Azure Arc documentation

Simplify complex and distributed environments across on-premises, edge, and multicloud.

OVERVIEW
About Azure Arc

SAMPLE
Azure Arc Jumpstart

OVERVIEW
Azure Arc-enabled servers

OVERVIEW
Azure Arc-enabled Kubernetes

OVERVIEW
Azure Arc-enabled data services

OVERVIEW
SQL Server enabled by Azure Arc

Azure Arc-enabled servers

- Connect hybrid machines
- Plan and deploy
- ESU for Windows Server 2012

See more >

Azure Arc-enabled Kubernetes

- Connect a cluster to Azure Arc
- Apply configurations on clusters using GitOps
- Access connected clusters from anywhere

See more >

Azure Arc-enabled data services

- Plan deployment
- Connectivity modes
- Create SQL Managed Instance

See more >

SQL Server enabled by Azure Arc

- Connect SQL Server to Azure Arc
- Assess instance
- Configure advanced data security

See more >

Azure Arc-enabled private clouds

- Azure Arc resource bridge
- Azure Arc-enabled VMware vSphere
- Azure Arc-enabled System Center Virtual Machine Manager
- Azure Arc VM management on Azure

Training modules

- Introduction to Azure Arc
- Plan and deploy Azure Arc-enabled servers at scale
- Secure hybrid and multicloud machines
- Monitor hybrid and multicloud machines

Local

Explore more

Azure Arc blog

Get the latest news from the Azure Arc team.

Azure Arc landing zone accelerator for hybrid and multicloud

Establish patterns for building hybrid architectures.

Azure Kubernetes Service (AKS) enabled by Azure Arc

Extend AKS to your on-premises environment.

Multicloud connector enabled by Azure Arc

Connect non-Azure public cloud resources to centralize management and governance in Azure.

Azure Container Apps on Azure Arc

Run Container Apps on Azure Arc-enabled Kubernetes clusters.

Azure IoT Operations Preview – enabled by Azure Arc

Azure IoT Operations is a unified data plane for the edge that helps organizations deploy the industrial...

Azure Arc site manager (preview)

Use Arc sites to represent your on-premises environments and see centralized monitoring information across your edge...

Edge RAG Preview enabled by Azure Arc

Search on-premises data with generative AI, using Retrieval Augmented Generation.

Azure Container Storage enabled by Azure Arc

A first-party storage system designed for Arc-connected Kubernetes clusters

Azure Arc overview

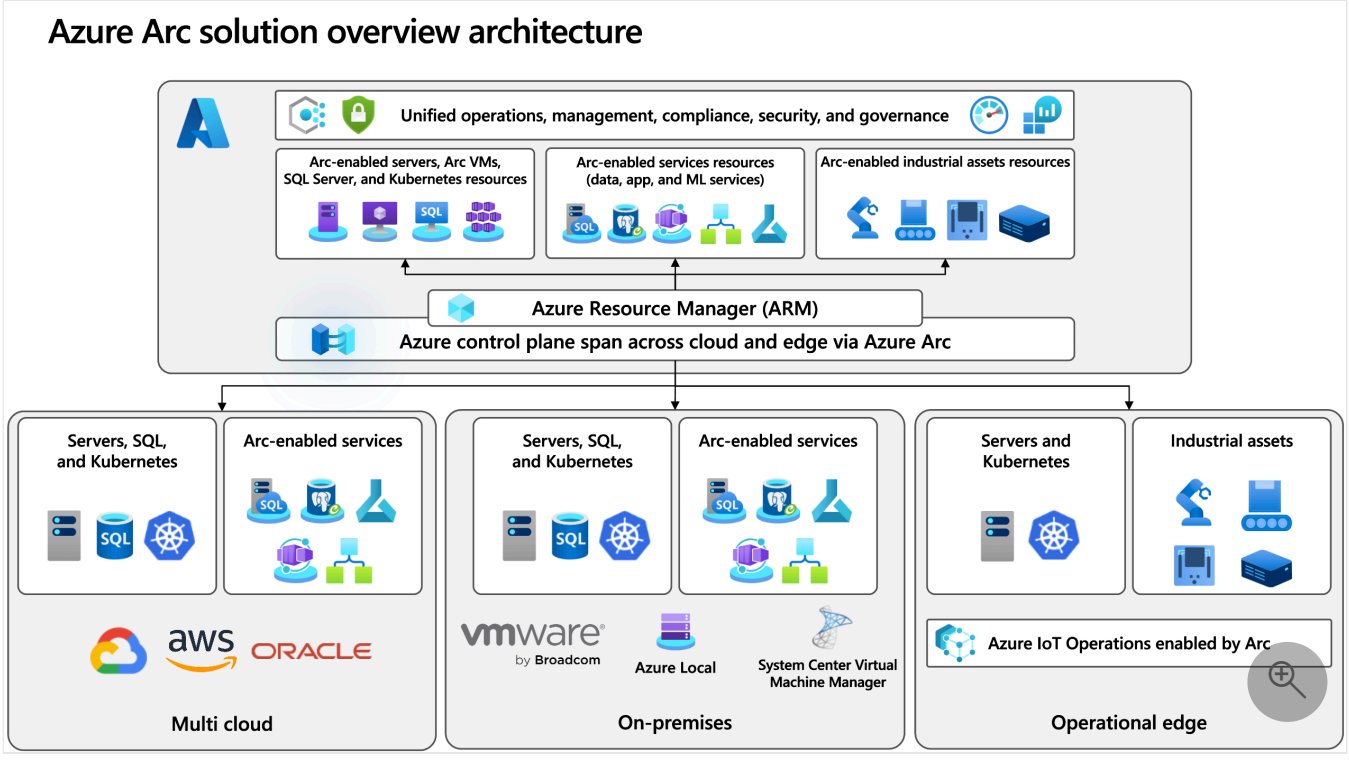
08/26/2025

Today, companies struggle to control and govern increasingly complex environments that extend across data centers, multiple clouds, and edge. Each environment and cloud possesses its own set of management tools, and new DevOps and ITOps operational models can be hard to implement across resources.

Azure Arc simplifies governance and management by delivering a consistent multicloud and on-premises management platform.

Azure Arc provides a centralized, unified way to:

- Manage your entire environment together by projecting your existing non-Azure and/or on-premises resources into Azure Resource Manager.
- Manage virtual machines, Kubernetes clusters, and databases as if they are running in Azure.
- Use familiar Azure services and management capabilities, regardless of where your resources live.
- Continue using traditional ITOps while introducing DevOps practices to support new cloud native patterns in your environment.
- Configure custom locations as an abstraction layer on top of Azure Arc-enabled Kubernetes clusters and cluster extensions.



To download architecture diagrams in high resolution, visit Jumpstart Gems.

Currently, Azure Arc allows you to manage the following resource types hosted outside of Azure:

- Servers and virtual machines: Manage Windows and Linux physical servers and virtual machines hosted outside of Azure. Provision, resize, delete, and manage virtual machines based on Azure Local and on VMware vCenter or System Center Virtual Machine Manager managed on-premises environments.
- Kubernetes clusters: Attach and configure Kubernetes clusters running anywhere, with multiple supported distributions.
- Azure data services: Run SQL Managed Instance on-premises, at the edge, and in public clouds using Kubernetes and the infrastructure of your choice.
- SQL Server: Extend Azure services to SQL Server instances hosted outside of Azure.

> **Note**
>
> For more information regarding the different services Azure Arc offers, see **Choosing the right Azure Arc service for machines**.

Indirectly connected mode

As of September, 2025 indirectly connected mode is retired.

Key features and benefits

Some of the key scenarios that Azure Arc supports are:

- Implement consistent inventory, management, governance, and security for servers across your environment.
- Configure Azure VM extensions to use Azure management services to monitor, secure, and update your servers.
- Manage and govern Kubernetes clusters at scale.
- Use GitOps to deploy configurations across one or more clusters from Git repositories.
- Zero-touch compliance and configuration for Kubernetes clusters using Azure Policy.
- Run Azure data services on any Kubernetes environment as if it runs in Azure (specifically Azure SQL Managed Instance, with benefits such as upgrades, updates, security, and monitoring). Use elastic scale and apply updates without any application downtime, even without continuous connection to Azure.

- Create custom locations on top of your Azure Arc-enabled Kubernetes clusters, using them as target locations for deploying Azure services instances. Deploy your Azure service cluster extensions for Azure Arc-enabled data services, Azure Container Apps on Azure Arc, and Event Grid on Kubernetes.

- Perform virtual machine lifecycle and management operations on Azure Local and on-premises environments managed by VMware vCenter and System Center Virtual Machine Manager (SCVMM) through interactive and non-interactive methods. Empower developers and application teams to self-serve VM operations on-demand using Azure role-based access control (RBAC).

- A unified experience viewing your Azure Arc-enabled resources, whether you are using the Azure portal, the Azure CLI, Azure PowerShell, or Azure REST API.

Pricing

Below is pricing information for the features available today with Azure Arc.

Azure Arc-enabled servers

The following Azure Arc control plane functionality is offered at no extra cost:

- Resource organization through Azure management groups and tags
- Searching and indexing through Azure Resource Graph
- Access and security through Azure Role-based access control (RBAC)
- Environments and automation through templates and extensions

Any Azure service that is used on Azure Arc-enabled servers, such as Microsoft Defender for Cloud or Azure Monitor, will be charged as per the pricing for that service. For more information, see the Azure pricing page.

Azure Arc-enabled VMware vSphere and System Center Virtual Machine Manager

The following Azure Arc-enabled VMware vSphere and System Center Virtual Machine Manager (SCVMM) capabilities are offered at no extra cost:

- All the Azure Arc control plane functionalities that are offered at no extra cost with Azure Arc-enabled servers.
- Discovery and single pane of glass inventory view of your VMware vCenter and SCVMM managed estate (VMs, templates, networks, datastores, clouds/clusters/hosts/resource pools).

- Lifecycle (create, resize, update, and delete) and power cycle (start, stop, and restart) operations of VMs, including the ability to delegate self-service access for these operations using Azure role-based access control (RBAC).
- Management of VMs using Azure portal, CLI, REST APIs, SDKs, and automation through Infrastructure as Code (IaC) templates such as ARM, Terraform, and Bicep.

Any Azure service that is used on Azure Arc-enabled VMware vSphere and SCVMM VMs, such as Microsoft Defender for Cloud or Azure Monitor, will be charged as per the pricing for that service. For more information, see the Azure pricing page.

Azure Arc-enabled Kubernetes

Any Azure service that is used on Azure Arc-enabled Kubernetes, such as Microsoft Defender for Cloud or Azure Monitor, will be charged as per the pricing for that service.

For more information on pricing for configurations on top of Azure Arc-enabled Kubernetes, see the Azure pricing page.

Azure Arc-enabled data services

For information, see the Azure pricing page.

Azure Arc and the adaptive cloud approach

Azure Arc is a key part of Microsoft's adaptive cloud approach. This approach helps organizations run and manage apps and services across many environments, including Azure, other cloud providers, on-premises datacenters, and edge locations. Azure Arc supports this approach by extending Azure's management, security, and governance tools to resources outside Azure. This ability makes it easier to keep operations consistent and secure, no matter where your workloads run.

Next steps

- Choose the right Azure Arc service for your physical and virtual machines.
- Learn about Azure Arc-enabled servers.
- Learn about Azure Arc-enabled Kubernetes.
- Learn about Azure Arc-enabled data services.
- Learn about SQL Server enabled by Azure Arc.
- Learn about Azure Arc-enabled VM Management on Azure Local.
- Learn about Azure Arc-enabled VMware vSphere.

- Learn about Azure Arc-enabled System Center Virtual Machine Manager.
- Experience Azure Arc by exploring the Azure Arc Jumpstart.
- Learn about best practices and design patterns through the Azure Arc Landing Zone Accelerators.
- Understand network requirements for Azure Arc.

ⓘ **Note:** The author created this article with assistance from AI. Learn more

Choosing the right Azure Arc service for machines

Article • 05/07/2025

Azure Arc offers different services based on your existing IT infrastructure and management needs. Before onboarding your resources to Azure Arc-enabled servers, you should investigate the different Azure Arc offerings to determine which best suits your requirements. Choosing the right Azure Arc service provides the best possible inventorying and management of your resources.

There are several different ways you can connect your existing Windows and Linux machines to Azure Arc:

- Azure Arc-enabled servers
- Azure Arc-enabled VMware vSphere
- Azure Arc-enabled System Center Virtual Machine Manager (SCVMM)
- Azure Local

Each of these services extends the Azure control plane to your existing infrastructure and enables the use of Azure security, governance, and management capabilities using the Connected Machine agent. Other services besides Azure Arc-enabled servers also use an Azure Arc resource bridge, a part of the core Azure Arc platform that provides self-servicing and additional management capabilities.

The following table provides a quick way to see the major capabilities of the Azure Arc services that connect your existing Windows and Linux machines to Azure Arc.

Expand table

_	**Arc-enabled servers**	**Arc-enabled VMware vSphere**	**Arc-enabled SCVMM**	**Azure Local**
Microsoft Defender for Cloud	✓	✓	✓	✓
Microsoft Sentinel	✓	✓	✓	✓
Azure Automation	✓	✓	✓	✓
Azure Update Manager	✓	✓	✓	✓
Change Tracking and Inventory	✓	✓	✓	✓
Azure Monitor	✓	✓	✓	✓

_	Arc-enabled servers	Arc-enabled VMware vSphere	Arc-enabled SCVMM	Azure Local
VM extensions	✓	✓	✓	✓
Extended Security Updates for Windows Server 2012/2012R2 and SQL Server 2012 (11.x)	✓	✓ (free for AVS)	✓	✓
Agentless discovery and inventory		✓	✓	
Lifecycle and powercycle operations (create/delete/start/stop VMs, etc.)		✓	✓	✓
Self-serve VM provisioning		✓	✓	✓
SQL Server enabled by Azure Arc	✓	✓	✓	✓
Windows Server management and pay-as-you-go	✓	✓	✓	✓

General recommendations

General recommendations about the right service to use are as follows:

Expand table

If your machine is a...	...connect to Azure with...
VMware VM (not running on AVS)	Azure Arc-enabled VMware vSphere (to get the complete set of Azure capabilities). Azure Arc-enabled servers (to use Azure services only).
Azure VMware Solution (AVS) VM	Azure Arc-enabled VMware vSphere for Azure VMware Solution
VM managed by System Center Virtual Machine Manager	Azure Arc-enabled SCVMM (to get the complete set of Azure capabilities). Azure Arc-enabled servers (to use Azure services only).
Azure Local machine, including the ones managed by SCVMM	Azure Local
Physical server	Azure Arc-enabled servers
VM on another hypervisor	Azure Arc-enabled servers
VM on another cloud provider	Azure Arc-enabled servers

If you're unsure about which of these services to use, you can start with Azure Arc-enabled servers and add a resource bridge for additional management capabilities later. Azure Arc-enabled servers allows you to connect servers containing all of the types of VMs supported by the other services and provides a wide range of capabilities such as Azure Policy and monitoring, while adding resource bridge can extend additional capabilities.

Region availability also varies between Azure Arc services, so you may need to use Azure Arc-enabled servers if a more specialized version of Azure Arc is unavailable in your preferred region. See Azure Products by Region to learn more about region availability for Azure Arc services.

Where your machine runs determines the best Azure Arc service to use. Organizations with diverse infrastructure may end up using more than one Azure Arc service; this is alright. The core set of features remains the same no matter which Azure Arc service you use.

Azure Arc-enabled servers

Azure Arc-enabled servers lets you manage Windows and Linux physical servers and virtual machines hosted outside of Azure, on your corporate network, or other cloud provider. When connecting your machine to Azure Arc-enabled servers, you can perform various operational functions similar to native Azure virtual machines.

Capabilities

- Govern: Assign Azure Automanage machine configurations to audit settings within the machine. Utilize Azure Policy pricing guide for cost understanding.
- Protect: Safeguard non-Azure servers with Microsoft Defender for Endpoint, integrated through Microsoft Defender for Cloud. This includes threat detection, vulnerability management, and proactive security monitoring. Utilize Microsoft Sentinel for collecting security events and correlating them with other data sources.
- Configure: Employ Azure Automation for managing tasks using PowerShell and Python runbooks. Use Change Tracking and Inventory for assessing configuration changes. Utilize Update Management for handling OS updates. Perform post-deployment configuration and automation tasks using supported Azure Arc-enabled servers VM extensions.
- Monitor: Utilize VM insights for monitoring OS performance and discovering application components. Collect log data, such as performance data and events, through the Log Analytics agent, storing it in a Log Analytics workspace.

- Procure Extended Security Updates (ESUs) at scale for your Windows Server 2012 and 2012R2 machines running on vCenter managed estate.

> **Important**
>
> Azure Arc-enabled VMware vSphere and Azure Arc-enabled SCVMM have all the capabilities of Azure Arc-enabled servers, but also provide specific, additional capabilities.

Azure Arc-enabled VMware vSphere

Azure Arc-enabled VMware vSphere simplifies the management of hybrid IT resources distributed across VMware vSphere and Azure.

Running software in Azure VMware Solution, as a private cloud in Azure, offers some benefits not realized by operating your environment outside of Azure. For software running in a VM, such as SQL Server and Windows Server, running in Azure VMware Solution provides additional value such as free Extended Security Updates (ESUs).

To take advantage of these benefits if you're running in an Azure VMware Solution, it's important to follow respective onboarding processes to fully integrate the experience with the AVS private cloud.

Additionally, when a VM in Azure VMware Solution private cloud is Azure Arc-enabled using a method distinct from the one outlined in the AVS public document, the steps are provided in the document to refresh the integration between the Azure Arc-enabled VMs and Azure VMware Solution.

Capabilities

- Discover your VMware vSphere estate (VMs, templates, networks, datastores, clusters/hosts/resource pools) and register resources with Azure Arc at scale.
- Perform various virtual machine (VM) operations directly from Azure, such as create, resize, delete, and power cycle operations such as start/stop/restart on VMware VMs consistently with Azure.
- Empower developers and application teams to self-serve VM operations on-demand using Azure role-based access control (RBAC).
- Install the Azure Arc-connected machine agent at scale and leverage all the capabilities offered by Azure Arc-enabled servers on VMware VMs.

- Browse your VMware vSphere resources (VMs, templates, networks, and storage) in Azure, providing you with a single pane view for your infrastructure across both environments.
- Build automation and self-service pipelines using Python, Java, JavaScript, and .NET SDKs; Terraform, ARM, Bicep templates; REST APIs, CLI, and PowerShell.

Azure Arc-enabled System Center Virtual Machine Manager (SCVMM)

Azure Arc-enabled System Center Virtual Machine Manager (SCVMM) empowers System Center customers to connect their VMM environment to Azure and perform VM self-service operations from Azure portal.

Azure Arc-enabled System Center Virtual Machine Manager also allows you to manage your hybrid environment consistently and perform self-service VM operations through Azure portal. For Microsoft Azure Pack customers, this solution is intended as an alternative to perform VM self-service operations.

Capabilities

- Discover and onboard existing SCVMM managed VMs to Azure.
- Perform various VM lifecycle operations such as start, stop, pause, and delete VMs on SCVMM managed VMs directly from Azure.
- Empower developers and application teams to self-serve VM operations on demand using Azure role-based access control (RBAC).
- Browse your VMM resources (VMs, templates, VM networks, and storage) in Azure, providing you with a single pane view for your infrastructure across both environments.
- Install the Azure Arc-connected machine agents at scale and leverage all the capabilities offered by Azure Arc-enabled servers on SCVMM VMs.
- Build automation and self-service pipelines using Python, Java, JavaScript, and .NET SDKs; Terraform, ARM, Bicep templates; REST APIs, CLI, and PowerShell.

Azure Local

Azure Local is a hyperconverged infrastructure operating system delivered as an Azure service. This is a hybrid solution that is designed to host virtualized Windows and Linux VM or

containerized workloads and their storage. Azure Local is a hybrid product that is offered on validated hardware and connects on-premises estates to Azure, enabling cloud-based services, monitoring and management. This helps customers manage their infrastructure from Azure and run virtualized workloads on-premises, making it easy for them to consolidate aging infrastructure and connect to Azure.

> ⓘ **Note**
>
> Azure Local comes with Azure resource bridge installed and uses the Azure Arc control plane for infrastructure and workload management, allowing you to monitor, update, and secure your Azure Local infrastructure from the Azure portal.

Capabilities

- Deploy and manage workloads, including VMs and Kubernetes clusters from Azure through the Azure Arc resource bridge.
- Manage VM lifecycle operations such as start, stop, delete from Azure control plane.
- Manage Kubernetes lifecycle operations such as scale, update, upgrade, and delete clusters from Azure control plane.
- Install Azure connected machine agent and Azure Arc-enabled Kubernetes agent on your VM and Kubernetes clusters to use Azure services (i.e., Azure Monitor, Azure Defender for cloud, etc.).
- Leverage Azure Virtual Desktop for Azure Local to deploy session hosts on to your on-premises infrastructure to better meet your performance or data locality requirements.
- Empower developers and application teams to self-serve VM and Kubernetes cluster operations on demand using Azure role-based access control (RBAC).
- Monitor, update, and secure your Azure Local infrastructure and workloads across fleets of locations directly from the Azure portal.
- Deploy and manage static and DHCP-based logical networks on-premises to host your workloads.
- VM image management with Azure Marketplace integration and ability to bring your own images from Azure storage account and cluster shared volumes.
- Create and manage storage paths to store your VM disks and config files.

Switching from Arc-enabled servers to another service

If you currently use Azure Arc-enabled servers, you can get the additional capabilities that come with Arc-enabled VMware vSphere or Arc-enabled SCVMM:

- Enable virtual hardware and VM CRUD capabilities in a VMware machine with Azure Arc agent installed
- Enable virtual hardware and VM CRUD capabilities in an SCVMM machine with Azure Arc agent installed

Custom locations

07/21/2025

As an extension of the Azure location construct, a *custom location* provides a reference as a deployment target that administrators can set up when creating an Azure resource. The custom location feature abstracts the backend infrastructure details from application developers, database admin users, or other users in the organization. These users can then reference the custom location without having to be aware of these details.

Custom locations can be used to enable Azure Arc-enabled Kubernetes clusters as target locations for deploying Azure services instances. Azure offerings that can be deployed on top of custom locations include databases, such as SQL Managed Instance enabled by Azure Arc.

On Arc-enabled Kubernetes clusters, a custom location represents an abstraction of a namespace within the Azure Arc-enabled Kubernetes cluster. Custom locations create the granular RoleBindings and ClusterRoleBindings necessary for other Azure services to access the cluster.

Custom location permissions

Since the custom location is an Azure Resource Manager resource that supports Azure role-based access control (Azure RBAC), an administrator or operator can determine which users have access to create resource instances on:

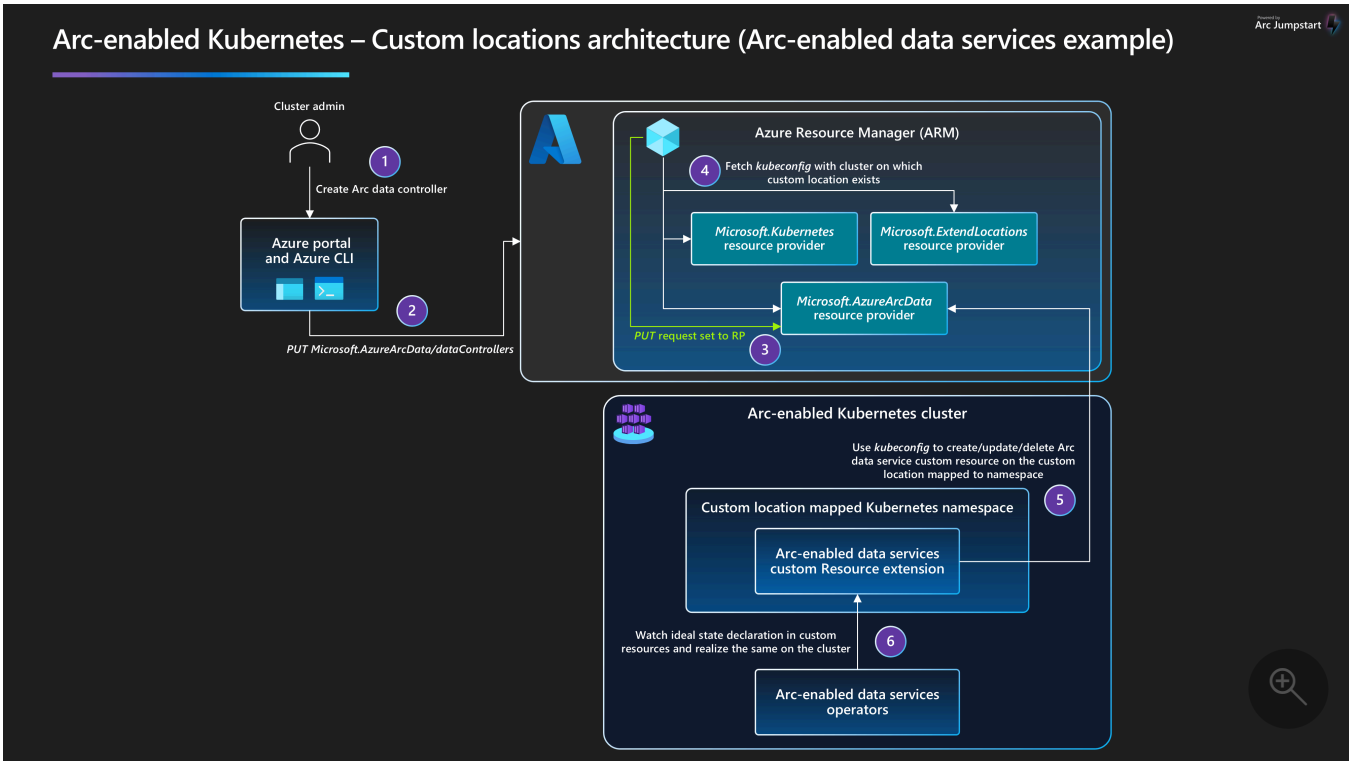
- A namespace within a Kubernetes cluster to target deployment of SQL Managed Instance enabled by Azure Arc.
- The compute, storage, networking, and other vCenter or Azure Local resources to deploy and manage VMs.

For example, a cluster operator could create a custom location **Contoso-Michigan-Healthcare-App** representing a namespace on a Kubernetes cluster in your organization's Michigan Data Center. The operator can assign Azure RBAC permissions to application developers on this custom location so that they can deploy healthcare-related web applications. The developers can then deploy these applications to **Contoso-Michigan-Healthcare-App** without having to know details of the namespace and Kubernetes cluster.

Architecture for Arc-enabled Kubernetes

When an administrator enables the custom locations feature on a cluster, a ClusterRoleBinding is created, authorizing the Microsoft Entra application used by the Custom Locations Resource Provider (RP). Once authorized, the Custom Locations RP can create ClusterRoleBindings or

RoleBindings needed by other Azure RPs to create custom resources on this cluster. The cluster extensions installed on the cluster determine the list of RPs to authorize.



When the user creates a data service instance on the cluster:

1. The **PUT** request is sent to Azure Resource Manager.
2. The **PUT** request is forwarded to the Azure Arc-enabled Data Services RP.
3. The RP fetches the `kubeconfig` file associated with the Azure Arc-enabled Kubernetes cluster, on which the custom location exists.
    - The custom location is referenced as `extendedLocation` in the original PUT request.
4. The Azure Arc-enabled Data Services RP uses the `kubeconfig` to communicate with the cluster to create a custom resource of the Azure Arc-enabled Data Services type on the namespace mapped to the custom location.
    - The Azure Arc-enabled Data Services operator was deployed via cluster extension creation before the custom location existed.
5. The Azure Arc-enabled Data Services operator reads the new custom resource created on the cluster and creates the data controller, translating into realization of the desired state on the cluster.

Next steps

- Use our quickstart to connect a Kubernetes cluster to Azure Arc.
- Learn how to create a custom location on your Azure Arc-enabled Kubernetes cluster.

Access Azure services over Azure Firewall Explicit Proxy (Public Preview)

Article • 04/22/2025

The Azure Firewall Explicit proxy feature can route all Azure Arc traffic securely through your private connection (ExpressRoute or Site-to-Site VPN) to Azure. This feature allows you to use Azure Arc without exposing your on-premises environment to the public internet.

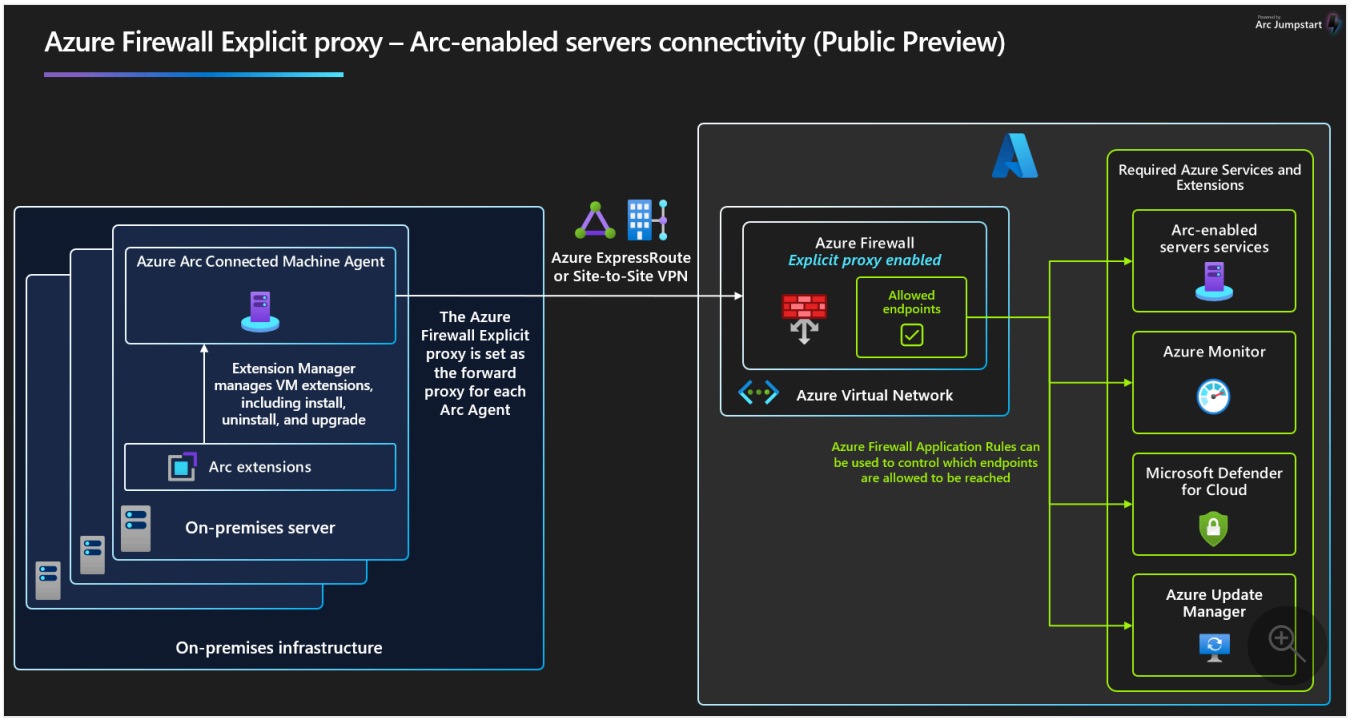
This article explains the steps to configure Azure Firewall with the Explicit Proxy feature as the forward proxy for your Arc-enabled servers or Kubernetes resources.

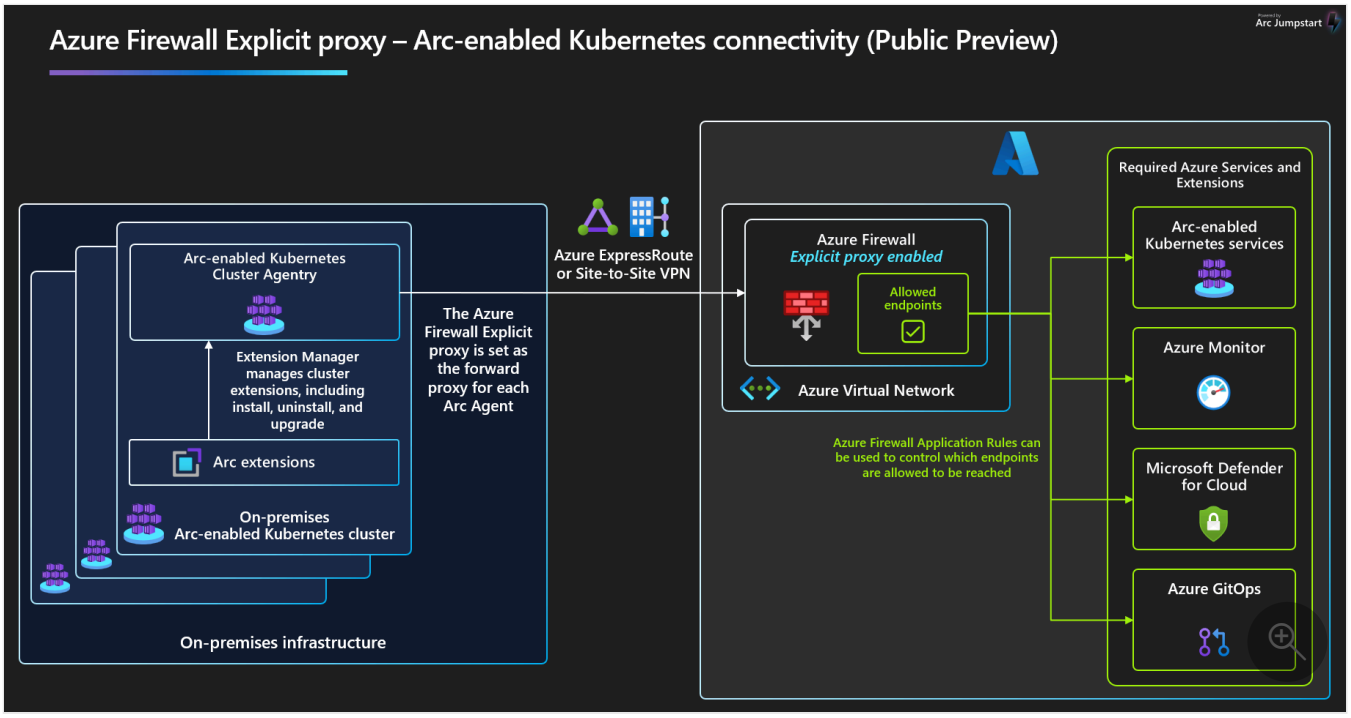
> **Important**
>
> Azure Firewall Explicit proxy is currently in PREVIEW. See the Supplemental Terms of Use for Microsoft Azure Previews for legal terms that apply to Azure features that are in beta, preview, or otherwise not yet released into general availability.

How the Azure Firewall Explicit proxy feature works

Azure Arc agents can use a forward proxy to connect to Azure services. The Azure Firewall Explicit proxy feature enables you to use an Azure Firewall within your virtual network (VNet) as the forward proxy for your Arc agents.

As the Azure Firewall Explicit proxy operates within your private VNet, and you have a secure connection to it via ExpressRoute or Site-to-Site VPN, all Azure Arc traffic can be routed to its intended destination within the Microsoft network, without requiring any public internet access.





To download Arc diagrams in high resolution, visit Jumpstart Gems.

Restrictions and current limitations

- This solution uses Azure Firewall Explicit proxy as a forward proxy. The Explicit proxy feature doesn't support TLS Inspection.
- TLS certificates can't be applied to the Azure Firewall Explicit proxy.
- This solution can't currently be used with Arc gateway for Azure Arc-enabled servers or Arc gateway for Arc-enabled Kubernetes.
- This solution isn't currently supported by Azure Local or Azure Arc VMs running in Azure Local.

Azure Firewall costs

Azure Firewall pricing is based on deployment hours and total data processed. Details on pricing for Azure Firewall can be found on the Azure Firewall Pricing page.

Prerequisites and network requirements

To use this solution, you must have:

- An existing Azure VNet.
- An existing ExpressRoute or site-to-site VPN connection from your on-premises environment to your Azure VNet.

Configure the Azure Firewall

Follow these steps to enable the Explicit proxy feature on your Azure Firewall.

Create the Azure Firewall resource

If you have an existing Azure Firewall in your VNet, you can skip this section. Otherwise, follow these steps to create a new Azure Firewall resource.

1. From your browser, sign in to the Azure portal and navigate to the **Azure Firewalls** page.
2. Select **Create** to create a new firewall.
3. Enter your **Subscription**, **Resource group**, **Name**, and **Region**.
4. For the **Firewall SKU**, select **Standard** or **Premium** .
5. Complete the rest of the **Basics** tab as needed for your configuration.
6. Select **Review + create**, then select **Create** to create the firewall.

For more information, see Deploy and configure Azure Firewall.

Enable the Explicit proxy (preview) feature

1. Navigate to your Azure Firewall resource, then go to the Firewall Policy.
2. In **Settings**, navigate to the **Explicit Proxy (Preview)** pane.
3. Select **Enable Explicit Proxy**.
4. Enter the desired values for the HTTP and HTTPS ports.

> **Note**
>
> It's common to use *8080* for the HTTP Port, and *8443* for the HTTPS port.

5. Select **Apply** to save the changes.

Create an application rule

If you want to create an allowlist for your Azure Firewall Explicit proxy, you can optionally create an application rule to allow communication to the required endpoints for your scenarios.

1. Navigate to the applicable firewall policy.
2. In **Settings**, navigate to the **Application Rules** pane.
3. Select **Add a rule collection**.
4. Provide a **Name** for the rule collection.
5. Set the rule **Priority** based on other rules you may have.
6. Provide a **Name** for the rule.
7. For the **Source**, enter "*", or any source IPs you may have.
8. Set **Protocol** as **http:80,https:443**.
9. Set **Destination** as a comma-separated list of URLs required for your scenario. For details on required URLs, see Azure Arc network requirements.
10. Select **Add** to save the rule collection and rule.

Set your Azure Firewall as the forward proxy

Follow these steps to set your Azure Firewall as the forward proxy for your Arc resources.

Arc-enabled servers

To set your Azure Firewall as the forward proxy while onboarding new Arc servers:

1. Generate the onboarding script.
2. Set **Connectivity Method** as **Proxy Server**, and set the **Proxy Server URL** as `http://<Your Azure Firewall's Private IP>:<Explicit Proxy HTTPS Port>`.
3. Onboard your servers using the script.

