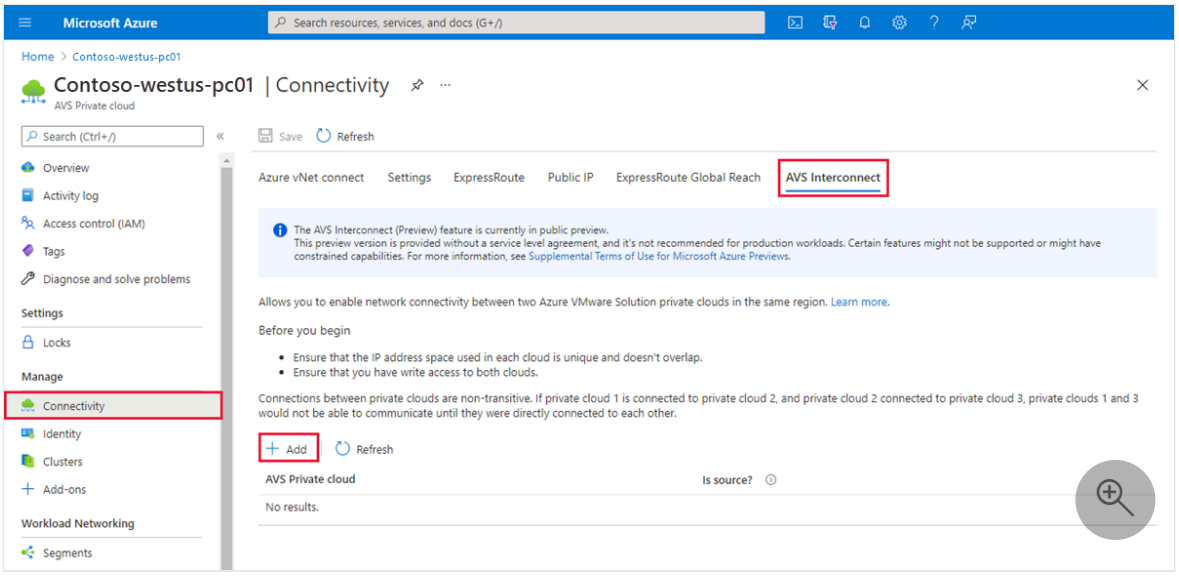
- Write access to each private cloud you're connecting
- Routed IP address space in each cloud is unique and doesn't overlap

> **Note**
>
> The **AVS Interconnect** feature doesn't check for overlapping IP space the way native Azure vNet peering does before creating the peering. Therefore, it's your responsibility to ensure that there isn't overlap between the private clouds.
>
> In Azure VMware Solution environments, it's possible to configure non-routed, overlapping IP deployments on NSX segments that aren't routed to Azure. These don't cause issues with the AVS Interconnect feature, as it only routes between the NSX-T Data Center T0 gateway on each private cloud.

Add connection between private clouds

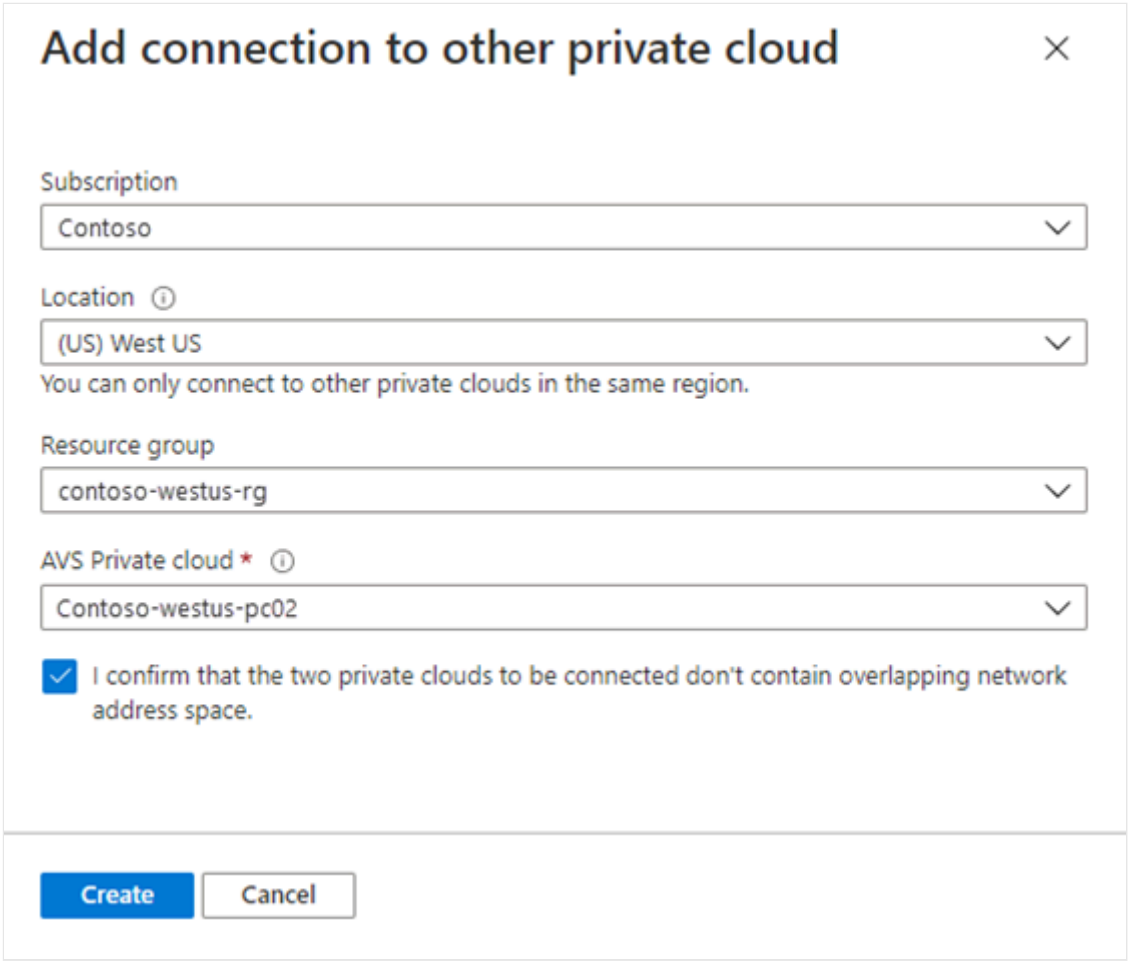
1. In your Azure VMware Solution private cloud, under **Manage**, select **Connectivity**.

2. Select the **AVS Interconnect** tab and then **Add**.



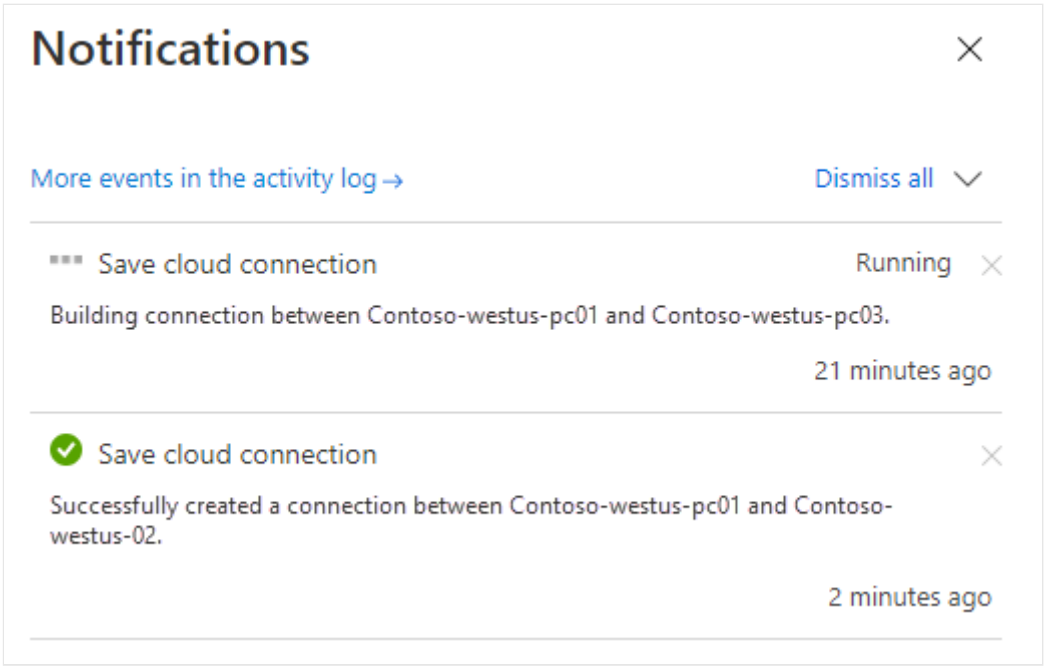
3. Select the information and Azure VMware Solution private cloud for the new connection.

> **Note**
>
> You can only connect to private clouds in the same region. To connect to private clouds that are in different regions, use ExpressRoute Global Reach to connect your private clouds in the same way you connect your private cloud to your on-premises circuit.

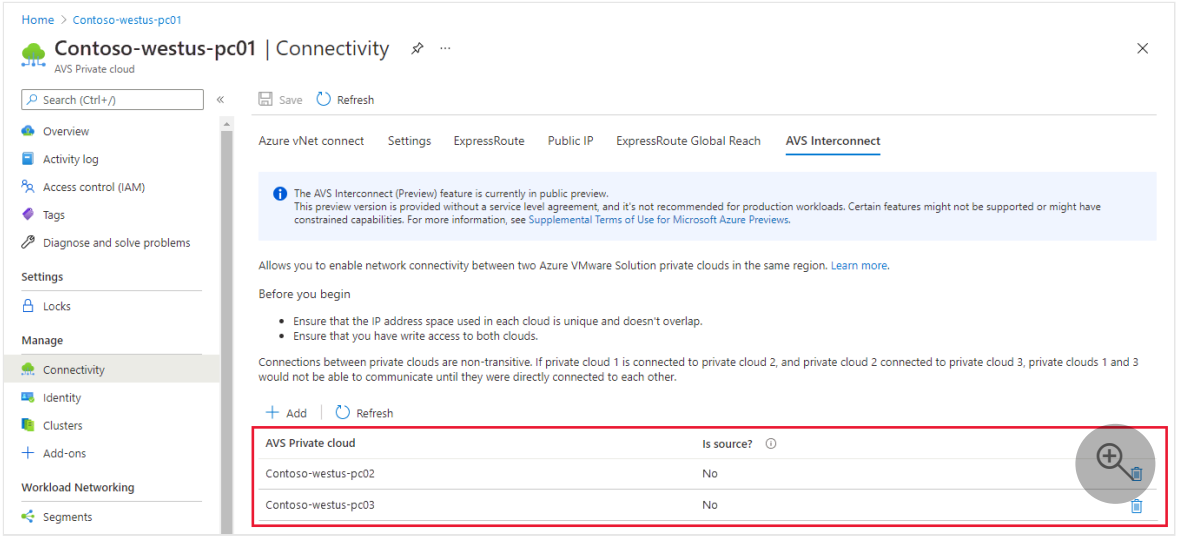


4. Select the **I confirm** checkbox acknowledging that there are no overlapping routed IP spaces in the two private clouds.

5. Select **Create**. You can check the status of the connection creation.



See all of your connections under **AVS Private Cloud**.



Remove connection between private clouds

1. In your Azure VMware Solution private cloud, under **Manage**, select **Connectivity**.
2. For the connection you want to remove, select **Delete** (trash can) and then **Yes**.

Next steps

Now that you connected multiple private clouds in the same region, learn more about:

- Move Azure VMware Solution resources to another region
- Move Azure VMware Solution subscription to another subscription

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Configure DHCP for Azure VMware Solution

Article • 06/12/2024

Applications and workloads running in a private cloud environment require name resolution and DHCP services for lookup and IP address assignments. A proper DHCP and DNS infrastructure are required to provide these services. You can configure a virtual machine to provide these services in your private cloud environment.

Use the DHCP service built-in to NSX-T Data Center or use a local DHCP server in the private cloud instead of routing broadcast DHCP traffic over the WAN back to on-premises.

> **Important**
>
> If you advertise a default route to the Azure VMware Solution, then you must allow the DNS forwarder to reach the configured DNS servers and they must support public name resolution.

In this article, learn how to use NSX Manager to configure DHCP for Azure VMware Solution in one of the following ways:

- Use the Azure portal to create a DHCP server or relay
- Use NSX to host your DHCP server
- Use a third-party external DHCP server

> **Tip**
>
> If you want to configure DHCP using a simplified view of NSX operations, see **Configure DHCP for Azure VMware Solution**.

> **Important**
>
> For clouds created on or after July 1, 2021, the simplified view of NSX operations must be used to configure DHCP on the default Tier-1 Gateway in your environment.

DHCP does not work for virtual machines (VMs) on the VMware HCX L2 stretch network when the DHCP server is in the on-premises datacenter. NSX, by default, blocks all DHCP requests from traversing the L2 stretch. For the solution, see the Configure DHCP on L2 stretched VMware HCX networks procedure.

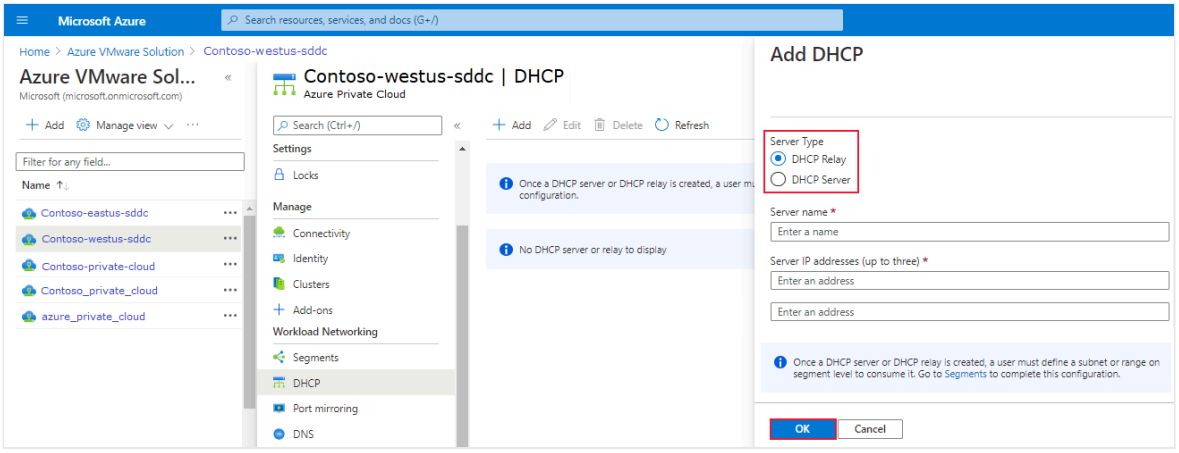
Use the Azure portal to create a DHCP server or relay

You can create a DHCP server or relay directly from Azure VMware Solution in the Azure portal. The DHCP server or relay connects to the Tier-1 gateway created when you deployed Azure VMware Solution. All the segments where you gave DHCP ranges are part of this DHCP. After you create a DHCP server or DHCP relay, you must define a subnet or range on segment level to consume it.

1. In your Azure VMware Solution private cloud, under **Workload Networking**, select **DHCP** > **Add**.

2. Select either **DHCP Server** or **DHCP Relay** and then provide a name for the server or relay and three IP addresses.

   > **Note**
   >
   > For DHCP relay, you only require one IP address for a successful configuration.



3. Complete the DHCP configuration by providing DHCP ranges on the logical segments and then select **OK**.

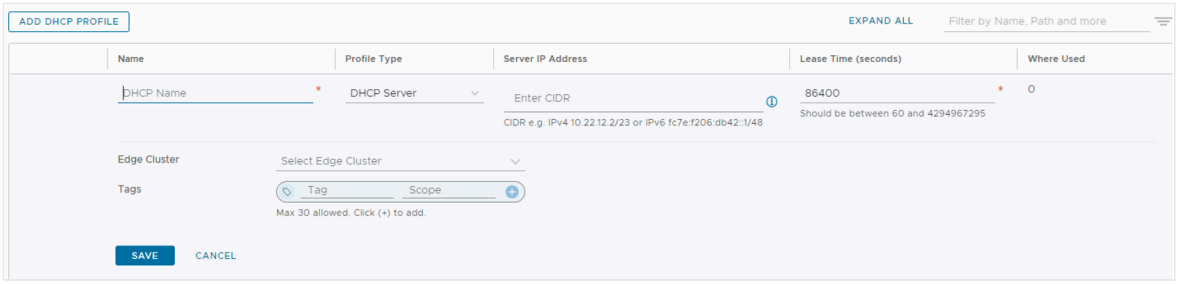
Use NSX to host your DHCP server

If you want to use NSX to host your DHCP server, create a DHCP server and a relay service. Next add a network segment and specify the DHCP IP address range.

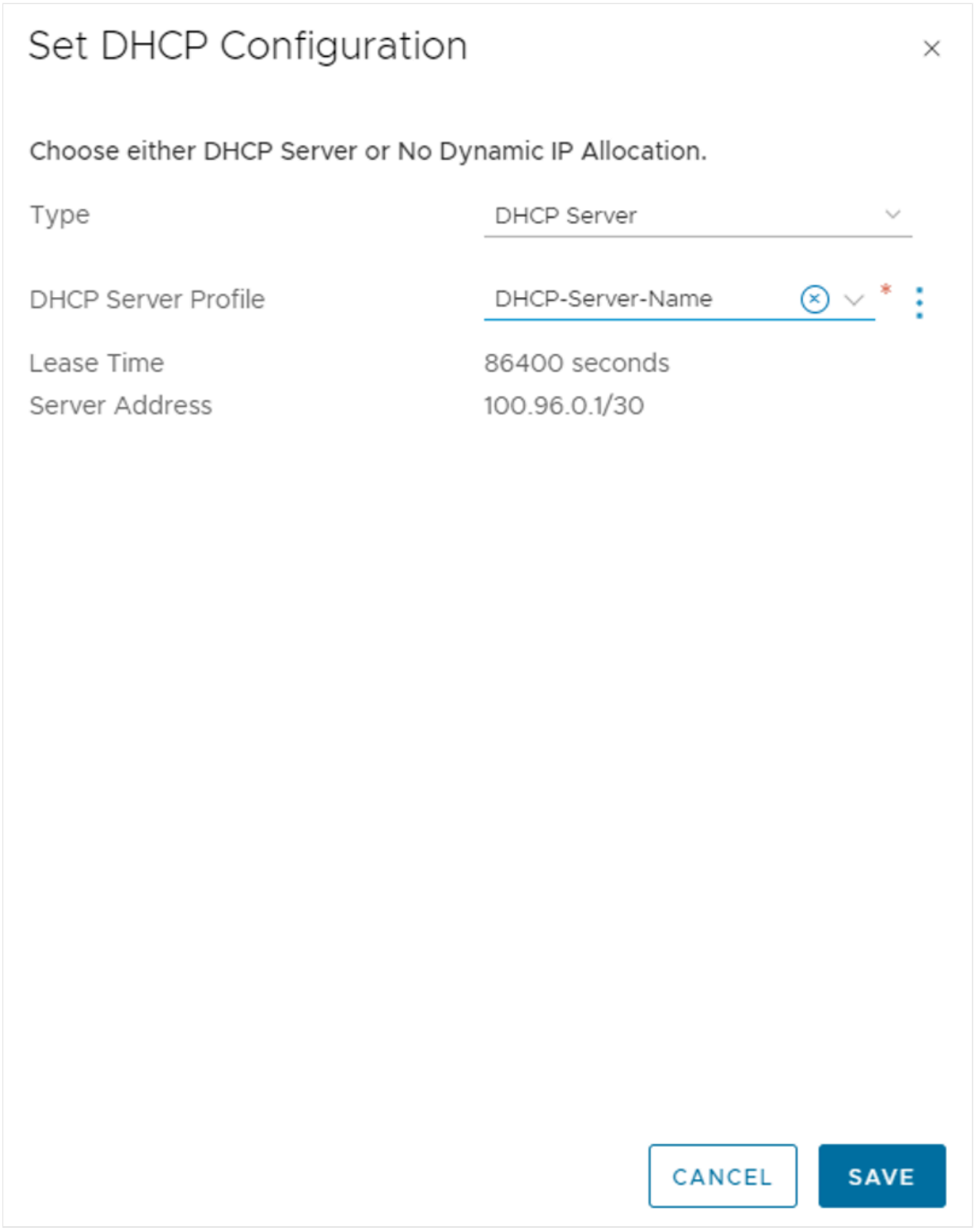
Create a DHCP server

1. In NSX Manager, select **Networking** > **DHCP**, then select **Add DHCP Profile**.
2. Select **Add DHCP Profile**, enter a name, and select **Save**.

> **Note**
>
> An IP address isn't required so if none is entered, NSX Manager sets one.

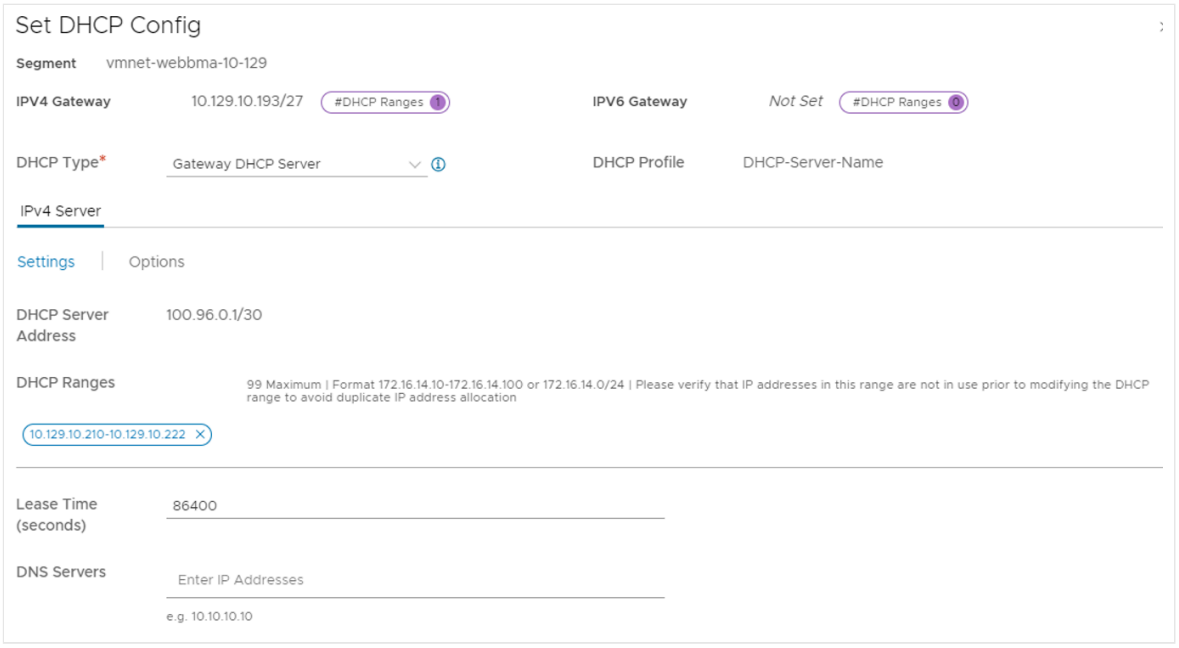


3. Under **Networking** > **Tier-1 Gateways**, select the gateway where the segments are connected that DHCP is required. Edit the Tier-1 Gateway by clicking on the three ellipses and choose **Edit**.
4. Select **Set DHCP Configuration**, select **DHCP Server** and then select the DHCP Server Profile created earlier. Select **Save**, then **Close Editing**.



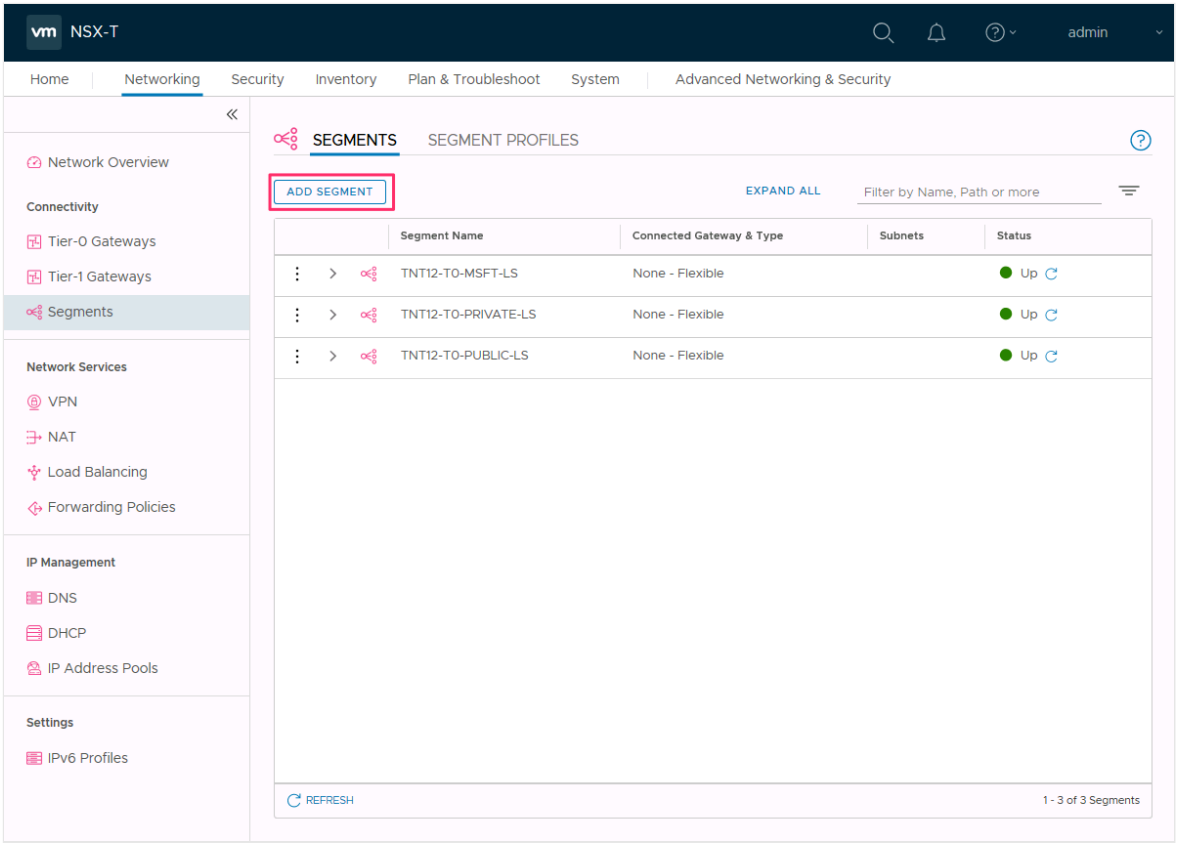
5. Navigate to **Networking** > **Segments** and find the segment where DHCP is required. Select on **Edit** then **Set DHCP Config**.

6. Select **Gateway DHCP Server** for DHCP Type, add a DHCP range, and select **Apply**.

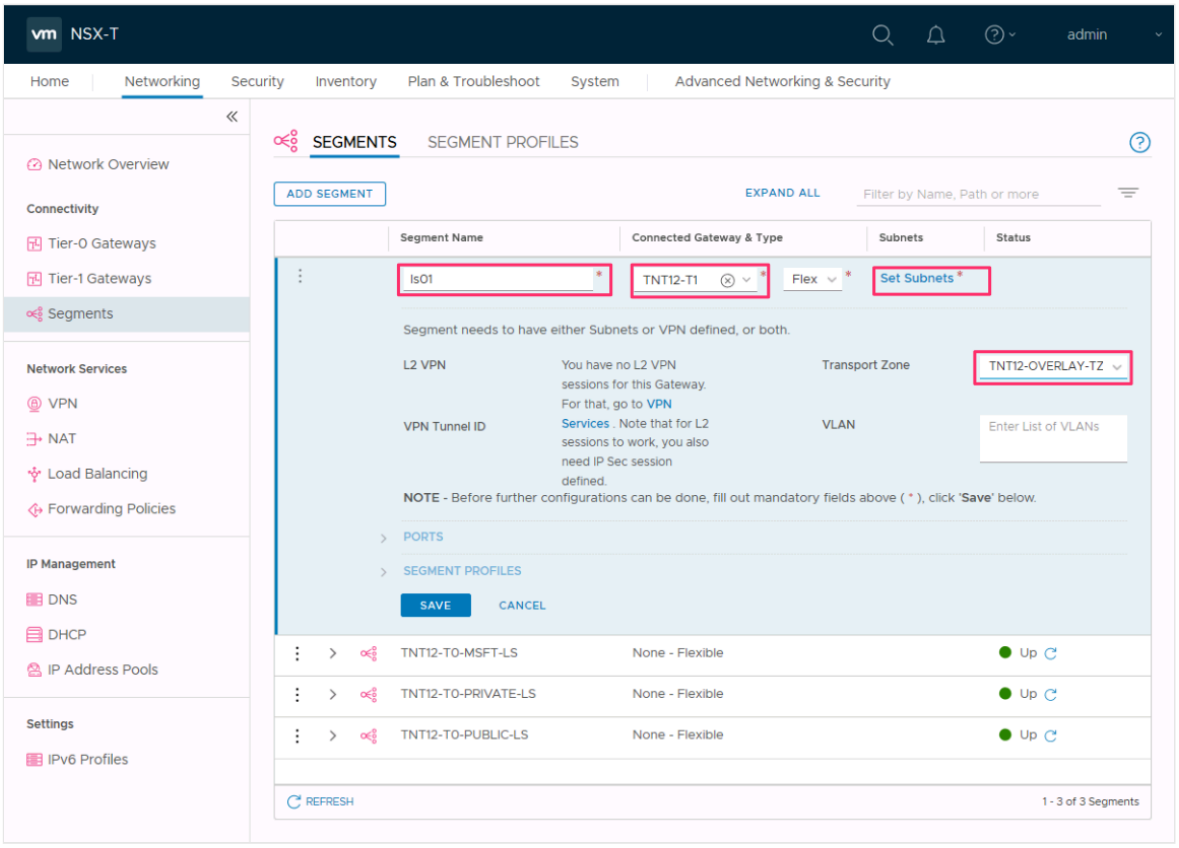


Add a network segment

1. In NSX Manager, select **Networking** > **Segments**, and then select **Add Segment**.

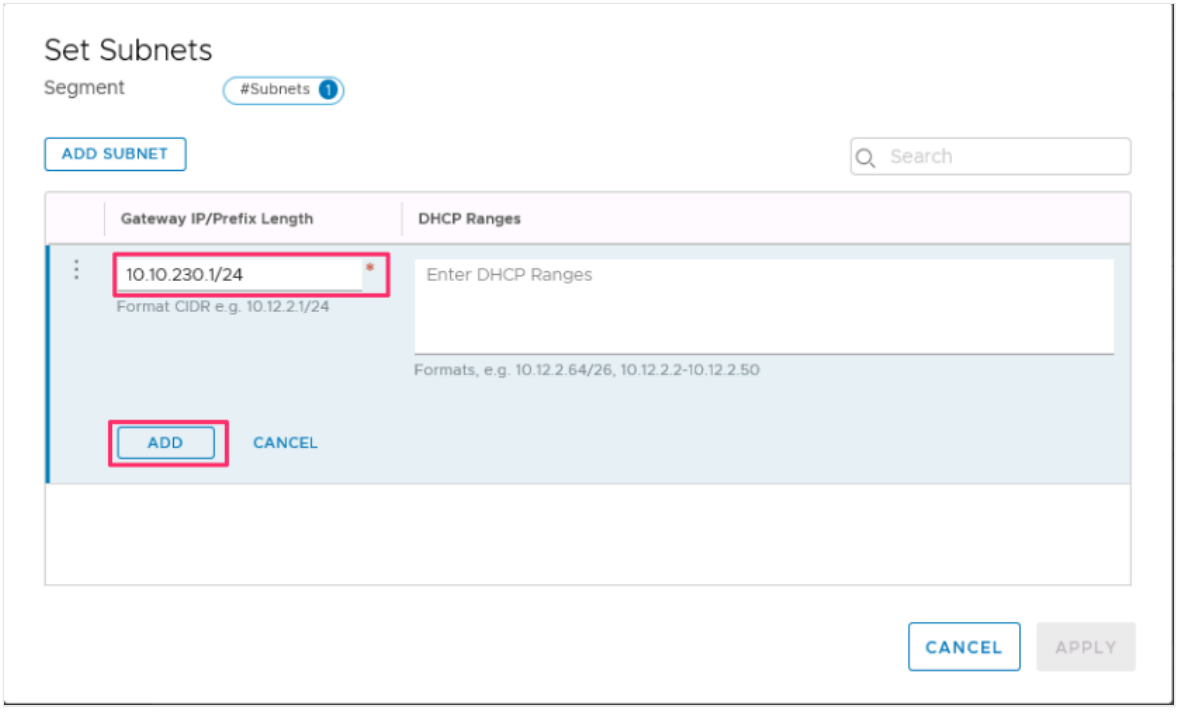


2. Enter a name for the segment.
3. Select the Tier-1 Gateway (TNTxx-T1) as the **Connected Gateway** and leave the **Type** as Flexible.
4. Select the preconfigured overlay **Transport Zone** (TNTxx-OVERLAY-TZ) and then select **Set Subnets**.



5. Enter the gateway IP address and then select **Add**.

> **Important**
>
> The IP address needs to be on a non-overlapping RFC1918 address block, which ensures connection to the VMs on the new segment.



6. Select **Apply** and then **Save**.

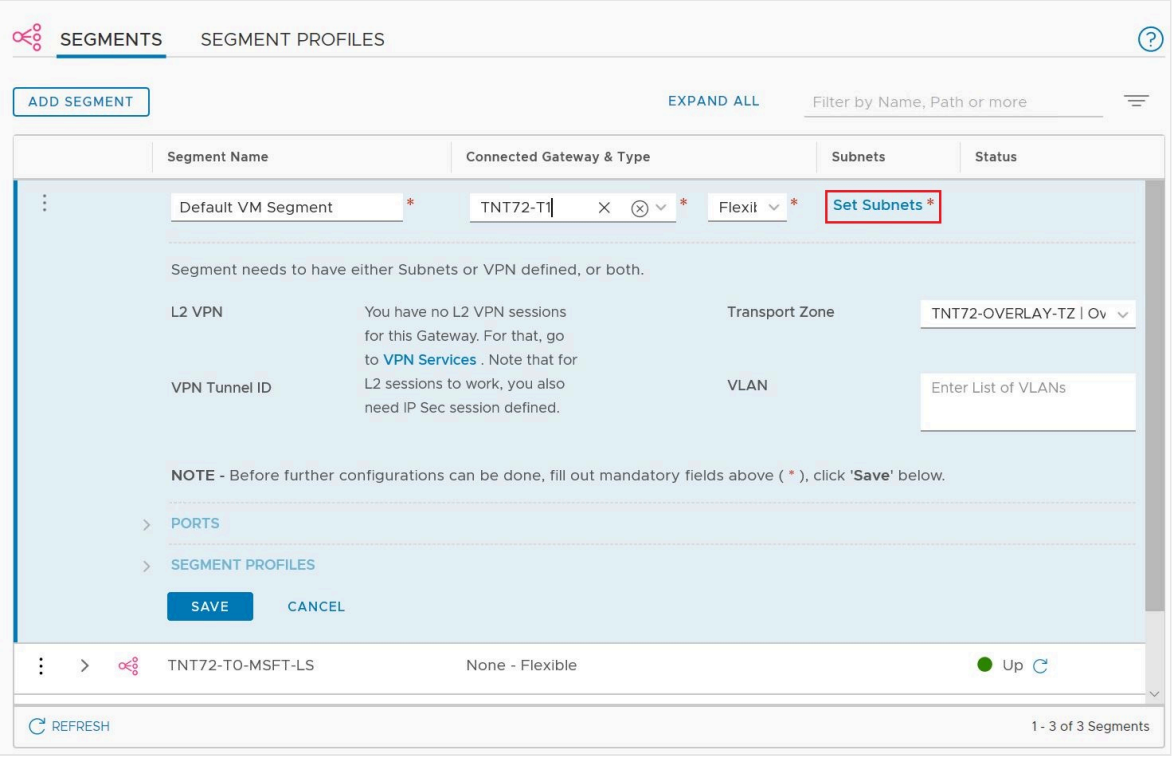
7. Select **No** to decline the option to continue configuring the segment.

Specify the DHCP IP address range

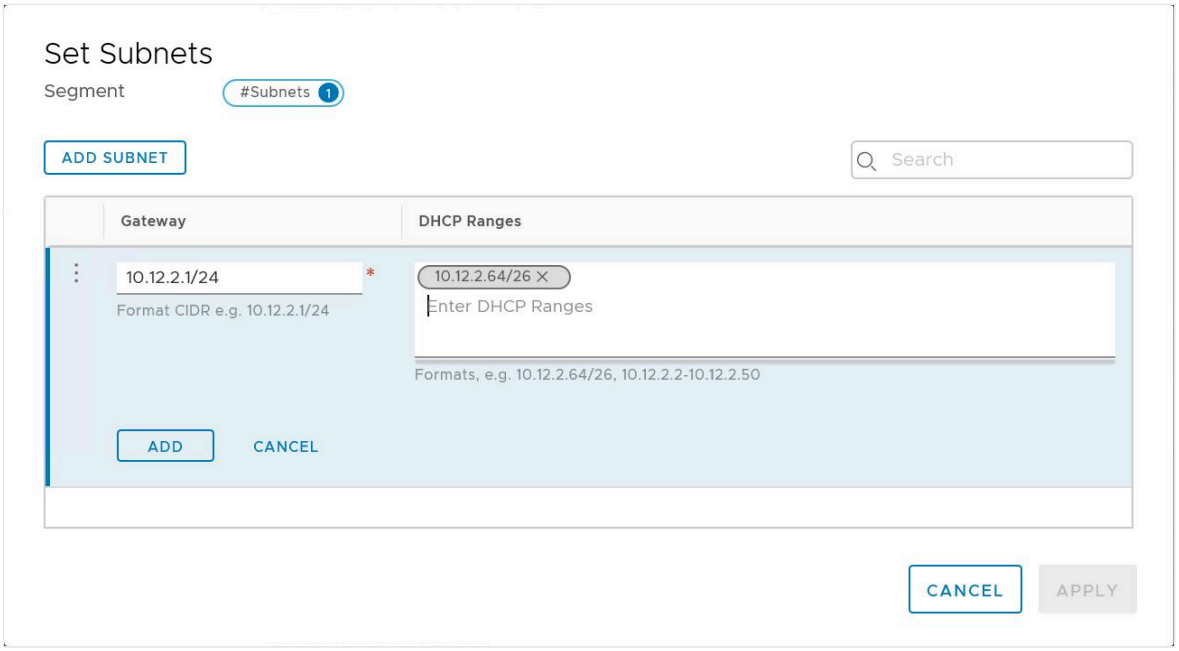
When you create a relay to a DHCP server, you need to specify the DHCP IP address range.

> **Note**
>
> The IP address range shouldn't overlap with the IP range used in other virtual networks in your subscription and on-premises networks.

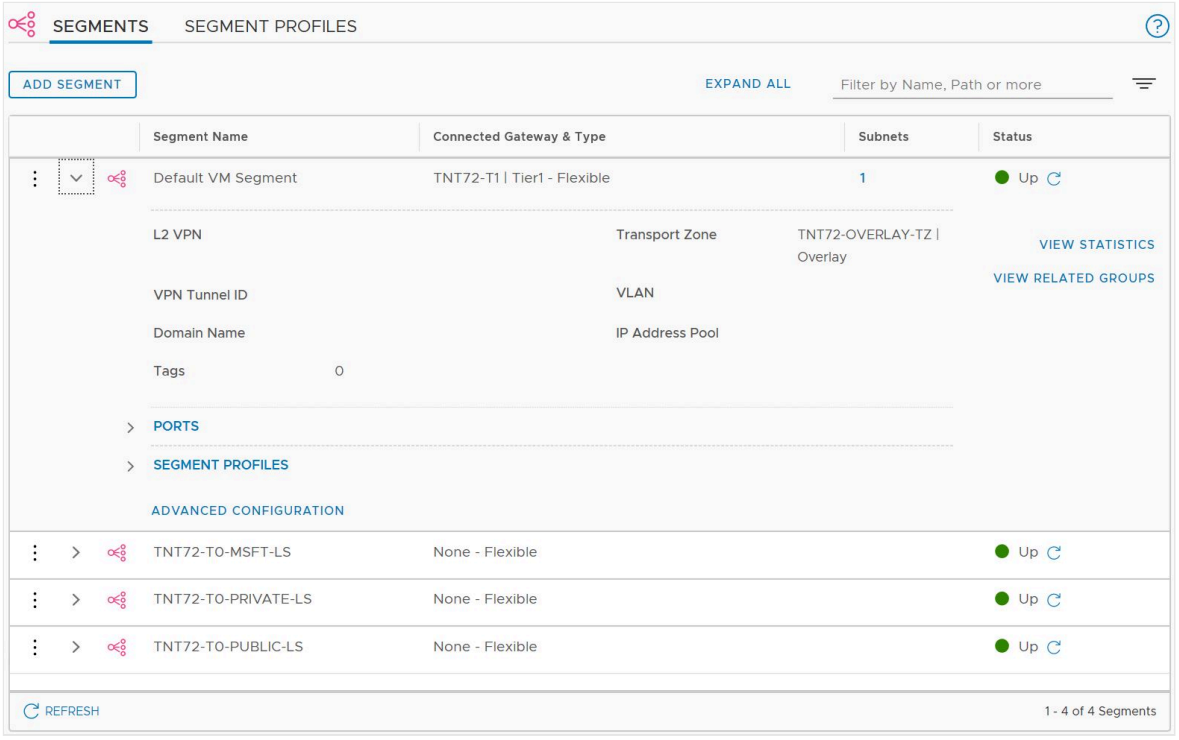
1. In NSX Manager, select **Networking** > **Segments**.
2. Select the vertical ellipsis on the segment name and select **Edit**.
3. Select **Set Subnets** to specify the DHCP IP address for the subnet.



4. Modify the gateway IP address if needed, and enter the DHCP range IP.



5. Select **Apply**, and then **Save**. The segment is assigned a DHCP server pool.



Use a third-party external DHCP server

If you want to use a third-party external DHCP server, create a DHCP relay service in NSX Manager. You need to specify the DHCP IP address range.

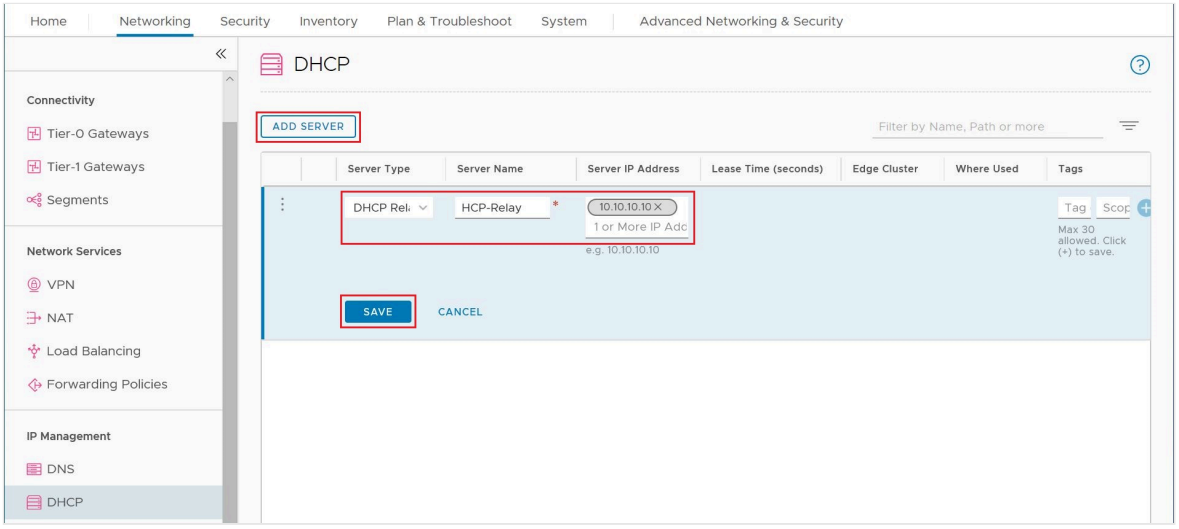
ⓘ Important

For clouds created on or after July 1, 2021, the simplified view of NSX operations must be used to configure DHCP on the default Tier-1 Gateway in your environment.

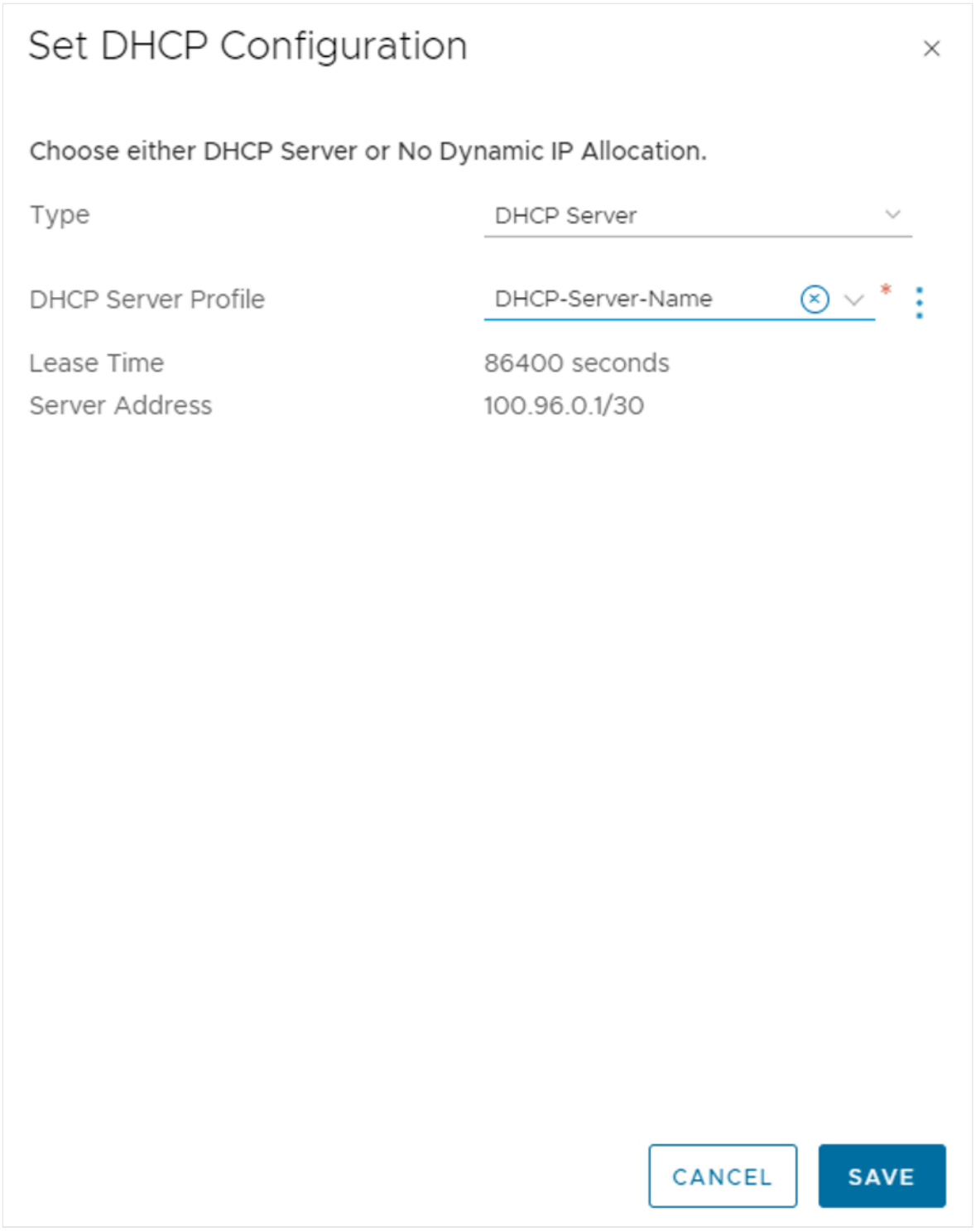
Create DHCP relay service

Use a DHCP relay for any non-NSX-based DHCP service. For example, a VM running DHCP in Azure VMware Solution, Azure IaaS, or on-premises.

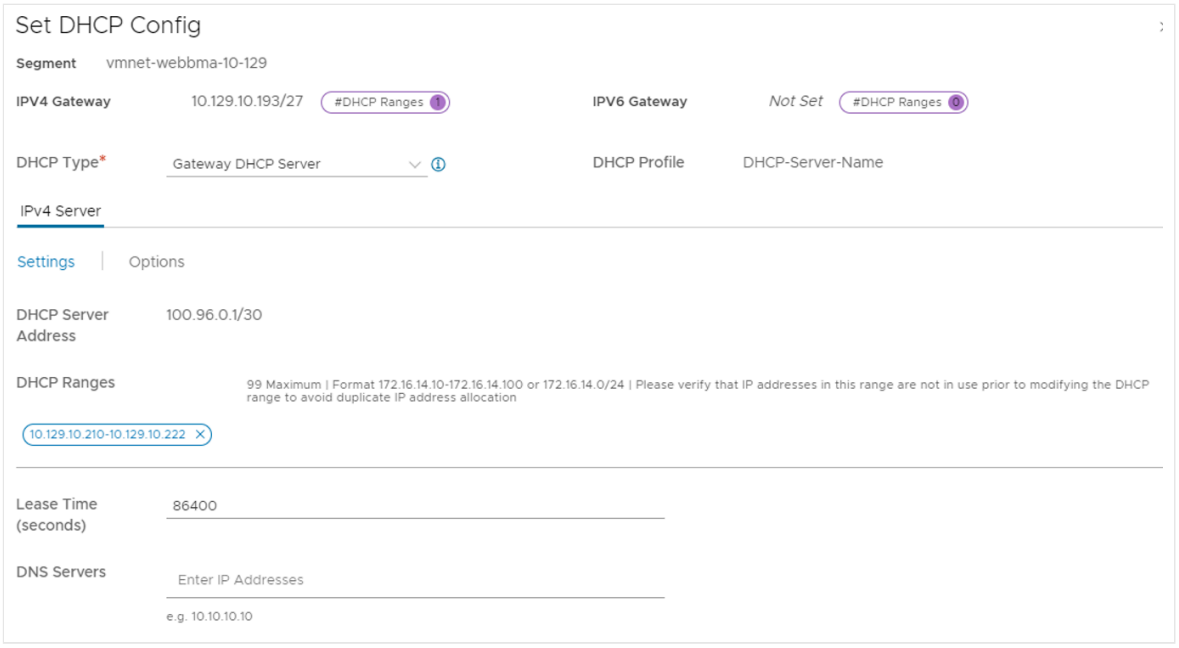
1. In NSX Manager, select **Networking** > **DHCP**, and then select **Add Server**.
2. Select **DHCP Relay** for the **Server Type**, provide the server name and IP address, and select **Save**.



3. Select **Tier 1 Gateways**, select the vertical ellipsis on the Tier-1 gateway, and then select **Edit**.



4. Select **No IP Allocation Set** to define the IP address allocation.



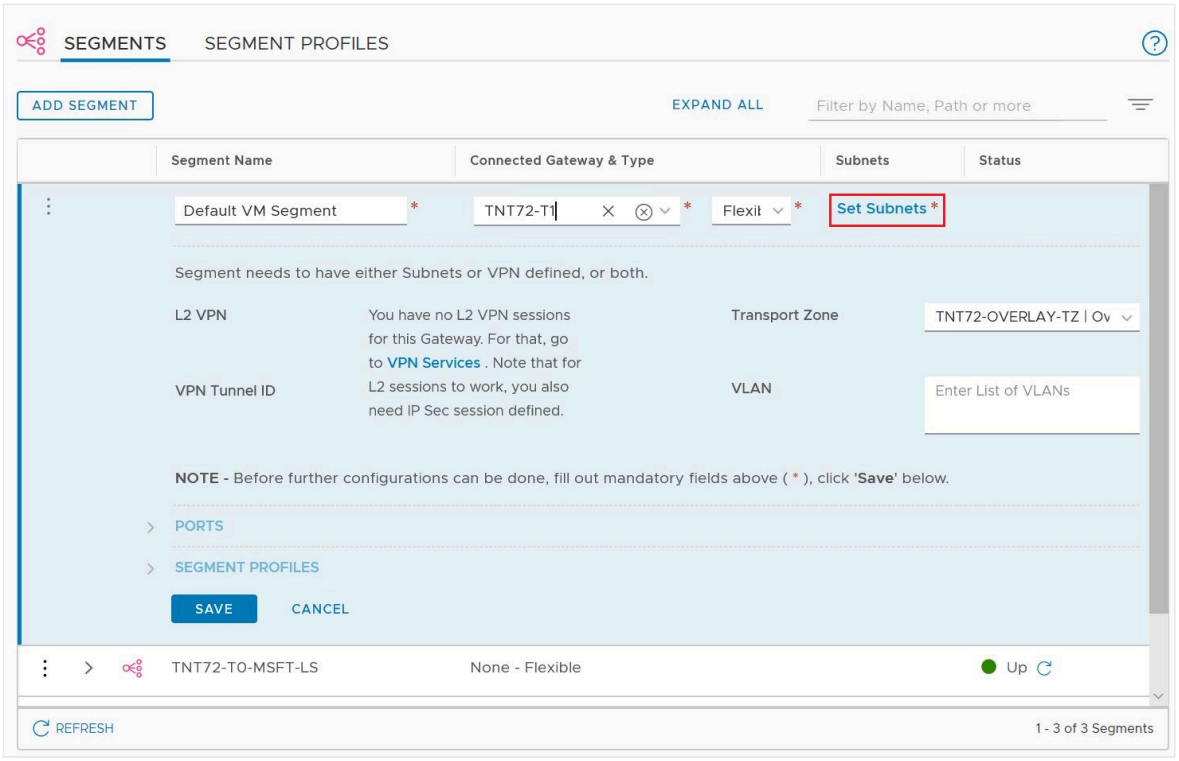
5. For **Type**, select **DHCP Server**.
6. For the **DHCP Server**, select **DHCP Relay**, and then select **Save**.
7. Select **Save** again and then select **Close Editing**.

Specify the DHCP IP address range

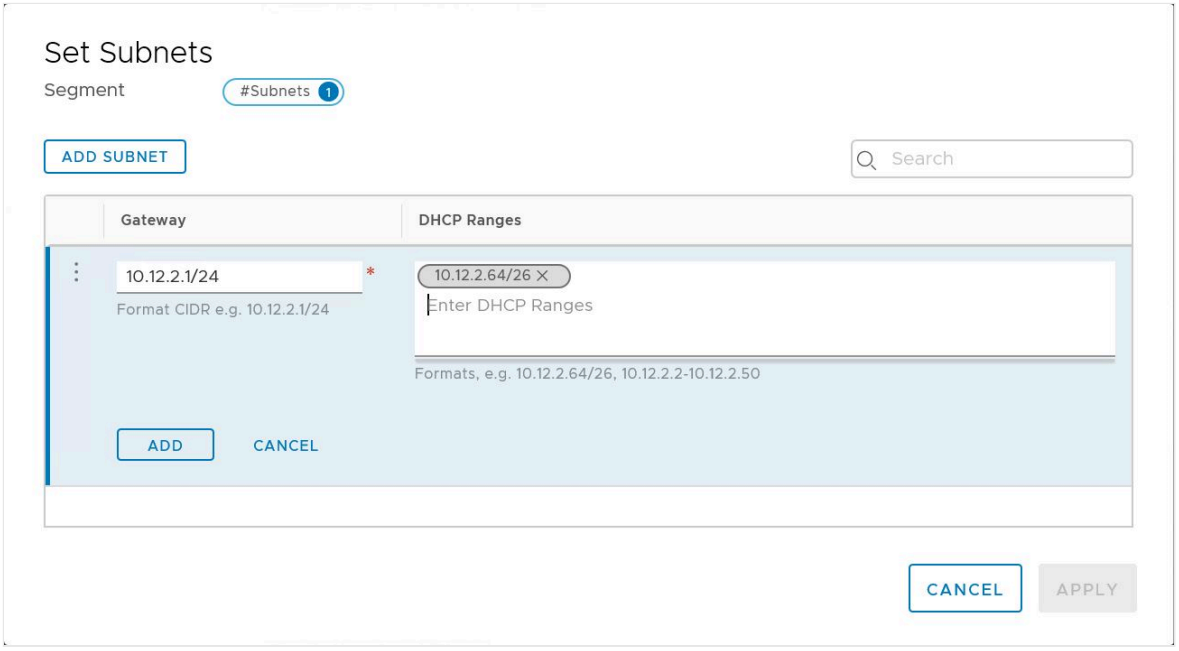
When you create a relay to a DHCP server, you need to specify the DHCP IP address range.

> ⓘ **Note**
>
> The IP address range shouldn't overlap with the IP range used in other virtual networks in your subscription and on-premises networks.

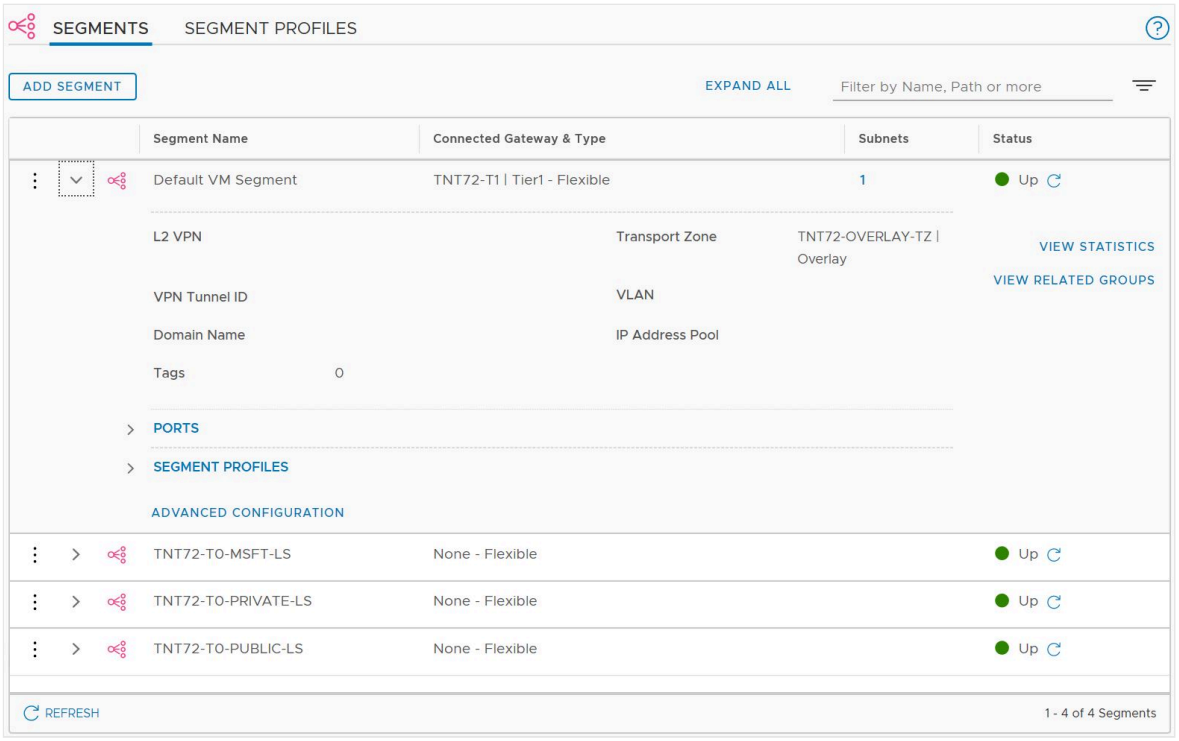
1. In NSX Manager, select **Networking** > **Segments**.
2. Select the vertical ellipsis on the segment name and select **Edit**.
3. Select **Set Subnets** to specify the DHCP IP address for the subnet.



4. Modify the gateway IP address if needed, and enter the DHCP range IP.



5. Select **Apply**, and then **Save**. The segment is assigned a DHCP server pool.



Next steps

If you want to send DHCP requests from your Azure VMware Solution VMs to a non-NSX DHCP server, see the Configure DHCP on L2 stretched VMware HCX networks procedure.

Feedback

Was this page helpful? Yes No

Provide product feedback

Configure DHCP on L2 stretched VMware HCX networks

Article • 03/07/2024

DHCP doesn't work for virtual machines (VMs) on the VMware HCX L2 stretched network when the DHCP server is in the on-premises data center because NSX, by default, blocks all DHCP requests from traversing the L2 stretch. Therefore, to send DHCP requests from your Azure VMware Solution VMs to a non-NSX DHCP server, you need to configure DHCP on L2 stretched VMware HCX networks.

Configuring DHCP Relay in NSX is unnecessary while the network is stretched. Implementing DHCP relay on an extended network may lead to unintended issues, resulting in clients not receiving the correct responses. Following a failover to Azure VMware Solution, DHCP Relay or NSX DHCP server configuration would be necessary to continue serving clients effectively.

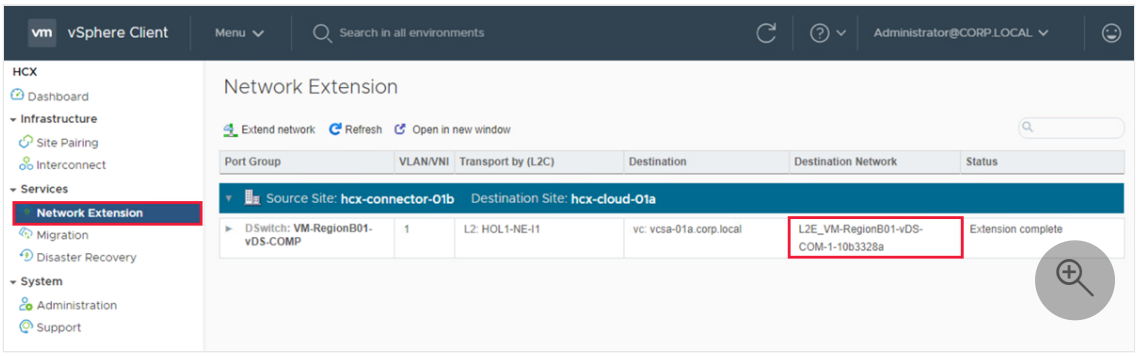
1. (Optional) If you need to locate the segment name of the L2 extension:

   a. Sign in to your on-premises vCenter Server, and under **Home**, select **HCX**.

   b. Select **Network Extension** under **Services**.

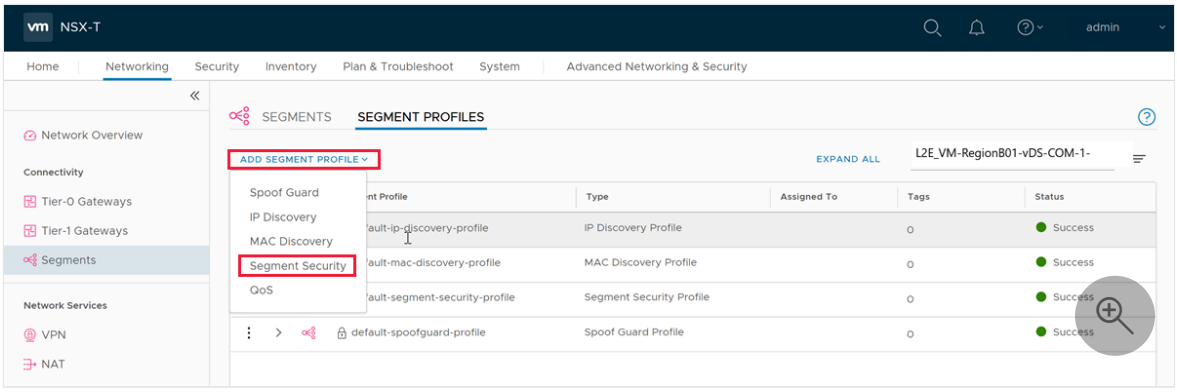
   c. Select the network extension you want to support DHCP requests from Azure VMware Solution to on-premises.

   d. Take note of the destination network name.

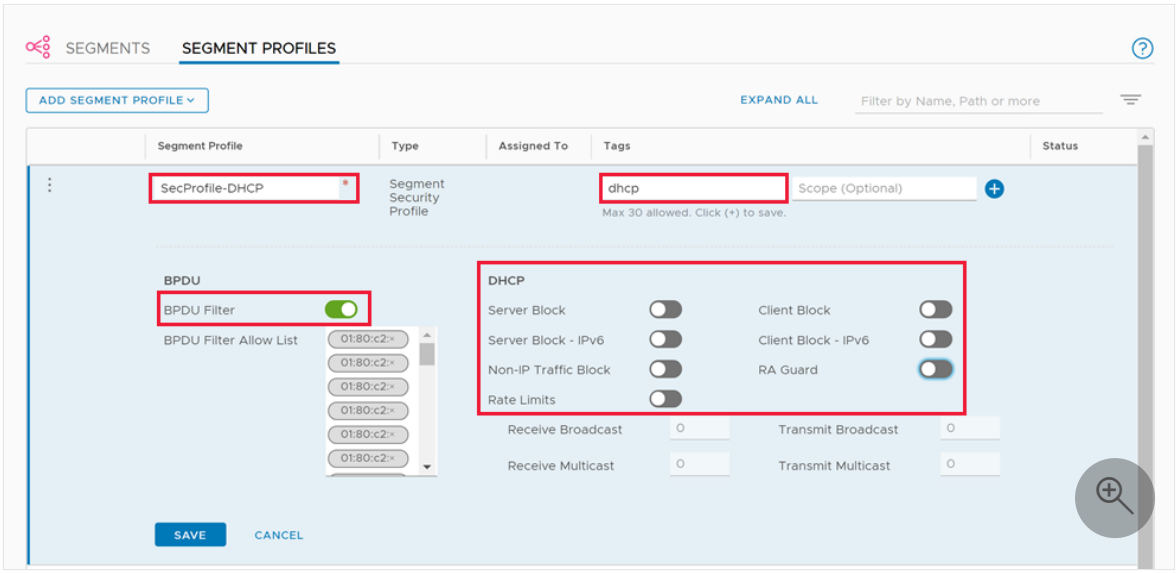


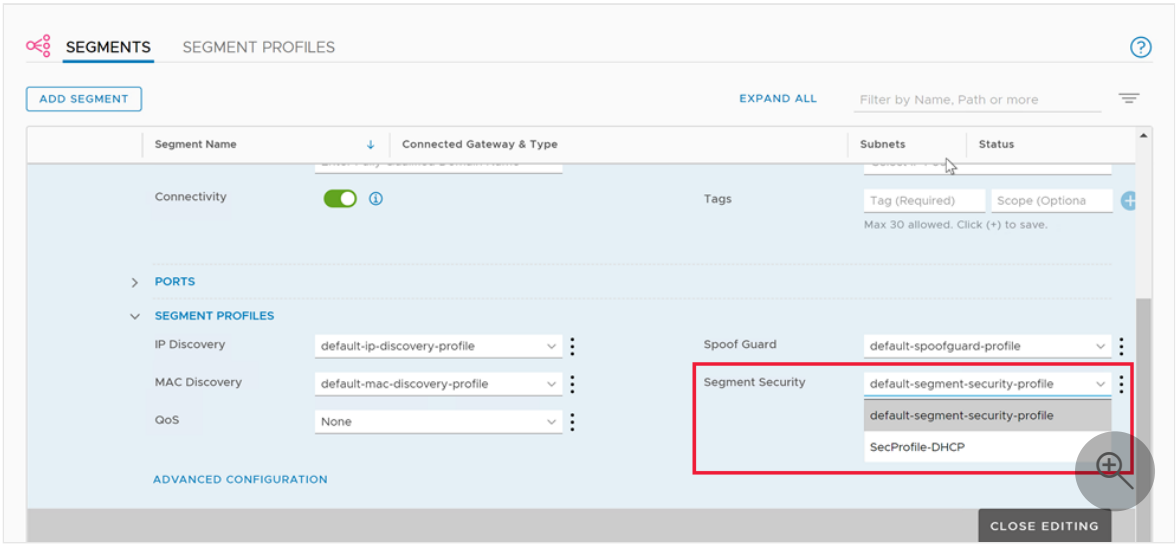
2. In NSX-T Manager, select **Networking** > **Segments** > **Segment Profiles**.

3. Select **Add Segment Profile** and then **Segment Security**.



4. Provide a name and a tag, and then set the **BPDU Filter** toggle to ON and all the DHCP toggles to OFF.





Configure a DNS forwarder in the Azure portal

Article • 02/27/2024

> **Important**
>
> For Azure VMware Solution private clouds created on or after July 1, 2021, you now have the ability to configure private DNS resolution. For private clouds created before July 1, 2021, that need private DNS resolution, open a support request and request Private DNS configuration.

By default, Azure VMware Solution management components such as vCenter Server can only resolve name records available through Public DNS. However, certain hybrid use cases require Azure VMware Solution management components to resolve name records from privately hosted DNS to properly function, including customer-managed systems such as vCenter Server and Active Directory.

Private DNS for Azure VMware Solution management components lets you define conditional forwarding rules for the desired domain name to a selected set of private DNS servers through the NSX-T Data Center DNS Service.

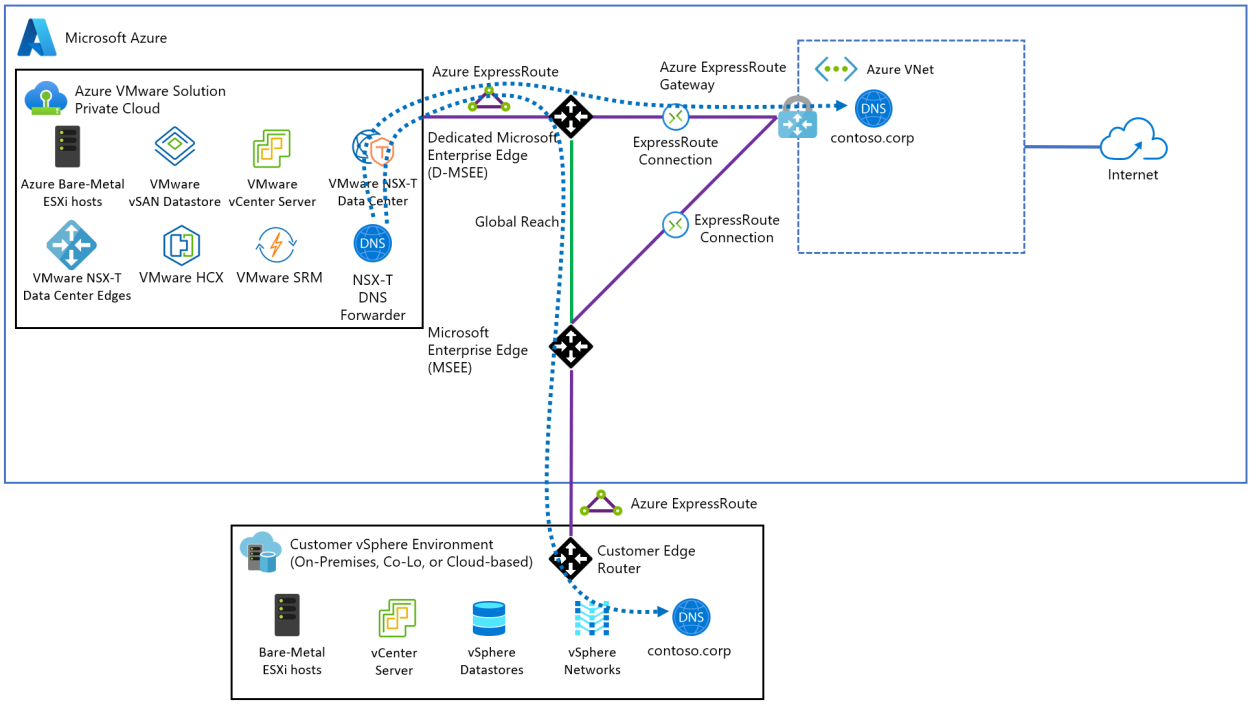
This capability uses the DNS Forwarder Service in NSX-T Data Center. A DNS service and default DNS zone are provided as part of your private cloud. To enable Azure VMware Solution management components to resolve records from your private DNS systems, you must define an FQDN zone and apply it to the NSX-T Data Center DNS Service. The DNS Service conditionally forwards DNS queries for each zone based on the external DNS servers defined in that zone.

> **Note**
>
> The DNS Service is associated with up to five FQDN zones. Each FQDN zone is associated with up to three DNS servers.

> **Tip**
>
> If desired, you can also use the conditional forwarding rules for workload segments by configuring virtual machines on those segments to use the NSX-T Data Center DNS Service IP address as their DNS server.

Architecture

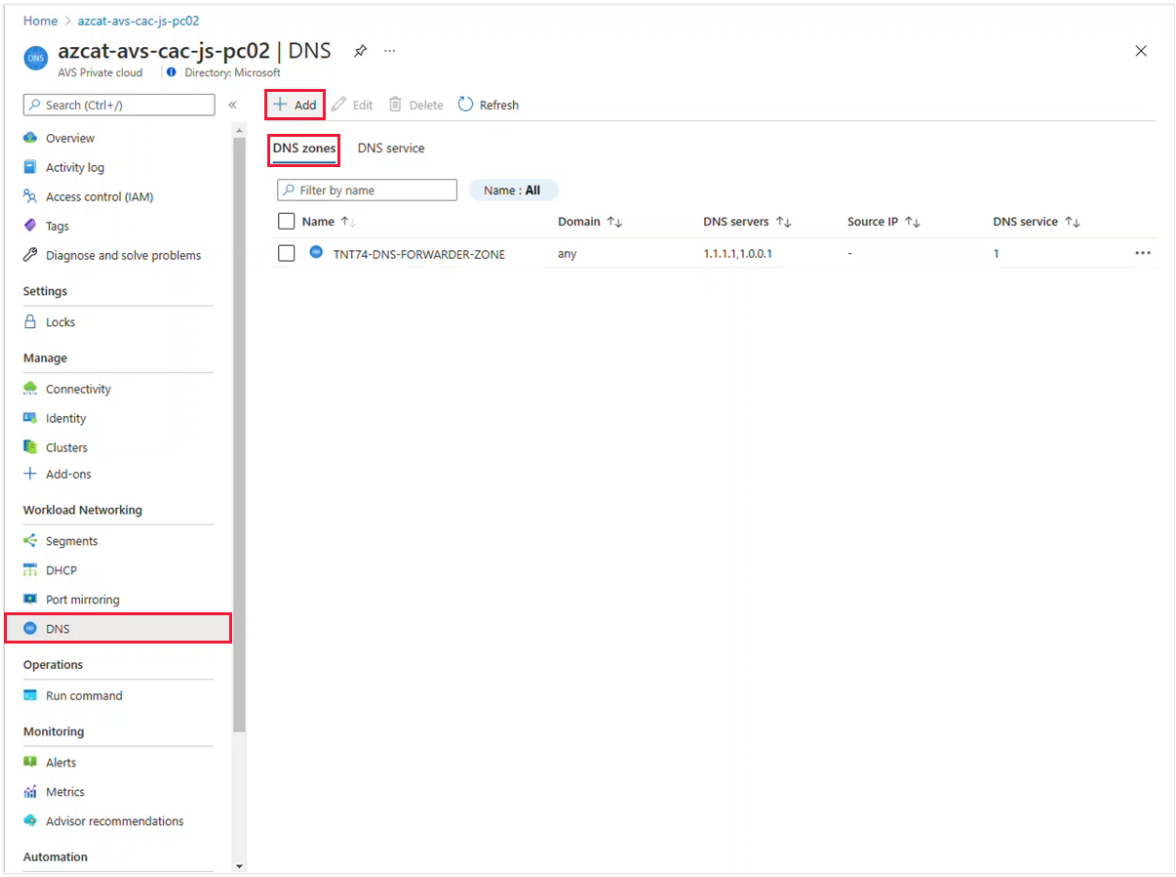
The diagram shows that the NSX-T Data Center DNS Service can forward DNS queries to DNS systems hosted in Azure and on-premises environments.



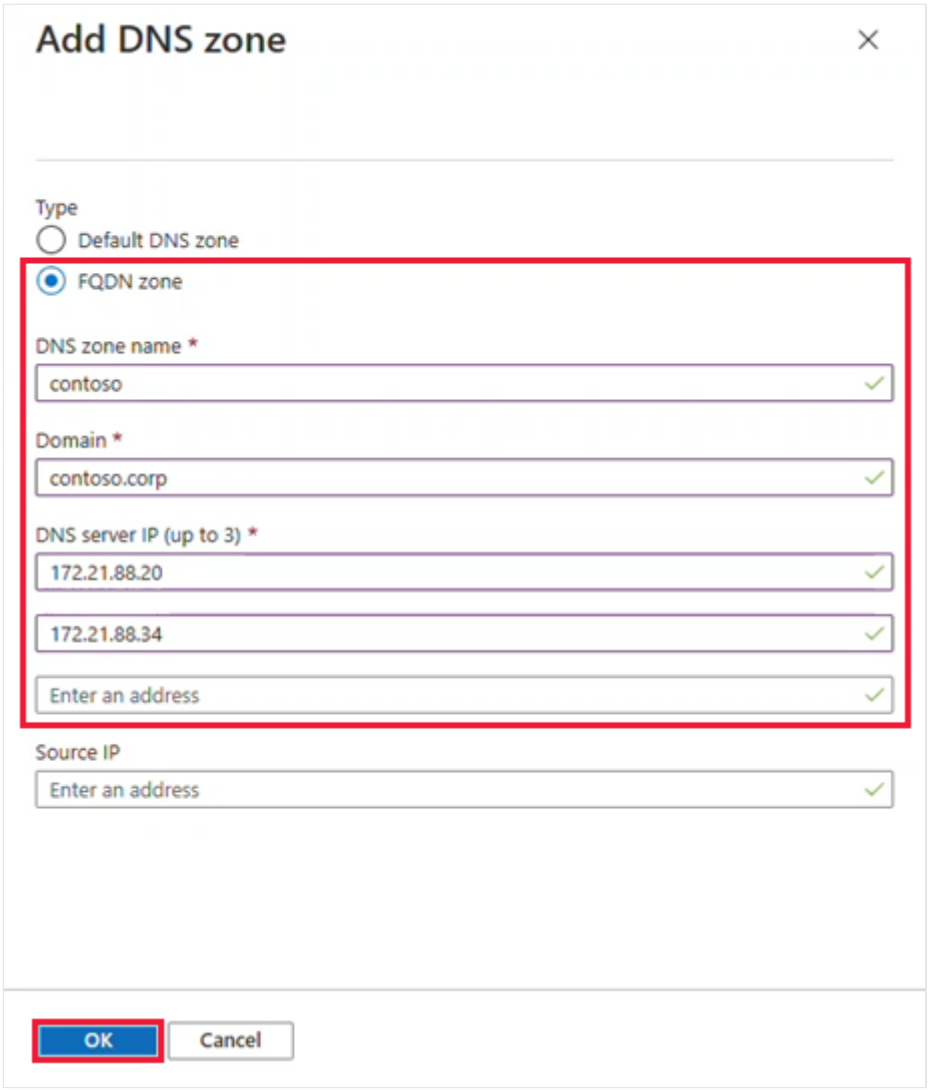
Configure DNS forwarder

1. In your Azure VMware Solution private cloud, under **Workload Networking**, select **DNS** > **DNS zones**. Then select **Add**.

> **Note**
>
> For private clouds created on or after July 1, 2021, the default DNS zone is created for you during the private cloud creation.



2. Select **FQDN zone**, provide a name and up to three DNS server IP addresses in the format of **10.0.0.53**. Then select **OK**.



> **ⓘ Important**
>
> While NSX-T Data Center allows spaces and other non-alphanumeric characters in a DNS zone name, certain NSX-T Data Center resources such as a DNS Zone are mapped to an Azure resource whose names don't permit certain characters.
>
> As a result, DNS zone names that would otherwise be valid in NSX-T Data Center may need adjustment to adhere to the Azure resource naming conventions.

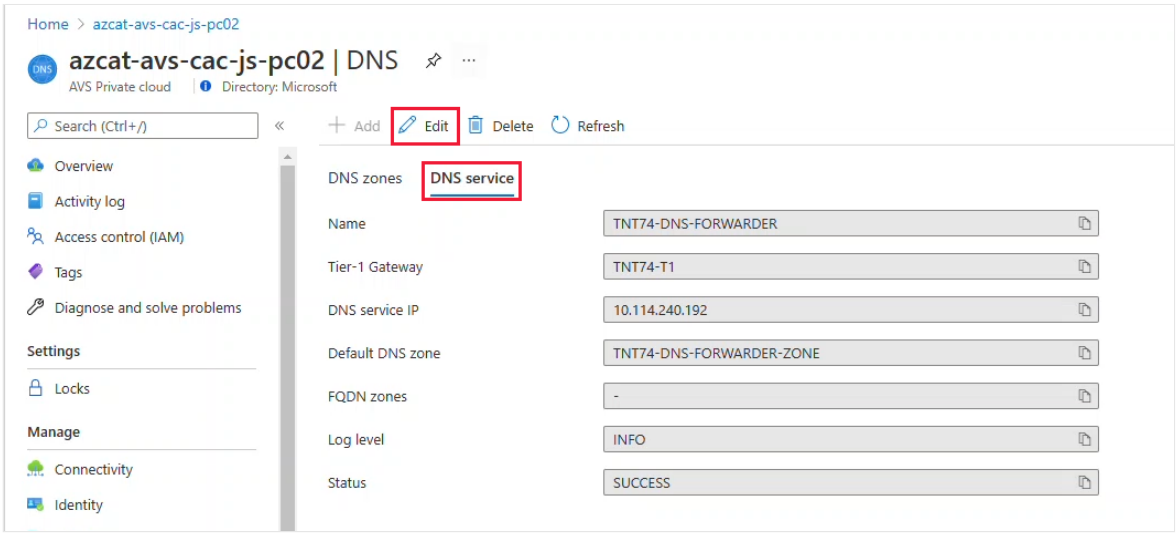
It takes several minutes to complete, you can follow the progress from **Notifications**. You see a message in the Notifications when the DNS zone is created.

3. Ignore the message about a default DNS zone because one gets created for you as part of your private cloud.

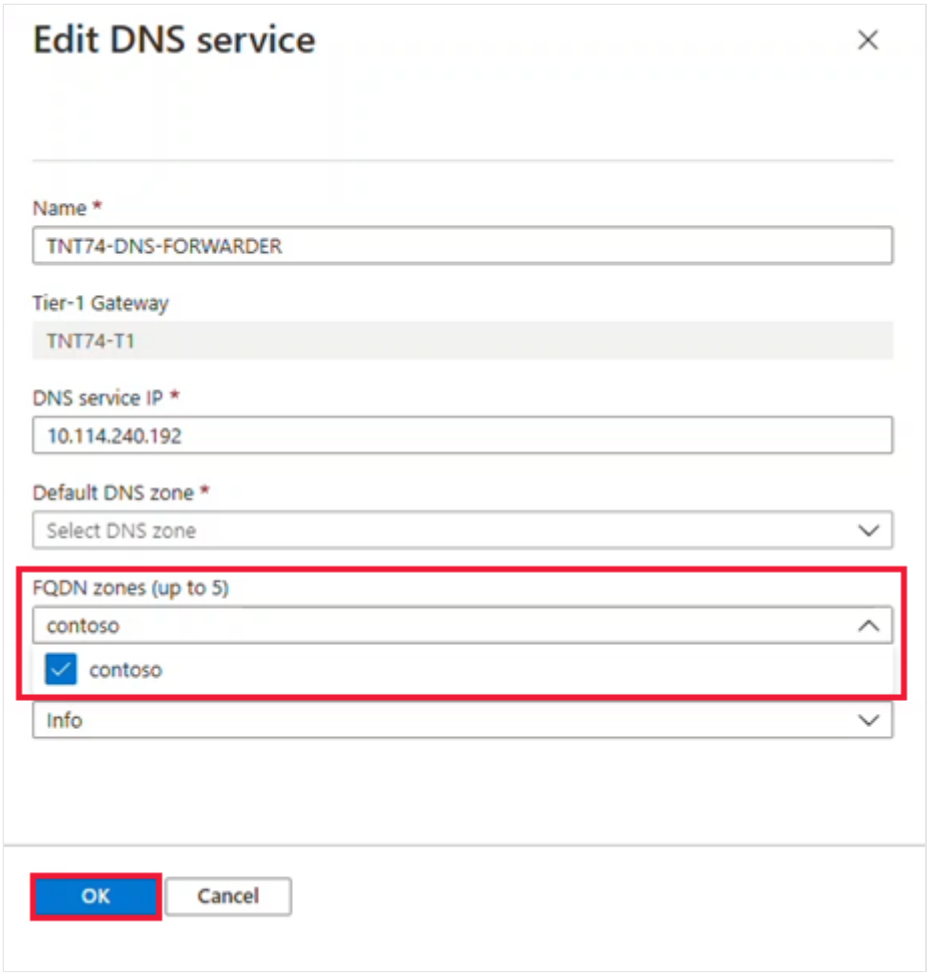
4. Select the **DNS service** tab and then select **Edit**.

> **Tip**
>
> For private clouds created on or after July 1, 2021, you can ignore the message about a default DNS zone as one is created for you during private cloud creation.

> **Important**
>
> While certain operations in your private cloud may be performed from NSX-T Manager, for private clouds created on or after July 1, 2021, you *must* edit the DNS service from the Simplified Networking experience in the Azure portal for any configuration changes made to the default Tier-1 Gateway.



5. From the **FQDN zones** drop-down, select the newly created FQDN, and then select **OK**.

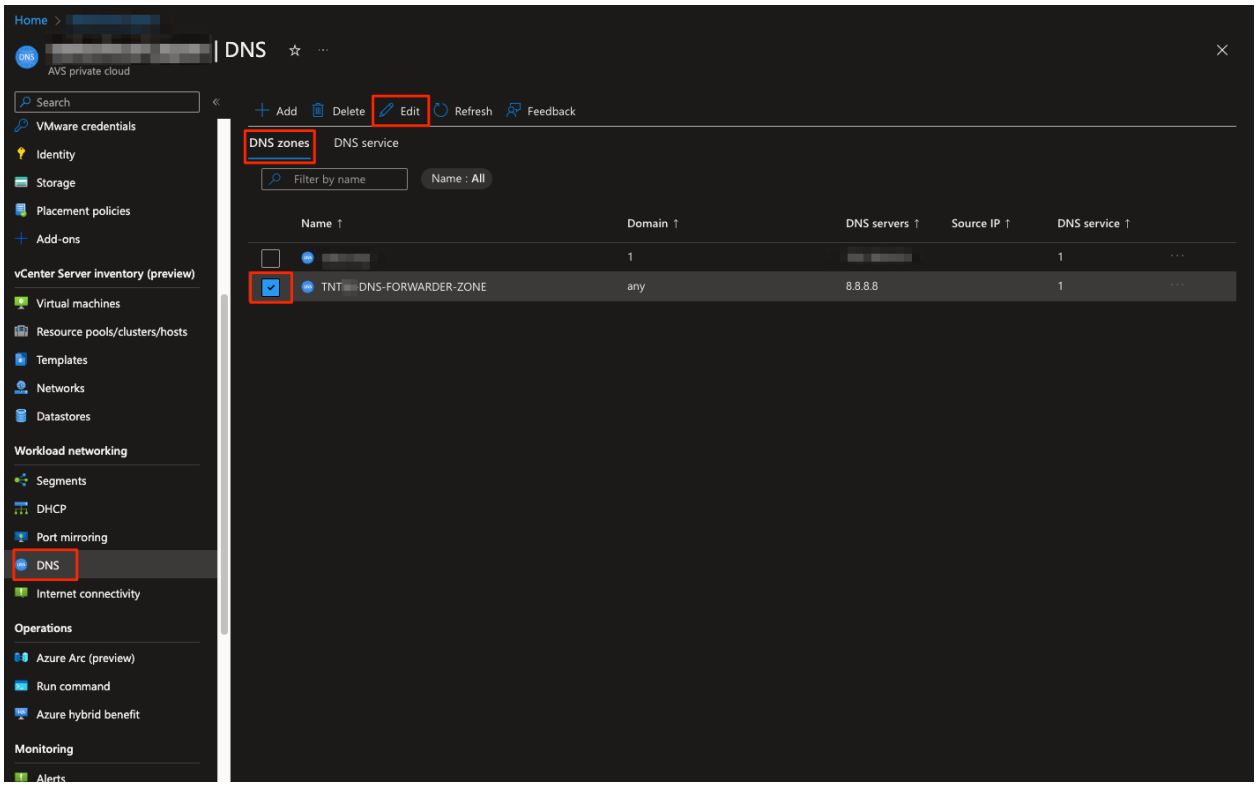


It takes several minutes to complete, and once finished, you see the *Completed* message from **Notifications**. At this point, management components in your private cloud should be able to resolve DNS entries from the FQDN zone provided to the NSX-T Data Center DNS Service.

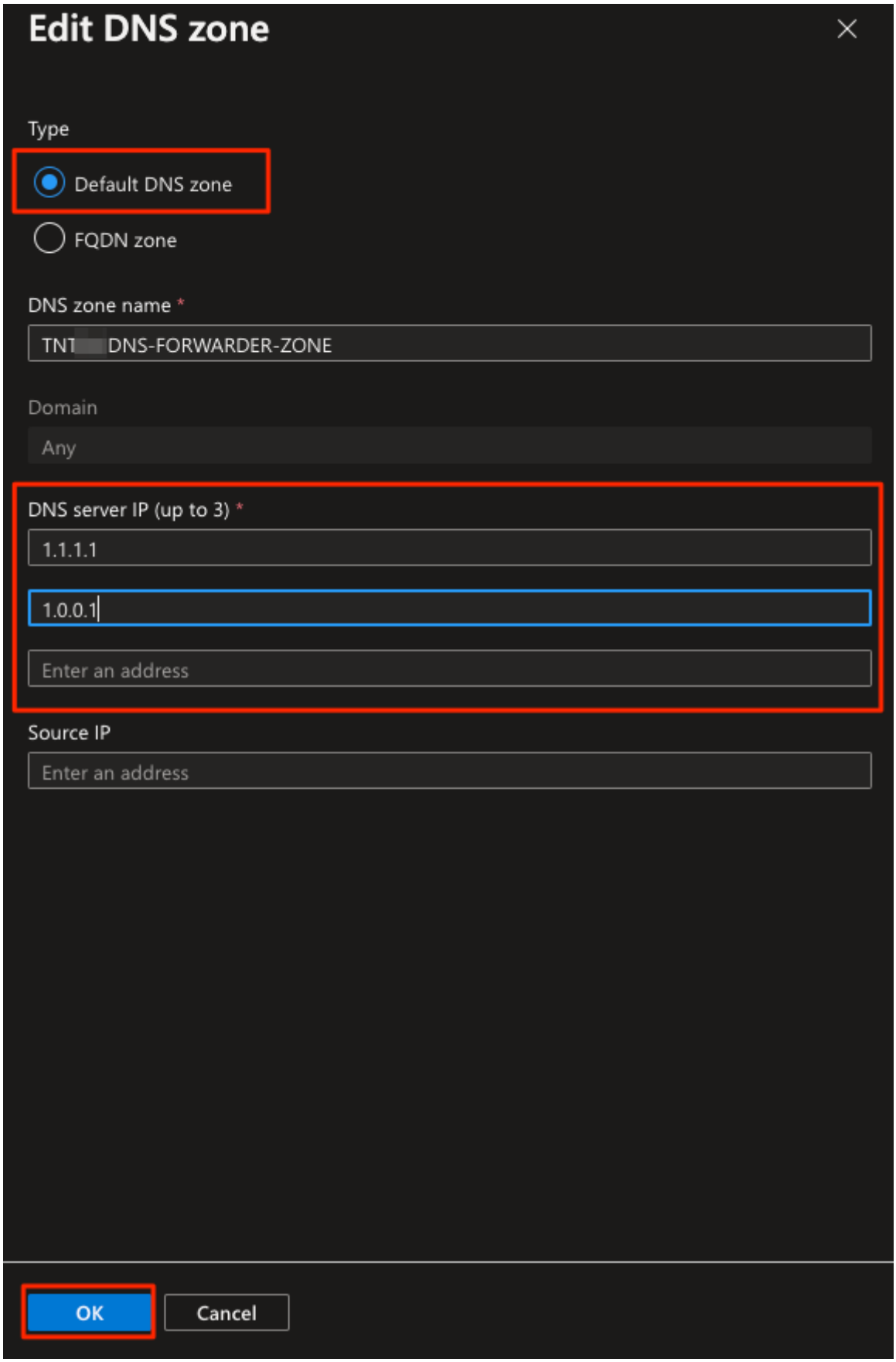
6. Repeat the above steps for other FQDN zones, including any applicable reverse lookup zones.

Change Default T1 DNS Forwarder Zone

1. In your Azure VMware Solution private cloud, under **Workload Networking**, select **DNS** > **DNS zones** > Check **TNT##-DNS-FORWARDER-ZONE**. Then select **Edit**.



2. Change DNS server entries to valid reachable IP addresses. Then select **OK**



ⓘ Important

A DNS endpoint that is unreachable by the NSX-T DNS server will result in an NSX-T alarm stating that the endpoint is unreachable. In cases of the default configuration provided with Azure VMware Solution, this is due to internet that is

disabled by default. The alarm can be acknowledged and ignored, or the default configuration can be changed to a valid endpoint.

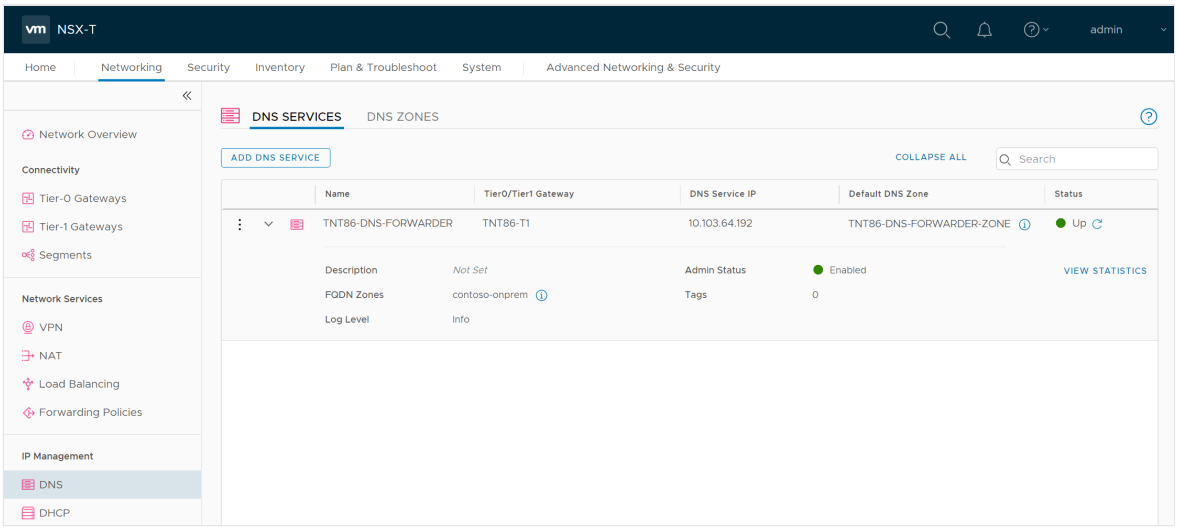
Verify name resolution operations

After you configure the DNS forwarder, you have some options available to verify name resolution operations.

VMware NSX-T Manager

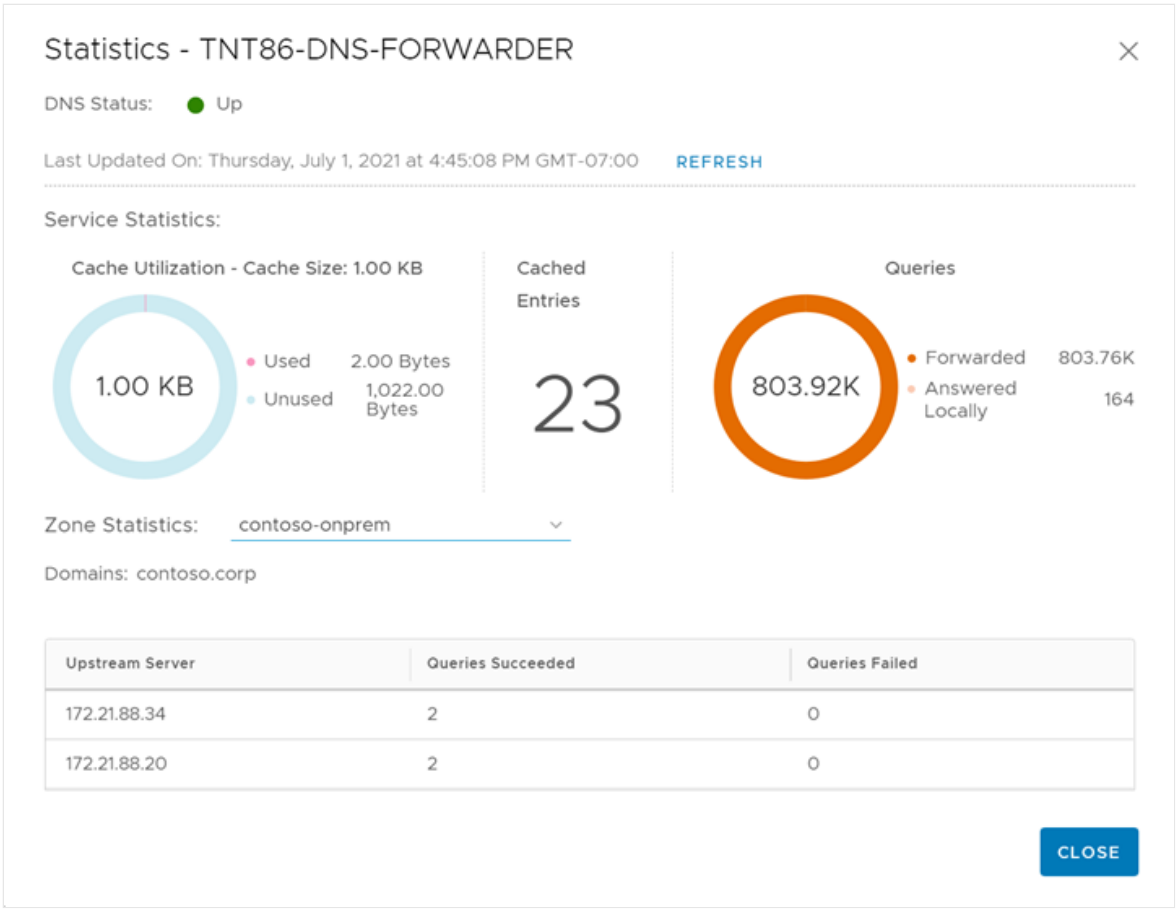
NSX-T Manager provides the DNS Forwarder Service statistics at the global service level and on a per zone basis.

1. In NSX-T Manager, select **Networking** > **DNS**, and then expand your DNS Forwarder Service.



2. Select **View Statistics**, and then from the **Zone Statistics** drop-down, select your FQDN Zone.

   The top half shows the statistics for the entire service, and the bottom half shows the statistics for your specified zone. In this example, you can see the forwarded queries to the DNS services specified during the configuration of the FQDN zone.



PowerCLI

The NSX-T Policy API lets you run nslookup commands from the NSX-T Data Center DNS Forwarder Service. The required cmdlets are part of the `VMware.VimAutomation.Nsxt` module in PowerCLI. The following example demonstrates output from version 12.3.0 of that module.

1. Connect to your NSX-T Manager cluster.

   > **Tip**
   >
   > You can obtain the IP address of your NSX-T Manager cluster from the Azure portal under **Manage** > **Identity**.

   PowerShell

   ```
   Connect-NsxtServer -Server 10.103.64.3
   ```

2. Obtain a proxy to the DNS Forwarder's nslookup service.

   PowerShell

```
$nslookup = Get-NsxtPolicyService -Name
com.vmware.nsx_policy.infra.tier_1s.dns_forwarder.nslookup
```

3. Perform lookups from the DNS Forwarder Service.

```PowerShell
$response = $nslookup.get('TNT86-T1', 'vc01.contoso.corp')
```

The first parameter in the command is the ID for your private cloud's T1 gateway, which you can obtain from the DNS service tab in the Azure portal.

1. Obtain a raw answer from the lookup using the following properties of the response.

```PowerShell
$response.dns_answer_per_enforcement_point.raw_answer; (()) DiG 9.10.3-
P4-Ubuntu (()) @10.103.64.192 -b 10.103.64.192 vc01.contoso.corp
+timeout=5 +tries=3 +nosearch ; (1 server found) ;; global options:
+cmd ;; Got answer: ;; -))HEADER((- opcode: QUERY, status: NOERROR, id:
10684 ;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0,
ADDITIONAL: 1  ;; OPT PSEUDOSECTION: ; EDNS: version: 0, flags:; udp:
4096 ;; QUESTION SECTION: ;vc01.contoso.corp.  IN A  ;; ANSWER SECTION:
vc01.contoso.corp. 3046 IN A 172.21.90.2  ;; Query time: 0 msec ;;
SERVER: 10.103.64.192:53(10.103.64.192) ;; WHEN: Thu Jul 01 23:44:36
UTC 2021 ;; MSG SIZE  rcvd: 62
```

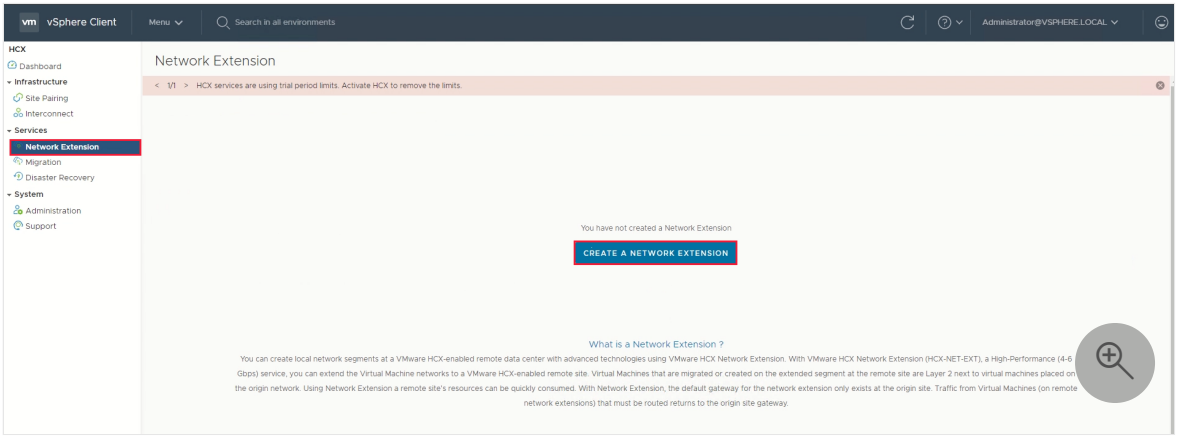
   In this example, you can see an answer for the query of vc01.contoso.corp showing an A record with the address 172.21.90.2. Also, this example shows a cached response from the DNS Forwarder Service, so your output might vary slightly.

Create an HCX network extension

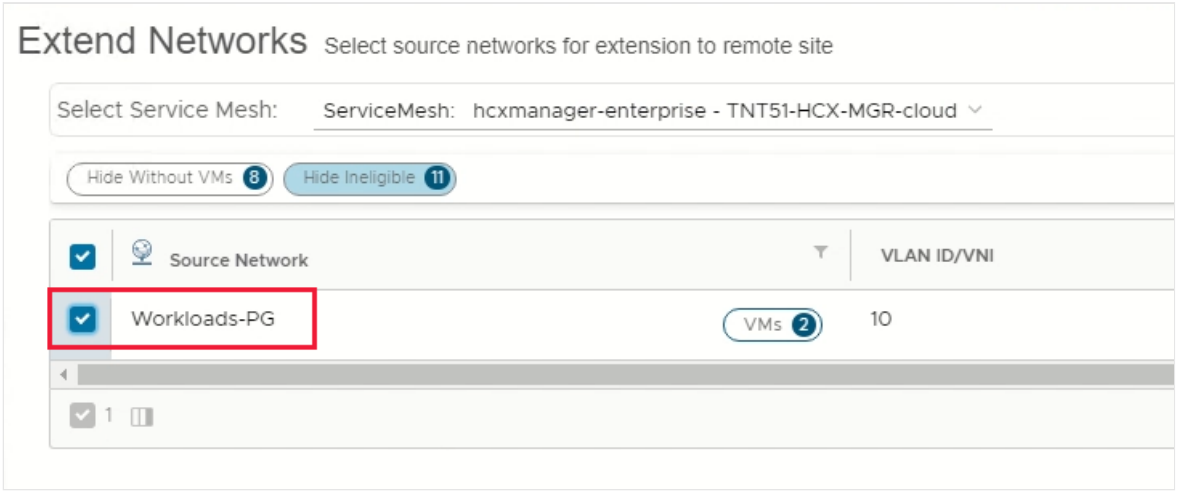
Article • 12/08/2023

Create an HCX network extension is an optional step to extend any networks from your on-premises environment to Azure VMware Solution.

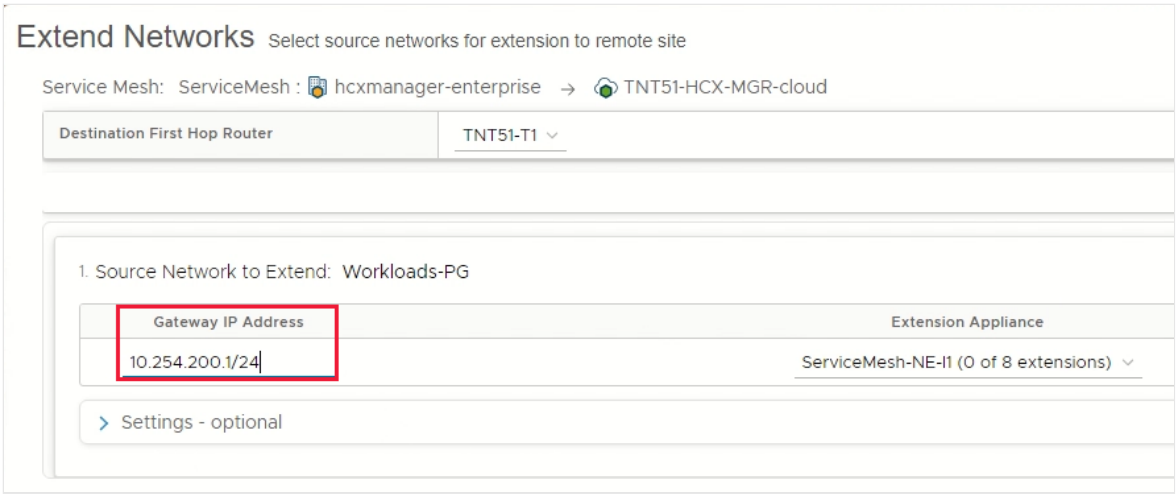
1. Under **Services**, select **Network Extension** > **Create a Network Extension**.



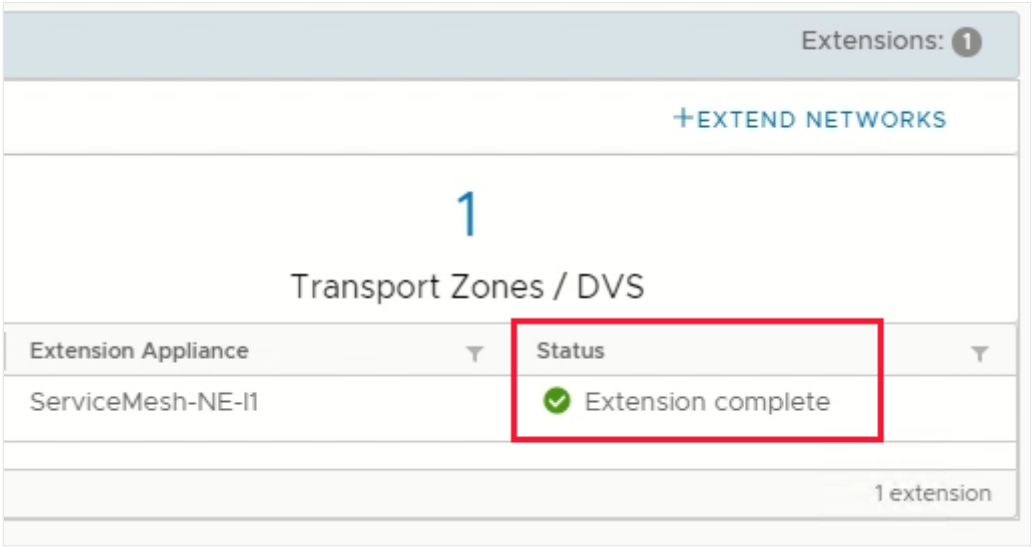
2. Select each of the networks you want to extend to Azure VMware Solution, and then select **Next**.



3. Enter the on-premises gateway IP for each of the networks you're extending, and then select **Submit**.



It takes a few minutes for the network extension to finish. When it does, you see the status change to **Extension complete**.



Next steps

Now that you configured the HCX Network Extension, learn more about:

- VMware HCX Mobility Optimized Networking (MON) guidance

VMware HCX Mobility Optimized Networking (MON) guidance

Article • 02/28/2024

> **Note**
>
> VMware HCX Mobility Optimized Networking is officially supported by VMware and Azure VMware Solution from HCX version 4.1.0.

> **Important**
>
> Before you enable HCX MON, please read the below limitations and unsupported configurations:
>
> **Unsupported source configurations for HCX NE**
>
> **Limitations for any HCX deployment including MON**
>
> VMware HCX Mobility Optimized Networking (MON) is not supported with the use of a 3rd party gateway. It may only be used with the T1 gateway directly connected to the T0 gateway without a network virtual appliance (NVA). You may be able to make this configuration function, but we do not support it.

HCX Mobility Optimized Networking (MON) is an optional feature to enable when using HCX Network Extensions (NE). MON provides optimal traffic routing under certain scenarios to prevent network tromboning between the on-premises and cloud-based resources on extended networks.

As MON is an enterprise capability of the NE feature, make sure you enabled the VMware HCX Enterprise through the Azure portal.

Throughout the migration cycle, MON optimizes application mobility for:

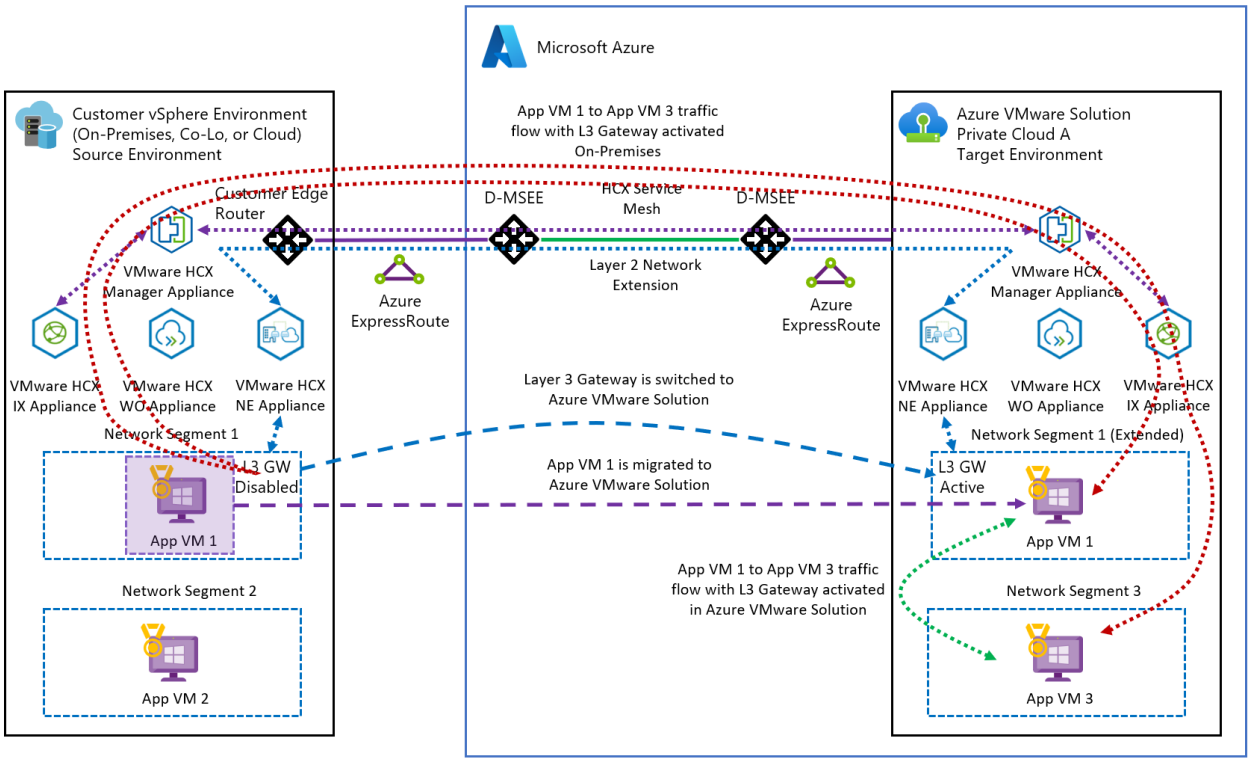
- Optimizing for virtual machine (VM) to VM L2 communication when using stretched networks
- Optimizing and avoiding asymmetric traffic flows between on-premises, Azure VMware Solution, and Azure

In this article, learn about the Azure VMware Solution-specific use cases for MON.

Optimize traffic flows across standard and stretched segments on the private cloud side

In this scenario, VM1 is migrated to the cloud using the NE, which provides optimal VM to VM latency. As a result, VM1 needs low latency to VM3 on the local Azure VMware Solution segment. We migrate the VM1 gateway from on-premises to Azure VMware Solution (cloud) to ensure an optimal path for traffic (blue line). If the gateway remains on-premises (red line), a tromboning effect and higher latency are observed.

> **Note**
>
> When you enable MON without migrating the VM gateway to the cloud side, it doesn't ensure an optimal path for traffic flow. It also doesn't allow the evaluation of policy routes.



Optimize and avoid asymmetric traffic flows

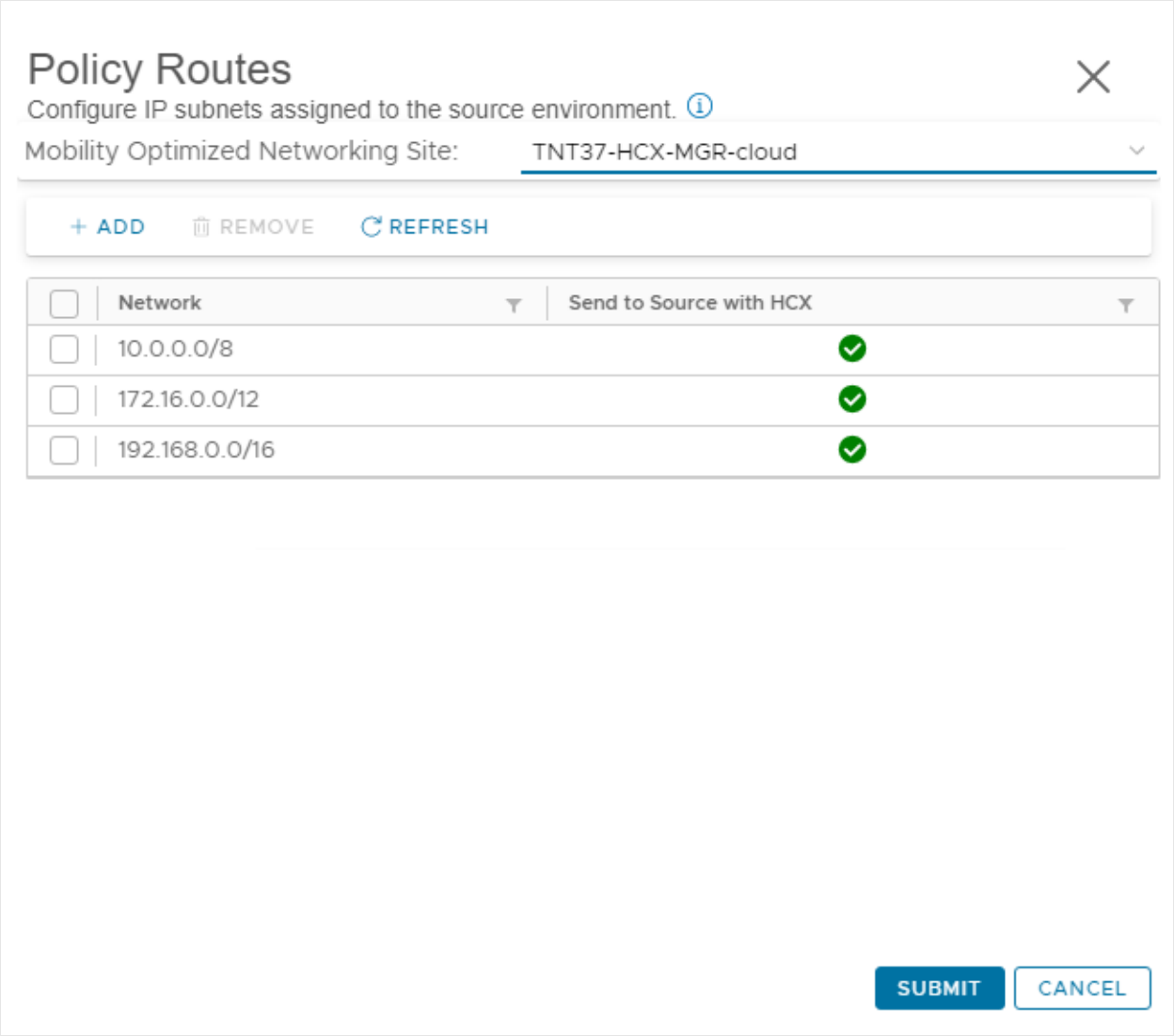
In this scenario, we assume a VM from on-premises is migrated to Azure VMware Solution and participates in L2, and L3 traffic flows back to on-premises to access services. We also assume some VM communication from Azure (in the Azure VMware Solution connected virtual network) could reach down in to the Azure VMware Solution private cloud.

> **Important**
>
> The main point here is to plan and avoid asymmetric traffic flows carefully.

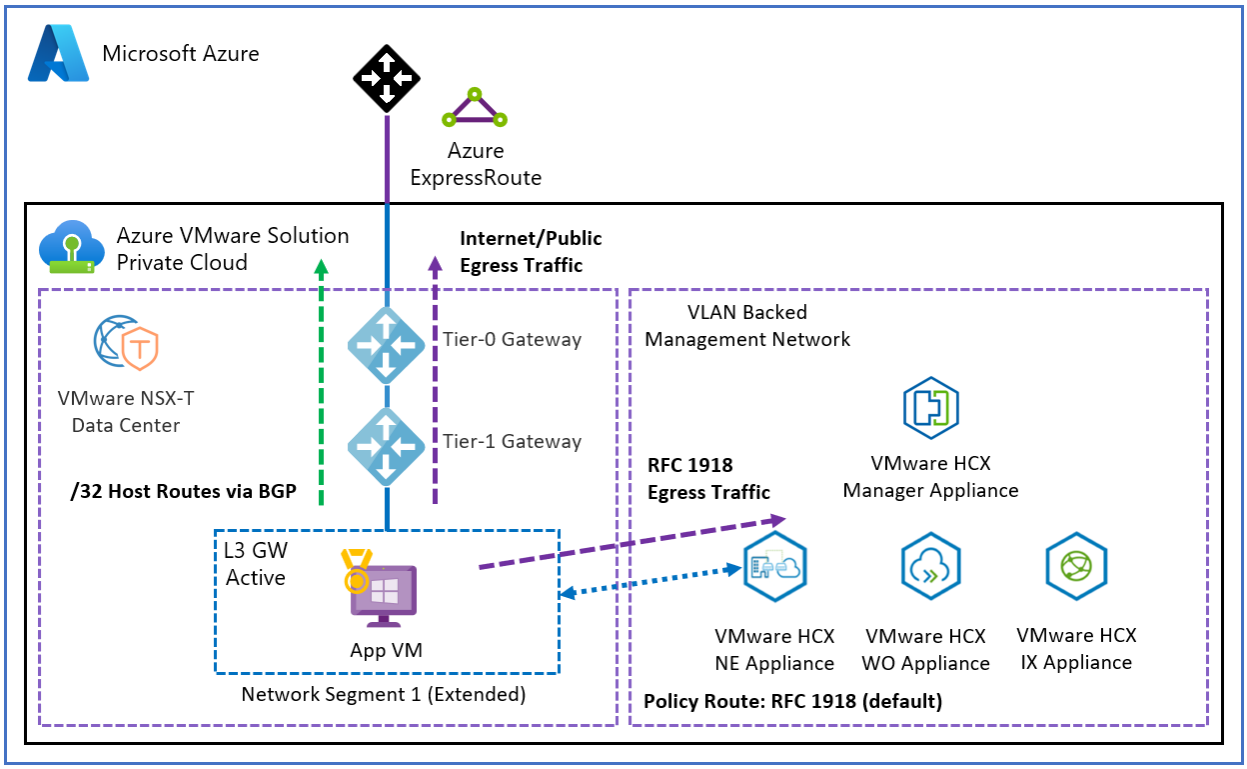
By default and without using MON, a VM in Azure VMware Solution on a stretched network without MON can communicate back to on-premises using the ExpressRoute preferred path. Based on customer use-cases, one should evaluate how a VM on an Azure VMware Solution stretched segment enabled with MON should be traversing back to on-premises, either over the Network Extension or the T0 gateway via the ExpressRoute while keeping traffic flows symmetric.

If choosing the NE path for example, the MON policy routes have to specifically address the subnet at the on-premises side; otherwise, the 0.0.0.0/0 default route is used. Policy routes can be found under the NE segment, by selecting advanced.

By default, all RFC 1918 IP addresses are included in the MON policy routes definition.



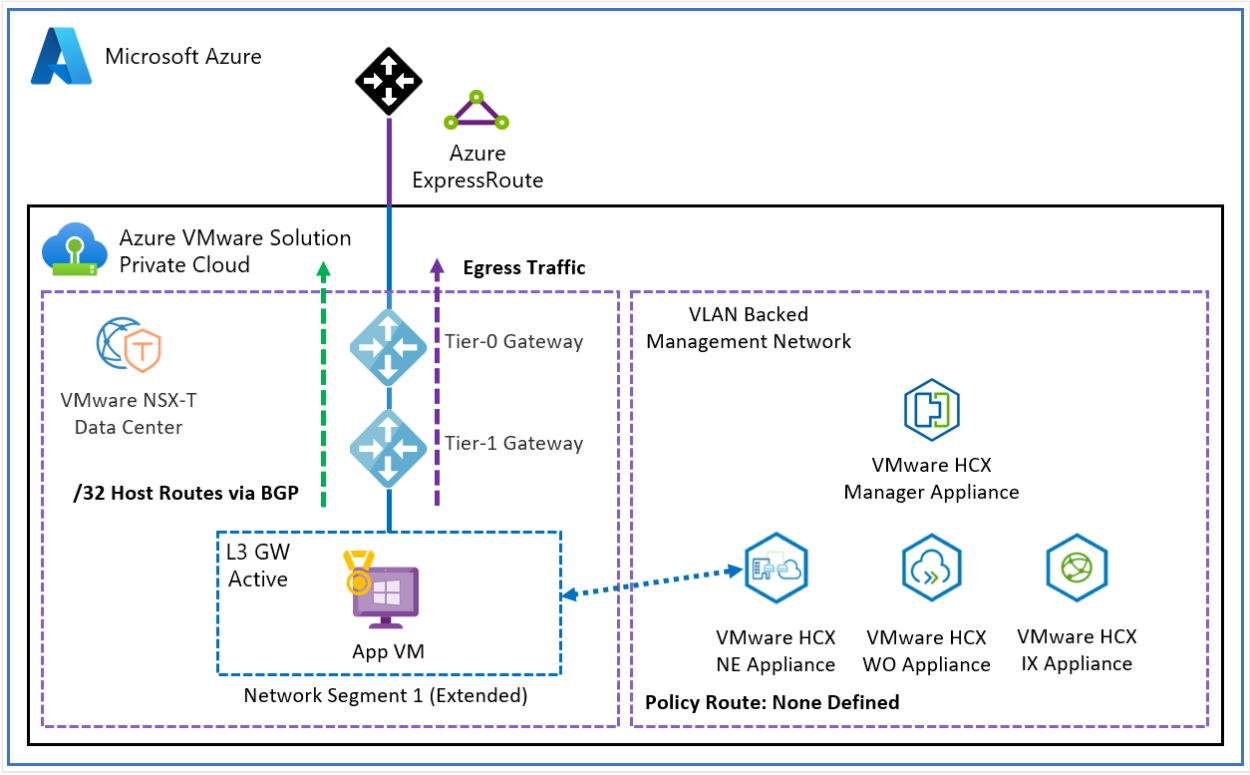
This results in all RFC 1918 egress traffic being tunneled over the NE path and all internet and public traffic being routed to the T0 gateway.



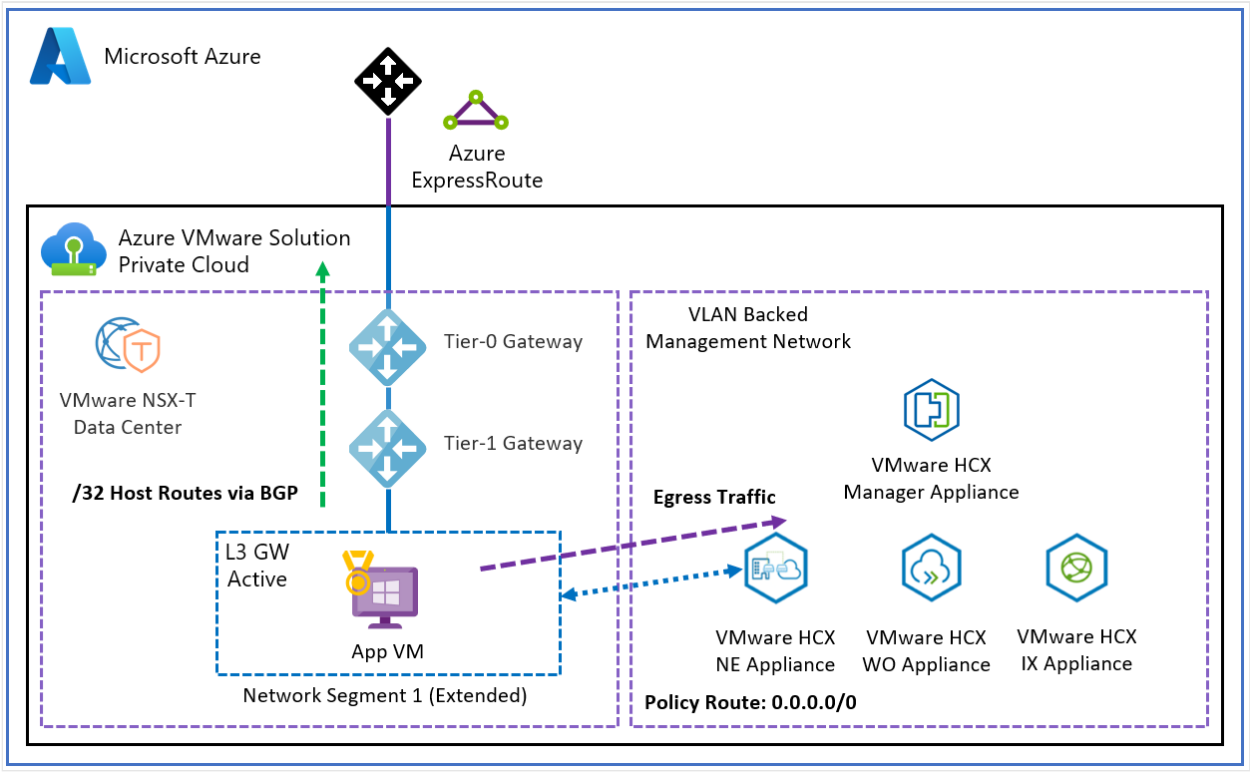
Policy routes are evaluated only if the VM gateway is migrated to the cloud. The effect of this configuration is that any matching subnets for the destination get tunneled over the NE appliance. If not matched, they get routed through the T0 gateway.

> **Note**
>
> Special consideration for using MON in Azure VMware Solution is to give the /32 routes advertised over BGP to its peers; this includes on-premises and Azure over the ExpressRoute connection. For example, a VM in Azure learns the path to an Azure VMware Solution VM on an Azure VMware Solution MON enabled segment. Once the return traffic is sent back to the T0 gateway as expected, if the return subnet is an RFC 1918 match, traffic is forced over the NE instead of the T0. Then egresses over the ExpressRoute back to Azure on the on-premises side. This can cause confusion for stateful firewalls in the middle and asymmetric routing behavior. It's also a good idea to determine how VMs on NE MON segments will need to access the internet, either via the T0 gateway in Azure VMware Solution or only through the NE back to on-premises. In general, all of the default policy routes should be removed to avoid asymmetric traffic. Only enable policy routes if the network infrastructure as been configured in such a way to account for and prevent asymmetric traffic.

The MON policy routes can be deleted with none defined. This results in all egress traffic being routed to the T0 gateway.



The MON policy routes can be updated with a default route (0.0.0.0/0). This results in all egress traffic being tunneled over the NE path.



As outlined in the above diagrams, the importance is to match a policy route to each required subnet. Otherwise, the traffic gets routed over the T0 and not tunneled over the NE.

To learn more about policy routes, see Mobility Optimized Networking Policy Routes.

Configure NSX network components using Azure VMware Solution

Article • 06/12/2024

An Azure VMware Solution private cloud comes with NSX by default. The private cloud comes pre-provisioned with an NSX Tier-0 gateway in **Active/Active** mode and a default NSX Tier-1 gateway in Active/Standby mode. These gateways let you connect the segments (logical switches) and provide East-West and North-South connectivity.

After deploying Azure VMware Solution, you can configure the necessary NSX objects from the Azure portal. It presents a simplified view of NSX operations a VMware administrator needs daily and is targeted at users not familiar with NSX Manager.

You have four options to configure NSX components in the Azure VMware Solution console:

- **Segments** - Create segments that display in NSX Manager and vCenter Server. For more information, see Add an NSX segment using the Azure portal.
- **DHCP** - Create a DHCP server or DHCP relay if you plan to use DHCP. For more information, see Use the Azure portal to create a DHCP server or relay.
- **Port mirroring** – Create port mirroring to help troubleshoot network issues. For more information, see Configure port mirroring in the Azure portal.
- **DNS** – Create a DNS forwarder to send DNS requests to a designated DNS server for resolution. For more information, see Configure a DNS forwarder in the Azure portal.

> **Important**
>
> You'll still have access to the NSX Manager console, where you can use the advanced settings mentioned and other NSX features.

Feedback

Was this page helpful? Yes No

Provide product feedback

Configure port mirroring in the Azure portal

Article • 12/08/2023

After deploying Azure VMware Solution, you can configure port mirroring from the Azure portal. Port mirroring places a protocol analyzer on the port that receives the mirrored data. It analyzes traffic from a source, a virtual machine (VM), or a group of VMs, and then sent to a defined destination. Use the following steps to configure port mirroring to monitor network traffic, which involves forwarding a copy of each packet from one network switch port to another.

> **Important**
>
> Port Mirroring is intended to be used as a temporary investigative tool and not a permanent network data collection feature. This is because NSX-T Data Center does not have the resources to port mirror all traffic continuously. The IPFIX feature should be used if a continuous meta-data network flow logging solution is required.

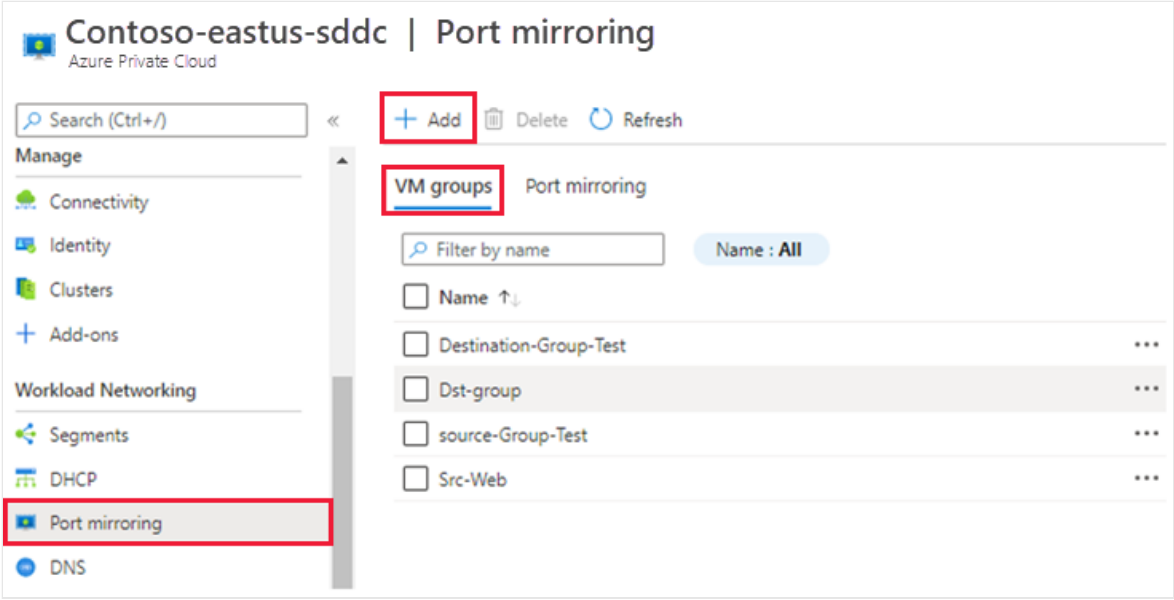
Prerequisites

An Azure VMware Solution private cloud with access to the vCenter Server and NSX-T Manager interfaces. For more information, see the Configure networking tutorial.

Create the VMs or VM groups

Create the source and destination VMs or VM groups. The source group has a single VM or multiple VMs where the traffic is mirrored.

1. In your Azure VMware Solution private cloud, under **Workload Networking**, select **Port mirroring** > **VM groups** > **Add**.



2. Provide a name for the new VM group, select VMs from the list, and then **OK**.

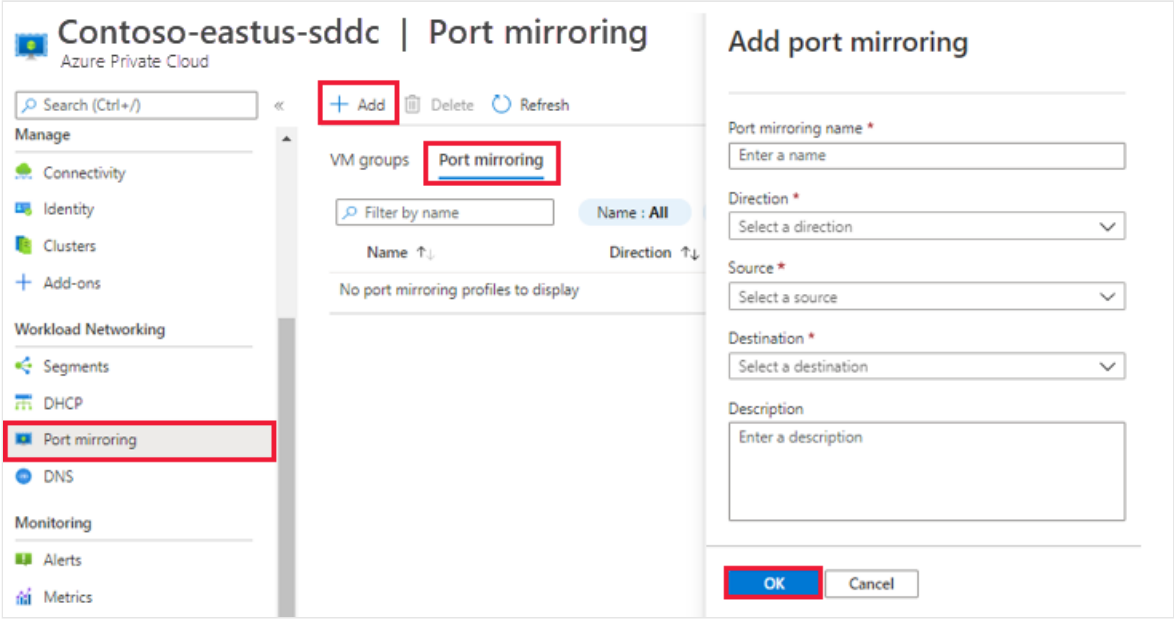
3. Repeat these steps to create the destination VM group.

> **Note**
>
> Before creating a port mirroring profile, make sure that you've created both the source and destination VM groups.

Create a port mirroring profile

Create a port mirroring profile that defines the traffic direction for the source and destination VM groups.

1. Select **Port mirroring** > **Port mirroring** > **Add** and then provide:



- **Port mirroring name** - Descriptive name for the profile.
- **Direction** - Select from Ingress, Egress, or Bi-directional.
- **Source** - Select the source VM group.
- **Destination** - Select the destination VM group.
- **Description** - Enter a description for the port mirroring.

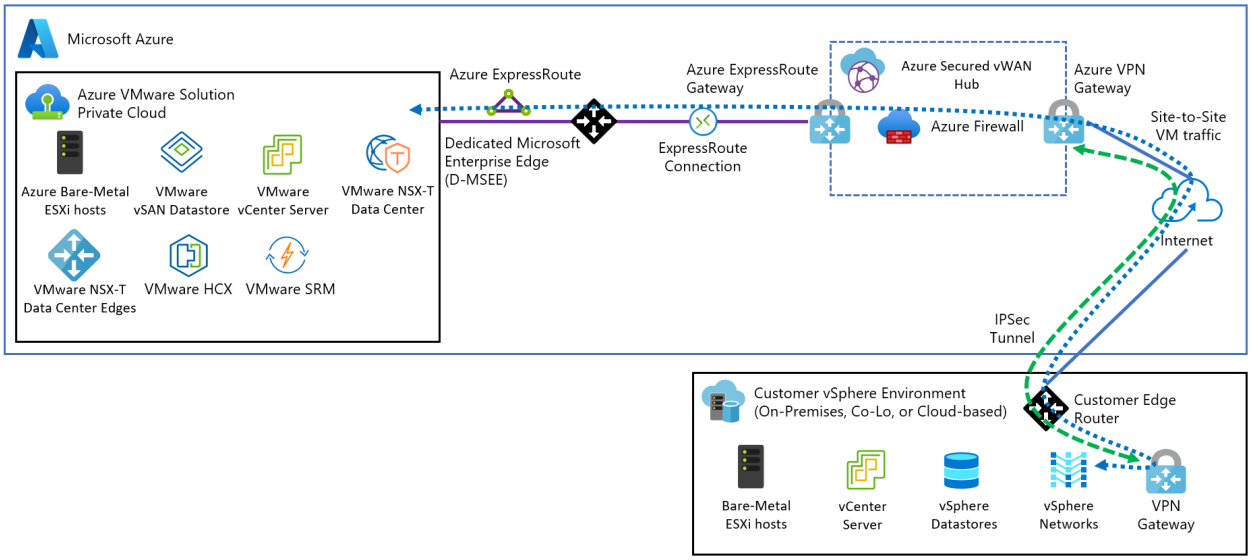
2. Select **OK** to complete the profile.

The profile and VM groups are visible in the Azure VMware Solution console.

Configure a site-to-site VPN in vWAN for Azure VMware Solution

Article • 02/27/2024

In this article, learn how to establish a VPN (IPsec IKEv1 and IKEv2) site-to-site tunnel terminating in the Microsoft Azure Virtual WAN hub. The hub contains the Azure VMware Solution ExpressRoute gateway and the site-to-site VPN gateway. It connects an on-premises VPN device with an Azure VMware Solution endpoint.



Prerequisites

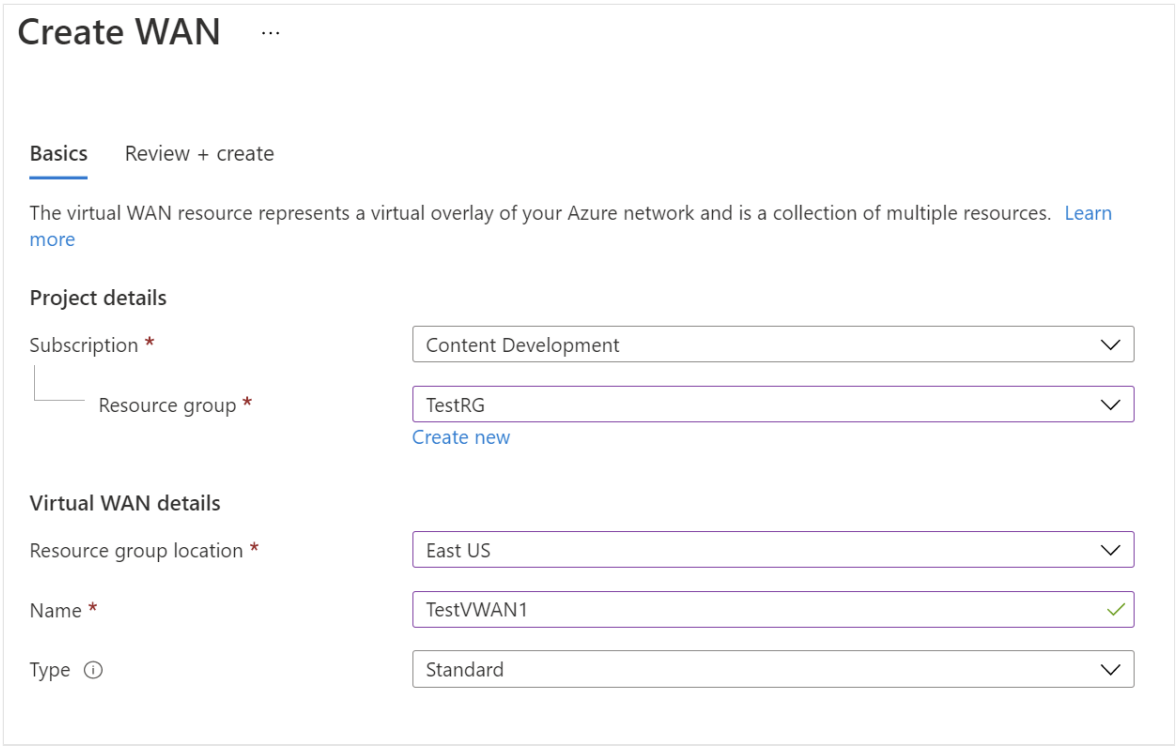
You must have a public-facing IP address terminating on an on-premises VPN device.

Create an Azure Virtual WAN

1. In the portal, in the **Search resources** bar, type **Virtual WAN** in the search box and select **Enter**.

2. Select **Virtual WANs** from the results. On the Virtual WANs page, select **+ Create** to open the **Create WAN** page.

3. On the **Create WAN** page, on the **Basics** tab, fill in the fields. Modify the example values to apply to your environment.



- **Subscription**: Select the subscription that you want to use.
- **Resource group**: Create new or use existing.
- **Resource group location**: Choose a resource location from the dropdown. A WAN is a global resource and doesn't live in a particular region. However, you must select a region in order to manage and locate the WAN resource that you create.
- **Name**: Type the Name that you want to call your virtual WAN.
- **Type**: Basic or Standard. Select **Standard**. If you select Basic, understand that Basic virtual WANs can only contain Basic hubs. Basic hubs can only be used for site-to-site connections.

4. After you finish filling out the fields, at the bottom of the page, select **Review +Create**.

5. Once validation passes, click **Create** to create the virtual WAN.

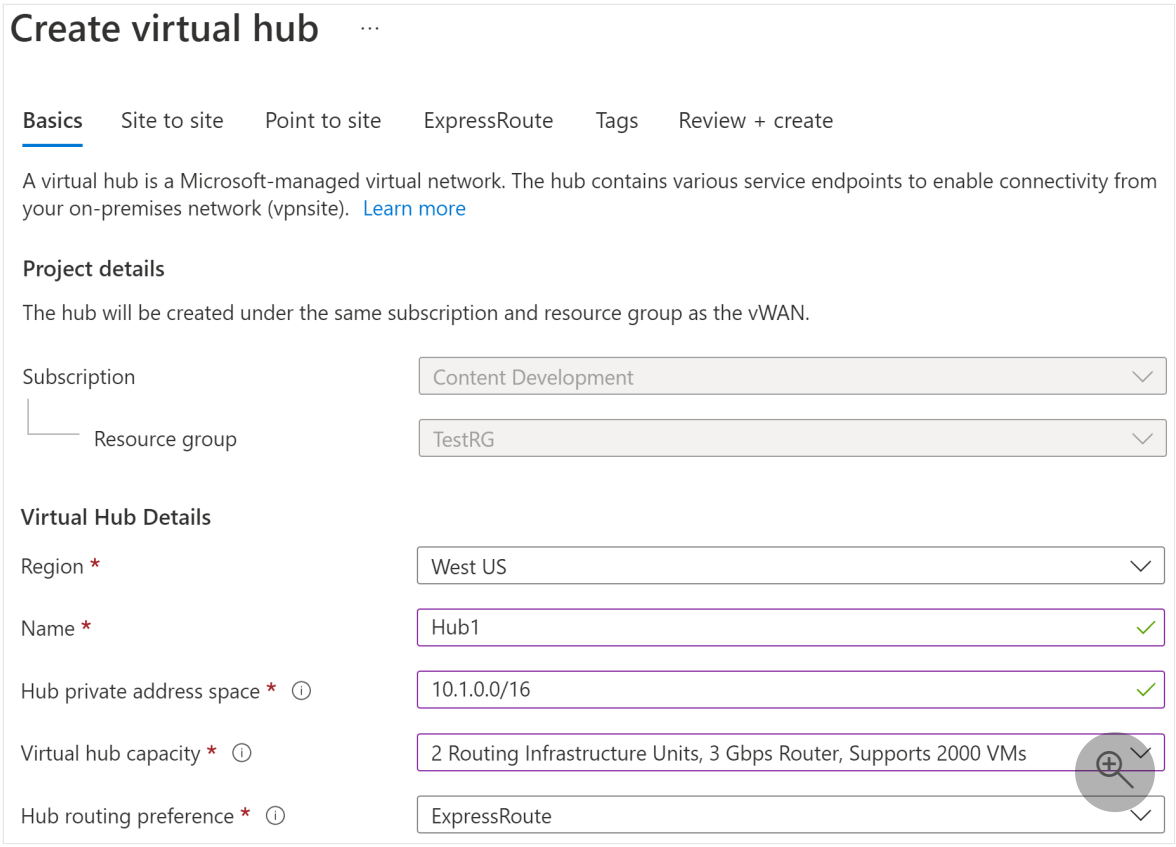
Create a virtual hub

A virtual hub is a virtual network that is created and used by Azure Virtual WAN. It's the core of your Virtual WAN network in a region. It can contain gateways for site-to-site and ExpressRoute.

> **Tip**
>
> You can also create a gateway in an existing hub.

1. Go to the virtual WAN that you created. On the virtual WAN page left pane, under the **Connectivity**, select **Hubs**.

2. On the **Hubs** page, select **+New Hub** to open the **Create virtual hub** page.

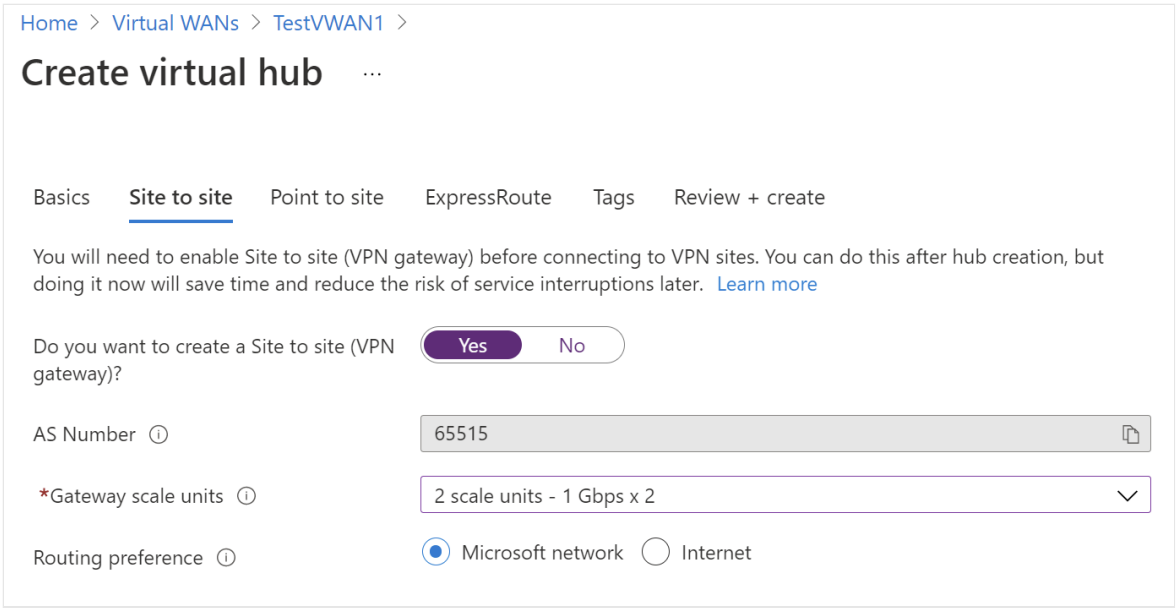


3. On the **Create virtual hub** page **Basics** tab, complete the following fields:

   - **Region**: Select the region in which you want to deploy the virtual hub.
   - **Name**: The name by which you want the virtual hub to be known.
   - **Hub private address space**: The hub's address range in CIDR notation. The minimum address space is /24 to create a hub.
   - **Virtual hub capacity**: Select from the dropdown. For more information, see Virtual hub settings.
   - **Hub routing preference**: Leave as default. For more information, see Virtual hub routing preference.

Create a VPN gateway

1. On the **Create virtual hub** page, click **Site to site** to open the **Site to site** tab.



2. On the **Site to site** tab, complete the following fields:

   - Select **Yes** to create a Site-to-site VPN.
   - **AS Number**: The AS Number field can't be edited.
   - **Gateway scale units**: Select the **Gateway scale units** value from the dropdown. The scale unit lets you pick the aggregate throughput of the VPN gateway being created in the virtual hub to connect sites to.

     If you pick 1 scale unit = 500 Mbps, it implies that two instances for redundancy will be created, each having a maximum throughput of 500 Mbps. For example, if you had five branches, each doing 10 Mbps at the branch, you'll need an aggregate of 50 Mbps at the head end. Planning for aggregate capacity of the Azure VPN gateway should be done after assessing the capacity needed to support the number of branches to the hub.

   - **Routing preference**: Azure routing preference lets you choose how your traffic routes between Azure and the internet. You can choose to route traffic either via the Microsoft network, or via the ISP network (public internet). These options are also referred to as cold potato routing and hot potato routing, respectively.

     The public IP address in Virtual WAN is assigned by the service, based on the routing option selected. For more information about routing preference via Microsoft network or ISP, see the Routing preference article.

3. Select **Review + Create** to validate.

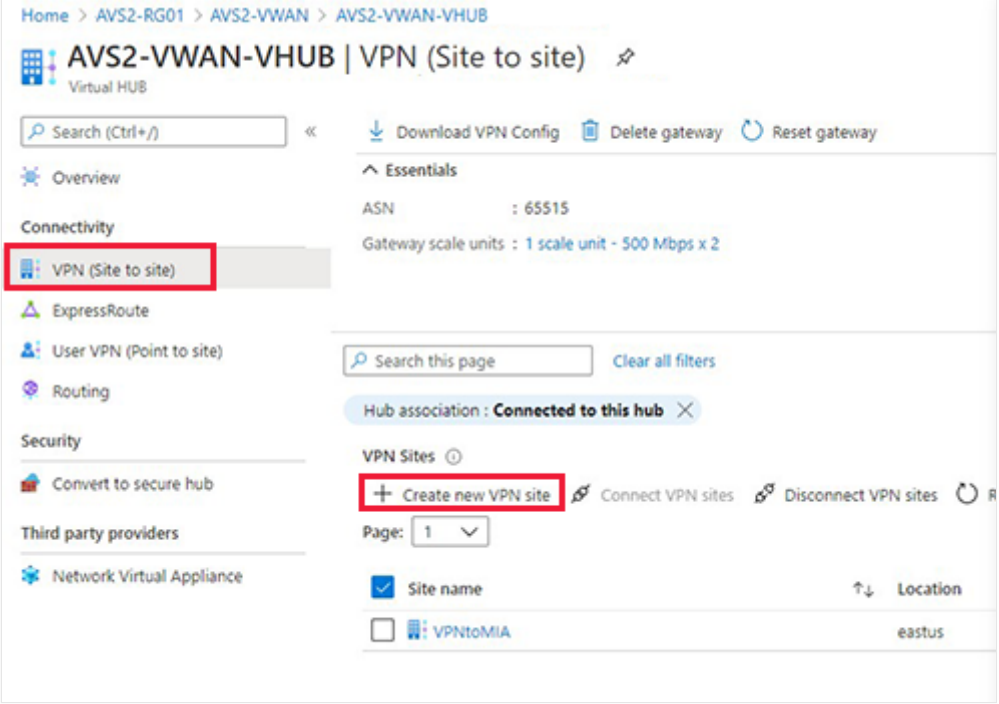
4. Select **Create** to create the hub and gateway. This can take up to 30 minutes. After 30 minutes, **Refresh** to view the hub on the **Hubs** page. Select **Go to resource** to

navigate to the resource.

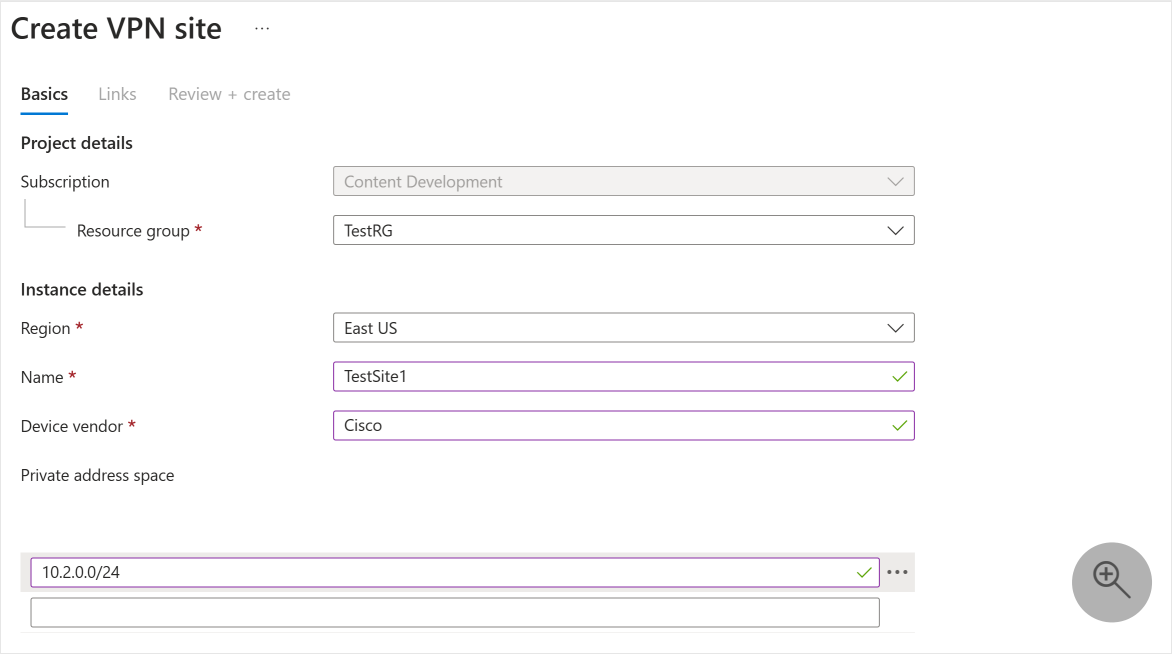
Create a site-to-site VPN

1. In the Azure portal, select the virtual WAN you created earlier.

2. In the **Overview** of the virtual hub, select **Connectivity** > **VPN (Site-to-site)** > **Create new VPN site**.



3. On the **Basics** tab, enter the required fields.



- **Region** - Previously referred to as location. It's the location you want to create this site resource in.

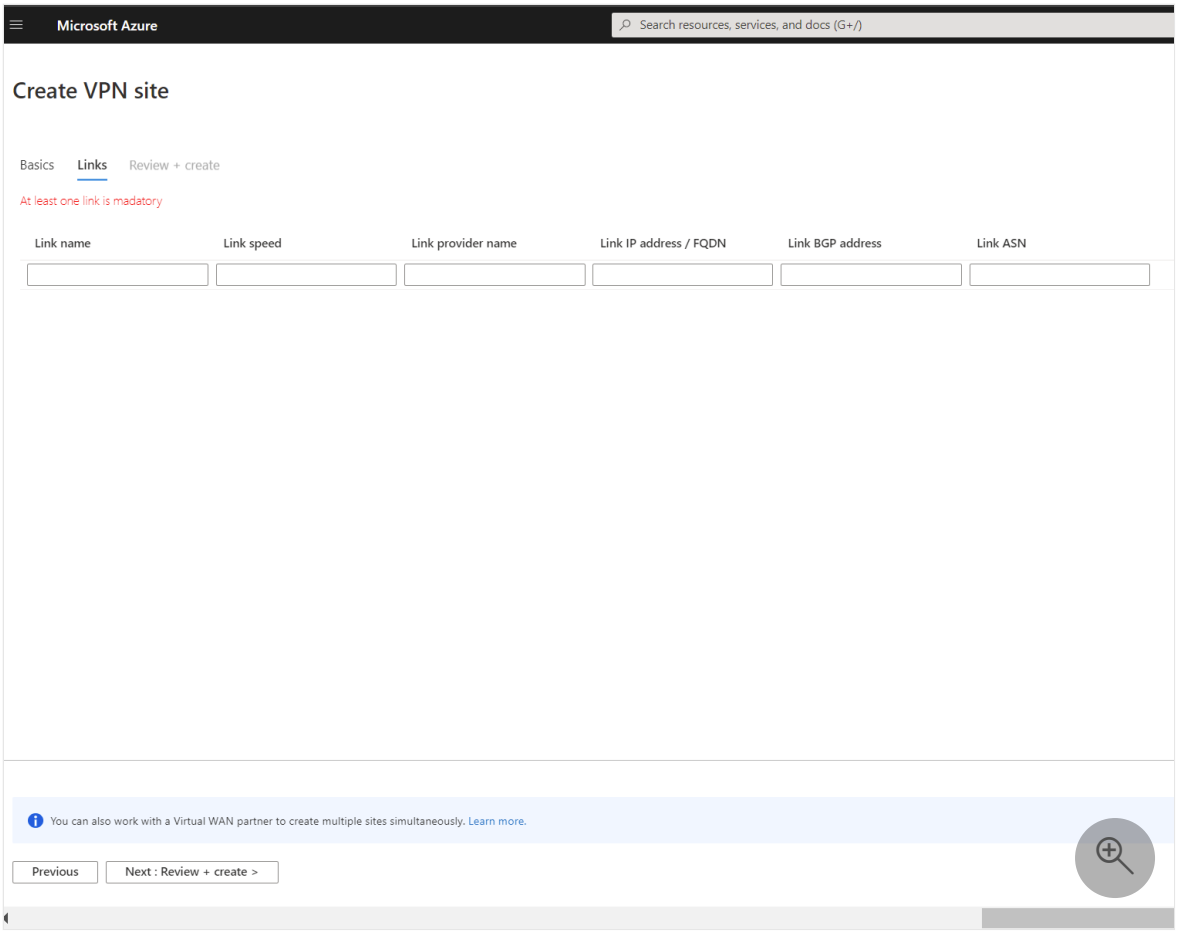
- **Name** - The name by which you want to refer to your on-premises site.
- **Device vendor** - The name of the VPN device vendor, for example, Citrix, Cisco, or Barracuda. It helps the Azure Team better understand your environment to add more optimization possibilities in the future or help you troubleshoot.
- **Private address space** - The CIDR IP address space located on your on-premises site. Traffic destined for this address space is routed to your local site. The CIDR block is only required if you BGP isn't enabled for the site.

> **Note**
>
> If you edit the address space after creating the site (for example, add an additional address space) it can take 8-10 minutes to update the effective routes while the components are recreated.

4. Select **Links** to add information about the physical links at the branch. If you have a Virtual WAN partner CPE device, check with them to see if this information gets exchanged with Azure as a part of the branch information upload set up from their systems.