To set the forward proxy for existing Arc-enabled servers, run the following command using the local Azure Connected Machine agent CLI:

Azure CLI

```
azcmagent config set proxy.url http://<Your Azure Firewall's Private IP>:<Explicit Proxy HTTPS Port>`
```

Arc-enabled Kubernetes

To set your Azure Firewall as the forward proxy while onboarding new Kubernetes clusters, run the connect command with the `proxy-https` and `proxy-http` parameters specified:

Azure CLI

```
az connectedk8s connect --name <cluster-name> --resource-group <resource-group> --proxy-https http://<Your Azure Firewall's Private IP>:<Explicit Proxy HTTPS Port> --proxy-http http://<Your Azure Firewall's Private IP>:<Explicit Proxy HTTPS Port>
```

To set the forward proxy for existing Arc-enabled Kubernetes clusters, run the following command:

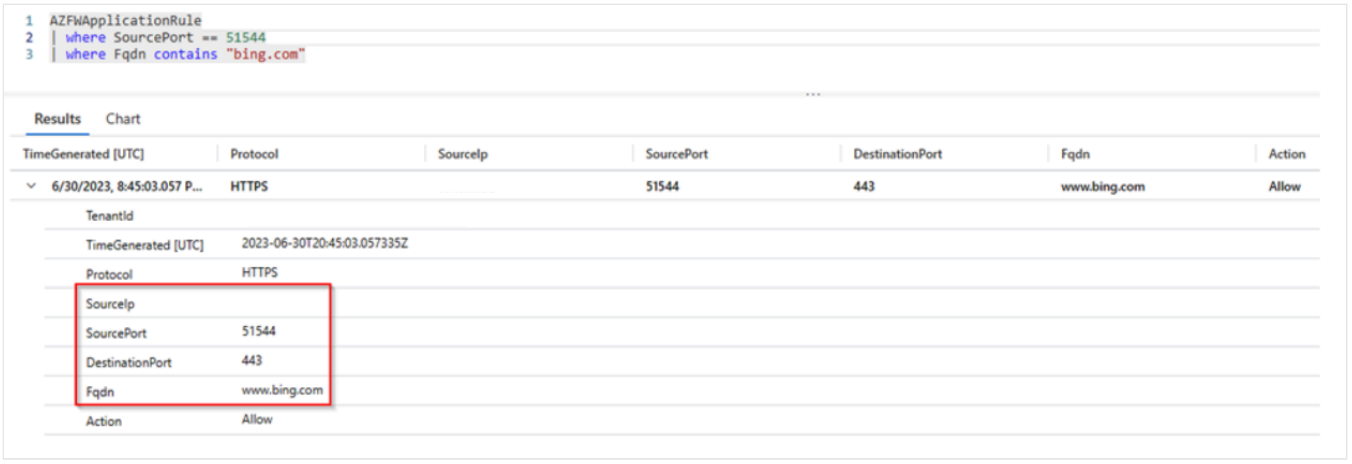
Azure CLI

```
az connectedk8s update --proxy-https http://<Your Azure Firewall's Private IP>:<Explicit Proxy HTTPS Port>
```

Troubleshooting

To verify that traffic is successfully being proxied via your Azure Firewall Explicit Proxy, you should first ensure that the Explicit proxy is accessible and working as expected from your network. To do so, run the following command: `curl -x <proxy IP> <target FQDN>`

Additionally, you can view the Azure Firewall Application rule logs to verify traffic. Explicit proxy relies on Application rules, so all the logs are available in the AZFWApplicationRules table, as shown in this example:



Private Link integration

You can use Azure Firewall Explicit proxy in conjunction with Azure Private Link. To use these solutions together, configure your environment so that traffic to endpoints that don't support Private Link route via the Explicit proxy, while allowing traffic to Azure Arc endpoints that do support Private Link to bypass the Explicit proxy and instead route traffic directly to the relevant private endpoint:

- For Azure Private Link for Arc-enabled servers, use the Proxy Bypass feature.
- For Azure Private Link for Arc-enabled Kubernetes (preview), include Microsoft Entra ID, Azure Resource Manager, Azure Front Door, and Microsoft Container Registry endpoints in your cluster's proxy skip range.

Next steps

- Learn more about Azure Firewall Explicit proxy (preview)
- Read Demystifying Explicit proxy: Enhancing Security with Azure Firewall

Azure Resource Graph sample queries for Azure Arc

05/19/2025

Azure Resource Graph is an Azure service that lets you query at scale, helping you effectively govern your environment. Queries are created using Kusto Query Language (KQL). For more information, see Understanding the Azure Resource Graph query language.

This page provides a list of sample Azure Resource Graph queries for Azure Arc. You can run these queries through Azure PowerShell or Azure CLI, or in the Azure portal using the Resource Graph Explorer. Feel free to modify the queries to suit your needs.

> **Tip**
>
> You can use Microsoft Copilot in Azure to author Azure Resource Graph queries using natural language. For more information, see **Get resource information using Microsoft Copilot in Azure**.

General Arc sample queries

Get enabled resource types for Azure Arc-enabled custom locations

Provides a list of enabled resource types for Azure Arc-enabled custom locations.

Kusto

```
ExtendedLocationResources
| where type == 'microsoft.extendedlocation/customlocations/enabledresourcetypes'
```

Azure CLI

Azure CLI

```
az graph query -q "ExtendedLocationResources | where type ==
'microsoft.extendedlocation/customlocations/enabledresourcetypes'"
```

List Azure Arc-enabled custom locations with VMware or SCVMM enabled

Provides a list of all Azure Arc-enabled custom locations that have either VMware or SCVMM resource types enabled.

Kusto

```
Resources
| where type =~ 'microsoft.extendedlocation/customlocations' and
properties.provisioningState =~ 'succeeded'
| extend clusterExtensionIds=properties.clusterExtensionIds
| mvexpand clusterExtensionIds
| extend clusterExtensionId = tolower(clusterExtensionIds)
| join kind=leftouter(
  ExtendedLocationResources
  | where type =~
'microsoft.extendedlocation/customLocations/enabledResourcetypes'
  | project clusterExtensionId = tolower(properties.clusterExtensionId),
extensionType = tolower(properties.extensionType)
  | where extensionType in~ ('microsoft.scvmm','microsoft.vmware')
) on clusterExtensionId
| where extensionType in~ ('microsoft.scvmm','microsoft.vmware')
| summarize virtualMachineKindsEnabled=make_set(extensionType) by id,name,location
| sort by name asc
```

Azure CLI

Azure CLI

```
az graph query -q "Resources | where type =~
'microsoft.extendedlocation/customlocations' and properties.provisioningState
=~ 'succeeded' | extend clusterExtensionIds=properties.clusterExtensionIds |
mvexpand clusterExtensionIds | extend clusterExtensionId =
tolower(clusterExtensionIds) | join kind=leftouter( ExtendedLocationResources
| where type =~
'microsoft.extendedlocation/customLocations/enabledResourcetypes' | project
clusterExtensionId = tolower(properties.clusterExtensionId), extensionType =
tolower(properties.extensionType) | where extensionType in~
('microsoft.scvmm','microsoft.vmware') ) on clusterExtensionId | where
extensionType in~ ('microsoft.scvmm','microsoft.vmware') | summarize
virtualMachineKindsEnabled=make_set(extensionType) by id,name,location | sort
by name asc"
```

Arc-enabled servers sample queries

Get count and percentage of Arc-enabled servers by domain

This query summarizes the `domainName` property on Azure Arc-enabled servers and uses a calculation with `bin` to create a `Pct` column for the percent of Arc-enabled servers per domain.

Kusto

```
Resources
| where type == 'microsoft.hybridcompute/machines'
| project domain=tostring(properties.domainName)
| summarize Domains=make_list(domain), TotalMachineCount=sum(1)
| mvexpand EachDomain = Domains
| summarize PerDomainMachineCount = count() by tostring(EachDomain),
TotalMachineCount
| extend Pct = 100 * bin(todouble(PerDomainMachineCount) /
todouble(TotalMachineCount), 0.001)
```

Azure CLI

Azure CLI

```
az graph query -q "Resources | where type ==
'microsoft.hybridcompute/machines' | project
domain=tostring(properties.domainName) | summarize Domains=make_list(domain),
TotalMachineCount=sum(1) | mvexpand EachDomain = Domains | summarize
PerDomainMachineCount = count() by tostring(EachDomain), TotalMachineCount |
extend Pct = 100 * bin(todouble(PerDomainMachineCount) /
todouble(TotalMachineCount), 0.001)"
```

List all extensions installed on an Azure Arc-enabled server

First, this query uses `project` on the hybrid machine resource type to get the ID in uppercase (`toupper()`), get the computer name, and the operating system running on the machine. Getting the resource ID in uppercase is a good way to prepare to `join` to another property. Then, the query uses `join` with `kind` as `leftouter` to get extensions by matching an uppercase `substring` of the extension ID. The portion of the ID before `/extensions/<ExtensionName>` is the same format as the hybrid machine ID, so we use this property for the `join`. `summarize` is then used with `make_list` on the name of the virtual machine extension to combine the name of each extension where *ID*, *OSName*, and *ComputerName* are the same into a single array property. Lastly, we order by lowercase *OSName* with `asc`. By default, `order by` is descending.

Kusto

```
Resources
| where type == 'microsoft.hybridcompute/machines'
| project
  id,
  JoinID = toupper(id),
  ComputerName = tostring(properties.osProfile.computerName),
  OSName = tostring(properties.osName)
| join kind=leftouter(
  Resources
  | where type == 'microsoft.hybridcompute/machines/extensions'
  | project
    MachineId = toupper(substring(id, 0, indexof(id, '/extensions'))),
    ExtensionName = name
) on $left.JoinID == $right.MachineId
| summarize Extensions = make_list(ExtensionName) by id, ComputerName, OSName
| order by tolower(OSName) asc
```

Azure CLI

Azure CLI

```
az graph query -q "Resources | where type ==
'microsoft.hybridcompute/machines' | project id, JoinID = toupper(id),
ComputerName = tostring(properties.osProfile.computerName), OSName =
tostring(properties.osName) | join kind=leftouter( Resources | where type ==
'microsoft.hybridcompute/machines/extensions' | project  MachineId =
toupper(substring(id, 0, indexof(id, '/extensions'))),  ExtensionName = name )
on \$left.JoinID == \$right.MachineId | summarize Extensions =
make_list(ExtensionName) by id, ComputerName, OSName | order by
tolower(OSName) asc"
```

List Arc-enabled servers not running latest released agent version

This query returns all Arc-enabled servers running an outdated version of the Connected Machine agent. Agents with a status of **Expired** are excluded from the results. The query uses `leftouter` `join` to bring together the Advisor recommendations raised about any Connected Machine agents identified as out of date, and Hybrid Computer machines to filter out any agent that hasn't communicated with Azure over a period of time.

Kusto

```
AdvisorResources
| where type == 'microsoft.advisor/recommendations'
| where properties.category == 'HighAvailability'
| where properties.shortDescription.solution == 'Upgrade to the latest version of
```

```
the Azure Connected Machine agent'
| project
    id,
    JoinId = toupper(properties.resourceMetadata.resourceId),
    machineName = tostring(properties.impactedValue),
    agentVersion = tostring(properties.extendedProperties.installedVersion),
    expectedVersion = tostring(properties.extendedProperties.latestVersion)
| join kind=leftouter(
  Resources
  | where type == 'microsoft.hybridcompute/machines'
  | project
    machineId = toupper(id),
    status = tostring (properties.status)
  ) on $left.JoinId == $right.machineId
| where status != 'Expired'
| summarize by id, machineName, agentVersion, expectedVersion
| order by tolower(machineName) asc
```

Azure CLI

Azure CLI

```
az graph query -q "AdvisorResources | where type ==
'microsoft.advisor/recommendations' | where properties.category ==
'HighAvailability' | where properties.shortDescription.solution == 'Upgrade to
the latest version of the Azure Connected Machine agent' | project  id,
JoinId = toupper(properties.resourceMetadata.resourceId),  machineName =
tostring(properties.impactedValue),  agentVersion =
tostring(properties.extendedProperties.installedVersion),  expectedVersion =
tostring(properties.extendedProperties.latestVersion) | join kind=leftouter(
Resources | where type == 'microsoft.hybridcompute/machines' | project
machineId = toupper(id),  status = tostring (properties.status) ) on
\$left.JoinId == \$right.machineId | where status != 'Expired' | summarize by
id, machineName, agentVersion, expectedVersion | order by tolower(machineName)
asc"
```

List Arc-enabled servers with SQL Server, PostgreSQL, or MySQL installed

This query returns all Arc-enabled servers that have SQL Server, PostgreSQL, or MySQL installed.

Kusto

```
resources
| where type =~ 'microsoft.hybridcompute/machines'
| extend machineId = tolower(tostring(id)), datacenter =
iif(isnull(tags.Datacenter), '', tags.Datacenter), status =
```

```
tostring(properties.status)
| extend mssqlinstalled =
coalesce(tobool(properties.detectedProperties.mssqldiscovered),false)
| extend pgsqlinstalled =
coalesce(tobool(properties.detectedProperties.pgsqldiscovered),false)
| extend mysqlinstalled =
coalesce(tobool(properties.detectedProperties.mysqldiscovered),false)
| extend osSku = properties.osSku, osName = properties.osName, osVersion =
properties.osVersion
| extend coreCount = tostring(properties.detectedProperties.logicalCoreCount),
totalPhysicalMemoryinGB =
tostring(properties.detectedProperties.totalPhysicalMemoryInGigabytes)
| extend operatingSystem = iif(isnotnull(osSku), osSku, osName)
| where mssqlinstalled or mysqlinstalled or pgsqlinstalled
| project id ,name, type, resourceGroup, subscriptionId, location, kind,
osVersion, status, osSku,coreCount,totalPhysicalMemoryinGB,tags, mssqlinstalled,
mysqlinstalled, pgsqlinstalled
| sort by (tolower(tostring(name))) asc
```

Azure CLI

Azure CLI

```
az graph query -q "resources | where type =~
'microsoft.hybridcompute/machines' | extend machineId = tolower(tostring(id)),
datacenter = iif(isnull(tags.Datacenter), '', tags.Datacenter), status =
tostring(properties.status) | extend mssqlinstalled =
coalesce(tobool(properties.detectedProperties.mssqldiscovered),false) | extend
pgsqlinstalled =
coalesce(tobool(properties.detectedProperties.pgsqldiscovered),false) | extend
mysqlinstalled =
coalesce(tobool(properties.detectedProperties.mysqldiscovered),false) | extend
osSku = properties.osSku, osName = properties.osName, osVersion =
properties.osVersion | extend coreCount =
tostring(properties.detectedProperties.logicalCoreCount),
totalPhysicalMemoryinGB =
tostring(properties.detectedProperties.totalPhysicalMemoryInGigabytes)  |
extend operatingSystem = iif(isnotnull(osSku), osSku, osName) | where
mssqlinstalled or mysqlinstalled or pgsqlinstalled | project id ,name, type,
resourceGroup, subscriptionId, location, kind, osVersion, status,
osSku,coreCount,totalPhysicalMemoryinGB,tags, mssqlinstalled, mysqlinstalled,
pgsqlinstalled | sort by (tolower(tostring(name))) asc"
```

Arc-enabled Kubernetes sample queries

List all Azure Arc-enabled Kubernetes resources

Returns a list of each Azure Arc-enabled Kubernetes cluster and relevant metadata for each cluster.

Kusto

```
Resources
| project id, subscriptionId, location, type, properties.agentVersion,
properties.kubernetesVersion, properties.distribution, properties.infrastructure,
properties.totalNodeCount, properties.totalCoreCount
| where type =~ 'Microsoft.Kubernetes/connectedClusters'
```

Azure CLI

Azure CLI

```
az graph query -q "Resources | project id, subscriptionId, location, type,
properties.agentVersion, properties.kubernetesVersion,
properties.distribution, properties.infrastructure, properties.totalNodeCount,
properties.totalCoreCount | where type =~
'Microsoft.Kubernetes/connectedClusters'"
```

List all Azure Arc-enabled Kubernetes clusters with Azure Monitor extension

Returns the connected cluster ID of each Azure Arc-enabled Kubernetes cluster that has the Azure Monitor extension installed.

Kusto

```
KubernetesConfigurationResources
| where type == 'microsoft.kubernetesconfiguration/extensions'
| where properties.ExtensionType  == 'microsoft.azuremonitor.containers'
| parse id with connectedClusterId
'/providers/Microsoft.KubernetesConfiguration/Extensions' *
| project connectedClusterId
```

Azure CLI

Azure CLI

```
az graph query -q "KubernetesConfigurationResources | where type ==
'microsoft.kubernetesconfiguration/extensions' | where
properties.ExtensionType == 'microsoft.azuremonitor.containers' | parse id
with connectedClusterId
```

```
'/providers/Microsoft.KubernetesConfiguration/Extensions' * | project
connectedClusterId"
```

List all Azure Arc-enabled Kubernetes clusters without Azure Monitor extension

Returns the connected cluster ID of each Azure Arc-enabled Kubernetes cluster that is missing the Azure Monitor extension.

Kusto

```
Resources
| where type =~ 'Microsoft.Kubernetes/connectedClusters' | extend
connectedClusterId = tolower(id) | project connectedClusterId
| join kind = leftouter
  (KubernetesConfigurationResources
  | where type == 'microsoft.kubernetesconfiguration/extensions'
  | where properties.ExtensionType  == 'microsoft.azuremonitor.containers'
  | parse tolower(id) with connectedClusterId
'/providers/microsoft.kubernetesconfiguration/extensions' *
  | project connectedClusterId
)  on connectedClusterId
| where connectedClusterId1 == ''
| project connectedClusterId
```

Azure CLI

Azure CLI

```
az graph query -q "Resources | where type =~
'Microsoft.Kubernetes/connectedClusters' | extend connectedClusterId =
tolower(id) | project connectedClusterId | join kind = leftouter
(KubernetesConfigurationResources | where type ==
'microsoft.kubernetesconfiguration/extensions' | where
properties.ExtensionType == 'microsoft.azuremonitor.containers' | parse
tolower(id) with connectedClusterId
'/providers/microsoft.kubernetesconfiguration/extensions' * | project
connectedClusterId ) on connectedClusterId | where connectedClusterId1 == '' |
project connectedClusterId"
```

List all clusters that contain a Flux configuration

Returns the `connectedCluster` and `managedCluster` IDs for clusters that contain at least one `fluxConfiguration`.

Kusto

```
resources
| where type =~ 'Microsoft.Kubernetes/connectedClusters' or type =~
'Microsoft.ContainerService/managedClusters' | extend clusterId = tolower(id) |
project clusterId
| join
( kubernetesconfigurationresources
| where type == 'microsoft.kubernetesconfiguration/fluxconfigurations'
| parse tolower(id) with clusterId
'/providers/microsoft.kubernetesconfiguration/fluxconfigurations' *
| project clusterId
) on clusterId
| project clusterId
```

Azure CLI

Azure CLI

```
az graph query -q "resources | where type =~
'Microsoft.Kubernetes/connectedClusters' or type =~
'Microsoft.ContainerService/managedClusters' | extend clusterId = tolower(id)
| project clusterId | join ( kubernetesconfigurationresources | where type ==
'microsoft.kubernetesconfiguration/fluxconfigurations' | parse tolower(id)
with clusterId
'/providers/microsoft.kubernetesconfiguration/fluxconfigurations' * | project
clusterId ) on clusterId | project clusterId"
```

List all Flux configurations in a noncompliant state

Returns the `fluxConfiguration` IDs of configurations that are failing to sync resources on the cluster.

Kusto

```
kubernetesconfigurationresources
| where type == 'microsoft.kubernetesconfiguration/fluxconfigurations'
| where properties.complianceState == 'Non-Compliant'
| project id
```

Azure CLI

Azure CLI

```
az graph query -q "kubernetesconfigurationresources | where type ==
'microsoft.kubernetesconfiguration/fluxconfigurations' | where
properties.complianceState == 'Non-Compliant' | project id"
```

Next steps

- Learn more about the query language.
- Learn more about how to explore resources.

What is Azure Arc resource bridge?

08/09/2025

Azure Arc resource bridge is a prepackaged virtual appliance that runs as a Kubernetes-based management cluster deployed on your on-premises infrastructure (private cloud). It acts as a core component of the Azure Arc private cloud products and enables Azure-based management of on-premises resources. Azure Arc resource bridge provides a secure conduit between Azure and your on-premises infrastructure. It allows projection of on-premises resources into Azure as native Azure resources, enabling consistent governance, automation, and management with Azure tools. The resource bridge facilitates self-service provisioning and lifecycle management of on-premises Windows and Linux virtual machines directly from Azure.

Azure Arc resource bridge integrates with the following private cloud platforms:

- Azure Local (via Azure Arc VM management)
- VMware (via Azure Arc-enabled VMware vSphere)
- System Center Virtual Machine Manager (via Azure Arc-enabled SCVMM)

Once deployed in your private cloud, the resource bridge is granted credentials to the local virtualization infrastructure, allowing it to project on-premises resources into Azure as Arc-enabled resources. This projection enables consistent management and automation using Azure tools, such as Azure Policy, and Azure CLI.

Arc resource bridge enables the following hybrid management capabilities:

- **Native Azure experience**: Projects on-premises VMs as Azure resources, allowing you to view on-premises VMs in Azure and apply tags, policies, and extensions just like native Azure VMs.
- **VM self-service from Azure**: Create, manage, and delete VMs on-premises through the Azure portal or CLI.
- **Native Azure integration**: Extend Azure governance, monitoring, and automation capabilities to on-premises VMs.

Overview

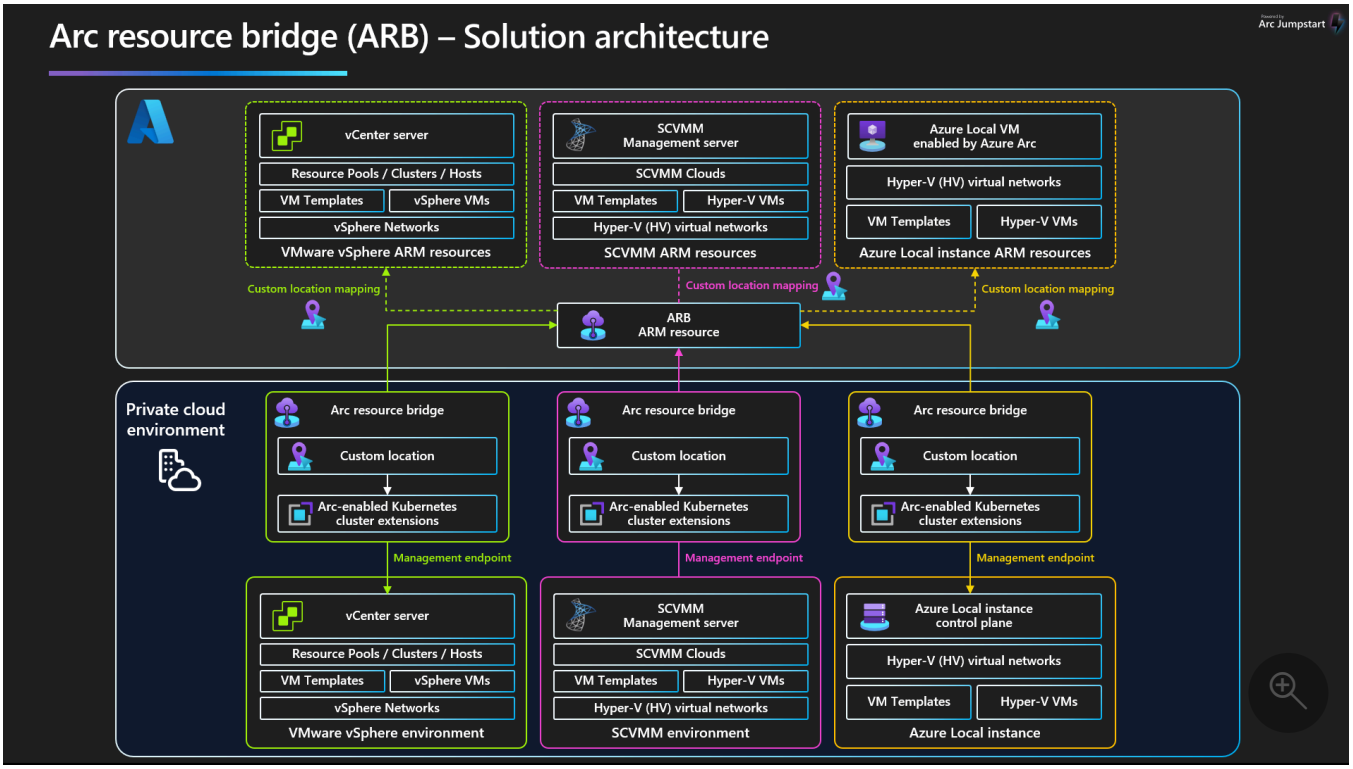
Azure Arc resource bridge is a key component that allows Azure to manage on-premises private cloud infrastructure. Supported private clouds are VMware vSphere, SCVMM, and Azure Local. It acts as a local appliance VM that connects your private cloud to Azure, enabling Azure to project and manage your on-premises resources as if they were native cloud assets.

To deliver this functionality, the resource bridge hosts additional Azure Arc components, including:

- **Custom location** – These define the target infrastructure for deployments. The custom location maps to your private cloud infrastructure. When you create a VM from Azure, you choose a custom location. Azure knows where to route the request and what private cloud location it maps to based on the custom location. For example, for Arc-enabled VMware, the custom location maps to an instance of vCenter. For Azure Local, it maps to an Azure Local instance. For more information about custom location, refer to Create and manage custom locations.

- **Cluster extension** – A cluster extension enables capabilities on the resource bridge. The supported extensions are Arc-enabled VMware (microsoft.vmware), Arc-enabled AVS (microsoft.avs), Arc-enabled SCVMM (microsoft.scvmm), Azure Local (microsoft.azstackhci.operator, microsoft.diagnosis.operator) and AKS Arc (microsoft.hybridaksoperator).

- **Azure Arc agents** – Power the communication and control layer between Azure and your infrastructure.



To download architecture diagrams in high resolution, visit Jumpstart Gems.

Custom locations and cluster extensions are both Azure resources linked to the Azure Arc resource bridge resource in Azure Resource Manager. When you create a VM from Azure, you select the custom location. Azure uses the custom location to determine the mapping to your private cloud infrastructure and routes the create VM request to your private cloud. A VM is created in your private cloud and a corresponding Azure resource is created in Azure as a

representation of your on-premises VM in Azure. Azure Arc resource bridge enables this hybrid management of your on-premises resources from Azure.

Some VM creation inputs vary based on the private cloud:

- For VMware, you must specify the resource pool, network, and VM template.
- For Azure Local, you provide the custom location, network, and template.

The custom location, infrastructure and VM resources in Azure are *projections* of your on-premises environment. If an underlying on-premises resource becomes unhealthy, this status may be reflected in its corresponding Azure resource.

Azure Arc resource bridge enables this projection and acts as the control plane that enables Azure to manage your private cloud infrastructure. If the resource bridge becomes unavailable or unhealthy, Azure may lose visibility or management capabilities of your on-premises resources. However, your on-premises resources, such as VMs running in vCenter, Azure Local or SCVMM, should not be affected and should continue to remain operational.

Azure Arc resource bridge requires ongoing operational maintenance. Maintenance tasks include updating the private cloud credentials, monitoring the appliance health and ensuring the appliance stays within the supported versions. Microsoft may offer cloud-managed upgrades to assist in maintenance, but this does not replace the need for regular manual upgrades every 6 months.

Benefits of Azure Arc resource bridge

Azure Arc resource bridge enables you to manage on-premises Windows and Linux virtual machines directly from Azure. Depending on the supported private cloud, you may be able to perform the following VM management operations:

- Provision and delete VMs from Azure portal or CLI
- Start, stop, and restart VMs
- Control access using Azure RBAC and apply Azure tags
- Add, remove or update networking, disks, and VM size (CPU cores and memory)
- Enable guest management
- Install supported Azure Arc VM extensions (Ex: Azure Monitor, Azure Policy)

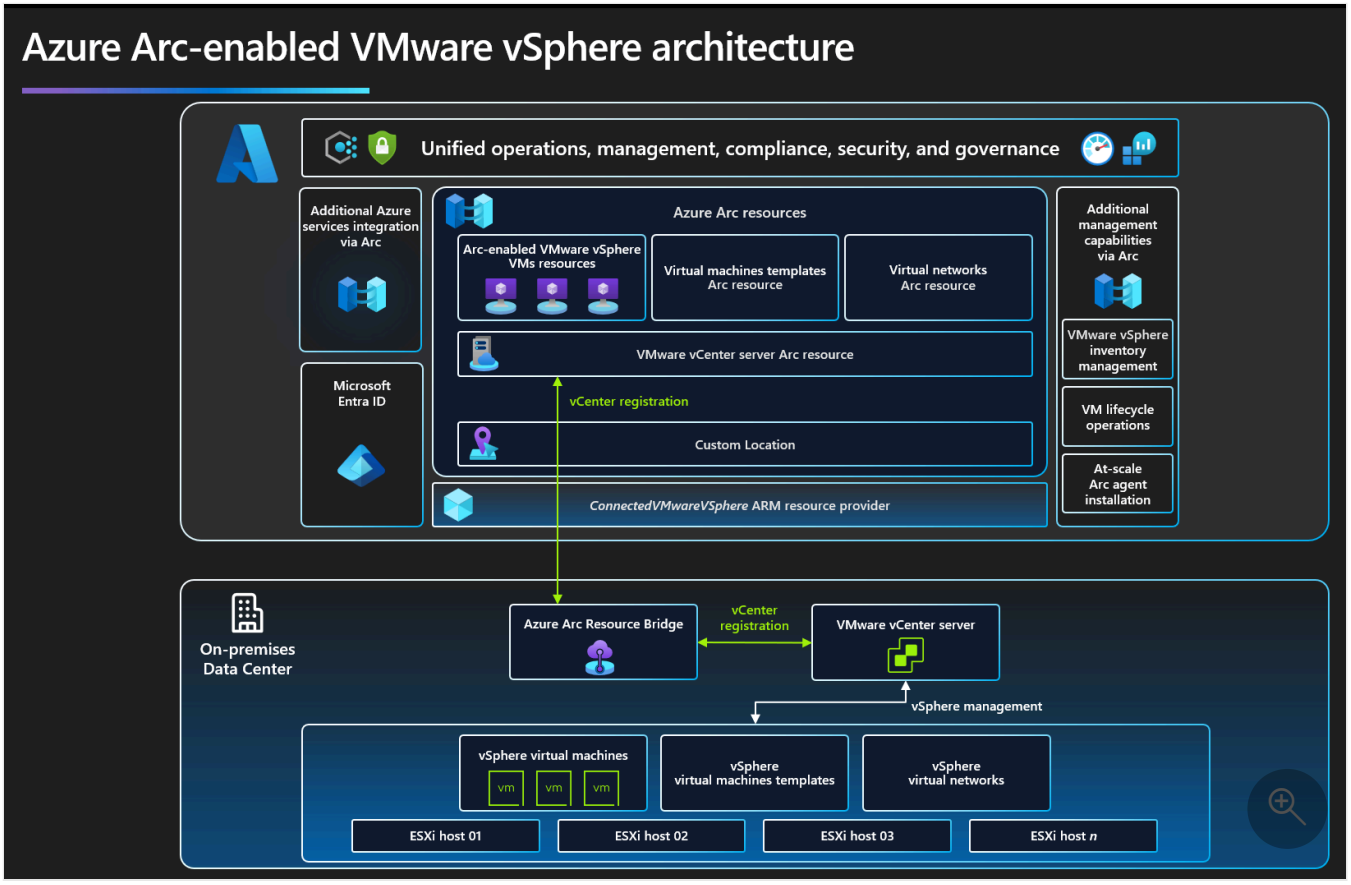
Example scenarios

These examples show how Azure Arc resource bridge enables hybrid management of on-premises environments from Azure.

Apply Azure Policy and other Azure services to on-premises VMware VMs

A customer deploys the Arc resource bridge into their on-premises VMware vSphere environment. The resource bridge connects to their vCenter instance. Visibility and management of VMware virtual machines in Azure are scoped to specific resource pools, networks, and VM templates defined during deployment.

From Azure portal, the customer selects the VMware virtual machines and enables Azure Arc. The Arc-enabled virtual machines can now be managed alongside native Azure VMs. The customer can enable Azure services, such as Defender for Cloud and Azure Policy, to their on-premises VMware workloads. This enables consistent security and compliance enforcement across both cloud and on-premises environments, with centralized policy management through Azure.



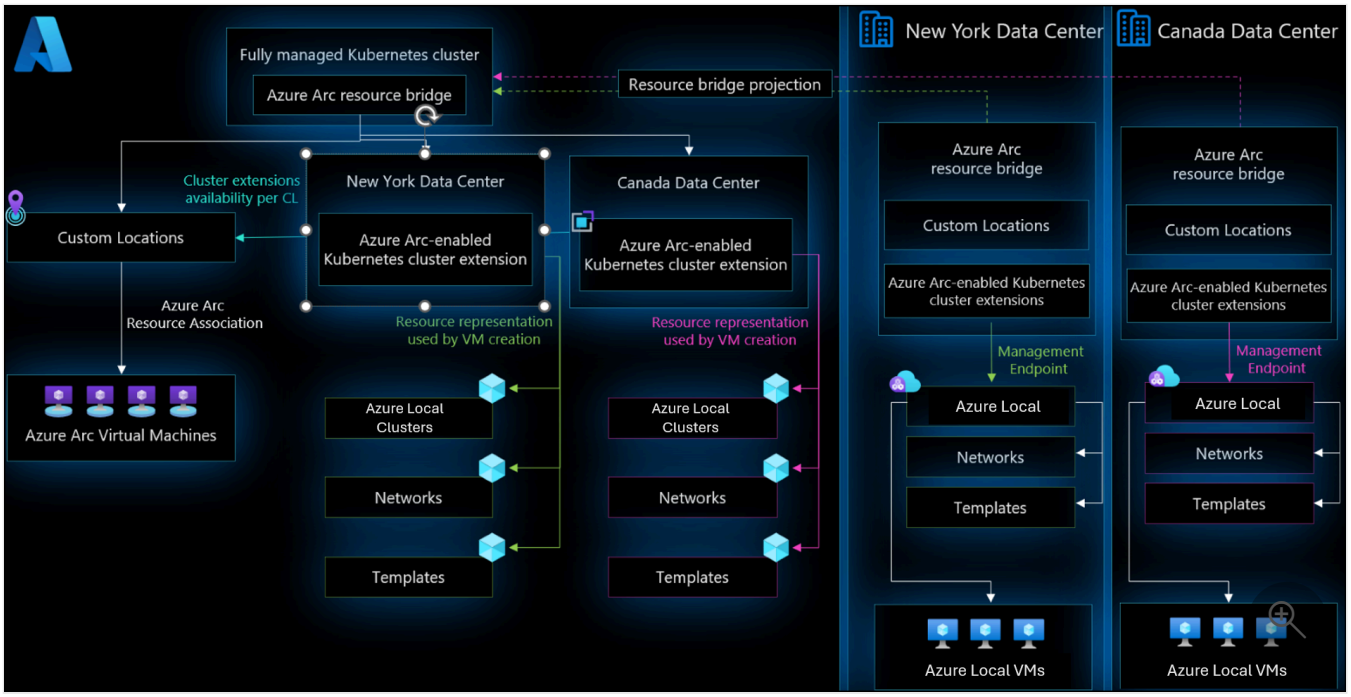
Create physical Azure Local VMs on-premises from Azure

A customer has multiple datacenter locations in Canada and New York. They deploy Arc resource bridge in each datacenter and enable Azure Arc VM management of their Azure Local

VMs in Azure. They can then sign into Azure portal and see all their Arc-enabled VMs from the two physical locations in one central view from Azure portal. From Azure portal, they can:

- View and manage all Arc-enabled VMs across both datacenters
- Centrally create new VMs in either datacenter from Azure portal

Each new VM is provisioned on-premises in the selected location but appears in Azure portal as an Arc-enabled VM. This setup enables centralized VM management across multiple physical sites all from within Azure.



Version and region support

Supported regions

To use an Azure Arc-enabled private cloud in a specific region, both Azure Arc resource bridge and the Arc-enabled private cloud must be supported in that region. For example, to use Azure-Arc enabled VMware in East US, both Arc resource bridge and Arc-enabled VMware must be available in East US. To confirm region availability for an Arc-enabled private cloud, review the corresponding onboarding documentation. There could be instances where Arc resource bridge is available in a region but the private cloud isn't yet available.

Arc resource bridge supports the following Azure regions:

- East US
- East US 2

- West US 2
- West US 3
- Central US
- North Central US
- South Central US
- US Gov Virginia
- Canada Central
- Australia East
- Australia SouthEast
- West Europe
- North Europe
- UK South
- UK West
- Sweden Central
- Italy North
- Japan East
- Southeast Asia
- East Asia
- Central India

Regional resiliency

While Azure includes redundancy across all levels of its infrastructure, the Azure Arc resource bridge does not currently support cross-region failover or other resiliency capabilities. If a service-impacting event occurs and the resource bridge becomes unavailable, your on-premises VMs will continue to run without interruption. However, management capabilities from Azure will be temporarily unavailable until the service is restored.

Private cloud environments

The following private clouds and their versions are officially supported for Arc resource bridge:

- VMware vSphere version 7.0, 8.0
- Azure Local
- SCVMM

Supported versions

We generally recommend keeping your Arc resource bridge on a version released within the last 6 months or within the latest n-3 versions, whichever is more recent. This ensures your appliance benefits from the latest features, security updates, and refreshed internal components such as certificates. While the support policy includes the latest version and the three preceding versions (n-3), you must still upgrade at least once every 6 months, even if your current version is technically within the supported range. This is critical to maintain system health and compatibility. To estimate your last upgrade date, check your appliance version and its corresponding release date. For version release news, please refer to Arc resource bridge release notes

Private link support

Arc resource bridge currently doesn't support private link.

Next steps

- Learn how Azure Arc-enabled VMware vSphere extends Azure's governance and management capabilities to VMware vSphere infrastructure.
- Learn how Azure Arc-enabled SCVMM extends Azure's governance and management capabilities to System Center managed infrastructure.
- Learn about provisioning and managing on-premises Windows and Linux VMs running on Azure Local instances.
- Review the system requirements for deploying and managing Arc resource bridge.

What's new with Azure Arc resource bridge

To stay up to date with the most recent developments, this article provides you with information about recent releases of the Arc resource bridge Azure CLI extension, `az arcappliance`.

The version support policy for Arc resource bridge generally covers version(s) released within the last 6 months or within the latest n-3 versions, **whichever is more recent**. Even if a version is within the version support policy (n-3), the appliance should be manually upgraded at least once every six months. This is to ensure the internal components and certificates are refreshed. You can check your appliance version and the version release date for an estimate on the last upgrade date. When a patch version is released, the upgrade path might skip the minor version and directly upgrade to the patch version. In such cases, the supported versions (n-3) exclude the skipped minor version and include the patch version instead.

Version 1.7.0 (Dec 2025)

- Support version: n
- Appliance: 1.7.0
- CLI extension: 1.7.0
- Kubernetes: 1.32.6
- Mariner: 3.0.20251030

Arc resource bridge platform

- Update the network proxy settings with new command: `az arcappliance configuration proxy update`. This command requires a resource bridge deployed or upgraded to 1.7.0. This command is only supported for Azure Local and VMware. If an ARB upgrade fails due to incorrect or out-of-date network proxy settings, you can run a proxy update to fix the values. If a proxy update operation fails, you must retry and have it succeed before performing any other operation, including retrying upgrade.
- New CLI command to show the local resource bridge configuration: `az arcappliance configuration show`. For ARM configuration, continue to use: `az arcappliance show`.
- Configuration setting overlaps with Service CIDR (10.96.0.0/12) will now be blocked from deployment.
- Return error for VMware credentials that contain an invalid character (single quote)
- New user management key is downloaded with the `az arcappliance get-credentials` CLI command. This key is used for network proxy settings update. This key is only downloaded for resource bridges on version 1.7.0.

- The `--config-file` argument is now optional for the `az arcappliance create` command. If it is not provided, please pass these other arguments: `--name ,--resource-group, --location`.
- The `--config-file` argument is now optional for the `az arcappliance delete` command. If it is not provided, please pass these other arguments based on private cloud type: Azure Local: `--name, --resource-group` VMware: `--name, --resource-group, --datacenter, --datastore, --folder` SCVMM: `--name, --resource-group`
- The `--config-file` argument is now optional for the `az arcappliance upgrade` command. If it is not provided, please pass these other arguments: `--name, --resource-group, --kubeconfig`. The kubeconfig can be retrieved using the CLI command `az arcappliance get-credentials`. This is only supported for Azure Local and VMware.