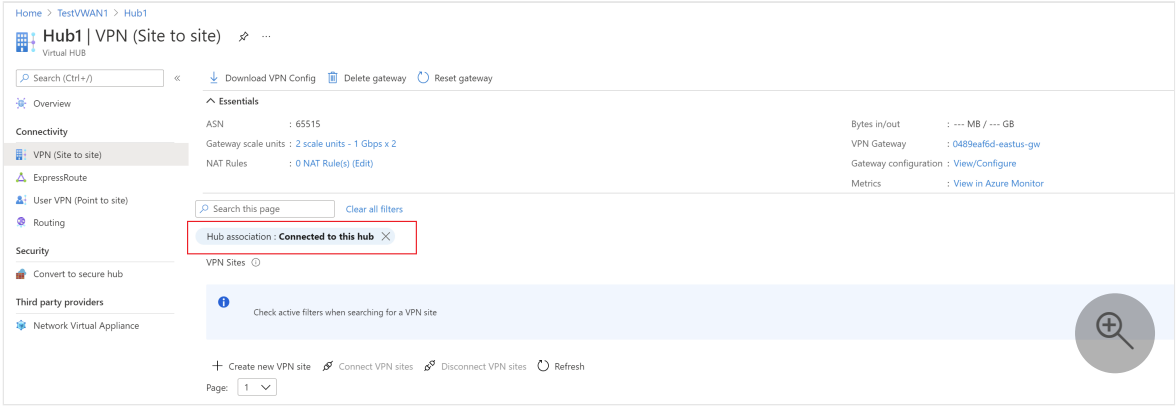
   Specifying link and provider names allow you to distinguish between any number of gateways that can eventually be created as part of the hub. BGP and autonomous system number (ASN) must be unique inside your organization. BGP ensures that both Azure VMware Solution and the on-premises servers advertise their routes across the tunnel. If disabled, the subnets that need to be advertised must be manually maintained. If subnets are missed, HCX fails to form the service mesh.

   > **Important**
   >
   > By default, Azure assigns a private IP address from the GatewaySubnet prefix range automatically as the Azure BGP IP address on the Azure VPN gateway. The custom Azure APIPA BGP address is needed when your on premises VPN devices use an APIPA address (169.254.0.1 to 169.254.255.254) as the BGP IP. Azure VPN Gateway will choose the custom APIPA address if the corresponding local network gateway resource (on-premises network) has an APIPA address as the BGP peer IP. If the local network gateway uses a regular IP address (not APIPA), Azure VPN Gateway will revert to the private IP address from the GatewaySubnet range.



5. Select **Review + create**.

6. Navigate to the virtual hub you want, and deselect **Hub association** to connect your VPN site to the hub.



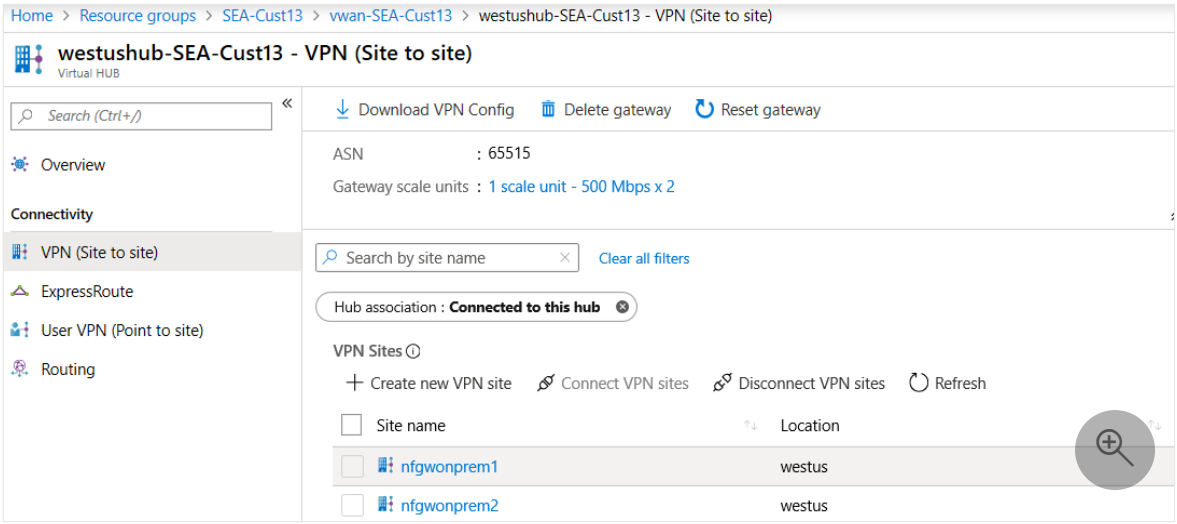
(Optional) Create policy-based VPN site-to-site tunnels

> **Important**
>
> This is an optional step and applies only to policy-based VPNs.

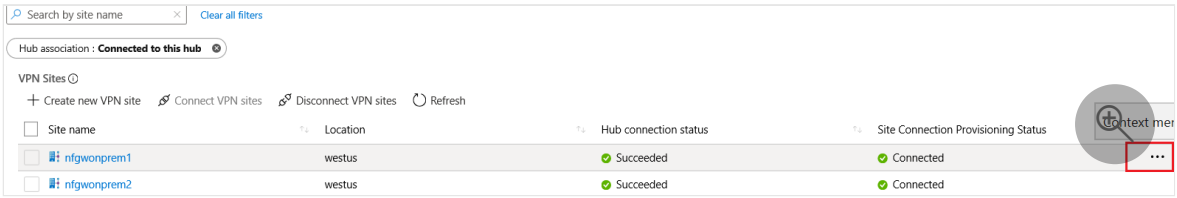
Policy-based VPN setups require on-premises and Azure VMware Solution networks to be specified, including the hub ranges. These ranges specify the encryption domain of the policy-based VPN tunnel on-premises endpoint. The Azure VMware Solution side only requires the policy-based traffic selector indicator to be enabled.

1. In the Azure portal, go to your Virtual WAN hub site and, under **Connectivity**, select **VPN (Site to site)**.

2. Select the VPN Site for which you want to set up a custom IPsec policy.

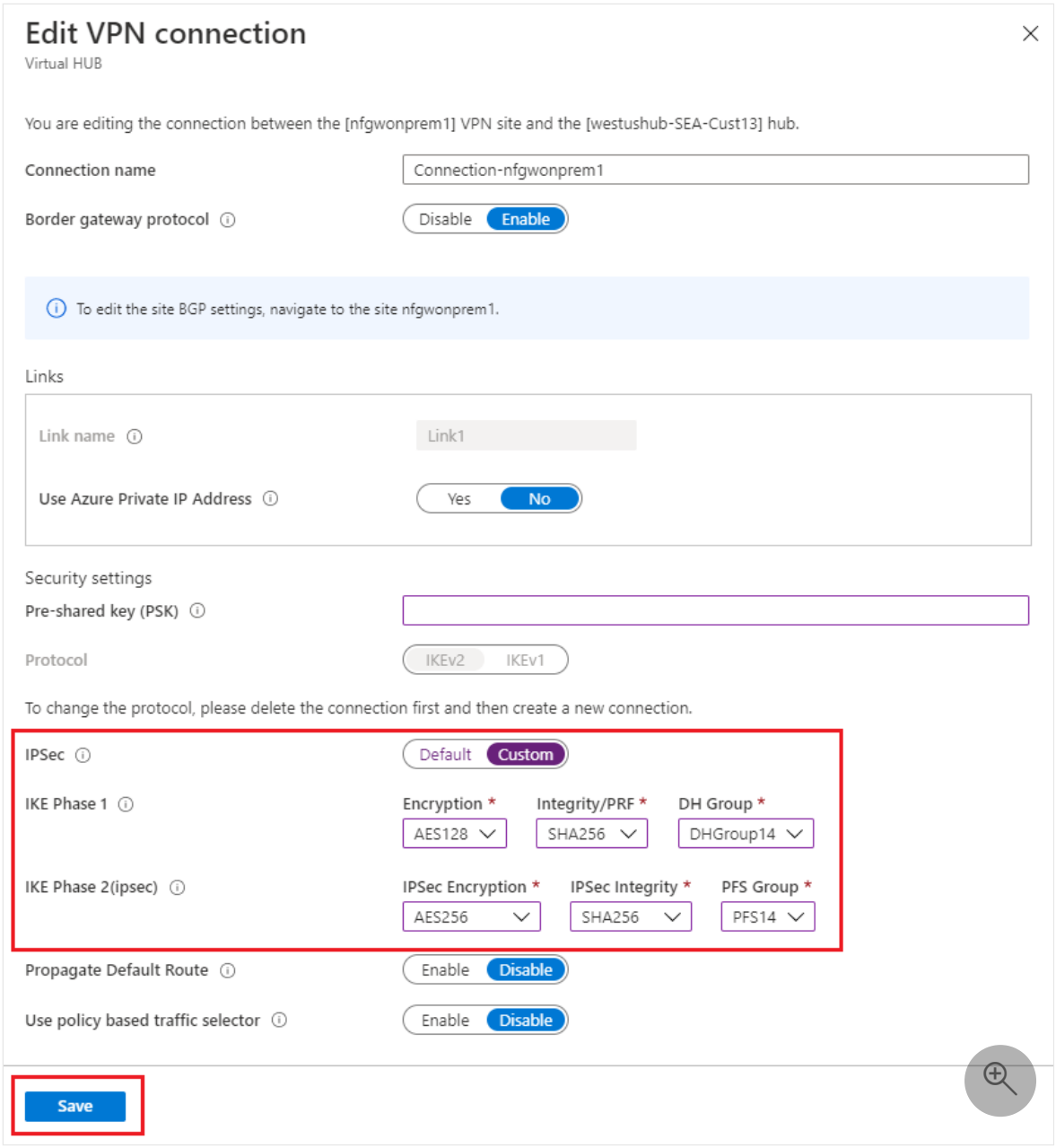


3. Select your VPN site name, select **More** (...) at the far right, and then select **Edit VPN Connection**.



   - Internet Protocol Security (IPSec), select **Custom**.
   - Use policy-based traffic selector, select **Enable**
   - Specify the details for **IKE Phase 1** and **IKE Phase 2(ipsec)**.

4. Change the IPsec setting from default to custom and customize the IPsec policy. Then select **Save**.



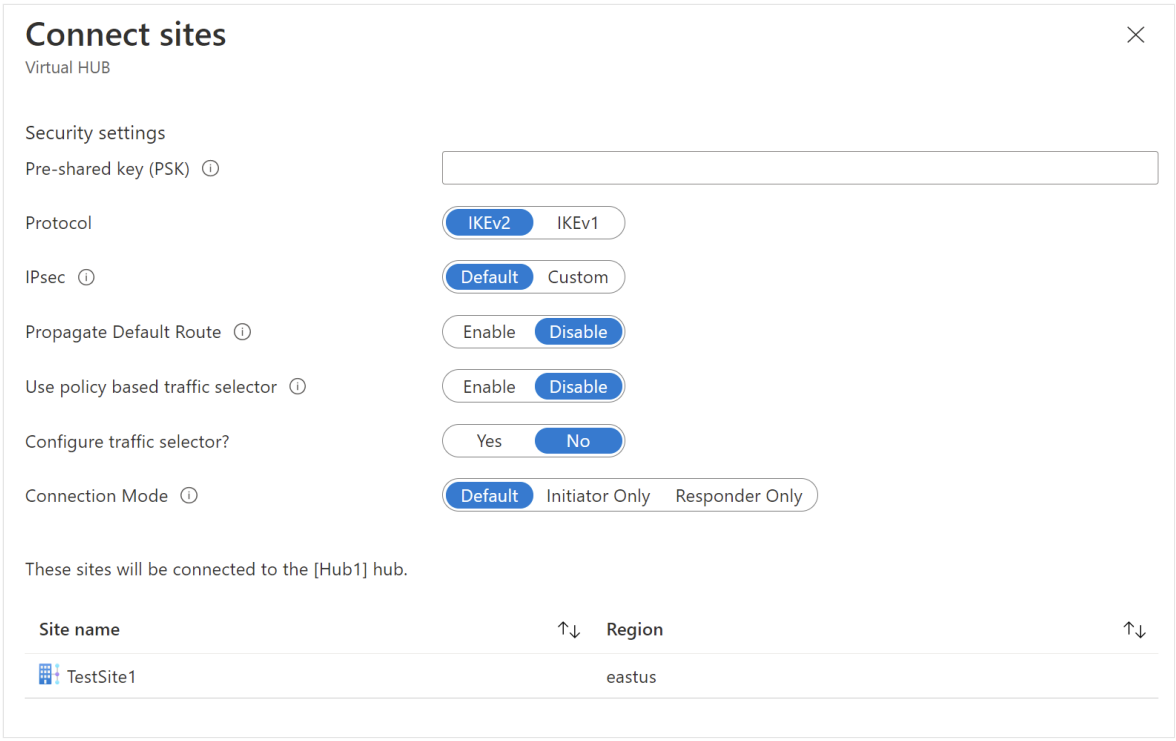
Your traffic selectors or subnets that are part of the policy-based encryption domain should be:

- Virtual WAN hub `/24`
- Azure VMware Solution private cloud `/22`
- Connected Azure virtual network (if present)

Connect your VPN site to the hub

1. Select your VPN site name and then select **Connect VPN sites**.
2. In the **Pre-shared key** field, enter the key previously defined for the on-premises endpoint.

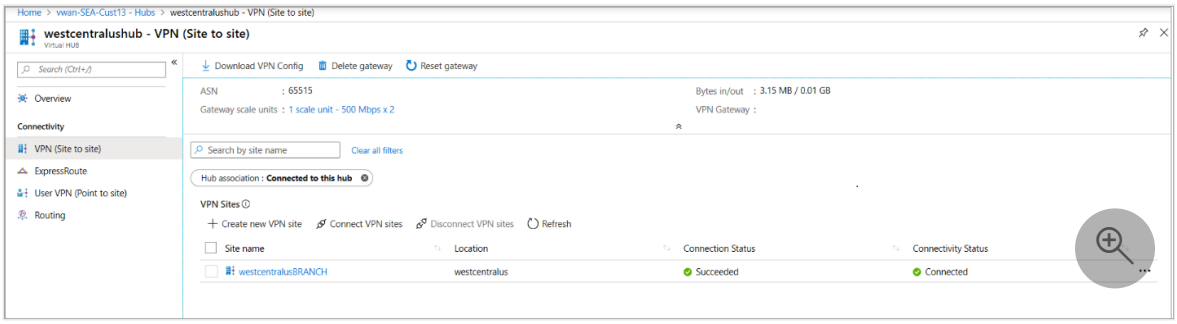
> **Tip**
>
> If you don't have a previously defined key, you can leave this field blank. A key is generated for you automatically.



3. If you're deploying a firewall in the hub and it's the next hop, set the **Propagate Default Route** option to **Enable**.

   When enabled, the Virtual WAN hub propagates to a connection only if the hub already learned the default route when deploying a firewall in the hub or if another connected site forced tunneling enabled. The default route doesn't originate in the Virtual WAN hub.

4. Select **Connect**. After a few minutes, the site shows the connection and connectivity status.



Connection Status: Status of the Azure resource for the connection that connects the VPN site to the Azure hub's VPN gateway. Once this control plane operation is

successful, the Azure VPN gateway and the on-premises VPN device establish connectivity.

Connectivity Status: Actual connectivity (data path) status between Azure's VPN gateway in the hub and VPN site. It can show any of the following states:

- **Unknown**: Typically seen if the backend systems are working to transition to another status.
- **Connecting**: Azure VPN gateway is trying to reach out to the actual on-premises VPN site.
- **Connected**: Connectivity established between Azure VPN gateway and on-premises VPN site.
- **Disconnected**: Typically seen if disconnected for any reason (on-premises or in Azure)

5. Download the VPN configuration file and apply it to the on-premises endpoint.

   a. On the VPN (Site to site) page, near the top, select **Download VPN Config**. Azure creates a storage account in the resource group 'microsoft-network-[location]', where location is the location of the WAN. After you apply the configuration to your VPN devices, you can delete this storage account.

   b. Once created, select the link to download it.

   c. Apply the configuration to your on-premises VPN device.

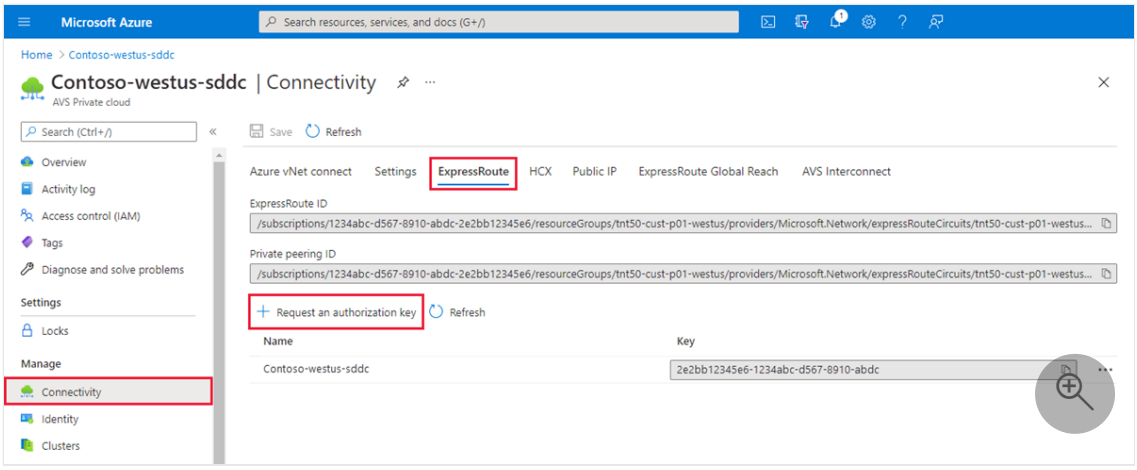
   For more information about the configuration file, see About the VPN device configuration file.

6. Patch the Azure VMware Solution ExpressRoute in the Virtual WAN hub.

   > **ⓘ Important**
   >
   > You must first have a private cloud created before you can patch the platform.

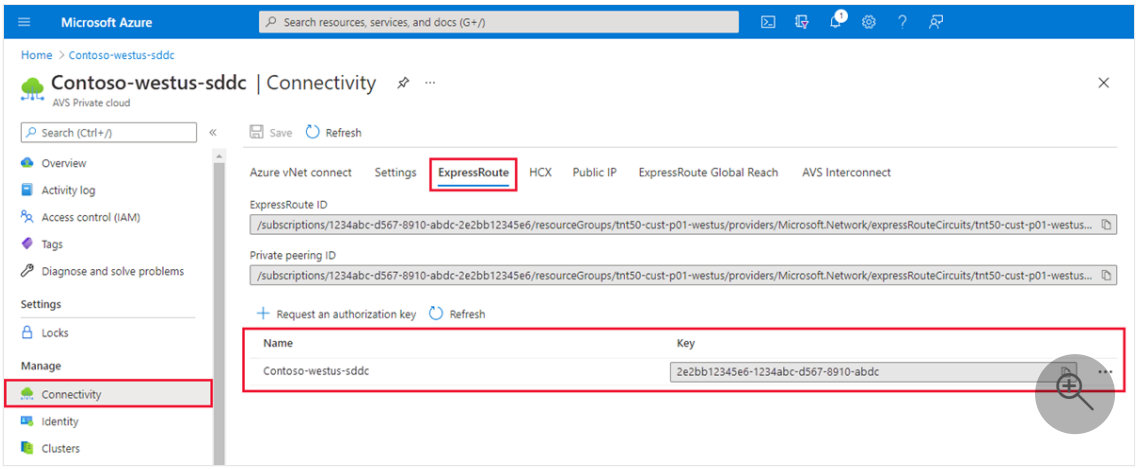
   > **ⓘ Important**
   >
   > You must also have an ExpressRoute Gateway configured as part of your Virtual WAN Hub.

   a. In the Azure portal, navigate to the Azure VMware Solution private cloud. Select **Manage** > **Connectivity** > **ExpressRoute** and then select **+ Request an authorization key**.



b. Provide a name for it and select **Create**.

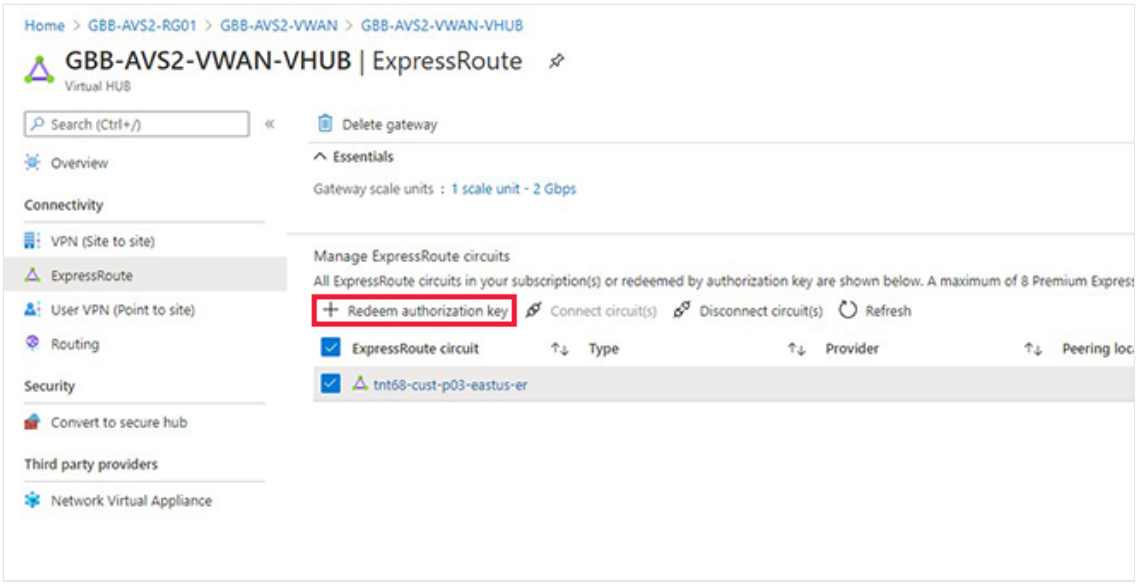
It can take about 30 seconds to create the key. Once created, the new key appears in the list of authorization keys for the private cloud.



c. Copy the authorization key and ExpressRoute ID. You need them to complete the peering. The authorization key disappears after some time, so copy it as soon as it appears.

7. Link Azure VMware Solution and the VPN gateway together in the Virtual WAN hub. You use the authorization key and ExpressRoute ID (peer circuit URI) from the previous step.

a. Select your ExpressRoute gateway and then select **Redeem authorization key**.



b. Paste the authorization key in the **Authorization Key** field.

c. Paste the ExpressRoute ID into the **Peer circuit URI** field.

d. Select **Automatically associate this ExpressRoute circuit with the hub** check box.

e. Select **Add** to establish the link.

8. Test your connection by creating an NSX-T Data Center segment and provisioning a VM on the network. Ping both the on-premises and Azure VMware Solution endpoints.

> **Note**
>
> Wait approximately 5 minutes before you test connectivity from a client behind your ExpressRoute circuit, for example, a VM in the VNet that you created earlier.

Turn on Managed SNAT for Azure VMware Solution workloads

Article • 03/22/2024

In this article, learn how to turn on Source Network Address Translation (SNAT) via the Azure VMware Solution Managed SNAT service to connect to outbound internet.

A SNAT service translates from an RFC 1918 space to the public internet for simple outbound internet access. Internet Control Message Protocol (ICMP) is turned off by design so that users can't ping an internet host. The SNAT service doesn't work when you have a default route from Azure.

The Managed SNAT service in Azure VMware Solution gives you:

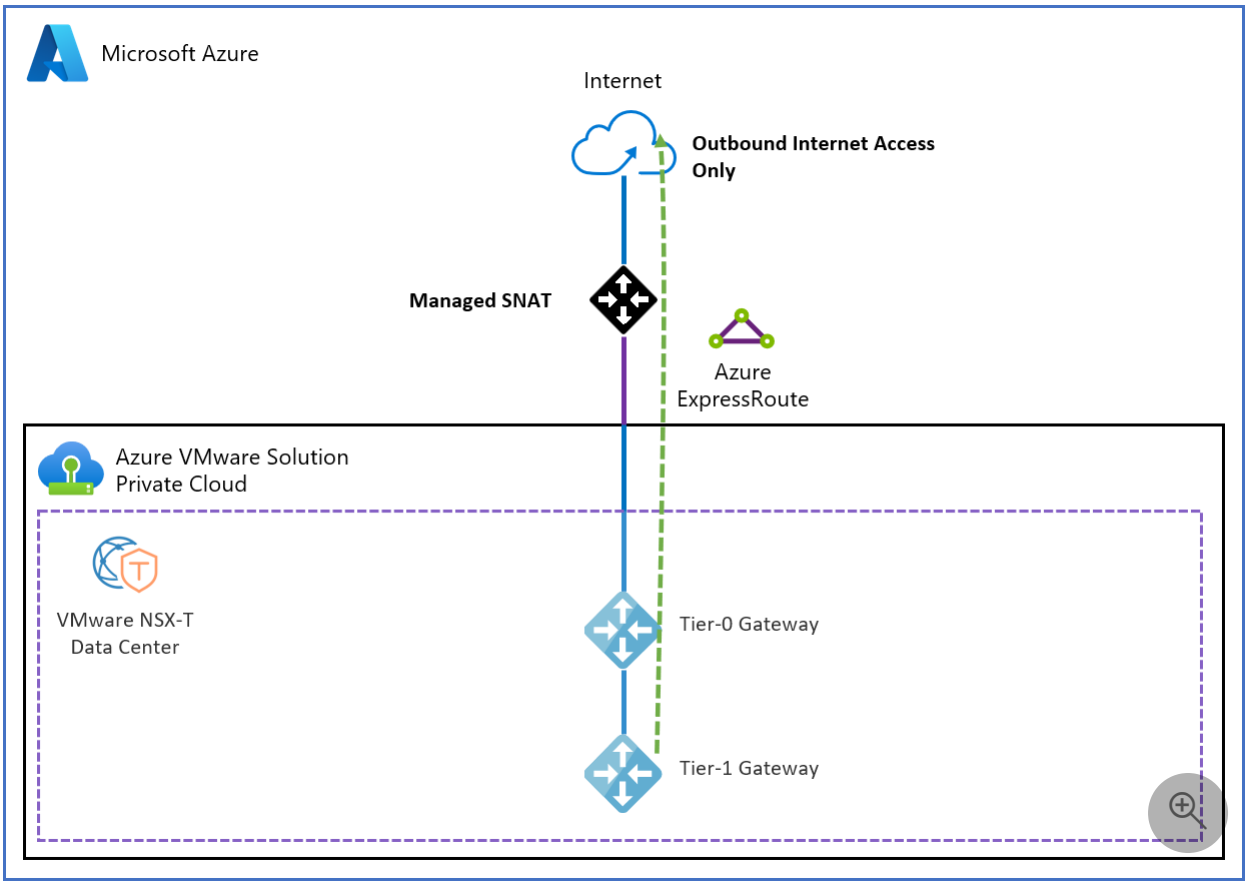
- A basic SNAT service with outbound internet connectivity from your Azure VMware Solution private cloud.
- A limit of 128,000 concurrent connections.

By using the Managed SNAT service, you *don't* have:

- Control of outbound SNAT rules.
- Control of the public IP address that's used.
- The ability to terminate inbound-initiated internet traffic.
- The ability to view connection logs.

Reference architecture

The following figure shows internet access that's outbound from your Azure VMware Solution private cloud via the Managed SNAT service in Azure VMware Solution.



Set up outbound internet access by using the Managed SNAT service

To set up outbound internet access via Managed SNAT, use the Azure portal:

1. Sign in to the Azure portal.
2. Search for **Azure VMware Solution**, and then select it in the search results.
3. Select your Azure VMware Solution private cloud.
4. On the resource menu under **Workload networking**, select **Internet connectivity**.
5. Select **Connect using SNAT**, and then select **Save**.

Related content

- Internet connectivity design considerations
- Turn on public IP addresses to an NSX-T Edge node for NSX-T Data Center
- Set a default internet route or disable internet access

Turn on public IP addresses to an NSX Edge node for VMware NSX

Article • 03/24/2024

In this article, learn how to turn on public IP addresses on a VMware NSX Edge node to run VMware NSX for your instance of Azure VMware Solution.

> **Tip**
>
> Before you turn on internet access to your instance of Azure VMware Solution, review **Internet connectivity design considerations**.

Public IP addresses to an NSX Edge node for NSX is a feature in Azure VMware Solution that turns on inbound and outbound internet access for your Azure VMware Solution environment.

> **Important**
>
> IPv4 public IP address usage can be consumed directly in Azure VMware Solution and charged based on the IPv4 public IP address prefix that's shown in **Pricing - Virtual machine IP addresses**. No charges for data ingress or egress are related to this service.

The public IP address range is configured in Azure VMware Solution through the Azure portal and the NSX interface within your Azure VMware Solution private cloud.

With this capability, you have the following features:

- A cohesive and simplified experience for reserving and using a public IP address to the NSX Edge node.
- The ability to receive 1,000 or more public IP addresses. Turn on internet access at scale.
- Inbound and outbound internet access for your workload VMs.
- Distributed denial-of-service (DDoS) security protection against network traffic to and from the internet.
- VMware HCX migration support over the public internet.

> **Important**

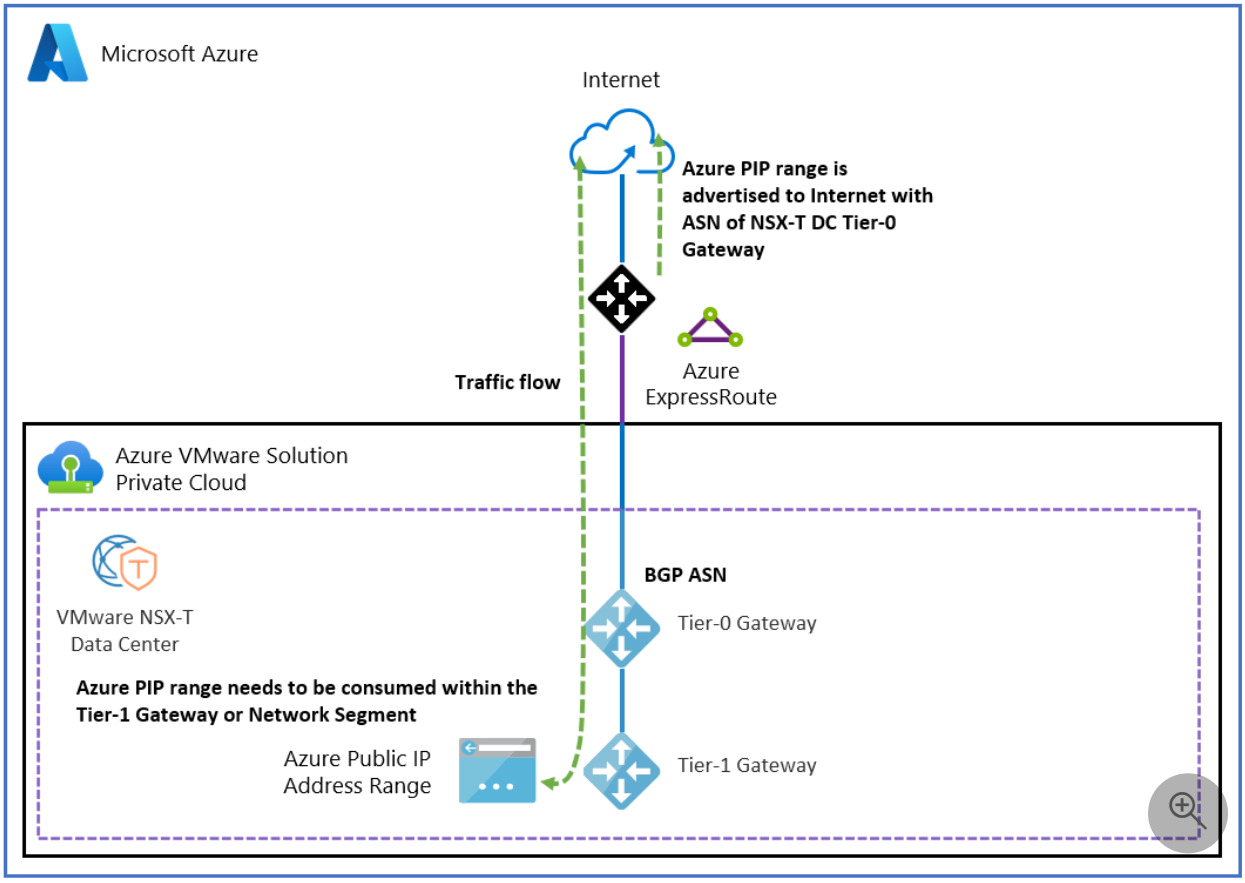
You can set up a maximum of 64 total public IP addresses across these network blocks. If you want to configure more than 64 public IP addresses, please submit a support ticket that indicates the number of addresses you need.

Prerequisites

- An Azure VMware Solution private cloud.
- A DNS server set up for your instance of NSX.

Reference architecture

The following figure shows internet access to and from your Azure VMware Solution private cloud via a public IP address directly to the NSX Edge node for NSX.



Important

Using a public IP address at the NSX Edge node for NSX is not compatible with reverse DNS lookup. If you use this scenario, you can't host a mail server in Azure VMware Solution.

Set up a public IP address or range

To set up a public IP address or range, use the Azure portal:

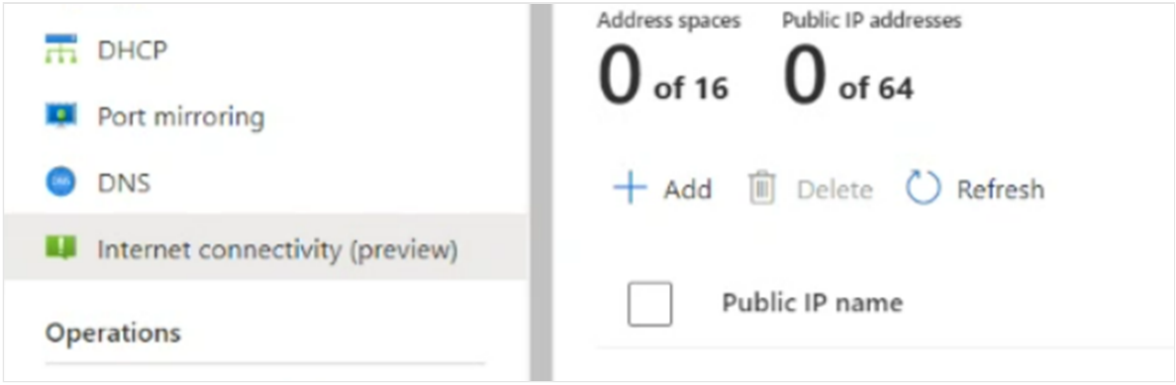
1. Sign in to the Azure portal, and then go to your Azure VMware Solution private cloud.

2. On the resource menu under **Workload networking**, select **Internet connectivity**.

3. Select the **Connect using Public IP down to the NSX Edge** checkbox.

   > **ⓘ Important**
   >
   > Before you select a public IP address, ensure that you understand the implications to your existing environment. For more information, see **Internet connectivity design considerations**. Considerations should include a risk mitigation review with your relevant networking and security governance and compliance teams.

4. Select **Public IP**.



5. Enter a value for **Public IP name**. In the **Address space** dropdown list, select a subnet size. Then, select **Configure**.

   This public IP address is available within approximately 20 minutes.

   Check that the subnet is listed. If you don't see the subnet, refresh the list. If the refresh fails to display the subnet, try the configuration again.

6. After you set the public IP address, select the **Connect using the public IP down to the NSX Edge** checkbox to turn off all other internet options.

7. Select **Save**.

You successfully turned on internet connectivity for your Azure VMware Solution private cloud and reserved a Microsoft-allocated public IP address. You can now set this public IP address to the NSX Edge node for NSX to use for your workloads. NSX is used for all virtual machine (VM) communication.

You have three options for configuring your reserved public IP address to the NXS Edge node for NSX:

- Outbound internet access for VMs
- Inbound internet access for VMs
- A gateway firewall to filter traffic to VMs at T1 gateways

Outbound internet access for VMs

A Source Network Address Translation (SNAT) service with Port Address Translation (PAT) is used to allow many VMs to use one SNAT service. Using this type of connection means that you can provide internet connectivity for many VMs.

> **ⓘ Important**
>
> To enable SNAT for your specified address ranges, you must **configure a gateway firewall rule** and SNAT for the specific address ranges that you want to use. If you don't want SNAT turned on for specific address ranges, you must create a **No-NAT rule** for address ranges to exclude from Network Address Translation (NAT). For your SNAT service to work as expected, the No-NAT rule should be a lower priority than the SNAT rule.

Create a SNAT rule

1. In your Azure VMware Solution private cloud, select **VMware credentials**.

2. Locate your NSX Manager URL and credentials.

3. Sign in to VMware NSX Manager.

4. Go to **NAT Rules**.

5. Select the T1 router.

6. Select **Add NAT Rule**.
7. Enter a name for the rule.
8. Select **SNAT**.

   Optionally, enter a source, such as a subnet to SNAT or a destination.
9. Enter the translated IP address. This IP address is from the range of public IP addresses that you reserved in the Azure VMware Solution portal.

   Optionally, give the rule a higher-priority number. This prioritization moves the rule further down the rule list to ensure that more specific rules are matched first.
10. Select **Save**.

Logging is turned on via the logging slider.

For more information on VMware NSX NAT configuration and options, see the NSX Data Center NAT Administration Guide.

Create a No-NAT rule

You can create a No-NAT or No-SNAT rule in NSX Manager to exclude certain matches from performing NAT. This policy can be used to allow private IP address traffic to bypass existing network translation rules.

1. In your Azure VMware Solution private cloud, select **VMware credentials**.
2. Locate your NSX Manager URL and credentials.
3. Sign in to NSX Manager, and then select **NAT Rules**.
4. Select the T1 router, and then select **Add NAT Rule**.
5. Select **No SNAT** rule as the type of NAT rule.
6. Select the **Source IP** value as the range of addresses that you don't want to be translated. The **Destination IP** value should be any internal addresses that you're reaching from the range of source IP address ranges.
7. Select **Save**.

Inbound internet access for VMs

A Destination Network Translation (DNAT) service is used to expose a VM on a specific public IP address or on a specific port. This service provides inbound internet access to your workload VMs.

Create a DNAT rule

1. In your Azure VMware Solution private cloud, select **VMware credentials**.
2. Locate your NSX Manager URL and credentials.
3. Sign in to NSX Manager, and then select **NAT Rules**.
4. Select the T1 router, and then select **Add DNAT Rule**.
5. Enter a name for the rule.
6. Select **DNAT** as the action.
7. For the destination match, enter the reserved public IP address. This IP address is from the range of public IP addresses that are reserved in the Azure VMware Solution portal.
8. For the translated IP, enter the VM private IP address.
9. Select **Save**.

   Optionally, configure the translated port or the source IP address for more specific matches.

The VM is now exposed to the internet on the specific public IP address or on specific ports.

Set up a gateway firewall to filter traffic to VMs at T1 gateways

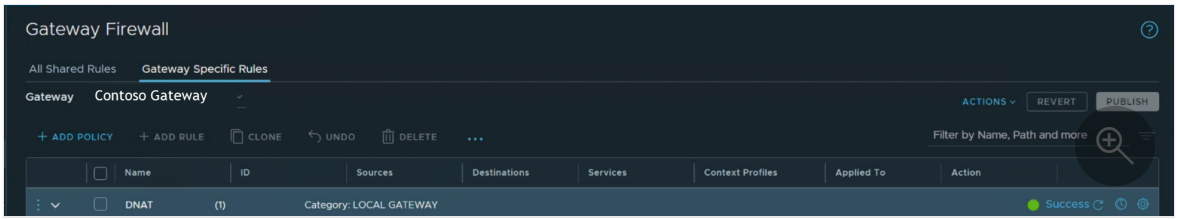
You can provide security protection for your network traffic in and out of the public internet through your gateway firewall.

1. In your Azure VMware Solution private cloud, select **VMware credentials**.
2. Locate your NSX Manager URL and credentials.
3. Sign in to NSX Manager.
4. On the NSX overview page, select **Gateway Policies**.
5. Select **Gateway Specific Rules**, choose the T1 gateway, and then select **Add Policy**.
6. Select **New Policy** and enter a policy name.
7. Select the policy and select **Add Rule**.

8. Configure the rule:
    a. Select **New Rule**.
    b. Enter a descriptive name.
    c. Configure the source, destination, services, and action.

9. Select **Match External Address** to apply firewall rules to the external address of a NAT rule.

    For example, the following rule is set to **Match External Address**. The setting allows Secure Shell (SSH) traffic inbound to the public IP address.



If **Match Internal Address** was specified, the destination is the internal or private IP address of the VM.

For more information on the NSX gateway firewall, see the NSX Gateway Firewall Administration Guide. The distributed firewall can be used to filter traffic to VMs. For more information, see NSX Distributed Firewall Administration Guide.

Related content

- Internet connectivity design considerations
- Turn on Managed SNAT for Azure VMware Solution workloads
- Set a default internet route or turn off internet access
- Turn on VMware HCX access over the internet

Set a default internet route or turn off internet access

Article • 03/22/2024

In this article, learn how to set a default internet route or turn off internet access in your Azure VMware Solution private cloud.

You have multiple options to set up a default internet access route. You can use a virtual WAN hub or a network virtual appliance (NVA) in a virtual network, or you can use a default route from an on-premises environment. If you don't set a default route, your Azure VMware Solution private cloud has no internet access.

With a default route set, you can achieve the following tasks:

- Turn off internet access to your Azure VMware Solution private cloud.

  > **Note**
  >
  > Ensure that a default route is not advertised from on-premises or from Azure. An advertised default route overrides this setup.

- Turn on internet access by generating a default route from Azure Firewall or from a third-party NVA.

Prerequisites

- An Azure VMware Solution private cloud.
- If internet access is required, a default route must be advertised from an instance of Azure Firewall, an NVA, or a virtual WAN hub.

Set a default internet access route

To set a default internet access route or to turn off internet access, use the Azure portal:

1. Sign in to the Azure portal.
2. Search for **Azure VMware Solution**, and then select it in the search results.
3. Find and select your Azure VMware Solution private cloud.
4. On the resource menu under **Workload networking**, select **Internet connectivity**.

5. Select the **Connect using default route from Azure** option or the **Don't connect using default route from Azure** option, and then select **Save**.

If you don't have a default route from on-premises or from Azure, by completing the preceding steps, you turned off internet connectivity to your Azure VMware Solution private cloud.

Related content

- Internet connectivity design considerations
- Turn on Managed SNAT for Azure VMware Solution workloads
- Turn on public IP addresses to an NSX-T Edge node for NSX-T Data Center

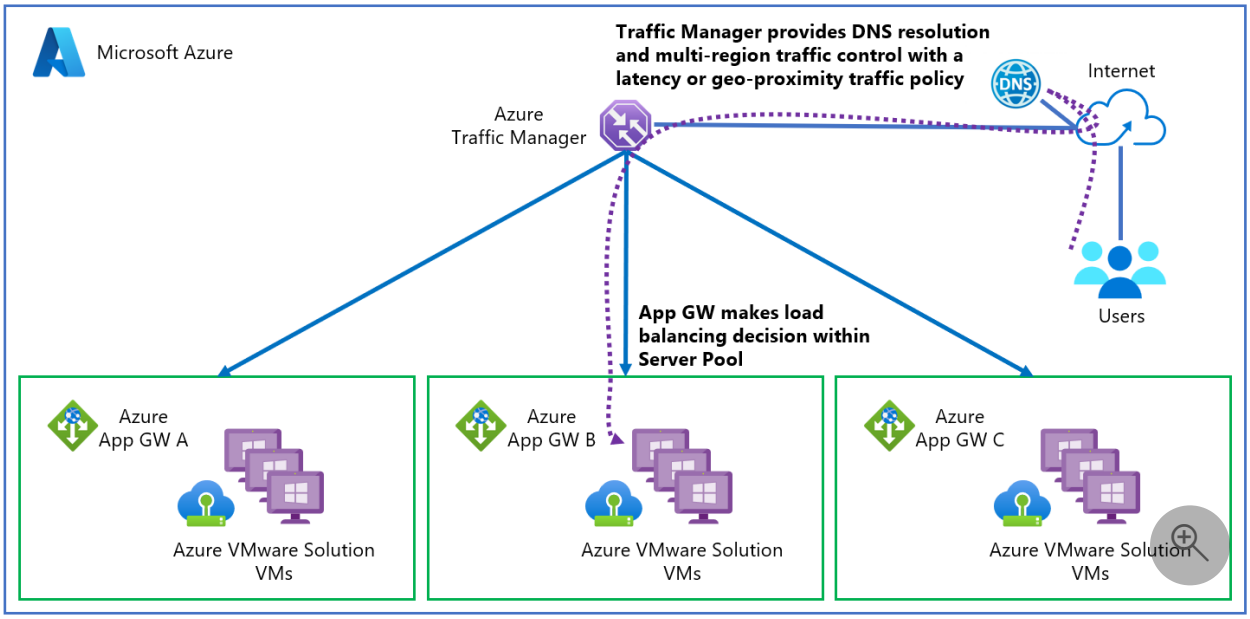
Deploy Azure Traffic Manager to balance Azure VMware Solution workloads

Article • 03/22/2024

This article walks through the steps of how to integrate Azure Traffic Manager with Azure VMware Solution. The integration balances application workloads across multiple endpoints. This article also walks through the steps of how to configure Traffic Manager to direct traffic between three Azure Application Gateway spanning several Azure VMware Solution regions.

The gateways have Azure VMware Solution virtual machines (VMs) configured as backend pool members to load balance the incoming layer 7 requests. For more information, see Use Azure Application Gateway to protect your web apps on Azure VMware Solution

The diagram shows how Traffic Manager provides load balancing for the applications at the DNS level between regional endpoints. The gateways have backend pool members configured as IIS Servers and referenced as Azure VMware Solution external endpoints. Connection over the virtual network between the three private cloud regions uses an ExpressRoute gateway.



Before you begin, review the Prerequisites list, then go through the following procedures:

- ✓ Verify configuration of your application gateways and the NSX segment
- ✓ Create your Traffic Manager profile

✔ Add external endpoints into your Traffic Manager profile

Prerequisites

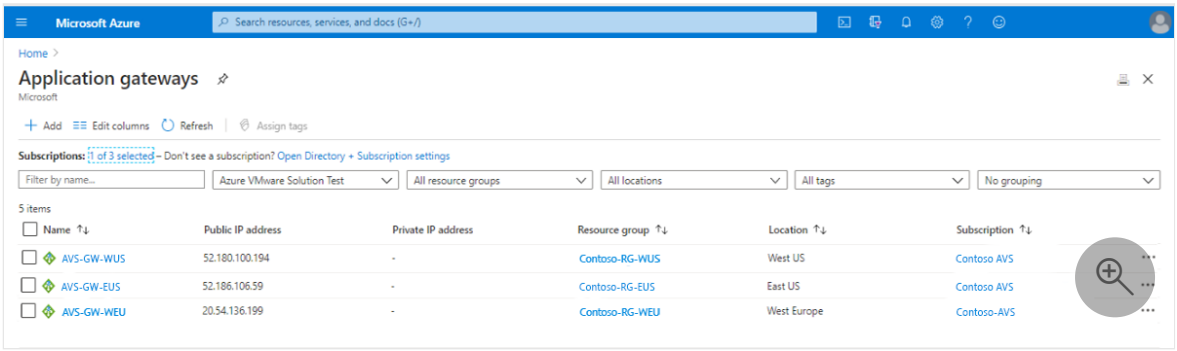
- Three VMs configured as Microsoft IIS Servers running in different Azure VMware Solution regions:
  - West US
  - West Europe
  - East US (on-premises)
- An application gateway with external endpoints in the Azure VMware Solution regions previously mentioned.
- Host with internet connectivity for verification.
- An NSX network segment created in Azure VMware Solution.

Verify your application gateways configuration

The following steps verify the configuration of your application gateways.

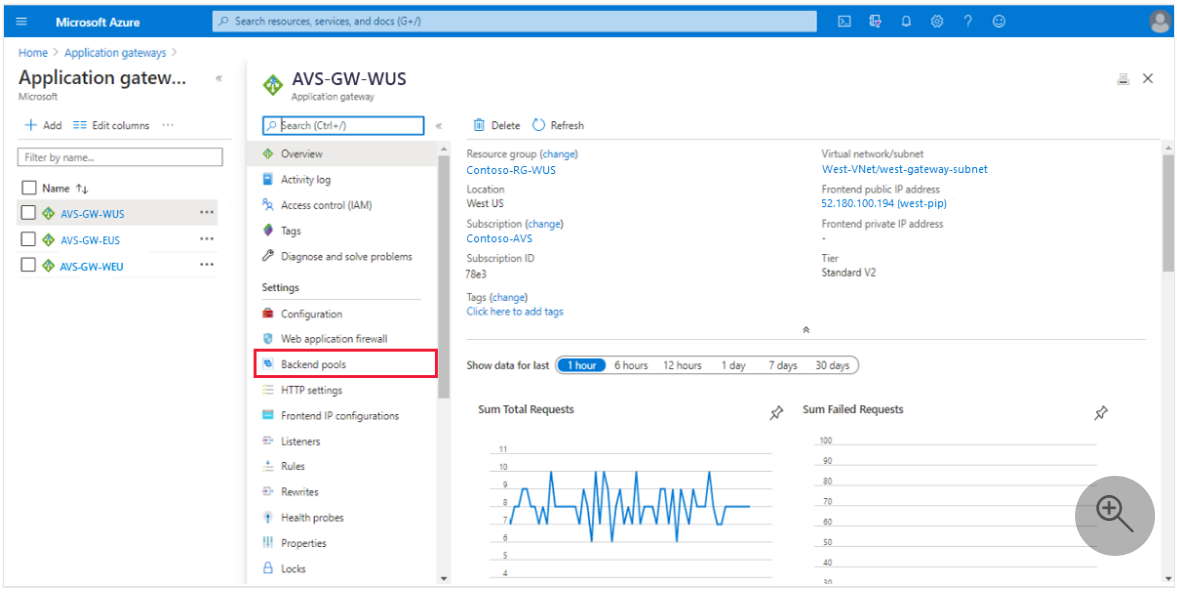
1. In the Azure portal, select **Application gateways** to view a list of your current application gateways:

   - AVS-GW-WUS
   - AVS-GW-EUS (on-premises)
   - AVS-GW-WEU

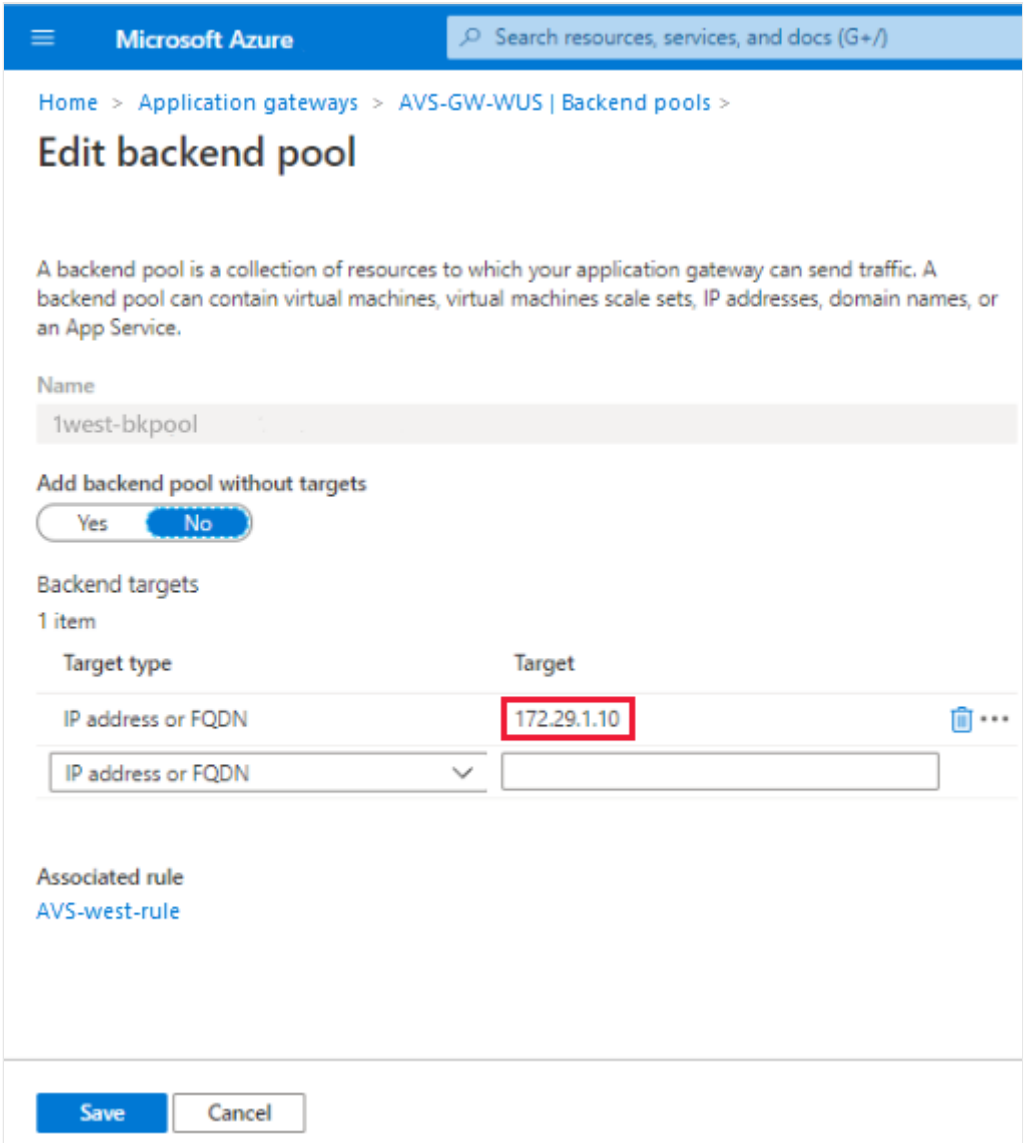


2. Select one of your previously deployed application gateways.

   A window opens showing various information on the application gateway.



3. Select **Backend pools** to verify the configuration of one of the backend pools. You see one VM backend pool member configured as a web server with an IP address of 172.29.1.10.

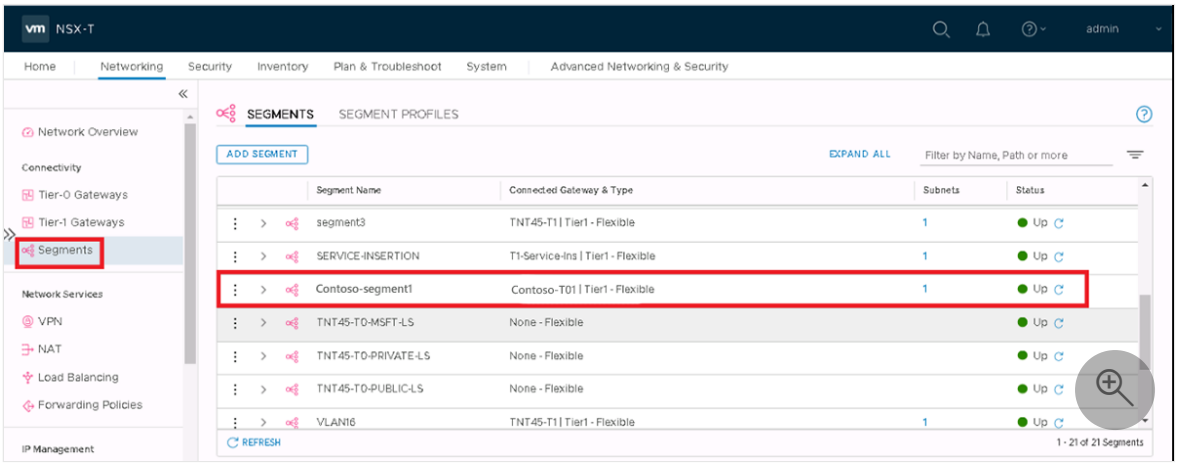


4. Verify the configuration of the other application gateways and backend pool members.

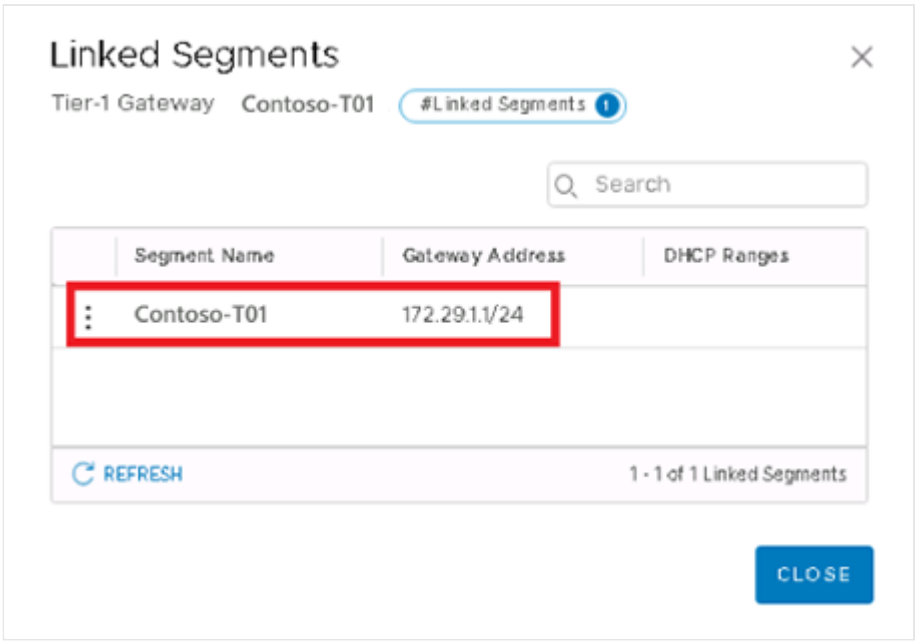
Verify the NSX segment configuration

The following steps verify the configuration of the NSX segment in the Azure VMware Solution environment.

1. Select **Segments** to view your configured segments. You see Contoso-segment1 connected to Contoso-T01 gateway, a Tier-1 flexible router.



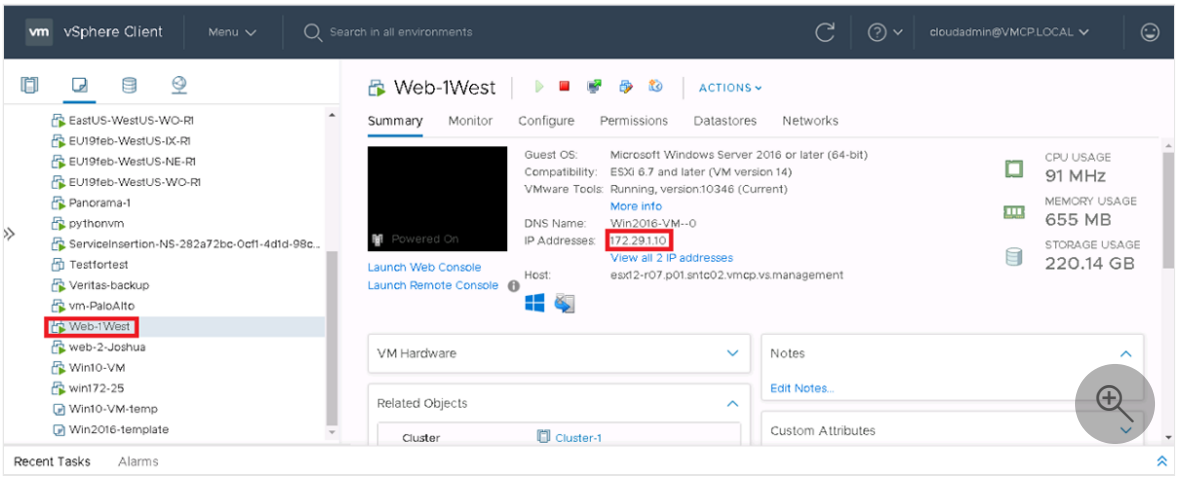
2. Select **Tier-1 Gateways** to see a list of Tier-1 gateways with the number of linked segments.



3. Select the segment linked to Contoso-T01. A window opens showing the logical interface configured on the Tier-01 router. It serves as a gateway to the backend pool member VM connected to the segment.

4. In the vSphere client, select the VM to view its details.

> **Note**
>
> Its IP address matches VM backend pool member configured as a web server from the preceding section: 172.29.1.10.



5. Select the VM, then select **ACTIONS** > **Edit Settings** to verify connection to the NSX segment.

Create your Traffic Manager profile

1. Sign in to the Azure portal. Under **Azure Services** > **Networking**, select **Traffic Manager profiles**.

2. Select **+ Add** to create a new Traffic Manager profile.

3. Provide the following information and then select **Create**:

   - Profile name
   - Routing method (use weighted)
   - Subscription
   - Resource group

Add external endpoints into the Traffic Manager profile

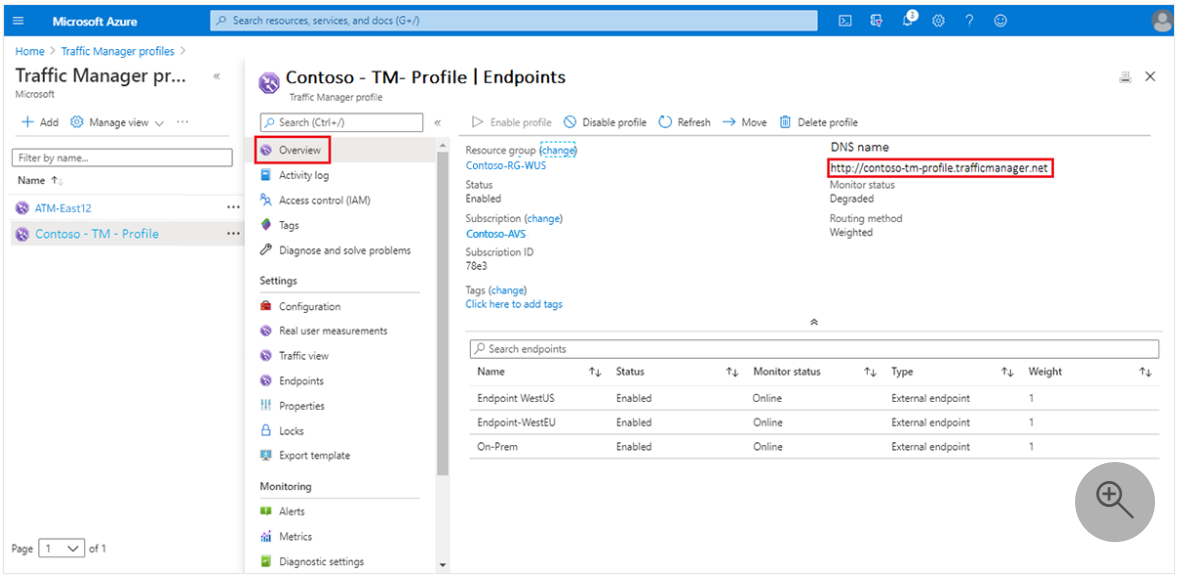
1. Select the Traffic Manager profile from the search results pane, select **Endpoints**, and then **+ Add**.

2. For each of the external endpoints in the different regions, enter the required details and then select **Add**:

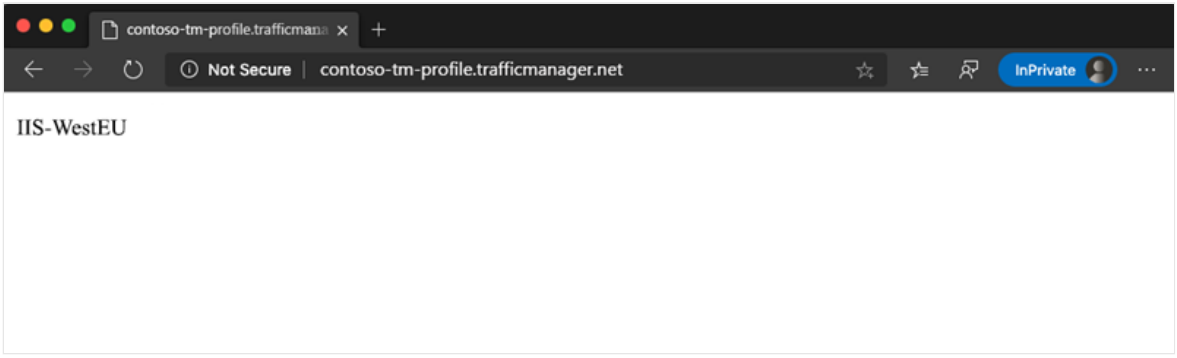
- Type
- Name
- Fully Qualified domain name (FQDN) or IP
- Weight (assign a weight of 1 to each endpoint).

Once created, all three shows in the Traffic Manager profile. The monitor status of all three must be **Online**.

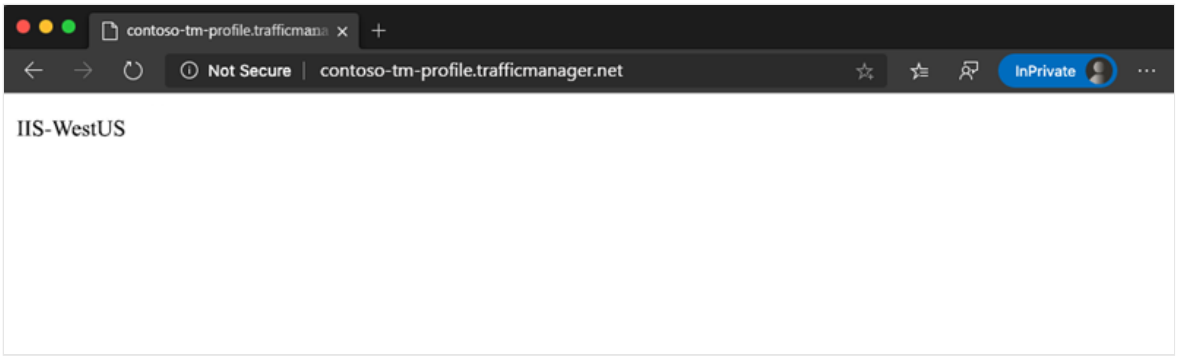
3. Select **Overview** and copy the URL under **DNS Name**.



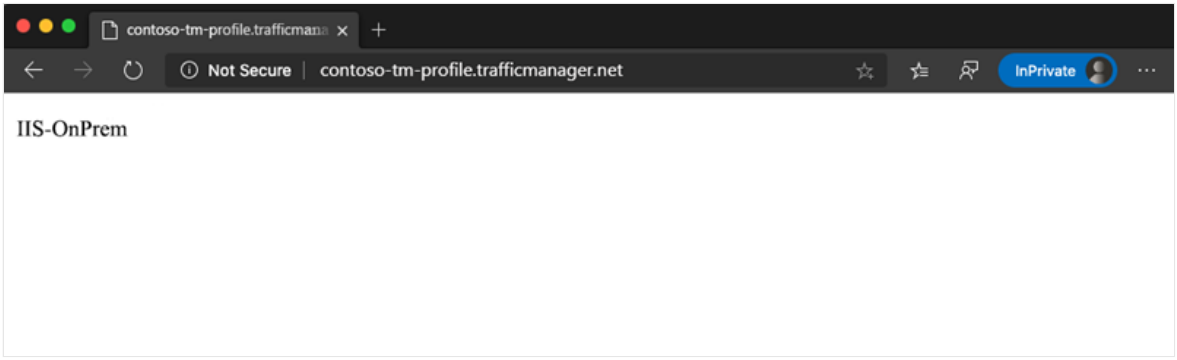
4. Paste the DNS name URL in a browser. The screenshot shows traffic directing to the West Europe region.



5. Refresh your browser. The screenshot shows traffic directing to another set of backend pool members in the West US region.



6. Refresh your browser again. The screenshot shows traffic directing to the final set of backend pool members on-premises.



Next steps

Now that you covered integrating Azure Traffic Manager with Azure VMware Solution, learn more about:

- Using Azure Application Gateway on Azure VMware Solution
- Traffic Manager routing methods
- Combining load-balancing services in Azure
- Measuring Traffic Manager performance

Migration solutions for Azure VMware Solution virtual machines (VMs)

Article • 12/20/2023

One of the most common use cases for using Azure VMware Solution is data center evacuation. It allows you to continue to maximize your VMware investments, because Azure VMware Solution is always up to date. Additionally, you can enhance your workloads with the full range of native Azure services. An initial key step in this process is the migration of your legacy VMware-based environment onto Azure VMware Solution.

Our migration partners have industry-leading migration solutions in VMware-based environments. Customers around the world use these solutions for their migrations to both Azure and Azure VMware Solution.

You aren't required to use VMware HCX as a migration tool, which means you can also migrate physical workloads into Azure VMware Solution. Additionally, migrations to your Azure VMware Solution environment don't need an ExpressRoute connection if it's not available within your source environment. Migrations can be done to multiple locations if you decide to host those workloads in multiple Azure regions.

You can find more information on these migration solutions here:

- RiverMeadow .

Install and activate VMware HCX in Azure VMware Solution

Article • 12/18/2023

VMware HCX is an application mobility platform designed for simplifying application migration, rebalancing workloads, and optimizing disaster recovery across data centers and clouds.

VMware HCX has two component services: **HCX Cloud Manager** and **HCX Connector**. These components work together for VMware HCX operations.

This article shows you how to install and activate the VMware HCX Cloud Manager and VMware HCX Connector components.

HCX Cloud manager is typically deployed as the destination (cloud side), but it can also be used as the source in cloud-to-cloud deployments. HCX Connector is deployed at the source (on-premises environment). A download link is provided for deploying HCX Connector appliance from within the HCX Cloud Manager.

This article also teaches you how to do the following tasks:

- Install VMware HCX Cloud through the Azure portal.
- Download and deploy the VMware HCX Connector in on-premises.
- Activate VMware HCX with a license key.

After HCX is deployed, follow the recommended Next steps.

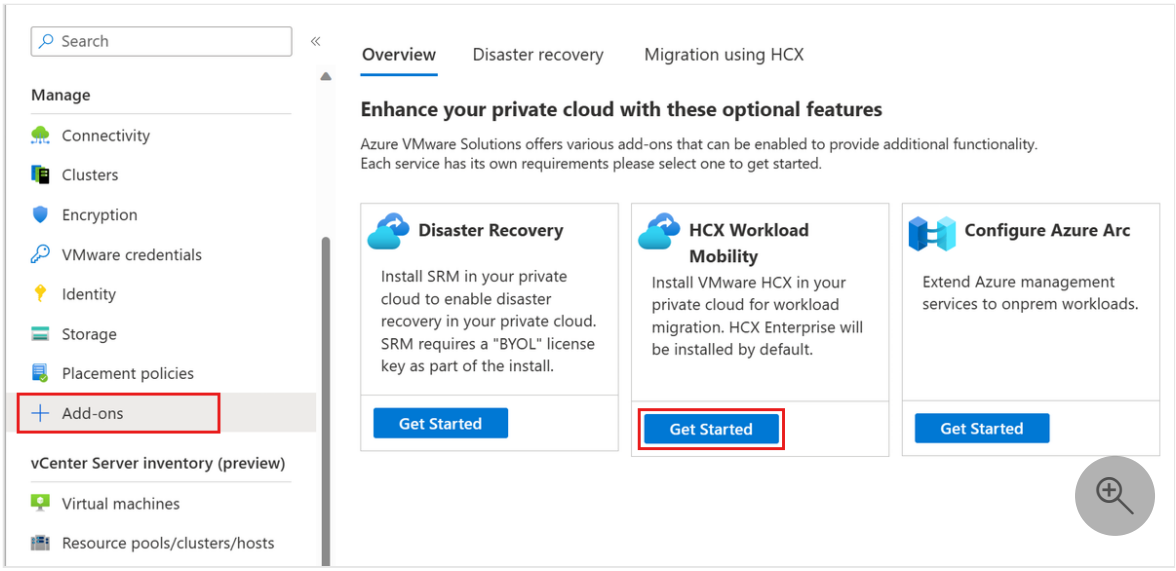
Prerequisite

- See Prepare for HCX installations

Install VMware HCX Cloud

1. In your Azure VMware Solution private cloud, select **Manage** > **Add-ons**.

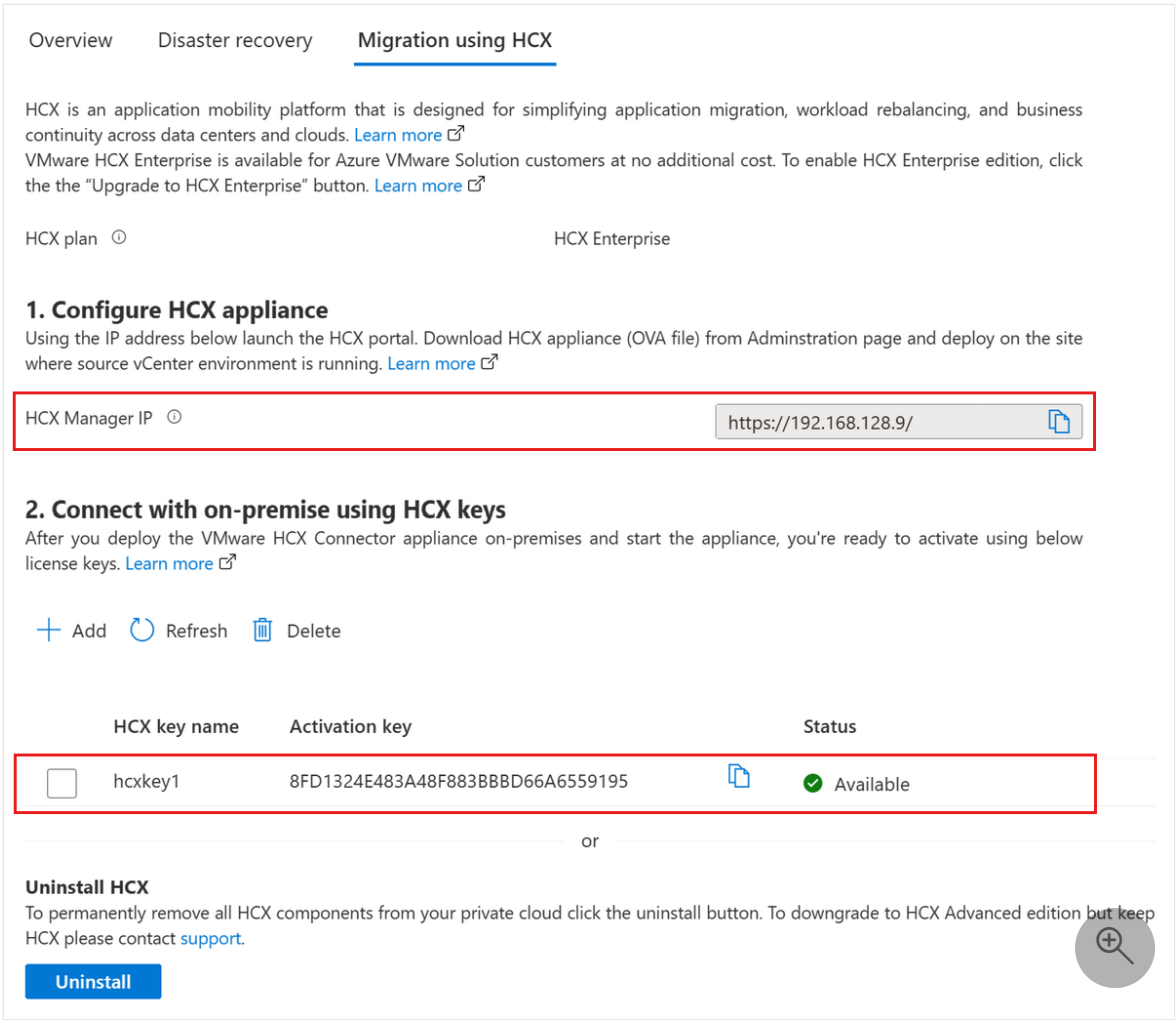
2. Select **Get started** for **HCX Workload Mobility**.



3. Select the **I agree with terms and conditions** checkbox and then select **Install**.

   Once installed, you should see the HCX Manager IP and the HCX keys required for the HCX on-premises connector site pairing on the **Migration using HCX** tab.

> **Important**
>
> If you don't see the HCX key after installing, click the **ADD** button to generate the key which you can then use for site pairing.



VMware HCX license edition

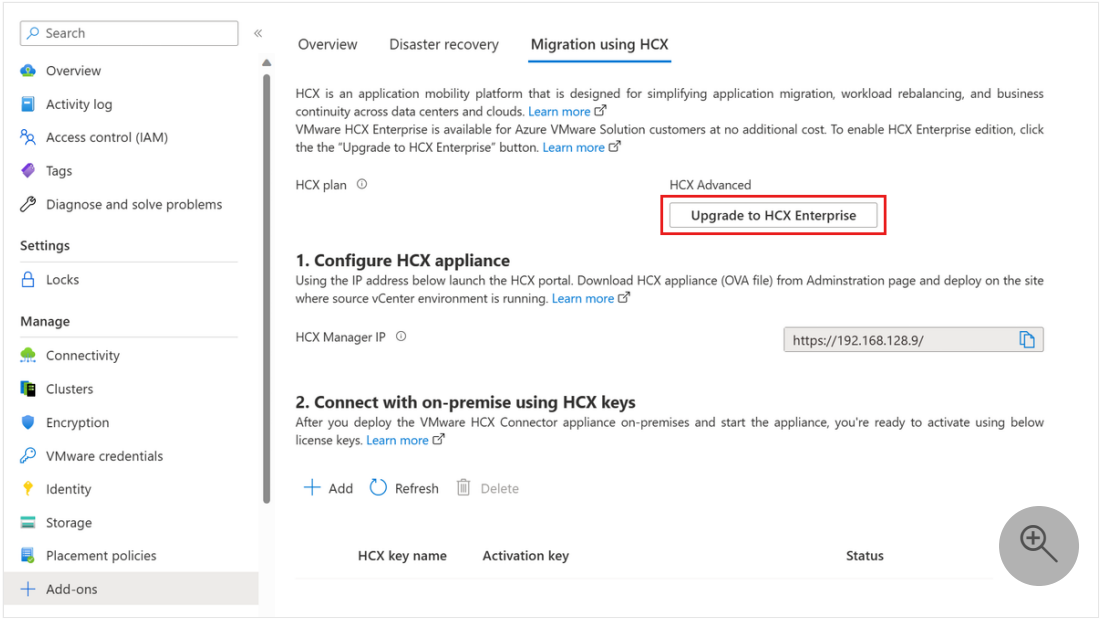
HCX offers various services based on the type of license installed with the system. Advanced delivers basic connectivity and mobility services to enable hybrid interconnect and migration services. HCX Enterprise offers more services than what standard licenses provide. Some of those services include; Mobility Groups, Replication assisted vMotion (RAV), Mobility Optimized Networking, Network Extension High availability, OS assisted Migration, and others.

> **Note**
>
> VMware HCX Enterprise is available for Azure VMware Solution customers at no additional cost.

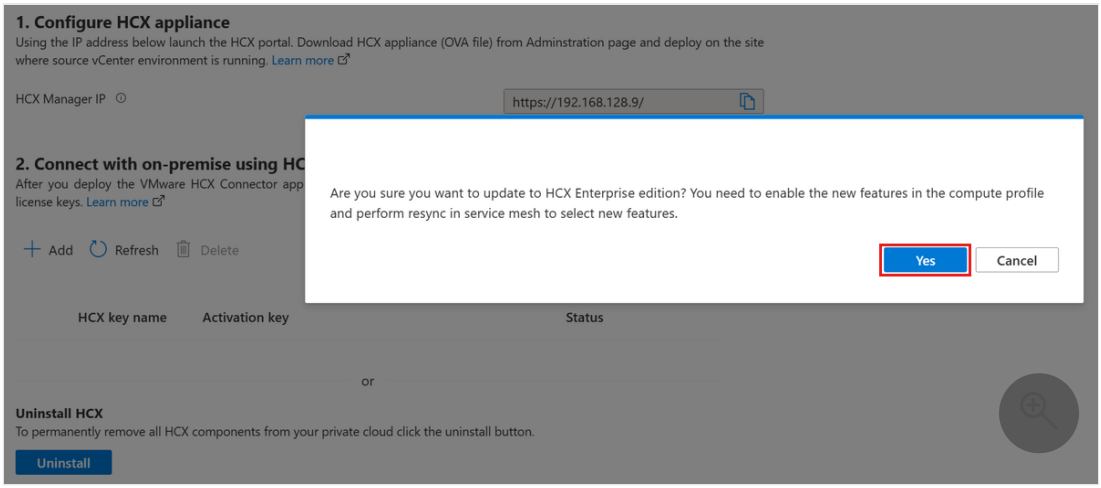
- HCX is now installed as Enterprise for all new HCX installations in Azure VMware solution.
- Existing HCX Advanced customers can upgrade to HCX Enterprise using the Azure portal. Use the following steps to upgrade to HCX Enterprise using Azure portal.

1. Under **Manage** in the left navigation, select **Add-ons**, then the **Migration using HCX** tab.

2. Select the **Upgrade to HCX Enterprise** button to enable HCX Enterprise edition.



3. Confirm the update to HCX Enterprise edition by selecting **Yes**.



> **ⓘ Important**
>
> If you upgraded VMware HCX from advanced to Enterprise, enable the new features in the compute profile and perform resync in service mesh to select a new feature like, Replication Assisted vMotion (RAV).

4. Change Compute profile after HCX upgrade to HCX Enterprise.
   a. On HCX UI, select **Infrastructure** > **Interconnect**, then select **Edit**.
   b. Select services you want activated like, Replication Assisted vMotion (RAV) and OS assisted Migration, which is available with VMware HCX Enterprise

only.

c. Select **Continue**, review the settings, then select **Finish** to create the Compute Profile.

5. If compute profile is being used in service mesh(es), resync service mesh.
   a. Go to **Interconnect** > **Service Mesh**.
   b. Select **Resync**, then verify that the changes appear in the Service Mesh configuration.

- Downgrading from HCX Enterprise Edition to HCX Advanced is possible without redeploying.

  1. Verify that you reverted to an HCX Advanced configuration state and you aren't using the Enterprise features.
  2. If you plan to downgrade, verify that no scheduled migrations, Enterprise services like RAV and HCX MON, etc. are in use. Open a support request to request downgrade.

Download and deploy the VMware HCX Connector on-premises

Use the following steps to download the VMware HCX Connector OVA file, and then deploy the VMware HCX Connector to your on-premises vCenter Server.

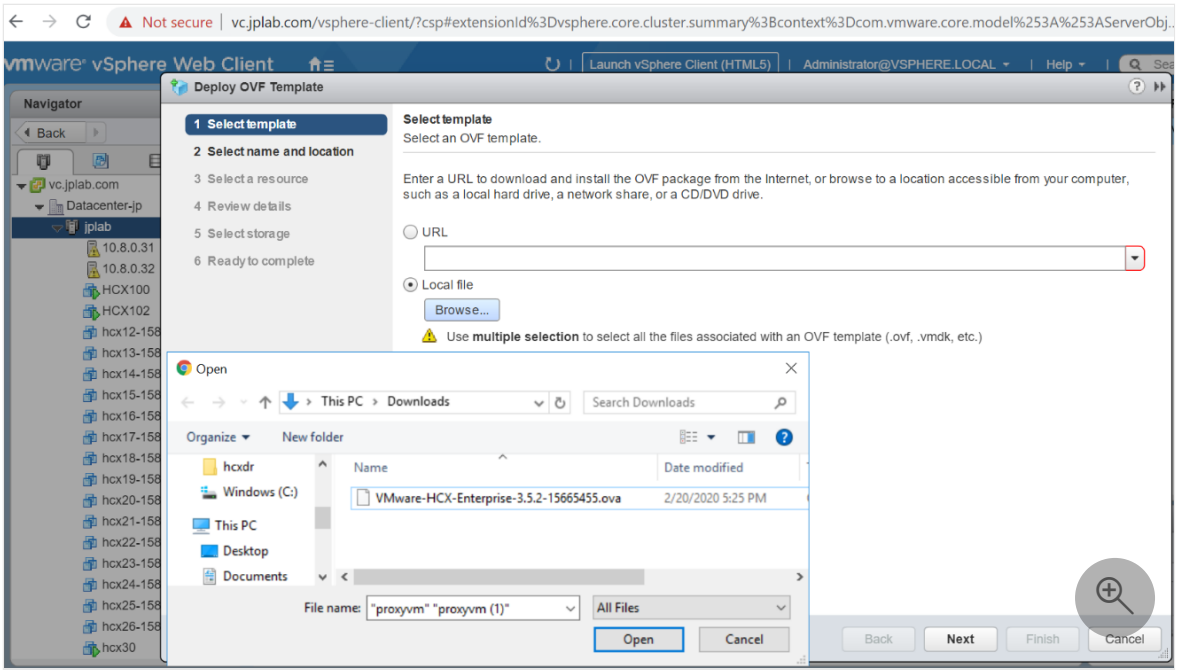
1. Open a browser window, sign in to the Azure VMware Solution HCX Manager on `https://x.x.x.9` port 443 with the **cloudadmin@vsphere.local** user credentials

2. Under **Administration** > **System Updates**, select **Request Download Link**. If the box is greyed, wait a few seconds for it to generate a link.

3. Either download or receive a link for the VMware HCX Connector OVA file you deploy on your local vCenter Server.

4. In your on-premises vCenter Server, select an OVF template to deploy the VMware HCX Connector to your on-premises vSphere cluster.

5. Navigate to and select the OVA file that you downloaded and then select **Open**.

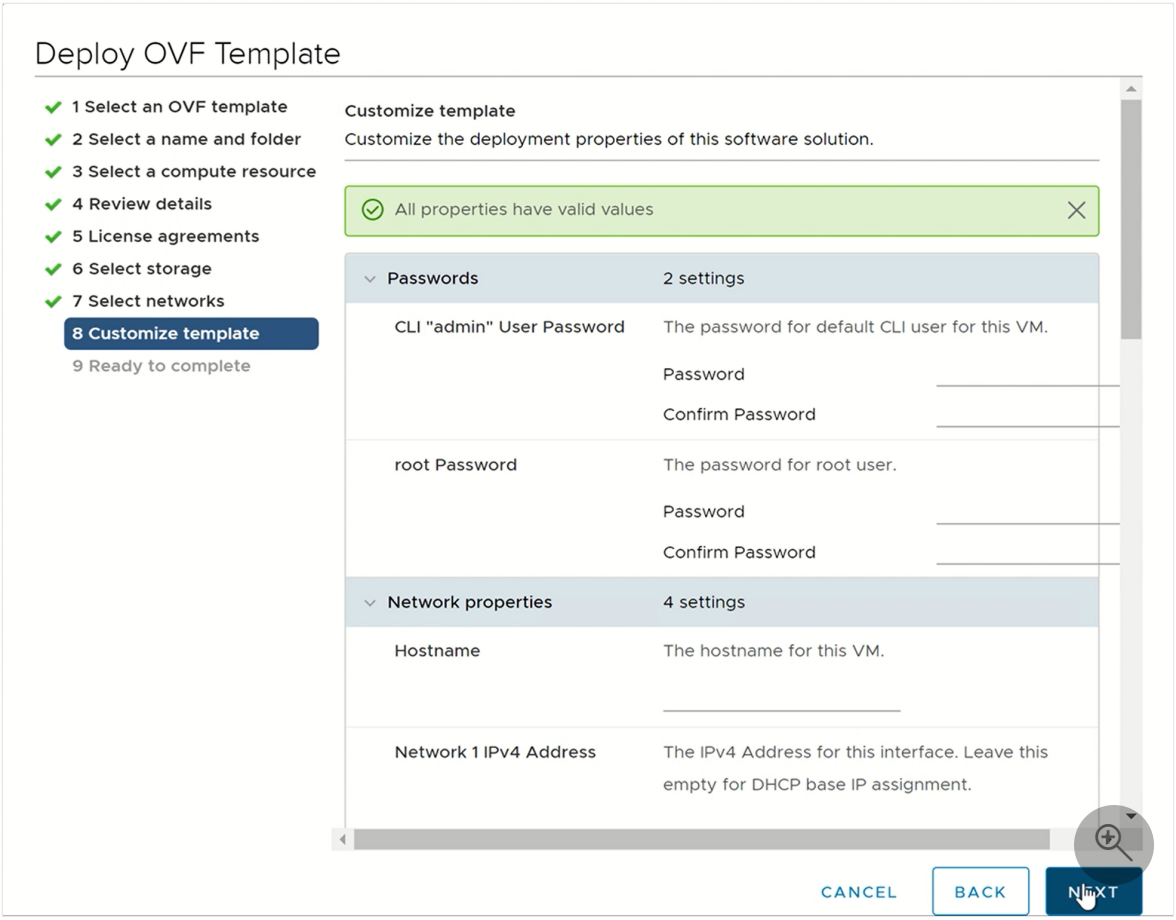


6. Select a name and location, and select a resource or cluster where you're deploying the VMware HCX Connector. Then review the details and required resources and select **Next**.

7. Review license terms, select the required storage and network, and then select **Next**.

8. Select the VMware HCX management network segment that you defined during the planning state. Then select **Next**.

9. In **Customize template**, enter all required information and then select **Next**.



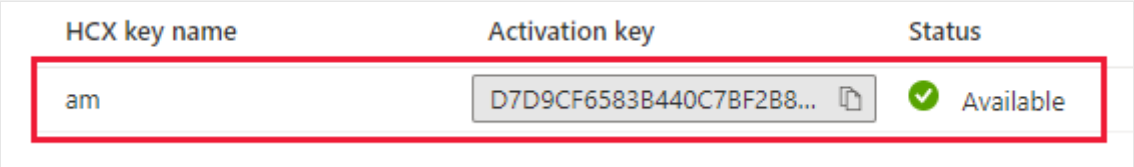
10. Verify and then select **Finish** to deploy the VMware HCX Connector OVA.

> **Important**
>
> You will need to turn on the virtual appliance manually. After powering on, wait 10-15 minutes before proceeding to the next step.

Activate VMware HCX

After deploying the VMware HCX Connector OVA on-premises and starting the appliance, you're ready to activate it. First, you need to get a license key from the Azure VMware Solution portal and activate it in VMware HCX Manager. Then you need a key for each on-premises HCX connector deployed.

1. In your Azure VMware Solution private cloud, select **Manage** > **Add-ons** > **Migration using HCX**. Then copy the **Activation key**.



2. Sign in to the on-premises VMware HCX Manager at `https://HCXManagerIP:9443` with the `admin` credentials. Make sure to include the `9443` port number with the VMware HCX Manager IP address.

   > **Tip**
   >
   > You defined the **admin** user password during the VMware HCX Manager OVA file deployment.

3. In **Licensing**, enter your key for **HCX Advanced Key** and select **Activate**.

   > **Important**
   >
   > VMware HCX Manager must have open internet access or a proxy configured.

4. In **Datacenter Location**, provide the nearest location for installing the VMware HCX Manager on-premises. Then select **Continue**.

5. In **System Name**, modify the name or accept the default and select **Continue**.

6. Select **Yes, Continue**.

7. In **Connect your vCenter**, provide the FQDN or IP address of your vCenter server and the appropriate credentials, and then select **Continue**.

   > **Tip**
   >
   > The vCenter Server is where you deployed the VMware HCX Connector in your datacenter.

8. In **Configure SSO/PSC**, provide your Platform Services Controller's FQDN or IP address, and select **Continue**.

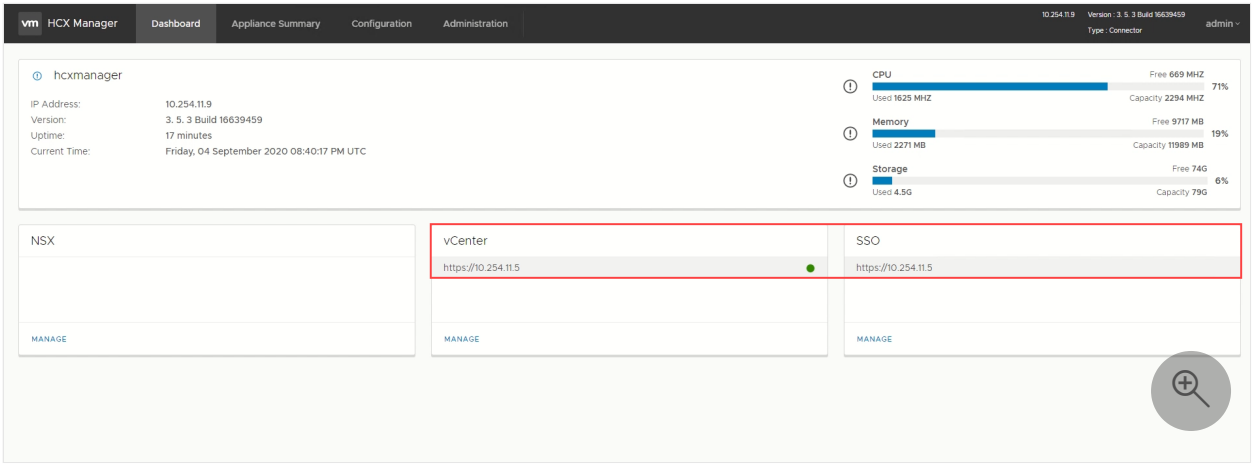
   > **Note**
   >
   > Typically, it's the same as your vCenter Server FQDN or IP address.

9. Verify that the information entered is correct and select **Restart**.

   > **Note**

> You'll experience a delay after restarting before being prompted for the next step.

After the services restart, you'll see vCenter Server displayed as green on the screen that appears. Both vCenter Server and SSO must have the appropriate configuration parameters, which should be the same as the previous screen.



Next steps

Continue to the next tutorial to configure the VMware HCX Connector. After you configured the VMware HCX Connector, you have a production-ready environment for creating virtual machines (VMs) and migration.

> Configure VMware HCX in Azure VMware Solution

> Understanding HCX Network Underlay Requirements

> VMware blog series - cloud migration

> Uninstall VMware HCX in Azure VMware Solution

Configure on-premises VMware HCX Connector

Article • 05/15/2024

After you install the VMware HCX add-on, configure the on-premises VMware HCX Connector for your Azure VMware Solution private cloud.

In this article, learn how to:

- ✓ Pair your on-premises VMware HCX Connector with your Azure VMware > Solution HCX Cloud Manager
- ✓ Configure the network profile, compute profile, and service mesh
- ✓ Check the appliance status and validate that migration is possible

After you complete these steps, you'll have a production-ready environment for creating virtual machines (VMs) and migration.

Prerequisites

- Install VMware HCX Connector.
- VMware HCX Enterprise is now available and supported on Azure VMware Solution at no extra cost. HCX Enterprise is automatically installed for all new HCX add-on requests, and existing HCX Advanced customers can upgrade to HCX Enterprise using the Azure portal.
- If you plan to enable VMware HCX MON, make sure you have:
  - VMware NSX or vSphere Distributed Switch (vDS) on-premises for HCX Network Extension (vSphere Standard Switch not supported).
  - One or more active stretched network segments.
- Meet the VMware software version requirements.
- Your on-premises vSphere environment (source environment) meets the minimum requirements.
- Azure ExpressRoute Global Reach is configured between on-premises and Azure VMware Solution private cloud ExpressRoute circuits.
- All required ports are open for communication between on-premises components and Azure VMware Solution private.

- Define VMware HCX network segments. The primary use cases for VMware HCX are workload migrations and disaster recovery.
- Review the VMware HCX Documentation for information on using HCX.

Add a site pairing

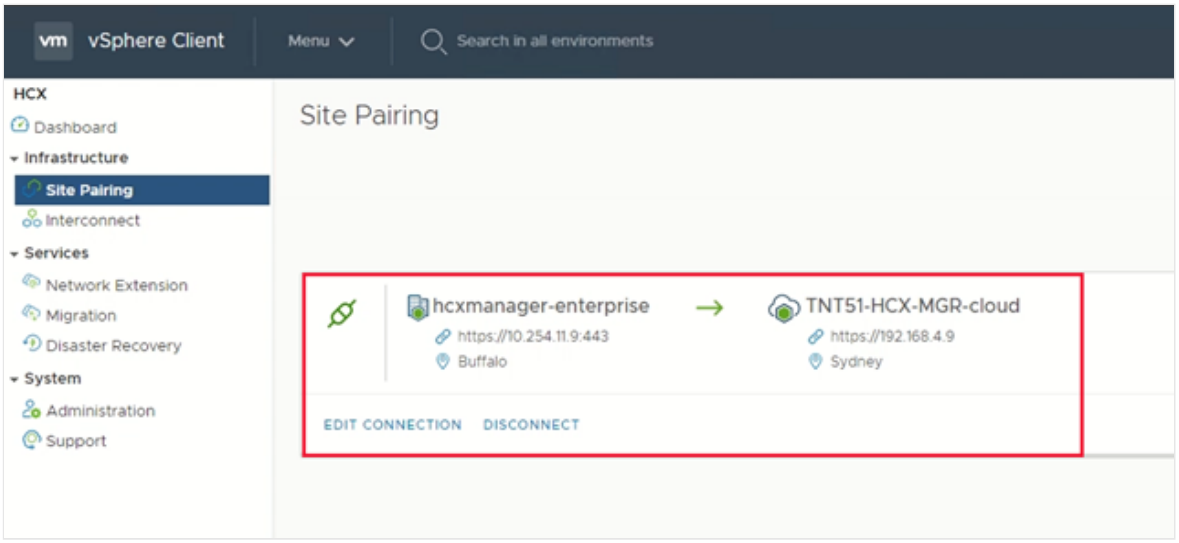
In your data center, connect or pair the VMware HCX Cloud Manager in Azure VMware Solution with the VMware HCX Connector.

> **Important**
>
> According to the Azure VMware Solution limits, a single HCX manager system can have a maximum of 25 site pairs and 10 service meshes, including inbound and outbound site pairings.

1. Sign in to your on-premises vCenter Server, and under **Home**, select **HCX**.
2. Under **Infrastructure**, select **Site Pairing** and choose the **Connect to Remote Site** option (in the middle of the screen).
3. Enter the Azure VMware Solution HCX Cloud Manager URL or IP address that you noted earlier `https://x.x.x.9` and the credentials for a user with the CloudAdmin role in your private cloud. Then select **Connect**.

   > **Note**
   >
   > To successfully establish a site pair:
   >
   > - Your VMware HCX Connector must be able to route to your HCX Cloud Manager IP over port 443.
   > - A service account from your external identity source, such as Active Directory, is recommended for site pairing connections. For more information about setting up separate accounts for connected services, see Access and identity architecture.

   A screen displays the connection (pairing) between your VMware HCX Cloud Manager in Azure VMware Solution and your on-premises VMware HCX Connector.



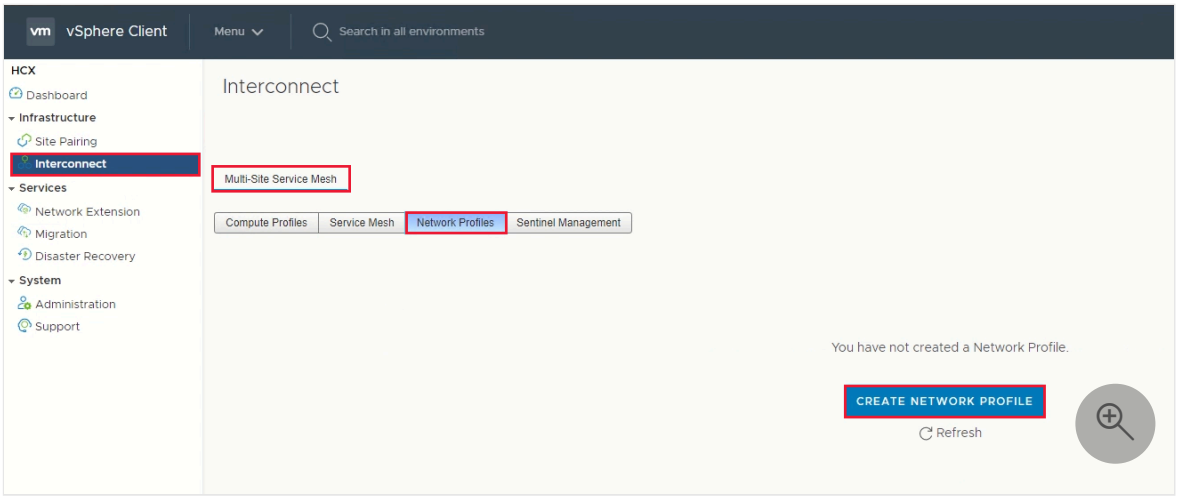
Create network profiles

VMware HCX Connector deploys a subset of virtual appliances (automated) that require multiple IP segments. Create your network profiles using the IP segments identified during the planning phase. Create four network profiles:

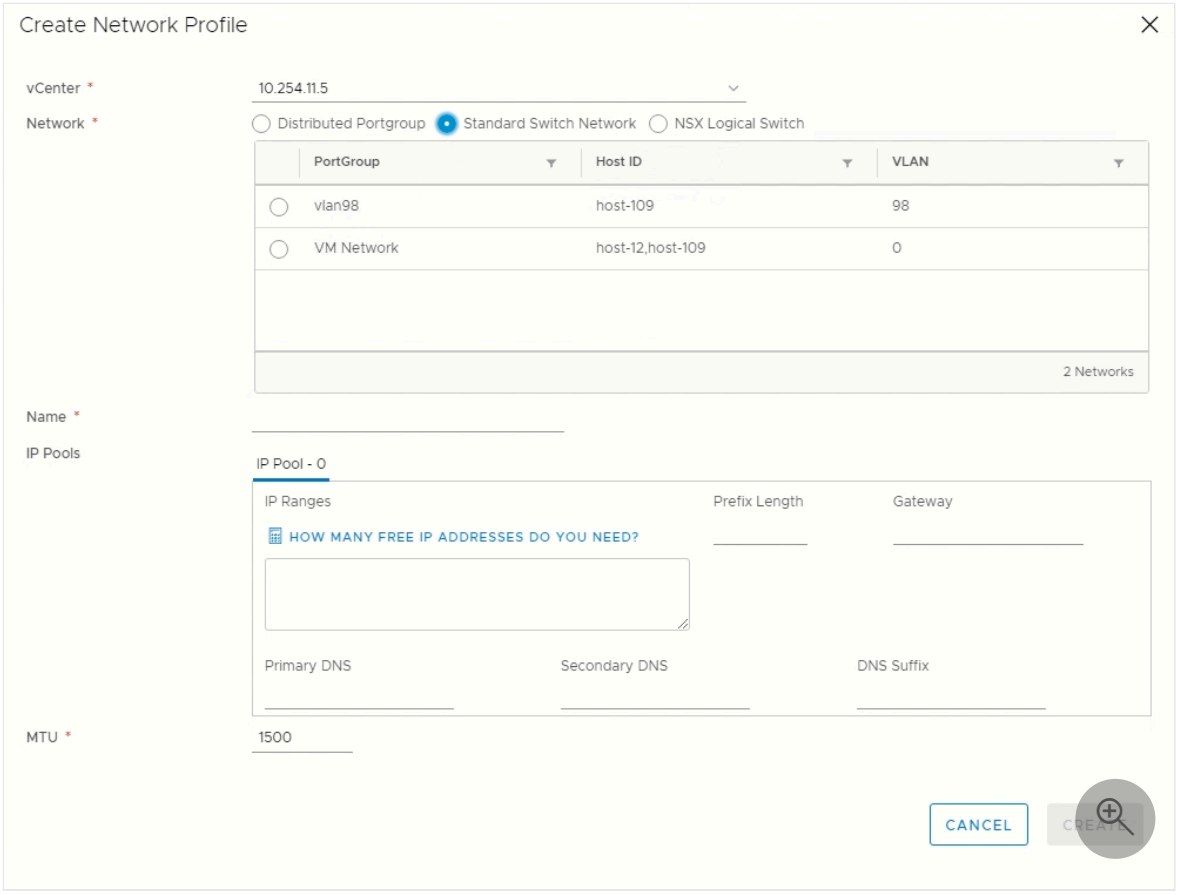
- Management
- vMotion
- Replication
- Uplink

> ⓘ **Note**
>
> - For Azure VMware Solution connected via VPN, set Uplink Network Profile MTU's to 1350 to account for IPSec overhead.
> - Azure VMware Solution defaults to 1500 MTU, which is sufficient for most ExpressRoute implementations.
>   - If your ExpressRoute provider does not support jumbo frames, you may need to lower the MTU in ExpressRoute setups as well.
>   - Adjust MTU settings on both HCX Connector (on-premises) and HCX Cloud Manager (Azure VMware Solution) network profiles.

1. Under **Infrastructure**, select **Interconnect** > **Multi-Site Service Mesh** > **Network Profiles** > **Create Network Profile**.



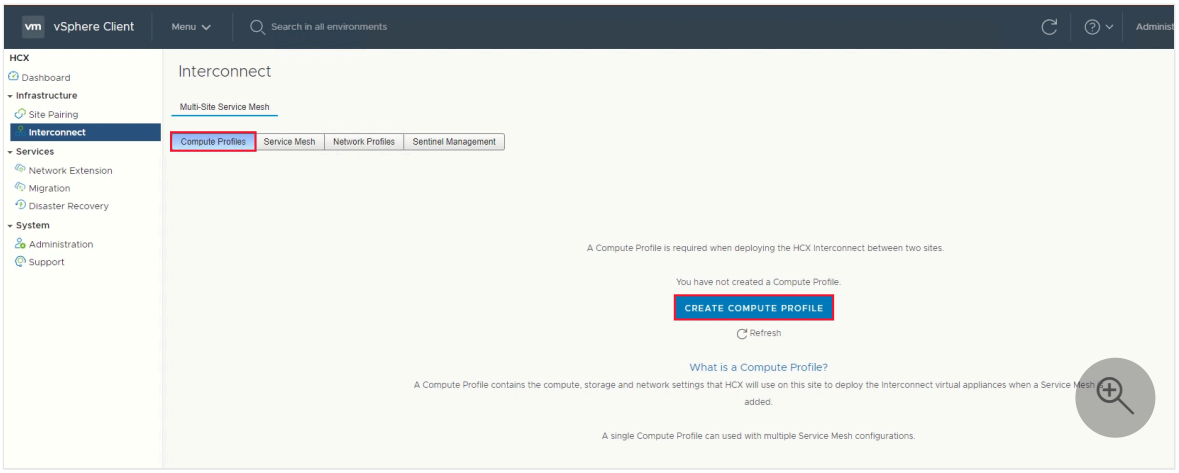
2. For each network profile, select the network and port group, provide a name, and create the segment's IP pool. Then select **Create**.



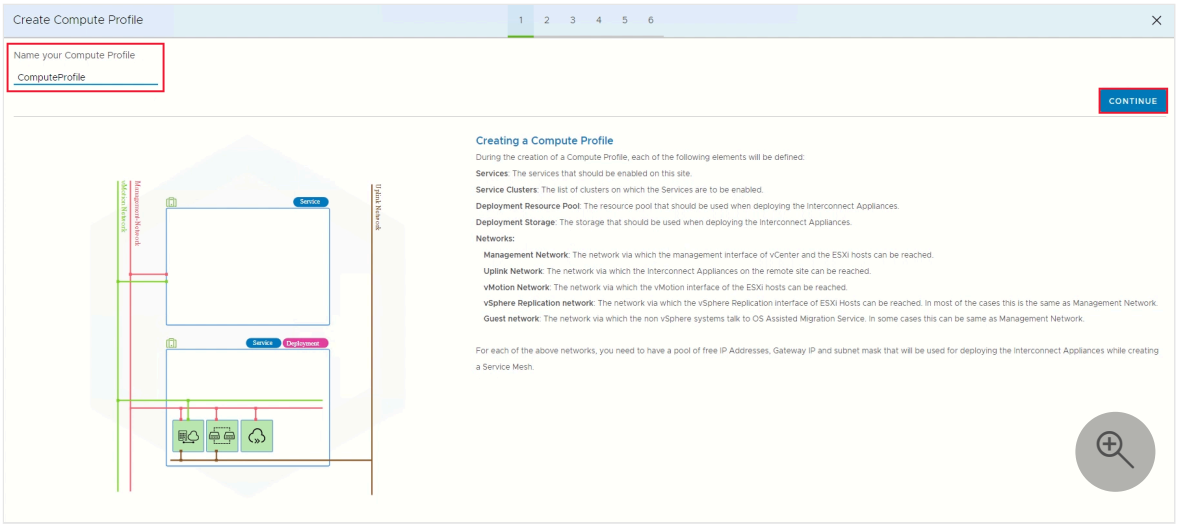
For an end-to-end overview of this procedure, watch the Azure VMware Solution: HCX Network Profile video.

Create a compute profile

1. Under **Infrastructure**, select **Interconnect** > **Compute Profiles** > **Create Compute Profile**.



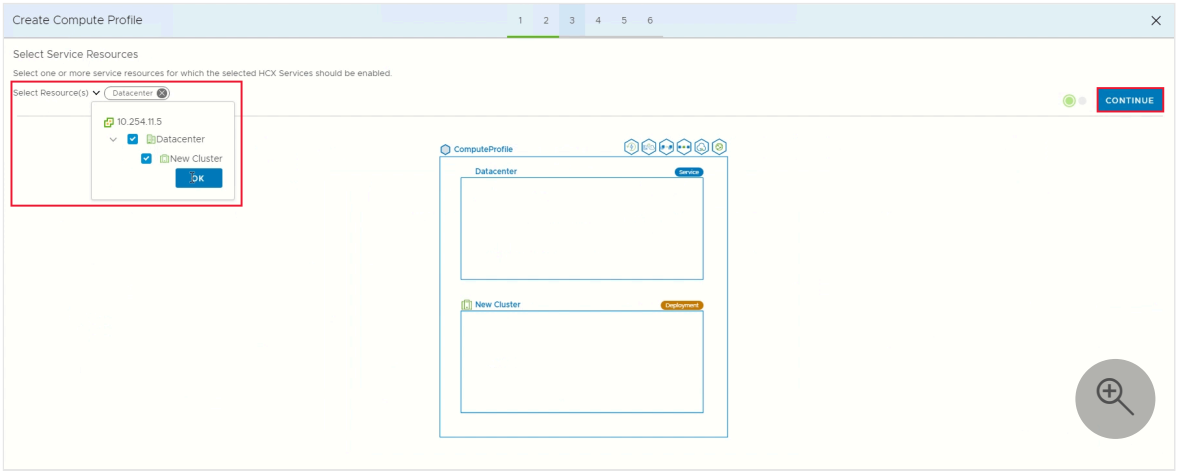
2. Enter a name for the profile and select **Continue**.



3. Select the services to enable, such as migration, network extension, or disaster recovery, and then select **Continue**.

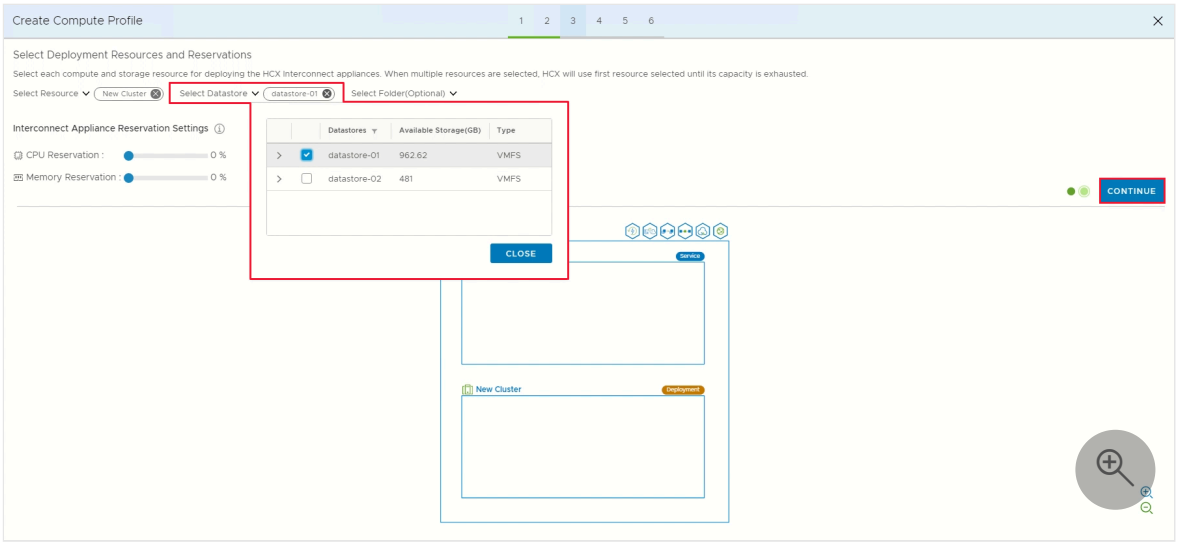
4. In **Select Service Resources**, select one or more service resources (clusters) to enable the selected VMware HCX services.

5. When you see the clusters in your on-premises datacenter, select **Continue**.

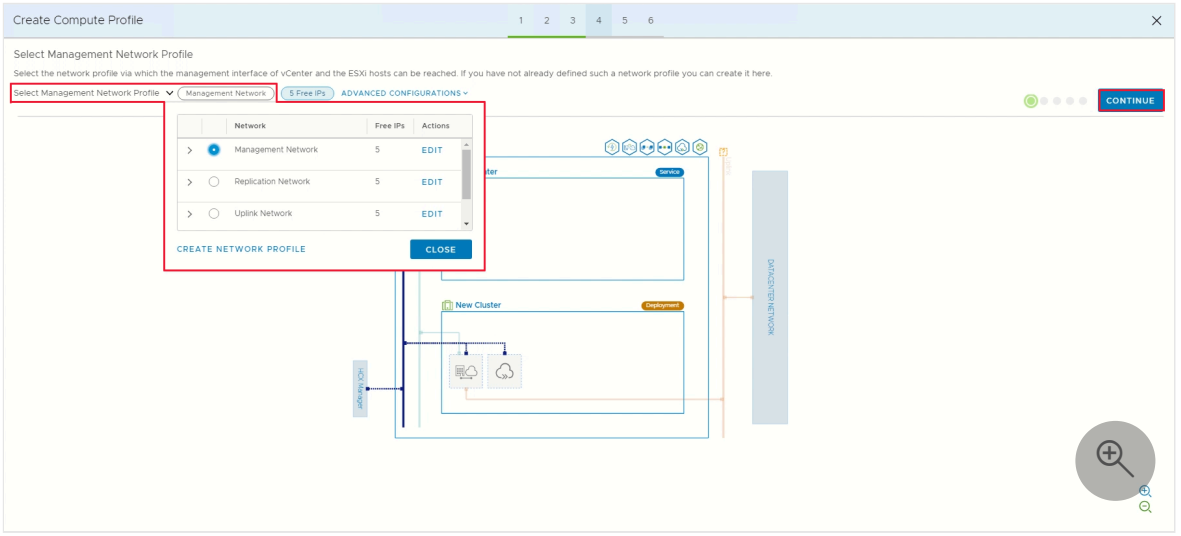


6. From **Select Datastore**, select the datastore storage resource for deploying the VMware HCX Interconnect appliances. Then select **Continue**.

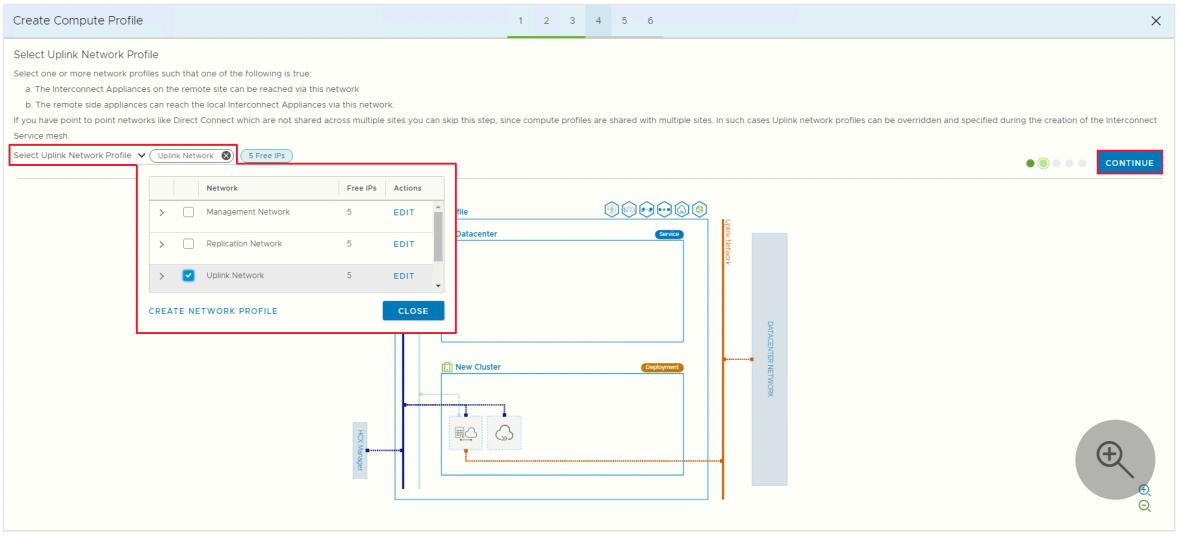
   When multiple resources are selected, VMware HCX uses the first resource selected until its capacity is exhausted.



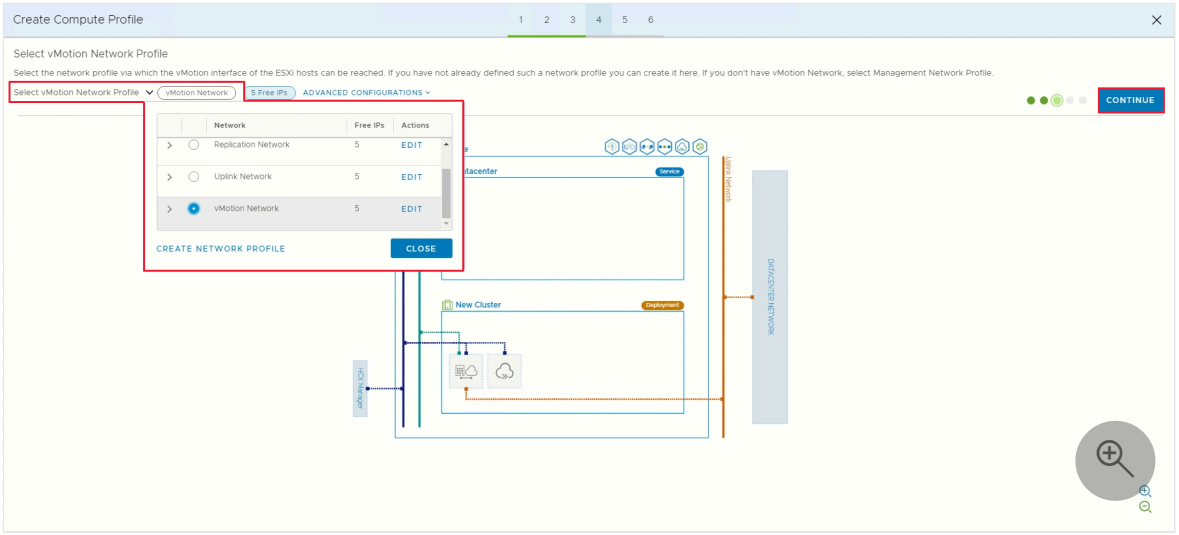
7. From **Select Management Network Profile**, select the management network profile that you created in previous steps. Then select **Continue**.



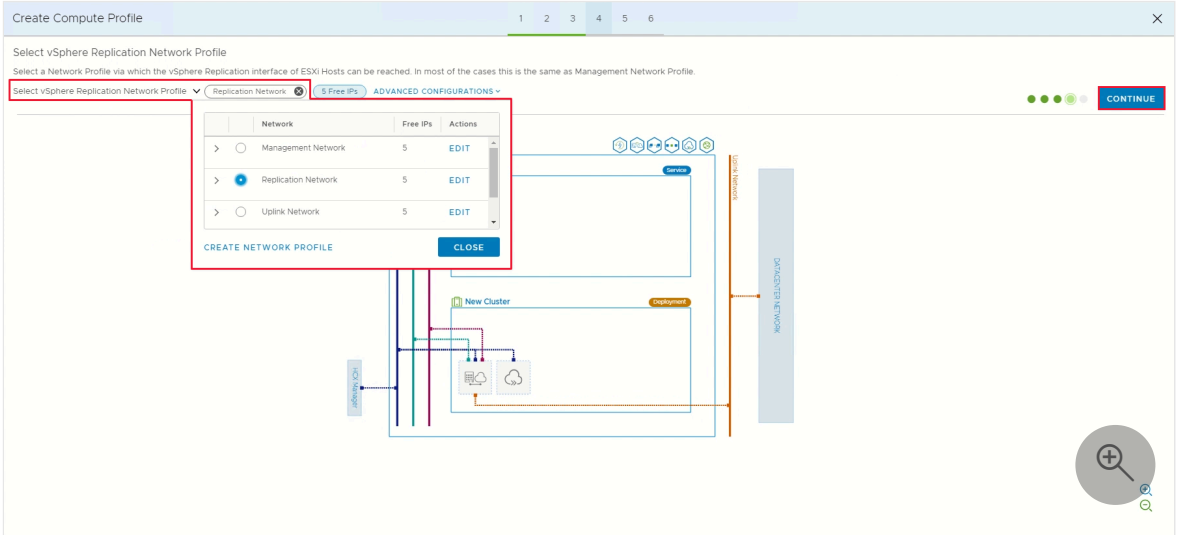
8. From **Select Uplink Network Profile**, select the uplink network profile you created in the previous procedure. Then select **Continue**.



9. From **Select vMotion Network Profile**, select the vMotion network profile that you created in previous steps. Then select **Continue**.



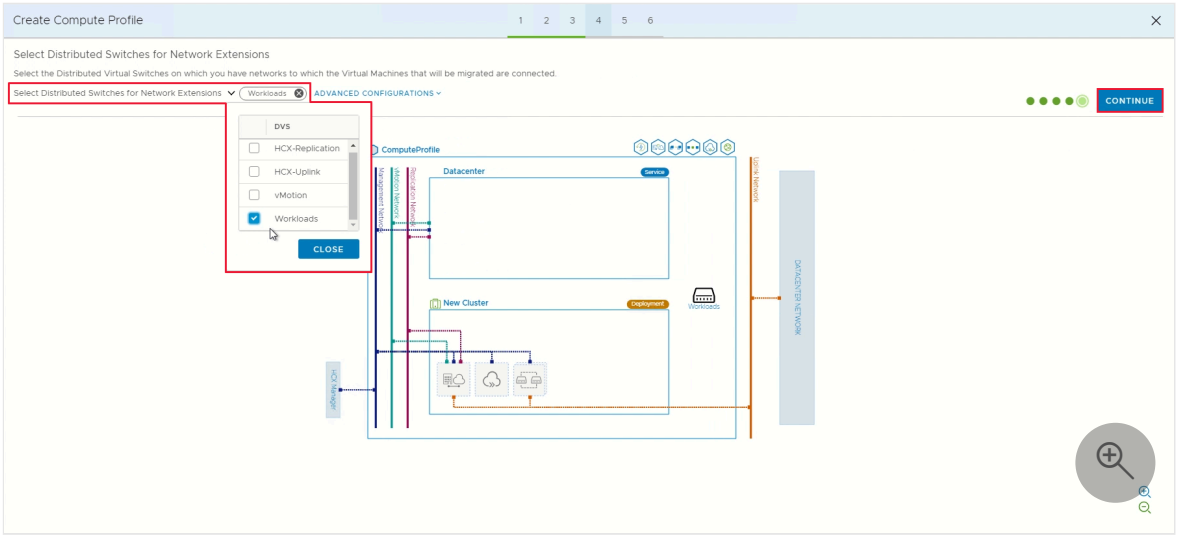
10. From **Select vSphere Replication Network Profile**, select the replication network profile that you created in previous steps. Then select **Continue**.



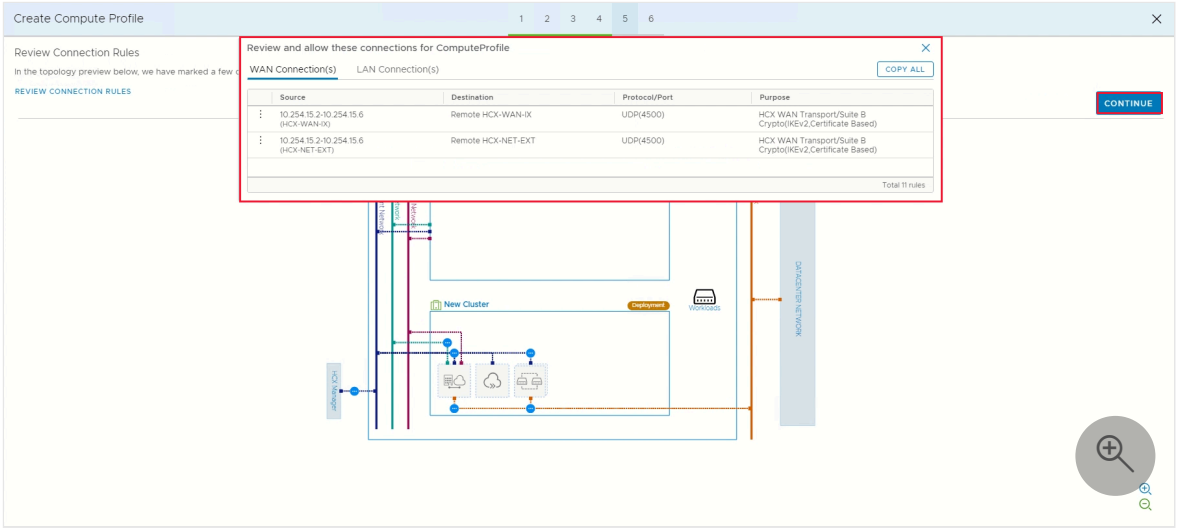
11. From **Select Distributed Switches for Network Extensions**, select the switches containing the virtual machines to be migrated to Azure VMware Solution on a

layer-2 extended network. Then select **Continue**.

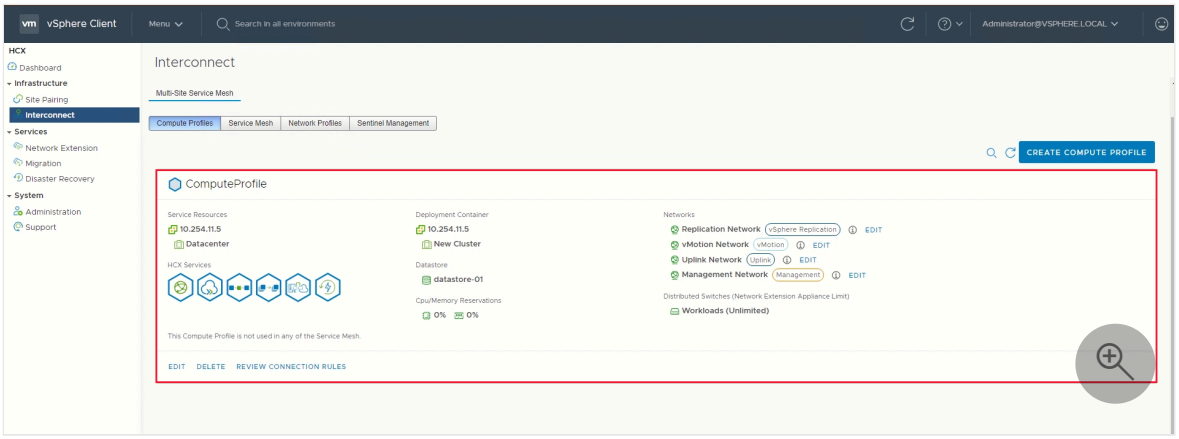
> **Note**
>
> If you're not migrating virtual machines on layer-2 (L2) extended networks, skip this step.



12. Review the connection rules and select **Continue**.



13. Select **Finish** to create the compute profile.

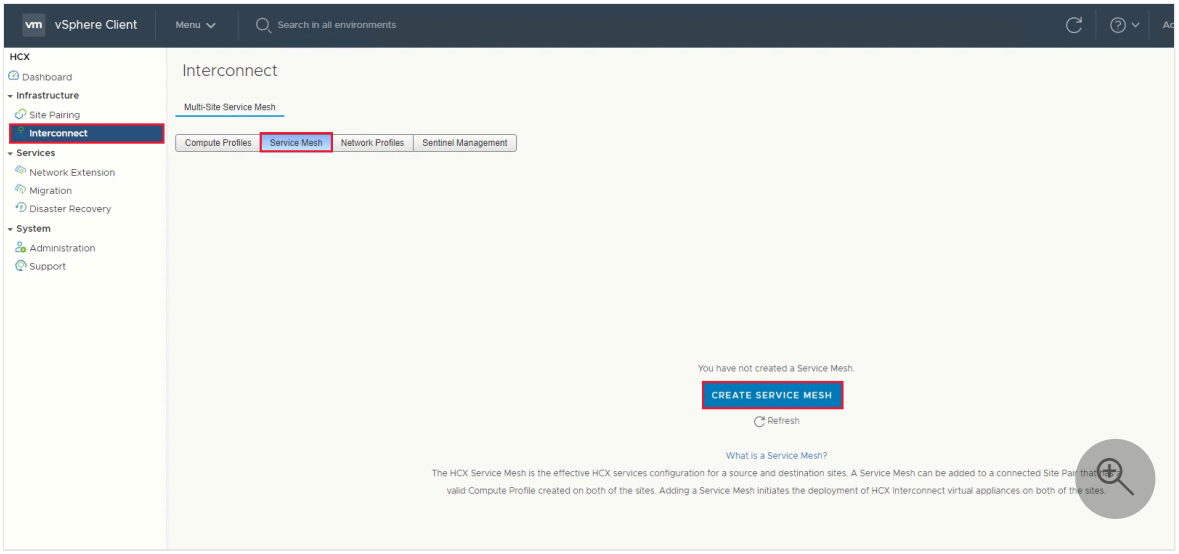


For an end-to-end overview of this procedure, view the Azure VMware Solution: Compute Profile video.

Create a service mesh

> **Important**
>
> Make sure port UDP 4500 is open between your on-premises VMware HCX Connector 'uplink' network profile addresses and the Azure VMware Solution HCX Cloud 'uplink' network profile addresses. (UDP 500 was required in legacy versions of HCX. See https://ports.vmware.com for the latest information.)

1. Under **Infrastructure**, select **Interconnect** > **Service Mesh** > **Create Service Mesh**.



2. Review the prepopulated sites, and then select **Continue**.

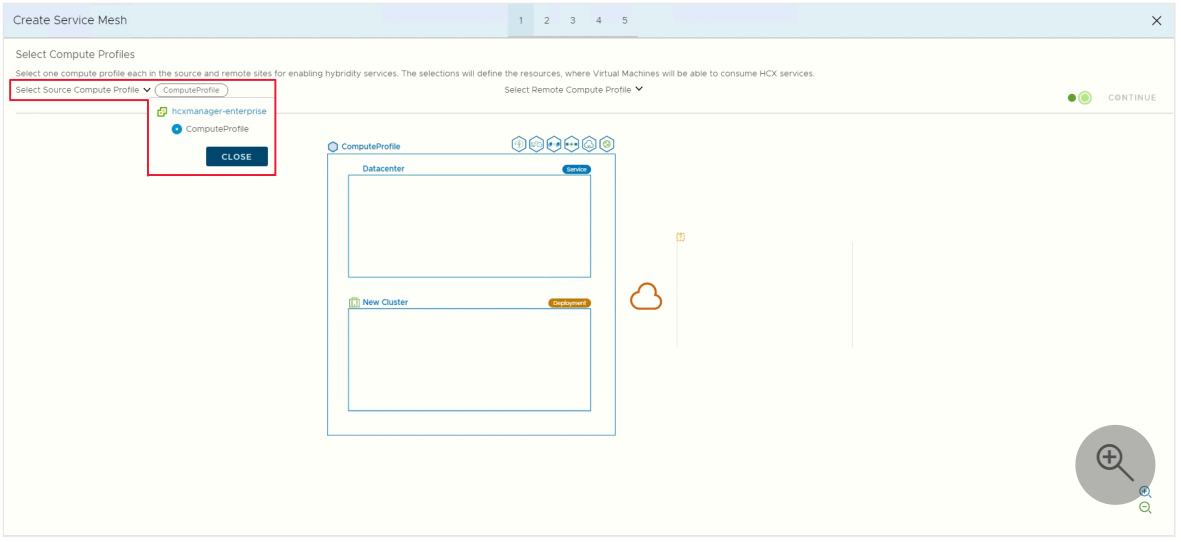
> **Note**

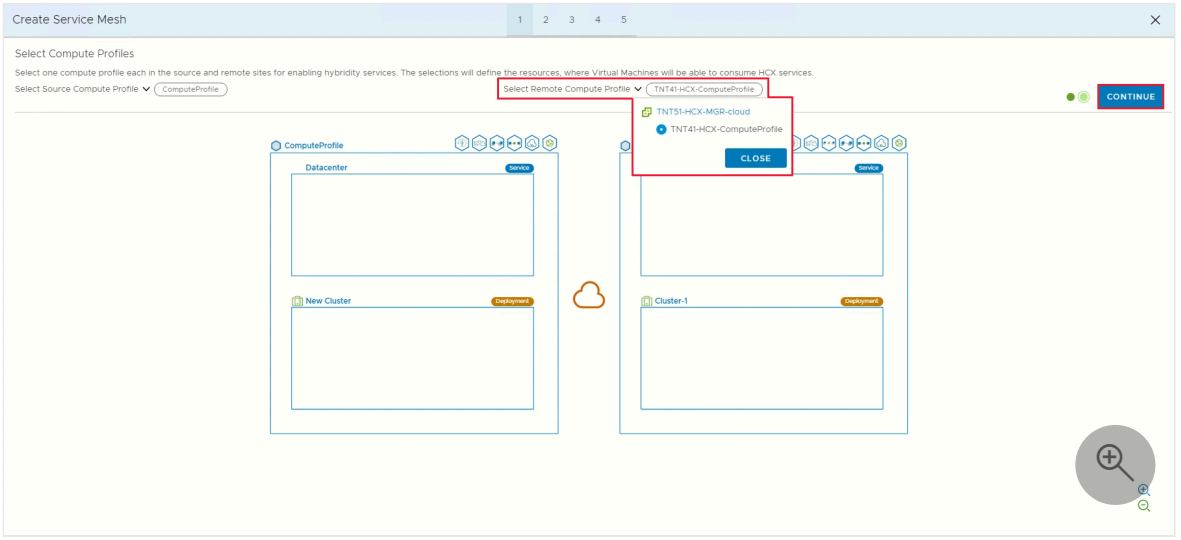
If this is your first service mesh configuration, you won't need to modify this screen.

3. Select the source and remote compute profiles from the drop-down lists, and then select **Continue**.

   The selections define the resources where VMs can consume VMware HCX services.

> **Note**
>
> In a mixed-mode SDDC with an AV64 cluster, deploying service mesh appliances on the AV64 cluster is not viable or supported. Nevertheless, this doesn't impede you from conducting HCX migration or network extension directly onto AV64 clusters. The deployment container can be cluster-1, hosting the HCX appliances.





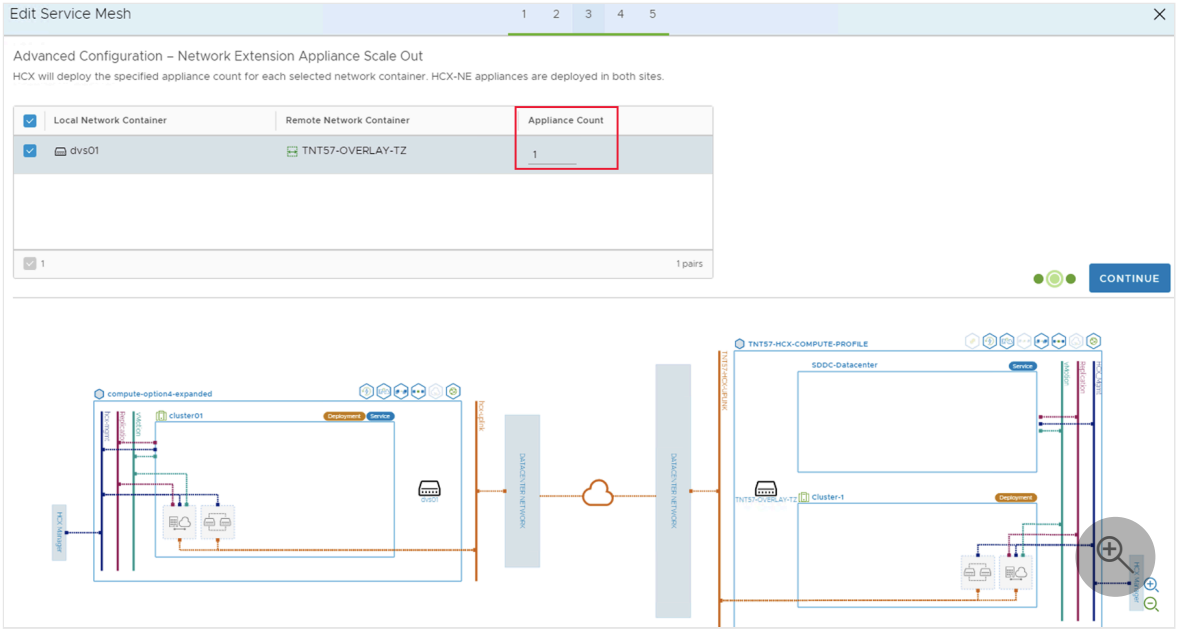
4. Review services to be enabled, and then select **Continue**.

5. In **Advanced Configuration - Override Uplink Network profiles**, select **Continue**.

   Uplink network profiles connect to the network through which the remote site's interconnect appliances can be reached.

6. In **Advanced Configuration - Network Extension Appliance Scale Out**, review and select **Continue**.

   You can have up to eight VLANs per appliance, but you can deploy another appliance to add another eight VLANs. You must also have IP space to account for the more appliances, and it's one IP per appliance. For more information, see VMware HCX Configuration Limits.

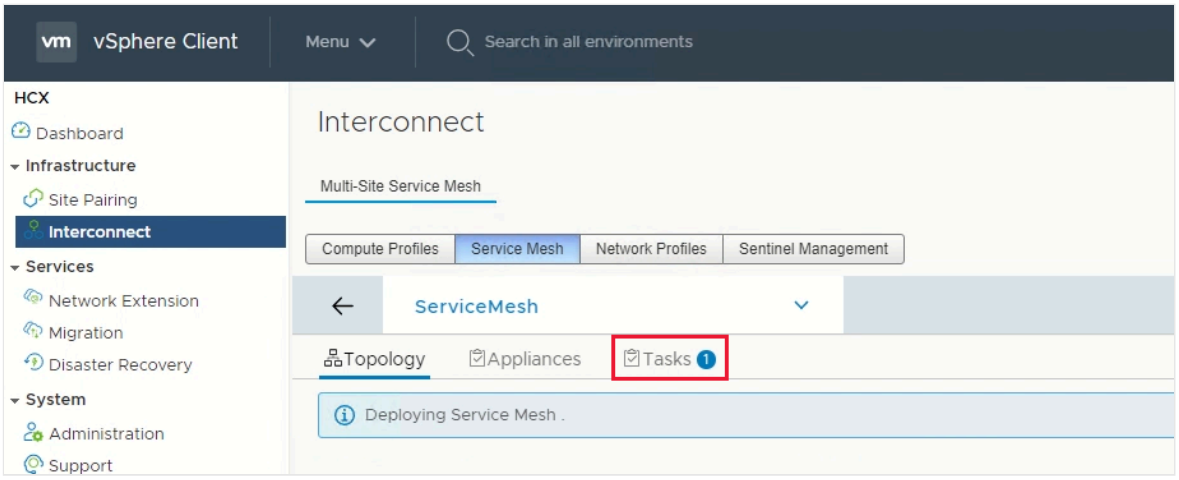


7. In **Advanced Configuration - Traffic Engineering**, review and make any modifications that you feel are necessary, and then select **Continue**.

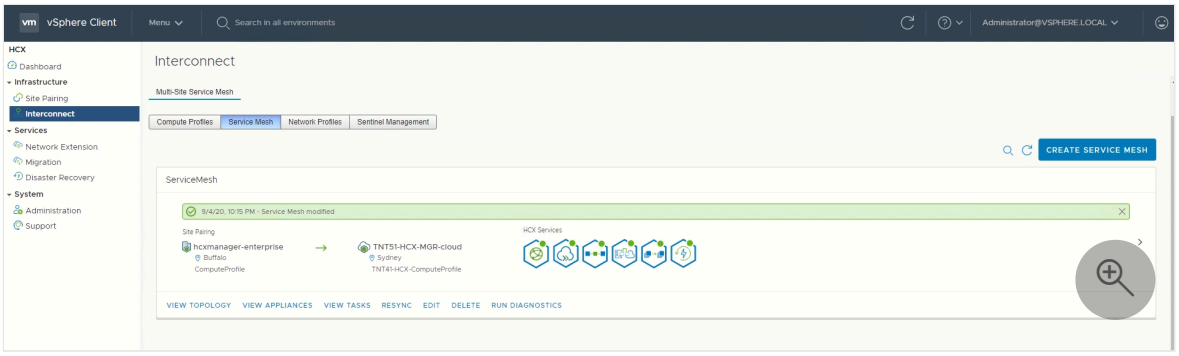
8. Review the topology preview and select **Continue**.

9. Enter a user-friendly name for this service mesh and select **Finish** to complete.

10. Select **View Tasks** to monitor the deployment.

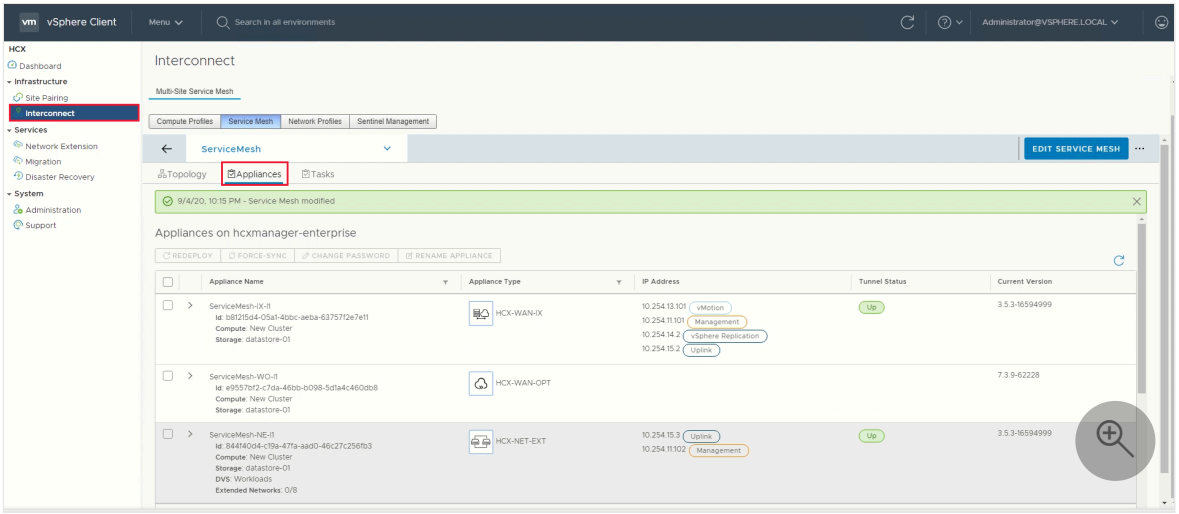


When the service mesh deployment finishes successfully, the services show as green.

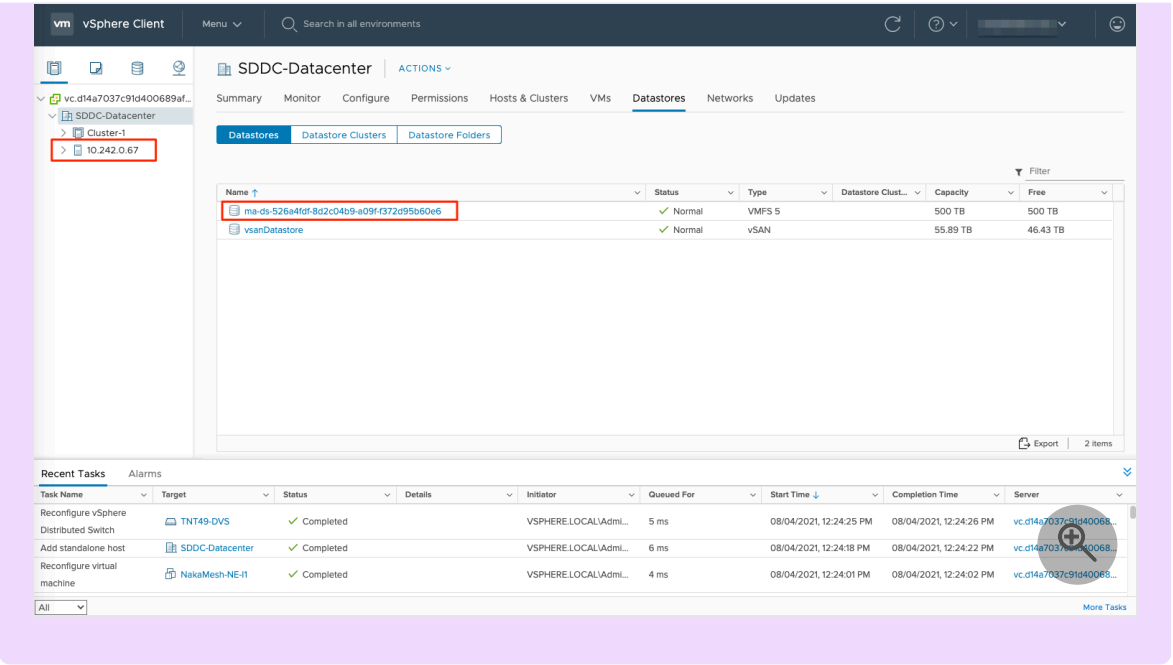


11. Verify the service mesh's health by checking the appliance status.

12. Select **Interconnect** > **Appliances**.



> **Note**
>
> After establishing the service mesh, you may notice a new datastore and a new host in your private cloud. This is normal behavior after establishing a service mesh.



The HCX interconnect tunnel status should display **UP** in green. Now you're ready to migrate and protect Azure VMware Solution VMs using VMware HCX. Azure VMware Solution supports workload migrations with or without a network extension that allow you to migrate workloads in your vSphere environment, create networks on-premises, and deploy VMs onto those networks. For more information, see the VMware HCX Documentation.

For an end-to-end overview of this procedure, watch the Azure VMware Solution: Service Mesh video.

Next steps

Now that you configured the HCX Connector, explore the following articles:

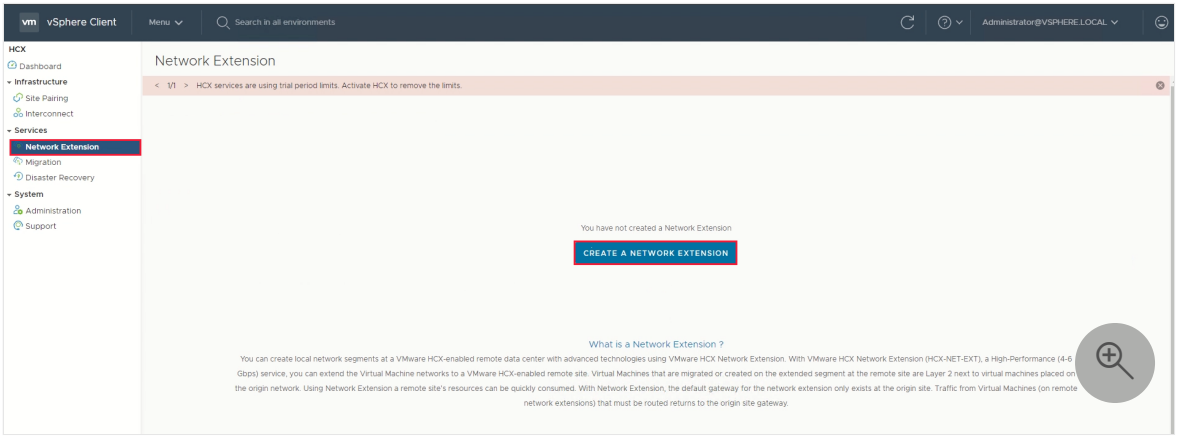
- Create an HCX network extension
- VMware HCX Mobility Optimized Networking (MON) guidance

Create an HCX network extension

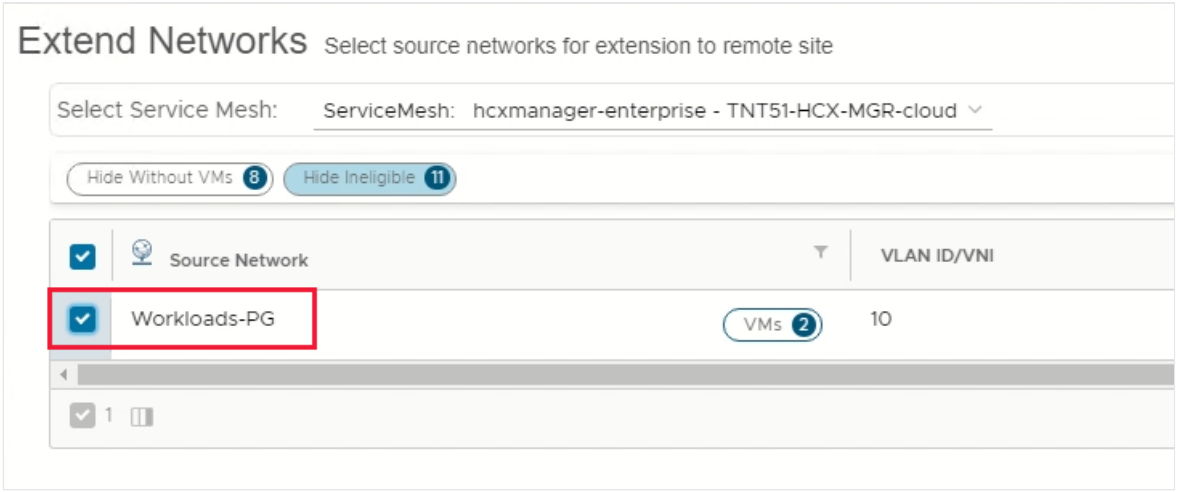
Article • 12/08/2023

Create an HCX network extension is an optional step to extend any networks from your on-premises environment to Azure VMware Solution.

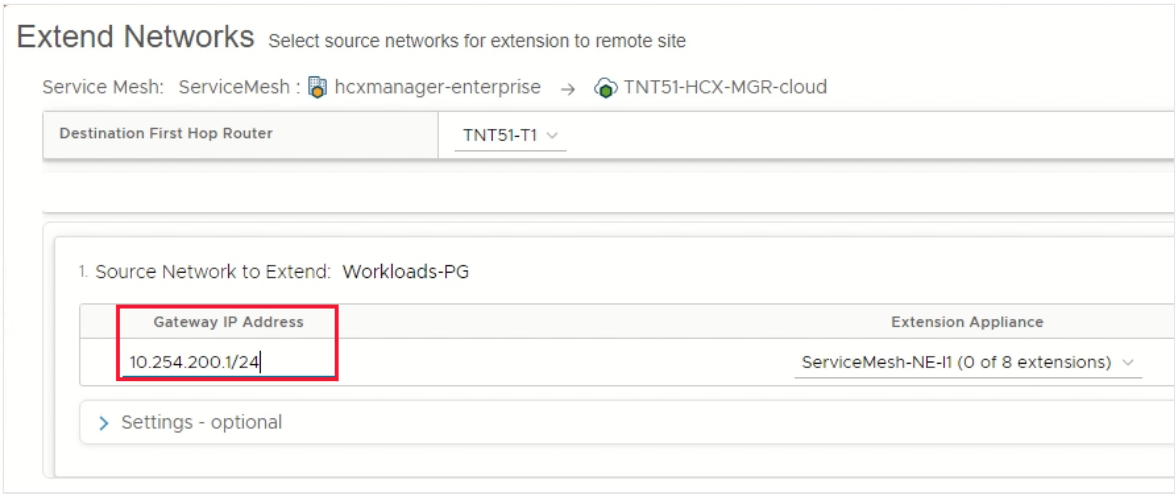
1. Under **Services**, select **Network Extension** > **Create a Network Extension**.



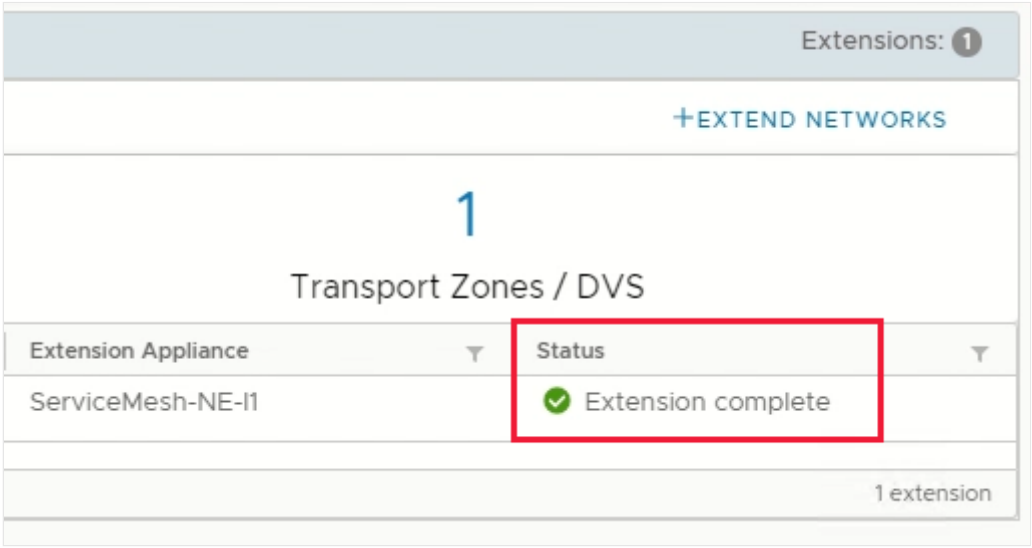
2. Select each of the networks you want to extend to Azure VMware Solution, and then select **Next**.



3. Enter the on-premises gateway IP for each of the networks you're extending, and then select **Submit**.



It takes a few minutes for the network extension to finish. When it does, you see the status change to **Extension complete**.



Next steps

Now that you configured the HCX Network Extension, learn more about:

- VMware HCX Mobility Optimized Networking (MON) guidance

VMware HCX Mobility Optimized Networking (MON) guidance

Article • 02/28/2024

> **Note**
>
> VMware HCX Mobility Optimized Networking is officially supported by VMware and Azure VMware Solution from HCX version 4.1.0.

> **Important**
>
> Before you enable HCX MON, please read the below limitations and unsupported configurations:
>
> **Unsupported source configurations for HCX NE**
>
> **Limitations for any HCX deployment including MON**
>
> VMware HCX Mobility Optimized Networking (MON) is not supported with the use of a 3rd party gateway. It may only be used with the T1 gateway directly connected to the T0 gateway without a network virtual appliance (NVA). You may be able to make this configuration function, but we do not support it.

HCX Mobility Optimized Networking (MON) is an optional feature to enable when using HCX Network Extensions (NE). MON provides optimal traffic routing under certain scenarios to prevent network tromboning between the on-premises and cloud-based resources on extended networks.

As MON is an enterprise capability of the NE feature, make sure you enabled the VMware HCX Enterprise through the Azure portal.

Throughout the migration cycle, MON optimizes application mobility for:

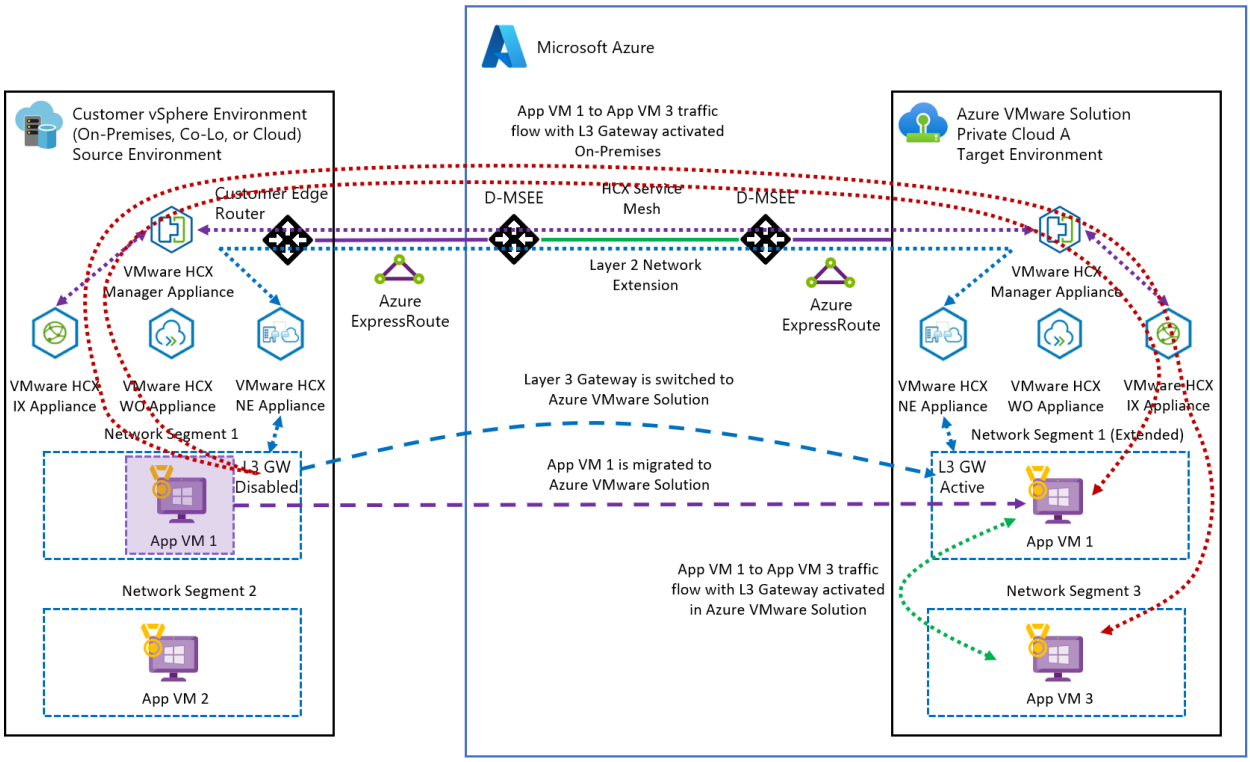
- Optimizing for virtual machine (VM) to VM L2 communication when using stretched networks
- Optimizing and avoiding asymmetric traffic flows between on-premises, Azure VMware Solution, and Azure

In this article, learn about the Azure VMware Solution-specific use cases for MON.

Optimize traffic flows across standard and stretched segments on the private cloud side

In this scenario, VM1 is migrated to the cloud using the NE, which provides optimal VM to VM latency. As a result, VM1 needs low latency to VM3 on the local Azure VMware Solution segment. We migrate the VM1 gateway from on-premises to Azure VMware Solution (cloud) to ensure an optimal path for traffic (blue line). If the gateway remains on-premises (red line), a tromboning effect and higher latency are observed.

> **Note**
>
> When you enable MON without migrating the VM gateway to the cloud side, it doesn't ensure an optimal path for traffic flow. It also doesn't allow the evaluation of policy routes.



Optimize and avoid asymmetric traffic flows

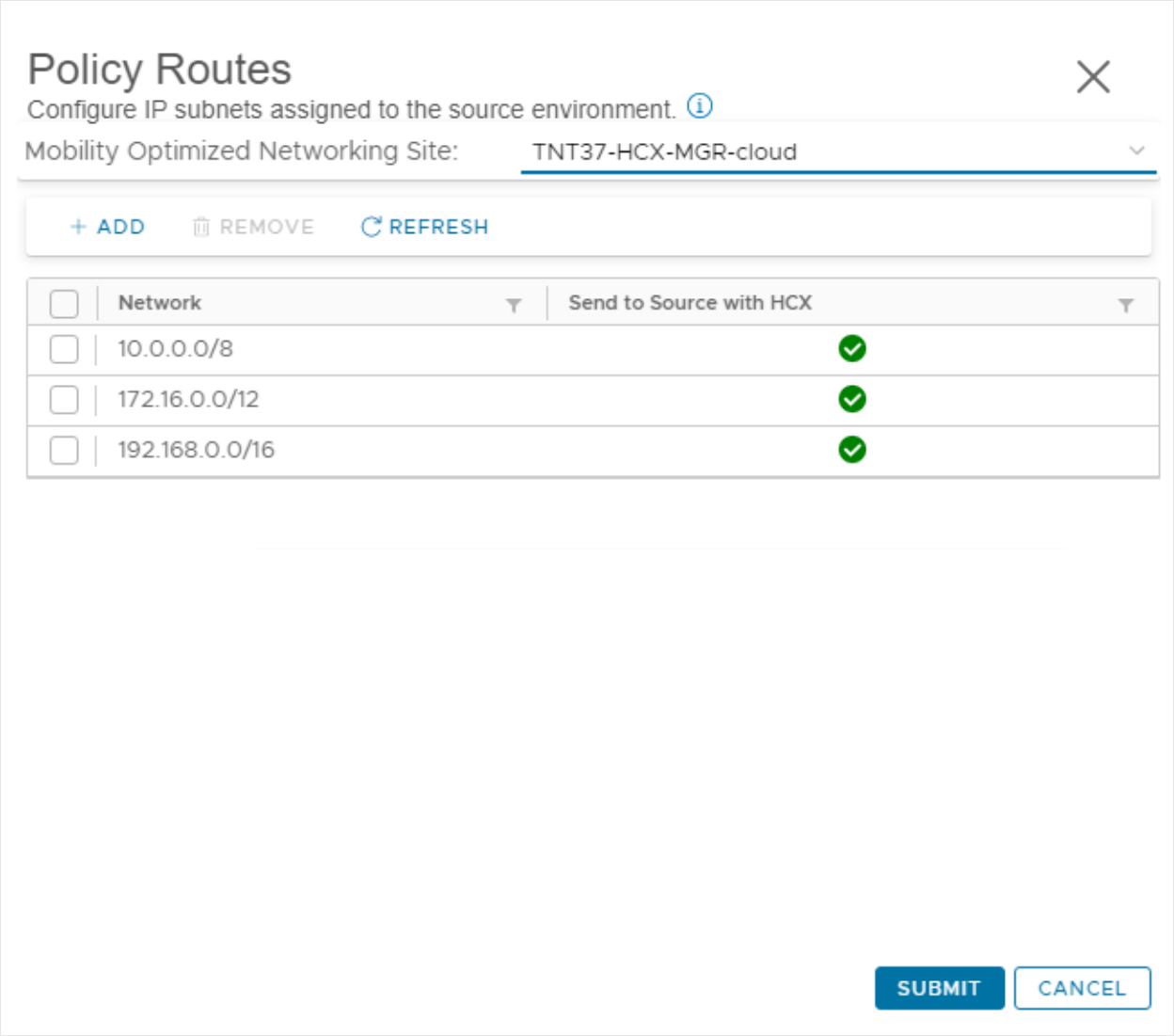
In this scenario, we assume a VM from on-premises is migrated to Azure VMware Solution and participates in L2, and L3 traffic flows back to on-premises to access services. We also assume some VM communication from Azure (in the Azure VMware Solution connected virtual network) could reach down in to the Azure VMware Solution private cloud.