Version 1.6.0 (Sept 2025)

- Support version: n-1
- Appliance: 1.6.0
- CLI extension: 1.6.0
- Kubernetes: 1.31.5
- Mariner: 3.0.20250402

Arc resource bridge platform

- [PREVIEW] Node Identity feature added
- Enabled managed identity at the appliance VM layer
- [PREVIEW] Arc Gateway feature added for Arc-enabled VMware
- KVAIO cleanup and optimizations for cloud login or RBAC failures
- Improvements to Validate, CreateConfig, and error messages
- Pass network profile even when proxy is not enabled
- Bump Kubernetes SDK to 1.32.0.1

Version 1.5.0 (June 2025)

- Support version: n-2
- Appliance: 1.5.0
- CLI extension: 1.5.0
- Kubernetes: 1.30.4
- Mariner: 3.0.20250402

Arc resource bridge platform

- Cloud logs collection feature added: Enables automatic log collection and upload to cloud on deployment failure
- Prevent non-essential debug file operations from blocking critical functionality
- ARB container image signed and removed old unsigned cached images
- Added validation to prevent network overlaps with the K8s Pod CIDR 10.244.0.0/16
- Added validation to warn for network overlaps with the K8s Service CIDR 10.96.0.0/12
- Added validation to prevent the usage of Proxy URLs ending in .local.
- Addressed bug in vSphere Cluster Client Set command creating conflicts.
- Downloadsdk dyanmic parts - reducing the number of concurrent downloads with each retry.
- Added kms-plugin token rotation to credential rotation

Version 1.4.1 (February 2025)

- Support version: past 6 months, unsupported
- Appliance: 1.4.0
- CLI extension: 1.4.0
- Kubernetes: 1.30.4
- Mariner: 3.0.20250102

Bug fixes

- fix for compatibility with Azure CLI v2.70.0. From this version forward, Azure CLI version needs to be 2.70.0 or higher.

> **Note**
>
> This patch version of the Azure CLI extension `az arcappliance` doesn't change the appliance version. Therefore, `az arcappliance` CLI extension 1.4.1 and 1.4.0 both have the same appliance version, 1.4.0.

Version 1.4.0 (February 2025)

- Support version: past 6 months, unsupported

- Appliance: 1.4.0
- CLI extension: 1.4.0
- Kubernetes: 1.30.4
- Mariner: 3.0.20250102

Arc-enabled SCVMM

- Validate command - Add custom time-outs

Arc resource bridge platform

- Enhanced telemetry for error type categorization
- Support for US Gov Virginia/Fairfax region

Version 1.3.1 (December 2024)

> **Note**
>
> This `az arcappliance` Azure CLI extension requires Azure CLI v2.69.0 or below. It isn't compatible with Azure CLI v2.70.0 or higher.

- Appliance: 1.3.1
- CLI extension: 1.3.1
- Kubernetes: 1.29.4
- Mariner: 2.0.20241029

Arc-enabled SCVMM

- CreateConfig CLI command - Improve prompt messages, reorder Library Share input prompt
- CreateConfig CLI command - Display Library Share, Cloud Names, and IP Pools inputs in alphabetical order
- Image Provisioning from remote machine - Decompress Vhdx disk space error message improvement
- Add retry and error message improvement for SCVMM createClient
- Validate VLAN ID check error message improvement
- Add TSG link in error message - validate checks, prep-createclient, createVM

Arc resource bridge platform

- Error category framework update

Bug fixes

- Azure Stack HCI CVE fix

Version 1.3.0 (October 2024)

- Support version: skipped, upgrades go directly to patch version 1.3.1
- Appliance: 1.3.0
- CLI extension: 1.3.0
- SFS release: 0.1.34.10926
- Kubernetes: 1.29.4
- Mariner: 2.0.20240609

Arc-enabled SCVMM

- Validation - fail if user isn't part of an Admin User Group like DomainAdmins
- Conditional Validation on Gateway IP for SCVMM IP Pool Scenario and sshkeygen removal
- Silently clean appliance VM resources like HW profiles, ISO Files, and VM templates in delete command
- CAPVMM update to 1.1.19
- SCVMM Image Provisioning Decompress Mariner Vhdx disk space error message improvement
- SCVMM appliance deployment failing in Deploy due to IPPool missing access to HG

Arc-enabled VMware vSphere

- Remove root folder privilege validations from vSphere
- extra validations on the canary image

Arc resource bridge platform

- New error additional info field to add more context to errors
- Add ACR image pull test suite
- Add time-out for API Server Endpoint
- Added DNSError category

Bug fixes

- CVE fixes

Version 1.2.0 (July 2024)

- Appliance: 1.2.0
- CLI extension: 1.2.0
- SFS release: 0.1.32.10710
- Kubernetes: 1.28.5
- Mariner: 2.0.20240609

Arc-enabled SCVMM

- `CreateConfig`: Improve prompt messages and reorder networking prompts for the custom IP range scenario
- `CreateConfig`: Validate Gateway IP input against specified IP range for the custom IP range scenario
- `CreateConfig`: Add validation to check infra configuration capability for HA VM deployment. If HA isn't supported, reprompt users to proceed with standalone VM deployment

Arc-enabled VMware vSphere

- Improve prompt messages in createconfig for VMware
- Validate proxy scheme and check for required `no_proxy` entries

Features

- Reject double commas (`,,`) in `no_proxy` string
- Add default folder to createconfig list
- Add conditional Fairfax URLs for US Gov Virginia support
- Add new error codes

Bug fixes

- Fix for openSSH CVE-2024-63870

Version 1.1.1 (April 2024)

- Appliance: 1.1.1
- CLI extension: 1.1.1
- SFS release: 0.1.26.10327
- Kubernetes: 1.27.3
- Mariner: 2.0.20240301

Arc-enabled SCVMM

- Add quotes for resource names

Azure Stack HCI

- HCI auto rotation logic on upgrade

Features

- Updated log collection with describe nodes
- Error message enhancement for failure to reach Arc resource bridge VM
- Improve troubleshoot command error handling with scoped access key
- Longer time-out for individual pod pulls
- Updated `execute` command to allow passing in a kubeconfig
- Catch `<>` in no_proxy string
- Add validation to see if connections from the client machine are proxied
- Diagnostic checker enhancement - Add default gateway and dns servers check to telemetry mode
- Log collection enhancement

Bug fixes

- HCI MOC image client fix to set storage container on catalog

Version 1.1.0 (April 2024)

- Appliance: 1.1.0
- CLI extension: 1.1.0
- SFS release: 0.1.25.10229
- Kubernetes: 1.27.3
- Mariner: 2.0.20240223

Arc-enabled SCVMM

- Use same `vmnetwork` key for HG and Cloud (`vmnetworkid`)
- SCVMM - Add fallback for VMM IP pool with support for IP range in appliance network, add `--vlanid` parameter to accept `vlanid`
- Non-interactive mode for SCVMM `troubleshoot` and `logs` commands
- `Createconfig` command uses styled text to warn about saving config files instead of standard logger
- Improved handling and error reporting for time-outs while provisioning/deprovisioning images from the cloud fabric
- Verify template and snapshot health after provisioning an image, and clean up files associated to the template on image deprovision failures
- Missing VHD state handing in SCVMM
- SCVMM `validate` and `createconfig` fixes

Arc-enabled VMware vSphere

- SSD storage validations added to VMware vSphere in telemetry mode to check if the ESXi host backing the resource pool has any SSD-backed storage
- Improve missing privilege error message, and show some privileges in error message
- Validate host ESXi version and provide a concrete error message for placement profile
- Improve message for no datacenters found, and display default folder
- Surface VMware error when finder fails during validate
- Verify template health and fix it during image provision

Features

- `deploy` command - diagnostic checker enhancements that add retries with exponential backoff to proxy client calls
- `deploy` command - diagnostic checker enhancement: adds storage performance checker in telemetry mode to evaluate the storage performance of the VM used to deploy the appliance
- `deploy` command - Add time-out for SSH connection: New error message: "Error: Timeout occurred due to management machine being unable to reach the appliance VM IP, 192.168.0.11. Ensure that the requirements are met: `https://aka.ms/arb-machine-reqs: dial tcp 192.168.0.11:22: connect: connection timed out`"
- `validate` command - The appliance deployment now fails if Proxy Connectivity and No Proxy checks report any errors

Bug fixes

- SCVMM ValueError fix - fallback option for VMM IP Pools with support for Custom IP Range based Appliance Network

Version 1.0.18 (February 2024)

- Appliance: 1.0.18
- CLI extension: 1.0.3
- SFS release: 0.1.24.10201
- Kubernetes: 1.26.6
- Mariner: 2.0.20240123

Fabric/Private cloud provider

- SCVMM `createconfig` command improvements - retry until valid Port and FQDN provided
- SCVMM and VMware - Validate control plane IP address; add reprompts
- SCVMM and VMware - extend `deploy` command time-out from 30 to 120 minutes

Features

- `deploy` command - diagnostic checker enhancement: proxy checks in telemetry mode

Product

- Reduction in CPU requests
- ETCD preflight check enhancements for upgrade

Bug fixes

- Fix for clusters impacted by the `node-ip` being set as `kube-vip` IP issue
- Fix for SCVMM cred rotation with the same credentials

Version 1.0.17 (December 2023)

- Appliance: 1.0.17
- CLI extension: 1.0.2
- SFS release: 0.1.22.11107

- Kubernetes: 1.26.6
- Mariner: 2.0.20231106

Fabric/Private cloud provider

- SCVMM `createconfig` command improvements
- Azure Local - extend `deploy` command time-out from 30 to 120 minutes
- All private clouds - enable provider credential parameters to be passed in each command
- All private clouds - basic validations for select `createconfig` command inputs
- VMware - basic reprompts for select `createconfig` command inputs

Features

- `deploy` command - diagnostic checker enhancement - improve `context` error messages

Bug fixes

- Fix for `context` error always being returned as `Deploying`

Known bugs

- Arc resource bridge upgrade shows appliance version as upgraded, but status shows upgrade failed

Version 1.0.16 (November 2023)

- Appliance: 1.0.16
- CLI extension: 1.0.1
- SFS release: 0.1.21.11013
- Kubernetes: 1.25.7
- Mariner: 2.0.20231004

Fabric/Private cloud provider

- SCVMM image provisioning and upgrade fixes
- VMware vSphere - use full inventory path for networks
- VMware vSphere error improvement for denied permission
- Azure Stack HCI - enable default storage container

Features

- `deploy` command - diagnostic checker enhancement - add `azurearcfork8s.azurecr.io` URL

Bug fixes

- vSphere credential issue
- Don't set storage container for non-`arc-appliance` catalog image provision requests
- Monitoring agent not installed issue

Version 1.0.15 (September 2023)

- Appliance: 1.0.15
- CLI extension: 1.0.0
- SFS release: 0.1.20.10830
- Kubernetes: 1.25.7
- Mariner: 2.0.20230823

Fabric/Infrastructure

- `az arcappliance` CLI commands now only support static IP deployments for VMware and SCVMM
- For test purposes only, Arc resource bridge on Azure Stack HCI may be deployed with DHCP configuration
- Support for using canonical region names
- Removal of VMware vSphere 6.7 fabric support (vSphere 7 and 8 are both supported)

Features

- (new) `get-upgrades` command- fetches the new upgrade edge available for a current appliance cluster
- (new) `upgrade` command - upgrades the appliance to the next available version (not available for SCVMM)
- (update) `deploy` command - In addition to `deploy`, this command now also calls `create` command. `Create` command is now optional.
- (new) `get-credentials` command - now allows fetching of SSH keys and kubeconfig, which are needed to run the `logs` command from a different machine than the one used to deploy Arc resource bridge

- Allowing usage of `config-file` parameter for `get-credentials` command (new)
  Troubleshoot command - help debug live-site issues by running allowed actions directly on the appliance using a JIT access key

Bug fix

- IPClaim premature deletion issue vSphere static IP

Next steps

- Learn more about Arc resource bridge.
- Learn how to upgrade Arc resource bridge.

Last updated on 12/18/2025

Azure Arc resource bridge system requirements

Article • 05/12/2025

This article describes the system requirements for deploying Azure Arc resource bridge.

Arc resource bridge is used with other partner products, such as Azure Local, Arc-enabled VMware vSphere, and Arc-enabled System Center Virtual Machine Manager (SCVMM). These products may have additional requirements.

Required Azure permissions

- To onboard Arc resource bridge, you must have the Contributor role for the resource group.
- To read, modify, and delete Arc resource bridge, you must have the Contributor role for the resource group.

Management tool requirements

Azure CLI is required to deploy the Azure Arc resource bridge on supported private cloud environments.

If deploying Arc resource bridge on VMware, Azure CLI 64-bit is required to be installed on the management machine to run the deployment commands.

If deploying on Azure Local, then Azure CLI 32-bit should be installed on the management machine.

The Arc appliance CLI extension, `arcappliance`, needs to be installed by running this command: `az extension add --name arcappliance`

Minimum resource requirements

Arc resource bridge has the following minimum resource requirements:

- 200 GB disk space
- 4 vCPUs
- 8 GB memory
- supported storage configuration - hybrid storage (flash and HDD) or all-flash storage (SSDs or NVMe)

These minimum requirements enable most scenarios for products that use Arc resource bridge. Review the product's documentation for specific resource requirements. Failure to provide sufficient resources may cause errors during deployment or upgrade.

IP address prefix (subnet) requirements

The IP address prefix (subnet) where Arc resource bridge will be deployed requires a minimum prefix of /29. The IP address prefix must have enough available IP addresses for the gateway IP, control plane IP, appliance VM IP, and reserved appliance VM IP. Arc resource bridge only uses the IP addresses assigned to the IP pool range (Start IP, End IP) and the Control Plane IP. We recommend that the End IP immediately follow the Start IP. Ex: Start IP = 192.168.0.2, End IP = 192.168.0.3. Work with your network engineer to ensure that there is an available subnet with the required available IP addresses and IP address prefix for Arc resource bridge.

The IP address prefix is the subnet's IP address range for the virtual network and subnet mask (IP Mask) in CIDR notation, for example `192.168.7.1/29`. You provide the IP address prefix (in CIDR notation) during the creation of the configuration files for Arc resource bridge.

Consult your network engineer to obtain the IP address prefix in CIDR notation. An IP Subnet CIDR calculator may be used to obtain this value.

Static IP configuration

If deploying Arc resource bridge to a production environment, static configuration must be used when deploying Arc resource bridge. Static IP configuration is used to assign three static IPs (that are in the same subnet) to the Arc resource bridge control plane, appliance VM, and reserved appliance VM.

DHCP is only supported in a test environment for testing purposes only for VM management on Azure Local. It should not be used in a production environment. DHCP isn't supported on any other Arc-enabled private cloud, including Arc-enabled VMware, Arc for AVS, or Arc-enabled SCVMM.

If using DHCP, you must reserve the IP addresses used by the control plane and appliance VM. In addition, these IPs must be outside of the assignable DHCP range of IPs. Ex: The control plane IP should be treated as a reserved/static IP that no other machine on the network will use or receive from DHCP. If the control plane IP or appliance VM IP changes, this impacts the resource bridge availability and functionality.

Management machine requirements

The machine used to run the commands to deploy and maintain Arc resource bridge is called the *management machine*.

Management machine requirements:

- Azure CLI x64 installed
- Communication to Control Plane IP (SSH TCP port 22, Kubernetes API port 6443)
- Communication to Appliance VM IPs (SSH TCP port 22, Kubernetes API port 6443)
- Communication to the reserved Appliance VM IPs (SSH TCP port 22, Kubernetes API port 6443)
- communication over port 443 to the private cloud management console (ex: VMware vCenter machine)
- Internal and external DNS resolution. The DNS server must resolve internal names, such as the vCenter endpoint for vSphere or cloud agent service endpoint for Azure Local. The DNS server must also be able to resolve external addresses that are required URLs for deployment.
- Internet access

Appliance VM IP address requirements

Arc resource bridge consists of an appliance VM that is deployed on-premises. The appliance VM has visibility into the on-premises infrastructure and can tag on-premises resources (guest management) for projection into Azure Resource Manager (ARM). The appliance VM is assigned an IP address from the `k8snodeippoolstart` parameter in the `createconfig` command. It may be referred to in partner products as Start Range IP, RB IP Start or VM IP 1. The appliance VM IP is the starting IP address for the appliance VM IP pool range, and this IP is initially assigned to your appliance VM when you first deploy Arc resource bridge. The VM IP pool range requires a minimum of 2 IP addresses.

Appliance VM IP address requirements:

- Communication with the management machine (SSH TCP port 22, Kubernetes API port 6443).
- Communication with the private cloud management endpoint via Port 443 (such as VMware vCenter).
- Internet connectivity to required URLs enabled in proxy/firewall.
- Static IP assigned and within the IP address prefix.
- Internal and external DNS resolution.

- If using a proxy, the proxy server has to be reachable from this IP and all IPs within the VM IP pool.

Reserved appliance VM IP requirements

Arc resource bridge reserves an additional IP address to be used for the appliance VM upgrade. The reserved appliance VM IP is assigned an IP address via the `k8snodeippoolend` parameter in the `az arcappliance createconfig` command. This IP address may be referred to as End Range IP, RB IP End, or VM IP 2. The reserved appliance VM IP is the ending IP address for the appliance VM IP pool range. When your appliance VM is upgraded for the first time, the reserved appliance VM IP is assigned to your appliance VM post-upgrade, and the initial appliance VM IP is returned to the IP pool to be used for a future upgrade. If specifying an IP pool range larger than two IP addresses, the additional IPs are reserved.

Reserved appliance VM IP requirements:

- Communication with the management machine (SSH TCP port 22, Kubernetes API port 6443).
- Communication with the private cloud management endpoint via Port 443 (such as VMware vCenter).
- Internet connectivity to required URLs enabled in proxy/firewall.
- Static IP assigned and within the IP address prefix.
- Internal and external DNS resolution.
- If using a proxy, the proxy server has to be reachable from this IP and all IPs within the VM IP pool.

Control plane IP requirements

The appliance VM hosts a management Kubernetes cluster with a control plane that requires a single, static IP address. This IP is assigned from the `controlplaneendpoint` parameter in the `createconfig` command or equivalent configuration files creation command.

Control plane IP requirements:

- Communication with the management machine (SSH TCP port 22, Kubernetes API port 6443).
- Static IP address assigned and within the IP address prefix.
- If using a proxy, the proxy server has to be reachable from IPs within the IP address prefix, including the reserved appliance VM IP.

DNS server

DNS servers must have internal and external endpoint resolution. The appliance VM and control plane need to resolve the management machine and vice versa. All three IPs must be able to reach the required URLs for deployment.

Gateway

The gateway IP is the IP of the gateway for the network where Arc resource bridge is deployed. The gateway IP should be an IP from within the subnet designated in the IP address prefix.

Example minimum configuration for static IP deployment

The following example shows valid configuration values that can be passed during configuration file creation for Arc resource bridge.

Notice that the IP addresses for the gateway, control plane, appliance VM and DNS server (for internal resolution) are within the IP address prefix. The VM IP Pool Start/End are sequential. This key detail helps ensure successful deployment of the appliance VM.

IP Address Prefix (CIDR format): 192.168.0.0/29

Gateway IP: 192.168.0.1

VM IP Pool Start (IP format): 192.168.0.2

VM IP Pool End (IP format): 192.168.0.3

Control Plane IP: 192.168.0.4

DNS servers (IP list format): 192.168.0.1, 10.0.0.5, 10.0.0.6

User account and credentials

Arc resource bridge may require a dedicated user account with the necessary roles to view and manage resources in the on-premises private cloud. If so, during creation of the configuration files, the `username` and `password` parameters are required. The account credentials are then stored as a secret within the appliance VM.

> ⚠ **Warning**

> Arc resource bridge can only use a user account that does not have multifactor authentication enabled. If the user account is set to periodically change passwords, **the credentials must be immediately updated on the resource bridge**. This user account can also be set with a lockout policy to protect the on-premises infrastructure, in case the credentials aren't updated and the resource bridge makes multiple attempts to use expired credentials to access the on-premises control center.

For example, with Arc-enabled VMware, Arc resource bridge needs a dedicated user account for vCenter with the necessary roles. If the credentials for the user account change, then the credentials stored in Arc resource bridge must be immediately updated by running `az arcappliance update-infracredentials` from the management machine. Otherwise, the appliance makes repeated attempts to use the expired credentials to access vCenter, which can result in a lockout of the account.

Internal Certificates

Arc resource bridge contains internal certificates that are required to maintain secure communication to Azure and verify internal components. These certificates require that Arc resource bridge remain online and maintain a persistent connection to Azure. If Arc resource bridge is offline for greater than 45 days, there is a risk that the certificate will expire, requiring a redeployment as the certificate is irrecoverable. Arc resource bridge also requires an upgrade once every six months to ensure that internal certificates are refreshed. If Arc resource bridge is unable to upgrade and the certificates expire, then a redeployment is required. Please review the Maintenance page for important information to maintain your Arc resource bridge.

Configuration files

Arc resource bridge consists of an appliance VM that is deployed in the on-premises infrastructure. To maintain the appliance VM, the configuration files generated during deployment must be saved in a secure location and available on the management machine.

There are several different types of configuration files, based on the on-premises infrastructure.

Appliance configuration files

Three configuration files are created when deploying the Arc resource bridge: `<appliance-name>-resource.yaml`, `<appliance-name>-appliance.yaml` and `<appliance-name>-infra.yaml`.

By default, these files are generated in the current CLI directory of where the deployment commands are run. These files should be saved on the management machine because they're

required for maintaining the appliance VM. The configuration files reference each other and should be stored in the same location.

The az arcappliance CLI commands that rely on the YAML configuration files are 'az arcappliance delete' to delete the Arc resource bridge and its Azure backend associations, and 'az arcappliance upgrade' to manually upgrade the Arc resource bridge.

Kubeconfig

The appliance VM hosts a management Kubernetes cluster. The kubeconfig is a low-privilege Kubernetes configuration file that is used to maintain the appliance VM. By default, it's generated in the current CLI directory when the `deploy` command completes. The kubeconfig should be saved in a secure location on the management machine, because it's required for maintaining the appliance VM. If the kubeconfig is lost, it can be retrieved by running the `az arcappliance get-credentials` command.

> **ⓘ Important**
>
> Once the Arc resource bridge VM is created, the configuration settings can't be modified or updated. Currently, the appliance VM must stay in the location where it was initially deployed. The Arc resource bridge VM name is a unique GUID that can't be renamed, because it's an identifier used for cloud-managed upgrade.

Next steps

- Understand network requirements for Azure Arc resource bridge.
- Review the Azure Arc resource bridge overview to understand more about features and benefits.
- Learn about security configuration and considerations for Azure Arc resource bridge.

Azure Arc resource bridge network requirements

07/23/2025

This article describes the networking requirements for deploying Azure Arc resource bridge in your enterprise.

General network requirements

The lowest network bandwidth validated for deployment of Arc resource bridge is 100 mbps. If your network bandwidth is slower, you may experience problems with deployment.

Arc resource bridge communicates outbound securely to Azure Arc over TCP port 443. If the appliance needs to connect through a firewall or proxy server to communicate over the internet, it communicates outbound using the HTTPS protocol.

Generally, connectivity requirements include these principles:

- All connections are TCP unless otherwise specified.
- All HTTP connections use HTTPS and SSL/TLS with officially signed and verifiable certificates.
- All connections are outbound unless otherwise specified.

To use a proxy, verify that the agents and the machine performing the onboarding process meet the network requirements in this article.

Outbound connectivity requirements

The firewall and proxy URLs below must be allowlisted in order to enable communication from the management machine, Arc resource bridge VM (initially deployed), Arc resource bridge VM 2 (upgrade creates a new VM using a different VM IP), and Control Plane IP to the required Arc resource bridge URLs.

> **ⓘ Important**
>
> When onboarding Arc Resource Bridge, you must provide two IP addresses for the appliance VMs. These are specified as either:
>
> - A range of IPs
> - Two individual IPs (one for each VM)

To ensure successful upgrades, all appliance VM IPs must have outbound access to the required URLs. Make sure these URLs are allowlisted in your network.

Firewall/Proxy URL allowlist

Expand table

Service	Port	URL	Direction	Notes
SFS API endpoint	443	`msk8s.api.cdp.microsoft.com`	Management machine & Appliance VM IPs need outbound connection.	Download product catalog, product bits, and OS images from SFS.
Resource bridge (appliance) image download	443	`msk8s.sb.tlu.dl.delivery.mp.microsoft.com`	Management machine & Appliance VM IPs need outbound connection.	Download the Arc Resource Bridge OS images.
Microsoft Container Registry	443	`mcr.microsoft.com`	Management machine & Appliance VM IPs need outbound connection.	Discover container images for Arc Resource Bridge.
Microsoft Container Registry	443	`*.data.mcr.microsoft.com`	Management machine & Appliance VM IPs need outbound connection.	Download container images for Arc Resource Bridge.
Windows NTP Server	123	`time.windows.com`	Management machine & Appliance VM IPs (if Hyper-V default is Windows NTP) need outbound connection on UDP	OS time sync in appliance VM & Management machine (Windows NTP).

Service	Port	URL	Direction	Notes
Azure Resource Manager	443	`management.azure.com`	Management machine & Appliance VM IPs need outbound connection.	Manage resources in Azure.
Microsoft Graph	443	`graph.microsoft.com`	Management machine & Appliance VM IPs need outbound connection.	Required for Azure RBAC.
Azure Resource Manager	443	`login.microsoftonline.com`	Management machine & Appliance VM IPs need outbound connection.	Required to update ARM tokens.
Azure Resource Manager	443	`*.login.microsoft.com`	Management machine & Appliance VM IPs need outbound connection.	Required to update ARM tokens.
Azure Resource Manager	443	`login.windows.net`	Management machine & Appliance VM IPs need outbound connection.	Required to update ARM tokens.
Resource bridge (appliance) Dataplane service	443	`*.dp.prod.appliances.azure.com`	Appliance VMs IP need outbound connection.	Communicate with resource provider in Azure.
Resource bridge (appliance) container image download	443	`*.blob.core.windows.net, ecpacr.azurecr.io`	Appliance VM IPs need outbound connection.	Required to pull container images.

Service	Port	URL	Direction	Notes
Managed Identity	443	`*.his.arc.azure.com`	Appliance VM IPs need outbound connection.	Required to pull system-assigned Managed Identity certificates.
Azure Arc for Kubernetes container image download	443	`azurearcfork8s.azurecr.io`	Appliance VM IPs need outbound connection.	Pull container images.
ADHS telemetry service	443	`adhs.events.data.microsoft.com`	Appliance VM IPs need outbound connection.	Periodically sends Microsoft required diagnostic data from appliance VM.
Microsoft events data service	443	`v20.events.data.microsoft.com`	Appliance VM IPs need outbound connection.	Send diagnostic data from Windows.
Log collection for Arc Resource Bridge	443	`linuxgeneva-microsoft.azurecr.io`	Appliance VM IPs need outbound connection.	Push logs for Appliance managed components.
Resource bridge components download	443	`kvamanagementoperator.azurecr.io`	Appliance VM IPs need outbound connection.	Pull artifacts for Appliance managed components.
Microsoft open source packages manager	443	`packages.microsoft.com`	Appliance VM IPs need outbound connection.	Download Linux installation package.
Custom Location	443	`sts.windows.net`	Appliance VM IPs need outbound connection.	Required for Custom Location.
Azure Arc	443	`guestnotificationservice.azure.com`	Appliance VM IPs need	Required for Azure Arc.

Service	Port	URL	Direction	Notes
			outbound connection.	
Diagnostic data	443	`gcs.prod.monitoring.core.windows.net`	Appliance VM IPs need outbound connection.	Periodically sends Microsoft required diagnostic data.
Diagnostic data	443	`*.prod.microsoftmetrics.com`	Appliance VM IPs need outbound connection.	Periodically sends Microsoft required diagnostic data.
Diagnostic data	443	`*.prod.hot.ingest.monitor.core.windows.net`	Appliance VM IPs need outbound connection.	Periodically sends Microsoft required diagnostic data.
Diagnostic data	443	`*.prod.warm.ingest.monitor.core.windows.net`	Appliance VM IPs need outbound connection.	Periodically sends Microsoft required diagnostic data.
Azure portal	443	`*.arc.azure.net`	Appliance VM IPs need outbound connection.	Manage cluster from Azure portal.
Azure CLI	443	`*.blob.core.windows.net`	Management machine needs outbound connection.	Download Azure CLI Installer.
Arc Extension	443	`*.web.core.windows.net`	Management machine needs outbound connection.	Download Arc resource bridge extension.
Azure Arc Agent	443	`*.dp.kubernetesconfiguration.azure.com`	Management machine needs	Dataplane used for Arc agent.

Service	Port	URL	Direction	Notes
			outbound connection.	
Python package	443	`pypi.org`, `*.pypi.org`	Management machine needs outbound connection.	Validate Kubernetes and Python versions.
Azure CLI	443	`pythonhosted.org`, `*.pythonhosted.org`	Management machine needs outbound connection.	Python packages for Azure CLI installation.

Inbound connectivity requirements

Communication between the following ports must be allowed from the management machine, Appliance VM IPs, and Control Plane IPs. Ensure these ports are open and that traffic is not being routed through a proxy to facilitate the deployment and maintenance of Arc resource bridge.

> **Important**
>
> During onboarding, you must provide two IP addresses for the Arc Resource Bridge appliance VMs — either as a range or as two individual IPs. For successful deployment, operations, and upgrades:
>
> - Ensure communication is allowed between the management machine, appliance VM IPs, and control plane IPs over the required ports as listed below.
> - Do not route traffic through a proxy for these connections.

Expand table

Service	Port	IP/machine	Direction	Notes
SSH	22	`appliance VM IPs` and `Management machine`	Bidirectional	Management machine connects outbound to the appliance VM IPs. Appliance VM IPs must allow inbound connections.
Kubernetes API server	6443	`appliance VM IPs` and `Management machine`	Bidirectional	Management machine connects outbound to the appliance VM

Service	Port	IP/machine	Direction	Notes
				IPs. Appliance VM IPs must allow inbound connections.
SSH	22	`control plane IP` and `Management machine`	Bidirectional	Used for deploying and maintaining the appliance VM.
Kubernetes API server	6443	`control plane IP` and `Management machine`	Bidirectional	Management of the appliance VM.
HTTPS	443	`private cloud control plane address` and `Management machine`	Management machine needs outbound connection.	Communication with private cloud (ex: VMware vCenter address and vSphere datastore).
Kubernetes API server	6443, 2379, 2380, 10250, 10257, 10259	`appliance VM IPs` (to each other)	Bidirectional	Required for appliance VM upgrade. Ensure all appliance VM IPs have outbound connectivity to each other over these ports.
HTTPS	443	`private cloud control plane address` and `appliance VM IPs`	appliance VM IPs need outbound connection.	Communication with private cloud (ex: VMware vCenter address and vSphere datastore).

> **Note**
>
> The URLs listed here are required for Arc resource bridge only. Other Arc products (such as Arc-enabled VMware vSphere) may have additional required URLs. For details, see Azure Arc network requirements.

Designated IP ranges for Arc resource bridge

When deploying Arc resource bridge, specific IP ranges are reserved exclusively for the Kubernetes pods and services within the appliance VM. These internal IP ranges must not overlap with any configuration inputs for the resource bridge, such as IP address prefix, control plane IP, appliance VM IPs, DNS servers, proxy servers, or vSphere ESXi hosts. For details on the Arc resource bridge configuration, refer to the system requirements.

> **Note**

These designated IP ranges are only used internally within the Arc resource bridge. They don't affect Azure resources or networks.

Expand table

Service	Designated IP range
Arc resource bridge Kubernetes pods	10.244.0.0/16
Arc resource bridge Kubernetes services	10.96.0.0/12

SSL proxy configuration

Important

Arc Resource Bridge supports only direct (explicit) proxies, including unauthenticated proxies, proxies with basic authentication, SSL terminating proxies, and SSL passthrough proxies.

If using a proxy, the Arc Resource Bridge must be configured to use the proxy in order to connect to Azure services.

- To configure the Arc resource bridge with proxy, provide the proxy certificate file path during creation of the configuration files.
- The format of the certificate file is *Base-64 encoded X.509 (.CER)*.
- Only pass the single proxy certificate. If a certificate bundle is passed, the deployment will fail.
- The proxy server endpoint can't be a `.local` domain.
- The proxy server has to be reachable from all IPs within the IP address prefix, including the control plane and appliance VM IPs.

There are only two certificates that should be relevant when deploying the Arc resource bridge behind an SSL proxy:

- SSL certificate for your SSL proxy (so that the management machine and appliance VM trust your proxy FQDN and can establish an SSL connection to it)
- SSL certificate of the Microsoft download servers. This certificate must be trusted by your proxy server itself, as the proxy is the one establishing the final connection and needs to

trust the endpoint. Non-Windows machines may not trust this second certificate by default, so you may need to ensure that it's trusted.

In order to deploy Arc resource bridge, images need to be downloaded to the management machine and then uploaded to the on-premises private cloud gallery. If your proxy server throttles download speed, you may not be able to download the required images (~3.5 GB) within the allotted time (90 min).

Exclusion list for no proxy

If a proxy server is being used, the following table contains the list of addresses that should be excluded from proxy by configuring the `noProxy` settings.

Expand table

IP Address	Reason for exclusion
localhost, 127.0.0.1	Localhost traffic
.svc	Internal Kubernetes service traffic (.svc) where *.svc* represents a wildcard name. This is similar to saying *.svc, but none is used in this schema.
10.0.0.0/8	private network address space
172.16.0.0/12	Private network address space - Kubernetes Service CIDR
192.168.0.0/16	Private network address space - Kubernetes Pod CIDR
.contoso.com	You may want to exempt your enterprise namespace (.contoso.com) from being directed through the proxy. To exclude all addresses in a domain, you must add the domain to the `noProxy` list. Use a leading period rather than a wildcard (*) character. In the sample, the addresses `.contoso.com` excludes addresses `prefix1.contoso.com`, `prefix2.contoso.com`, and so on.

The default value for `noProxy` is `localhost,127.0.0.1,.svc,10.0.0.0/8,172.16.0.0/12,192.168.0.0/16`. While these default values will work for many networks, you may need to add more subnet ranges and/or names to the exemption list. For example, you may want to exempt your enterprise namespace (.contoso.com) from being directed through the proxy. You can achieve that by specifying the values in the `noProxy` list.

Important

When listing multiple addresses for the `noProxy` settings, don't add a space after each comma to separate the addresses. The addresses must immediately follow the commas.

Internal port listening

Be aware that the appliance VM is configured to listen on the following ports. These ports are used exclusively for internal processes and do not require external access:

- 8443 – Endpoint for Microsoft Entra Authentication Webhook
- 10257 – Endpoint for Arc resource bridge metrics
- 10250 – Endpoint for Arc resource bridge metrics
- 2382 – Endpoint for Arc resource bridge metrics

Next steps

- Review the Azure Arc resource bridge overview to understand more about requirements and technical details.
- Learn about security configuration and considerations for Azure Arc resource bridge.
- View troubleshooting tips for networking issues.

Azure Arc resource bridge security overview

Article • 09/20/2024

This article describes the security configuration and considerations you should evaluate before deploying Azure Arc resource bridge in your enterprise.

Managed identity

By default, a Microsoft Entra system-assigned managed identity is created and assigned to the Azure Arc resource bridge. Azure Arc resource bridge currently supports only a system-assigned identity. The `clusteridentityoperator` identity initiates the first outbound communication and fetches the Managed Service Identity (MSI) certificate used by other agents for communication with Azure.

Identity and access control

Azure Arc resource bridge is represented as a resource in a resource group inside an Azure subscription. Access to this resource is controlled by standard Azure role-based access control. From the **Access Control (IAM)** page in the Azure portal, you can verify who has access to your Azure Arc resource bridge.

Users and applications who are granted the Contributor or Administrator role to the resource group can make changes to the resource bridge, including deploying or deleting cluster extensions.

Data residency

Azure Arc resource bridge follows data residency regulations specific to each region. If applicable, data is backed up in a secondary pair region in accordance with data residency regulations. Otherwise, data resides only in that specific region. Data isn't stored or processed across different geographies.

Data encryption at rest

Azure Arc resource bridge stores resource information in Azure Cosmos DB. As described in Data encryption in Azure Cosmos DB, all the data is encrypted at rest.

Security audit logs

The activity log is an Azure platform log that provides insight into subscription-level events. This includes tracking when the Azure Arc resource bridge is modified, deleted, or added.

You can view the activity log in the Azure portal or retrieve entries with PowerShell and Azure CLI. By default, activity log events are retained for 90 days and then deleted.

Next steps

- Understand system requirements and network requirements for Azure Arc resource bridge.
- Review the Azure Arc resource bridge overview to understand more about features and benefits.
- Learn more about Azure Arc.

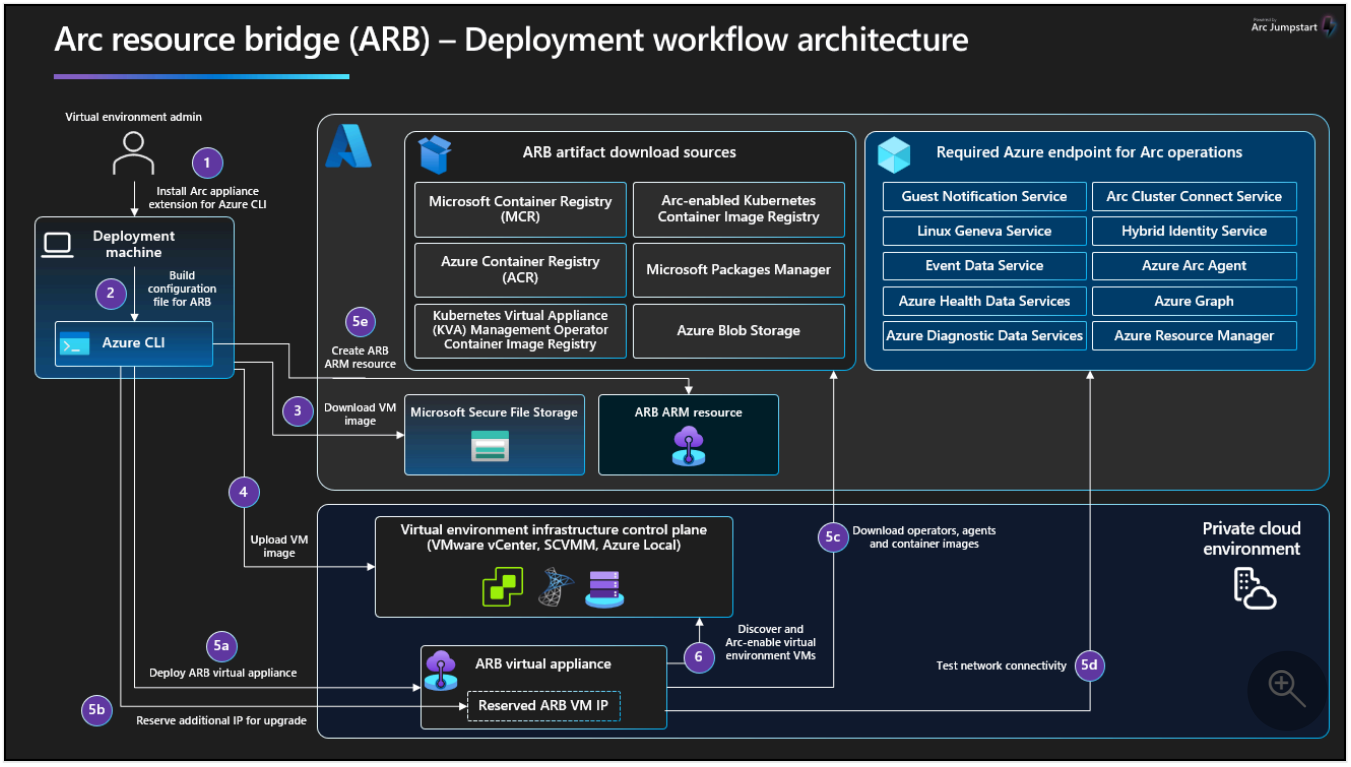
Feedback

Azure Arc resource bridge deployment command overview

Article • 04/23/2025

Azure CLI is required to deploy the Azure Arc resource bridge. When you deploy Arc resource bridge with a corresponding partner product, Azure CLI commands may be combined into an automation script, along with additional provider-specific commands.

The following diagram illustrates the deployment architecture for Arc resource bridge.



To download Arc diagrams in high resolution, visit Jumpstart Gems.