> **Important**
>
> The main point here is to plan and avoid asymmetric traffic flows carefully.

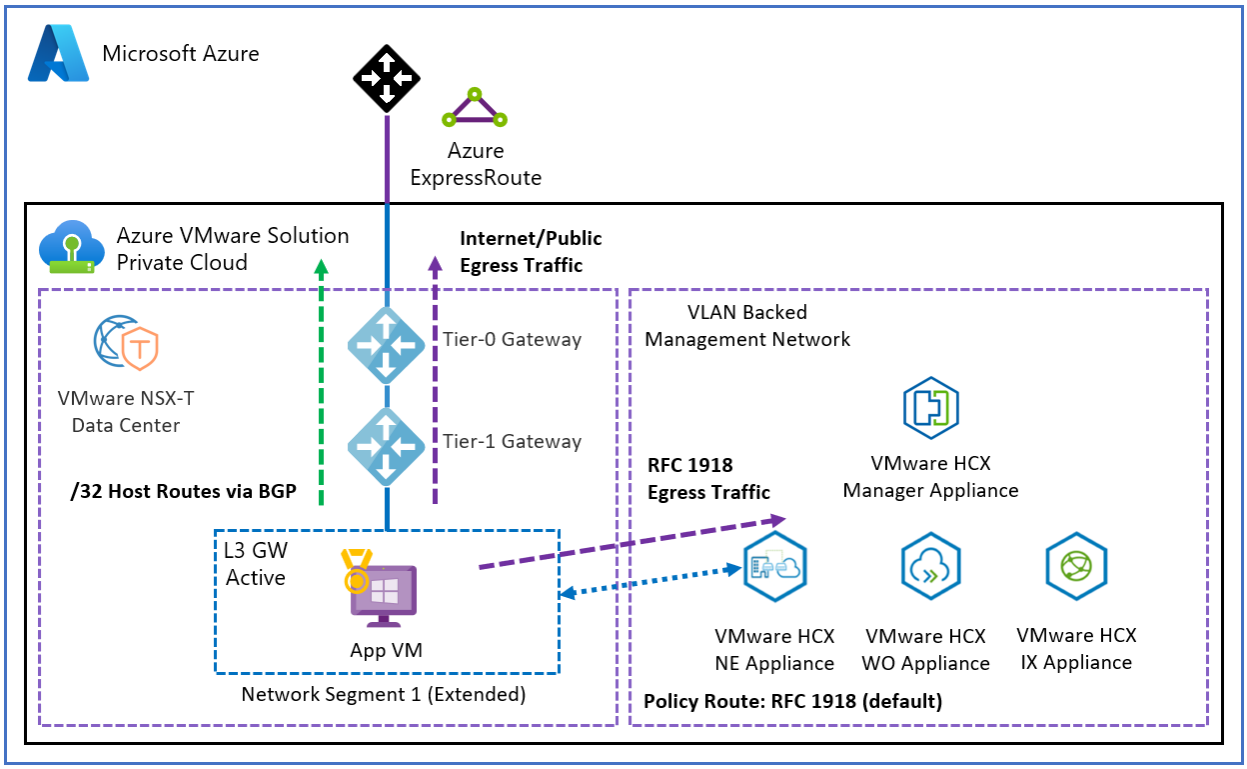
By default and without using MON, a VM in Azure VMware Solution on a stretched network without MON can communicate back to on-premises using the ExpressRoute preferred path. Based on customer use-cases, one should evaluate how a VM on an Azure VMware Solution stretched segment enabled with MON should be traversing back to on-premises, either over the Network Extension or the T0 gateway via the ExpressRoute while keeping traffic flows symmetric.

If choosing the NE path for example, the MON policy routes have to specifically address the subnet at the on-premises side; otherwise, the 0.0.0.0/0 default route is used. Policy routes can be found under the NE segment, by selecting advanced.

By default, all RFC 1918 IP addresses are included in the MON policy routes definition.



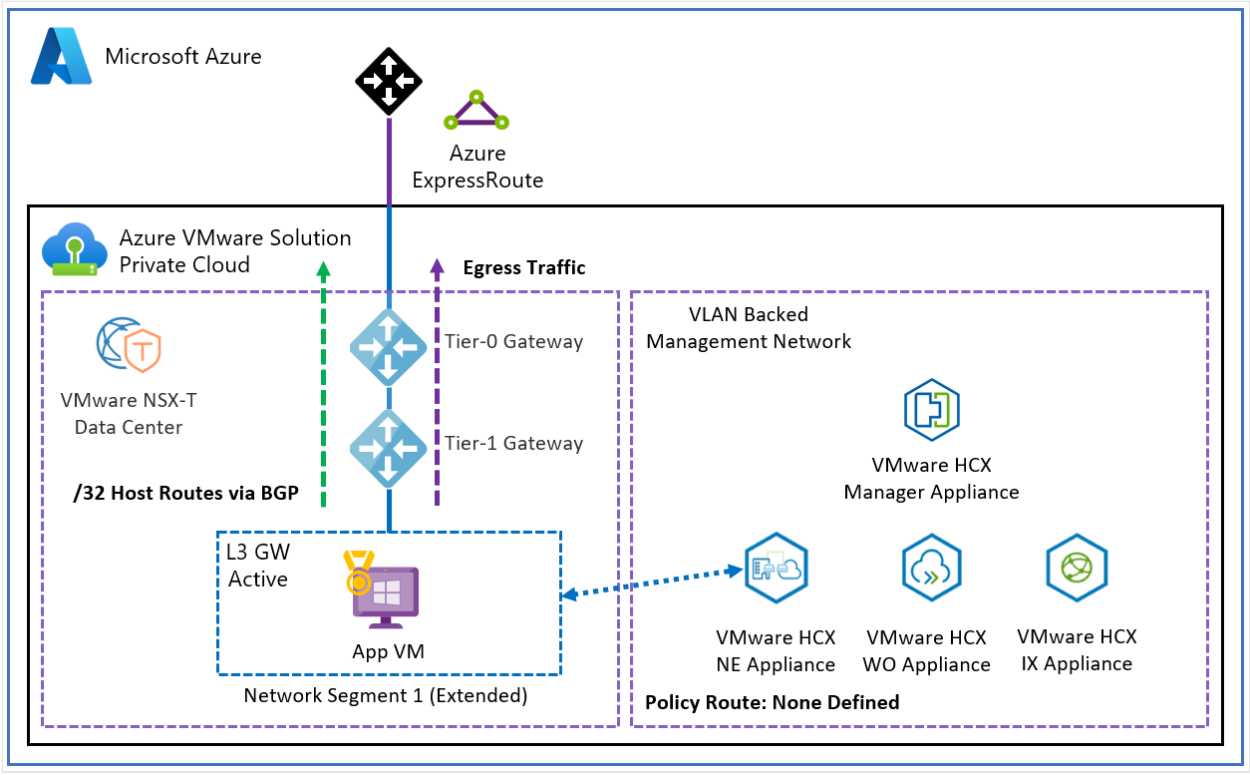
This results in all RFC 1918 egress traffic being tunneled over the NE path and all internet and public traffic being routed to the T0 gateway.



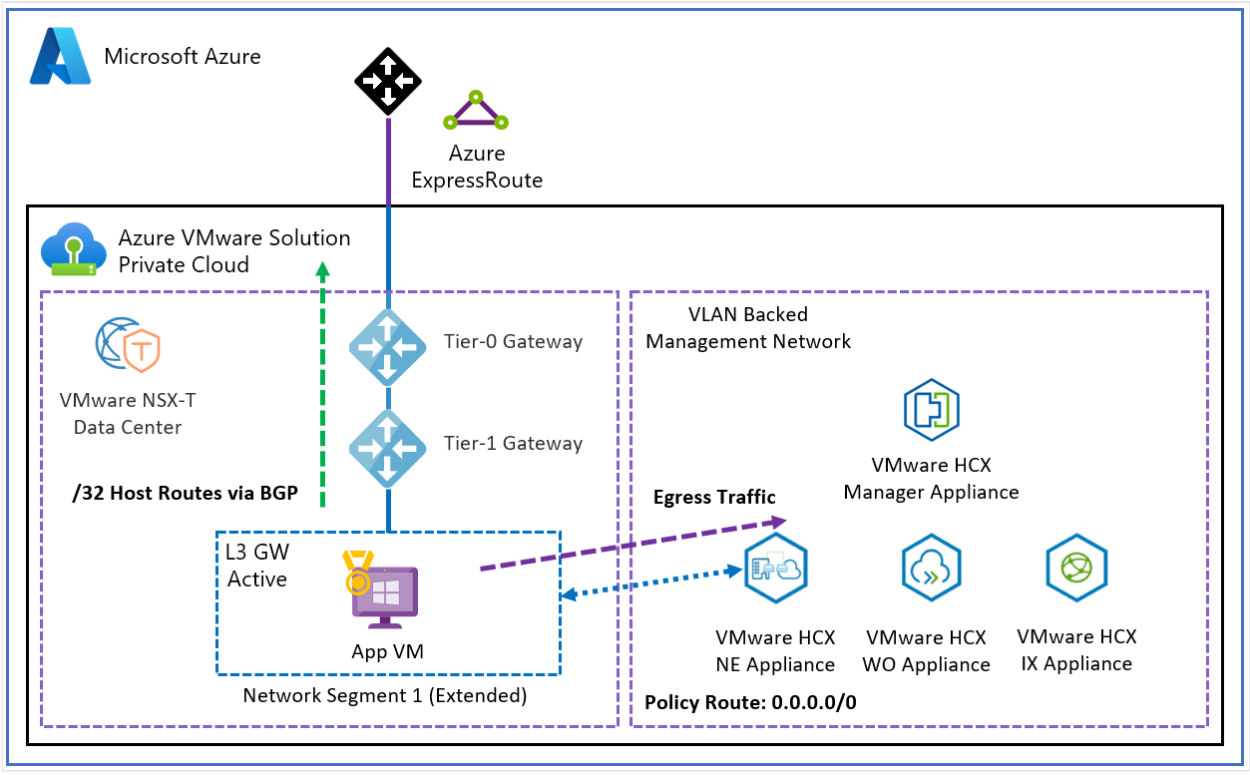
Policy routes are evaluated only if the VM gateway is migrated to the cloud. The effect of this configuration is that any matching subnets for the destination get tunneled over the NE appliance. If not matched, they get routed through the T0 gateway.

> **Note**
>
> Special consideration for using MON in Azure VMware Solution is to give the /32 routes advertised over BGP to its peers; this includes on-premises and Azure over the ExpressRoute connection. For example, a VM in Azure learns the path to an Azure VMware Solution VM on an Azure VMware Solution MON enabled segment. Once the return traffic is sent back to the T0 gateway as expected, if the return subnet is an RFC 1918 match, traffic is forced over the NE instead of the T0. Then egresses over the ExpressRoute back to Azure on the on-premises side. This can cause confusion for stateful firewalls in the middle and asymmetric routing behavior. It's also a good idea to determine how VMs on NE MON segments will need to access the internet, either via the T0 gateway in Azure VMware Solution or only through the NE back to on-premises. In general, all of the default policy routes should be removed to avoid asymmetric traffic. Only enable policy routes if the network infrastructure as been configured in such a way to account for and prevent asymmetric traffic.

The MON policy routes can be deleted with none defined. This results in all egress traffic being routed to the T0 gateway.



The MON policy routes can be updated with a default route (0.0.0.0/0). This results in all egress traffic being tunneled over the NE path.



As outlined in the above diagrams, the importance is to match a policy route to each required subnet. Otherwise, the traffic gets routed over the T0 and not tunneled over the NE.

To learn more about policy routes, see Mobility Optimized Networking Policy Routes.

HCX Network extension high availability (HA)

Article • 12/06/2023

VMware HCX is an application mobility platform designed to simplify application migration, workload rebalancing, and business continuity across data centers and clouds.

The HCX Network Extension service provides layer 2 connectivity between sites. Network Extension HA protects extended networks from a Network Extension appliance failure at either the source or remote site.

HCX 4.3.0 or later allows network extension high availability. Network Extension HA operates in Active/Standby mode. In this article, learn how to configure HCX network extension High Availability on Azure private cloud.

Prerequisites

The Network Extension High Availability (HA) setup requires four Network Extension appliances, with two appliances at the source site and two appliances at the remote site. Together, these two pairs form the HA Group, which is the mechanism for managing Network Extension High Availability. Appliances on the same site require a similar configuration and must have access to the same set of resources.

- Network Extension HA requires an HCX Enterprise license.
- In the HCX Compute Profile, the Network Extension Appliance Limit is set to allow for the number of Network Extension appliances. The Azure VMware Solutions Limit is automatically set to unlimited.
- In the HCX Service Mesh, the Network Extension Appliance Scale Out Appliance Count is set to provide enough appliances to support network extension objectives, including any Network Extension HA groups.

When you create a service mesh, set the appliance count to a minimum of two. For an existing service mesh, you can edit and adjust the appliance count to provide the required appliance count.

- The Network Extension appliances selected for HA activation must have no networks extended over them.
- Only Network Extension appliances upgraded to HCX 4.3.0 or later can be added to HA Groups.

- Learn more about the Network Extension High Availability feature, prerequisites, considerations and limitations.

Activate high availability (HA)

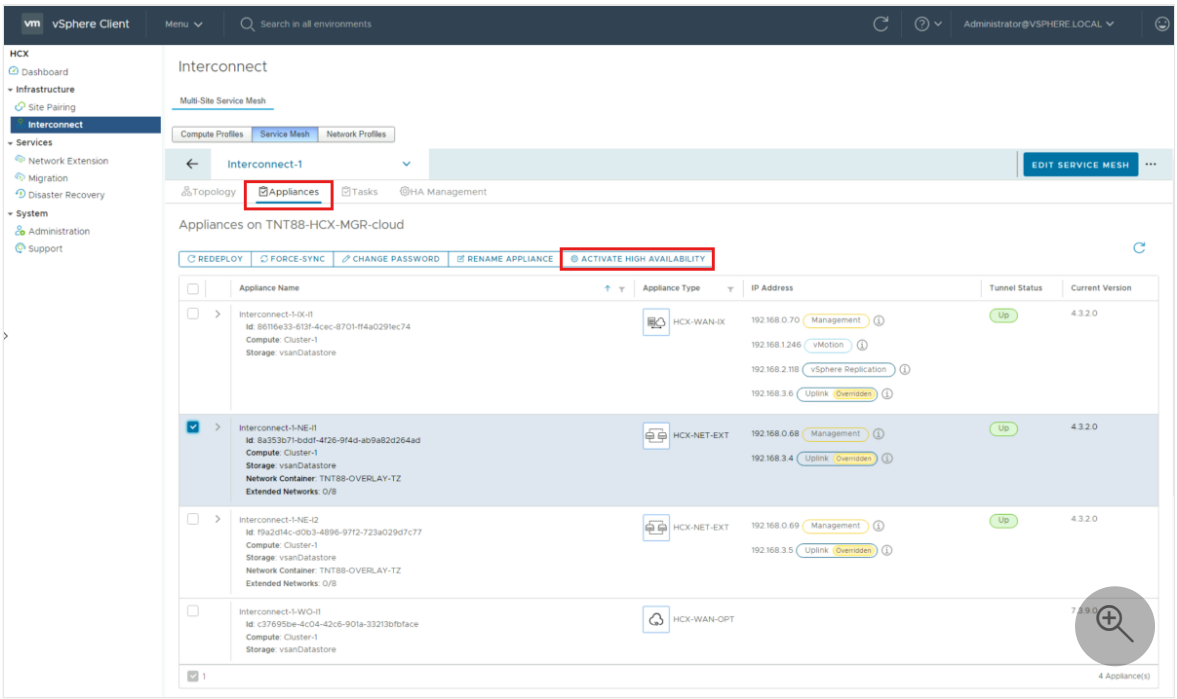
Use the following steps to activate HA, create HA groups, and view the HA roles and options available.

1. Sign in to HCX Manager UI in one of two ways:
   a. cloudadmin@vsphere.local.
   b. HCX UI through vCenter HCX Plugin.

2. Navigate to **Infrastructure**, then **Interconnect**.

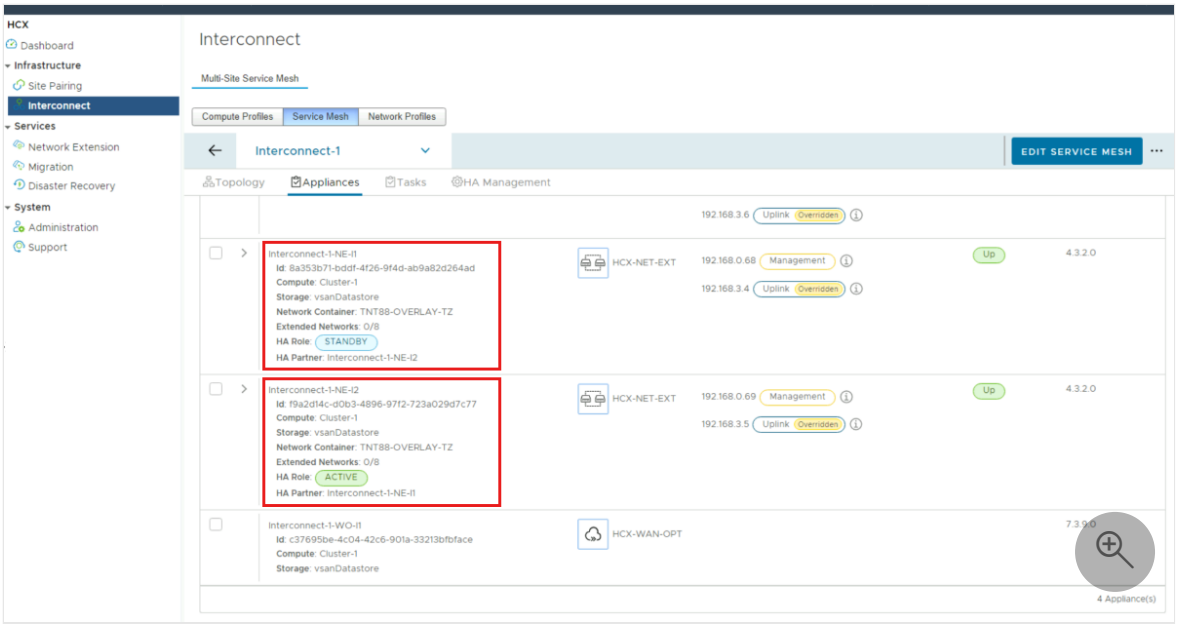
3. Select **Service Mesh**, then select **View Appliances**.

4. Select **Appliances** from the **Interconnect** tab options.
   a. Check the network appliance that you want to make highly available and select **Activate High Availability**.

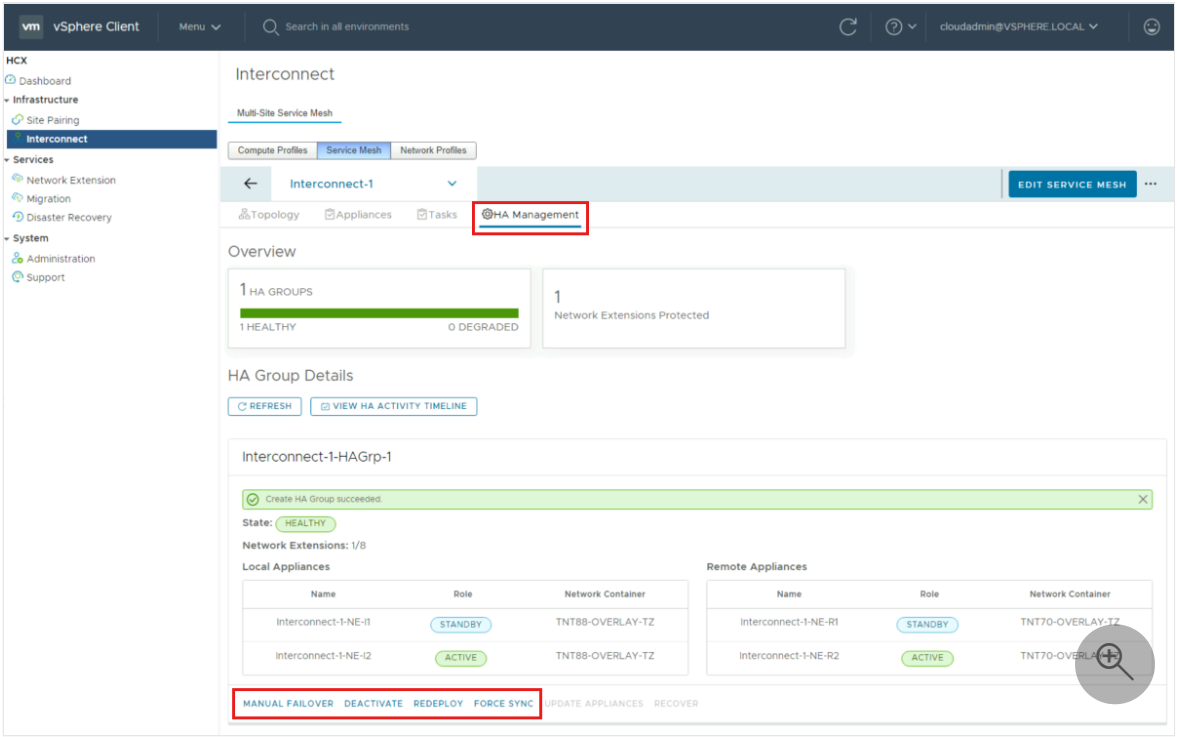


5. Confirm by selecting **Activate HA**.
   a. Activating HA initiates the process to create an HA group. The process automatically selects an HA partner from the available NE Appliances.

6. After the HA group is created, the **HA Roles** for the local and remote appliances display **Active** and **Standby**.



7. Select **HA Management** from the **Interconnect** tab options to view the HA group details and the available options: **Manual failover, Deactivate, Redeploy, and Force Sync**.

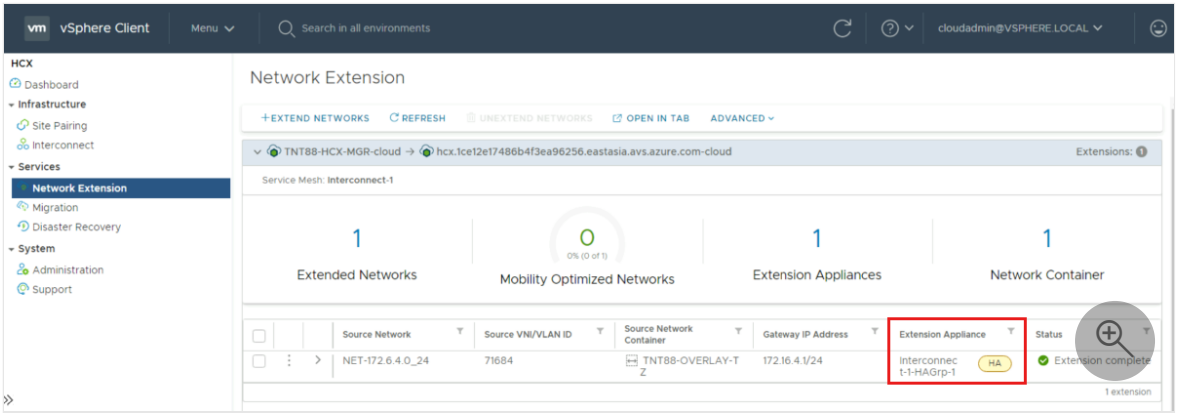


Extend network using network HA group

1. Locate **Services** in the left navigation and select **Network Extension**.
2. Select **Create a Network Extension**.
3. Choose the Network you want and select **Next**.

4. In **mandatory fields**, provide the gateway IP address in CIDR format, select the HA group under **Extension Appliances** (created in the previous step), and select **Submit** to extend the Network.

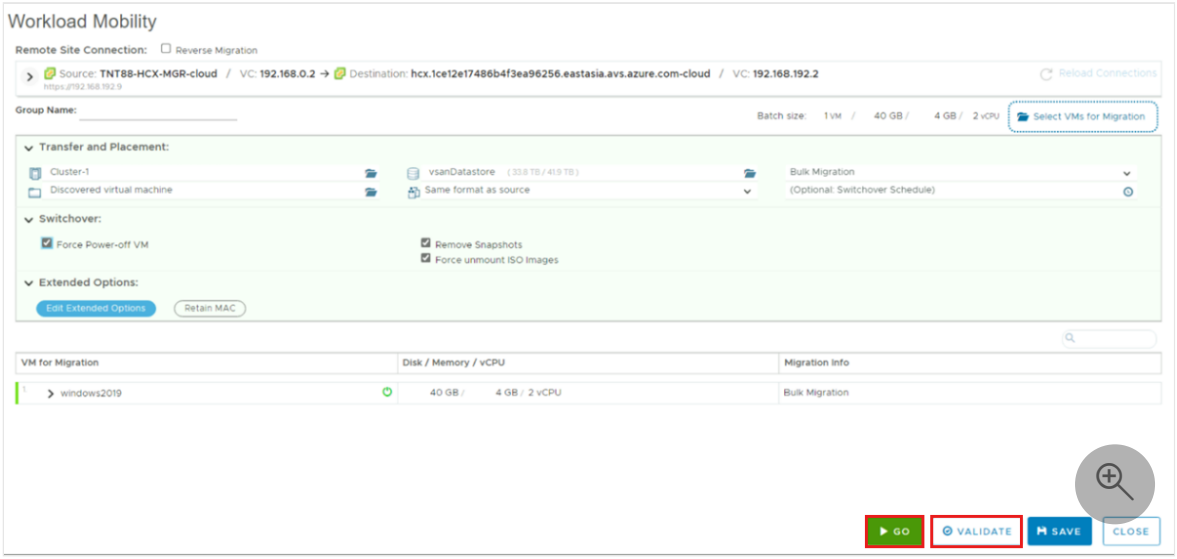
5. After the network is extended, under **Extension Appliance**, you can see the extension details and HA group.



6. To migrate virtual machines (VMs), navigate to **Services** and select **Migration**.
   a. Select **Migrate** from the **Migration** window to start the workload mobility wizard.

7. In **Workload Mobility**, add and replace details as needed, then select **Validate**.

8. After validation completes, select **Go** to start the migration using Extended Network.



Next steps

Now that you learned how to configure and extend HCX network extension high availability (HA), use the following resource to learn more about how to manage HCX network extension HA.

Managing Network Extension High Availability

Enable HCX access over the internet

Article • 12/12/2023

In this article, learn how to perform HCX migration over a public IP address using Azure VMware Solution.

> **Important**
>
> Before configuring a public IP on your Azure VMware Solution private cloud, consult your network administrator to understand the implications and the impact to your environment.

You also learn how to pair HCX sites and create service mesh from on-premises to an Azure VMware Solution private cloud using Public IP. The service mesh allows you to migrate a workload from an on-premises datacenter to an Azure VMware Solution private cloud over the public internet. This solution is useful when the customer isn't using ExpressRoute or VPN connectivity with the Azure cloud.

> **Important**
>
> The on-premises HCX appliance should be reachable from the internet to establish HCX communication from on-premises to the Azure VMware Solution private cloud.

Configure public IP block

For HCX manager to be available over the public IP address, you need one public IP address for DNAT rule.

To perform HCX migration over the public internet, you need other IP addresses. You can have a /29 subnet to create minimum configuration when defining HCX network profile (usable IPs in subnet are assigned to IX, NE appliances). You can choose a bigger subnet based on the requirements. Create an NSX-T segment using this public subnet. This segment can be used for creating HCX network profile.

> **Note**

After assigning a subnet to NSX-T segment, you can't use an IP from that subnet to create a DNAT rule. Both subnets should be different.

Configure a Public IP block through portal by using the Public IP feature of the Azure VMware Solution private cloud.

Use public IP address for Cloud HCX Manager public access

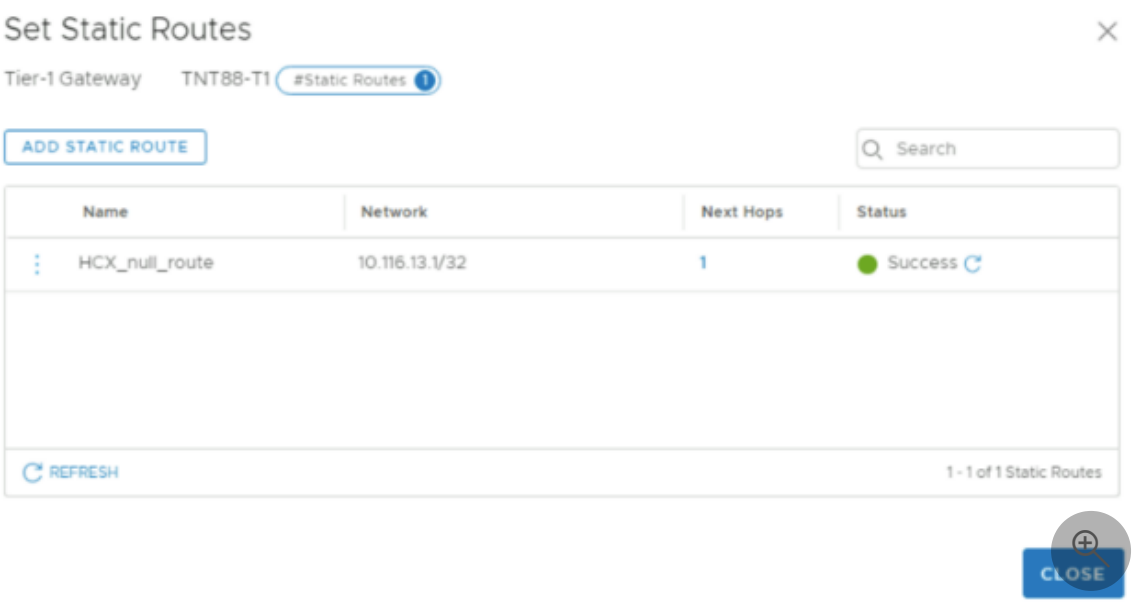
Cloud HCX manager can be available over a public IP address by using a DNAT rule. However, since Cloud HCX manager is in the provider space, the null route is necessary to allow HCX Manager to route back to the client by way of the DNAT rule. It forces the NAT traffic through NSX-T Tier-0 router.

Add static null route to the Tier 1 router

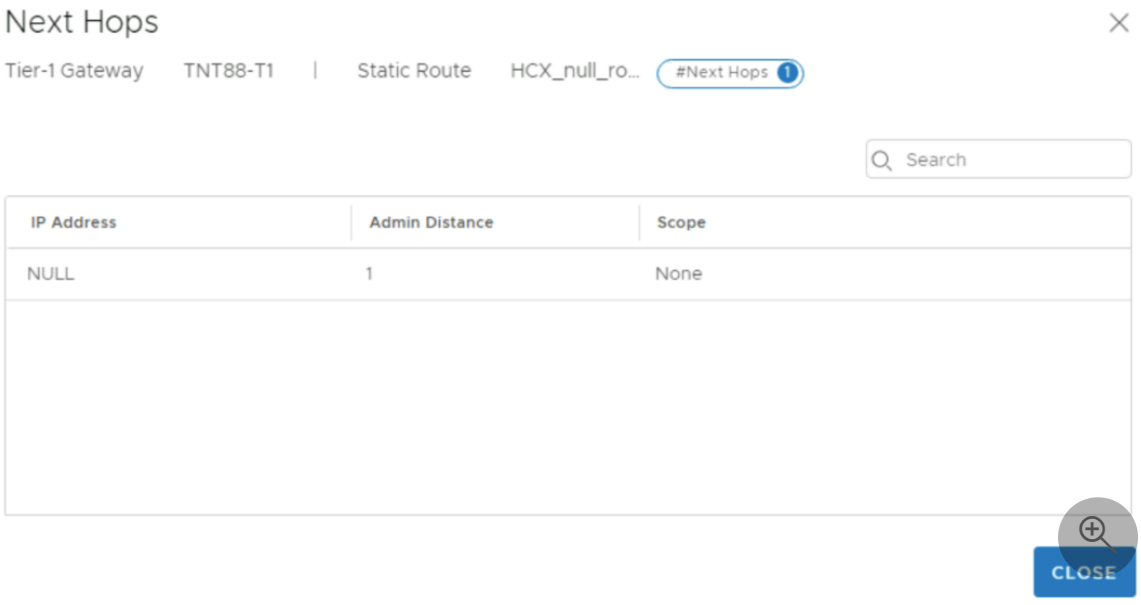
The static null route is used to allow HCX private IP to route through the NSX Tier-1 for public endpoints. This static route can be the default Tier-1 router created in your private cloud or you can create a new tier-1 router.

1. Sign in to NSX-T manager, and select **Networking**.
2. Under the **Connectivity** section, select **Tier-1 Gateways**.
3. Edit the existing Tier-1 gateway.
4. Expand **STATIC ROUTES**.
5. Select the number next to **Static Routes**.
6. Select **ADD STATIC ROUTE**.
   A pop-up window is displayed.
7. Under **Name**, enter the name of the route.
8. Under **Network**, enter a nonoverlapping /32 IP address under Network.

> **Note**
>
> This address should not overlap with any other IP addresses on the private cloud network and the customer network.



9. Under **Next hops**, select **Set**.
10. Select **NULL** as IP Address.
    Leave defaults for Admin distance and scope.
11. Select **ADD**, then select **APPLY**.
12. Select **SAVE**, then select **CLOSE**.



13. Select **CLOSE EDITING**.

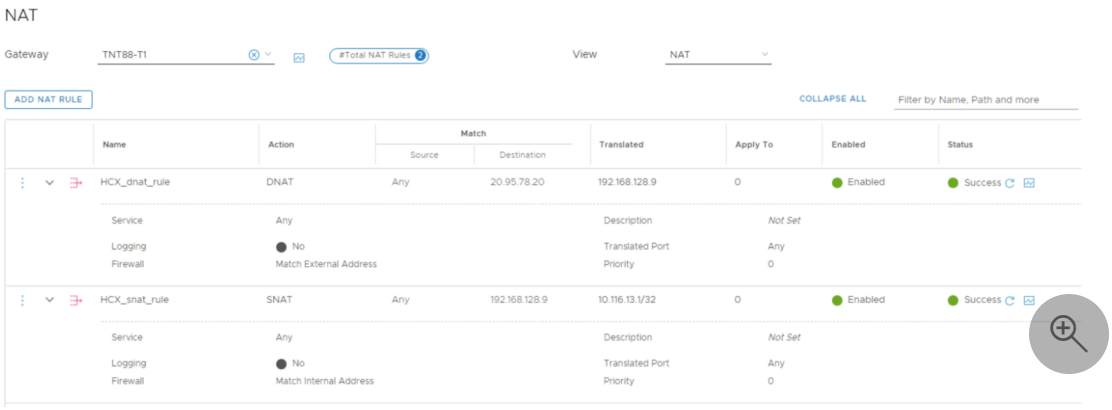
Add NAT rule to Tier-1 gateway

1. Sign in to NSX-T Manager, and select **Networking**.
2. Select **NAT**.

3. Select the Tier-1 Gateway. Use same Tier-1 router to create NAT rule that you used to create null route in previous steps.

4. Select **ADD NAT RULE**.

5. Add one SNAT rule and one DNAT rule for HCX Manager.
   a. The DNAT Rule Destination is the Public IP for HCX Manager. The Translated IP is the HCX Manager IP in the cloud.
   b. The SNAT Rule Destination is the HCX Manager IP in the cloud. The Translated IP is the nonoverlapping /32 IP from the Static Route.
   c. Make sure to set the Firewall option on DNAT rule to **Match External Address**.



6. Create Tier-1 Gateway Firewall rules to allow only expected traffic to the Public IP for HCX Manager and drop everything else.
   a. Create a Gateway Firewall rule on the T1 that allows your on-premises as the **Source IP** and the Azure VMware Solution reserved Public as the **Destination IP**. This rule should be the highest priority.
   b. Create a Gateway Firewall rule on the Tier-1 that denies all other traffic where the **Source IP** is **Any** and **Destination IP** is the Azure VMware Solution reserved Public IP.

For more information, see HCX ports

> **Note**
>
> HCX manager can now be accessed over the internet using public IP.

Pair sites using HCX Cloud manager's public IP address

Site pairing is required before you create service mesh between source and destination sites.

1. Sign in to the **Source** site HCX Manager.
2. Select **Site Pairing** and select **ADD SITE PAIRING**.
3. Enter the **Cloud HCX Manager Public URL** as remote site and sign in credentials, then select **Connect**.

After pairing is done, it will appear under site pairing.

Create public IP segment on NSX-T

Before you create a Public IP segment, get your credentials for NSX-T Manager from Azure VMware Solution portal.

1. Under the **Networking** section select **Connectivity**, **Segments**, and then select **ADD SEGMENT**.
2. Provide Segment name, select **Tier-1 router** as connected gateway, and provide the reserved public IP under subnets.
3. Select **Save**.

Create network profile for HCX at destination site

1. Sign in to Destination HCX Manager (cloud manager in this case).
2. Select **Interconnect** and then select the **Network Profiles** tab.
3. Select **Create Network Profile**.
4. Select **NSX Networks** as network type under **Network**.
5. Select the **Public-IP-Segment** created on NSX-T.
6. Enter **Name**.
7. Under IP pools, enter the **IP Ranges** for HCX uplink, **Prefix Length**, and **Gateway** of public IP segment.
8. Scroll down and select the **HCX Uplink** checkbox under **HCX Traffic Type**, this profile is used for the HCX uplink.
9. Select **Create** to create the network profile.

Create service mesh

Service Mesh deploys HCX WAN Optimizer, HCX Network Extension and HCX-IX appliances.

1. Sign in to **Source** site HCX Manager.
2. Select **Interconnect** and then select the **Service Mesh** tab.

3. Select **CREATE SERVICE MESH**.
4. Select the **destination** site to create service mesh with and then select **Continue**.
5. Select the compute profiles for both sites and select **Continue**.
6. Select the HCX services to be activated and select **Continue**.

   > ⓘ **Note**
   >
   > Premium services require an additional HCX Enterprise license.

7. Select the network profile of source site.
8. Select the network profile of destination that you created in the **Network Profile** section.
9. Select **Continue**.
10. Review the **Transport Zone** information, and then select **Continue**.
11. Review the **Topological view**, and select **Continue**.
12. Enter the **Service Mesh name** and select **FINISH**.
13. Add the public IP addresses in firewall to allow required ports only.

Extend network

The HCX Network Extension service provides layer 2 connectivity between sites. The extension service also allows you to keep the same IP and MAC addresses during virtual machine migrations.

1. Sign in to **source** HCX Manager.
2. Under the **Network Extension** section, select the site for which you want to extend the network, and then select **EXTEND NETWORKS**.
3. Select the network that you want to extend to destination site, and select **Next**.
4. Enter the subnet details of network that you're extending.
5. Select the destination first hop route (Tier-1), and select **Submit**.
6. Sign in to the **destination** NSX, you see that Network 10.14.27.1/24 is now extended.

After the network is extended to destination site, VMs can be migrated over Layer 2 extension.

Next steps

Enable Public IP to the NSX Edge for Azure VMware Solution

For detailed information on HCX network underlay minimum requirements, see Network Underlay Minimum Requirements.

Upgrade HCX on Azure VMware Solution

Article • 12/20/2023

In this article, you learn how to upgrade Azure VMware Solution for HCX service updates, which can include new features, software fixes, or security patches.

You can update HCX Connector and HCX Cloud systems during separate maintenance windows, but for optimal compatibility, we recommend you update both systems together. Apply service updates during a maintenance window where no new HCX operations are queued up.

> **Important**
>
> Starting with HCX 4.4.0, HCX appliances install the VMware Photon Operating System. When upgrading to HCX 4.4.x or later from an HCX version prior to version 4.4.0, you must also upgrade all Service Mesh appliances.

System requirements

- For systems requirements, compatibility, and upgrade prerequisites, see the VMware HCX release notes.
- For more information about the upgrade path, see the Product Interoperability Matrix.
- For information regarding VMware product compatibility by version, see the Compatibility Matrix.
- Review VMware Software Versioning, Skew and Legacy Support Policies here.
- Ensure HCX manager and site pair configurations are healthy.
- As part of HCX update planning, and to ensure that HCX components are updated successfully, review the service update considerations and requirements. For planning HCX upgrade, see Planning for HCX Updates.
- Ensure that you have a backup and snapshot of HCX connector in the on-premises environment, if applicable.

Backup HCX

- Azure VMware Solution backs up HCX Cloud Manager configuration daily.
- Use the appliance management interface to create backup of HCX in on-premises, see Backing Up HCX Manager. You can use the configuration backup to restore the appliance to its state before the backup. The contents of the backup file supersede configuration changes made before restoring the appliance.
- HCX cloud manager snapshots are taken automatically during upgrades to HCX 4.4 or later. HCX retains automatic snapshots for 24 hours before deleting them. To take a manual snapshot on HCX Cloud Manager or help with reverting from a snapshot, create a support ticket.

Upgrade HCX

The upgrade process is in two steps:

1. Upgrade HCX Manager
   a. HCX cloud manager
   b. HCX connector (You can update site-paired HCX Managers simultaneously)
2. Upgrade HCX Service Mesh appliances

Upgrade HCX manager

The HCX update is first applied to the HCX Manager systems.

What to expect

- HCX manager is rebooted as part of the upgrade process.
- HCX vCenter Plugins are updated.
- There's no data-plane outage during this procedure.

Prerequisites

- Verify the HCX Manager system reports healthy connections to the connected (vCenter Server, NSX Manager (if applicable).
- Verify the HCX Manager system reports healthy connections to the HCX Interconnect service components. (Ensure HCX isn't in an out of sync state)
- Verify that Site Pair configurations are healthy.
- No VM migrations should be in progress during this upgrade.

Procedure

To follow the HCX Manager upgrade process, see Upgrading the HCX Manager

Upgrade HCX Service Mesh appliances

While Service Mesh appliances are upgraded independently to the HCX Manager, they must be upgraded. These appliances are flagged for new available updates anytime the HCX Manager has newer software available.

What to expect

- Service VMs are rebooted as part of the upgrade.
- There's a small data plane outage during this procedure.
- In-service upgrade of Network-extension can be considered to reduce downtime during HCX Network extension upgrades.

Prerequisites

- All paired HCX Managers on both the source and the target site are updated and all services are returned to a fully converged state.
- Service Mesh appliances must be initiated using the HCX plug-in of vCenter or the 443 console at the source site
- No VM migrations should be in progress during this upgrade.

Procedure

To follow the Service Mesh appliances upgrade process, see Upgrading the HCX Service Mesh Appliances

FAQ

What is the impact of an HCX upgrade?

Apply service updates during a maintenance window where no new HCX operations and migration are queued up. The upgrade window accounts for a brief disruption to the Network Extension service, while the appliances are redeployed with the updated code. For individual HCX component upgrade impact, see Planning for HCX Updates.

Do I need to upgrade the service mesh appliances?

The HCX Service Mesh can be upgraded once all paired HCX Manager systems are updated, and all services are returned to a fully converged state. Check HCX release notes for upgrade requirements. Starting with HCX 4.4.0, HCX appliances installed the

VMware Photon Operating System. When upgrading to HCX 4.4.x or later from an HCX version prior to 4.4.0 version, you must upgrade all Service Mesh appliances.

How do I roll back HCX upgrade using a snapshot?

See Rolling Back an Upgrade Using Snapshots. On the cloud side, open a support ticket to roll back the upgrade.

Next steps

Software Versioning, Skew and Legacy Support Policies

Updating VMware HCX

Use VMware HCX Run Commands

Article • 04/19/2024

In this article, learn how to use VMware HCX Run Commands. Use run commands to perform operations that would normally require elevated privileges through a collection of PowerShell cmdlets. This document outlines the available VMware HCX Run Commands and how to use them.

This article describes two VMware HCX commands: **Restart HCX Manager** and **Scale HCX Manager**.

Restart VMware HCX Manager

This Command checks for active VMware HCX migrations and replications. If none are found, it restarts the VMware HCX Cloud Manager (VMware HCX VM's guest OS).

1. Navigate to the Run Command panel under Operations in an Azure VMware Solution private cloud on the Azure portal. Select package "Microsoft.AVS.HCX" to view available HCX run commands.

2. Select the **Microsoft.AVS.HCX** package dropdown menu and select the **Restart-HcxManager** command.

3. Set parameters and select **Run**. Optional run command parameters.

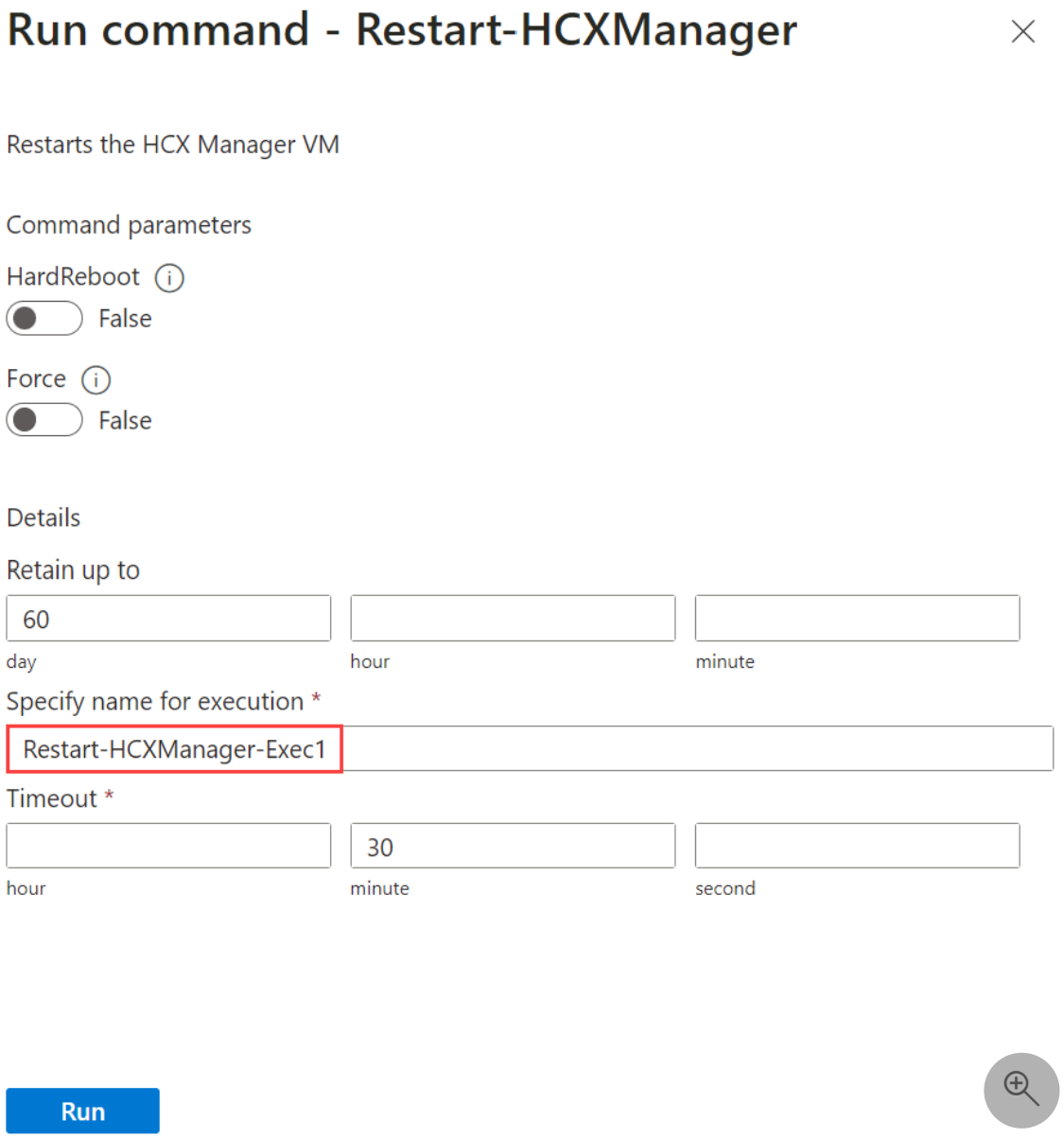
   If the parameters are used incorrectly, they can halt active migrations, and replications and cause other issues. Brief description of each parameter with an example of when it should be used.

   Hard Reboot Parameter - Restarts the virtual machine instead of the default of a GuestOS Reboot. This command is like pulling the power plug on a machine. We don't want to risk disk corruption so a hard reboot should only be used if a normal reboot fails, and all other options are exhausted.

   Force Parameter - If there are ANY active HCX migrations/replications, this parameter avoids the check for active HCX migrations/replications. If the Virtual machine is in a powered off state, this parameter powers the machine on.

   Scenario 1: A customer has a migration that is stuck in an active state for weeks and they need a restart of HCX for a separate issue. Without this parameter, the script fails due to the detection of the active migration. **Scenario 2**: The VMware

HCX Cloud Manager is powered off and the customer would like to power it back on.



4. Wait for command to finish. It can take few minutes for the VMware HCX appliance to come online.

Scale VMware HCX manager

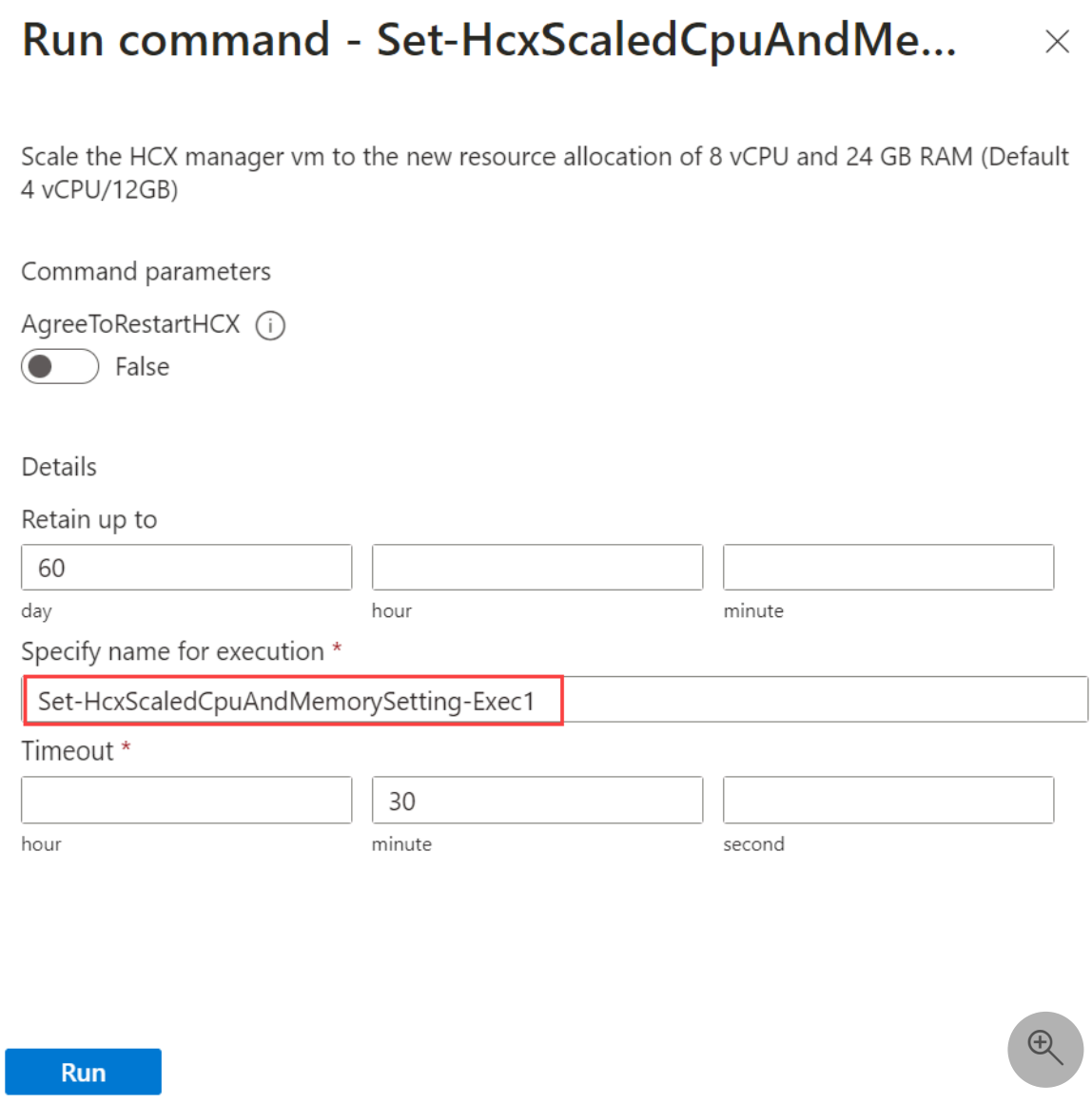
Use the Scale VMware HCX Cloud Manager Run Command to increase the resource allocation of your VMware HCX Cloud Manager virtual machine to 8 vCPUs and 24-GB RAM from the default setting of 4 vCPUs and 12-GB RAM, ensuring scalability.

Scenario: Mobility Optimize Networking (MON) requires VMware HCX Scalability. For more details on MON scaling

Note

VMware HCX Cloud Manager will be rebooted during this operation, and this may affect any ongoing migration processes.

1. Navigate to the Run Command panel on in an Azure VMware Solution private cloud on the Azure portal.
2. Select the **Microsoft.AVS.HCX** package dropdown menu and select the `Set-HcxScaledCpuAndMemorySetting` command.



3. Agree to restart VMware HCX by toggling `AgreeToRestartHCX` to **True**. You need to acknowledge that the virtual machine will be restarted.

> **Note**
>
> If this required parameter is set to false that cmdlet execution will fail.

4. Select **Run** to execute. This process takes between 10-15 minutes.

> **Note**
>
> VMware HCX cloud manager will be unavailable during the scaling.

Next step

To learn more about Run Commands, see Run Commands

Uninstall VMware HCX in Azure VMware Solution

Article • 12/20/2023

In this article, learn how to uninstall HCX in Azure VMware solution. You can uninstall HCX from the cloud side through the portal, which removes the existing pairing and software. Removing HCX returns the resources to your private cloud occupied by the HCX virtual appliances.

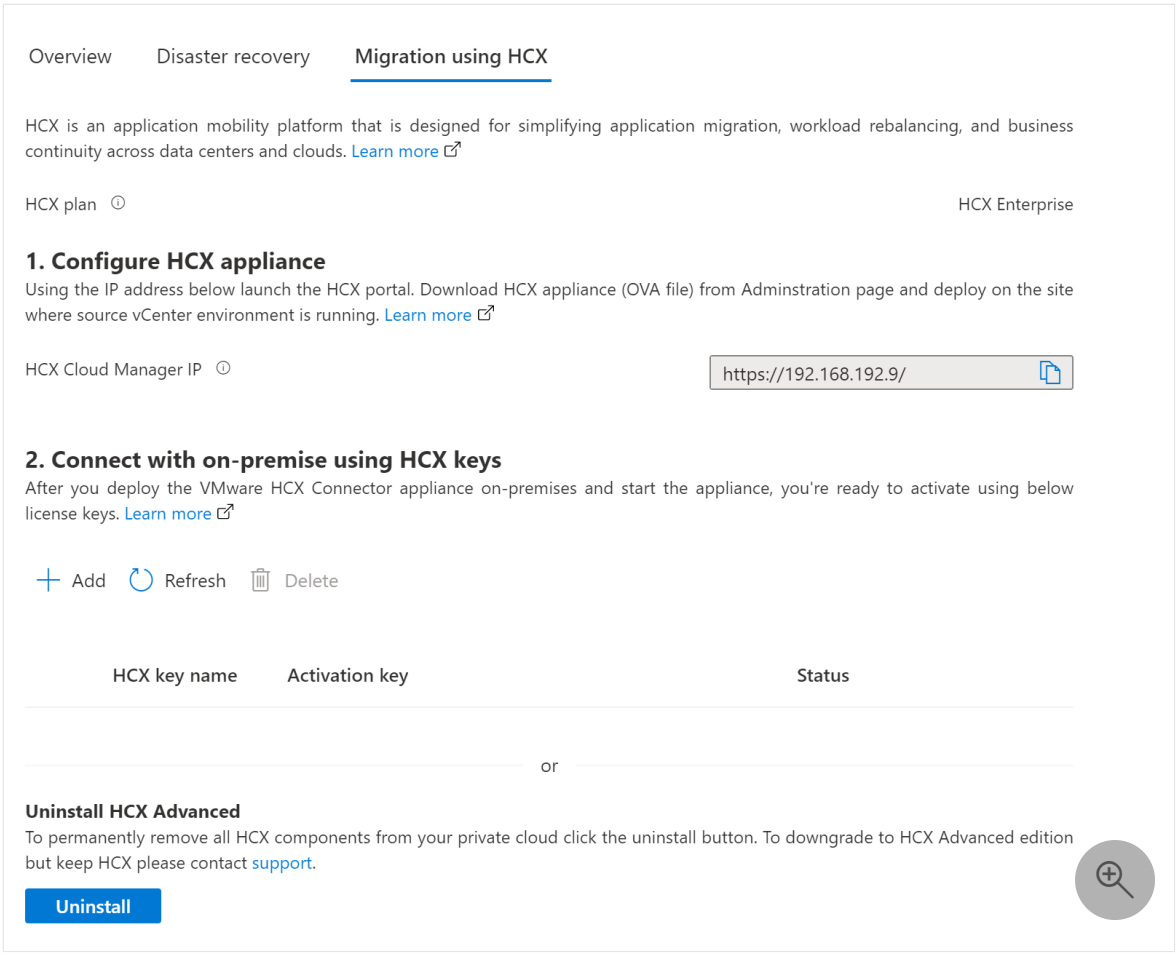
Generally, the workflow cleans up from the HCX on-premises side first, then clean up on the HCX Cloud side afterwards.

Prerequisites

- Make sure you don't have any active migrations in progress.
- Ensure that L2 extensions are no longer needed or the networks are `unstretched` to the destination.
- For workloads using MON, ensure that you removed the default gateways. Otherwise, it can result in workloads not being able to communicate or function.
- Uninstall HCX deployment from Connector on-premises.

Uninstall HCX

1. In your Azure VMware Solution private cloud, select **Manage** > **Add-ons**.
2. Select **Get started** for **HCX Workload Mobility**, then select **Uninstall**.
3. Enter **yes** to confirm the uninstall.



After you uninstall HCX, it no longer has the vCenter Server plugin. If necessary, you can reinstall it.

> Configure VMware HCX in Azure VMware Solution

> VMware blog series - cloud migration

> Install and activate VMware HCX in Azure VMware Solution

Migrate a SQL Server standalone instance to Azure VMware Solution

Article • 12/18/2023

In this article, learn how to migrate a SQL Server standalone instance to Azure VMware Solution.

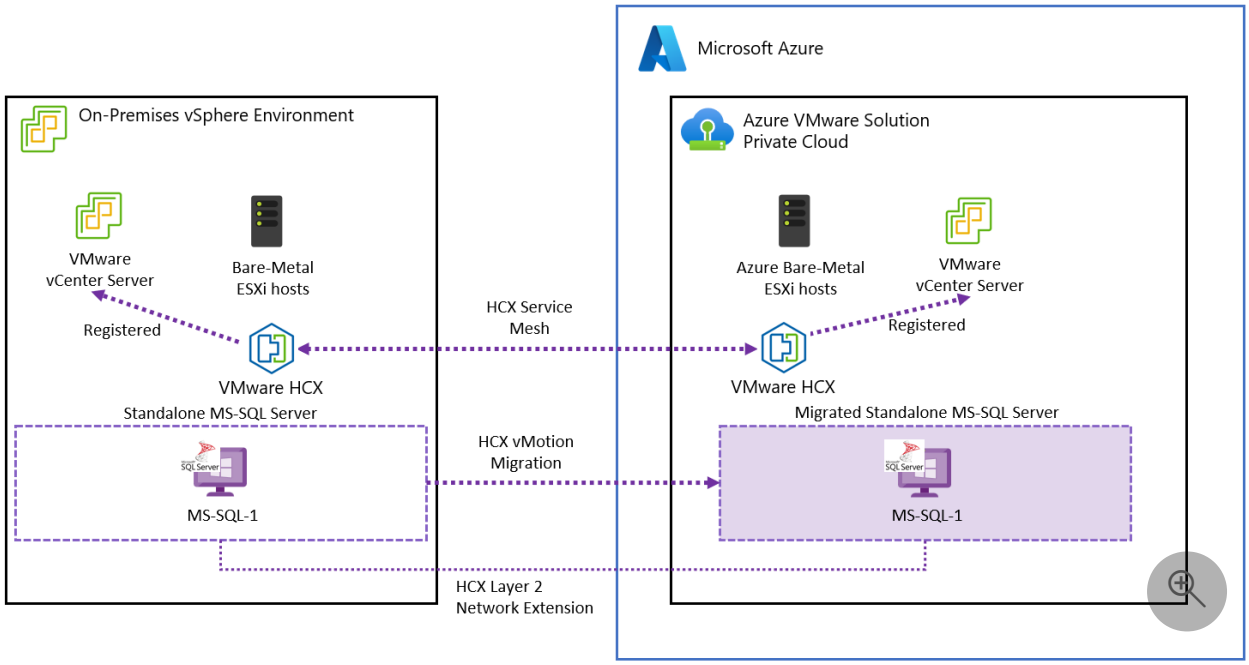
VMware HCX offers two migration profiles when migrating a SQL Server standalone instance to Azure VMware Solution:

- HCX vMotion
- HCX Cold Migration

In both cases, consider the size and criticality of the database being migrated. For this how-to procedure, we validated VMware HCX vMotion. VMware HCX Cold Migration is also valid, but it requires a longer downtime period.

This scenario was validated using the following editions and configurations:

- Microsoft SQL Server (2019 and 2022)
- Windows Server (2019 and 2022) Data Center edition
- Windows Server and SQL Server were configured following best practices and recommendations from Microsoft and VMware.
- The on-premises source infrastructure was VMware vSphere 7.0 Update 3 and VMware vSAN running on Dell PowerEdge servers and Intel Optane P4800X SSD NVMe devices.



Tested configurations

This scenario was validated using the following editions and configurations:

- Microsoft SQL Server (2019 and 2022)
- Windows Server (2019 and 2022) Data Center edition
- Windows Server and SQL Server were configured following best practices and recommendations from Microsoft and VMware.
- The on-premises source infrastructure was VMware vSphere 7.0 Update 3 and VMware vSAN running on Dell PowerEdge servers and Intel Optane P4800X SSD NVMe devices.+

Prerequisites

- Review and record the storage and network configuration of every node in the cluster.
- Maintain backups of all the databases.
- Back up the virtual machine running the SQL Server instance.
- Remove all cluster node VMs from any Distributed Resource Scheduler (DRS) groups and rules.
- Configure VMware HCX between your on-premises datacenter and the Azure VMware Solution private cloud that runs the migrated workloads. For more information about configuring VMware HCX, see Azure VMware Solution documentation.
- Ensure that all the network segments in use by the SQL Server and workloads using it are extended into your Azure VMware Solution private cloud. To verify this step in the process, see Configure VMware HCX network extension.

Either VMware HCX over VPN or ExpressRoute connectivity can be used as the networking configuration for the migration.

VMware HCX over VPN, due to its limited bandwidth, is typically suited for workloads that can sustain longer periods of downtime (such as nonproduction environments).

For any of the following scenarios, ExpressRoute connectivity is recommended for a migration:

- Production environments
- Workloads with large database sizes

- Scenarios in which there's a need to minimize downtime the ExpressRoute connectivity is recommended for the migration.migration.
- Production environments
- Workloads with large database sizes
- Any case where there's a need to minimize downtime

Further downtime considerations are discussed in the next section.

Downtime considerations

Downtime during a migration depends on the size of the database to be migrated and the speed of the private network connection to Azure cloud. Migration of a SQL Server standalone instance using the VMware HCX vMotion mechanism is intended to minimize the solution downtime, however we still recommend the migration take place during off-peak hours within a preapproved change window.

The following table indicates the estimated downtime for migration of each SQL Server topology.

Expand table

Scenario	Downtime expected	Notes
SQL Server standalone instance	Low	Migration is done using VMware vMotion, the database is available during migration time, but it isn't recommended to commit any critical data during it.
SQL Server Always On Availability Group	Low	The primary replica will always be available during the migration of the first secondary replica and the secondary replica will become the primary after the initial failover to Azure.
SQL Server Always On Failover Customer Instance	High	All nodes of the cluster are shut down and migrated using VMware HCX Cold Migration. Downtime duration depends upon database size and private network speed to Azure cloud.

Executing the migration

1. Log into your on-premises **vCenter Server** and access the VMware HCX plugin.

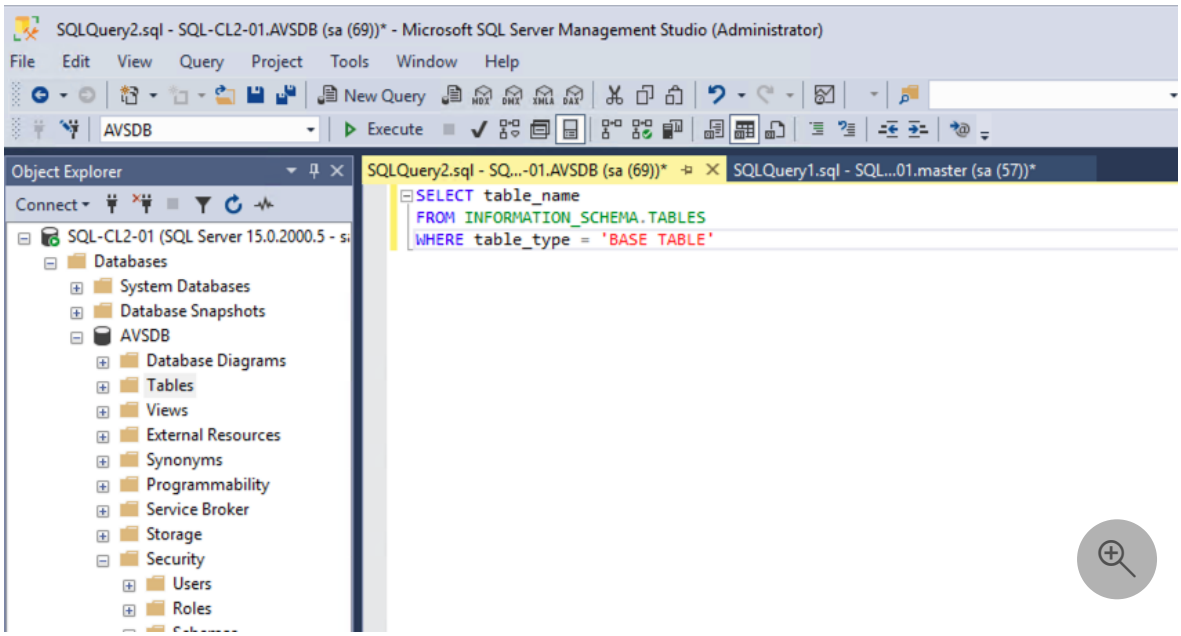
2. Under **Services**, select **Migration** > **Migrate**.
   a. Select the SQL Server virtual machine.

b. Set the vSphere cluster in the remote private cloud, which hosts the migrated SQL Server VM or VMs as the **Compute Container**.
c. Select the vSAN Datastore as remote storage.
d. Select a folder. It isn't mandatory, but we recommend separating the different workloads in your Azure VMware Solution private cloud.
e. Keep **Same format as source**.
f. Select **vMotion** as Migration profile.
g. In **Extended Options** select **Migrate Custom Attributes**.
h. Verify that on-premises network segments have the correct remote stretched segment in Azure VMware Solution.
i. Select **Validate** and ensure that all checks are completed with pass status.
j. Select **Go** to start the migration.

3. After the migration is complete, access the virtual machine using VMware Remote Console in the vSphere Client.

4. Verify the network configuration and check connectivity both with on-premises and Azure VMware Solution resources.

5. Verify your SQL Server and databases are up and accessible. For example, using SQL Server Management Studio, verify you can access the database.



Check the connectivity to SQL Server from other systems and applications in your infrastructure. Verify that all applications using the database or databases can still access them.

More information

- Enable SQL Azure Hybrid Benefit for Azure VMware Solution.

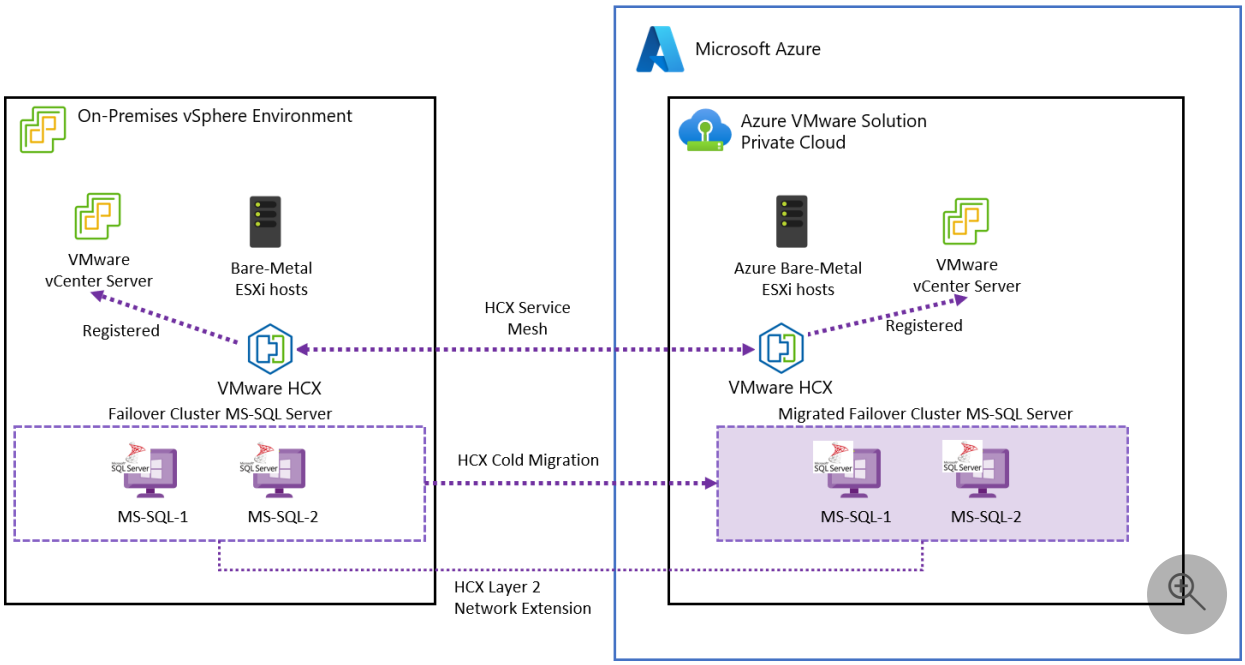
- Create a placement policy in Azure VMware Solution
- Windows Server Failover Clustering Documentation
- Microsoft SQL Server 2019 Documentation
- Microsoft SQL Server 2022 Documentation
- Windows Server Technical Documentation
- Planning Highly Available, Mission Critical SQL Server Deployments with VMware vSphere
- Microsoft SQL Server on VMware vSphere Availability and Recovery Options
- VMware KB 100 2951 – Tips for configuring Microsoft SQL Server in a virtual machine
- Microsoft SQL Server 2019 in VMware vSphere 7.0 Performance Study
- Architecting Microsoft SQL Server on VMware vSphere – Best Practices Guide
- Setup for Windows Server Failover Cluster in VMware vSphere 7.0

Migrate a SQL Server Always On Failover Cluster Instance to Azure VMware Solution

Article • 12/20/2023

In this article, you learn how to migrate a SQL Server Failover Cluster Instance to Azure VMware Solution. Currently Azure VMware Solution service doesn't support VMware Hybrid Linked Mode to connect an on-premises vCenter Server with one running in Azure VMware Solution. Due to this constraint, this process requires the use of VMware HCX for the migration. For more information about configuring HCX, see Install and activate VMware HCX in Azure VMware Solution.

VMware HCX doesn't support migrating virtual machines with SCSI controllers in physical sharing mode attached to a virtual machine. However, you can overcome this limitation by performing the steps shown in this procedure and using VMware HCX Cold Migration to move the different virtual machines that make up the cluster.



> **Note**
>
> This procedure requires a full shutdown of the cluster. Since the SQL Server service will be unavailable during the migration, plan accordingly for the downtime period.

Microsoft SQL Servers 2019 and 2022 were tested with Windows Servers 2019 and 2022 Data Center edition with the virtual machines deployed in the on-premises environment.

Windows Server and SQL Server were configured following best practices and recommendations from Microsoft and VMware. The on-premises source infrastructure was VMware vSphere 7.0 Update 3 and VMware vSAN running on Dell PowerEdge servers and Intel Optane P4800X SSD NVMe devices.

Prerequisites

- Review and record the storage and network configuration of every node in the cluster.
- Review and record the WSFC configuration.
- Maintain backups of all the SQL Server databases.
- Back up the cluster virtual machines.
- Remove all cluster node VMs from any Distributed Resource Scheduler (DRS) groups and rules they're part of.
- VMware HCX must be configured between your on-premises datacenter and the Azure VMware Solution private cloud that runs the migrated workloads. For more information about installing VMware HCX, see Azure VMware Solution documentation.
- Ensure that all the network segments in use by SQL Server and workloads using it are extended into your Azure VMware Solution private cloud. To verify this step, see Configure VMware HCX network extension.

Either VMware HCX over VPN or ExpressRoute connectivity can be used as the networking configuration for the migration.

With VMware HCX over VPN, due to its limited bandwidth, is typically suited for workloads that can sustain longer periods of downtime (such as nonproduction environments).

For any of the following instances, ExpressRoute connectivity is recommended for a migration:

- Production environments
- Workloads with large database sizes
- Scenarios in which there's a need to minimize downtime the ExpressRoute connectivity is recommended for the migration.

Downtime considerations

Downtime during a migration depends on the size of the database to be migrated and the speed of the private network connection to Azure cloud. Migration of SQL Server

Failover Cluster Instances Always On to Azure VMware Solution requires a full downtime of the database and all cluster nodes, however you should plan for the migration to be executed during off-peak hours with an approved change window.

The following table indicates the estimated downtime for migration of each SQL Server topology.

Expand table

Scenario	Downtime expected	Notes
SQL Server standalone instance	Low	Migration is done using VMware vMotion, the database is available during migration time, but it isn't recommended to commit any critical data during it.
SQL Server Always On Availability Group	Low	The primary replica will always be available during the migration of the first secondary replica and the secondary replica will become the primary after the initial failover to Azure.
SQL Server Always On Failover Customer Instance	High	All nodes of the cluster are shut down and migrated using VMware HCX Cold Migration. Downtime duration depends upon database size and private network speed to Azure cloud.

Windows Server Failover Cluster quorum considerations

Windows Server Failover Cluster requires a quorum mechanism to maintain the cluster.

Use an odd number of voting elements to achieve by an odd number of nodes in the cluster or by using a witness. Witnesses can be configured in three different forms:

- Disk witness
- File share witness
- Cloud witness

If the cluster uses **Disk witness**, then the disk must be migrated with the cluster shared storage using the Migrate fail over cluster.

If the cluster uses a **File share witness** running on-premises, then the type of witness for your migrated cluster depends on the Azure VMware Solution scenario:

- **Datacenter Extension**: Maintain the file share witness on-premises. Your workloads are distributed across your datacenter and Azure VMware Solution, therefore connectivity between both should always be available. In any case take into consideration bandwidth constraints and plan accordingly.
- **Datacenter Exit**: For this scenario, there are two options. In both cases, you can maintain the file share witness on-premises during the migration in case you need to do roll back.
  - Deploy a new **File share witness** in your Azure VMware Solution private cloud.
  - Deploy a **Cloud witness** running in Azure Blob Storage in the same region as the Azure VMware Solution private cloud.
- Disaster Recovery and Business Continuity: For a disaster recovery scenario, the best and most reliable option is to create a **Cloud Witness** running in Azure Storage.
- Application Modernization: For this use case, the best option is to deploy a **Cloud Witness**.

For more information about quorum configuration and management, see Failover Clustering documentation. For more information about deploying a Cloud witness in Azure Blob Storage, see Deploy a Cloud Witness for a Failover Cluster documentation for the details.

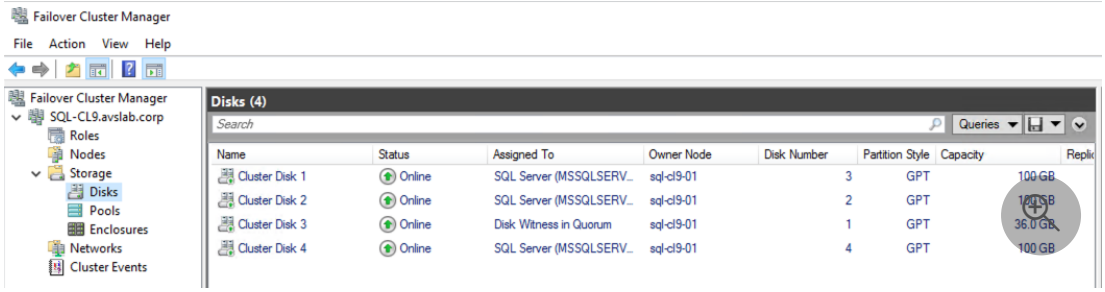
Migrate failover cluster

For illustration purposes, in this document we're using a two-node cluster with Windows Server 2019 Datacenter and SQL Server 2019 Enterprise. Windows Server 2022 and SQL Server 2022 are also supported with this procedure.

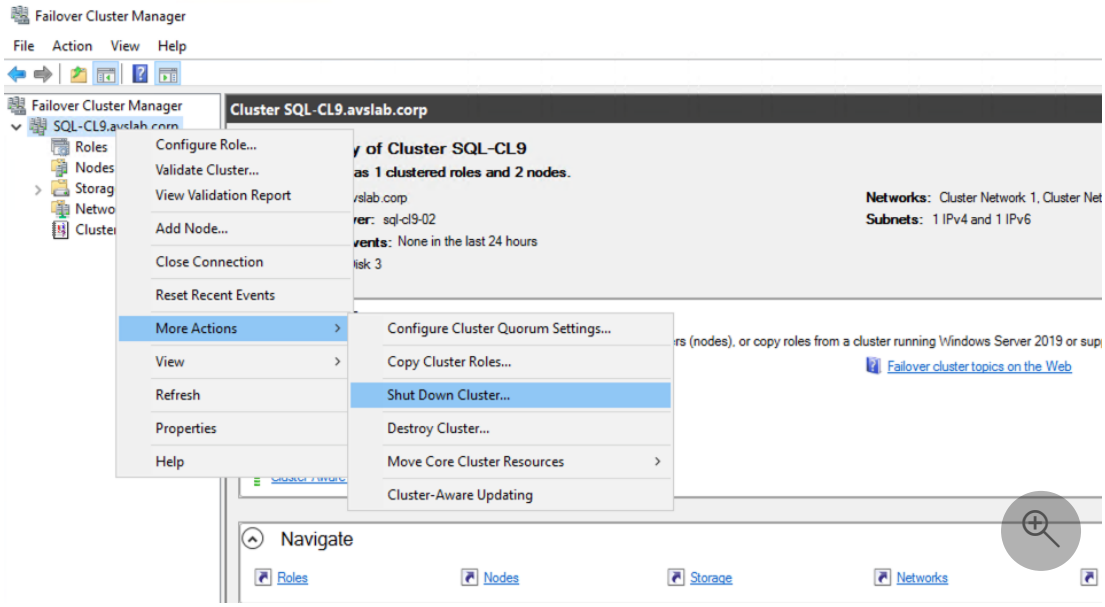
1. From vSphere Client shutdown, the second node of the cluster.

2. Access the first node of the cluster and open **Failover Cluster Manager**.

   - Verify that the second node is in **Offline** state and that all clustered services and storage are under the control of the first node.



   - Shut down the cluster.



- Check that all cluster services are successfully stopped without errors.

3. Shut down first node of the cluster.

4. From the **vSphere Client**, edit the settings of the second node of the cluster.

   - Remove all shared disks from the virtual machine configuration.
   - Ensure that the **Delete files from datastore** checkbox isn't selected as it permanently deletes the disk from the datastore. If that happens, you need to recover the cluster from a previous backup.
   - Set **SCSI Bus Sharing** from **Physical** to **None** in the virtual SCSI controllers used for the shared storage. Usually, these controllers are of VMware Paravirtual type.

5. Edit the first node virtual machine settings. Set **SCSI Bus Sharing** from **Physical** to **None** in the SCSI controllers.

6. From the **vSphere Client**, go to the HCX plugin area. Under **Services**, select **Migration** > **Migrate**.

   - Select the second node virtual machine.
   - Set the vSphere cluster in the remote private cloud, it hosts the migrated SQL Server VM or VMs, as the **Compute Container**.
   - Select the **vSAN Datastore** as remote storage.
   - Select a folder if you want to place the virtual machines in specific folder. It's not mandatory but is recommended to separate the different workloads in your Azure VMware Solution private cloud.
   - Keep **Same format as source**.
   - Select **Cold migration** as **Migration profile**.
   - In **Extended Options** select **Migrate Custom Attributes**.

- Verify that on-premises network segments have the correct remote stretched segment in Azure.
- Select **Validate** and ensure that all checks are completed with pass status. The most common error is one related to the storage configuration. Verify again that there are no SCSI controllers with physical sharing setting.
- Select **Go** and the migration initiates.

7. Repeat the same process for the first node.

8. Access **Azure VMware Solution vSphere Client** and edit the first node settings and set back to physical SCSI Bus sharing the SCSI controller or controllers managing the shared disks.

9. Edit node 2 settings in **vSphere Client**.

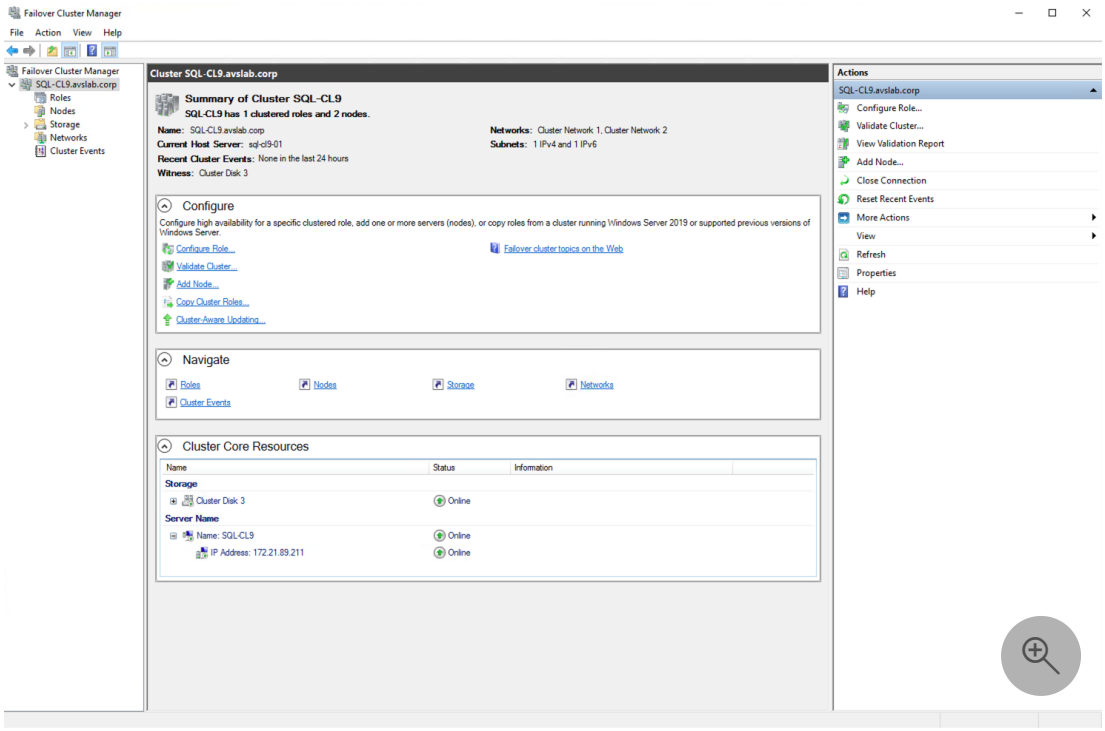
    - Set SCSI Bus sharing back to physical in the SCSI controller managing shared storage.
    - Add the cluster shared disks to the node as extra storage. Assign them to the second SCSI controller.
    - Ensure that all the storage configuration is the same as the one recorded before the migration.

10. Power on the first node virtual machine.

11. Access the first node VM with **VMware Remote Console**.

    - Verify virtual machine network configuration and ensure it can reach on-premises and Azure resources.

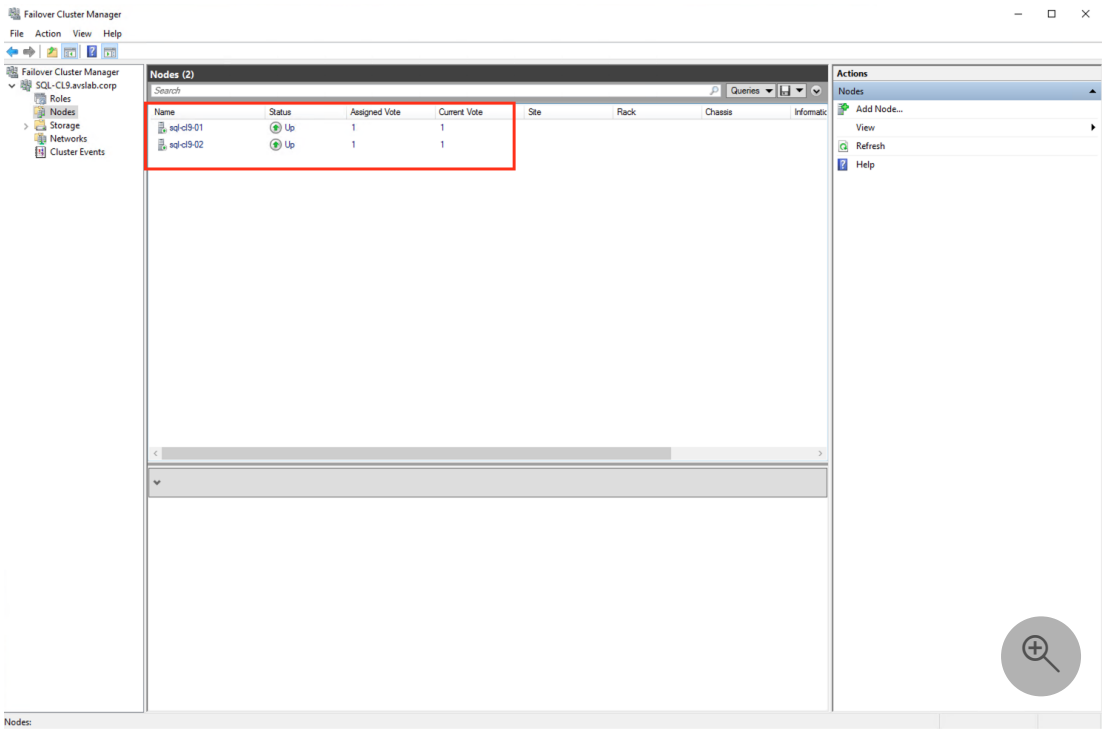
    - Open **Failover Cluster Manager** and verify cluster services.



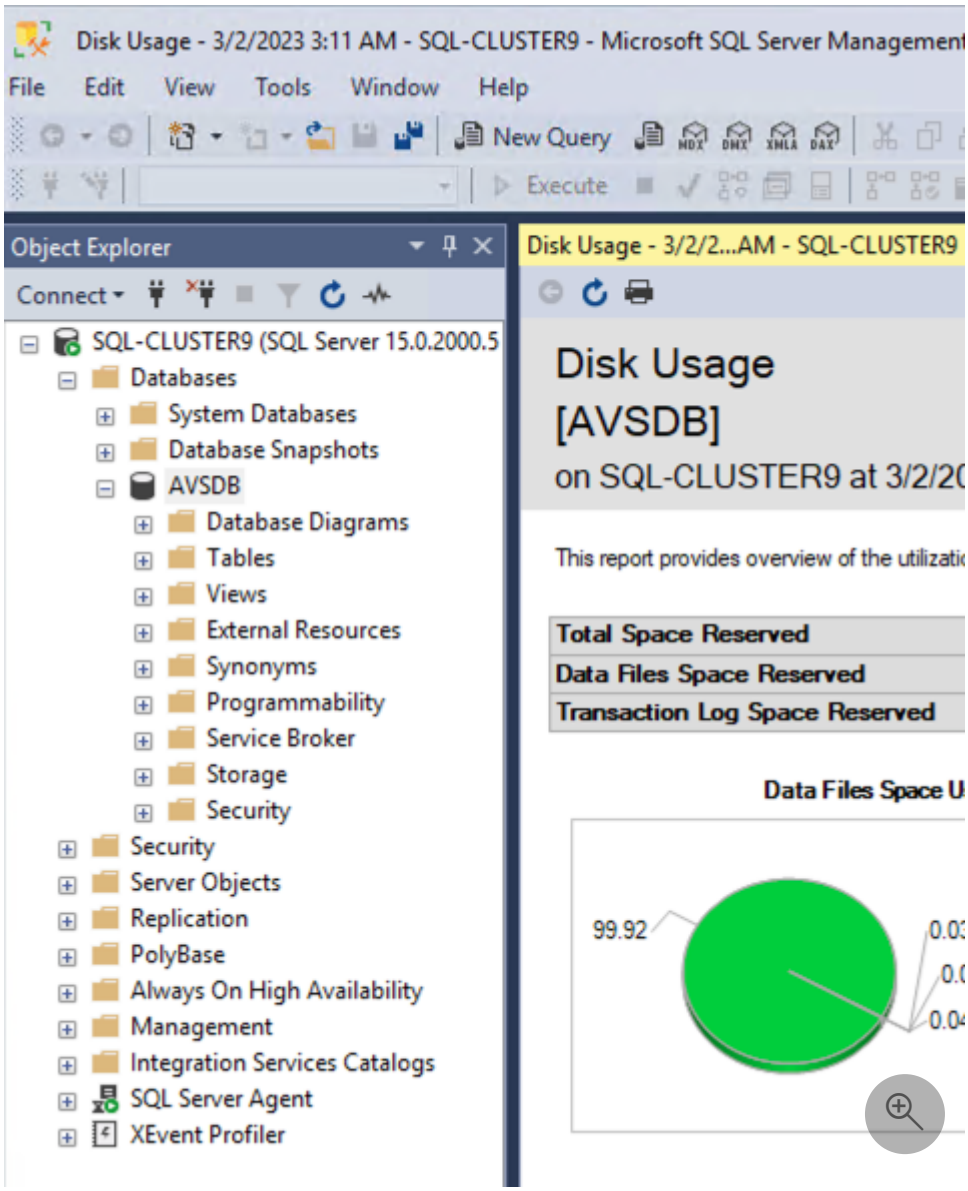
12. Power on the second node virtual machine.

13. Access the second node VM from the **VMware Remote Console**.

    - Verify that Windows Server can reach the storage.
    - In the **Failover Cluster Manager** review that the second node appears as **Online** status.



14. Using the **SQL Server Management Studio** connect to the SQL Server cluster resource network name. Confirm all databases are online and accessible.



Check the connectivity to SQL Server from other systems and applications in your infrastructure. Verify that all applications using the database or databases can still access them.

More information

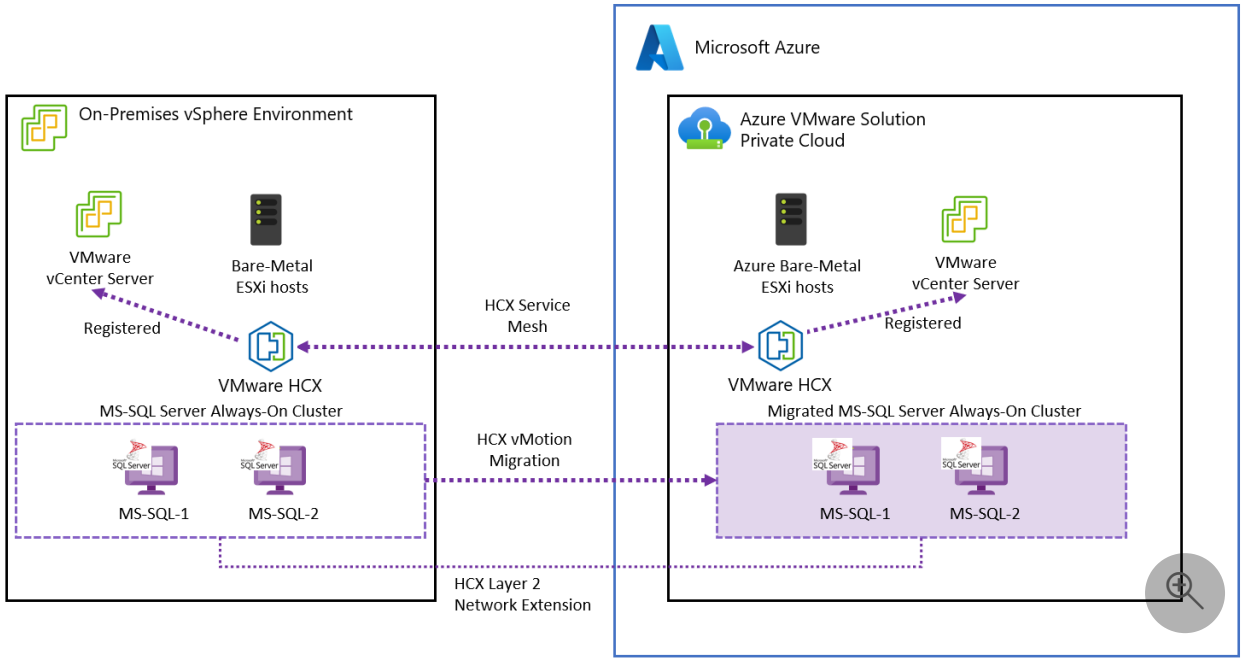
- Enable Azure Hybrid Benefit for SQL Server in Azure VMware Solution.
- Create a placement policy in Azure VMware Solution
- Windows Server Failover Clustering Documentation
- Microsoft SQL Server 2019 Documentation
- Microsoft SQL Server 2022 Documentation
- Windows Server Technical Documentation
- Planning Highly Available, Mission Critical SQL Server Deployments with VMware vSphere
- Microsoft SQL Server on VMware vSphere Availability and Recovery Options

- VMware KB 100 2951 – Tips for configuring Microsoft SQL Server in a virtual machine
- Microsoft SQL Server 2019 in VMware vSphere 7.0 Performance Study
- Architecting Microsoft SQL Server on VMware vSphere – Best Practices Guide
- Setup for Windows Server Failover Cluster in VMware vSphere 7.0

Migrate a SQL Server Always On Availability Group to Azure VMware Solution

Article • 12/18/2023

In this article, you learn how to migrate a SQL Server Always On Availability Group to Azure VMware Solution. For VMware HCX, you can follow the VMware vMotion migration procedure.



Microsoft SQL Server (2019 and 2022) was tested with Windows Server (2019 and 2022) Data Center edition with the virtual machines deployed in the on-premises environment. Windows Server and SQL Server are configured following best practices and recommendations from Microsoft and VMware. The on-premises source infrastructure was VMware vSphere 7.0 Update 3 and VMware vSAN running on Dell PowerEdge servers and Intel Optane P4800X SSD NVMe devices.

Prerequisites

The following are the prerequisites to migrating your SQL Server instance to Azure VMware Solution.

- Review and record the storage and network configuration of every node in the cluster.
- Maintain backups of all the SQL Server databases.
- Back up the virtual machine or virtual machines hosting SQL Server.

- Remove the virtual machine from any VMware vSphere Distributed Resource Scheduler (DRS) groups and rules.
- VMware HCX must be configured between your on-premises datacenter and the Azure VMware Solution private cloud that runs the migrated workloads. For more information on how to configure HCX, see Azure VMware Solution documentation.
- Ensure that all the network segments in use by SQL Server and workloads using it are extended into your Azure VMware Solution private cloud. To verify this step, see Configure VMware HCX network extension.

Either VMware HCX over VPN or ExpressRoute connectivity can be used as the networking configuration for the migration.

With VMware HCX over VPN, due to its limited bandwidth, is typically suited for workloads that can sustain longer periods of downtime (such as nonproduction environments).

For any of the following instances, ExpressRoute connectivity is recommended for a migration:

- Production environments
- Workloads with large database sizes
- Scenarios in which there's a need to minimize downtime the ExpressRoute connectivity is recommended for the migration.

Further downtime considerations are discussed in the next section.

Downtime considerations

Downtime during a migration depends upon the size of the database to be migrated and the speed of the private network connection to Azure cloud. While SQL Server Availability Group migrations can be executed with minimal solution downtime, it's optimal to conduct the migration during off-peak hours within a preapproved change window.

The following table indicates the estimated downtime for migration of each SQL Server topology.

Expand table

Scenario	Downtime expected	Notes
SQL Server standalone instance	Low	Migration is done using VMware vMotion, the database is available during migration time, but it isn't recommended

Scenario	Downtime expected	Notes
SQL Server Always On Availability Group	Low	The primary replica will always be available during the migration of the first secondary replica and the secondary replica will become the primary after the initial failover to Azure.
SQL Server Always On Failover Customer Instance	High	All nodes of the cluster are shut down and migrated using VMware HCX Cold Migration. Downtime duration depends upon database size and private network speed to Azure cloud.

Windows Server Failover Cluster quorum considerations

Microsoft SQL Server Always On Availability Groups rely on Windows Server Failover Cluster, which requires a quorum voting mechanism to maintain the coherence of the cluster.

An odd number of voting elements is required, which is achieved by an odd number of nodes in the cluster or by using a witness. Witness can be configured in three different ways:

- Disk witness
- File share witness
- Cloud witness

If the cluster uses **Disk witness**, then the disk must be migrated with the rest of cluster shared storage using the procedure described in this document.

If the cluster uses a **File share witness** running on-premises, then the type of witness for your migrated cluster depends upon the Azure VMware Solution scenario, there are several options to consider.

- **Datacenter Extension**: Maintain the file share witness on-premises. Your workloads are distributed across your datacenter and Azure. Therefore the connectivity between your datacenter and Azure should always be available. In any case, take into consideration bandwidth constraints and plan accordingly.
- **Datacenter Exit**: For this scenario, there are two options. In both options, you can maintain the file share witness on-premises during the migration in case you need to do roll back during the process.
    - Deploy a new **File share witness** in your Azure VMware Solution private cloud.

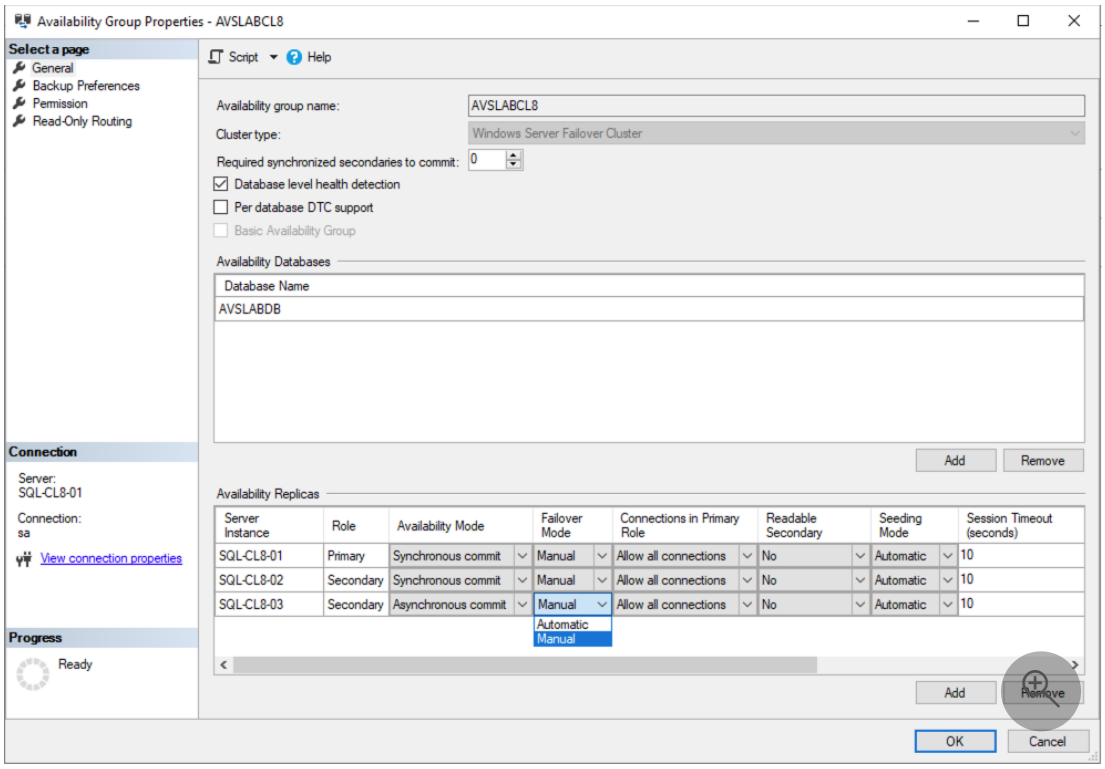
    - Deploy a **Cloud witness** running in Azure Blob Storage in the same region as the Azure VMware Solution private cloud.
- **Disaster Recovery and Business Continuity**: For a disaster recovery scenario, the best and most reliable option is to create a **Cloud Witness** running in Azure Storage.
- **Application Modernization**: For this use case, the best option is to deploy a **Cloud Witness**.

For details about configuring and managing the quorum, see Failover Clustering documentation. For information about deployment of Cloud witness in Azure Blob Storage, see Manage a cluster quorum for a Failover Cluster.

Migrate SQL Server Always On Availability Group

1. Access your Always On Availability Group with SQL Server Management Studio using administration credentials.

    - Select your primary replica and open **Availability Group Properties**.



    - Change **Availability Mode** to **Asynchronous commit** only for the replica to be migrated.
    - Change **Failover Mode** to **Manual** for every member of the availability group.

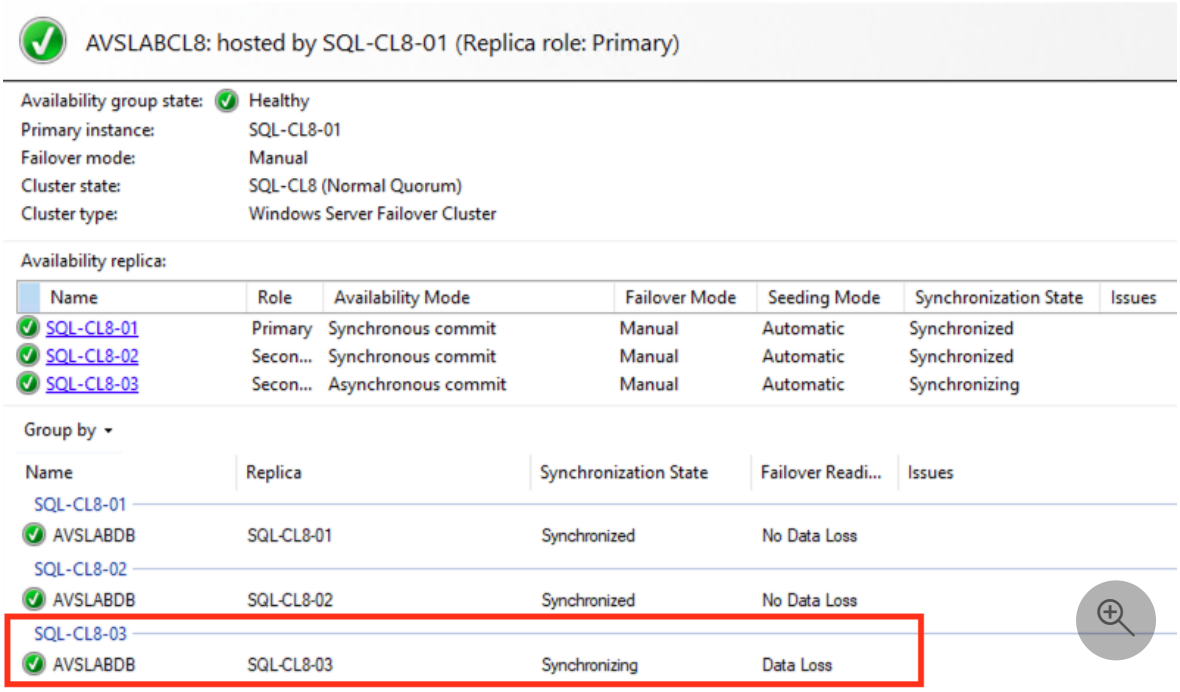
2. Access the on-premises vCenter Server and proceed to HCX area.

3. Under **Services**, select **Migration** > **Migrate**.

- Select one virtual machine running the secondary replica of the database the is going to be migrated.
- Set the vSphere cluster in the remote private cloud, which now hosts the migrated SQL Server VM or VMs as the **Compute Container**.
- Select the **vSAN Datastore** as remote storage.
- Select a folder. It's not mandatory, but is recommended to separate the different workloads in your Azure VMware Solution private cloud.
- Keep **Same format as source**.
- Select **vMotion** as **Migration profile**.
- In **Extended Options** select **Migrate Custom Attributes**.
- Verify that on-premises network segments have the correct remote stretched segment in Azure.
- Select **Validate** and ensure that all checks are completed with pass status. The most common error is related to the storage configuration. Verify again that there are no virtual SCSI controllers have the physical sharing setting.
- Select **Go** to start the migration.

4. Once the migration is completed, access the migrated replica and verify connectivity with the rest of the members in the availability group.

5. In SQL Server Management Studio, open the **Availability Group Dashboard** and verify that the replica appears as **Online**.



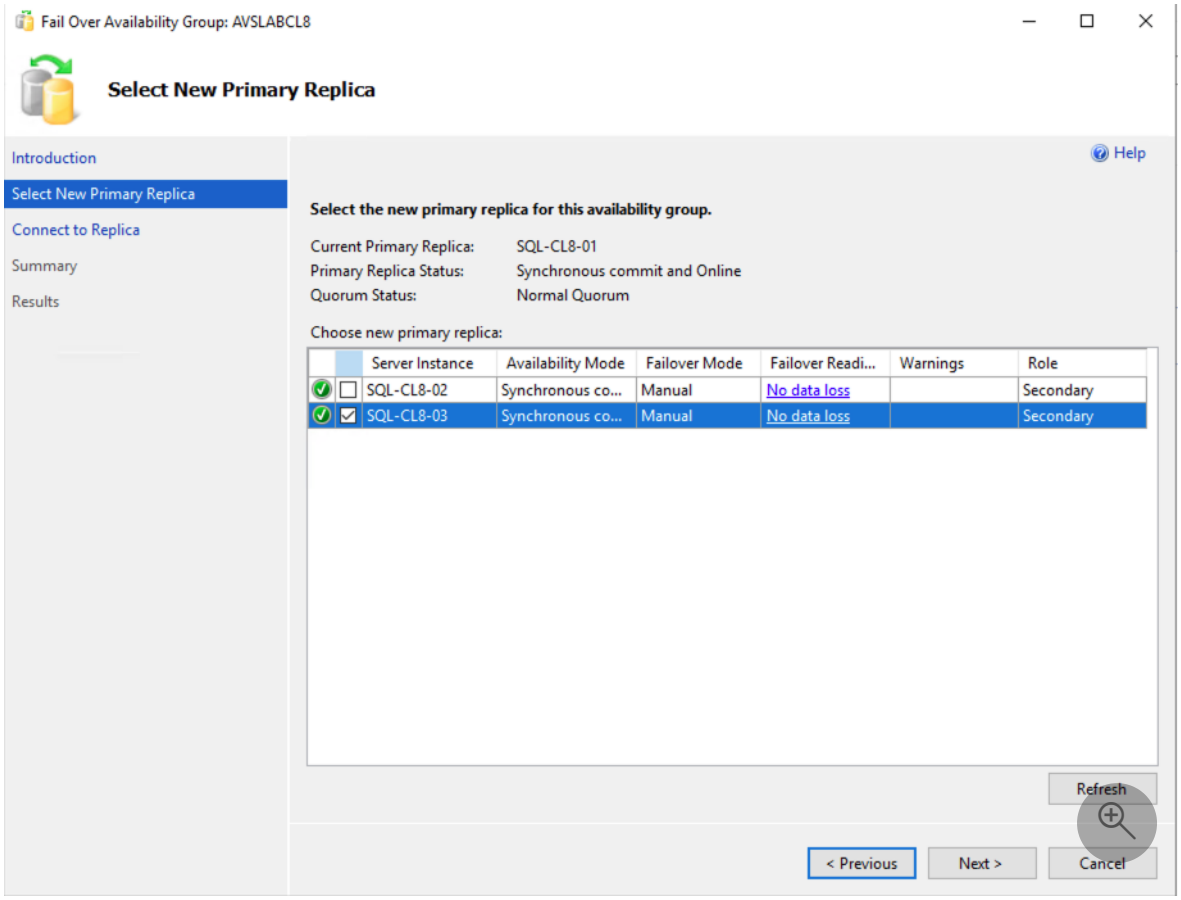
- **Data Loss** status in the **Failover Readiness** column is expected since the replica is out-of-sync with the primary during the migration.

6. Edit the **Availability Group Properties** again and set **Availability Mode** back to **Synchronous commit**.

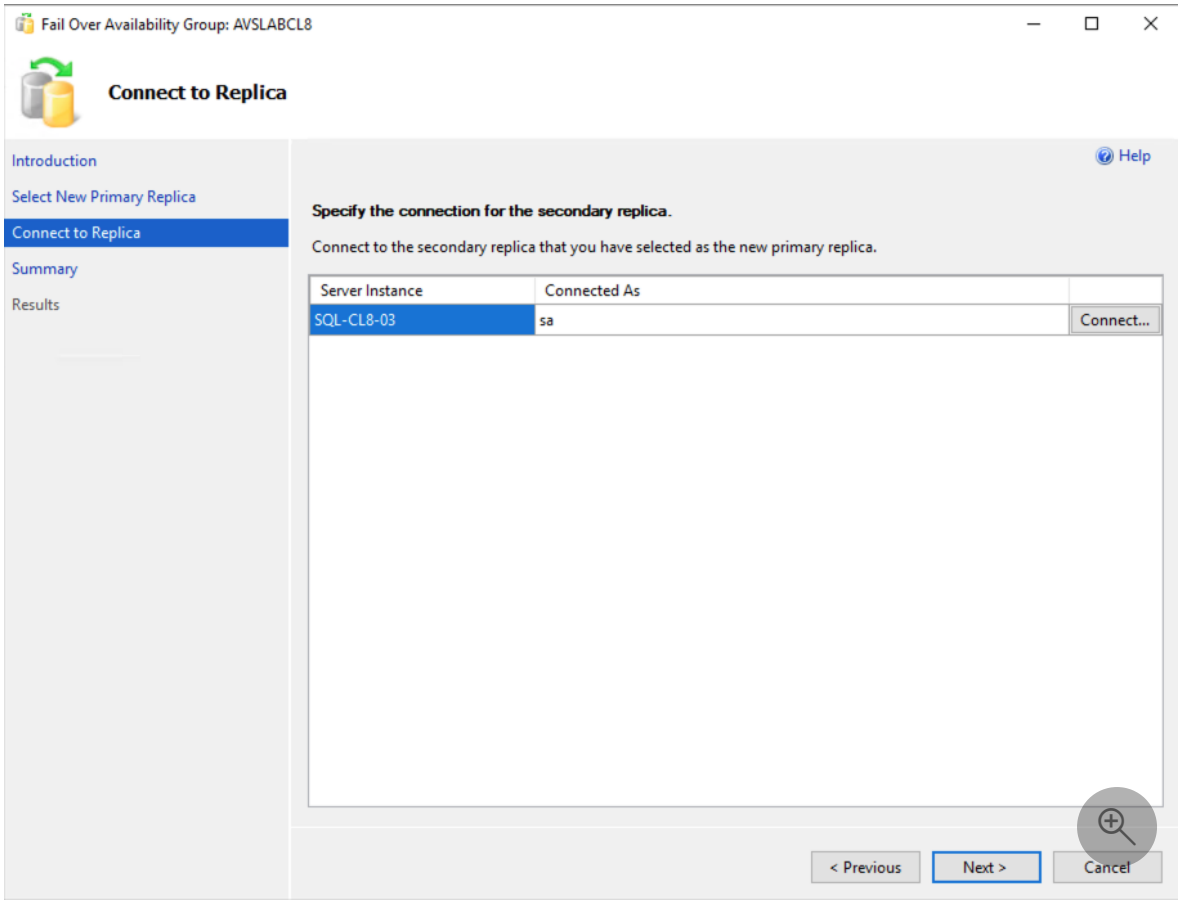
- The secondary replica starts to synchronize back all the changes made to the primary replica during the migration. Wait until it appears in Synchronized state.

7. From the **Availability Group Dashboard**, in SSMS, select **Start Failover Wizard**.

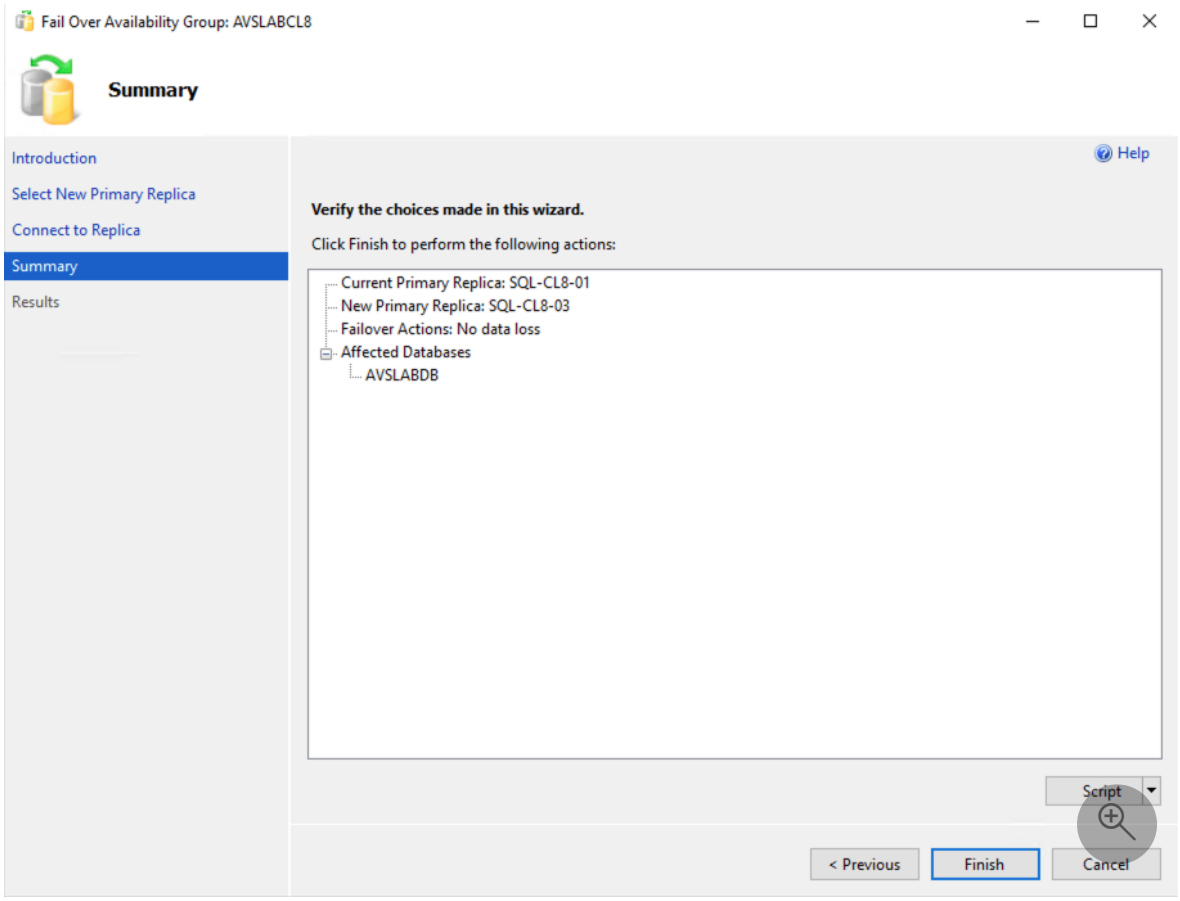
8. Select the migrated replica and select **Next**.



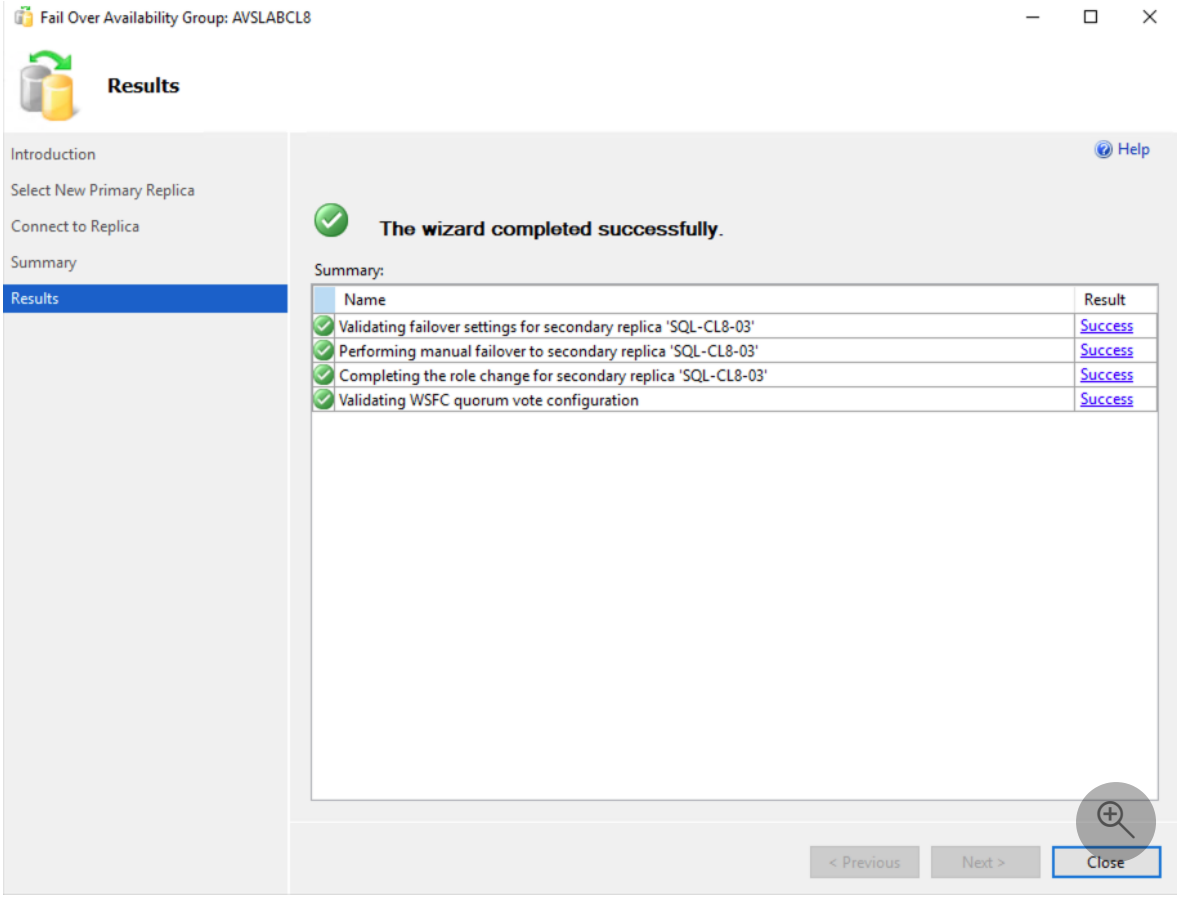
9. Connect to the replica in the next screen with your DB admin credentials.



10. Review the changes and select **Finish** to start the failover operation.



11. Monitor the progress of the failover in the next screen, select **Close** when the operation is finished.



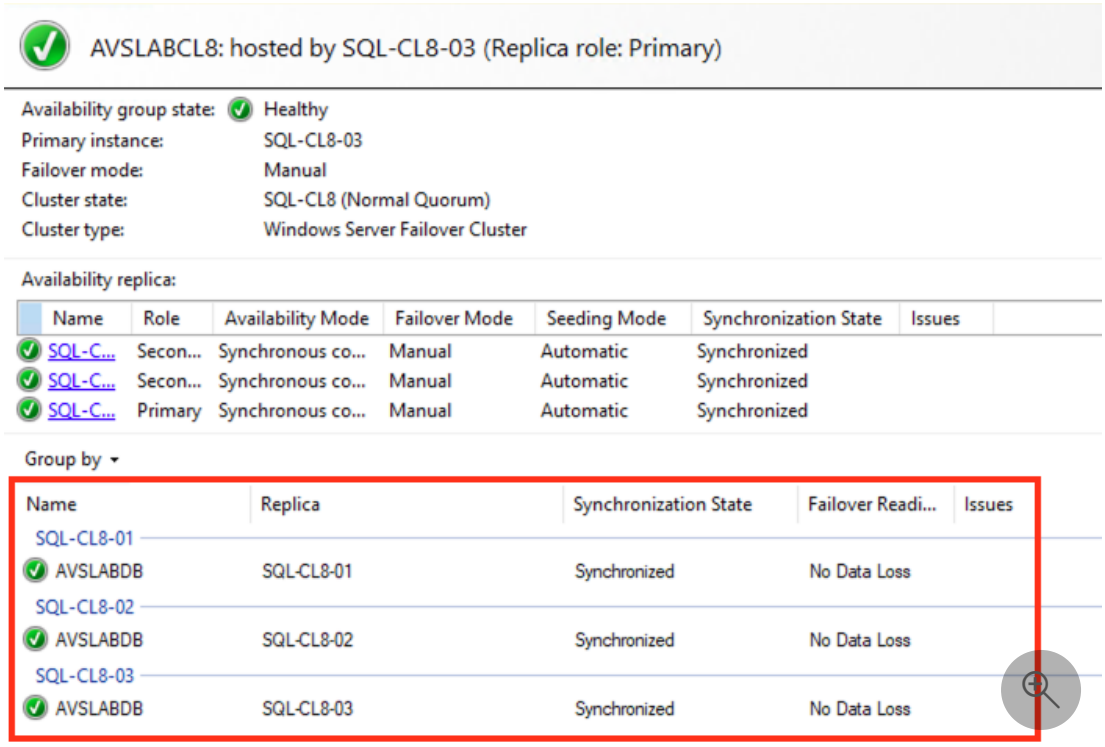
12. Refresh the **Object Explorer** view in SQL Server Management Studio (SSMS), verify that the migrated instance is now the primary replica.

13. Repeat steps 1 to 6 for the rest of the replicas of the availability group.

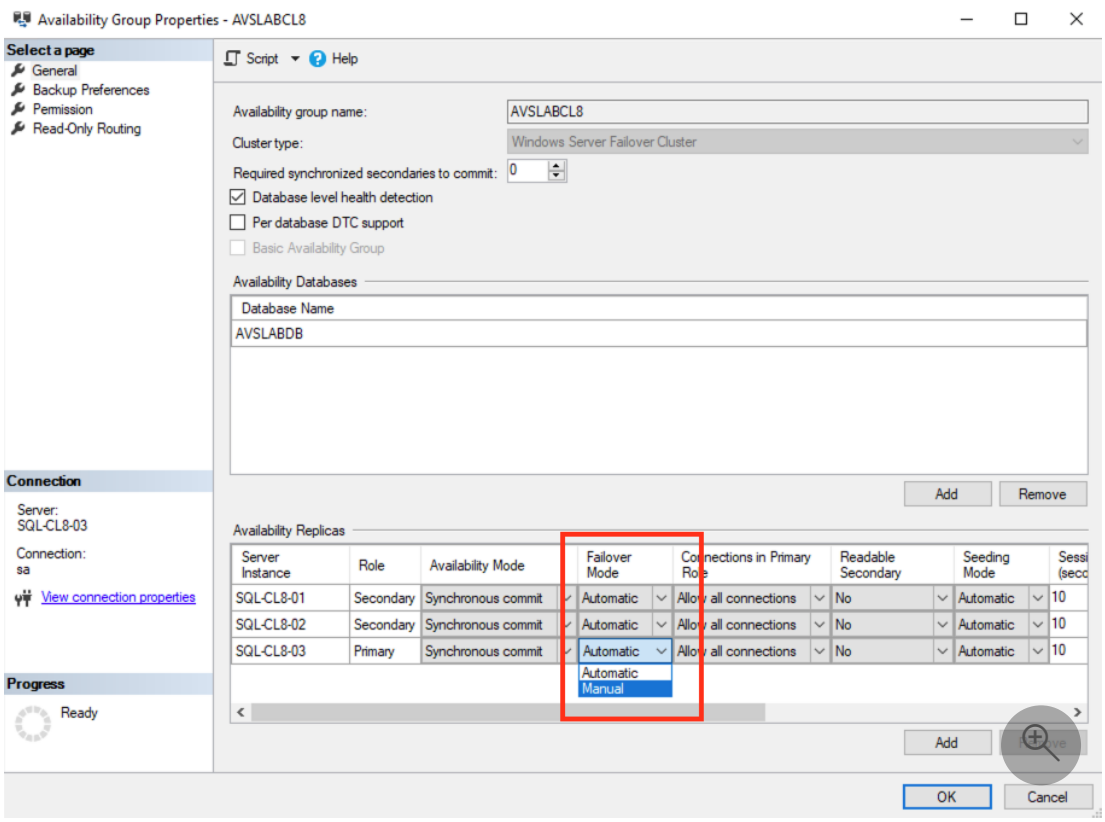
> ⓘ **Note**
>
> Migrate one replica at a time and verify that all changes are synchronized back to the replica after each migration. Do not migrate all the replicas at the same time using **HCX Bulk Migration**.

14. After the migration of all the replicas is completed, access your Always On availability group with **SQL Server Management Studio**.

    - Open the Dashboard and verify there's no data loss in any of the replicas and that all are in a **Synchronized** state.



- Edit the **Properties** of the availability group and set **Failover Mode** to **Automatic** in all replicas.



Next steps

- Enable SQL Azure hybrid benefit for Azure VMware Solution.
- Create a placement policy in Azure VMware Solution
- Windows Server Failover Clustering Documentation

- Microsoft SQL Server 2019 Documentation
- Microsoft SQL Server 2022 Documentation
- Windows Server Technical Documentation
- Planning Highly Available, Mission Critical SQL Server Deployments with VMware vSphere
- Microsoft SQL Server on VMware vSphere Availability and Recovery Options
- VMware KB 100 2951 – Tips for configuring Microsoft SQL Server in a virtual machine
- Microsoft SQL Server 2019 in VMware vSphere 7.0 Performance Study
- Architecting Microsoft SQL Server on VMware vSphere – Best Practices Guide
- Setup for Windows Server Failover Cluster in VMware vSphere 7.0

Operating system support for Azure VMware Solution virtual machines

Article • 12/12/2023

Azure VMware Solution supports a wide range of operating systems to be used in the guest virtual machines. Being based on VMware vSphere, currently 7.0 version, all operating systems currently supported by vSphere can be used by any Azure VMware Solution customer for their workloads.

Check the list of operating systems and configurations supported in the VMware Compatibility Guide, create a query for ESXi 7.0 Update 3 and select all operating systems and vendors.

Additionally to the supported operating systems by VMware for vSphere, we worked with Red Hat, SUSE and Canonical to extend the support model currently in place for Azure Virtual Machines to the workloads running on Azure VMware Solution, given that it's a first-party Azure service. You can check the following sites of vendors for more information about the benefits of running their operating system on Azure.

- Red Hat Enterprise Linux
- Ubuntu Server
- SUSE Enterprise Linux Server

Configure Windows Server Failover Cluster on Azure VMware Solution vSAN

Article • 03/29/2024

In this article, learn how to configure Failover Clustering in Windows Server on Azure VMware Solution vSAN with native shared disks.

Windows Server Failover Cluster, previously known as Microsoft Service Cluster Service (MSCS), is a Windows Server Operating System (OS) feature. WSFC is a business-critical feature, and for many applications is required. For example, WSFC is required for the following configurations:

- SQL Server configured as:
  - Always On Failover Cluster Instance (FCI), for instance-level high availability.
  - Always On Availability Group (AG), for database-level high availability.
- Windows File Services:
  - Generic File share running on active cluster node.
  - Scale-Out File Server (SOFS), which stores files in cluster shared volumes (CSV).
  - Storage Spaces Direct (S2D); local disks used to create storage pools across different cluster nodes.

You can host the WSFC cluster on different Azure VMware Solution instances, known as Cluster-Across-Box (CAB). You can also place the WSFC cluster on a single Azure VMware Solution node. This configuration is known as Cluster-in-a-Box (CIB). We don't recommend using a CIB solution for a production implementation, use CAB instead with placement policies. Were the single Azure VMware Solution node to fail, all WSFC cluster nodes would be powered off, and the application would experience downtime. Azure VMware Solution requires a minimum of three nodes in a private cloud cluster.

It's important to deploy a supported WSFC configuration. You want your solution to be supported on VMware vSphere and with Azure VMware Solution. VMware provides a detailed document about WSFC on vSphere 7.0, Setup for Failover Clustering and Microsoft Cluster Service.

This article focuses on WSFC on Windows Server 2016 and Windows Server 2019. Unfortunately, older Windows Server versions are out of mainstream support, so we don't consider them here.

First, you need to create a WSFC. Then, use the information we provide in this article to specify a WSFC deployment on Azure VMware Solution.

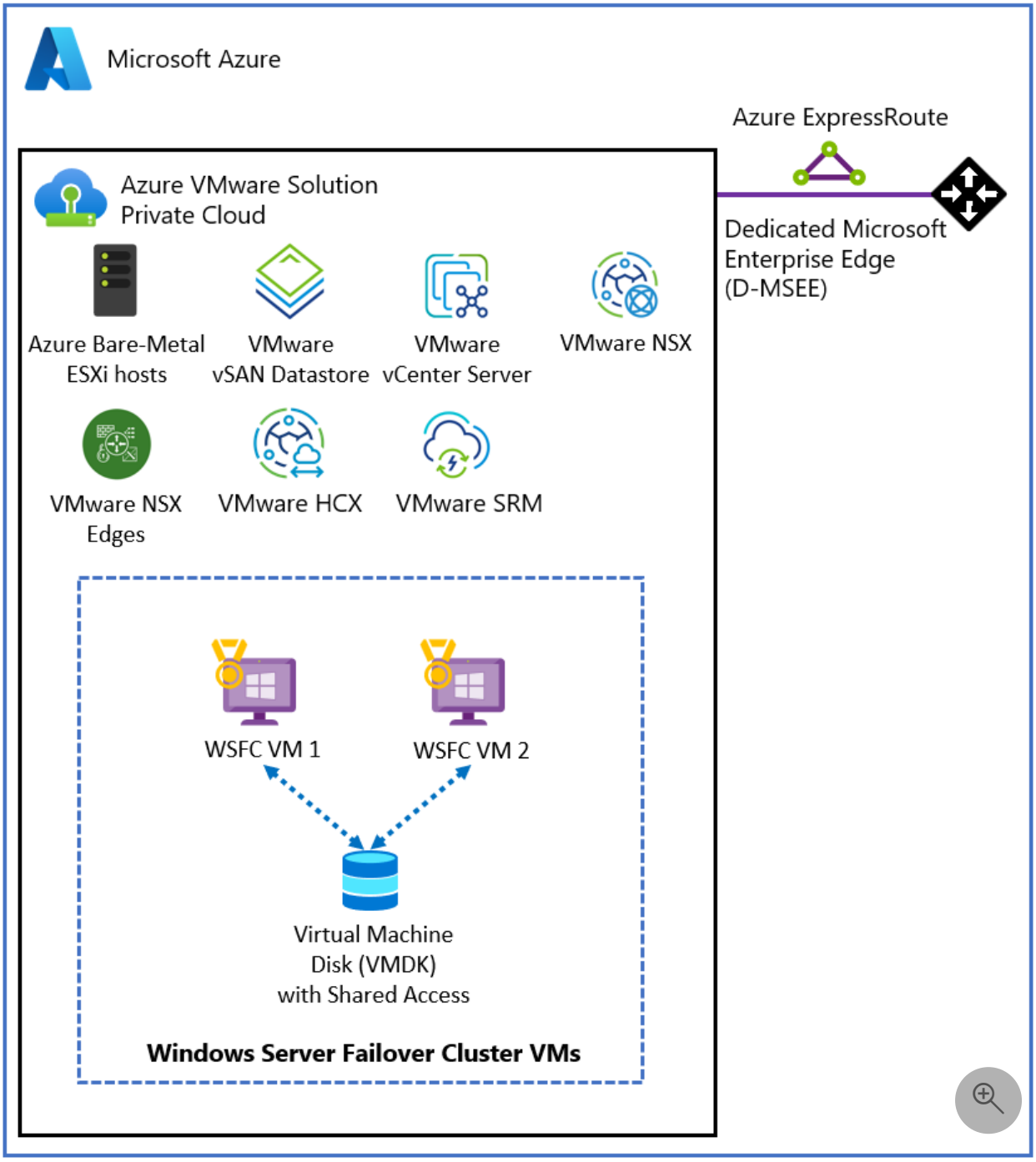
Prerequisites

- Azure VMware Solution environment
- Microsoft Windows Server OS installation media

Reference architecture

Azure VMware Solution provides native support for virtualized WSFC. It supports SCSI-3 Persistent Reservations (SCSI3PR) on a virtual disk level. WSFC requires this support to arbitrate access to a shared disk between nodes. Support of SCSI3PRs enables configuration of WSFC with a disk resource shared between VMs natively on vSAN datastores.

The following diagram illustrates the architecture of WSFC virtual nodes on an Azure VMware Solution private cloud. It shows where Azure VMware Solution resides, including the WSFC virtual servers (blue box), in relation to the broader Azure platform. This diagram illustrates a typical hub-spoke architecture, but a similar setup is possible using Azure Virtual WAN. Both offer all the value other Azure services can bring you.



Supported configurations

Currently, the configurations supported are:

- Microsoft Windows Server 2012 or later
- Up to five failover clustering nodes per cluster
- Up to four PVSCSI adapters per VM
- Up to 64 disks per PVSCSI adapter

Virtual machine configuration requirements

WSFC node configuration parameters

- Install the latest VMware Tools on each WSFC node.
- Mixing nonshared and shared disks on a single virtual SCSI adapter isn't supported. For example, if the system disk (drive C:) is attached to SCSI0:0, the first shared disk would be attached to SCSI1:0. A VM node of a WSFC has the same virtual SCSI controller maximum as an ordinary VM - up to four (4) virtual SCSI Controllers.
- Virtual discs SCSI IDs should be consistent between all VMs hosting nodes of the same WSFC.

Expand table

Component	Requirements
VM hardware version	11 or higher to support Live vMotion.
Virtual NIC	VMXNET3 paravirtualized network interface card (NIC); enable the in-guest Windows Receive Side Scaling (RSS) on the virtual NIC.
Memory	Use full VM reservation memory for nodes in the WSFC cluster.
Increase the I/O timeout of each WSFC node.	Modify HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Disk\TimeOutValueSet to 60 seconds or more. (If you recreate the cluster, this value might be reset to its default, so you must change it again.)
Windows cluster health monitoring	The value of the SameSubnetThreshold Parameter of Windows cluster health monitoring must be modified to allow 10 missed heartbeats at minimum. It's the default in Windows Server 2016. This recommendation applies to all applications using WSFC, including shared and nonshared disks.

WSFC node - Boot disks configuration parameters

Expand table

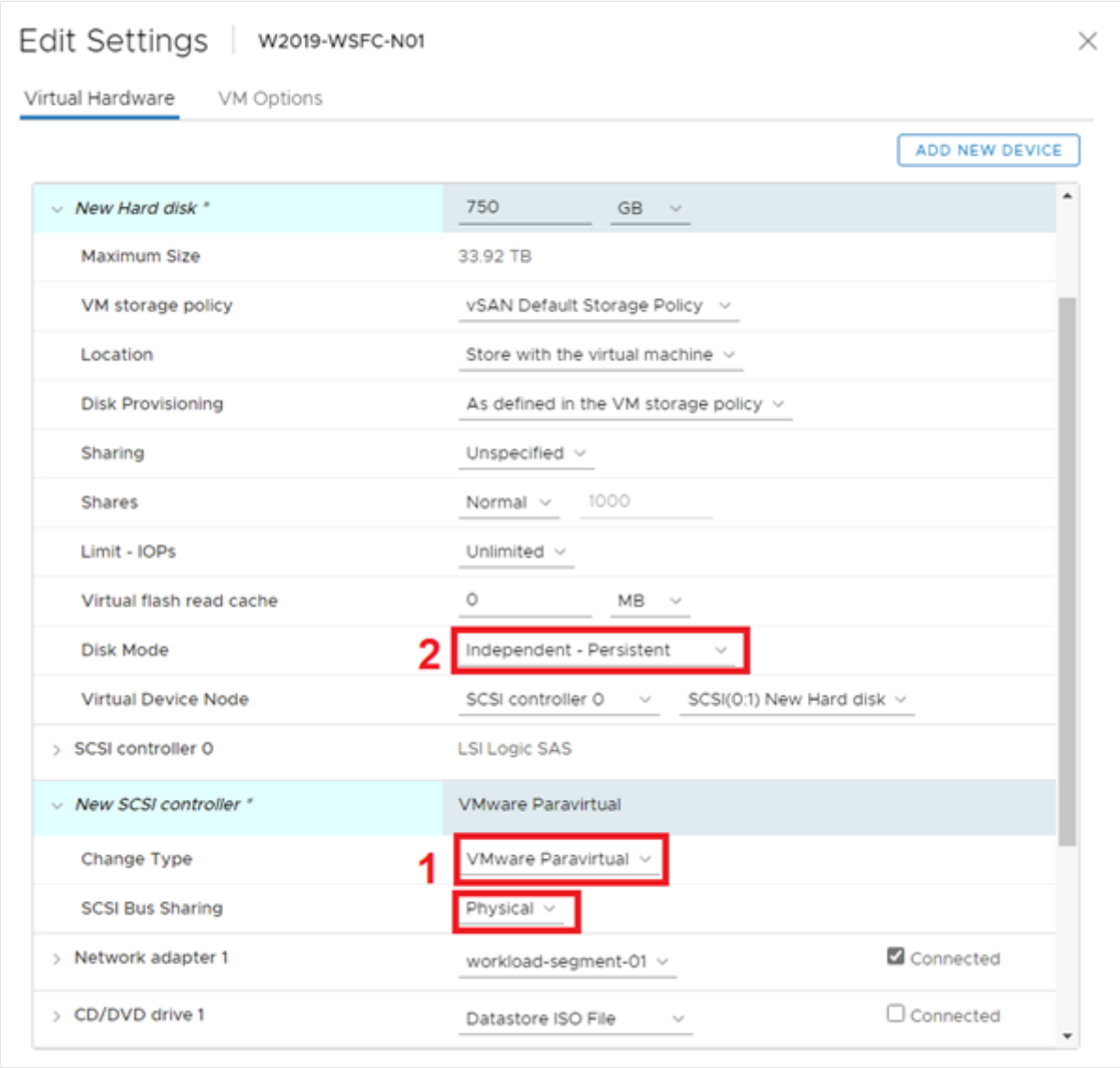
Component	Requirements
SCSI Controller Type	LSI Logic SAS
Disk mode	Virtual
SCSI bus sharing	None

Component	Requirements
Modify advanced settings for a virtual SCSI controller hosting the boot device.	Add the following advanced settings to each WSFC node: scsiX.returnNoConnectDuringAPD = "TRUE" scsiX.returnBusyOnNoConnectStatus = "FALSE" Where X is the boot device SCSI bus controller ID number. By default, X is set to 0.

WSFC node - Shared disks configuration parameters

Expand table

Component	Requirements
SCSI Controller Type	VMware Paravirtualized (PVSCSI)
Disk mode	Independent - Persistent (see step 2 in the following illustration). By using this setting, you ensure that all disks are excluded from snapshots. Snapshots aren't supported for WSFC-based VMs.
SCSI bus sharing	Physical (see step 1 in the following illustration)
Multi-writer flag	Not used
Disk format	Thick provisioned (Eager Zeroed Thick (EZT) isn't required with vSAN)



Unsupported scenarios

The following functionalities aren't supported for WSFC on Azure VMware Solution:

- NFS data stores
- Storage Spaces
- vSAN using iSCSI Service
- vSAN Stretched Cluster
- Enhanced vMotion Compatibility (EVC)
- vSphere Fault Tolerance (FT)
- Snapshots
- Live (online) storage vMotion
- N-Port ID Virtualization (NPIV)

Hot changes to virtual machine hardware might disrupt the heartbeat between the WSFC nodes.

The following activities aren't supported and might cause WSFC node failover:

- Hot adding memory
- Hot adding CPU
- Using snapshots
- Increasing the size of a shared disk
- Pausing and resuming the virtual machine state
- Memory over-commitment leading to ESXi swapping or VM memory ballooning
- Hot Extend Local VMDK file, even if it isn't associated with SCSI bus sharing controller

Configure WSFC with shared disks on Azure VMware Solution vSAN

1. Ensure that an Active Directory environment is available.
2. Create virtual machines (VMs) on the vSAN datastore.
3. Power on all VMs, configure the hostname and IP addresses, join all VMs to an Active Directory domain, and install the latest available OS updates.
4. Install the latest VMware Tools.
5. Enable and configure the Windows Server Failover Cluster feature on each VM.
6. Configure a Cluster Witness for quorum (can be a file share witness).
7. Power off all nodes of the WSFC cluster.
8. Add one or more Para virtual SCSI controllers (up to four) to each VM part of the WSFC. Use the settings per the previous paragraphs.
9. On the first cluster node, add all needed shared disks using **Add New Device** > **Hard Disk**. Leave Disk sharing as **Unspecified** (default) and Disk mode as **Independent - Persistent**. Then attach it to the controller(s) created in the previous steps.
10. Continue with the remaining WSFC nodes. Add the disks created in the previous step by selecting **Add New Device** > **Existing Hard Disk**. Be sure to maintain the same disk SCSI IDs on all WSFC nodes.
11. Power on the first WSFC node, sign in, and open the disk management console (mmc). Make sure the added shared disks are manageable by the OS and are initialized. Format the disks and assign a drive letter.
12. Power on the other WSFC nodes.

13. Add the disk to the WSFC cluster using the **Add Disk wizard** and add them to a Cluster Shared Volume.

14. Test a failover using the **Move disk wizard** and make sure the WSFC cluster with shared disks works properly.

15. Run the **Validation Cluster wizard** to confirm whether the cluster and its nodes are working properly.

    It's important to keep the following specific items from the Cluster Validation test in mind:

    - **Validate Storage Spaces Persistent Reservation**. If you aren't using Storage Spaces with your cluster (such as on Azure VMware Solution vSAN), this test isn't applicable. You can ignore any results of the Validate Storage Spaces Persistent Reservation test including this warning. To avoid warnings, you can exclude this test.

    - **Validate Network Communication**. The Cluster Validation test displays a warning indicating that only one network interface per cluster node is available. You can ignore this warning. Azure VMware Solution provides the required availability and performance needed, since the nodes are connected to one of the NSX-T Data Center segments. However, keep this item as part of the Cluster Validation test, as it validates other aspects of network communication.

16. Create the relevant Placement Policies to situate the WSFC VMs on the correct Azure VMware Solution nodes depending upon the WSFC CIB or CAB configuration. To do so, you need a host-to-VM affinity rule. This way, cluster nodes run on the same or separate Azure VMware Solution host(s) respectively.

Related information

- Failover Clustering in Windows Server
- Guidelines for Microsoft Clustering on vSphere (1037959) (vmware.com)
- About Setup for Failover Clustering and Microsoft Cluster Service (vmware.com)
- vSAN 6.7 U3 - WSFC with Shared Disks & SCSI-3 Persistent Reservations (vmware.com)
- Azure VMware Solution limits

Next steps

Now that we covered setting up a WSFC in Azure VMware Solution, learn more about:

- Setting up your new WSFC by adding more applications that require the WSFC capability. For instance, SQL Server and SAP ASCS.
- Setting up a backup solution.
  - Setting up Azure Backup Server for Azure VMware Solution
  - Backup solutions for Azure VMware Solution virtual machines

Create a content library to deploy VMs in Azure VMware Solution

Article • 12/20/2023

A content library stores and manages content in the form of library items. A single library item consists of files you use to deploy virtual machines (VMs).

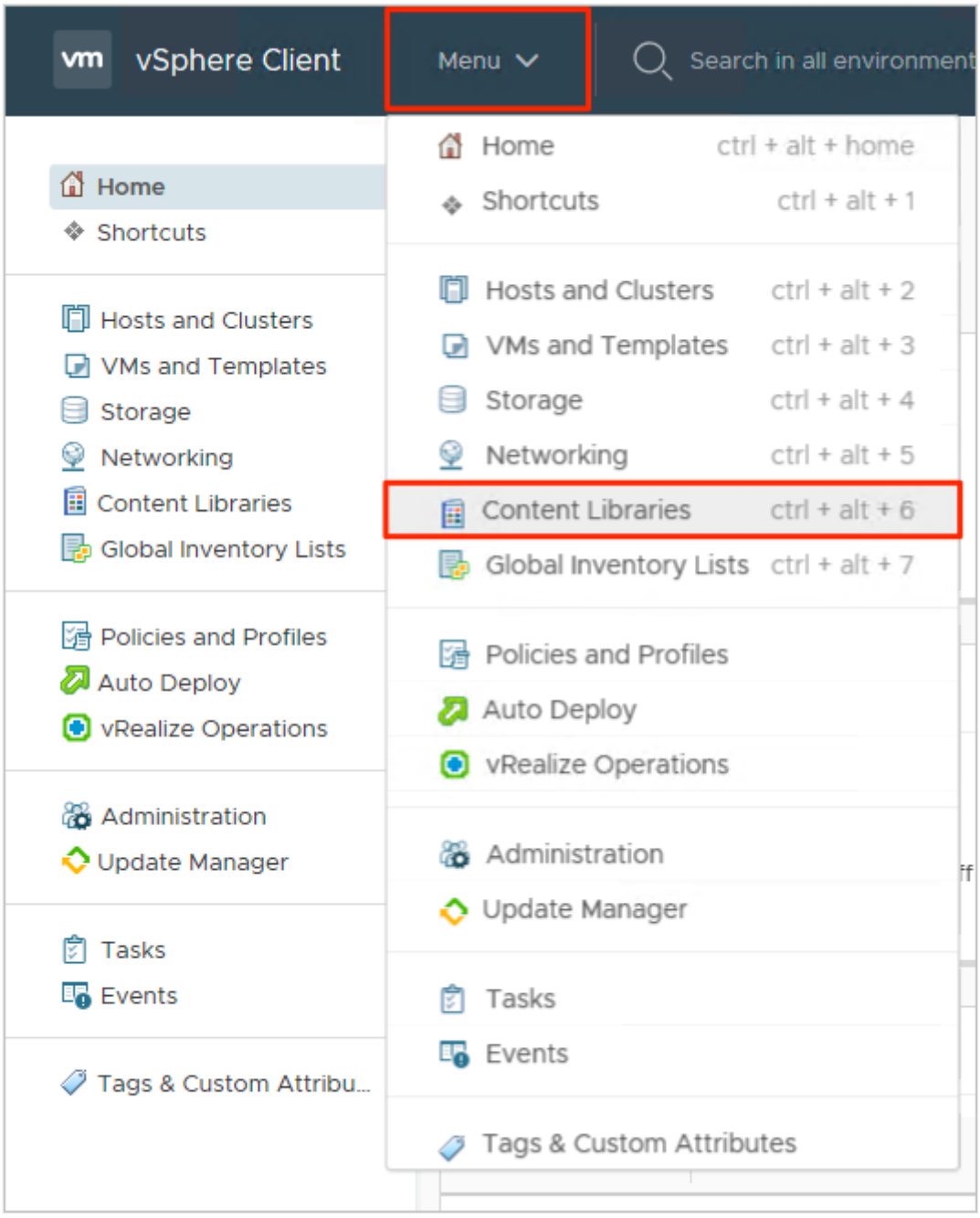
In this article, learn how to create a content library in the vSphere Client and deploy a VM using an ISO image from the content library.

Prerequisites

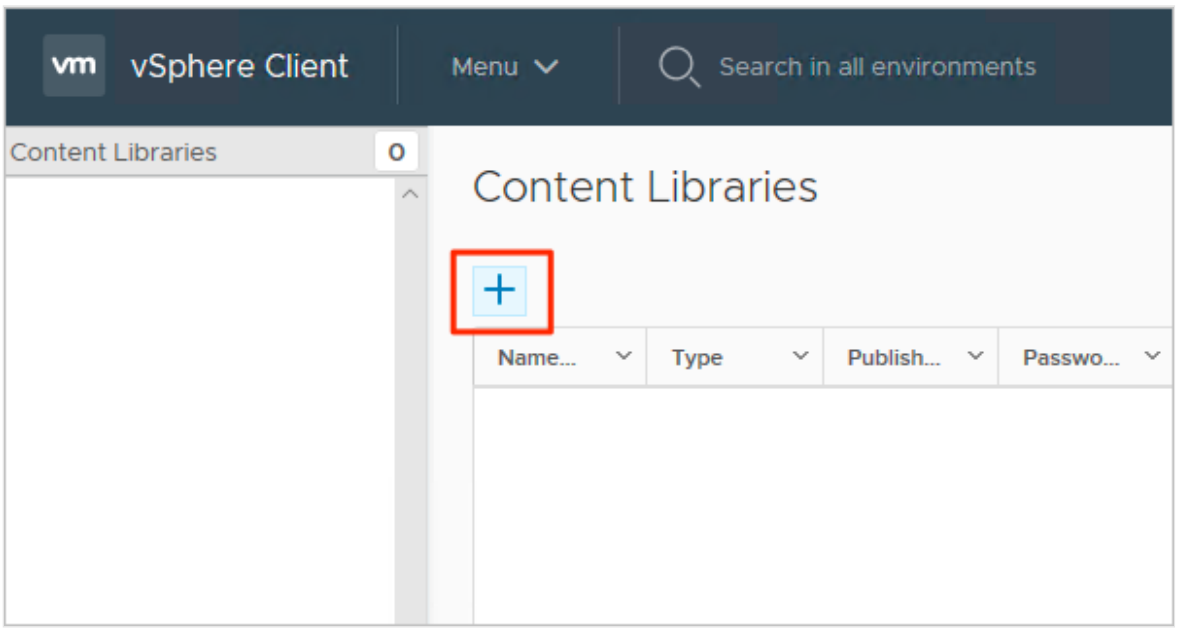
An NSX-T Data Center segment and a managed DHCP service are required to complete this tutorial. For more information, see Configure DHCP for Azure VMware Solution.

Create a content library

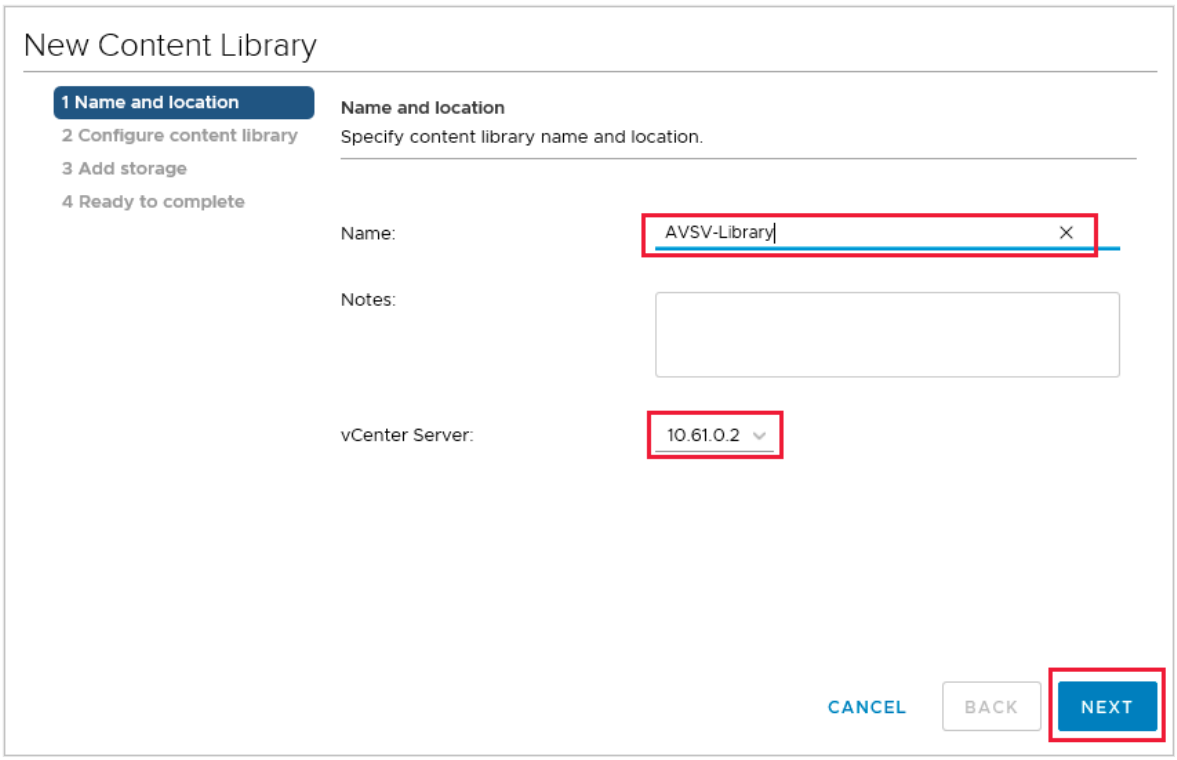
1. From the on-premises vSphere Client, select **Menu** > **Content Libraries**.



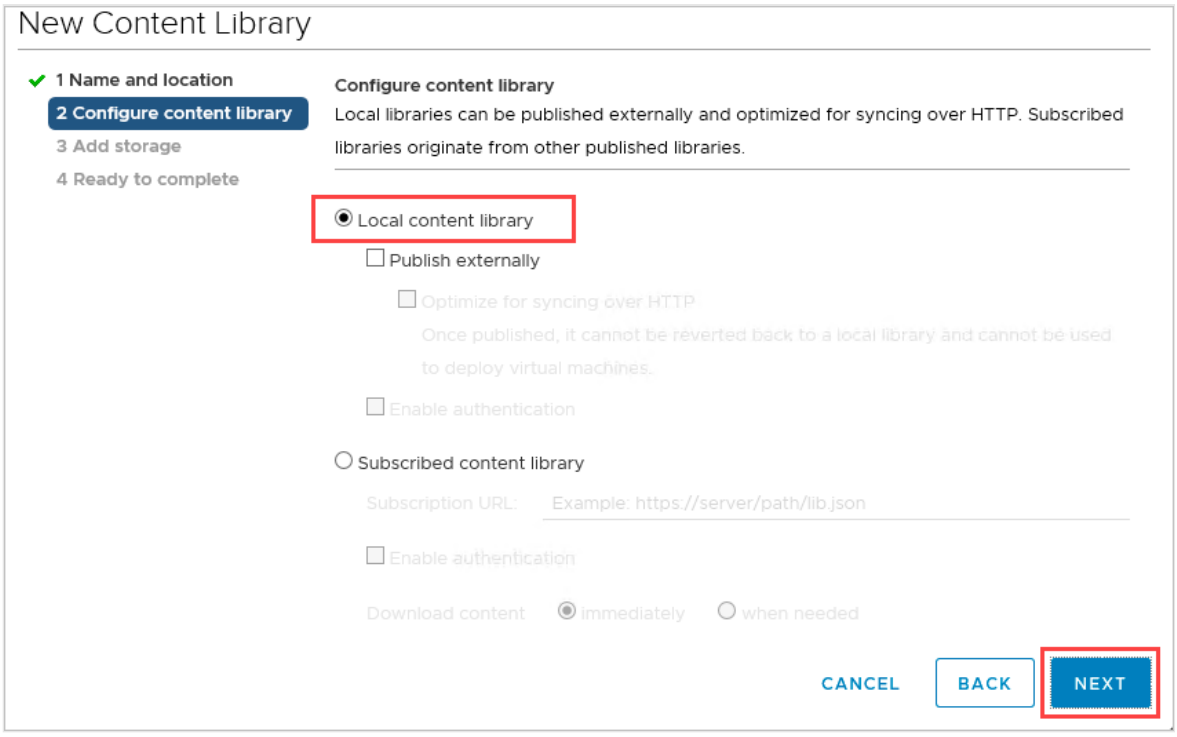
2. Select **Add** to create a new content library.



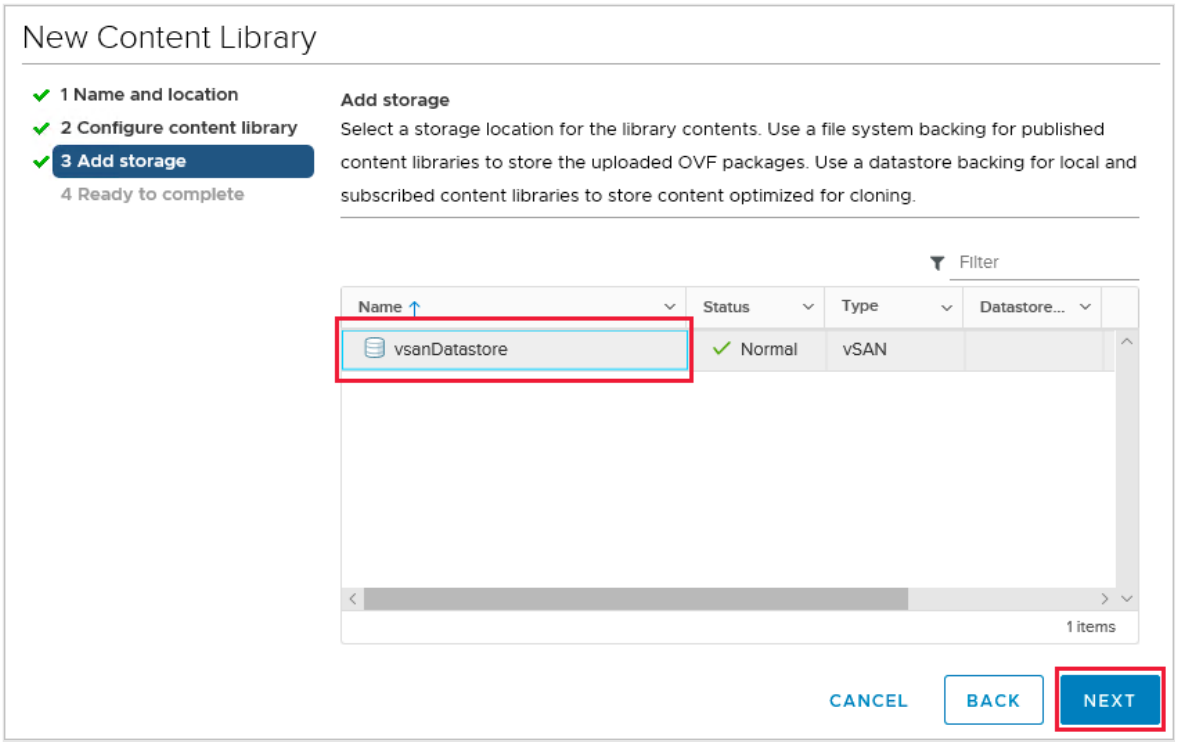
3. Provide a name and confirm the IP address of the vCenter Server and select **Next**.



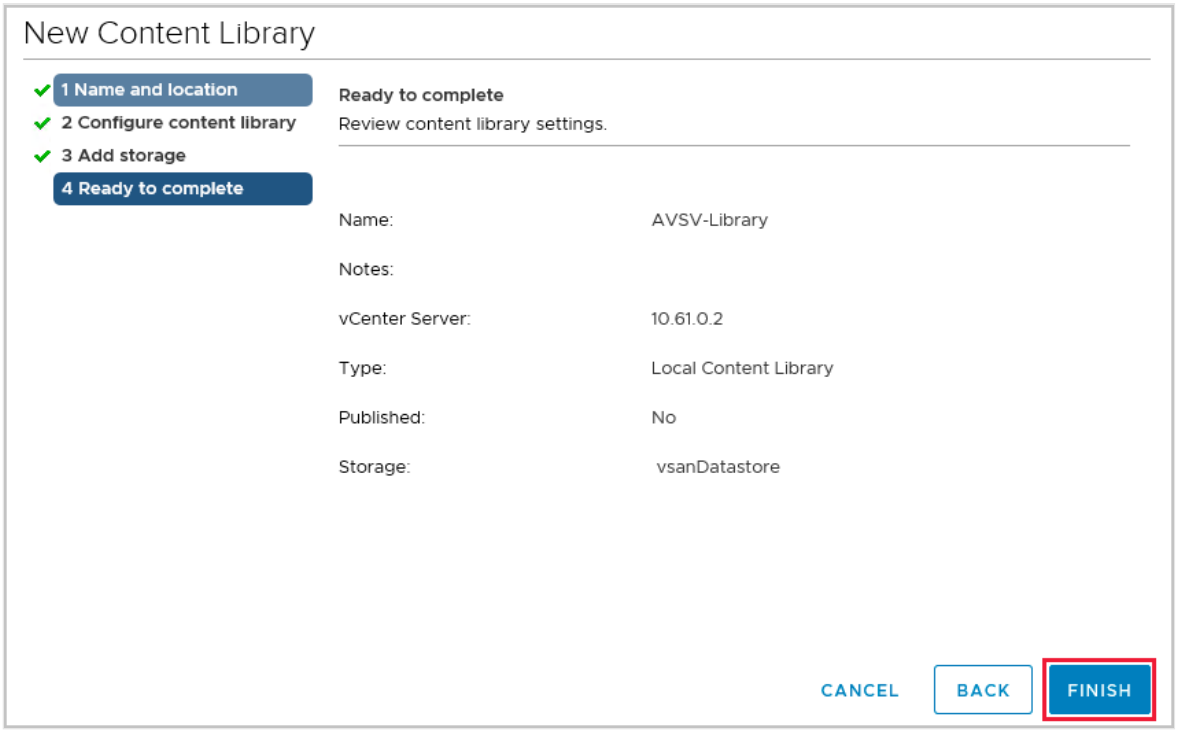
4. Select the **Local content library** and select **Next**.



5. Select the datastore for storing your content library, and then select **Next**.



6. Review the content library settings and select **Finish**.



Upload an ISO image to the content library

Now that you created the content library, you can add an ISO image to deploy a VM to a private cloud cluster.

1. From the vSphere Client, select **Menu** > **Content Libraries**.

2. Right-click the content library you want to use for the new ISO and select **Import Item**.

3. Import a library item for the Source by doing one of the following, and then select **Import**:

   a. Select URL and provide a URL to download an ISO.

   b. Select **Local File** to upload from your local system.

   > **Tip**
   >
   > Optional, you can define a custom item name and notes for the Destination.

4. Open the library and select the **Other Types** tab to verify that your ISO was uploaded successfully.

Deploy a VM to a private cloud cluster

1. From the vSphere Client, select **Menu** > **Hosts and Clusters**.
2. In the left panel, expand the tree and select a cluster.
3. Select **Actions** > **New Virtual Machine**.
4. Go through the wizard and modify the settings you want.
5. Select **New CD/DVD Drive** > **Client Device** > **Content Library ISO File**.
6. Select the ISO uploaded in the previous section and then select **OK**.
7. Select the **Connect** check box so the ISO is mounted at power-on time.
8. Select **New Network** > **Select dropdown** > **Browse**.
9. Select the **logical switch (segment)** and select **OK**.
10. Modify any other hardware settings and select **Next**.
11. Verify the settings and select **Finish**.

Next steps

Now that you created a content library to deploy VMs in Azure VMware Solution, learn more about:

- Migrating VM workloads to your private cloud

- Integrating Azure native services in Azure VMware Solution

Configure GitHub Enterprise Server on Azure VMware Solution

Article • 12/08/2023

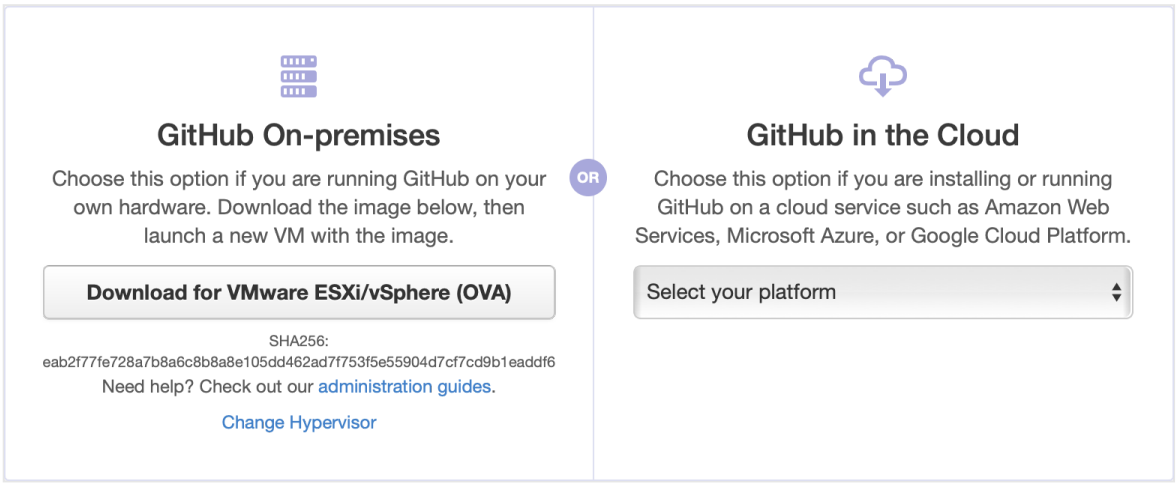
In this article, learn how to set up GitHub Enterprise Server, the "on-premises" version of GitHub.com, on your Azure VMware Solution private cloud. The scenario covers a GitHub Enterprise Server instance that can serve up to 3,000 developers running up to 25 jobs per minute on GitHub Actions. It includes the setup of (at time of writing) *preview* features, such as GitHub Actions. To customize the setup for your particular needs, review the requirements listed in Installing GitHub Enterprise Server on VMware.

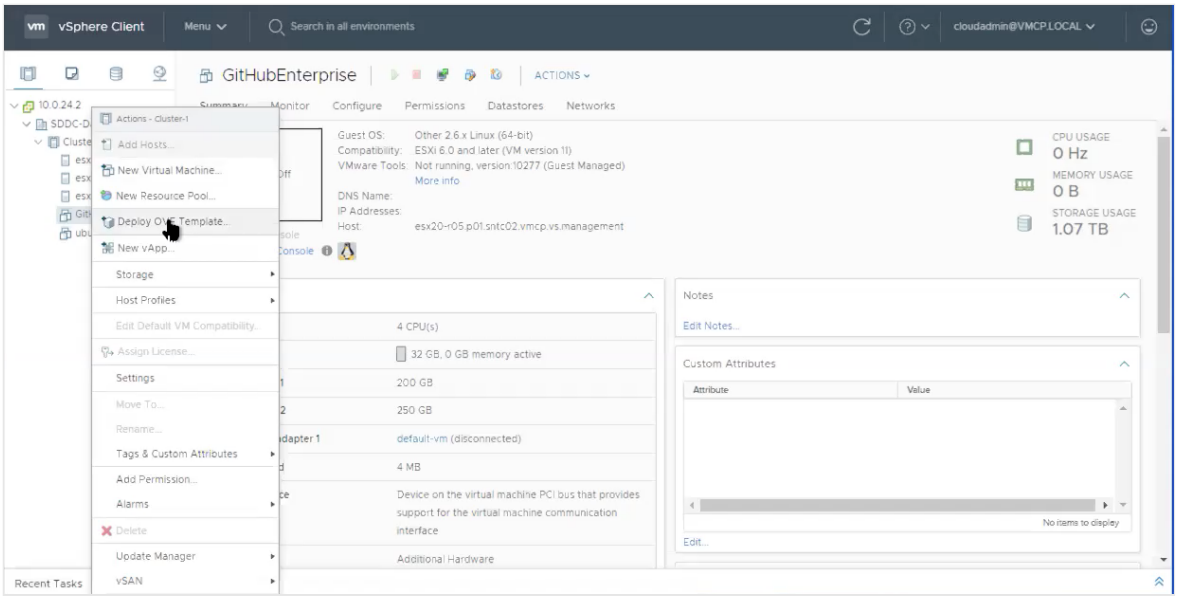
Before you begin

GitHub Enterprise Server requires a valid license key. You can sign up for a trial license. If you're looking to extend the capabilities of GitHub Enterprise Server via an integration, check if you qualify for a free five-seat developer license. Apply for this license through GitHub's Partner Program.

Install GitHub Enterprise Server on VMware

1. Download the current release of GitHub Enterprise Server for VMware ESXi/vSphere (OVA) and deploy the OVA template you downloaded.





2. Provide a recognizable name for your new virtual machine, such as GitHubEnterpriseServer. You don't need to include the release details in the VM name, as these details become stale when the instance is upgraded.

3. Select all the defaults for now (details to be edited later) and wait for the OVA to be imported.

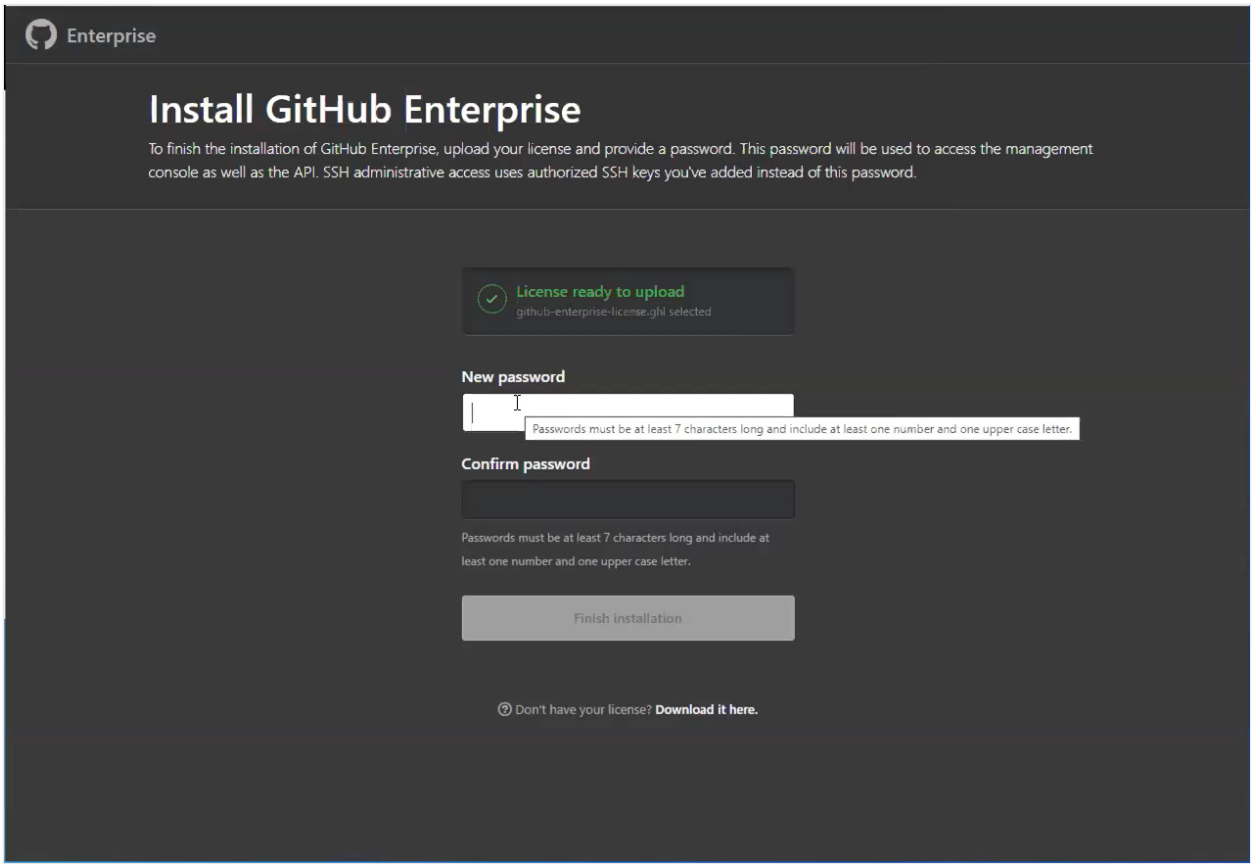
4. Once imported, adjust the hardware configuration based on your needs. In our example scenario, we need the following configuration.

Expand table

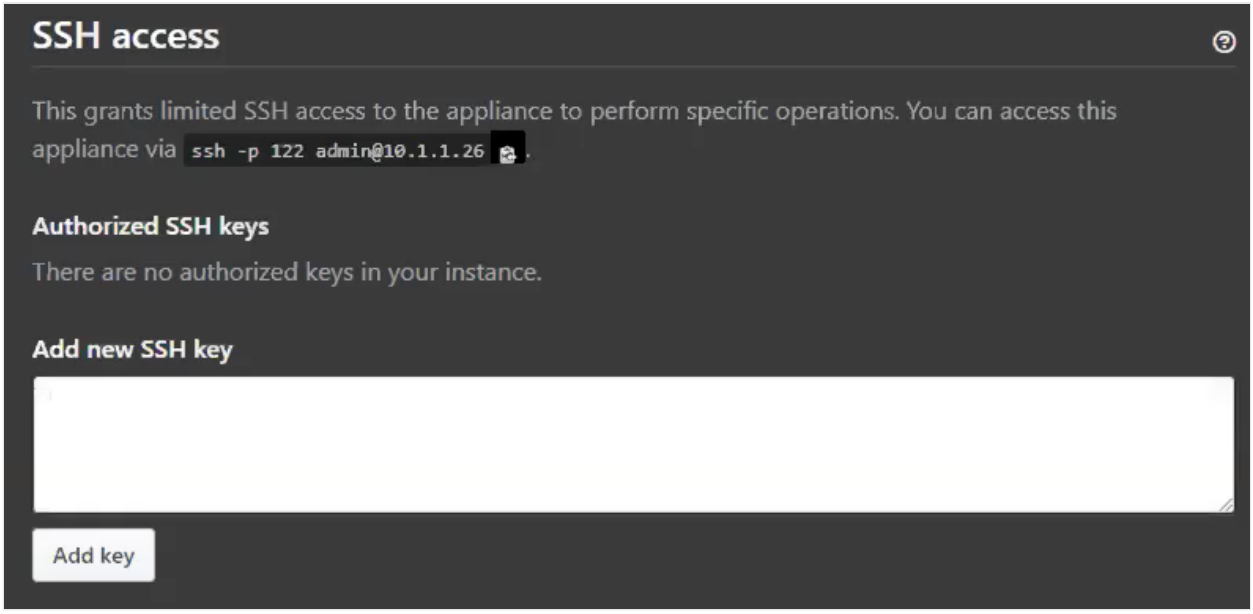
Resource	Standard Setup	Standard Set up + "Beta Features" (Actions)
vCPUs	4	8
Memory	32 GB	61 GB
Attached storage	250 GB	300 GB
Root storage	200 GB	200 GB

Your needs can vary. Refer to the guidance on hardware considerations in Installing GitHub Enterprise Server on VMware. Also see Adding CPU or memory resources for VMware to customize the hardware configuration based on your situation.

Configure the GitHub Enterprise Server instance

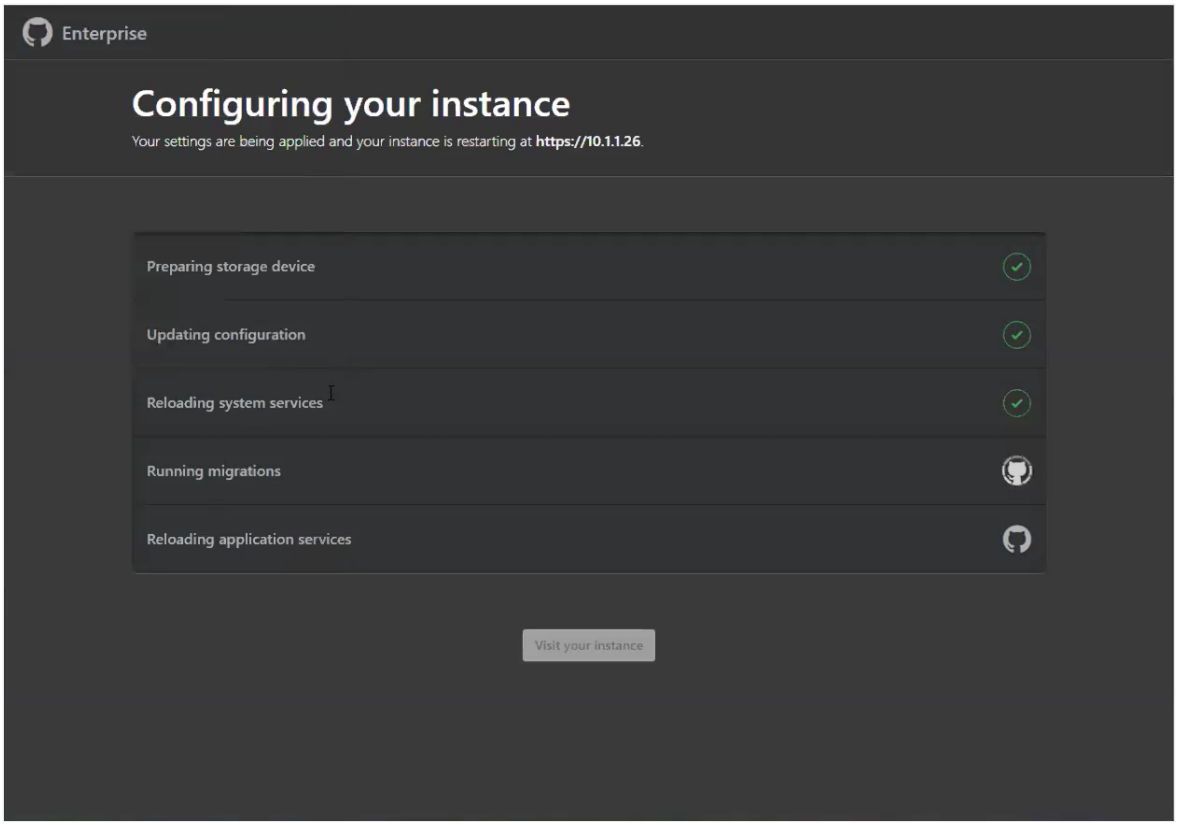


After the newly provisioned virtual machine (VM) is powered on, configure it through your browser. You need to upload your license file and set a management console password. Be sure to write down this password somewhere safe.



We recommend at least take the following steps:

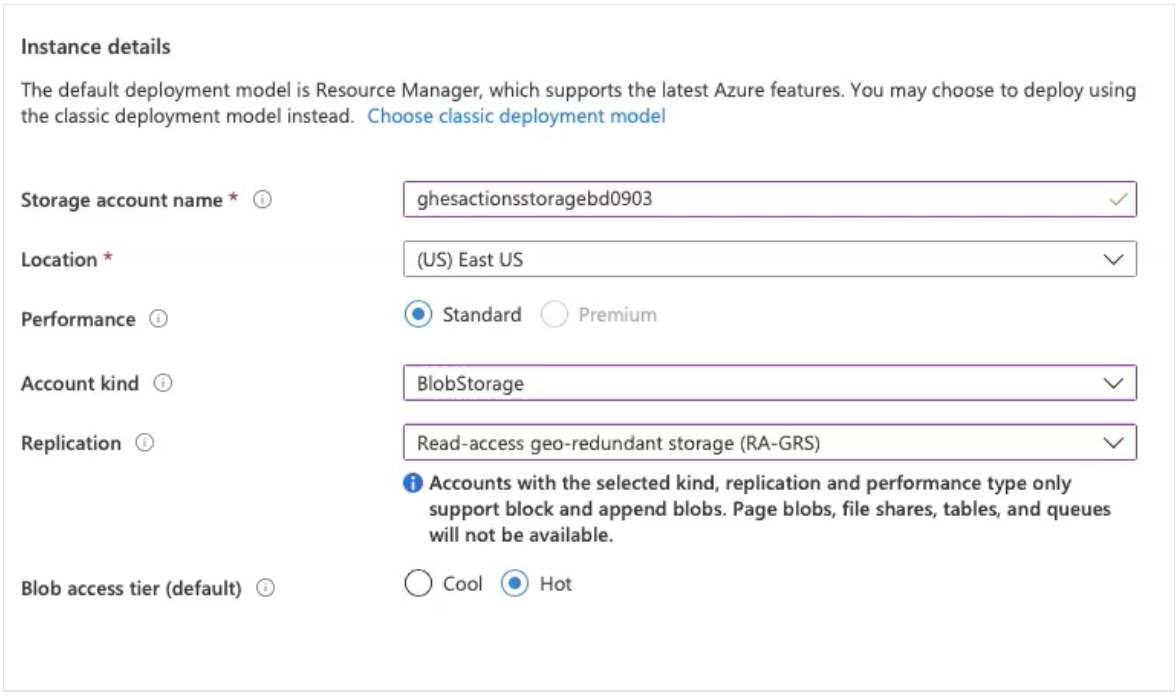
1. Upload a public SSH key to the management console so that you can access the administrative shell via SSH.
2. Configure TLS on your instance so that you can use a certificate signed by a trusted certificate authority. Apply your settings.



3. While the instance restarts, configure blob storage for GitHub Actions.

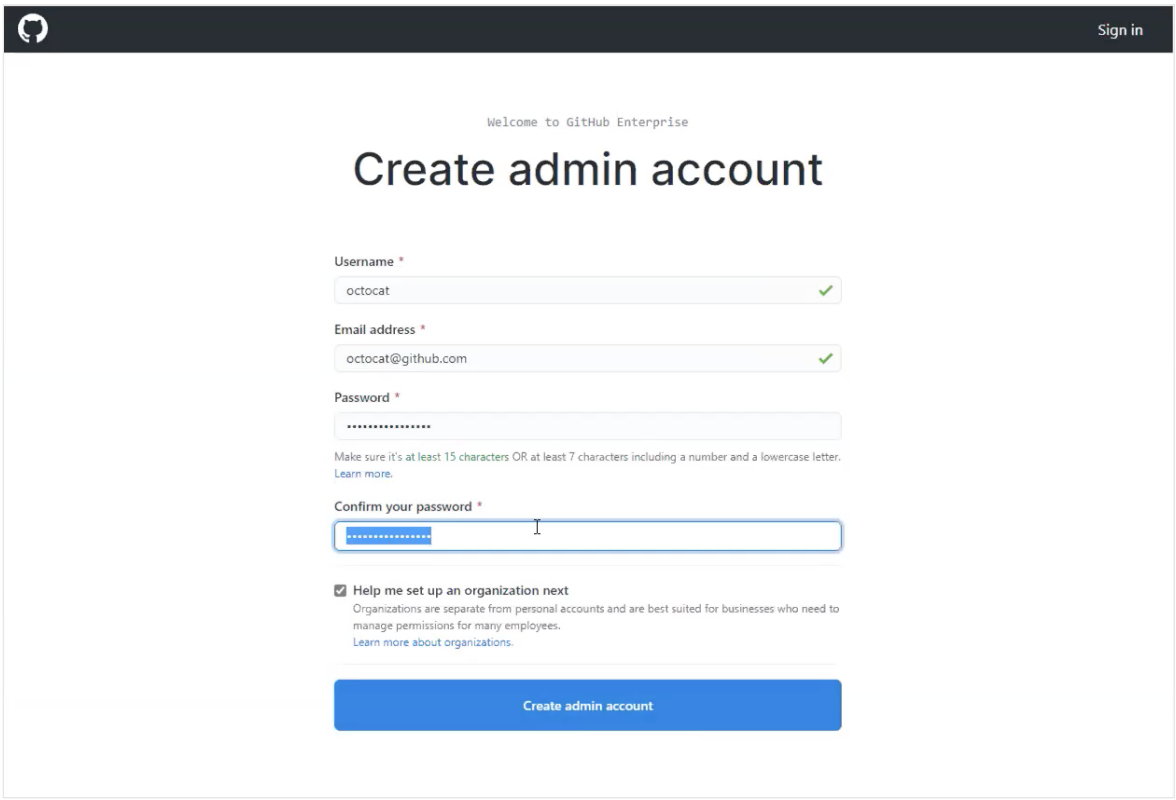
> **Note**
>
> GitHub Actions is **currently available as a limited beta on GitHub Enterprise Server release 2.22**.

External blob storage is necessary to enable GitHub Actions on GitHub Enterprise Server (currently available as a "beta" feature). Actions use this external blob storage to store artifacts and logs. Actions on GitHub Enterprise Server supports Azure Blob Storage as a storage provider (and some others). You need to create a new Azure storage account with a storage account type of BlobStorage.



4. Once the new BlobStorage resource deployment completes, save the connection string (available under Access keys) to use later.

5. After the instance restarts, create a new admin account on the instance. Be sure to make a note of this user's password as well.



Other configuration steps

To harden your instance for production use, the following optional setup steps are recommended:

1. Configure high availability for protection against:

    - Software crashes (OS or application level)
    - Hardware failures (storage, CPU, RAM, and so on)
    - Virtualization host system failures
    - Logically or physically severed network

2. Configure backup-utilities, providing versioned snapshots for disaster recovery, hosted in availability that is separate from the primary instance.

3. Setup subdomain isolation, using a valid TLS certificate, to mitigate cross-site scripting and other related vulnerabilities.

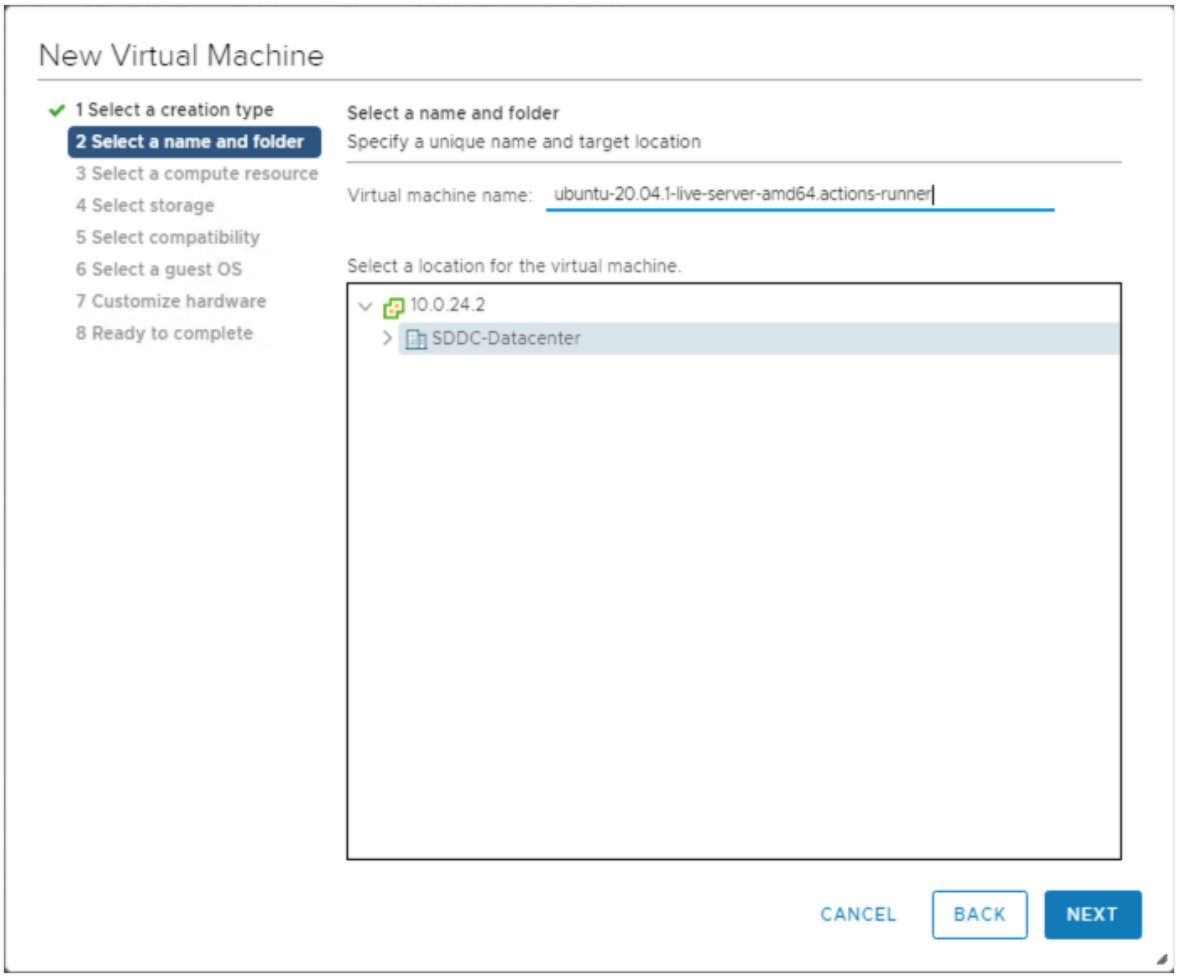
Set up the GitHub Actions runner

> **Note**
>
> GitHub Actions is **currently available as a limited beta on GitHub Enterprise Server release 2.22**.

At this point, you should have an instance of GitHub Enterprise Server running, with an administrator account created. You should also have external blob storage that GitHub Actions uses for persistence.

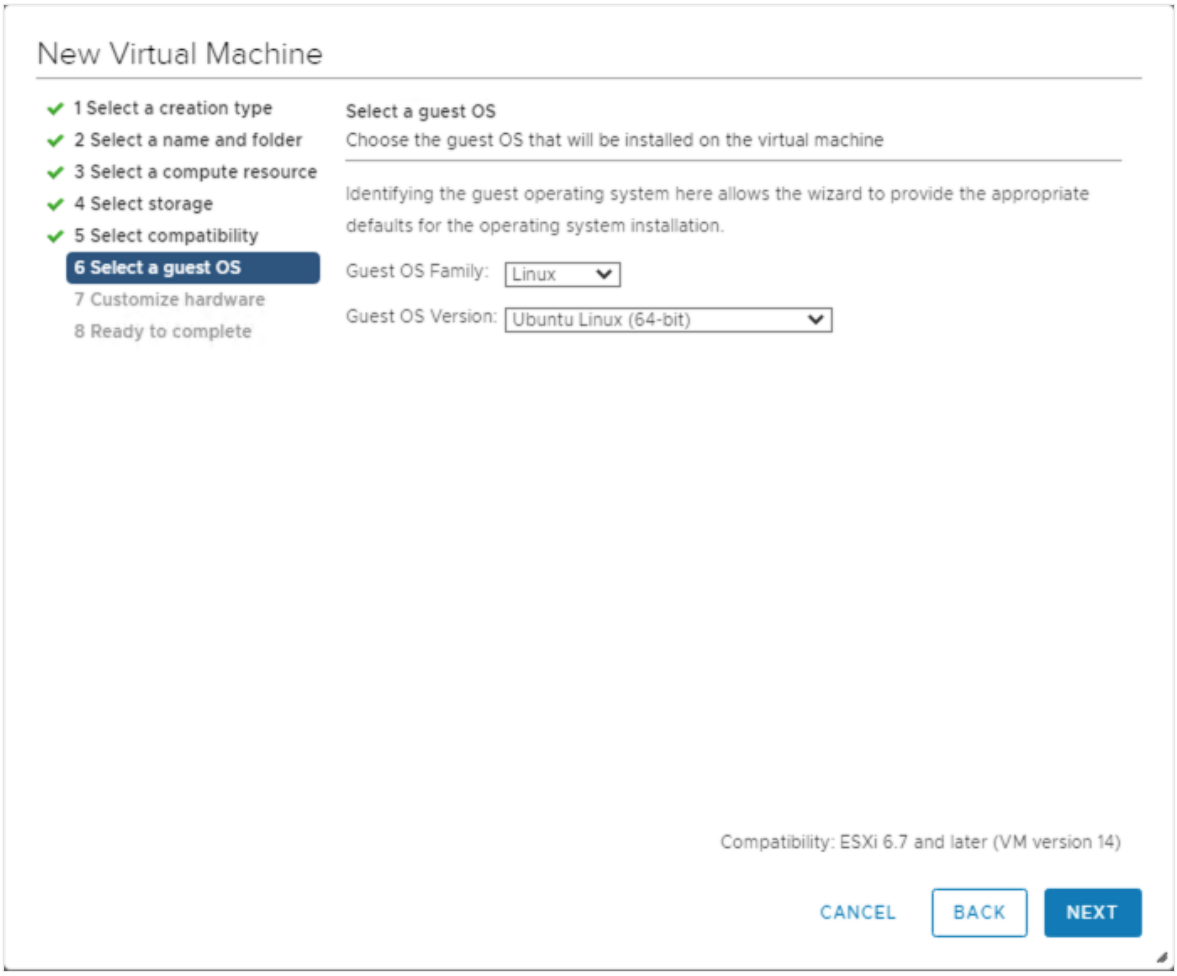
Create somewhere for GitHub Actions to run using Azure VMware Solution.

1. Provision a new VM on the cluster and base it on a recent release of Ubuntu Server.



2. Continue through the setup selecting the compute resource, storage, and compatibility.

3. Select the guest OS you want installed on the VM.



4. Once the VM is created, power it up and connect to it via SSH.

5. Install the Actions runner application, which runs a job from a GitHub Actions workflow. Identify and download the most current Linux x64 release of the Actions runner, either from the releases page or by running the following quick script. This script requires both curl and jq to be present on your VM.

```bash
LATEST\_RELEASE\_ASSET\_URL=$( curl https://api.github.com/repos/actions/runner/releases/latest | \

jq -r '.assets | .[] | select(.name | match("actions-runner-linux-arm64")) | .url' )

DOWNLOAD\_URL=$( curl $LATEST\_RELEASE\_ASSET\_URL | \

jq -r '.browser\_download\_url' )

curl -OL $DOWNLOAD\_URL
```

   You should now have a file locally on your VM, actions-runner-linux-arm64-*.tar.gz. Extract this tarball locally:

```bash
tar xzf actions-runner-linux-arm64-\*.tar.gz
```

This extraction unpacks a few files locally, including a `config.sh` and `run.sh` script.

Enable GitHub Actions

> **Note**
>
> GitHub Actions is **currently available as a limited beta on GitHub Enterprise Server release 2.22**.

Configure and enable GitHub Actions on the GitHub Enterprise Server instance.

1. Access the GitHub Enterprise Server instance's administrative shell over SSH, and then run the following commands:
2. Set an environment variable containing your Blob storage connection string.

   ```bash
   export CONNECTION\_STRING="<your connection string from the blob storage step>"
   ```

3. Configure actions storage.

   ```bash
   ghe-config secrets.actions.storage.blob-provider azure

   ghe-config secrets.actions.storage.azure.connection-string "$CONNECTION\_STRING`
   ```

4. Apply the settings.

   ```bash
   ghe-config-apply
   ```

5. Execute a precheck to install more software required by Actions on GitHub Enterprise Server.

```bash
ghe-actions-precheck -p azure -cs "$CONNECTION\_STRING"
```

6. Enable actions, and reapply the configuration.

```bash
ghe-config app.actions.enabled true

ghe-config-apply
```

7. Check the health of your blob storage.

```bash
ghe-actions-check -s blob
```

   You should see output: *Blob Storage is healthy*.

8. Now that **GitHub Actions** is configured, enable it for your users. Sign in to your GitHub Enterprise Server instance as an administrator, and select the 🚀 in the upper right corner of any page.

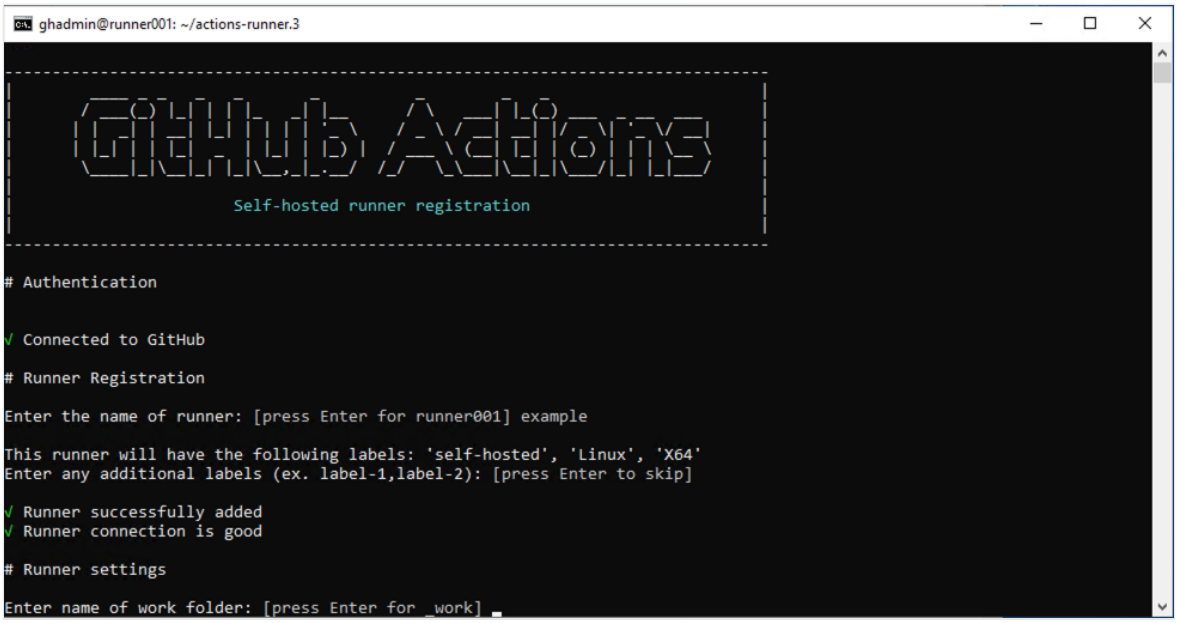
9. In the left sidebar, select **Enterprise overview**, then **Policies**, **Actions**, and select the option to **enable Actions for all organizations**.

10. Configure your runner from the **Self-hosted runners** tab. Select **Add new** and then **New runner** from the drop-down. You're presented with a set of commands to run.

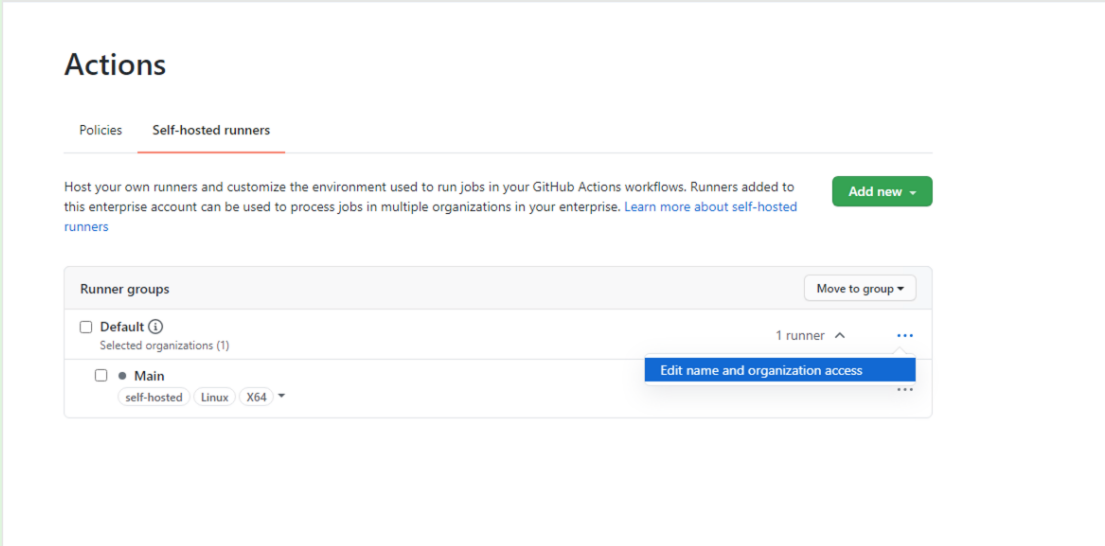
11. Copy the command to **configure** the runner, for instance:

```bash
./config.sh --url https://10.1.1.26/enterprises/octo-org --token
AAAAAA5RHF34QLYBDCHWLJC7L73MA
```

12. Copy the `config.sh` command and paste it into a session on your Actions runner (created previously).



13. Use the `./run.sh` command to *run* the runner:

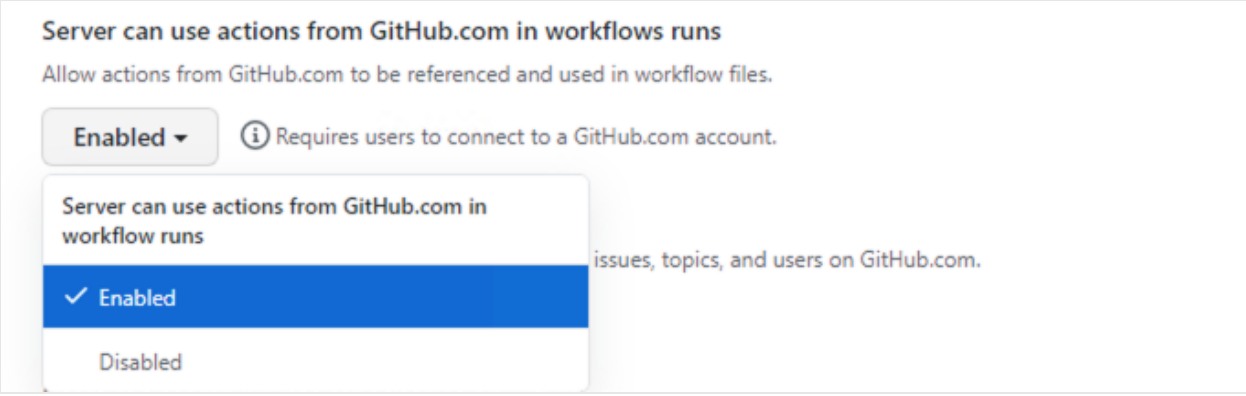
> **Tip**
>
> To make this runner available to organizations in your enterprise, edit its organization access. You can limit access to a subset of organizations, and even to specific repositories.
>
> 
>

(Optional) Configure GitHub Connect

Although this step is optional, we recommend it if you plan to consume open-source actions available on GitHub.com. It allows you to build on the work of others by referencing these reusable actions in your workflows.

To enable GitHub Connect, follow the steps in Enabling automatic access to GitHub.com actions using GitHub Connect.

Once GitHub Connect is enabled, select the **Server to use actions from GitHub.com in workflow runs** option.



Set up and run your first workflow

Now that Actions and GitHub Connect is set up, let's put all this work to good use. Here's an example workflow that references the excellent octokit/request-action, allowing us to "script" GitHub through interactions using the GitHub API, powered by GitHub Actions.

In this basic workflow, use `octokit/request-action` to open an issue on GitHub using the API.

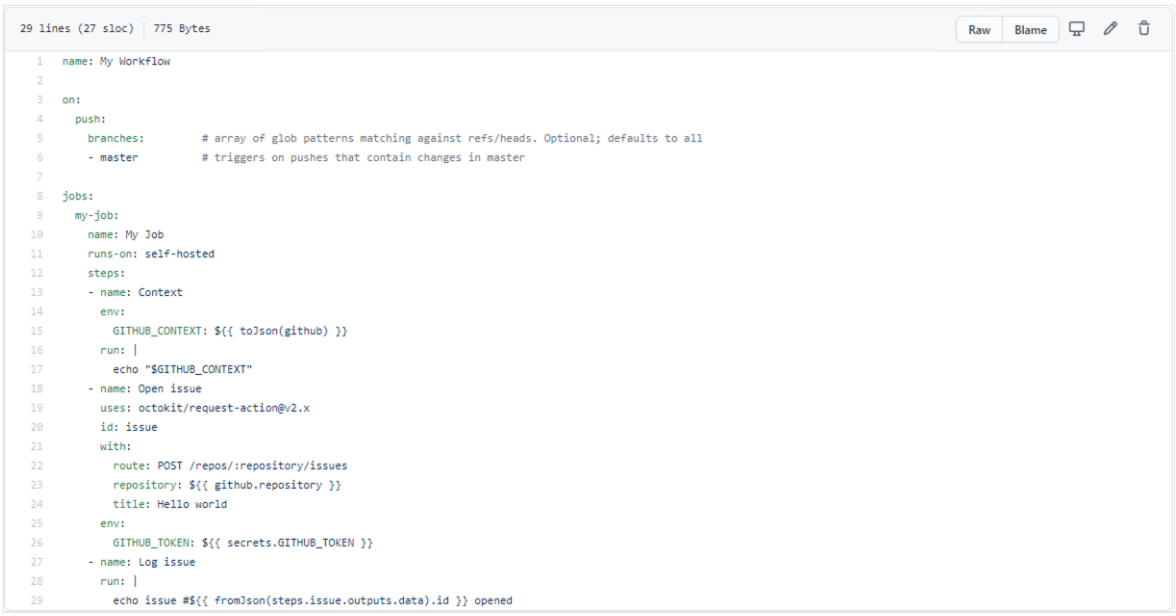
```
name: Open Issue

on:
  push

jobs:
  my-job:
    name: My Job
    runs-on: self-hosted
    steps:
    - name: Open issue
      uses: octokit/request-action@v2.x
      id: issue
      with:
        route: POST /repos/:repository/issues
        repository: ${{ github.repository }}
        title: Hello world
      env:
        GITHUB_TOKEN: ${{ secrets.GITHUB_TOKEN }}
    - name: Log issue
      run: |
        echo issue #${{ fromJson(steps.issue.outputs.data).id }}
opened
```

> **Note**
>
> GitHub.com hosts the action, but when it runs on GitHub Enterprise Server, it *automatically* uses the GitHub Enterprise Server API.

If you chose not to enable GitHub Connect, you could use the following alternative workflow.

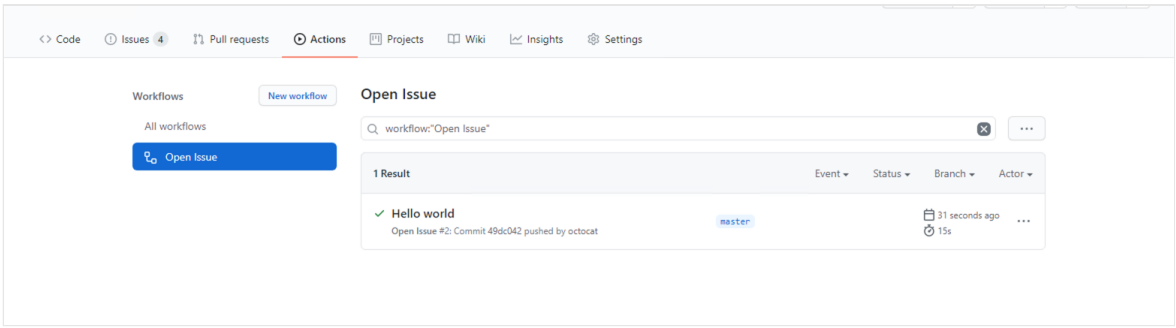
```
name: Open Issue

on:
  push

jobs:
  my-job:
    name: My Job
    runs-on: self-hosted
    steps:
    - name: Open issue
      run: |
        curl -H "Authorization: bearer $GITHUB_TOKEN" -d '{"title":
"Hello world"}' "$GITHUB_API_URL/repos/${{ github.repository }}/issues"
      env:
        GITHUB_TOKEN: ${{ secrets.GITHUB_TOKEN }}
```

1. Navigate to a repo on your instance, and add the above workflow as: `.github/workflows/hello-world.yml`

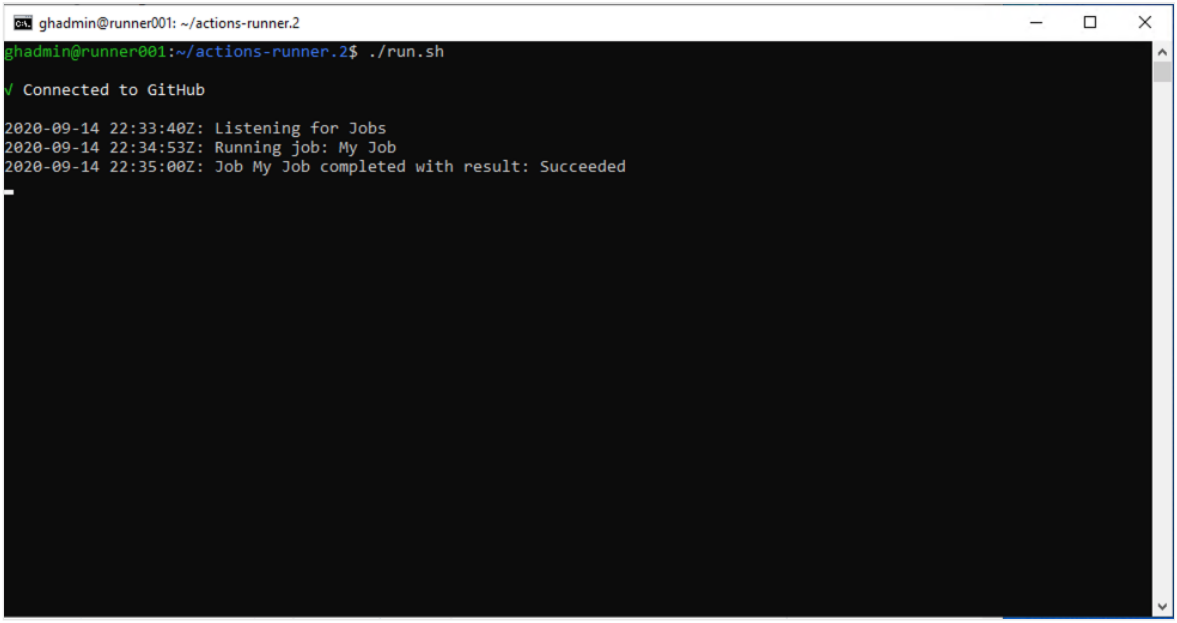


```
29 lines (27 sloc) | 775 Bytes                                                    Raw  Blame

1  name: My Workflow
2
3  on:
4    push:
5      branches:        # array of glob patterns matching against refs/heads. Optional; defaults to all
6      - master         # triggers on pushes that contain changes in master
7
8  jobs:
9    my-job:
10     name: My Job
11     runs-on: self-hosted
12     steps:
13     - name: Context
14       env:
15         GITHUB_CONTEXT: ${{ toJson(github) }}
16       run: |
17         echo "$GITHUB_CONTEXT"
18     - name: Open issue
19       uses: octokit/request-action@v2.x
20       id: issue
21       with:
22         route: POST /repos/:repository/issues
23         repository: ${{ github.repository }}
24         title: Hello world
25       env:
26         GITHUB_TOKEN: ${{ secrets.GITHUB_TOKEN }}
27     - name: Log issue
28       run: |
29         echo issue #${{ fromJson(steps.issue.outputs.data).id }} opened
```

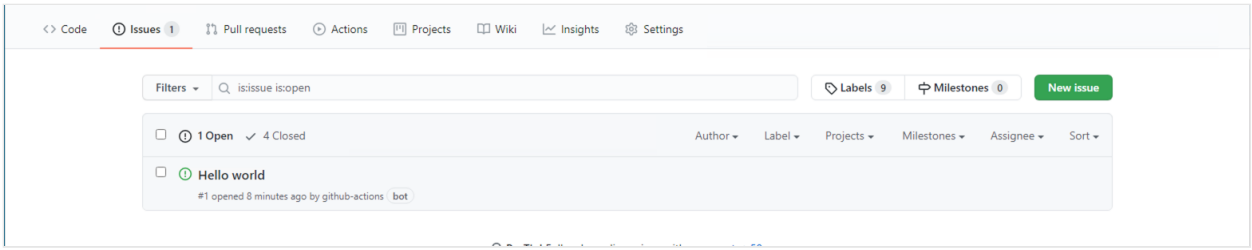
2. In the **Actions** tab for your repo, wait for the workflow to execute.



You can see it being processed.



If everything ran successfully, you should see a new issue in your repo, entitled "Hello world."



Congratulations! You just completed your first Actions workflow on GitHub Enterprise Server, running on your Azure VMware Solution private cloud.

This article set up a new instance of GitHub Enterprise Server, the self-hosted equivalent of GitHub.com, on top of your Azure VMware Solution private cloud. The instance includes support for GitHub Actions and uses Azure Blob Storage for persistence of logs and artifacts. But we're just scratching the surface of what you can do with GitHub Actions. Check out the list of Actions on GitHub's Marketplace, or create your own.

Next steps

Now that you covered setting up GitHub Enterprise Server on your Azure VMware Solution private cloud, learn more about:

- How to get started with GitHub Actions
- How to join the beta program
- Administration of GitHub Enterprise Server

Bitnami appliance deployment

Article • 11/28/2023

Bitnami by VMware provides a rich catalog of turnkey virtual appliances. You can deploy any vSphere compatible appliance by Bitnami available in the VMware Marketplace, including many of the most common open-source software projects.

In this article, learn how to install and configure the following virtual appliances packaged by Bitnami on your Azure VMware Solution private cloud:

- LAMP
- Jenkins
- PostgreSQL
- NGINX
- RabbitMQ

Prerequisites

- Azure VMware Solution private cloud deployed with a minimum of three nodes.
- Networking configured as described in Network planning checklist.

Step 1: Download the Bitnami virtual appliance OVA/OVF file

1. Go to the VMware Marketplace and download the virtual appliance you want to install on your Azure VMware Solution private cloud:
    - LAMP virtual appliance packaged by Bitnami
    - Jenkins
    - PostgreSQL
    - NGINX
    - RabbitMQ
2. Select the version, select **Download**, and then accept the EULA license.

> **Note**
>
> Make sure the file is accessible from the virtual machine.

Step 2: Access the local vCenter Server of your private cloud

1. Sign in to the Azure portal.

   > **Note**
   >
   > If you need access to the Azure US Gov portal, go to **https://portal.azure.us/**

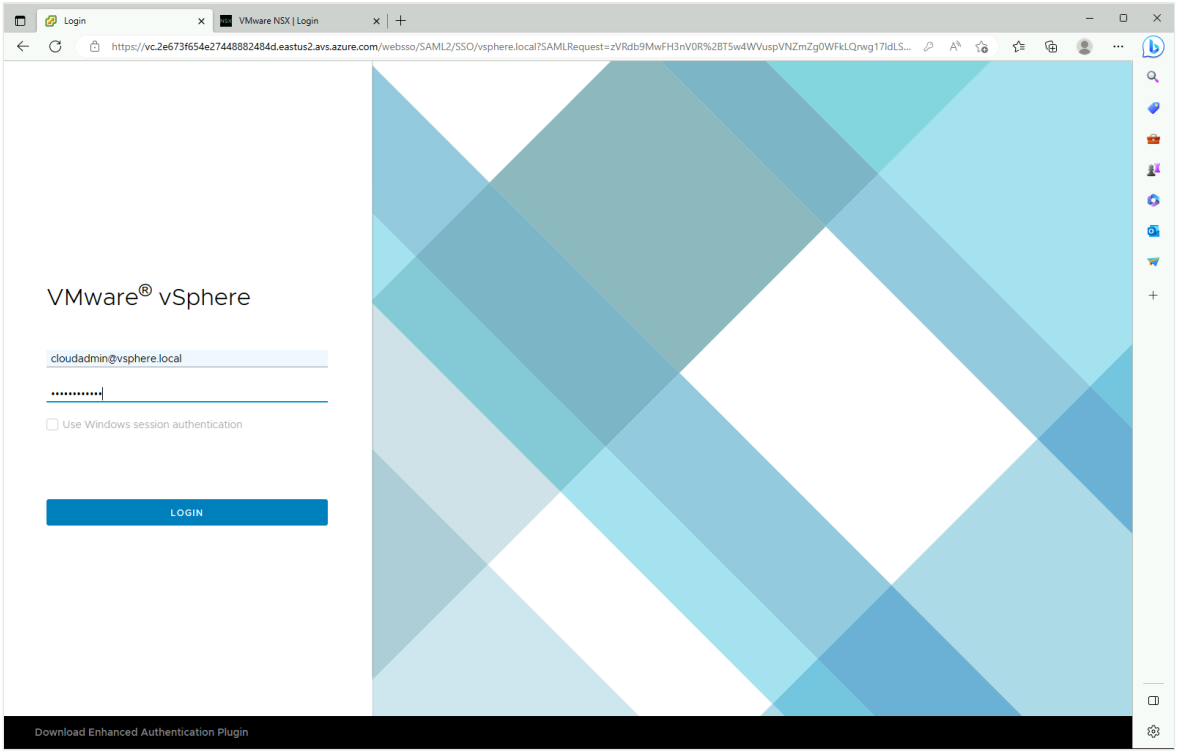
2. Select your private cloud, and then **Manage** > **Identity**.

3. Copy the vCenter Server URL, username, and password. You'll use them to access your virtual machine (VM).

4. Select **Overview**, select the VM, and then connect to it through RDP. If you need help with connecting, see connect to a virtual machine for details.

5. In the VM, open a browser and navigate to the vCenter URL.

6. Sign in with the `cloudadmin@vsphere.local` user credentials you copied earlier.



Step 3: Install the Bitnami OVA/OVF file in vCenter Server

1. Right-click the cluster that you want to install the LAMP virtual appliance and select **Deploy OVF Template**.
2. Select **Local file** and navigate to the OVF file you downloaded earlier. Then select **Next**.
3. Select your data center and provide a name for your virtual appliance VM, for example, **bitnami-lampstack**. Then select **Next**.
4. Select the ESXi host as the compute resource to run your VM and then select **Next**.
5. Review the details and select **Next**.
6. Accept the license agreement and select **Next**.
7. Select the storage for your VM and select **Next**.
8. Select the destination network for your VM and select **Next**.
9. Provide the required information to customize the template, such as the VM and networking properties. Then select **Next**.
10. Review the configuration settings and then select **Finish**.
11. From the **Task Console**, verify that the status of the OVF template deployment has completed successfully.
12. After the installation finishes, under **Actions**, select **Power on** to turn on the appliance.
13. From the vCenter Server console, select **Launch Web Console** and sign in to the Bitnami virtual appliance. Check the Bitnami virtual appliance support documentation for the default username and password.

> **Note**
>
> You can change the default password to a more secure one. For more information, see ...

Step 4: Assign a static IP to the virtual appliance

In this step, you'll modify the *bootproto* and *onboot* parameters and assign a static IP address to the Bitnami virtual appliance.

1. Search for the network configuration file.

```
Bash

sudo find /etc -name \*ens160\*
```

2. Edit the */etc/sysconfig/network-scripts/ifcfg-ens160* file and modify the boot parameters. Then add the static IP, netmask, and gateway addresses.

   - bootproto=static
   - onboot=yes

3. View and confirm the changes to the **ifcfg-ens160** file.

```
Bash

cat ifcfg-ens160
```

4. Restart the networking service. This stops the networking services first and then applies the IP configuration.

```
Bash

sudo systemctl restart network
```

5. Ping the gateway IP address to verify the configuration and VM connectivity to the network.

6. Confirm that the default route 0.0.0.0 is listed.

```
Bash

sudo route -n
```

Step 5: Enable SSH access to the virtual appliance

In this step, you'll enable SSH on your virtual appliance for remote access control. The SSH service is disabled by default. You'll also use an OpenSSH client to connect to the host console.

1. Enable and start the SSH service.

```
Bash

sudo rm /etc/ssh/sshd_not_to_be_run
sudo systemctl enable sshd
sudo systemctl start sshd
```

2. Edit the */etc/ssh/sshd_config* file to change the password authentication.

```
Bash

PasswordAuthentication yes
```

3. View and confirm the changes to the **sshd_config** file.

```
Bash

sudo cat sshd_config
```

4. Reload the changes made to the file.

```
Bash

sudo /etc/init.d/ssh force-reload
```

5. Start the SSH session.

```
Bash

ssh hostname:22
```

6. At the virtual appliance console prompt, enter the Bitnami username and password to connect to the host.

Deploy Horizon on Azure VMware Solution

Article • 04/01/2024

> **Note**
>
> This document focuses on the VMware Horizon product, formerly known as Horizon 7. Horizon is a different solution than Horizon Cloud on Azure, although there are some shared components. Key advantages of the Azure VMware Solution include both a more straightforward sizing method and the integration of Software-Defined Data Center (SDDC) private cloud management into the Azure portal.

VMware Horizon ®, a virtual desktop and applications platform, runs in the data center and provides simple and centralized management. It delivers virtual desktops and applications on any device, anywhere. Horizon lets you create, and broker connections to Windows and Linux virtual desktops, Remote Desktop Server (RDS) hosted applications, desktops, and physical machines.

Here, we focus specifically on deploying Horizon on Azure VMware Solution. For general information on VMware Horizon, refer to the Horizon production documentation:

- What is VMware Horizon?
- Learn more about VMware Horizon
- Horizon Reference Architecture

With Horizon's introduction on Azure VMware Solution, there are now two Virtual Desktop Infrastructure (VDI) solutions on the Azure platform:

- VMware Horizon on Azure VMware Solution
- VMware Horizon Cloud (Desktop-as-a-Service Model)

Horizon 2006 and later versions on the Horizon 8 release line supports both on-premises and Azure VMware Solution deployment. There are a few Horizon features that are supported on-premises but not on Azure VMware Solution. Other products in the Horizon ecosystem are also supported. For more information, see feature parity and interoperability.

Deploy Horizon in a hybrid cloud

You can deploy Horizon in a hybrid cloud environment by using Horizon Cloud Pod Architecture (CPA) to interconnect on-premises and Azure data centers. CPA scales up your deployment, builds a hybrid cloud, and provides redundancy for Business Continuity and Disaster Recovery. For more information, see Expanding Existing Horizon 7 Environments.

> **Important**
>
> CPA is not a stretched deployment; each Horizon pod is distinct, and all Connection Servers that belong to each of the individual pods are required to be located in a single location and run on the same broadcast domain from a network perspective.

Like on-premises or private data centers, you can deploy Horizon in an Azure VMware Solution private cloud. In the following sections, we discuss the key differences in deploying Horizon on-premises and Azure VMware Solution.

The *Azure private cloud* is conceptually the same as the *VMware SDDC*, a term typically used in Horizon documentation. The rest of this document uses both terms interchangeably.

The Horizon Cloud Connector is required for Horizon on Azure VMware Solution to manage subscription licenses. You can deploy Cloud Connector in Azure Virtual Network alongside Horizon Connection Servers.

> **Important**
>
> Horizon Control Plane support for Horizon on Azure VMware Solution is not yet available. Be sure to download the VHD version of Horizon Cloud Connector.

vCenter Server Cloud Admin role

Since Azure VMware Solution is an SDDC service and Azure manages the lifecycle of the SDDC on Azure VMware Solution, the vCenter Server permission model on Azure VMware Solution is limited by design.

Customers are required to use the Cloud Admin role, which has a limited set of vCenter Server permissions. The Horizon product was modified to work with the Cloud Admin role on Azure VMware Solution, specifically:

- Instant clone provisioning was modified to run on Azure VMware Solution.
- A specific vSAN policy (VMware_Horizon) was created on Azure VMware Solution to work with Horizon, which must be available and used in the SDDCs deployed for Horizon.
- vSphere Content-Based Read Cache (CBRC), also known as View Storage Accelerator, is disabled when running on the Azure VMware Solution.

> **Important**
>
> CBRC must not be turned back on.

> **Note**
>
> Azure VMware Solution automatically configures specific Horizon settings as long as you deploy Horizon 2006 (Horizon 8) and higher on the Horizon 8 branch and select the **Azure** option in the Horizon Connection Server installer.

Horizon on Azure VMware Solution deployment architecture

A typical Horizon architecture design uses a pod and block strategy. A block is a single vCenter Server, while multiple blocks combined make a pod. A Horizon pod is a unit of organization determined by Horizon scalability limits. Each Horizon pod has a separate management portal, and so a standard design practice is to minimize the number of pods.

Every cloud has its own network connectivity scheme. Combine that with VMware NSX, the Azure VMware Solution network connectivity presents unique requirements for deploying Horizon that is different from on-premises.

Each Azure VMware Solution private cloud and SDDC can handle 4,000 desktop or application sessions, assuming:

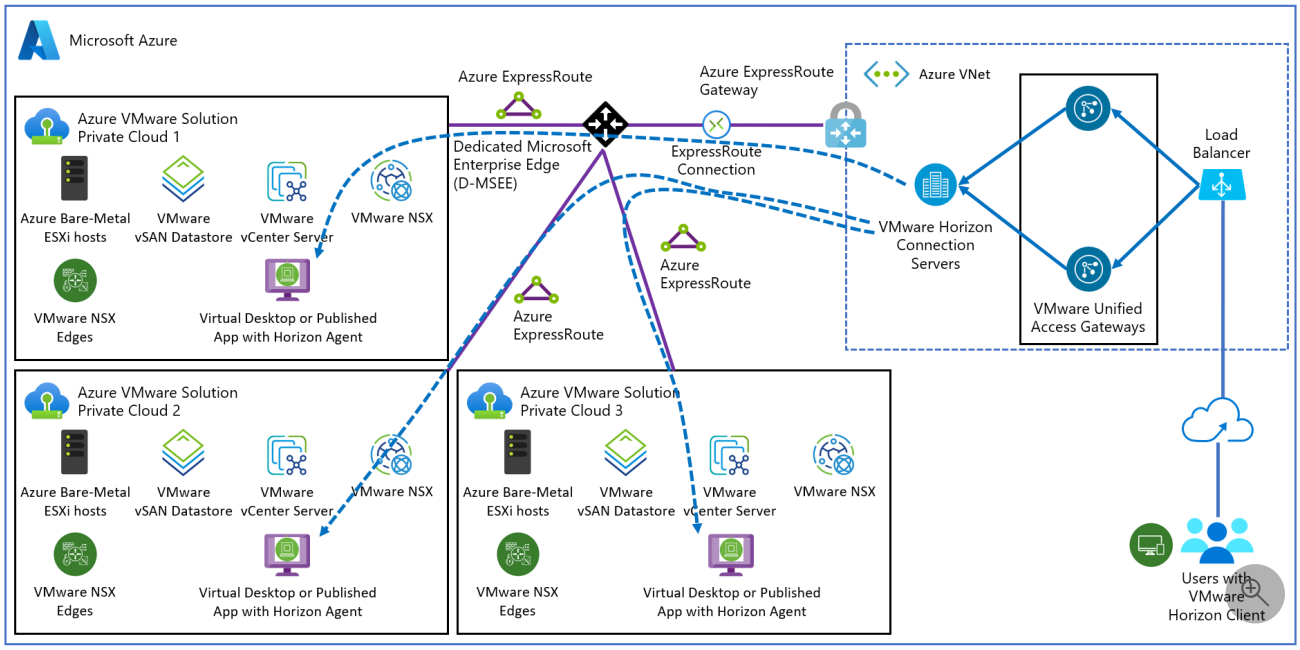
- The workload traffic aligns with the LoginVSI task worker profile.
- Only protocol traffic is considered, no user data.
- NSX Edge is configured to be large.

> **Note**
>
> Your workload profile and needs may be different, and therefore results may vary based on your use case. User Data volumes may lower scale limits in the context of your workload. Size and plan your deployment accordingly. For more information, see the sizing guidelines in the Size Azure VMware Solution hosts for Horizon deployments section.

Given the Azure private cloud and SDDC max limit, we recommend a deployment architecture where the Horizon Connection Servers and VMware Unified Access Gateways (UAGs) are running inside the Azure Virtual Network. It effectively

turns each Azure private cloud and SDDC into a block. In turn, maximizing the scalability of Horizon running on Azure VMware Solution.

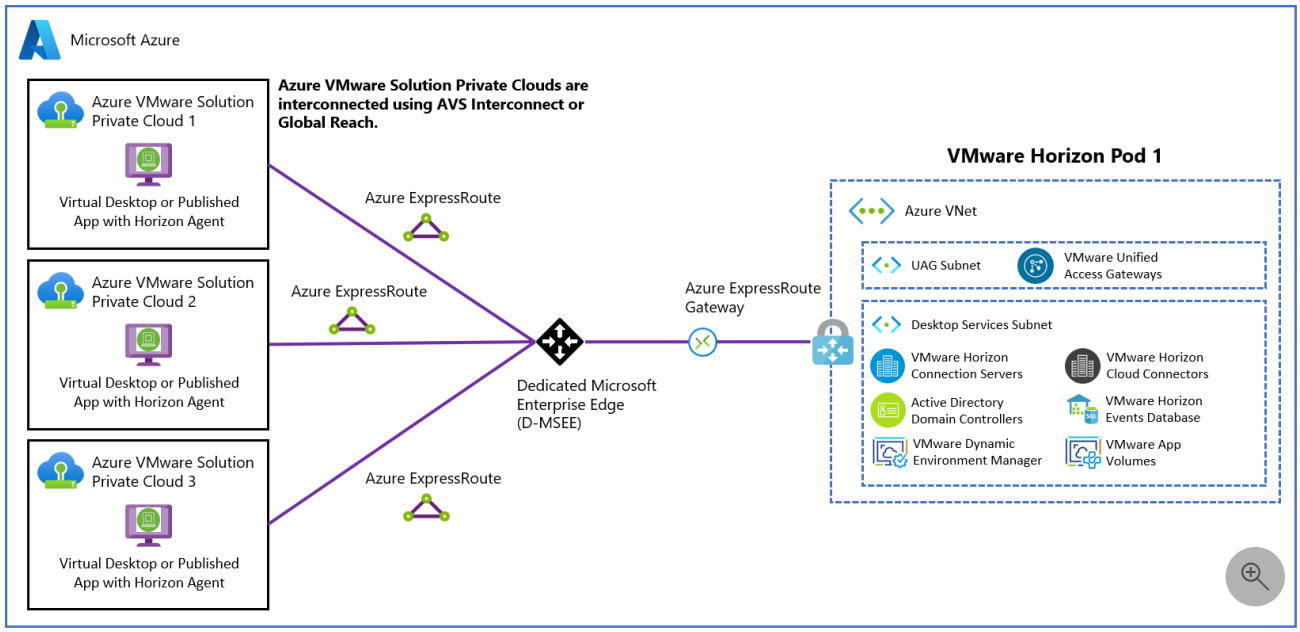
The connection from Azure Virtual Network to the Azure private clouds / SDDCs should be configured with ExpressRoute Connections (FastPath enabled). The following diagram shows a basic Horizon pod deployment.



Network connectivity to scale Horizon on Azure VMware Solution

This section lays out the network architecture at a high level with some common deployment examples to help you scale Horizon on Azure VMware Solution. The focus is specifically on critical networking elements.

Single Horizon pod on Azure VMware Solution



A single Horizon pod is the most straight forward deployment scenario because you deploy just one Horizon pod in the US East region. Since each private cloud and SDDC is estimated to handle 4,000 desktop sessions, you deploy the maximum Horizon pod size. You can plan the deployment of up to three private clouds/SDDCs.

With the Horizon infrastructure virtual machines (VMs) deployed in Azure Virtual Network, you can reach the 12,000 sessions per Horizon pod. The connection between each private cloud and SDDC to the Azure Virtual Network is an ExpressRoute Connection (FastPath enabled). No east-west traffic between private clouds is needed.

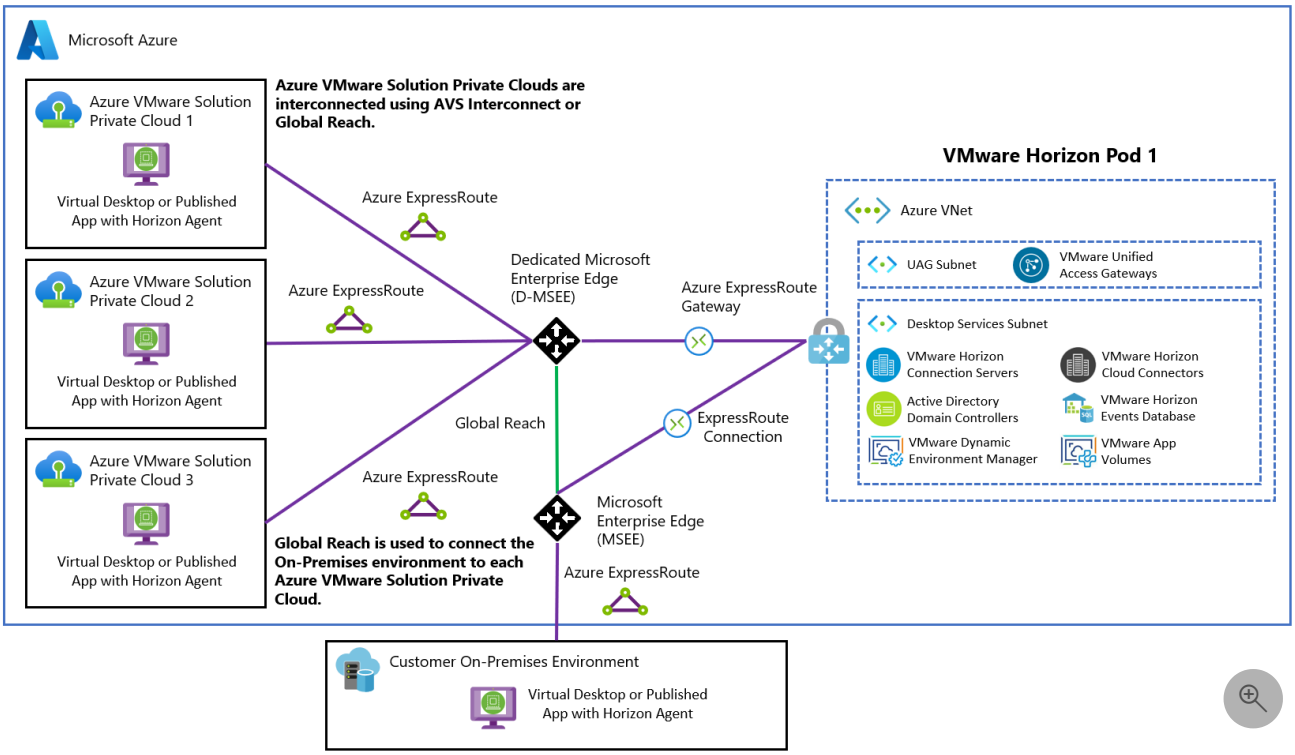
Key assumptions for this basic deployment example include that:

- You don't have an on-premises Horizon pod that you want to connect to this new pod using Cloud Pod Architecture (CPA).
- End users connect to their virtual desktops through the internet (vs. connecting via an on-premises datacenter).

You connect your AD domain controller in Azure Virtual Network with your on-premises AD through VPN or ExpressRoute circuit.

A variation on the basic example might be to support connectivity for on-premises resources. For example, users access desktops and generate virtual desktop application traffic or connect to an on-premises Horizon pod using CPA.

The diagram shows how to support connectivity for on-premises resources. To connect to your corporate network to the Azure Virtual Network, you need an ExpressRoute circuit. You need to connect your corporate network with each of the private cloud and SDDCs using ExpressRoute Global Reach. It allows the connectivity from the SDDC to the ExpressRoute circuit and on-premises resources.

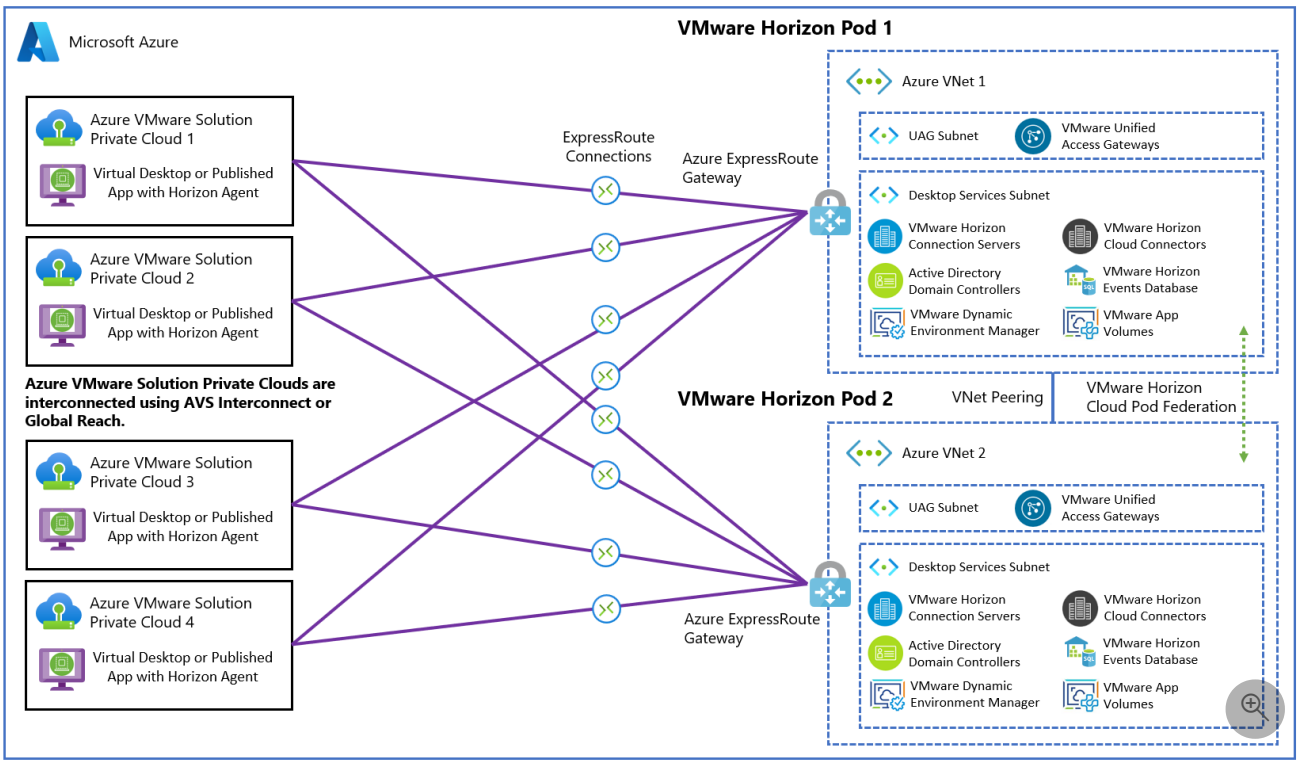


Multiple Horizon pods on Azure VMware Solution across multiple regions

Another scenario is scaling Horizon across multiple pods. In this scenario, you deploy two Horizon pods in two different regions and federate them using CPA. It's similar to the network configuration in the previous example, but with more cross-regional links.

Connect the Azure Virtual Network in each region to the private clouds/SDDCs in the other region. It allows Horizon connection servers part of the CPA federation to connect to all desktops under management. Adding extra private clouds/SDDCs to this configuration would allow you to scale to 24,000 sessions overall.

The same principles apply if you deploy two Horizon pods in the same region. Make sure to deploy the second Horizon pod in a *separate Azure Virtual Network*. Just like the single pod example, you can connect your corporate network and on-premises pod to this multi-pod/region example using ExpressRoute and Global Reach.



Size Azure VMware Solution hosts for Horizon deployments

Horizon's sizing methodology on a host running in Azure VMware Solution is simpler than Horizon on-premises. It's simpler because the Azure VMware Solution host is standardized. Exact host sizing helps determine the number of hosts needed to support your VDI requirements. It's central to determining the cost-per-desktop.

Sizing tables

Specific vCPU/vRAM requirements for Horizon virtual desktops depend on the customer's specific workload profile. Work with your MSFT and VMware sales team to help determine your vCPU/vRAM requirements for your virtual desktops.

Expand table

vCPU per VM	vRAM per VM (GB)	Instance	100 VMs	200 VMs	300 VMs	400 VMs	500 VMs	600 VMs	700 VMs	800 VMs	900 VMs	1000 VMs	2000 VMs	3000 VMs	4000 VMs	5000 VMs	6000 VMs	6400 VMs
2	3.5	AVS	3	3	4	4	5	6	6	7	8	9	17	25	33	41	49	53
2	4	AVS	3	3	4	5	6	6	7	8	9	9	18	26	34	42	51	54
2	6	AVS	3	4	5	6	7	9	10	11	12	13	26	38	51	62	75	79
2	8	AVS	3	5	6	8	9	11	12	14	16	18	34	51	67	84	100	106
2	12	AVS	4	6	9	11	13	16	19	21	23	26	51	75	100	124	149	158
2	16	AVS	5	8	11	14	18	21	24	27	30	34	67	100	133	165	198	211
4	3.5	AVS	3	3	4	5	6	7	8	9	10	11	22	33	44	55	66	70
4	4	AVS	3	3	4	5	6	7	8	9	10	11	22	33	44	55	66	70
4	6	AVS	3	4	5	6	7	9	10	11	12	13	26	38	51	62	75	79
4	8	AVS	3	5	6	8	9	11	12	14	16	18	34	51	67	84	100	106
4	12	AVS	4	6	9	11	13	16	19	21	23	26	51	75	100	124	149	158

vCPU per VM	vRAM per VM (GB)	Instance	100 VMs	200 VMs	300 VMs	400 VMs	500 VMs	600 VMs	700 VMs	800 VMs	900 VMs	1000 VMs	2000 VMs	3000 VMs	4000 VMs	5000 VMs	6000 VMs	6400 VMs
4	16	AVS	5	8	11	14	18	21	24	27	30	34	67	100	133	165	198	211
6	3.5	AVS	3	4	5	6	7	9	10	11	13	14	27	41	54	68	81	86
6	4	AVS	3	4	5	6	7	9	10	11	13	14	27	41	54	68	81	86
6	6	AVS	3	4	5	6	7	9	10	11	13	14	27	41	54	68	81	86
6	8	AVS	3	5	6	8	9	11	12	14	16	18	34	51	67	84	100	106
6	12	AVS	4	6	9	11	13	16	19	21	23	26	51	75	100	124	149	158
6	16	AVS	5	8	11	14	18	21	24	27	30	34	67	100	133	165	198	211
8	3.5	AVS	3	4	6	7	9	10	12	14	15	17	33	49	66	82	98	105
8	4	AVS	3	4	6	7	9	10	12	14	15	17	33	49	66	82	98	105
8	6	AVS	3	4	6	7	9	10	12	14	15	17	33	49	66	82	98	105
8	8	AVS	3	5	6	8	9	11	12	14	16	18	34	51	67	84	100	106
8	12	AVS	4	6	9	11	13	16	19	21	23	26	51	75	100	124	149	158
8	16	AVS	5	8	11	14	18	21	24	27	30	34	67	100	133	165	198	211

Horizon sizing inputs

Here's what you need to gather for your planned workload:

- Number of concurrent desktops
- Required vCPU per desktop
- Required vRAM per desktop
- Required storage per desktop

In general, VDI deployments are either CPU or RAM constrained, which determines the host size. Let's take the following example for a LoginVSI Knowledge Worker type of workload, validated with performance testing:

- 2,000 concurrent desktop deployment
- 2vCPU per desktop.
- 4-GB vRAM per desktop.
- 50 GB of storage per desktop

For this example, the total number of hosts factors out to 18, yielding a VM-per-host density of 111.

> **ⓘ Important**
>
> Customer workloads will vary from this example of a LoginVSI Knowledge Worker. As a part of planning your deployment, work with your VMware EUC SEs for your specific sizing and performance needs. Be sure to run your own performance testing using the actual, planned workload before finalizing host sizing and adjust accordingly.

Horizon on Azure VMware Solution licensing

There are four components to the overall costs of running Horizon on Azure VMware Solution.

Azure VMware Solution Capacity Cost

For information on the pricing, see the Azure VMware Solution pricing page

Horizon Licensing Cost

There are two available licenses for use with the Azure VMware Solution, which can be either Concurrent User (CCU) or Named User (NU):

- Horizon Subscription License
- Horizon Universal Subscription License

If only deploying Horizon on Azure VMware Solution for the foreseeable future, then use the Horizon Subscription License as it is a lower cost.

If deployed on Azure VMware Solution and on-premises, choose the Horizon Universal Subscription License as a disaster recovery use case. However, it includes a vSphere license for on-premises deployment, so it has a higher cost.

Work with your VMware EUC sales team to determine the Horizon licensing cost based on your needs.

Azure Instance Types

To understand the Azure virtual machine sizes that are required for the Horizon Infrastructure, see Horizon Installation on Azure VMware Solution.

References

System Requirements For Horizon Agent for Linux

Next steps

To learn more about VMware Horizon on Azure VMware Solution, read the VMware Horizon FAQ.

Deploy Citrix on Azure VMware Solution

Article • 12/08/2023

Citrix Virtual Apps and Desktop service supports Azure VMware Solution. Azure VMware Solution provides cloud infrastructure containing vSphere clusters created by Azure infrastructure. You can apply the Citrix Virtual Apps and Desktop Service to use Azure VMware Solution for provisioning your Virtual Delivery Agent (VDA) workload in the same way you'd use vSphere in on-premises environments.

Learn more about Citrix virtual apps and desktops

Deployment guide

Solution brief

FAQ (review Q&As)

- Q. Can I migrate my existing Citrix desktops and apps to Azure VMware Solution, or operate a hybrid environment that consists of on-premises and Azure VMware Solution-based Citrix workloads?

  A. Yes. You can use the same machine images, application packages, and processes you currently use. You're able to seamlessly link on-premises and Azure VMware Solution-based environments together for a migration.

- Q. Can Citrix be deployed as a standalone environment within Azure VMware Solution?

  A. Yes. You're free to migrate, operate a hybrid environment, or deploy a standalone directly into Azure VMware Solution.

- Q. Does Azure VMware Solution support both PVS and MCS?

  A. Yes.

- Q. Are GPU-based workloads supported in Citrix on Azure VMware Solution?

  A. Not at this time. However, Citrix workloads on Microsoft Azure support GPU if that use case is important to you.

- Q. Is Azure VMware Solution supported with on-premises Citrix deployments or LTSR?

  A. No. Azure VMware Solution is only supported with the Citrix Virtual Apps and Desktops service offerings.

- Q. Who do I call for support?

  A. Customers should contact Citrix support www.citrix.com/support for assistance.

- Q. Can I use my Azure Virtual Desktop benefit from Microsoft with Citrix on Azure VMware Solution?

  A. No. Azure Virtual Desktop benefits are applicable to native Microsoft Azure workloads only. Citrix Virtual Apps and Desktops service, as a native Azure offering, can apply your Azure Virtual Desktop benefit alongside your Azure VMware Solution deployment.

- Q. How do I purchase Citrix Virtual Apps and Desktops service to use Azure VMware Solution?

  A. You can purchase Citrix offerings via your Citrix partner or directly from the Azure Marketplace.

Configure storage policy

Article • 12/06/2023

VMware vSAN storage policies define storage requirements for your virtual machines (VMs). These policies guarantee the required level of service for your VMs because they determine how storage is allocated to the VM. Each VM deployed to a vSAN datastore is assigned at least one VM storage policy.

You can assign a VM storage policy in an initial deployment of a VM or when you do other VM operations, such as cloning or migrating. Post-deployment cloudadmin users or equivalent roles can't change the default storage policy for a VM. However, **VM storage policy** per disk changes is permitted.

The Run command lets authorized users change the default or existing VM storage policy to an available policy for a VM post-deployment. There are no changes made on the disk-level VM storage policy. You can always change the disk level VM storage policy as per your requirements.

> **Note**
>
> Run commands are executed one at a time in the order submitted.

In this article learn how to:

- ✓ List all storage policies
- ✓ Set the storage policy for a VM
- ✓ Specify default storage policy for a cluster
- ✓ Create storage policy
- ✓ Remove storage policy

Prerequisites

Make sure that the minimum level of hosts are met.

Expand table

RAID configuration	Failures to tolerate (FTT)	Minimum hosts required
RAID-1 (Mirroring) Default setting.	1	3

RAID configuration	Failures to tolerate (FTT)	Minimum hosts required
RAID-5 (Erasure Coding)	1	4
RAID-1 (Mirroring)	2	5
RAID-6 (Erasure Coding)	2	6
RAID-1 (Mirroring)	3	7

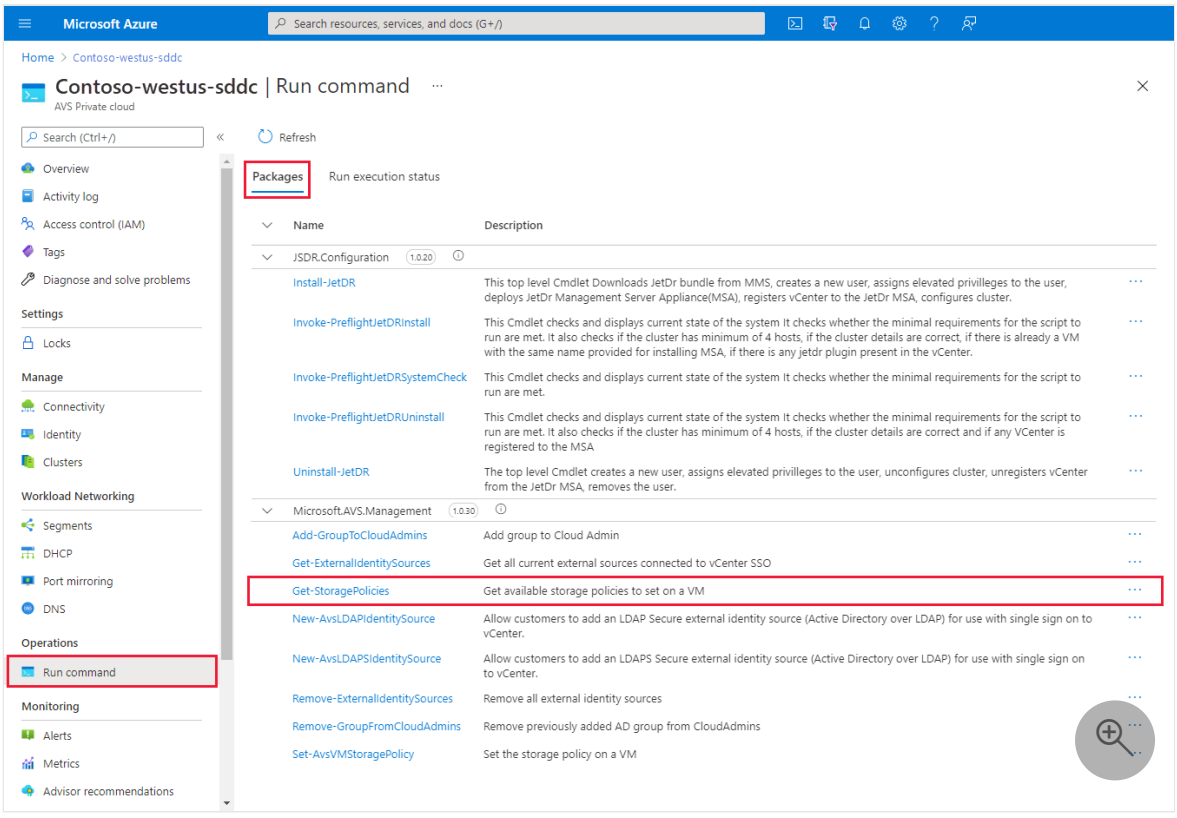
List storage policies

Run the `Get-StoragePolicy` cmdlet to list the vSAN based storage policies available to set on a VM.

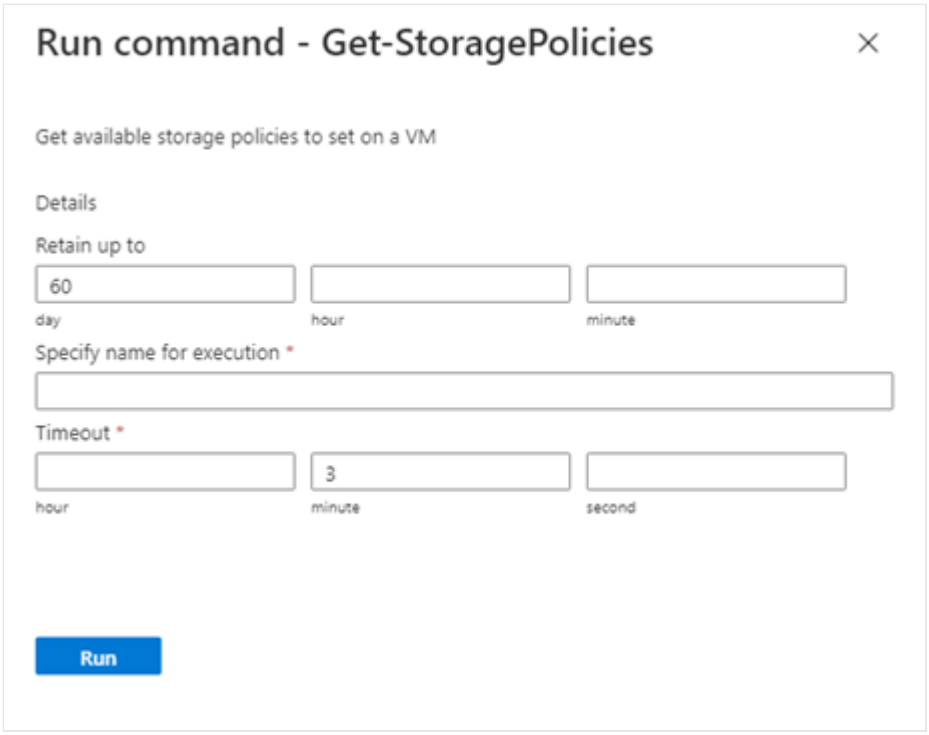
1. Sign in to the Azure portal.

> **Note**
>
> If you need access to the Azure US Gov portal, go to **https://portal.azure.us/**

2. Select **Run command** > **Packages** > **Get-StoragePolicies**.



3. Provide the required values or change the default values, and then select **Run**.



Expand table

Field	Value
Retain up to	Retention period of the cmdlet output. The default value is 60.
Specify name for execution	Alphanumeric name, for example, **Get-StoragePolicies-Exec1**.
Timeout	The period after which a cmdlet exits if taking too long to finish.

4. Check **Notifications** to see the progress.

Set storage policy on VM

Run the `Set-VMStoragePolicy` cmdlet to modify vSAN-based storage policies on a default cluster, individual VM, or group of VMs sharing a similar VM name. For example, if you have three VMs named "MyVM1", "MyVM2", and "MyVM3", supplying "MyVM*" to the VMName parameter would change the StoragePolicy on all three VMs.

> **Note**
>
> You cannot use the vSphere Client to change the default storage policy or any existing storage policies for a VM.

1. Select **Run command** > **Packages** > **Set-VMStoragePolicy**.
2. Provide the required values or change the default values, and then select **Run**.

Expand table

Field	Value
VMName	Name of the target VM.
StoragePolicyName	Name of the storage policy to set. For example, **RAID-FTT-1**.
Retain up to	Retention period of the cmdlet output. The default value is 60.
Specify name for execution	Alphanumeric name, for example, **changeVMStoragePolicy**.
Timeout	The period after which a cmdlet exits if taking too long to finish.

3. Check **Notifications** to see the progress.

Set storage policy on all VMs in a location

Run the `Set-LocationStoragePolicy` cmdlet to Modify vSAN based storage policies on all VMs in a location where a location is the name of a cluster, resource pool, or folder. For example, if you have 3 VMs in Cluster-3, supplying "Cluster-3" would change the storage policy on all three VMs.

> **Note**
>
> You cannot use the vSphere Client to change the default storage policy or any existing storage policies for a VM.

1. Select **Run command** > **Packages** > **Set-LocationStoragePolicy**.
2. Provide the required values or change the default values, and then select **Run**.

Expand table

Field	Value
Location	Name of the target VM.

Field	Value
StoragePolicyName	Name of the storage policy to set. For example, **RAID-FTT-1**.
Retain up to	Retention period of the cmdlet output. The default value is 60.
Specify name for execution	Alphanumeric name, for example, **changeVMStoragePolicy**.
Timeout	The period after which a cmdlet exits if taking too long to finish.

3. Check **Notifications** to see the progress.

Specify storage policy for a cluster

Run the `Set-ClusterDefaultStoragePolicy` cmdlet to specify default storage policy for a cluster,

1. Select **Run command** > **Packages** > **Set-ClusterDefaultStoragePolicy**.
2. Provide the required values or change the default values, and then select **Run**.

Expand table

Field	Value
ClusterName	Name of the cluster.
StoragePolicyName	Name of the storage policy to set. For example, **RAID-FTT-1**.
Retain up to	Retention period of the cmdlet output. The default value is 60.
Specify name for execution	Alphanumeric name, for example, **Set-ClusterDefaultStoragePolicy-Exec1**.
Timeout	The period after which a cmdlet exits if taking too long to finish.

3. Check **Notifications** to see the progress.

Create custom AVS storage policy

Run the `New-AVSStoragePolicy` cmdlet to create or overwrite an existing policy. This function creates a new or overwrites an existing vSphere Storage Policy. Non vSAN-

Based, vSAN Only, VMEncryption Only, Tag Only based and/or any combination of these policy types are supported.

> **Note**
>
> You cannot modify existing AVS default storage policies. Certain options enabled in storage policies will produce warnings to associated risks.

1. Select **Run command** > **Packages** > **New-AVSStoragePolicy**.
2. Provide the required values or change the default values, and then select **Run**.

Expand table

Field	Value
Overwrite	Overwrite existing Storage Policy. - Default is $false. - Passing overwrite true provided overwrites an existing policy exactly as defined. - Those values not passed are removed or set to default values.
NotTags	Match to datastores that do NOT have these tags. - Tags are case sensitive. - Comma separate multiple tags. - Example: Tag1,Tag 2,Tag_3
Tags	Match to datastores that do have these tags. - Tags are case sensitive. - Comma separate multiple tags. - Example: Tag1,Tag 2,Tag_3
vSANForceProvisioning	Force provisioning for the policy. - Default is $false. - Valid values are $true or $false - **WARNING** - vSAN Force Provisioned Objects aren't covered under Microsoft SLA. Data LOSS and vSAN instability can occur. - Recommended value is $false.
vSANChecksumDisabled	Enable or disable checksum for the policy. - Default is $false. - Valid values are $true or $false. - **WARNING** - Disabling checksum can lead to data LOSS and/or corruption. - Recommended value is $false.

Field	Value
vSANCacheReservation	Percentage of cache reservation for the policy. - Default is 0. - Valid values are 0..100.
vSANIOLimit	Sets limit on allowed IO. - Default is unset. - Valid values are 0..2147483647. - IOPS limit for the policy.
vSANDiskStripesPerObject	The number of HDDs across which each replica of a storage object is striped. - Default is 1. Valid values are 1..12. - A value higher than 1 may result in better performance (for example, when flash read cache misses need to get serviced from HDD), but also results in higher use of system resources.
vSANObjectSpaceReservation	Object Reservation. - Default is 0. - Valid values are 0..100. - 0=Thin Provision - 100=Thick Provision
VMEncryption	Sets VM Encryption. - Default is None. - Valid values are None, Pre-IO, Post-IO. - Pre-IO allows VAIO filtering solutions to capture data prior to VM encryption. - Post-IO allows VAIO filtering solutions to capture data after VM encryption.
vSANFailuresToTolerate	Number of vSAN Hosts failures to Tolerate. - Default is "R1FTT1". - Valid values are "None", "R1FTT1", "R1FTT2", "R1FTT3", "R5FTT1", "R6FTT2", "R1FTT3" - None = No Data Redundancy - R1FTT1 = 1 failure - RAID-1 (Mirroring) - R1FTT2 = 2 failures - RAID-1 (Mirroring) - R1FTT3 = 3 failures - RAID-1 (Mirroring) - R5FTT1 = 1 failure - RAID-5 (Erasure Coding), - R6FTT2 = 2 failures - RAID-6 (Erasure Coding) - No Data Redundancy options aren't covered under Microsoft SLA.
vSANSiteDisasterTolerance	Only valid for stretch clusters. - Default is "None". - Valid Values are "None", "Dual", "Preferred", "Secondary", "NoneStretch"

Field	Value
	- None = No Site Redundancy (Recommended Option for Non-Stretch Clusters, NOT recommended for Stretch Clusters) - Dual = Dual Site Redundancy (Recommended Option for Stretch Clusters) - Preferred = No site redundancy - keep data on Preferred (stretched cluster) - Secondary = No site redundancy - Keep data on Secondary Site (stretched cluster) - NoneStretch = No site redundancy - Not Recommended (https://kb.vmware.com/s/article/88358)
Description	Description of Storage Policy you're creating, free form text.
Name	Name of the storage policy to set. For example, **RAID-FTT-1**.
Retain up to	Retention period of the cmdlet output. The default value is 60.
Specify name for execution	Alphanumeric name, for example, **New-AVSStoragePolicy-Exec1**.
Timeout	The period after which a cmdlet exits if taking too long to finish.

3. Check **Notifications** to see the progress.

Remove AVS Storage Policy

Run the `Remove-AVSStoragePolicy` cmdlet to specify default storage policy for a cluster,

1. Select **Run command** > **Packages** > **Remove-AVSStoragePolicy**.
2. Provide the required values or change the default values, and then select **Run**.

Expand table

Field	Value
Name	Name of Storage Policy. Wildcards aren't supported and will be stripped.
Retain up to	Retention period of the cmdlet output. The default value is 60.

Field	Value
Specify name for execution	Alphanumeric name, for example, **Remove-AVSStoragePolicy-Exec1**.
Timeout	The period after which a cmdlet exits if taking too long to finish.

3. Check **Notifications** to see the progress.

Next steps

Now that you learned how to configure VMware vSAN storage policies, learn more about:

- How to attach disk pools to Azure VMware Solution hosts (Preview) - You can use disks as the persistent storage for Azure VMware Solution for optimal cost and performance.
- How to configure external identity for vCenter Server - vCenter Server has a built-in local user called cloudadmin and assigned to the CloudAdmin role. The local cloudadmin user is used to set up users in Active Directory (AD). With the Run command feature, you can configure Active Directory over LDAP or LDAPS for vCenter as an external identity source.

Configure VMware vSAN

Article • 12/08/2023

VMware vSAN has more capabilities that are set with every Azure VMware Solution deployment. Each cluster has their own VMware vSAN Datastore. Azure VMware Solution defaults with the following configurations per cluster:

Expand table

Field	Value
TRIM/UNMAP	Disabled
Space Efficiency	Deduplication and Compression

> **Note**
>
> Run commands are executed one at a time in the order submitted.

In this article, learn how to:

- ✓ Enable or Disable vSAN TRIM/UNMAP
- ✓ Enable vSAN Compression Only
- ✓ Disable vSAN Deduplication and Compression

Set VMware vSAN TRIM/UNMAP

Run the `Set-AVSVSANClusterUNMAPTRIM` cmdlet to enable or disable TRIM/UNMAP.

1. Sign in to the Azure portal.

   > **Note**
   >
   > Enabling TRIM/UNMAP on your vSAN Datastore may have a negative performance impact. **https://core.vmware.com/resource/vsan-space-efficiency-technologies#sec19560-sub6**

2. Select **Run command** > **Packages** > **Set-AVSVSANClusterUNMAPTRIM**.

3. Provide the required values or change the default values, and then select **Run**.

Expand table

Field	Value
Name	Cluster name as defined in vCenter Server. Comma delimit to target only certain clusters. (Blank targets all clusters)
Enable	True or False.
Retain up to	Retention period of the cmdlet output. The default value is 60.
Specify name for execution	Alphanumeric name, for example, **Disable vSAN TRIMUNMAP**.
Timeout	The period after which a cmdlet exits if taking too long to finish.

4. Check **Notifications** to see the progress.

> **Note**
>
> After vSAN TRIM/UNMAP is Enabled, the following lists additional requirements for it to function as intended. Once enabled, there are several prerequisites that must be met for TRIM/UNMAP to successfully reclaim no longer used capacity.
>
> - Prerequisites - VM Level
> - A minimum of virtual machine hardware version 11 for Windows
> - A minimum of virtual machine hardware version 13 for Linux.
> - disk.scsiUnmapAllowed flag is not set to false. The default is implied true. This setting can be used as a "stop switch" at the virtual machine level should you wish to disable this behavior on a per VM basis and do not want to use in guest configuration to disable this behavior. VMX file changes require a reboot to take effect.
> - The guest operating system must be able to identify the virtual disk as thin.
> - After enabling at a cluster level, the VM must be powered off and back on (a reboot is insufficient).
> - Additional guidance can be found here: **https://core.vmware.com/resource/vsan-space-efficiency-technologies#sec19560-sub6**

Set VMware vSAN Space Efficiency

Run the `Set-vSANCompressDedupe` cmdlet to set preferred space efficiency model.

> **Note**
>
> Changing this setting will cause a vSAN resync and performance degradation while disks are reformatted. Assure enough space is available when changing to new configuration. 25% free space or greater is recommended in general.

1. Sign in to the Azure portal.
2. Select **Run command** > **Packages** > **Set-vSANCompressDedupe**.
3. Provide the required values or change the default values, and then select **Run**.

Expand table

Field	Value
Compression	True or False.
Deduplication	True or False. (Enabling deduplication, enables both dedupe and compression)
ClustersToChange	Cluster name as defined in vCenter Server. Comma delimit to target multiple clusters.
Retain up to	Retention period of the cmdlet output. The default value is 60.
Specify name for execution	Alphanumeric name, for example, **set cluster-1 to compress only**.
Timeout	The period after which a cmdlet exits if taking too long to finish.

> **Note**
>
> Setting Compression to False and Deduplication to True sets vSAN to Dedupe and Compression. Setting Compression to False and Dedupe to False, disables all space efficiency. Azure VMware Solution default is Dedupe and Compression Compression only provides slightly better performance Disabling both compression and deduplication offers the greatest performance gains, however at the cost of space utilization.

4. Check **Notifications** to see the progress.

Next steps

Now that you learned how to configure VMware vSAN, learn more about:

- How to configure storage policies - Create and configure storage policies for your Azure VMware Solution virtual machines.
- How to configure external identity for vCenter Server - vCenter Server has a built-in local user called cloudadmin and assigned to the CloudAdmin role. The local cloudadmin user is used to set up users in Active Directory (AD). With the Run command feature, you can configure Active Directory over LDAP or LDAPS for vCenter Server as an external identity source.

Configure customer-managed key encryption at rest in Azure VMware Solution

Article • 04/12/2024

This article illustrates how to encrypt VMware vSAN key encryption keys (KEKs) with customer-managed keys (CMKs) managed by a customer-owned Azure Key Vault instance.

When CMK encryptions are enabled on your Azure VMware Solution private cloud, Azure VMware Solution uses the CMK from your key vault to encrypt the vSAN KEKs. Each ESXi host that participates in the vSAN cluster uses randomly generated disk encryption keys (DEKs) that ESXi uses to encrypt disk data at rest. vSAN encrypts all DEKs with a KEK provided by the Azure VMware Solution key management system. The Azure VMware Solution private cloud and the key vault don't need to be in the same subscription.

When you manage your own encryption keys, you can:

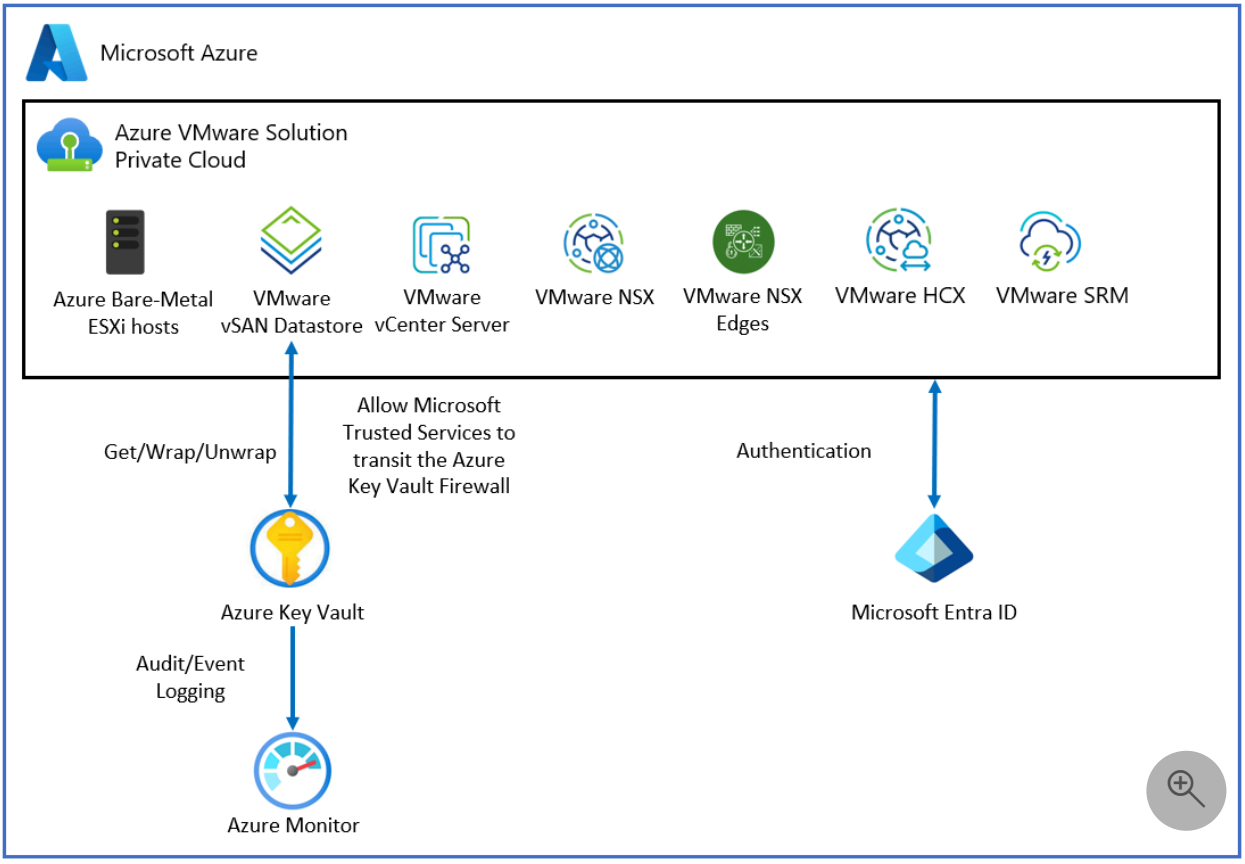
- Control Azure access to vSAN keys.
- Centrally manage the lifecycle of CMKs.
- Revoke Azure access to the KEK.

The CMKs feature supports the following key types and their key sizes:

- **RSA**: 2048, 3072, 4096
- **RSA-HSM**: 2048, 3072, 4096

Topology

The following diagram shows how Azure VMware Solution uses Microsoft Entra ID and a key vault to deliver the CMK.



Prerequisites

Before you begin to enable CMK functionality, ensure that the following requirements are met:

- You need a key vault to use CMK functionality. If you don't have a key vault, you can create one by using Quickstart: Create a key vault using the Azure portal.
- If you enabled restricted access to Key Vault, you need to allow Microsoft Trusted Services to bypass the Key Vault firewall. Go to Configure Azure Key Vault networking settings to learn more.

> **Note**
>
> After firewall rules are in effect, users can only perform Key Vault data plane operations when their requests originate from allowed VMs or IPv4 address ranges. This restriction also applies to accessing Key Vault from the Azure portal. It also affects the Key Vault Picker by Azure VMware Solution. Users might be able to see a list of key vaults, but not list keys, if firewall rules prevent their client machine or the user doesn't have list permission in Key Vault.

- Enable System Assigned identity on your Azure VMware Solution private cloud if you didn't enable it during software-defined datacenter (SDDC) provisioning.

  Portal

  To enable System Assigned identity:

  1. Sign in to the Azure portal.
  2. Go to **Azure VMware Solution** and locate your private cloud.
  3. On the leftmost pane, open **Manage** and select **Identity**.
  4. In **System Assigned**, select **Enable** > **Save**. **System Assigned identity** should now be enabled.

  After System Assigned identity is enabled, you see the tab for **Object ID**. Make a note of the Object ID for use later.

- Configure the key vault access policy to grant permissions to the managed identity. You use it to authorize access to the key vault.

  Portal

  1. Sign in to the Azure portal.
  2. Go to **Key vaults** and locate the key vault you want to use.
  3. On the leftmost pane, under **Settings**, select **Access policies**.
  4. In **Access policies**, select **Add Access Policy** and then:
     a. In the **Key Permissions** dropdown, choose **Select**, **Get**, **Wrap Key**, and **Unwrap Key**.
     b. Under **Select principal**, select **None selected**. A new **Principal** window with a search box opens.
     c. In the search box, paste the **Object ID** from the previous step. Or search for the private cloud name you want to use. Choose **Select** when you're finished.
     d. Select **ADD**.
     e. Verify that the new policy appears under the current policy's Application section.
     f. Select **Save** to commit changes.

Customer-managed key version lifecycle

You can change the CMK by creating a new version of the key. The creation of a new version doesn't interrupt the virtual machine (VM) workflow.

In Azure VMware Solution, CMK key version rotation depends on the key selection setting that you chose during CMK setup.

Key selection setting 1

A customer enables CMK encryption without supplying a specific key version for CMK. Azure VMware Solution selects the latest key version for CMK from the customer's key vault to encrypt the vSAN KEKs. Azure VMware Solution tracks the CMK for version rotation. When a new version of the CMK key in Key Vault is created, it gets captured by Azure VMware Solution automatically to encrypt vSAN KEKs.

> **Note**
>
> Azure VMware Solution can take up to 10 minutes to detect a new autorotated key version.

Key selection setting 2

A customer can enable CMK encryption for a specified CMK key version to supply the full key version URI under the **Enter Key from URI** option. When the customer's current key expires, they need to extend the CMK key expiration or disable CMK.

Enable CMK with system-assigned identity

System-assigned identity is restricted to one per resource and is tied to the lifecycle of the resource. You can grant permissions to the managed identity on Azure resource. The managed identity is authenticated with Microsoft Entra ID, so you don't have to store any credentials in code.

> **Important**
>
> Ensure that Key Vault is in the same region as the Azure VMware Solution private cloud.

Portal

Go to your Key Vault instance and provide access to the SDDC on Key Vault by using the principal ID captured on the **Enable MSI** tab.

1. From your Azure VMware Solution private cloud, under **Manage**, select **Encryption**. Then select **Customer-managed keys (CMKs)**.

2. CMK provides two options for **Key Selection** from Key Vault:

   Option 1:
   a. Under **Encryption key**, choose **select from Key Vault**.
   b. Select the encryption type. Then select the **Select Key Vault and key** option.
   c. Select the **Key Vault and key** from the dropdown. Then choose **Select**.

   Option 2:
   a. Under **Encryption key**, select **Enter key from URI**.
   b. Enter a specific Key URI in the **Key URI** box.

   > **Important**
   >
   > If you want to select a specific key version instead of the automatically selected latest version, you need to specify the Key URI with the key version. This choice affects the CMK key version lifecycle.

   The Key Vault Managed Hardware Security Module (HSM) option is only supported with the Key URI option.

3. Select **Save** to grant access to the resource.

Change from a customer-managed key to a Microsoft managed key

When a customer wants to change from a CMK to a Microsoft-managed key (MMK), the VM workload isn't interrupted. To make the change from a CMK to an MMK:

1. Under **Manage**, select **Encryption** from your Azure VMware Solution private cloud.
2. Select **Microsoft-managed keys (MMK)**.
3. Select **Save**.

Limitations

Key Vault must be configured as recoverable. You need to:

- Configure Key Vault with the **Soft Delete** option.
- Turn on **Purge Protection** to guard against force deletion of the secret vault, even after soft delete.

Updating CMK settings don't work if the key is expired or the Azure VMware Solution access key was revoked.

Troubleshooting and best practices

Here are troubleshooting tips for some common issues you might encounter and also best practices to follow.

Accidental deletion of a key

If you accidentally delete your key in the key vault, the private cloud can't perform some cluster modification operations. To avoid this scenario, we recommend that you keep soft deletes enabled in the key vault. This option ensures that if a key is deleted, it can be recovered within a 90-day period as part of the default soft-delete retention. If you're within the 90-day period, you can restore the key to resolve the issue.

Restore key vault permission

If you have a private cloud that has lost access to the CMK, check if Managed System Identity (MSI) requires permissions in the key vault. The error notification returned from Azure might not correctly indicate MSI requiring permissions in the key vault as the root cause. Remember, the required permissions are `get`, `wrapKey`, and `unwrapKey`. See step 4 in Prerequisites.

Fix an expired key

If you aren't using the autorotate function and the CMK expired in Key Vault, you can change the expiration date on the key.

Restore key vault access

Ensure that the MSI is used for providing private cloud access to the key vault.

Deletion of MSI

If you accidentally delete the MSI associated with a private cloud, you need to disable the CMK. Then follow the steps to enable the CMK from the start.

Next steps

- Learn about Azure Key Vault backup and restore.
- Learn about Azure Key Vault recovery.

Use Azure VMware Solution with Azure Elastic SAN

Article • 10/17/2024

This article explains how to use Azure Elastic SAN as backing storage for Azure VMware Solution. Azure VMware Solution supports attaching iSCSI datastores as a persistent storage option. You can create Virtual Machine File System (VMFS) datastores with Azure Elastic SAN volumes and attach them to clusters of your choice. By using VMFS datastores backed by Azure Elastic SAN, you can expand your storage instead of scaling the clusters.

Azure Elastic storage area network (SAN) addresses the problem of workload optimization and integration between your large scale databases and performance-intensive mission-critical applications. For more information on Azure Elastic SAN, see What is Azure Elastic SAN?.

Prerequisites

The following prerequisites are required to continue.

- Verify you have a private cloud in a region that Elastic SAN is available in.
- Know the availability zone your private cloud is in.
  - In the UI, select an Azure VMware Solution host.

    > **Note**
    >
    > The host exposes its Availability Zone. You should use that AZ when deploying other Azure resources for the same subscription.

- You have permission to set up new resources in the subscription your private cloud is in.
- Register the following feature flags for your subscription:
  - iSCSIMultipath
  - ElasticSanDatastore
- Reserve a dedicated address block for your external storage.

Supported host types

To use Elastic SAN with Azure VMware Solution, you can use any of these three host types:

- AV36
- AV36P
- AV52

Using AV64 with Elastic SAN is not currently supported.

Set up Elastic SAN

In this section, you create a virtual network for your Elastic SAN. Then you create the Elastic SAN that includes creating at least one volume group and one volume that becomes your VMFS datastore. Next, you set up private endpoints for your Elastic SAN that allows your private cloud to connect to the Elastic SAN volume. Then you're ready to add an Elastic SAN volume as a datastore in your private cloud.

1. Use one of the following instruction options to set up a dedicated virtual network for your Elastic SAN:

   - Azure portal
   - Azure PowerShell module
   - Azure CLI

2. Use one of the following instruction options to set up an Elastic SAN, your dedicated volume group, and initial volume in that group:

   > **ⓘ Important**
   >
   > Create your Elastic SAN in the same region and availability zone as your private cloud for best performance.

   - Azure portal
   - PowerShell
   - Azure CLI

3. Use one of the following instructions to configure a Private Endpoint (PE) for your Elastic SAN:

> **Important**
>
> You must have a Private Endpoint set up for your dedicated volume group to be able to connect your SDDC to the Elastic SAN.

- Azure Portal
- PowerShell
- Azure CLI

Configuration recommendations

You should use multiple private endpoints to establish multiple sessions between an Elastic SAN and each volume group you intend to connect to your SDDC. Because of how Elastic SAN handles sessions, having multiple sessions comes with two benefits: increased performance thanks to parallelization, and increased reliability to handle single session disconnects due to unexpected factors like network glitches. When you establish multiple sessions, it mitigates the impact of session disconnects, as long as the connection re-established within a few seconds, your other sessions help load-balance traffic.

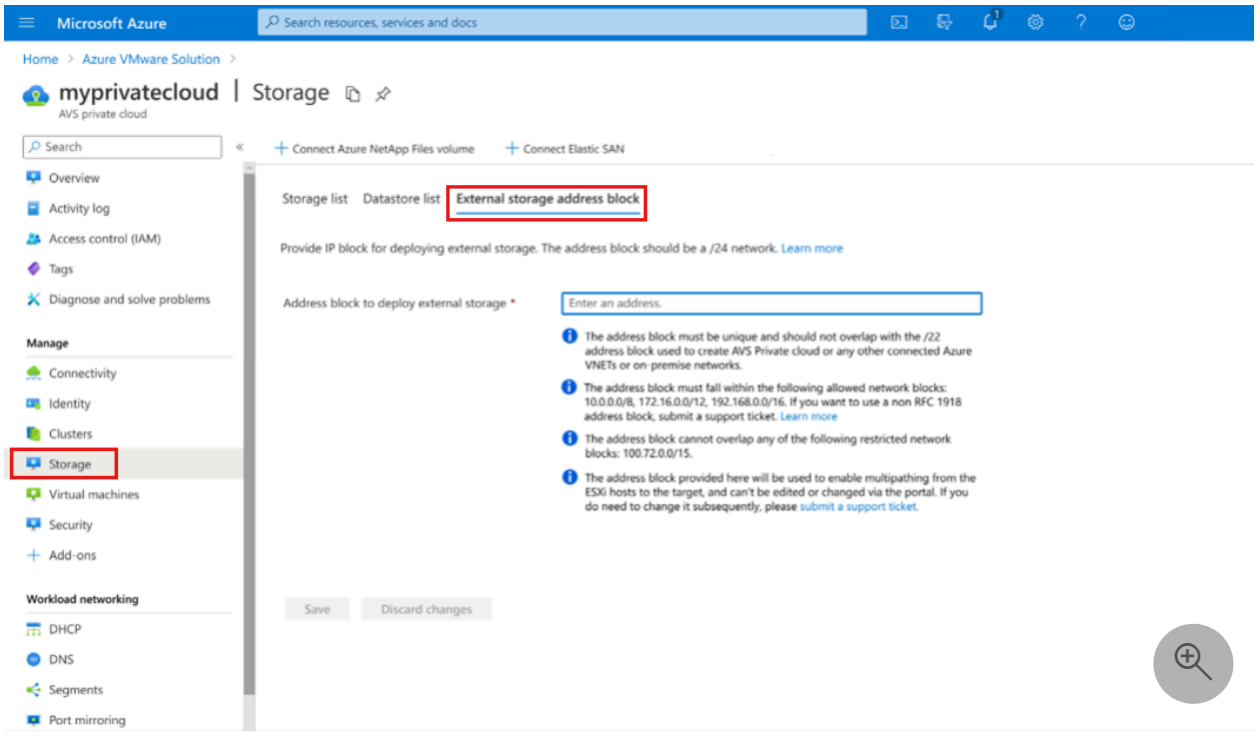
> **Note**
>
> Session disconnects may still show up as "All Paths Down" or "APD" events, which can be seen in the Events section of the ESXi Host at vCenter. You can also see them in the logs: it will show the identifier of a device or filesystem, and state it has entered the All Paths Down state.

Each private endpoint provides two sessions to Elastic SAN per host. The recommended number of sessions to Elastic SAN per host is 8, but because the maximum number of sessions an Elastic SAN datastore can handle is 128, the ideal number for your setup depends on the number of hosts in your private cloud.

> **Important**
>
> You should configure all Private Endpoints before attaching a volume as a datastore. Adding Private Endpoints after a volume is attached as a datastore will require detaching the datastore and reconnecting it to the cluster.

Configure external storage address block

Start by providing an IP block for deploying external storage. Navigate to the **Storage** tab in your Azure VMware Solution private cloud in the Azure portal. The address block should be a /24 network.



- The address block must be unique and not overlap with the /22 used to create your Azure VMware Solution private cloud or any other connected Azure virtual networks or on-premises network.
- The address block must fall within the following allowed network blocks: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16. If you want to use a non-RFC 1918 address block, submit a support request.
- The address block can't overlap any of the following restricted network blocks: 100.72.0.0/15
- The address block provided is used to enable multipathing from the ESXi hosts to the target, it can’t be edited or changed. If you do need to change it, submit a support request.

Connect Elastic SAN

After you provide an External storage address block, you need to connect your private cloud express route with the private endpoint(s) you set up for your Elastic SAN volume group(s). To learn how to establish these connections, see Configure networking for your VMware private cloud in Azure.

> **Note**
>
> Connection to Elastic SAN from Azure VMWare Solution happens via private endpoints to provide the highest network security. Since your private cloud connects to Elastic SAN in Azure through an ExpressRoute virtual network gateway, you may experience intermittent connectivity issues during gateway maintenance. These connectivity issues aren't expected to impact the availability of the datastore backed by Elastic SAN as the connection will be re-established within seconds. The potential impact from gateway maintenance is covered under the Service Level Agreement for ExpressRoute virtual network gateways and private endpoints.

Add an Elastic SAN volume as a datastore

Once your SDDC express route is connected with the private endpoint for your Elastic SAN volume group, use the following steps to connect the volume to your SDDC:

1. From the left navigation in your Azure VMware Solution private cloud, select **Storage**, then **+ Connect Elastic SAN**.
2. Select your **Subscription**, **Resource**, **Volume Group**, **Volume(s)**, and **Client cluster**.
3. From section, "Rename datastore as per VMware requirements", under **Volume name** > **Data store name**, give names to the Elastic SAN volumes.

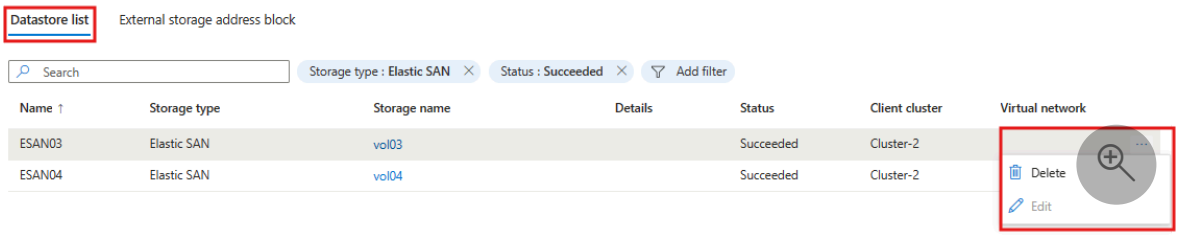
   > **Note**
   >
   > For best performance, verify that your Elastic SAN volume and private cloud are in the same Region and Availability Zone.

Disconnect and delete an Elastic SAN-based datastore

To delete the Elastic SAN-based datastore, use the following steps from the Azure portal.

1. From the left navigation in your Azure VMware Solution private cloud, select **Storage**, then **Datastore list**.

2. On the far right is an **ellipsis**. Select **Delete** to disconnect the datastore from the Cluster(s).



3. Optionally you can delete the volume you previously created in your Elastic SAN.

> **Note**
>
> This operation can't be completed if virtual machines or virtual disks reside on an Elastic SAN VMFS Datastore.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Attach Azure NetApp Files datastores to Azure VMware Solution hosts

Article • 10/15/2024

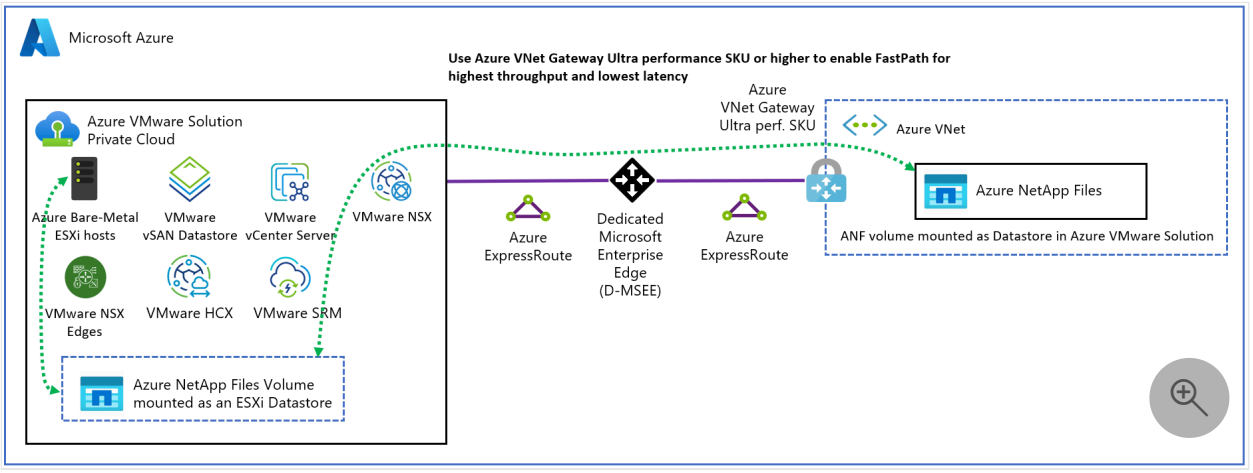
Azure NetApp Files is an enterprise-class, high-performance, metered file storage service. The service supports the most demanding enterprise file-workloads in the cloud: databases, SAP, and high-performance computing applications, with no code changes. For more information on Azure NetApp Files, see Azure NetApp Files documentation.

Azure VMware Solution supports attaching Network File System (NFS) datastores as a persistent storage option. You can create NFS datastores with Azure NetApp Files volumes and attach them to clusters of your choice. You can also create virtual machines (VMs) for optimal cost and performance.

By using NFS datastores backed by Azure NetApp Files, you can expand your storage instead of scaling the clusters. You can also use Azure NetApp Files volumes to replicate data from on-premises or primary VMware vSphere environments for the secondary site.

Create your Azure VMware Solution and create Azure NetApp Files NFS volumes in the virtual network connected to it using an ExpressRoute. Ensure there's connectivity from the private cloud to the NFS volumes created. Use those volumes to create NFS datastores and attach the datastores to clusters of your choice in a private cloud. As a native integration, you need no other permissions configured via vSphere.

The following diagram demonstrates a typical architecture of Azure NetApp Files backed NFS datastores attached to an Azure VMware Solution private cloud via ExpressRoute.



Prerequisites

Before you begin the prerequisites, review the Performance best practices section to learn about optimal performance of NFS datastores on Azure NetApp Files volumes.

1. Deploy Azure VMware Solution private cloud and a dedicated virtual network connected via ExpressRoute gateway. The virtual network gateway should be configured with the Ultra performance or ErGw3Az SKU and have FastPath enabled. For more information, see Configure networking for your VMware private cloud and Network planning checklist.
2. Create an NFSv3 volume for Azure NetApp Files in the same virtual network created in the previous step.
   a. Verify connectivity from the private cloud to Azure NetApp Files volume by pinging the attached target IP.
   b. Based on your performance requirements, select the correct service level needed for the Azure NetApp Files capacity pool. Select option **Azure VMware Solution Datastore** listed under the **Protocol** section.
   c. Create a volume with **Standard** network features if available for ExpressRoute FastPath connectivity.
   d. Under the **Protocol** section, select **Azure VMware Solution Datastore** to indicate the volume is created to use as a datastore for Azure VMware Solution private cloud.
   e. If you're using export policies to control access to Azure NetApp Files volumes, enable the Azure VMware private cloud IP range, not individual host IPs. Faulty hosts in a private cloud could get replaced. If the IP isn't enabled, connectivity to datastore is impacted.

Supported regions

Azure NetApp Files datastores for Azure VMware Solution are currently supported in the following regions:

- Australia East
- Australia Southeast
- Brazil South
- Canada Central
- Canada East
- Central India
- Central US
- East Asia
- East US
- East US 2
- France Central

- Germany West Central
- Italy North
- Japan East
- Japan West
- North Central US
- North Europe
- Qatar Central
- South Africa North
- South Central US
- Southeast Asia
- Sweden Central
- Switzerland North
- Switzerland West
- UK South
- UK West
- US Gov Arizona
- US Gov Virginia
- West Europe
- West US
- West US 2
- West US 3

Supported host types

Azure NetApp Files datastores for Azure VMware Solution are currently supported in the following host types:

- AV36
- AV36P
- AV52
- AV64

Performance best practices

There are some important best practices to follow for optimal performance of NFS datastores on Azure NetApp Files volumes.

- Create Azure NetApp Files volumes using **Standard** network features to enable optimized connectivity from Azure VMware Solution private cloud via ExpressRoute FastPath connectivity.

- For optimized performance, choose either **UltraPerformance** gateway or **ErGw3Az** gateway, and enable FastPath from a private cloud to Azure NetApp Files volumes virtual network. View more detailed information on gateway SKUs at About ExpressRoute virtual network gateways.
- Based on your performance requirements, select the correct service level needed for the Azure NetApp Files capacity pool. See Service levels for Azure NetApp Files to understand the throughput allowed per provisioned TiB for each service level.

  > **Important**
  >
  > If you've changed the Azure NetApp Files volumes performance tier after creating the volume and datastore, see **Service level change for Azure NetApp files datastore** to ensure that volume/datastore metadata is in sync to avoid unexpected behavior in the portal or the API due to metadata mismatch.

- Create one or more volumes based on the required throughput and capacity. See Performance considerations for Azure NetApp Files to understand how volume size, service level, and capacity pool QoS type determines volume throughput. For assistance calculating workload capacity and performance requirements, contact your Azure VMware Solution or Azure NetApp Files field expert. The default maximum number of Azure NetApp Files datastores is 8, but it can be increased to a maximum of 256 by submitting a support ticket. To submit a support ticket, see Create an Azure support request.
- Ensure that the Azure VMware Solution private cloud and the Azure NetApp Files volumes are deployed within the same availability zone using the the availability zone volume placement in the same subscription. Information regarding your AVS private cloud's availability zone can be viewed from the overview pane within the AVS private cloud.

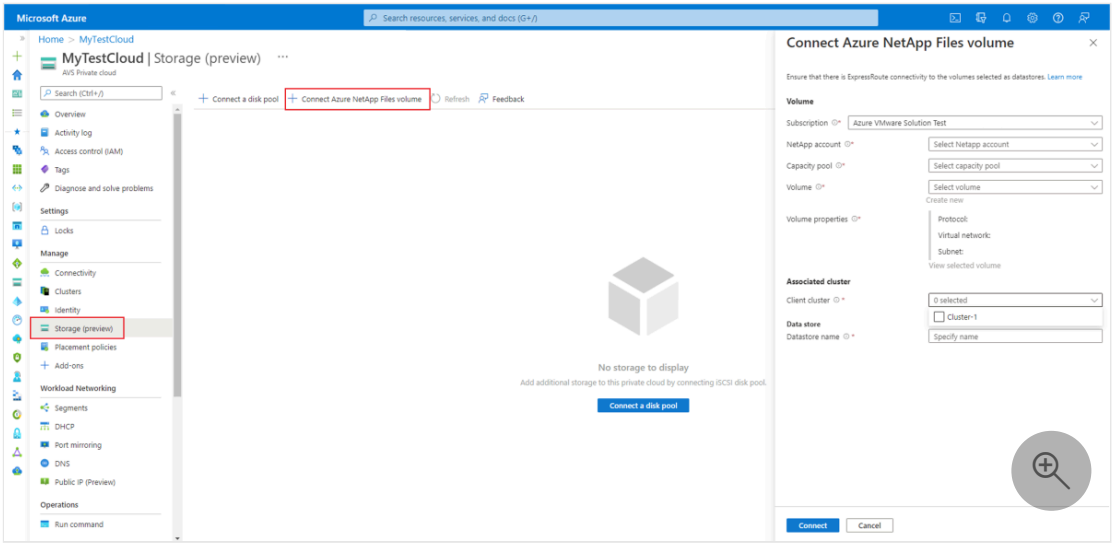
For performance benchmarks that Azure NetApp Files datastores deliver for VMs on Azure VMware Solution, see Azure NetApp Files datastore performance benchmarks for Azure VMware Solution.

Attach an Azure NetApp Files volume to your private cloud

Portal

To attach an Azure NetApp Files volume to your private cloud using Portal, follow these steps:

1. Sign in to the Azure portal.
2. Navigate to your Azure VMware Solution. Under **Manage**, select **Storage**.
3. Select **Connect Azure NetApp Files volume**.
4. In **Connect Azure NetApp Files volume**, select the **Subscription**, **NetApp account**, **Capacity pool**, and **Volume** to be attached as a datastore.



5. Verify the protocol is NFS. You need to verify the virtual network and subnet to ensure connectivity to the Azure VMware Solution private cloud.
6. Under **Associated cluster**, in the **Client cluster** field, select one or more clusters to associate the volume as a datastore.
7. Under **Data store**, create a personalized name for your **Datastore name**.
   a. When the datastore is created, you should see all of your datastores in the **Storage**.
   b. Notice that the NFS datastores are added in vCenter Server.

Protect Azure NetApp Files datastores and VMs

Cloud Backup for Virtual Machines is a plug-in for Azure VMware Solution that provides backup and restore capabilities for datastores and VMs residing on Azure NetApp Files datastores. With Cloud Backup for Virtual Machines, you can take VM-consistent snapshots for quick recovery points and easily restore VMs and VMDKs residing on

Azure NetApp Files datastores. For more information, see Install Cloud Backup for Virtual Machines.

Service level change for Azure NetApp Files datastore

Based on performance requirements of the datastore, you can change the service level of the Azure NetApp Files volume used for the datastore. Use the instructions provided to dynamically change the service level of a volume for Azure NetApp Files.

Changing the service level has no effect on the datastore or private cloud. There's no downtime and the volume IP address/mount path remains unchanged. However, the volume resource ID changes as a result of the capacity pool change. To correct any metadata mismatch, rerun the datastore creation in Azure CLI for the existing datastore with the new Resource ID for the Azure NetApp Files volume:

Azure CLI

```
az vmware datastore netapp-volume create \
    --name <name of existing datastore> \
    --resource-group <resource group containing AVS private cloud> \
    --cluster <cluster name in AVS private cloud> \
    --private-cloud <name of AVS private cloud> \
    --net-app-volume /subscriptions/<subscription
ID>/resourceGroups/<resource
group>/providers/Microsoft.NetApp/netAppAccounts/<NetApp
account>/capacityPools/<changed capacity pool>/volumes/<volume name>
```

Important

The parameters for datastore **name**, **resource-group**, **cluster**, and **private-cloud** must be **exactly the same as those on the existing datastore in the private cloud**. The **volume-id** is the updated Resource ID of the Azure NetApp Files volume after the service level change.

Disconnect an Azure NetApp Files-based datastore from your private cloud

You can use the instructions provided to disconnect an Azure NetApp Files-based datastore using either Azure portal or Azure CLI. There's no maintenance window

required for this operation. The disconnect action only disconnects the Azure NetApp Files volume as a datastore, it doesn't delete the data or the Azure NetApp Files volume.

Disconnect an Azure NetApp Files datastore using the Azure Portal

1. Select the datastore you want to disconnect from.
2. Right-click on the datastore and select **disconnect**.

Disconnect an Azure NetApp Files datastore using Azure CLI

```
az vmware datastore delete --name ANFDatastore1 --resource-group MyResourceGroup --cluster Cluster-1 --private-cloud MyPrivateCloud
```

Next steps

Now that you attached a datastore on Azure NetApp Files-based NFS volume to your Azure VMware Solution hosts, you can create your VMs. Use the following resources to learn more.

- Service levels for Azure NetApp Files
- Datastore protection using Azure NetApp Files snapshots
- About ExpressRoute virtual network gateways
- Understand Azure NetApp Files backup
- Guidelines for Azure NetApp Files network planning
- Azure NetApp Files datastore performance benchmarks for Azure VMware Solution

Video: Deploy Azure VMware Solution with Azure NetApp Files datastore

https://learn-video.azurefd.net/vod/player?show=inside-azure-for-it&ep=how-to-deploy-azure-vmware-solution-with-azure-netapp-files-datastore&locale=en-us&embedUrl=%2Fazure%2Fazure-vmware%2Fattach-azure-netapp-files-to-azure-vmware-solution-hosts

FAQs

- **Are there any special permissions required to create the datastore with the Azure NetApp Files volume and attach it onto the clusters in a private cloud?**

  No other special permissions are needed. The datastore creation and attachment is implemented via Azure VMware Solution control plane.

- **Which NFS versions are supported?**

  NFSv3 is supported for datastores on Azure NetApp Files.

- **Should Azure NetApp Files be in the same subscription as the private cloud?**

  The recommendation is to create the Azure NetApp Files volumes for the datastores in the same virtual network that has connectivity to the private cloud.

- **How many datastores are we supporting with Azure VMware Solution?**

  The default maximum is 8 but it can be increased to 256 by submitting a support ticket. To submit a support ticket, go to Create an Azure support request.

- **What latencies and bandwidth can be expected from the datastores backed by Azure NetApp Files?**

  We're currently validating and working on benchmarking. For now, follow the Performance best practices outlined in this article.

- **What are my options for backup and recovery?**

  Azure NetApp Files supports snapshots of datastores for quick checkpoints for near term recovery or quick clones. Azure NetApp Files backup lets you offload your Azure NetApp Files snapshots to Azure storage. With snapshots, copies and stores-changed blocks relative to previously offloaded snapshots are stored in an efficient format. This ability decreases Recovery Point Objective (RPO) and Recovery Time Objective (RTO) while lowering backup data transfer burden on the Azure VMware Solution service.

- **How do I monitor Storage Usage?**

  Use Metrics for Azure NetApp Files to monitor storage and performance usage for the Datastore volume and to set alerts.

- **What metrics are available for monitoring?**

  Usage and performance metrics are available for monitoring the Datastore volume. Replication metrics are also available for Azure NetApp Files datastore that can be replicated to another region using Cross Regional Replication. For more information about metrics, see Metrics for Azure NetApp Files.

- **What happens if a new node is added to the cluster, or an existing node is removed from the cluster?**

When you add a new node to the cluster, it automatically gains access to the datastore. Removing an existing node from the cluster doesn't affect the datastore.

- **How are the datastores charged, is there an additional charge?**

  Azure NetApp Files NFS volumes that are used as datastores are billed following the capacity pool based billing model. Billing depends on the service level. There's no extra charge for using Azure NetApp Files NFS volumes as datastores.

- **Can a single Azure NetApp Files datastore be added to multiple clusters within the same Azure VMware Solution private cloud?**

  Yes, you can select multiple clusters at the time of creating the datastore. More clusters can be added or removed after the initial creation as well.

- **Can a single Azure NetApp Files datastore be added to multiple clusters within different Azure VMware Solution private clouds?**

  Yes, you can connect an Azure NetApp Files volume as a datastore to multiple clusters in different private clouds. Each private cloud needs connectivity via the ExpressRoute gateway in the Azure NetApp Files virtual network. Latency considerations apply.

Feedback

Attach Azure NetApp Files to Azure VMware Solution VMs

Article • 04/12/2024

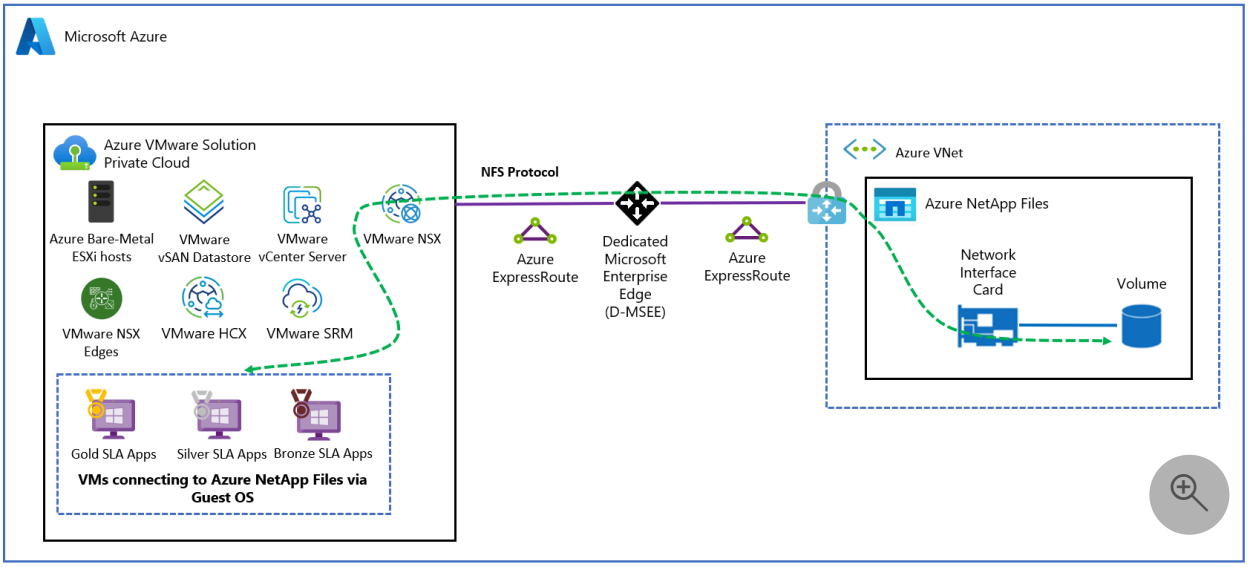
Azure NetApp Files is an Azure service for migration and running the most demanding enterprise file-workloads in the cloud: databases, SAP, and high-performance computing applications, with no code changes. In this article, learn how to set up, test, and verify the Azure NetApp Files volume as a file share for Azure VMware Solution workloads using the Network File System (NFS) protocol. The guest operating system runs inside virtual machines (VMs) accessing Azure NetApp Files volumes.

Azure NetApp Files and Azure VMware Solution are created in the same Azure region. Azure NetApp Files is available in many Azure regions and supports cross-region replication. For information on Azure NetApp Files configuration methods, see Storage hierarchy of Azure NetApp Files.

Services where Azure NetApp Files are used:

- **Active Directory connections**: Azure NetApp Files supports Understand guidelines for Active Directory Domain Services site design and planning for Azure NetApp Files.
- **Share Protocol**: Azure NetApp Files supports Server Message Block (SMB) and Network File System (NFS) protocols. This support means the volumes can be mounted on the Linux client and can be mapped on Windows client.
- **Azure VMware Solution**: Azure NetApp Files shares can be mounted from VMs that are created in the Azure VMware Solution environment.

The diagram shows a connection through Azure ExpressRoute to an Azure VMware Solution private cloud. The Azure VMware Solution environment accesses the Azure NetApp Files share mounted on Azure VMware Solution VMs.



Prerequisites

- ✓ Azure subscription with Azure NetApp Files enabled
- ✓ Subnet for Azure NetApp Files
- ✓ Linux VM on Azure VMware Solution
- ✓ Windows VMs on Azure VMware Solution

Create and mount Azure NetApp Files volumes

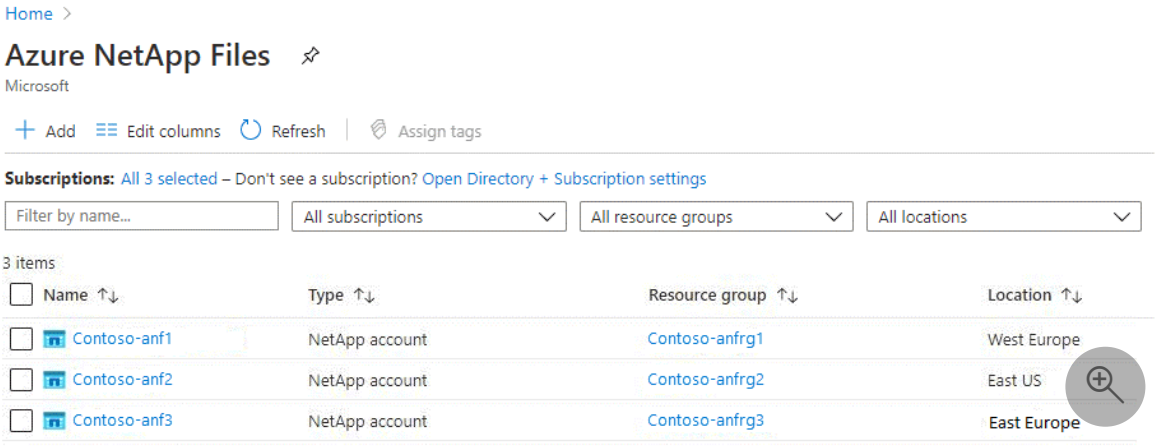
Use the following steps to create and mount Azure NetApp Files volumes onto Azure VMware Solution VMs.

1. Create a NetApp account.
2. Set up a capacity pool.
3. Create an SMB volume for Azure NetApp Files.
4. Create an NFS volume for Azure NetApp Files.
5. Delegate a subnet to Azure NetApp Files.

Verify preconfigured Azure NetApp Files

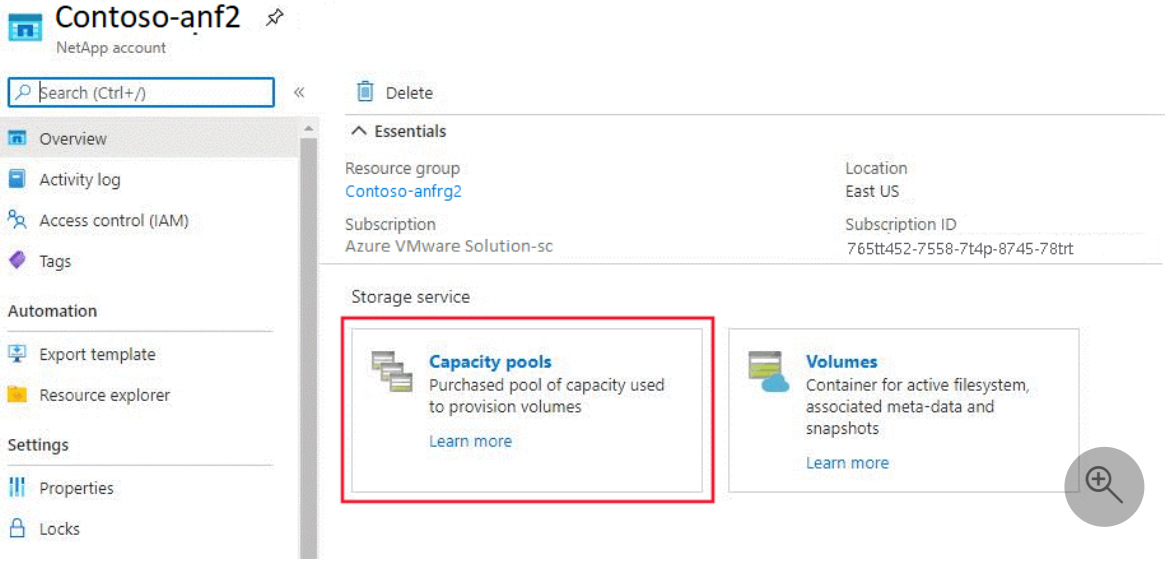
Verify the preconfigured Azure NetApp Files created in Azure on Azure NetApp Files Premium service level.

1. In the Azure portal, under **STORAGE**, select **Azure NetApp Files**. A list of your configured Azure NetApp Files appears.



2. Select a configured NetApp Files account to view its settings. For example, select **Contoso-anf2**.

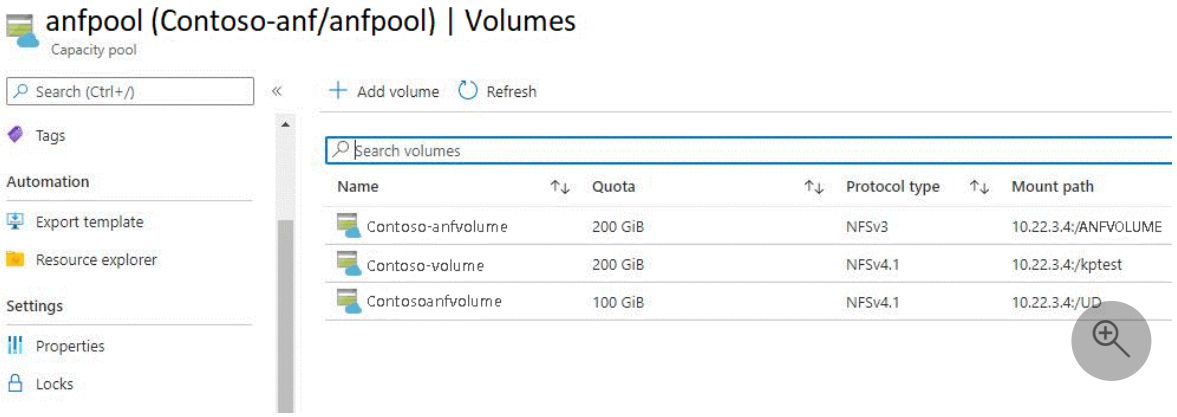
3. Select **Capacity pools** to verify the configured pool.



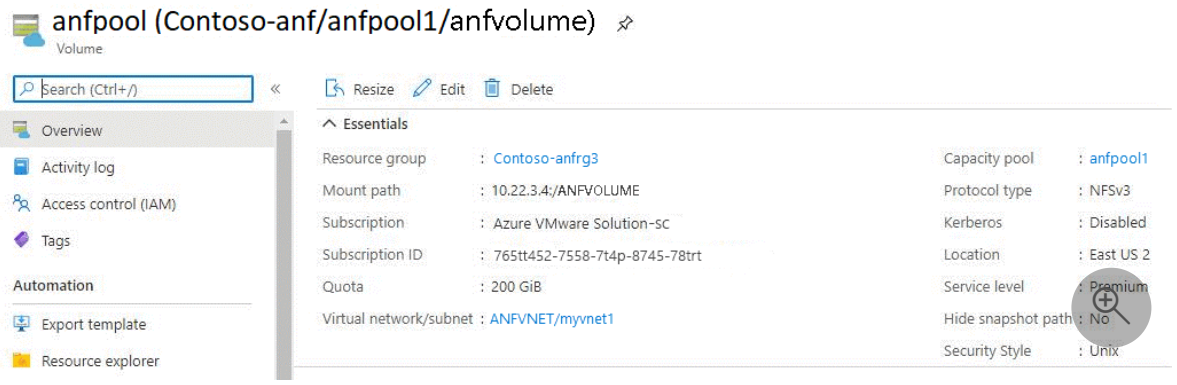
The Capacity pools page opens showing the capacity and service level. In this example, the storage pool is configured as 4 TiB with a Premium service level.

4. Select **Volumes** to view volumes created under the capacity pool. (See preceding screenshot.)

5. Select a volume to view its configuration.



A window opens showing the configuration details of the volume.



You can see that anfvolume has a size of 200 GiB and is in capacity pool anfpool1. It gets exported as an NFS file share via 10.22.3.4:/ANFVOLUME. One private IP from the Azure virtual network was created for Azure NetApp Files and the NFS path to mount on the VM.

To learn about Azure NetApp Files volume performance by size or "Quota," see Performance considerations for Azure NetApp Files.

Verify preconfigured Azure VMware Solution VM share mapping

To make your Azure NetApp Files share accessible to your Azure VMware Solution VM, you need to understand SMB and NFS share mapping. Once the SMB or NFS volumes are configured, you can mount them as documented here.

- **SMB share:** Create an Active Directory connection before deploying an SMB volume. The specified domain controllers must be accessible by the delegated subnet of Azure NetApp Files for a successful connection. Once the Active Directory is configured within the Azure NetApp Files account, it appears as a selectable item while creating SMB volumes.

- **NFS share:** Azure NetApp Files contributes to creating the volumes using NFS or dual protocol (NFS and SMB). A volume's capacity consumption counts against its pool's provisioned capacity. NFS can be mounted to the Linux server by using the command lines or /etc/fstab entries.

Next steps

Now that you covered integrating Azure NetApp Files with your Azure VMware Solution workloads, learn more about:

- Resource limitations for Azure NetApp Files
- Guidelines for Azure NetApp Files network planning
- Cross-region replication of Azure NetApp Files volumes
- Azure NetApp Files NFS FAQs
- Azure NetApp Files SMB FAQs

Install Cloud Backup for Virtual Machines (preview)

Article • 12/18/2023

Cloud Backup for Virtual Machines is a plug-in installed in the Azure VMware Solution and enables you to back up and restore Azure NetApp Files datastores and virtual machines (VMs).

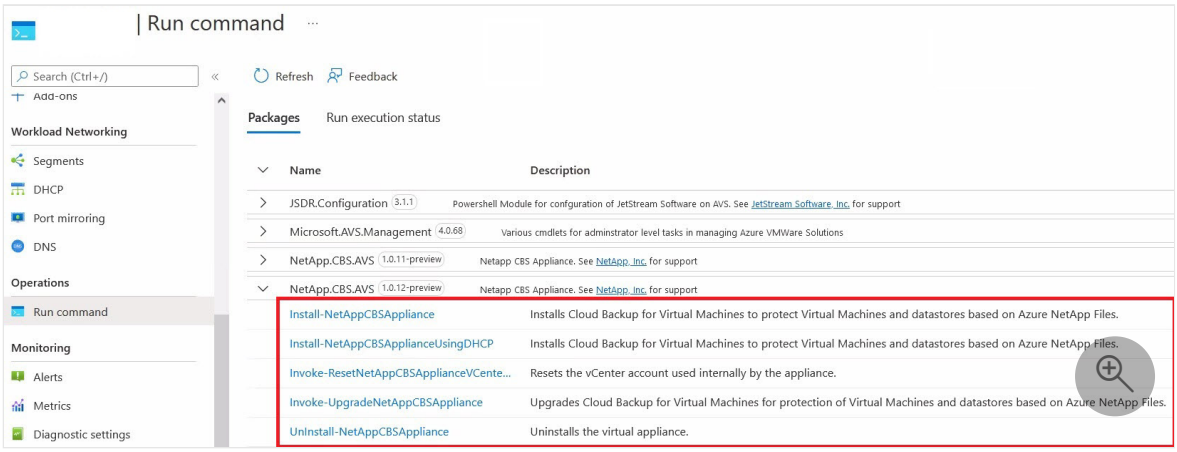
Cloud Backup for Virtual Machines features:

- Simple deployment via AVS `run command` from Azure portal
- Integration into the vSphere client for easy operations
- VM-consistent snapshots for quick recovery points
- Quick restoration of VMs and VMDKs on Azure NetApp Files datastores

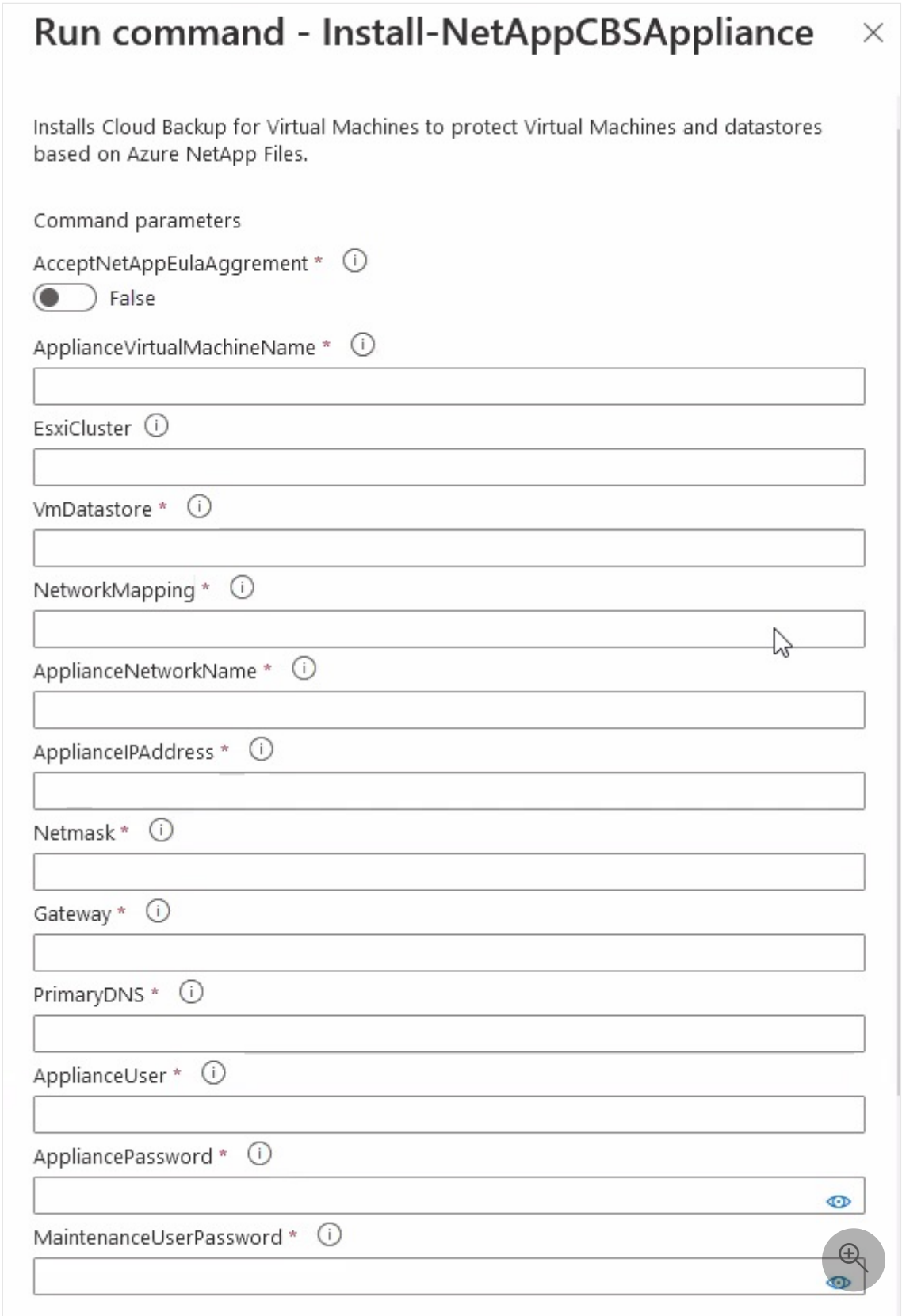
Install Cloud Backup for Virtual Machines

You need to install Cloud Backup for Virtual Machines through the Azure portal as an add-on.