To learn about installing Arc resource bridge with a corresponding partner product, see:

- Connect VMware vCenter Server to Azure with Arc resource bridge
- Connect System Center Virtual Machine Manager (SCVMM) to Azure with Arc resource bridge
- Azure Arc VM Management on Azure Local through Arc resource bridge

This article provides an overview of the Azure CLI commands that are used to manage Arc resource bridge deployment, in the order in which they're typically used for deployment.

`az arcappliance createconfig`

This command creates the configuration files used by Arc resource bridge. Credentials that are provided during `createconfig`, such as vCenter credentials for VMware vSphere, are stored in a configuration file and locally within Arc resource bridge. These credentials should be a separate user account used only by Arc resource bridge, with permission to view, create, delete, and manage on-premises resources. If the credentials change, then the credentials on the resource bridge should be updated.

The `createconfig` command features two modes: interactive and non-interactive. Interactive mode provides helpful prompts that explain the parameter and what to pass. To initiate interactive mode, pass only the three required parameters. Non-interactive mode allows you to pass all the parameters needed to create the configuration files without being prompted, which saves time and is useful for automation scripts.

Three configuration files are generated: resource.yaml, appliance.yaml and infra.yaml. These files should be kept and stored in a secure location, as they're required for maintenance of Arc resource bridge.

This command also calls the `validate` command to check the configuration files.

> **Note**
>
> Azure Local uses different commands to create the Arc resource bridge configuration files.

`az arcappliance validate`

The `validate` command checks the configuration files for a valid schema, cloud and core validations (such as management machine connectivity to required URLs), network settings, and proxy settings. It also performs tests on identity privileges and role assignments, network configuration, load balancer configuration, and content delivery network connectivity.

`az arcappliance prepare`

This command downloads the OS images from Microsoft that are used to deploy the on-premises appliance VM. Once downloaded, the images are then uploaded to the local cloud image gallery to prepare for the creation of the appliance VM.

This command generally takes 10-30 minutes to complete, depending on the network speed. Allow the `prepare` command to complete before continuing with the deployment.

`az arcappliance deploy`

The `deploy` command deploys an on-premises instance of Arc resource bridge as an appliance VM, bootstrapped to be a Kubernetes management cluster. This command gets all necessary pods and agents within the Kubernetes cluster into a running state. Once the appliance VM is up, the kubeconfig file is generated.

`az arcappliance create`

This command creates Arc resource bridge in Azure as an ARM resource, then establishes the connection between the ARM resource and on-premises appliance VM.

Once the `create` command initiates the connection, it returns in the terminal, even though the connection between the ARM resource and on-premises appliance VM isn't complete yet. The resource bridge needs about five minutes to establish the connection between the ARM resource and the on-premises VM.

`az arcappliance show`

The `show` command gets the status of the Arc resource bridge and ARM resource information. It can be used to check the progress of the connection between the ARM resource and on-premises appliance VM.

While the Arc resource bridge is connecting the ARM resource to the on-premises VM, the resource bridge progresses through the following stages:

`ProvisioningState` may be `Creating`, `Created`, `Failed`, `Deleting`, or `Succeeded`.

`Status` transitions between `WaitingForHeartbeat` -> `Validating` -> `Connecting` -> `Connected` -> `Running`.

- `WaitingForHeartbeat`: Azure is waiting to receive a signal from the appliance VM.
- `Validating`: Appliance VM is checking Azure services for connectivity and serviceability.
- `Connecting`: Appliance VM is syncing on-premises resources to Azure.
- `Connected`: Appliance VM completed sync of on-premises resources to Azure.
- `Running`: Appliance VM and Azure have completed hybrid sync, and Arc resource bridge is now operational.

Successful Arc resource bridge creation results in `ProvisioningState = Succeeded` and `Status = Running`.

`az arcappliance delete`

This command deletes the appliance VM and Azure resources. It doesn't clean up the OS image, which remains in the on-premises cloud gallery.

If a deployment fails, run this command to clean up the environment before you attempt to deploy again.

Next steps

- Explore the full list of Azure CLI commands and required parameters for Arc resource bridge.
- Get troubleshooting tips for Arc resource bridge.

Upgrade Arc resource bridge

This article describes how Arc resource bridge is upgraded, and the two ways upgrade can be performed: cloud-managed upgrade or manual upgrade. Currently, some private cloud providers differ in how they handle Arc resource bridge upgrades.

Private cloud providers

Private cloud providers have different support policies and upgrade procedures for Arc resource bridge. Review the sections below to learn how to upgrade your Arc resource bridge for your private cloud.

Arc-enabled VMware vSphere

For **Arc-enabled VMware vSphere**, you are responsible for upgrading your Azure Arc resource bridge to a version released within the past 6 months. The appliance version should also be within the most recent 3 versions released. We recommend performing manual upgrades every 6 months to refresh critical certificates within the appliance. If these certificates expire or the appliance is offline for longer than 45 days, your resource bridge may need to be recovered. To find the version release date, see the Arc resource bridge release notes.

For Arc-enabled VMware, Microsoft may offer cloud-managed upgrades as a supplementary service. Arc resource bridges on version 1.0.15 or higher are automatically opted into supplemental cloud-managed upgrades. Supplemental cloud-managed upgrades do not replace the need for you to manually upgrade at least once every 6 months. You should ensure that prerequisites are met for a supplemental cloud-managed upgrade to succeed. Microsoft may attempt to upgrade your Arc resource bridge at any time. If your appliance is not healthy, supplemental cloud-managed upgrades may fail. They also may not succeed due to network disruptions or errors. You are primarily responsible for ensuring your resource bridge is on a supported version with regular manual upgrades. If your appliance is nearing the end of its supported version, a manual upgrade should be performed to avoid service disruptions.

Azure Local

For **Azure Arc VM management on Azure Local**, appliance version 1.0.15 or higher is available only on Azure Local build 23H2. In this version, you should use the built-in LCM tool to manage upgrades for Azure Local, Arc resource bridge, and extensions as a single package. Remove any preview version of Arc resource bridge before updating from 22H2 to 23H2. Do not upgrade Arc resource bridge separately from other Azure Local components, as this can cause critical issues. For details, see About updates for Azure Local.

Azure Arc-enabled SCVMM

For **Arc-enabled System Center Virtual Machine Manager (SCVMM)**, you are responsible for upgrading your Azure Arc resource bridge to a version released within the past 6 months. The appliance version should also be within the most recent 3 versions released. We recommend performing manual upgrades at least once every 6 months to refresh critical certificates within the appliance. If these certificates expire or the appliance is offline for longer than 45 days, you may need to perform recovery of the resource bridge.

To find the version release date, refer to the Arc resource bridge release notes. Manual upgrade is available for appliance version 1.0.15 and higher. Appliances running a version lower than 1.0.15 need to perform the recovery option to get to version 1.0.15 or higher.

Overview

The upgrade process deploys a new resource bridge using the reserved appliance virtual machine (VM) IP. When the new resource bridge is ready, it becomes active. The upgrade process deletes the old resource bridge and reserves its VM IP for the next upgrade.

The upgrade process consists of the following actions:

- Download the appliance image (~3.5 GB) from the cloud.
- Use the image to deploy a new appliance VM.
- Verify that the new resource bridge is running and connect it to Azure.
- Delete the old appliance VM.
- Reserve the old IP for a future upgrade.

The upgrade usually takes at least 30 minutes, depending on network speed. Expect a brief downtime during the transition from the old resource bridge to the new one. More downtime may occur if prerequisites are not met or if there are network issues.

Prerequisites

Before an Arc resource bridge can be upgraded, the following prerequisites must be met:

- Arc resource bridge must be online and healthy with a status of `Running`. You can check the Azure resource of your Arc resource bridge to verify.
- The credentials in the appliance VM must be valid. To test the credentials, perform an operation on an Arc-enabled private cloud VM from the Azure portal.
- Arc resource bridge must be in the same location path where it was originally deployed.
- The appliance VM needs 35 GB of free space.

- For Arc-enabled VMware, upgrading the resource bridge requires 200 GB of free space on the datastore. A new template is also created.
- (Manual upgrade only) When performing a manual upgrade, you should run the upgrade command from the management machine used to initially deploy the Arc resource bridge. You can also run the upgrade command from a different machine that meets the management machine requirements.
- (Manual upgrade only) The management machine needs 3.5 GB of free space.

Check the version

To check the appliance version of your Arc resource bridge, you can check the Azure resource of your resource bridge in Azure Resource Manager. If the appliance status or provisioning state is "Upgrade Failed" or "Failed", an upgrade attempt may have failed. Upon upgrade failure, the appliance version shown may not reflect the actual version. The actual version is most likely the version prior to upgrading. The upgrade must succeed for your appliance to be on the new version.

Manual upgrade

> ⚠ **Warning**
>
> For Azure Local, you must use the built-in Azure Local LCM tool to upgrade Arc resource bridge. If you attempt to manual upgrade using the Azure CLI command, your environment will break and be irrecoverable. If you need assistance with an Arc resource bridge upgrade, please contact Microsoft Support.

You can manually upgrade the Arc resource bridge from your management machine. Before upgrading, make sure you meet all prerequisites. The management machine must have the kubeconfig locally stored. Manual upgrade generally takes about 30-90 minutes, depending on your network speeds. An upgrade takes your Arc resource bridge to the next appliance version, which may not be the newest appliance version. Multiple upgrades may be needed to reach a supported version. During an upgrade, the status of your resource bridge may change based on its progress. Upgrade is complete when the appliance status is `Running` and `provisioningState` is `Succeeded`. You can view the status by going to your Azure resource in the Azure portal.

Perform a manual upgrade

1. Before upgrading, you should get the latest Azure CLI extension for `arcappliance`:

Azure CLI

```
az extension add --upgrade --name arcappliance
```

2. The appliance kubeconfig is required to run a manual upgrade. By default, it is stored in the management machine's CLI directory used to deploy the resource bridge. It can also be retrieved with the following get-credentials command:

Azure CLI

```
az arcappliance get-credentials --resource-group [REQUIRED] --name [REQUIRED] --credentials-dir [OPTIONAL]
```

3. (Arc-enabled VMware) To upgrade a resource bridge on VMware without the configuration file, the following required and optional parameters should be provided in lieu of the configuration file:

```
az arcappliance upgrade vmware --resource-group [REQUIRED] --name [REQUIRED] --kubeconfig [REQUIRED] --address [OPTIONAL] --username [OPTIONAL] --password [OPTIONAL]
```

(Arc-enabled SCVMM) To upgrade on SCVMM without the configuration file, the following optional parameters should be provided in lieu of the configuration file:

```
az arcappliance upgrade scvmm --address [OPTIONAL] --kubeconfig [OPTIONAL] --location [OPTIONAL] --name [OPTIONAL] --password [OPTIONAL] --resource-group [OPTIONAL] --username [OPTIONAL]
```

(Azure Local) To upgrade a resource bridge on Azure Local, transition to 23H2 and use the built-in upgrade management tool. For more information, see About updates for Azure Local, version 23H2.

Upgrade guidance

We generally recommend performing manual upgrades at least once every 6 months to refresh critical certificates within the appliance. Your appliance version should also be within the 3 most recently released versions. You can review the supported version policy for more information.

When a patch version is released, the upgrade path may skip the minor version and directly upgrade to the patch version. In such cases, the supported versions (n-3) excludes the skipped minor version and includes the patch version instead. To see what versions are in support, please refer to Arc resource bridge release notes.

If a resource bridge isn't upgraded to a supported version, it will be unsupported. It may not be possible to upgrade an unsupported resource bridge to a newer version because internal components may no longer be compatible. In addition, the unsupported resource bridge may not be able to provide reliable monitoring and health metrics. You may also stop receiving email notifications about your Arc resource bridge. If you can't upgrade your Arc resource bridge to a supported version, you may need to perform recovery.

Notification and upgrade availability

You may receive an email notification about your Arc resource bridge being unsupported due to a new version release. If you receive this email, we recommend that you upgrade the resource bridge as soon as possible to allow time for troubleshooting any issues during manual upgrade. To see the current version of an Arc resource bridge, check the Azure resource of your Arc resource bridge. To check if your Arc resource bridge has an upgrade available, you can run the following command:

Azure CLI

```
az arcappliance get-upgrades --resource-group [REQUIRED] --name [REQUIRED]
```

Next steps

- Learn about Arc resource bridge maintenance operations.
- Learn about troubleshooting Arc resource bridge.

Last updated on 12/30/2025

Azure Arc resource bridge maintenance

Summarize this article for me

To keep your Azure Arc resource bridge healthy and available, you need to perform maintenance such as updating credentials, monitoring upgrades, and creating a resource health alert. You can also update the proxy settings if there are changes post-deployment.

> **Important**
>
> Arc resource bridge can't be offline for longer than 45 days because the security key within the appliance VM may expire and can't be refreshed. As a best practice, create a resource health alert in the Azure portal to stay informed if an Arc resource bridge becomes unavailable.

Prerequisites

The management machine used to perform maintenance must meet all of the Arc resource bridge requirements.

The following sections describe common maintenance tasks for Arc resource bridge.

Update credentials in the appliance VM

Arc resource bridge consists of an on-premises appliance VM. The appliance VM stores credentials that are used to access the control plane of the on-premises infrastructure to view and manage on-premises resources (ex: vCenter credentials). The credentials used by Arc resource bridge are the same ones provided during deployment. It gives the resource bridge visibility to on-premises resources for guest management in Azure. If the credentials change (ex: your company requires a password change every 90 days), then the credentials stored in the Arc resource bridge must be updated.

You can test if the credentials within the appliance VM are valid by going to the Azure portal and performing an action on a machine that's Arc-enabled via the resource bridge. You can also attempt to upgrade the resource bridge. If you receive an error, then it is possible that the credentials need to be updated. For guidance on maintaining credentials for Arc-enabled VMware, see Update the vSphere account credentials. For Arc-enabled SCVMM, see Update the SCVMM account credentials.

Upgrade Arc resource bridge

Each Arc-enabled private cloud has its own upgrade guidelines and procedures. For more information, please refer to the Upgrade page.

Create resource health alerts

You can create a resource health alert rule in the Azure portal to monitor the state of your Arc resource bridge. Follow these steps to create an alert that notifies you if an Arc resource bridge becomes unavailable.

1. In the Azure portal, search and navigate to **Service Health**.
2. In the service menu, under **RESOURCE HEALTH**, select **Resource health**.
3. In the **Subscription** dropdown, select the subscription used to deploy your resource bridge.
4. In the **Resource type** dropdown, select **Azure Arc Resource Bridge**.
5. Select the resource bridge(s) from the list for which you want to configure alerts. If you want to set up alerts for all the resource bridges in your subscription, you can select **Add resource health alert** without selecting any resource bridges. This will also add health alerts for resource bridges you may deploy in the future.
6. To receive notifications only when the resource bridge becomes unhealthy, set the following conditions in the **Condition** tab:
    - **Event status**: **Active**
    - **Current resource status**: **Unavailable**
    - **Previous resource status**: **Available**
7. Select one or more **Reason type** values for your alert:
    - **Platform Initiated** : Alerts you when a resource becomes unavailable due to platform issues.
    - **Unknown**: Alerts you when a resource becomes unavailable, but the reason isn't known.
    - **User Initiated**: Alerts you when a resource becomes unavailable due to an action taken by a user.
8. Select **Next: Actions** to continue. In the **Actions** tab, if you want to receive an email when the alert is triggered, select **Use quick actions (preview)** and complete the following:

    a. Enter an **Action group name** and **Display name**

b. Check the **Email** box and enter an email address.

c. Select **Save.**

9. Select **Next: Details** to continue. In the **Details** tab:
   a. Select the resource group and region in which to create the alert rule.
   b. Enter a name for your alert rule, and a description if desired.

10. Select **Review + create**, then select **Create**.

For more information about resource health alert rule options, see Create or edit an activity log, service health, or resource health alert rule.

Update proxy settings (Preview)

Starting with appliance version 1.7.0 and `az arcappliance` CLI version 1.7.0, you can update proxy settings on an appliance using the Azure CLI command: az arcappliance configuration proxy update. The proxy update command is only supported for Azure Local and Arc-enabled VMware.

Use this command when:

- Your organization switches to a new proxy server.
- You need to disable proxy usage entirely.
- You want to rotate proxy credentials or certificates.

If an upgrade fails due to incorrect network proxy settings, you can run a proxy update to fix the values. If a proxy update operation fails, you must retry and have it succeed before performing any other operation, including retrying upgrade.

Recovery procedure

Each Arc private cloud has its own recovery procedure that should be followed to ensure a successful redeployment of the Arc resource bridge and re-connection to the existing custom location and Arc private cloud extension.

For Arc-enabled VMware, you can follow the Arc-enabled VMware recovery procedure.

For Arc-enabled SCVMM, you can follow the Arc-enabled SCVMM recovery procedure.

For Azure Local, you must contact support and only attempt to recover the Arc resource bridge with guidance by Microsoft. Arc resource bridge is a critical component to Azure Local and attempting a major operation without guidance may cause irrecoverable damage to your Azure Local environment.

Delete Arc resource bridge

> **Important**
>
> For Azure Local, do not delete the Arc resource bridge unless you are given guidance by Microsoft. Arc resource bridge is a critical component to Azure Local and deleting it without guidance may cause irrecoverable damage to your Azure Local environment.

You might need to delete Arc resource bridge due to deployment failures, or when the resource bridge is no longer needed. Use the az arcappliance delete command to delete the Arc resource bridge. This command deletes the on-premises appliance VM, along with the Azure resource and underlying components across the two environments. Manually deleting the appliance VM or Azure resource may cause errors in future deployments as the connections between the two resources still exist on the backend.

Next steps

- Learn about upgrading Arc resource bridge.
- Review the Azure Arc resource bridge overview to understand more about requirements and technical details.
- Learn about system requirements for Azure Arc resource bridge.

Last updated on 02/05/2026

Troubleshoot Azure Arc resource bridge issues

08/06/2025

This article provides information on troubleshooting and resolving issues that could occur while attempting to deploy, use, or remove the Azure Arc resource bridge. The resource bridge is a packaged virtual machine, which hosts a *management* Kubernetes cluster. For general information, see Azure Arc resource bridge overview.

> **Note**
>
> - For ***Arc-enabled System Center Virtual Machine Manager***, refer to the Arc-enabled SCVMM troubleshoot guide.
> - For ***Azure Local***, refer to Troubleshoot Azure Arc VM management for Azure Local or contact Microsoft Support. Arc resource bridge is a critical component of Azure Local and should not be deleted without guidance from Microsoft Support.

General issues

Logs collection

For issues encountered with Arc resource bridge, collect logs for further investigation using the Azure CLI az arcappliance logs command. This command needs to be run from the management machine used to deploy the Arc resource bridge. If you're using a different machine, the machine must meet the management machine requirements.

If there's a problem collecting logs, most likely the management machine is unable to reach the Appliance VM. Contact your network administrator to allow SSH communication from the management machine to the Appliance VM on TCP port 22.

You can collect the Arc resource bridge logs by passing either the appliance VM IP or the kubeconfig in the logs command.

To collect Arc resource bridge logs on VMware using the appliance VM IP address:

Azure CLI

```
az arcappliance logs vmware --ip <appliance VM IP> --username <vSphere username> --password <vSphere password> --address <vCenter address> --out-dir <path to output
```

```
directory>
```

To collect Arc Resource Bridge logs for Azure Local, see Collect logs.

If you're unsure of your appliance VM IP, there's also the option to use the kubeconfig. You can retrieve the kubeconfig by running the get-credentials command then run the logs command.

To retrieve the kubeconfig and log key then collect logs for Arc-enabled VMware from a different machine than the one used to deploy Arc resource bridge for Arc-enabled VMware:

Azure CLI

```
az account set -s <subscription id>
az arcappliance get-credentials -n <Arc resource bridge name> -g <resource group
name>
az arcappliance logs vmware --kubeconfig kubeconfig --out-dir <path to specified
output directory>
```

Get login credentials error on Azure CLI v2.70.0

You may encounter an error when running az arcappliance commands that looks like this:

`File "C:\Program Files\Common Files\AzureCliExtensionDirectory\arcappliance\azext_arcappliance\helpers.py", line 103, in get_tenant_id_and_cloud

```
_, _, tenant =
profile.get_login_credentials(resource=cmd.cli_ctx.cloud.endpoints.active_director
y_graph_resource_id)
```TypeError: get_login_credentials() got an unexpected keyword argument
'resource'``

Azure CLI v2.70.0 released a breaking change which triggers this error in arcappliance CLI extension v1.4.0 and below. A fix is available in arcappliance CLI extension 1.4.1 for compatibility with Azure CLI v2.70.0. You can get the latest arcappliance CLI extension by running the following command:


```azurecli
az extension add --upgrade --name arcappliance
```

If you are on az arcappliance extension is 1.4.0 or lower, you need to downgrade Azure CLI to v2.69.0.

If you used the Azure CLI installer, you can uninstall the current version and install Azure CLI v2.69.0 from the Azure CLI installation page. If you used the pip installer, you can run the following command to downgrade: `pip install azure-cli==2.69.0`.

Also, for the Arc-enabled VMware onboarding script, you may need to comment out the below code in the script to not update the AZ CLI to latest again:

```
if (shouldInstallAzCli) {
   installAzCli64Bit
}
```

Error downloading release file information

> **⚠ Warning**
>
> For Azure Local, you must use the built-in LCM tool to upgrade Arc resource bridge. If you attempt to manual upgrade using the Azure CLI command, your environment will break and be irrecoverable. If you need assistance with an Arc resource bridge upgrade, please contact Microsoft Support.

When upgrading Arc resource bridge using Azure CLI, you may get the following error:

Azure CLI

```
az arcappliance upgrade vmware' failed: (DownloadError) "{\n\"message\": \"Error downloading file release information.: Unable to find file release: ^mariner-2-0-(.*)-vhdx-rpm-(.*)$ with version:  in product release: arc-appliance-stable-releases\"\n}
```

If you are using an az arcappliance Azure CLI extension version that is below 1.4.0 and attempting to upgrade to appliance version 1.4.0, you need to update your Azure CLI extension to the latest version:

Azure CLI

```
az extension add --upgrade --name arcappliance
```

Once your az arcappliance extension is 1.4.0, re-try the upgrade to appliance version 1.4.0. When upgrading an Arc resource bridge, the upgrade will be to the next version which may not be the latest version. Refer to Arc resource bridge release notes.

Download/upload connectivity was not successful

If your network speed is slow, you might not be able to successfully download the Arc resource bridge VM image, resulting in this error: `ErrorCode: ValidateKvaError, Error: Pre-deployment validation of your download/upload connectivity was not successful. Timeout error occurred during download and preparation of appliance image to the on-premises fabric storage. Common causes of this timeout error are slow network download/upload speeds, a proxy limiting the network speed or slow storage performance.`

As a workaround, try creating a VM directly on the on-premises private cloud, and then run the Arc resource bridge deployment script from that VM. Doing this should result in a faster upload of the image to the datastore.

Context timed out during phase `ApplyingKvaImageOperator`

When you deploy Arc resource bridge, you might see this error: `Deployment of the Arc resource bridge appliance VM timed out. Collect logs with _az arcappliance logs_ and create a support ticket for help. To troubleshoot the error, refer to aka.ms/arc-rb-error { _errorCode_: _ContextError_, _errorResponse_: _{\n_message_: _Context timed out during phase _ApplyingKvaImageOperator__\n}_ }`

This error typically occurs when trying to download the `KVAIO` image (400 MB compressed) over a network that is slow or experiencing intermittent connectivity. The `KVAIO` controller manager waits for the image download to complete, and times out.

Check that your network speed between the Arc resource bridge VM and Microsoft Container Registry (`mcr.microsoft.com`) is stable and at least 2 Mbps. If your network connectivity and speed are stable, and you're still getting this error, wait at least 30 minutes before you retry, as it could be due to Microsoft Container Registry receiving a high volume of traffic.

Context timed out during phase `WaitingForAPIServer`

When you deploy Arc resource bridge, you might see this error: `Deployment of the Arc resource bridge appliance VM timed out. Collect logs with _az arcappliance logs_ and create a support ticket for help. To troubleshoot the error, refer to aka.ms/arc-rb-error { _errorCode_: _ContextError_, _errorResponse_: _{\n_message_: _Context timed out during phase _WaitingForAPIServer`

This error indicates that the deployment machine can't contact the control plane IP for Arc resource bridge within the time limit. Common causes of the error are often networking related, such as communication between the deployment machine and control plane IP being

routed through a proxy. Traffic from the deployment machine to the control plane and the appliance VM IPs must not pass through proxy. If traffic is being proxied, configure the proxy settings on your network or deployment machine to not proxy traffic between the deployment machine to the control plane IP and appliance VM IPs. Another cause for this error is if a firewall is closing access to port 6443 and port 22 between the deployment machine and control plane IP or the deployment machine and appliance VM IPs.

403 Forbidden or 404 Site Not Found

When you deploy Arc resource bridge, you might see this error: `{ _errorCode_: _UploadError_, _errorResponse_: _{\n\_message\_: \_Pre-deployment validation of your download/upload connectivity was not successful. {\\n \\\_code\\\_: \\\_ImageProvisionError\\\_,\\n \\\_message\\\_: \\\_403 Forbidden` or `{ _errorCode_: _UploadError_, _errorResponse_: _{\n\_message\_: \_Pre-deployment validation of your download/upload connectivity was not successful. {\\n \\\_code\\\_: \\\_ImageProvisionError\\\_,\\n \\\_message\\\_: \\\_404 Site Not Found`

This error occurs when images need to be downloaded from Microsoft registries to the deployment machine, but a proxy or firewall blocks the download. Review the network requirements and verify that all required URLs are reachable. You may need to update your no proxy settings to ensure that traffic from your deployment machine to Microsoft required URLs aren't going through a proxy.

SSH folder access denied

The CLI requires permission to access the SSH folder during deployment or operations that involve accessing files within the folder. This folder contains essential files such as the kubeconfig and logs key for the appliance VM. For instance, the CLI needs to access the logs key stored in the SSH folder to collect logs from the appliance VM.

You might see this error: `Access to the file in the SSH folder was denied. This may occur if the CLI doesn't have permission to the SSH folder or if another CLI instance is using the file`. There are two common causes for this issue:

- Insufficient permissions: The CLI lacks the necessary permissions to access the SSH folder. Ensure that the user account running the CLI has appropriate permissions to access the SSH folder.
- Concurrent file access: Another instance of the CLI might be using the file in the SSH folder. This often happens on workstations with shared profiles. Ensure that any other CLI instance completes or terminates its operation before you proceed.

Arc resource bridge is offline

There are a number of reasons Arc resource bridge may be offline. In general, if Arc resource bridge is unable to communicate with Azure, the appliance VM will go offline. For Arc-enabled VMware and SCVMM, you may need to update the credentials stored within Arc resource bridge. Communication to Azure may have been impacted by networking changes in the infrastructure, environment or cluster. If you're unable to determine what changed, you can reboot the appliance VM, collect logs and submit a support ticket for investigation. As a best practice, create a resource health alert to stay informed if an Arc resource bridge becomes unavailable. Arc resource bridge can't be offline for longer than 45 days. After 45 days, the security key within the appliance VM may no longer be valid and can't be refreshed. If you are unable to get Arc resource bridge back online, please contact Microsoft Support.

Remote PowerShell isn't supported

If you run `az arcappliance` CLI commands for Arc resource bridge via remote PowerShell, you might see an authentication handshake failure error when trying to install the resource bridge on an Azure Local instance or another type of error.

Using `az arcappliance` commands from remote PowerShell isn't currently supported. Instead, sign in to the node through Remote Desktop Protocol (RDP) or use a console session.

Appliance Network Unavailable

If Arc resource bridge experiences network problems, you might see an `Appliance Network Unavailable` error. In general, any network or infrastructure connectivity issue to the appliance VM may cause this error. This error can also surface as `Error while dialing dial tcp xx.xx.xxx.xx:55000: connect: no route to host`. The problem could be that communication from the host to the Arc resource bridge VM needs to be opened over TCP port 22 with the help of your network administrator. A temporary network issue may not allow the host to reach the Arc resource bridge VM. Once the network issue is resolved, you can retry the operation. You can also check that the appliance VM for Arc resource bridge isn't stopped or offline. With Azure Local, this error can be caused when the host storage is full.

Token refresh error

When you run Azure CLI commands, you may see the following error: `The refresh token has expired or is invalid due to sign-in frequency checks by conditional access.`

This error occurs because when you sign in to Azure, the token has a maximum lifetime. When that lifetime is exceeded, you need to sign in to Azure again by using the `az login` command.

Default host resource pools are unavailable for deployment

When you use the `az arcappliance createconfig` or `az arcappliance run` command, an interactive experience shows the list of VMware entities which you can select to deploy the virtual appliance. This list shows all user-created resource pools along with default cluster resource pools, but the default host resource pools aren't listed. When the appliance is deployed to a host resource pool, there's no high availability if the host hardware fails. We recommend that you don't deploy the appliance in a host resource pool.

Expired credentials in the appliance VM

Arc resource bridge consists of an appliance VM that is deployed to the on-premises infrastructure. The appliance VM maintains a connection to the management endpoint (ex: VMware vCenter) of the on-premises infrastructure using locally stored credentials. If these credentials aren't updated, the resource bridge is no longer able to communicate with the management endpoint. This can cause problems when trying to upgrade the resource bridge or manage VMs through Azure.

To fix this problem, the credentials in the appliance VM need to be updated. For more information, see Update credentials in the appliance VM.

Private link is unsupported

Arc resource bridge doesn't support private link. Calls coming from the appliance VM shouldn't be going through your private link setup. Private link IPs may conflict with the appliance IP pool range, which isn't configurable on the resource bridge. Arc resource bridge reaches out to required URLs that shouldn't go through a private link connection. You must deploy Arc resource bridge on a separate network segment unrelated to the private link setup.

Unapproved extension installation

Arc resource bridge is a locked-down virtual appliance built to host only approved Azure Arc-enabled private cloud extensions. If you attempt to install any other extension onto the resource bridge, you will receive an error:

```
```

```
Extension installation failed. The specified extension is not permitted on Azure
Arc Resource Bridge. Only Azure Arc resource bridge approved extensions can be
installed.
```

Error downloading file release information

When attempting to upgrade the Arc resource bridge, you may encounter the following error:

```
'az arcappliance upgrade hci' failed: (DownloadError) "{\n\"message\": \"Error
downloading file release information.: Unable to find file release: ^mariner-2-0-
(.*)-vhdx-rpm-(.*)$ with version:  in product release: arc-appliance-stable-
releases\"\n}",
```

This error occurs from using an older version of the Azure CLI `arcappliance` extension that is not forward-compatible with the upgraded version of Arc resource bridge. Before upgrading, update your Azure CLI extension for `arcappliance` by running the following Azure CLI command:

Azure CLI

```
az extension add --upgrade --name arcappliance
```

GLIBC version not found

You may receive the following error when deploying Arc resource bridge:

```
"error_message": /lib64/libc.so.6: version `GLIBC_2.34_ not found (required by
/root/.azure/cliextensions/arcappliance/azext_arcappliance/pkg/providers/kva//../.
./binaries/arcsdk.so)
```

This error message indicates that the Arc Resource Bridge CLI extension (arcappliance) is trying to load a shared library (arcsdk.so) that was compiled against glibc 2.34, but your Linux system has an older version of glibc or doesn't have the required glibc version. This may happen if you are running an old version of Linux. You can check the current glibc version using `- ldd --version`. It is recommended to use a supported Linux distribution with the required glibc version or onboard from a jumpbox or client VM that meets the glibc requirement.

Networking issues

Back-off pulling image error

When trying to deploy Arc resource bridge, you might see an error that contains `back-off pulling image \\\"url"\\\: FailFastPodCondition`. This error is caused when the appliance VM can't reach the URL specified in the error. To resolve this issue, make sure the appliance VM meets system requirements, including internet access connectivity to required allowlist URLs.

Management machine unable to reach appliance

When trying to deploy Arc resource bridge, you might receive an error message similar to:

```
{ _errorCode_: _PostOperationsError_, _errorResponse_: _{\n\_message\_: \_Timeout occurred due to management machine being unable to reach the appliance VM IP, 10.2.196.170. Ensure that the requirements are met: https://aka.ms/arb-machine-reqs: dial tcp 10.2.196.170:22: connectex: A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because connected host has failed to respond.\_\n}_, _errorMetadata_: { _errorCategory_: __ }
```

This error occurs when the management machine can't reach the Arc resource bridge VM IP by SSH (Port 22) or API Server (Port 6443). It could also occur if the Arc resource bridge API server is being proxied; the Arc resource bridge API server needs to be added to the noproxy settings. For more information, see Azure Arc resource bridge network requirements.

Not able to connect to URL

If you receive an error that contains `Not able to connect to https://example.url.com`, check with your network administrator to ensure your network allows all of the required firewall and proxy URLs to deploy Arc resource bridge. For more information, see Azure Arc resource bridge network requirements.

Not able to connect - network and internet connectivity validation failed

When you deploy Arc resource bridge, you may receive an error with `errorCode` as `PostOperationsError`, `errorResponse` as code `GuestInternetConnectivityError` with a URL specifying port 53 (DNS). This error may be due to the appliance VM IPs being unable to reach DNS servers, so they can't resolve the endpoint specified in the error.

Error examples:

```
{ _errorCode_: _PostOperationsError_, _errorResponse_: _{\n\_message\_: \_{\\n
 \\\_code\\\_:\\\_GuestInternetConnectivityError\\\_,\\n\\\_message\\\_:\\\_Not able to
connect to http://aszhcitest01.company.org:55000. Error returned: action failed after 5
attempts: Get \\\\\\\_http://aszhcitest01.company.org:55000\\\\\\\_: dial tcp: lookup
aszhcitest01.company.org on 127.0.0.53:53: read udp 127.0.0.1:32975-\\u003e127.0.0.53:53:
i/o timeout. Arc Resource Bridge network and internet connectivity validation failed:
cloud-agent-connectivity-test. 1. check your networking setup and ensure the URLs
mentioned in : https://aka.ms/AAla73m are reachable from the Appliance VM.   2. Check
firewall/proxy settings\\\_\\n }\_\n}_ }
```

```
{ _errorCode_: _PostOperationsError_, _errorResponse_: _{\n\_message\_: \_{\\n
 \\\_code\\\_: \\\_GuestInternetConnectivityError\\\_,\\n  \\\_message\\\_: \\\_Not able
to connect to https://linuxgeneva-microsoft.azurecr.io. Error returned: action failed
after 5 attempts: Get \\\\\\\_https://linuxgeneva-microsoft.azurecr.io\\\\\\\_: dial tcp:
lookup linuxgeneva-microsoft.azurecr.io on 127.0.0.53:53: server misbehaving. Arc
Resource Bridge network and internet connectivity validation failed: http-connectivity-
test-arc. 1. Please check your networking setup and ensure the URLs mentioned in :
https://aka.ms/AAla73m are reachable from the Appliance VM.   2. Check firewall/proxy
settings\\\_\\n }\_\n}_ }
```

To resolve these errors, work with your network administrator to allow the appliance VM IPs to reach the DNS servers. For more information, see Azure Arc resource bridge network requirements.

Http2 server sent GOAWAY

When trying to deploy Arc resource bridge, you might receive error messages similar to the ones below:

```
"errorResponse": "{\n\"message\": \"Post
\\\"https://region.dp.kubernetesconfiguration.azure.com/azure-arc-appliance-
k8sagents/GetLatestHelmPackagePath?api-version=2019-11-01-
preview\\u0026releaseTrain=stable\\\": http2: server sent GOAWAY and closed the
connection; LastStreamID=1, ErrCode=NO_ERROR, debug=\\\"\\\"\"\n}"
```

or

```
Post \_https://canadacentral.dp.kubernetesconfiguration.azure.com/azure-arc-appliance-
k8sagents/GetLatestHelmPackagePath?api-version=2019-11-01-
```

`preview\u0026releaseTrain=stable\_: read tcp 10.128.131.173:52425-\u003e52.228.84.81:443: wsarecv: An existing connection was forcibly closed by the remote host.`

These errors may occur when a firewall or proxy has SSL/TLS inspection enabled and blocks http2 calls from the machine used to deploy the resource bridge. To confirm the problem, run the following PowerShell cmdlet to invoke the web request with http2 (requires PowerShell version 7 or above), replacing the region in the URL and `api-version` (for example, `2019-11-01`) with values from the error:

```
Invoke-WebRequest -HttpVersion 2.0 -UseBasicParsing -Uri https://region.dp.kubernetesconfiguration.azure.com/azure-arc-appliance-k8sagents/GetLatestHelmPackagePath?api-version=2019-11-01-preview"&"releaseTrain=stable -Method Post -Verbose
```

If the result is `The response ended prematurely while waiting for the next frame from the server`, then the http2 call is being blocked and needs to be allowed. Work with your network administrator to disable the SSL/TLS inspection to allow http2 calls from the machine used to deploy the bridge.

No such host - `.local` not supported

When trying to set the configuration for Arc resource bridge, you might receive an error message similar to:

```
"message": "Post \"https://esx.lab.local/52c-acac707ce02c/disk-0.vmdk\": dial tcp: lookup esx.lab.local: no such host"
```

This error occurs when a `.local` path is provided for a configuration setting, such as proxy, dns, datastore, or management endpoint (such as vCenter). Arc resource bridge appliance VM uses Azure Linux OS, which doesn't support `.local` by default. A workaround could be to provide the IP address where applicable.

Azure Arc resource bridge is unreachable

Azure Arc resource bridge runs a Kubernetes cluster, and its control plane requires a static IP address. The IP address is specified in the `infra.yaml` file. If the IP address is assigned from a DHCP server, the address can change if it's not reserved. Rebooting the Azure Arc resource bridge or VM can trigger an IP address change and result in failing services.

Arc resource bridge may intermittently lose the reserved IP configuration. This loss is due to the behavior described in loss of VIPs when systemd-networkd is restarted. When the IP address isn't assigned to the Azure Arc resource bridge VM, any call to the resource bridge API

server fails. Core operations, such as creating a new resource, connecting to your private cloud from Azure, or creating a custom location, won't function as expected.

To resolve this issue, reboot the resource bridge VM, and it should recover its IP address. If the address is assigned from a DHCP server, reserve the IP address associated with the resource bridge.

The Arc resource bridge may also be unreachable due to slow disk access. Azure Arc resource bridge uses Kubernetes extended configuration tree (ETCD), which requires latency of 10 ms or less. If the underlying disk has low performance, operations are impacted and failures can occur.

SSL proxy configuration issues

Be sure that the proxy server on your management machine trusts both the SSL certificate for your SSL proxy and the SSL certificate of the Microsoft download servers. For more information, see SSL proxy configuration.

No such host - `dp.kubernetesconfiguration.azure.com`

When deploying Arc resource bridge, you may receive an error message similar to:

```
{ _message_: _Post \_https://eastus.dp.kubernetesconfiguration.azure.com/azure-arc-appliance-k8sagents/GetLatestHelmPackagePath?api-version=2019-11-01-preview\u0026releaseTrain=stable\_: dial tcp: lookup eastus.dp.kubernetesconfiguration.azure.com: no such host_ }
```

The error indicates an issue reaching out to the URL indicated in the error message, in this case, `eastus.dp.kubernetesconfiguration.azure.com`. This could be due to a few reasons:

- The configuration data plane may be temporarily unavailable in the specified region.
- DNS resolution issue to the *.dp.kubernetesconfiguration.azure.com endpoint.
- Network reachability error to the *.dp.kubernetesconfiguration.azure.com endpoint.

Recommended Actions:

- Wait for the service to be available, then retry the deployment.
- Verify DNS server settings on the host.
- Confirm outbound internet access to the endpoint is not blocked by firewall or proxy.