1. Sign in to your Azure VMware Solution private cloud.
2. Select **Run command** > **Packages** > **NetApp.CBS.AVS** > **Install-NetAppCBSA**.



3. Provide the required values, then select **Run**.



Expand table

Field	Value
ApplianceVirtualMachineName	VM name for the appliance.
EsxiCluster	Destination ESXi cluster name to be used for deploying the appliance.

Field	Value
VmDatastore	Datastore to be used for the appliance.
NetworkMapping	Destination network to be used for the appliance.
ApplianceNetworkName	Network name to be used for the appliance.
ApplianceIPAddress	IPv4 address to be used for the appliance.
Netmask	Subnet mask.
Gateway	Gateway IP address.
PrimaryDNS	Primary DNS server IP address.
ApplianceUser	User Account for hosting API services in the appliance.
AppliancePassword	Password of the user hosting API services in the appliance.
MaintenanceUserPassword	Password of the appliance maintenance user.

> **Tip**
>
> You can also install Cloud Backup for Virtual Machines using DHCP by running the package `NetAppCBSApplianceUsingDHCP`. If you install Cloud Backup for Virtual Machines using DHCP, you don't need to provide the values for the PrimaryDNS, Gateway, Netmask, and ApplianceIPAddress fields. These values are automatically generated.

4. Check **Notifications** or the **Run Execution Status** tab to see the progress. For more information about the status of the execution, see Run command in Azure VMware Solution.

Upon successful execution, the Cloud Backup for Virtual Machines is automatically displayed in the VMware vSphere client.

Upgrade Cloud Backup for Virtual Machines

Before you initiate the upgrade, you must:

- Back up the MySQL database of Cloud Backup for Virtual Machines.
- With vSphere, take VMware snapshot copies of the Cloud Backup VM.

Back up the MySQL database

Don't start backup of the MySQL database when an on-demand backup job is already running.

1. From the VMware vSphere web client, select the VM where the SnapCenter VMware plug-in is located.
2. Right-click the VM. On the **Summary** tab of the virtual appliance, select **Launch Remote Console or Launch Web Console** to open a maintenance console window.

   The sign in defaults for the SnapCenter VMware plug-in maintenance console are:

   Username: `maint` Password: `admin123`
3. From the main menu, enter option **1) Application Configuration**.
4. From the Application Configuration menu, enter option **6) MySQL backup and restore**.
5. From the MySQL Backup and Restore Configuration menu, enter option **1) Configure MySQL backup**.
6. At the prompt, enter the backup location for the repository, the number of backups to keep, and the time the backup should start. All inputs are saved when you enter them. When the backup retention number is reached, older backups are deleted when new backups are performed.

   > ⓘ **Note**
   >
   > Repository backups are named `"backup-<date>"`. Because the repository restore function looks for the "backup" prefix, you should not change it.

Upgrade

Use the following steps to execute a run command to upgrade the Cloud Backup for Virtual Machines to the next available version.

1. Select **Run command** > **Packages** > **NetApp.CBS.AVS** > **Invoke-UpgradeNetAppCBSAppliance**.
2. Provide the required values, and then select **Run**.
3. Check **Notifications** or the **Run Execution Status** pane to monitor the progress.

Uninstall Cloud Backup for Virtual Machines

You can execute the run command to uninstall Cloud Backup for Virtual Machines.

> **Important**
>
> Before you initiate the upgrade, you must:
>
> - Backup the MySQL database of Cloud Backup for Virtual Machines.
> - Ensure that there are no other VMs installed in the VMware vSphere tag: `AVS_ANF_CLOUD_ADMIN_VM_TAG`. All VMs with this tag are deleted when you uninstall.

1. Select **Run command** > **Packages** > **NetApp.CBS.AVS** > **Uninstall-NetAppCBSAppliance**.
2. Provide the required values, and then select **Run**.
3. Check **Notifications** or the **Run Execution Status** pane to monitor the progress.

Change vCenter account password

Use the following steps to execute the command to reset the vCenter account password:

1. Select **Run command** > **Packages** > **NetApp.CBS.AVS** > **Invoke-ResetNetAppCBSApplianceVCenterPasswordA**.
2. Provide the required values, then select **Run**.
3. Check **Notifications** or the **Run Execution Status** pane to monitor the progress.

Next steps

- Back up Azure NetApp Files datastores and VMs using Cloud Backup for Virtual Machines
- Restore VMs using Cloud Backup for Virtual Machines

Back up Azure NetApp Files datastores and VMs using Cloud Backup for Virtual Machines (preview)

Article • 03/22/2024

From the VMware vSphere client, you can back up datastores and Virtual Machines (VMs) to the cloud. This article explains how to configure your subscription, create a backup policy, and create and back up a resource group.

Configure subscriptions

Before you back up your Azure NetApp Files datastores, you must add your Azure and Azure NetApp Files cloud subscriptions.

Prerequisites

- Cloud Backup for Virtual Machines uses the Azure REST API to collect information about your Azure NetApp Files datastores and create Azure NetApp Files snapshots. To interact with the Azure REST API, the Cloud Backup for Virtual Machines virtual appliance requires outbound internet access from your Azure VMware Solution SDDC via HTTPS. For more information, see Internet connectivity design considerations.

- You must have sufficient permissions to Create a Microsoft Entra app and service principal within your Microsoft Entra tenant and assign to the application a role in your Azure subscription. You can use the built-in role of "contributor" or you can create a custom role with only the required permissions:

  JSON

  ```
  "actions": [
      "Microsoft.NetApp/*",
      "Microsoft.Resources/resources/read",
      "Microsoft.Resources/subscriptions/resourceGroups/read",
      "Microsoft.Resources/subscriptions/resourceGroups/resources/read",
      "Microsoft.Resources/subscriptions/resourceGroups/write",
      "Microsoft.Network/virtualNetworks/read",
      "Microsoft.Insights/Metrics/Read"
      ],
  ```

For more information on creating custom roles, see Azure custom roles.

Add an Azure cloud subscription

1. Sign in to the VMware vSphere client.
2. From the left navigation, select **Cloud Backup for Virtual Machines**.
3. Select the **Settings** page and then select the **Cloud Subscription** tab.
4. Select **Add**. Provide the **Subscription ID**, **Tenant ID**, **Client IID**, and **Client secret key** from the app registration you previously created.

Add an Azure NetApp Files cloud subscription account

1. From the left navigation, select **Cloud Backup for Virtual Machines**.
2. Select **Storage Systems**.
3. Select **Add** to add the Azure NetApp Files cloud subscription account details.
4. Provide the required values and then select **Add** to save your settings.

Create a backup policy

You must create backup policies before you can use Cloud Backup for Virtual Machines to back up Azure NetApp Files datastores and VMs.

1. In the left navigation of the vCenter web client page, select **Cloud Backup for Virtual Machines** > **Policies**.
2. On the **Policies** page, select **Create** to initiate the wizard.
3. On the **New Backup Policy** page, select the vCenter Server that uses the policy, then enter the policy name and a description.

- **Only alphanumeric characters and underscores (_) are supported in VM, datastore, cluster, policy, backup, or resource group names.** Other special characters aren't supported.

4. Specify the retention settings. The maximum retention value is 255 backups. If the **"Backups to keep"** option is selected during the backup operation, Cloud Backup for Virtual Machines retains backups within the specified retention count and delete the backups that exceed the retention count.

5. Specify the frequency settings. The policy specifies the backup frequency only. The specific protection schedule for backing up is defined in the resource group. Therefore, two or more resource groups can share the same policy and backup frequency but have different backup schedules.

6. **Optional:** In the **Advanced** fields, select the fields that are needed. The Advanced field details are listed in the following table.

Expand table

Field	Action
VM consistency	Check this box to pause the VMs and create a VMware snapshot each time the backup job runs. When you check the VM consistency box, backup operations might take longer and require more storage space. In this scenario, the VMs are first paused, then VMware performs a VM consistent snapshot. Cloud Backup for Virtual Machines then performs its backup operation, and then VM operations are resumed. VM guest memory isn't included in VM consistency snapshots.
Include datastores with independent disks	Check this box to include any datastores with independent disks that contain temporary data in your backup.

7. Select **Add** to save your policy. You can verify the policy was created successfully and review the configuration by selecting the policy in the **Policies** page.

Resource groups

A resource group is the container for VMs and datastores that you want to protect.

Don't add VMs in an inaccessible state to a resource group. Although a resource group can contain a VM in an inaccessible state, the inaccessible state causes backups for the resource group to fail.

Considerations for resource groups

You can add or remove resources from a resource group at any time.

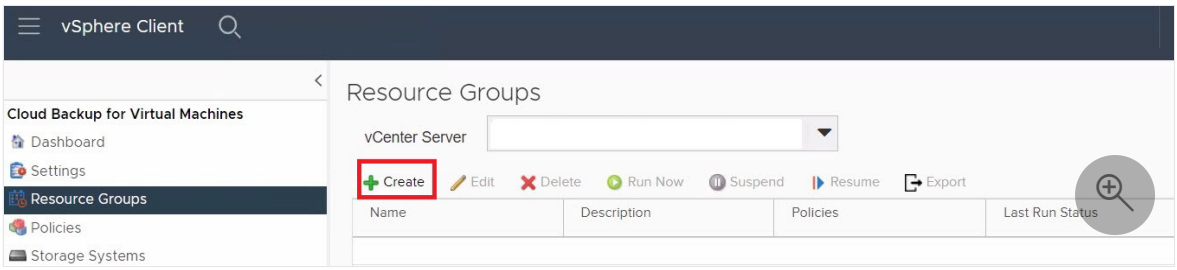
- **Back up a single resource:** To back up a single resource (for example, a single VM), you must create a resource group that contains that single resource.
- **Back up multiple resources:** To back up multiple resources, you must create a resource group that contains multiple resources.
- **Optimize snapshot copies:** To optimize snapshot copies, group the VMs and datastores that are associated with the same volume into one resource group.
- **Backup policies:** Although it's possible to create a resource group without a backup policy, you can only perform scheduled data protection operations when at

least one policy is attached to the resource group. You can use an existing policy, or you can create a new policy while creating a resource group.

- **Compatibility checks:** Cloud Backup for VMs performs compatibility checks when you create a resource group. Reasons for incompatibility might be:
  - Virtual machine disks (VMDKs) are on unsupported storage.
  - A shared PCI device is attached to a VM.
  - The Azure subscription account wasn't added.

Create a resource group using the wizard

1. In the left navigation of the vCenter web client page, select **Cloud Backup** for **Virtual Machines** > **Resource Groups**. Then select **+ Create** to start the wizard



2. On the **General Info & Notification** page in the wizard, enter the required values.

3. On the **Resource** page, do the following:

Expand table

Field	Action
Scope	Select the type of resource you want to protect: -Datastores -Virtual Machines
Datacenter	Navigate to the VMs or datastores
Available entities	Select the resources you want to protect. Then select > to move your selections to the Selected entities list.

When you select **Next**, the system first checks that Cloud Backup for Virtual Machines manages and is compatible with the storage on which the selected resources are located.

> **Important**
>
> If you receive the message `selected <resource-name> is not Cloud Backup for Virtual Machines compatible` then a selected resource is not compatible

with Cloud Backup for Virtual Machines.

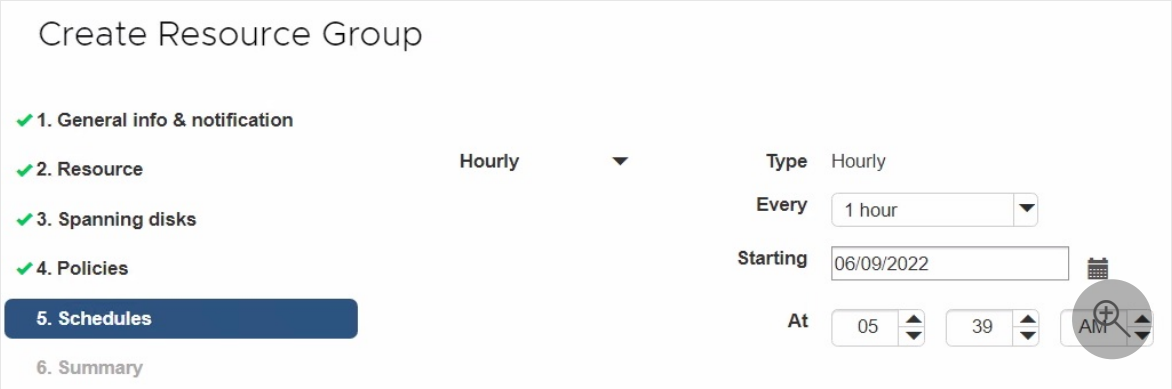
4. On the **Spanning disks** page, select an option for VMs with multiple VMDKs across multiple datastores:

   - Always exclude all spanning datastores (The default option for datastores)
   - Always include all spanning datastores (The default for VMs)
   - Manually select the spanning datastores to be included

5. On the **Policies** page, select or create one or more backup policies.

   - To use **an existing policy**, select one or more policies from the list.
   - To **create a new policy**:
     a. Select + **Create**.
     b. Complete the New Backup Policy wizard to return to the Create Resource Group wizard.

6. On the **Schedules** page, configure the backup schedule for each selected policy. In the **Starting** field, enter a date and time other than zero. The date must be in the format day/month/year. You must fill in each field. The Cloud Backup for Virtual Machines creates schedules in the time zone in which the Cloud Backup for Virtual Machines is deployed. You can modify the time zone by using the Cloud Backup for Virtual Machines GUI.



7. Review the summary. If you need to change any information, you can return to any page in the wizard to do so. Select **Finish** to save your settings.

   After you select **Finish**, the new resource group is added to the resource group list.

   If the pause operation fails for any of the VMs in the backup, then the backup is marked as not VM-consistent even if the policy selected has VM consistency selected. In this case, it's possible that some of the VMs were successfully paused.

Other ways to create a resource group

In addition to using the wizard, you can:

- **Create a resource group for a single VM:**

  1. Select **Menu** > **Hosts and Clusters**.
  2. Right-click the Virtual Machine you want to create a resource group for and select **Cloud Backup for Virtual Machines**. Select **+ Create**.

- **Create a resource group for a single datastore:**

  1. Select **Menu** > **Hosts and Clusters**.
  2. Right-click a datastore, then select **Cloud Backup for Virtual Machines**. Select **+ Create**.

Back up resource groups

Backup operations are performed on all the resources defined in a resource group. If a resource group has a policy attached and a schedule configured, backups occur automatically according to the schedule.

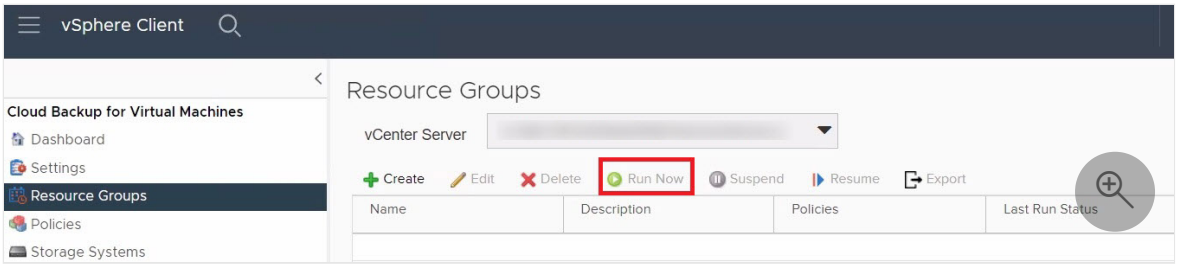
Prerequisites to back up resource groups

- You must have a resource group created with a policy attached.

  > ⓘ **Note**
  >
  > Do not start an on-demand backup job when a job to back up the Cloud Backup for Virtual Machines MySQL database is already running. Use the maintenance console to see the configured backup schedule for the MySQL database.

Back up resource groups on demand

1. In the left navigation of the vCenter web client page, select **Cloud Backup for Virtual Machines** > **Resource Groups**, then select a resource group. Select **Run Now** to start the backup.



a. If the resource group has multiple policies configured, then in the **Backup Now** dialog box, select the policy you want to use for this backup operation.

2. Select **OK** to initiate the backup.

> **Note**
>
> You can't rename a backup once it's created.

3. **Optional:** Monitor the operation progress by selecting **Recent Tasks** at the bottom of the window or on the dashboard Job Monitor for more details. If the pause operation fails for any of the VMs in the backup, then the backup completes with a warning. It's marked as not VM-consistent even if the selected policy has VM consistency selected. In this case, it's possible that some of the VMs were successfully paused. In the job monitor, the failed VM details show the pause operation as failed.

Next steps

- Restore VMs using Cloud Backup for Virtual Machines

Restore VMs using Cloud Backup for Virtual Machines (preview)

Article • 12/19/2023

Cloud Backup for Virtual Machines enables you to restore virtual machines (VMs) from the cloud backup to the vCenter.

This article covers how to:

- Restore VMs from backups
- Restore deleted VMs from backups
- Restore VM disks (VMDKs) from backups
- Recovery of Cloud Backup for Virtual Machines internal database

Restore VMs from backups

When you restore a VM, you can overwrite the existing content with the backup copy that you select or you can restore a deleted VM from a backup copy.

You can restore VMs to the original datastore mounted on the original ESXi host, which overwrites the original VM.

Prerequisites to restore VMs

- A backup must exist: you need to create a backup of the VM using the Cloud Backup for Virtual Machines before you can restore the VM.

> **Note**
>
> Restore operations cannot finish successfully if there are snapshots of the VM that were performed by software other than the Cloud Backup for Virtual Machines.

- The VM must not be in transit: the VM that you want to restore must not be in a state of vMotion or Storage vMotion.
- High Availability (HA) configuration errors: ensure there are no HA configuration errors displayed on the vCenter ESXi Host Summary screen before restoring backups to a different location.

Considerations for restoring VMs from backups

- VM is unregistered and registered again: The restore operation for VMs unregisters the original VM, restores the VM from a backup snapshot, and registers the restored VM with the same name and configuration on the same ESXi server. You must manually add the VMs to resource groups after the restore.
- Restoring datastores: You can't restore a datastore, but you can restore any VM in the datastore.
- VMware consistency snapshot failures for a VM: Even if a VMware consistency snapshot for a VM fails, the VM is nevertheless backed up. You can view the entities contained in the backup copy in the Restore wizard and use it for restore operations.

Restore a VM from a backup

1. In the VMware vSphere web client GUI, select **Menu** in the toolbar. Select **Inventory** and then **Virtual Machines and Templates**.
2. In the left navigation, right-click a Virtual Machine, then select **NetApp Cloud Backup**. In the drop-down list, select **Restore** to initiate the wizard.
3. In the Restore wizard, on the **Select Backup** page, select the backup snapshot copy that you want to restore.

   > ⓘ **Note**
   >
   > You can search for a specific backup name or a partial backup name, or you can filter the backup list by selecting the filter icon and then choosing a date and time range, selecting whether you want backups that contain VMware snapshots, whether you want mounted backups, and the location. Select **OK** to return to the wizard.

4. On the **Select Scope** page, select **Entire Virtual Machine** in the **Restore scope** field, then select **Restore location**, and then enter the destination ESXi information where the backup should be mounted.
5. When you restore partial backups, the restore operation skips the Select Scope page.
6. Enable **Restart VM** checkbox if you want the VM to be powered on after the restore operation.
7. On the **Select Location** page, select the location for the primary location.
8. Review the **Summary** page and then select **Finish**.
9. **Optional:** Monitor the operation progress by selecting Recent Tasks at the bottom of the screen.

Although the VMs are restored, they're not automatically added to their former resource groups. Therefore, you must manually add the restored VMs to the appropriate resource groups.

Restore deleted VMs from backups

You can restore a deleted VM from a datastore primary backup to an ESXi host that you select. You can restore VMs to the original datastore mounted on the original ESXi host, which creates a clone of the VM.

Prerequisites to restore deleted VMs

- You need to add the Azure cloud Subscription account. The user account in vCenter must have the minimum vCenter privileges required for Cloud Backup for Virtual Machines.
- A backup must exist. You need to create a backup of the VM using the Cloud Backup for Virtual Machines before you can restore the VMDKs on that VM.

Considerations for restoring deleted VMs

You can't restore a datastore, but you can restore any VM in the datastore.

Restore deleted VMs

1. Select **Menu** and then select the **Inventory** option.
2. Select a datastore, then select the **Configure** tab, then the **Backups in the Cloud Backup for Virtual Machines** section.
3. Select (double-click) a backup to see a list of all VMs that are included in the backup.
4. Select the deleted VM from the backup list and then select **Restore**.
5. On the **Select Scope** page, select **Entire Virtual Machine** in the **Restore scope field**, then select the restore location, and then enter the destination ESXi information where the backup should be mounted.
6. Enable **Restart VM** checkbox if you want the VM to be powered on after the restore operation.
7. On the **Select Location** page, select the location of the backup that you want to restore to.
8. Review the **Summary** page, then select **Finish**.

Restore VMDKs from backups

You can restore existing VMDKs or deleted or detached VMDKs from either a primary or secondary backup. You can restore one or more VMDKs on a VM to the same datastore.

Prerequisites to restore VMDKs

- A backup must exist. You need to create a backup of the VM using the Cloud Backup for Virtual Machines.
- The VM must not be in transit. The VM that you want to restore must not be in a state of vMotion or Storage vMotion.

Considerations for restoring VMDKs

- If the VMDK is deleted or detached from the VM, then the restore operation attaches the VMDK to the VM.
- Attach and restore operations connect VMDKs using the default SCSI controller. VMDKs that are attached to a VM with an NVME controller are backed up, but for attach and restore operations they're connected back using a SCSI controller.

Restore VMDKs

1. In the VMware vSphere web client GUI, select **Menu** in the toolbar. Select **Inventory**, then **Virtual Machines and Templates**.
2. In the left navigation, right-click a VM and select **NetApp Cloud Backup**. In the drop-down list, select **Restore**.
3. In the Restore wizard, on the **Select Backup** page, select the backup copy from which you want to restore. To find the backup, do one of the following options:

    - Search for a specific backup name or a partial backup name.
    - Filter the backup list by selecting the filter icon and a date and time range. Select if you want backups that contain VMware snapshots, if you want mounted backups, and primary location. Select **OK** to return to the wizard.

4. On the **Select Scope** page, select **Particular virtual disk** in the Restore scope field, then select the virtual disk and destination datastore.
5. On the **Select Location** page, select the location that you want to restore to.
6. Review the **Summary** page and then select **Finish**.
7. **Optional:** Monitor the operation progress by clicking Recent Tasks at the bottom of the screen.

Recovery of Cloud Backup for Virtual Machines internal database

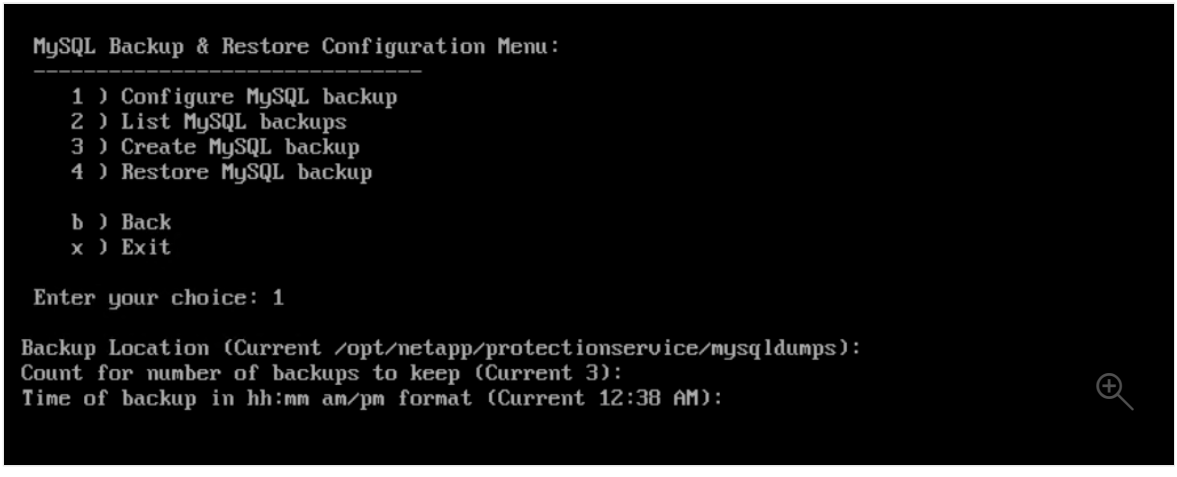
You can use the maintenance console to restore a specific backup of the MySQL database (also called an NSM database) for Cloud Backup for Virtual Machines.

1. Open a maintenance console window.
2. From the main menu, enter option **1 Application Configuration**.
3. From the Application Configuration menu, enter option **6 MySQL backup and restore**.
4. From the MySQL Backup and Restore Configuration menu, enter option **2 List MySQL backups**. Make note of the backup you want to restore.
5. From the MySQL Backup and Restore Configuration menu, enter option **3 Restore MySQL backup**.
6. At the prompt "Restore using the most recent backup," enter **N**.
7. At the prompt "Backup to restore from," enter the backup name, and then select **Enter**. The selected backup MySQL database gets restored to its original location.

If you need to change the MySQL database backup configuration, you can modify:

- The backup location (the default is: `/opt/netapp/protectionservice/mysqldumps`)
- The number of backups kept (the default value is three)
- The time of day the backup is recorded (the default value is 12:39 a.m.)

1. Open a maintenance console window.
2. From the main menu, enter option **1 Application Configuration**.
3. From the Application Configuration menu, enter option **6 MySQL backup and restore**.
4. From the MySQL Backup & Restore Configuration, menu, enter option **1 Configure MySQL backup**.



External storage solutions overview

Article • 03/10/2024

External storage solutions for Azure VMware Solution

Azure VMware Solution is a Hyperconverged Infrastructure (HCI) service that offers VMware vSAN as the primary storage option. However, a significant requirement with on-premises VMware deployments is external storage, especially block storage. Providing the same consistent external block storage architecture in the cloud is crucial for some customers. Some workloads can't be migrated or deployed to the cloud without consistent external block storage. As a key principle of Azure VMware Solution is to enable customers to continue to use their investments and their favorite VMware solutions running on Azure, we engaged storage providers with similar goals.

Solutions

Pure Cloud Block Storage

Pure Cloud Block Store

Article • 03/11/2024

Pure Cloud Block Store for Azure VMware Solution

Pure Cloud Block Store, offered by Pure Storage, is one of the external block storage solutions supported by Azure VMware Solution. It helps bridge the gap by allowing customers to provision external block storage as needed to make full use of an Azure VMware Solution deployment without the need to scale out compute resources, while helping customers migrate their on-premises workloads to Azure. Pure Cloud Block Store is a 100% software-delivered product running entirely on native Azure infrastructure that brings all the relevant Purity features and capabilities to Azure.

Onboarding and support

Pure Storage manages onboarding of Pure Cloud Block Store for Azure VMware Solution. As Pure Cloud Block Store (CBS) is a customer deployed and managed solution, reach out to Pure Storage for Customer Support.

For more information, see the following resources:

- Azure VMware Solution + CBS Implementation Guide
- CBS Deployment Guide
- CBS Deployment Troubleshooting
- CBS support articles
- Videos

Backup solutions for Azure VMware Solution virtual machines (VMs)

Article • 12/12/2023

A key principle of Azure VMware Solution is to enable you to continue to use your investments and your favorite VMware solutions running on Azure. Independent software vendor (ISV) technology support, validated with Azure VMware Solution, is an important part of this strategy.

Our backup partners have industry-leading backup and restore solutions in VMware-based environments. Customers widely adopted these solutions for their on-premises deployments. These partners extended their solutions to Azure VMware Solution, using Azure to provide a backup repository and a storage target for long-term retention and archival.

Back up network traffic between Azure VMware Solution VMs and the backup repository in Azure travels over a high-bandwidth, low-latency link. Replication traffic across regions travels over the internal Azure backplane network, which lowers bandwidth costs for users.

> **Note**
>
> For common questions, see **our third-party backup solution FAQ**.

You can find more information on these backup solutions here:

- Cohesity
- Commvault
- Dell Technologies
- Rubrik
- Veeam
- Veritas

Set up Azure Backup Server for Azure VMware Solution

Article • 03/29/2024

Azure Backup Server contributes to your business continuity and disaster recovery (BCDR) strategy. With Azure VMware Solution, you can only configure a virtual machine (VM)-level backup using Azure Backup Server.

Azure Backup Server can store backup data to:

- **Disk**: For short-term storage, Azure Backup Server backs up data to disk pools.
- **Azure cloud**: For both short-term and long-term storage off-premises, Azure Backup Server data stored in disk pools can be backed up to the Microsoft Azure cloud by using Azure Backup.

Use Azure Backup Server to restore data to the source or an alternate location. That way, if the original data is unavailable because of planned or unexpected issues, you can restore data to an alternate location.

This article helps you prepare your Azure VMware Solution environment to back up VMs by using Azure Backup Server. We walk you through the steps to:

- ✓ Determine the recommended VM disk type and size to use.
- ✓ Create a Recovery Services vault that stores the recovery points.
- ✓ Set the storage replication for a Recovery Services vault.
- ✓ Add storage to Azure Backup Server.

Supported VMware vSphere features

- **Agentless backup:** Azure Backup Server doesn't require an agent to be installed on the vCenter Server or ESXi server to back up the VM. Instead, provide the IP address or fully qualified domain name (FQDN) and the sign-in credentials used to authenticate the VMware vCenter Server with Azure Backup Server.
- **Cloud-integrated backup:** Azure Backup Server protects workloads to disk and the cloud. The backup and recovery workflow of Azure Backup Server helps you manage long-term retention and offsite backup.
- **Detect and protect VMs managed by vCenter Server:** Azure Backup Server detects and protects VMs deployed on a vCenter Server or ESXi hosts. Azure Backup Server also detects VMs managed by vCenter Server so that you can protect large deployments.

- **Folder-level auto protection:** vCenter Server lets you organize your VMs into Virtual Machine folders. Azure Backup Server detects these folders. You can use it to protect VMs at the folder level, including all subfolders. During the protection of folders, Azure Backup Server protects the VMs in that folder and protects VMs added later. Azure Backup Server detects new VMs daily, protecting them automatically. As you organize your VMs in recursive folders, Azure Backup Server automatically detects and protects the new VMs deployed in the recursive folders.
- **Azure Backup Server continues to protect vMotioned VMs within the cluster:** As VMs are vMotioned for dynamic resource load balancing within the cluster, Azure Backup Server automatically detects and continues VM protection.
- **Recover necessary files faster:** Azure Backup Server can recover files or folders from a Windows VM without recovering the entire VM.
- **Application Consistent Backups:** If the *VMware Tools* aren't installed, a crash consistent backup gets executed. When the *VMware Tools* are installed with Microsoft Windows virtual machines, all applications that support VSS freeze and thaw operations support application consistent backups. When the *VMware Tools* are installed with Linux virtual machines, application consistent snapshots are supported by calling the pre and post scripts.

Limitations

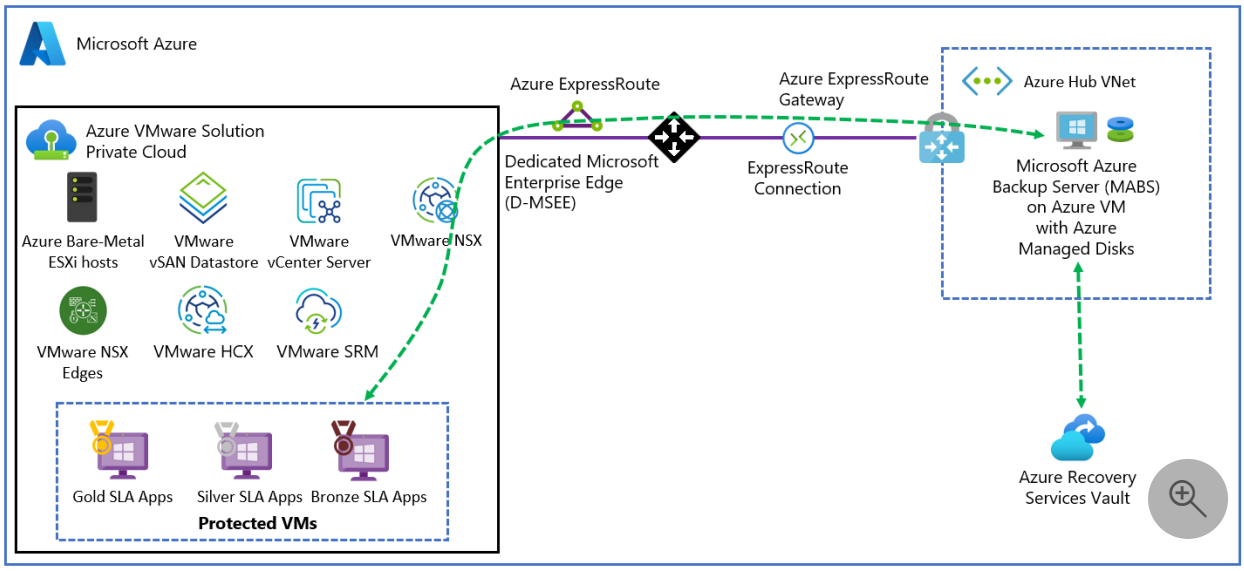
- If you're using *Azure Backup Server V3*, then you must install Update Rollup 2. New installations from the Azure portal now use *Azure Backup Server V4* that supports vSphere, version *6.5* to *8.0*.
- You can't back up user snapshots before the first Azure Backup Server backup. After Azure Backup Server finishes the first backup, then you can back up user snapshots.
- Update Rollup 2 for Azure Backup Server v3 must be installed.
- Azure Backup Server can't protect VMware vSphere VMs with pass-through disks and physical raw device mappings (pRDMs).
- Azure Backup Server can't detect or protect VMware vSphere vApps.

To set up Azure Backup Server for Azure VMware Solution, you must finish the following steps:

- Set up the prerequisites and environment.
- Create a Recovery Services vault.
- Download and install Azure Backup Server.
- Add storage to Azure Backup Server.

Deployment architecture

Azure Backup Server is deployed as an Azure infrastructure as a service (IaaS) VM to protect Azure VMware Solution VMs.



Prerequisites for the Azure Backup Server environment

Consider the recommendations in this section when you install Azure Backup Server in your Azure environment.

Azure Virtual Network

Ensure that you configure networking for your VMware private cloud in Azure.

Determine the size of the VM

Use the MABS Capacity Planner to determine the correct VM size. Based on your inputs, the capacity planner gives you the required memory size and CPU core count. Use this information to choose the appropriate Azure VM size. The capacity planner also provides total disk size required for the VM along with the required disk IOPS. We recommend using a standard SSD disk for the VM. By pooling more than one SSD, you can achieve the required IOPS.

Follow the instructions in the Create your first Windows VM in the Azure portal tutorial. You created the VM in the virtual network that you created in the previous step. Start with a gallery image of Windows Server 2019 Datacenter to run the Azure Backup Server.

> **Note**

Azure Backup Server is designed to run on a dedicated, single-purpose server. You can't install Azure Backup Server on a computer that:

- Runs as a domain controller.
- Has the Application Server role installed.
- Is a System Center Operations Manager management server?
- Runs Exchange Server.
- Is a node of a cluster?

Disks and storage

Azure Backup Server requires disks for installation.

Expand table

Requirement	Recommended size
Azure Backup Server installation	Installation location: 3 GB Database files drive: 900 MB System drive: 1 GB for SQL Server installation You need space for Azure Backup Server to copy the file catalog to a temporary installation location when you archive.
Disk for storage pool (Uses basic volumes, can't be on a dynamic disk)	Two to three times the protected data size. For detailed storage calculation, see DPM Capacity Planner.

To learn how to attach a new managed data disk to an existing Azure VM, see Attach a managed data disk to a Windows VM by using the Azure portal.

Note

A single Azure Backup Server has a soft limit of 120 TB for the storage pool.

Store backup data on local disk and in Azure

Storing backup data in Azure reduces backup infrastructure on the Azure Backup Server VM. For operational recovery (backup), Azure Backup Server stores backup data on Azure disks attached to the VM. After the disks and storage space are attached to the VM, Azure Backup Server manages the storage for you. The amount of storage depends

on the number and size of disks attached to each Azure VM. Each size of the Azure VM has a maximum number of disks that can be attached. For example, A2 is four disks, A3 is eight disks, and A4 is 16 disks. Again, the size and number of disks determine the total backup storage pool capacity.

> **ⓘ Important**
>
> You should *not* retain operational recovery data on Azure Backup Server-attached disks for more than five days. If data is more than five days old, store it in a Recovery Services vault.

To store backup data in Azure, create or use a Recovery Services vault. When you prepare to back up the Azure Backup Server workload, you configure the Recovery Services vault. Once configured, each time an online backup job runs, a recovery point gets created in the vault. Each Recovery Services vault holds up to 9,999 recovery points. Depending on the number of recovery points created and how long kept, you can keep backup data for many years. For example, you could create monthly recovery points and keep them for five years.

> **ⓘ Important**
>
> Whether you send backup data to Azure or keep it locally, you must register Azure Backup Server with a Recovery Services vault.

Scale deployment

If you want to scale your deployment, you have the following options:

- **Scale up**: Increase the size of the Azure Backup Server VM from A series to DS3 series, and increase the local storage.
- **Offload data**: Send older data to Azure and keep only the newest data on the storage attached to the Azure Backup Server machine.
- **Scale out**: Add more Azure Backup Server machines to protect the workloads.

.NET Framework

The VM must have .NET Framework 4.5 or higher installed.

Join a domain

The Azure Backup Server VM must be joined to a domain. A domain user with administrator privileges on the VM must install Azure Backup Server.

Azure Backup Server deployed in an Azure VM can back up workloads on the VMs in Azure VMware Solution. The workloads should be in the same domain to enable the backup operation.

Create a Recovery Services vault

A Recovery Services vault is a storage entity that stores the recovery points created over time. It also contains backup policies that are associated with protected items.

1. Sign in to the Azure portal, and on the left menu, select **All services**.
2. In the **All services** dialog box, enter **Recovery Services** and select **Recovery Services vaults** from the list.

   The list of Recovery Services vaults in the subscription appears.
3. On the **Recovery Services vaults** dashboard, select **Add**.

   The **Recovery Services vault** dialog box opens.
4. Enter values, then select **Create**.

   - **Name**: Enter a friendly name to identify the vault. The name must be unique to the Azure subscription. Specify a name that has at least two but not more than 50 characters. The name must start with a letter and consist only of letters, numbers, and hyphens.
   - **Subscription**: Choose the subscription to use. If you're a member of only one subscription, you see that name. If you're not sure which subscription to use, use the default (suggested) subscription. There are multiple choices only if your work or school account is associated with more than one Azure subscription.
   - **Resource group**: Use an existing resource group or create a new one. To see the list of available resource groups in your subscription, select **Use existing**, then select a resource from the drop-down list. To create a new resource group, select **Create new** and enter the name.
   - **Location**: Select the geographic region for the vault. To create a vault to protect Azure VMware Solution virtual machines, the vault *must* be in the same region as the Azure VMware Solution private cloud.

   It can take a while to create the Recovery Services vault. Monitor the status notifications in the **Notifications** area in the upper-right corner of the portal. After

creating your vault, it's visible in the list of Recovery Services vaults. If you don't see your vault, select **Refresh**.

Set storage replication

The storage replication option lets you choose between geo-redundant storage (the default) and locally redundant storage. Geo-redundant storage copies the data in your storage account to a secondary region, making your data durable. Locally redundant storage is a cheaper option that isn't as durable. To learn more about geo-redundant and locally redundant storage options, see Azure Storage redundancy.

> **Important**
>
> Changing the setting of **Storage replication type Locally-redundant/Geo-redundant** for a Recovery Services vault must be done before you configure backups in the vault. After you configure backups, the option to modify it is disabled, and you can't change the storage replication type.

1. From **Recovery Services vaults**, select the new vault.
2. Under **Settings**, select **Properties**. Under **Backup Configuration**, select **Update**.
3. Select the storage replication type, and select **Save**.

Download and install the software package

Follow the steps in this section to download, extract, and install the software package.

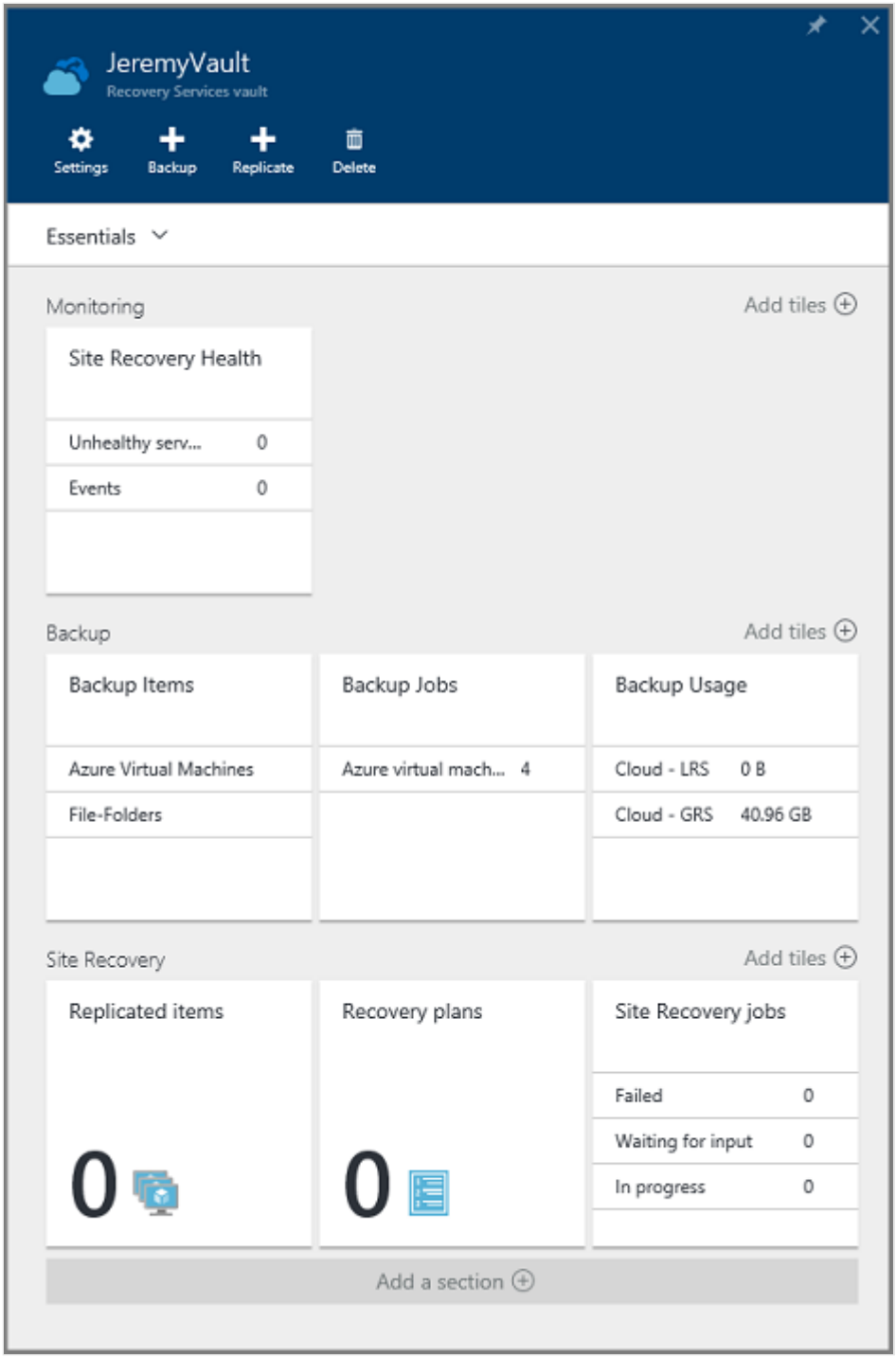
Download the software package

1. Sign in to the Azure portal.
2. If you already have a Recovery Services vault open, continue to the next step.

> **Tip**
>
> If you don't have a Recovery Services vault open, and you're in the Azure portal, in the list of resources enter **Recovery Services** > **Recovery Services vaults**.

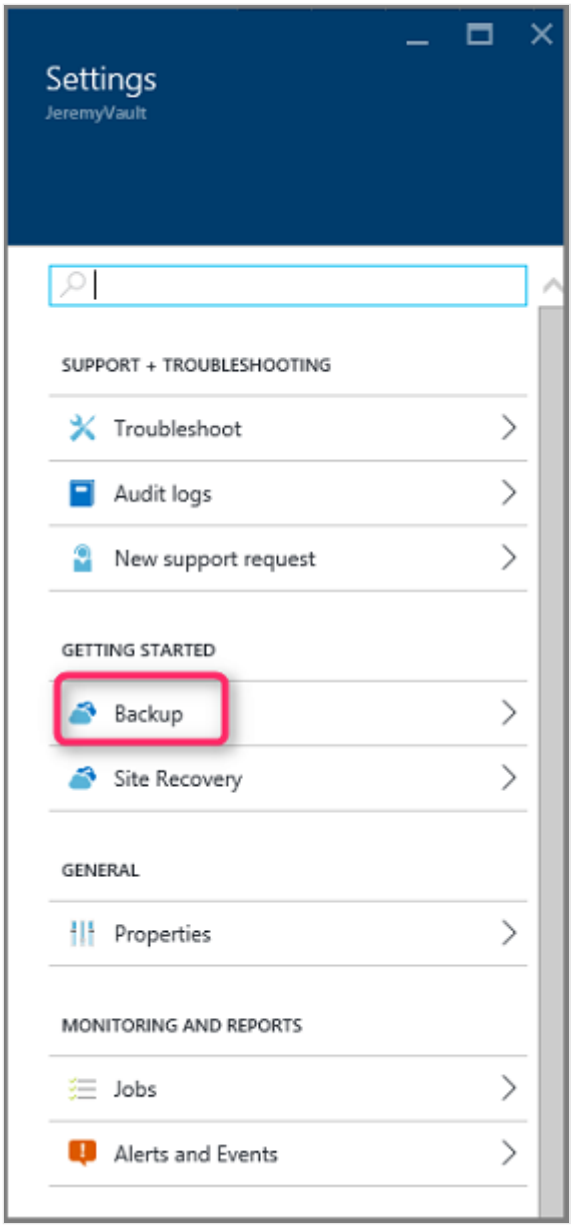
3. From the list of Recovery Services vaults, select a vault.

   The selected vault dashboard opens.



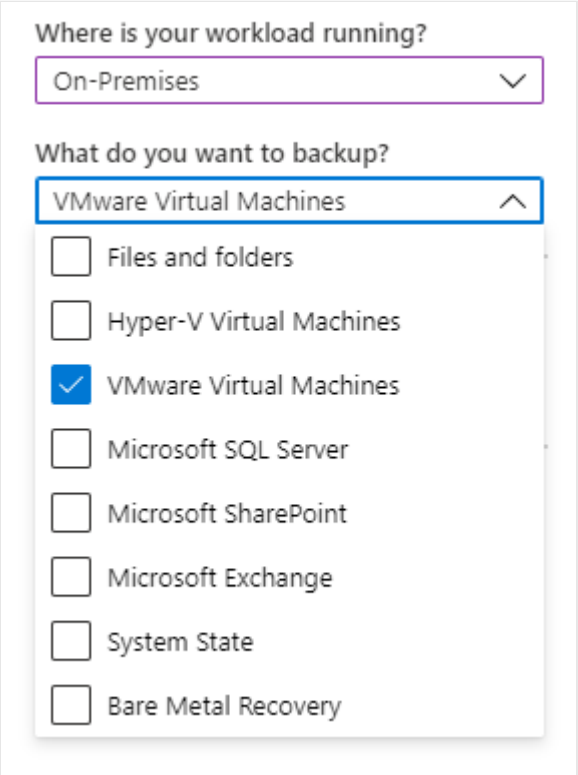
   The **Settings** option opens by default. If closed, select **Settings** to open it.

4. Select **Backup** to open the **Getting Started** wizard.



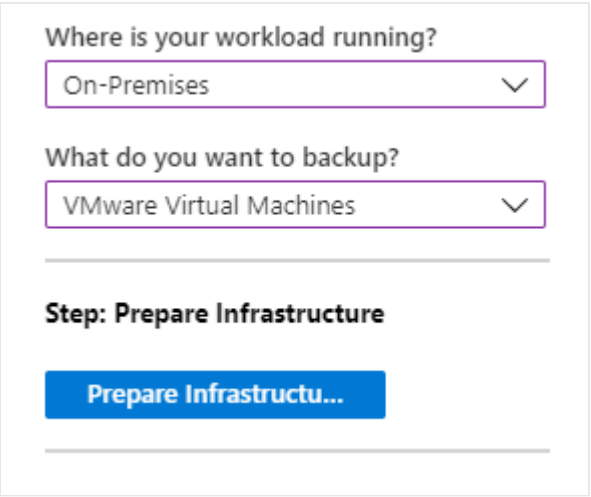
5. In the window that opens:

   a. From the **Where is your workload running?** menu, select **On-Premises**.



b. From the **What do you want to back up?** menu, select the workloads you want to protect by using Azure Backup Server.

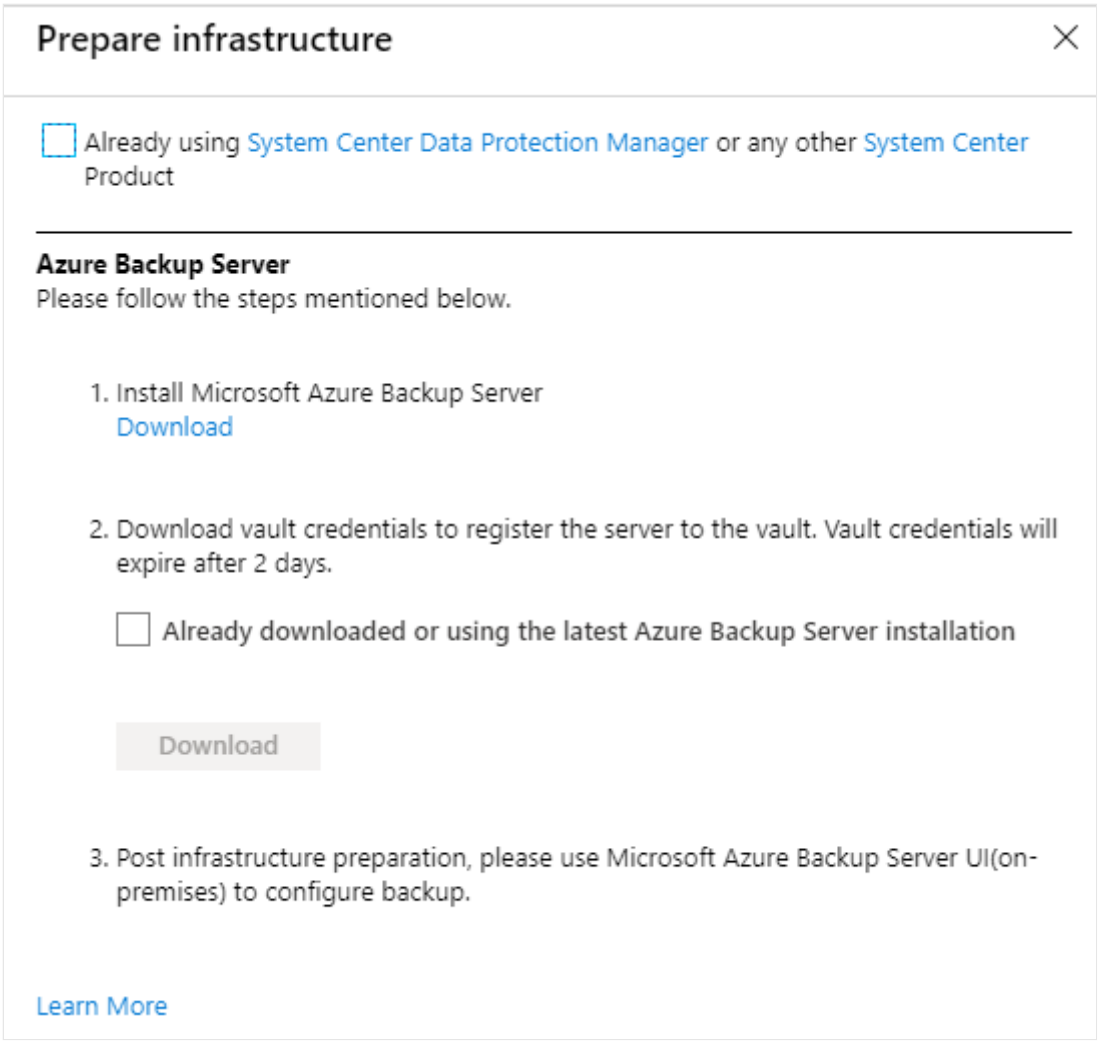
c. Select **Prepare Infrastructure** to download and install Azure Backup Server and the vault credentials.



6. In the **Prepare infrastructure** window that opens:

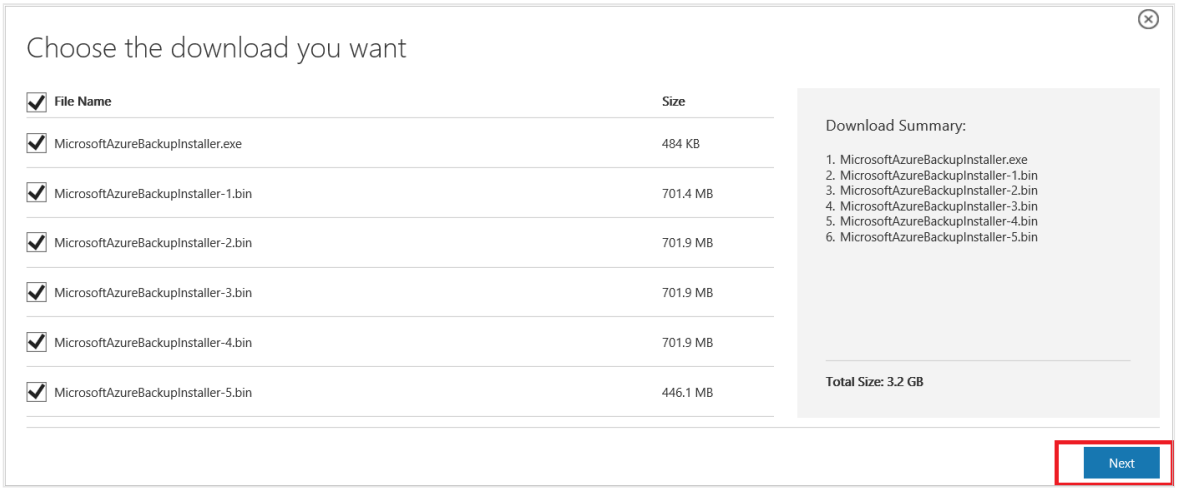
a. Select the **Download** link to install Azure Backup Server.

b. Select **Already downloaded or using the latest Azure Backup Server installation**, then **Download** to download the vault credentials. You use these credentials when you register the Azure Backup Server to the Recovery Services vault. The links take you to the Download Center, where you download the software package.



7. On the download page, select all the files and select **Next**.

> **Note**
>
> You must download all the files to the same folder. Because the download size of the files together is greater than 3 GB, it might take up to 60 minutes for the download to complete.

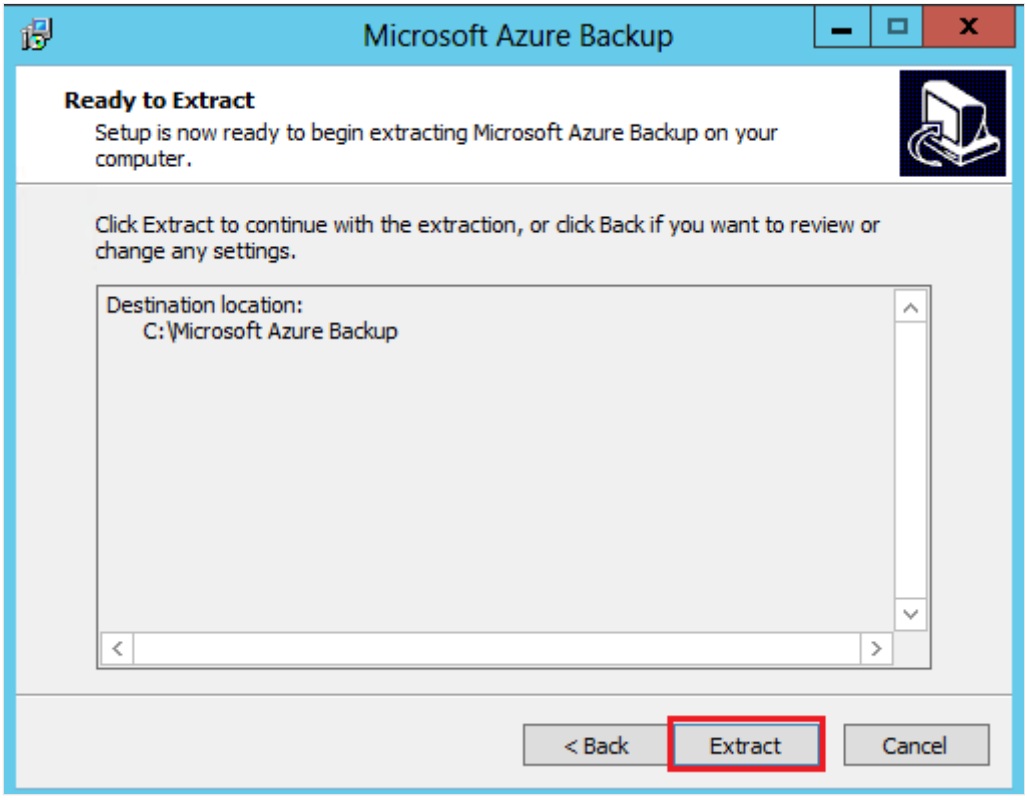


Extract the software package

If you downloaded the software package to a different server, copy the files to the VM you created to deploy Azure Backup Server.

> ⚠ **Warning**
>
> At least 4 GB of free space is required to extract the setup files.

1. After you downloaded all the files, double-click **MicrosoftAzureBackupInstaller.exe** to open the **Microsoft Azure Backup** setup wizard, then select **Next**.
2. Select the location to extract the files to and select **Next**.
3. Select **Extract** to begin the extraction process.



4. Once extracted, select the option to **Execute setup.exe**, then select **Finish**.

> 💡 **Tip**
>
> - You can also locate the setup.exe file from the folder where you extracted the software package.
> - To use your own SQL Server instance, ensure that you're using the supported SQL Server versions - SQL Server 2022 and 2019.

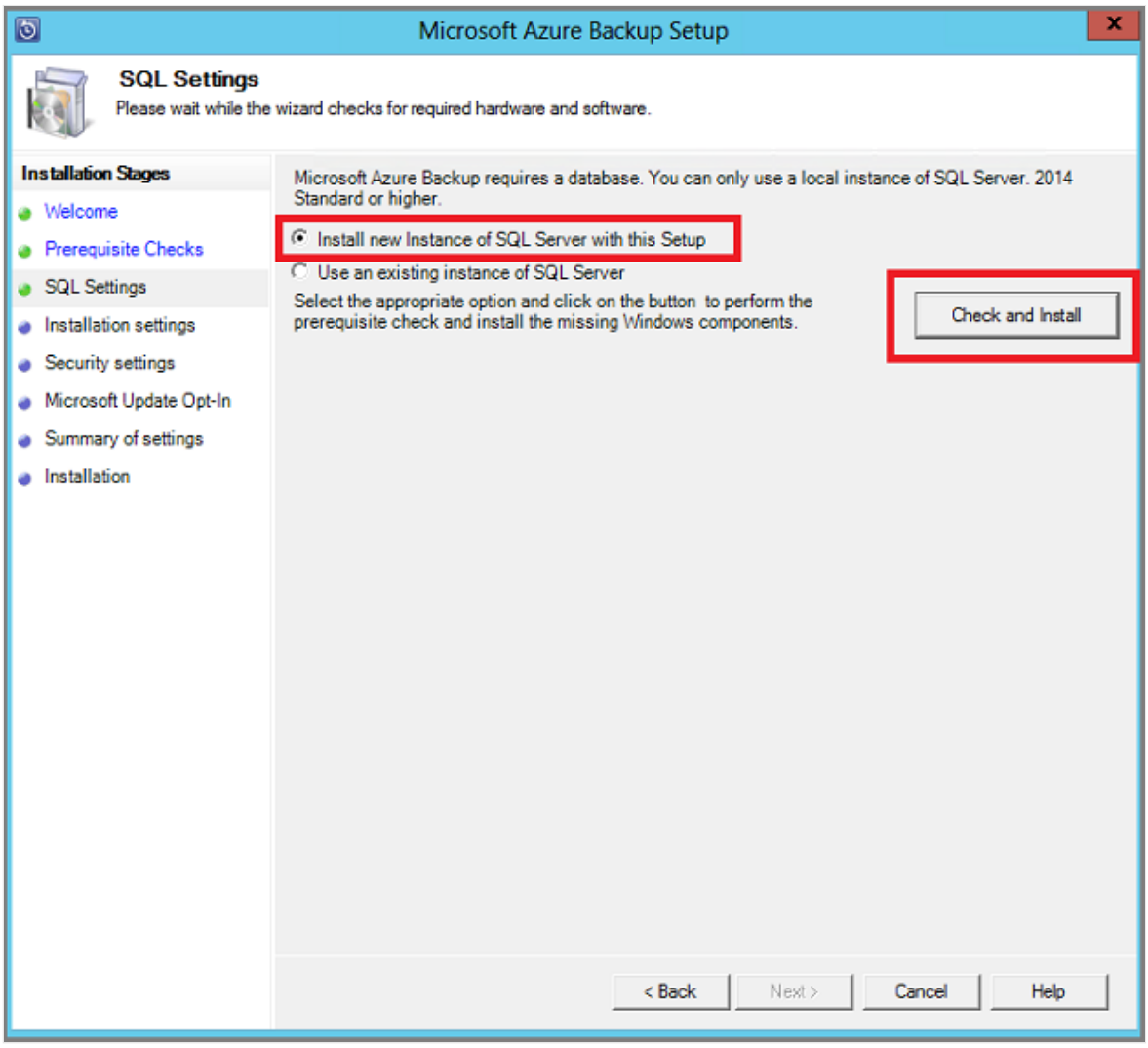
Install the software package

1. On the setup window under **Install**, select **Microsoft Azure Backup** to open the setup wizard and accept any licensing terms from the list that appears.

2. On the **Welcome** screen, select **Next** to continue to the **Prerequisite Checks** page.

3. To determine if the hardware and software meet the prerequisites for Azure Backup Server, select **Check Again**. If met successfully, select **Next**.

4. The Azure Backup Server installation package comes bundled with the appropriate SQL Server binaries that are needed. When you start a new Azure Backup Server installation, select the **Install new Instance of SQL Server with this Setup** option. Then select **Check and Install**.



> **Note**
>
> If you want to use your own SQL Server instance, the supported SQL Server versions are SQL Server 2014 SP1 or higher, 2016, and 2017. All SQL Server versions should be Standard or Enterprise 64-bit. The instance used by Azure

Backup Server must be local only; it can't be remote. If you use an existing SQL Server instance for Azure Backup Server, the setup only supports the use of *named instances* of SQL Server.

If a failure occurs with a recommendation to restart the machine, do so, and select **Check Again**. For any SQL Server configuration issues, reconfigure SQL Server according to the SQL Server guidelines. Then retry to install or upgrade Azure Backup Server using the existing instance of SQL Server.

Manual configuration

When you use your own SQL Server instance, make sure you add builtin\Administrators to the sysadmin role to the main database sysadmin role.

Configure reporting services with SQL Server 2019 or 2022

If you use your instance of SQL Server, you must configure SQL Server Reporting Services (SSRS) manually. After configuring SSRS, make sure to set the **IsInitialized** property of SSRS to **True**. When set to **True**, Azure Backup Server assumes that SSRS is already configured and skips the SSRS configuration.

To check the SSRS configuration status, run:

PowerShell

```
$configset =Get-WmiObject –namespace
"root\Microsoft\SqlServer\ReportServer\RS_SSRS\v14\Admin" -class
MSReportServer_ConfigurationSetting -ComputerName localhost

$configset.IsInitialized
```

Use the following values for SSRS configuration:

- **Service Account**: **Use built-in account** should be **Network Service**.
- **Web Service URL**: **Virtual Directory** should be **ReportServer_<SQLInstanceName>**.
- **Database**: **DatabaseName** should be **ReportServer$<SQLInstanceName>**.
- **Web Portal URL**: **Virtual Directory** should be **Reports_<SQLInstanceName>**.

Learn more about SSRS configuration.

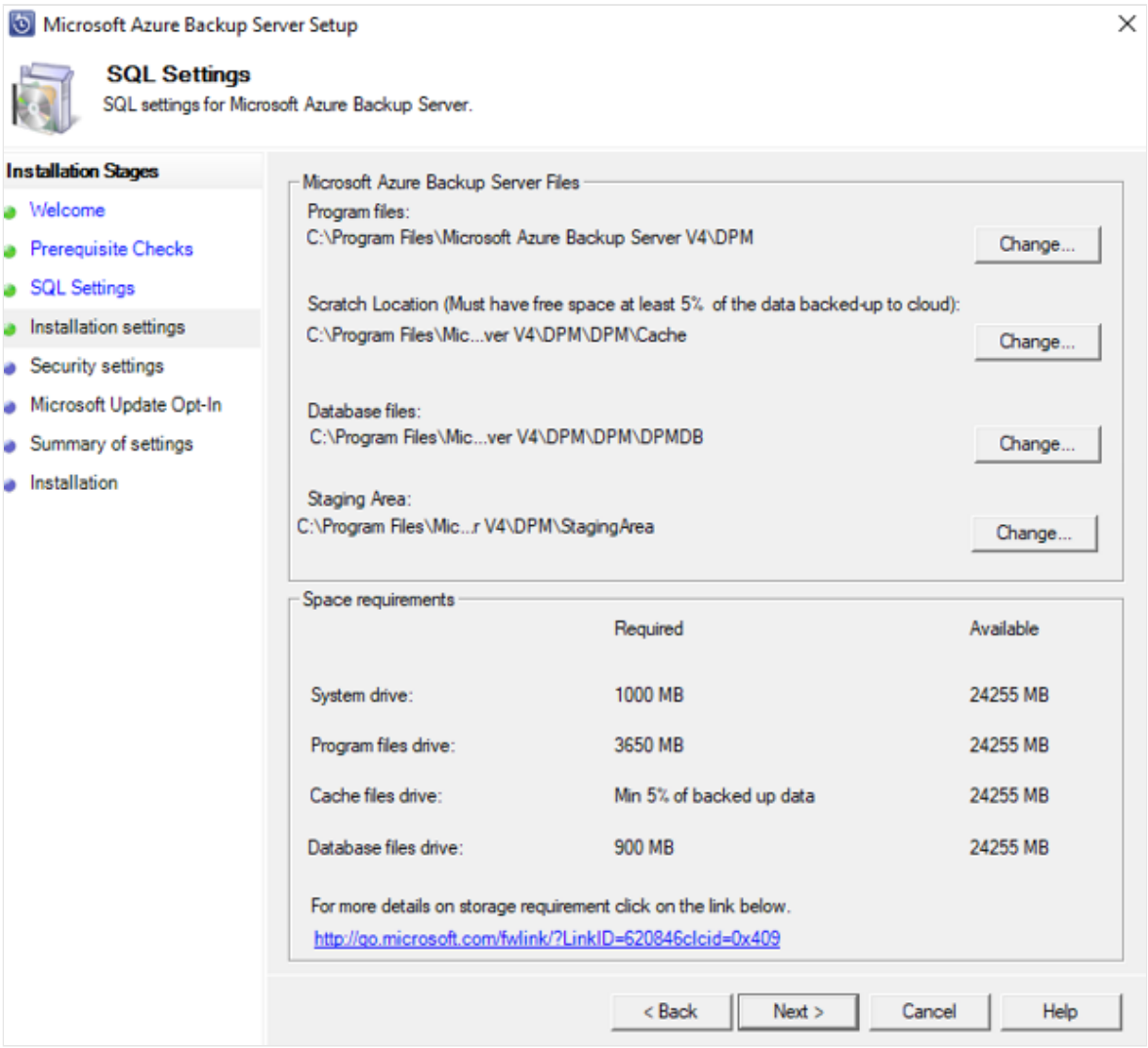
ⓘ **Note**

> [Microsoft Online Services Terms](#) (OST) governs the licensing for SQL Server used as the database for Azure Backup Server. According to OST, only use SQL Server bundled with Azure Backup Server as the database for Azure Backup Server.

5. After the installation is successful, select **Next**.

6. Provide a location for installing Microsoft Azure Backup Server files, and select **Next**.

> **Note**
>
> The scratch location is required for backup to Azure. Ensure the scratch location is at least 5% of the data planned for backing up to the cloud. For disk protection, separate disks need configuring after the installation finishes. For more information about storage pools, see [Configure storage pools and disk storage](#).



7. Provide a strong password for restricted local user accounts, and select **Next**.

8. Select whether you want to use Microsoft Update to check for updates, and select **Next**.

   > **Note**
   >
   > We recommend having Windows Update redirect to Microsoft Update, which offers security and important updates for Windows and other products like Azure Backup Server.

9. Review the **Summary of Settings**, and select **Install**.

   The installation happens in phases.

   - The first phase installs the Microsoft Azure Recovery Services Agent.
   - The second phase checks for internet connectivity. If available, you can continue with the installation. If not available, you must provide proxy details to connect to the internet.
   - The final phase checks the prerequisite software. If not installed, any missing software gets installed along with the Microsoft Azure Recovery Services Agent.

10. Select **Browse** to locate your vault credentials to register the machine to the Recovery Services vault, then select **Next**.

11. Select a passphrase to encrypt or decrypt the data sent between Azure and your premises.

    > **Tip**
    >
    > You can automatically generate a passphrase or provide your minimum 16-character passphrase.

12. Enter the location to save the passphrase, then select **Next** to register the server.

    > **Important**
    >
    > Save the passphrase to a safe location other than the local server. We strongly recommend using the Azure Key Vault to store the passphrase.

    After the Microsoft Azure Recovery Services Agent setup finishes, the installation step moves on to the installation and configuration of SQL Server and the Azure

Backup Server components.

13. After the installation step finishes, select **Close**.

Install Update Rollup 2 for Microsoft Azure Backup Server (MABS) version 3

Installing the Update Rollup 2 for Microsoft Azure Backup Server (MABS) version 3 is mandatory for protecting the workloads. You can find the bug fixes and installation instructions in the knowledge base article.

Add storage to Azure Backup Server

Azure Backup Server v3 supports Modern Backup Storage that offers:

- Storage savings of 50%.
- Backups that are three times faster.
- More efficient storage.
- Workload-aware storage.

Volumes in Azure Backup Server

Add the data disks with the Azure Backup Server VM's required storage capacity if not already added.

Azure Backup Server only accepts storage volumes. When you add a volume, Azure Backup Server formats the volume to Resilient File System (ReFS), which Modern Backup Storage requires.

Add volumes to Azure Backup Server disk storage

1. In the **Management** pane, rescan the storage, then select **Add**.
2. Select from the available volumes to add to the storage pool.
3. After you add the available volumes, give them a friendly name to help you manage them.
4. Select **OK** to format these volumes to ReFS so that Azure Backup Server can use Modern Backup Storage benefits.

Upgrade to Azure Backup Server V4 from Azure Backup Server V3

If you're already using Azure Backup Server V3 to back up AVS VMs, you can upgrade to Azure Backup Server V4 to get access to the latest features and bug fixes.

Next steps

Now that you learned how to set up Azure Backup Server for Azure VMware Solution, use the following resources to learn more.

- Configuring backups for your Azure VMware Solution VMs.
- Protecting your Azure VMware Solution VMs with Microsoft Defender for Cloud integration.

Back up Azure VMware Solution VMs with Azure Backup Server

Article • 12/21/2023

This article shows you how to back up VMware virtual machines (VMs) running on Azure VMware Solution with Azure Backup Server. First, thoroughly go through Set up Microsoft Azure Backup Server for Azure VMware Solution.

Then, walk through all of the necessary procedures to:

- ✓ Set up a secure channel so that Azure Backup Server can communicate with VMware vCenter Server over HTTPS.
- ✓ Add the account credentials to Azure Backup Server.
- ✓ Add the vCenter Server to Azure Backup Server.
- ✓ Set up a protection group that contains the VMware vSphere VMs you want to back up, specify backup settings, and schedule the backup.

Create a secure connection to the vCenter Server

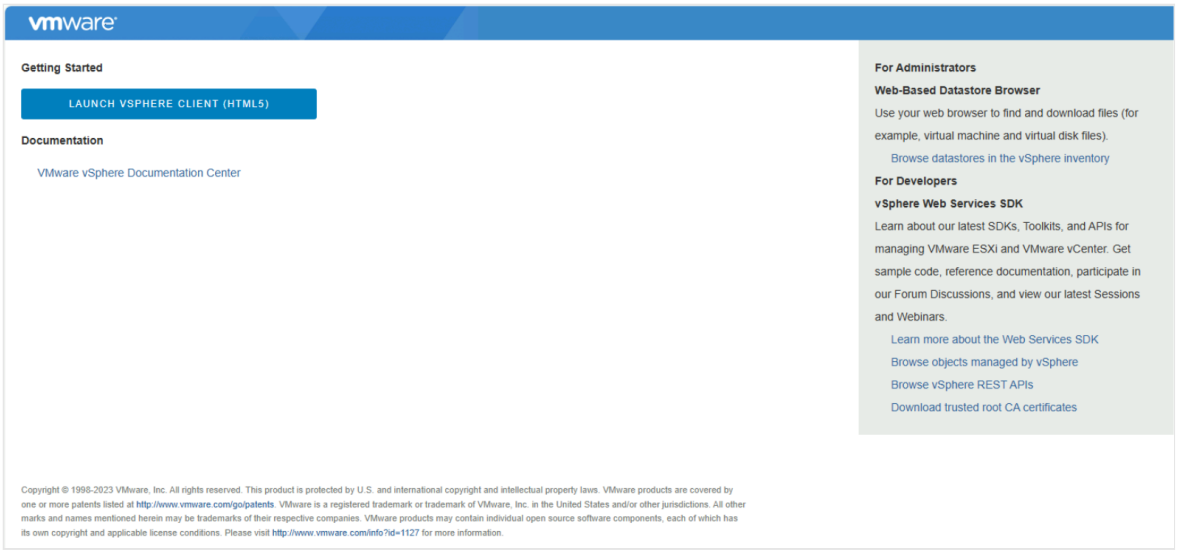
By default, Azure Backup Server communicates with VMware vCenter Server over HTTPS. To set up the HTTPS connection, download the VMware certificate authority (CA) certificate and import it on the Azure Backup Server.

Set up the certificate

1. In the browser, on the Azure Backup Server machine, enter the vSphere Client URL.

   > ⓘ **Note**
   >
   > If the VMware vSphere Client **Getting Started** page doesn't appear, verify the connection and browser proxy settings and try again.

2. On the VMware vSphere Client **Getting Started** page, select **Download trusted root CA certificates**.



3. Save the **download.zip** file to the Azure Backup Server machine, and then extract its contents to the **certs** folder, which contains the:

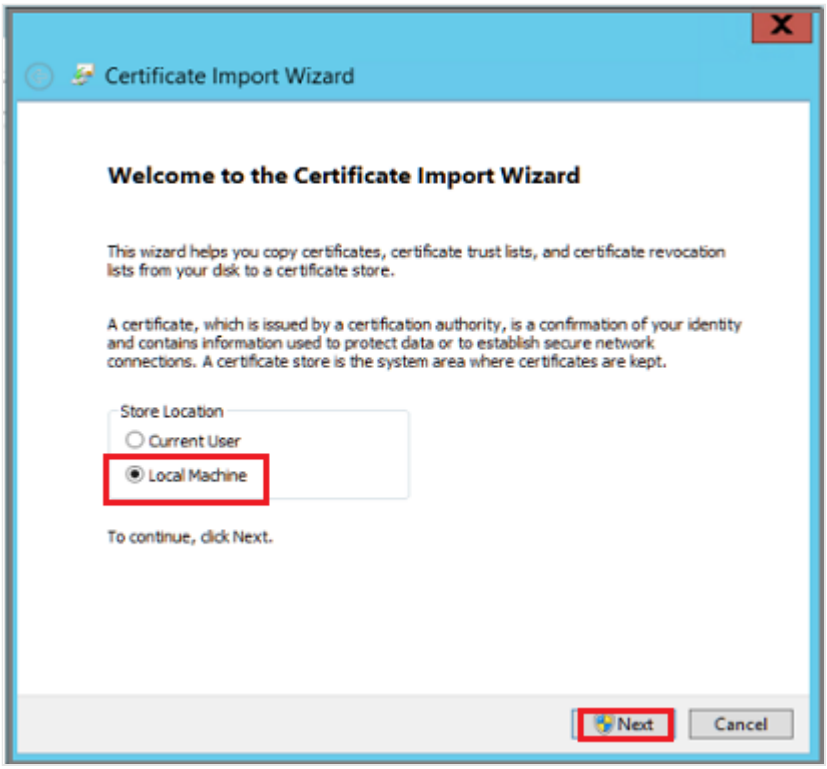
    - Root certificate file with an extension that begins with a numbered sequence like 0.0 and 0.1.
    - CRL file with an extension that begins with a sequence like, .r0 or .r1.

4. In the **certs** folder, right-click the root certificate file and select **Rename** to change the extension to **.crt**.

    The file icon changes to one that represents a root certificate.

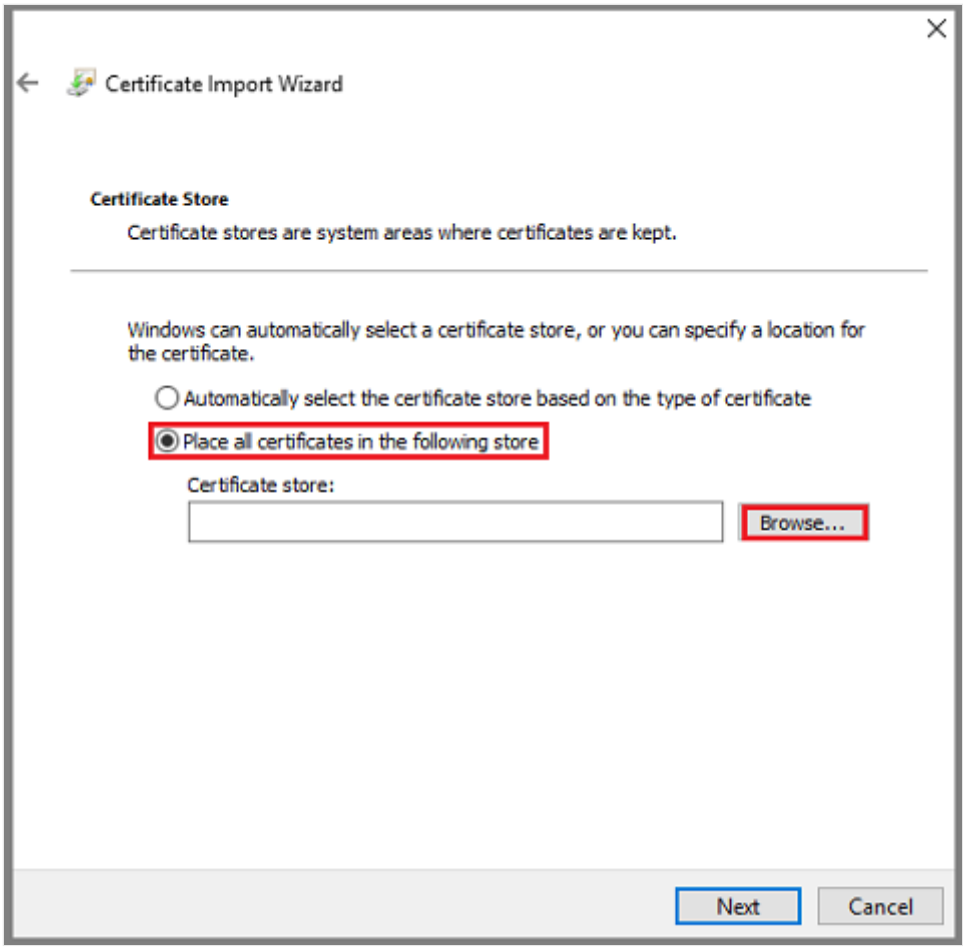
5. Right-click the root certificate, and select **Install Certificate**.

6. In the **Certificate Import Wizard**, select **Local Machine** as the destination for the certificate, and select **Next**.



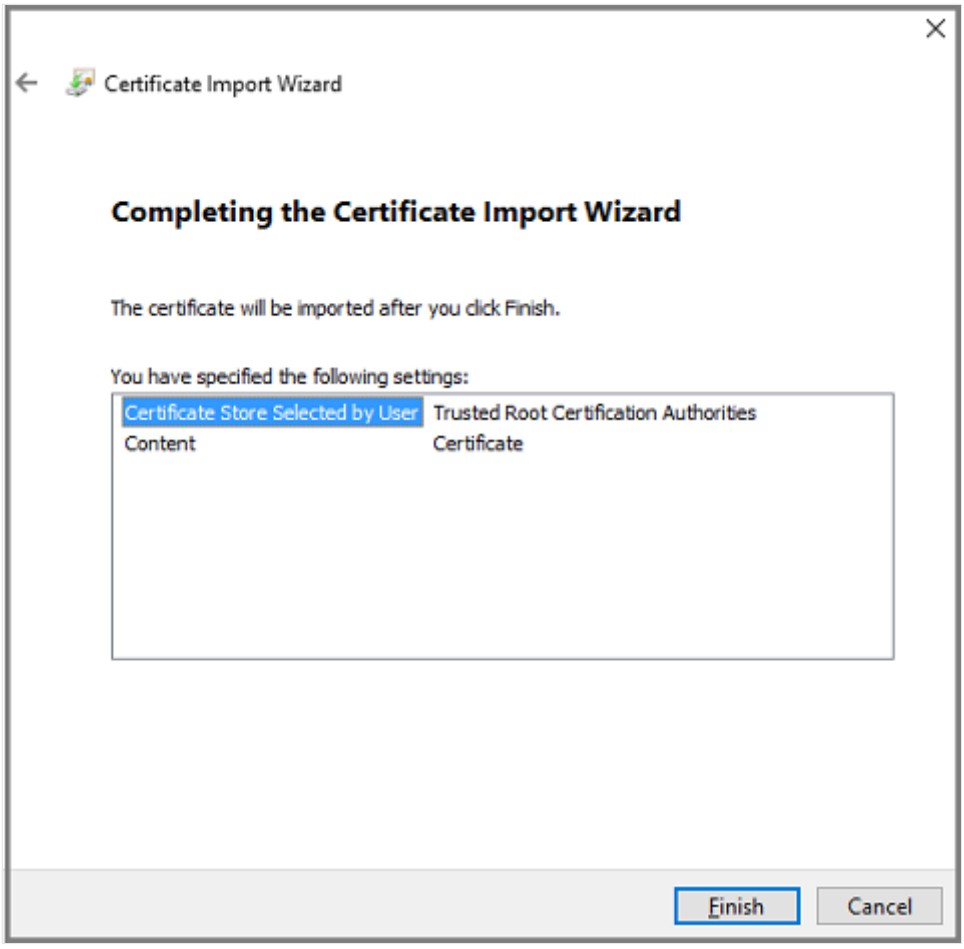
> ⓘ **Note**
>
> If asked, confirm that you want to allow changes to the computer.

7. Select **Place all certificates in the following store**, and select **Browse** to choose the certificate store.



8. Select **Trusted Root Certification Authorities** as the destination folder, and select **OK**.

9. Review the settings, and select **Finish** to start importing the certificate.



10. After the certificate import is confirmed, sign in to the vCenter Server to confirm that your connection is secure.

Enable TLS 1.2 on Azure Backup Server

VMware vSphere 6.7 onwards has TLS enabled as the communication protocol.

1. Copy the following registry settings, and paste them into Notepad. Then save the file as TLS.REG without the .txt extension.

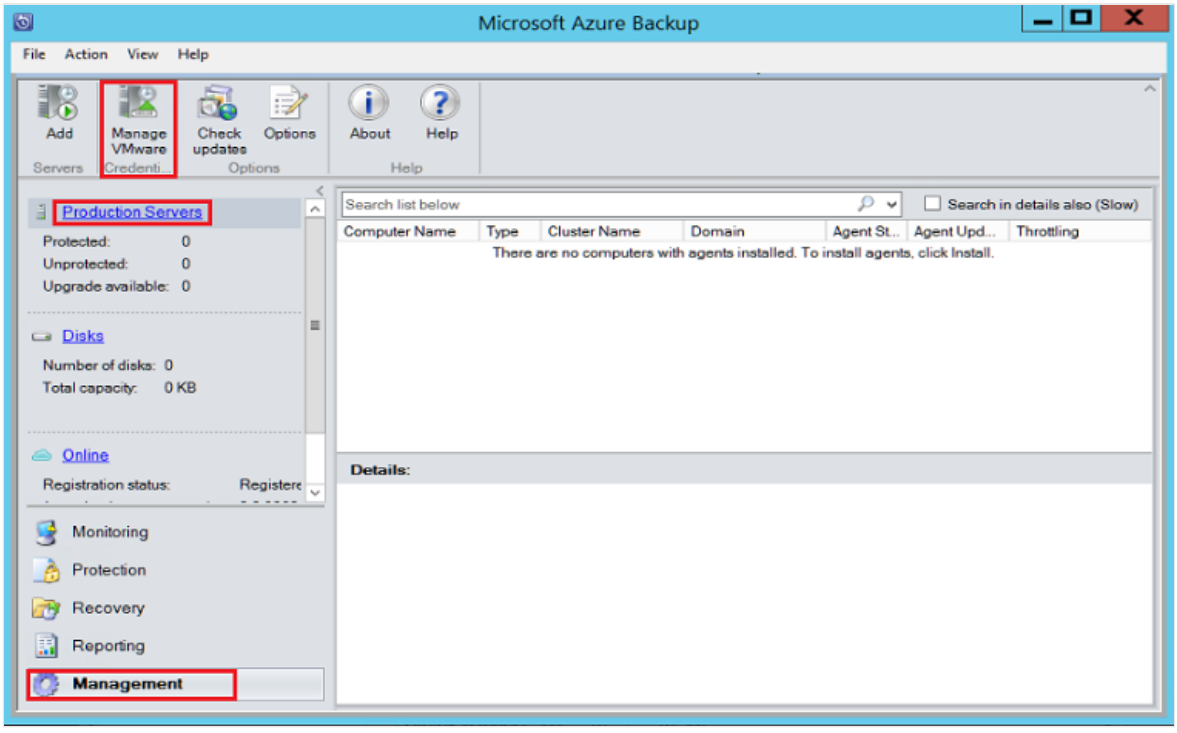
```text
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\.NETFramework\v2.0.50727]

   "SystemDefaultTlsVersions"=dword:00000001

   "SchUseStrongCrypto"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\.NETFramework\v4.0.30319]

   "SystemDefaultTlsVersions"=dword:00000001
```

```
   "SchUseStrongCrypto"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v2.0.50727]

   "SystemDefaultTlsVersions"=dword:00000001

   "SchUseStrongCrypto"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319]

   "SystemDefaultTlsVersions"=dword:00000001

   "SchUseStrongCrypto"=dword:00000001
```

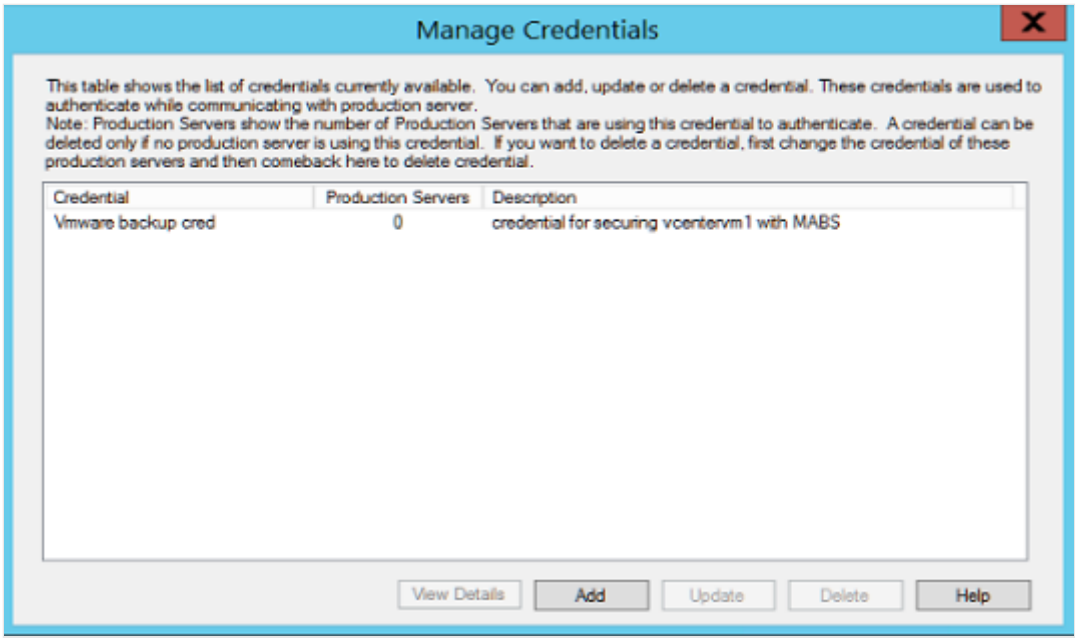
2. Right-click the TLS.REG file, and select **Merge** or **Open** to add the settings to the registry.

Add the account on Azure Backup Server

1. Open Azure Backup Server, and in the Azure Backup Server console, select **Management** > **Production Servers** > **Manage VMware**.

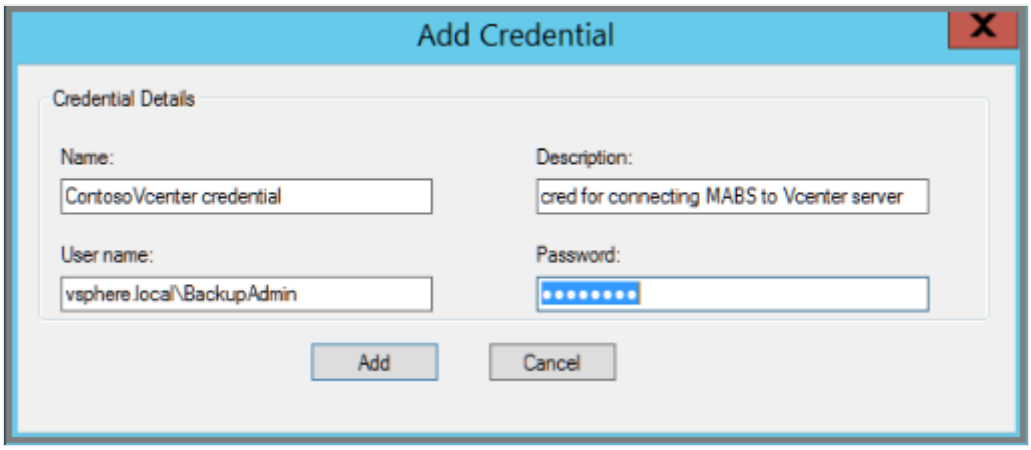


2. In the **Manage Credentials** dialog box, select **Add**.

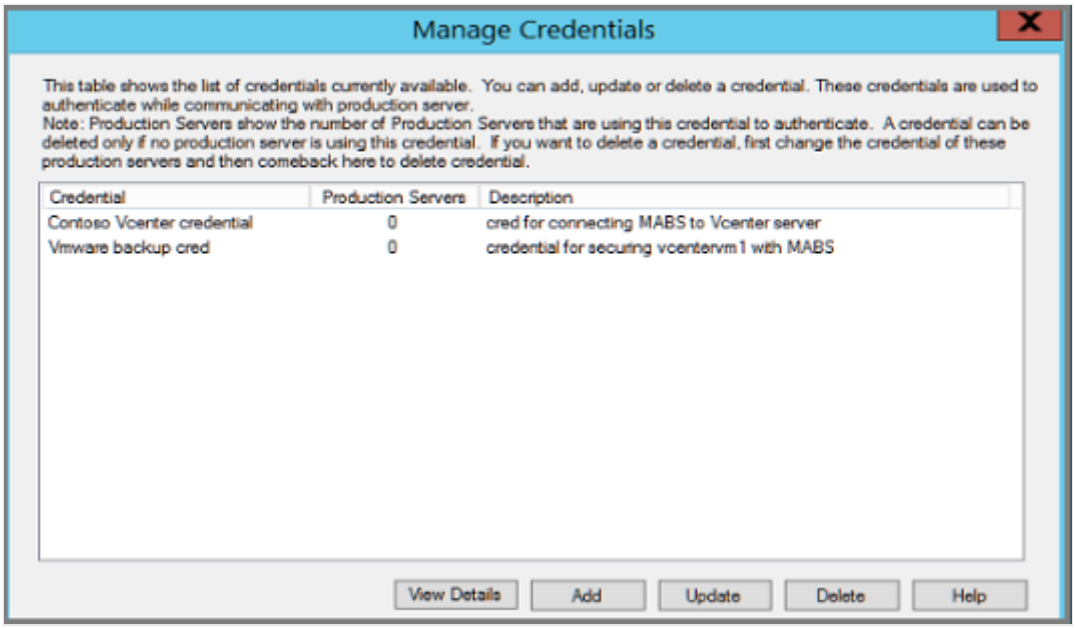


3. In the **Add Credential** dialog box, enter a name and a description for the new credential. Specify the user name and password you defined on the VMware server.

> ⓘ **Note**
>
> If the VMware vSphere virtual machine and Azure Backup Server aren't in the same domain, specify the domain in the **User name** box.

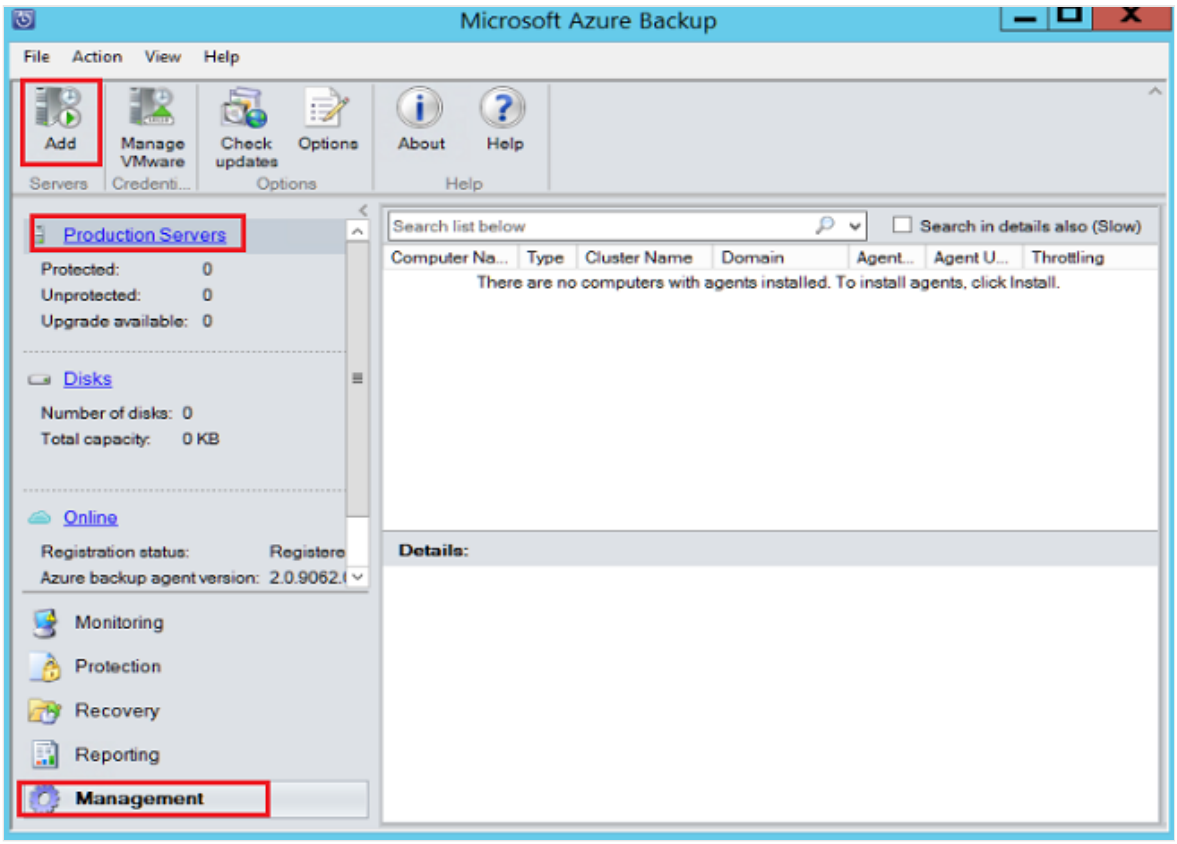


4. Select **Add** to add the new credential.

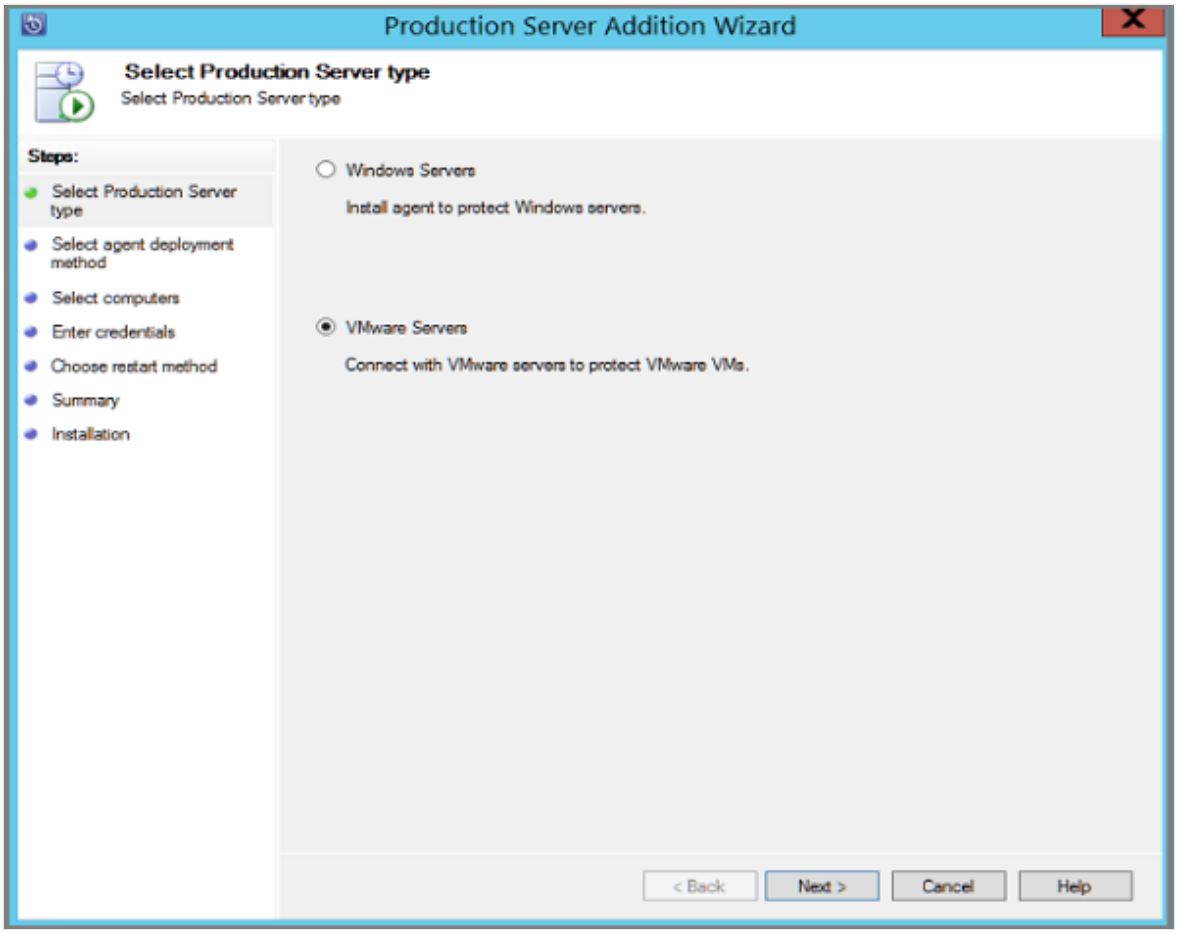


Add the vCenter Server to Azure Backup Server

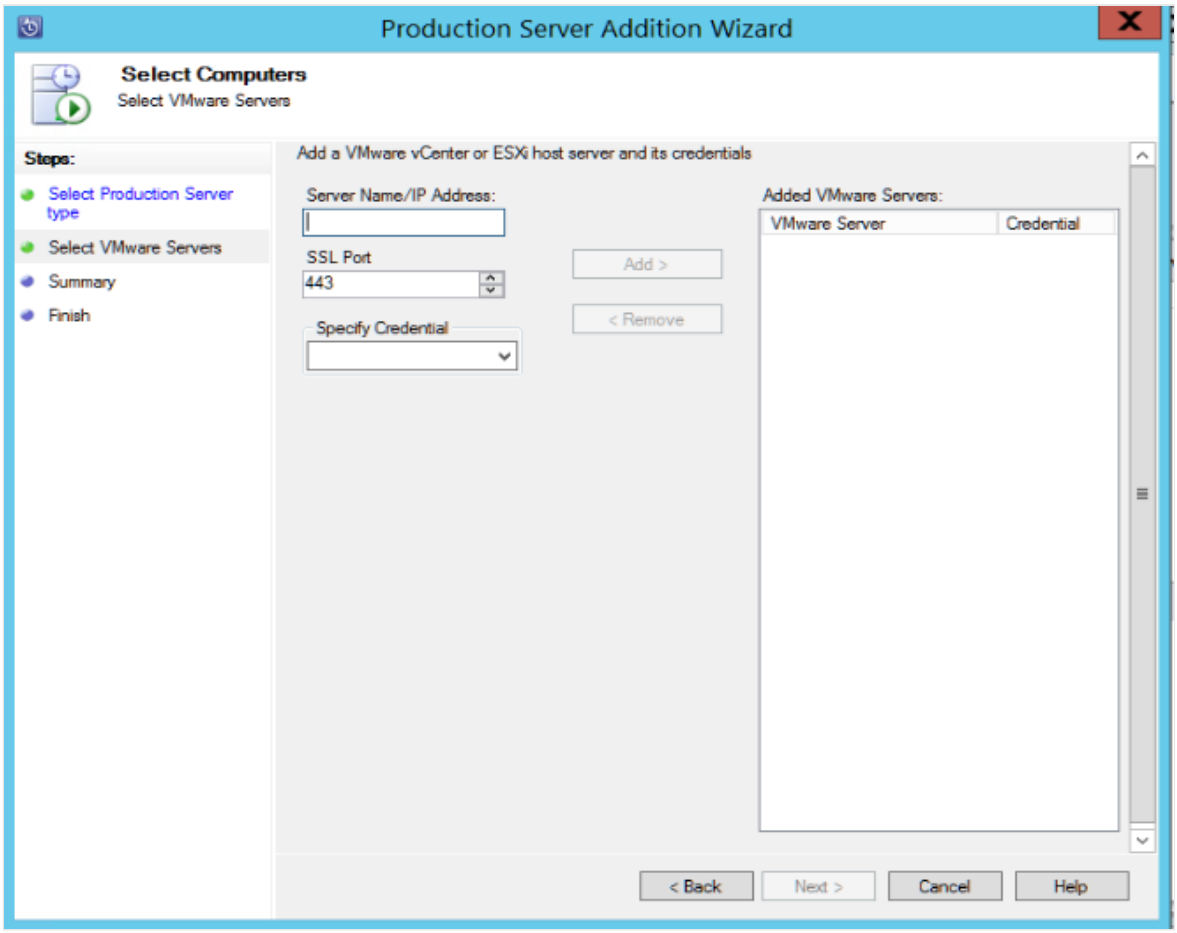
1. In the Azure Backup Server console, select **Management** > **Production Servers** > **Add**.



2. Select **VMware Servers**, and select **Next**.



3. Specify the IP address of the vCenter Server.

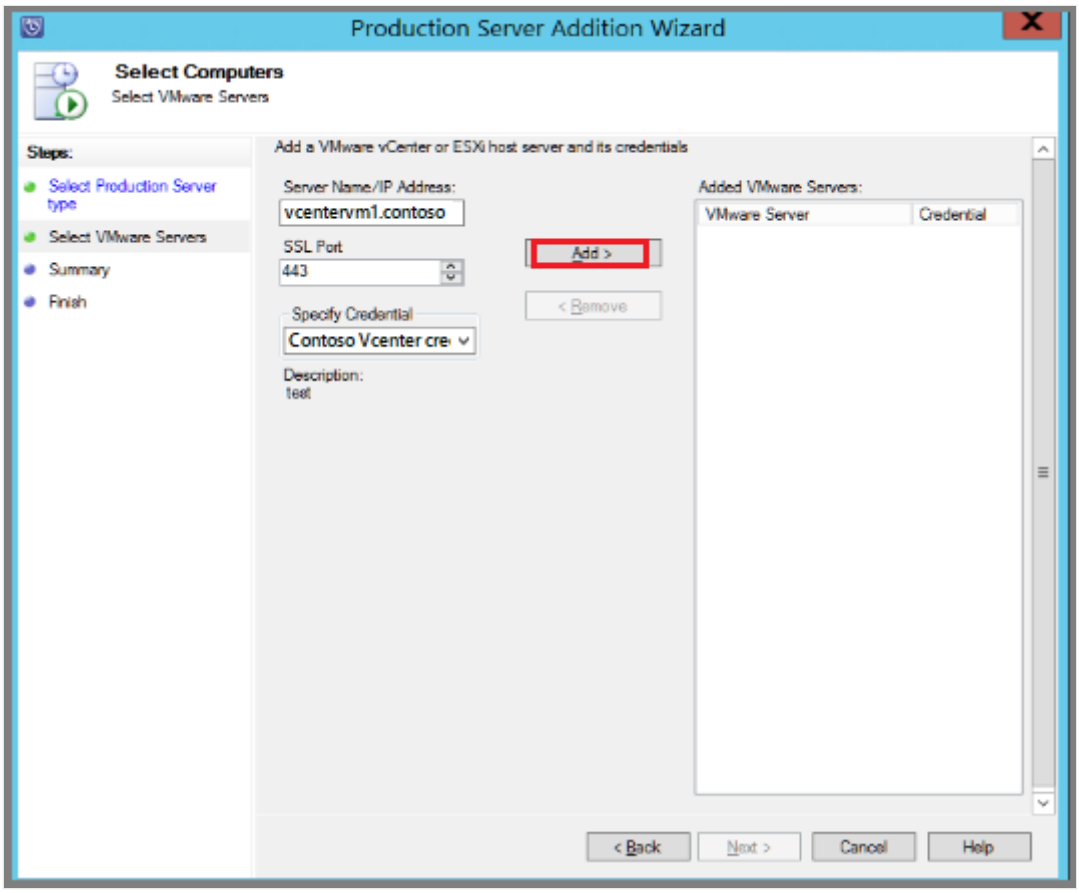


4. In the **SSL Port** box, enter the port used to communicate with the vCenter Server.

> **Tip**
>
> Port 443 is the default port, but you can change it if your vCenter Server listens on a different port.

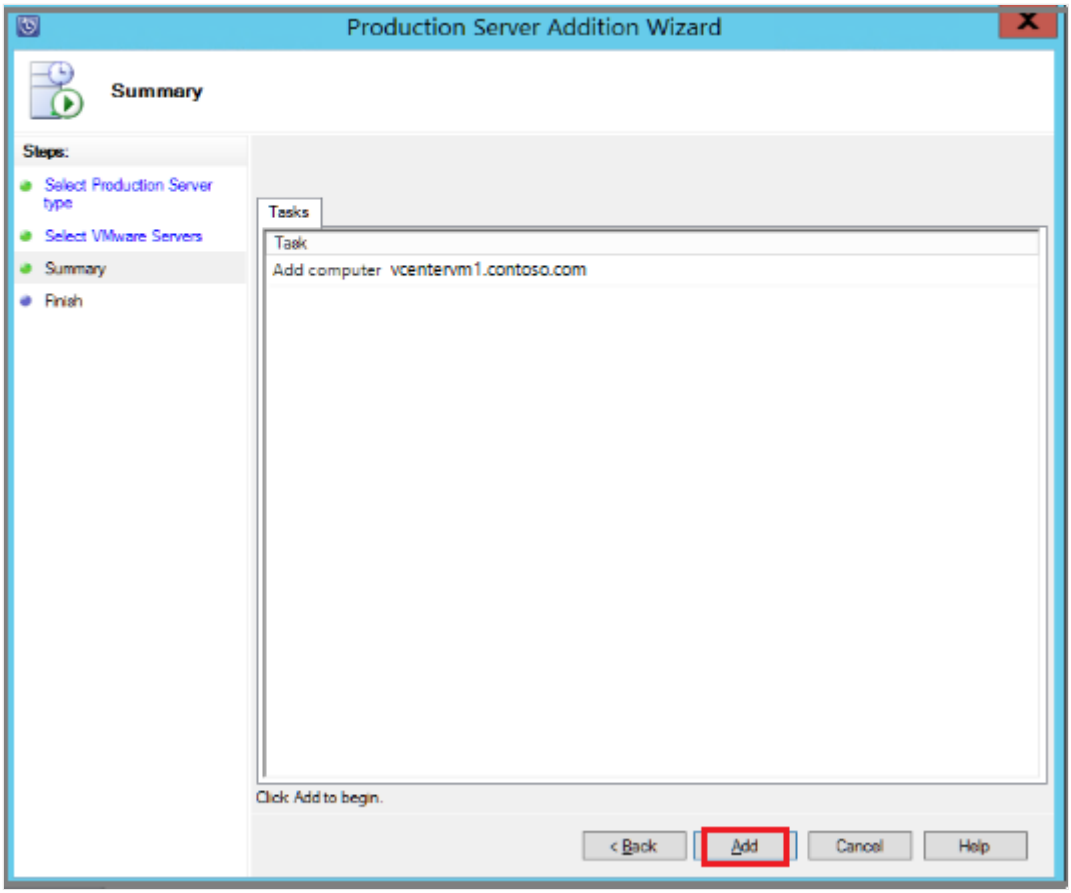
5. In the **Specify Credential** box, select the credential that you created in the previous section.

6. Select **Add** to add the vCenter Server to the servers list, and select **Next**.

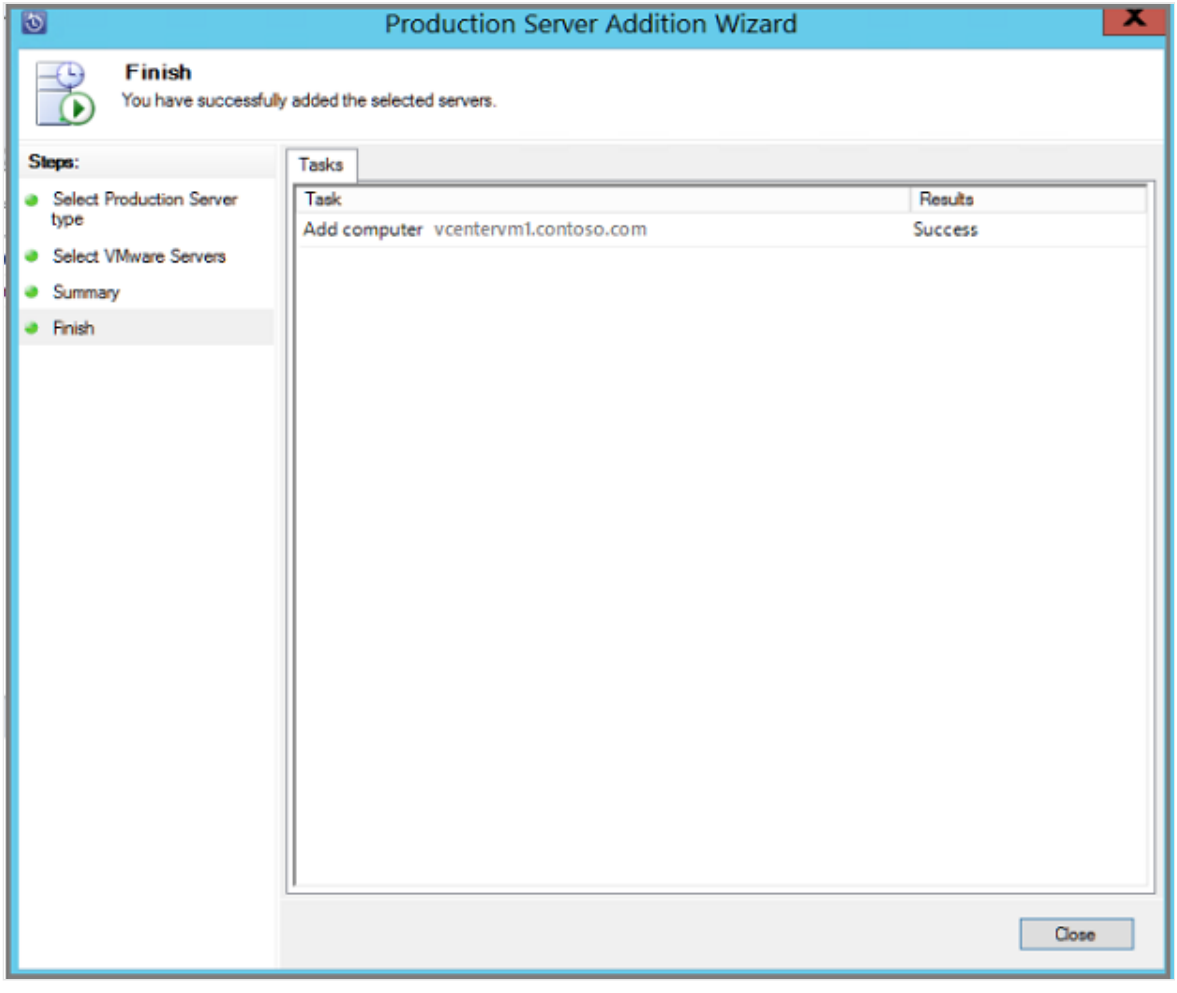


7. On the **Summary** page, select **Add** to add the vCenter Server to Azure Backup Server.

   The new vCenter Server gets added immediately. vCenter Server doesn't need an agent.



8. On the **Finish** page, review the settings, and then select **Close**.



You see the vCenter Server listed under **Production Server** with:

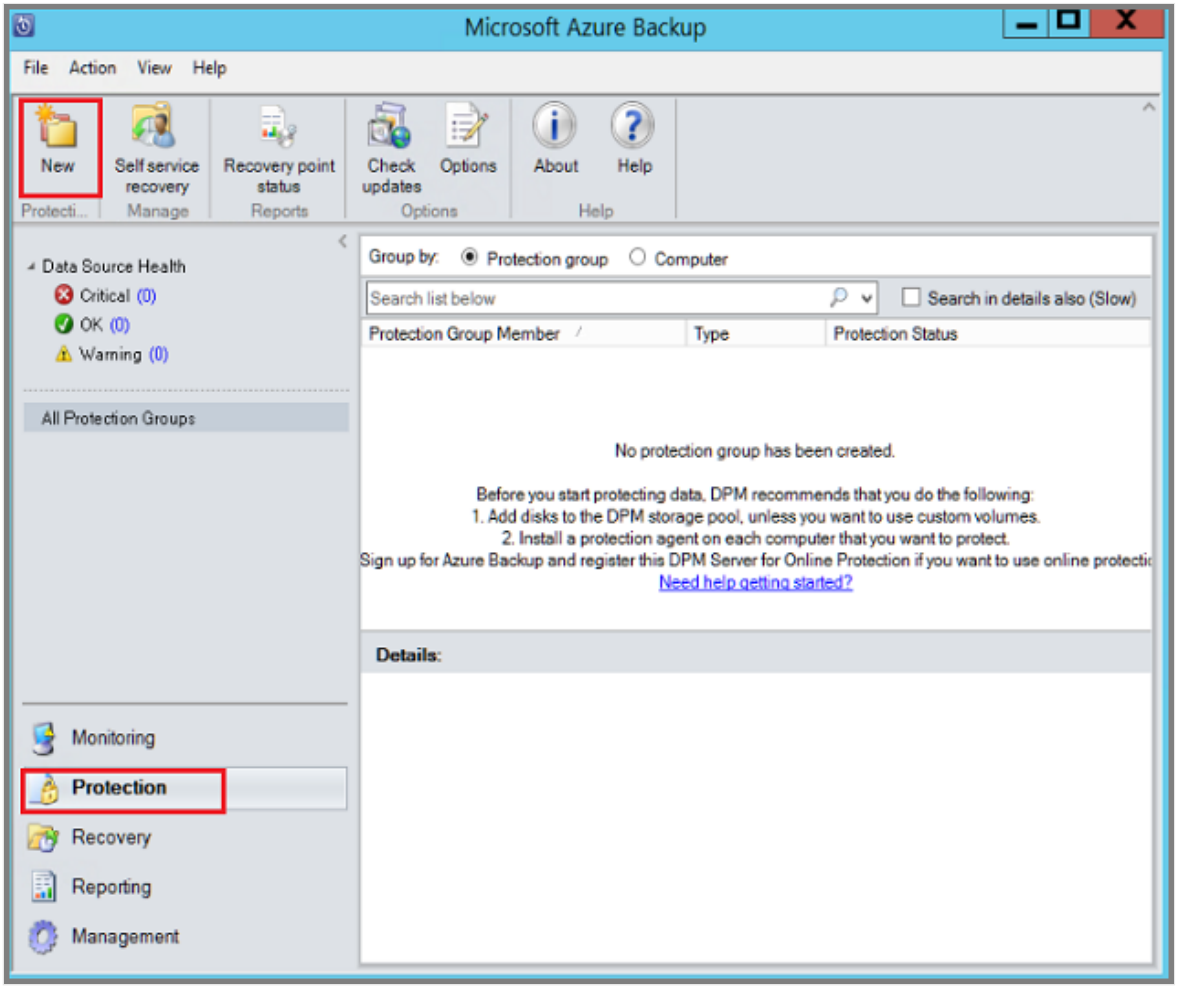
- Type as **VMware Server**
- Agent Status as **OK**

  If you see **Agent Status** as **Unknown**, select **Refresh**.

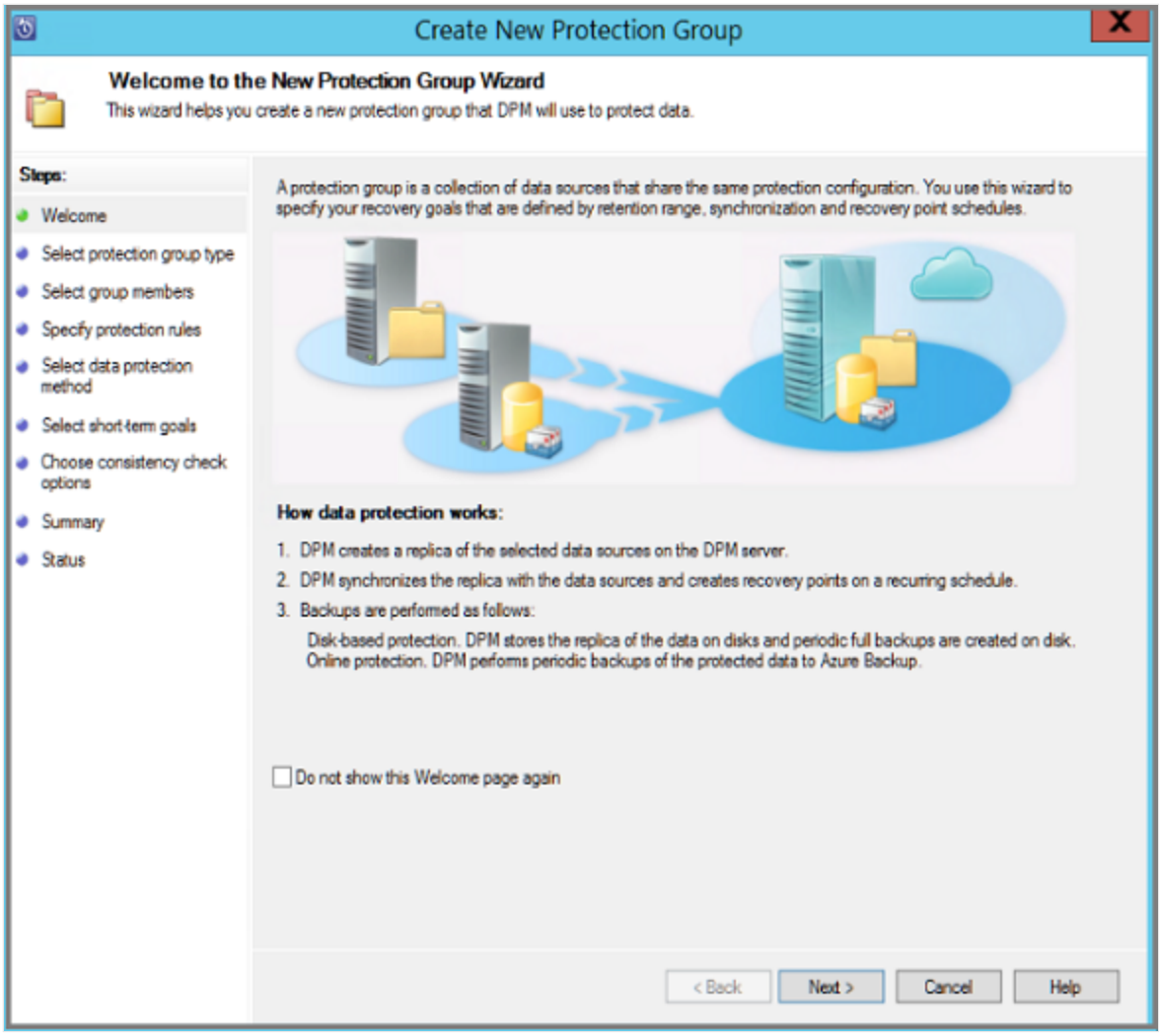
Configure a protection group

Protection groups gather multiple VMs and apply the same data retention and backup settings to all VMs in the group.

1. In the Azure Backup Server console, select **Protection** > **New**.



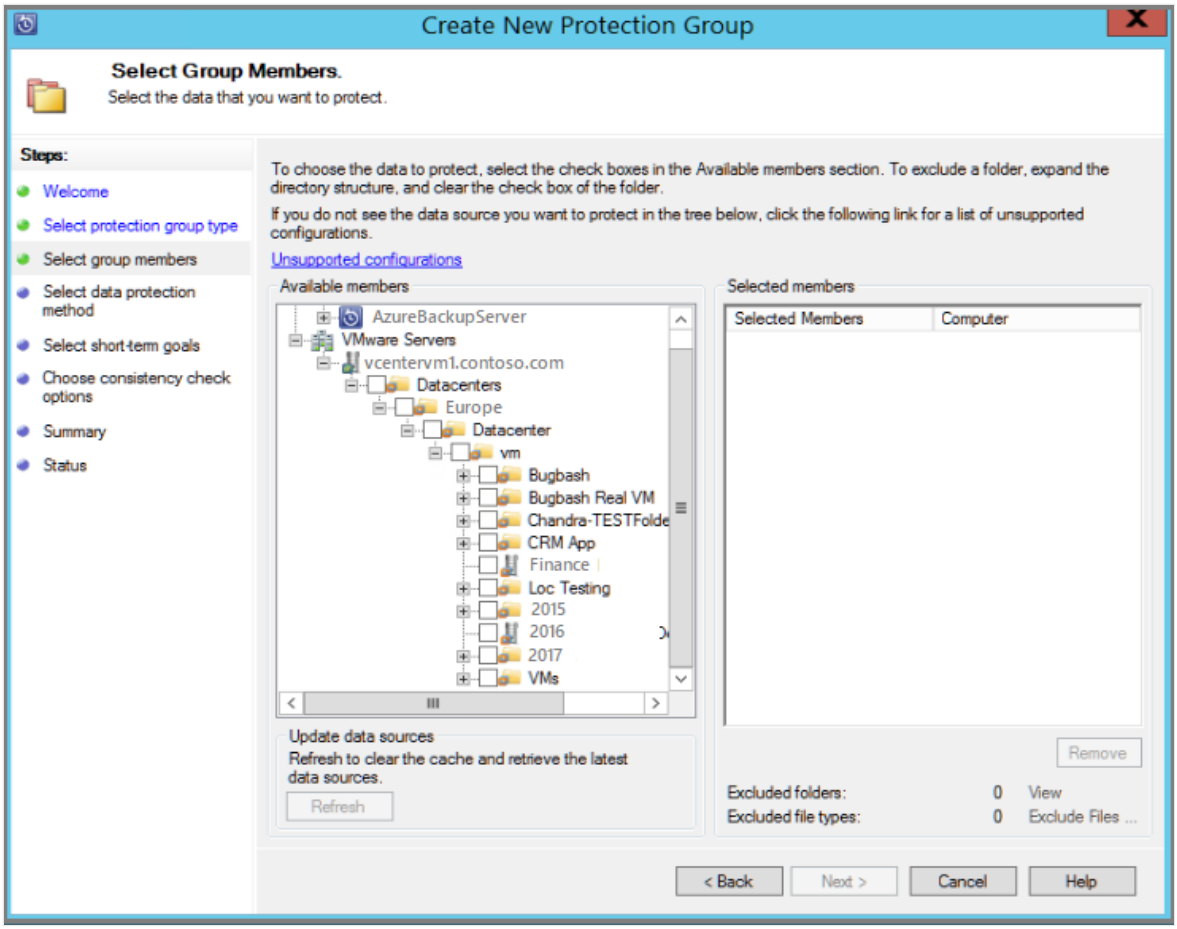
2. On the **Create New Protection Group** wizard welcome page, select **Next**.



3. On the **Select Protection Group Type** page, select **Servers**, and then select **Next**. The **Select Group Members** page appears.

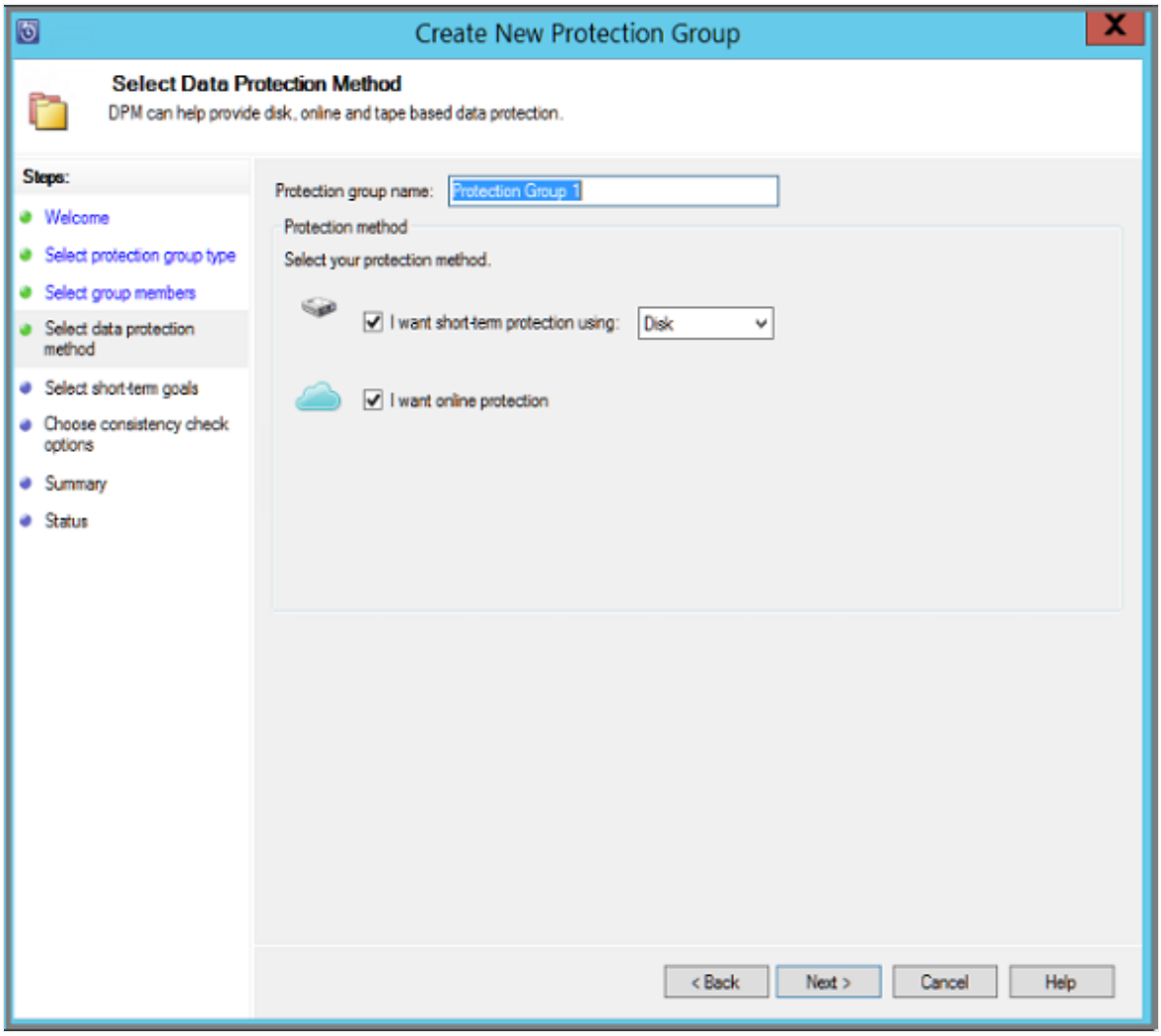
4. On the **Select Group Members** page, select the VMs (or VM folders) that you want to back up, and then select **Next**.

> ⓘ **Note**
>
> When you select a folder or VMs, folders inside that folder are also selected for backup. You can uncheck folders or VMs you don't want to back up. If a VM or folder is already being backed up, you can't select it, which ensures duplicate recovery points aren't created for a VM.



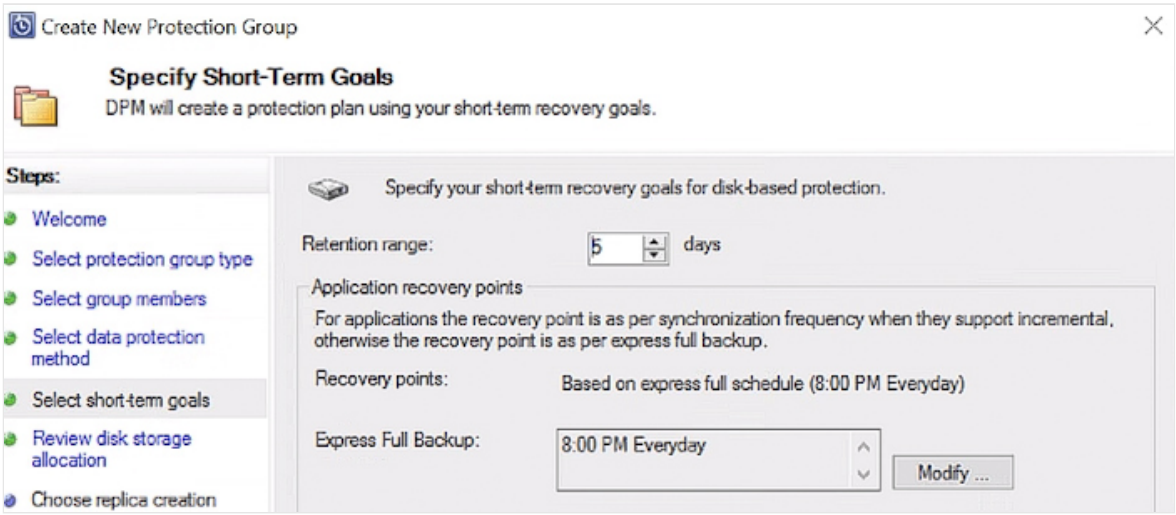
5. On the **Select Data Protection Method** page, enter a name for the protection group and protection settings.

6. Set the short-term protection to **Disk**, enable online protection, and then select **Next**.



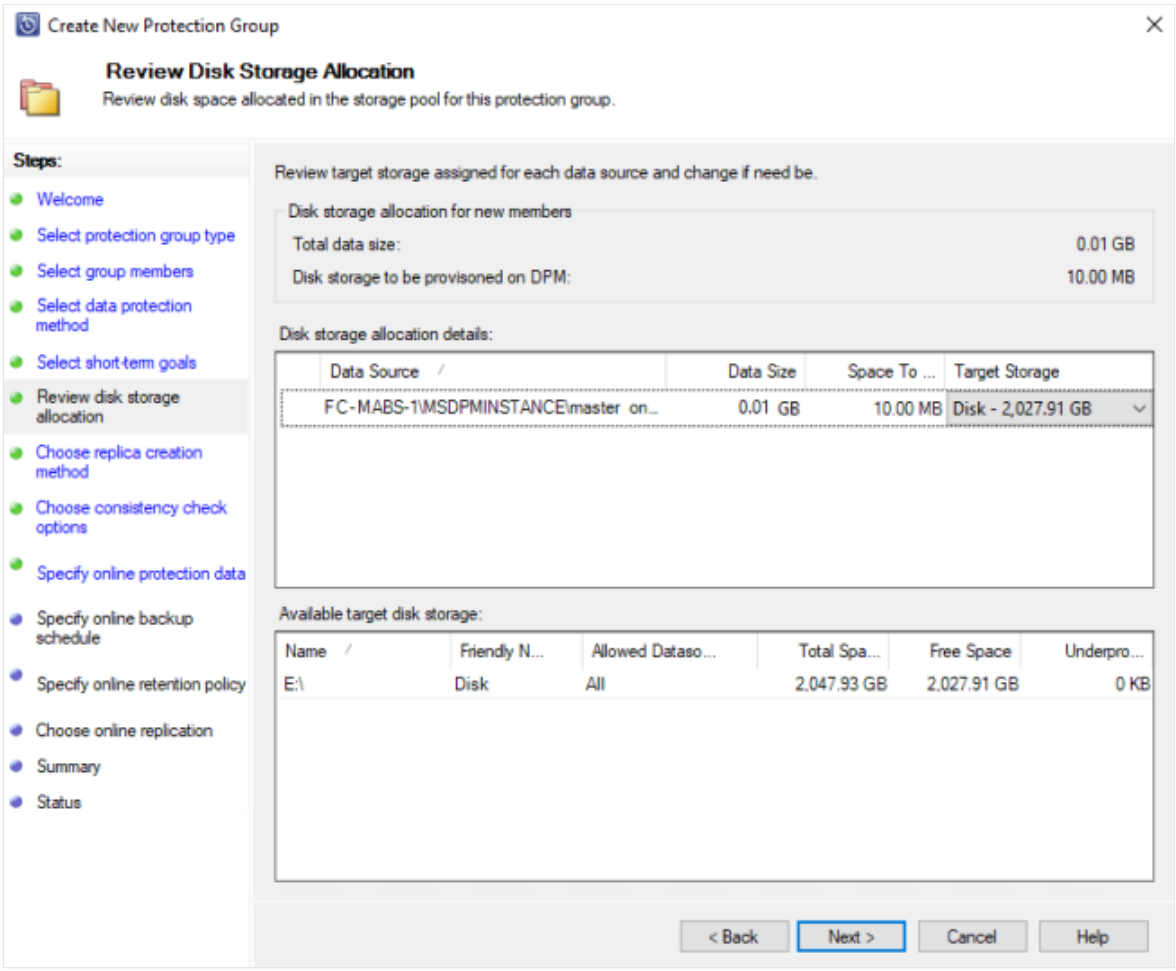
7. Specify how long you want to keep data backed up to disk.

   - **Retention range**: The number of days that disk recovery points are kept.
   - **Express Full Backup**: How often disk recovery points are taken. To change the times or dates when short-term backups occur, select **Modify**.



8. On the **Review Disk Storage Allocation** page, review the disk space provided for the VM backups.

- The recommended disk allocations are based on the retention range you specified, the workload type, and the protected data size. Make any changes that are required, then select **Next**.
- **Data size:** Size of the data in the protection group.
- **Disk space:** Recommended amount of disk space for the protection group. If you want to modify this setting, select space lightly larger than the amount you estimate each data source grows.
- **Storage pool details:** Shows the status of the storage pool, which includes total and remaining disk size.

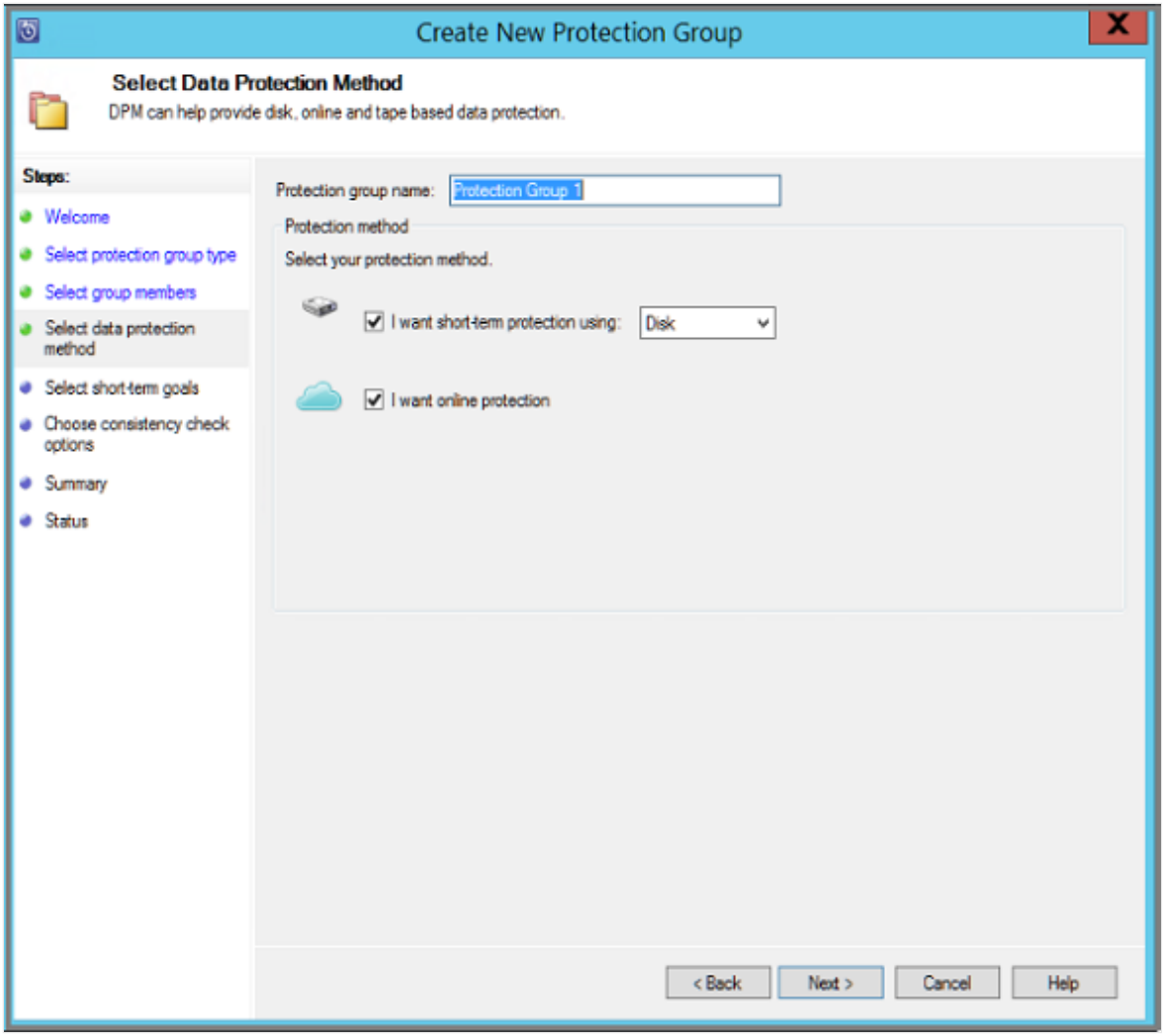


> **Note**
>
> In some scenarios, the data size reported is higher than the actual VM size. We're aware of the issue and currently investigating it.

9. On the **Choose Replica Creation Method** page, indicate how you want to take the initial backup, and select **Next**.

   - The default is **Automatically over the network** and **Now**. If you use the default, specify an off-peak time. If you choose **Later**, specify a day and time.

- For large amounts of data or less-than-optimal network conditions, consider replicating the data offline by using removable media.

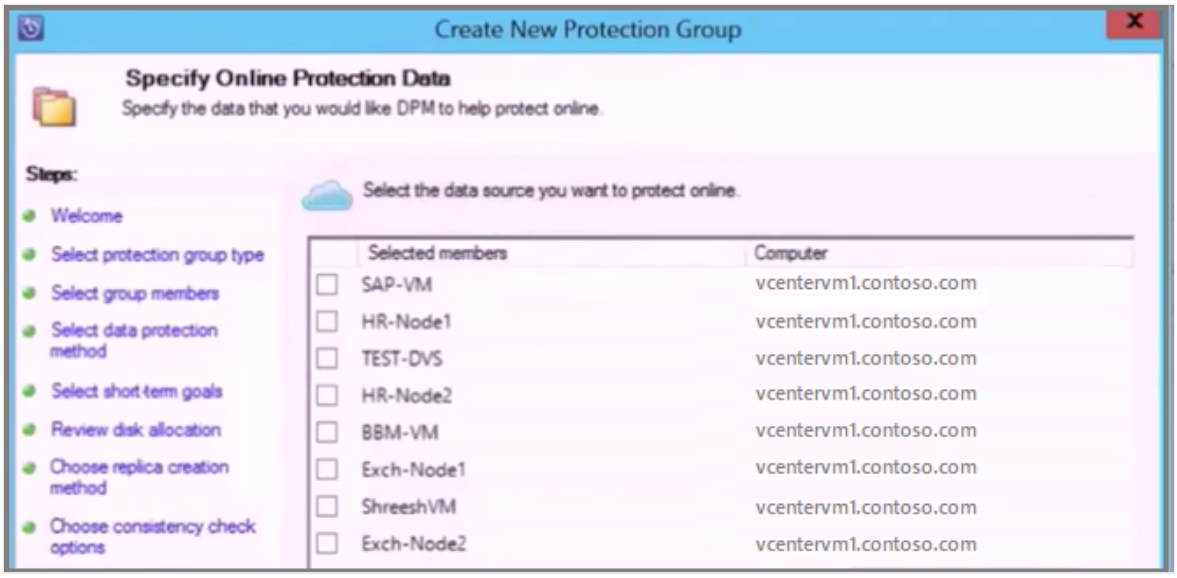


10. For **Consistency check options**, select how and when to automate the consistency checks and select **Next**.

    - You can run consistency checks when replica data becomes inconsistent, or on a set schedule.
    - If you don't want to configure automatic consistency checks, you can run a manual check by right-clicking the protection group **Perform Consistency Check**.

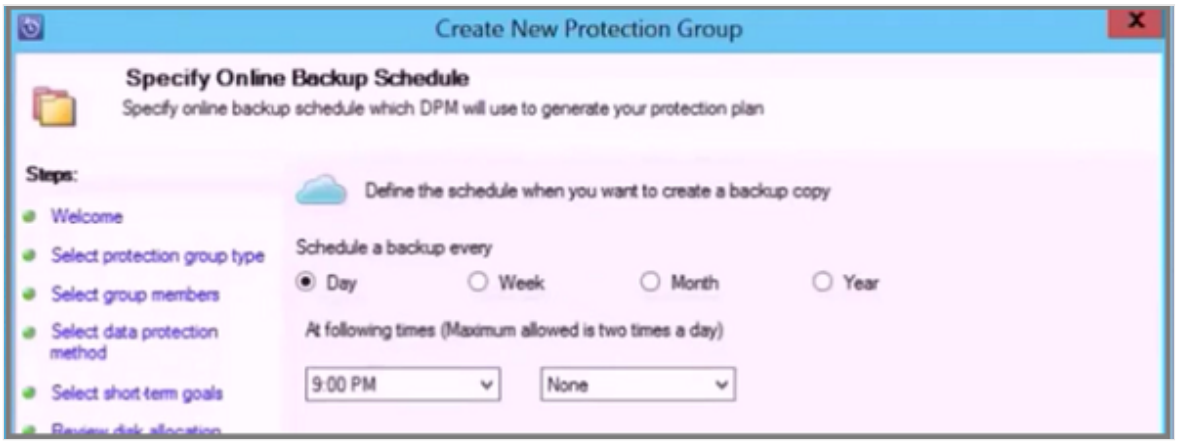
11. On the **Specify Online Protection Data** page, select the VMs or VM folders that you want to back up, and then select **Next**.

    > **Tip**
    >
    > You can select the members individually or choose **Select All** to choose all members.



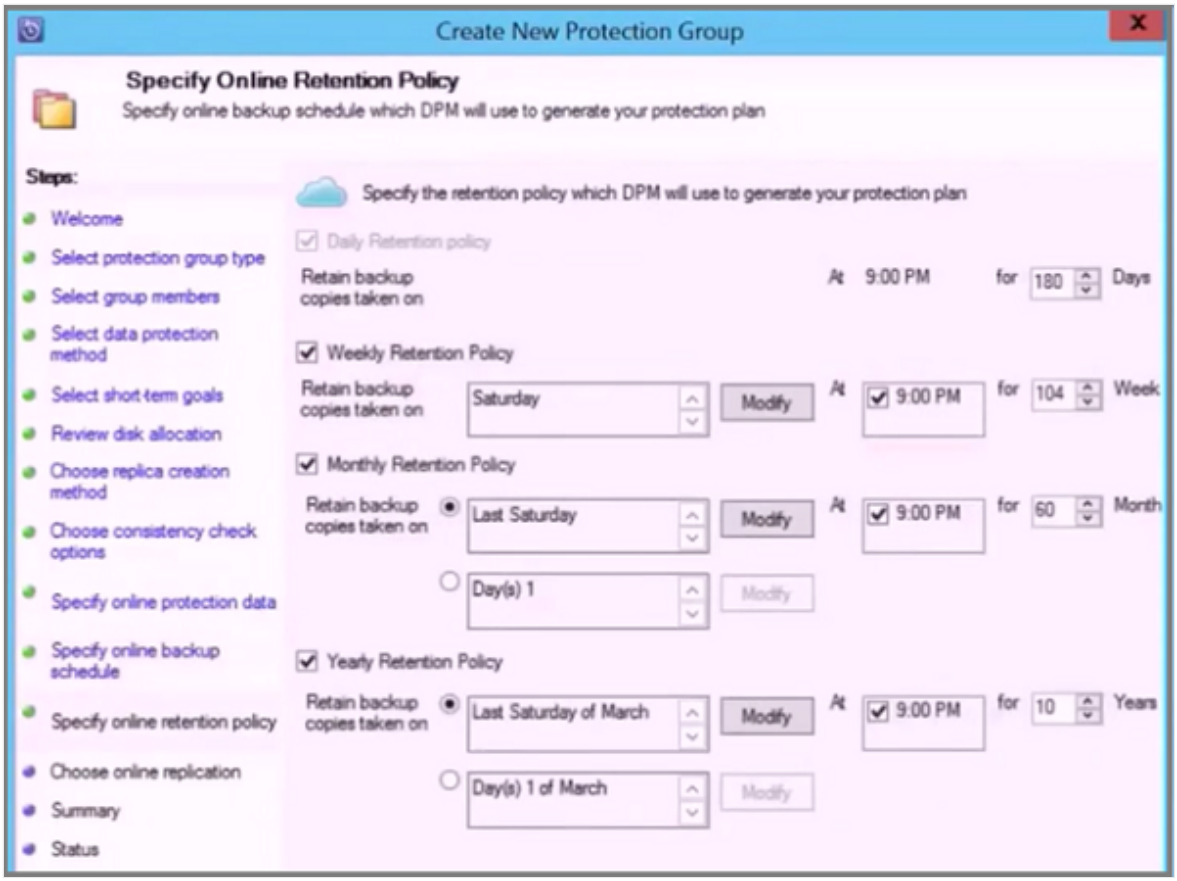
12. On the **Specify Online Backup Schedule** page, indicate how often you want to back up data from local storage to Azure.

    - Cloud recovery points for the data to get generated according to the schedule.
    - After the recovery point gets generated, it gets transferred to the Recovery Services vault in Azure.

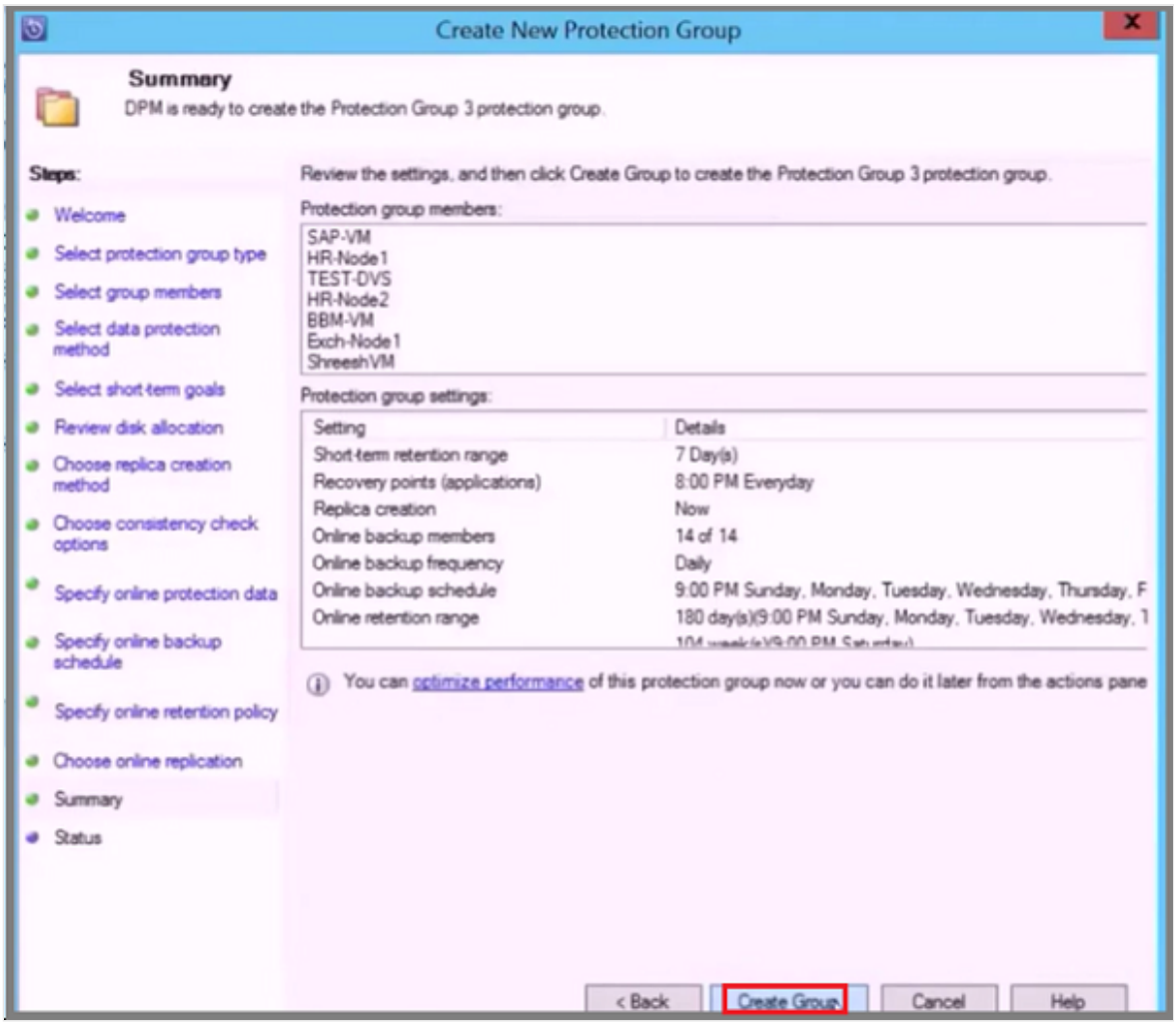


13. On the **Specify Online Retention Policy** page, indicate how long you want to keep the recovery points created from the backups to Azure.

    - There's no time limit for how long you can keep data in Azure.
    - The only limit is that you can't have more than 9,999 recovery points per protected instance. In this example, the protected instance is the VMware vCenter Server.



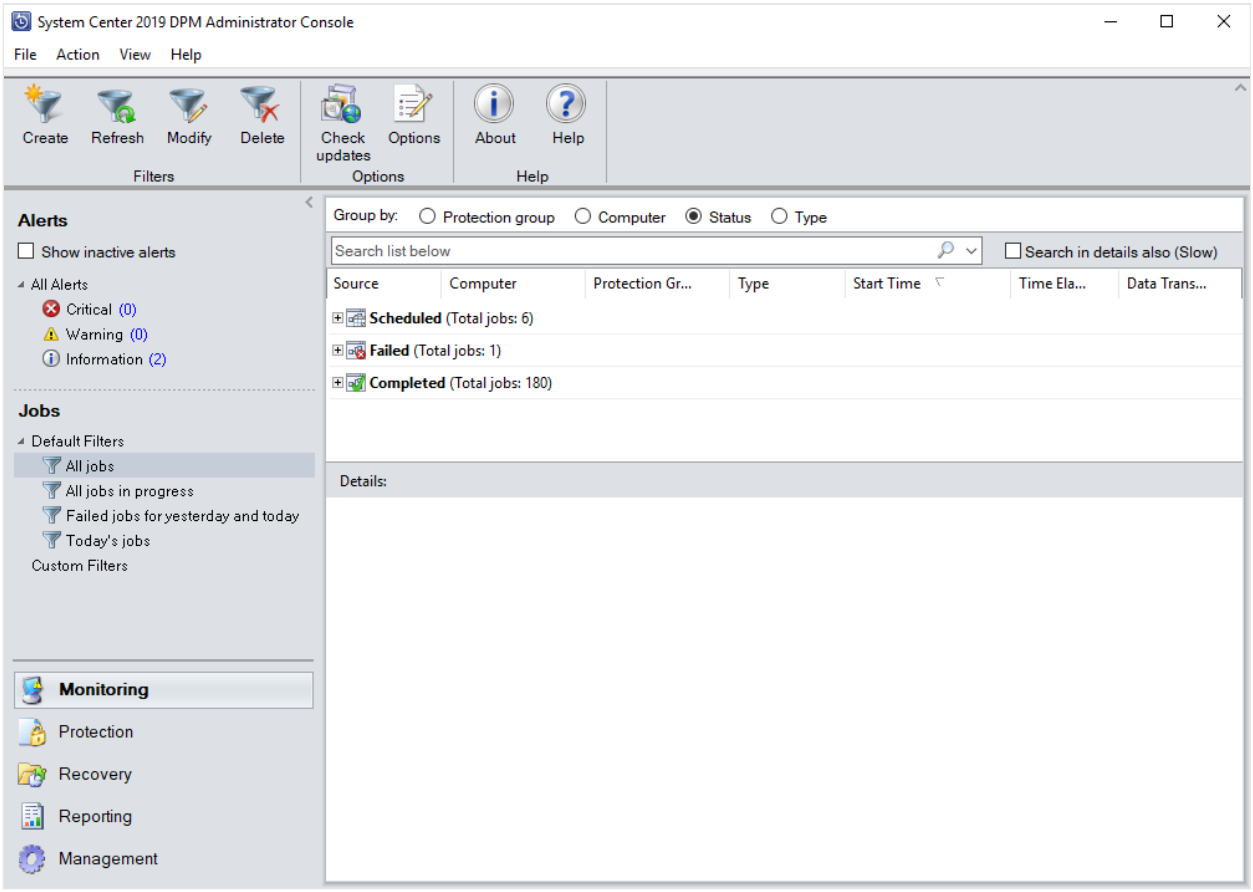
14. On the **Summary** page, review the settings and then select **Create Group**.



Monitor with the Azure Backup Server console

After you configure the protection group to back up Azure VMware Solution VMs, you can monitor the backup job status and alert by using the Azure Backup Server console. Here's what you can monitor.

- In the **Monitoring** task area:
  - Under **Alerts**, you can monitor errors, warnings, and general information. You can view active and inactive alerts and set up email notifications.
  - Under **Jobs**, you can view jobs started by Azure Backup Server for a specific protected data source or protection group. You can follow job progress or check resources consumed by jobs.
- In the **Protection** task area, you can check the status of volumes and shares in the protection group. You can also check configuration settings such as recovery settings, disk allocation, and the backup schedule.
- In the **Management** task area, you can view the **Disks, Online**, and **Agents** tabs to check the status of disks in the storage pool, registration to Azure, and deployed DPM agent status.



Restore VMware vSphere virtual machines

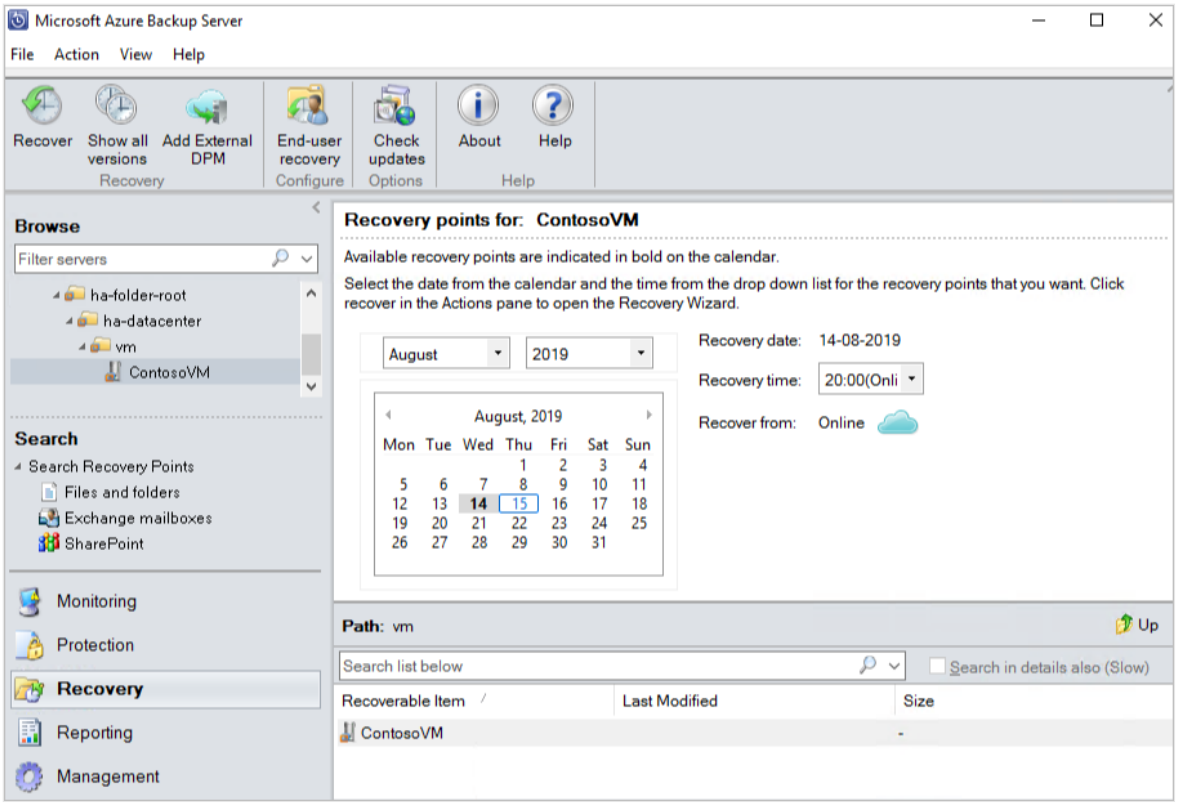
In the Azure Backup Server Administrator Console, there are two ways to find recoverable data. You can search or browse. When you recover data, you might or might not want to restore data or a VM to the same location. For this reason, Azure Backup Server supports three recovery options for VMware VM backups:

- **Original location recovery (OLR)**: Use OLR to restore a protected VM to its original location. You can restore a VM to its original location only if no disks were added or deleted since the backup occurred. If disks were added or deleted, you must use alternate location recovery.
- **Alternate location recovery (ALR)**: Use when the original VM is missing, or you don't want to disturb the original VM. Provide the location of an ESXi host, resource pool, folder, and the storage datastore and path. To help differentiate the restored VM from the original VM, Azure Backup Server appends "-*Recovered*" to the name of the VM.
- **Individual file location recovery (ILR)**: If the protected VM is a Windows Server VM, individual files or folders inside the VM can be recovered by using the ILR capability of Azure Backup Server. To recover individual files, see the procedure later in this article. Restoring an individual file from a VM is available only for Windows VM and disk recovery points.