Certificate signed by unknown authority

You may encounter the following error when deploying Arc resource bridge:

```
"errorResponse": "{\n\"message\": \"{\\n  \\\"code\\\":
\\\"GuestInternetConnectivityError\\\",\\n  \\\"message\\\": \\\"Name: http-
connectivity-test-arc. Message: Not able to connect to
https://msk8s.api.cdp.microsoft.com. Error returned: action failed after 5
attempts: Get \\\\\\\"https://msk8s.api.cdp.microsoft.com\\\\\\\": **tls: failed
to verify certificate: x509: certificate signed by unknown authority.** Arc
Resource Bridge network and internet connectivity validation failed: http-
connectivity-test-arc. 1. Please check your networking setup and ensure the URLs
mentioned in : https://aka.ms/AA1a73m are reachable from the Appliance VM.   2.
Check firewall/proxy settings\\\",\\n  \\\"category\\\": \\\"\\\"\\n }\"\n}",
```

This error occurs when SSL inspection is occurring within the network and that is preventing HTTPS/SSL trust from being established with the endpoint referenced in the error. This error is most commonly seen with a SSL proxy server that is doing SSL inspection/termination and is intercepting the connection to the endpoint and breaking the connectivity. If you have not configured a proxy server during deployment, then your network may have a transparent proxy or a network security device which is interfering with this connection. We recommend that you work with your networking team to debug the cause using your proxy/firewall/security device logs.

Proxy connect tcp - No such host for Arc resource bridge required URL

An error that contains an Arc resource bridge required URL with the message `proxyconnect tcp: dial tcp: lookup http: no such host` indicates that DNS is unable to resolve the URL. The error may look similar to this example, where the required URL is `https://msk8s.api.cdp.microsoft.com`:

`Error: { _errorCode_: _InvalidEntityError_, _errorResponse_: _{\n_message_: _Post _https://msk8s.api.cdp.microsoft.com/api/v1.1/contents/default/namespaces/default/names/arc-appliance-stable-catalogs-ext/versions/latest?action=select_: POST https://msk8s.api.cdp.microsoft.com/api/v1.1/contents/default/namespaces/default/names/arc-appliance-stable-catalogs-ext/versions/latest?action=select giving up after 6 attempt(s): Post _https://msk8s.api.cdp.microsoft.com/api/v1.1/contents/default/namespaces/default/names/arc-appliance-stable-catalogs-ext/versions/latest?action=select_: proxyconnect tcp: dial tcp: lookup http: no such host_\n}_ }`

This error can occur if the DNS settings provided during deployment aren't correct or there's a problem with the DNS servers. You can check if your DNS server is able to resolve the url by running the following command from the management machine or a machine that has access to the DNS servers:

```
nslookup
> set debug
> <hostname> <DNS server IP>
```

To resolve the error, configure your DNS servers to resolve all Arc resource bridge required URLs. The DNS servers must be correctly provided when you deploy Arc resource bridge.

KVA timeout error

The KVA timeout error is a generic error caused by various network misconfigurations that involve the management machine, For instance, the appliance VM or Control Plane IP may not have communication with each other, to the internet, or required URLs. These communication failures are often due to issues with DNS resolution, proxy settings, network configuration, or internet access.

For clarity, management machine refers to the machine where deployment CLI commands are being run. Appliance VM is the VM that hosts Arc resource bridge. Control Plane IP is the IP of the control plane for the Kubernetes management cluster in the Appliance VM.

Top causes of the KVA timeout error

- Management machine is unable to communicate with Control Plane IP and Appliance VM IP.
- Appliance VM is unable to communicate with the management machine, vCenter endpoint (for VMware), or MOC cloud agent endpoint (for Azure Local).
- Appliance VM doesn't have internet access.
- Appliance VM has internet access, but connectivity to one or more required URLs is being blocked, possibly due to a proxy or firewall.
- Appliance VM is unable to reach a DNS server that can resolve internal names, such as vCenter endpoint for vSphere or cloud agent endpoint for Azure Local. The DNS server must also be able to resolve external addresses, such as Azure service addresses and container registry names.
- Proxy server configuration on the management machine or Arc resource bridge configuration files is incorrect. This can impact both the management machine and the Appliance VM. When the `az arcappliance prepare` command is run and the host proxy

isn't correctly configured, the management machine can't connect and download OS images. Internet access on the Appliance VM might be broken by incorrect or missing proxy configuration, which impacts the VM's ability to pull container images.

Troubleshoot KVA timeout error

To resolve the error, one or more network misconfigurations might need to be addressed.

- The first step is to collect logs by Appliance VM IP (not by kubeconfig, as the kubeconfig could be empty if the deploy command didn't complete). Problems collecting logs are most likely due to the management machine being unable to reach the Appliance VM.

  Once logs are collected, extract the folder and open `kva.log`. Review the log for information that might help pinpoint the cause of the KVA timeout error.

- The management machine must be able to communicate with the Appliance VM IP and Control Plane IP. Ping the Control Plane IP and Appliance VM IP from the management machine and verify that there's a response from both IPs.

  If a request times out, the management machine can't communicate with the IPs. This issue might be caused by a closed port, network misconfiguration, or firewall block. Work with your network administrator to allow communication between the management machine to the Control Plane IP and Appliance VM IP.

- Appliance VM IP and Control Plane IP must be able to communicate with the management machine and vCenter endpoint (for VMware) or MOC cloud agent endpoint (for Azure Local. Work with your network administrator to ensure the network is configured to permit this communication. You might need to add a firewall rule to open port 443 from the Appliance VM IP and Control Plane IP to vCenter, or to open port 65000 and 55000 for Azure Local MOC cloud agent. Review network requirements for Azure Local and VMware for Arc resource bridge.

- Appliance VM IP and Control Plane IP need internet access to these required URLs. Azure Local requires additional URLs. Work with your network administrator to ensure that the IPs can access the required URLs.

- In a non-proxy environment, the management machine must have external and internal DNS resolution. The management machine must be able to reach a DNS server that can resolve internal names such as vCenter endpoint for vSphere or cloud agent endpoint for Azure Local. The DNS server also needs to be able to resolve external addresses, such as Azure URLs and OS image download URLs. Work with your system administrator to ensure that the management machine has internal and external DNS resolution. In a proxy

environment, the DNS resolution on the proxy server should resolve internal endpoints and required external addresses.

To test DNS resolution to an internal address from the management machine in a non-proxy scenario, open a command prompt and run `nslookup <vCenter endpoint or HCI MOC cloud agent IP>`. You should receive an answer if the management machine has internal DNS resolution in a non-proxy scenario.

1. Appliance VM needs to be able to reach a DNS server that can resolve internal names, such as vCenter endpoint for vSphere or cloud agent endpoint for Azure Local. The DNS server also needs to be able to resolve external/internal addresses, such as Azure service addresses and container registry names for download of the Arc resource bridge container images from the cloud.

   Verify that the DNS server IP used to create the configuration files has internal and external address resolution.

Move Arc resource bridge location

Resource move of Arc resource bridge isn't currently supported.

Azure Arc-enabled VMs on Azure Local issues

For general help resolving issues related to Azure Arc-enabled VMs on Azure Local, see Troubleshoot Azure Arc VM management for Azure Local.

If you are running Azure Local, version 23H2 or later, and your Arc Resource Bridge is offline, try restarting the Arc Resource Bridge VM to bring it back online. If the issue persists, contact Microsoft Support for assistance. You should not delete the Arc Resource Bridge VM without guidance from Microsoft Support.

Action failed - no such host

When you deploy Arc resource bridge, if you receive an error with `errorCode` as `PostOperationsError`, `errorResponse` as code `GuestInternetConnectivityError` and `no such host`, the appliance VM IPs may not be able to reach the endpoint specified in the error.

Error example:

```
{ _errorCode_: _PostOperationsError_, _errorResponse_: _{\n\_message\_: \_{\\n
 \\\_code\\\_: \\\_GuestInternetConnectivityError\\\_,\\n  \\\_message\\\_: \\\_Not able
to connect to http://aszhcitest01.company.org:55000. Error returned: action failed after
```

```
5 attempts: Get \\\\\\\_http://aszhcitest01.company.org:55000\\\\\\\_: dial tcp: lookup aszhcitest01.company.org: on 127.0.0.53:53: no such host. Arc Resource Bridge network and internet connectivity validation failed: cloud-agent-connectivity-test. 1. check your networking setup and ensure the URLs mentioned in : https://aka.ms/AAla73m are reachable from the Appliance VM.   2. Check firewall/proxy settings
```

In the example, the appliance VM IPs are unable to access `http://aszhcitest01.company.org:55000`, which is the MOC endpoint. Work with your network administrator to make sure that the DNS server is able to resolve the required URLs.

To test connectivity to the DNS server:

```
ping <dns-server.com>
```

To check if the DNS server is able to resolve an address, run this command from a machine that can reach the DNS servers:

```
Resolve-DnsName -Name "http://aszhcitest01.company.org:55000" -Server "<dns-server.com>"
```

Authentication required

You may receive the following error when deploying Arc resource bridge:

```
{ _message_: _Post
\_https://westeurope.dp.kubernetesconfiguration.azure.com/azure-arc-appliance-k8sagents/GetLatestHelmPackagePath?api-version=2019-11-01-preview\u0026releaseTrain=stable\_: authenticationrequired_ }
```

This error is likely due to a proxy intercepting the request that requires authentication. To successfully run Azure CLI behind such a proxy, ensure proper proxy support.

Recommended Actions:

1. Confirm whether a proxy is active in the environment.
2. If so, configure environment variables (HTTPS_PROXY, HTTP_PROXY, and optionally NO_PROXY) with authentication credentials if required. Refer to Azure Arc resource bridge network requirements.
3. You may also need to ensure that Azure CLI is able to work behind a proxy. For detailed instructions, refer to the Azure CLI proxy troubleshooting guide.

Azure Arc-enabled VMware VCenter issues

`errorResponse: error getting the vsphere sdk client`

Errors with `errorCode: CreateConfigKvaCustomerError` and `errorResponse: error getting the vsphere sdk client` occur when your deployment machine is trying to establish a TCP connection to your vCenter address but encounters a problem. This can happen when your vCenter address is incorrect (403 or 404 error), or because a network/proxy/firewall configuration blocks it (connection attempt failed).

If you enter your vCenter address as a hostname and receive the error `no such host`, then your deployment machine isn't able to resolve the vCenter hostname via the client DNS. This may occur when the deployment machine is able to resolve the vCenter hostname, but the deployment machine can't reach the IP address it received from DNS. You might also see this error if the endpoint returned by DNS isn't your vCenter address, or if the traffic was intercepted by proxy. If your deployment machine is able to communicate with your vCenter address, confirm that your username and password are correct.

vSphere SDK client - Connection attempt failed

If you receive an error during deployment that states: `errorCode_: _CreateConfigKvaCustomerError_, _errorResponse_: _error getting the vsphere sdk client: Post _https://ip.address/sdk_: dial tcp ip.address:443: connectex: A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because connected host has failed to respond._ }` then your management machine is unable to communicate with your vCenter server.

To resolve this issue, ensure that your management machine meets the management machine requirements and that there's not a firewall or proxy blocking communication.

vSphere SDK client - 403 Forbidden or 404 not found

Errors that contain `errorCode_: _CreateConfigKvaCustomerError_, _errorResponse_: _error getting the vsphere sdk client: POST \_/sdk\_: 403 Forbidden` or `404 not found` while deploying Arc resource bridge are most likely due to an incorrect vCenter address. This address is provided during configuration file creation, when you're prompted to enter the vCenter address as either a hostname or IP address.

There are different ways to find your vCenter address. One option is to access the vSphere client via its web interface. The vCenter hostname or IP address is typically what you use in the browser to access the vSphere client. If you're already logged in, you can look at the browser's address bar, where the URL you use to access vSphere is your vCenter server's hostname or IP address. Verify your vCenter address, then try the deployment again.

vSphere SDK client - no such host

The error `{ _errorCode_: _CreateConfigKvaCustomerError_, _errorResponse_: _error getting the vsphere sdk client: Post \_https://your.vcenter.hostname/sdk\_: dial tcp: lookup your.vcenter.hostname: no such host_ }` can occur during deployment when the deployment machine can't resolve the vCenter hostname to an IP address. This issue arises because the deployment process is attempting to establish a TCP connection from your deployment machine to the vCenter hostname, but the connection fails due to DNS resolution problems.

To fix this error, ensure the DNS configuration on your deployment machine is correct, verify that the DNS server is online, and check for a missing DNS entry for the vCenter hostname. You can test the DNS resolution by running `nslookup your.vcenter.hostname` or `ping your.vcenter.hostname` from the deployment machine. If you specified your vCenter address as a hostname, consider using the IP address directly instead.

Predeployment validation errors

When you deploy Arc resource bridge, you might see various `pre-deployment validation of your download\upload connectivity wasn't successful` errors, such as:

```
Pre-deployment validation of your download/upload connectivity wasn't successful. {\\n \\\_code\\\_: \\\_ImageProvisionError\\\_,\\n \\\_message\\\_: \\\_Post \\\\\\\_https://vcenter-server.com/nfc/unique-identifier/disk-0.vmdk\\\\\\\_: Service Unavailable
```

```
Pre-deployment validation of your download/upload connectivity wasn't successful. {\\n \\\_code\\\_: \\\_ImageProvisionError\\\_,\\n \\\_message\\\_: \\\_Post \\\\\\\_https://vcenter-server.com/nfc/unique-identifier/disk-0.vmdk\\\\\\\_: dial tcp 172.16.60.10:443: connectex: A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because connected host has failed to respond.
```

```
Pre-deployment validation of your download/upload connectivity wasn't successful. {\\n \\\_code\\\_: \\\_ImageProvisionError\\\_,\\n \\\_message\\\_: \\\_Post \\\\\\\_https://vcenter-server.com/nfc/unique-identifier/disk-0.vmdk\\\\\\\_: use of closed network connection.
```

```
Pre-deployment validation of your download/upload connectivity wasn't successful. {\\n \\\_code\\\_: \\\_ImageProvisionError\\\_,\\n \\\_message\\\_: \\\_Post
```

`\\\\\\\_https://vcenter-server.com/nfc/unique-identifier/disk-0.vmdk\\\\\\\_: dial tcp: lookup hostname.domain: no such host`

A combination of these errors usually indicates that the management machine has lost connection to the datastore, or that there's a networking issue causing the datastore to be unreachable. This connection is needed in order to upload the OVA from the management machine used to build the appliance VM in vCenter.

To fix the issue, reestablish the connection between the management machine and datastore, then try deploying Arc resource bridge again.

Time difference causing x509 certificate has expired

When you deploy Arc resource bridge, you may encounter the error:

```
Error: { _errorCode_: _PostOperationsError_, _errorResponse_: _{\n\_message\_: \_{\\n \\\_code\\\_: \\\_GuestInternetConnectivityError\\\_,\\n \\\_message\\\_: \\\_Not able to connect to https://msk8s.api.cdp.microsoft.com. Error returned: action failed after 3 attempts: Get \\\\\\\_https://msk8s.api.cdp.microsoft.com\\\\\\\_: x509: certificate has expired or isn't yet valid: current time 2022-01-18T11:35:56Z is before 2023-09-07T19:13:21Z. Arc Resource Bridge network and internet connectivity validation failed: http-connectivity-test-arc. 1. check your networking setup and ensure the URLs mentioned in : https://aka.ms/AAla73m are reachable from the Appliance VM. 2. Check firewall/proxy settings
```

This error is caused when there's a time difference between ESXi hosts and the management machine running the deployment commands for Arc resource bridge. To resolve this issue, turn on NTP time sync on the ESXi hosts, confirm that the management machine is also synced to NTP, then try the deployment again.

Clock skew error between appliance VM and management machine

If you encounter an error similar to the following:

```
"ErrorCode": "PostOperationsError", "errorResponse": "{\n\"message\": \"{\\n \\\"code\\\": \\\"ClockSkewError\\\",\\n \\\"message\\\": \\\"The time in Appliance VM is too far behind in the past compared to Management Machine : Time in Appliance VM is 2025-02-24T10:59:59Z, time in Management Machine is 2025-02-24T16:49:13Z. Max allowed difference is 30m0s. Recommendation: Please verify that the time of the workstation machine and the appliance VM are in sync.
```

This error is caused when there's a time difference between ESXi hosts and the management machine running the deployment commands for Arc resource bridge. To resolve this issue, turn on NTP time sync on the ESXi hosts, confirm that the management machine is also synced to NTP, then try the deployment again.

Resolves to multiple networks

When you deploy or upgrade Arc resource bridge, you may encounter an error similar to:

```
{ "ErrorCode": "PreflightcheckErrorOnPrem", "ErrorDetails": "Upgrade Operation Failed with error: \"{\\n \\\"code\\\": \\\"PreflightcheckError\\\",\\n \\\"message\\\": \\\"{\\\\n \\\\\\\"code\\\\\\\": \\\\\\\"InvalidEntityError\\\\\\\",\\\\n \\\\\\\"message\\\\\\\": \\\\\\\"Cannot retrieve vSphere Network 'vmware-azure-arc-01': path 'vmware-azure-arc-01' resolves to multiple networks\\\\\\\",\\\\n \\\\\\\"category\\\\\\\": \\\\\\\"\\\\\\\"\\\\n }\\\",\\n \\\"category\\\": \\\"\\\"\\n }\"" }
```

This error occurs when the vSphere network segment resolves to multiple networks, due to multiple vSphere network segments using the same name that is specified in the error. To fix this error, change the duplicate network name in vCenter (not the network with the appliance VM) or deploy Arc resource bridge on a different network.

Arc resource bridge status is disconnected

When running the initial Arc-enabled VMware onboarding script, you're prompted to provide a vSphere account. This account is stored locally within the Arc resource bridge as an encrypted Kubernetes secret. The account is used to allow the Arc resource bridge to interact with vCenter.

If the vSphere account stored locally within the resource bridge expires, your Arc resource bridge status can become disconnected. Update the credentials within Arc resource bridge and for Arc-enabled VMware by following the updating vSphere account credentials instructions.

Error during host configuration

If you use the same template to deploy and delete the Arc resource bridge multiple times, you might encounter the following error:

```
Appliance cluster deployment failed with error: Error: An error occurred during host configuration
```

To resolve this issue, manually delete the existing template. Then run az arcappliance prepare to download a new template for deployment.

Unable to find folders

When you deploy Arc resource bridge on VMware, you specify the folder in which the template and VM are created. The selected folder must be a VM and template folder type. Other types of folder, such as storage folders, network folders, or host and cluster folders, can't be used for the resource bridge deployment.

Cannot retrieve resource - resource not found or does not exist

When you deploy Arc resource bridge, you specify where the appliance VM is deployed as its location path. The appliance VM can't be moved from that location path. If any component within that path changes, such as the datastore or resource pool, then the appliance VM loses its Azure connection. If the Arc resource bridge location is changed and you try to upgrade, you might see errors similar to the following:

```
{\n \"code\": \"PreflightcheckError\",\n \"message\": \"{\\n \\\"code\\\": \\\"InvalidEntityError\\\",\\n \\\"message\\\": \\\"Cannot retrieve <resource> 'resource-name': <resource> 'resource-name' not found\\\"\\n }\"\n }"
```

```
{\n \"code\": \"PreflightcheckError\",\n \"message\": \"{\\n \\\"code\\\": \\\"InvalidEntityError\\\",\\n \\\"message\\\": \\\"The specified vSphere Datacenter '/VxRail-Datacenter' does not exist\\\"\\n }\"\n }"
```

To fix these errors, use one of these options:

- Move the appliance VM back to its original location and ensure RBAC credentials are updated for the location change.
- Create a resource with the same name, then move Arc resource bridge to that new resource, ensuring the original location path is recreated.
- For Arc-enabled VMware, run the Arc-enabled VMware disaster recovery script. The script deletes the appliance, deploys a new appliance, and reconnects the appliance with the previously deployed custom location, cluster extension, and Arc-enabled VMs.

vCenter account is locked out - Update credentials

Arc resource bridge uses the vCenter account provided to it during initial deployment to connect to vCenter. If the vCenter account is updated and the corresponding account info is not updated in Arc resource bridge, this may cause the account to lockout. To immediately update the credentials without waiting for the lockout period to expire, run the following command with the `--skipWait` flag:

```
az

az arcappliance update-infracredentials vmware --kubeconfig [REQUIRED] --address
[REQUIRED] --username [REQUIRED] --password [REQUIRED] --skipWait
```

If you need to retrieve the kubeconfig, you can run the following command:

```
az

az arcappliance get-credentials --resource-group [REQUIRED] --name [REQUIRED] --
credentials-dir [OPTIONAL]
```

> **Note**
>
> The Arc-enabled VMware cluster extension installed on the Arc resource bridge may also need the vCenter credentials to be updated. Refer to: Update the vSphere account credentials

Insufficient privileges

When you deploy or upgrade the resource bridge on VMware vCenter, you might see an error similar to:

```
{ ""code"": ""PreflightcheckError"", ""message"": ""{\n \""code\"":
\""InsufficientPrivilegesError\"",\n \""message\"": \""The provided vCenter account is
missing required vSphere privileges on the resource 'root folder (MoRefId: Folder:group-
d1)'. Missing privileges: [Sessions.ValidateSession]. add the privileges to the vCenter
account and try again. To review the full list of required privileges, go to
https://aka.ms/ARB-vsphere-privilege.\""\n }
```

When you deploy Arc resource bridge, you provide vCenter credentials. Arc resource bridge stores these vCenter credentials locally to interact with vCenter. To resolve the missing privileges issue, the vCenter account used by the resource bridge needs the following privileges in VMware vCenter:

Datastore:

- Allocate space
- Browse datastore
- Low level file operations

Folder:

- Create folder

vSphere Tagging:

- Assign or Unassign vSphere Tag

Network:

- Assign network

Resource:

- Assign virtual machine to resource pool
- Migrate powered off virtual machine
- Migrate powered on virtual machine

Sessions:

- Validate session

vApp:

- Assign resource pool
- Import

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 resource
  - Configure managedBy

    - Display connection settings
    - Extend virtual disk
    - Modify device settings
    - Query Fault Tolerance compatibility
    - Query unowned files
    - Reload from path
    - Remove disk
    - Rename
    - Reset guest information
    - Set annotation
    - Toggle disk change tracking
    - Toggle fork parent
    - Upgrade virtual machine compatibility
- Edit Inventory
    - Create from existing
    - Create new
    - Register
    - Remove
    - Unregister
- Guest operations
    - Guest operation alias modification
    - Guest operation modifications
    - Guest operation program execution
    - Guest operation queries
- Interaction
    - Connect devices
    - Console interaction
    - Guest operating system management by VIX API
    - Install VMware Tools
    - Power off
    - Power on
    - Reset
    - Suspend
- Provisioning
    - Allow disk access
    - Allow file access
    - Allow read-only disk access
    - Allow virtual machine download
    - Allow virtual machine files upload
    - Clone virtual machine
    - Deploy template

    - Mark as template
    - Mark as virtual machine
    - Customize guest
- Snapshot management
    - Create snapshot
    - Remove snapshot
    - Revert to snapshot

Next steps

Understand recovery operations for resource bridge in Azure Arc-enabled VMware vSphere disaster scenarios

If you don't see your problem here or you can't resolve your issue, try one of the following channels for support:

- Get answers from Azure experts through Microsoft Q&A.
- Connect with @AzureSupport, the official Microsoft Azure account for improving customer experience. Azure Support connects the Azure community to answers, support, and experts.
- Open an Azure support request

What is Azure Arc-enabled servers?

Summarize this article for me

Azure Arc-enabled servers lets you manage Windows and Linux physical servers and virtual machines hosted *outside* of Azure, on your corporate network or with another cloud provider. With Azure Arc, these machines that you host outside of Azure are considered hybrid machines, with a representation of each machine in Azure. You manage these hybrid machines in Azure Arc the same way you manage native Azure virtual machines.

When you connect a machine to Azure Arc, it's treated as a resource in Azure. Each connected machine has an Azure Resource ID, so you can include it in an Azure resource group along with other native Azure resources.

To connect hybrid machines to Azure, install the Azure Connected Machine agent on the machine. You can install the Connected Machine agent manually or at scale on multiple machines by using the deployment method that works best for your scenario.

> **Note**
>
> For additional guidance regarding the different services Azure Arc offers, see **Choosing the right Azure Arc service for machines**.

Supported cloud operations

When you connect your machine to Azure Arc-enabled servers, you can perform many operational functions, just as you would with native Azure virtual machines. The following list describes some of the key supported actions for connected machines.

- **Govern**:
  - Assign Azure machine configurations to audit settings inside the machine. For cost information, see the Azure Policy pricing guide.
- **Protect**:
  - Protect non-Azure servers by using Microsoft Defender for Endpoint, included through Microsoft Defender for Cloud, for threat detection, vulnerability management, and to proactively monitor for potential security threats. Microsoft Defender for Cloud presents the alerts and remediation suggestions from the threats detected.
  - Use Microsoft Sentinel to collect security-related events and correlate them with other data sources.
- **Configure**:

    - Use Azure Automation for frequent and time-consuming management tasks by using PowerShell and Python runbooks. Assess configuration changes for installed software, Microsoft services, Windows registry and files, and Linux daemons by using the Azure Monitor agent for change tracking and inventory.
    - Use Azure Update Manager to manage operating system updates for your Windows and Linux servers.
    - Use machine enrollment (preview) to automatically configure Arc-enabled servers with a curated set of features for monitoring, security, and management.
    - Perform post-deployment configuration and automation tasks by using supported Arc-enabled servers VM extensions for your non-Azure Windows or Linux machine.
- **Monitor**:
    - Monitor operating system performance and discover application components to monitor processes and dependencies with other resources by using VM insights.
    - Collect other log data, such as performance data and events, from the operating system or workloads running on the machine by using the Azure Monitor Agent. This data is stored in a Log Analytics workspace and contains properties specific to the machine, such as a Resource ID, to support resource-context log access.

To learn more about Azure monitoring, security, and update services across hybrid and multicloud environments, watch the following video.

https://www.youtube-nocookie.com/embed/mJnmXBrU1ao

> **Note**
>
> This service supports **Azure Lighthouse**, which lets service providers sign in to their own tenant to manage subscriptions and resource groups that customers have delegated.

Agent status

You can view the status for a connected machine in the Azure portal under **Azure Arc** > **Machines**.

The Connected Machine agent sends a regular heartbeat message to the service every five minutes. If the service stops receiving these heartbeat messages from a machine, the service considers that machine offline, and the status will change to **Disconnected** within 15 to 30 minutes. When the service receives a subsequent heartbeat message from the Connected Machine agent, the status automatically changes back to **Connected**.

If a machine remains disconnected for 45 days, its status might change to **Expired**. An expired machine can't be managed through Azure Arc until a server administrator disconnects and

then reconnects it to Azure. The expiration date of the managed identity's credential determines the exact date upon which a machine expires. The credential is valid for up to 90 days and renews every 45 days.

If a machine receives 429 error messages or shows intermittent connection statuses, it might be an incorrectly cloned machine. For more information, see Cloning guidelines.

Supported regions

For a list of supported regions with Azure Arc-enabled servers, see the Azure products by region page.

In most cases, you should select the Azure region geographically closest to your machine's location when you create the installation script. Data at rest is stored within the Azure geography containing the region you specify, which might affect your choice of region if you have data residency requirements.

Supported environments

Azure Arc-enabled servers supports the management of physical servers and virtual machines hosted *outside* of Azure. For specific details about supported environments, see the connected Machine agent prerequisites.

> **Note**
>
> Azure Arc-enabled servers isn't designed or supported to enable management of virtual machines running in Azure.

Service limits

There's no limit to the number of Arc-enabled servers and VM extensions you can deploy in a resource group or subscription. The standard 800 instance limit per resource group limit does apply to the Azure Arc Private Link Scope resource type.

Data residency

Azure Arc-enabled servers stores customer data. By default, customer data stays within the region the customer deploys the service instance in. For regions with data residency

requirements, customer data is always kept within the same region. For example, if you register the machine with Azure Arc using the East US region, data is stored in East US.

For example, instance metadata information about the connected machine is collected and stored in this region. This metadata includes the following information:

- Operating system name and version
- Computer name
- Computer fully qualified domain name (FQDN)
- Connected Machine agent version

Next steps

- Before evaluating or enabling Azure Arc-enabled servers across multiple hybrid machines, review the Connected Machine agent overview to understand requirements, technical details about the agent, and deployment methods.
- Try out Arc-enabled servers by using the Azure Arc Jumpstart.
- Review the Planning and deployment guide to plan for deploying Azure Arc-enabled servers at any scale and implement centralized management and monitoring.
- Explore the Cloud Adoption Framework Unified hybrid and multicloud operations guide and Identity and access management for Azure Arc-enabled servers.

Last updated on 02/26/2026

What is Azure Arc-enabled Kubernetes?

Azure Arc-enabled Kubernetes lets you attach Kubernetes clusters running anywhere so that you can manage and configure them in Azure. When you manage all your Kubernetes resources in a single control plane, you get a more consistent development and operation experience. This approach helps you run cloud-native apps anywhere and on any Kubernetes platform.

When you deploy Azure Arc agents to the cluster, the agents create a secure outbound connection to Azure.

Each Kubernetes cluster that you connect to Azure appears as its own resource in Azure Resource Manager. You can organize these clusters with resource groups and tagging, just like your other Azure resources.

Supported Kubernetes distributions

Azure Arc-enabled Kubernetes works with any Cloud Native Computing Foundation (CNCF) certified Kubernetes clusters. This support includes clusters running on other public cloud providers, such as Google Cloud Platform (GCP) or Amazon Web Services (AWS), and clusters running in your on-premises data center, such as VMware vSphere or Azure Local.

The Azure Arc team works with key industry partners to validate conformance of Kubernetes distributions with Azure Arc-enabled Kubernetes.

Arc-enabled Kubernetes scenarios and enhanced functionality

After you connect your Kubernetes clusters to Azure, you can use a wide variety of Azure services and features to manage your clusters at scale, such as:

- View all connected Kubernetes clusters for inventory, grouping, and tagging, along with your Azure Kubernetes Service (AKS) clusters.
- Configure clusters and deploy applications by using GitOps-based configuration management with Argo CD or Flux v2.
- View and monitor your clusters by using Azure Monitor.
- Enable threat protection by using Microsoft Defender for Containers.
- Manage and report on compliance by using Azure Policy.

- Connect to your Kubernetes clusters from anywhere, and manage access by using Azure role-based access control (Azure RBAC).
- Deploy machine learning workloads by using Azure Machine Learning for Kubernetes clusters.
- Deploy and manage Kubernetes applications from Microsoft Marketplace.
- Deploy services that allow you to take advantage of specific hardware, comply with data residency requirements, or enable new scenarios, such as Azure Arc-enabled data services or Event Grid on Kubernetes.
- Use Azure Kubernetes Fleet Manager and its Arc-enabled Kubernetes cluster extension to tackle hybrid and multicloud Kubernetes management challenges at scale.

> **Note**
>
> This service supports **Azure Lighthouse**, which lets service providers sign in to their own tenant to manage subscriptions and resource groups that customers have delegated.

Next steps

- Learn about best practices and design patterns through the Cloud Adoption Framework for hybrid and multicloud.
- Try out Azure Arc-enabled Kubernetes without provisioning a full environment by using the Azure Arc Jumpstart.
- See what's new with Azure Arc-enabled Kubernetes.
- Connect an existing Kubernetes cluster to Azure Arc.
- Help protect your cluster by following the guidance in the security book for Azure Arc-enabled Kubernetes.

Last updated on 03/24/2026

What are Azure Arc-enabled data services?

Azure Arc makes it possible to run Azure data services on-premises, at the edge, and in public clouds using Kubernetes and the infrastructure of your choice.

Currently, the following Azure Arc-enabled data services are available:

- SQL Managed Instance

For an introduction to how Azure Arc-enabled data services supports your hybrid work environment, see this introductory video:

https://learn.microsoft.com/Shows/Inside-Azure-for-IT/Choose-the-right-data-solution-for-your-hybrid-environment/player?format=ny

Always current

Azure Arc-enabled data services such as SQL Managed Instance enabled by Azure Arc receive updates on a frequent basis including servicing patches and new features similar to the experience in Azure. Updates from the Microsoft Container Registry are provided to you and deployment cadences are set by you in accordance with your policies. This way, on-premises databases can stay up to date while ensuring you maintain control. Because Azure Arc-enabled data services are a subscription service, you will no longer face end-of-support situations for your databases.

Elastic scale

Cloud-like elasticity on-premises enables you to scale databases up or down dynamically in much the same way as they do in Azure, based on the available capacity of your infrastructure. This capability can satisfy burst scenarios that have volatile needs, including scenarios that require ingesting and querying data in real time, at any scale, with sub-second response time.

Self-service provisioning

Azure Arc also provides other cloud benefits such as fast deployment and automation at scale. Thanks to Kubernetes-based orchestration, you can deploy a database in seconds using either GUI or CLI tools.

Unified management

Using familiar tools such as the Azure portal, Visual Studio Code, and the Azure CLI (`az`) with the `arcdata` extension, you can now gain a unified view of all your data assets deployed with Azure Arc. You are able to not only view and manage a variety of relational databases across your environment and Azure, but also get logs and telemetry from Kubernetes APIs to analyze the underlying infrastructure capacity and health. Besides having localized log analytics and performance monitoring, you can now leverage Azure Monitor for comprehensive operational insights across your entire estate.

Supported regions

To see the regions that currently support Azure Arc-enabled data services, go to Azure Products by Region - Azure Arc.

To get the region segment of a regional endpoint, remove all spaces from the Azure region name. For example, *East US 2* region, the region name is `eastus2`.

For example: `*.<region>.arcdataservices.com` should be `*.eastus2.arcdataservices.com` in the East US 2 region.

To see a list of all regions, run this command:

Azure CLI

```azurecli
az account list-locations -o table
```

Azure PowerShell

```azurepowershell
Get-AzLocation | Format-Table
```

Related content

> **Just want to try things out?**
> Get started quickly with Azure Arc Jumpstart on Azure Kubernetes Service (AKS), AWS Elastic Kubernetes Service (EKS), Google Cloud Kubernetes Engine (GKE) or in an Azure VM.
>
> In addition, deploy Jumpstart ArcBox for DataOps, an easy to deploy sandbox for all things SQL Managed Instance enabled by Azure Arc. ArcBox is designed to be completely self-contained within a single Azure subscription and resource group, which will make it easy for you to get hands-on with all available Azure Arc-enabled technology with nothing more than an available Azure subscription.

Install the client tools

Plan your Azure Arc data services deployment (requires installing the client tools first)

Create a SQL Managed Instance enabled by Azure Arc (requires creation of an Azure Arc data controller first)

Last updated on 02/05/2026

What is Azure Arc-enabled VMware vSphere?

Summarize this article for me

Azure Arc-enabled VMware vSphere is an Azure Arc service that helps you simplify management of a hybrid IT estate distributed across VMware vSphere and Azure. It extends the Azure control plane to VMware vSphere infrastructure and enables the use of Azure experiences for VM management and Azure services for consistent security, governance, monitoring, and patching across VMware vSphere on-premises private clouds, Azure VMware Solution (AVS) private clouds, and Azure.

Azure Arc-enabled VMware vSphere allows you to:

- Discover your VMware vSphere estate (VMs, templates, networks, datastores, clusters, hosts, and resource pools) and register resources with Azure at scale.
- Perform various virtual machine (VM) operations directly from Azure, such as create, resize, delete, and power cycle operations like start, stop, and restart on VMware VMs consistently with Azure.
- Empower developers and application teams to self-serve VM operations on-demand by using Azure role-based access control (RBAC).
- Install the Azure connected machine agent at scale on VMware VMs to govern, protect, configure, and monitor them.
- Browse your VMware vSphere resources (VMs, templates, networks, and storage) in Azure, providing you with a single pane view for your infrastructure across both environments.
- Build automation and self-service pipelines by using Python, Java, JavaScript, Go, and .NET SDKs; Terraform, ARM, and Bicep templates; Azure REST APIs, CLI, and PowerShell.
- Leverage Azure Arc benefits such as Windows Server management for VMs with Software Assurance licenses, Extended Security Updates benefits for Windows Server and SQL Server with pay-as-you-go billing for on-premises VMs and free SQL ESUs for AVS VMs.

For updates on the capabilities and enhancements of Azure Arc, see the Tech Community blog for Azure Arc.

How does it work?

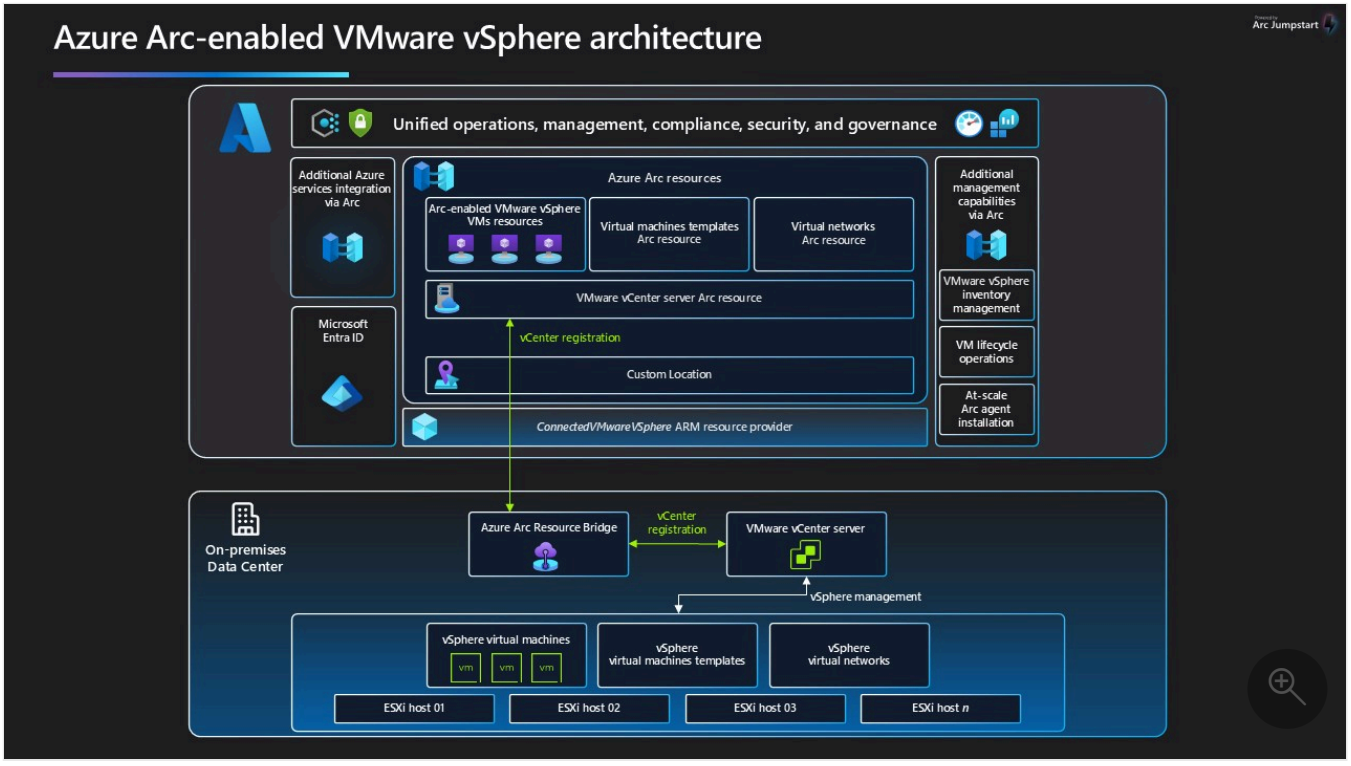
Azure Arc-enabled VMware vSphere provides these capabilities by integrating with your VMware vCenter Server. To connect your VMware vCenter Server to Azure Arc, you need to deploy the Azure Arc resource bridge in your vSphere environment. Azure Arc resource bridge is a virtual appliance that hosts the components that communicate with your vCenter Server and Azure.

When a VMware vCenter Server connects to Azure, it automatically discovers the inventory of vSphere resources. This inventory data is continuously kept in sync with the vCenter Server.

All guest OS-based capabilities are provided by enabling guest management (installing the Arc agent) on the VMs. Once guest management is enabled, you can install VM extensions to use the Azure management capabilities. You can perform virtual hardware operations such as resizing, deleting, adding disks, and power cycling without guest management enabled.