Restore a recovery point

1. In the Azure Backup Server Administrator Console, select the **Recovery** view.

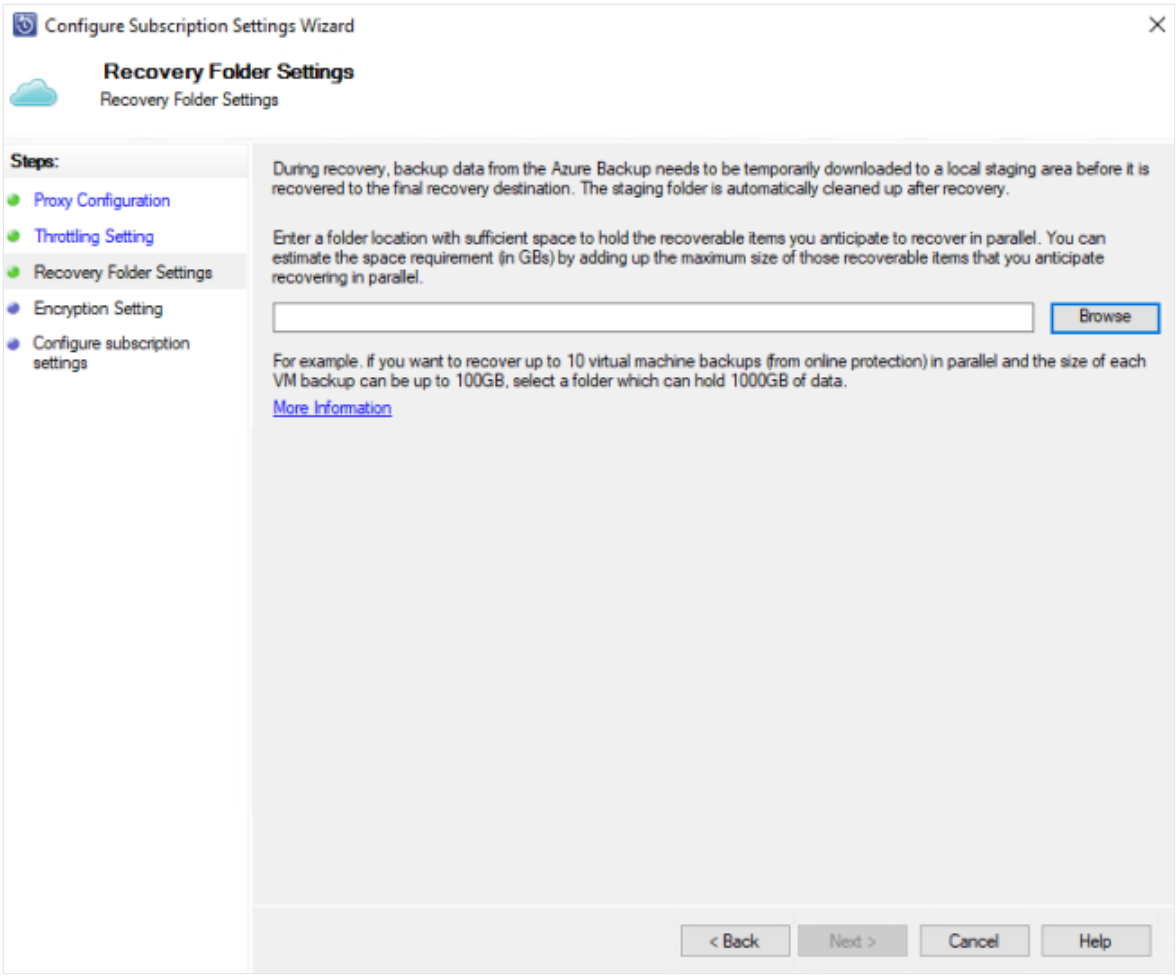
2. Use the **Browse** pane and browse or filter to find the VM you want to recover. After you select a VM or folder, the **Recovery points for pane display the available recovery points.



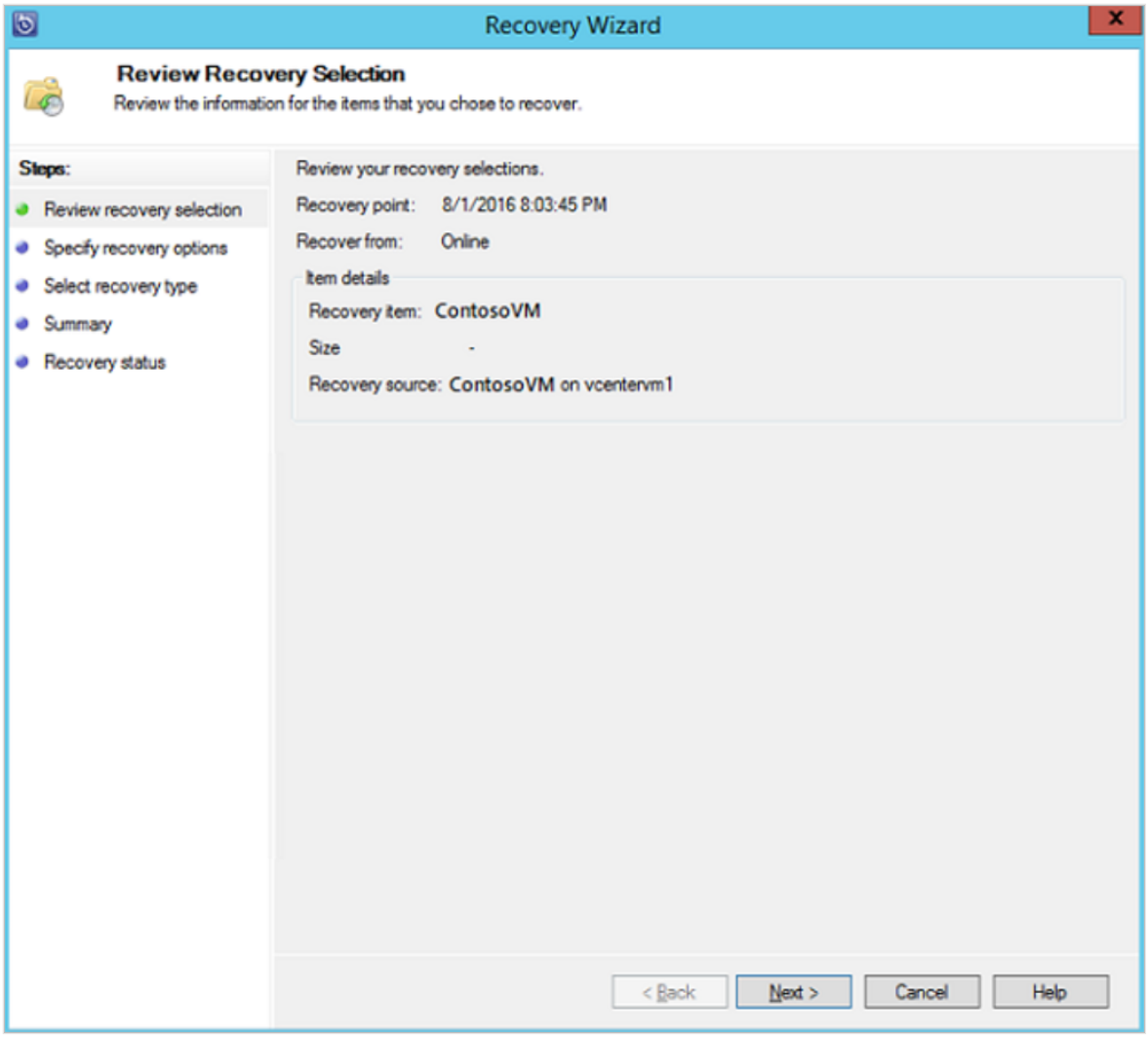
3. In the **Recovery points for** pane, select a date when a recovery point was taken. For example, calendar dates in bold have available recovery points. Alternately, you can right-click the VM, select **Show all recovery points**, and then select the recovery point from the list.

> ⓘ **Note**
>
> For short-term protection, select a disk-based recovery point for faster recovery. After short-term recovery points expire, you see only **Online** recovery points to recover.

4. Before recovering from an online recovery point, ensure the staging location contains enough free space to house the full uncompressed size of the VM you want to recover. The staging location can be viewed or changed by running the **Configure Subscription Settings Wizard**.



5. Select **Recover** to open the **Recovery Wizard**.

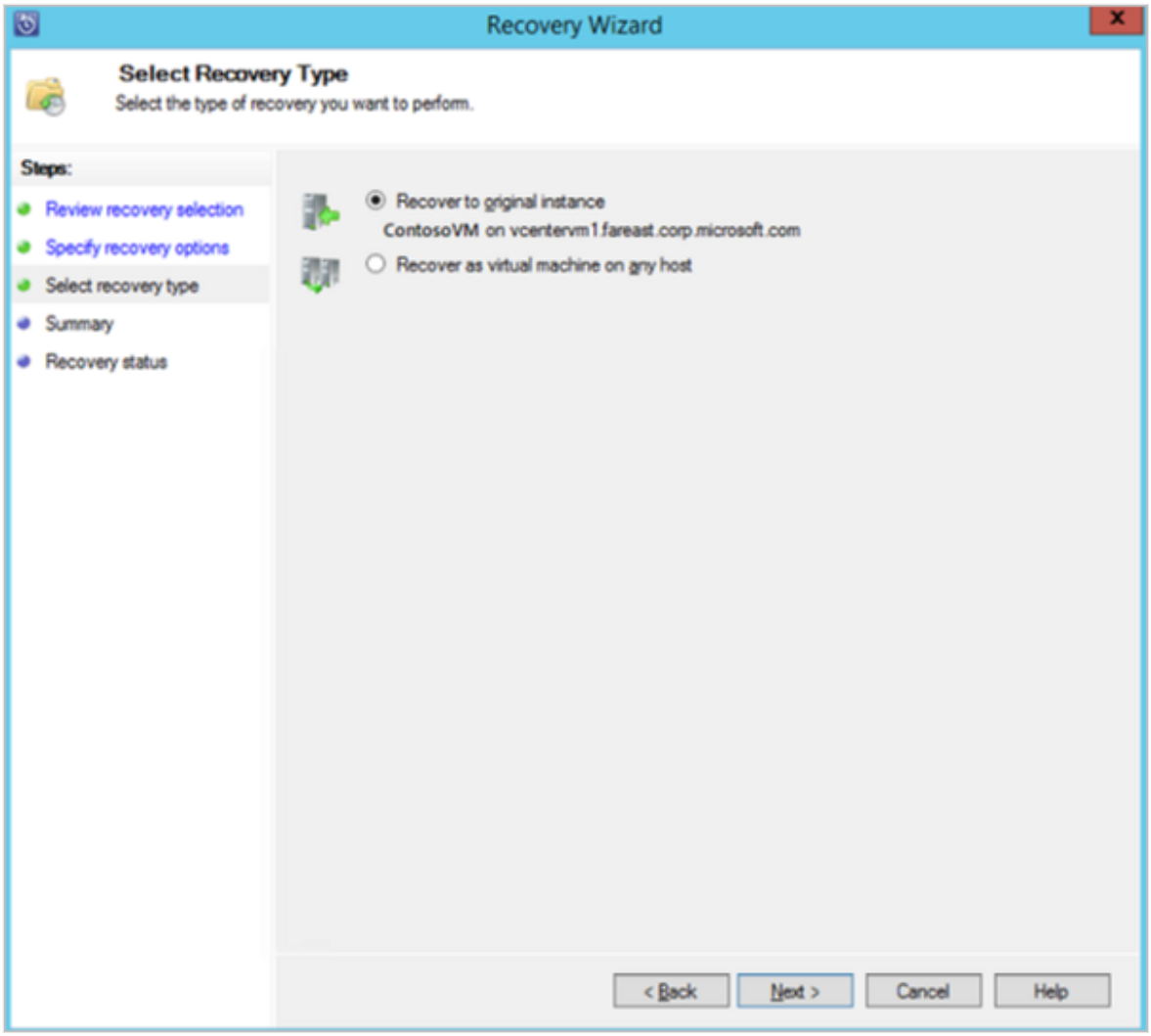


6. Select **Next** to go to the **Specify Recovery Options** screen. Select **Next** again to go to the **Select Recovery Type** screen.

> ⓘ **Note**
>
> VMware vSphere workloads don't support enabling network bandwidth throttling.

7. On the **Select Recovery Type** page, either recover to the original instance or a new location.

   - If you choose **Recover to original instance**, you don't need to make any more choices in the wizard. The data for the original instance is used.
   - If you choose **Recover as virtual machine on any host**, then on the **Specify Destination** screen, provide the information for **ESXi Host**, **Resource Pool**, **Folder**, and **Path**.



8. On the **Summary** page, review your settings and select **Recover** to start the recovery process.

   The **Recovery status** screen shows the progression of the recovery operation.

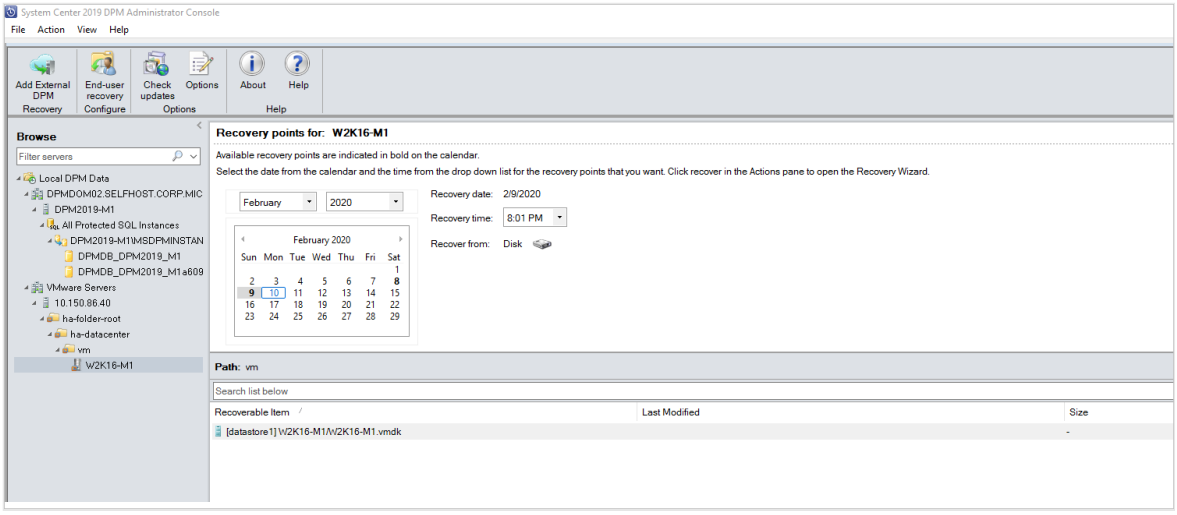
Restore an individual file from a VM

You can restore individual files from a protected VM recovery point. This feature is only available for Windows Server VMs. Restoring individual files is similar to restoring the entire VM, except you browse in the VMDK and find the files you want before you start the recovery process.

> ⓘ **Note**
>
> Restoring an individual file from a VM is available only for Windows VM and disk recovery points.

1. In the Azure Backup Server Administrator Console, select the **Recovery** view.

2. In the **Browse** pane, browse or filter to find the VM you want to recover. After you select a VM or folder, the **Recovery points for pane display the available recovery points.



3. In the **Recovery points for** pane, use the calendar to select the wanted recovery points' date. Depending on how the backup policy was configured, dates can have more than one recovery point.

4. After you select the day when the recovery point was taken, make sure you choose the correct **Recovery time**.

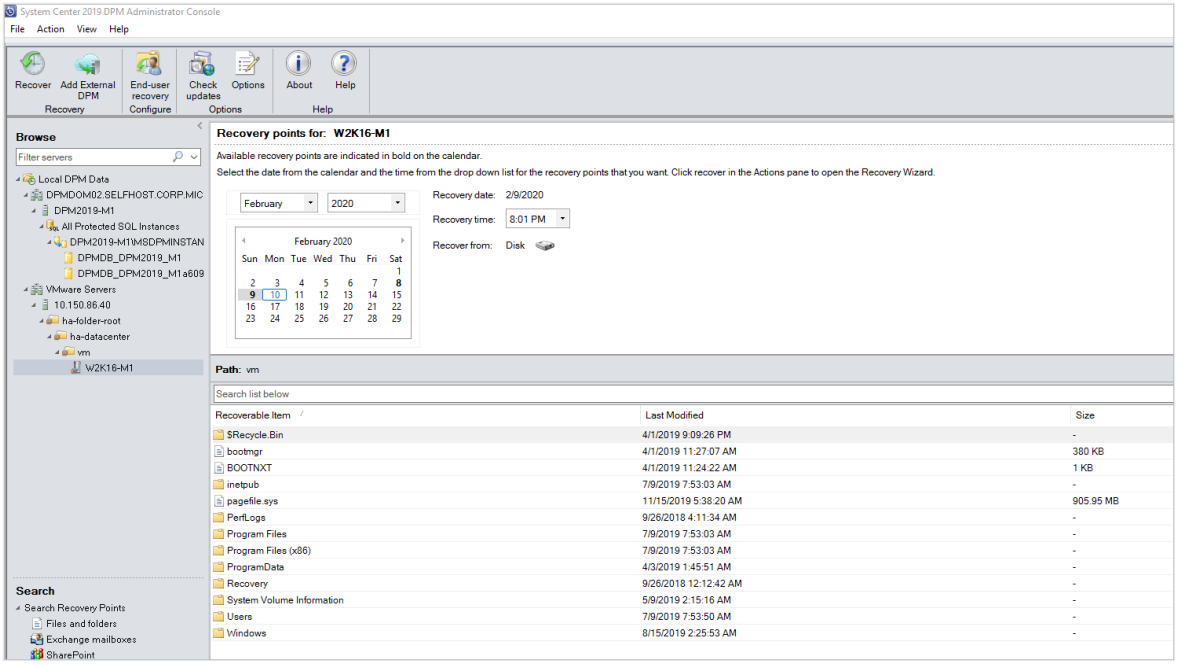
> ⓘ Note
>
> If the selected date has multiple recovery points, choose your recovery point by selecting it in the **Recovery time** drop-down menu.

   After you choose the recovery point, the list of recoverable items appears in the **Path** pane.

5. To find the files you want to recover, in the **Path** pane, double-click the item in the **Recoverable Item** column to open it. Then select the file or folders you want to recover. To select multiple items, select the **Ctrl** key while you select each item. Use the **Path** pane to search the list of files or folders that appear in the **Recoverable Item** column.

> ⓘ Note
>
> The option, **Search list below** doesn't search into subfolders. To search through subfolders, double-click the folder. Use the **Up** button to move from a child folder into the parent folder. You can select multiple items (files and

folders), but they must be in the same parent folder. You can't recover items from multiple folders in the same recovery job.



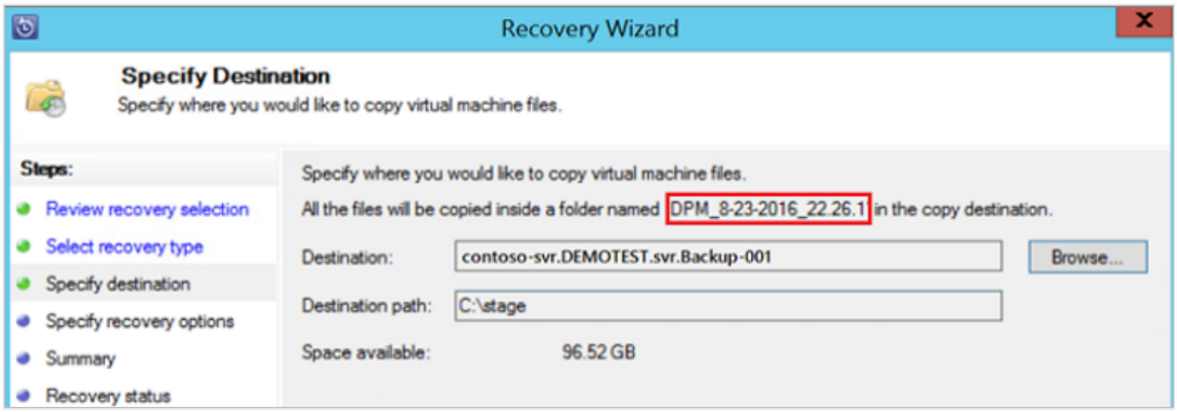
6. After selecting the items for recovery, in the Administrator Console tool ribbon, select **Recover** to open the **Recovery Wizard**. In the **Recovery Wizard**, the **Review Recovery Selection** screen shows the selected items to be recovered.

7. On the **Specify Recovery Options** screen, do one of the following steps:

    - Select **Modify** to enable network bandwidth throttling. In the **Throttle** dialog box, select **Enable network bandwidth usage throttling** to turn it on. Once enabled, configure the **Settings** and **Work Schedule**.
    - Select **Next** to leave network throttling disabled.

8. On the **Select Recovery Type** screen, select **Next**. You can only recover your files or folders to a network folder.

9. On the **Specify Destination** screen, select **Browse** to find a network location for your files or folders. Azure Backup Server creates a folder where all recovered items are copied. The folder name has the prefix MABS_day-month-year. When you select a location for the recovered files or folder, the details for that location are provided.



10. On the **Specify Recovery Options** screen, choose which security setting to apply. You can opt to modify the network bandwidth usage throttling, but throttling is disabled by default. Also, **SAN Recovery** and **Notification** aren't enabled.

11. On the **Summary** screen, review your settings and select **Recover** to start the recovery process. The **Recovery status** screen shows the progression of the recovery operation.

Next steps

Now that you know how to back up your Azure VMware Solution VMs with Azure Backup Server, expand your knowledge and learn more about:

- Troubleshooting when setting up backups in Azure Backup Server.
- Lifecycle management of Azure VMware Solution VMs.

Disaster recovery solutions for Azure VMware Solution virtual machines (VMs)

Article • 12/12/2023

One of the most important aspects of any Azure VMware Solution deployment is disaster recovery. You can create disaster recovery plans between different Azure VMware Solution regions or between Azure and an on-premises vSphere environment.

We currently offer customers the possibility to implement their disaster recovery plans using state-of-the-art VMware solution like SRM or HCX.

Following our principle of giving customers the choice to apply their investments in skills and technology, we collaborated with some of the leading partners in the industry.

You can find more information about their solutions in the following links:

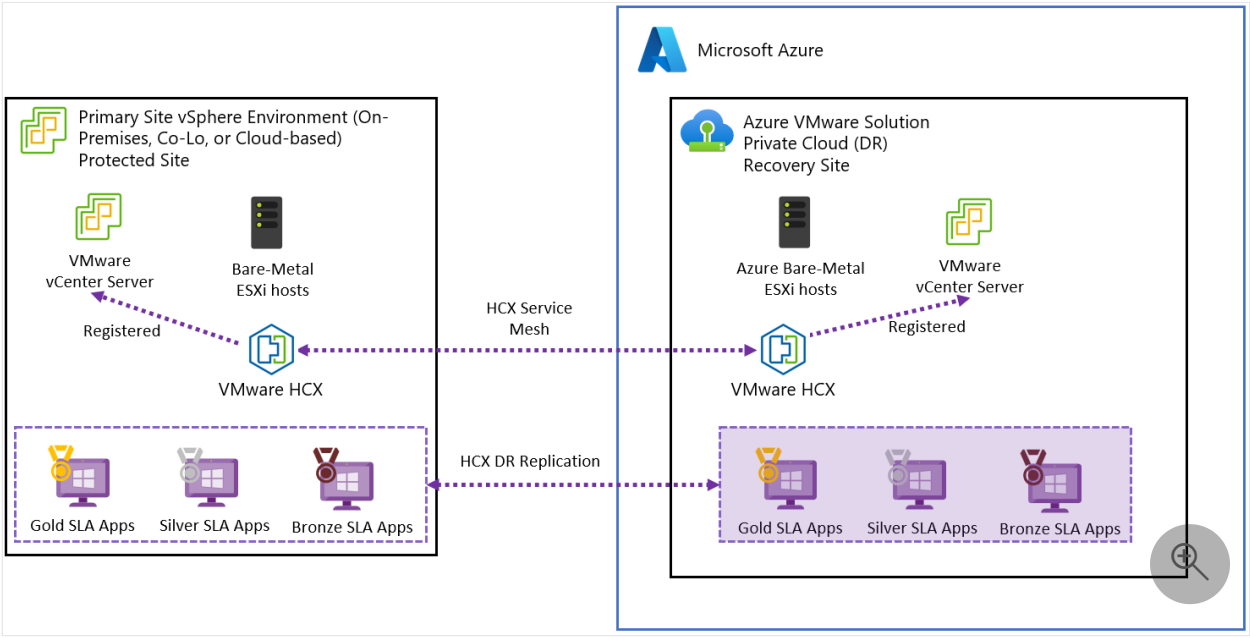
- JetStream
- Zerto
- RiverMeadow

Deploy disaster recovery using VMware HCX

Article • 12/20/2023

In this article, learn how to deploy disaster recovery of your virtual machines (VMs) with VMware HCX solution and use an Azure VMware Solution private cloud as the recovery or target site.

The diagram shows the deployment of VMware HCX from on-premises VMware vSphere to Azure VMware Solution private cloud disaster recovery scenario.



> **Important**
>
> Although part of VMware HCX, VMware HCX Disaster Recovery (DR) is not recommended for large deployments. The disaster recovery orchestration is 100% manual, and Azure VMware Solution currently doesn't have runbooks or features to support manual VMware HCX DR failover. For enterprise-class disaster recovery, refer to VMware Site Recovery Manager (SRM) or VMware business continuity and disaster recovery (BCDR) solutions.

VMware HCX provides various operations that provide fine control and granularity in replication policies. Available Operations include:

- **Reverse** – After a disaster occurs, reverse helps make Site B the source site and Site A, where the protected VM now lives.

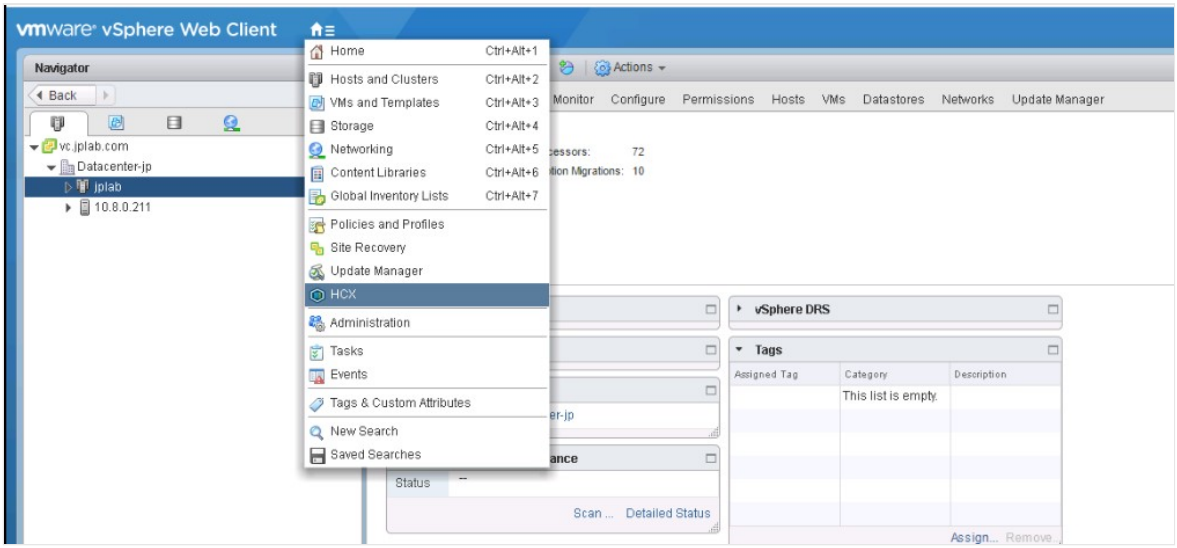
- **Pause** – Pause the current replication policy associated with the VM selected.
- **Resume** - Resume the current replication policy associated with the VM selected.
- **Remove** - Remove the current replication policy associated with the VM selected.
- **Sync Now** – Out of bound sync source VM to the protected VM.

This guide covers the following replication scenarios:

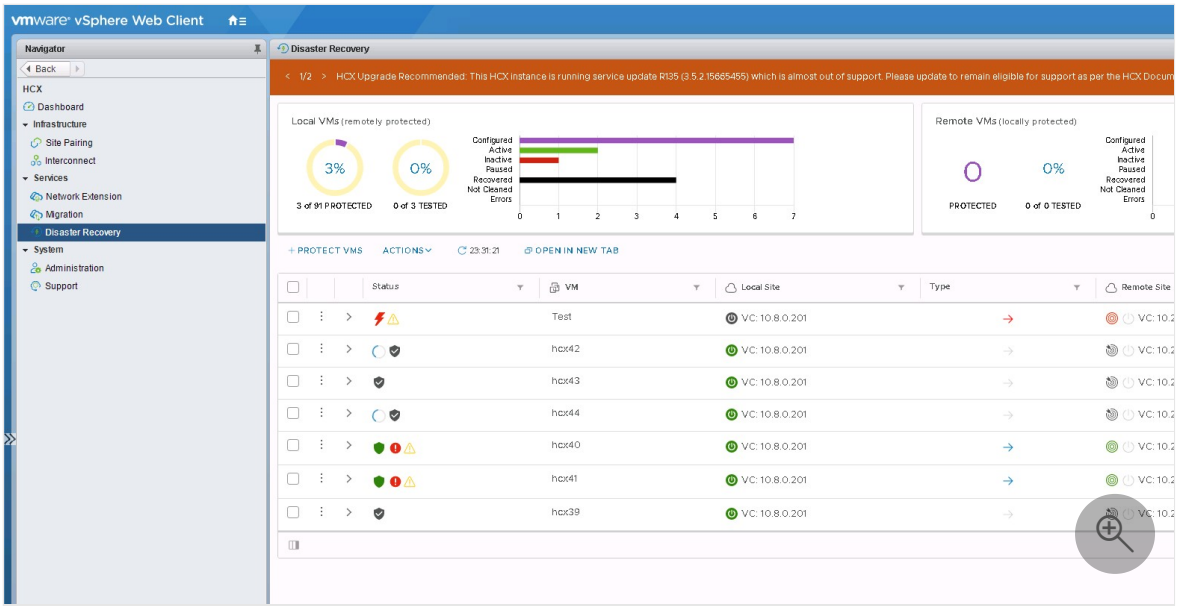
- Protect a VM or a group of VMs.
- Complete a Test Recover of a VM or a group of VMs.
- Recover a VM or a group of VMs.
- Reverse Protection of a VM or a group of VMs.

Protect VMs

1. Sign in to **vSphere Client** on the source site and access **HCX plugin**.



2. Enter the **Disaster Recovery** area and select **PROTECT VMS**.

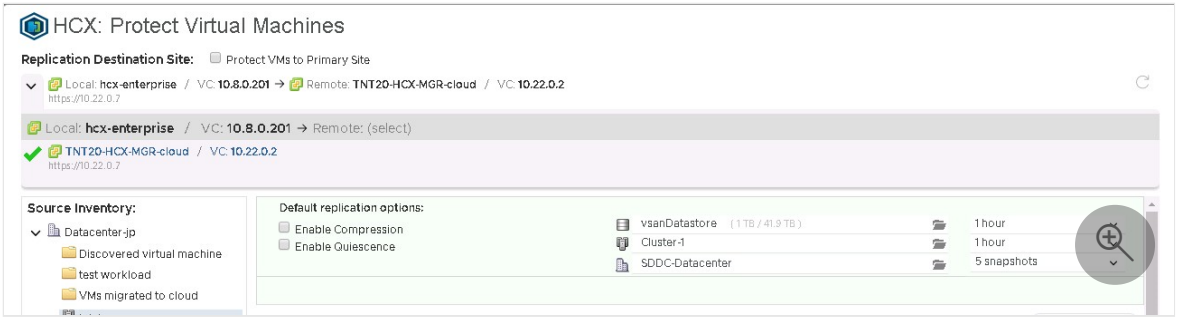


3. Select the Source and the Remote sites. The Remote site in this case should be the Azure VMware Solution private cloud.

4. If needed, select the **Default replication** options:

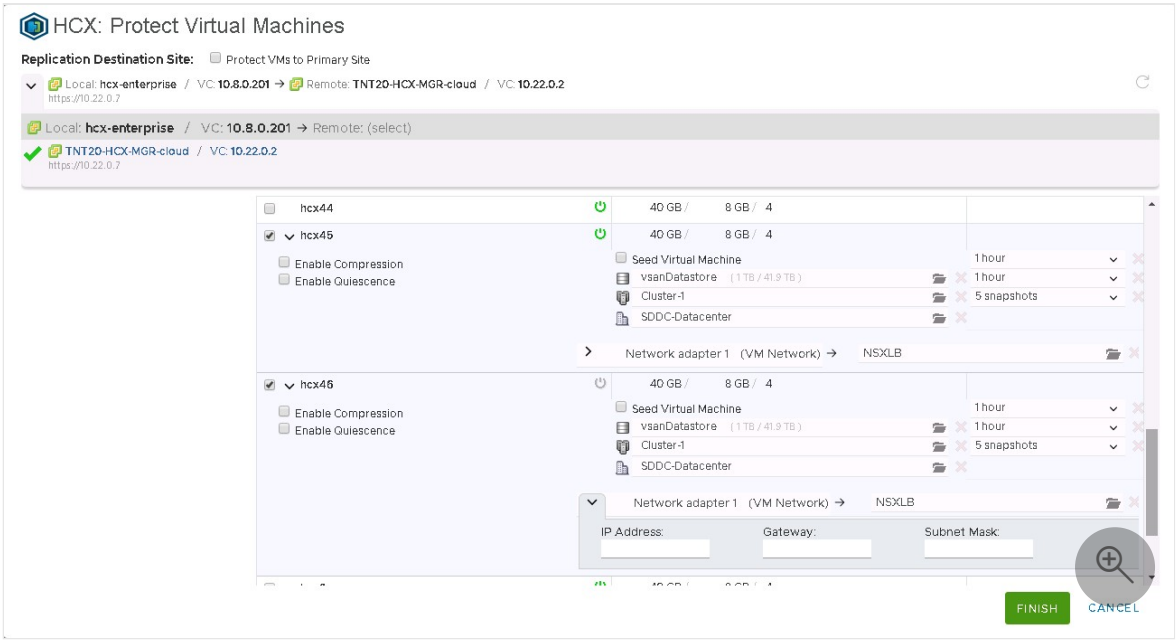
   - **Enable Compression:** Recommended for low throughput scenarios.
   - **Enable Quiescence:** Pauses the VM to ensure a consistent copy is synced to the remote site.
   - **Destination Storage:** Remote datastore for the protected VMs, and in an Azure VMware Solution private cloud, which can be a vSAN datastore or an Azure NetApp Files datastore.
   - **Compute Container:** Remote vSphere Cluster or Resource Pool.
   - **Destination Folder:** Remote destination folder, which is optional, and if no folder is selected, the VMs are placed directly under the selected cluster.
   - **RPO:** Synchronization interval between the source VM and the protected VM. It can be anywhere from 5 minutes to 24 hours.
   - **Snapshot interval:** Interval between snapshots.

- **Number of Snapshots:** Total number of snapshots within the configured snapshot interval.

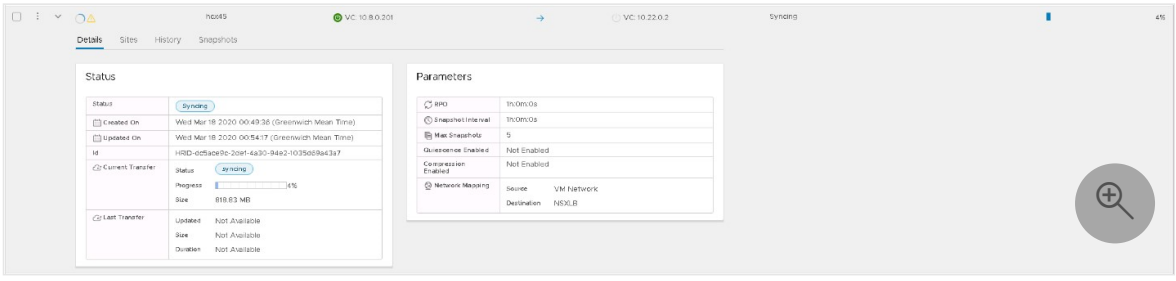


5. Select one or more VMs from the list and configure the replication options as needed.

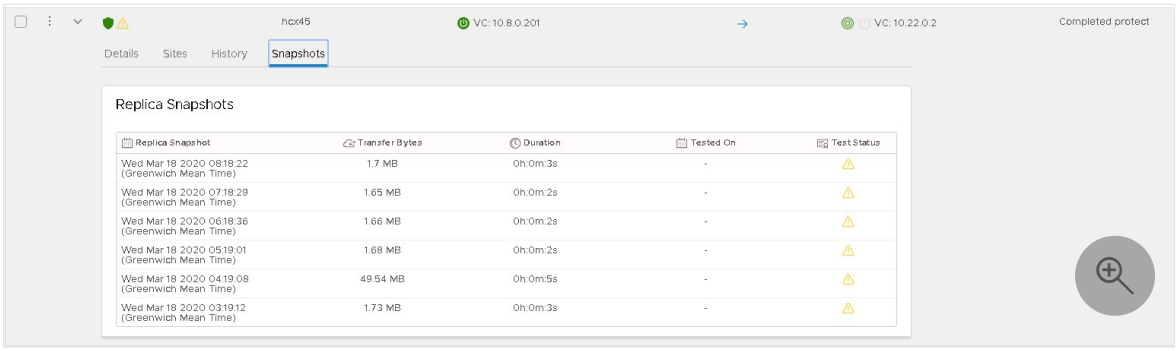
   By default, the VMs inherit the Global Settings Policy configured in the Default replication options. For each network interface in the selected VM, configure the remote **Network Port Group** and select **Finish** to start the protection process.



6. Monitor the process for each of the selected VMs in the same disaster recovery area.



7. After the VM is protected, you can view the different snapshots in the **Snapshots** tab.



The yellow triangle means the snapshots and the virtual machines weren't tested in a Test Recovery operation.

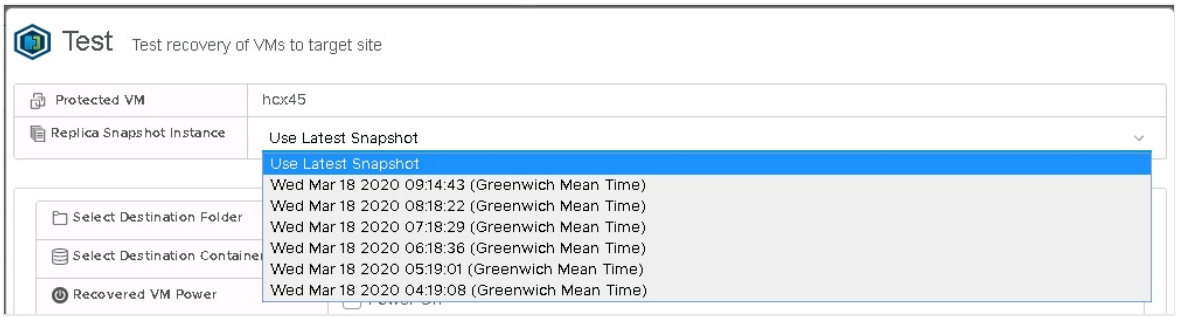
There are key differences between a VM that is powered off and one powered on. The image shows the syncing process for a powered-on VM. It starts the syncing process until it finishes the first snapshot, which is a full copy of the VM, and then completes the next ones in the configured interval. It syncs a copy for a powered off VM, and then the VM appears as inactive, and protection operation shows as completed. When the VM is powered on, it starts the syncing process to the remote site.

Complete a test recover of VMs

1. Sign in to **vSphere Client** on the remote site, which is the Azure VMware Solution private cloud.

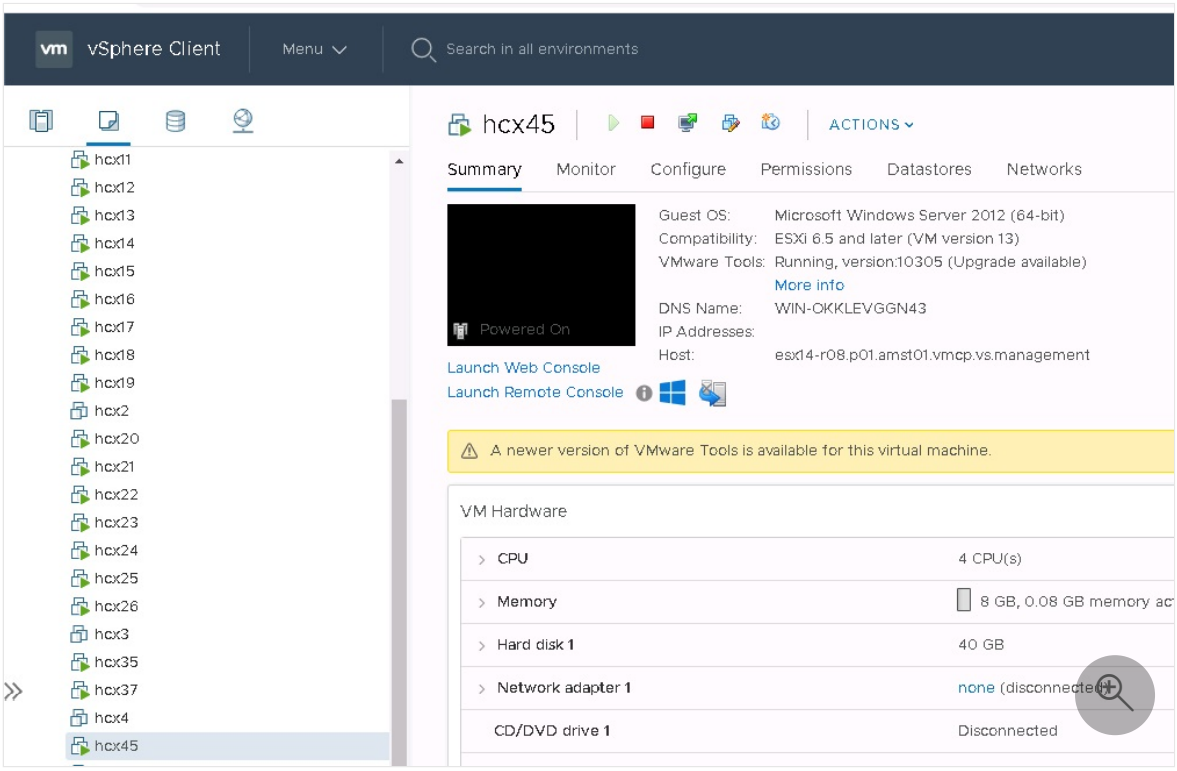
2. Within the **HCX plugin**, in the Disaster Recovery area, select the vertical ellipses on any VM to display the operations menu and then select **Test Recover VM**.

3. Select the options for the test and the snapshot you want to use to test different states of the VM.

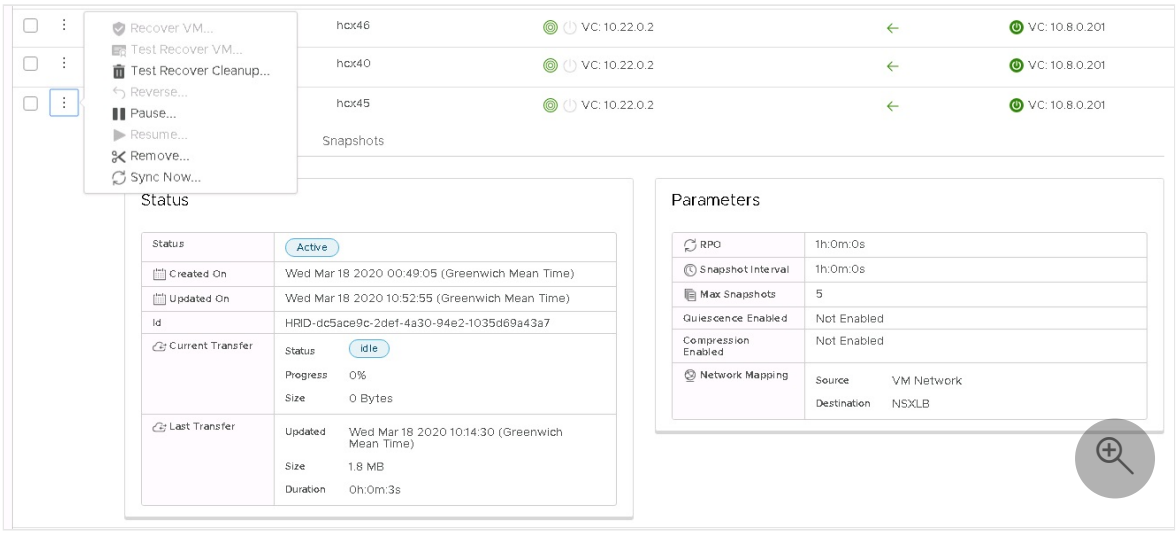


4. After you select **Test**, the recovery operation begins.

5. When finished, you can check the new VM in the Azure VMware Solution private cloud vCenter Server.



6. After testing on the VM or any application running on it are finished, do a cleanup to delete the test instance.

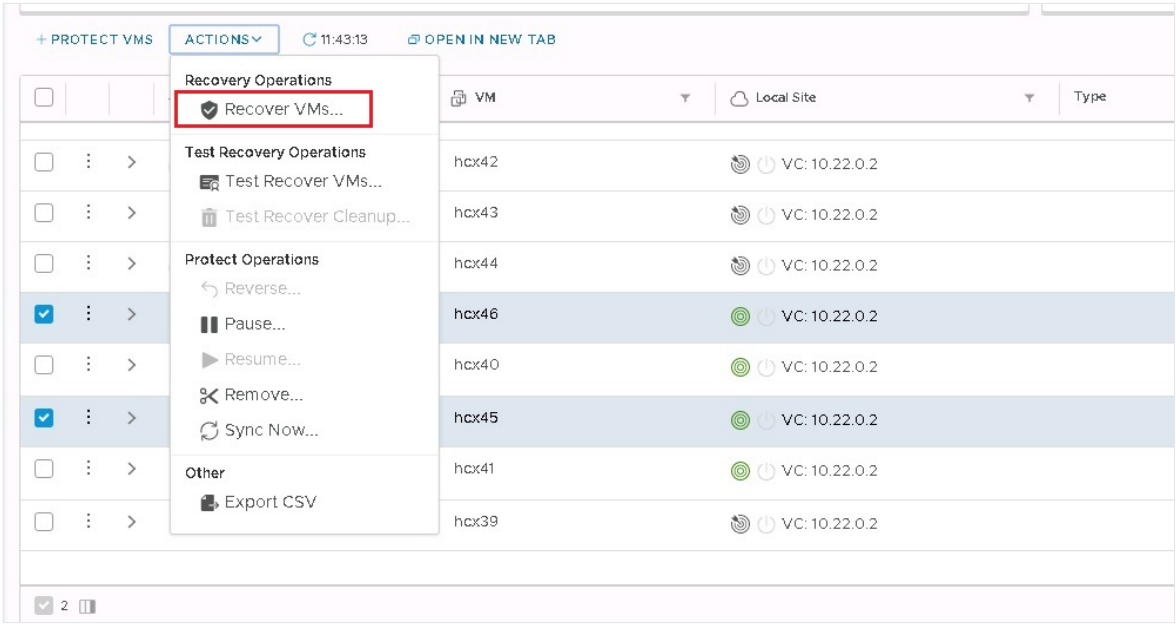


Recover VMs

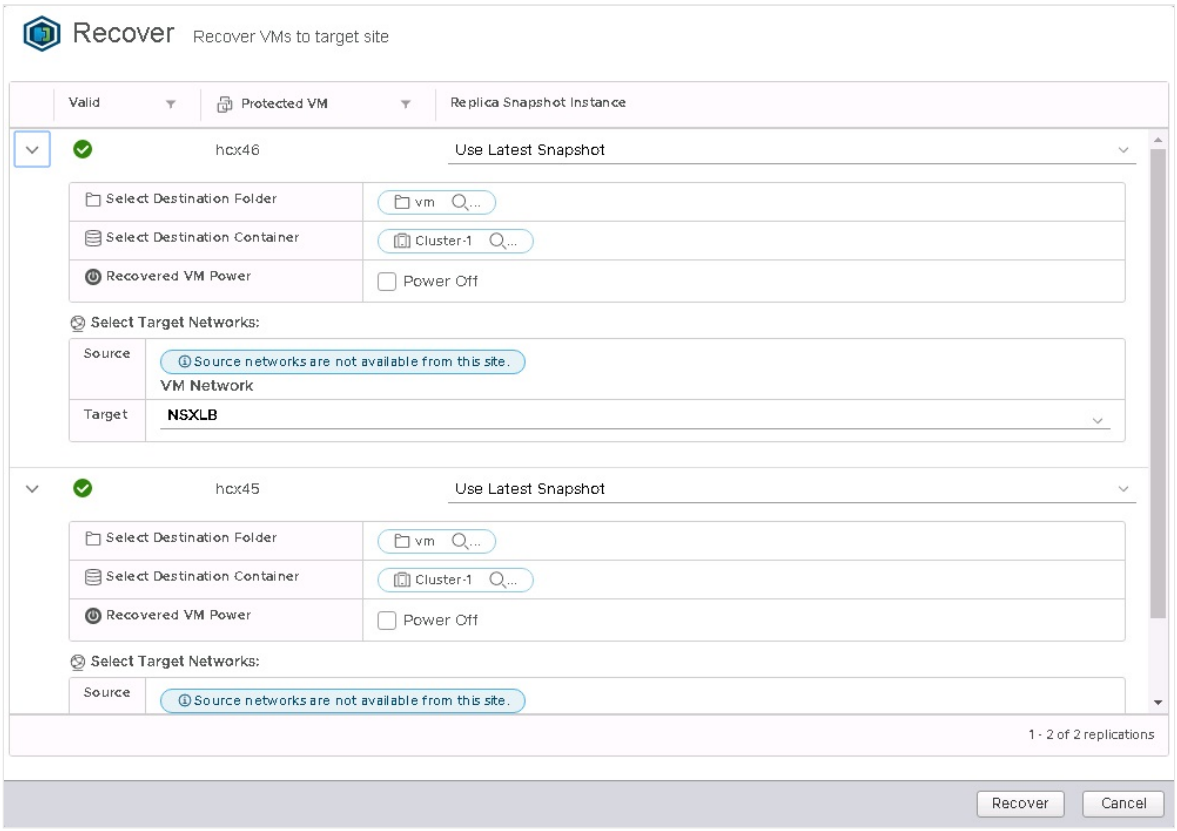
1. Sign in to **vSphere Client** on the remote site, which is the Azure VMware Solution private cloud, and access the **HCX plugin**.

   For the recovery scenario, a group of VMs used for this example.

2. Select the VM to be recovered from the list, open the **ACTIONS** menu, and select **Recover VMs**.



3. Configure the recovery options for each instance and select **Recover** to start the recovery operation.



4. After the recovery operation is completed, the new VMs appear in the remote vCenter Server inventory.

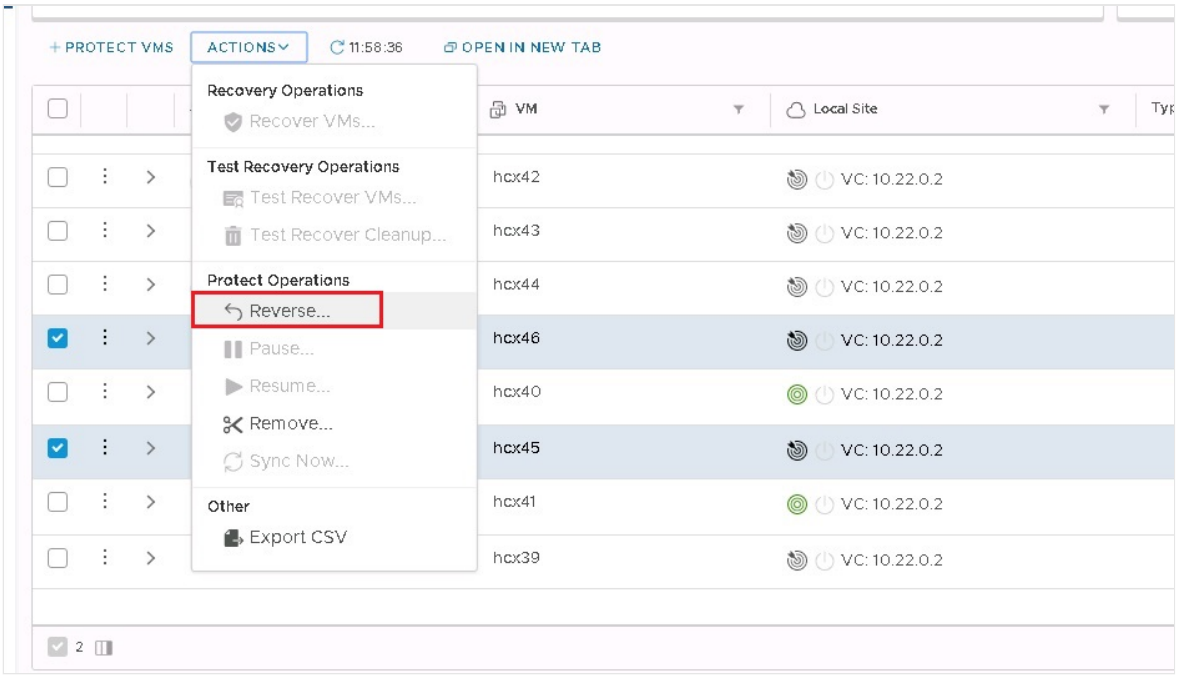
Complete a reverse replication on VMs

1. Sign in to **vSphere Client** on your Azure VMware Solution private cloud, and access **HCX plugin**.

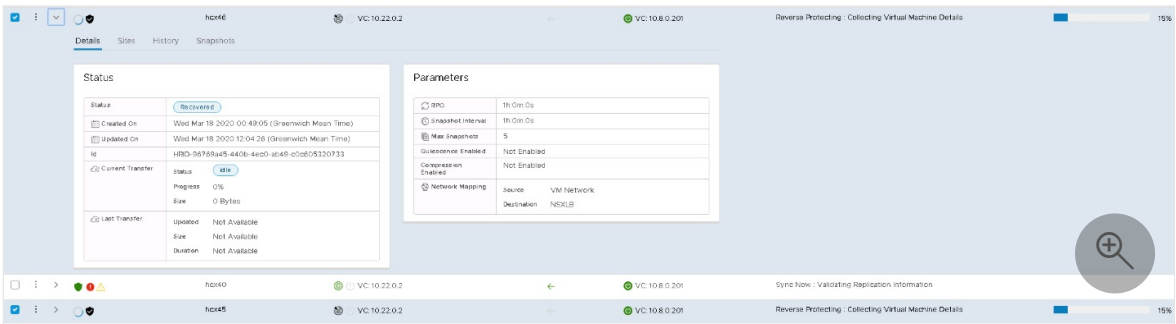
   > **Note**
   >
   > Ensure the original VMs on the source site are powered off before you start the reverse replication. The operation fails if the VMs aren't powered off.

2. From the list, select the VMs to be replicated back to the source site, open the **ACTIONS** menu, and select **Reverse**.

3. Select **Reverse** to start the replication.



4. Monitor on the details section of each VM.



Disaster recovery plan automation

VMware HCX currently doesn't have a built-in mechanism to create and automate a disaster recovery plan. However, VMware HCX provides a set of REST APIs, including APIs for the Disaster Recovery operation. The API specification can be accessed within VMware HCX Manager in the URL.

These APIs cover the following operations in Disaster Recovery.

- Protect
- Recover
- Test Recover
- Planned Recover
- Reverse
- Query
- Test Cleanup
- Pause
- Resume
- Remove Protection
- Reconfigure

The following example shows a recover operation payload in JSON.

JSON

```
[
    {
        "replicationId": "string",
        "needPowerOn": true,
        "instanceId": "string",
        "source": {
            "endpointType": "string",
            "endpointId": "string",
```

```
            "endpointName": "string",
            "resourceType": "string",
            "resourceId": "string",
            "resourceName": "string"
        },
        "destination": {
            "endpointType": "string",
            "endpointId": "string",
            "endpointName": "string",
            "resourceType": "string",
            "resourceId": "string",
            "resourceName": "string"
        },
        "placement": [
            {
                "containerType": "string",
                "containerId": "string"
            }
        ],
        "resourceId": "string",
        "forcePowerOff": true,
        "isTest": true,
        "forcePowerOffAfterTimeout": true,
        "isPlanned": true
    }
]
```

With these APIs, you can build a custom mechanism to automate a disaster recovery plan's creation and execution.

Deploy disaster recovery with VMware Site Recovery Manager (SRM)

Article • 12/14/2023

This article explains how to implement disaster recovery for on-premises VMware vSphere virtual machines (VMs) or Azure VMware Solution-based VMs. The solution in this article uses VMware Site Recovery Manager (SRM) and vSphere Replication with Azure VMware Solution. Instances of VMware SRM and replication servers are deployed at both the protected and the recovery sites.

VMware SRM is a disaster recovery solution designed to minimize downtime of the virtual machines in an Azure VMware Solution environment if there was a disaster. VMware SRM automates and orchestrates failover and failback, ensuring minimal downtime in a disaster. Also, built-in nondisruptive testing ensures your recovery time objectives are met. Overall, VMware SRM simplifies management through automation and ensures fast and highly predictable recovery times.

VMware vSphere Replication is VMware's hypervisor-based replication technology for VMware vSphere VMs. It protects VMs from partial or complete site failures. In addition, it simplifies DR protection through storage-independent, VM-centric replication. VMware vSphere Replication is configured on a per-VM basis, allowing more control over which VMs are replicated.

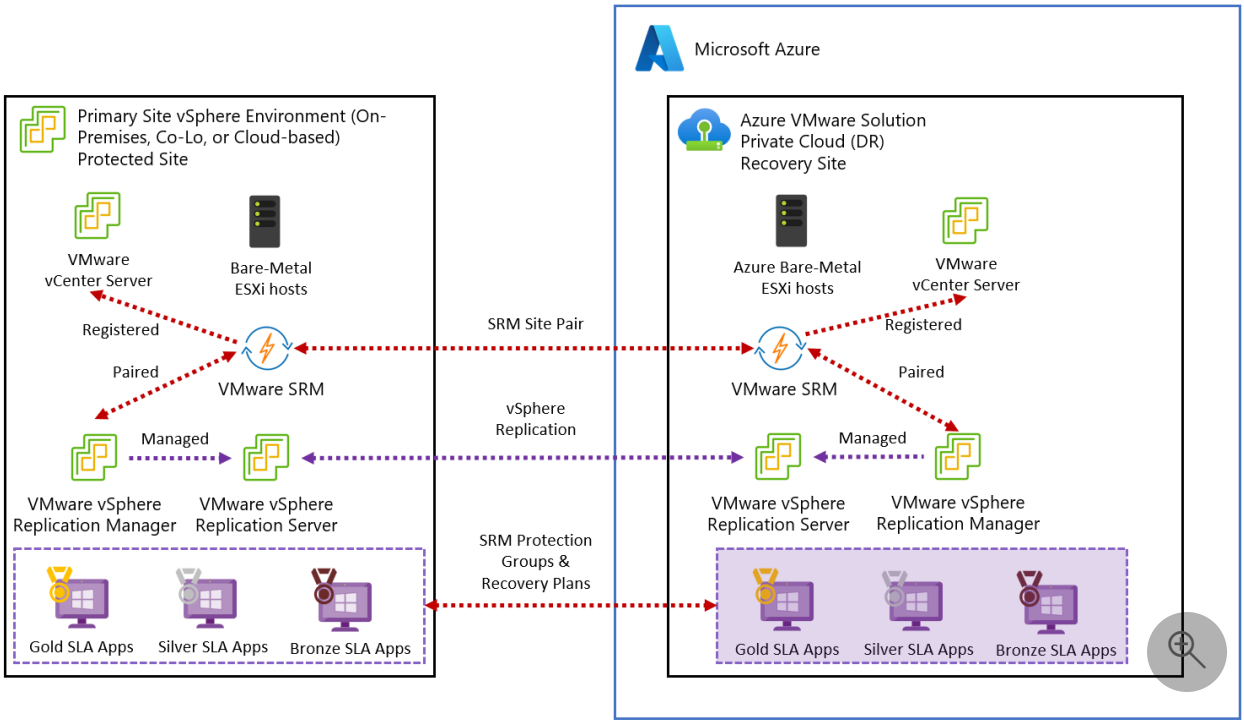
> **Note**
>
> The current version of VMware Site Recovery Manager (SRM) in Azure VMware Solution is 8.7.0.3.

Supported scenarios

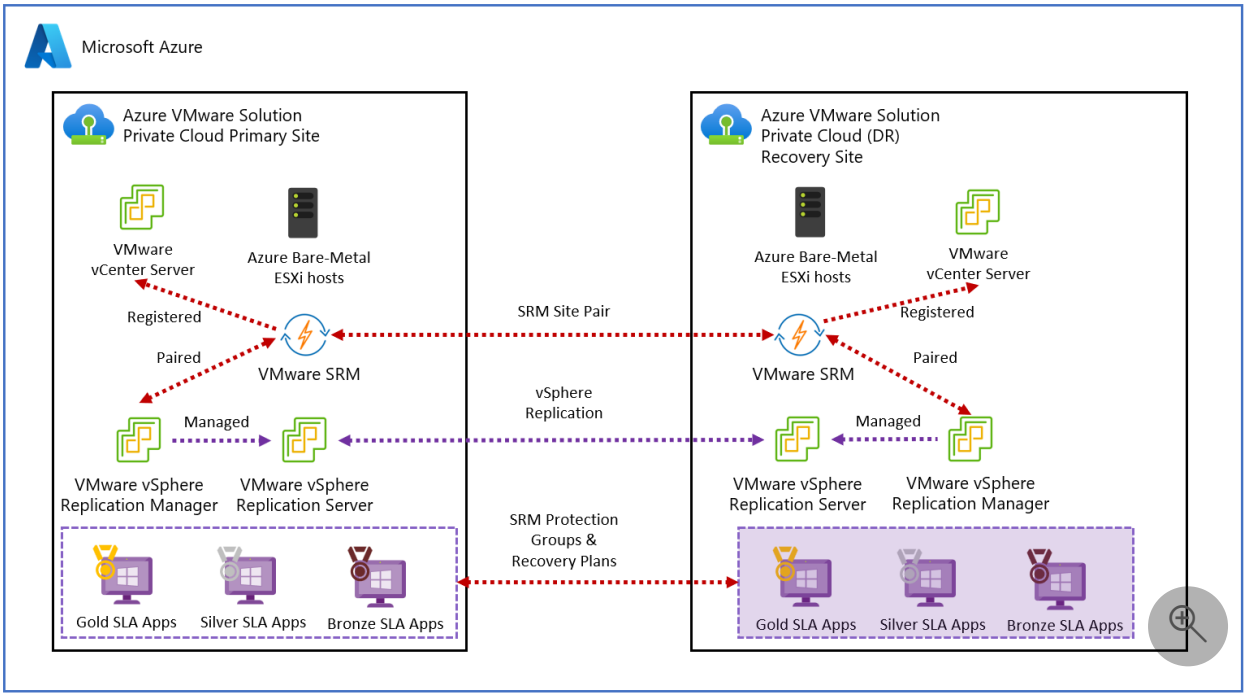
VMware SRM helps you plan, test, and run the recovery of VMs between a protected VMware vCenter Server site and a recovery VMware vCenter Server site. You can use VMware SRM with Azure VMware Solution with the following two DR scenarios:

- On-premises VMware vSphere to Azure VMware Solution private cloud disaster recovery
- Primary Azure VMware Solution to Secondary Azure VMware Solution private cloud disaster recovery

The diagram shows the deployment of the on-premises VMware vSphere to Azure VMware Solution private cloud disaster recovery scenario.



The diagram shows the deployment of the primary Azure VMware Solution to secondary Azure VMware Solution scenario.



You can use VMware SRM to implement different types of recovery, such as:

- **Planned migration** commences when both primary and secondary Azure VMware Solution sites are running and fully functional. It's an orderly migration of virtual machines from the protected site to the recovery site where no data loss is expected when migrating workloads in an orderly fashion.

- **Disaster recovery** using SRM can be invoked when the protected Azure VMware Solution site goes offline unexpectedly. VMware Site Recovery Manager orchestrates the recovery process with the replication mechanisms to minimize data loss and system downtime.

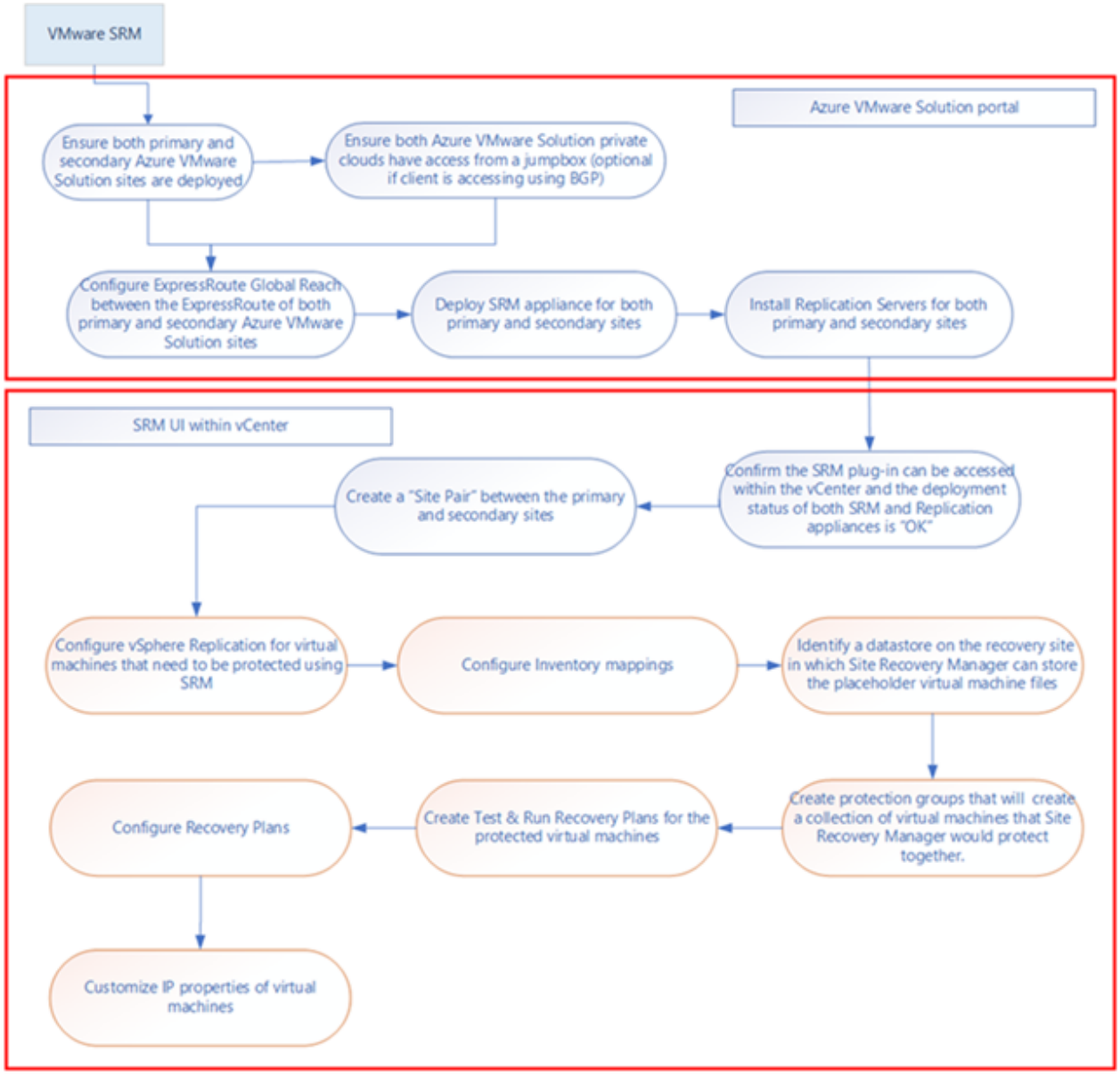
  In Azure VMware Solution, only individual VMs can be protected on a host by using VMware SRM in combination with VMware vSphere Replication.

- **Bidirectional Protection** uses a single set of paired VMware SRM sites to protect VMs in both directions. Each site can simultaneously be a protected site and a recovery site, but for a different set of VMs.

> **ⓘ Important**
>
> Azure VMware Solution doesn't support:
>
> - Array-based replication and storage policy protection groups
> - VMware vVOLs Protection Groups
> - VMware SRM IP customization using SRM command-line tools
> - One-to-Many and Many-to-One topologies
> - Custom VMware SRM plug-in identifier or extension ID

Deployment workflow

The workflow diagram shows the Primary Azure VMware Solution to secondary workflow. In addition, it shows steps to take within the Azure portal and the VMware vSphere environments of Azure VMware Solution to achieve the end-to-end protection of VMs.



Prerequisites

Ensure you provide the remote user the VMware VRM administrator and VMware SRM administrator roles in the remote vCenter Server.

Scenario: On-premises to Azure VMware Solution

- Azure VMware Solution private cloud deployed as a secondary region.
- DNS resolution to on-premises VMware SRM and virtual cloud appliances.

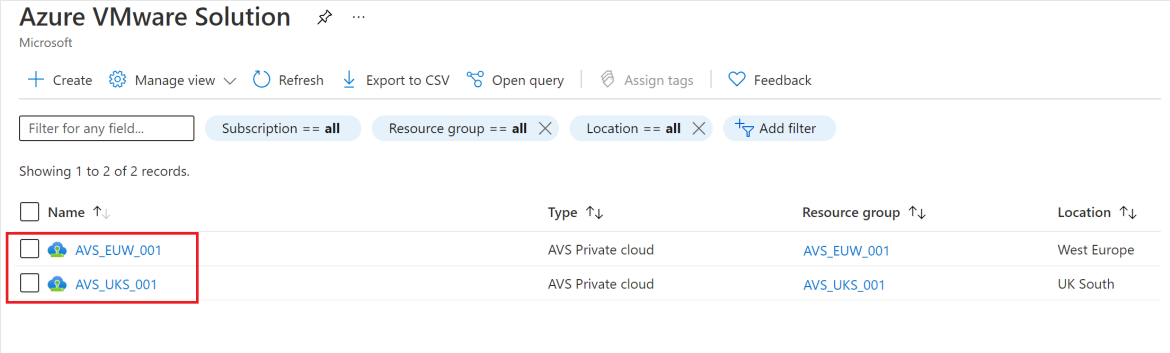
> **Note**
>
> For private clouds created on or after July 1, 2021, you can configure private DNS resolution. For private clouds created before July 1, 2021, that need a

private DNS resolution, open a **support request** to request **Private DNS configuration**.

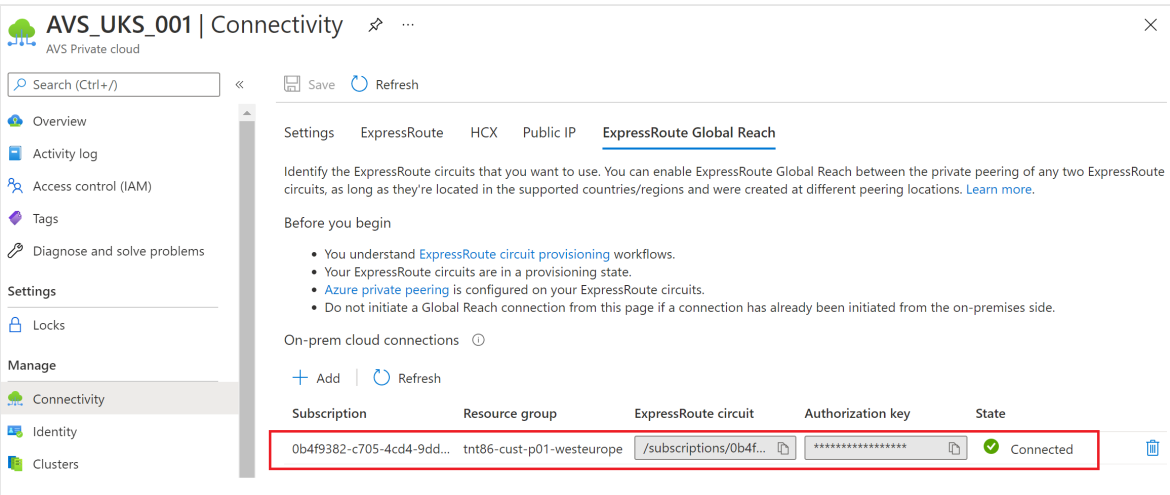
- ExpressRoute connectivity between on-premises VMware vSphere and Azure VMware Solution - 2 Gbps.

Scenario: Primary Azure VMware Solution to secondary

- Azure VMware Solution private cloud must be deployed in the primary and secondary region.



- Connectivity, like ExpressRoute Global Reach, between the source and target Azure VMware Solution private cloud.



Install SRM in Azure VMware Solution

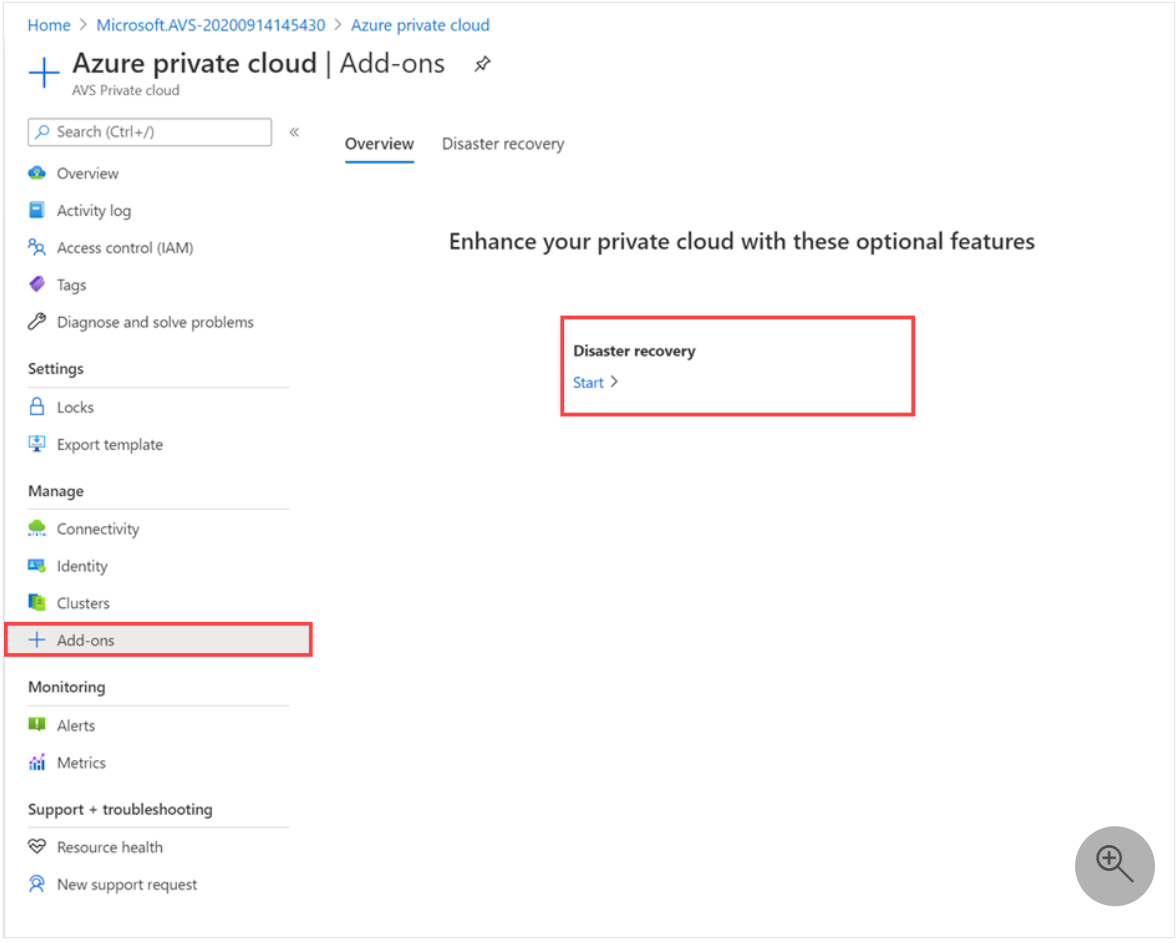
1. In your on-premises data center, install VMware SRM and vSphere Replication.

> **Note**
>
> Use the **Two-site Topology with one vCenter Server instance per PSC** deployment model. Also, make sure that the **required vSphere Replication**

Network ports are opened.

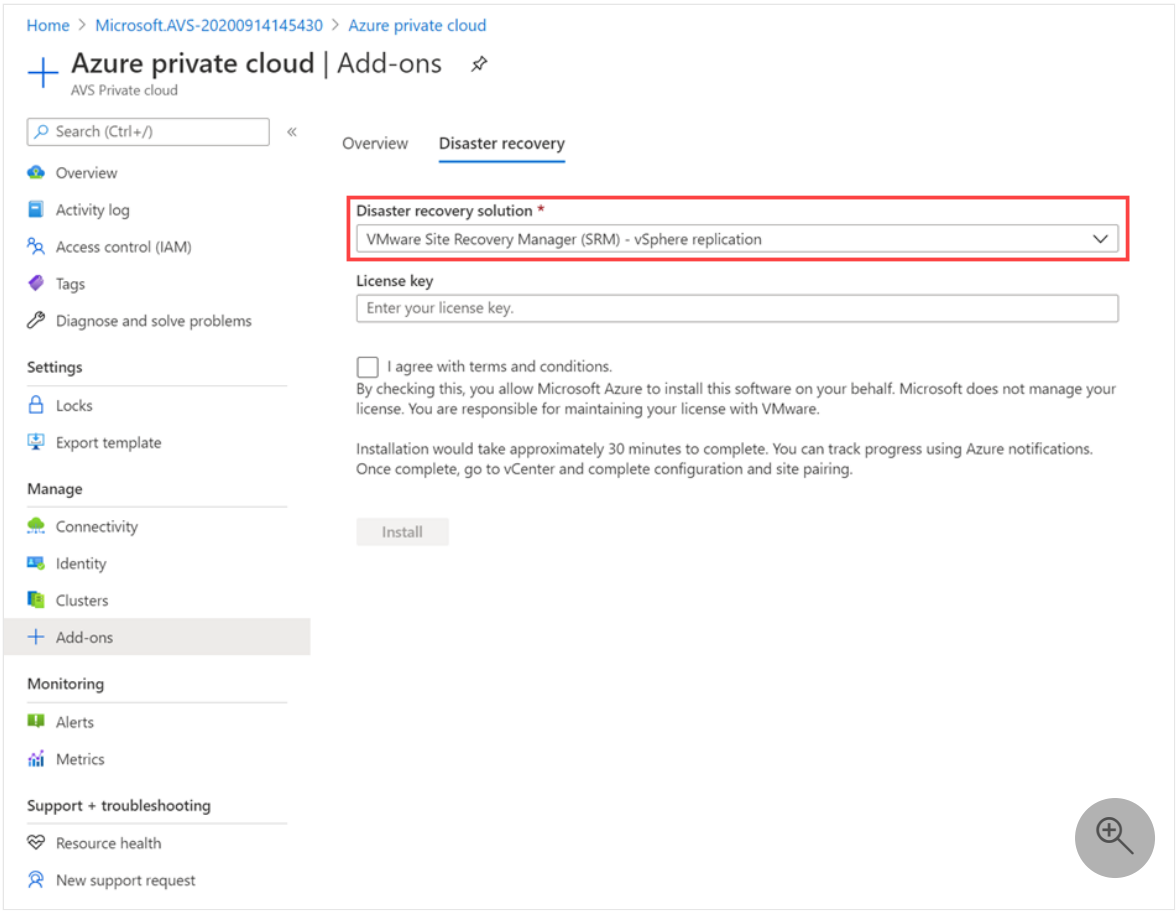
2. In your Azure VMware Solution private cloud, under **Manage**, select **Add-ons** > **Disaster recovery**.

3. The default CloudAdmin user in the Azure VMware Solution private cloud doesn't have sufficient privileges to install VMware SRM or vSphere Replication. The installation process involves multiple steps outlined in the Prerequisites section. Instead, you can install VMware SRM with vSphere Replication as an add-on service from your Azure VMware Solution private cloud.

4. 

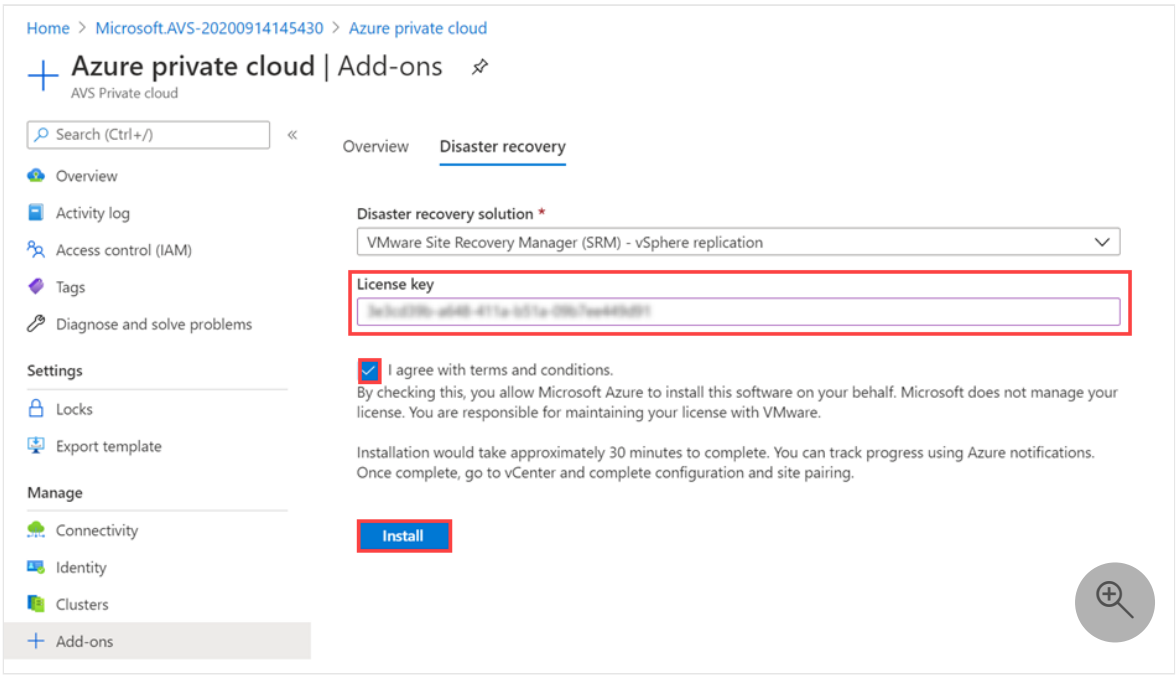
> **Note**
>
> The current version of VMware Site Recovery Manager (SRM) in Azure VMware Solution is 8.5.0.3.

1. From the **Disaster Recovery Solution** drop-down, select **VMware Site Recovery Manager (SRM) – vSphere Replication**.



2. Provide the License key, select agree with terms and conditions, and then select **Install**.

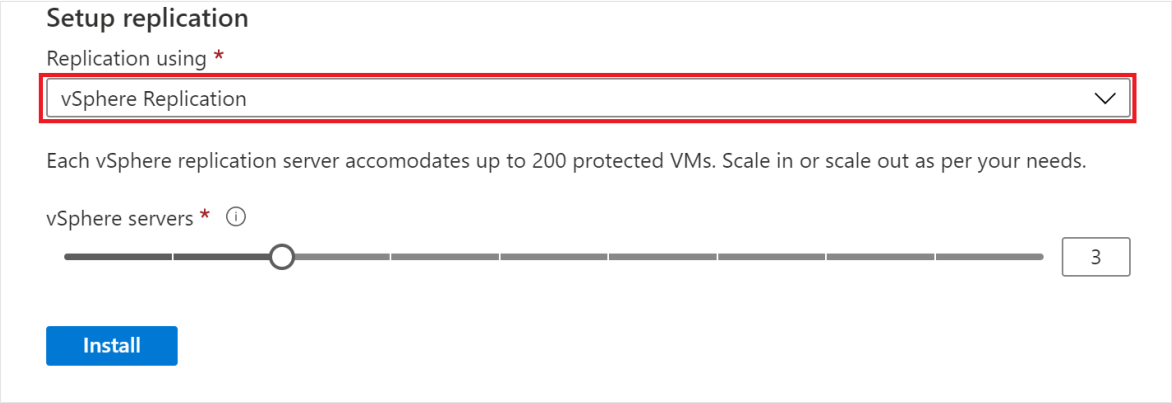
> **Note**
>
> If you don't provide the license key, SRM is installed in an Evaluation mode. The license is used only to enable VMware SRM.



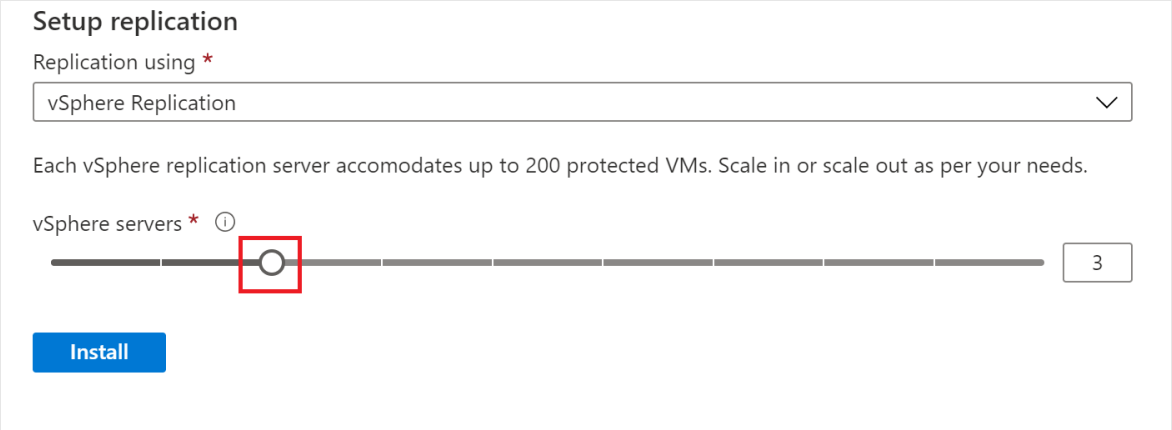
Install the vSphere Replication appliance

After the VMware SRM appliance installs successfully, you'll need to install the vSphere Replication appliances. Each replication server accommodates up to 200 protected VMs. Scale in or scale out as per your needs.

1. From the **Replication using** drop-down, on the **Disaster recovery** tab, select **vSphere Replication**.

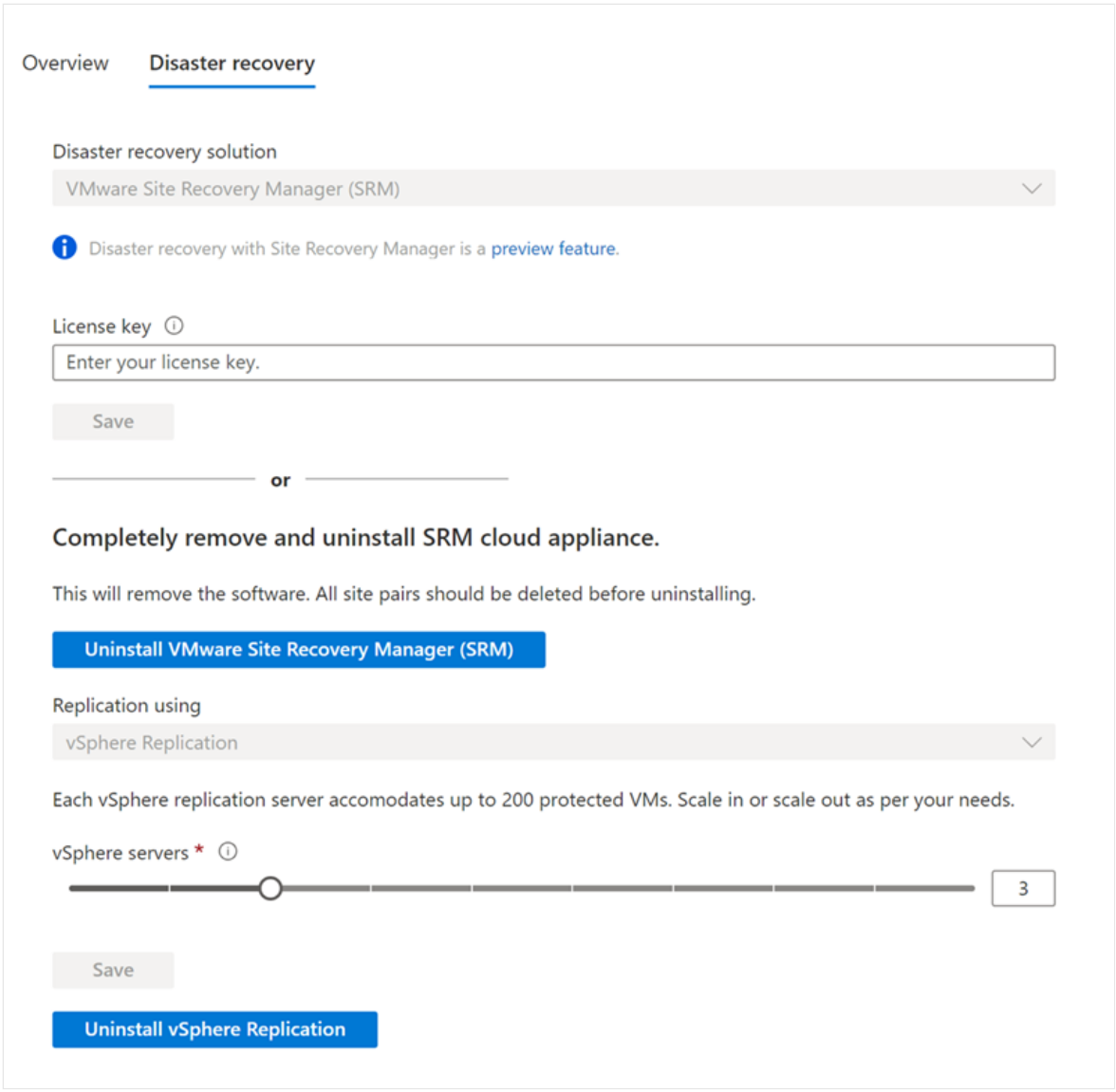


2. Move the vSphere server slider to indicate the number of replication servers you want based on the number of VMs to be protected. Then select **Install**.



3. Once installed, verify that both VMware SRM and the vSphere Replication appliances are installed.

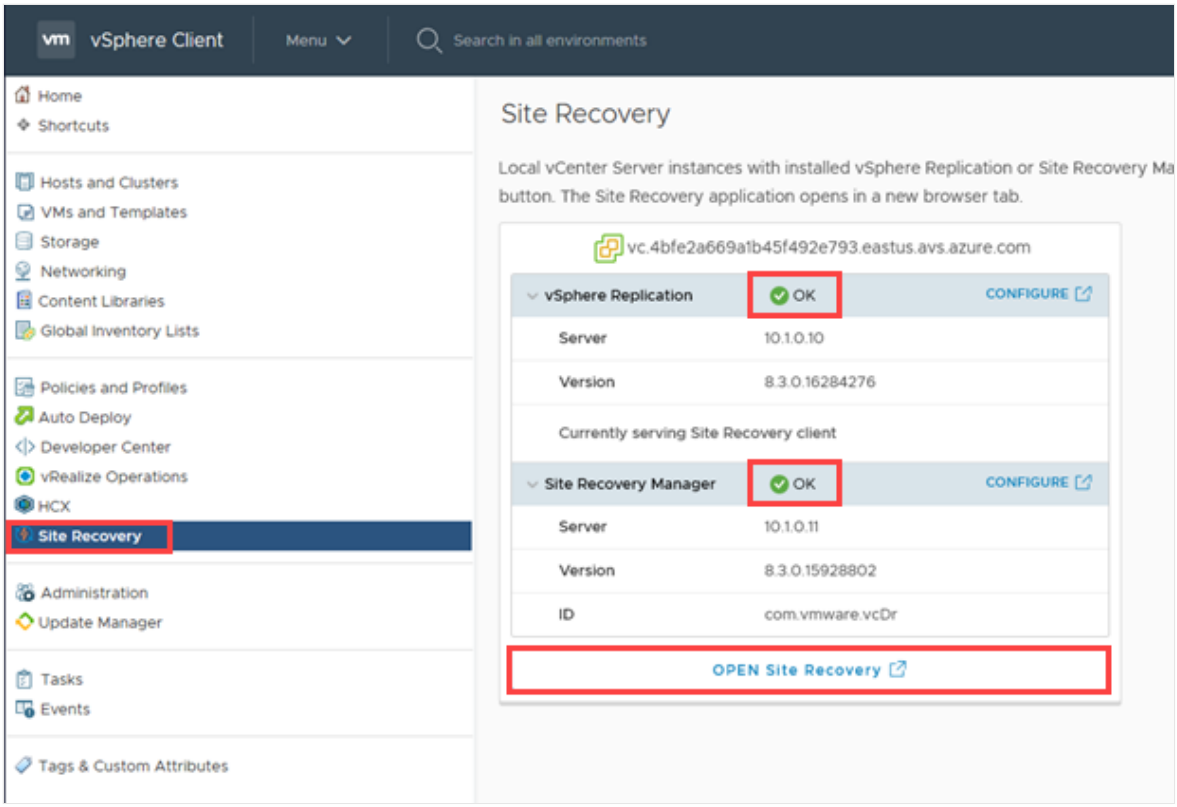
> **Tip**
>
> The Uninstall button indicates that both VMware SRM and the vSphere Replication appliances are currently installed.



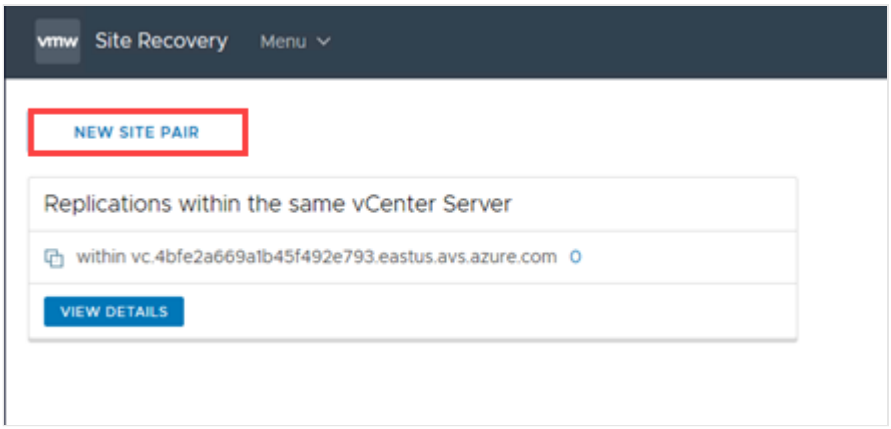
Configure site pairing in vCenter Server

After installing VMware SRM and vSphere Replication, you need to complete the configuration and site pairing in vCenter Server.

1. Sign in to the vSphere Client as cloudadmin@vsphere.local.
2. Navigate to **Site Recovery**, check the status of both vSphere Replication and VMware SRM, and then select **OPEN Site Recovery** to launch the client.



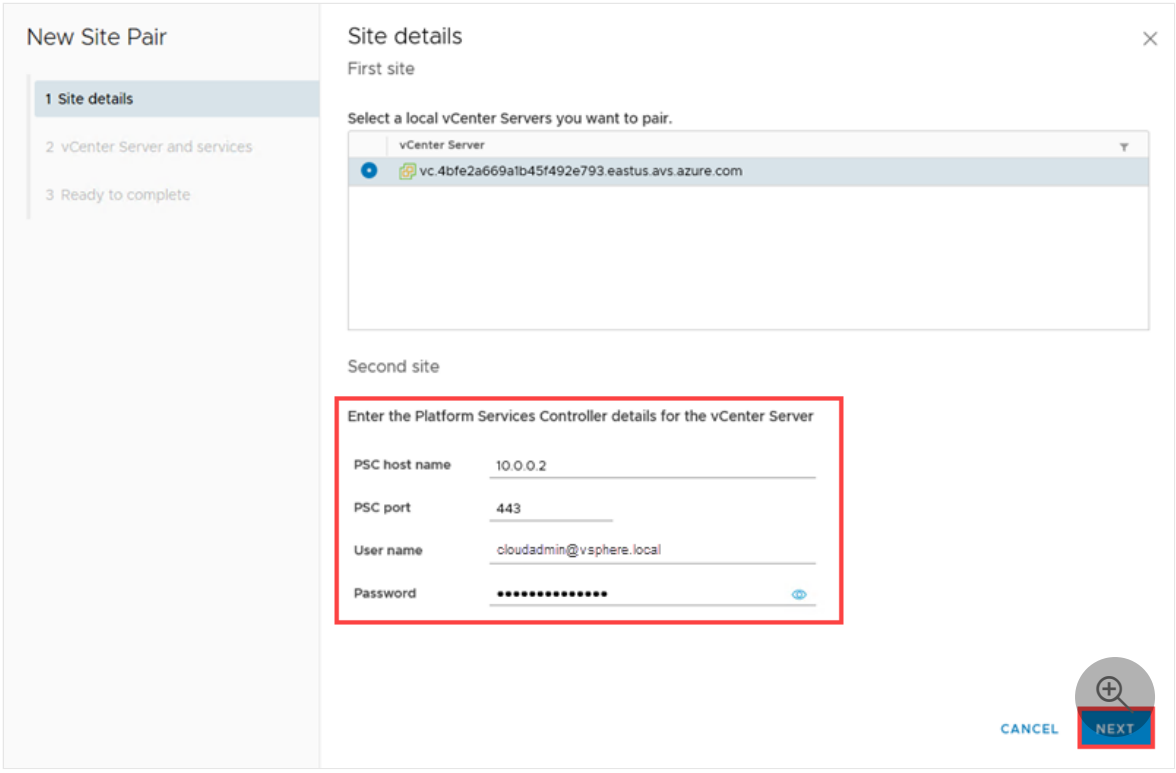
3. Select **NEW SITE PAIR** in the Site Recovery (SR) client in the new tab that opens.



4. Enter the remote site details, and then select **NEXT**.

> **Note**
>
> An Azure VMware Solution private cloud operates with an embedded Platform Services Controller (PSC), so only one local vCenter Server can be selected. If the remote vCenter Server is using an embedded Platform Service Controller (PSC), use the vCenter Server's FQDN (or its IP address) and port to specify the PSC.
>
> The remote user must have sufficient permissions to perform the pairings. An easy way to ensure this is to give that user the VRM administrator and SRM

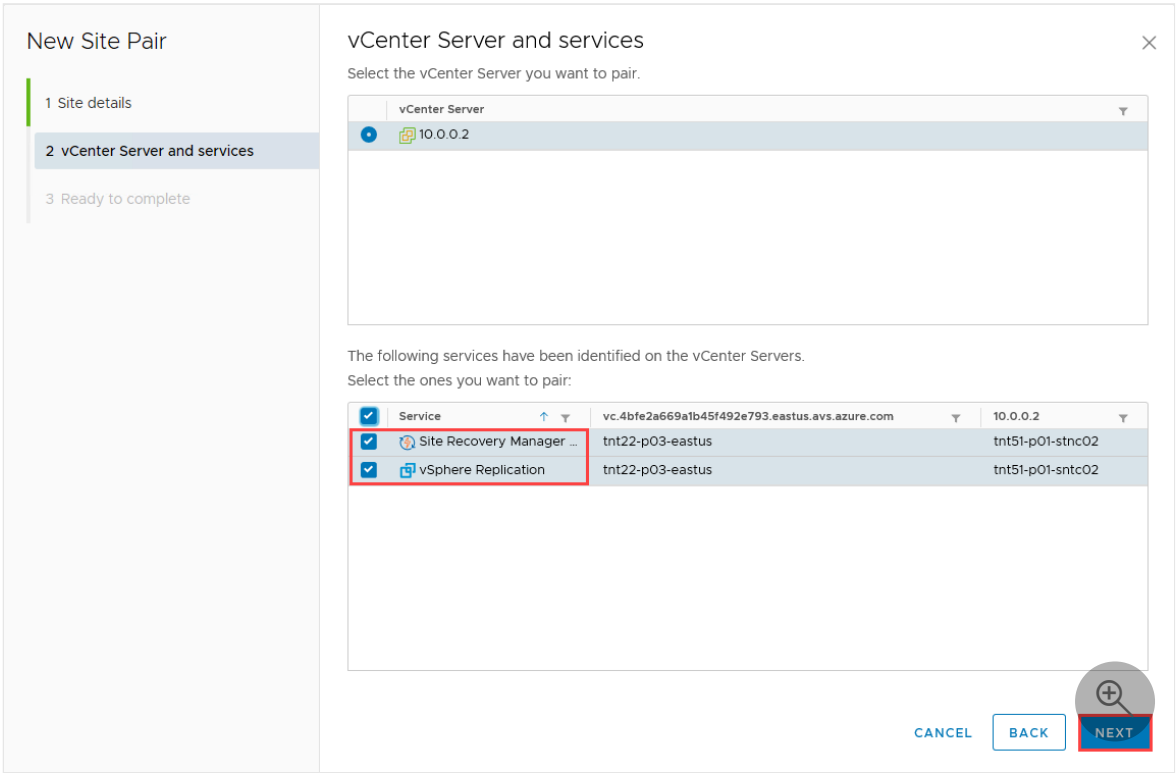
administrator roles in the remote vCenter Server. For a remote Azure VMware Solution private cloud, cloudadmin is configured with those roles.



5. Select **CONNECT** to accept the certificate for the remote vCenter Server.

   At this point, the client should discover the VMware VRM and VMware SRM appliances on both sides as services to pair.

6. Select the appliances to pair and then select **NEXT**.



7. Select **CONNECT** to accept the certificates for the remote VMware SRM and the remote vCenter Server (again).

8. Select **CONNECT** to accept the certificates for the local VMware SRM and the local vCenter Server.

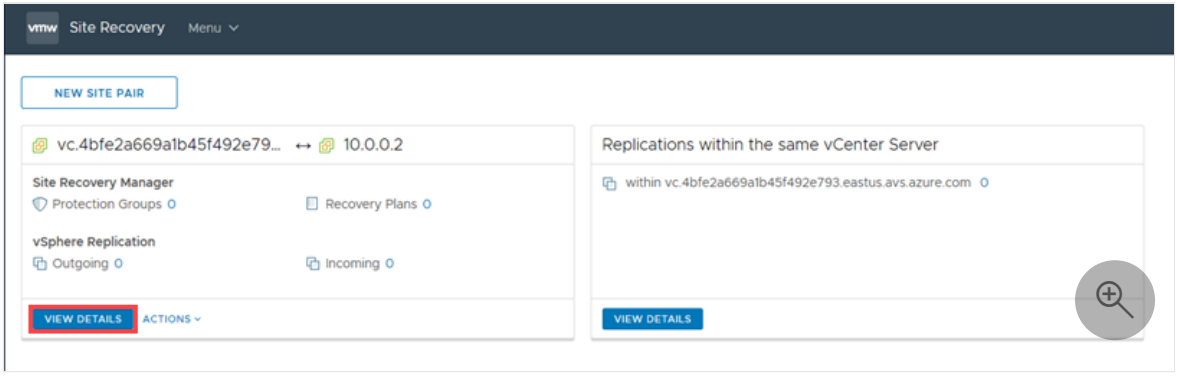
9. Review the settings and then select **FINISH**.

   If successful, the client displays another panel for the pairing. However, if unsuccessful, an alarm is reported.

10. At the bottom, in the right corner, select the double-up arrow to expand the panel to show **Recent Tasks** and **Alarms**.

    > ⓘ Note
    >
    > The SR client sometimes takes a long time to refresh. If an operation seems to take too long or appears "stuck", select the refresh icon on the menu bar.

11. Select **VIEW DETAILS** to open the panel for remote site pairing, which opens a dialog to sign in to the remote vCenter Server.

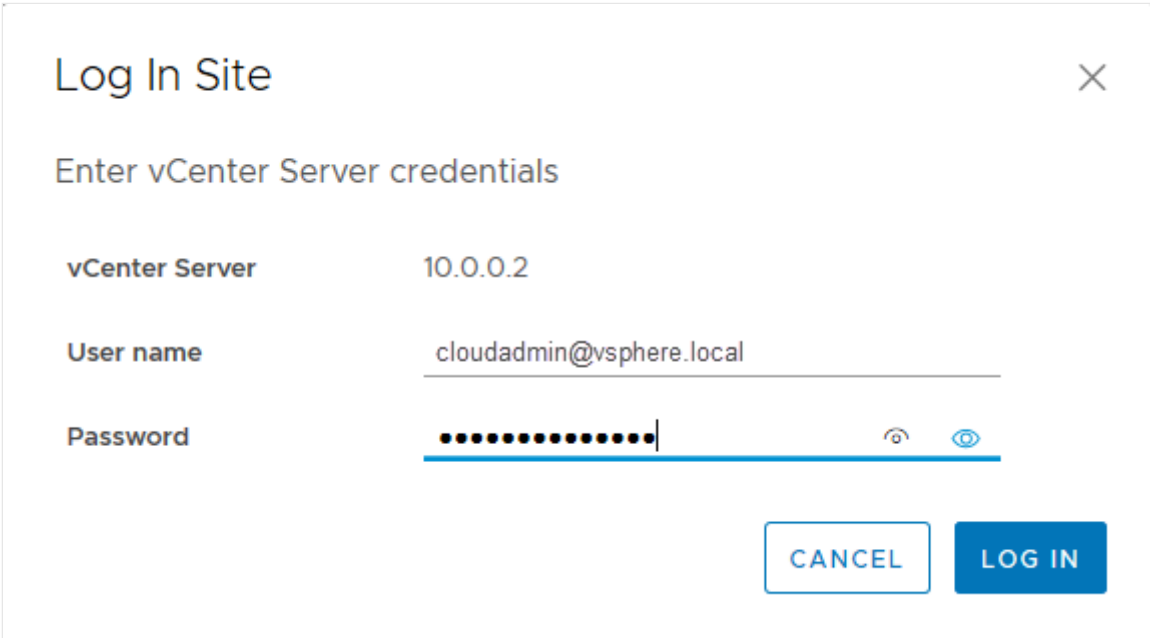


12. Enter the username with sufficient permissions to do replication and site recovery and then select **LOG IN**.

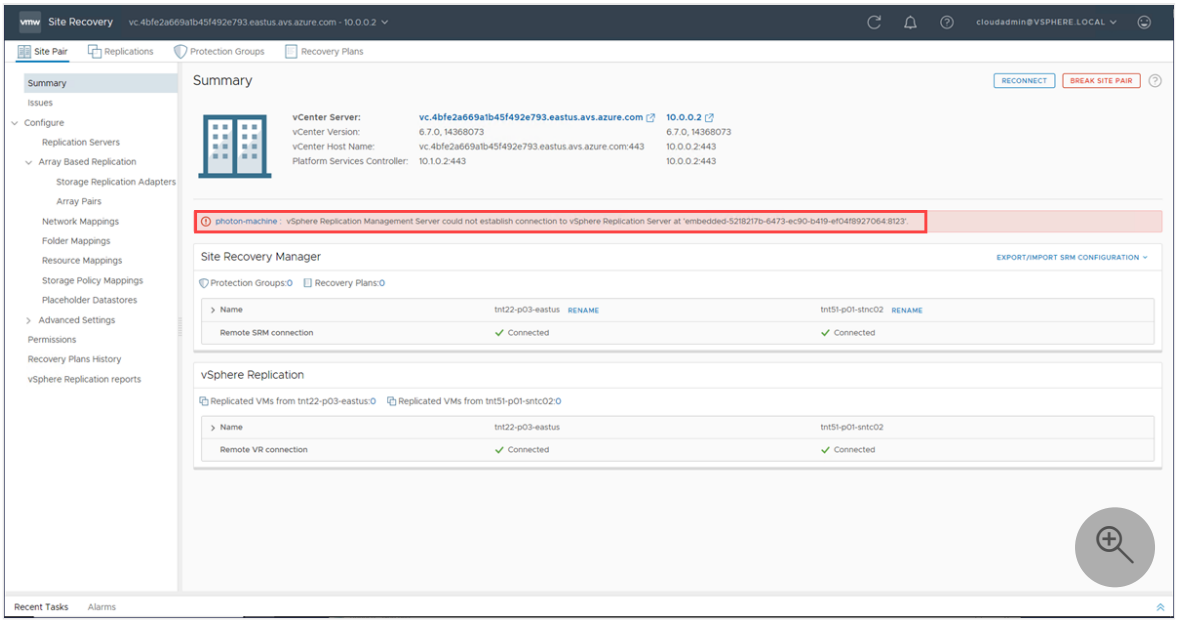
    For pairing, the sign in, which is often a different user, is a one-time action to establish pairing. The SR client requires this sign in every time the client is launched to work with the pairing.

    > ⓘ Note
    >
    > The user with sufficient permissions should have **VRM administrator** and **SRM administrator** roles given to them in the remote vCenter Server. The user should also have access to the remote vCenter Server inventory, like folders

and datastores. For a remote Azure VMware Solution private cloud, the cloudadmin user has the appropriate permissions and access.



You see a warning message indicating that the embedded VRS in the local VRM isn't running. The warning is because Azure VMware Solution doesn't use the embedded VRS in an Azure VMware Solution private cloud, it uses VRS appliances instead.



VMware SRM protection, reprotection, and failback

After you created the site pairing, use the following VMware documentation for end-to-end protection of VMs from the Azure portal.

- Using vSphere Replication with Site Recovery Manager (vmware.com)
- Inventory Mappings for Array-Based Replication Protection Groups and vSphere Replication Protection Groups (vmware.com)
- About Placeholder Virtual Machines (vmware.com)
- vSphere Replication Protection Groups (vmware.com)
- Creating, Testing, and Running Recovery Plans (vmware.com)
- Configuring a Recovery Plan (vmware.com)
- Customizing IP Properties for Virtual Machines (vmware.com)
- How Site Recovery Manager Reprotects Virtual Machines with vSphere Replication (vmware.com)
- Perform a Failback (vmware.com)

> **Note**
>
> If IP Customization Rules have been defined for network mappings between the Azure VMware Solution environment and the on-premises environment, these rules will not be applied on failback from the Azure VMware Solution environment to the on-premises environment due to a **known issue** with SRM 8.3.0. You can work around this limitation by removing protection from all VMs in the Protection Group and then reconfiguring protection on them prior to initiating the failback.

Ongoing management of your VMware SRM solution

Microsoft aims to simplify VMware SRM and vSphere Replication installation on an Azure VMware Solution private cloud. You're responsible for managing your license and the day-to-day operation of the disaster recovery solution.

Scale limitations

To learn about the limits for the VMware Site Recovery Manager Add-On with the Azure VMware Solution, check the Azure subscription and service limits, quotas, and constraints.

VMware SRM licenses

You can install VMware SRM using an evaluation license or a production license. The evaluation license is valid for 60 days. After the evaluation period, you'll be required to obtain a production license of VMware SRM.

You can't use pre-existing on-premises VMware SRM licenses for your Azure VMware Solution private cloud. Work with your sales teams and VMware to acquire a new term-based production license of VMware SRM.

Once a production license of VMware SRM is acquired, you can start using the Azure VMware Solution portal to update VMware SRM with the new production license.

Uninstall VMware SRM

If you no longer require VMware SRM, you must uninstall it in a clean manner. Before you uninstall VMware SRM, you must remove all VMware SRM configurations from both sites in the correct order. If you don't remove all configurations before uninstalling VMware SRM, some VMware SRM components, such as placeholder VMs, might remain in the Azure VMware Solution infrastructure.

1. In the vSphere Client, select **Site Recovery** > **Open Site Recovery**.
2. On the **Site Recovery** home tab, select a site pair and select **View Details**.
3. Select the **Recovery Plans** tab, right-click on a recovery plan and select **Delete**.

   > ⓘ **Note**
   >
   > You cannot delete recovery plans that are running.

4. Select the **Protection Groups** tab, select a protection group, and select the **Virtual Machines** tab.
5. Highlight all virtual machines, right-click, and select **Remove Protection**.

   Removing protection from a VM deletes the placeholder VM from the recovery site. Repeat this operation for all protection groups.
6. In the **Protection Groups** tab, right-click a protection group and select **Delete**.

   > ⓘ **Note**

> You cannot delete a protection group that is included in a recovery plan. You cannot delete vSphere Replication protection groups that contain virtual machines on which protection is still configured.

7. Select **Site Pair** > **Configure** and remove all inventory mappings.

   a. Select each of the **Network Mappings**, **Folder Mappings**, and **Resource Mappings** tabs.

   b. In each tab, select a site, right-click a mapping, and select **Delete**.

8. For both sites, select **Placeholder Datastores**, right-click the placeholder datastore, and select **Remove**.

9. Select **Site Pair** > **Summary**, and select **Break Site Pair**.

   > ⓘ **Note**
   >
   > Breaking the site pairing removes all information related to registering Site Recovery Manager with Site Recovery Manager, vCenter Server, and the Platform Services Controller on the remote site.

10. In your private cloud, under **Manage**, select **Add-ons** > **Disaster recovery**, and then select **Uninstall the replication appliances**.

11. Once replication appliances are uninstalled, from the **Disaster recovery** tab, select **Uninstall for the Site Recovery Manager**.

12. Repeat these steps on the secondary Azure VMware Solution site.

Support

VMware Site Recovery Manager (SRM) is a Disaster Recovery solution from VMware.

Microsoft only supports install/uninstall of VMware SRM and vSphere Replication Manager and scale up/down of vSphere Replication appliances within Azure VMware Solution.

For all other issues, such as configuration and replication, contact VMware for support.

VMware and Microsoft support teams engage each other as needed to troubleshoot VMware SRM issues on Azure VMware Solution.

References

- VMware Site Recovery Manager Documentation
- Compatibility Matrices for VMware Site Recovery Manager 8.3
- VMware SRM 8.3 release notes
- VMware vSphere Replication Documentation
- Compatibility Matrices for vSphere Replication 8.3
- Operational Limits of Site Recovery Manager 8.3
- Operational Limits of vSphere Replication 8.3
- Calculate bandwidth for vSphere Replication
- SRM installation and configuration
- vSphere Replication administration
- Prerequisites and Best Practices for SRM installation
- Network ports for SRM
- Network ports for vSphere Replication

Deploy Zerto disaster recovery on Azure VMware Solution

Article • 08/08/2024

> **Important**
>
> AV64 node type does not support Zerto Disaster Recovery at the moment. You can contact your Zerto account team to get more information and an estimate of when this will be available.

In this article, learn how to implement disaster recovery for on-premises VMware or Azure VMware Solution-based virtual machines (VMs). The solution in this article uses Zerto disaster recovery. Instances of Zerto are deployed at both the protected and the recovery sites.

Zerto is a disaster recovery solution designed to minimize downtime of VMs should a disaster occur. Zerto's platform is built on the foundation of Continuous Data Protection (CDP) that enables minimal or close to no data loss. The platform provides the level of protection wanted for many business-critical and mission-critical enterprise applications. Zerto also automates and orchestrates failover and failback to ensure minimal downtime in a disaster. Overall, Zerto simplifies management through automation and ensures fast and highly predictable recovery times.

Core components of the Zerto platform

Expand table

Component	Description
Zerto Virtual Manager (ZVM)	Management application for Zerto implemented as a Windows service installed on a Windows VM. The private cloud administrator installs and manages the Windows VM. The ZVM enables Day 0 and Day 2 disaster recovery configuration. For example, configuring primary and disaster recovery sites, protecting VMs, recovering VMs, and so on. However, it doesn't handle the replication data of the protected customer VMs.
Virtual Replication appliance (vRA)	Linux VM to handle data replication from the source to the replication target. One instance of vRA is installed per ESXi host, delivering a true scale architecture that grows and shrinks along with the private cloud's hosts. The vRA manages data replication to and from protected VMs to its local or remote target, storing the data in the journal.

Component	Description
Zerto ESXi host driver	Installed on each VMware ESXi host configured for Zerto disaster recovery. The host driver intercepts a vSphere VM's IO and sends the replication data to the chosen vRA for that host. The vRA is then responsible for replicating the VM's data to one or more disaster recovery targets.
Zerto Cloud Appliance (ZCA)	Windows VM only used when Zerto is used to recover vSphere VMs as Azure Native IaaS VMs. The ZCA is composed of: • **ZVM:** A Windows service that hosts the UI and integrates with the native APIs of Azure for management and orchestration. • **VRA:** A Windows service that replicates the data from or to Azure. The ZCA integrates natively with the platform it gets deployed on, allowing you to use Azure Blob storage within a storage account on Microsoft Azure. As a result, it ensures the most cost-efficient deployment on each of these platforms.
Virtual Protection Group (VPG)	Logical group of VMs created on the ZVM. Zerto allows configuring disaster recovery, Backup, and Mobility policies on a VPG. This mechanism enables a consistent set of policies to be applied to a group of VMs.

To learn more about Zerto platform architecture, see the Zerto Platform Architecture Guide.

Supported Zerto scenarios

You can use Zerto with Azure VMware Solution for the following three scenarios.

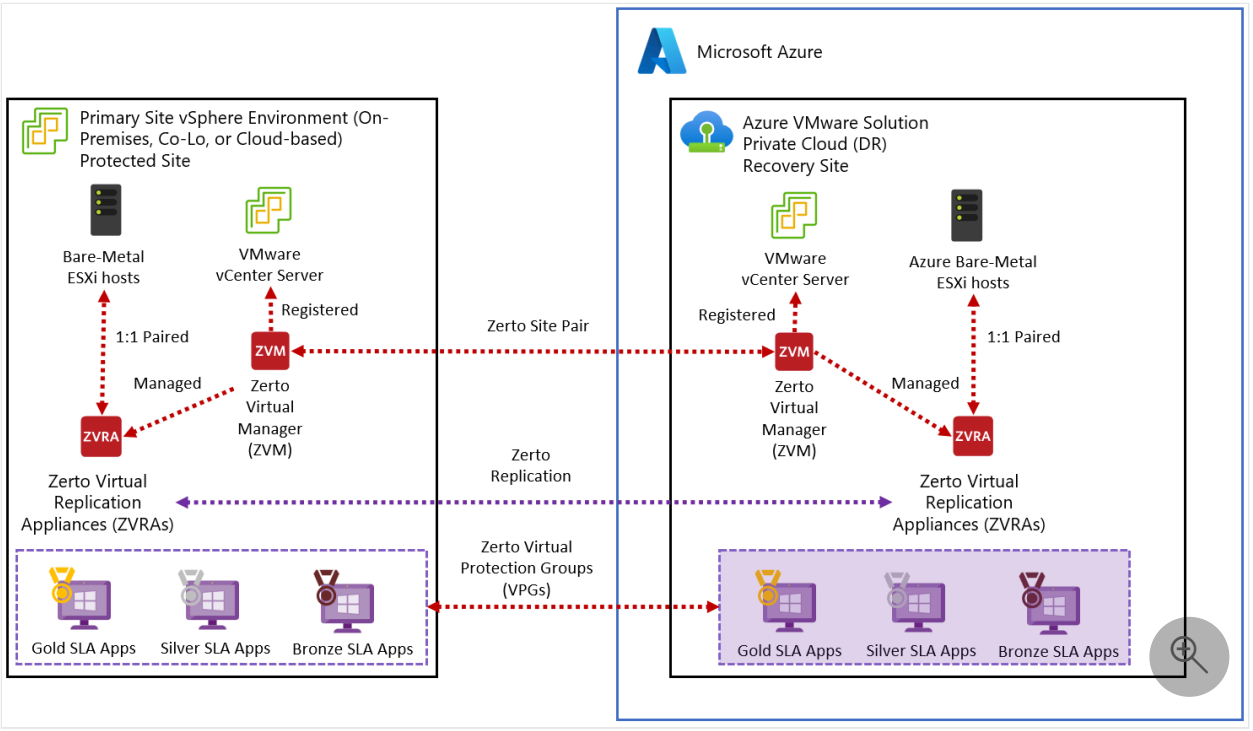
> **Note**
>
> For Azure NetApp Files (ANFs), Azure VMware Solution supports Network File System (NFS) datastores as a persistent storage option. You can create NFS datastores with Azure NetApp Files volumes and attach them to clusters of your choice. You can also create virtual machines (VMs) for optimal cost and performance. To leverage ANF datastores, select them as a Recovery Datastore in the Zerto VPG wizard when creating or editing a VPG.

> **Tip**
>
> Explore more about ANF datastores and how to Attach Azure NetApp datastores to Azure VMware Solution hosts.

> **Important**
>
> AV64 node type does not support Zerto Disaster Recovery at the moment. You can contact your Zerto account team to get more information and an estimate of when this will be available.

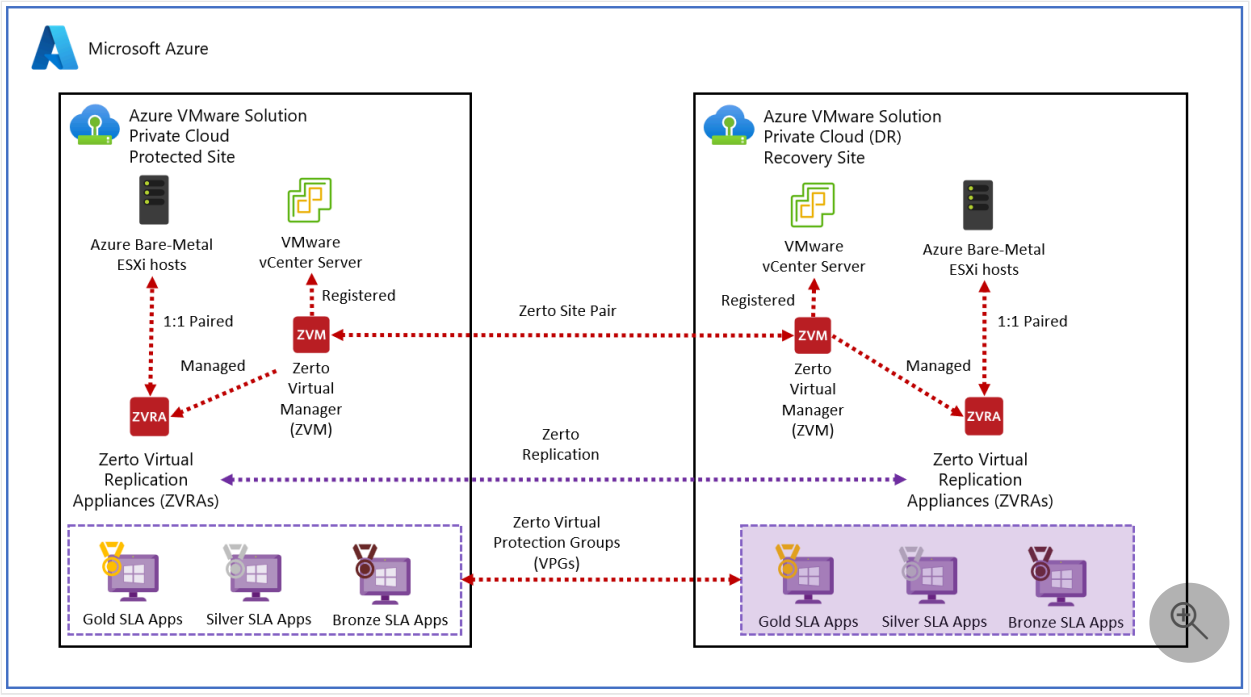
Scenario 1: On-premises VMware vSphere to Azure VMware Solution disaster recovery

In this scenario, the primary site is an on-premises vSphere-based environment. The disaster recovery site is an Azure VMware Solution private cloud.



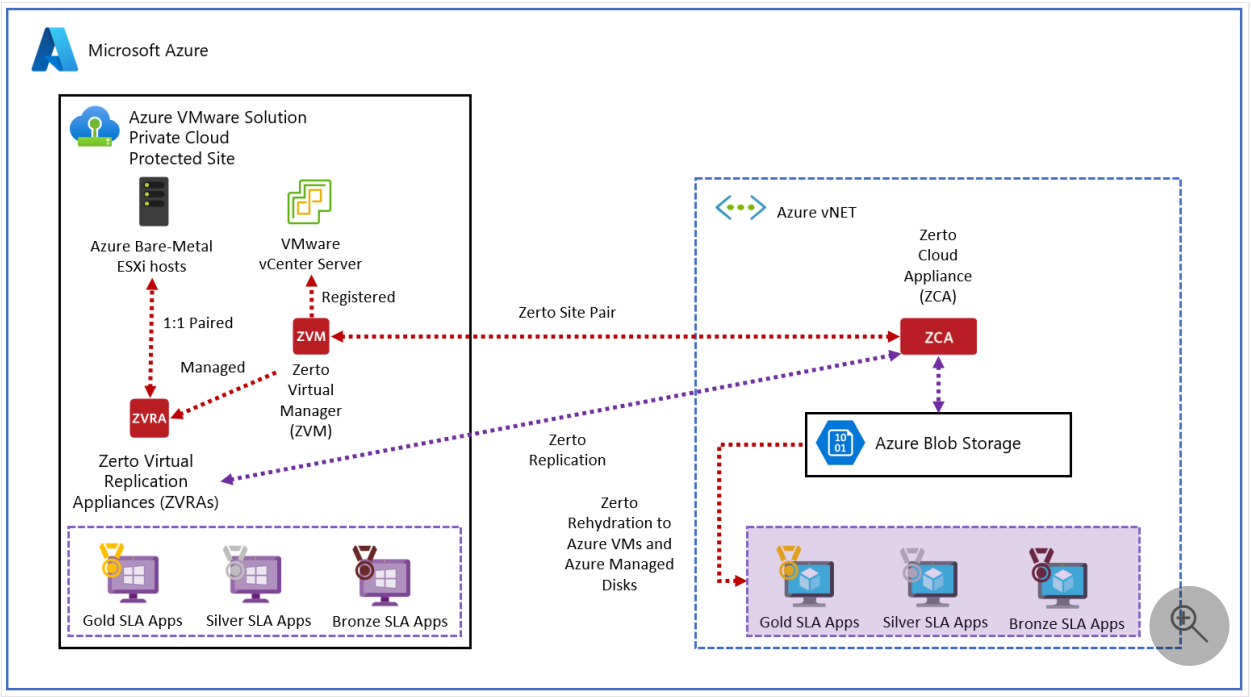
Scenario 2: Azure VMware Solution to Azure VMware Solution cloud disaster recovery

In this scenario, the primary site is an Azure VMware Solution private cloud in one Azure Region. The disaster recovery site is an Azure VMware Solution private cloud in a different Azure Region.



Scenario 3: Azure VMware Solution to Azure VMs cloud disaster recovery

In this scenario, the primary site is an Azure VMware Solution private cloud in one Azure Region. Azure Blobs and Azure VMs (Hyper-V based) are used in times of Disaster.



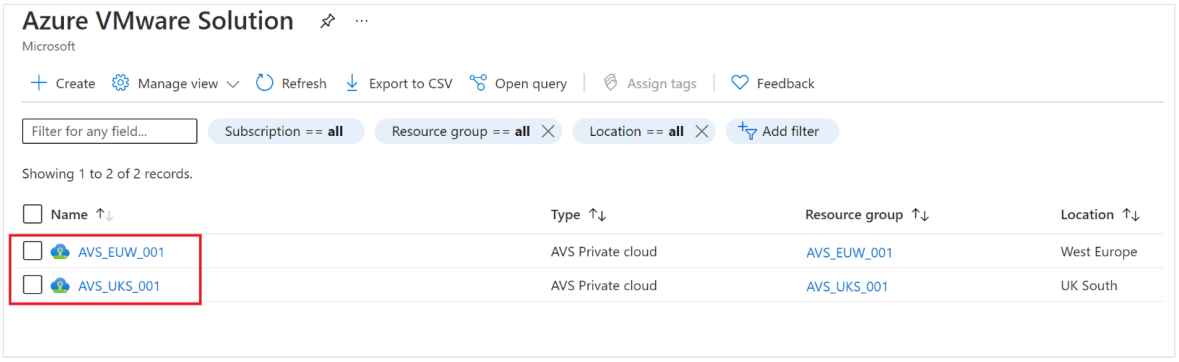
Prerequisites

On-premises VMware to Azure VMware Solution disaster recovery

- Azure VMware Solution private cloud deployed as a secondary region.
- VPN or ExpressRoute connectivity between on-premises and Azure VMware Solution.

Azure VMware Solution to Azure VMware Solution cloud disaster recovery

- Azure VMware Solution private cloud must be deployed in the primary and secondary regions.



- Connectivity, like ExpressRoute Global Reach, between the source and target Azure VMware Solution private cloud.

Azure VMware Solution IaaS VMs cloud disaster recovery

- Network connectivity, ExpressRoute based, from Azure VMware Solution to the virtual network used for disaster recovery.
- Follow the Zerto Virtual Replication Azure Quickstart Guide for the rest of the prerequisites.

Install Zerto on Azure VMware Solution

To deploy Zerto on Azure VMware Solution, follow these instructions.

FAQs

Can I use a pre-existing Zerto product license on Azure VMware Solution?

You can reuse pre-existing Zerto product licenses for Azure VMware Solution environments. If you need new Zerto licenses, email Zerto at **info@zerto.com** to acquire new licenses.

How is Zerto supported?

Zerto disaster recovery is a solution sold and supported by Zerto. For any support issue with Zerto disaster recovery, always contact Zerto support.

Zerto and Microsoft support teams engage each other as needed to troubleshoot Zerto disaster recovery issues on Azure VMware Solution.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Deploy disaster recovery using JetStream DR software

Article • 03/22/2024

JetStream DR is a cloud-native disaster recovery solution designed to minimize downtime of virtual machines (VMs) if there's a disaster. Instances of JetStream DR are deployed at both the protected and recovery sites.

JetStream is built on the foundation of Continuous Data Protection (CDP), using VMware vSphere API for I/O filtering (VAIO) framework, which enables minimal or close to no data loss. JetStream DR provides the level of protection wanted for business and mission-critical applications. It also enables cost-effective DR by using minimal resources at the DR site and using cost-effective cloud storage, such as Azure Blob Storage.

In this article, learn how to implement JetStream DR for your Azure VMware Solution private cloud and on-premises VMware vSphere workloads.

To learn more about JetStream DR, see:

- JetStream Solution brief
- JetStream DR on Azure Marketplace

Core components of the JetStream DR solution

Expand table

Items	Description
JetStream Management Server Virtual Appliance (MSA)	MSA enables both Day 0 and Day 2 configuration, such as primary sites, protection domains, and recovering VMs. The MSA is deployed from an OVA file on a vSphere node by the cloud admin. The MSA collects and maintains statistics relevant to VM protection and implements a vCenter Server plugin that allows you to manage JetStream DR natively with the vSphere Client. The MSA doesn't handle replication data of protected VMs.
JetStream DR Virtual Appliance (DRVA)	Linux-based Virtual Machine appliance receives protected VMs replication data from the source ESXi host. It maintains the replication log and manages the transfer of the VMs and their data to the object store such as Azure Blob Storage. Depending upon the number of protected VMs and the amount of VM data to replicate, the private cloud admin can create one or more DRVA instances.

Items	Description
JetStream ESXi host components (IO Filter packages)	JetStream software installed on each ESXi host configured for JetStream DR. The host driver intercepts the vSphere VMs I/O and sends the replication data to the DRVA. The IO filters also monitor relevant events, such as vMotion, Storage vMotion, snapshots, etc.
JetStream Protected Domain	Logical group of VMs that are protected together using the same policies and runbook. The data for all VMs in a protection domain is stored in the same Azure Blob container instance. A single DRVA instance handles replication to remote DR storage for all VMs in a Protected Domain.
Azure Blob Storage containers	The protected VM's replicated data is stored in Azure Blobs. JetStream software creates one Azure Blob container instance for each JetStream Protected Domain.

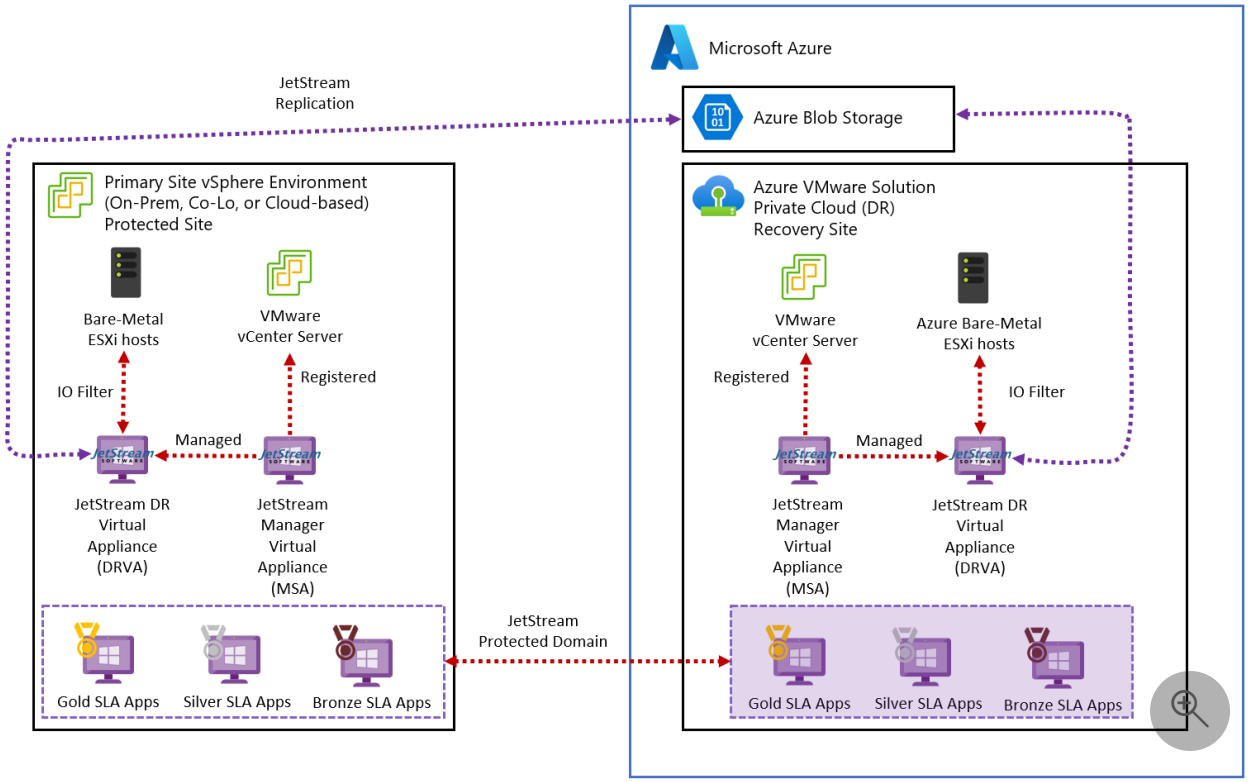
JetStream scenarios on Azure VMware Solution

You can use JetStream DR with Azure VMware Solution for the following two scenarios:

- On-premises VMware vSphere to Azure VMware Solution DR
- Azure VMware Solution to Azure VMware Solution DR

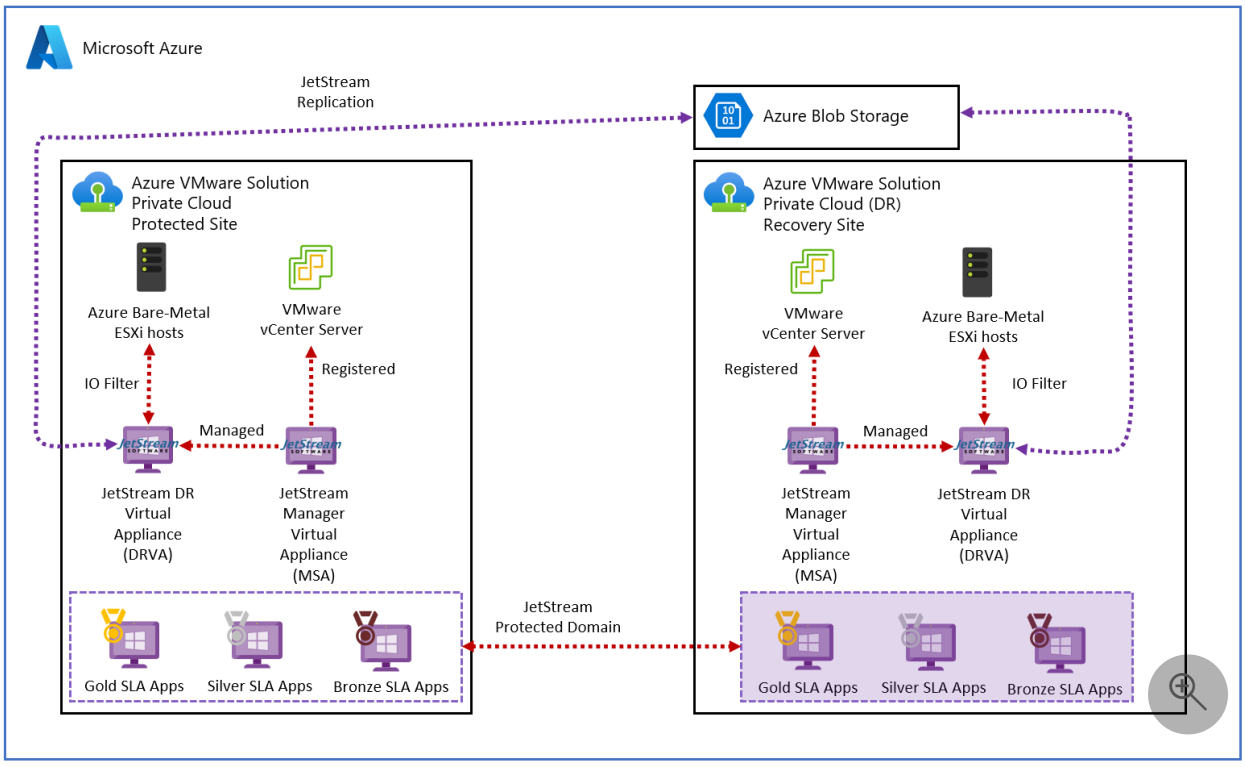
Scenario 1: On-premises VMware vSphere to Azure VMware Solution DR

In this scenario, the primary site is your on-premises VMware vSphere environment and the DR site is an Azure VMware Solution private cloud.



Scenario 2: Azure VMware Solution to Azure VMware Solution DR

In this scenario, the primary site is an Azure VMware Solution private cloud in one Azure region. The disaster recovery site is an Azure VMware Solution private cloud in a different Azure region.



Disaster Recovery with Azure NetApp Files, JetStream DR and Azure VMware Solution

Disaster Recovery to cloud is a resilient and cost-effective way of protecting the workloads against site outages and data corruption events like ransomware. Using the VMware VAIO framework, on-premises VMware workloads can be replicated to Azure Blob storage and recovered with minimal or close to no data loss and near-zero Recovery Time Objective (RTO). JetStream DR can seamlessly recover workloads replicated from on-premises to Azure VMware Solution and specifically to Azure NetApp Files.

JetStream DR enables cost-effective disaster recovery by consuming minimal resources at the DR site and using cost-effective cloud storage. JetStream DR automates recovery to Azure NetApp Files (ANF) datastores using Azure Blob Storage. It can recover independent VMs or groups of related VMs into the recovery site infrastructure according to runbook settings. It also provides point-in-time recovery for ransomware protection.

Install JetStream DR

To install JetStream DR in the on-premises data center and in the Azure VMware Solution private cloud:

- Install JetStream DR in the on-premises data center:
  - Download the JetStream DR bundle from Azure Marketplace (ZIP) and deploy the JetStream DR MSA (OVA) in the designated cluster.
  - Configure the cluster with the IO filter package (install JetStream VIB).
  - Create Azure Blob (Azure Storage Account) in the same region as the DR Azure VMware Solution cluster.
  - Deploy the disaster recovery virtual appliance (DRVA) and assign a replication log volume (VMDK from existing datastore or shared iSCSI storage).
  - Create Protected Domains (groups of related VMs) and assign DRVAs and the Azure Blob Storage/ANF.
  - Start protection.

- Install JetStream DR in the Azure VMware Solution private cloud:
  - Use the Run command to install and configure JetStream DR.
  - Add the same Azure Blob container and discover domains using the Scan Domain option.
  - Deploy the DRVA appliance.
  - Create a replication log volume using an available vSAN or ANF datastore.

    - Import protected domains and configure RocVA (recovery VA) to use ANF datastore for VM placements.
    - Select the appropriate failover option and start continuous rehydration for near-zero RTO domains/VMs.

- During a disaster event, trigger failover to Azure NetApp Files datastores in the designated Azure VMware Solution DR site.

- Invoke failback to the protected site after the protected site is recovered.

Ransomware recovery

Recovering from ransomware can be a daunting task. It can be hard for IT organizations to pinpoint what the 'safe point of return' is and how to ensure that recovered workloads are safeguarded from the attacks reoccurring by sleeping malware or through vulnerable applications.

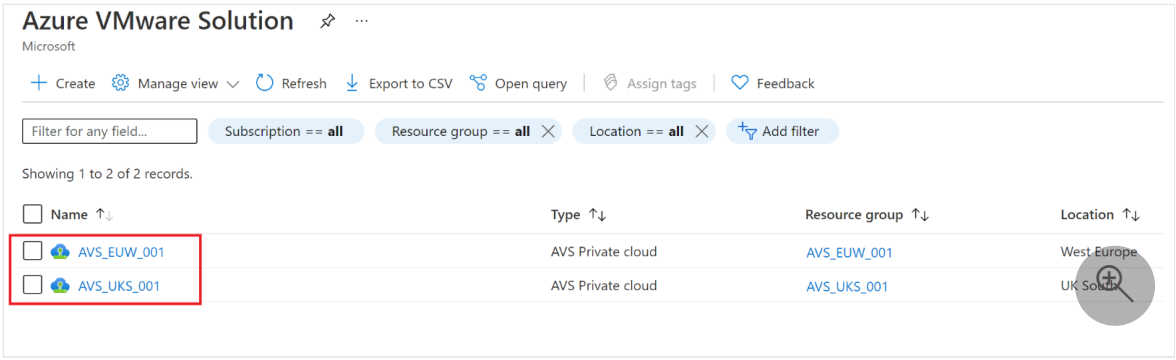
JetStream DR for Azure VMware Solution together with Azure NetApp Files datastores can address these concerns by allowing organizations to recover from an available point-in-time. It ensures workloads are recovered to a functional and isolated network if necessary. It allows the applications to function and communicate with each other without exposing them to any North-South traffic. It also gives security teams a safe place to perform forensics, and conduct other recovery measures.

For full details, refer to the article: Disaster Recovery with Azure NetApp Files, JetStream DR and Azure VMware Solution.

Prerequisites

Scenario 1: On-premises VMware vSphere to Azure VMware Solution DR

- Azure VMware Solution private cloud deployed with a minimum of three nodes in the target DR region.



- Network connectivity configured between the primary site JetStream appliances and the Azure Storage blob instance.
- Setup and Subscribe to JetStream DR from the Azure Marketplace to download the JetStream DR software.
- Azure Blob Storage account created using either Standard or Premium Performance tier. For access tier, select **Hot**.

  > **Note**
  >
  > The **Enable hierarchical namespace** option on the blob isn't supported.

- An NSX-T network segment configured on Azure VMware Solution private cloud with DHCP enabled on the segment for the transient JetStream Virtual appliances is employed during recovery or failover.
- A DNS server configured to resolve the IP addresses of Azure VMware Solution vCenter Server, Azure VMware Solution ESXi hosts, Azure Storage account, and the JetStream Marketplace service for the JetStream virtual appliances.
- (Optional) Azure NetApp Files volume(s) are created and attached to the Azure VMware Solution private cloud for recovery or failover of protected VMs to Azure NetApp Files backed datastores.
  - Attach Azure NetApp Files datastores to Azure VMware Solution hosts
  - Disaster Recovery with Azure NetApp Files, JetStream DR, and Azure VMware Solution

Scenario 2: Azure VMware Solution to Azure VMware Solution DR

- Azure VMware Solution private cloud deployed with a minimum of three nodes in both the primary and secondary regions.

- Network connectivity configured between the primary site JetStream appliances and the Azure Storage blob instance.
- Setup and Subscribe to JetStream DR from the Azure Marketplace to download the JetStream DR software.
- Azure Blob Storage account created using either Standard or Premium Performance tier. For access tier, select **Hot**.

  > **Note**
  >
  > The **Enable hierarchical namespace** option on the blob isn't supported.

- An NSX-T network segment configured on Azure VMware Solution private cloud with DHCP enabled on the segment for the transient JetStream Virtual appliances employed during recovery or failover.
- DNS configured on both the primary and DR sites to resolve the IP addresses of Azure VMware Solution vCenter Server, Azure VMware Solution ESXi hosts, Azure Storage account, the JetStream DR Management Server Appliance (MSA) and the JetStream Marketplace service for the JetStream virtual appliances.
- (Optional) Azure NetApp Files volume(s) are created and attached to the Azure VMware Solution private cloud for recovery or failover of protected VMs to Azure NetApp Files backed datastores.
  - Attach Azure NetApp Files datastores to Azure VMware Solution hosts
  - Disaster Recovery with Azure NetApp Files, JetStream DR, and Azure VMware Solution

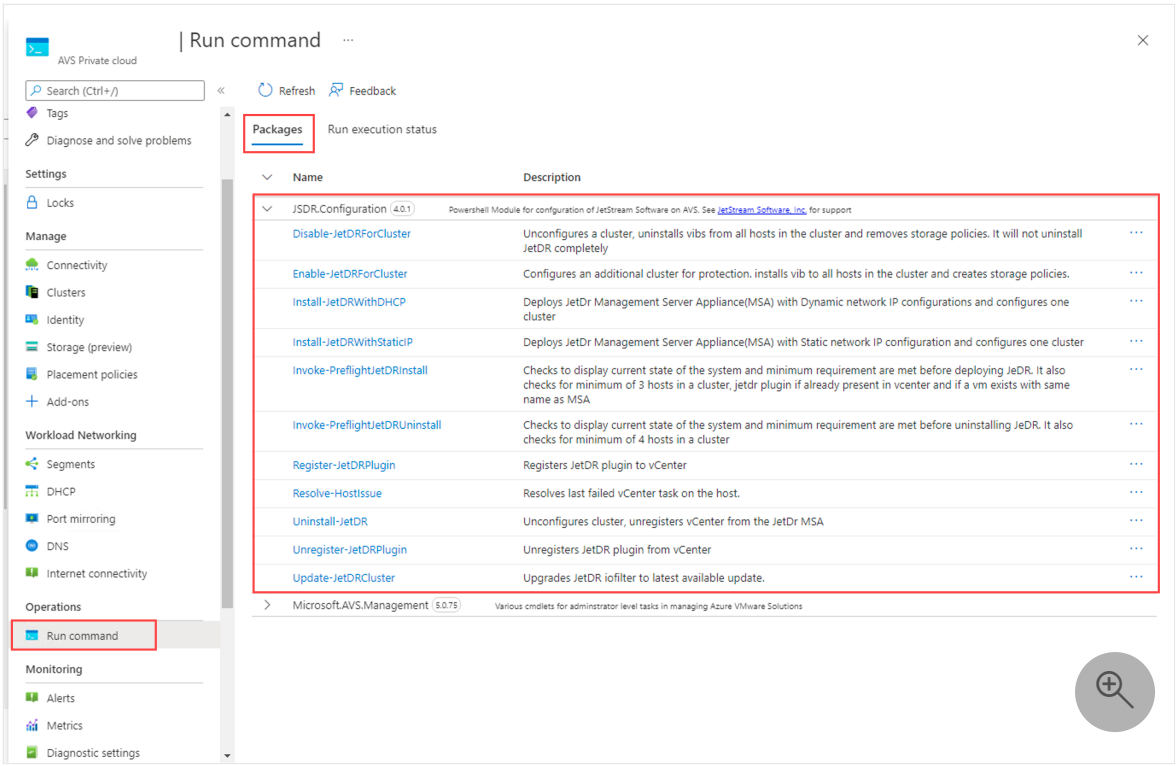
For more on-premises JetStream DR prerequisites, see the JetStream Pre-Installation Guide.

Install JetStream DR on Azure VMware Solution

You can follow these steps for both supported scenarios.

1. In your on-premises data center, install JetStream DR following the JetStream documentation.
2. In your Azure VMware Solution private cloud, install JetStream DR using a Run command. From the Azure portal,select **Run command** > **Packages** > **JSDR.Configuration**.

> **Note**
>
> If you need access to the Azure US Gov portal, go to https://portal.azure.us/



> **Note**
>
> The default CloudAdmin user in Azure VMware Solution doesn't have sufficient privileges to install JetStream DR. Azure VMware Solution enables simplified and automated installation of JetStream DR by invoking the Azure VMware Solution Run command for JetStream DR.

3. Run the **Invoke-PreflightJetDRInstall** cmdlet, which checks if the prerequisites for installing JetStream DR are met. For example, it validates the required number of hosts, cluster names, and unique VM names.

4. Provide the required values or change the default values, and then select **Run**.

Expand table

Field	Value
Network	Name of the NSX-T Data Center network segment where you must deploy the JetStream MSA.
Datastore	Name of the datastore where you deploy the JetStream MSA.

Field	Value
ProtectedCluster	Name of the Azure VMware Solution private cloud cluster to be protected, for example, **Cluster-1**. You can only provide one cluster name.
Cluster	Name of the Azure VMware Solution private cluster where the JetStream MSA gets deployed, for example, **Cluster-1**.
VMName	Name of JetStream MSA VM, for example, **jetstreamServer**.
Specify name for execution	Alphanumeric name of the execution, for example, **Invoke-PreflightJetDRInstall-Exec1**. Used to verify if the cmdlet ran successfully.
Timeout	The period after which a cmdlet exits if taking too long to finish.

5. View the status of the execution.

Install the JetStream DR MSA

Azure VMware Solution supports the installation of JetStream using either static IP addresses or using DHCP-based IP addresses.

Static IP address

1. Select **Run command** > **Packages** > **Install-JetDRWithStaticIP**.
2. Provide the required values or change the default values, and then select **Run**.

Expand table

Field	Value
ProtectedCluster	Name of the Azure VMware Solution private cloud cluster to be protected, for example, **Cluster-1**. You can only provide one cluster name during the install.
Datastore	Name of the datastore where the JetStream MSA gets deployed.
VMName	Name of JetStream MSA VM, for example, **jetstreamServer**.
Cluster	Name of the Azure VMware Solution private cluster where the JetStream MSA gets deployed, for example, **Cluster-1**.
Netmask	Netmask of the MSA to be deployed, for example, **255.255.255.0**.

Field	Value
MSIp	IP address of the JetStream MSA VM.
Dns	DNS IP that the JetStream MSA VM should use.
Gateway	IP address of the network gateway for the JetStream MSA VM.
Credential	Credentials of the root user of the JetStream MSA VM.
HostName	Hostname (FQDN) of the JetStream MSA VM.
Network	Name of the NSX-T Data Center network segment where the JetStream MSA gets deployed.
Specify name for execution	Alphanumeric name of the execution, for example, **Install-JetDRWithStaticIP-Exec1**. Used to verify if the cmdlet ran successfully and should be unique for each run.

3. View the status of the execution.

DHCP-based IP address

This step also installs JetStream vSphere Installation Bundle (VIB) on the clusters that need DR protection.

1. Select **Run command** > **Packages** > **Install-JetDRWithDHCP**.
2. Provide the required values or change the default values, and then select **Run**.

Expand table

Field	Value
ProtectedCluster	Name of the Azure VMware Solution private cloud cluster to be protected, for example, **Cluster-1**. You can only provide one cluster name during the install.
Datastore	Name of the datastore where the JetStream MSA gets deployed.
VMName	Name of JetStream MSA VM, for example, **jetstreamServer**.
Cluster	Name of the Azure VMware Solution private cluster where the JetStream MSA gets deployed, for example, **Cluster-1**.
Credential	Credentials of the root user of the JetStream MSA VM.
HostName	Hostname (FQDN) of the JetStream MSA VM.

Field	Value
Network	Name of the NSX-T Data Center network segment where the JetStream MSA gets deployed.
Specify name for execution	Alphanumeric name of the execution, for example, **Install-JetDRWithDHCP-Exec1**. Used to verify if the cmdlet ran successfully and should be unique for each run.

3. View the status of the execution.

Add JetStream DR to new Azure VMware Solution clusters

1. Select **Run command** > **Packages** > **Enable-JetDRForCluster**.

2. Provide the required values or change the default values, and then select **Run**.

Expand table

Field	Value
ProtectedCluster	Name of the Azure VMware Solution private cloud cluster to be protected, for example, **Cluster-1**. You can only provide one cluster name during the install.
Credential	Credentials of the root user of the JetStream MSA VM.
MSIp	IP address of the JetStream MSA VM.
Specify name for execution	Alphanumeric name of the execution, for example, **Enable-JetDRForCluster-Exec1**. Used to verify if the cmdlet ran successfully and should be unique for each run.

3. View the status of the execution.

Configure JetStream DR

This section only covers an overview of the steps required for configuring JetStream DR. For detailed descriptions and steps, see the Configuring JetStream DR documentation.

Once JetStream DR MSA and JetStream VIB are installed on the Azure VMware Solution clusters, use the JetStream portal to complete the remaining configuration steps.

1. Access the JetStream portal from the vCenter appliance.

2. Add an external storage site.

3. Deploy a JetStream DRVA appliance.

4. Create a JetStream replication log store volume using one of the datastores available to the Azure VMware Solution cluster.

   > **Tip**
   >
   > Fast local storage, such as vSAN datastore, is preferred for the replication log volume.

5. Create a JetStream protected domain. Provide the Azure Blob Storage site, JetStream DRVA instance, and replication log volume created in previous steps.

6. Select the VMs you want to protect, then start VM protection.

For remaining configuration steps for JetStream DR, such as creating a failover runbook, invoking failover to the DR site, and invoking failback to the primary site, see the JetStream Admin Guide documentation.

Disable JetStream DR on an Azure VMware Solution cluster

This cmdlet disables JetStream DR only on one of the clusters and doesn't completely uninstall JetStream DR.

1. Select **Run command** > **Packages** > **Disable-JetDRForCluster**.

2. Provide the required values or change the default values, and then select **Run**.

Expand table

Field	Value
ProtectedCluster	Name of the Azure VMware Solution private cloud cluster currently protected by JetStream DR, for example, **Cluster-1**. You can only provide one cluster name to be disabled.
Credential	Credentials of the root user of the JetStream MSA VM.
MSIp	IP address of the JetStream MSA VM.
Specify name for execution	Alphanumeric name of the execution, for example, **Disable-JetDRForCluster-Exec1**. Used to verify if the cmdlet ran successfully

Field	Value
	and should be unique for each run.

3. View the status of the execution.

Uninstall JetStream DR

1. Select **Run command** > **Packages** > **Invoke-PreflightJetDRUninstall**. This cmdlet checks if the cluster has at least four hosts (minimum required).

2. Provide the required values or change the default values, and then select **Run**.

Expand table

Field	Value
ProtectedCluster	Name of the Azure VMware Solution private cloud cluster currently protected by JetStream DR, for example, **Cluster-1**. You can only provide one cluster name during uninstall.
Credential	Credentials of the root user of the JetStream MSA VM.
MSIp	IP address of the JetStream MSA VM.
Specify name for execution	Alphanumeric name of the execution, for example, **Invoke-PreflightJetDRUninstall-Exec1**. Used to verify if the cmdlet ran successfully and should be unique for each run.

3. View the status of the execution.

4. After the preflight cmdlet completes successfully, select **Uninstall-JetDR**, provide the required values or change the default values, and select **Run**.

Expand table

Field	Value
ProtectedCluster	Name of the Azure VMware Solution private cloud cluster currently protected by JetStream DR, for example, **Cluster-1**. You can only provide one cluster name during uninstall.
Credential	Credentials of the root user of the JetStream MSA VM.
MSIp	IP address of the JetStream MSA VM.
Specify name for execution	Alphanumeric name of the execution, for example, **Uninstall-JetDR-Exec1**. Used to verify if the cmdlet ran successfully and should be unique for each run.

5. View the status of the execution.

Support

JetStream DR is a solution that JetStream Software supports. For any product or support issues with JetStream, contact support-avs@jetstreamsoft.com.

Azure VMware Solution uses the Run command to automate both the install and uninstall of JetStream DR. Contact Microsoft support for any issue with the run commands. For issues with JetStream install and uninstall cmdlets, contact JetStream for support.

Next steps

- Infrastructure Setup: JetStream DR for Azure VMware Solution
- JetStream DR for Azure VMware Solution (Full demo)
  - Get started with JetStream DR for Azure VMware Solution
  - Configure and protect VMs
  - Failover to Azure VMware Solution
  - Failback to on-premises

Prepare Azure Site Recovery resources for disaster recovery of Azure VMware Solution VMs

Article • 02/19/2024

This tutorial describes how to prepare Azure resources and components so that you can set up disaster recovery of Azure VMware Solution virtual machines (VMs) by using the Azure Site Recovery service. Azure VMware Solution provides private clouds in Azure. These private clouds contain vSphere clusters that are built from dedicated bare-metal Azure infrastructure.

This is the first tutorial in a series that shows you how to set up disaster recovery for Azure VMware Solution VMs.

In this tutorial, you learn how to:

- ✓ Create a Recovery Services vault. A vault holds metadata and configuration information for VMs, along with other replication components.
- ✓ Set up an Azure virtual network. When Azure VMs are created after failover, they're joined to this network.

> **Note**
>
> - Tutorials show you the simplest deployment path for a scenario. They use default options where possible, and they don't show all possible settings and paths.
> - Some of the concepts of using Azure Site Recovery for Azure VMware Solution overlap with disaster recovery of on-premises VMware VMs. Documentation is cross-referenced accordingly.

Sign in to Azure

If you don't have an Azure subscription, create a free account before you begin. Then sign in to the Azure portal.

Prerequisites

Before you begin:

- Deploy an Azure VMware Solution private cloud in Azure.
- Review the architecture for VMware disaster recovery.
- Read common questions for VMware.

If you just created your free Azure account, you're the administrator of your subscription and you have the necessary permissions. If you're not the subscription administrator, work with the administrator to assign the necessary permissions. To enable replication for a new virtual machine, you must have permission to:

- Create a VM in the selected resource group.
- Create a VM in the selected virtual network.
- Write to an Azure storage account.
- Write to an Azure managed disk.

To complete these tasks, your account should be assigned the Virtual Machine Contributor built-in role. In addition, to manage Site Recovery operations in a vault, your account should be assigned the Site Recovery Contributor built-in role.