Architecture

The following image shows the architecture for the Azure Arc-enabled VMware vSphere:



How is Arc-enabled VMware vSphere different from Arc-enabled Servers

The easiest way to think of this difference is as follows:

- Azure Arc-enabled servers interact on the guest operating system level, with no awareness of the underlying infrastructure fabric and the virtualization platform that

they're running on. Since Arc-enabled servers also support bare-metal machines, some cases don't even include a host hypervisor.

- Azure Arc-enabled VMware vSphere is a superset of Arc-enabled servers that extends management capabilities beyond the guest operating system to the VM itself. This extension provides lifecycle management and CRUD (Create, Read, Update, and Delete) operations on a VMware vSphere VM. The Azure portal exposes these lifecycle management capabilities and they look and feel just like a regular Azure VM. Azure Arc-enabled VMware vSphere also provides guest operating system management - in fact, it uses the same components as Azure Arc-enabled servers.

You have the flexibility to start with either option, and incorporate the other one later without any disruption. With both options, you enjoy the same consistent experience.

> **Note**
>
> For guidance on choosing the right Azure Arc service for your virtual machines, see Choose the right Azure Arc service for machines.

Supported scenarios

- Azure Arc-enabled VMware vSphere currently works with vCenter Server versions 7 and 8 with a maximum of 9,500 VMs.
- You can onboard multiple vCenters by using a single Azure Arc resource bridge if the total number of VMs managed by these vCenters doesn't exceed 9,500 VMs.
- Azure Arc-enabled VMware vSphere works with Azure VMware Solution (AVS) private clouds.
- Virtualized Infrastructure Administrators and Cloud Administrators can connect a vCenter instance to Azure.
- Administrators can use the Azure portal to browse VMware vSphere inventory and register virtual machines, resource pools, networks, and templates into Azure.
- Administrators can provide app teams and developers fine-grained permissions on those VMware resources through Azure RBAC.
- App teams can use Azure interfaces (portal, CLI, PowerShell, SDKs, Terraform, Bicep, ARM templates, or REST API) to manage the lifecycle of on-premises VMs they use for deploying their applications (CRUD, Start/Stop/Restart).

- Administrators can install Azure Connected Machine agent on vCenter-managed VMs at scale and can perform the following actions:
  - **Govern**:
    - Assign Azure machine configurations to audit settings inside the machine.
  - **Protect**:
    - Protect non-Azure servers by using Microsoft Defender for Endpoint, included through Microsoft Defender for Cloud, for threat detection, for vulnerability management, and to proactively monitor for potential security threats. Microsoft Defender for Cloud presents the alerts and remediation suggestions from the threats detected.
    - Use Microsoft Sentinel to collect security-related events and correlate them with other data sources.
  - **Configure**:
    - Use Azure Automation for frequent and time-consuming management tasks by using PowerShell and Python runbooks. Assess configuration changes for installed software, Microsoft services, Windows registry and files, and Linux daemons by using the Azure Monitor agent for change tracking and inventory.
    - Use Azure Update Manager to manage operating system updates for Windows and Linux servers. Automate onboarding and configuration of a set of Azure services when you use Azure Automanage.
    - Perform post-deployment configuration and automation tasks by using supported Arc-enabled servers VM extensions for non-Azure Windows or Linux machine.
  - **Monitor**:
    - Monitor operating system performance and discover application components to monitor processes and dependencies with other resources by using VM insights.
    - Collect other log data, such as performance data and events, from the operating system or workloads running on the machine by using the Azure Monitor Agent. This data is stored in a Log Analytics workspace.

  Log data collected and stored in a Log Analytics workspace from the hybrid machine contains properties specific to the machine, such as a Resource ID, to support resource-context log access.

  Watch this video to learn more about Azure monitoring, security, and update services across hybrid and multicloud environments.

  https://www.youtube-nocookie.com/embed/mJnmXBrU1ao

- Administrators can install the Azure Connected Machine agent at scale and leverage Azure Arc benefits such as Windows Server management for VMs with Software Assurance licenses, and pay-as-you-go billing for Extended Security Updates for Windows Server and SQL Server VMs.

> **Important**
>
> Microsoft is retiring Azure Kubernetes Service on VMware (Preview) on March 16, 2026. We recommend you to deploy **AKS on Azure Local** to leverage AKS on-premises. After March 16, 2026, you can't deploy or receive support for Azure Kubernetes Service on VMware. If you have additional questions, contact us through the **AKS enabled by Azure Arc GitHub repository**.

Supported regions

For the most up-to-date information about region availability of Azure Arc-enabled VMware vSphere, see Azure Products by Region.

Data residency

Azure Arc-enabled VMware vSphere doesn't store or process customer data outside the region where the customer deploys the service instance. By default, customer data stays within the deployment region. For regions with data residency requirements, the service always keeps customer data within the same region.

Next steps

- Plan your resource bridge deployment by reviewing the support matrix for Arc-enabled VMware vSphere.
- When ready, connect VMware vCenter to Azure Arc using the helper script.
- To enable Arc for Azure VMware Solution (AVS) private cloud, see Deploy Arc-enabled VMware vSphere for Azure VMware Solution private cloud.
- Try out Azure Arc-enabled VMware vSphere by using the Azure Arc Jumpstart.
- Consider unified operations and plan for hybrid and multicloud environments with the Cloud Adoption Framework.
- Choose the Azure Hybrid solution that meets your business requirements with guidance from the Azure Architecture Center.

Last updated on 02/11/2026

Overview of Azure Arc-enabled System Center Virtual Machine Manager

Azure Arc-enabled System Center Virtual Machine Manager (SCVMM) empowers System Center customers to connect their VMM environment to Azure and perform VM self-service operations from Azure portal. By extending the Azure control plane to SCVMM managed infrastructure, Azure Arc-enabled SCVMM enables you to use Azure security, governance, and management capabilities consistently across your System Center managed estate and Azure.

By using Azure Arc-enabled SCVMM, you can manage your hybrid environment consistently and perform self-service VM operations through Azure portal. For Microsoft Azure Pack customers, this solution is intended as an alternative to perform VM self-service operations.

Azure Arc-enabled SCVMM allows you to:

- Perform various VM lifecycle operations such as start, stop, pause, and delete VMs on SCVMM managed VMs directly from Azure.
- Empower developers and application teams to self-serve VM operations on demand by using Azure role-based access control (RBAC).
- Browse your VMM resources (VMs, templates, VM networks, and storage) in Azure, providing you with a single pane view for your infrastructure across both environments.
- Discover and onboard existing SCVMM managed VMs to Azure.
- Install the Azure Connected Machine agent at scale on SCVMM VMs to govern, protect, configure, and monitor them.
- Build automation and self-service pipelines by using Python, Java, JavaScript, Go, and .NET SDKs; Terraform, ARM, and Bicep templates; Azure REST APIs, CLI, and PowerShell.
- Leverage Azure Arc benefits such as Windows Server management for VMs with Software Assurance licenses, and pay-as-you-go billing for Extended Security Updates for Windows Server and SQL Server VMs.

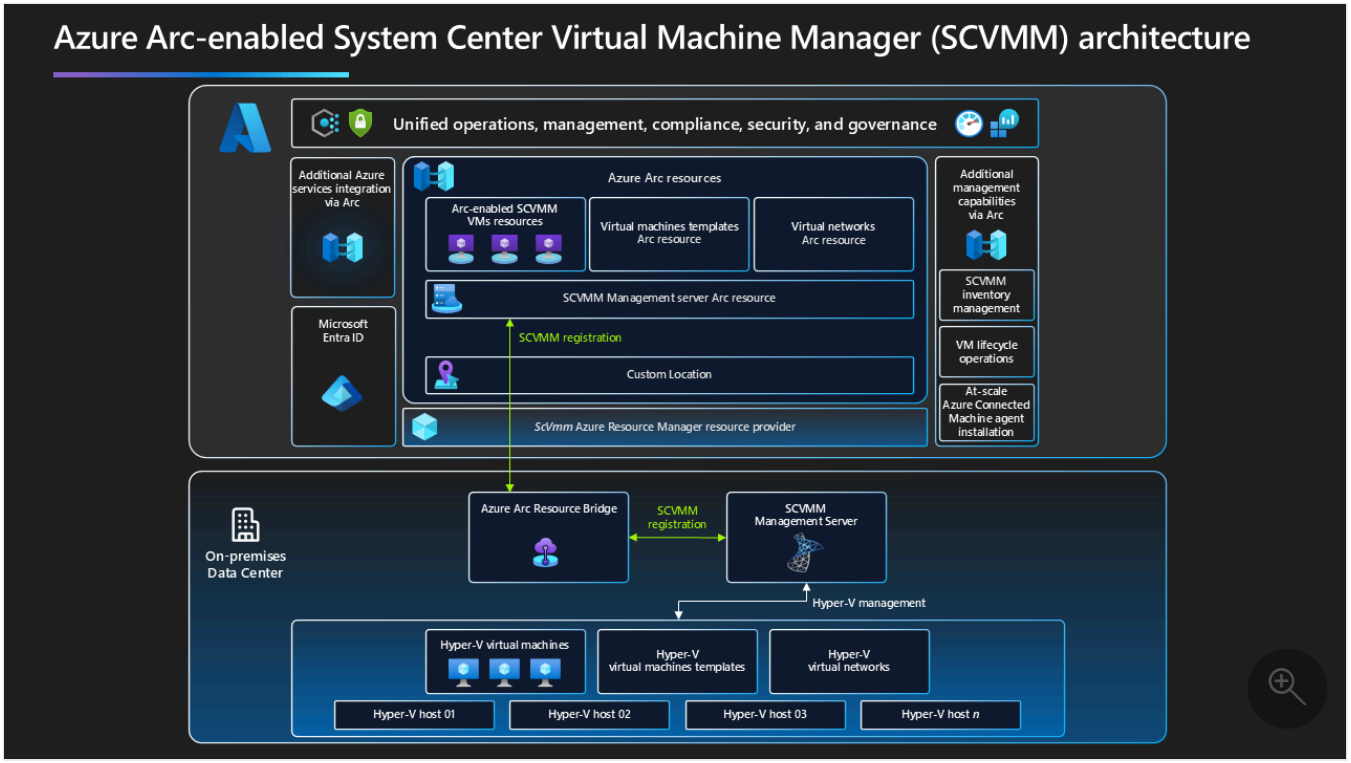
For updates on the capabilities and enhancements of Azure Arc, see the Tech Community blog for Azure Arc.

How does it work?

To Azure Arc-enable an SCVMM management server, deploy Azure Arc resource bridge in the VMM environment. Azure Arc resource bridge is a virtual appliance that connects VMM management server to Azure. By using Azure Arc resource bridge, you can represent the SCVMM resources (clouds, VMs, templates, and more) in Azure and perform various operations on them.

Architecture

The following image shows the architecture for the Azure Arc-enabled SCVMM:



To download architecture diagrams in high resolution, visit Jumpstart Gems.

How is Azure Arc-enabled SCVMM different from Azure Arc-enabled servers

- Azure Arc-enabled servers interact on the guest operating system level, with no awareness of the underlying infrastructure fabric and the virtualization platform that they're running on. Since Azure Arc-enabled servers also support bare-metal machines, a host hypervisor might not exist in some cases.
- Azure Arc-enabled SCVMM is a superset of Azure Arc-enabled servers that extends management capabilities beyond the guest operating system to the VM itself. This extension provides lifecycle management and CRUD (Create, Read, Update, and Delete) operations on an SCVMM VM. The Azure portal exposes these lifecycle management capabilities, and they look and feel just like a regular Azure VM. Azure Arc-enabled SCVMM also provides guest operating system management by using the same components as Azure Arc-enabled servers.

You can start with either option and add the other one later without any disruption. Both options provide the same consistent experience.

> ⓘ Note
>
> For guidance on choosing the right Azure Arc service for your virtual machines, see Choose the right Azure Arc service for machines.

Supported scenarios

Azure Arc-enabled SCVMM supports the following scenarios:

- SCVMM administrators can connect a VMM instance to Azure and browse the SCVMM virtual machine inventory in Azure.
- Administrators can use the Azure portal to browse SCVMM inventory and register SCVMM cloud, virtual machines, VM networks, and VM templates into Azure.
- Administrators can provide app teams/developers fine-grained permissions on those SCVMM resources through Azure RBAC.
- App teams can use Azure interfaces (portal, CLI, PowerShell, SDKs, Terraform, Bicep, ARM templates, or REST API) to manage the lifecycle of on-premises VMs they use for deploying their applications (CRUD, Start/Stop/Restart).
- Administrators can install Azure Connected Machine agent on SCVMM-managed VMs at-scale and can perform the following actions:
  - **Govern**:
    - Assign Azure machine configurations to audit settings inside the machine.
  - **Protect**:
    - Protect non-Azure servers with Microsoft Defender for Endpoint, included through Microsoft Defender for Cloud, for threat detection, for vulnerability management, and to proactively monitor for potential security threats. Microsoft Defender for Cloud presents the alerts and remediation suggestions from the threats detected.
    - Use Microsoft Sentinel to collect security-related events and correlate them with other data sources.
  - **Configure**:
    - Use Azure Automation for frequent and time-consuming management tasks using PowerShell and Python runbooks. Assess configuration changes for installed software, Microsoft services, Windows registry and files, and Linux daemons using the Azure Monitor agent for change tracking and inventory.
    - Use Azure Update Manager to manage operating system updates for Windows and Linux servers. Automate onboarding and configuration of a set of Azure services when you use Azure Automanage.

    - Perform post-deployment configuration and automation tasks using supported Arc-enabled servers VM extensions for non-Azure Windows or Linux machine.
  - **Monitor**:
    - Monitor operating system performance and discover application components to monitor processes and dependencies with other resources using VM insights.
    - Collect other log data, such as performance data and events, from the operating system or workloads running on the machine with the Azure Monitor Agent. This data is stored in a Log Analytics workspace.

  Log data collected and stored in a Log Analytics workspace from the hybrid machine contains properties specific to the machine, such as a Resource ID, to support resource-context log access.

  Watch this video to learn more about Azure monitoring, security, and update services across hybrid and multicloud environments.

  https://www.youtube-nocookie.com/embed/mJnmXBrU1ao

- Administrators can install the Azure Connected Machine agent at scale and leverage Azure Arc benefits such as Windows Server management for VMs with Software Assurance licenses, and pay-as-you-go billing for Extended Security Updates for Windows Server and SQL Server VMs.

Unsupported scenarios

Azure Arc-enabled SCVMM doesn't support:

- Azure-based management of VMware vCenter VMs managed by SCVMM. To onboard VMware VMs to Azure Arc, use Azure Arc-enabled VMware vSphere.
- Azure-based management of Azure Local VMs managed by SCVMM. To onboard Azure Local VMs to Azure Arc, use Azure Arc VM management capabilities of Azure Local.

Supported VMM versions

Azure Arc-enabled SCVMM works with VMM 2025, 2022, and 2019 versions. It supports SCVMM management servers with a maximum of 15,000 VMs.

Supported regions

For the most up-to-date information about regional availability of Azure Arc-enabled SCVMM, see Product Availability by Region.

Data residency

Azure Arc-enabled SCVMM stores customer data. By default, customer data stays within the region the customer deploys the service instance in. For regions with data residency requirements, customer data is always kept within the same region.

Next steps

- Plan your Azure Arc-enabled SCVMM deployment by reviewing the support matrix.
- When ready, connect your SCVMM management server to Azure Arc using the onboarding script.
- Deliver operations Management disciplines using hybrid and multicloud tools in Cloud adoption Framework.
- Cloud Adoption Framework introduces Azure hybrid and multicloud products on Azure.

Last updated on 02/09/2026

What is Azure Local VM management?

> Applies to: Hyperconverged deployments of Azure Local

This article provides an overview of virtual machine (VM) management in hyperconverged deployments of Azure Local (*formerly Azure Stack HCI*), including its benefits, components, and a high-level workflow.

Azure Local VM management enables IT admins to provision and manage Windows and Linux VMs hosted in an on-premises Azure Local environment. IT admins can use the feature to create, modify, delete, and assign permissions and roles to app owners, thereby enabling self-service VM management.

Administrators can manage Azure Local VMs enabled by Azure Arc on their Azure Local instances by using Azure management tools, including the Azure portal, the Azure CLI, Azure PowerShell, and Azure Resource Manager templates. By using Azure Resource Manager templates, you can also automate VM provisioning in a secure cloud environment.

To find answers to frequently asked questions about Azure Local VM management, see the FAQ.

Benefits of Azure Local VM management

Although Hyper-V provides capabilities to manage your on-premises VMs, Azure Local VMs offer many benefits over traditional on-premises tools. These benefits include:

- Role-based access control (RBAC) via built-in Azure Local roles enhances security by ensuring that only authorized users can perform VM management operations. For more information, see Use role-based access control to manage Azure Local virtual machines.
- Azure Local VM management provides the ability to deploy with Resource Manager templates, Bicep, and Terraform.
- The Azure portal acts as a single pane of glass to manage VMs on Azure Local and Azure VMs. With Azure Local VM management, you can perform various operations from the Azure portal or the Azure CLI, including:
  - Create, manage, update, and delete VMs. For more information, see Create Azure Local VMs enabled by Azure Arc.

    - Create, manage, and delete VM resources such as virtual disks, logical networks, network interfaces, and VM images.

- The self-service capabilities of Azure Local VM management reduce administrative overhead.

Limitations of Azure Local VM management

Consider the following limitations when you're managing VMs on Azure Local:

- Changes to VM configurations, such as static network interface IP, or data disk configuration made either within the VM or through local management tools will not be reflected in Azure.

- Moving a resource group isn't supported for VMs on Azure Local and its associated resources (such as network interfaces and disks).

- Azure has limitations on subscriptions and services. For more information, see Azure subscription and service limits, quotas, and constraints.

- Creation of VMs by using Windows Server 2012 and Windows Server 2012 R2 images isn't supported via the Azure portal. You can do it only via the Azure CLI. See Additional parameters for Windows Server 2012 and Windows Server 2012 R2 images.

  Azure Local VMs running Windows Server 2012 and Windows Server 2012 R2 do not support enabling guest management as it lacks Hyper-V sockets support which is required for this feature. For more information on Hyper-V sockets, see Make your own integration services.

- Azure Local VMs only support IPv4 addresses. IPv6 addresses aren't supported.

- Once a logical network is created, you can't update the following:
    - Default gateway
    - IP pools
    - IP address space
    - VLAN ID
    - Virtual switch name

- Azure Local doesn't support provisioning an Azure Local VM using an IP address that is configured as the DNS server or a gateway on the same logical network.

> **Note**
>
> Taking a VM checkpoint locally is only supported for Azure Local 2504 and later.

Components of Azure Local VM management

Azure Local VM management has several components, including:

- **Azure Arc resource bridge**: A prepackaged virtual appliance that runs as a virtual machine (VM) on your Azure Local cluster. It hosts an Azure Arc-enabled Kubernetes cluster that acts as the management cluster and enables the projection of on-premises resources such as VMs, logical networks, network interfaces, disks, and other related resources into Azure for cloud-based management. The Azure Arc resource bridge is created automatically when you deploy Azure Local. The Arc resource bridge appears:
  - **In Azure**: as an Azure resource named <*instance-name*>-arcbridge
  - **On the local cluster**: as a VM named <*GUID*>-control-plane-<*GUID*>

    > **Important**
    >
    > Azure Arc resource bridge is a critical component for Azure Local VM management and should not be deleted unless you plan to reimage or decommission your Azure Local instance. Deleting this resource results in loss of the Azure control plane used to manage Azure Local VMs.
    >
    > If you need to delete the Arc resource bridge, do so only after you've deleted all Azure resources associated with workload management, including:
    > - Azure Local VMs
    > - AKS Arc clusters
    > - VM images
    > - Storage paths
    > - Logical networks
    > - Network interfaces
    > - Virtual hard disks
    > - Network security groups

To delete the Arc resource bridge, follow the guidance here: [Azure Arc resource bridge deployment command overview](#).

For more information, see What is Azure Arc resource bridge?.

- **Infrastructure logical network**: A logical network associated with the Azure Local VM management and is created automatically when you deploy Azure Local. The Azure Arc resource bridge, a crucial component of Azure Local VM management, uses this logical network.

  For more information, see Manage logical networks for Azure Local VMs enabled by Azure Arc.

- **Custom location**: An Azure resource that represents a target location for deploying Azure Local VMs and other associated resources. You can think of it as your organization's private Azure region. By selecting a custom location, Azure understands where and how to deploy resources within your Azure Local environment.

  Just like the Azure Arc resource bridge, a custom location is created automatically when you deploy Azure Local. It represents your Azure Local instance as a target location for deploying Azure resources. Custom locations bring Azure's consistent deployment model to Azure Local by abstracting away the underlying infrastructure details. Virtual machine administrators can deploy Azure resources such as VMs, disks, and network interfaces directly from Azure by simply choosing the custom location, without needing to interact directly with the underlying infrastructure.

  Each Azure Local instance has one custom location, and each custom location has a one-to-one mapping to the Azure Arc-enabled Kubernetes cluster namespace running inside the Azure Arc resource bridge.

  > **Important**
  >
  > The custom location should only be deleted after the Arc resource bridge has been deleted.

- **Kubernetes cluster extension for Azure Local VMs**: This extension is a Kubernetes controller installed into the Azure Arc-enabled Kubernetes management cluster hosted inside the Azure Arc resource bridge. This extension implements the core business logic for Azure Local VM lifecycle management. It orchestrates fabric operations such as power

operations, attaching and detaching disks and network interfaces, and GPU assignment on Azure Local VMs. The cluster extension processes requests from Azure Resource Manager (ARM), triggered by customer-initiated actions from the Azure control plane, and executes them locally on the Azure Local cluster.

By integrating these components, Azure Arc offers a unified and efficient VM management solution that bridges the gap between on-premises and cloud infrastructures.

Azure Local VM management workflow

In this release, the Azure Local VM management workflow is as follows:

1. During your deployment of Azure Local, one Azure Arc resource bridge is installed per cluster. A custom location is also created.
2. You assign built-in RBAC roles for Azure Local VM management.
3. You create VM resources such as:
   a. Storage paths for VM disks.
   b. VM images, starting with an image in Azure Marketplace, in an Azure Storage account, or in a local share. These images are then used with other VM resources to create VMs.
   c. Logical networks.
   d. VM network interfaces.
4. You use the VM resources to create VMs.

To troubleshoot problems with your VMs or to learn about known issues and limitations, see Troubleshoot Azure Local VM management.

Related content

- Azure Local VM management prerequisites

Last updated on 04/22/2026

SQL Server enabled by Azure Arc

Applies to: SQL Server

SQL Server enabled by Azure Arc extends Azure services to SQL Server instances hosted outside of Azure:

- In your data center
- In edge site locations like retail stores
- On any public cloud or hosting provider

Managing SQL Server through Azure Arc can also be configured for SQL Server VMs in Azure VMware Solution. See Deploy Arc-enabled Azure VMware Solution.

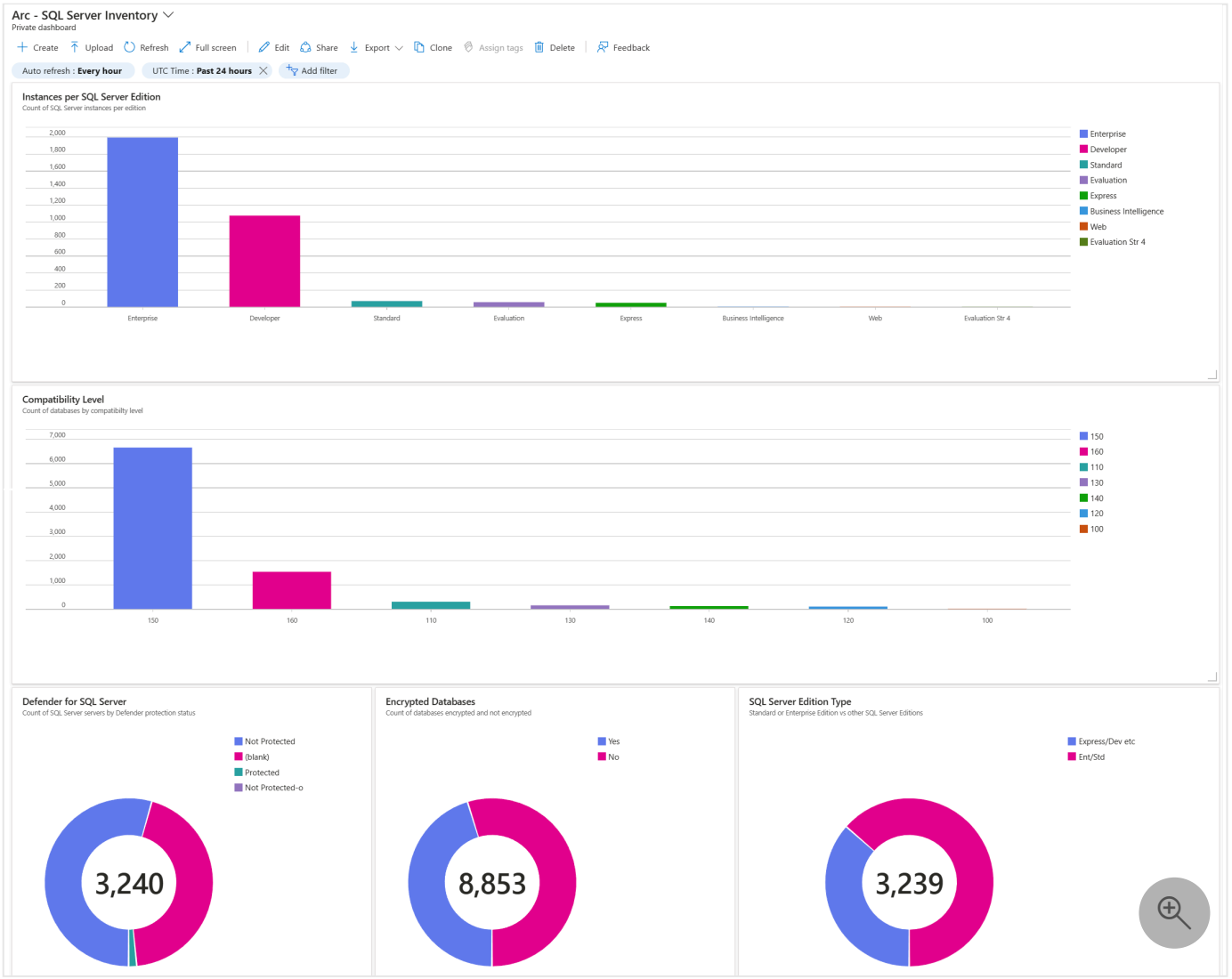
Manage your SQL Server instances at scale from a single point of control

Azure Arc enables you to manage all of your SQL Server instances from a single point of control: Azure. As you connect your SQL Server instances to Azure, you get a single place to view the detailed inventory of your SQL Server instances and databases.

- Look at details for a given SQL Server in the Azure portal such as the name, version, edition, number of cores, and host operating system.
- Query across all of your SQL Server instances using Azure Resource Graph Explorer to answer questions like:
  - "How many SQL Server instances do I have that are SQL Server 2014?"
  - "What are the names of all the SQL Server instances that are running on Linux?"
- Quickly create charts from these queries and pin them to customizable dashboards.
- View a list of every database on a SQL Server and do cross-SQL Server queries of databases to see:
  - Databases that haven't been backed up recently.
  - Databases that aren't encrypted.
- Execute custom T-SQL scripts across onboarded instances using Azure Arc-enabled servers Run Command to gather specific information like permissions, configurations, or compliance data, then aggregate results centrally for reporting and analysis.

Example custom dashboard

Review an example of a custom dashboard in GitHub microsoft/sql-server-samples.



Best practices assessment

You can optimize the configuration of your SQL Server instances for best performance and security by running a best practices assessment. The assessment report shows you specific ways to improve your configuration. The assessment compares your configuration to best practices established by Microsoft Support through many years of real-world experience. Each suggestion includes the details on how to change the configuration.

Microsoft Entra authentication

> **Note**
>
> Microsoft Entra ID was previously known as Azure Active Directory (Azure AD).

Azure Arc enabled SQL Servers can utilize Microsoft Entra ID for authentication. This feature brings a modern centralized identity and access management solution to SQL Server. This feature requires SQL Server 2022 (16.x) or later.

Microsoft Entra authentication provides greatly enhanced security over traditional username and password-based authentication, which is **not recommended**. For more information about the risks and challenges passwords pose, refer to "What's the solution to the growing problem of passwords?" .

Microsoft Entra authentication removes the need for self-managed secrets entirely when communicating with Azure resources, through managed identity authentication. For user-based authentication, Microsoft Entra ID supports enhanced security measures including multifactor authentication (MFA), single sign-on (SSO), and modern identity practices.

Microsoft Defender for Cloud

Microsoft Defender for Cloud helps you discover and mitigate potential database vulnerabilities and alerts you to anomalous activities. These activities might indicate threats to your databases on SQL Server instances enabled for Azure Arc.

- Vulnerability assessment: Scan databases to discover, track, and remediate vulnerabilities.
- Threat protection: Receive detailed security alerts and recommended actions based on SQL Advanced Threat Protection to provide to mitigate threats.

When you enable Microsoft Defender through SQL Server enabled by Azure Arc, you can get substantial cost savings on Defender.

Microsoft Purview

Microsoft Purview provides a unified data governance solution to help manage and govern your on-premises, multicloud, and software as a service (SaaS) data. Easily create a holistic, up-to-date map of your data landscape with automated data discovery, sensitive data classification, and end-to-end data lineage. Enable data consumers to access valuable, trustworthy data management.

SQL Server enabled by Azure Arc powers some of the Microsoft Purview features such as access policies and it generally makes it easier for you to get your SQL Server instances connected into Purview.

Pay-as-you-go for SQL Server

Now, with SQL Server enabled by Azure Arc, you have the option of purchasing SQL Server using a 'pay-as-you-go' model instead of purchasing licenses. This model is a great alternative if you're looking to save costs on SQL Server instances that have variable demand for compute capacity over time. For example, when you can turn off a SQL Server at night or on weekends, or even just scale down the number of cores used during less busy times. It's also a great option if you only plan to use a SQL Server for a short period of time and then won't need it anymore. Pay-as-you-go, billed through Azure, is now available for all versions of SQL Server from 2012 to 2022.

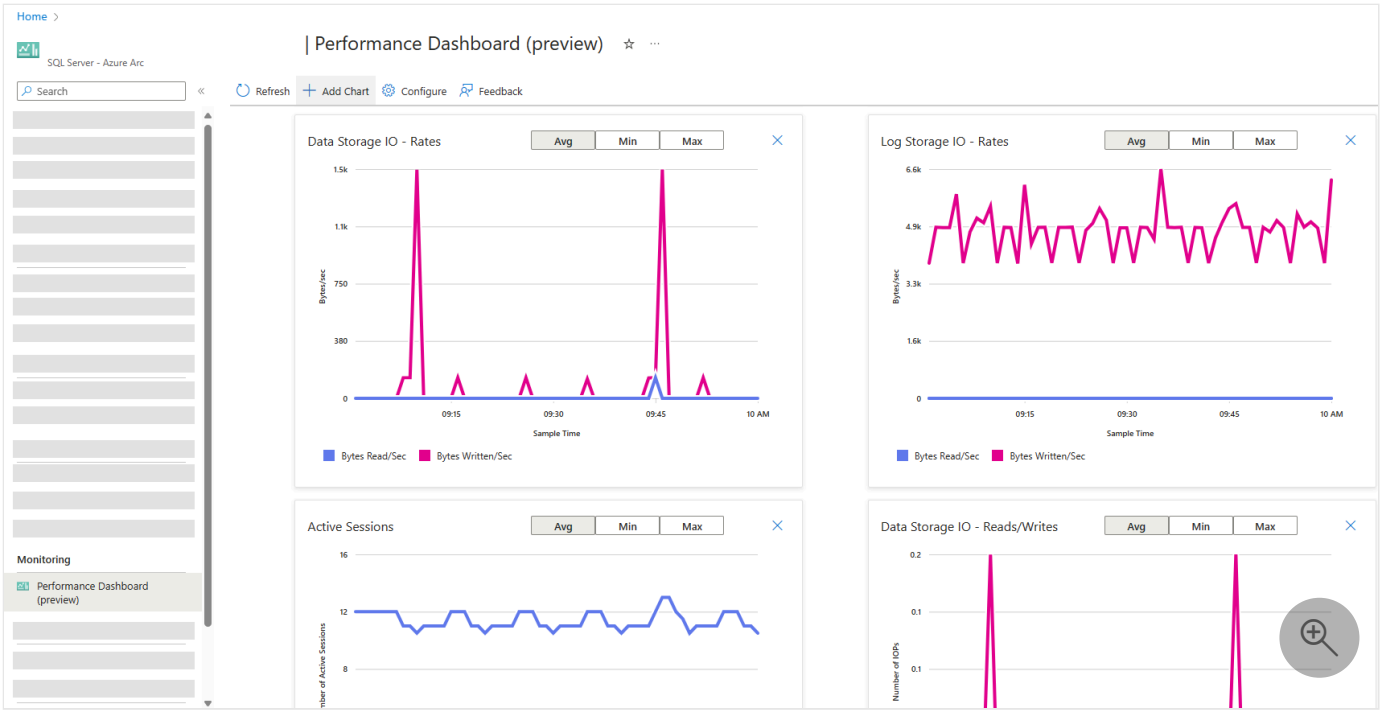
> **Note**
>
> On Linux, certain PAYG features aren't available, including automatic passive instance detection and connected user verification. All SQL Server instances on Linux are billed as active. For details, see Manage licensing and billing.

Extended Security Updates (ESU)

Once SQL Server has reached the end of its support lifecycle, you can sign up for an Extended Security Update (ESU) subscription for your servers and remain protected for up to three years. When you upgrade to a newer version of SQL Server, your ESU subscription is automatically canceled. When you migrate to Azure SQL, the ESU charges automatically stop but you continue to have access to the ESUs.

Performance dashboards

Monitor SQL Server instances from Azure portal with performance dashboards. Performance dashboards simplify performance monitoring in Azure portal.



For details, see Monitor SQL Server enabled by Azure Arc (preview).

Organizations can also build custom KQL dashboards and alerts over custom tables populated through the Logs Ingestion API, such as centralized SQL permissions results, complementing the built-in performance and assessment experiences.

Migration assessment

SQL Server enabled by Azure Arc migration assessment is a crucial tool for your cloud migration and modernization journey. It simplifies the discovery and readiness assessment for migration by providing:

- Cloud readiness analysis
- Identification of risks and mitigation strategies
- Recommendations for the specific service tier and Azure SQL configuration (SKU size) that best fits the workload needs
- Automatic generation of the assessment
- Continuous running on a default schedule of once per week
- Availability for all SQL Server editions

Migration assessment is for SQL Servers located in various environments, including your data center, edge sites, or any public cloud or hosting provider. It is available for any instance of SQL Server that is enabled by Azure Arc.

For details, review Configure SQL best practices assessment - SQL Server enabled by Azure Arc.

Custom data collection pipeline

For organizations requiring custom datasets beyond the built-in telemetry, an optional data collection pipeline can be implemented. This pipeline uses an Azure Automation Runbook authenticated with a Microsoft Entra ID service principal to:

1. Enumerate Arc-enabled SQL Server resources using Azure Resource Manager APIs
2. Invoke Azure Arc-enabled servers Run Command to execute T-SQL scripts on each host
3. Collect and process script output
4. Send results to Azure Monitor Log Analytics via a Data Collection Endpoint and Data Collection Rule using the Logs Ingestion API

This approach operates independently of the Azure Monitoring Agent and enables custom reporting scenarios like centralized permission auditing, compliance checks, or configuration validation.

For security best practices when implementing at-scale operations, including RBAC requirements, identity management, and network security, see Security overview | SQL Server enabled by Azure Arc.

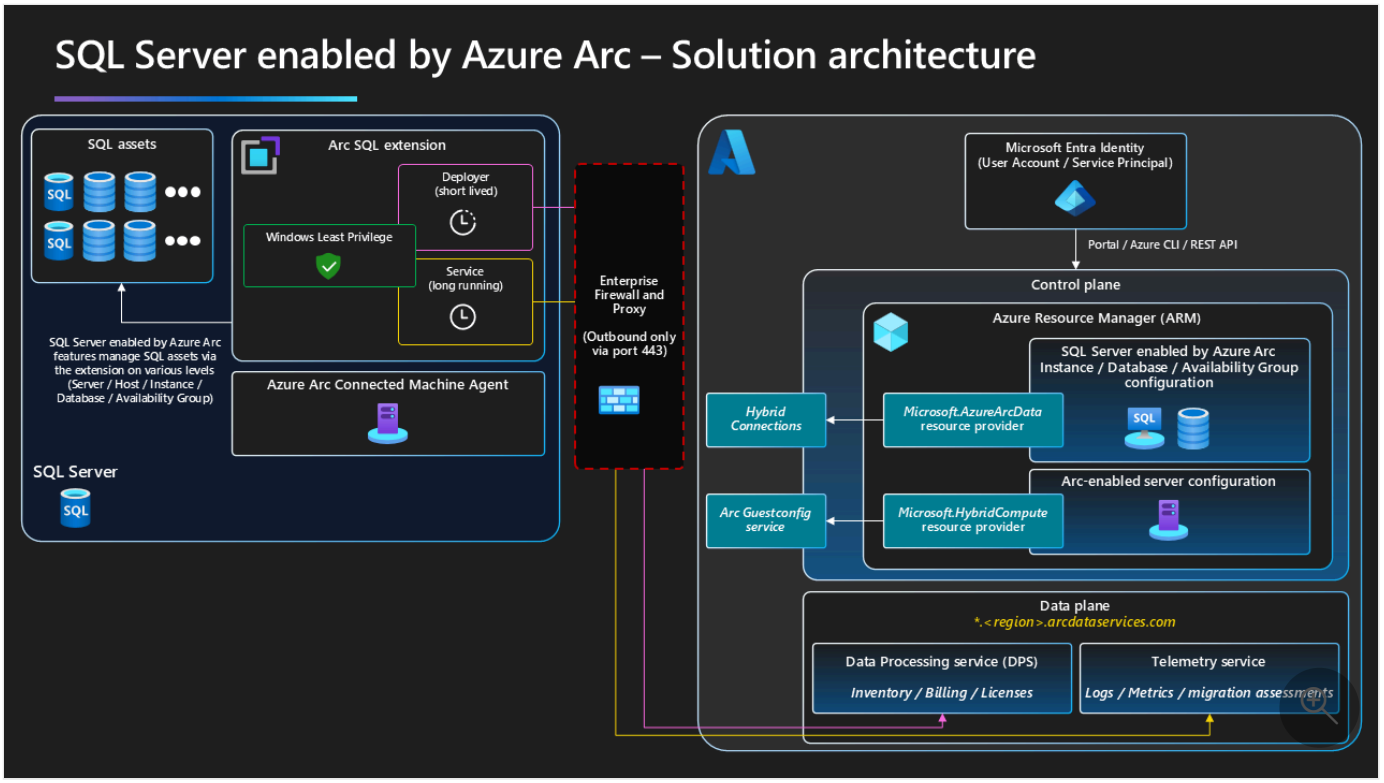
Architecture

The SQL Server instance that you want to enable with Azure Arc can be installed in a virtual or physical machine running Windows or Linux. The Azure Connected Machine agent and the Azure Extension for SQL Server securely connect to Azure to establish communication channels with multiple Azure services using only outbound HTTPS traffic on TCP port 443 using Transport Layer Security (TLS). The Azure Connected Machine agent can communicate through a configurable HTTPS proxy server over Azure Express Route, Azure Private Link or over the Internet. Review the overview, network requirements, and prerequisites for the Azure Connected Machine agent.

> **Important**
>
> Only Azure extension for SQL Server versions released within the last year are supported.