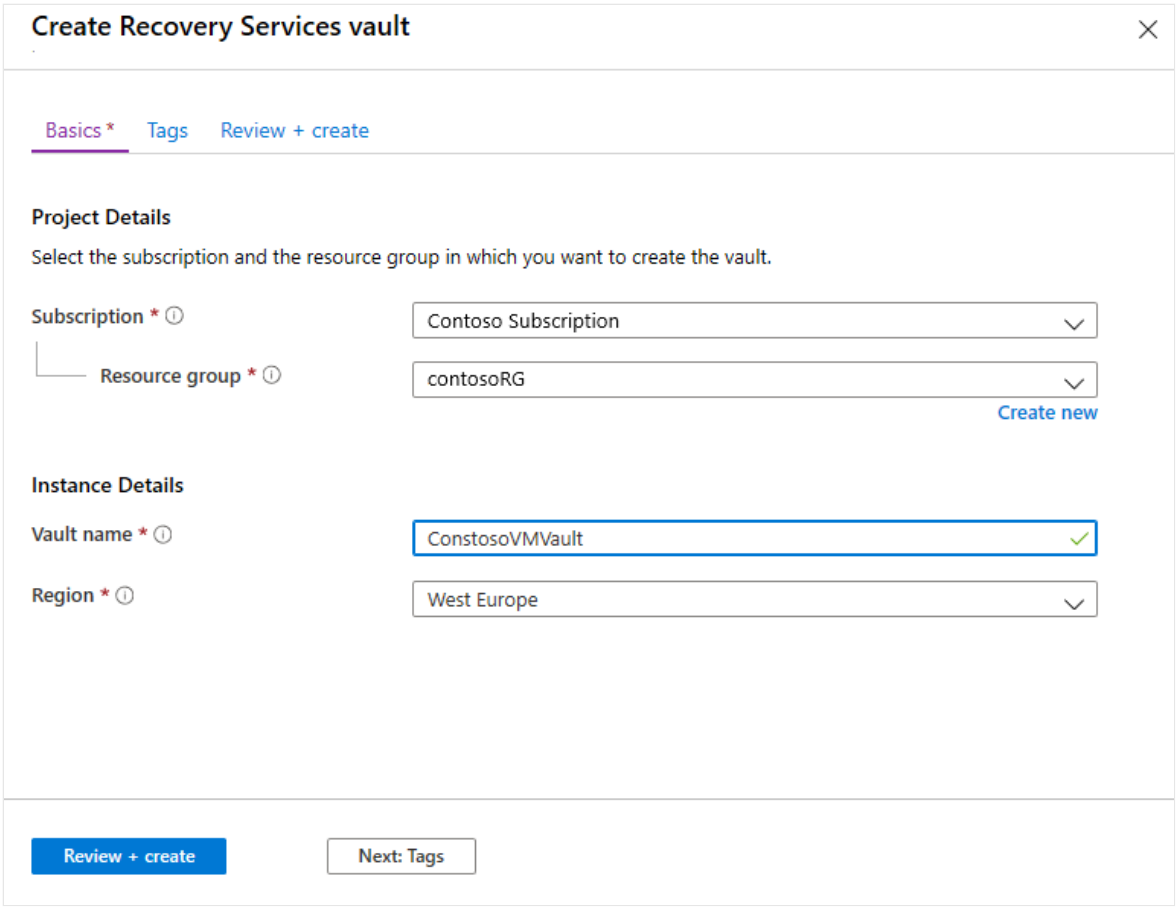
Create a Recovery Services vault

1. In the Azure portal, select **Create a resource**.

2. Search Azure Marketplace for **Recovery Services**.

3. Select **Backup and Site Recovery** from the search results. Then, select **Create**.

4. On the **Create Recovery Services vault** page, on the **Basics** tab, do the following:
   a. For **Subscription**, select the subscription in which you want to create the Recovery Services vault.
   b. For **Resource group**, select an existing resource group or create a new one. For example, create one named **contosoRG**.
   c. For **Vault name**, enter a friendly name to identify the vault. For example, enter **ContosoVMVault**.
   d. For **Region**, select the region where the vault should be located. For example, select **West Europe**.
   e. Select **Review + create**.



5. On the **Review + create** tab, select **Create**.

> **Tip**
>
> To quickly access the vault from the dashboard, select **Pin to dashboard**.

The new vault appears on **Dashboard** > **All resources**, and on the main **Recovery Services vaults** page.

Set up an Azure network

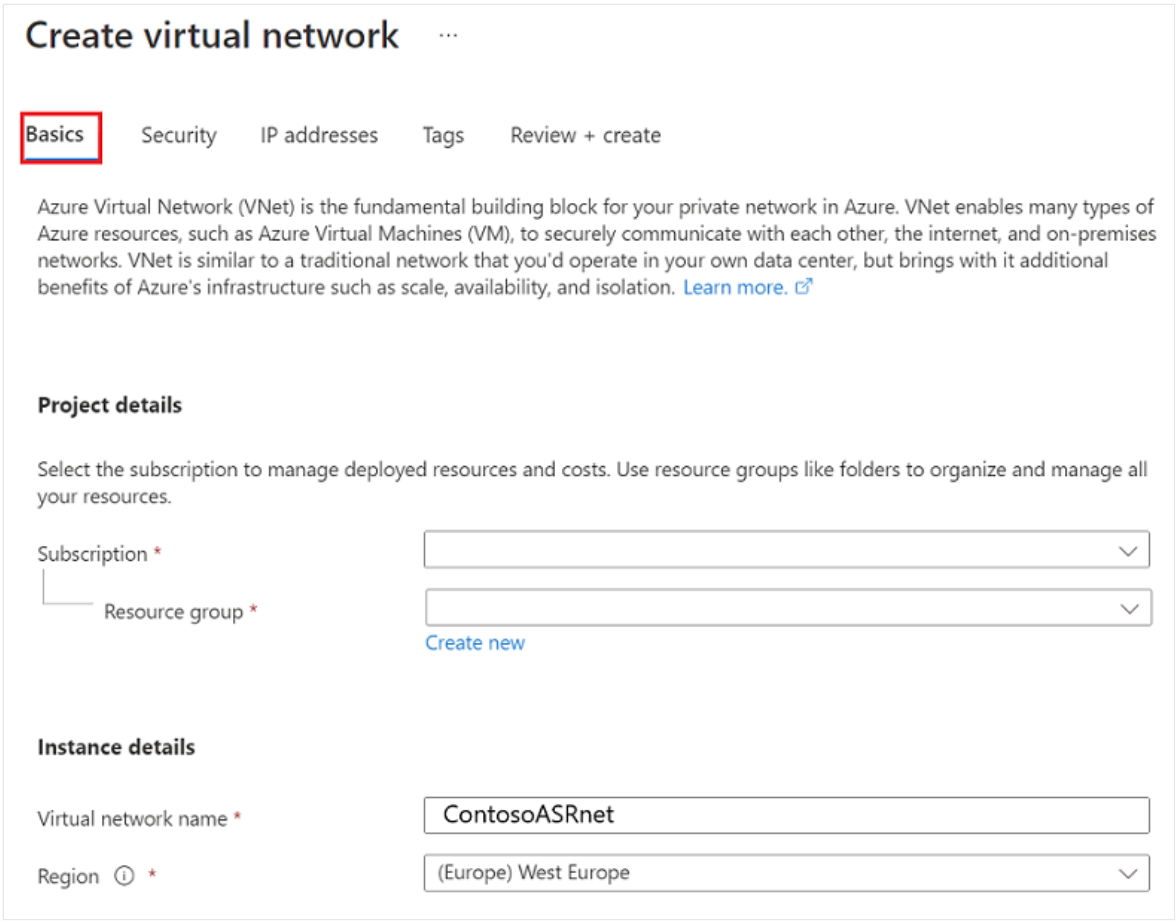
Azure VMware Solution VMs are replicated to Azure managed disks. When failover occurs, Azure VMs are created from these managed disks and joined to the Azure network that you specify in this procedure.

1. In the Azure portal, select **Create a resource**.

2. Under **Categories**, select **Networking** > **Virtual network**.

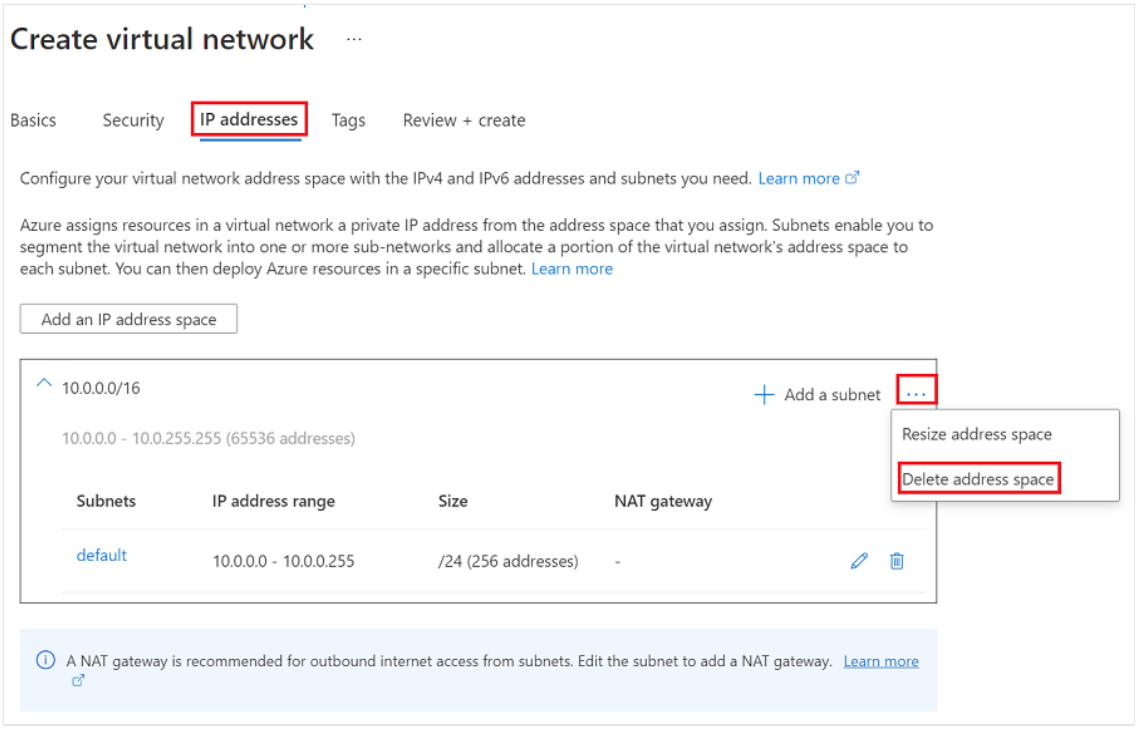
3. On the **Create virtual network** page, on the **Basics** tab, do the following:
   a. For **Subscription**, select the subscription in which to create the network.
   b. For **Resource group**, select the resource group in which to create the network. For this tutorial, use the existing resource group **contosoRG**.

c. For **Virtual network name**, enter a network name. The name must be unique within the Azure resource group. For example, enter **ContosoASRnet**.
d. For **Region**, select **(Europe) West Europe**. The network must be in the same region as the Recovery Services vault.

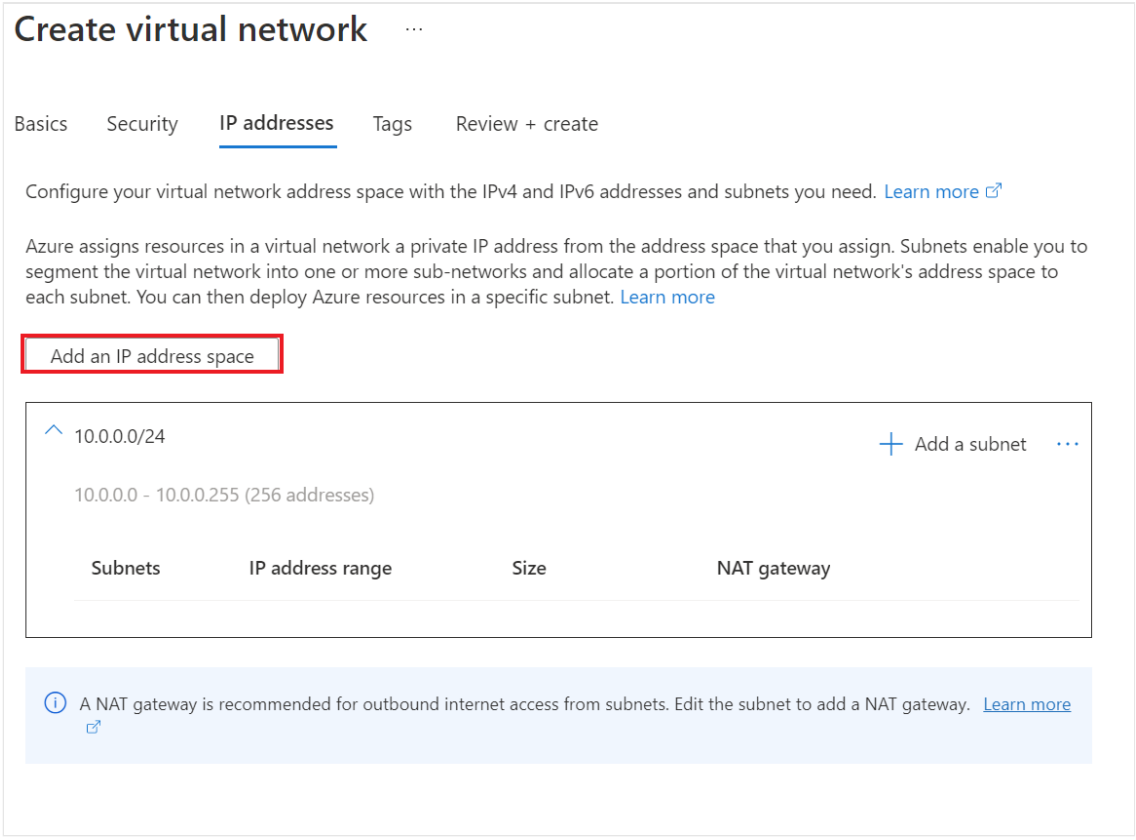


4. On the **IP addresses** tab, do the following:

a. Because there's no subnet for this network, you first delete the pre-existing address range. To do so, select the ellipsis (...) for the available IP address range, and then select **Delete address space**.



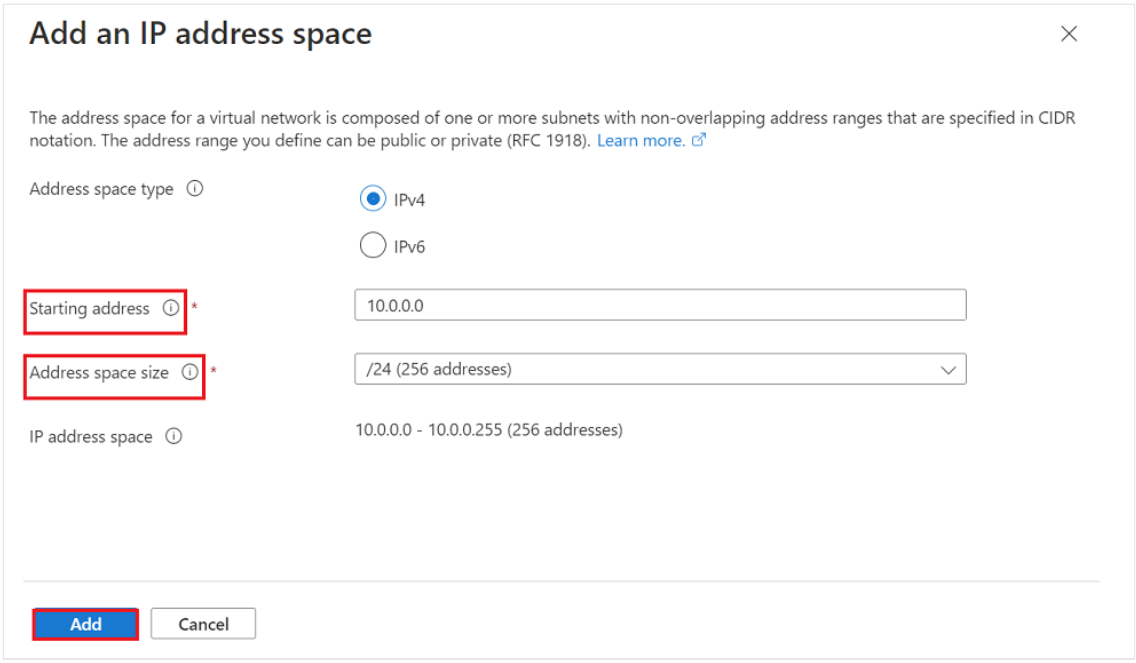
b. Select **Add an IP address space**.



c. For **Starting address**, enter **10.0.0.**

d. For **Address space size**, select **/24 (256 addresses)**.

e. Select **Add**.



f. Select **Review + create**.

5. On the **Review + create** tab, select **Create**.

The virtual network takes a few seconds to create. After it's created, it appears on the Azure portal dashboard.

Next steps

Learn more about:

- Preparing your infrastructure
- Azure networks
- Managed disks.

Prepare Azure VMware Solution for disaster recovery to Azure Site Recovery

Article • 03/22/2024

This tutorial describes how to prepare Azure VMware Solution servers for disaster recovery to Azure by using the Azure Site Recovery service.

This is the second tutorial in a series that shows you how to set up disaster recovery to Azure for Azure VMware Solution virtual machines (VMs). In the first tutorial, you set up the Azure components that you need for Azure VMware Solution disaster recovery.

In this tutorial, you learn how to:

- ✓ Prepare an account on the vCenter Server to automate VM discovery.
- ✓ Prepare an account for automatic installation of the Mobility service on VMware vSphere VMs.
- ✓ Review requirements and support for VMware vCenter servers and VMs.
- ✓ Prepare to connect to Azure VMs after failover.

> ⓘ **Note**
>
> Tutorials show you the simplest deployment path for a scenario. They use default options where possible, and they don't show all possible settings and paths.

Prerequisites

Before you begin, make sure that you prepared Azure as described in the first tutorial in this series.

Prepare an account for automatic discovery

Site Recovery needs access to Azure VMware Solution servers to:

- Automatically discover VMs. At least a read-only account is required.
- Orchestrate replication, failover, and failback. You need an account that can run operations such as creating and removing disks, and turning on VMs.

Create the account as follows:

1. To use a dedicated account, create a role at the vCenter server level. Give the role a name such as **Azure_Site_Recovery**.

2. Assign the role the permissions summarized in the following table.
3. Create a user on the vCenter server. Assign the role to the user.

Expand table

Task	Role/Permissions	Details
VM discovery	At least a read-only user Data Center object > Propagate to Child Object, role=Read-only	User is assigned at the datacenter level and has access to all the objects in the datacenter. To restrict access, assign the **No access** role with the **Propagate to child** object to the child objects (vSphere hosts, datastores, VMs, and networks).
Full replication, failover, failback	Create a role (Azure_Site_Recovery) with the required permissions, and then assign the role to a VMware user or group Data Center object > Propagate to Child Object, role=Azure_Site_Recovery Datastore > Allocate space, browse datastore, low-level file operations, remove file, update virtual machine files Network > Network assign Resource > Assign VM to resource pool, migrate powered off VM, migrate powered on VM Scheduled Tasks > Create task, update task Virtual machine > Configuration Virtual machine > Interact > answer question, device connection, configure CD media, configure floppy media, power off, power on, VMware tools install Virtual machine > Inventory > Create, register, unregister Virtual machine > Provisioning > Allow virtual machine download, allow virtual machine files upload	User is assigned at the datacenter level and has access to all the objects in the datacenter. To restrict access, assign the **No access** role with the **Propagate to child** object to the child objects (vSphere hosts, datastores, VMs, and networks).

Task	Role/Permissions	Details
	Virtual machine > Snapshots > Remove snapshots	

Prepare an account for Mobility service installation

The Mobility service must be installed on machines that you want to replicate. Azure Site Recovery can do a push installation of this service when you enable replication for a machine. Or, you can install it manually or by using installation tools.

In this tutorial, you install the Mobility service by using the push installation. For this push installation, you need to prepare an account that Azure Site Recovery can use to access the VM. You specify this account when you set up disaster recovery in the Azure console.

To prepare the account with permissions to install on the VM, take one of the following actions, based on your operating system:

- For a Windows VM, if you're not using a domain account, disable remote access control on the local machine:

    1. In the registry, go to *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System*.
    2. Add the `DWORD` entry `LocalAccountTokenFilterPolicy`, with a value of `1`.

- For a Linux VM, prepare a root account on the source Linux server.

Check Azure VMware Solution requirements

Make sure that the VMware vCenter server and VMs comply with requirements:

- Verify Azure VMware Solution software versions.
- Verify VMware vCenter server requirements.
- For Linux VMs, check file system and storage requirements.
- Check network and storage support.
- Check what's supported for Azure networking, storage, and compute after failover.
- Verify that the Azure VMware Solution VMs that you'll replicate to Azure comply with Azure VM requirements.
- For Linux VMs, ensure that no two devices or mount points have the same names. These names must be unique and aren't case-sensitive. For example, you can't name two devices for the same VM as *device1* and *Device1*.

Prepare to connect to Azure VMs after failover

After failover, you might want to connect to the Azure VMs from your Azure VMware Solution network.

Connect to a Windows VM by using RDP

Before failover, enable Remote Desktop Protocol (RDP) on the Azure VMware Solution VM:

- For internet access:
  - Make sure that TCP and UDP rules are added for the **Public** profile.
  - Make sure that RDP is allowed in **Windows Firewall** > **Allowed Apps** for all profiles.
- For site-to-site VPN access:
  - Make sure that RDP is allowed in **Windows Firewall** > **Allowed apps and features** for **Domain and Private** networks.
  - Check that the operating system's SAN policy is set to **OnlineAll**. Learn more.

There should be no Windows updates pending on the VM when you trigger a failover. If there are, you won't be able to sign in to the virtual machine until the update finishes.

After failover, check **Boot diagnostics** to view a screenshot of the VM. If you can't connect, check that the VM is running and review troubleshooting tips.

Connect to Linux VMs by using SSH

On the Azure VMware Solution VM before failover:

- Check that the Secure Shell (SSH) service is set to start automatically on system startup.
- Check that firewall rules allow an SSH connection.

After failover, allow incoming connections to the SSH port for the network security group rules on the failed-over VM, and for the Azure subnet to which it's connected. Add a public IP address for the VM.

You can check **Boot diagnostics** to view a screenshot of the VM.

Failback requirements

If you plan to fail back to your Azure VMware Solution cloud, there are several prerequisites for failback. You can prepare these now, but you don't need to. You can prepare after you fail over to Azure.

Next steps

- Learn how to set up disaster recovery.
- If you're replicating multiple VMs, perform capacity planning.

Set up Azure Site Recovery for Azure VMware Solution VMs

Article • 09/07/2023

This tutorial describes how to enable replication for Azure VMware Solution virtual machines (VMs) for disaster recovery to Azure by using the Azure Site Recovery service.

This is the third tutorial in a series that shows you how to set up disaster recovery to Azure for Azure VMware Solution VMs. In the previous tutorial, you prepared the Azure VMware Solution environment for disaster recovery to Azure.

In this tutorial, you learn how to:

- ✓ Set up the source replication settings and an Azure Site Recovery configuration server in an Azure VMware Solution private cloud.
- ✓ Set up the replication target settings.
- ✓ Create a replication policy.
- ✓ Enable replication for a VMware vSphere VM.

> **Note**
>
> Tutorials show you the simplest deployment path for a scenario. They use default options where possible, and they don't show all possible settings and paths.

Prerequisites

Before you begin, complete the previous tutorials. Confirm that you finished these tasks:

1. Set up Azure for disaster recovery to Azure.
2. Prepare your Azure VMware Solution deployment for disaster recovery to Azure.

Also make sure that you meet all prerequisites for successful setup of a configuration server.

Considerations

This tutorial shows you how to replicate a single VM. If you're deploying multiple VMs, you should use the Deployment Planner tool.

In this tutorial, Site Recovery automatically downloads and installs MySQL to the configuration server. If you prefer, you can set it up manually instead.

Select a protection goal

1. In **Recovery Services vaults**, select the vault name. This tutorial uses **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 **Yes, with VMware vSphere Hypervisor**. Then select **OK**.

Set up the source environment

In your source environment, you need a single, highly available, on-premises machine to host these on-premises Site Recovery components:

- **Configuration server**: This server coordinates communications between the Azure VMware Solution private cloud and Azure. It also manages data replication.
- **Process server**: This server acts as a replication gateway. It does these tasks:
  - Receives replication data, optimizes the data (with caching, compression, and encryption), and sends the data to a cache storage account in Azure.
  - Installs the Mobility Service agent on VMs that you want to replicate.
  - Performs automatic discovery of Azure VMware Solution VMs.
- **Primary target server**: This server handles replication data during failback from Azure.

All of these components are installed together on a single Azure VMware Solution machine that's known as the *configuration server*. By default, for Azure VMware Solution disaster recovery, you set up the configuration server as a highly available VMware vSphere VM. To do this, you download a prepared Open Virtualization Application (OVA) template that's based on Open Virtualization Format (OVF). Then, you import the template into VMware vCenter Server to create the VM.

The latest version of the configuration server is available in the portal. You can also download it directly from the Microsoft Download Center.

If you can't use an OVA template to set up a VM, you can set up the configuration server manually.

The license provided with the OVA template is an evaluation license that's valid for 180 days. Windows running on the VM must be activated with the required license.

Download the template

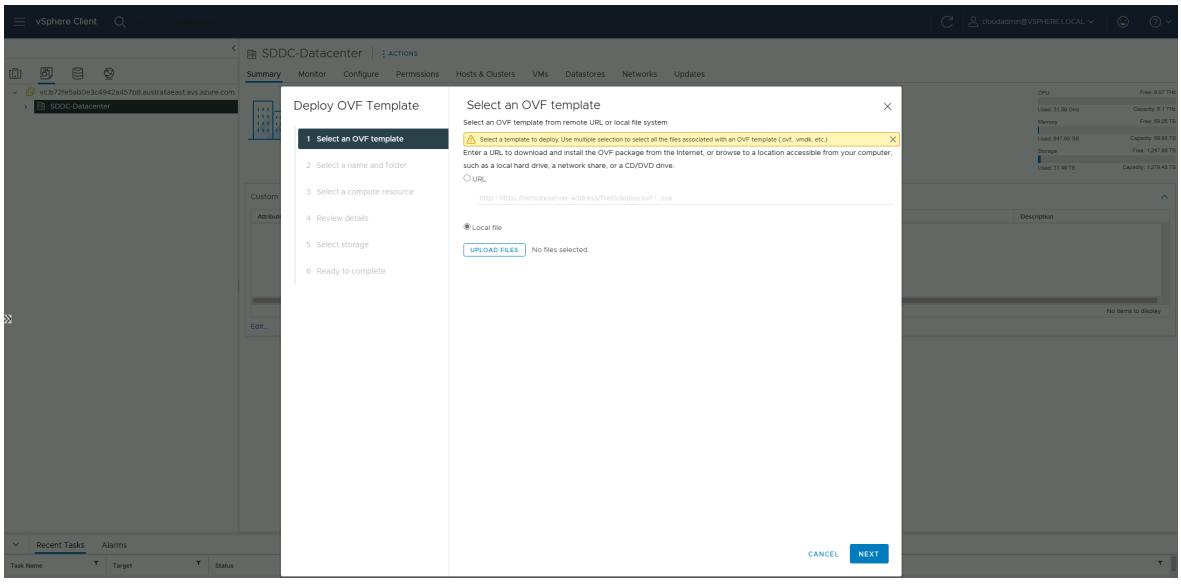
1. In the vault, go to **Prepare Infrastructure** > **Source**.
2. In **Prepare source**, select **+Configuration server**.
3. In **Add Server**, check that **Configuration server for VMware** appears in **Server type**.
4. Download the OVA template for the configuration server.

Import the template in VMware

1. Sign in to the VMware vCenter server by using the VMware vSphere client.

2. On the **File** menu, select **Deploy OVF Template** to start the **Deploy OVF Template** wizard.

3. On the **Select an OVF template** page, enter the location of the downloaded OVF file.



4. On the **Select name and folder** and **Select a compute resource** pages, accept the default settings.

5. On the **Review details** page, select **Next**.

6. On the **Select storage** page, for best performance, select **Thick Provision Eager Zeroed** in **Select virtual disk format**.

7. On the **Ready to complete** page, to set up the VM with the default settings, select **Power on after deployment** > **Finish**.

> **Tip**
>
> By default, the template contains a single network adapter. If you want to add an adapter, clear **Power on after deployment** before you select **Finish**. You can add adapters after deployment.

Add a network adapter

If you want to add a network adapter to the configuration server, add it before you register the server in the vault. You can't add adapters after registration.

1. In the vSphere Client inventory, right-click the VM and select **Edit Settings**.
2. In **Hardware**, select **Add** > **Ethernet Adapter**. Then select **Next**.
3. Select an adapter type and a network.
4. To connect the adapter when the VM is turned on, select **Connect at power on**.
5. Select **Next** > **Finish**. Then select **OK**.

Register the configuration server

After you set up the configuration server, you register it in the vault:

1. From the VMware vSphere Client console, turn on the VM.

2. The VM starts in a Windows Server 2016 installation experience. Accept the license agreement, and enter an administrator password.

3. After the installation finishes, sign in to the VM as the administrator.

   The first time you sign in, the Azure Site Recovery configuration tool starts within a few seconds.

4. Enter a name that's used to register the configuration server with Azure Site Recovery. Then select **Next**.

5. The tool checks that the VM can connect to Azure. After the connection is established, select **Sign in** to sign in to your Azure subscription. The credentials must have access to the vault in which you want to register the configuration server. Ensure that necessary roles are assigned to this user.

   The tool performs some configuration tasks and then restarts.

6. Sign in to the machine again. In a few seconds, the **Configuration Server Management** wizard starts automatically.

Configure settings and add the VMware vCenter server

Finish setting up and registering the configuration server:

1. In the **Configuration Server Management** wizard, select **Setup connectivity**.

   From the dropdown lists, first select the network adapter that the in-built process server uses for discovery and push installation of mobility service on source machines. Then select the adapter that the configuration server uses for connectivity with Azure. When you finish, select **Save**.

   You can't change this setting after it's configured.

2. In **Select Recovery Services vault**, select your Azure subscription and the relevant resource group and vault.

3. In **Install third-party software**, accept the license agreement. Select **Download and Install** to install MySQL Server. If you placed MySQL in the path, you can skip this step. Learn more about MySQL installation.

4. In **Validate appliance configuration**, wait until prerequisites are verified before you continue.

5. In **Configure vCenter Server/vSphere ESXi server**:
   a. Enter the fully qualified domain name (FQDN) or IP address of the VMware vCenter server that contains the VMs that you want to replicate.
   b. Enter the port on which the server is listening.
   c. Enter a friendly name to be used for the VMware vCenter server in the vault.

6. Enter user credentials that the configuration server will use to connect to the VMware vCenter server.

   Ensure that the user name and password are correct. Also ensure that the user is a part of the Administrators group of the virtual machine to be protected. Azure Site Recovery uses these credentials to automatically discover VMware vSphere VMs that are available for replication.

   Select **Add**, and then select **Continue**.

7. In **Configure virtual machine credentials**, enter the user name and password that will be used to automatically install the Mobility service on VMs when replication is enabled.

- For Windows, the account needs local administrator privileges on the machines that you want to replicate.
- For Linux, provide details for the root account.

8. Select **Finalize configuration**.

9. After registration finishes, open the Azure portal and verify that the configuration server and VMware server are listed on **Recovery Services Vault** > **Manage** > **Site Recovery Infrastructure** > **Configuration Servers**.

After the configuration server is registered, Site Recovery connects to the VMware vCenter server by using the specified settings, and it discovers VMs.

> **Note**
>
> It can take 15 minutes or more for the account name to appear in the portal. To update immediately, select **Configuration Servers**, select the server name, and then select **Refresh Server**.

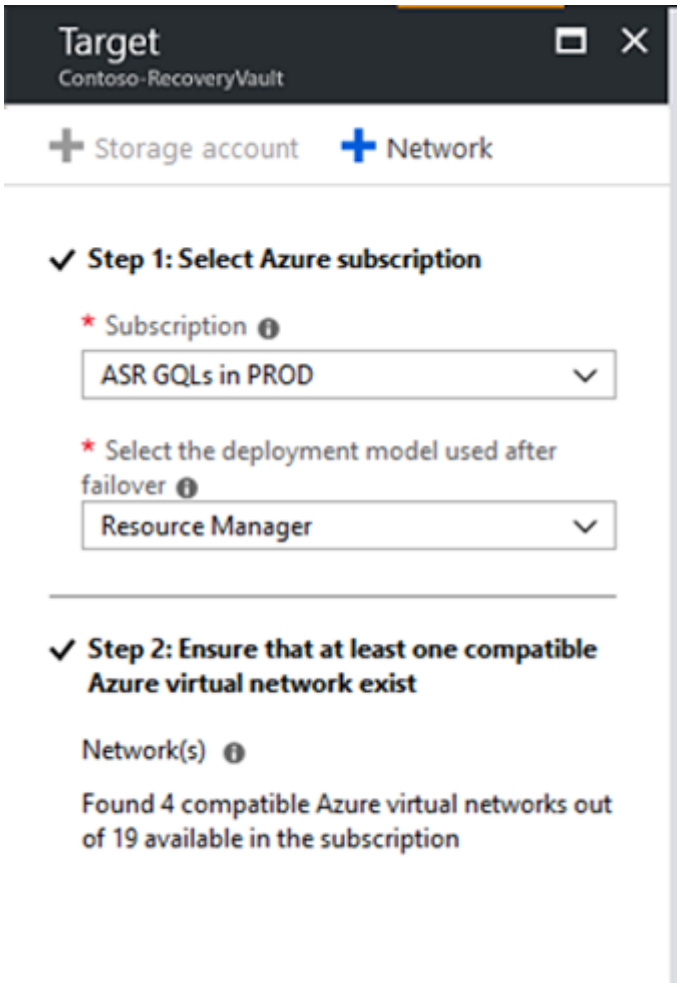
Set up the target environment

Select and verify target resources:

1. Select **Prepare infrastructure** > **Target**.

2. Select the Azure subscription that you want to use. The example in this tutorial uses an Azure Resource Manager model.

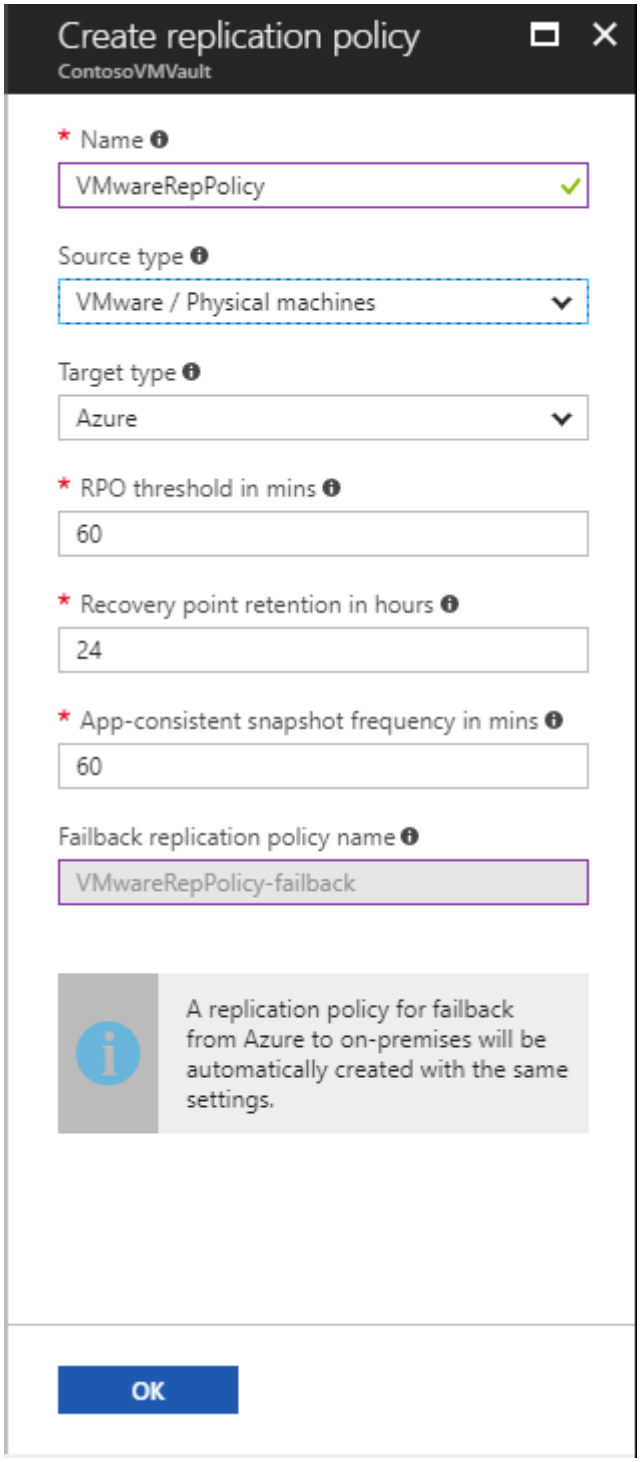
   Azure Site Recovery checks that you have one or more virtual networks. You should have these networks from setting up the Azure components in the first tutorial in this tutorial series.



Create a replication policy

1. Open the Azure portal. Search for and select **Recovery Services vaults**.
2. Select the Recovery Services vault (**ContosoVMVault** in this tutorial).
3. To create a replication policy, select **Site Recovery infrastructure** > **Replication Policies** > **+Replication Policy**.
4. On the **Create replication policy** pane, for **Name**, enter the policy name (**VMwareRepPolicy** in this tutorial).
5. For **RPO threshold in mins**, use the default of 60 minutes. This value defines how often recovery points are created. An alert is generated if continuous replication exceeds this limit.
6. In **Recovery point retention in hours**, specify how long each recovery point is retained (24 hours in this tutorial). Replicated VMs can be recovered to any point in a retention window.
7. In **App-consistent snapshot frequency in mins**, specify how often app-consistent snapshots are created. This tutorial uses the default of 60 minutes. Select **OK** to

create the policy.



The policy is automatically associated with the configuration server. A matching policy is automatically created for failback by default. For example, if the replication policy is **rep-policy**, the failback policy is **rep-policy-failback**. This policy isn't used until you start a failback from Azure.

> **Note**
>
> In VMware vSphere-to-Azure scenarios, the crash-consistent snapshot is taken at 5-minute intervals.

Enable replication

Enable replication for VMs as follows:

1. Select **Replicate application** > **Source**.
2. In **Source**, select **On-premises**, and then select the configuration server in **Source location**.
3. In **Machine type**, select **Virtual Machines**.
4. In **vCenter/vSphere Hypervisor**, select the vCenter Server that manages the host.
5. Select the process server (installed by default on the configuration server VM). Then select **OK**.

   The health status of each process server appears, based on recommended limits and other parameters. Choose a healthy process server. You can't choose a critical process server. You can either troubleshoot and resolve the errors *or* set up a scale-out process server.
6. In **Target**, select the subscription and the resource group in which you want to create the failed-over VMs. This tutorial uses the Resource Manager deployment model.
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 VMs on which you enable replication. Select **Configure later** to select the Azure network per machine.
9. In **Virtual Machines** > **Select virtual machines**, select each machine that you want to replicate. You can select only machines for which replication can be enabled. Then select **OK**.

   If you can't view or select any particular virtual machine, troubleshoot the problem.
10. In **Properties** > **Configure properties**, select the account that the process server will use to automatically install the Mobility service on the machine.
11. In **Replication settings** > **Configure replication settings**, verify that the correct replication policy is selected.
12. Select **Enable Replication**. Site Recovery installs the Mobility service when replication is enabled for a VM.

13. Track the progress of the **Enable Protection** job in **Settings** > **Jobs** > **Site Recovery Jobs**. After the **Finalize Protection** job runs and a recovery point generation is complete, the machine is ready for failover.

    It can take 15 minutes or longer for changes to take effect and appear in the portal.

14. To monitor VMs that 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**.

Next step

After you enable replication, run a drill to make sure that everything works as expected.

Run a disaster recovery drill

Run a disaster recovery drill from Azure VMware Solution to Azure

Article • 02/19/2024

This tutorial describes how to run a disaster recovery drill for an Azure VMware Solution virtual machine (VM) to Azure by using the Azure Site Recovery service. A drill validates your replication strategy without data loss.

This is the fourth tutorial in a series that shows you how to set up disaster recovery to Azure for Azure VMware Solution machines.

In this tutorial, learn how to:

- ✓ Set up an isolated network for the test failover.
- ✓ Prepare to connect to the Azure VM after failover.
- ✓ Run a test failover for a single machine.

> ⓘ **Note**
>
> Tutorials show you the simplest deployment path for a scenario. They use default options where possible, and they don't show all possible settings and paths. If you want to learn about the steps for a disaster recovery drill in more detail, review **this article**.

Prerequisites

Before you begin, complete the previous tutorials. Confirm that you finished these tasks:

1. Set up Azure for disaster recovery to Azure.
2. Prepare your Azure VMware Solution deployment to for disaster recovery to Azure.
3. Set up disaster recovery for Azure VMware Solution VMs.

Verify VM properties

Before you run a test failover, verify the VM properties and make sure that the VMware vSphere VM complies with Azure requirements:

1. In **Protected Items**, select **Replicated Items**, and then select the VM.

2. On the **Replicated item** pane, there's a summary of VM information, health status, and the latest available recovery points. Select **Properties** to view more details.

3. In **Compute and Network**, you can modify these properties as needed:

   - Azure name
   - Resource group
   - Target size
   - Availability set
   - Managed disk settings

   You can also view and modify network settings, including:

   - The network and subnet in which the Azure VM will be located after failover.
   - The IP address that will be assigned to the network and subnet.

4. In **Disks**, you can get information about the operating system and data disks on the VM.

Create a network for test failover

We recommend that for test failover, you choose a network that's isolated from the production recovery site network that's specified in the **Compute and Network** settings for each VM. By default, when you create an Azure virtual network, it's isolated from other networks. The test network should mimic your production network as follows:

- The test network should have same number of subnets as the production network. Subnets should have the same names.
- The test network should use same IP address class and subnet range as the production network.
- Update the DNS of the test network with the IP address specified for the DNS VM in **Compute and Network** settings. For details, read Test failover considerations.

Run a test failover for a single VM

When you run a test failover, the following actions happen:

1. A prerequisites check runs to make sure that all of the conditions required for failover are in place.
2. Failover processes the data, so that an Azure VM can be created. If you select the latest recovery point, a recovery point is created from the data.
3. An Azure VM is created from the data processed in the previous step.

Run the test failover as follows:

1. In **Settings** > **Replicated Items**, select the VM, and then select **+Test Failover**.
2. Select the **Latest processed** recovery point for this tutorial. This step fails over the VM to the latest available point in time. The time stamp is shown.

   With this option, no time is spent processing data, so it provides a low recovery time objective (RTO).
3. In **Test Failover**, select the target Azure network to which Azure VMs will be connected after failover.
4. Select **OK** to begin the failover.

   You can track progress by selecting the VM to open its properties. Or you can select the **Test Failover** job in *vault name* > **Settings** > **Jobs** > **Site Recovery jobs**.
5. After the failover finishes, the replica Azure VM appears in the Azure portal, under **Virtual Machines**. Check that the VM is the appropriate size, that it's connected to the right network, and that it's running.

   You should now be able to connect to the replicated VM in Azure.
6. To delete Azure VMs created during the test failover, select **Cleanup test failover** on the VM. In **Notes**, record and save any observations associated with the test failover.

In some scenarios, failover requires additional processing that takes around 8 to 10 minutes to complete. You might notice longer test failover times for:

- VMware Linux machines.
- VMware VMs that don't have the DHCP service enabled.
- VMware VMs that don't have the following boot drivers: storvsc, vmbus, storflt, intelide, atapi.

Connect after failover

If you want to connect to Azure VMs by using Remote Desktop Protocol (RDP) or Secure Shell (SSH) after failover, prepare to connect. If you encounter any connectivity problems after failover, follow the troubleshooting guide.

Next step

- Learn more about running a failover.

Fail over Azure VMware Solution VMs

Article • 02/19/2024

This tutorial describes how to fail over Azure VMware Solution virtual machines (VMs) to Azure by using Azure Site Recovery.

This is the fifth tutorial in a series that shows you how to set up disaster recovery to Azure for Azure VMware Solution VMs.

In this tutorial, you learn how to:

- ✓ Verify that the Azure VMware Solution VM properties conform with Azure requirements.
- ✓ Fail over specific VMs to Azure.

> ⓘ **Note**
>
> Tutorials show you the simplest deployment path for a scenario. They use default options where possible, and they don't show all possible settings and paths. If you want to learn about failover in detail, see **Fail over VMs**.

To better understand the following tasks, you can learn about the types of failover. If you want to fail over multiple VMs in a recovery plan, review this article.

Prerequisites

Before you begin, complete the previous tutorials. Confirm that you finished these tasks:

1. Set up Azure for disaster recovery to Azure.
2. Prepare your Azure VMware Solution deployment for disaster recovery to Azure.
3. Set up disaster recovery for Azure VMware Solution VMs.
4. Run a disaster recovery drill to make sure that everything works as expected.

Verify VM properties

Before you run a failover, check the VM properties to make sure that the VMs meet Azure requirements:

1. In **Protected Items**, select **Replicated Items**, and then select the VM that you want to verify.

2. On the **Replicated item** pane, there's a summary of VM information, health status, and the latest available recovery points. Select **Properties** to view more details.

3. In **Compute and Network**, you can modify these properties as needed:

   - Azure name
   - Resource group
   - Target size
   - Availability set
   - Managed disk settings

   You can also view and modify network settings, including:

   - The network and subnet in which the Azure VM will be located after failover.
   - The IP address that will be assigned to the network and subnet.

4. In **Disks**, you can get information about the operating system and data disks on the VM.

Run a failover to Azure

1. In **Settings** > **Replicated items**, select the VM that you want to fail over, and then select **Failover**.

2. In **Failover**, for **Recovery Point**, select a recovery point to fail over to. You can use one of the following options:

   - **Latest**: This option first processes all the data sent to Site Recovery. It provides the lowest recovery point objective (RPO) because the Azure VM that's created after failover has all the data that was replicated to Site Recovery when the failover was triggered.
   - **Latest processed**: This option fails over the VM to the latest recovery point that Site Recovery processed. This option provides a low recovery time objective (RTO) because no time is spent processing unprocessed data.
   - **Latest app-consistent**: This option fails over the VM to the latest app-consistent recovery point that Site Recovery processed.
   - **Custom**: This option lets you specify a recovery point.

3. Select **Shut down machine before beginning failover** to try to shut down source VMs before triggering the failover. Failover continues even if the shutdown fails. You can follow the failover progress on the **Jobs** page.

In some scenarios, failover requires additional processing that takes around 8 to 10 minutes to complete. You might notice longer test failover times for:

- VMware vSphere VMs running a Mobility service version older than 9.8.
- VMware vSphere Linux VMs.
- VMware vSphere VMs that don't have the DHCP service enabled.
- VMware vSphere VMs that don't have the following boot drivers: storvsc, vmbus, storflt, intelide, atapi.

> ⚠ **Warning**
>
> Don't cancel a failover in progress. Before failover is started, VM replication stops. If you cancel a failover in progress, failover stops, but the VM won't replicate again.

Connect to a failed-over VM

If you want to connect to an Azure VM after failover by using Remote Desktop Protocol (RDP) and Secure Shell (SSH):

1. Verify that you meet the requirements.
2. After failover, go to the VM and validate by connecting to it.
3. Use **Change recovery point** if you want to use a different recovery point after failover. After you commit the failover in the next step, this option will no longer be available.
4. After validation, select **Commit** to finalize the recovery point of the VM after failover.

   After you commit, all the other available recovery points are deleted. This step completes the failover.

If you encounter any connectivity problems after failover, follow the troubleshooting guide.

Next steps

After failover, reprotect the Azure VMs to the Azure VMware Solution private cloud. Then, after the VMs are reprotected and replicating to the Azure VMware Solution private cloud, fail back from Azure when you're ready.

- Learn how to reprotect Azure VMs.
- Learn how to fail back from Azure.

Reprotect from Azure to Azure VMware Solution private cloud

Article • 11/03/2022

After failover of Azure VMware Solution VMs to Azure, the first step in failing back to your Azure VMware Solution private cloud is to reprotect the Azure VMs that were created during failover. This article describes how to do this.

Before you begin

1. Follow the steps in this article to prepare for reprotection and failback, including setting up a process server in Azure, and an Azure VMware Solution private cloud master target server, and configuring a site-to-site VPN, or ExpressRoute private peering, for failback.
2. Make sure that the Azure VMware Solution private cloud configuration server is running and connected to Azure. During failback, the VM must exist in the configuration server database. Otherwise, failback is unsuccessful.
3. Delete any snapshots on the Azure VMware Solution private cloud master target server. Reprotection won't work if there are snapshots. The snapshots on the VM are automatically merged during a reprotect job.
4. If you're reprotecting VMs gathered into a replication group for multi-VM consistency, make sure they all have the same operating system (Windows or Linux) and make sure that the master target server you deploy has the same type of operating system. All VMs in a replication group must use the same master target server.
5. Open the required ports for failback.
6. Ensure that the vCenter Server is connected before failback. Otherwise, disconnecting disks and attaching them back to the virtual machine fails.
7. If a vCenter Server manages the VMs to which you'll fail back, make sure that you have the required permissions. If you perform a read-only user vCenter Server discovery and protect virtual machines, protection succeeds, and failover works. However, during reprotection, failover is unsuccessful because the datastores can't be discovered, and aren't listed during reprotection. To resolve this problem, you can update the vCenter Server credentials with an appropriate account/permissions, and then retry the job.
8. If you used a template to create your virtual machines, ensure that each VM has its own UUID for the disks. If the Azure VMware Solution VM UUID clashes with the

UUID of the master target server because both were created from the same template, reprotection fails. Deploy from a different template.

9. If you're failing back to an alternate vCenter Server, make sure that the new vCenter Server and the master target server are discovered. Typically if they're not the datastores aren't accessible, or aren't visible in **Reprotect**.
10. Verify the following scenarios in which you can't fail back:

    - If you're using either the ESXi 5.5 free edition or the vSphere 6 Hypervisor free edition. Upgrade to a different version.
    - If you have a Windows Server 2008 R2 SP1 physical server.
    - VMware vSphere VMs can't fail back to Hyper-V.
    - VMs that have been migrated.
    - A VM that's been moved to another resource group.
    - A replica Azure VM that's been deleted.
    - A replica Azure VM that isn't protected.

11. Review the types of failback you can use - original location recovery and alternate location recovery.

Enable reprotection

Enable replication. You can reprotect specific VMs, or a recovery plan:

- If you reprotect a recovery plan, you must provide the values for every protected machine.
- If VMs belong to a replication group for multi-VM consistency, they can only be reprotected using a recovery plan. VMs in a replication group must use the same master target server

> **Note**
>
> The amount of data sent from Azure to erstwhile source during reprotect, can be anything between 0 bytes and sum of disk size for all protected machines, and can't be calculated.

Before you start

- After a VM boots in Azure after failover, it takes some time for the agent to register back to the configuration server (up to 15 minutes). During this time, you won't be able to reprotect and an error message indicates that the agent isn't installed. If this happens, wait for a few minutes, and then reprotect.

- If you want to fail back the Azure VM to an existing Azure VMware Solution VM, mount the VM datastores with read/write access on the master target server's ESXi host.
- If you want to fail back to an alternate location, for example if the Azure VMware Solution VM doesn't exist, select the retention drive and datastore that are configured for the master target server. When you fail back to the Azure VMware Solution private cloud, the virtual machines in the failback protection plan use the same datastore as the master target server. A new VM is then created in vCenter.

Enable reprotection as follows:

1. Select **Vault** > **Replicated items**. Right-click the virtual machine that failed over, and then select **Re-Protect**. Or, from the command buttons, select the machine, and then select **Re-Protect**.

2. Verify that the **Azure to On-premises** direction of protection is selected.

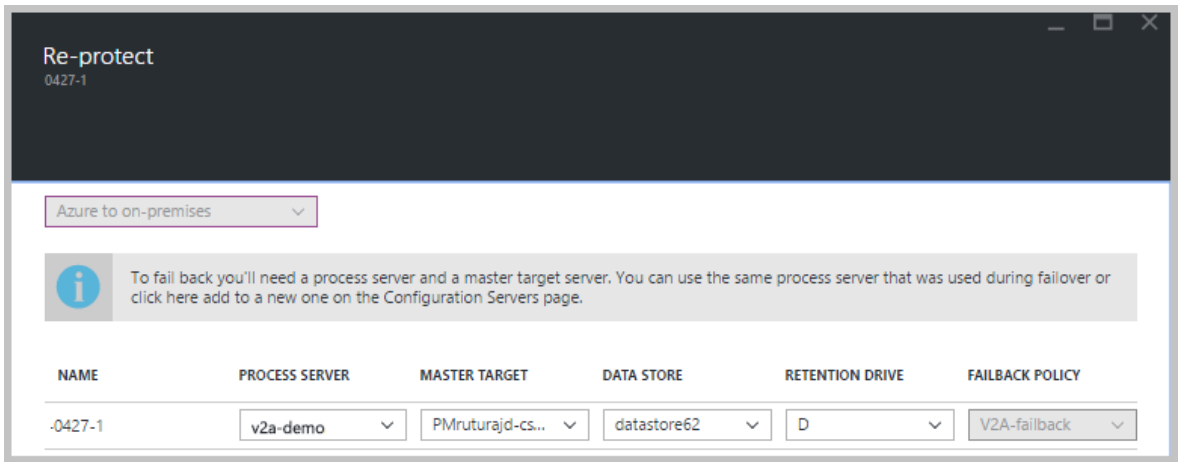
3. In **Master Target Server** and **Process Server**, select the on-premises master target server and the process server.

4. For **Datastore**, select the datastore to which you want to recover the disks in Azure VMware Solution. This option is used when the Azure VMware Solution VM is deleted, and you need to create new disks. This option is ignored if the disks already exist. You still need to specify a value.

5. Select the retention drive.

6. The failback policy is automatically selected.

7. Select **OK** to begin reprotection.



8. A job begins to replicate the Azure VM to the Azure VMware Solution private cloud. You can track the progress on the **Jobs** tab.

- When the reprotection succeeds, the VM enters a protected state.
- The Azure VMware Solution VM is turned off during reprotection. This helps ensure data consistency during replication.
- Don't turn on the Azure VMware Solution VM after reprotection finishes.

Next steps

- If you encounter any issues, review the troubleshooting article.
- After the Azure VMs are protected, you can run a failback. Failback shuts down the Azure VM and boots the Azure VMware Solution VM. Expect some downtime for the application, and choose a failback time accordingly.

Fail back VMs to Azure VMware Solution private cloud

Article • 11/03/2022

This article describes how to failback Azure VMs to an Azure VMware Solution private cloud, following failover of Azure VMware Solution VMs to Azure with Azure Site Recovery. After failback, you enable replication so that the Azure VMware Solution VMs start replicating to Azure.

Before you start

1. Learn about VMware vSphere failback.
2. Make sure you've reviewed and completed the steps to prepare for failback, and that all the required components are deployed. Components include a process server in Azure, a master target server, and a VPN site-to-site connection (or ExpressRoute private peering) for failback.
3. Make sure you've completed the requirements for reprotection and failback, and that you've enabled reprotection of Azure VMs, so that they're replicating from Azure to the Azure VMware Solution private cloud. VMs must be in a replicated state in order to fail back.

Run a failover to fail back

1. Make sure that Azure VMs are reprotected and replicating to the Azure VMware Solution private cloud.

    - A VM needs at least one recovery point in order to fail back.
    - If you fail back a recovery plan, then all machines in the plan should have at least one recovery point.

2. In the vault > **Replicated items**, select the VM. Right-click the VM > **Unplanned Failover**.
3. In **Confirm Failover**, verify the failover direction (from Azure).
4. Select the recovery point that you want to use for the failover.

    - We recommend that you use the **Latest** recovery point. The app-consistent point is behind the latest point in time, and causes some data loss.
    - **Latest** is a crash-consistent recovery point.

- With **Latest**, a VM fails over to its latest available point in time. If you have a replication group for multi-VM consistency within a recovery plan, each VM in the group fails over to its independent latest point in time.
- If you use an app-consistent recovery point, each VM fails back to its latest available point. If a recovery plan has a replication group, each group recovers to its common available recovery point.

5. Failover begins. Azure Site Recovery shuts down the Azure VMs.
6. After failover completes, check everything's working as expected. Check that the Azure VMs are shut down.
7. With everything verified, right-click the VM > **Commit**, to finish the failover process. Commit removes the failed-over Azure VM.

> ⓘ **Note**
>
> For Windows VMs, Azure Site Recovery disables the VMware tools during failover. During failback of the Windows VM, the VMware tools are enabled again.

Reprotect from Azure VMware Solution to Azure

After committing the failback, the Azure VMs are deleted. The VM is back in the Azure VMware Solution private cloud, but it isn't protected. To start replicating VMs to Azure again,as follows:

1. In the vault > **Replicated items**, select failed back VMs, and then select **Re-Protect**.
2. Specify the process server that's used to send data back to Azure.
3. Select **OK** to begin the reprotect job.

> ⓘ **Note**
>
> After an Azure VMware Solution VM starts, it takes up to 15 minutes for the agent to register back to the configuration server. During this time, reprotect fails and returns an error message stating that the agent isn't installed. If this occurs, wait for a few minutes, and reprotect.

Next steps

After the reprotect job finishes, the Azure VMware Solution VM is replicating to Azure. As needed, you can run another failover to Azure.

Run Command in Azure VMware Solution

Article • 03/24/2024

In Azure VMware Solution, vCenter Server has a built-in local user called *cloudadmin* assigned to the CloudAdmin role. The CloudAdmin role has vCenter Server privileges that differ from other VMware cloud solutions and on-premises deployments. The Run Command feature lets you perform operations that would normally require elevated privileges through a collection of PowerShell cmdlets.

Azure VMware Solution supports the following operations:

- Configure an external identity source
- View and set storage policies
- Deploy disaster recovery using JetStream
- Use VMware HCX Run Commands

> **Note**
>
> Run Commands are executed one at a time in the order submitted.

View the status of an execution

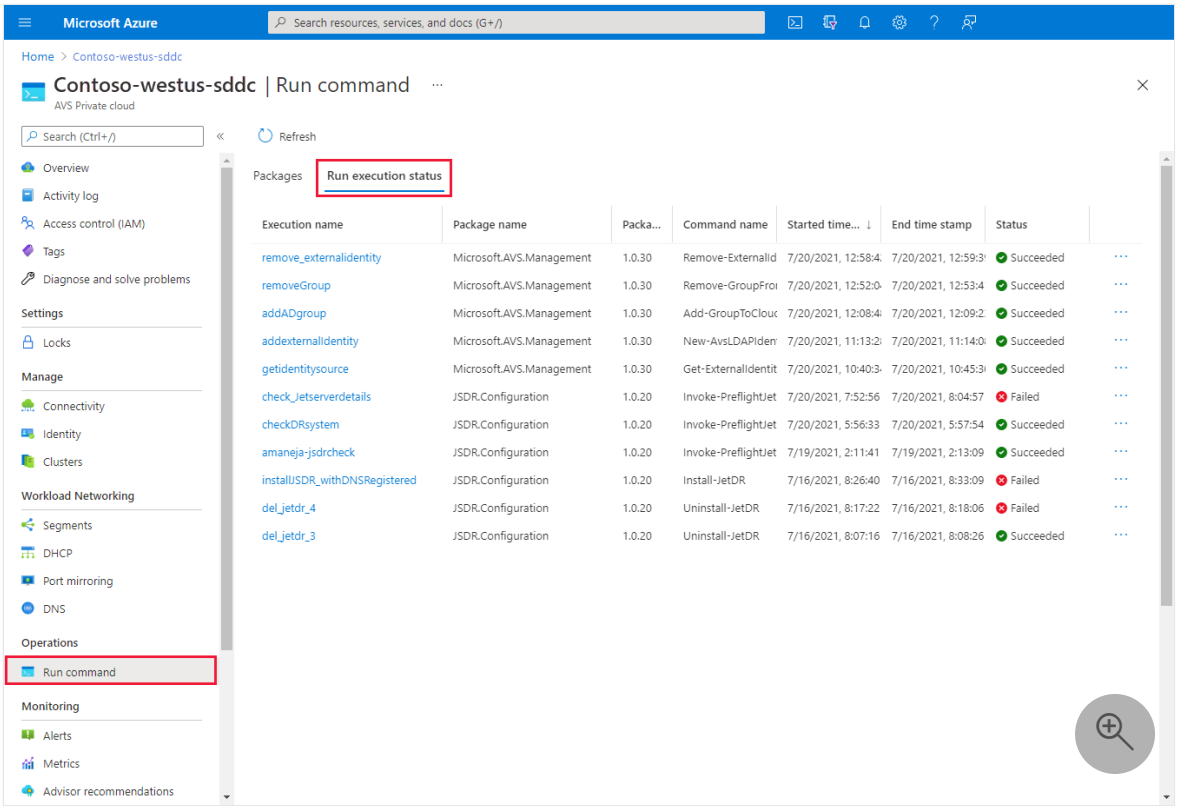
You can view the status of any executed Run Command, including the output, errors, warnings, and information logs of the cmdlets.

1. Sign in to the Azure portal.

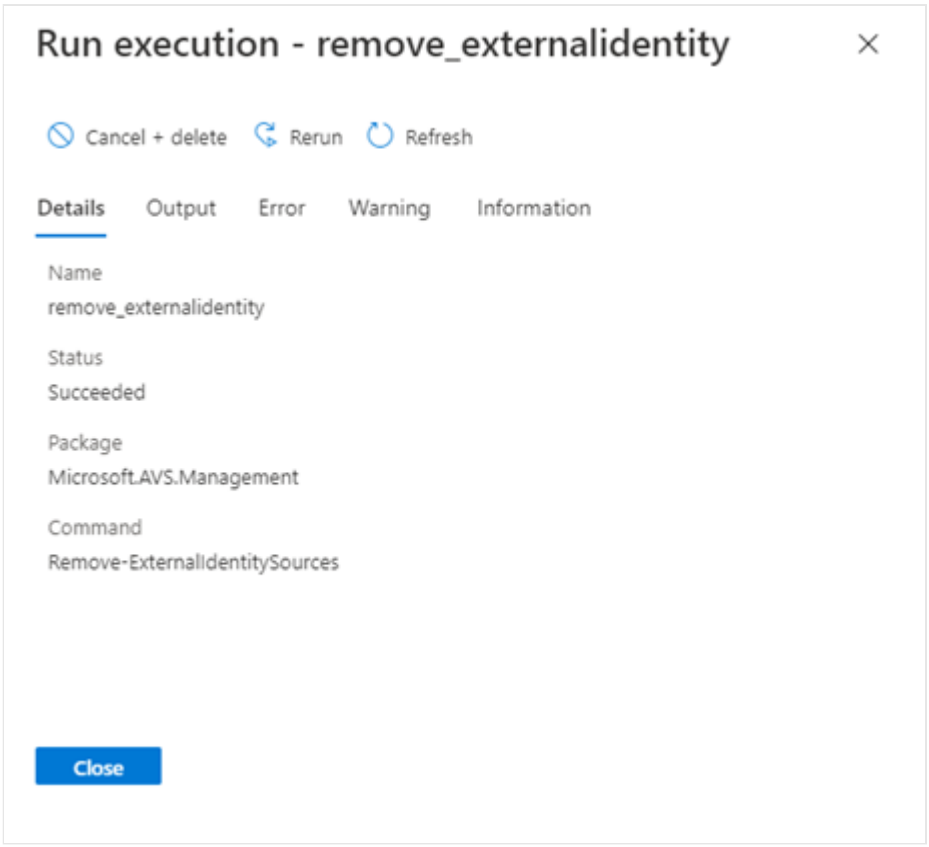
   > **Note**
   >
   > If you need access to the Azure US Gov portal, go to https://portal.azure.us/

2. Select **Run command** > **Run execution status**.

   You can sort by the various columns by selecting the column.

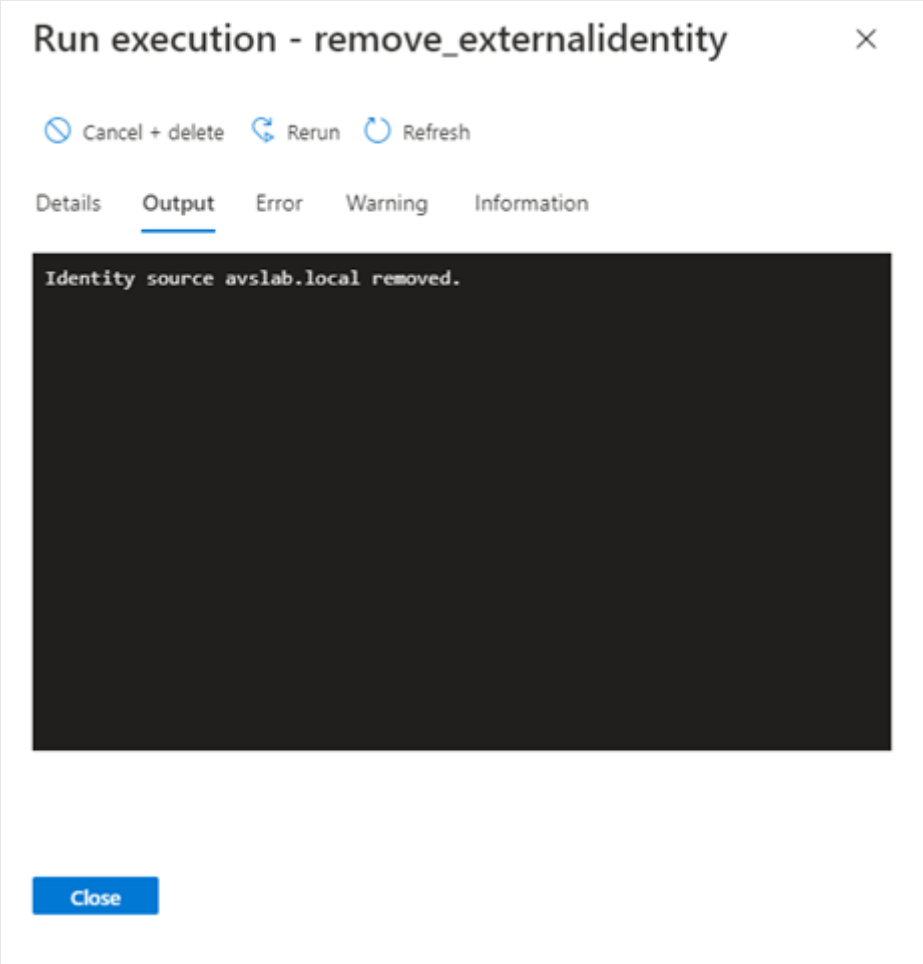


3. Select the execution you want to view. A pane opens with details about the execution, and other tabs for the various types of output generated by the cmdlet.

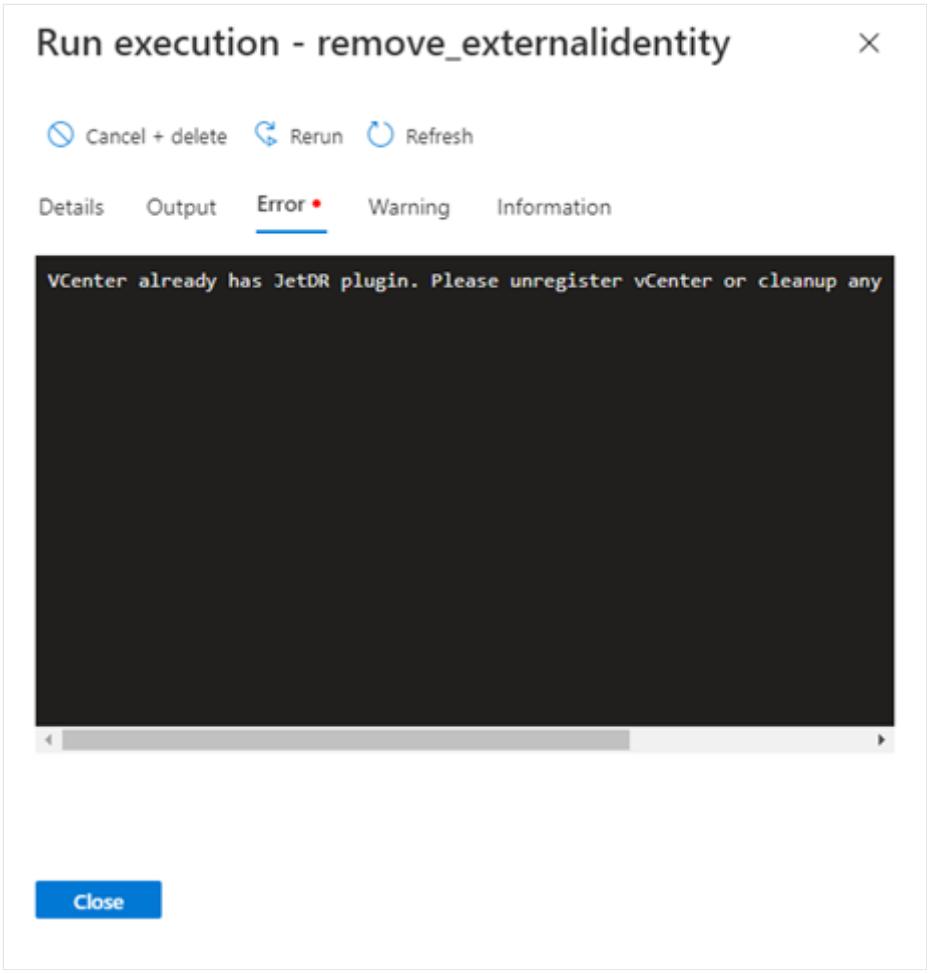


You can view more details about the execution including the output, errors, warnings, and information.

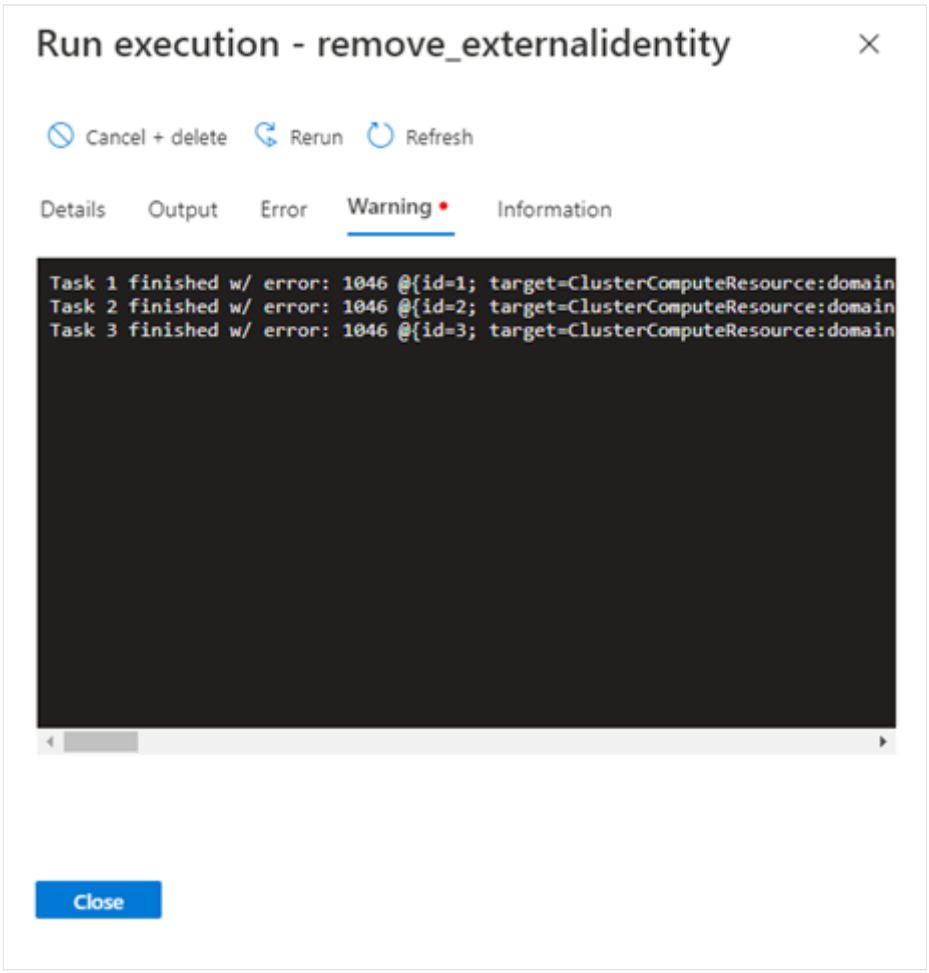
- **Details** - Summary of the execution details, such as the name, status, package, cmdlet name, and error if the command failed.
- **Output** - Messages output by the cmdlet can include progress or the result of the operation. Not all cmdlets have output.



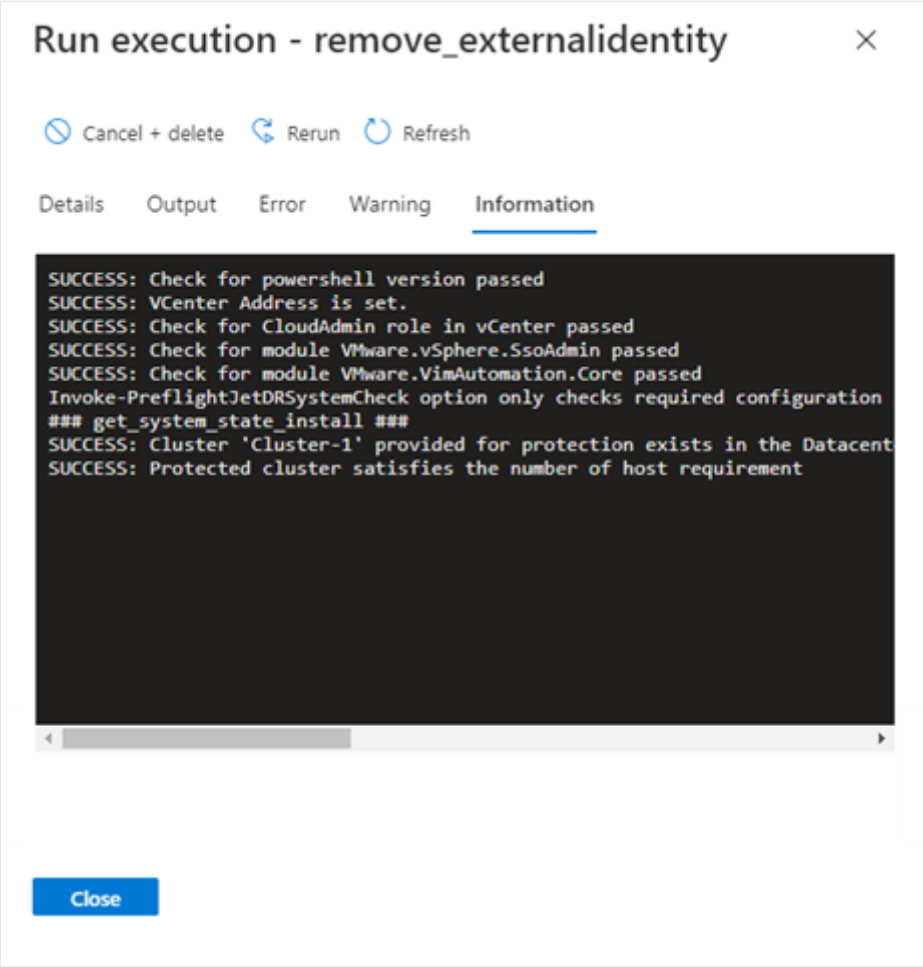
- **Error** - Error messages generated in the execution of the cmdlet in addition to the terminating error message on the details pane.



- **Warning** - Warning messages generated during the execution.



- **Information** - Progress and diagnostic generated messages during the execution of a cmdlet.



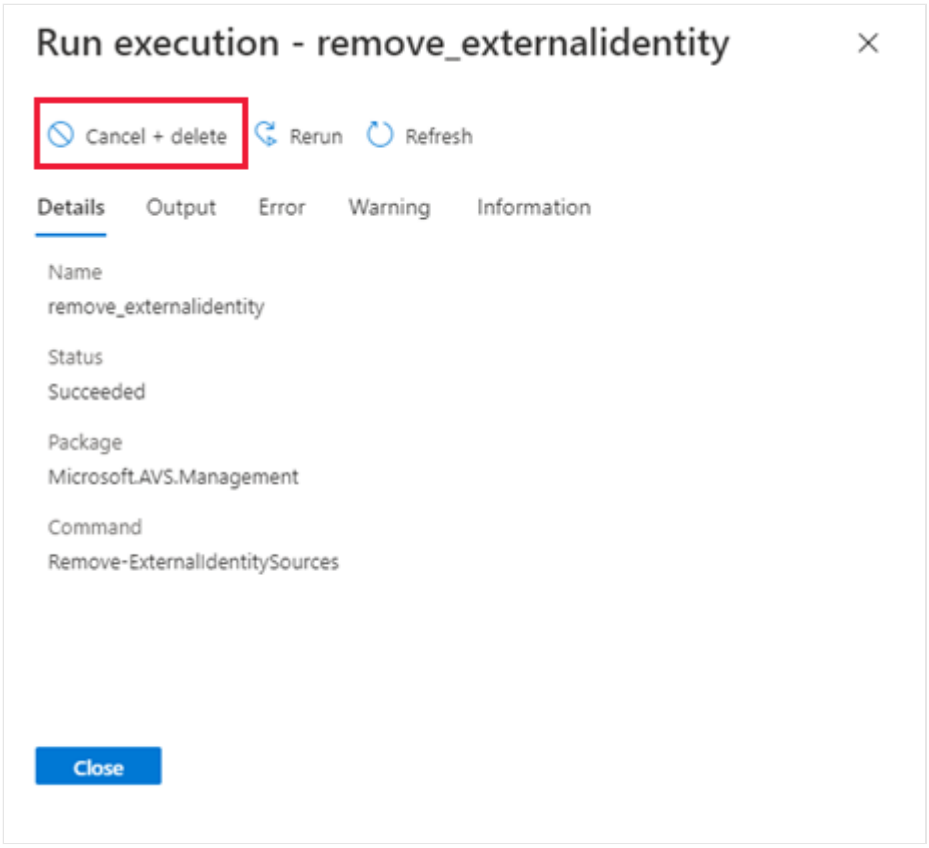
Cancel or delete a job

Method 1

This method attempts to cancel the execution, and then deletes it upon completion.

> **ⓘ Important**
>
> Method 1 is irreversible.

1. Select **Run command** > **Run execution status** and then select the job you want to cancel.

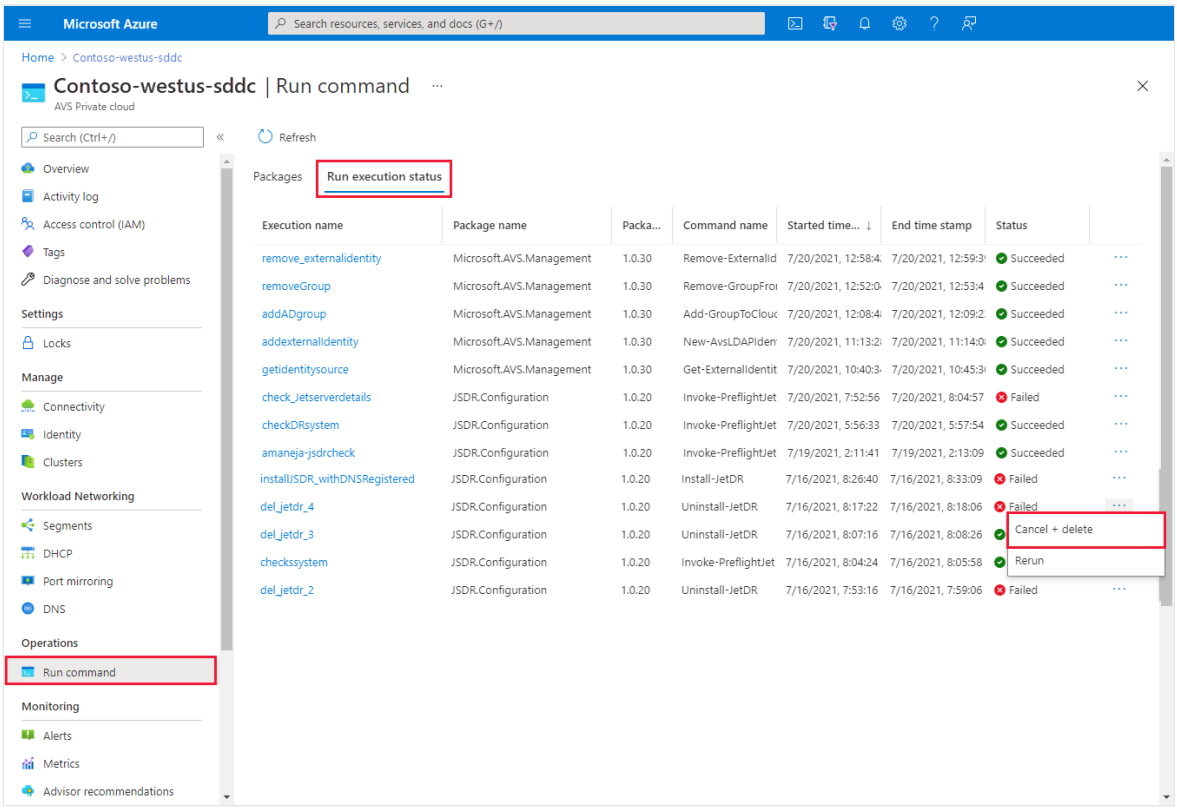


2. Select **Yes** to cancel and remove the job for all users.

Method 2

1. Select **Run command** > **Packages** > **Run execution status**.

2. Select **More** (...) for the job you want to cancel and delete.



3. Select **Yes** to cancel and remove the job for all users.

Next steps

Now that you've learned about the Run Command concepts, you can use the Run Command feature to:

- Configure storage policy - Each VM deployed to a vSAN datastore is assigned a vSAN storage policy. You can assign a vSAN storage policy in an initial deployment of a VM or when you do other VM operations, such as cloning or migrating.
- Configure external identity source for vCenter Server (Run Command) - Configure Active Directory over LDAP or LDAPS for vCenter Server, which enables the use of an external identity source as an Active Directory. Then, you can add groups from the external identity source to the CloudAdmin role.
- Deploy disaster recovery using JetStream - Store data directly to a recovery cluster in vSAN. The data gets captured through I/O filters that run within vSphere. The underlying vSphere datastore can be VMFS, vSAN, vVol, or any supported HCI platform.

Configure VMware syslogs for Azure VMware Solution

Article • 06/07/2024

Diagnostic settings are used to configure streaming export of platform logs and metrics for a resource to the destination of your choice. You can create up to five different diagnostic settings to send different logs and metrics to independent destinations.

In this article, learn how to configure a diagnostic setting to collect VMware syslogs for your Azure VMware Solution private cloud. Then, learn how to store the syslog to a storage account to view the vCenter Server logs and analyze for diagnostic purposes.

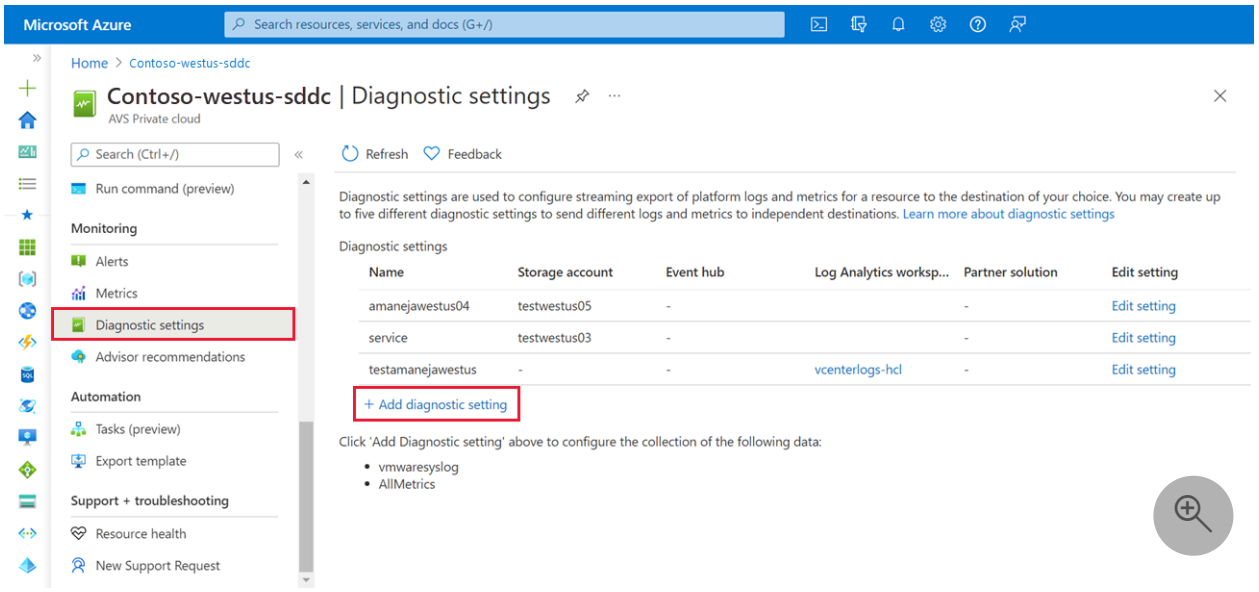
> **ⓘ Important**
>
> The **VMware syslogs** contains the following logs:
>
> - vCenter Server logs
> - ESXi logs
> - vSAN logs
> - NSX Manager logs
> - NSX Distributed Firewall logs
> - NSX Gateway Firewall logs
> - NSX Edge Appliance logs

Prerequisites

Make sure you have an Azure VMware Solution private cloud with access to the vCenter Server and NSX Manager interfaces.

Configure diagnostic settings

1. From your Azure VMware Solution private cloud, select **Diagnostic settings**, then **Add diagnostic settings**.



1. Select the **vmwaresyslog**, **All metrics**, and select one of the following options presented.

Send to Log Analytics workspace

How to set up Log Analytics

A Log Analytics workspace:

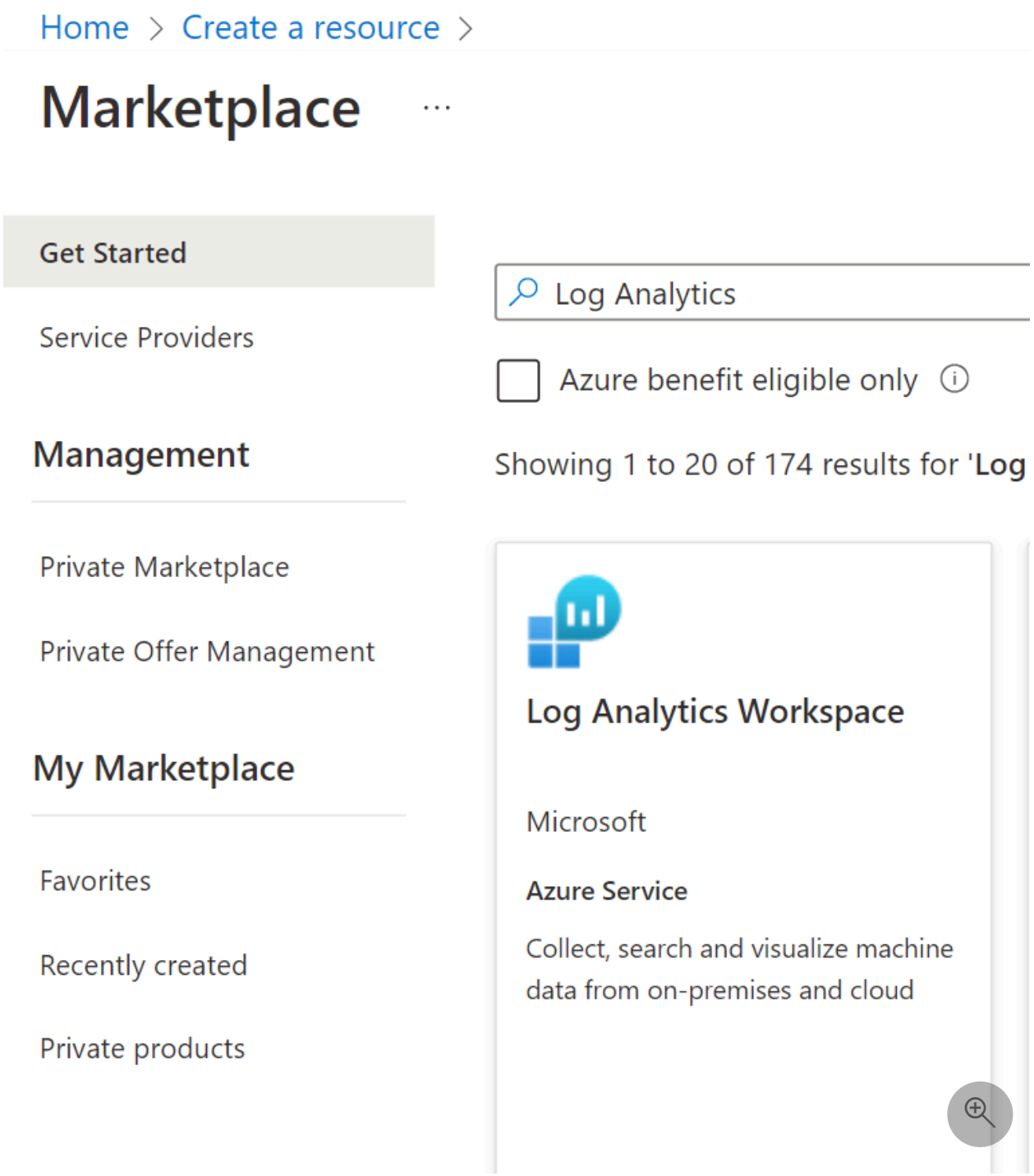
- Contains your Azure VMware Solution private cloud logs.
- Is the workspace from which you can take desired actions, such as querying for logs.

In this section, you'll:

- Configure a Log Analytics workspace
- Create a diagnostic setting in your private cloud to send your logs to this workspace

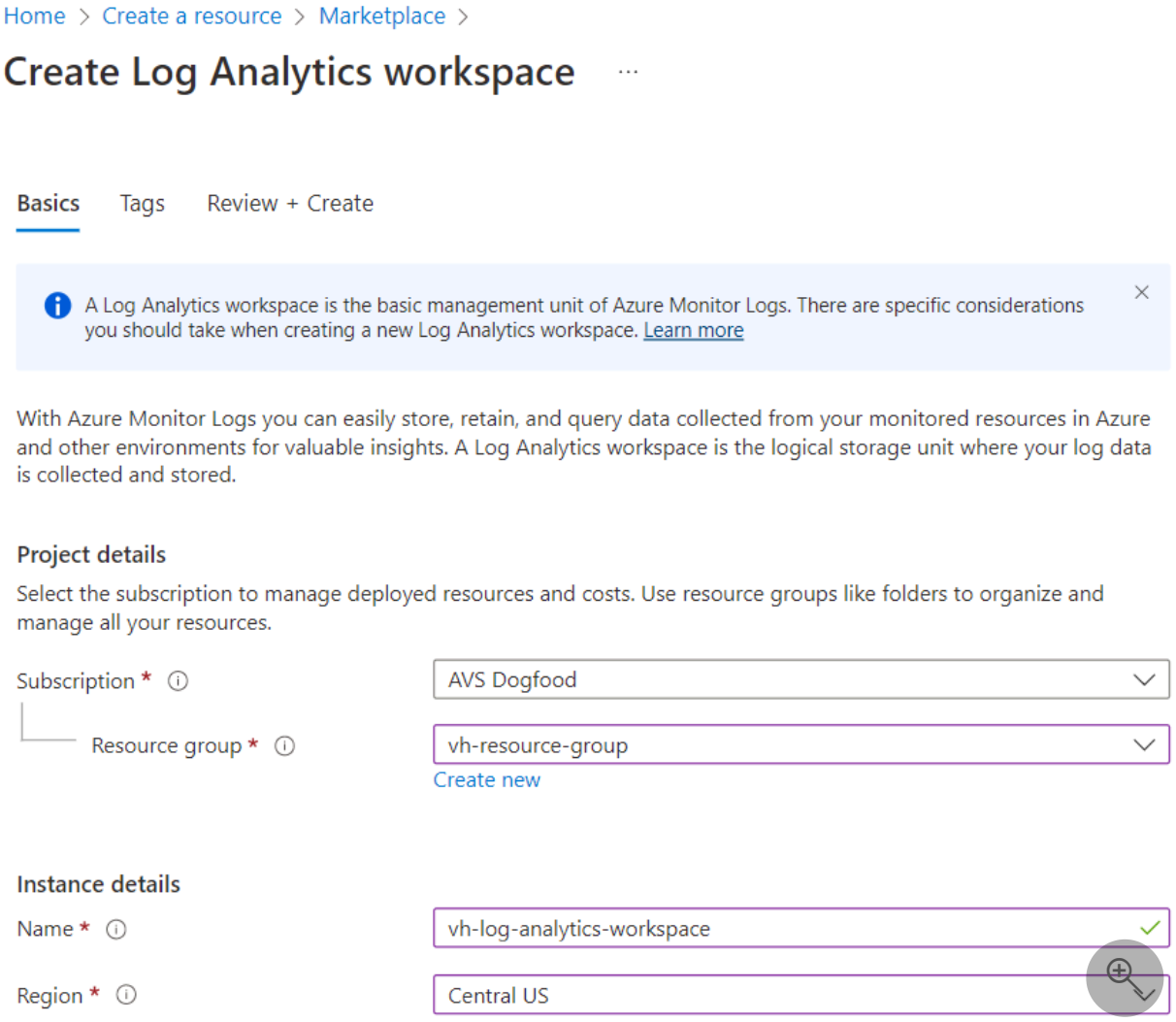
Create a resource

1. In the Azure portal, go to **Create a resource**.
2. Search for "Log Analytics Workspace" and select **Create** -> **Log Analytics Workspace**.



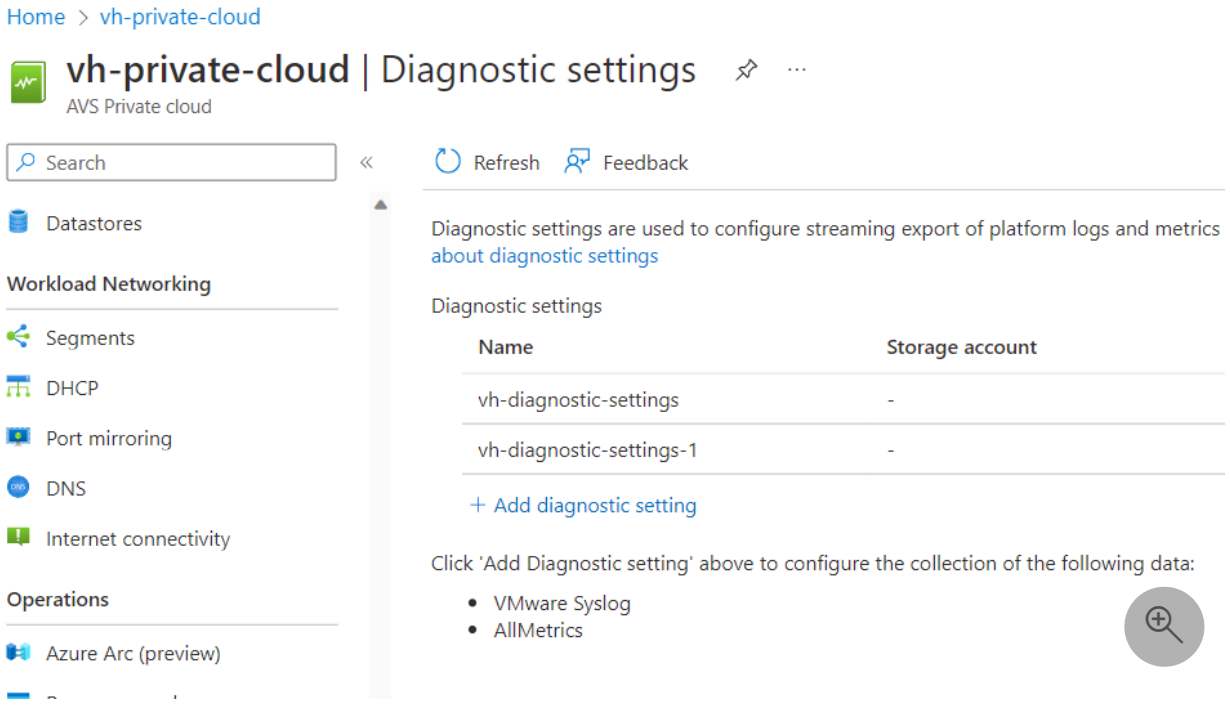
Set up your workspace

1. Enter the Subscription you intend to use, the Resource Group chosen to house this workspace. Give it a name and select a region.
2. Select **Review** + **Create**.



Add a diagnostic setting

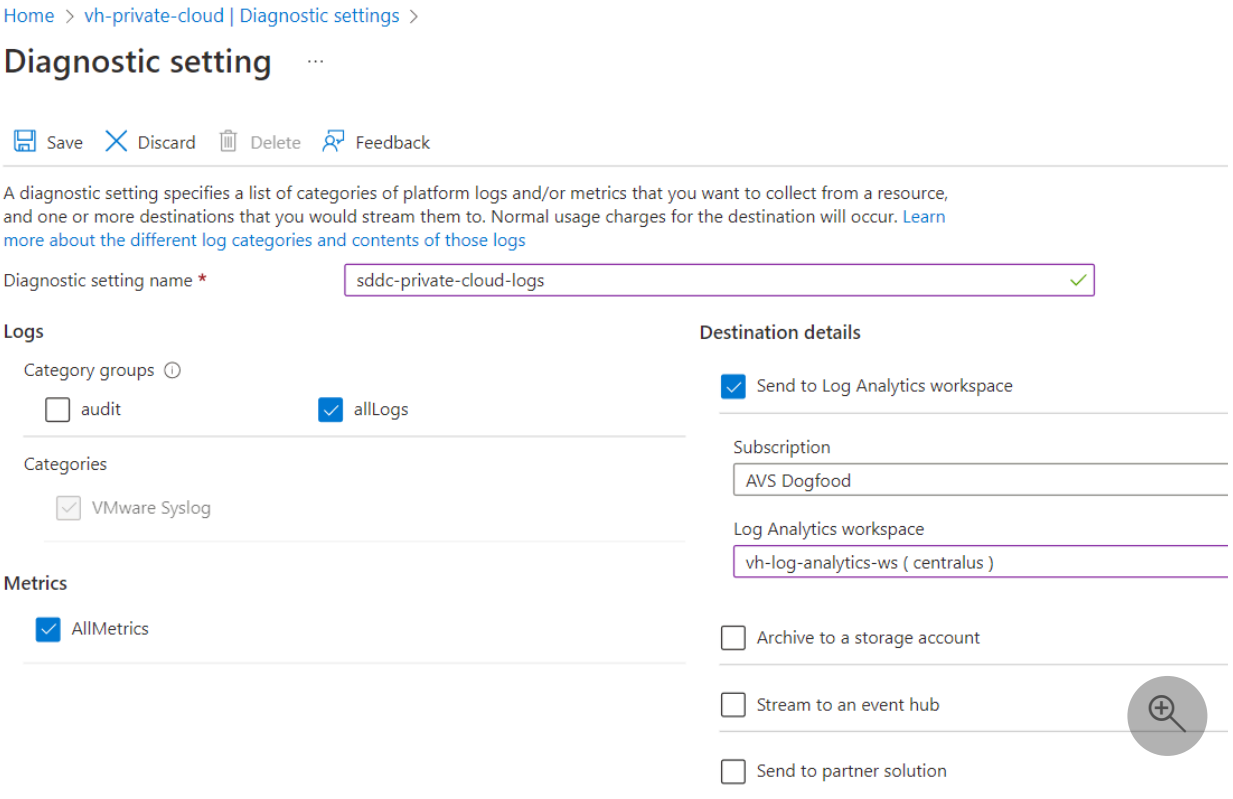
Next, we add a diagnostic setting in your Azure VMware Solution private cloud, so it knows where to send your logs to.



1. Select your Azure VMware Solution private cloud. Go to Diagnostic settings on the left-hand menu under Monitoring. Select **Add diagnostic setting**.

2. Give your diagnostic setting a name. Select the log categories you're interested in sending to your Log Analytics workspace.

3. Make sure to select the checkbox next to **Send to Log Analytics workspace**. Select the Subscription your Log Analytics workspace lives in and the Log Analytics workspace. Select **Save** on the top left.



At this point, your Log Analytics workspace is now successfully configured to receive logs from your Azure VMware Solution private cloud.

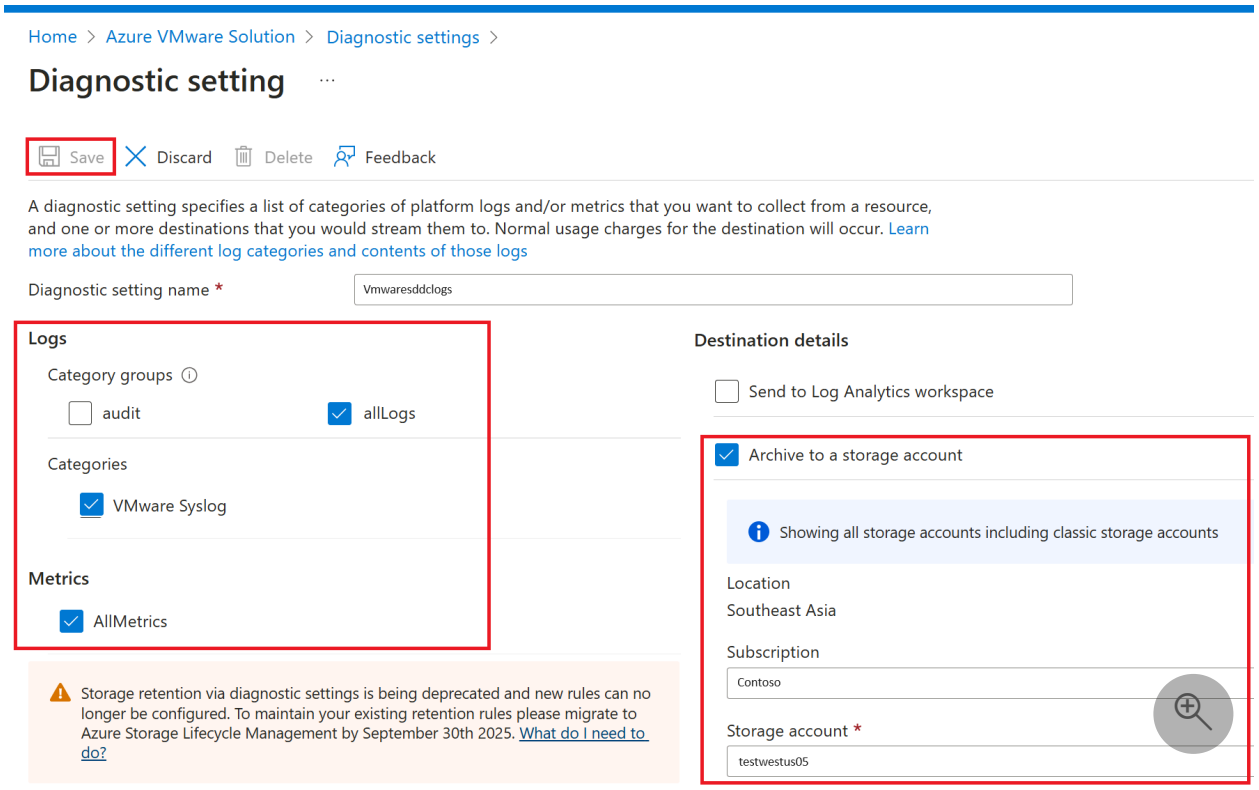
Search and analyze logs using Kusto

Now that you successfully configured your logs to go to your Log Analytics workspace, you can use that data to gain meaningful insights with the Log Analytics search feature. Log Analytics uses a language called the Kusto Query Language (or Kusto) to search through your logs.

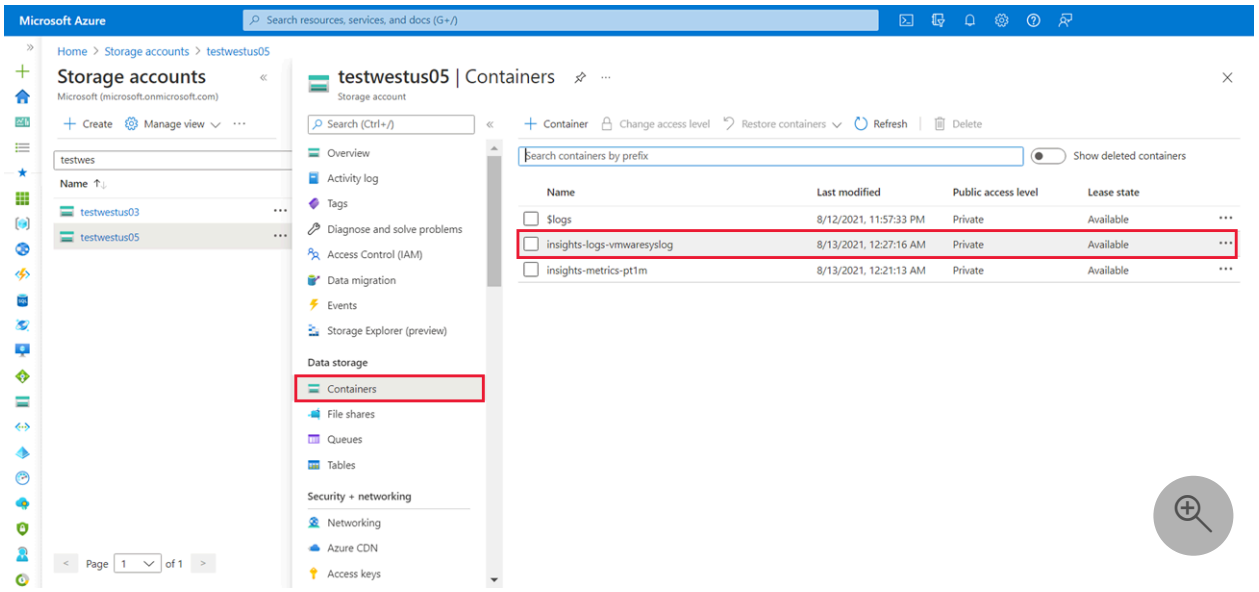
For more information, see Data analysis in Azure Data Explorer with Kusto Query Language.

Archive to storage account

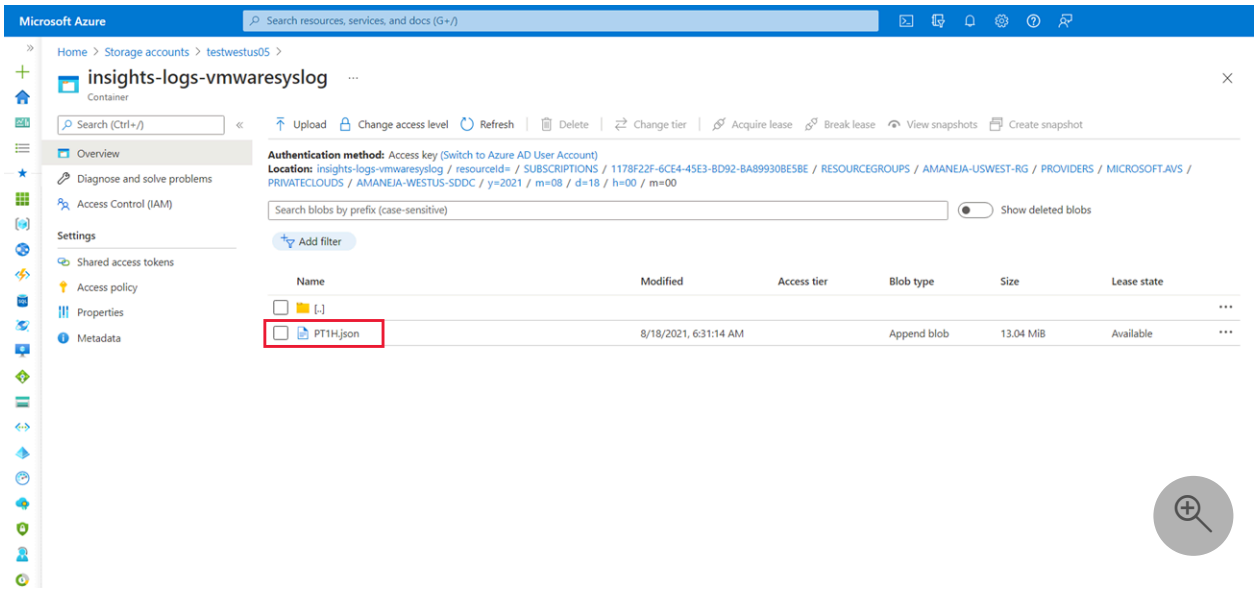
1. In **Diagnostic setting**, select the storage account where you want to store the logs and select **Save**.



2. Go to your **Storage accounts**, verify **Insight logs vmwarelog** was created, and select it.

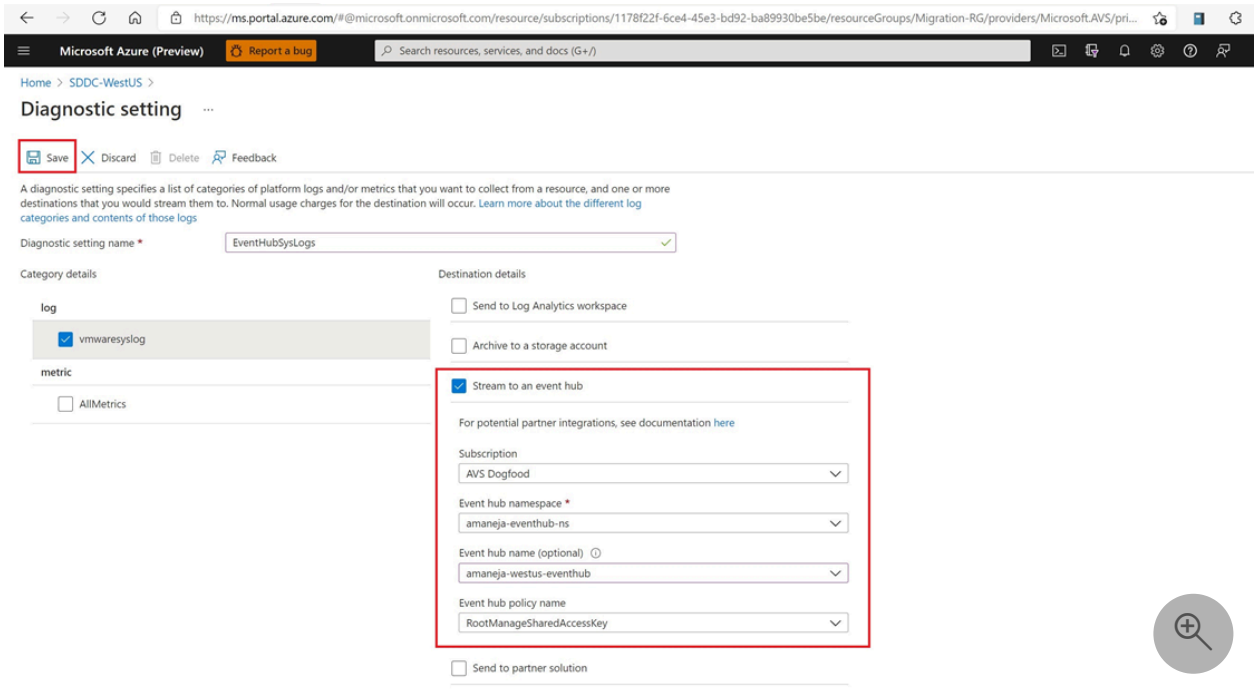


3. Browse **Insight logs vmwarelog** to locate and download the json file to view the logs.



Stream to Microsoft Azure Event Hubs

1. In **Diagnostic setting**, under Destination details, select **Stream to an Event Hub**.
2. From the **Event Hub namespace** drop-down menu, choose where you want to send the logs, select, and **Save**.


https://ms.portal.azure.com/#@microsoft.onmicrosoft.com/resource/subscriptions/1178f22f-6ce4-45e3-bd92-ba89930be5be/resourceGroups/Migration-RG/providers/Microsoft.AVS/pri...
Microsoft Azure (Preview)
Report a bug
Search resources, services, and docs (G+/)
Home > SDDC-WestUS >
Diagnostic setting
Save
Discard
Delete
Feedback
A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. Learn more about the different log categories and contents of those logs
Diagnostic setting name *
EventHubSysLogs
Category details
log
vmwaresyslog
metric
AllMetrics
Destination details
Send to Log Analytics workspace
Archive to a storage account
Stream to an event hub
For potential partner integrations, see documentation here
Subscription
AVS Dogfood
Event hub namespace *
amaneja-eventhub-ns
Event hub name (optional)
amaneja-westus-eventhub
Event hub policy name
RootManageSharedAccessKey
Send to partner solution

Configure Azure Alerts in Azure VMware Solution

Article • 12/08/2023

In this article, learn how to configure Azure Action Groups in Microsoft Azure Alerts to receive notifications of triggered events that you define. Also learn about using Azure Monitor Metrics to gain deeper insights into your Azure VMware Solution private cloud.

> **Note**
>
> Incidents affecting the availability of an Azure VMware Solution host and its corresponding restoration are sent automatically to the Account Administrator, Service Administrator (Classic Permission), Co-Admins (Classic Permission), and Owners (RBAC Role) of the subscription(s) containing Azure VMware Solution private clouds.

Supported metrics and activities

The following metrics are visible through Azure Monitor Metrics.

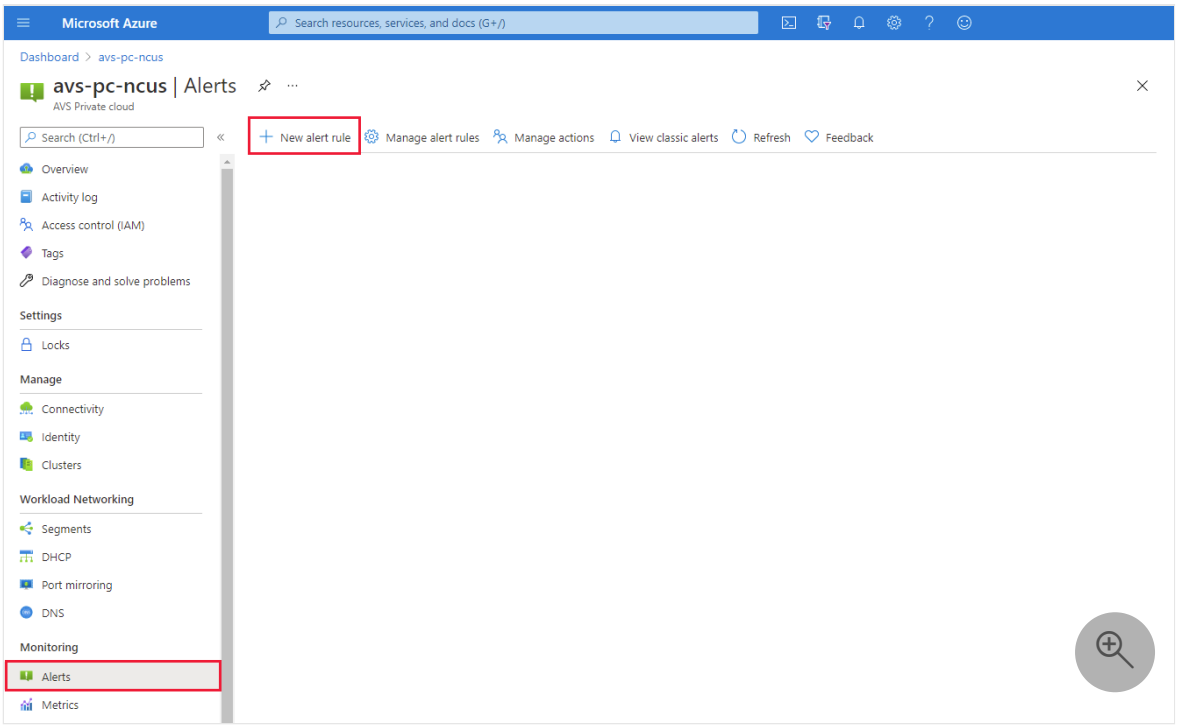
Expand table

Signal name	Signal type	Monitor service
Datastore Disk Total Capacity	Metric	Platform
Percentage Datastore Disk Used	Metric	Platform
Percentage CPU	Metric	Platform
Average Effective Memory	Metric	Platform
Average Memory Overhead	Metric	Platform
Average Total Memory	Metric	Platform
Average Memory Usage	Metric	Platform
Datastore Disk Used	Metric	Platform
All Administrative operations	Activity Log	Administrative

Signal name	Signal type	Monitor service
Register Microsoft.AVS resource provider. (Microsoft.AVS/privateClouds)	Activity Log	Administrative
Create or update a PrivateCloud. (Microsoft.AVS/privateClouds)	Activity Log	Administrative
Delete a PrivateCloud. (Microsoft.AVS/privateClouds)	Activity Log	Administrative

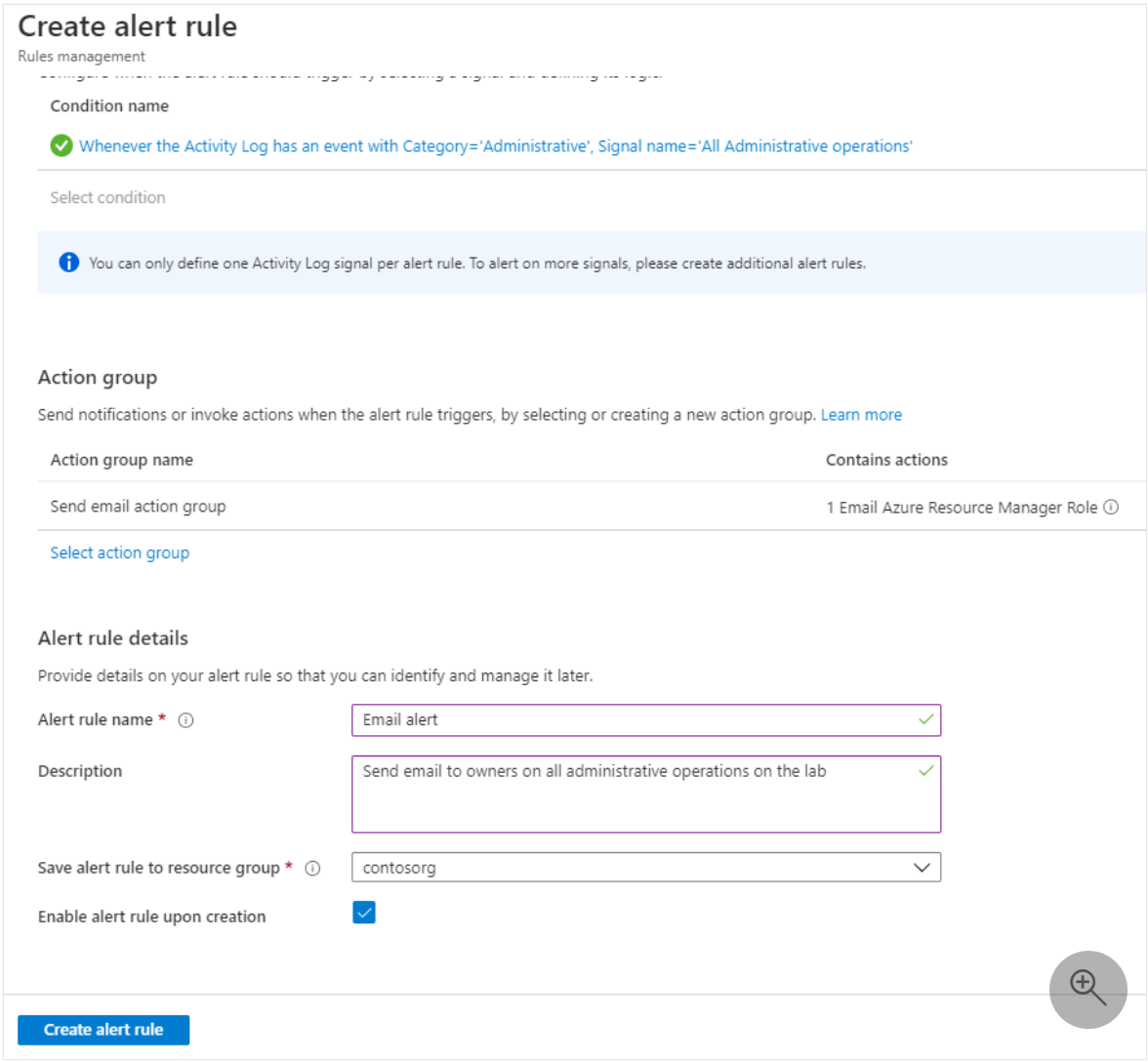
Configure an alert rule

1. From your Azure VMware Solution private cloud, select **Monitoring** > **Alerts**, and then **New alert rule**.



A new configuration screen opens where you'll:

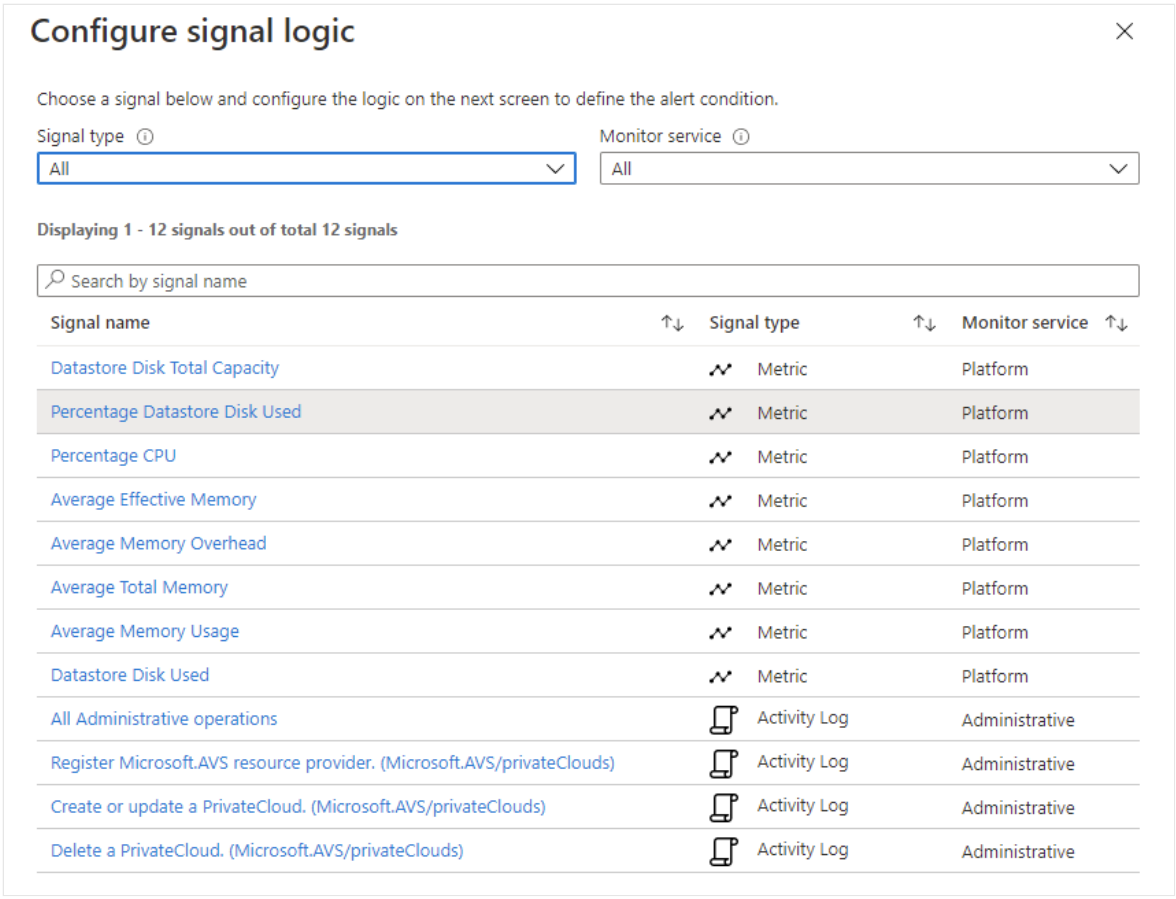
- Define the Scope
- Configure a Condition
- Set up the Action Group
- Define the Alert rule details



2. Under **Scope**, select the target resource you want to monitor. By default, the Azure VMware Solution private cloud from where you opened the Alerts menu is defined.

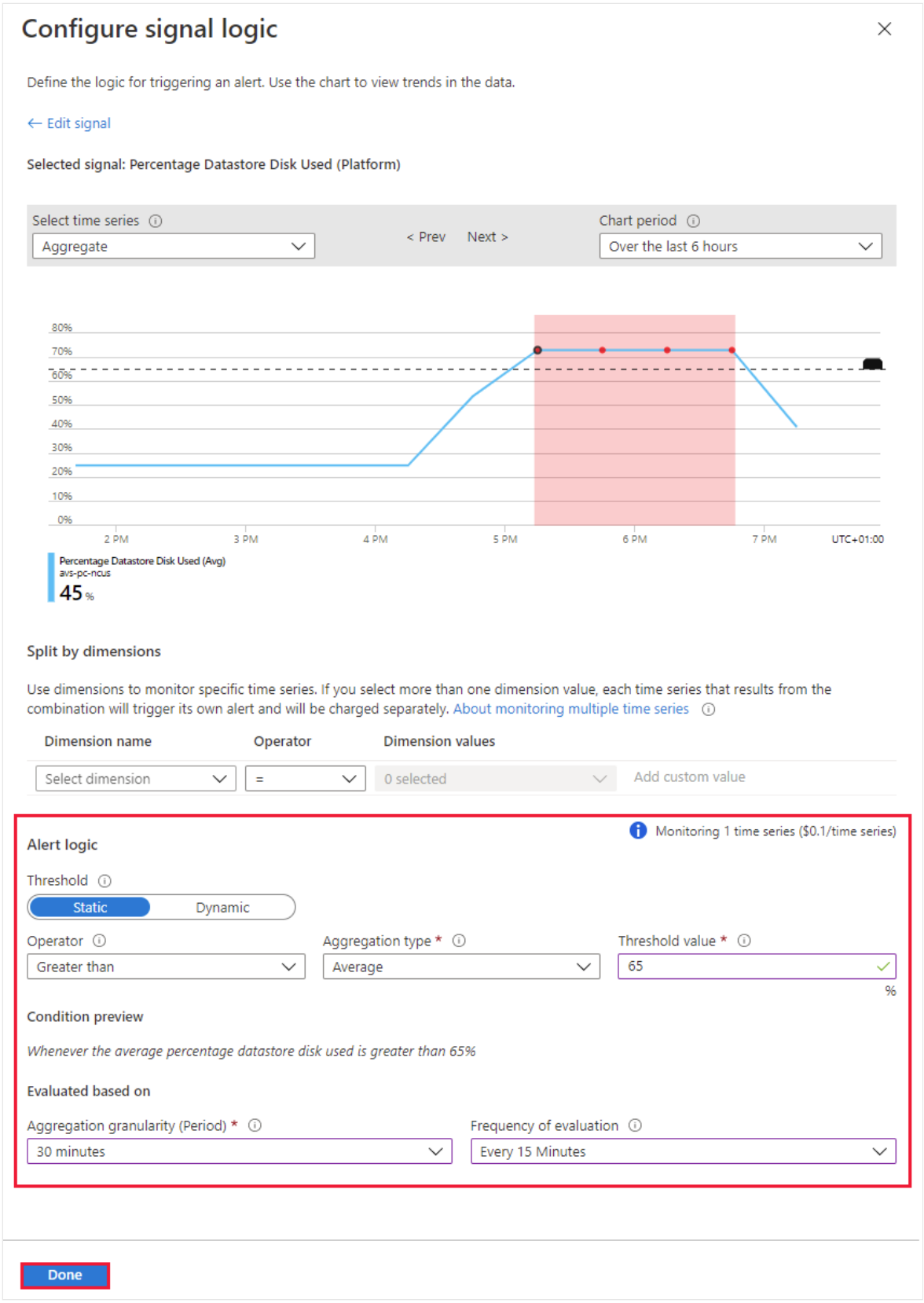
3. Under **Condition**, select **Add condition**, and in the window that opens, selects the signal you want to create for the alert rule.

   In our example, we selected **Percentage Datastore Disk Used**, which is relevant from an Azure VMware Solution SLA perspective.



4. Define the logic that triggers the alert and then select **Done**.

   In our example, only the **Threshold** and **Frequency of evaluation** were adjusted.



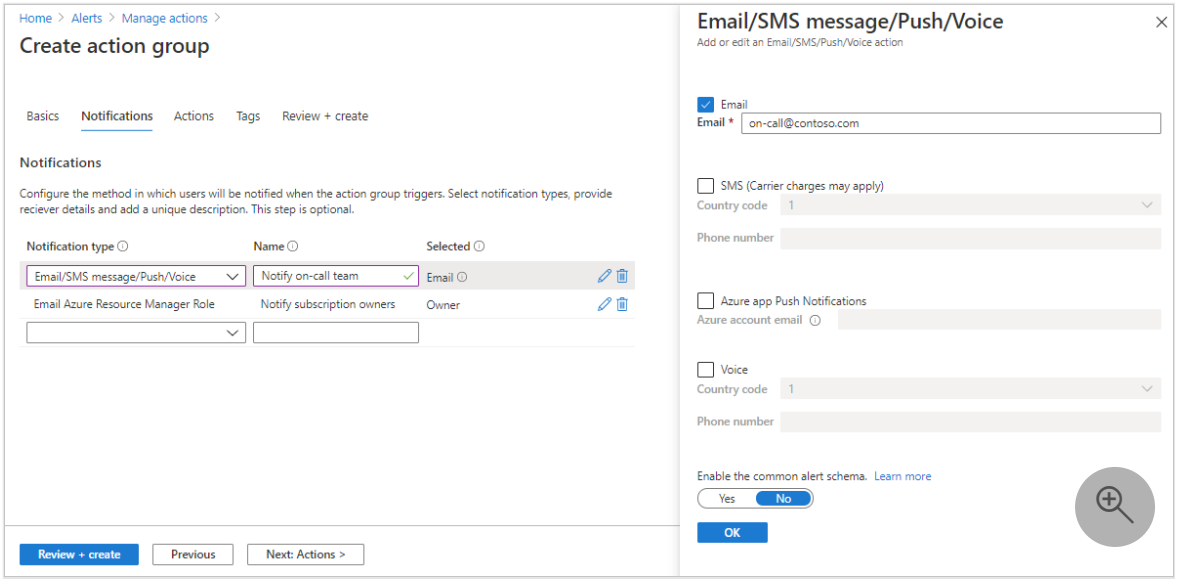
5. Under **Actions**, select **Add action groups**. The action group defines *how* the notification is received and *who* receives it. You can receive notifications by email, SMS, Azure Mobile App Push Notification or voice message.

6. Select an existing action group or select **Create action group** to create a new one.

7. In the window that opens, on the **Basics** tab, give the action group a name and a display name.

8. Select the **Notifications** tab, select a **Notification Type** and **Name**. Then select **OK**.

   Our example is based on email notification.

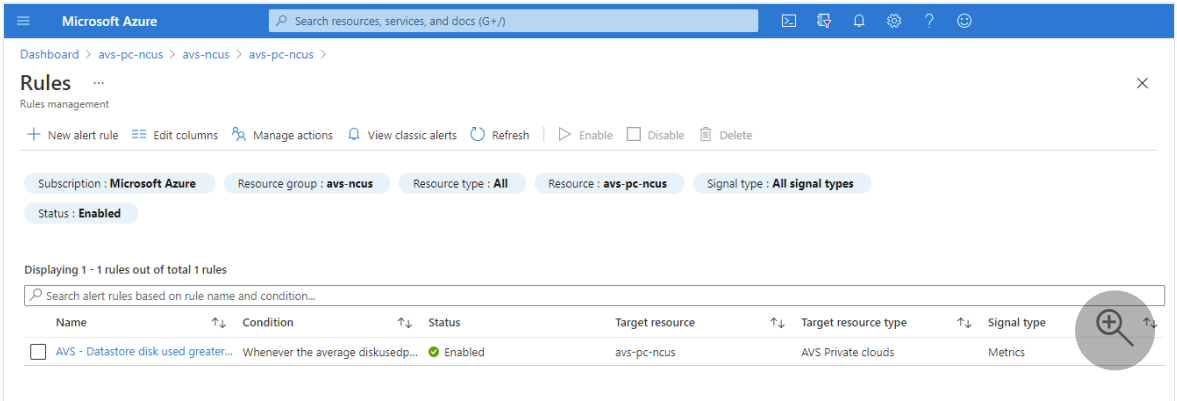


9. (Optional) Configure the **Actions** if you want to take proactive actions and receive notification on the event. Select an available **Action type** and then select **Review + create**.

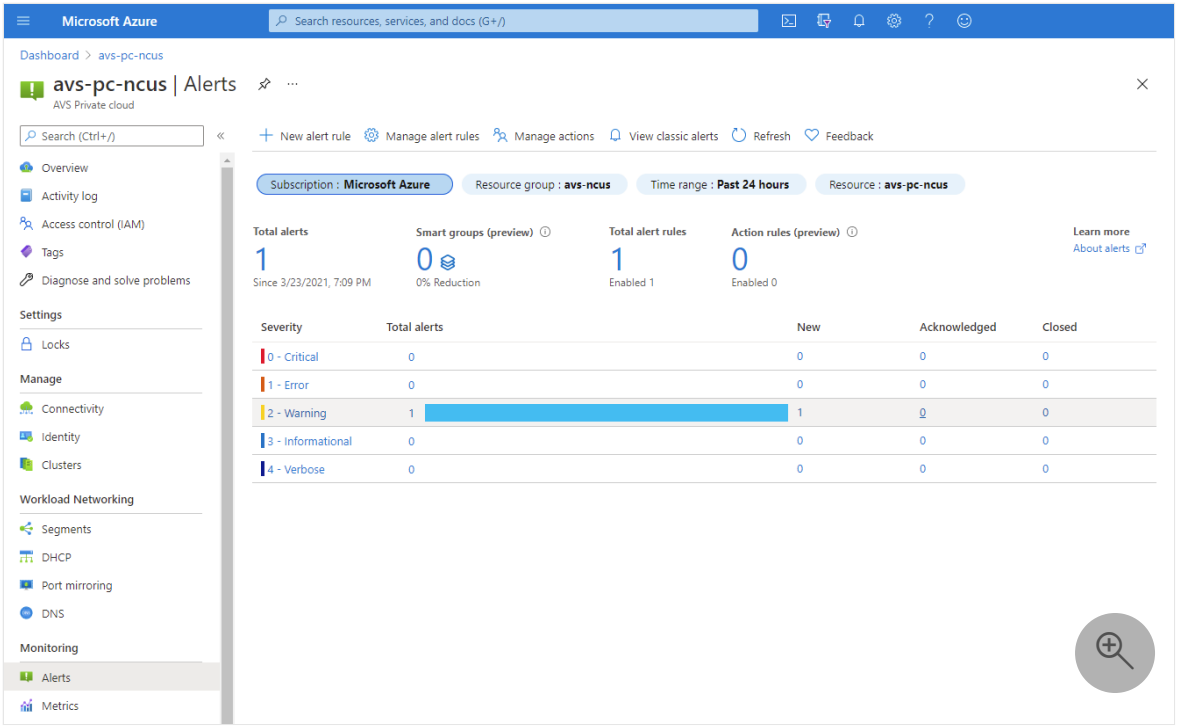
   - **Automation Runbooks** - to automate tasks based on alerts
   - **Azure Functions** – for custom event-driven serverless code execution
   - **ITSM** – to integrate with a service provider like ServiceNow to create a ticket
   - **Logic App** - for more complex workflow orchestration
   - **Webhooks** - to trigger a process in another service

10. Under the **Alert rule details**, provide a name, description, resource group to store the alert rule, the severity. Then select **Create alert rule**.

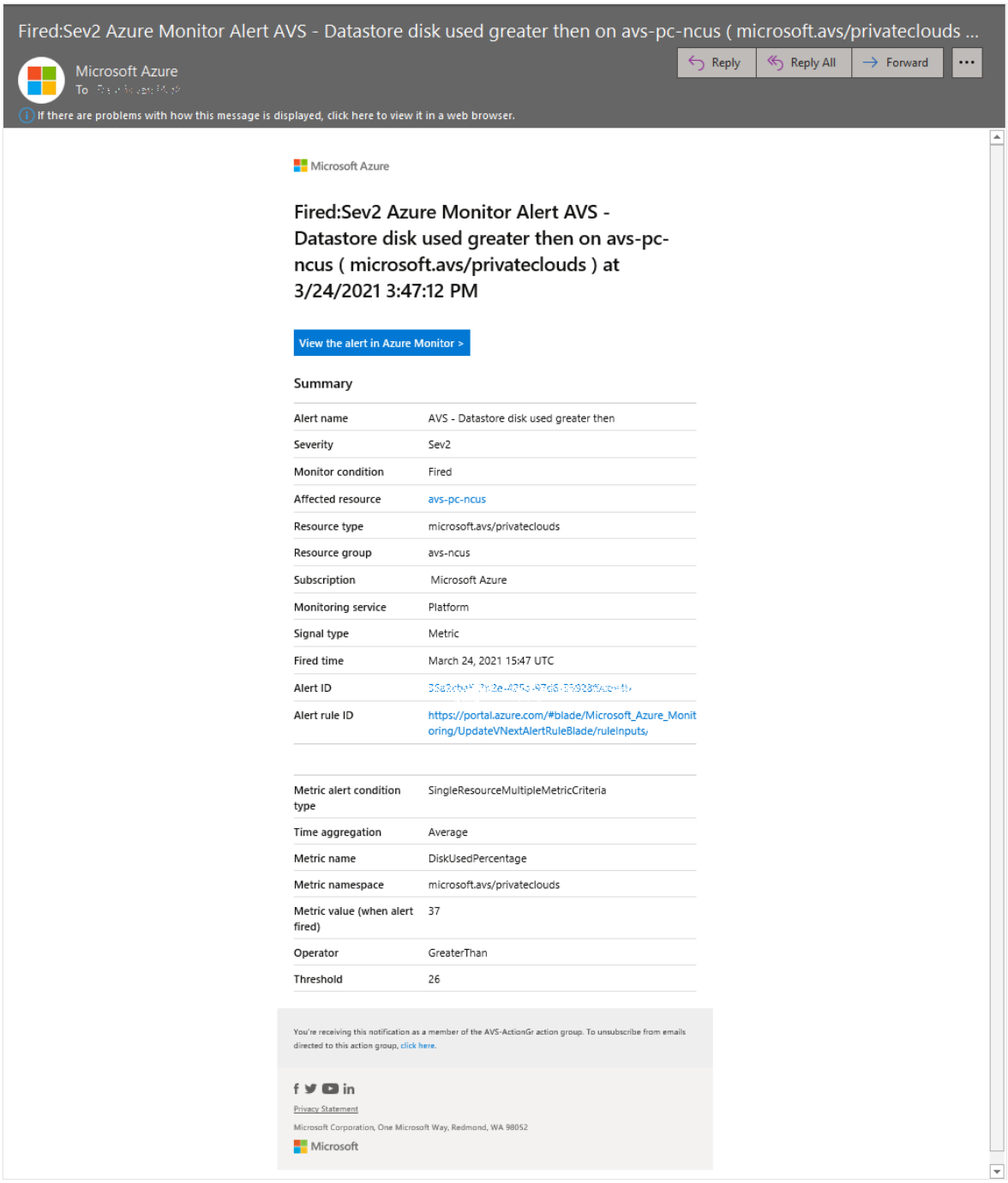
    The alert rule is visible and can be managed from the Azure portal.



As soon as a metric reaches the threshold as defined in an alert rule, the **Alerts** menu is updated and made visible.

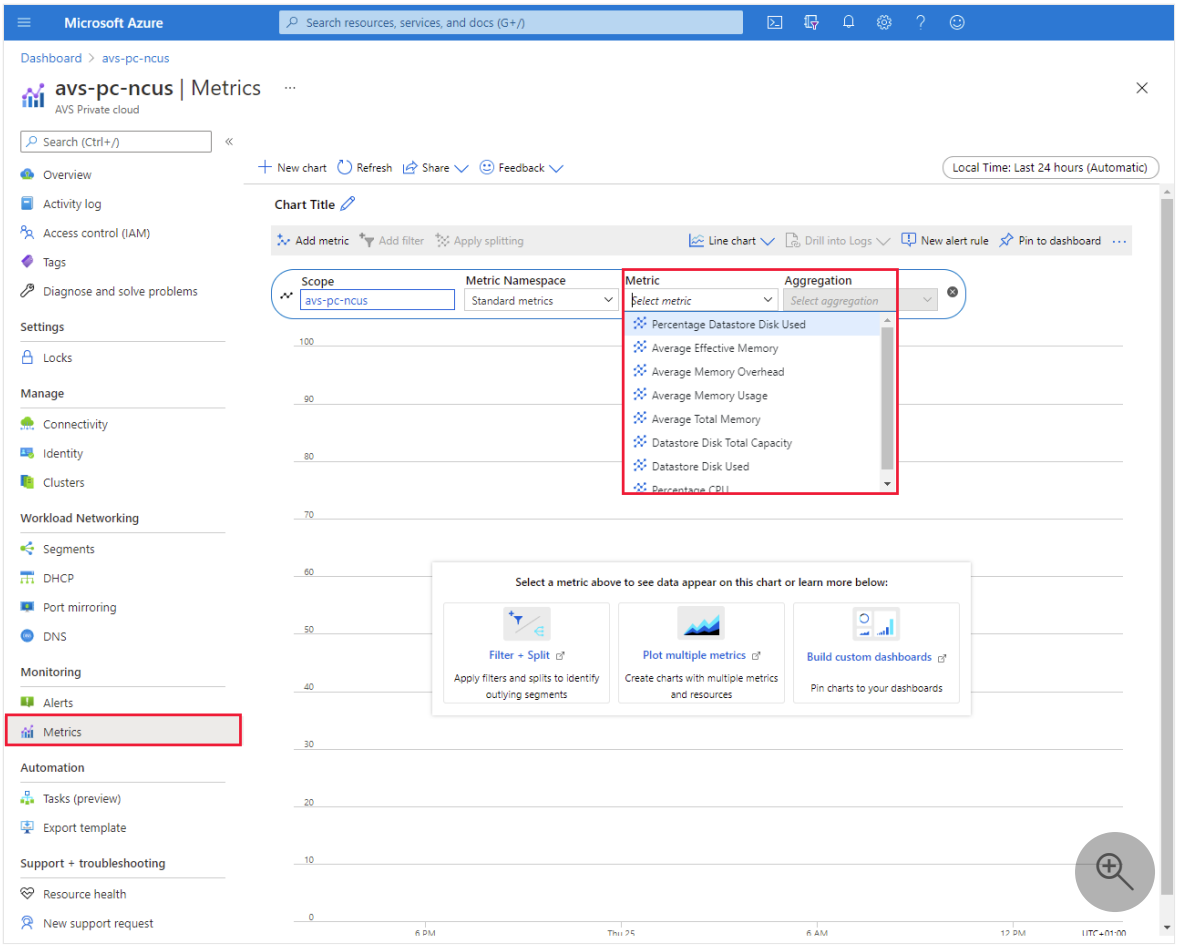


Depending on the configured Action Group, you receive a notification through the configured medium. In our example, we configured email.



Work with metrics

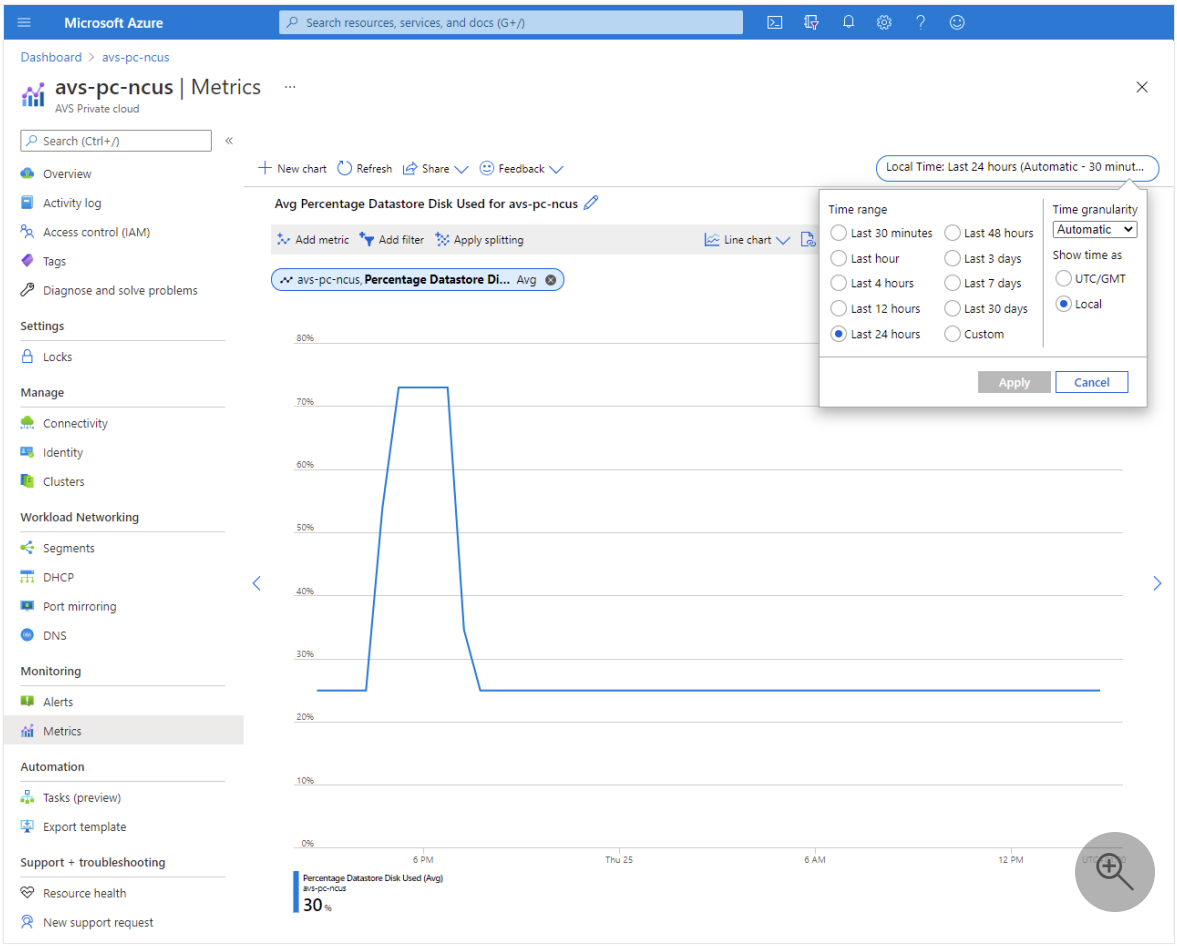
1. From your Azure VMware Solution private cloud, select **Monitoring** > **Metrics**. Then select the metric you want from the drop-down.



2. You can change the diagram's parameters, such as the **Time range** or the **Time granularity**.

   Other options are:

   - **Drill into Logs** and query the data in the related Log Analytics workspace
   - **Pin this diagram** to an Azure Dashboard for convenience.



Next steps

Now that you configured an alert rule for your Azure VMware Solution private cloud, you can learn more about:

- Azure Monitor Metrics
- Azure Monitor Alerts
- Azure Action Groups

You can also continue with one of the other Azure VMware Solution how-to guides.

Deploy Arc-enabled VMware vSphere for Azure VMware Solution private cloud

Article • 05/15/2024

In this article, learn how to deploy Arc-enabled VMware vSphere for Azure VMware Solution private cloud. Once you set up the components needed, you're ready to execute operations in Azure VMware Solution vCenter Server from the Azure portal. Arc-enabled Azure VMware Solution allows you to do the following actions:

- Identify your VMware vSphere resources (VMs, templates, networks, datastores, clusters/hosts/resource pools) and register them with Arc at scale.
- Perform different virtual machine (VM) operations directly from Azure like; create, resize, delete, and power cycle operations (start/stop/restart) on VMware VMs consistently with Azure.
- Permit developers and application teams to use VM operations on-demand with Role-based access control.
- Install the Arc-connected machine agent to govern, protect, configure, and monitor them.
- Browse your VMware vSphere resources (vms, templates, networks, and storage) in Azure

Deployment considerations

When you run software in Azure VMware Solution, as a private cloud in Azure, there are benefits not realized by operating your environment outside of Azure. For software running in a virtual machine (VM) like, SQL Server and Windows Server, running in Azure VMware Solution provides more value such as free Extended Security Updates (ESUs).

To take advantage of the benefits of running in an Azure VMware Solution, use this article to enable Arc and fully integrate the experience with the Azure VMware Solution private cloud. Alternatively, Arc-enabling VMs through the following mechanisms won't create the necessary attributes to register the VM and software as part of Azure VMware Solution and will result in billing for SQL Server ESUs for:

- Arc-enabled servers
- Arc-enabled VMware vSphere
- SQL Server enabled by Azure Arc

Deploy Arc

The following requirements must be met in order to use Azure Arc-enabled Azure VMware Solution.

Prerequisites

The following Register features are for provider registration using Azure CLI.

.NET CLI

```
az provider register --namespace Microsoft.ConnectedVMwarevSphere
az provider register --namespace Microsoft.ExtendedLocation
az provider register --namespace Microsoft.KubernetesConfiguration
az provider register --namespace Microsoft.ResourceConnector
az provider register --namespace Microsoft.AVS
```

Alternately, you can sign in to your Subscription and follow these steps.

1. Navigate to the Resource providers tab.
2. Register the resource providers mentioned above.

> **ⓘ Important**
>
> You can't create the resources in a separate resource group. Ensure you use the same resource group from where the Azure VMware Solution private cloud was created to create your resources.

You need the following items to ensure you're set up to begin the onboarding process to deploy Arc for Azure VMware Solution.

- Validate the regional support before you start the onboarding process. Arc for Azure VMware Solution is supported in all regions where Arc for VMware vSphere on-premises is supported. For details, see Azure Arc-enabled VMware vSphere.
- A management VM with internet access that has a direct line of site to the vCenter Server.
- From the Management VM, verify you have access to vCenter Server and NSX Manager portals.
- A resource group in the subscription where you have an owner or contributor role.
- An unused, NSX network segment that is a static network segment used for deploying the Arc for Azure VMware Solution OVA. If an unused NSX network segment doesn't exist, one gets created.

- The firewall and proxy URLs must be allowlisted to enable communication from the management machine and Appliance VM to the required Arc resource bridge URLs. See the Azure Arc resource bridge network requirements.
- Verify your vCenter Server version is 7.0 or higher.
- A resource pool or a cluster with a minimum capacity of 16 GB of RAM and four vCPUs.
- A datastore with a minimum of 100 GB of free disk space is available through the resource pool or cluster.

> **Note**
>
> - Private endpoint is currently not supported.
> - DHCP support isn't available to customers at this time, only static IP addresses are currently supported.

If you want to use a custom DNS, use the following steps:

1. In your Azure VMware Solution private cloud, navigate to the DNS page, under **Workload networking**, select **DNS, and identify the default forwarder-zones under the **DNS zones** tab.
2. Edit the forwarder zone to add the custom DNS server IP. By adding the custom DNS as the first IP, it allows requests to be directly forwarded to the first IP and decreases the number of retries.

Onboard process to deploy Azure Arc

Use the following steps to guide you through the process to onboard Azure Arc for Azure VMware Solution.

1. Sign in to the Management VM and extract the contents from the compressed file from the following location. The extracted file contains the scripts to install the software.

2. Open the 'config_avs.json' file and populate all the variables.

   Config JSON

   JSON

```
{
  "subscriptionId": "",
  "resourceGroup": "",
  "applianceControlPlaneIpAddress": "",
```

```
  "privateCloud": "",
  "isStatic": true,
  "staticIpNetworkDetails": {
   "networkForApplianceVM": "",
   "networkCIDRForApplianceVM": "",
   "k8sNodeIPPoolStart": "",
   "k8sNodeIPPoolEnd": "",
   "gatewayIPAddress": ""
  }
}
```

- Populate the `subscriptionId`, `resourceGroup`, and `privateCloud` names respectively.
- `isStatic` is always true.
- `networkForApplianceVM` is the name for the segment for Arc appliance VM. One gets created if it doesn't already exist.
- `networkCIDRForApplianceVM` is the IP CIDR of the segment for Arc appliance VM. It should be unique and not affect other networks of Azure VMware Solution management IP CIDR.
- `GatewayIPAddress` is the gateway for the segment for Arc appliance VM.
- `applianceControlPlaneIpAddress` is the IP address for the Kubernetes API server that should be part of the segment IP CIDR provided. It shouldn't be part of the K8s node pool IP range.
- `k8sNodeIPPoolStart`, `k8sNodeIPPoolEnd` are the starting and ending IP of the pool of IPs to assign to the appliance VM. Both need to be within the `networkCIDRForApplianceVM`.
- `k8sNodeIPPoolStart`, `k8sNodeIPPoolEnd`, `gatewayIPAddress` , `applianceControlPlaneIpAddress` are optional. You can choose to skip all the optional fields or provide values for all. If you choose not to provide the optional fields, then you must use /28 address space for `networkCIDRForApplianceVM` with the first Ip as the gateway.
- If all the parameters are provided, the firewall and proxy URLs must be allowlisted for the Ips between K8sNodeIPPoolStart, k8sNodeIPPoolEnd.
- If you're skipping the optional fields, the firewall and proxy URLs must be allowlisted the following IPs in the segment. If the networkCIDRForApplianceVM is x.y.z.1/28, the IPs to allowlist are between x.y.z.11 – x.y.z.14. See the Azure Arc resource bridge network requirements.

Json example

JSON

```
{
  "subscriptionId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
  "resourceGroup": "test-rg",
  "privateCloud": "test-pc",
  "isStatic": true,
  "staticIpNetworkDetails": {
   "networkForApplianceVM": "arc-segment",
   "networkCIDRForApplianceVM": "10.14.10.1/28"
  }
}
```

3. Run the installation scripts. You can optionionally setup this preview from a Windows or Linux-based jump box/VM.

   Run the following commands to execute the installation script.

   Windows based jump box/VM

   Script isn't signed so we need to bypass Execution Policy in PowerShell. Run the following commands.

   ```
   Set-ExecutionPolicy -Scope Process -ExecutionPolicy ByPass;
   .\run.ps1 -Operation onboard -FilePath {config-json-path}
   ```

4. More Azure resources are created in your resource group.

   - Resource bridge
   - Custom location
   - VMware vCenter Server

> **ⓘ Important**
>
> After the successful installation of Azure Arc Resource Bridge, it's recommended to retain a copy of the resource bridge config.yaml files in a place that facilitates easy retrieval. These files could be needed later to run commands to perform management operations (e.g. az arcappliance upgrade) on the resource bridge. You can find the three .yaml files (config files) in the same folder where you ran the script.

When the script is run successfully, check the status to see if Azure Arc is now configured. To verify if your private cloud is Arc-enabled, do the following actions:

- In the left navigation, locate **Operations**.
- Choose **Azure Arc**.
- Azure Arc state shows as **Configured**.

To recover from failed deployments:

If the Azure Arc resource bridge deployment fails, consult the Azure Arc resource bridge troubleshooting guide. While there can be many reasons why the Azure Arc resource bridge deployment fails, one of them is KVA timeout error. Learn more about the KVA timeout error and how to troubleshoot.

Discover and project your VMware vSphere infrastructure resources to Azure

When Arc appliance is successfully deployed on your private cloud, you can do the following actions.

- View the status from within the private cloud left navigation under **Operations** > **Azure Arc**.
- View the VMware vSphere infrastructure resources from the private cloud left navigation under **Private cloud** then select **Azure Arc vCenter Server resources**.
- Discover your VMware vSphere infrastructure resources and project them to Azure by navigating, **Private cloud** > **Arc vCenter Server resources** > **Virtual Machines**.
- Similar to VMs, customers can enable networks, templates, resource pools, and data-stores in Azure.

Enable virtual machines, resource pools, clusters, hosts, datastores, networks, and VM templates in Azure

Once you connected your Azure VMware Solution private cloud to Azure, you can browse your vCenter Server inventory from the Azure portal. This section shows you how to make these resources Azure enabled.

> **Note**
>
> Enabling Azure Arc on a VMware vSphere resource is a read-only operation on vCenter Server. It doesn't make changes to your resource in vCenter Server.

1. On your Azure VMware Solution private cloud, in the left navigation, locate **vCenter Server Inventory**.
2. Select the resources you want to enable, then select **Enable in Azure**.
3. Select your Azure **Subscription** and **Resource Group**, then select **Enable**.

The enable action starts a deployment and creates a resource in Azure, creating representative objects in Azure for your VMware vSphere resources. It allows you to manage who can access those resources through Role-based access control granularly.

Repeat the previous steps for one or more virtual machine, network, resource pool, and VM template resources.

Additionally, for virtual machines there's an another section to configure **VM extensions**. This enables guest management to facilitate more Azure extensions to be installed on the VM. The steps to enable this would be:

1. Select **Enable guest management**.
2. Choose a **Connectivity Method** for the Arc agent.
3. Provide an Administrator/Root access username and password for the VM.

If you choose to enable the guest management as a separate step or have issues with the VM extension install steps, review the prerequisites and steps discussed in the following section.

Enable guest management and extension installation

Before you install an extension, you must enable guest management on the VMware VM.

Prerequisite

Before you can install an extension, ensure your target machine meets the following conditions:

- Is running a supported operating system.
- Is able to connect through the firewall to communicate over the internet and these URLs aren't blocked.
- Has VMware tools installed and running.
- Is powered on and the resource bridge has network connectivity to the host running the VM.
- Is Enabled in Azure.

Enable guest management

You need to enable guest management on the VMware VM before you can install an extension. Use the following steps to enable guest management.

1. Navigate to Azure portal.
2. From the left navigation, locate **vCenter Server Inventory** and choose **Virtual Machines** to view the list of VMs.
3. Select the VM you want to install the guest management agent on.
4. Select **Enable guest management** and provide the administrator username and password to enable guest management then select **Apply**.
5. Locate the VMware vSphere VM you want to check for guest management and install extensions on, select the name of the VM.
6. Select **Configuration** from the left navigation for a VMware VM.
7. Verify **Enable guest management** is now checked.

From here more extensions can be installed. See the VM extensions Overview for a list of current extensions.

Manually integrate an Arc-enabled VM into Azure VMware Solutions

When a VM in Azure VMware Solution private cloud is Arc-enabled using a method distinct from the one outlined in this document, the following steps are provided to refresh the integration between the Arc-enabled VMs and Azure VMware Solution.

These steps change the VM machine type from *Machine – Azure Arc* to type *Machine – Azure Arc (AVS),* which has the necessary integrations with Azure VMware Solution.

There are two ways to refresh the integration between the Arc-enabled VMs and Azure VMware Solution:

1. In the Azure VMware Solution private cloud, navigate to the vCenter Server inventory and Virtual Machines section within the portal. Locate the virtual machine that requires updating and follow the process to 'Enable in Azure'. If the option is grayed out, you must first **Remove from Azure** and then proceed to **Enable in Azure**

2. Run the az connectedvmware vm create Azure CLI command on the VM in Azure VMware Solution to update the machine type.

Azure CLI

```
az connectedvmware vm create --subscription <subscription-id> --location
<Azure region of the machine> --resource-group <resource-group-name> --
custom-location
/providers/microsoft.extendedlocation/customlocations/<custom-location-name>
--name <machine-name> --inventory-item /subscriptions/<subscription-
id>/resourceGroups/<resource-group-
name>/providers/Microsoft.ConnectedVMwarevSphere/VCenters/<vcenter-
name>/InventoryItems/<machine-name>
```

Next Steps

To manage Arc-enabled Azure VMware Solution go to: Manage Arc-enabled Azure VMware private cloud - Azure VMware Solution To remove Arc-enabled Azure VMware Solution resources from Azure go to: Remove Arc-enabled Azure VMware Solution vSphere resources from Azure - Azure VMware Solution.

Manage Arc-enabled Azure VMware private cloud

Article • 02/06/2024

In this article, learn how to update the Arc appliance credentials, upgrade the Arc resource bridge, and collect logs from the Arc resource bridge.

Update Arc appliance credential

When **cloud admin** credentials are updated, use the following steps to update the credentials in the appliance store.

1. Sign in to the Management VM from where the onboard process was performed. Change the directory to **onboarding directory**.
2. Run the following command: For Windows-based Management VM.

   `./.temp/.env/Scripts/activate`

   For Linux-based Management VM

   `./.temp/.env/bin/activate
3. Run the following command:

   `az arcappliance update-infracredentials vmware --kubeconfig <kubeconfig file>`
4. Run the following command:

`az connectedvmware vcenter connect --debug --resource-group {resource-group} --name {vcenter-name-in-azure} --location {vcenter-location-in-azure} --custom-location {custom-location-name} --fqdn {vcenter-ip} --port {vcenter-port} --username cloudadmin@vsphere.local --password {vcenter-password}`

> **Note**
>
> Customers need to ensure kubeconfig and SSH keys remain available as they will be required for log collection, appliance Upgrade, and credential rotation. These parameters will be required at the time of upgrade, log collection, and credential update scenarios.

Parameters

Required parameters

`-kubeconfig # kubeconfig of Appliance resource`

Examples

The following command invokes the set credential for the specified appliance resource.

```
az arcappliance setcredential <provider> --kubeconfig <kubeconfig>
```

Upgrade the Arc resource bridge

> **Note**
>
> Arc resource bridges, on a supported private cloud provider with an appliance version **1.0.15 or higher**, are automatically opted in to cloud-managed upgrade.

Azure Arc-enabled Azure VMware Private Cloud requires the Arc resource bridge to connect your VMware vSphere environment with Azure. Periodically, new images of Arc resource bridge are released to include security and feature updates. The Arc resource bridge can be manually upgraded from the vCenter server. You must meet all upgrade prerequisites before attempting to upgrade. The vCenter server must have the kubeconfig and appliance configuration files stored locally. If the cloudadmin credentials change after the initial deployment of the resource bridge, update the Arc appliance credential before you attempt a manual upgrade.