Some of the services provided by SQL Server enabled by Azure Arc, such as Microsoft Defender for Cloud and best practices assessment, require the Azure Monitoring agent (AMA) extension to be installed and connected to an Azure Log Analytics workspace for data collection and reporting.

The following diagram illustrates the architecture of SQL Server enabled by Azure Arc.



> **Note**
>
> To download this architecture diagram in high-resolution, visit Jumpstart Gems.

Supported Azure regions

SQL Server enabled by Azure Arc is available in the following regions:

- East US
- East US 2
- West US
- West US 2
- West US 3
- Central US
- North Central US
- South Central US
- West Central US
- US Government Virginia [1]
- Canada Central
- Canada East
- UK South

- UK West
- France Central
- West Europe
- North Europe
- Switzerland North
- Central India
- Brazil South
- South Africa North
- UAE North
- Japan East
- Korea Central
- Southeast Asia
- Australia East
- Sweden Central
- Norway East

[1] Not all features are supported yet in the US Government Virginia region. For details, review SQL Server enabled by Azure Arc in US Government.

> **Important**
>
> - For successful onboarding and functioning, assign the same region to both Arc-enabled Server and Arc-enabled SQL Server.

Feature availability depending on license type

The following table identifies the capabilities and use rights offered with each license type:

Expand table

Capability and use rights	License only	License with Software Assurance or SQL Server subscription	Pay-as-you-go subscription
Free new version upgrade	No	Yes	Yes
High availability and disaster recovery benefit	No	Yes	Yes

Capability and use rights	License only	License with Software Assurance or SQL Server subscription	Pay-as-you-go subscription
Unlimited virtualization with Enterprise edition	No	Yes	Yes
Flexible Virtualization Benefit licensing guide	No	Yes	Yes
Option to license by virtual machine	No	Yes	Yes
Free Power BI Report Server license	Yes[1]	Yes	Yes
180-day dual-use benefit	No	Yes	Yes
Connect your SQL Server to Azure Arc[2]	Yes	Yes	Yes
ESU Subscription	No	Yes	Yes
SQL Server inventory	Yes	Yes	Yes
Best practices assessment	No	Yes	Yes
Migration readiness	Yes	Yes	Yes
Database migration	Yes	Yes	Yes
Detailed inventory	Yes	Yes	Yes
Microsoft Entra authentication	Yes	Yes	Yes
Microsoft Defender for Cloud	Yes	Yes	Yes
Govern through Microsoft Purview	Yes	Yes	Yes
Automated backups to local storage (preview)	No	Yes	Yes
Point-in-time restore	No	Yes	Yes
Automatic updates	No	Yes	Yes
Failover cluster instances	Yes	Yes	Yes
Always On availability groups	Yes	Yes	Yes
Monitoring (preview)	No	Yes	Yes
Client connection summary	No	Yes	Yes

Capability and use rights	License only	License with Software Assurance or SQL Server subscription	Pay-as-you-go subscription
Operate with least privilege	Yes	Yes	Yes

[1] For SQL Server 2022 (16.x) and earlier versions, the free Power BI Report Server license is limited to Enterprise Edition (EE) customers with Software Assurance (SA) or subscriptions. For SQL Server 2025 (17.x), the free Power BI Report Server license is available to both Standard Edition (SE) and Enterprise Edition (EE) customers with all license types.

[2] Connecting SQL Server to Azure Arc is subject to outsourcing rules.

Feature availability by operating system

The following table identifies features available by operating system:

Expand table

Feature	Windows	Linux
Discover and register SQL Server instances in Azure	Yes	Yes
Azure pay-as-you-go billing	Yes	Yes [2]
Install Azure extension for SQL Server during setup [1]	Yes	No
Best practices assessment	Yes	No
Migration assessment	Yes	No
Database migration	Yes	No
Detailed inventory	Yes	No
Microsoft Entra ID authentication [1]	Yes	Yes
Microsoft Defender for Cloud	Yes	No
Microsoft Purview	Yes	Yes
Automated backups to local storage (preview)	Yes	No
Point-in-time-restore (preview)	Yes	No
Automatic updates	Yes	No
SQL Server 2012 extended security updates	Yes	Not applicable

Feature	Windows	Linux
Failover cluster instances	Yes	Not applicable
Always On availability groups	Yes	Not applicable
Monitoring (preview)	Yes	No
Client connection summary	Yes	No
Operate with least privilege	Yes	No

[1] SQL Server 2022 (16.x) only.

[2] PAYG billing is supported on Linux with limitations. Passive instance detection, connected user verification, and Database Engine-level core visibility aren't available. All instances are billed as active. For details, see Manage licensing and billing.

Feature availability by version

The following table identifies features available by SQL Server version:

Expand table

Feature availability based on SQL Server version	2012 2014	2016 2017 2019	2022	2025
Azure pay-as-you-go billing	Yes	Yes	Yes	Yes
Best practices assessment	Yes	Yes	Yes	Yes
Migration assessment	Yes	Yes	Yes	Yes
Database migration	LRS only	LRS & MI link	LRS & MI link	LRS & MI link
Detailed inventory	Yes	Yes	Yes	Yes
Microsoft Entra ID authentication for SQL Server	No	No	Yes	Yes
Microsoft Defender for Cloud	Yes	Yes	Yes	Yes
Microsoft Purview: DevOps policies	No	No	Yes	No
Microsoft Purview: data owner policies (preview)	No	No	Yes	No
Automated backups to local storage (preview)	Yes	Yes	Yes	Yes

Feature availability based on SQL Server version	2012 2014	2016 2017 2019	2022	2025
Point-in-time-restore (preview)	Yes	Yes	Yes	Yes
Automatic updates	Yes [1]	Yes	Yes	Yes
Failover cluster instances	Yes	Yes	Yes	Yes
Always On availability groups	Yes	Yes	Yes	Yes
Monitoring (preview)	No	Yes [2]	Yes	Yes
Client connection summary	No	Yes [2]	Yes	Yes
Operate with least privilege	Yes	Yes	Yes	Yes

[1] Requires subscription to Extended Security Updates (ESU) enabled by Azure Arc for SQL Server 2012 (11.x).

[2] Requires SQL Server 2016 (13.x) SP1 or later versions. For more information, see prerequisites.

Feature availability by edition

The following table identifies features available by SQL Server edition:

> **Note**
>
> This table applies to versions beginning with SQL Server 2025 (17.x). To view earlier versions, use the version selector at the top of the page.

Expand table

Feature	Enterprise	Standard	Express	Enterprise Developer Standard Developer	Evaluation
Azure pay-as-you-go billing	Yes	Yes	Not applicable	Not applicable	Not applicable
Best practices assessment	Yes	Yes	Yes	Yes	Yes
Migration readiness	Yes	Yes	Yes	Yes	Yes

Feature	Enterprise	Standard	Express	Enterprise Developer Standard Developer	Evaluation
Detailed inventory	Yes	Yes	Yes	Yes	Yes
Microsoft Entra authentication	Yes	Yes	Yes	Yes	Yes
Microsoft Defender for Cloud	Yes	Yes	Yes [1]	Yes	Yes
Microsoft Purview: Govern using DevOps and data owner policies	Yes	Yes	Yes	Yes	Yes
Automated backups to local storage (preview)	Yes	Yes	Yes	Yes	Yes
Point-in-time restore	Yes	Yes	Yes	Yes	Yes
Automatic updates	Yes	Yes	Yes	Yes	Yes
Failover cluster instances	Yes	Yes	Not applicable	Yes	Not applicable
Always On availability groups	Yes	Yes	Not applicable	Yes	Not applicable
Monitoring (preview)	Yes	Yes	No	No	No
Client connection summary	Yes	Yes	Yes	Yes	Yes
Operate with least privilege	Yes	Yes	Yes	Yes	Yes

[1] Express LocalDB isn't supported.

Feature availability by service type

The following table identifies features available by SQL Server service type:

Expand table

Feature	SQL Server Database Engine	SQL Server Integration Services	SQL Server Reporting Services	SQL Server Analysis Services	Power BI Report Server
Connect to Azure Arc	Yes	Yes	Yes	Yes	Yes
Azure pay-as-you-go	Yes	Yes	Yes	Yes	Yes

Feature	SQL Server Database Engine	SQL Server Integration Services	SQL Server Reporting Services	SQL Server Analysis Services	Power BI Report Server
billing					
ESU subscription	Yes	Yes	Yes	Yes	Yes
SQL Server inventory	Yes	Yes	Yes	Yes	Yes
Best practices assessment	Yes	No	No	No	No
Migration readiness	Yes	No	No	No	No
Database migration	Yes	No	No	No	No
Detailed inventory	Yes	Not applicable	Not applicable	Not applicable	Not applicable
Microsoft Entra ID authentication	Yes [1]	No	No	No	No
Microsoft Defender for Cloud	Yes	No	No	No	No
Microsoft Purview: Govern using DevOps and data owner policies	Yes	No	No	No	No
Automated backups to local storage (preview)	Yes	No	No	No	No
Point-in-time-restore	Yes	No	No	No	No
Automatic updates	Yes	Yes	Yes	Yes	Yes
Failover cluster instances	Yes	Not applicable	Not applicable	Not applicable	Not applicable
Always On availability groups	Yes	Not applicable	Not applicable	Not applicable	Not applicable
Monitoring (preview)	Yes	No	No	No	No
Client connection summary	Yes	No	No	No	No
Operate with least privilege	Yes	Yes	Yes	Yes	Yes

[1] SQL Server 2022 (16.x) only.

Supported configurations

SQL Server version

SQL Server 2012 (11.x) and later versions.

> ⓘ **Note**
>
> Only 64-bit SQL Server versions are supported.

Operating systems

- Windows 10 and 11
- Windows Server 2012 and later versions
- Ubuntu 20.04 (x64)
- Red Hat Enterprise Linux (RHEL) 8 (x64)
- SUSE Linux Enterprise Server (SLES) 15 (x64)

> ⓘ **Important**
>
> Windows Server 2012 and Windows Server 2012 R2 support ended on October 10, 2023. For more information, see SQL Server 2012 and Windows Server 2012/2012 R2 end of support.

.NET Framework

On Windows, .NET Framework 4.7.2 and later.

This requirement begins with extension version `1.1.2504.99` (November, 14 2023 release). Without this version, the extension might not function as intended. Windows Server 2012 R2 doesn't come with .NET Framework 4.7.2 by default and must be updated accordingly.

Support on VMware

You can deploy SQL Server enabled by Azure Arc in VMware VMs running:

- On-premises
- In VMware solutions, for example:
    - Azure VMware Solution (AVS)

VMware vSphere remains the underlying virtualization platform. Following Broadcom's acquisition of VMware, the vSphere product name didn't change; however, VMware updated how vSphere is packaged and licensed (for example, through VMware vSphere Foundation and VMware Cloud Foundation).

> **⚠ Warning**
>
> If you're running SQL Server VMs in Azure VMware Solution (AVS) private cloud, follow the steps in Deploy Arc-enabled Azure VMware Solution to enable.
>
> This is the only deployment mechanism that provides you with a fully integrated experience with Arc capabilities within the AVS private cloud.

- VMware Cloud on AWS
- Google Cloud VMware Engine

VMware packaging and support scope

SQL Server enabled by Azure Arc supports SQL Server instances running on virtual machines hosted in VMware vSphere–based environments, including Azure VMware Solution.

Support doesn't depend on specific VMware commercial bundles, editions, or packaging. The following requirements determine support:

- The supported guest operating system
- The supported SQL Server version
- Azure Arc Connected Machine agent requirements

VMware (Broadcom) defines VMware packaging, licensing, and lifecycle policies and may change them independently of Azure Arc.

Settings

The following table identifies settings, if they're enabled by default, and where the setting is configured:

Expand table

Setting Name	Default (Enabled or Disabled)	Can be disabled	Configuration location
Extended security updates	Disabled	Yes	Extension
Least privilege mode	Disabled	Yes	Extension
Automated patching	Disabled	Yes	Extension
Best practices assessment	Disabled	Yes	Extension
Microsoft Entra Authentication	Disabled	Yes	Extension per instance
Purview	Disabled	Yes	Extension, Instance
Automated backups	Disabled	Yes	Instance, Database
Collect performance metrics (preview)	Enabled	Yes	Instance
Migration assessment	Enabled	Yes	Instance
Database migration	Enabled	No	Extension
Availability Group discovery management	Enabled	Yes	`AvailabilityGroupDiscovery` feature flag
Extension log collection	Enabled	No	Not configurable
SQL Server instance and DB discovery	Enabled	No	Not configurable

Recommended system requirements

To use SQL Server enabled by Azure Arc, the following minimum system requirements are recommended:

- **Cores**: 2 cores minimum
- **Memory**: 512 MB of RAM available

Unsupported configurations

Azure Arc-enabled SQL Server doesn't currently support the following configurations:

- Windows Server 2012 or older versions of Windows Server. They don't have the minimum required versions of TLS to securely authenticate to Azure.

- Windows Server 2012 R2 is supported for DPS because it supports TLS 1.2. Windows Server 2012 R2 doesn't support the telemetry endpoint. Therefore features such as performance dashboard, migration assessment, and others aren't supported.
- SQL Server running in containers.
- SQL Server editions: Business Intelligence.
- Private Link connections to the Azure Arc data processing service at the `<region>.arcdataservices.com` endpoint used for inventory and usage upload.
- SQL Server 2008 (10.0.x), SQL Server 2008 R2 (10.50.x), and older versions.
- Installing the Arc agent and SQL Server extension can't be done as part of sysprep image creation.
- Multiple instances of SQL Server installed on the same host operating system with the same instance name.
- SQL Server in Azure Virtual Machines.
- An Always On availability group where one or more replicas is on a failover cluster instance.
- SQL Server Reporting Services (SharePoint Mode).
- DBCC CLONEDATABASE (Transact-SQL) throws error on the default installation of the Azure extension for SQL Server. To run the `DBCC CLONEDATABASE`, the Azure extension must be run in least privilege mode.
- Database and availability group names with trailing whitespace (for example, `MyDb `) aren't supported on instances using binary collations (`BIN`/`BIN2`). These objects are skipped by the extension with a warning. On non-binary collations (the default), trailing whitespace is automatically trimmed, and the objects are managed normally.
- SQL Server instance names containing a `#` symbol aren't supported. For a complete list of naming rules and restrictions, review naming rules and restrictions.

Installation

The SQL Server 2022 (16.x) Setup Installation Wizard doesn't support installation of the Azure extension for SQL Server. You can install this component from the command line, or by connecting the server to Azure Arc.

- Install Azure extension for SQL Server from the command line
- SQL Server enabled by Azure Arc deployment options

For VMware vSphere–based environments, review Support on VMware.

Related content

- Learn about the prerequisites to connect your SQL Server to Azure Arc
- SQL Server enabled by Azure Arc deployment options
- Learn more about Microsoft Defender for Cloud
- Learn more about Microsoft Purview
- Azure Arc-enabled servers Run Command
- Tutorial: Send data to Azure Monitor Logs with Logs ingestion API
- Azure Automation Runbooks
- Security overview | SQL Server enabled by Azure Arc

ⓘ **Note:** The author created this article with assistance from AI. Learn more

---

Last updated on 04/28/2026

What is Azure Arc site manager (preview)?

Article • 04/23/2025

Azure Arc site manager allows you to manage and monitor your on-premises environments as Azure Arc *sites*. Arc sites are scoped to an Azure resource group or subscription and enable you to track connectivity, alerts, and updates across your environment. The experience is tailored for on-premises scenarios where infrastructure is often managed within a common physical boundary, such as a store, restaurant, or factory.

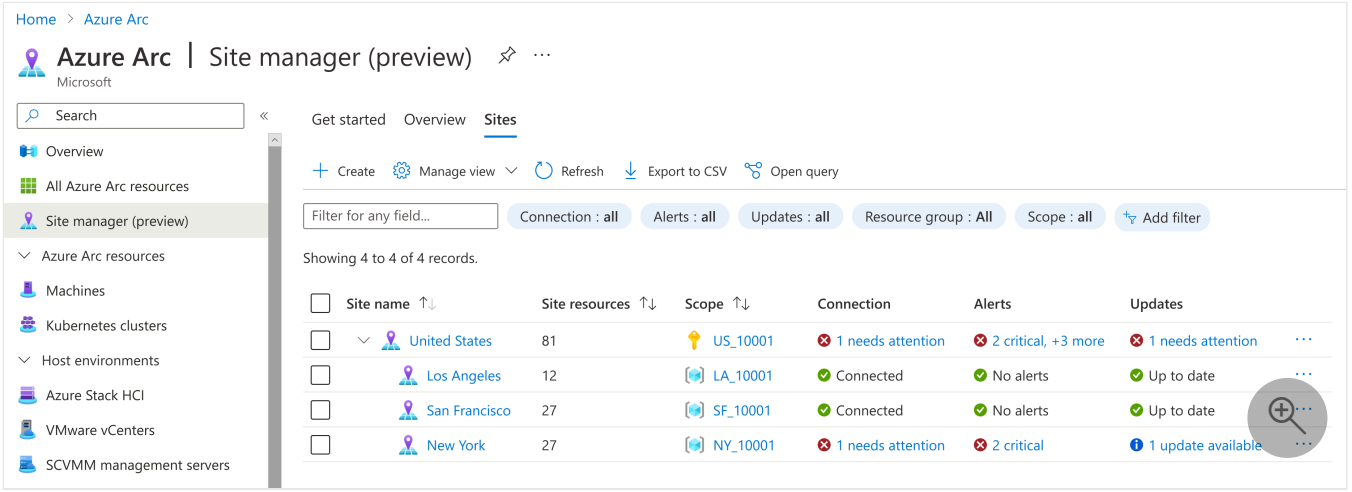
> **Important**
>
> Azure Arc site manager is currently in PREVIEW. See the Supplemental Terms of Use for Microsoft Azure Previews for legal terms that apply to Azure features that are in beta, preview, or otherwise not yet released into general availability.

Set an Arc site scope

When you create a site, you scope it to either a resource group or a subscription. The site automatically pulls in any supported resources within its scope.

Arc sites currently have a 1:1 relationship with resource groups and subscriptions. Any given Arc site can only be associated to one resource group or subscription, and vice versa.

You can create a hierarchy of sites by creating one site for a subscription and more sites for the resource groups within the subscription. The following screenshot shows an example of a hierarchy, with sites for **Los Angeles**, **San Francisco**, and **New York** nested within the site **United States**.



With site manager, customers who manage on-premises infrastructure can view resources based on their physical site or location. Sites don't logically have to be associated with a

physical grouping. You can use sites in whatever way supports your scenario. For example, you could create a site that groups resources by function or type rather than location.

Supported resource types

Currently, site manager supports the following Azure resources with the following capabilities:

Expand table

Resource	Inventory	Connectivity status	Updates	Alerts
Azure Local	✅	✅	✅ (Minimum OS required: HCI 23H2)	✅
Arc-enabled Servers	✅	✅	✅	✅
Arc-enabled VMs	✅	✅	✅	✅
Arc-enabled Kubernetes	✅	✅		✅
Azure Kubernetes Service (AKS) hybrid	✅	✅	✅ (only provisioned clusters)	✅
Assets	✅			

Site manager only provides status aggregation for the supported resource types. Site manager doesn't manage resources of other types that exist in the resource group or subscription, but those resources continue to function normally otherwise.

Regions

Site manager supports resources that exist in supported regions, with a few exceptions. For the following regions, connectivity and update status aren't supported for Arc-enabled machines or Arc-enabled Kubernetes clusters:

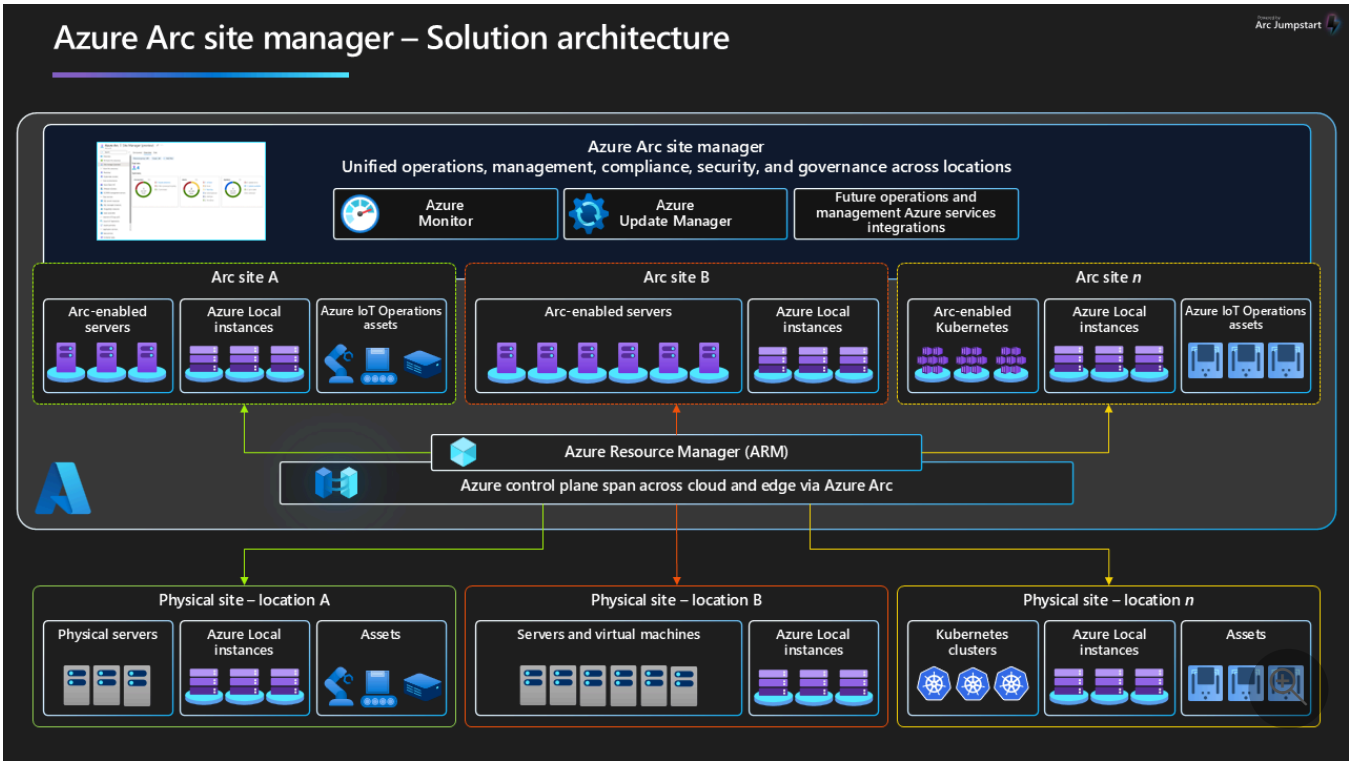
- Brazil South
- UAE North
- South Africa North

Pricing

Site manager is free to use, but integrates with other Azure services that have their own pricing models. For your managed resources and monitoring configuration, including Azure Monitor

alerts, refer to the individual service's pricing page.

Architecture



To download Arc diagrams in high resolution, visit Jumpstart Gems.

Next steps

Quickstart: Create a site in Azure Arc site manager (preview)

What is Multicloud connector enabled by Azure Arc?

Multicloud connector enabled by Azure Arc lets you connect non-Azure public cloud resources to Azure, providing a centralized source for management and governance. Currently, the multicloud connector provides support for connecting resources from these public clouds:

- Amazon Web Services (AWS)
- Google Cloud Platform (GCP) (preview)

The multicloud connector supports these solutions:

- **Inventory**: Allows you to see an up-to-date view of your resources from other public clouds in Azure, providing you with a single place to see all of your cloud resources. You can query all your cloud resources through Azure Resource Graph. When assets are represented in Azure, metadata from the source cloud is also included. For instance, if you need to query all of your Azure, AWS, and GCP resources with a certain tag, you can do so. The **Inventory** solution scans your source cloud on a periodic basis to ensure a complete, correct view is represented in Azure. You can also apply Azure tags or Azure policies on these resources.
- **Arc onboarding**: Auto-discovers EC2 instances running in your AWS environment, or VMs running in your GCP environment, and installs the Azure Connected Machine agent on the VMs so that they're onboarded to Azure Arc. This simplified experience lets you use Azure management services such as Azure Monitor on these VMs, providing a centralized way to manage Azure, AWS, and GCP resources together.
- **Storage - Data management**: Reads data from Amazon Simple Storage Service (Amazon S3) in your AWS environment cloud. This solution is used to set up the Azure Storage Mover data connection for cloud-to-cloud migration.

For more information about how the multicloud connector works, including prerequisites, see Add a public cloud with the multicloud connector in the Azure portal.

The multicloud connector can work side-by-side with Defender for Cloud support for AWS accounts and GCP projects. If you choose, you can use these connectors together.

Supported regions

In Azure, the following regions are supported for the multicloud connector:

- East US, East US 2, West US 2, West US 3, West Central US, South Central US, Canada Central, West Europe, North Europe, Sweden Central, UK South, Southeast Asia, AU East

The multicloud connector isn't available in national clouds (Azure Government, Microsoft Azure operated by 21Vianet). The multicloud connector doesn't store customer data outside the region the customer deploys the service instance in.

In AWS, we scan for resources in the following regions:

- us-east-1, us-east-2, us-west-1, us-west-2, ca-central-1, ap-southeast-1, ap-southeast-2, ap-northeast-1, ap-northeast-3, eu-west-1, eu-west-2, eu-central-1, eu-north-1, sa-east-1, ap-south1

In GCP, we scan for resources in the following regions:

- us-east1, us-east4, us-central1, us-west1, us-west2, europe-west1, europe-west2, europe-west3, europe-north2, northamerica-northeast1, southamerica-east1, australia-southeast1

Scanned resources are automatically mapped to corresponding Azure regions.

Pricing

The multicloud connector is free to use, but it integrates with other Azure services that have their own pricing models. Any Azure service that is used with the Multicloud Connector, such as Azure Monitor, will be charged as per the pricing for that service. For more information, see the Azure pricing page.

After you connect your AWS or GCP cloud, the multicloud connector queries the relevant resource APIs several times a day. These read-only API calls incur no charges in AWS or GCP. However, for AWS, these calls *are* registered in CloudTrail if you've enabled a trail for read events.

Additionally, for GCP, the **Arc onboarding** solution requires Google Cloud VM Manager to be enabled. VM Manager incurs costs based on usage.

Next steps

- Learn how to connect a public cloud in the Azure portal.
- Learn how to use the multicloud connector **Inventory** solution.

- Learn how to use the multicloud connector **Arc onboarding** solution.
- Learn how to use the multicloud connector **Storage - Data management** solution.

Last updated on 04/13/2026

Overview of Azure Arc-enabled service validation

07/21/2025

Microsoft recommends running Azure Arc-enabled services on validated platforms whenever possible. This article explains how various Azure Arc-enabled components are validated.

Currently, validated solutions are available from partners for Azure Arc-enabled Kubernetes and Azure Arc-enabled data services.

Validated Azure Arc-enabled Kubernetes distributions

Azure Arc-enabled Kubernetes works with any Cloud Native Computing Foundation (CNCF) certified Kubernetes clusters. The Azure Arc team worked with key industry Kubernetes offering providers to validate Azure Arc-enabled Kubernetes with their Kubernetes distributions. Future major and minor versions of Kubernetes distributions released by these providers will be validated for compatibility with Azure Arc-enabled Kubernetes.

Validated data services solutions

The Azure Arc team worked with original equipment manufacturer (OEM) partners and storage providers to validate Azure Arc-enabled data services solutions. This includes partner solutions, versions, Kubernetes versions, and SQL engine versions that have been verified to support the data services.

Validation process

For more details about the validation process, see the Azure Arc validation process in GitHub. Here you find information about how offerings are validated with Azure Arc, the test harness, strategy, and more.

Next steps

- Learn about Validated Kubernetes distributions
- Learn about validated solutions for data services

Azure Arc-enabled Kubernetes validation

09/26/2025

The Azure Arc team works with key industry Kubernetes offering providers to validate Azure Arc-enabled Kubernetes with their Kubernetes distributions. Future major and minor versions of Kubernetes distributions released by these providers will be validated for compatibility with Azure Arc-enabled Kubernetes.

> **Important**
>
> Azure Arc-enabled Kubernetes works with any Kubernetes clusters that are certified by the Cloud Native Computing Foundation (CNCF), even if they are not listed on this page.

Validated distributions

The following Microsoft-provided Kubernetes distributions and infrastructure providers successfully passed the conformance tests for Azure Arc-enabled Kubernetes:

Expand table

Distribution and infrastructure provider	Version
Cluster API Provider on Azure	Release version: 1.20.1; API version v1.10.4; Kubernetes version: v1.33.1
AKS Enabled by Azure Arc	Release version: AKS on Azure Local version 2503; Kubernetes version: 1.30.4; 1.29.9; 1.28.14
K8s on Azure Stack Edge	Release version: Azure Stack Edge 2501 (3.3.2501.1176); Kubernetes version: 1.29.4
AKS Edge Essentials	Release version 1.10.868.0; Kubernetes version 1.29.9

The following providers and their corresponding Kubernetes distributions successfully passed the conformance tests for Azure Arc-enabled Kubernetes:

Expand table

Provider name	Distribution name	Validated versions
SUSE Rancher	Rancher Kubernetes Engine (RKE1/RKE2)	v1.33.3-rc2+rke2r1 v1.32.7-rc2+rke2r1 v1.31.11-rc2+rke2r1
SUSE Rancher	K3s	K3S version v1.33.2+k3s1 K3S version v1.32.3+k3s1 K3S version v1.31.5+k3s1
Red Hat	OpenShift Container Platform	4.19.4, 4.18.9, 4.17.5,
VMware	Tanzu Kubernetes Grid/vSphere Kubernetes Service	VKS 3.3, TKr v1.32.0+vmware.6-fips, Upstream K8s 1.32 VKS 3.3, TKr v1.31.4+vmware.1-fips, Upstream K8s 1.31
Canonical	Charmed Kubernetes	1.33, 1.32, 1.31
Wind River	Wind River Cloud Platform	Wind River Cloud Platform 24.09; Upstream K8s version: 1.30.6

Scenarios validated

The conformance tests run as part of the Azure Arc-enabled Kubernetes validation cover the following scenarios:

1. Connect Kubernetes clusters to Azure Arc:
    - Deploy Azure Arc-enabled Kubernetes agent Helm chart on cluster.
    - Agents send cluster metadata to Azure.
2. Configuration:
    - Create configuration on top of Azure Arc-enabled Kubernetes resource.
    - Flux, needed for setting up GitOps workflow, is deployed on the cluster.
    - Flux pulls manifests and Helm charts from demo Git repo and deploys to cluster.

Next steps

- Learn how to connect an existing Kubernetes cluster to Azure Arc
- Learn about the Azure Arc agents deployed on Kubernetes clusters when connecting them to Azure Arc.

Azure Arc-enabled data services Kubernetes validation

Azure Arc-enabled data services team has worked with industry partners to validate specific distributions and solutions to host Azure Arc-enabled data services. This validation extends the Azure Arc-enabled Kubernetes validation for the data services. This article identifies partner solutions, versions, Kubernetes versions and SQL engine versions that have been verified to support the data services.

To see how all Azure Arc-enabled components are validated, see Validation program overview

> **Note**
>
> At the current time, SQL Managed Instance enabled by Azure Arc is generally available in select regions.

Partners

DataON

Expand table

Solution and version	Kubernetes version	Azure Arc-enabled data services version	SQL engine version
DataON AZS-6224	1.24.11	1.20.0_2023-06-13	16.0.5100.7242

Dell

Expand table

Solution and version	Kubernetes version	Azure Arc-enabled data services version	SQL engine version
PowerStore 4.0	1.28.10	1.30.0_2024-06-11	16.0.5349.20214
Unity XT	1.24.3	1.15.0_2023-01-10	16.0.816.19223
PowerFlex	1.25.0	1.21.0_2023-07-11	16.0.5100.7242

Hitachi

Expand table

Solution and version	Kubernetes version	Azure Arc-enabled data services version	SQL engine version
Hitachi UCP with Microsoft AKS-HCI	1.27.3	1.29.0_2024-04-09*	16.0.5290.8214
Hitachi UCP with Red Hat OpenShift	1.25.11	1.25.0_2023-11-14	16.0.5100.7246
Hitachi Virtual Storage Software Block software-defined storage (VSSB)	1.24.12	1.20.0_2023-06-13	16.0.5100.7242
Hitachi Virtual Storage Platform (VSP)	1.24.12	1.19.0_2023-05-09	16.0.937.6221

*: The solution was validated in indirect mode only (learn more about the different connectivity modes).

HPE

Expand table

Solution and version	Kubernetes version	Azure Arc-enabled data services version	SQL engine version
HPE Superdome Flex 280	1.25.12	1.22.0_2023-08-08	16.0.5100.7242
HPE Apollo 4200 Gen10 Plus	1.22.6	1.11.0_2022-09-13	16.0.312.4243

Kublr

Expand table

Solution and version	Kubernetes version	Azure Arc-enabled data services version	SQL engine version
Kublr 1.26.0	1.26.4, 1.25.6, 1.24.13, 1.23.17, 1.22.17	1.21.0_2023-07-11	16.0.5100.7242
Kublr 1.21.2	1.22.10	1.9.0_2022-07-12	16.0.312.4243

Lenovo

Expand table

Solution and version	Kubernetes version	Azure Arc-enabled data services version	SQL engine version
Lenovo ThinkEdge SE455 V3	1.26.6	1.24.0_2023-10-10	16.0.5100.7246
Lenovo ThinkAgile MX1020	1.26.6	1.24.0_2023-10-10	16.0.5100.7246
Lenovo ThinkAgile MX3520	1.22.6	1.10.0_2022-08-09	16.0.312.4243

Nutanix

Expand table

Solution and version	Kubernetes version	Azure Arc-enabled data services version	SQL engine version
Karbon 2.2 AOS: 5.19.1.5 AHV: 20201105.1021 PC: Version pc.2021.3.02	1.19.8-0	1.0.0_2021-07-30	15.0.2148.140

PureStorage

Expand table

Solution and version	Kubernetes version	Azure Arc-enabled data services version	SQL engine version
Portworx Enterprise 3.3.1.1 Microsoft Azure Marketplace	1.31.9	1.39.0_2025-05-13	16.0.5564.41214
Portworx Enterprise 3.1	1.28.7	1.30.0_2024-06-11	16.0.5349.20214

Red Hat

Expand table

Solution and version	Kubernetes version	Azure Arc-enabled data services version	SQL engine version
OpenShift 4.15.0	1.28.6	1.27.0_2024-02-13	16.0.5100.7246
OpenShift 4.13.4	1.26.5	1.21.0_2023-07-11	16.0.5100.7242
OpenShift 4.10.16	1.23.5	1.11.0_2022-09-13	16.0.312.4243

VMware

Expand table

Solution and version	Kubernetes version	Azure Arc-enabled data services version	SQL engine version
TKGs 2.2	1.25.7	1.23.0_2023-09-12	16.0.5100.7246
TKGm 2.3	1.26.5	1.23.0_2023-09-12	16.0.5100.7246
TKGm 2.2	1.25.7	1.19.0_2023-05-09	16.0.937.6223
TKGm 2.1.0	1.24.9	1.15.0_2023-01-10	16.0.816.19223

Wind River

Expand table

Solution and version	Kubernetes version	Azure Arc-enabled data services version	SQL engine version
Wind River Cloud Platform 26.03	1.34.1	1.44.0_2026-02-10	17.0.429.2218
Wind River Cloud Platform 25.09	1.32.2	1.41.0_2025-09-09	17.0.429.2218
Wind River Cloud Platform 24.09	1.30.6	1.37.0_2025-03-11	16.0.5564
Wind River Cloud Platform 22.12	1.24.4	1.26.0_2023-12-12	16.0.5100.7246

Data services validation process

The Sonobuoy Azure Arc-enabled data services plug-in automates the provisioning and testing of Azure Arc-enabled data services on a Kubernetes cluster.

Prerequisites

- Azure Data CLI (azdata)
- kubectl

Create a Kubernetes config file configured to access the target Kubernetes cluster and set as the current context. How this file is generated and brought local to your computer is different from platform to platform. See Kubernetes.io.

Process

The conformance tests run as part of the Azure Arc-enabled Data services validation. A pre-requisite to running these tests is to pass on the Azure Arc-enabled Kubernetes tests for the Kubernetes distribution in use.

These tests verify that the product is compliant with the requirements of running and operating data services. This process helps assess if the product is enterprise ready for deployments.

1. Deploy data controller in both indirect and direct connect modes (learn more about connectivity modes)
2. Deploy SQL Managed Instance enabled by Azure Arc

More tests will be added in future releases of Azure Arc-enabled data services.

Additional information

- Validation program overview
- Azure Arc-enabled Kubernetes validation
- Azure Arc validation program - GitHub project

Related content

- Plan an Azure Arc-enabled data services deployment
- Create a data controller - indirectly connected with the CLI
- To create a directly connected data controller, start with Prerequisites to deploy the data controller in direct connectivity mode.

Last updated on 04/08/2026

Azure Arc network requirements

This article lists the endpoints, ports, and protocols required for Azure Arc-enabled services and features.

Generally, connectivity requirements include these principles:

- All connections are TCP unless otherwise specified.
- All HTTP connections use HTTPS and SSL/TLS with officially signed and verifiable certificates.
- All connections are outbound unless otherwise specified.

To use a proxy, verify that the agents and the machine performing the onboarding process meet the network requirements in this article.

> **Tip**
>
> For the Azure public cloud, you can reduce the number of required endpoints by using the Azure Arc gateway for Arc-enabled servers or Arc-enabled Kubernetes.

Azure Arc-enabled Kubernetes endpoints

Connectivity to the Arc Kubernetes-based endpoints is required for all Kubernetes-based Arc offerings, including:

- Azure Arc-enabled Kubernetes
- Azure Container Apps on Azure Arc
- Azure Arc-enabled Machine Learning
- Azure Arc-enabled data services (direct connectivity mode only)

Azure Cloud

> **Important**
>
> Azure Arc agents require the following outbound URLs on `https://:443` (unless otherwise noted). For `*.servicebus.windows.net`, websockets need to be enabled for outbound access on firewall and proxy.

Expand table

Endpoint (DNS)	Description
`https://management.azure.com`	Required for the agent to connect to Azure and register the cluster.
`https://<region>.dp.kubernetesconfiguration.azure.com`	Data plane endpoint for the agent to push status and fetch configuration information.

`https://login.microsoftonline.com`
`https://<region>.login.microsoft.com`
`login.windows.net`
	Required to fetch and update Azure Resource Manager tokens.

`https://mcr.microsoft.com` `https://*.data.mcr.microsoft.com`	Required to pull container images for Azure Arc agents.
`dl.k8s.io`	Required to download kubectl binaries during Azure Arc onboarding by Azure CLI connectedk8s extension.
`https://gbl.his.arc.azure.com`	Required to get the regional endpoint for pulling system-assigned Managed Identity certificates.
`https://*.his.arc.azure.com`	Required to pull system-assigned Managed Identity certificates.

`guestnotificationservice.azure.com`
`*.guestnotificationservice.azure.com`
`sts.windows.net`
	For Cluster Connect and for Custom Location based scenarios.

`*.servicebus.windows.net`	For Cluster Connect and for Custom Location based scenarios.
`https://graph.microsoft.com/`	Required when Azure RBAC is configured.
`*.arc.azure.net`	Required to manage connected clusters in Azure portal.
`https://<region>.obo.arc.azure.com:8084/`	Required when Cluster Connect and Azure RBAC is configured.
`https://linuxgeneva-microsoft.azurecr.io`	Required if using Azure Arc-enabled Kubernetes extensions.

To translate the `*.servicebus.windows.net` wildcard into specific endpoints, use the command:

rest

```
GET https://guestnotificationservice.azure.com/urls/allowlist?api-version=2020-01-01&location=<region>
```

To get the region segment of a regional endpoint, remove all spaces from the Azure region name. For example, *East US 2* region, the region name is `eastus2`.