Arc resource bridge can be manually upgraded from the management machine. The manual upgrade generally takes between 30-90 minutes, depending on the network speed. The upgrade command takes your Arc resource bridge to the immediate next version, which might not be the latest available version. Multiple upgrades could be needed to reach a supported version. Verify your resource bridge version by checking the Azure resource of your Arc resource bridge.

Collect logs from the Arc resource bridge

Perform ongoing administration for Arc-enabled VMware vSphere by collecting logs from the Arc resource bridge.

Remove Arc-enabled Azure VMware Solution vSphere resources from Azure

Article • 07/02/2024

> **⊗ Caution**
>
> This article references CentOS, a Linux distribution that is End Of Life (EOL) status. Please consider your use and planning accordingly. For more information, see the CentOS End Of Life guidance.

In this article, learn how to cleanly remove your VMware vCenter environment from Azure Arc-enabled VMware vSphere. For VMware vSphere environments that you no longer want to manage with Azure Arc-enabled VMware vSphere, use the information in this article to perform the following actions:

- Remove guest management from VMware virtual machines (VMs).
- Remove VMware vSphere resource from Azure Arc.
- Remove Arc resource bridge related items in your vCenter.

Remove guest management from VMware VMs

To prevent continued billing of Azure management services, after you remove the vSphere environment from Azure Arc, you must first remove guest management from all Arc-enabled Azure VMware Solution VMs where it was enabled.

When you enable guest management on Arc-enabled Azure VMware Solution VMs, the Arc connected machine agent is installed on them. Once guest management is enabled, you can install VM extensions on them and use Azure management services like the Log Analytics on them.

To completely remove guest management, use the following steps to remove any VM extensions from the virtual machine, disconnect the agent, and uninstall the software from your virtual machine. It's important to complete each of the three steps to fully remove all related software components from your virtual machines.

Remove VM extensions

Use the following steps to uninstall extensions from the portal.

> ⓘ Note
>
> **Steps 2-5** must be performed for all the VMs that have VM extensions installed.

1. Sign in to your Azure VMware Solution private cloud.
2. Select **Virtual machines** in **Private cloud**, found in the left navigation under "vCenter Server Inventory Page".
3. Search and select the virtual machine where you have **Guest management** enabled.
4. Select **Extensions**.
5. Select the extensions and select **Uninstall**.

Disable guest management from Azure Arc

To avoid problems onboarding the same VM to **Guest management**, we recommend you do the following steps to cleanly disable guest management capabilities.

> ⓘ Note
>
> **Steps 2-3** must be performed for **all VMs** that have **Guest management** enabled.

1. Sign into the virtual machine using administrator or root credentials and run the following command in the shell.
   a. `azcmagent disconnect --force-local-only`.
2. Uninstall the `ConnectedMachine agent` from the machine.
3. Set the **identity** on the VM resource to **none**.

Uninstall agents from Virtual Machines (VMs)

Windows VM uninstall

To uninstall the Windows agent from the machine, use the following steps:

1. Sign in to the computer with an account that has administrator permissions.
2. In **Control Panel**, select **Programs and Features**.
3. In **Programs and Features**, select **Azure Connected machine Agent**, select **Uninstall**, then select **Yes**.
4. Delete the `C:\Program Files\AzureConnectedMachineAgent` folder.

Linux VM uninstall

To uninstall the Linux agent, the command to use depends on the Linux operating system. You must have `root` access permissions or your account must have elevated rights using sudo.

- For Ubuntu, run the following command:

  ```
  Bash

  sudo apt purge azcmagent
  ```

- For RHEL, CentOS, Oracle Linux run the following command:

  ```
  Bash

  sudo yum remove azcmagent
  ```

- For SLES, run the following command:

  ```
  Bash

  sudo zypper remove azcmagent
  ```

Remove VMware vSphere resources from Azure

When you activate Arc-enabled Azure VMware Solution resources in Azure, a representation is created for them in Azure. Before you can delete the vCenter Server resource in Azure, you need to delete all of the Azure resource representations you created for your vSphere resources. To delete the Azure resource representations you created, do the following steps:

1. Go to the Azure portal.
2. Choose **Virtual machines** from Arc-enabled VMware vSphere resources in the private cloud.
3. Select all the VMs that have an Azure Enabled value as **Yes**.
4. Select **Remove from Azure**. This step starts deployment and removes these resources from Azure. The resources remain in your vCenter Server.
   a. Repeat steps 2, 3 and 4 for **Resourcespools/clusters/hosts**, **Templates**, **Networks**, and **Datastores**.
5. When the deletion completes, select **Overview**.

a. Note the Custom location and the Azure Arc Resource bridge resources in the Essentials section.
6. Select **Remove from Azure** to remove the vCenter Server resource from Azure.
7. Go to vCenter Server resource in Azure and delete it.
8. Go to the Custom location resource and select **Delete**.
9. Go to the Azure Arc Resource bridge resources and select **Delete**.

At this point, all of your Arc-enabled VMware vSphere resources are removed from Azure.

Remove Arc resource bridge related items in your vCenter

During onboarding, to create a connection between your VMware vCenter and Azure, an Azure Arc resource bridge is deployed into your VMware vSphere environment. As the last step, you must delete the resource bridge VM as well the VM template created during the onboarding.

As a last step, run the following command:

```
az rest --method delete --
"https://management.azure.com/subscriptions/%3Csubscrption-
id%3E/resourcegroups/%3Cresource-group-
name%3E/providers/Microsoft.AVS/privateClouds/%3Cprivate-cloud-
name%3E/addons/arc?api-version=2022-05-01%22"
```

Once that step is done, Arc no longer works on the Azure VMware Solution private cloud. When you delete Arc resources from vCenter Server, it doesn't affect the Azure VMware Solution private cloud for the customer.

Feedback

Application performance monitoring and troubleshooting solutions for Azure VMware Solution

Article • 12/12/2023

A key objective of Azure VMware Solution is to maintain the performance and security of applications and services across VMware on Azure and on-premises. Getting there requires visibility into complex infrastructures and quickly pinpointing the root cause of service disruptions across the hybrid cloud.

Microsoft solutions

Microsoft recommends Application Insights, a feature of Azure Monitor, to maximize the availability and performance of your applications and services.

Learn how modern monitoring with Azure Monitor can transform your business by reviewing the product overview, features, getting started guide and more.

Third-party solutions

Our application performance monitoring and troubleshooting partners have industry-leading solutions in VMware-based environments that assure the availability, reliability, and responsiveness of applications and services. Our customers adopt many of the solutions integrated with VMware NSX-T Data Center for their on-premises deployments. As one of our key principles, we want to enable them to continue to use their investments and VMware solutions running on Azure. Many of the Independent Software Vendors (ISV) already validated their solutions with Azure VMware Solution.

You can find more information about these solutions here:

- NETSCOUT
- Turbonomic

Configure Aria Operations for Azure VMware Solution

Article • 03/22/2024

Aria Operations is an operations management platform that allows VMware infrastructure administrators to monitor system resources. These system resources could be application-level or infrastructure level (both physical and virtual) objects. Most VMware administrators use Aria Operations to monitor and manage their VMware private cloud components – vCenter Server, ESXi, NSX, vSAN, and VMware HCX. Each provisioned Azure VMware Solution private cloud includes a dedicated vCenter Server, NSX Manager, vSAN, and HCX deployment.

Thoroughly review Before you begin and Prerequisites first.

Before you begin

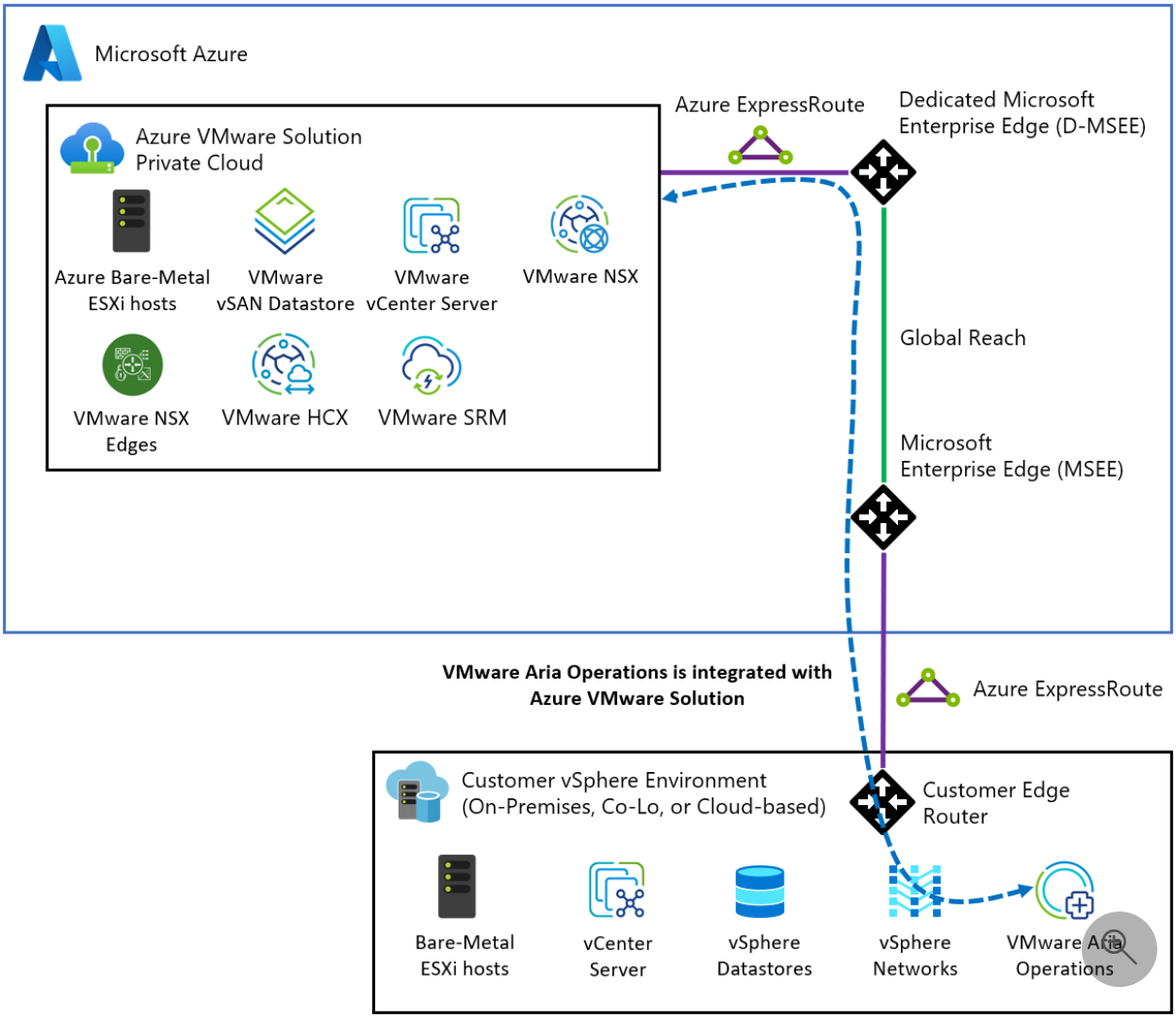
- Review the Aria Operations product documentation to learn more about deploying Aria Operations.
- Review the basic Azure VMware Solution Software-Defined Datacenter (SDDC) tutorial series.
- Optionally, review the Aria Operations Remote Collector Nodes product documentation for the on-premises Aria Operations managing Azure VMware Solution deployment option.

Prerequisites

- Aria Operations is installed.
- An Azure VMware Solution private cloud is deployed in Azure.
- A VPN or an Azure ExpressRoute configured between on-premises and Azure VMware Solution private cloud.

On-premises Aria Operations managing Azure VMware Solution deployment

Most customers have an existing on-premises deployment of Aria Operations to manage one or more on-premises vCenter Server SSO domains. When they provision an Azure VMware Solution private cloud, they connect their on-premises environment with their private cloud using an Azure ExpressRoute or a Layer 3 VPN solution.



To extend the Aria Operations capabilities to the Azure VMware Solution private cloud, you create an adapter instance for the private cloud resources. It collects data from the Azure VMware Solution private cloud and brings it into the on-premises Aria Operations. The on-premises Aria Operations instance can directly connect to the vCenter Server and NSX Manager of the Azure VMware Solution. Optionally, you can deploy an Aria Operations Remote Collector in the Azure VMware Solution private cloud. The collector compresses and encrypts the data collected from the private cloud before it's sent over the ExpressRoute or VPN network to the Aria Operations running on-premises.

> **Tip**
>
> Refer to the VMware documentation for step-by-step guide for installing Aria Operations.

Aria Operations Cloud managing Azure VMware Solution deployment

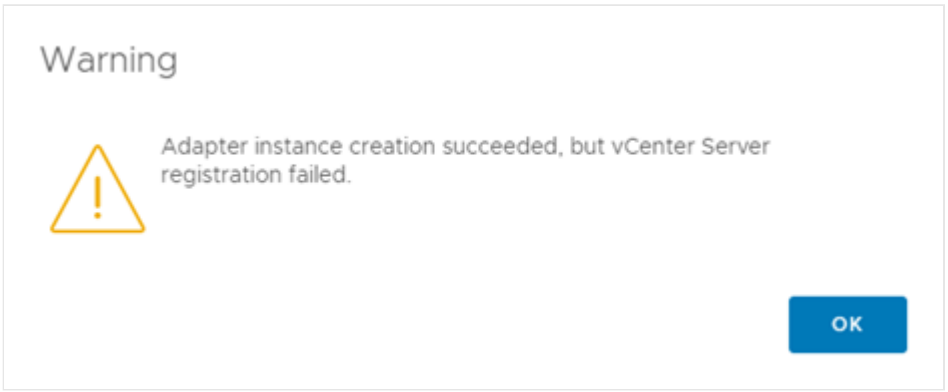
VMware Aria Operations Cloud supports the Azure VMware Solution, including the vCenter Server, vSAN and NSX adapters.

> **Important**
>
> Refer to the VMware documentation for the step-by-step guide for connecting Aria Operations Cloud to Azure VMware Solution.

Known limitations

- The **cloudadmin@vsphere.local** user in Azure VMware Solution has limited privileges. Virtual machines (VMs) on Azure VMware Solution doesn't support in-guest memory collection using VMware tools. Active and consumed memory utilization continues to work in this case.
- Workload optimization for host-based business intent doesn't work because Azure VMware Solutions manage cluster configurations, including DRS settings.
- Workload optimization for the cross-cluster placement within the private cloud using the cluster-based business intent is fully supported with Aria Operations. However, workload optimization isn't aware of resource pools and places the VMs at the cluster level. A user can manually correct it in the Azure VMware Solution vCenter Server interface.
- You can't sign into Aria Operations using your Azure VMware Solution vCenter Server credentials.
- Azure VMware Solution doesn't support the Aria Operations plugin.

When you connect the Azure VMware Solution vCenter Server to Aria Operations using a vCenter Server CloudAdmin Account, you see a warning:



The warning occurs because the **cloudadmin@vsphere.local** user in Azure VMware Solution doesn't have sufficient privileges to do all vCenter Server actions required for registration. However, the privileges are sufficient for the adapter instance to do data collection, as seen in the following example:

Name	Adapter Type	Object Type	Collection State	Collection Status
vc-avs	vCenter Adapter	vCenter Server		

For more information, see Privileges Required for Configuring a vCenter Server Adapter Instance .

> **Note**
>
> VMware Aria Operations integration with the NSX Manager component of the Azure VMware Solution requires the “auditor” role to be added to the user with the NSX Manager cloudadmin role.

The Azure VMware Solution REST API allows you to manage private clouds.

Article • 10/31/2023

The Azure VMware Solution REST API provides operations for working with the following resources

az vmware

Reference

> **Note**
>
> This reference is part of the **vmware** extension for the Azure CLI (version 2.54.0 or higher). The extension will automatically install the first time you run an **az vmware** command. Learn more about extensions.

Commands to manage Azure VMware Solution.

Commands

Expand table

Name	Description	Type	Status
az vmware addon	Commands to manage addons for a private cloud.	Extension	GA
az vmware addon arc	Commands to manage a Arc addon.	Extension	GA
az vmware addon arc create	Create an Arc addon for a private cloud.	Extension	GA
az vmware addon arc delete	Delete an Arc addon for a private cloud.	Extension	GA
az vmware addon arc show	Show details of an Arc addon for a private cloud.	Extension	GA
az vmware addon arc update	Update an Arc addon for a private cloud.	Extension	GA
az vmware addon hcx	Commands to manage a HCX addon.	Extension	GA
az vmware addon hcx create	Create a HCX addon for a private cloud.	Extension	GA
az vmware addon hcx delete	Delete a HCX addon for a private cloud.	Extension	GA
az vmware addon hcx show	Show details of a HCX addon for a private cloud.	Extension	GA

Name	Description	Type	Status
az vmware addon hcx update	Update a HCX addon for a private cloud.	Extension	GA
az vmware addon list	List addons in a private cloud.	Extension	GA
az vmware addon srm	Commands to manage a Site Recovery Manager (SRM) addon.	Extension	GA
az vmware addon srm create	Create a Site Recovery Manager (SRM) addon for a private cloud.	Extension	GA
az vmware addon srm delete	Delete a Site Recovery Manager (SRM) addon for a private cloud.	Extension	GA
az vmware addon srm show	Show details of a Site Recovery Manager (SRM) addon.	Extension	GA
az vmware addon srm update	Update a Site Recovery Manager (SRM) addon for a private cloud.	Extension	GA
az vmware addon vr	Commands to manage a vSphere Replication (VR) addon.	Extension	GA
az vmware addon vr create	Create a vSphere Replication (VR) addon for a private cloud.	Extension	GA
az vmware addon vr delete	Delete a vSphere Replication (VR) addon for a private cloud.	Extension	GA
az vmware addon vr show	Show details of a vSphere Replication (VR) addon for a private cloud.	Extension	GA
az vmware addon vr update	Update a vSphere Replication (VR) addon for a private cloud.	Extension	GA
az vmware authorization	Commands to manage the authorizations of an ExpressRoute Circuit for a private cloud.	Extension	GA
az vmware authorization create	Create an ExpressRoute Circuit Authorization in a private cloud.	Extension	GA
az vmware authorization delete	Delete an ExpressRoute Circuit Authorization in a private cloud.	Extension	GA
az vmware authorization list	List ExpressRoute Circuit Authorizations in a private cloud.	Extension	GA
az vmware authorization show	Get an ExpressRoute Circuit Authorization by name in a private cloud.	Extension	GA

Name	Description	Type	Status
az vmware authorization wait	Place the CLI in a waiting state until a condition is met.	Extension	GA
az vmware cloud-link	Commands to manage cloud links in a private cloud.	Extension	GA
az vmware cloud-link create	Create a cloud link in a private cloud.	Extension	GA
az vmware cloud-link delete	Delete a cloud link in a private cloud.	Extension	GA
az vmware cloud-link list	List cloud link in a private cloud.	Extension	GA
az vmware cloud-link show	Show details of a cloud link in a private cloud.	Extension	GA
az vmware cloud-link update	Update a cloud link in a private cloud.	Extension	GA
az vmware cloud-link wait	Place the CLI in a waiting state until a condition is met.	Extension	GA
az vmware cluster	Commands to manage all the clusters in a private cloud, excluding the first cluster which is the default management cluster.	Extension	GA
az vmware cluster create	Create a cluster in a private cloud.	Extension	GA
az vmware cluster delete	Delete a cluster in a private cloud, excluding the first cluster which is the default management cluster.	Extension	GA
az vmware cluster list	List clusters in a private cloud, excluding the first cluster which is the default management cluster.	Extension	GA
az vmware cluster list-zones	List hosts by zone in a cluster in a private cloud, including the first cluster which is the default management cluster.	Extension	GA
az vmware cluster show	Get a cluster by name in a private cloud, excluding the first cluster which is the default management cluster.	Extension	GA
az vmware cluster update	Update a cluster in a private cloud, excluding the first cluster which is the default management cluster.	Extension	GA

Name	Description	Type	Status
az vmware cluster wait	Place the CLI in a waiting state until a condition is met.	Extension	GA
az vmware datastore	Commands to manage a datastore in a private cloud cluster.	Extension	GA
az vmware datastore create	Please use "netapp-volume create" or "disk-pool-volume create" instead.	Extension	Deprecated
az vmware datastore delete	Delete a datastore in a private cloud cluster.	Extension	GA
az vmware datastore disk-pool-volume	Manage disk pool volume resource.	Extension	GA
az vmware datastore disk-pool-volume create	Create a VMFS datastore in a private cloud cluster using Microsoft.StoragePool provided iSCSI target.	Extension	GA
az vmware datastore elastic-san-volume	Manage Elastic SAN volume resource.	Extension	GA
az vmware datastore elastic-san-volume create	Create an Elastic SAN volume in a private cloud cluster using Microsoft.ElasticSan provider.	Extension	GA
az vmware datastore list	List datastores in a private cloud cluster.	Extension	GA
az vmware datastore netapp-volume	Manage NetApp volume resource.	Extension	GA
az vmware datastore netapp-volume create	Create a new Microsoft.NetApp provided NetApp volume in a private cloud cluster.	Extension	GA
az vmware datastore show	Show details of a datastore in a private cloud cluster.	Extension	GA
az vmware datastore wait	Place the CLI in a waiting state until a condition is met.	Extension	GA
az vmware global-reach-connection	Commands to manage global reach connections in a private cloud.	Extension	GA
az vmware global-reach-connection create	Create a global reach connection in a private cloud.	Extension	GA
az vmware global-reach-connection delete	Delete a global reach connection in a private cloud.	Extension	GA

Name	Description	Type	Status
az vmware global-reach-connection list	List global reach connections in a private cloud.	Extension	GA
az vmware global-reach-connection show	Get a global reach connection by name in a private cloud.	Extension	GA
az vmware global-reach-connection wait	Place the CLI in a waiting state until a condition is met.	Extension	GA
az vmware hcx-enterprise-site	Commands to manage HCX Enterprise Sites in a private cloud.	Extension	GA
az vmware hcx-enterprise-site create	Create an HCX Enterprise Site in a private cloud.	Extension	GA
az vmware hcx-enterprise-site delete	Delete an HCX Enterprise Site in a private cloud.	Extension	GA
az vmware hcx-enterprise-site list	List HCX Enterprise Sites in a private cloud.	Extension	GA
az vmware hcx-enterprise-site show	Get an HCX Enterprise Site by name in a private cloud.	Extension	GA
az vmware iscsi-path	Commands to manage IscsiPath resources in a private cloud.	Extension	GA
az vmware iscsi-path create	Create an IscsiPath in a private cloud.	Extension	GA
az vmware iscsi-path delete	Delete an IscsiPath in a private cloud.	Extension	GA
az vmware iscsi-path list	List IscsiPath resources in a private cloud.	Extension	GA
az vmware iscsi-path show	Get an IscsiPath in a private cloud.	Extension	GA
az vmware iscsi-path wait	Place the CLI in a waiting state until a condition is met.	Extension	GA
az vmware location	Commands to check availability by location.	Extension	GA
az vmware location check-quota-availability	Return quota for subscription by region.	Extension	GA
az vmware location check-trial-availability	Return trial status for subscription by region.	Extension	GA
az vmware location checkquotaavailability	Return quota for subscription by region.	Extension	Deprecated

Name	Description	Type	Status
az vmware location checktrialavailability	Return trial status for subscription by region.	Extension	Deprecated
az vmware placement-policy	Commands to manage placement policies.	Extension	GA
az vmware placement-policy list	List placement policies in a private cloud cluster.	Extension	GA
az vmware placement-policy show	Get a placement policy by name in a private cloud cluster.	Extension	GA
az vmware placement-policy vm	Commands to manage VM placement policies.	Extension	GA
az vmware placement-policy vm-host	Commands to manage VM Host placement policies.	Extension	GA
az vmware placement-policy vm-host create	Create a VM Host placement policy in a private cloud cluster.	Extension	GA
az vmware placement-policy vm-host delete	Delete a VM Host placement policy in a private cloud cluster.	Extension	GA
az vmware placement-policy vm-host update	Update a VM Host placement policy in a private cloud cluster.	Extension	GA
az vmware placement-policy vm create	Create a VM placement policy in a private cloud cluster.	Extension	GA
az vmware placement-policy vm delete	Delete a VM placement policy in a private cloud cluster.	Extension	GA
az vmware placement-policy vm update	Update a VM placement policy in a private cloud cluster.	Extension	GA
az vmware private-cloud	Commands to manage private clouds.	Extension	GA
az vmware private-cloud add-cmk-encryption	Add a Customer Managed Keys Encryption to a private cloud.	Extension	Deprecated
az vmware private-cloud add-identity-source	Add a vCenter Single Sign On Identity Source to a private cloud.	Extension	Deprecated
az vmware private-cloud addidentitysource	Add a vCenter Single Sign On Identity Source to a private cloud.	Extension	Deprecated
az vmware private-cloud create	Create a private cloud.	Extension	GA

Name	Description	Type	Status
az vmware private-cloud delete	Delete a private cloud.	Extension	GA
az vmware private-cloud delete-cmk-encryption	Delete a Customer Managed Keys Encryption from a private cloud.	Extension	Deprecated
az vmware private-cloud delete-identity-source	Delete a vCenter Single Sign On Identity Source for a private cloud.	Extension	Deprecated
az vmware private-cloud deleteidentitysource	Delete a vCenter Single Sign On Identity Source for a private cloud.	Extension	Deprecated
az vmware private-cloud disable-cmk-encryption	Disable a Customer Managed Keys Encryption from a private cloud.	Extension	GA
az vmware private-cloud enable-cmk-encryption	Enable a Customer Managed Keys Encryption to a private cloud.	Extension	GA
az vmware private-cloud identity	Commands for Managed Identity in a private cloud.	Extension	GA
az vmware private-cloud identity-source	Manage a vCenter Single Sign On Identity Source of a private cloud.	Extension	GA
az vmware private-cloud identity-source create	Create a vCenter Single Sign On Identity Source to a private cloud.	Extension	GA
az vmware private-cloud identity-source delete	Delete a vCenter Single Sign On Identity Source of a private cloud.	Extension	GA
az vmware private-cloud identity-source list	List vCenter Single Sign On Identity Sources of a private cloud.	Extension	GA
az vmware private-cloud identity-source show	Show a vCenter Single Sign On Identity Source of a private cloud.	Extension	GA
az vmware private-cloud identity-source update	Update a vCenter Single Sign On Identity Source of a private cloud.	Extension	GA
az vmware private-cloud identity-source wait	Place the CLI in a waiting state until a condition is met.	Extension	GA
az vmware private-cloud identity assign	Assign a Managed Identity in a private cloud.	Extension	GA
az vmware private-cloud identity remove	Remove a Managed Identity in a private cloud.	Extension	GA
az vmware private-cloud identity show	Show Managed Identities in a private cloud.	Extension	GA

Name	Description	Type	Status
az vmware private-cloud list	List the private clouds.	Extension	GA
az vmware private-cloud list-admin-credentials	List the admin credentials for the private cloud.	Extension	GA
az vmware private-cloud listadmincredentials	List the admin credentials for the private cloud.	Extension	Deprecated
az vmware private-cloud rotate-nsxt-password	Rotate the NSX-T Manager password.	Extension	GA
az vmware private-cloud rotate-vcenter-password	Rotate the vCenter password.	Extension	GA
az vmware private-cloud show	Get a private cloud.	Extension	GA
az vmware private-cloud update	Update a private cloud.	Extension	GA
az vmware private-cloud wait	Place the CLI in a waiting state until a condition is met.	Extension	GA
az vmware script-cmdlet	Commands to list and show script cmdlet resources.	Extension	GA
az vmware script-cmdlet list	List script cmdlet resources available for a private cloud to create a script execution resource on a private cloud.	Extension	GA
az vmware script-cmdlet show	Get information about a script cmdlet resource in a specific package on a private cloud.	Extension	GA
az vmware script-execution	Commands to manage script executions in a private cloud.	Extension	GA
az vmware script-execution create	Create or update a script execution in a private cloud.	Extension	GA
az vmware script-execution delete	Delete a ScriptExecution in a private cloud.	Extension	GA
az vmware script-execution list	List script executions in a private cloud.	Extension	GA
az vmware script-execution show	Get an script execution by name in a private cloud.	Extension	GA

Name	Description	Type	Status
az vmware script-execution wait	Place the CLI in a waiting state until a condition is met.	Extension	GA
az vmware script-package	Commands to list and show script packages available to run on the private cloud.	Extension	GA
az vmware script-package list	List script packages available to run on the private cloud.	Extension	GA
az vmware script-package show	Get a script package available to run on a private cloud.	Extension	GA
az vmware vm	Commands to manage Virtual Machines.	Extension	GA
az vmware vm list	List of virtual machines in a private cloud cluster.	Extension	GA
az vmware vm restrict-movement	Enable or disable DRS-driven VM movement restriction.	Extension	GA
az vmware vm show	Get a virtual machine by id in a private cloud cluster.	Extension	GA
az vmware workload-network	Commands to manage workload-networks in a private cloud.	Extension	GA
az vmware workload-network dhcp	Commands to manage a DHCP (Data Host Configuration Protocol) workload network.	Extension	GA
az vmware workload-network dhcp list	List dhcp in a private cloud workload network.	Extension	GA
az vmware workload-network dhcp relay	Commands to manage a DHCP (Data Host Configuration Protocol) workload network.	Extension	GA
az vmware workload-network dhcp relay create	Create DHCP by ID in a private cloud workload network.	Extension	GA
az vmware workload-network dhcp relay delete	Delete DHCP by ID in a private cloud workload network.	Extension	GA
az vmware workload-network dhcp relay update	Create DHCP by ID in a private cloud workload network.	Extension	GA
az vmware workload-network dhcp server	Commands to manage a DHCP (Data Host Configuration Protocol) workload network.	Extension	GA

Name	Description	Type	Status
az vmware workload-network dhcp server create	Create DHCP by ID in a private cloud workload network.	Extension	GA
az vmware workload-network dhcp server delete	Delete DHCP by ID in a private cloud workload network.	Extension	GA
az vmware workload-network dhcp server update	Update DHCP by ID in a private cloud workload network.	Extension	GA
az vmware workload-network dhcp show	Get dhcp by id in a private cloud workload network.	Extension	GA
az vmware workload-network dns-service	Commands to manage a DNS Service workload network.	Extension	GA
az vmware workload-network dns-service create	Create a DNS service by id in a private cloud workload network.	Extension	GA
az vmware workload-network dns-service delete	Delete a DNS service by id in a private cloud workload network.	Extension	GA
az vmware workload-network dns-service list	List of DNS services in a private cloud workload network.	Extension	GA
az vmware workload-network dns-service show	Get a DNS service by id in a private cloud workload network.	Extension	GA
az vmware workload-network dns-service update	Update a DNS service by id in a private cloud workload network.	Extension	GA
az vmware workload-network dns-service wait	Place the CLI in a waiting state until a condition is met.	Extension	GA
az vmware workload-network dns-zone	Commands to manage a DNS Zone workload network.	Extension	GA
az vmware workload-network dns-zone create	Create a DNS zone by id in a private cloud workload network.	Extension	GA
az vmware workload-network dns-zone delete	Delete a DNS zone by id in a private cloud workload network.	Extension	GA
az vmware workload-network dns-zone list	List of DNS zones in a private cloud workload network.	Extension	GA
az vmware workload-network dns-zone show	Get a DNS zone by id in a private cloud workload network.	Extension	GA

Name	Description	Type	Status
az vmware workload-network dns-zone update	Update a DNS zone by id in a private cloud workload network.	Extension	GA
az vmware workload-network dns-zone wait	Place the CLI in a waiting state until a condition is met.	Extension	GA
az vmware workload-network gateway	Commands to manage a Gateway workload network.	Extension	GA
az vmware workload-network gateway list	List of gateways in a private cloud workload network.	Extension	GA
az vmware workload-network gateway show	Get a gateway by id in a private cloud workload network.	Extension	GA
az vmware workload-network port-mirroring	Commands to manage a Port Mirroring workload network.	Extension	GA
az vmware workload-network port-mirroring create	Create a port mirroring profile by id in a private cloud workload network.	Extension	GA
az vmware workload-network port-mirroring delete	Delete a port mirroring profile by id in a private cloud workload network.	Extension	GA
az vmware workload-network port-mirroring list	List of port mirroring profiles in a private cloud workload network.	Extension	GA
az vmware workload-network port-mirroring show	Get a port mirroring profile by id in a private cloud workload network.	Extension	GA
az vmware workload-network port-mirroring update	Update a port mirroring profile by id in a private cloud workload network.	Extension	GA
az vmware workload-network port-mirroring wait	Place the CLI in a waiting state until a condition is met.	Extension	GA
az vmware workload-network public-ip	Commands to manage a Public-IP workload network.	Extension	GA
az vmware workload-network public-ip create	Create a Public IP Block by id in a private cloud workload network.	Extension	GA
az vmware workload-network public-ip delete	Delete a Public IP Block by id in a private cloud workload network.	Extension	GA

Name	Description	Type	Status
az vmware workload-network public-ip list	List of Public IP Blocks in a private cloud workload network.	Extension	GA
az vmware workload-network public-ip show	Get a Public IP Block by id in a private cloud workload network.	Extension	GA
az vmware workload-network public-ip wait	Place the CLI in a waiting state until a condition is met.	Extension	GA
az vmware workload-network segment	Commands to manage a Segment workload network.	Extension	GA
az vmware workload-network segment create	Create a segment by id in a private cloud workload network.	Extension	GA
az vmware workload-network segment delete	Delete a segment by id in a private cloud workload network.	Extension	GA
az vmware workload-network segment list	List of segments in a private cloud workload network.	Extension	GA
az vmware workload-network segment show	Get a segment by id in a private cloud workload network.	Extension	GA
az vmware workload-network segment update	Update a segment by id in a private cloud workload network.	Extension	GA
az vmware workload-network segment wait	Place the CLI in a waiting state until a condition is met.	Extension	GA
az vmware workload-network vm	Commands to manage a Virtual Machine workload network.	Extension	GA
az vmware workload-network vm-group	Commands to manage a VM Group workload network.	Extension	GA
az vmware workload-network vm-group create	Create a vm group by id in a private cloud workload network.	Extension	GA
az vmware workload-network vm-group delete	Delete a vm group by id in a private cloud workload network.	Extension	GA
az vmware workload-network vm-group list	List of vm groups in a private cloud workload network.	Extension	GA
az vmware workload-network vm-group show	Get a vm group by id in a private cloud workload network.	Extension	GA
az vmware workload-network vm-group update	Update a vm group by id in a private cloud workload network.	Extension	GA

Name	Description	Type	Status
az vmware workload-network vm-group wait	Place the CLI in a waiting state until a condition is met.	Extension	GA
az vmware workload-network vm list	List of virtual machines in a private cloud workload network.	Extension	GA
az vmware workload-network vm show	Get a virtual machine by id in a private cloud workload network.	Extension	GA

Az.VMware

Reference

Microsoft Azure PowerShell: Azure VMware Solution cmdlets

VMware

Expand table

Get-AzVMwareAddon	Get an addon by name in a private cloud
Get-AzVMwareAuthorization	Get a ExpressRouteAuthorization
Get-AzVMwareCloudLink	Get a CloudLink
Get-AzVMwareCluster	Get a Cluster
Get-AzVMwareClusterZone	List hosts by zone in a cluster
Get-AzVMwareDatastore	Get a Datastore
Get-AzVMwareGlobalReachConnection	Get a GlobalReachConnection
Get-AzVMwareIscsiPath	Get a IscsiPath
Get-AzVMwarePlacementPolicy	Get a PlacementPolicy
Get-AzVMwarePrivateCloud	Get a PrivateCloud
Get-AzVMwarePrivateCloudAdminCredential	List the admin credentials for the private cloud
Get-AzVMwareVirtualMachine	Get a VirtualMachine
New-AzVMwareAddon	Create or update a addon in a private cloud
New-AzVMwareAddonSrmPropertyObject	Create an in-memory object for AddonSrmProperties.
New-AzVMwareAddonVrPropertyObject	Create an in-memory object for AddonVrProperties.
New-AzVMwareAuthorization	Create a ExpressRouteAuthorization
New-AzVMwareCloudLink	Create a CloudLink

New-AzVMwareCluster	Create a Cluster
New-AzVMwareDatastore	Create a Datastore
New-AzVMwareGlobalReachConnection	Create a GlobalReachConnection
New-AzVMwareIscsiPath	Create a IscsiPath
New-AzVMwarePlacementPolicy	Create a PlacementPolicy
New-AzVMwarePrivateCloud	Create a private cloud
New-AzVMwarePrivateCloudNsxtPassword	Rotate the NSX-T Manager password
New-AzVMwarePrivateCloudVcenterPassword	Rotate the vCenter password
New-AzVMwarePSCredentialExecutionParameterObject	Create an in-memory object for PSCredentialExecutionParameter.
New-AzVMwareScriptSecureStringExecutionParameterObject	Create an in-memory object for ScriptSecureStringExecutionParameter.
New-AzVMwareScriptStringExecutionParameterObject	Create an in-memory object for ScriptStringExecutionParameter.
New-AzVMwareVmHostPlacementPolicyPropertyObject	Create an in-memory object for VmHostPlacementPolicyProperties.
New-AzVMwareVMPlacementPolicyPropertyObject	Create an in-memory object for VMPlacementPolicyProperties.
Remove-AzVMwareAddon	Delete a addon in a private cloud
Remove-AzVMwareAuthorization	Delete a ExpressRouteAuthorization
Remove-AzVMwareCloudLink	Delete a CloudLink
Remove-AzVMwareCluster	Delete a Cluster
Remove-AzVMwareDatastore	Delete a Datastore
Remove-AzVMwareGlobalReachConnection	Delete a GlobalReachConnection
Remove-AzVMwareIscsiPath	Delete a IscsiPath
Remove-AzVMwarePlacementPolicy	Delete a PlacementPolicy
Remove-AzVMwarePrivateCloud	Delete a private cloud
Test-AzVMwareLocationQuotaAvailability	Return quota for subscription by region
Test-AzVMwareLocationTrialAvailability	Return trial status for subscription by region

Update-AzVMwareAuthorization	Update a ExpressRouteAuthorization
Update-AzVMwareCloudLink	Update a CloudLink
Update-AzVMwareCluster	Update a Cluster
Update-AzVMwareDatastore	Update a Datastore
Update-AzVMwareGlobalReachConnection	Update a GlobalReachConnection
Update-AzVMwareIscsiPath	Update a IscsiPath
Update-AzVMwarePlacementPolicy	Update a PlacementPolicy
Update-AzVMwarePrivateCloud	Update a PrivateCloud

Microsoft.AVS privateClouds

Article • 04/10/2023

Bicep resource definition

The privateClouds resource type can be deployed with operations that target:

- **Resource groups** - See resource group deployment commands

For a list of changed properties in each API version, see change log.

Resource format

To create a Microsoft.AVS/privateClouds resource, add the following Bicep to your template.

Bicep

```
resource symbolicname 'Microsoft.AVS/privateClouds@2022-05-01' = {
  name: 'string'
  location: 'string'
  tags: {
    tagName1: 'tagValue1'
    tagName2: 'tagValue2'
  }
  sku: {
    name: 'string'
  }
  identity: {
    type: 'string'
  }
  properties: {
    availability: {
      secondaryZone: int
      strategy: 'string'
      zone: int
    }
    circuit: {}
    encryption: {
      keyVaultProperties: {
        keyName: 'string'
        keyVaultUrl: 'string'
        keyVersion: 'string'
      }
      status: 'string'
    }
    identitySources: [
```

```
      {
        alias: 'string'
        baseGroupDN: 'string'
        baseUserDN: 'string'
        domain: 'string'
        name: 'string'
        password: 'string'
        primaryServer: 'string'
        secondaryServer: 'string'
        ssl: 'string'
        username: 'string'
      }
    ]
    internet: 'string'
    managementCluster: {
      clusterSize: int
      hosts: [
        'string'
      ]
    }
    networkBlock: 'string'
    nsxtPassword: 'string'
    secondaryCircuit: {}
    vcenterPassword: 'string'
  }
}
```

Property values

privateClouds

Name	Description	Value
name	The resource name	string (required)
location	Resource location	string
tags	Resource tags	Dictionary of tag names and values. See Tags in templates
sku	The private cloud SKU	Sku (required)
identity	The identity of the private cloud, if configured.	PrivateCloudIdentity
properties	The properties of a private cloud resource	PrivateCloudProperties

PrivateCloudIdentity

Name	Description	Value
type	The type of identity used for the private cloud. The type 'SystemAssigned' refers to an implicitly created identity. The type 'None' will remove any identities from the Private Cloud.	'None' 'SystemAssigned'

PrivateCloudProperties

Name	Description	Value
availability	Properties describing how the cloud is distributed across availability zones	AvailabilityProperties
circuit	An ExpressRoute Circuit	Circuit
encryption	Customer managed key encryption, can be enabled or disabled	Encryption
identitySources	vCenter Single Sign On Identity Sources	IdentitySource[]
internet	Connectivity to internet is enabled or disabled	'Disabled' 'Enabled'
managementCluster	The default cluster used for management	ManagementCluster
networkBlock	The block of addresses should be unique across VNet in your subscription as well as on-premise. Make sure the CIDR format is conformed to (A.B.C.D/X) where A,B,C,D are between 0 and 255, and X is between 0 and 22	string (required)
nsxtPassword	Optionally, set the NSX-T Manager password when the private cloud is created	string
secondaryCircuit	A secondary expressRoute circuit from a separate AZ. Only present in a stretched private cloud	Circuit
vcenterPassword	Optionally, set the vCenter admin password when the private cloud is created	string

AvailabilityProperties

Name	Description	Value
secondaryZone	The secondary availability zone for the private cloud	int

Name	Description	Value
strategy	The availability strategy for the private cloud	'DualZone' 'SingleZone'
zone	The primary availability zone for the private cloud	int

Circuit

This object doesn't contain any properties to set during deployment. All properties are ReadOnly.

Encryption

Name	Description	Value
keyVaultProperties	The key vault where the encryption key is stored	EncryptionKeyVaultProperties
status	Status of customer managed encryption key	'Disabled' 'Enabled'

EncryptionKeyVaultProperties

Name	Description	Value
keyName	The name of the key.	string
keyVaultUrl	The URL of the vault.	string
keyVersion	The version of the key.	string

IdentitySource

Name	Description	Value
alias	The domain's NetBIOS name	string
baseGroupDN	The base distinguished name for groups	string
baseUserDN	The base distinguished name for users	string
domain	The domain's dns name	string
name	The name of the identity source	string

Name	Description	Value
password	The password of the Active Directory user with a minimum of read-only access to Base DN for users and groups.	string
primaryServer	Primary server URL	string
secondaryServer	Secondary server URL	string
ssl	Protect LDAP communication using SSL certificate (LDAPS)	'Disabled' 'Enabled'
username	The ID of an Active Directory user with a minimum of read-only access to Base DN for users and group	string

ManagementCluster

Name	Description	Value
clusterSize	The cluster size	int
hosts	The hosts	string[]

Sku

Name	Description	Value
name	The name of the SKU.	string (required)

Configure VMware Cloud Director Service in Azure VMware Solution

Article • 04/15/2024

In this article, learn how to configure VMware Cloud Director service in Azure VMware Solution.

Prerequisites

- Plan and deploy a VMware Cloud Director Service Instance in your preferred region using the process described here. How Do I Create a VMware Cloud Director Instance

  > **Note**
  >
  > VMware Cloud Director Instances can establish connections to Azure VMware Solution private clouds in regions where the round-trip time (RTT) latency remains under 150 ms.

- Plan and deploy Azure VMware Solution private cloud using the following links:
  - Plan Azure VMware Solution private cloud.
  - Deploy and configure Azure VMware Solution - Azure VMware Solution.
- After successfully gaining access to both your VMware Cloud Director instance and Azure VMware Solution private cloud, you can then proceed to the next section.

Plan and prepare Azure VMware Solution private cloud for VMware Reverse proxy

- VMware Reverse proxy VM is deployed within the Azure VMware Solution private cloud and requires outbound connectivity to your VMware Cloud director Service Instance. Plan how you would provide this internet connectivity.
- Public IP on NSX Edge can be used to provide outbound access for the VMware Reverse proxy VM as shown in this article. Learn more on, How to configure a public IP in the Azure portal and Outbound Internet access for VMs
- VMware Reverse proxy can acquire an IP address through either DHCP or manual IP configuration.

- Optionally create a dedicated Tier-1 router for the reverse proxy VM segment.

Prepare your Azure VMware Solution private cloud for deploying VMware Reverse proxy VM OVA

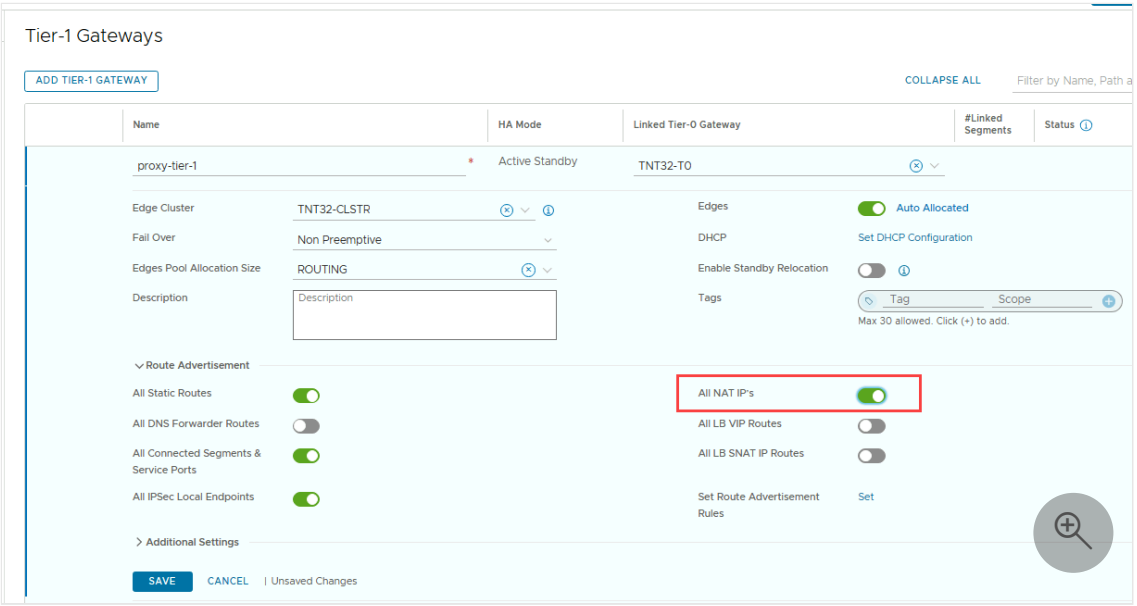
1. Obtain NSX cloud admin credentials from Azure portal under VMware credentials. Then, sign in to NSX Manager.

2. Create a dedicated Tier-1 router (optional) for VMware Reverse proxy VM.

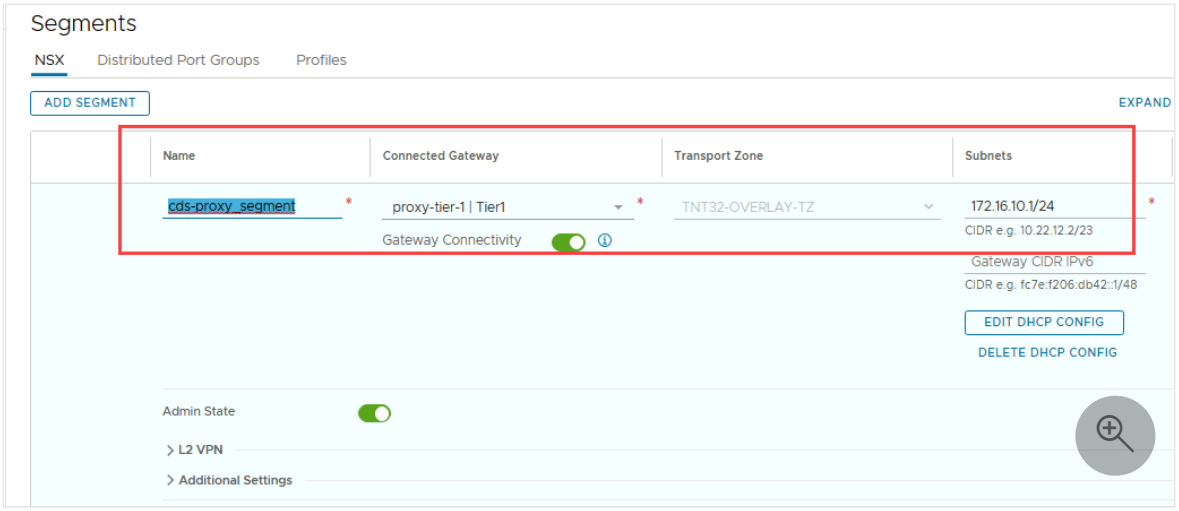
   a. Sign in to Azure VMware Solution NSX Manager and select **ADD Tier-1 Gateway**

   b. Provide name, Linked Tier-0 gateway and then select save.

   c. Configure appropriate settings under Route Advertisements.



3. Create a segment for VMware Reverse proxy VM.
   a. Sign in to Azure VMware Solution NSX Manager and under segments, select **ADD SEGMENT**
   b. Provide name, Connected Gateway, Transport Zone and Subnet information and then select save.



4. Optionally enable segment for DHCP by creating a DHCP profile and setting DHCP config. You can skip this step if you use static IPs.

5. Add two NAT rules to provide an outbound access to VMware Reverse proxy VM to reach VMware cloud director service. You can also reach the management components of Azure VMware Solution private cloud such as vCenter Server and NSX that are deployed in the management plane.

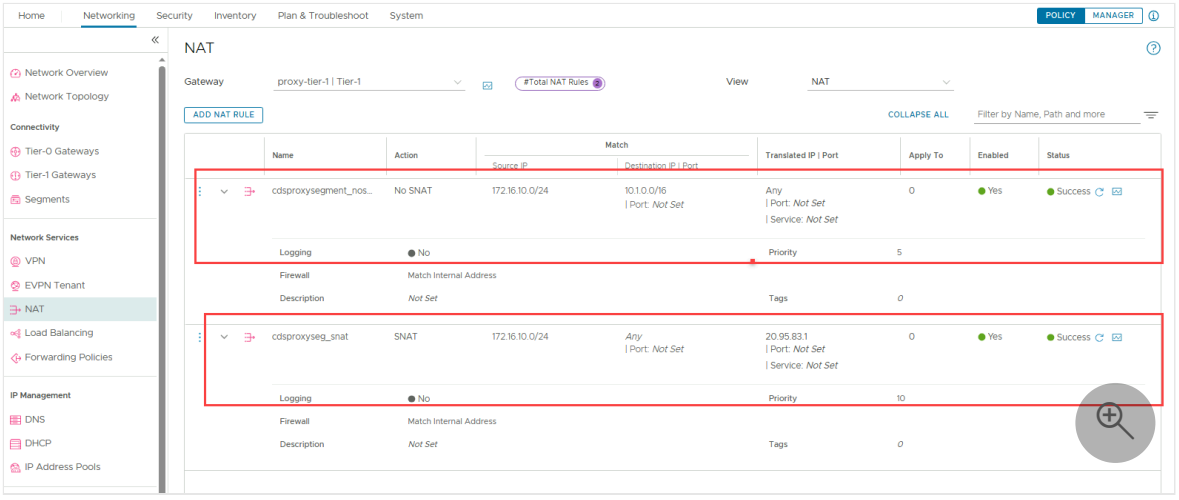
   a. Create **NOSNAT** rule,

   - Provide name of the rule and select source IP. You can use CIDR format or specific IP address.
   - Under destination port, use private cloud network CIDR.

   b. Create **SNAT** rule

   - Provide name and select source IP.
   - Under translated IP, provide a public IP address.
   - Set priority of this rule higher as compared to the NOSNAT rule.

   c. Select **Save**.



6. Ensure on Tier-1 gateway, NAT is enabled under router advertisement.

7. Configure gateway firewall rules to enhance security.

Generate and Download VMware Reverse proxy OVA

- What follows is a step-by-step procedure and how to obtain the required information on Azure portal and how to use it to generate VMware Reverse proxy VM.

Prerequisites on VMware cloud service

- Verify you're assigned the network administrator service role. See Managing Roles and Permissions and make changes using VMware Cloud Services Console.
- If you're accessing VMware Cloud Director service through VMware Cloud Partner Navigator, verify that you're a Provider Service Manager user and that you're assigned the provider:**admin** and provider:**network service** roles.
- See How do I change the roles of users in my organization in the VMware Cloud Partner Navigator documentation.

Procedure

1. Sign in to VMware Cloud Director service.

2. Select Cloud Director Instances.

3. In the card of the VMware Cloud Director instance for which you want to configure a reverse proxy service, select **Actions** > **Generate VMware Reverse Proxy OVA**.

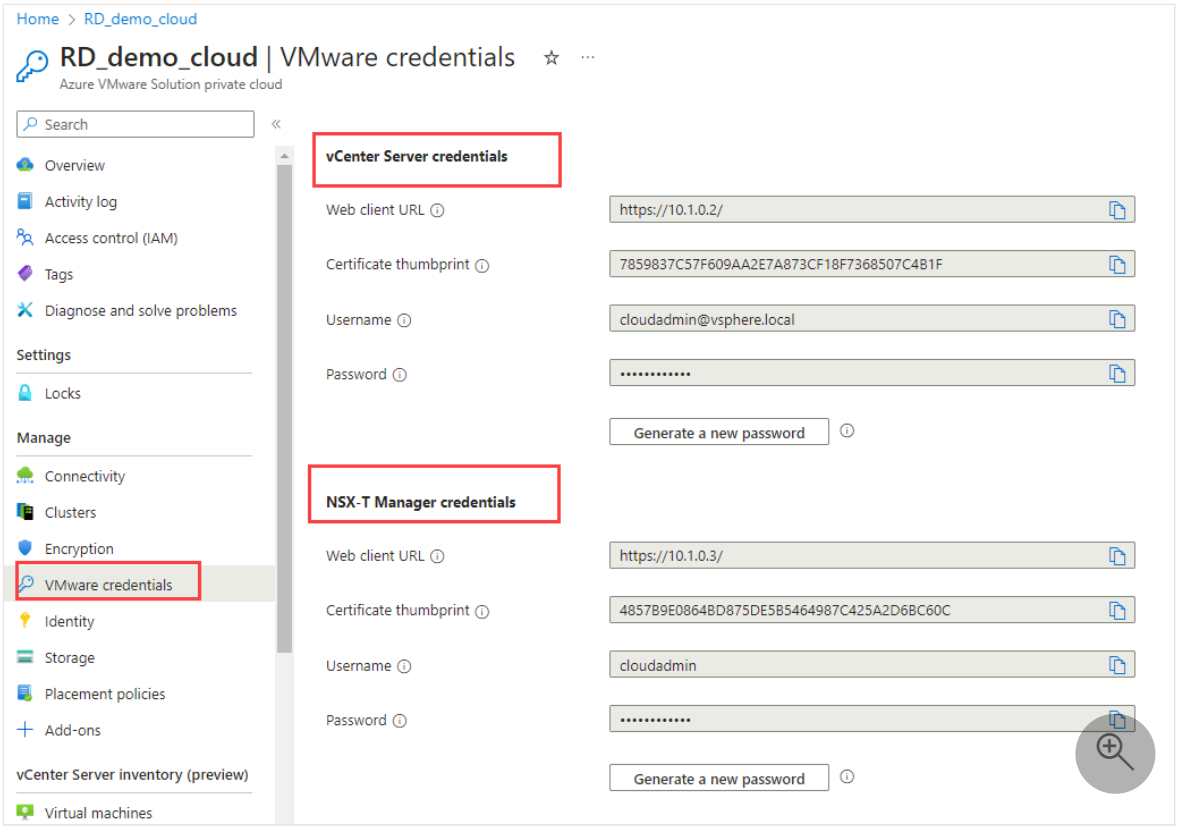
4. The **Generate VMware Reverse proxy OVA** wizard opens. Fill in the required information.

5. Enter Network Name

    - Network name is the name of the NSX segment you created in previous section for reverse proxy VM.

6. Enter the required information such as vCenter FQDN, Management IP for vCenter, NSX FQDN or IP and more hosts within the private cloud to proxy.

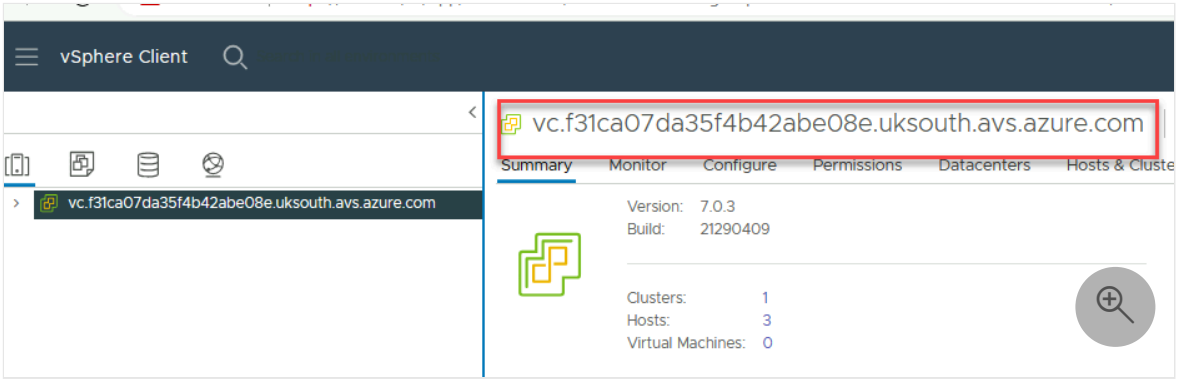
7. vCenter and NSX IP address of your Azure VMware Solution private cloud can be found under **Azure portal** -> **manage**-> **VMware credentials**



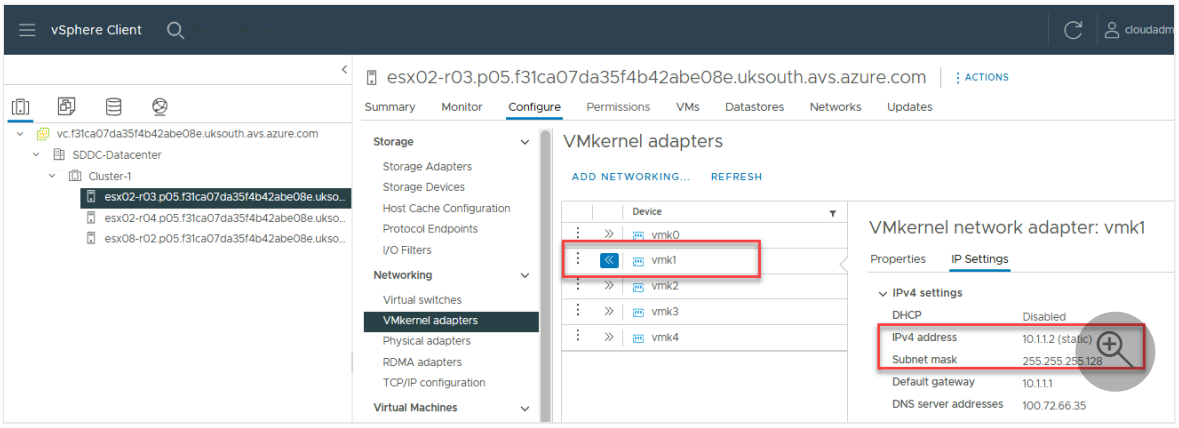
8. To find FQDN of vCenter of your Azure VMware Solution private cloud, sign in to the vCenter using VMware credential provided on Azure portal.

9. In vSphere Client, select vCenter, which displays FQDN of the vCenter Server.

10. To obtain FQDN of NSX, replace vc with nsx. NSX FQDN in this example would be, “nsx.f31ca07da35f4b42abe08e.uksouth.avs.azure.com”



11. Obtain ESXi management IP addresses and CIDR for adding IP addresses in allowlist when generating reverse proxy VM OVA.

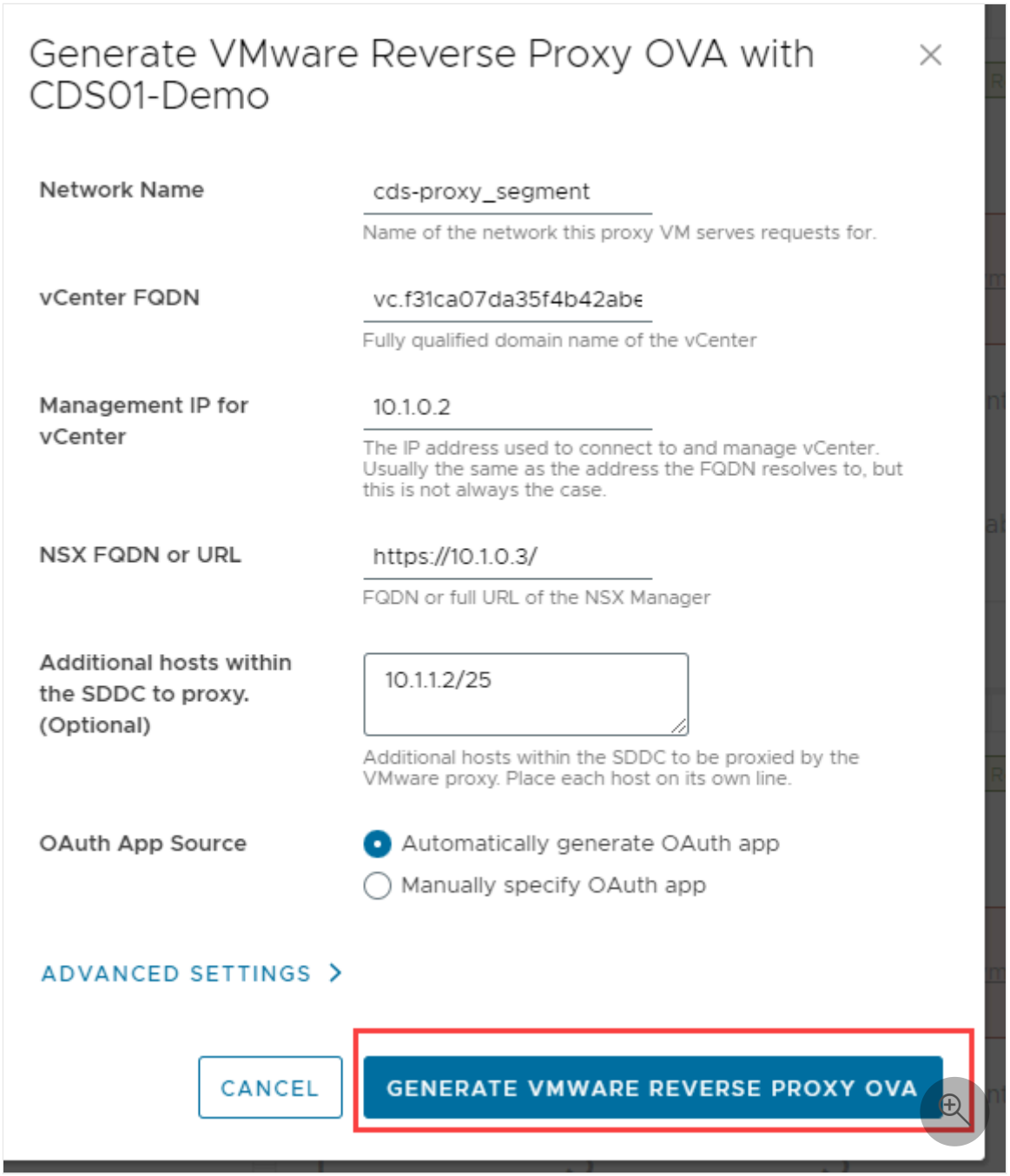


12. Enter a list of any other IP addresses that VMware Cloud Director must be able to access through the proxy, such as ESXi hosts to use for console proxy connection. Use new lines to separate list entries.

> **Tip**
>
> To ensure that future additions of ESXi hosts don't require updates to the allowed targets, use a CIDR notation to enter the ESXi hosts in the allow list. This way, you can provide any new host with an IP address that is already allocated as part of the CIDR block.

13. Once you gathered all the required information, add the information in the VMware Reverse proxy OVA generation wizard in the following diagram.

14. Select **Generate VMware Reverse Proxy OVA**.



15. On the **Activity log** tab, locate the task for generating an OVA and check its status. If the status of the task is **Success**, select the vertical ellipsis icon and select **View files**.

16. Download the reverse proxy OVA.

Deploy VMware Reverse proxy VM

1. Transfer reverse proxy VM OVA you generated in the previous section to a location from where you can access your private cloud.
2. Deploy reverse proxy VM using OVA.
3. Select appropriate parameters for OVA deployment for folder, computer resources, and storage.

- For network, select appropriate segment for reverse proxy.
- Under customize template, use DHCP or provide static IP if you aren't planning to use DHCP.
- Enable SSH to sign in to reverse proxy VM.
- Provide root password.

4. Once VM is deployed, power it on and then sign in using the root credentials provided during OVA deployment.
5. Sign in to the VMware Reverse proxy VM and use the command **transporter-status.sh** to verify that the connection between CDs instance and Transporter VM is established.

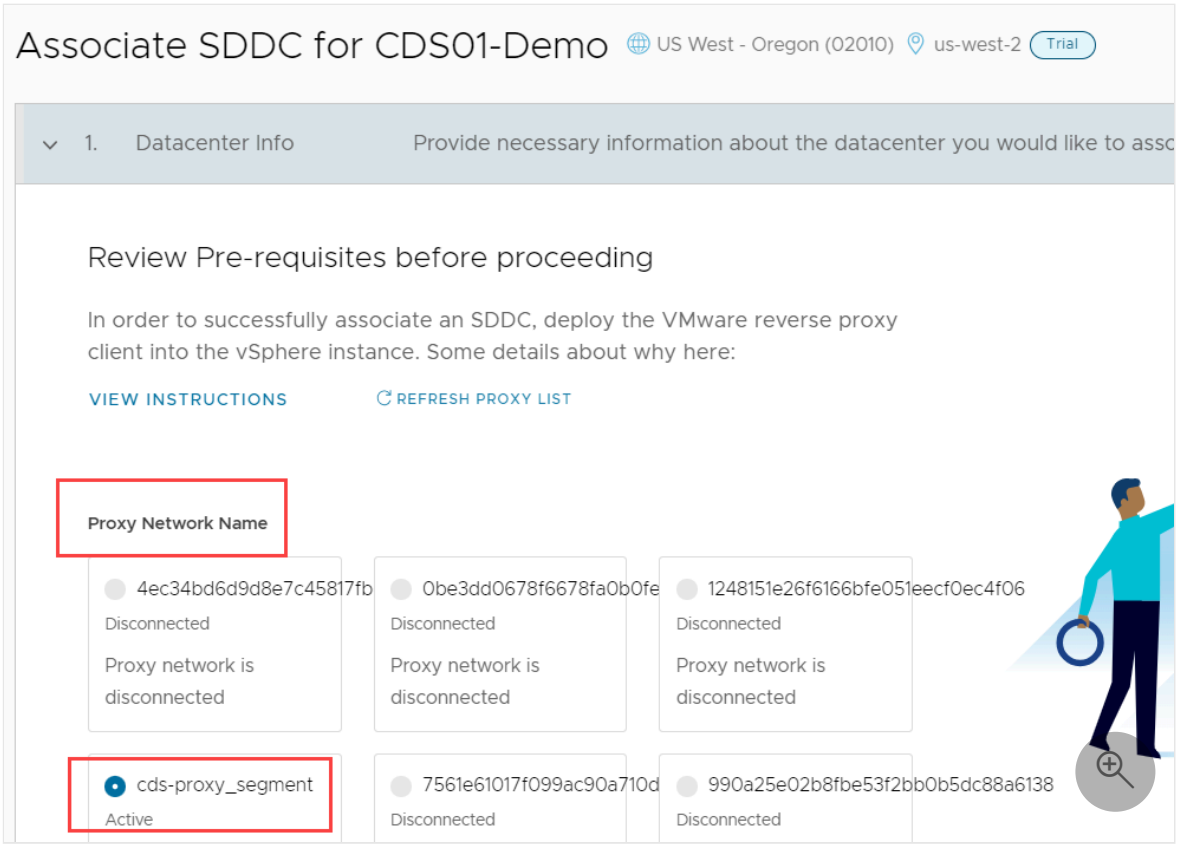
    - The status should indicate "UP." The command channel should display "Connected," and the allowed targets should be listed as "reachable."

6. Next step is to associate Azure VMware Solution private cloud with the VMware Cloud Director Instance.

Associate Azure VMware Solution private cloud with VMware Cloud Director Instance via VMware Reverse proxy

This process pools all the resources from Azure private Solution private cloud and creates a provider virtual datacenter (PVDC) in CDs.

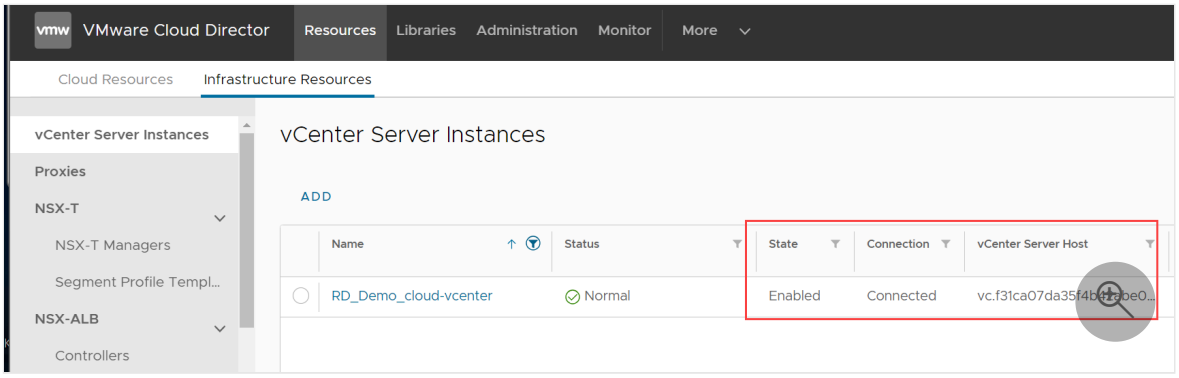
1. Sign in to VMware Cloud Director service.
2. Select **Cloud Director Instances**.
3. In the card of the VMware Cloud Director instance for which you want to associate your Azure VMware Solution private cloud, select **Actions** and then select **Associate datacenter via VMware reverse proxy**.
4. Review datacenter information.
5. Select a proxy network for the reverse proxy appliance to use. Ensure correct NSX segment is selected where reverse proxy VM is deployed.



6. In the **Data center name** text box, enter a name for the private cloud that you want to associate with datacenter. The name entered is only used to identify the data center in the VMware Cloud Director inventory, so it doesn't need to match the private cloud name entered when you generated the reverse proxy appliance OVA.
7. Enter the FQDN for your vCenter Server instance.
8. Enter the URL for the NSX Manager instance and wait for a connection to establish.
9. Select **Next**.
10. Under **Credentials**, enter your user name and password for the vCenter Server endpoint.
11. Enter your user name and password for NSX Manager.
12. To create infrastructure resources for your VMware Cloud Director instance, such as a network pool, an external network and a provider VDC, select **Create Infrastructure**.
13. Select **Validate Credentials**. Ensure that validation is successful.
14. Confirm that you acknowledge the costs associated with your instance, and select Submit.
15. Check activity log to note the progress.

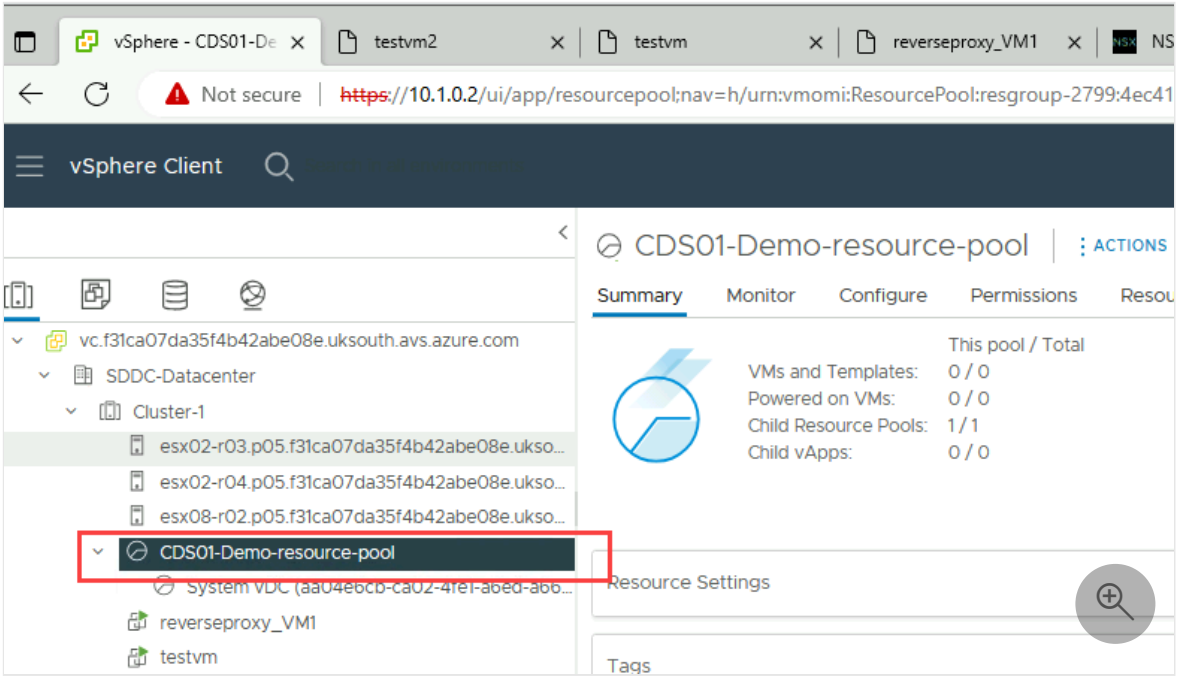
16. Once this process is completed, you should see that your VMware Azure Solution private cloud is securely associated with your VMware Cloud Director instance.

17. When you open the VMware Cloud Director instance, the vCenter Server and the NSX Manager instances that you associated are visible in Infrastructure Resources.



18. A newly created Provider VDC is visible in Cloud Resources.

19. In your Azure VMware solution private cloud, when logged into vCenter Server you see that a Resource Pool is created as a result of this association.



You can use your VMware cloud director instance provider portal to configure tenants such as organizations and virtual data center.

What's next

- Configure tenant networking on VMware Cloud director service on Azure VMware solution using link Enable VMware Cloud Director service with Azure VMware Solution.

- Learn more about VMware cloud director service using VMware Cloud Director Service Documentation
- To learn about Cloud director Service provider admin portal, Visit VMware Cloud Director™ Service Provider Admin Portal Guide .

Self service maintenance orchestration (public preview)

Article • 10/01/2024

In this article, you learn about one of the advantages of Azure VMware Solution private cloud. The advantage is the managed platform where Microsoft handles the lifecycle management of VMware software (ESXi, vCenter Server, and vSAN) and NSX appliances. Microsoft also takes care of applying any patches, updates, or upgrades to ESXi, vCenter Server, vSAN, and NSX within your private cloud. Regular upgrades of the Azure VMware Solution private cloud and VMware software ensure the latest security, stability, and feature sets are running in your private cloud. For more information, see Host maintenance and lifecycle management.

Microsoft schedules maintenance and notifies customers through Service Health notifications. The details of the planned maintenance are available under the planned maintenance section. Currently, customers must raise a support ticket if they wish to change a scheduled maintenance window. The Self-Service Maintenance orchestration feature provides customers with the flexibility to reschedule their planned maintenance directly from the Azure portal.

Prerequisites

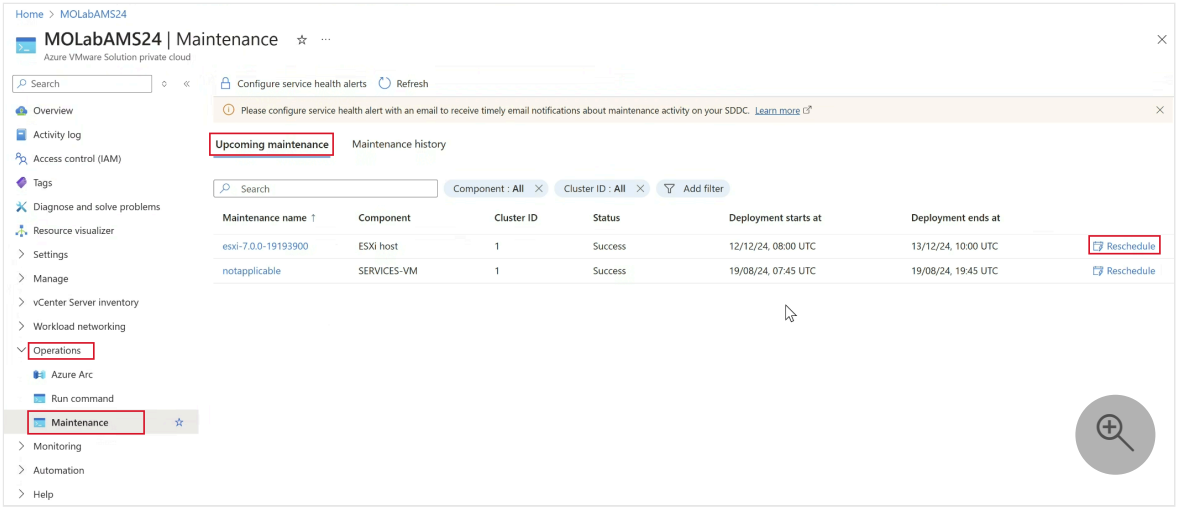
- An existing Azure VMware Solution private cloud.
- A registered subscription to the Microsoft Azure VMware Solution AFEC flags named Early Access and Self Serve for Maintenance. You can find these flags under **Preview Features** on the Azure portal.

Reschedule maintenance through Azure VMware Solution maintenance

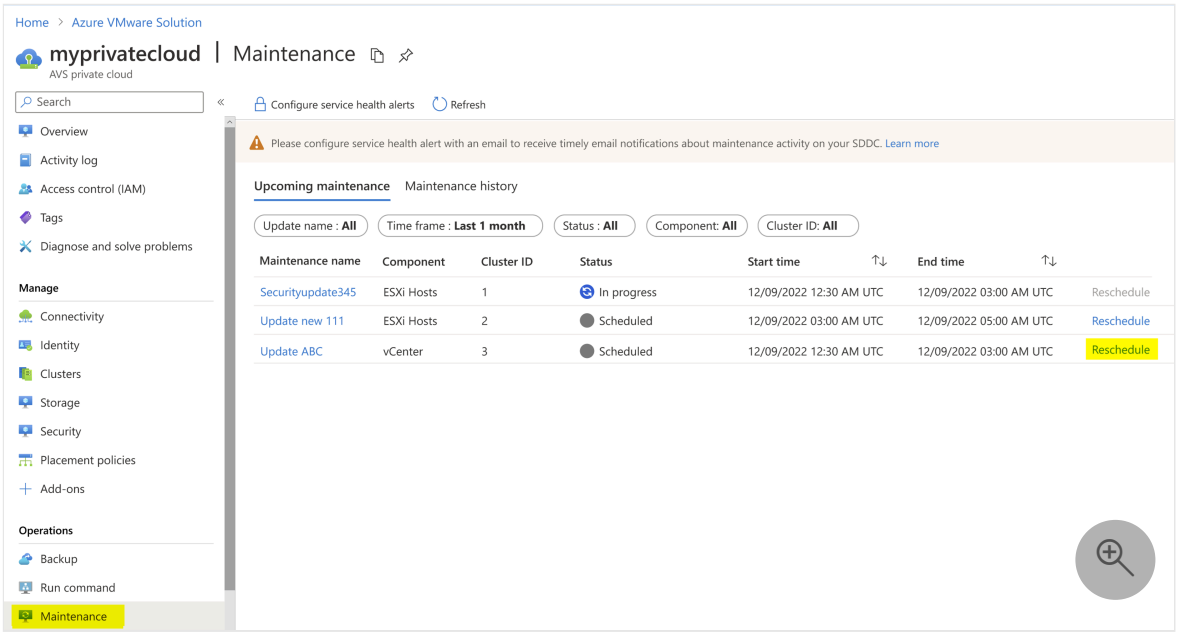
1. Sign in to your Azure VMware Solution private cloud.

> **Note**
>
> At least a contributor level access on the Azure VMware Solution private cloud is required.

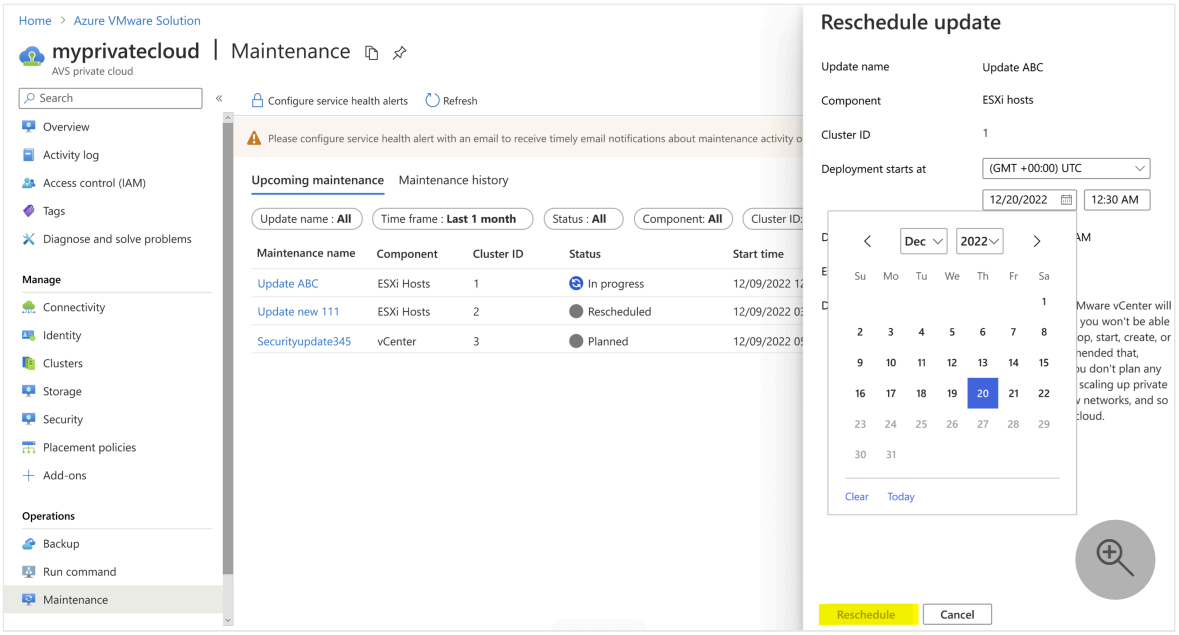
2. From the left navigation, locate **Operations** and select **Maintenance** from the drop-down list.



3. Under the **Upcoming maintenance** tab, select the **Reschedule** option located on the right side.



4. Input the revised date and time, then select **Reschedule**.



After you've selected **Reschedule**, the system modifies the schedule to the new date and the new schedule is displayed to the portal.

Additional Information

The following system error or warning messages appear while trying to reschedule maintenance tasks:

- Users aren't allowed to reschedule maintenance after the upgrade deadline and on freeze days.
- Users will be allowed to reschedule up to 1 hour before and after the start of the maintenance.
- Each maintenance task is assigned an internal deadline. Dates that exceed this deadline appear greyed out on the portal. If a customer needs to reschedule maintenance beyond this point, they should raise a support ticket.
- Maintenance that is critical or carries fix for a critical security vulnerability, might have the reschedule option greyed out.
- This feature is only enabled for a selected set of maintenance, therefore not all the Azure VMware Solution maintenance shows up in this navigation or have the reschedule option.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Enable VMware Cloud Director service with Azure VMware Solution

Article • 04/16/2024

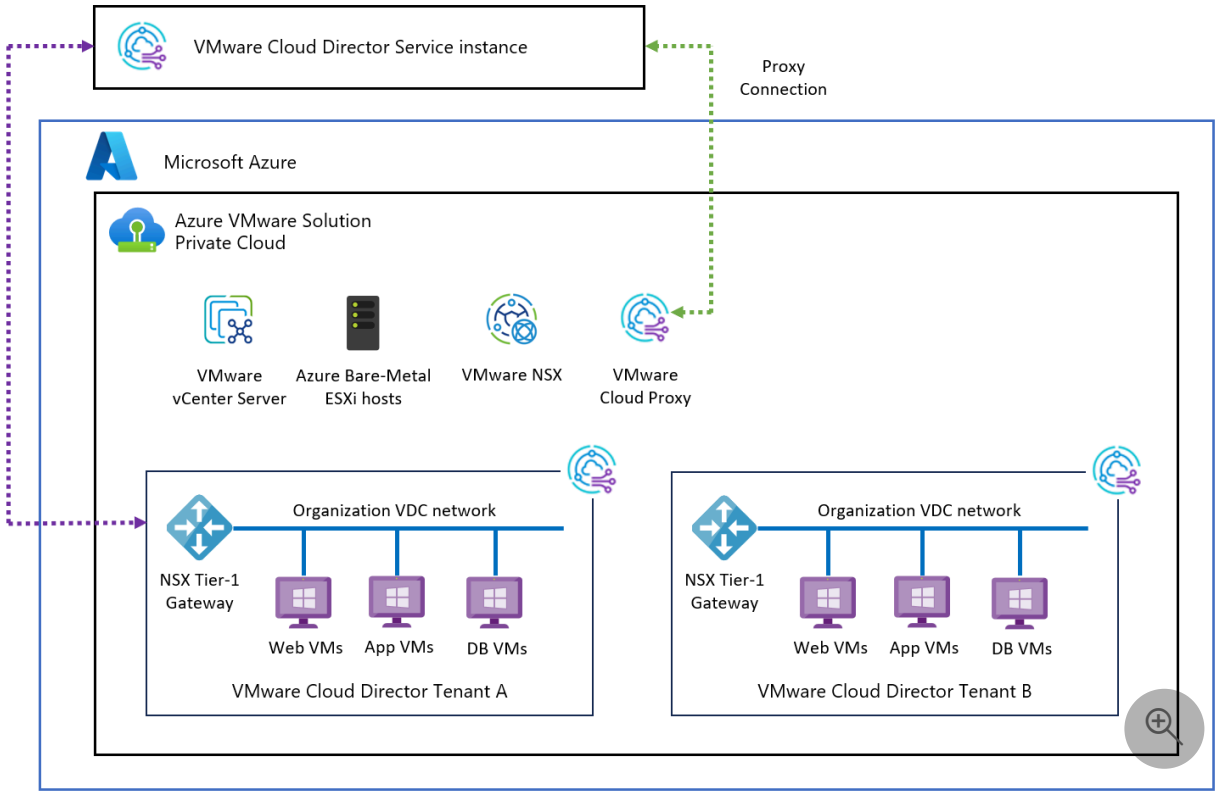
VMware Cloud Director service (CDs) with Azure VMware Solution enables enterprise customers to use APIs or the Cloud Director services portal to self-service, provision, and manage virtual datacenters through multi-tenancy with reduced time and complexity.

In this article, learn how to enable VMware Cloud Director service with Azure VMware Solution for enterprise customers to use Azure VMware Solution resources and Azure VMware Solution private clouds with underlying resources for virtual datacenters.

> **Important**
>
> VMware Cloud Director service is now available to use with Azure VMware Solution under the Enterprise Agreement (EA) model only. It's not suitable for MSP / Hosters to resell Azure VMware Solution capacity to customers at this point. For more information, see **Azure Service terms**.

Reference architecture

The following diagram shows typical architecture for Cloud Director services with Azure VMware Solution and how they're connected. An SSL reverse proxy supports communication to Azure VMware Solution endpoints from Cloud Director service.

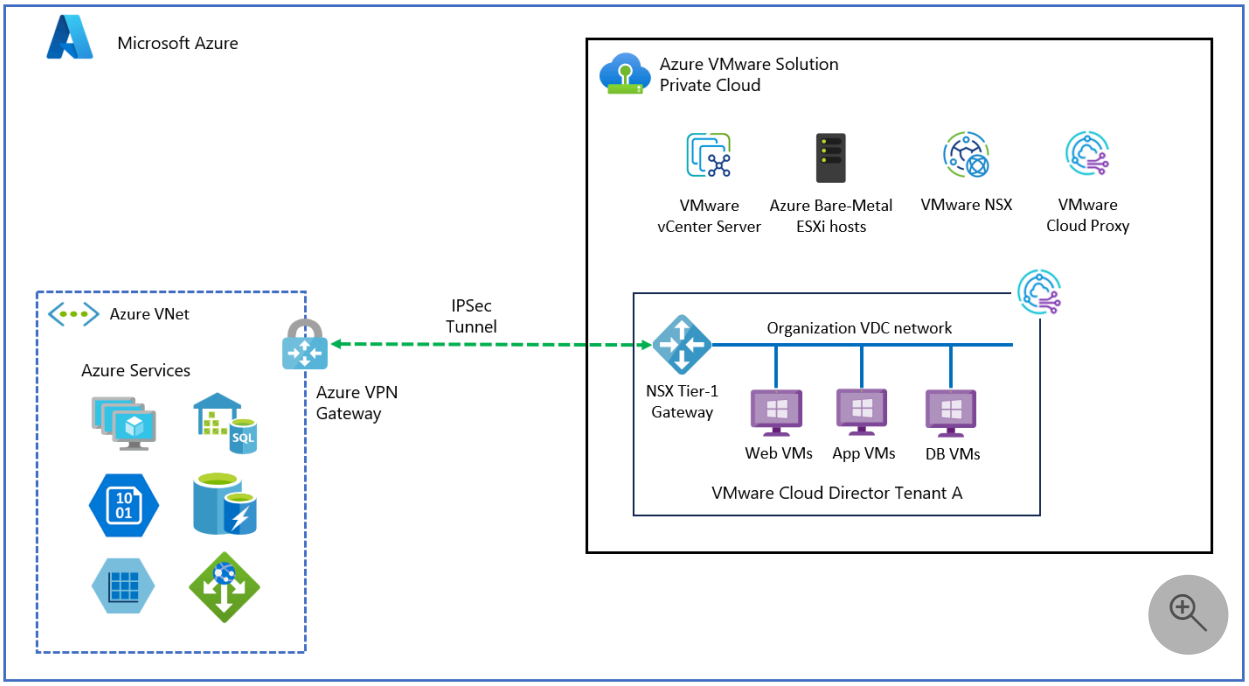


VMware Cloud Director supports multi-tenancy by using organizations. A single organization can have multiple organization virtual data centers (VDC). Each Organization's VDC can have their own dedicated Tier-1 router (Edge Gateway) which is further connected with the provider managed shared Tier-0 router.

Learn more about CDs on Azure VMware Solutions reference architecture

Connect tenants and their organization virtual datacenters to Azure VNet based resources

To provide access to VNet based Azure resources, each tenant can have their own dedicated Azure VNet with Azure VPN gateway. A site-to-site VPN between customer organization VDC and Azure VNet is established. To achieve this connectivity, the tenant provides public IP to the organization VDC. The organization VDC administrator can configure IPSEC VPN connectivity from the Cloud Director service portal.



As shown in the previous diagram, organization 01 has two organization virtual datacenters: VDC1 and VDC2. The virtual datacenter of each organization has its own Azure VNets connected with their respective organization VDC Edge gateway through IPSEC VPN. Providers provide public IP addresses to the organization VDC Edge gateway for IPSEC VPN configuration. An ORG VDC Edge gateway firewall blocks all traffic by default, specific allow rules needs to be added on organization Edge gateway firewall.

Organization VDCs can be part of a single organization and still provide isolation between them. For example, VM1 hosted in organization VDC1 can't ping Azure VM JSVM2 for tenant2.

Prerequisites

- Organization VDC is configured with an Edge gateway and has Public IPs assigned to it to establish IPSEC VPN by provider.
- Tenants created a routed Organization VDC network in tenant's virtual datacenter.
- Test VM1 and VM2 are created in the Organization VDC1 and VDC2 respectively. Both VMs are connected to the routed orgVDC network in their respective VDCs.
- Have a dedicated Azure VNet configured for each tenant. For this example, we created Tenant1-VNet and Tenant2-VNet for tenant1 and tenant2 respectively.
- Create an Azure Virtual network gateway for VNETs created earlier.
- Deploy Azure VMs JSVM1 and JSVM2 for tenant1 and tenant2 for test purposes.

> **Note**
>
> VMware Cloud Director service supports a policy-based VPN. Azure VPN gateway configures route-based VPN by default and to configure policy-based VPN policy-

based selector needs to be enabled.

Configure Azure VNet

Create the following components in tenant's dedicated Azure VNet to establish IPSEC tunnel connection with the tenant's ORG VDC Edge gateway.

- Azure Virtual network gateway
- Local network gateway.
- Add IPSEC connection on VPN gateway.
- Edit connection configuration to enable policy-based VPN.

Create Azure virtual network gateway

To create an Azure virtual network gateway, see the create-a-virtual-network-gateway tutorial.

Create local network gateway

1. Sign in to the Azure portal and select **Local network gateway** from marketplace and then select **Create**.
2. Local Network Gateway represents remote end site details. Therefore provide tenant1 OrgVDC public IP address and orgVDC Network details to create local end point for tenant1.
3. Under **Instance details**, select **Endpoint** as IP address
4. Add IP address (add Public IP address from tenant's OrgVDC Edge gateway).
5. Under **Address space** add **Tenants Org VDC Network**.
6. Repeat steps 1-5 to create a local network gateway for tenant 2.

Create IPSEC connection on VPN gateway

1. Select tenant1 VPN Gateway (created earlier) and then select **Connection** (in left pane) to add new IPSEC connection with tenant1 orgVDC Edge gateway.

2. Enter the following details.

Expand table

Name	Connection
Connection Type	Site to Site

Name	Connection
VPN Gateway	Tenant's VPN Gateway
Local Network Gateway	Tenant's Local Gateway
PSK	Shared Key (provide a password)
IKE Protocol	IKEV2 (ORG-VDC is using IKEv2)

3. Select **Ok** to deploy local network gateway.

Configure IPsec Connection

VMware Cloud Director service supports a policy-based VPN. Azure VPN gateway configures route-based VPN by default and to configure policy-based VPN policy-based selector needs to be enabled.

1. Select the connection you created earlier and then select **configuration** to view the default settings.
2. **IPSEC/IKE Policy**
3. **Enable policy base traffic selector**
4. Modify all other parameters to match what you have in OrgVDC.

> ⓘ **Note**
>
> Both source and destination of the tunnel should have identical settings for IKE,SA, DPD etc.

5. Select **Save**.

Configure VPN on organization VDC Edge router

1. Sign in to Organization VMware Cloud Director service tenant portal and select the tenants Edge gateway.

2. Select **IPSEC VPN** option under **Services** and then select **New**.

3. Under general setting, provide **Name** and select desired security profile. Ensure that security profile settings (IKE, Tunnel, and DPD configuration) are same on both sides of the IPsec tunnel.

4. Modify Azure VPN gateway to match the Security profile, if necessary. You can also do security profile customization from CDS tenant portal.

> ⓘ **Note**
>
> VPN tunnel won't establish if these settings were mismatched.

5. Under **Peer Authentication Mode**, provide the same preshared key that is used at the Azure VPN gateway.
6. Under **Endpoint configuration**, add the Organization's public IP and network details in local endpoint and Azure VNet details in remote endpoint configuration.
7. Under **Ready to complete**, review applied configuration.
8. Select **Finish** to apply configuration.

Apply firewall configuration

Organization VDC Edge router firewall denies traffic by default. You need to apply specific rules to enable connectivity. Use the following steps to apply firewall rules.

1. Add IP set in VMware Cloud Director service portal
   a. Sign in to Edge router then select **IP SETS** under the **Security** tab in left plane.
   b. Select **New** to create IP sets.
   c. Enter **Name** and **IP address** of test VM deployed in orgVDC.
   d. Create another IP set for Azure VNet for this tenant.
2. Apply firewall rules on ORG VDC Edge router.
   a. Under **Edge gateway**, select **Edge gateway** and then select **firewall** under **services**.
   b. Select **Edit rules**.
   c. Select **NEW ON TOP** and enter rule name.
   d. Add **source** and **destination** details. Use created IPSET in source and destination.
   e. Under **Action**, select **Allow**.
   f. Select **Save** to apply configuration.
3. Verify tunnel status
   a. Under **Edge gateway** select **Service**, then select **IPSEC VPN**,
   b. Select **View statistics**.
   Status of tunnel should show **UP**.
4. Verify IPsec connection
   a. Sign in to Azure VM deployed in tenants VNet and ping tenant's test VM IP address in tenant's OrgVDC.
   For example, ping VM1 from JSVM1. Similarly, you should be able to ping VM2

from JSVM2. You can verify isolation between tenants Azure VNets. Tenant 1 VM1 can't ping Tenant 2 Azure VM JSVM2 in tenant 2 Azure VNets.

Connect Tenant workload to public Internet

- Tenants can use public IP to do SNAT configuration to enable Internet access for VM hosted in organization VDC. To achieve this connectivity, the provider can provide public IP to the organization VDC.
- Each organization VDC can be created with dedicated T1 router (created by provider) with reserved Public & Private IP for NAT configuration. Tenants can use public IP SNAT configuration to enable Internet access for VM hosted in organization VDC.
- OrgVDC administrator can create a routed OrgVDC network connected to their OrgVDC Edge gateway. To provide Internet access.
- OrgVDC administrator can configure SNAT to provide a specific VM or use network CIDR to provide public connectivity.
- OrgVDC Edge has default DENY ALL firewall rule. Organization administrators need to open appropriate ports to allow access through the firewall by adding a new firewall rule. Virtual machines configured on such OrgVDC network used in SNAT configuration should be able to access the Internet.

Prerequisites

1. Public IP is assigned to the organization VDC Edge router. To verify, sign in to the organization's VDC. Under **Networking**> **Edges**, select **Edge Gateway**, then select **IP allocations** under **IP management**. You should see a range of assigned IP address there.
2. Create a routed Organization VDC network. (Connect OrgvDC network to the Edge gateway with public IP address assigned)

Apply SNAT configuration

1. Sign in to Organization VDC. Navigate to your Edge gateway and then select **NAT** under **Services**.
2. Select **New** to add new SNAT rule.
3. Provide **Name** and select **Interface type** as SNAT.
4. Under **External IP**, enter public IP address from public IP pool assigned to your orgVDC Edge router.
5. Under **Internal IP**, enter IP address for your test VM. This IP address is one of the orgVDC network IP assigned to the VM.

6. **State** should be enabled.
7. Under **Priority**, select a higher number. For example, 4096.
8. Select **Save** to save the configuration.

Apply firewall rule

1. Sign in to Organization VDC and navigate to **Edge Gateway**, then select **IP set** under security.
2. Create an IPset. Provide IP address of your VM (you can use CIDR also). Select **Save**.
3. Under **services**, select **Firewall**, then select **Edit rules**.
4. Select **New ON TOP** and create a firewall rule to allow desired port and destination.
5. Select the **IPset** your created earlier as source. Under **Action**, select **Allow**.
6. Select **Keep** to save the configuration.
7. Sign in to your test VM and ping your destination address to verify outbound connectivity.

Migrate workloads to VMware Cloud Director service on Azure VMware Solution

VMware Cloud Director Availability can be used to migrate VMware Cloud Director workload into the VMware Cloud Director service on Azure VMware Solution. Enterprise customers can drive self-serve one-way warm migration from the on-premises Cloud Director Availability vSphere plugin, or they can run the Cloud Director Availability plugin from the provider-managed Cloud Director instance and move workloads into Azure VMware Solution.

For more information about VMware Cloud Director Availability, see VMware Cloud Director Availability | Disaster Recovery & Migration

FAQs

What are the supported Azure regions for the VMware Cloud Director service?

This offering is supported in all Azure regions where Azure VMware Solution is available except for Brazil South and South Africa. Ensure that the region you wish to connect to

VMware Cloud Director service is within a 150-milliseconds round trip time for latency with VMware Cloud Director service.

How do I configure VMware Cloud Director service on Microsoft Azure VMware Solutions?

Learn about how to configure CDs on Azure VMware Solutions

How is VMware Cloud Director service supported?

VMware Cloud Director service (CDs) is VMware owned and supported product connected to Azure VMware solution. For any support queries on CDs, contact VMware support for assistance. Both VMware and Microsoft support teams collaborate as necessary to address and resolve Cloud Director Service issues within Azure VMware Solution.

Next steps

VMware Cloud Director Service Documentation
Migration to Azure VMware Solutions with Cloud Director service

Deploy VMware Cloud Director Availability in Azure VMware Solution

Article • 04/15/2024

In this article, learn how to deploy VMware Cloud Director Availability in Azure VMware Solution.

Customers can use VMware Cloud Director Availability, a Disaster Recovery as a Service (DRaaS) solution, to protect and migrate workloads both to and from the VMware Cloud Director service associated with Azure VMware Solution. The native integration of VMware Cloud Director Availability with VMware Cloud Director and VMware Cloud Director service (CDS) enables provider and their tenants to efficiently manage migration and disaster recovery for workloads through the VMware Cloud Director Availability provider and tenant portal.

VMware Cloud Director Availability scenarios on Azure VMware Solution

You can use VMware Cloud Director Availability with Azure VMware Solution for the following two scenarios:

- On-Premises to Azure VMware Solution

  VMware Cloud Director Availability provides migration, protection, failover, and reverse failover of VMs, vApps, and templates across on-premises VMware vCenter, VMware Cloud Director, or VMware Cloud Director service (CDS) to VMware CDS on Azure VMware Solution.

- Azure VMware Solution to Azure VMware Solution

  VMware Cloud Director Availability provides a flexible solution for multitenant customers. The flexible solution enables smooth workload migration between Cloud Director service (CDS) instances hosted on Azure VMware Solution SDDC, which empowers efficient cloud-to-cloud migration at the tenant level when using CDs with Azure VMware Solution.

Key components of VMware Cloud Director Availability

VMware Cloud Director Availability consists of the following types of appliances.

Replication Management Appliance

This appliance, also known as the manager, enables communication with VMware Cloud Director. The enabled communication gives VMware Cloud Director Availability the capability to discover resources like: Organization Virtual datacenter (OrgVDC), storage policies, datastores, and networks managed by VMware Cloud director and used by tenants.

The manager plays a vital role in identifying vApps and virtual machines (VMs) eligible for replication of migration and suitable destinations for incoming replications and migrations. It also provides user interface (UI) and API interfaces, which serve as a communication bridge for users interacting with VMware Cloud Director availability.

The responsibility of the manager extends to communication with local and remote replicators and collecting data about each protected or migrated workload.

Replication appliance instances

VMware Cloud Director Availability Cloud Replication appliance serves as the entity responsible for transferring replication data to and from ESXi hosts in the cloud. For outgoing replications or migrations, it communicates with the VM Kernel interface of an ESXi host; capturing, encrypting, and optionally compressing the replication data. The data is sent to a remote replicator, whether in the cloud or on-premises.

For incoming replications or migrations, the cloud replicator receives data from a replicator (whether in the cloud or on-premises), decrypts and decompresses it, and then transfers it to ESXi to be written to a datastore. You can deploy more replicators to scale as number of migrations or protections increases.

Tunnel appliance

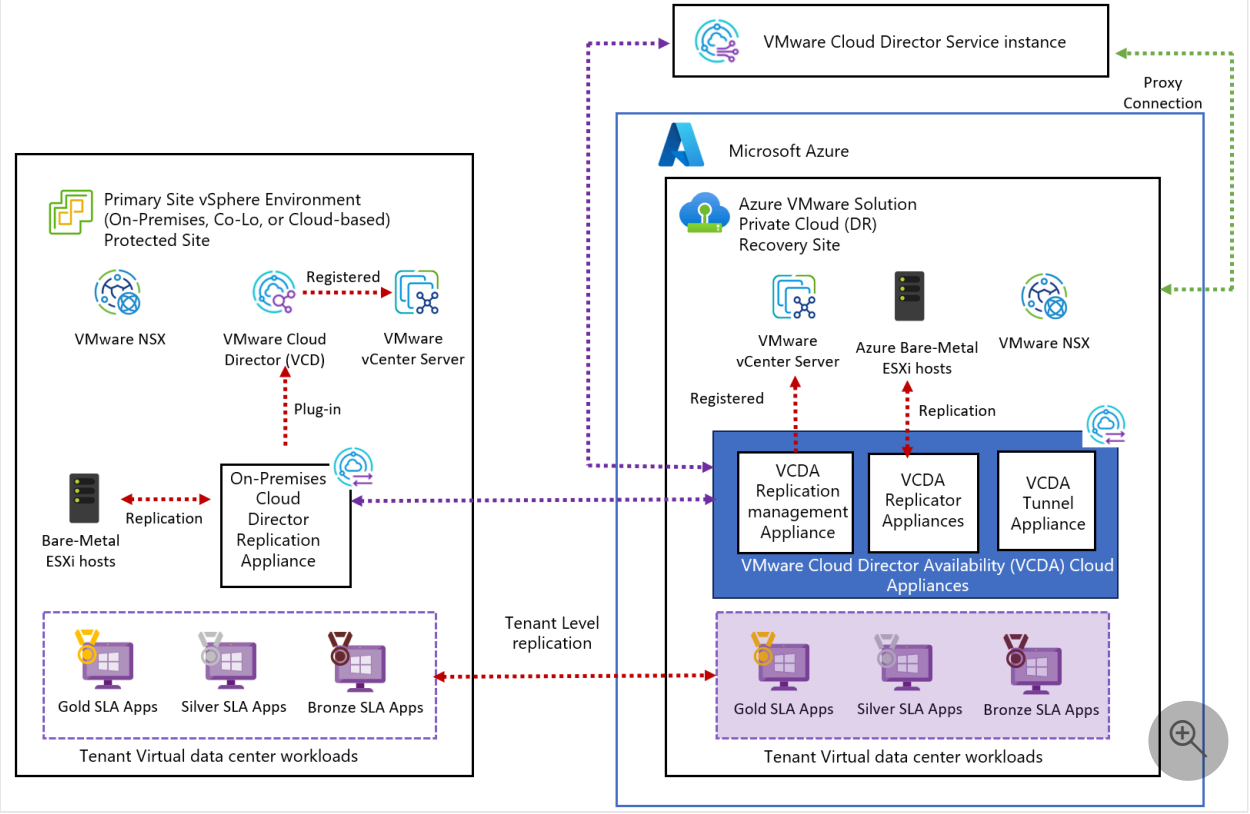
Tunnel appliance is the single-entry point to VMware Cloud Director Availability instance in the cloud and its role is to manage incoming management and replication traffic. Tunnel handles both data and management traffic and forwards it respectively to cloud replicators and manager.

On-premises Cloud director replication appliance

This appliance is deployed in tenant on-premises datacenters. It creates a pairing relation to VMware Cloud Director Availability in the cloud and can protect or migrate VMs running locally to the cloud and vice versa.

VMware Cloud Director Availability installation in the Azure VMware Solution cloud site consists of one Replication Manager, one Tunnel Appliance, and two Replicator Appliances. You can deploy more replicators using Azure portal.

The following diagram shows VMware Cloud Director Availability appliances installed in both on-premises and Azure VMware Solution.



Install and configure VMware Cloud Director Availability on Azure VMware Solution

Verify the following prerequisites to ensure you're ready to install and configure VMware Cloud Director Availability using Run commands.

Prerequisites

- Verify the Azure VMware Solution private cloud is configured.
- Verify the VMware-Cloud-Director-Availability-Providerrelease.number.xxxxxxx-build_sha_OVF10.ova version 4.7 is uploaded under the correct datastore.
- Verify the subnet, DNS zone and records for the VMware Cloud Director Availability appliances are configured.

- Verify the subnet has outbound Internet connectivity to communicate with: VMware Cloud Director service, remote VMware Cloud Director Availability sites, and the upgrade repository.
- Verify the DNS zone has a forwarding capability for the public IP addresses that need to be reached.

For using VMware Cloud Director Availability outside of the local network segment, turn on public IP addresses to an NSX-T Edge node for NSX-T Data Center.

- Verify the Cloud Director service is associated, and the Transport Proxy is configured with the Azure VMware Solution private cloud SDDC.

Install and manage VMware Cloud Directory Availability using Run commands

Customers can deploy VMware Cloud Director Availability using Azure Run commands on Azure portal.

> **ⓘ Important**
>
> Converting from manual installation of VMware Cloud Director Availability to Run command is not supported. Existing customers using VMware Cloud Director Availability can use Run commands and install VMware Cloud Director Availability to fully leverage the classic engine and Disaster Recovery capabilities.

To access Run commands for VCDA:

1. Navigate to Azure VMware Solution private cloud
2. Under **Operations**, select **Run command**
3. Select **VMware.VCDA.AVS package**

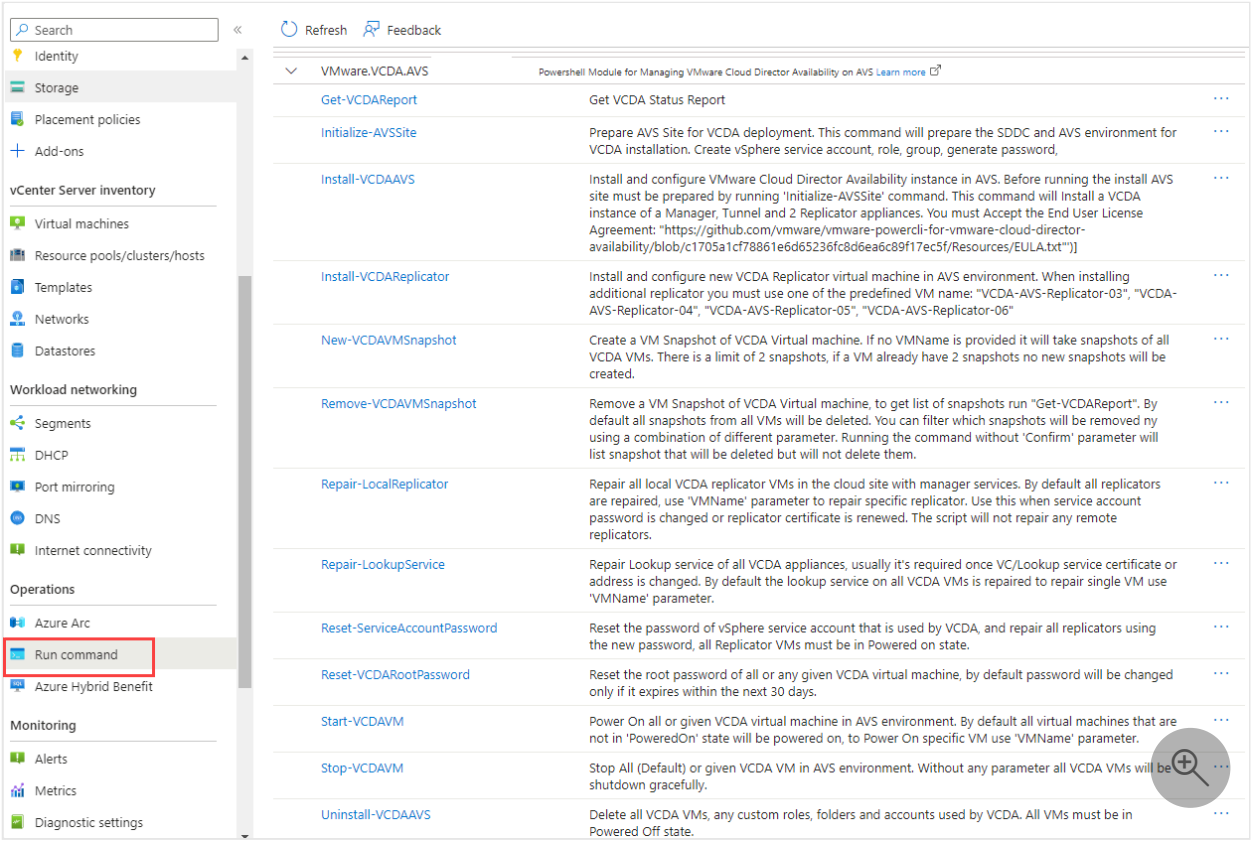
The Azure VMware Solution private cloud portal provides a range of Run commands for VCDA as are shown in the following screenshot. The commands empower you to perform various operations, including installation, configuration, uninstallation, scaling, and more.

The Run command **Install-VCDAAVS** installs and configures the VMware Cloud Director Availability instance in Azure VMware Solution. The instance includes VMware Cloud Director Replication Manager, Tunnel, and two Replicators. You can add more replicators by using **Install-VCDARepliactor** to scale.

> **Note**
>
> Run the **Initialize-AVSSite** command before you run the install command.

You can also use Run commands to perform many other functions such as start, stop VMware Cloud Director Availability VMs, uninstall VMware Cloud Director availability, and more.

The following image shows the Run commands that are available under **VMware.VCDA.AVS** for VMware Cloud Director Availability on Azure VMware Solution.



Refer to VMware Cloud Director Availability in Azure VMware Soltion for detailed instructions on utilizing the Run commands to effectively install and manage VMware Cloud Director Availability within your Azure solution private cloud.

FAQs

How do I install and configure VMware Cloud Director Availability in Azure VMware Solution and what are the prerequisites?

Deploy VMware Cloud Director Availability using Run commands to enable classic engines and to access Disaster Recovery functionality. See prerequisites and procedures in Run command in Azure VMware Solution.

How is VMware Cloud Director Availability supported?

VMware Cloud Director Availability is a VMware owned and supported product on Azure VMware Solution. For any support queries on VMware Cloud Director availability, contact VMware support for assistance. Both VMware and Microsoft support teams collaborate as necessary to address and resolve VMware Cloud Director Availability issues within Azure VMware Solution.

What are Run commands in Azure VMware Solution?

For more information, go to Run Command in Azure VMware Solution.

How can I add more Replicators in my existing VMware Cloud Director Availability instance in Azure VMware Solution?

You can use Run Command **Install-VCDAReplicator** to install and configure new VMware Cloud Director Availability replicator virtual machines in Azure VMware Solution.

How can I upgrade VMware Cloud Director availability?

VMware Cloud Director Availability can be upgraded using Appliances upgrade sequence and prerequisites.

Next steps

Learn more about VMware Cloud Director Availability Run commands in Azure VMware Solution, VMware Cloud Director availability.

Open a support request for an Azure VMware Solution deployment or provisioning failure

Article • 12/13/2023

This article shows you how to open a support request and provide key information for an Azure VMware Solution deployment or provisioning failure.

When you have a failure on your private cloud, you need to open a support request in the Azure portal. To open a support request, first get some key information in the Azure portal:

- Correlation ID
- Error messages
- Azure ExpressRoute circuit ID

Get the correlation ID

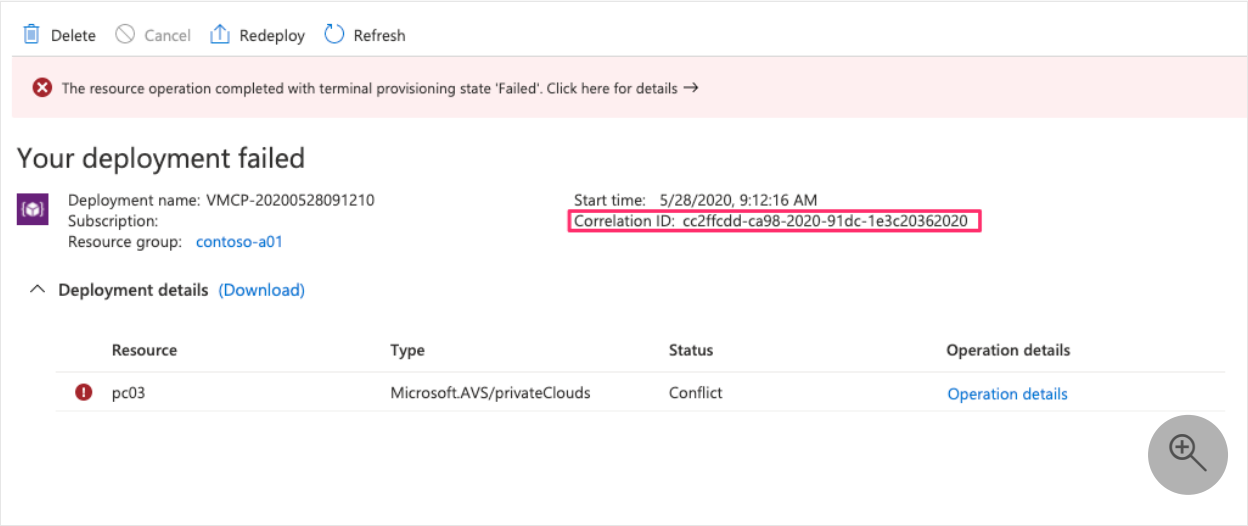
When you create a private cloud or any resource in Azure, a correlation ID for the resource is automatically generated for the resource. Include the private cloud correlation ID in your support request to more quickly open and resolve the request.

In the Azure portal, you can get the correlation ID for a resource in two ways:

- **Overview** pane
- Deployment logs

Get the correlation ID from the resource overview

Here's an example of the operation details of a failed private cloud deployment, with the correlation ID selected:



To access deployment results in a private cloud **Overview** pane:

1. In the Azure portal, select your private cloud.
2. In the left menu, select **Overview**.

After a deployment is initiated, the results of the deployment are shown in the private cloud **Overview** pane.

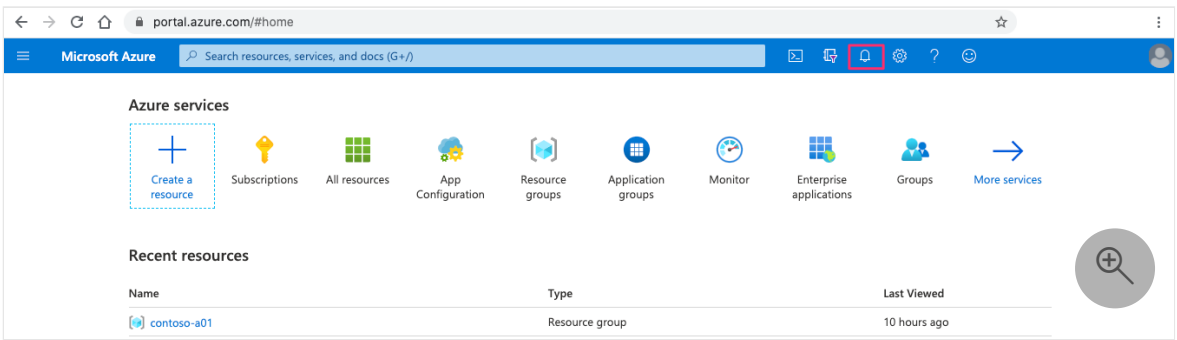
Copy and save the private cloud deployment correlation ID to include in the service request.

Get the correlation ID from the deployment log

You can get the correlation ID for a failed deployment by searching the deployment activity log located in the Azure portal.

To access the deployment log:

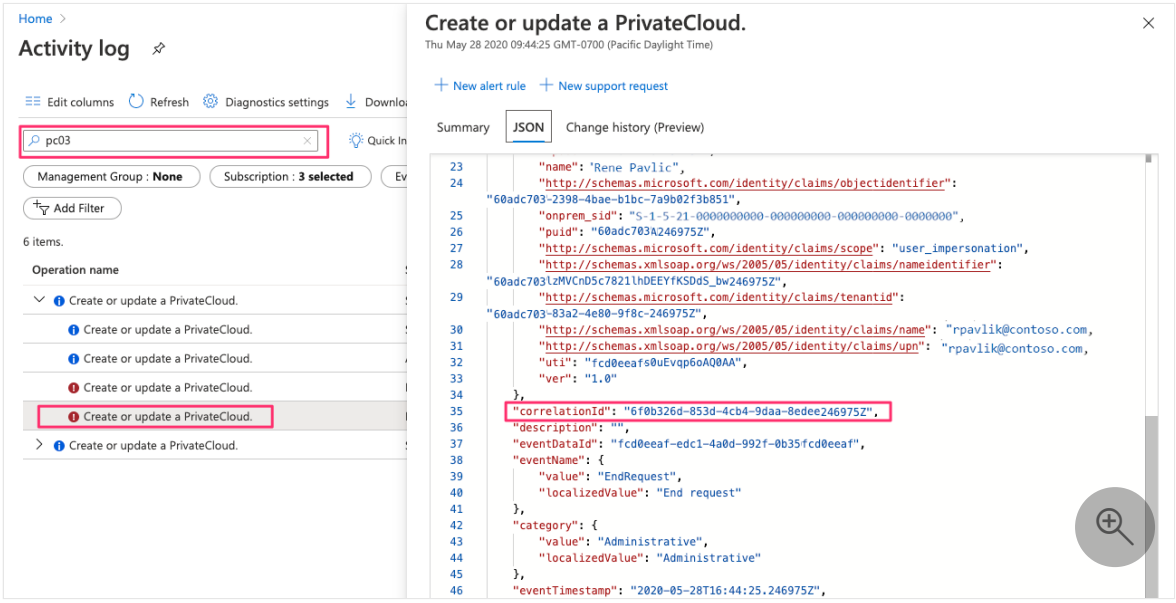
1. In the Azure portal, select your private cloud, and then select the notifications icon.



2. In the **Notifications** pane, select **More events in the activity log**:

3. To find the failed deployment and its correlation ID, search for the name of the resource or other information that you used to create the resource.

   The following example shows search results for a private cloud resource named pc03.

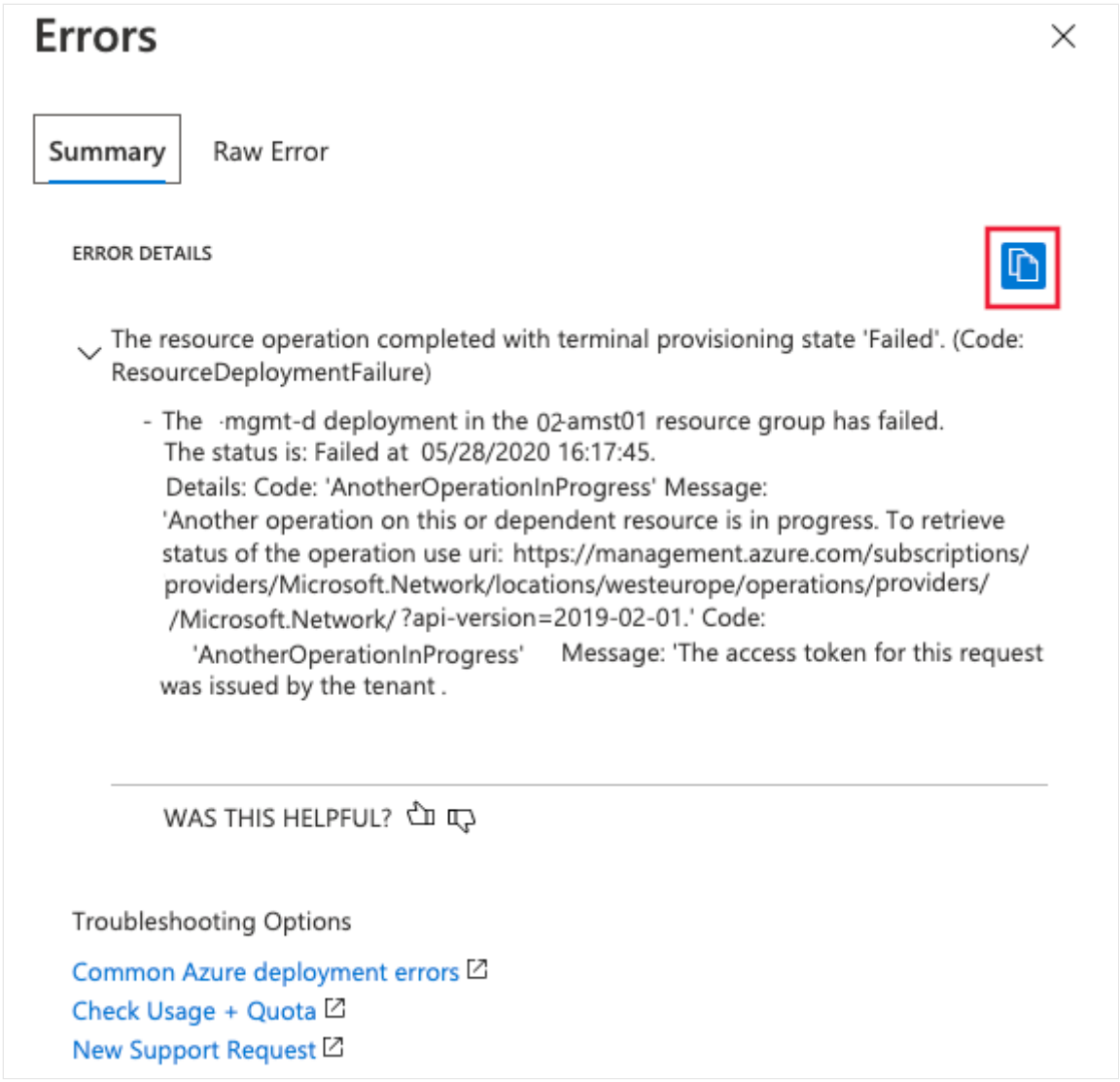


4. In the search results in the **Activity log** pane, select the operation name of the failed deployment.

5. In the **Create or update a PrivateCloud** pane, select the **JSON** tab, and then look for `correlationId` in the log that is shown. Copy the `correlationId` value to include it in your support request.

Copy error messages

To help resolve your deployment issue, include any error messages that are shown in the Azure portal. Select a warning message to see a summary of errors:



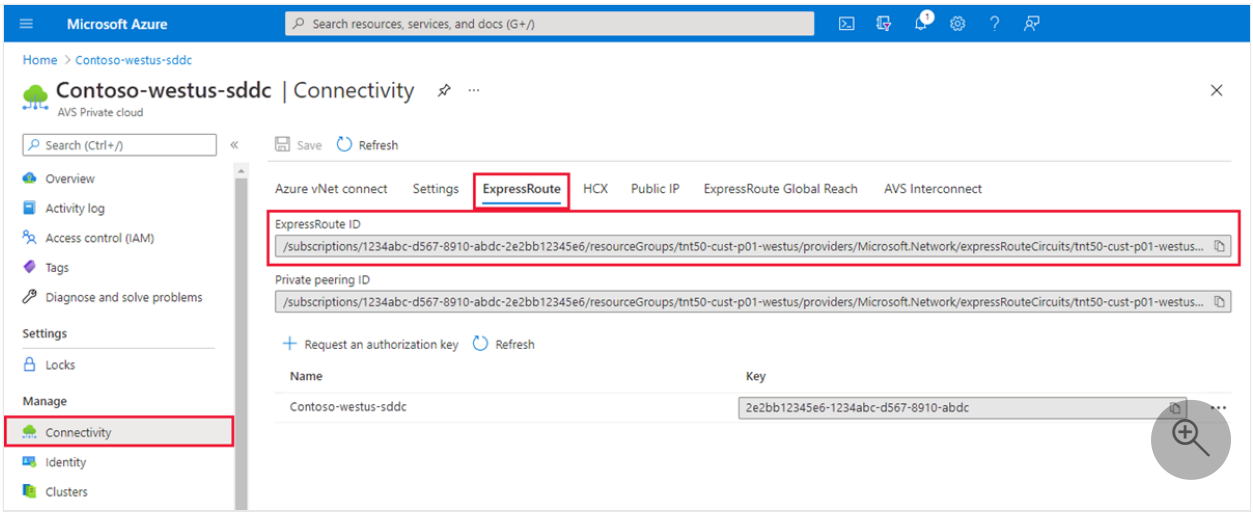
To copy the error message, select the copy icon. Save the copied message to include in your support request.

Get the ExpressRoute ID (URI)

Perhaps you're trying to scale or peer an existing private cloud with the private cloud ExpressRoute circuit, and it fails. In that scenario, you need the ExpressRoute ID to include in your support request.

To copy the ExpressRoute ID:

1. In the Azure portal, select your private cloud.
2. In the left menu, under **Manage**, select **Connectivity**.
3. In the right pane, select the **ExpressRoute** tab.
4. Select the copy icon for **ExpressRoute ID** and save the value to use in your support request.



Prevalidation failures

If your private cloud prevalidations check failed (before deployment), a correlation ID isn't generated. In this scenario, you can provide the following information in your support request:

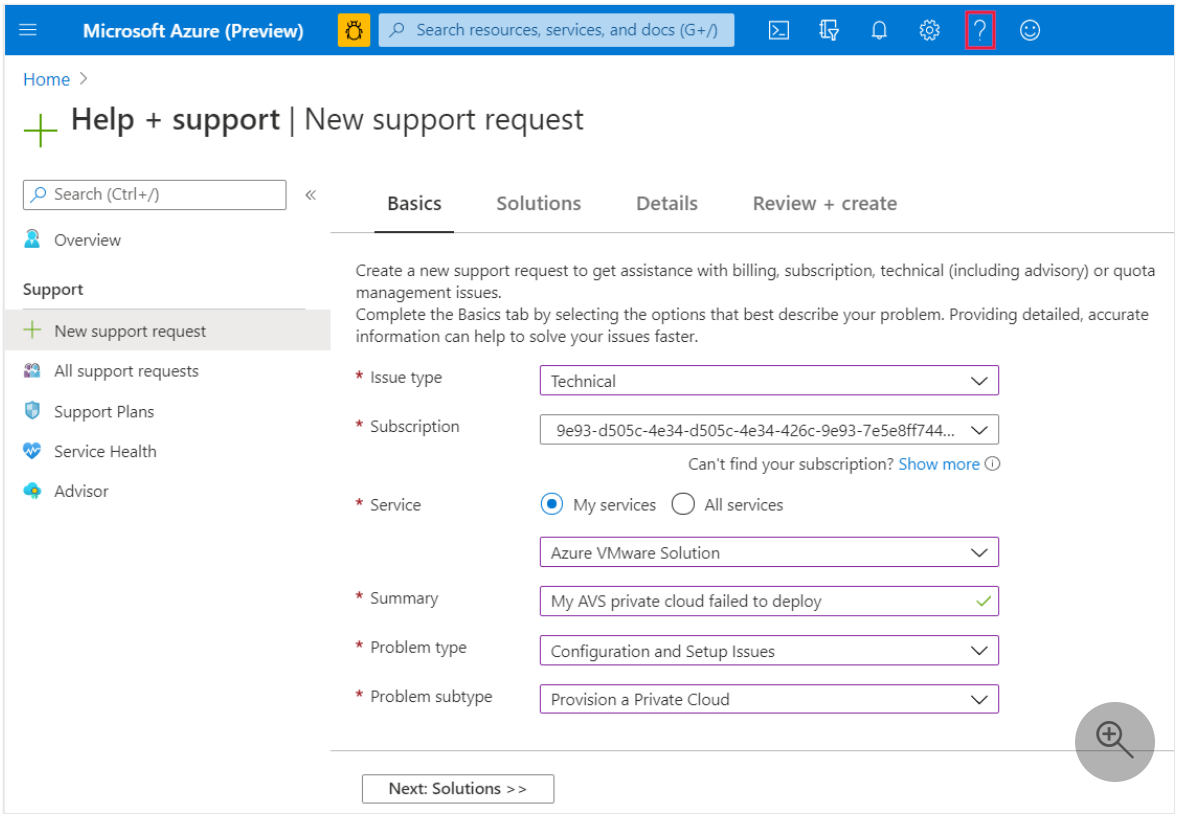
- Error and failure messages. These messages can be helpful in many failures, for example, for quota-related issues. It's important to copy these messages and include them in the support request, as described in this article.
- Information you used to create the Azure VMware Solution private cloud, including:
  - Location
  - Resource group
  - Resource name

Create your support request

For general information about creating a support request, see How to create an Azure support request.

To create a support request for an Azure VMware Solution deployment or provisioning failure:

1. In the Azure portal, select the **Help** icon, and then select **New support request**.



2. Enter or select the required information:

   a. On the **Basics** tab:

      i. For **Problem type**, select **Configuration and Setup Issues**.

      ii. For **Problem subtype**, select **Provision a private cloud**.

   b. On the **Details** tab:

      i. Enter or select the required information.

      ii. Paste your Correlation ID or ExpressRoute ID where this information is requested. If you don't see a specific text box for these values, paste them in the **Provide details about the issue** text box.

   c. Paste any error details, including the error or failure messages you copied, in the **Provide details about the issue** text box.

3. Review your entries, and then select **Create** to create your support request.

Common questions about Azure VMware Solution

FAQ

This article answers commonly asked questions about Azure VMware Solution.

General

What is Azure VMware Solution?

As enterprises pursue IT modernization strategies to improve business agility, reduce costs, and accelerate innovation, hybrid cloud platforms are key enablers of customers' digital transformation. Azure VMware Solution combines VMware's Software-Defined Data Center (SDDC) software with Microsoft's Azure global cloud service ecosystem. In addition, Azure VMware Solution meets performance, availability, security, and compliance requirements. For more information, see What is Azure VMware Solution.

Where is Azure VMware Solution available today?

The service is continuously being added to new regions. For details, see the latest service availability information.

Who supports Azure VMware Solution?

Microsoft delivers support for Azure VMware Solution. You can submit a support request. For Cloud Solution Provider (CSP) managed subscriptions, the first level of support provides the Solution Provider in the same fashion as CSP does for other Azure services.

Can workloads running in an Azure VMware Solution instance integrate with Azure services?

All Azure services are available to Azure VMware Solution customers. Performance and availability limitations for specific services should be addressed on a case-by-case basis.

What guest operating systems are compatible with Azure VMware Solution?

You can find information about guest operating system compatibility with vSphere by using the VMware Compatibility Guide. To identify the version of vSphere running in Azure VMware Solution, see VMware software versions.

What does the change control process look like?

Updates made follow Microsoft Azure's standard change management process. Customers are responsible for any workload administration tasks and the associated change management processes.

How is this version different from Azure VMware Solution by CloudSimple?

With the new Azure VMware Solution, Microsoft and VMware have a direct cloud provider partnership. Microsoft designed, built, and supported the new solution. The solution is endorsed by VMware. Architecturally, the solutions are consistent, with the VMware technology stack running on a dedicated Azure infrastructure.

Billing

Is there a Service Level Agreement (SLA) on disk replacement when failures occur?

Any hosts with disk issues are replaced. It rolls up to 99.9 SLA availability of the Azure VMware Solution service.

How is pricing structured for Azure VMware Solution?

For general questions on pricing, see the Azure VMware Solution pricing page.

Is VMware HCX Enterprise available, and if so, how much does it cost?

VMware HCX Enterprise is available on Azure VMware Solution at no other cost and is enabled by default.

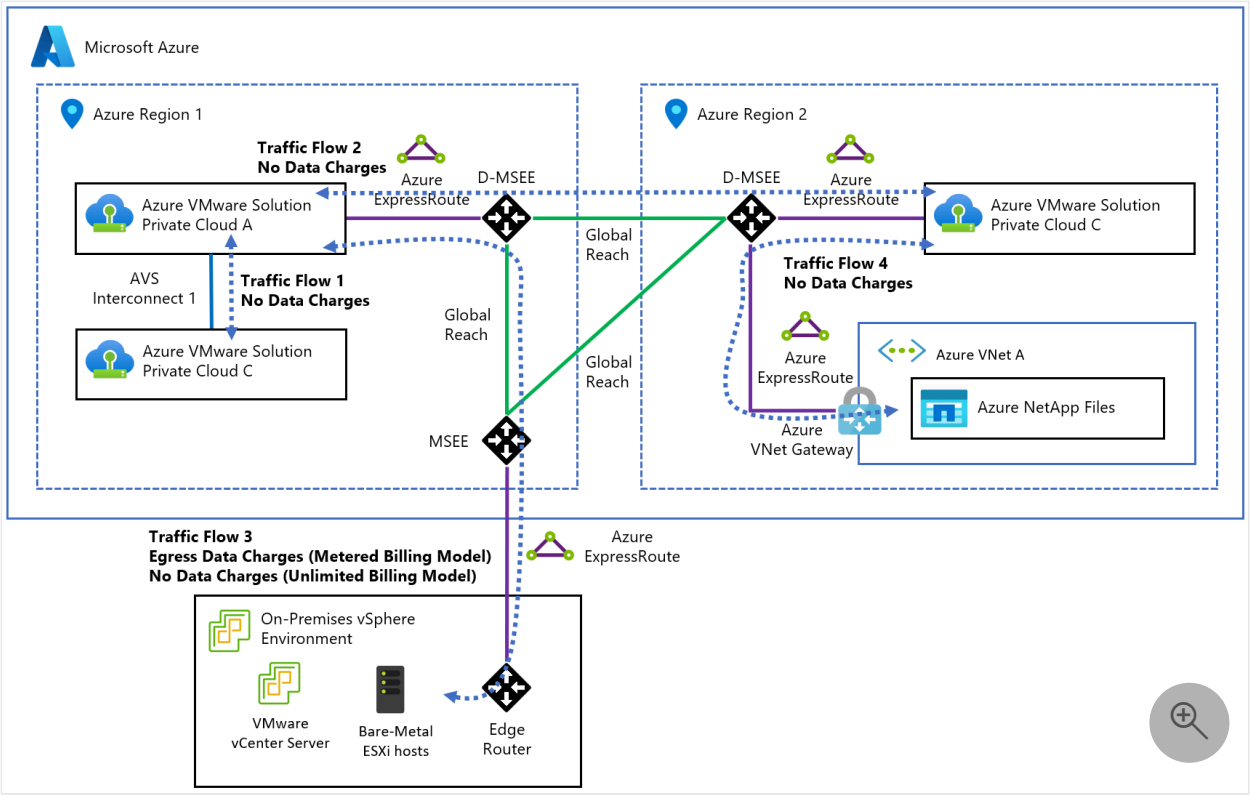
Will traffic between on-premises and Azure VMware Solution over ExpressRoute incur any outbound data transfer charge in the metered data plan?

Traffic in the Azure VMware Solution ExpressRoute circuit isn't metered. No billing for any Azure VMware Solution ExpressRoute circuit, or for Global Reach charges between Azure VMware Solution private clouds. This scenario includes Azure VMware Solution to on-premises, other than standard egress charges for traffic from your Azure ExpressRoute circuit connection to your on-premises site from Azure. These fees are charged according to Azure ExpressRoute pricing plans with the Metered Billing Model. If you're using the Azure ExpressRoute Unlimited Billing Model, egress traffic isn't charged.

- **Azure VMware Solution to Azure Virtual Network** is through an internal ExpressRoute circuit and is free of cost, regardless of region location (same region or cross-region).
- **Azure VMware Solution to on-premises site** is done through Azure Virtual Network or ExpressRoute Global Reach (between the internal ExpressRoute and external ExpressRoute). It's still free aside from the standard egress charges (Metered Billing Model) from the ExpressRoute to on-premises network. For the Unlimited Billing Model, there are no data charges.

For example:

- If we connect an Azure Virtual Network in Azure West Europe to an Azure VMware Solution private cloud in West Europe, there are no ExpressRoute charges other than the ExpressRoute gateway charges.
- If we connect an Azure Virtual Network in Azure North Europe to an Azure VMware Solution private cloud in West Europe, there are no ExpressRoute charges other than the ExpressRoute gateway charges.
- If you connect an Azure VMware Solution private cloud in West Europe to an Azure VMware Solution private cloud in North Europe via ExpressRoute Global Reach. There are no ExpressRoute Global Reach data transfer (egress and ingress) charges. There are charges when using an ExpressRoute gateway.



Is it necessary to procure other VMware licensing and resources other than the AV36 instance when migrating from the on-premises VM environment with an L2 extension?

No, you don't need to procure other VMware licensing beyond the Azure VMware Solution service. For more information, see the Azure VMware Solution pricing page to see what VMware technology is included.

Support

How do I request a host quota increase for Azure VMware Solution?

Whether you want more hosts for an existing private cloud or you're creating a new private cloud, you need to submit a support ticket to have your hosts allocated. For more information, see Request host quota for Azure VMware Solution.

What accounts do I need to create an Azure VMware Solution private cloud?

You need an Azure account in an Azure subscription.

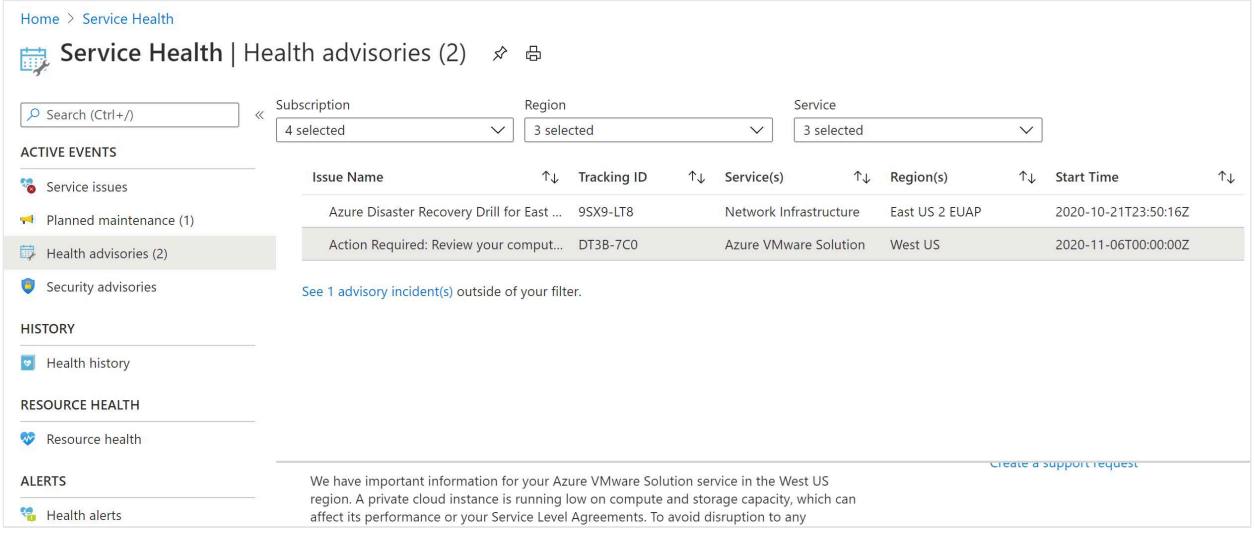
Are Red Hat solutions supported on Azure VMware Solution?

Microsoft and Red Hat share an integrated, colocated support team that provides a unified contact point for Red Hat ecosystems running on the Azure platform. Like other Azure platform services that work with Red Hat Enterprise Linux, Azure VMware Solution falls under the Cloud Access and integrated support umbrella. Red Hat Enterprise Linux supports running on top of Azure VMware Solution within Azure.

Customer communication

How can I receive an alert when Azure sends service health notifications to my Azure subscription?

You can find service issues, planned maintenance, health advisories, and security advisories notifications published through **Service Health** in the Azure portal. You can take timely actions when you set up activity log alerts for these notifications. For more information, see Create Service Health alerts using the Azure portal.



Configuration and setup

How long does it take to provision the initial three hosts in a cluster?

At the moment, the provisioning can take roughly 3-4 hours. Adding a single node in existing/same cluster takes between 30 - 45 minutes.

Can I use the folder name "AVS-vendor-folders" for vCenter Server VM folders in Azure VMware Solution?

No, "AVS-vendor-folders" is a reserved name within Azure VMware Solution and using it might lead to conflicts with the intended functionality or cause unexpected behavior within the vCenter management environment specific to Azure VMware Solution. Choose an alternative folder name that aligns with your organizational needs while avoiding conflicts with predefined naming conventions in Azure VMware Solution.

VMware solution software

Can Azure VMware Solution VMs be managed by VMRC?

Yes. Provided the system it's installed on can access the private cloud vCenter Server and is using public DNS to resolve ESXi hostnames.

Are there special instructions for installing and using VMRC with Azure VMware Solution VMs?

No. To meet the VM prerequisites, follow the instructions provided by VMware.

Can I use vRealize Suite running on-premises?

vRealize Automation, vRealize Operations Manager, and vRealize Network Insight are certified for use with Azure VMware Solution when those products are installed in an on-premises data center. The cloud-based versions of these products--vRealize Automation Cloud, vRealize Operations Cloud, and vRealize Network Insight Cloud--are also certified for use. Installing these products within an Azure VMware Solution private cloud isn't supported.

Can I migrate vSphere VMs from on-premises environments to Azure VMware Solution private

clouds?

Yes. This is possible and recommended via the VMware HCX add-on. While cross vCenter cold migration and cloning is possible, not cross vCenter vMotion, HCX is the fully supported method.

Is a specific version of vSphere required in on-premises environments?

The on-premises environment must be running vSphere 6.5 or later if VMware HCX will be used to migrate VMs.

How do I migrate a VM to a different plan?

To migrate an Azure Virtual Machine (VM) to a different plan, follow these steps:

1. Stop the VM in the Azure portal by selecting your VM and then selecting 'Stop' to deallocate resources.
2. With the VM stopped, access the 'Size' setting of the VM.
3. In the 'Choose a size' panel, select a new size that is compatible with either the current or desired series.
4. Select the 'Resize' button to apply the size change.
5. Restart the VM to finalize the migration.

Remember that you can only resize a VM within the same series or to an available series in the same Azure region. Ensure the new plan supports your VM's storage and networking configurations.

Is VMware HCX supported on VPNs?

Yes, provided VMware HCX Network Underlay Minimum Requirements are met.

What versions of VMware software are used in private clouds?

The VMware solution software versions used in new deployments of Azure VMware Solution private clouds are:

Expand table

Software	Version
VMware vCenter Server	8.0 U2b
VMware ESXi	8.0 U2b
VMware vSAN	8.0 U2
VMware vSAN on-disk format	19
VMware vSAN storage architecture	OSA
VMware NSX	4.1.1
VMware HCX	4.9.1
VMware Site Recovery Manager	8.8.0.3
VMware vSphere Replication	8.8.0.3

The current running software version is applied to new clusters added to an existing private cloud, if the vCenter Server version supports it.

How often is the VMware solution software (ESXi, vCenter Server, NSX) patched, updated, or upgraded in the Azure VMware Solution private cloud?

One benefit of Azure VMware Solution private clouds is that the platform is maintained for you. Microsoft is responsible for the lifecycle management of VMware software (ESXi, vCenter Server, and vSAN) and NSX appliances. Microsoft is also responsible for bootstrapping the network configuration, like creating the Tier-0 gateway and enabling North-South routing. You're responsible for the NSX SDN configuration: network segments, distributed firewall rules, Tier 1 gateways, and load balancers.

> **Note**

A T0 gateway is created and configured as part of a private cloud deployment. Any modification to that logical router or the NSX edge node VMs could affect connectivity to your private cloud and should be avoided.

Microsoft is responsible for applying any patches, updates, or upgrades to ESXi, vCenter Server, vSAN, and NSX in your private cloud. The impact of patches, updates, and upgrades on ESXi, vCenter Server, and NSX has the following considerations:

- **ESXi** - There's no impact to workloads running in your private cloud. Access to vCenter Server and NSX isn't blocked during this time. During this time, we recommend you don't plan other activities like: scaling up private cloud, scheduling or initiating active HCX migrations, making HCX configuration changes, and so on, in your private cloud.

- **vCenter Server** - There's no impact to workloads running in your private cloud. During this time, vCenter Server is unavailable and you can't manage VMs (stop, start, create, or delete). We recommend you don't plan other activities like scaling up private cloud, creating new networks, and so on, in your private cloud. When you use VMware Site Recovery Manager or vSphere Replication user interfaces, we recommend you don't do either of the actions: configure vSphere Replication, and configure or execute site recovery plans during the vCenter Server upgrade.

- **NSX** - The workload is impacted. When a particular host is being upgraded, the VMs on that host might lose connectivity from 2 seconds to 1 minute with any of the following symptoms:

  - Ping errors
  - Packet loss
  - Error messages (for example, *Destination Host Unreachable* and *Net unreachable*)

  During this upgrade window, all access to the NSX management plane is blocked. You can't make configuration changes to the NSX environment for the duration. Your workloads continue to run as normal, subject to the upgrade impact previously detailed.

  During the upgrade time, we recommend you don't plan other activities like, scaling up private cloud, and so on, in your private cloud. Other activities can prevent the upgrade from starting or could have adverse impacts on the upgrade and the environment.

You're notified through Azure Service Health that includes the timeline of the upgrade. This notification also provides details on the upgraded component, its effect on workloads, private cloud access, and other Azure services. You can reschedule an upgrade as needed.

Software updates include:

- **Patches** - Security patches or bug fixes released by VMware
- **Updates** - Minor version change of a VMware stack component
- **Upgrades** - Major version change of a VMware stack component

> **Note**
>
> Microsoft tests a critical security patch as soon as it becomes available from VMware.

Documented VMware workarounds are implemented in lieu of installing a corresponding patch until the next scheduled updates are deployed.

Do private clouds use VMware NSX? If so, which version is supported?

Yes, NSX is the only supported version of VMware network virtualization software.

VMware NSX 4.1.1 is used for the software-defined networking in Azure VMware Solution private clouds.

Is VMware NSX required in on-premises environments or networks that connect to a private cloud?

No, you aren't required to use VMware NSX on-premises. VMware HCX provides the necessary connectivity between on-premises vSphere and Azure VMware Solution.

Is NSX Identity Firewall and distributed IDS/IPS supported with Azure VMware Solution?

Yes with an add-on license. Azure VMware Solution supports distributed IDFW and distributed IDS/IPS with add-on firewall license. This add-on license needs to be bought

from VMware and Microsoft will apply that license to the Azure VMware Solution private cloud with a support request.

Is NSX Service Insertion supported with Azure VMware Solution?

No.

Is VMware Horizon 8 2012 compatible with Azure VMware Solution?

Yes.

Migrate

Why can't I see my Sentinel Management tab in the HCX Manager when using the Sentinel Appliance service?

The Sentinel Management tab provides you access to download the Sentinel software. It appears in the HCX Interconnect interface when an HCX Enterprise license is activated, and you have deployed a service mesh with a Sentinel Gateway (SGW) and Sentinel Data Receiver (SDR) pair deployed. Also, in traditional on-premises to cloud deployments, the Sentinel tab is only visible in the Connector, not cloud manager.

If we migrate a VM created with thick provisioning on the on-premises side to Azure VMware Solution, will the VM remain thick?

You can specify the type of format you want when you migrate a VM to Azure VMware Solution. However, vSAN is primarily the datastore you'll use in Azure VMware Solution, so it depends on the storage policy that's selected. The datastore default storage policy is the RAID-1 FTT-1, which is thin provisioned. You can use Run commands to change the default datastore storage policy.

Compute

What are the CPU specifications in each type of host?

The AV36 SKU servers have dual 18 core 2.3 GHz Intel CPUs. AV36P SKU servers have dual 18 core 2.6 GHz Intel CPUs and AV52 SKU servers have dual 26 core 2.7 GHz Intel CPUs.

How much memory is in each host?

The AV36 SKU servers have 576 GB of RAM. AV36P SKU servers have 768 GB of RAM and AV52 SKU servers have 1,536 GB of RAM.

Does Azure VMware Solution support running ESXi as a nested virtualization solution?

No. VMware doesn't officially support nested virtualization.

Backup/restore

What independent software vendors (ISVs) backup solutions work with Azure VMware Solution?

Commvault, Veritas, and Veeam have extended their backup solutions to work with Azure VMware Solution. However, any backup solution that uses VMware vStorage API for Data Protection (VADP) with the HotAdd transport mode works out of the box on Azure VMware Solution. For more information, see Backup solutions for Azure VMware Solution VMs.

What about support for ISV backup solutions?

As these backup solutions are installed and managed by customers, they can reach out to the respective ISV for support.

Networking and interconnectivity

Can Azure Bastion be used for connecting to Azure VMware Solution VMs?

Azure Bastion is the service recommended to connect to the jump box to prevent exposing Azure VMware Solution to the internet. You can't use Azure Bastion to connect to Azure VMware Solution VMs since they aren't Azure IaaS objects.

How much network bandwidth is available in each ESXi host?

Each ESXi host in Azure VMware Solution is configured with four 25-Gbps NICs, two NICs provisioned for ESXi system traffic, and two NICs provisioned for workload traffic.

Are the SNMP infrastructure logs shared?

No.

Does ExpressRoute support packets exceeding MTU of 1500?

No.

Can Azure Load Balancer internal be used for Azure VMware Solution VMs?

No. Azure Load Balancer internal-only supports Azure IaaS VMs. Azure Load Balancer doesn't support IP-based backend pools; only Azure VMs or Virtual Machine Scale Set objects in which Azure VMware Solution VMs aren't Azure objects.

Can an existing ExpressRoute Gateway be used to connect to Azure VMware Solution?

Yes. Use an existing ExpressRoute Gateway to connect to Azure VMware Solution as long as it doesn't exceed the limit of four ExpressRoute circuits per virtual network. To access Azure VMware Solution from on-premises through ExpressRoute, you must have ExpressRoute Global Reach since the ExpressRoute Gateway doesn't provide transitive routing between its connected circuits.

What network IP address planning is required to incorporate private clouds with on-premises environments?

A private network /22 address space is required to deploy an Azure VMware Solution private cloud. This private address space shouldn't overlap with other virtual networks in a subscription or with on-premises networks.

How do I connect from on-premises environments to an Azure VMware Solution private cloud?

You can connect to the service in one of two methods:

- With a VM or application gateway deployed on an Azure virtual network that is peered through ExpressRoute to the private cloud.
- Through ExpressRoute Global Reach from your on-premises data center to an Azure ExpressRoute circuit.

How do I connect a workload VM to the internet or an Azure service endpoint?

In the Azure portal, enable internet connectivity for a private cloud. With NSX Manager, create an NSX T1 gateway and a logical switch. You then use vCenter Server to deploy a VM on the network segment defined by the logical switch. That VM has network access to the internet and Azure services.

> **Note**
>
> A T0 gateway is created and configured as part of a private cloud deployment. Any modification to that logical router or the NSX edge node VMs could affect connectivity to your private cloud and should be avoided.

Do I need to restrict access from the internet to VMs on logical networks in a private cloud?

No. Network traffic inbound from the internet directly to private clouds isn't allowed by default. However, you're able to expose Azure VMware Solution VMs to the internet

through the Public IP option in your Azure portal for your Azure VMware Solution private cloud.

Do I need to restrict internet access from VMs on logical networks to the internet?

Yes. You need to use NSX Manager to create a firewall to restrict VM access to the internet.

Which IP range can be used for DNS service IP and DHCP server IP?

The IP address range shouldn't overlap with the IP range used in other virtual networks in your subscription and on-premises networks.

Can Azure VMware Solution use Azure Virtual WAN hosted ExpressRoute Gateways?

Yes.

Can transit connectivity be established between on-premises and Azure VMware Solution through Azure Virtual WAN over ExpressRoute Global Reach?

Azure Virtual WAN doesn't provide transitive routing between two connected ExpressRoute circuits and nonvirtual WAN ExpressRoute Gateway. ExpressRoute Global Reach allows connectivity between on-premises and Azure VMware Solution but goes through Microsoft's global network instead of the Virtual WAN Hub.

Is Windows 2008 supported as an Active Directory (AD) server or Remote Desktop Session Host (RDSH) OS in NSX?

No.

Why can't I reach the Azure VMware Solution vCenter Server Appliance and NSX Manager from on-premises or Azure Virtual Network?

By design, you won't be able to reach NSX Manager and vCenter Server Appliance (vCSA) from on-premises when only 0.0.0.0/0 (default route) is being advertised over ExpressRoute Global Reach between Azure VMware Solution and your on-premises ExpressRoute or through Azure Virtual Network to Azure VMware Solution. You need to advertise specific networking routes/subnets to access NSX Manager and vCSA.

Storage

What is the correct storage policy for the deduplication setup?

Use the *thin_provision* storage policy for your VM template.

What is the storage capacity of each host?

Each ESXi host has two vSAN disk groups with a capacity tier of 15.2 TB and a 3.2-TB NVMe cache tier (1.6 TB in each disk group).

Is data stored on the vSAN datastores encrypted at rest?

Yes, vSAN datastores use data-at-rest encryption by default using keys stored in Azure Key Vault. The encryption solution is KMS-based and supports vCenter Server operations for key management. When a host is removed from a vSphere cluster, data on disk is invalidated immediately.

Can I rename a datastore or cluster during creation?

No, you can't change the name of datastores or clusters.

What is the Fault tolerance of hardware failure on the vSAN?

RAID-1, FTT-1, with Object Space reservation set to Thin Provisioning is the Default Storage policy for the software-defined datacenters (SDDCs).

What is the difference between thick provisioning and thin provisioning?

Thick provisioning is reserved or preallocated storage space. Thick provisioning protects systems by allowing them to function even if the vSAN datastore is full because the space is already reserved. For example, suppose you create a 10-GB virtual disk with thick provisioning. In that case, the full amount of virtual disk storage capacity is preallocated on the physical storage where the virtual disk is created and consumes all the space allocated to it in the datastore. It won't allow other VMs to share the space from the datastore. A thin-provisioned virtual disk consumes the space that it needs initially and grows to the data space demand used in the datastore.

How many disks can fail on the vSAN before data loss occurs?

It depends on how you plan your application workloads to run inside the SDDC (private cloud). Microsoft governs these failures regularly and replaces the hardware when such events are detected from an infrastructure perspective. As a default, a setting of FTT-1 is used, which accommodates a single host's failure.

What kind of alerts can I expect to see for vSAN?

Microsoft provides alerts when capacity consumption exceeds 75%. Alternatively, you can also monitor capacity consumption metrics that are integrated into Azure Monitor.

How many 1.6-TB NVMe drives make up the disk groups to provide the 15.4 TB of raw SSD storage per host?

The AV36 SKU includes two 1.6-TB NVMe Cache and eight 1.9-TB raw storage capacity. These are then split into two disk groups. Check the AV36P and AV52 SKUs for their hardware specifications.

What is the RAID configuration of the disk groups?

The disk groups aren't RAID configured. Instead, they're just a bunch of disks (JBOD) and are directly controlled by vSAN.

Hosts, clusters, and private clouds

Is there more than one type of host available?

No. There's only one type available.

Do I use the same tools that I use now to manage private cloud resources?

Yes. The Azure portal is used for deployment and several management operations. vCenter Server and NSX Manager are used to manage vSphere and NSX resources.

Can I manage a private cloud with my on-premises vCenter Server?

At launch, Azure VMware Solution won't support a single management experience across on-premises and private cloud environments. You manage private cloud clusters with vCenter Server and NSX Manager local to a private cloud.

If a cluster is scaled up, and then workload demand falls, can it be scaled back down?

Yes, as long as you have the quota allocated against your private cloud, you can scale out your clusters. When workload demand falls, you can delete hosts from the cluster to scale it down. You can do this through the Azure VMware Solution portal.

Is the underlying infrastructure shared?

No, private cloud hosts and clusters are dedicated and securely erased before and after use.

What are the minimum and the maximum number of hosts per cluster? Can I scale my private cloud clusters?

Clusters can scale between three (minimum) and 16 (maximum) ESXi hosts.

Identity management

What accounts and privileges will I get with my new Azure VMware Solution private cloud?

You're provided credentials for a cloud admin user in vCenter Server and admin access on NSX Manager. You can also use a CloudAdmin group to incorporate Microsoft Active Directory. For more information, see Access and identity architecture.

Can have administrator access to ESXi hosts?

No, administrator access to ESXi is restricted to meet the security requirements of the solution.

What privileges and permissions will I have in vCenter Server?

You have CloudAdmin role privileges. For more information, see Access and identity architecture.

What privileges and permissions will I have on the NSX Manager?

You have CloudAdmin role privileges. For more information, see Access and identity architecture.

> **Note**
>
> A T0 gateway is created and configured as part of a private cloud deployment. Any modification to that logical router or the NSX edge node VMs could affect connectivity to your private cloud and should be avoided.

How can I change my credentials?

For information on resetting your credentials, see Rotate the cloudadmin credentials for Azure VMware Solution.

Are the cloudadmin extension privileges supported by Azure VMware Solution?

No. We currently don't support cloudadmin extension privileges and have no plans to support it.

CSP and multi-tenancy

Does Azure VMware Solution provide an option for hoster partners to resell the service?

Yes. For more information, see Request host quota for Azure VMware Solution.

Does Azure VMware Solution offer multi-tenancy for hosting CSP partners?

No. Currently, Azure VMware Solution doesn't offer multi-tenancy.

Does Azure VMware Solution enable a hoster partner to partition resources within the private cloud (SDDC) to manage for customers in a multi-tenanted way?

No, an Azure VMware Solution private cloud can't be shared between end customers.

I use Azure VMware Solution to create end-user applications or workloads accessed on multiple VMs through public IP. Can I sell this solution to multiple tenants?

Customers can create multitenant environments in their Azure VMware Solution private cloud and sell to customers provided the product isn't a standard VM and have added substantial intellectual property embedded in the VM as an application.

Can I connect VMware Cloud Director Service (CDS) to my Azure VMware Solution instance in Azure?

Yes. You can connect your Azure VMware Solution private cloud to VMware Cloud Director Service from VMware. This integration of both services is currently in public preview.

Can Azure VMware Solution be purchased through a Microsoft CSP?

Yes, customers can deploy Azure VMware Solution within an Azure subscription managed by a CSP.

Are Reserved Instances available for purchasing through the CSP program?

Yes. CSPs can purchase reserved instances for their customers. For more information, see Save costs with a reserved instance.

Feedback