For example: `*.<region>.arcdataservices.com` should be `*.eastus2.arcdataservices.com` in the East US 2 region.

To see a list of all regions, run this command:

Azure CLI

```azurecli
az account list-locations -o table
```

Azure PowerShell

```azurepowershell
Get-AzLocation | Format-Table
```

For more information, see Azure Arc-enabled Kubernetes network requirements.

Azure Arc-enabled data services

This section describes requirements specific to Azure Arc-enabled data services, in addition to the Arc-enabled Kubernetes endpoints listed above.

Expand table

Service	Port	URL	Direction	Notes

Helm chart (direct connected mode only)	443	`arcdataservicesrow1.azurecr.io`
		`arcdataservicesrow2.azurecr.io`
		`*.blob.core.windows.net`
			Outbound	Provisions the Azure Arc data controller bootstrapper and cluster level objects, such as custom resource definitions, cluster roles, and cluster role bindings, is pulled from an Azure Container Registry.

Azure monitor APIs [1]	443	`*.ods.opinsights.azure.com`
		`*.oms.opinsights.azure.com`
		`*.monitoring.azure.com`
			Outbound	Azure CLI connects to the Azure Resource Manager APIs to send and retrieve data to and from

Service	Port	URL	Direction	Notes
				Azure for some features. See Azure Monitor APIs.
Azure Arc data processing service [1]	443	`*.<region>.arcdataservices.com` [2]	Outbound	

[1] Requirement depends on deployment mode:

- For direct mode, the controller pod on the Kubernetes cluster needs to have outbound connectivity to the endpoints to send the logs, metrics, inventory, and billing information to Azure Monitor/Data Processing Service.
- For indirect mode, the machine that runs `az arcdata dc upload` needs to have the outbound connectivity to Azure Monitor and Data Processing Service.

[2] For extension versions up to and including February 13, 2024, use `san-af-<region>-prod.azurewebsites.net`.

Azure Monitor APIs

Connectivity to the Kubernetes API server uses the Kubernetes authentication and encryption that you have established. Each user that's using Azure CLI must have an authenticated connection to the Kubernetes API to perform many of the actions related to Azure Arc-enabled data services.

For more information, see Connectivity modes and requirements.

Azure Arc-enabled servers

Connectivity to Arc-enabled server endpoints is required for:

- SQL Server enabled by Azure Arc
- Azure Arc-enabled VMware vSphere *
- Azure Arc-enabled System Center Virtual Machine Manager *
- Azure Arc-enabled Azure Stack (HCI) *

*Only required for guest management enabled.

Azure Arc-enabled server endpoints are required for all server-based Azure Arc offerings.

Networking configuration

The Azure Connected Machine agent for Linux and Windows communicates outbound securely to Azure Arc over TCP port 443. By default, the agent uses the default route to the internet to reach Azure services. You can optionally configure the agent to use a proxy server if your network requires it. Proxy servers don't make the Connected Machine agent more secure because the traffic is already encrypted.

To further secure your network connectivity to Azure Arc, instead of using public networks and proxy servers, you can implement an Azure Arc private link scope.

> **Note**
>
> Azure Arc-enabled servers don't support using a Log Analytics gateway as a proxy for the Connected Machine agent. At the same time, Azure Monitor Agent supports Log Analytics gateways.

If your firewall or proxy server restricts outbound connectivity, make sure that the URLs and service tags listed here aren't blocked.

Service tags

Be sure to allow access to the following service tags:

- `AzureActiveDirectory`
- `AzureTrafficManager`
- `AzureResourceManager`
- `AzureArcInfrastructure`
- `Storage`
- `AzureFrontDoor.Frontend` (required as of April 2026)
- `WindowsAdminCenter` (if you use Windows Admin Center to manage Azure Arc-enabled servers)

For a list of IP addresses for each service tag/region, see the JSON file Azure IP Ranges and Service Tags - Public Cloud. Microsoft publishes weekly updates that contain each Azure service and the IP ranges it uses. The information in the JSON file is the current point-in-time list of the IP ranges that correspond to each service tag. The IP addresses are subject to

change. If IP address ranges are required for your firewall configuration, use the `AzureCloud` service tag to allow access to all Azure services. Don't disable security monitoring or inspection of these URLs. Allow them as you would other internet traffic.

If you filter traffic to the `AzureArcInfrastructure` service tag, you must allow traffic to the full service tag range. The ranges advertised for individual regions, for example, `AzureArcInfrastructure.AustraliaEast`, don't include the IP ranges that are used by global components of the service. The specific IP address resolved for these endpoints might change over time within the documented ranges. For this reason, using a lookup tool to identify the current IP address for a specific endpoint and allowing access to only that IP address isn't sufficient to ensure reliable access.

For more information, see Virtual network service tags.

> **Important**
>
> To filter traffic by IP addresses in Azure Government or Azure operated by 21Vianet, be sure to add the IP addresses from the `AzureArcInfrastructure` service tag for the Azure public cloud, in addition to using the `AzureArcInfrastructure` service tag for your cloud. After October 28, 2025, adding the `AzureArcInfrastructure` service tag for Azure public cloud will be required, and the service tags for Azure Government and Azure operated by 21Vianet will no longer be supported.

URLs

This table lists the URLs that must be available to install and use the Connected Machine agent.

Azure cloud platform

> **Note**
>
> When you configure the Connected Machine agent to communicate with Azure through a private link, some endpoints must still be accessed through the internet. The **Private link capable** column in the following table shows the endpoints that you can configure with a private endpoint. If the column shows *Public* for an endpoint, you must still allow access to that endpoint through your organization's firewall and/or proxy server for the agent to function. Network traffic is routed through private endpoints if a private link scope is assigned.

Expand table

Agent resource	Description	When required	Private link capable
`download.microsoft.com`	Used to download the Windows installation package.	Only at installation time.[1]	Public.
`packages.microsoft.com`	Used to download the Linux installation package.	Only at installation time.[1]	Public.
`login.microsoftonline.com`	Microsoft Entra ID.	Always.	Public.
`*.login.microsoft.com`	Microsoft Entra ID.	Always.	Public.
`pas.windows.net`	Microsoft Entra ID.	Always.	Public.
`management.azure.com`	Azure Resource Manager is used to create or delete the Azure Arc server resource.	Only when you connect or disconnect a server.	Public, unless a resource management private link is also configured.
`*.his.arc.azure.com`	Metadata and hybrid identity services.	Always.	Private.
`*.guestconfiguration.azure.com`	Extension management and guest configuration services.	Always.	Private.
`guestnotificationservice.azure.com`, `*.guestnotificationservice.azure.com`	Notification service for extension and connectivity scenarios.	Always.	Public.
`azgn*.servicebus.windows.net` or `*.servicebus.windows.net`	Notification service for extension and connectivity scenarios.	Always.	Public.
`*.servicebus.windows.net`	For Windows Admin Center and Secure Shell (SSH) scenarios.	If you use SSH or Windows Admin Center from Azure.	Public.

Agent resource	Description	When required	Private link capable
`*.waconazure.com`	For Windows Admin Center connectivity.	If you use Windows Admin Center.	Public.
`dc.services.visualstudio.com`	Agent telemetry.	Optional. Not used in agent versions 1.24+.	Public.
`*.<region>.arcdataservices.com`[2]	For Azure Arc-enabled SQL Server. Sends data processing service, service telemetry, and performance monitoring to Azure. Allows Transport Layer Security (TLS) 1.2 or 1.3 only.	If you use Azure Arc-enabled SQL Server.	Public.
`https://<azure-keyvault-name>.vault.azure.net/`, `https://graph.microsoft.com/`[2]	For Microsoft Entra authentication with Azure Arc-enabled SQL Server.	If you use Azure Arc-enabled SQL Server.	Public.
`www.microsoft.com/pkiops/certs`	Intermediate certificate updates for Extended Security Updates (uses HTTP/TCP 80 and HTTPS/TCP 443).	If you use Extended Security Updates enabled by Azure Arc. Always required for automatic updates or temporarily if you download certificates manually.	Public.
`dls.microsoft.com`	Used by Azure Arc machines to perform license validation.	Required when you use hotpatching, Windows Server Azure Benefits, or Windows Server pay-as-you-go billing on Azure Arc-	Public.

Agent resource	Description	When required	Private link capable
		enabled machines.	

[1] Access to this URL is also needed when updates are performed automatically.

[2] For details about what information is collected and sent, review Data collection and reporting for SQL Server enabled by Azure Arc.

For extension versions up to and including February 13, 2024, use `san-af-<region>-prod.azurewebsites.net`. Beginning March 12, 2024, both Azure Arc data processing and Azure Arc data telemetry use `*.<region>.arcdataservices.com`.

> **Note**
>
> To translate the `*.servicebus.windows.net` wildcard into specific endpoints, use the command `\GET https://guestnotificationservice.azure.com/urls/allowlist?api-version=2020-01-01&location=<region>`. Within this command, the region must be specified for the `<region>` placeholder. These endpoints might change periodically.

To get the region segment of a regional endpoint, remove all spaces from the Azure region name. For example, *East US 2* region, the region name is `eastus2`.

For example: `*.<region>.arcdataservices.com` should be `*.eastus2.arcdataservices.com` in the East US 2 region.

To see a list of all regions, run this command:

Azure CLI

```azurecli
az account list-locations -o table
```

Azure PowerShell

```azurepowershell
Get-AzLocation | Format-Table
```

Cryptographic protocols

To ensure the security of data in transit to Azure, we strongly encourage you to configure machines to use TLS 1.2 and 1.3. Older versions of TLS/Secure Sockets Layer (SSL) were found to be vulnerable. Although they still currently work to allow backward compatibility, they *aren't recommended*.

Starting from version 1.56 of the Connected Machine agent (Windows only), the following cipher suites must be configured for at least one of the recommended TLS versions:

- TLS 1.3 (suites in server-preferred order):
  - TLS_AES_256_GCM_SHA384 (0x1302) ECDH secp521r1 (eq. 15360 bits RSA) FS
  - TLS_AES_128_GCM_SHA256 (0x1301) ECDH secp256r1 (eq. 3072 bits RSA) FS
- TLS 1.2 (suites in server-preferred order):
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH secp521r1 (eq. 15360 bits RSA) FS
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH secp256r1 (eq. 3072 bits RSA) FS

For more information, see Windows TLS configuration issues.

The SQL Server enabled by Azure Arc endpoints located at `*.\<region\>.arcdataservices.com` support only TLS 1.2 and 1.3. Only Windows Server 2012 R2 and later have support for TLS 1.2. SQL Server enabled by Azure Arc telemetry endpoint isn't supported for Windows Server 2012 or Windows Server 2012 R2.

Expand table

Platform/Language	Support	More information
Linux	Linux distributions tend to rely on OpenSSL for TLS 1.2 support.	Check the OpenSSL Changelog to confirm that your version of OpenSSL is supported.
Windows Server 2012 R2 and later	Supported and enabled by default.	Confirm that you're still using the default settings.
Windows Server 2012	Partially supported. *Not recommended.*	Some endpoints still work, but other endpoints require TLS 1.2 or later, which isn't available on Windows Server 2012.

Subset of endpoints for ESU only

If you use Azure Arc-enabled servers only for Extended Security Updates for either or both of the following products:

- Windows Server 2012
- SQL Server 2012

You can enable the following subset of endpoints.

Azure cloud platform

Expand table

Agent resource	Description	When required	Endpoint used with private link
`download.microsoft.com`	Used to download the Windows installation package.	Only at installation time.[1]	Public.
`login.windows.net`	Microsoft Entra ID.	Always.	Public.
`login.microsoftonline.com`	Microsoft Entra ID.	Always.	Public.
`*.login.microsoft.com`	Microsoft Entra ID.	Always.	Public.
`management.azure.com`	Azure Resource Manager is used to create or delete the Azure Arc server resource.	Only when you connect or disconnect a server.	Public, unless a resource management private link is also configured.
`*.his.arc.azure.com`	Metadata and hybrid identity services.	Always.	Private.
`*.guestconfiguration.azure.com`	Extension management and guest configuration services.	Always.	Private.
`www.microsoft.com/pkiops/certs`	Intermediate certificate updates for Extended Security Updates (uses HTTP/TCP 80 and HTTPS/TCP 443).	Always for automatic updates or temporarily if you download certificates manually.	Public.
`*.<region>.arcdataservices.com`	Azure Arc data processing service and	SQL Server Extended Security	Public.

Agent resource	Description	When required	Endpoint used with private link
	service telemetry.	Updates.	

[1] Access to this URL is also needed when you perform updates automatically.

For more information, see Connected Machine agent network requirements.

Azure Arc resource bridge

This section describes additional networking requirements specific to deploying Azure Arc resource bridge in your enterprise. These requirements also apply to Azure Arc-enabled VMware vSphere and Azure Arc-enabled System Center Virtual Machine Manager.

Outbound connectivity requirements

The firewall and proxy URLs below must be allowlisted in order to enable communication from the management machine, Arc resource bridge VM (initially deployed), Arc resource bridge VM 2 (upgrade creates a new VM using a different VM IP), and Control Plane IP to the required Arc resource bridge URLs.

> **Important**
>
> When onboarding Arc Resource Bridge, you must provide two IP addresses for the appliance VMs. These are specified as either:
>
> - A range of IPs
> - Two individual IPs (one for each VM)
>
> To ensure successful upgrades, all appliance VM IPs must have outbound access to the required URLs. Make sure these URLs are allowlisted in your network.

Firewall/Proxy URL allowlist

Expand table

Service	Port	URL	Direction	Notes
DNS servers	53	Your DNS server IP(s)	Management machine &	Network connectivity to

Service	Port	URL	Direction	Notes
			Appliance VM IPs need outbound connection.	the DNS servers specified during deployment to resolve required service endpoints.
SFS API endpoint	443	`msk8s.api.cdp.microsoft.com`	Management machine & Appliance VM IPs need outbound connection.	Download product catalog, product bits, and OS images from SFS.
Resource bridge (appliance) image download	443	`msk8s.sb.tlu.dl.delivery.mp.microsoft.com`	Management machine & Appliance VM IPs need outbound connection.	Download the Arc Resource Bridge OS images.
Microsoft Container Registry	443	`mcr.microsoft.com`	Management machine & Appliance VM IPs need outbound connection.	Discover container images for Arc Resource Bridge.
Microsoft Container Registry	443	`*.data.mcr.microsoft.com`	Management machine & Appliance VM IPs need outbound connection.	Download container images for Arc Resource Bridge.
Windows NTP Server	123	`time.windows.com`	Management machine & Appliance VM IPs (if Hyper-V default is Windows NTP) need outbound connection on UDP	OS time sync in appliance VM & Management machine (Windows NTP).
Azure Resource	443	`management.azure.com`	Management machine &	Manage resources in

Service	Port	URL	Direction	Notes
Manager			Appliance VM IPs need outbound connection.	Azure.
Microsoft Graph	443	`graph.microsoft.com`	Management machine & Appliance VM IPs need outbound connection.	Required for Azure RBAC.
Azure Resource Manager	443	`login.microsoftonline.com`	Management machine & Appliance VM IPs need outbound connection.	Required to update ARM tokens.
Azure Resource Manager	443	`*.login.microsoft.com`	Management machine & Appliance VM IPs need outbound connection.	Required to update ARM tokens.
Azure Resource Manager	443	`login.windows.net`	Management machine & Appliance VM IPs need outbound connection.	Required to update ARM tokens.
Resource bridge (appliance) Dataplane service	443	`*.dp.prod.appliances.azure.com`	Appliance VMs IP need outbound connection.	Communicate with resource provider in Azure.
Resource bridge (appliance) container image download	443	`*.blob.core.windows.net, ecpacr.azurecr.io`	Appliance VM IPs need outbound connection.	Required to pull container images.
Managed Identity	443	`*.his.arc.azure.com`	Appliance VM IPs need	Required to pull system-assigned

Service	Port	URL	Direction	Notes
			outbound connection.	Managed Identity certificates.
Azure Arc for Kubernetes container image download	443	`azurearcfork8s.azurecr.io`	Appliance VM IPs need outbound connection.	Pull container images.
ADHS telemetry service	443	`adhs.events.data.microsoft.com`	Appliance VM IPs need outbound connection.	Periodically sends Microsoft required diagnostic data from appliance VM.
Microsoft events data service	443	`v20.events.data.microsoft.com`	Appliance VM IPs need outbound connection.	Send diagnostic data from Windows.
Log collection for Arc Resource Bridge	443	`linuxgeneva-microsoft.azurecr.io`	Appliance VM IPs need outbound connection.	Push logs for Appliance managed components.
Resource bridge components download	443	`kvamanagementoperator.azurecr.io`	Appliance VM IPs need outbound connection.	Pull artifacts for Appliance managed components.
Microsoft open source packages manager	443	`packages.microsoft.com`	Appliance VM IPs need outbound connection.	Download Linux installation package.
Custom Location	443	`sts.windows.net`	Appliance VM IPs need outbound connection.	Required for Custom Location.
Azure Arc	443	`guestnotificationservice.azure.com`	Appliance VM IPs need outbound connection.	Required for Azure Arc.
Diagnostic data	443	`gcs.prod.monitoring.core.windows.net`	Appliance VM IPs need	Periodically sends Microsoft

Service	Port	URL	Direction	Notes
			outbound connection.	required diagnostic data.
Diagnostic data	443	`*.prod.microsoftmetrics.com`	Appliance VM IPs need outbound connection.	Periodically sends Microsoft required diagnostic data.
Diagnostic data	443	`*.prod.hot.ingest.monitor.core.windows.net`	Appliance VM IPs need outbound connection.	Periodically sends Microsoft required diagnostic data.
Diagnostic data	443	`*.prod.warm.ingest.monitor.core.windows.net`	Appliance VM IPs need outbound connection.	Periodically sends Microsoft required diagnostic data.
Azure portal	443	`*.arc.azure.net`	Appliance VM IPs need outbound connection.	Manage cluster from Azure portal.
Azure service bus	443	`*.servicebus.windows.net`	Appliance VM IPs need outbound connection. Outbound WebSocket (wss://) connections must be allowed.	Enables secure control channel.
Azure CLI	443	`*.blob.core.windows.net`	Management machine needs outbound connection.	Download Azure CLI Installer.
Arc Extension	443	`*.web.core.windows.net`	Management machine needs outbound connection.	Download Arc resource bridge extension.
Azure Arc Agent	443	`*.dp.kubernetesconfiguration.azure.com`	Management machine needs outbound connection.	Dataplane used for Arc agent.

Service	Port	URL	Direction	Notes
Python package	443	`pypi.org`, `*.pypi.org`	Management machine needs outbound connection.	Validate Kubernetes and Python versions.
Azure CLI	443	`pythonhosted.org`, `*.pythonhosted.org`	Management machine needs outbound connection.	Python packages for Azure CLI installation.

Inbound connectivity requirements

Communication between the following ports must be allowed from the management machine, Appliance VM IPs, and Control Plane IPs. Ensure these ports are open and that traffic is not being routed through a proxy to facilitate the deployment and maintenance of Arc resource bridge.

> **Important**
>
> During onboarding, you must provide two IP addresses for the Arc Resource Bridge appliance VMs — either as a range or as two individual IPs. For successful deployment, operations, and upgrades:
>
> - Ensure communication is allowed between the management machine, appliance VM IPs, and control plane IPs over the required ports as listed below.
> - Do not route traffic through a proxy for these connections.

Expand table

Service	Port	IP/machine	Direction	Notes
SSH	22	`appliance VM IPs` and `Management machine`	Bidirectional	Management machine connects outbound to the appliance VM IPs. Appliance VM IPs must allow inbound connections.
Kubernetes API server	6443	`appliance VM IPs` and `Management machine`	Bidirectional	Management machine connects outbound to the appliance VM IPs. Appliance VM IPs must allow inbound connections.

Service	Port	IP/machine	Direction	Notes
SSH	22	`control plane IP` and `Management machine`	Bidirectional	Used for deploying and maintaining the appliance VM.
Kubernetes API server	6443	`control plane IP` and `Management machine`	Bidirectional	Management of the appliance VM.
HTTPS	443	`private cloud control plane address` and `Management machine`	Management machine needs outbound connection.	Communication with private cloud (ex: VMware vCenter address and vSphere datastore).
Kubernetes API server	6443, 2379, 2380, 10250, 10257, 10259	`appliance VM IPs` (to each other)	Bidirectional	Required for appliance VM upgrade. Ensure all appliance VM IPs have outbound connectivity to each other over these ports.
HTTPS	443	`private cloud control plane address` and `appliance VM IPs`	appliance VM IPs need outbound connection.	Communication with private cloud (ex: VMware vCenter address and vSphere datastore).

For more information, see Azure Arc resource bridge network requirements.

Azure Arc-enabled VMware vSphere

Azure Arc-enabled VMware vSphere also requires:

Expand table

Service	Port	URL	Direction	Notes
vCenter Server	443	URL of the vCenter server	Appliance VM IP and control plane endpoint need outbound connection.	Used to by the vCenter server to communicate with the Appliance VM and the control plane.
VMware Cluster Extension	443	`azureprivatecloud.azurecr.io`	Appliance VM IPs need outbound connection.	Pull container images for Microsoft.VMWare and Microsoft.AVS Cluster Extension.

Service	Port	URL	Direction	Notes
Azure CLI and Azure CLI Extensions	443	`*.blob.core.windows.net`	Management machine needs outbound connection.	Download Azure CLI Installer and Azure CLI extensions.
Azure Resource Manager	443	`management.azure.com`	Management machine needs outbound connection.	Required to create/update resources in Azure using ARM.
Helm Chart for Azure Arc Agents	443	`*.dp.kubernetesconfiguration.azure.com`	Management machine needs outbound connection.	Data plane endpoint for downloading the configuration information of Arc agents.
Azure CLI	443	- `login.microsoftonline.com` - `aka.ms`	Management machine needs outbound connection.	Required to fetch and update Azure Resource Manager tokens.

For more information, see Support matrix for Azure Arc-enabled VMware vSphere.

Azure Arc-enabled System Center Virtual Machine Manager

Azure Arc-enabled System Center Virtual Machine Manager (SCVMM) also requires:

Expand table

Service	Port	URL	Direction	Notes
SCVMM management Server	443	URL of the SCVMM management server	Appliance VM IP and control plane endpoint need outbound connection.	Used by the SCVMM server to communicate with the Appliance VM and the control plane.

For more information, see Overview of Arc-enabled System Center Virtual Machine Manager.

Additional endpoints

Depending on your scenario, you might need connectivity to other URLs, such as those used by the Azure portal, management tools, or other Azure services. In particular, review these lists to

ensure that you allow connectivity to any necessary endpoints:

- Azure portal URLs
- Azure CLI endpoints for proxy bypass

Last updated on 04/01/2026

az arcappliance

> **Note**
>
> This reference is part of the **arcappliance** extension for the Azure CLI (version 2.73.0 or higher). The extension will automatically install the first time you run an **az arcappliance** command. Learn more about extensions.

Commands to manage Arc resource bridge.

Commands

Expand table

Name	Description	Type	Status
az arcappliance configuration	Command group for configuration related commands for Arc resource bridge.	Extension	GA
az arcappliance configuration proxy	Command group for proxy configuration related commands for Arc resource bridge.	Extension	GA
az arcappliance configuration proxy update	Command group for updating proxy configuration on Arc resource bridge.	Extension	Preview
az arcappliance configuration proxy update hci	Command to update the proxy configuration for Arc resource bridge on Azure Stack HCI.	Extension	Preview
az arcappliance configuration proxy update vmware	Command to update the proxy configuration for Arc resource bridge on VMware.	Extension	Preview
az arcappliance configuration show	Command group to show the current configuration of an Arc resource bridge.	Extension	Preview
az arcappliance configuration show hci	Command to show the current configuration of an HCI Arc resource bridge.	Extension	Preview
az arcappliance configuration show	Command to show the current configuration of a VMware Arc resource bridge.	Extension	Preview

Name	Description	Type	Status
vmware			
az arcappliance create	Command group for creation of the connection between the Arc resource bridge on-premises appliance VM and its corresponding Azure resource.	Extension	GA
az arcappliance create hci	Command to create the connection between the on-premises appliance VM and Azure resource for Arc resource bridge (Azure Stack HCI).	Extension	GA
az arcappliance create scvmm	Command to create the connection between the on-premises appliance VM and Azure resource for Arc resource bridge on SCVMM.	Extension	GA
az arcappliance create vmware	Command to create the connection between the on-premises appliance VM and Azure resource for Arc resource bridge (Arc-enabled VMware).	Extension	GA
az arcappliance createconfig	Command group for creating configuration files for Arc resource bridge.	Extension	GA
az arcappliance createconfig hci	Command to create configuration files for Arc Resource Bridge on HCI.	Extension	GA
az arcappliance createconfig scvmm	Command to create Arc resource bridge configuration files for Arc-enabled SCVMM.	Extension	GA
az arcappliance createconfig vmware	Command to create Arc resource bridge configuration files for Arc-enabled VMware.	Extension	GA
az arcappliance delete	Command group for deletion of an Arc resource bridge on-premises appliance VM and its Azure resource.	Extension	GA
az arcappliance delete hci	Command to delete the on-premises appliance VM on Azure Stack HCI and Arc resource bridge Azure resource.	Extension	GA
az arcappliance delete scvmm	Command to delete the on-premises appliance VM on SCVMM and Azure resource.	Extension	GA
az arcappliance delete vmware	Command to delete the on-premises appliance VM and Azure resource for Arc resource bridge (Arc-enabled VMware).	Extension	GA
az arcappliance deploy	Command group for deployment of the Arc resource bridge on-premises appliance VM and creation of its corresponding Azure resource.	Extension	GA
az arcappliance deploy hci	Command to deploy the Arc resource bridge's on-premises appliance VM on Azure Stack HCI and its corresponding Azure resource.	Extension	GA

Name	Description	Type	Status
az arcappliance deploy scvmm	Command to deploy the Arc resource bridge's on-premises appliance VM and its Azure resource for Arc-enabled SCVMM.	Extension	GA
az arcappliance deploy vmware	Command to deploy the Arc resource bridge's on-premises appliance VM on VMWare and its corresponding Azure resource.	Extension	GA
az arcappliance get-credentials	Command to get the on-premises infrastructure credentials used by Arc resource bridge to manage on-premises resources.	Extension	GA
az arcappliance get-upgrades	Command to fetch the available upgrades for an Appliance.	Extension	GA
az arcappliance list	Command to list Arc resource bridge resources.	Extension	GA
az arcappliance logs	Command group for collecting logs for Arc resource bridge. Run get-credentials command before running logs command.	Extension	GA
az arcappliance logs hci	Command to collect logs for an Appliance on Azure Stack HCI.	Extension	GA
az arcappliance logs scvmm	Command to collect logs for Arc resource bridge on SCVMM (Arc-enabled SCVMM).	Extension	GA
az arcappliance logs vmware	Command to collect logs for Appliance on VMware.	Extension	GA
az arcappliance notice	Command to display the EULA & Notice File link for Arc resource bridge.	Extension	GA
az arcappliance prepare	Command group for preparing for an Arc resource bridge deployment. This downloads the necessary images to build the on-premises appliance VM and uploads it to the private cloud gallery.	Extension	GA
az arcappliance prepare hci	Command to prepare the on-premises Azure Stack HCI environment for an Arc resource bridge deployment. This downloads the necessary images to build the on-premises appliance VM and uploads it to the private cloud gallery.	Extension	GA
az arcappliance prepare scvmm	Command to prepare for an Arc resource bridge deployment on SCVMM for Arc-enabled SCVMM. This downloads the necessary images to build the on-premises appliance VM and uploads it to the private cloud gallery.	Extension	GA

Name	Description	Type	Status
az arcappliance prepare vmware	Command to prepare for an Arc resource bridge deployment on VMware for Arc-enabled VMware. This downloads the necessary images to build the on-premises appliance VM and uploads it to the private cloud gallery.	Extension	GA
az arcappliance run	Command group for consecutively running the Arc resource bridge commands required for deployment. This command is idempotent.	Extension	GA
az arcappliance run hci	Command to consecutively run the Arc resource bridge commands required for deployment on Azure Stack HCI. This command is idempotent.	Extension	GA
az arcappliance run scvmm	Command to consecutively run the Arc resource bridge commands required for deployment on SCVMM. This command is idempotent.	Extension	GA
az arcappliance run vmware	Command to consecutively run the Arc resource bridge commands required for deployment on VMware (Arc-enabled VMware). This command is idempotent.	Extension	GA
az arcappliance show	Command to provide information about an Arc resource bridge Azure resource. This is useful to monitor the status of the resource bridge.	Extension	GA
az arcappliance troubleshoot	Command group for troubleshooting an Appliance cluster.	Extension	GA
az arcappliance troubleshoot command	Command group for troubleshooting an Appliance cluster by executing a shell command.	Extension	GA
az arcappliance troubleshoot command hci	Command to execute a shell command on an HCI cluster for troubleshooting. Either --ip or --kubeconfig must be provided. If both are passed in, --ip will be used.	Extension	GA
az arcappliance troubleshoot command scvmm	Command to execute a shell command on an SCVMM cluster for troubleshooting. Either --ip or --kubeconfig must be provided. If both are passed in, --ip will be used.	Extension	GA
az arcappliance troubleshoot command vmware	Command to execute a shell command on an VMWare cluster for troubleshooting. Either --ip or --kubeconfig must be provided. If both are passed in, --ip will be used.	Extension	GA
az arcappliance update-infracredentials	Command group for updating the on-premises infrastructure credentials used by Arc resource bridge to manage on-premises resources.	Extension	GA
az arcappliance update-	Command to update the on-premises infrastructure credentials for Azure Stack HCI used by Arc resource	Extension	GA

Name	Description	Type	Status
infracredentials hci	bridge.		
az arcappliance update-infracredentials scvmm	Command to update the SCVMM credentials used by Arc resource bridge.	Extension	GA
az arcappliance update-infracredentials vmware	Command to update the VMware credentials used by Arc resource bridge.	Extension	GA
az arcappliance upgrade	Command group for upgrading an Appliance cluster.	Extension	GA
az arcappliance upgrade hci	Command to upgrade an Appliance on Azure Stack HCI.	Extension	GA
az arcappliance upgrade scvmm	Command to upgrade an Appliance on SCVMM.	Extension	GA
az arcappliance upgrade vmware	Command to upgrade an Appliance on VMware.	Extension	GA
az arcappliance validate	Command group to perform validations on Arc resource bridge configuration files and network settings.	Extension	GA
az arcappliance validate hci	Command to validate Arc resource bridge configuration files and network settings on Azure Stack HCI - should be done before 'prepare' command.	Extension	GA
az arcappliance validate scvmm	Command to validate Arc resource bridge configuration files and network settings for Arc-enabled SCVMM - should be done before 'prepare' command.	Extension	GA
az arcappliance validate vmware	Command to validate Arc resource bridge configuration files and network settings for Arc-enabled VMware - should be done before 'prepare' command.	Extension	GA

az arcappliance get-credentials

Command to get the on-premises infrastructure credentials used by Arc resource bridge to manage on-premises resources.

Azure CLI

```
az arcappliance get-credentials [--acquire-policy-token]
                                [--change-reference]
                                [--config-file]
                                [--credentials-dir]
                                [--name]
                                [--overwrite-existing {false, true}]
                                [--partner {false, true}]
                                [--resource-group]
                                [--yes {false, true}]
```

Examples

Command to get user credentials using resource name and resource group and write them to a dir.

Azure CLI

```
az arcappliance get-credentials --resource-group [REQUIRED] --name [REQUIRED] --
credentials-dir [OPTIONAL]
```

Command to get user credentials using config file and write them to a dir.

Azure CLI

```
az arcappliance get-credentials --config-file [REQUIRED] --credentials-dir
[OPTIONAL]
```

Command to get user credentials using config file and write them to a dir which does not exist, and create the dir without prompting.

Azure CLI

```
az arcappliance get-credentials --config-file [REQUIRED] --credentials-dir
[OPTIONAL] --y [OPTIONAL]
```

Command to get user credentials and write them to a file. Overwrite files if they exist.

Azure CLI

```
az arcappliance get-credentials --resource-group [REQUIRED] --name [REQUIRED] --
credentials-dir [OPTIONAL] --overwrite-existing [OPTIONAL]
```

Command to get partner credentials used by private cloud RP/service to access Arc Resource Bridge. Credentials will be printed to Stdout.

Azure CLI

```
az arcappliance get-credentials --resource-group [REQUIRED] --name [REQUIRED] --
partner [OPTIONAL]
```

Optional Parameters

The following parameters are optional, but depending on the context, one or more might become required for the command to execute successfully.

`--acquire-policy-token`

Acquiring an Azure Policy token automatically for this resource operation.

Expand table

Property	Value
Parameter group:	Global Policy Arguments

`--change-reference`

The related change reference ID for this resource operation.

Expand table

Property	Value
Parameter group:	Global Policy Arguments

`--config-file`

Path to Appliance Config File. This is required if name and resource group are not specified.

`--credentials-dir`

Specify a directory path where the log key, certificate output and kubeconfig are saved. If no value specified, for Darwin/Linux defaults to ~/.kva/.ssh for keys and current directory for kubeconfig,for windows defaults to C:\ProgramData\kva.ssh for keys and current directory for kubeconfig.

`--name -n`

Name of the Arc resource bridge.

`--overwrite-existing`

Overwrite existing kubeconfig file. Default: False.

Expand table

Property	Value
Default value:	False
Accepted values:	false, true

`--partner`

Returns the credentials used by private cloud RP/service to access Arc Resource Bridge. Default: customer user credentials.

Expand table

Property	Value
Default value:	False
Accepted values:	false, true

`--resource-group -g`

Name of resource group. You can configure the default group using `az configure --defaults group=<name>`.

`--yes -y`

Do not prompt for confirmation to create credentials_dir if directory does not exist. Default is to prompt for directory creation.

Expand table

Property	Value
Default value:	False

Property	Value
Accepted values:	false, true

Global Parameters

`--debug`

Increase logging verbosity to show all debug logs.

Expand table

Property	Value
Default value:	False

`--help -h`

Show this help message and exit.

`--only-show-errors`

Only show errors, suppressing warnings.

Expand table

Property	Value
Default value:	False

`--output -o`

Output format.

Expand table

Property	Value
Default value:	json
Accepted values:	json, jsonc, none, table, tsv, yaml, yamlc

`--query`

JMESPath query string. See http://jmespath.org/ for more information and examples.

`--subscription`

Name or ID of subscription. You can configure the default subscription using `az account set -s NAME_OR_ID`.

`--verbose`

Increase logging verbosity. Use --debug for full debug logs.

Expand table

Property	Value
Default value:	False

az arcappliance get-upgrades

Command to fetch the available upgrades for an Appliance.

Azure CLI

```
az arcappliance get-upgrades --name
                             --resource-group
                             [--acquire-policy-token]
                             [--change-reference]
```

Examples

Fetch the available upgrades for a specific Appliance.

Azure CLI

```
az arcappliance get-upgrades --resource-group [REQUIRED] --name [REQUIRED]
```

Required Parameters

`--name -n`

Name of the Arc resource bridge.

`--resource-group -g`

Name of resource group. You can configure the default group using `az configure --defaults group=<name>`.

Optional Parameters

The following parameters are optional, but depending on the context, one or more might become required for the command to execute successfully.

`--acquire-policy-token`

Acquiring an Azure Policy token automatically for this resource operation.

Expand table

Property	Value
Parameter group:	Global Policy Arguments

`--change-reference`

The related change reference ID for this resource operation.

Expand table

Property	Value
Parameter group:	Global Policy Arguments

Global Parameters

`--debug`

Increase logging verbosity to show all debug logs.

Expand table

Property	Value
Default value:	False

`--help -h`

Show this help message and exit.

`--only-show-errors`

Only show errors, suppressing warnings.

Expand table

Property	Value
Default value:	False

`--output -o`

Output format.

Expand table

Property	Value
Default value:	json
Accepted values:	json, jsonc, none, table, tsv, yaml, yamlc

`--query`

JMESPath query string. See http://jmespath.org/ for more information and examples.

`--subscription`

Name or ID of subscription. You can configure the default subscription using `az account set -s NAME_OR_ID`.

`--verbose`

Increase logging verbosity. Use --debug for full debug logs.

Expand table

Property	Value
Default value:	False

az arcappliance list

Command to list Arc resource bridge resources.

Azure CLI

```
az arcappliance list [--resource-group]
```

Examples

Command to list Arc resource bridge resources in a resource group in the current subscription.

Azure CLI

```
az arcappliance list -g [OPTIONAL]
```

Optional Parameters

The following parameters are optional, but depending on the context, one or more might become required for the command to execute successfully.

`--resource-group -g`

Name of resource group. You can configure the default group using `az configure --defaults group=<name>`.

Global Parameters

`--debug`

Increase logging verbosity to show all debug logs.

Expand table

Property	Value
Default value:	False

`--help -h`

Show this help message and exit.

`--only-show-errors`

Only show errors, suppressing warnings.

Expand table

Property	Value
Default value:	False

`--output -o`

Output format.

Expand table

Property	Value
Default value:	json
Accepted values:	json, jsonc, none, table, tsv, yaml, yamlc

`--query`

JMESPath query string. See http://jmespath.org/ for more information and examples.

`--subscription`

Name or ID of subscription. You can configure the default subscription using `az account set -s NAME_OR_ID`.

`--verbose`

Increase logging verbosity. Use --debug for full debug logs.

Expand table

Property	Value
Default value:	False

az arcappliance notice

Command to display the EULA & Notice File link for Arc resource bridge.

Azure CLI

```
az arcappliance notice [--acquire-policy-token]
                       [--change-reference]
```

Examples

Displays the EULA & Notice File link for Arc resource bridge.

Azure CLI

```
az arcappliance notice
```

Optional Parameters

The following parameters are optional, but depending on the context, one or more might become required for the command to execute successfully.

`--acquire-policy-token`

Acquiring an Azure Policy token automatically for this resource operation.

Expand table

Property	Value
Parameter group:	Global Policy Arguments

`--change-reference`

The related change reference ID for this resource operation.

Expand table

Property	Value
Parameter group:	Global Policy Arguments

Global Parameters

`--debug`

Increase logging verbosity to show all debug logs.

Expand table

Property	Value
Default value:	False

`--help -h`

Show this help message and exit.

`--only-show-errors`

Only show errors, suppressing warnings.

Expand table

Property	Value
Default value:	False

`--output -o`

Output format.

Expand table

Property	Value
Default value:	json
Accepted values:	json, jsonc, none, table, tsv, yaml, yamlc

`--query`

JMESPath query string. See http://jmespath.org/ for more information and examples.

`--subscription`

Name or ID of subscription. You can configure the default subscription using `az account set -s NAME_OR_ID`.

`--verbose`

Increase logging verbosity. Use --debug for full debug logs.

Expand table

Property	Value
Default value:	False

az arcappliance show

Command to provide information about an Arc resource bridge Azure resource. This is useful to monitor the status of the resource bridge.

Azure CLI

```
az arcappliance show --name
                     --resource-group
```

Examples

Command to show details about a particular Arc resource bridge in a resource group.

Azure CLI

```
az arcappliance show --resource-group [REQUIRED] --name [REQUIRED]
```

Required Parameters

`--name -n`

Name of the Arc resource bridge.

`--resource-group -g`

Name of resource group. You can configure the default group using `az configure --defaults group=<name>`.

Global Parameters

`--debug`

Increase logging verbosity to show all debug logs.

Expand table

Property	Value
Default value:	False

`--help -h`

Show this help message and exit.

`--only-show-errors`

Only show errors, suppressing warnings.

Expand table

Property	Value
Default value:	False

`--output -o`

Output format.

Expand table

Property	Value
Default value:	json
Accepted values:	json, jsonc, none, table, tsv, yaml, yamlc

`--query`

JMESPath query string. See http://jmespath.org/ for more information and examples.

`--subscription`

Name or ID of subscription. You can configure the default subscription using `az account set -s NAME_OR_ID`.

`--verbose`

Increase logging verbosity. Use --debug for full debug logs.

Expand table

Property	Value
Default value:	False