

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](#)
- [📁 Create SQL Managed Instance](#)
- [📁 Create PostgreSQL server](#)

[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 Stack HCI](#)

Training modules

- [📁 Introduction to Azure Arc](#)
- [📁 Introduction to Azure Arc-enabled servers](#)
- [📁 Introduction to Azure Arc-enabled Kubernetes](#)
- [📁 Introduction to Azure Arc-enabled data services](#)

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 \(preview\)](#)

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

[App Service, Functions, and Logic Apps on Azure Arc \(preview\)](#)

Run App Service, Functions, and Logic 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 metaverse.

[Azure Arc site manager \(preview\)](#)

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

Azure Arc overview

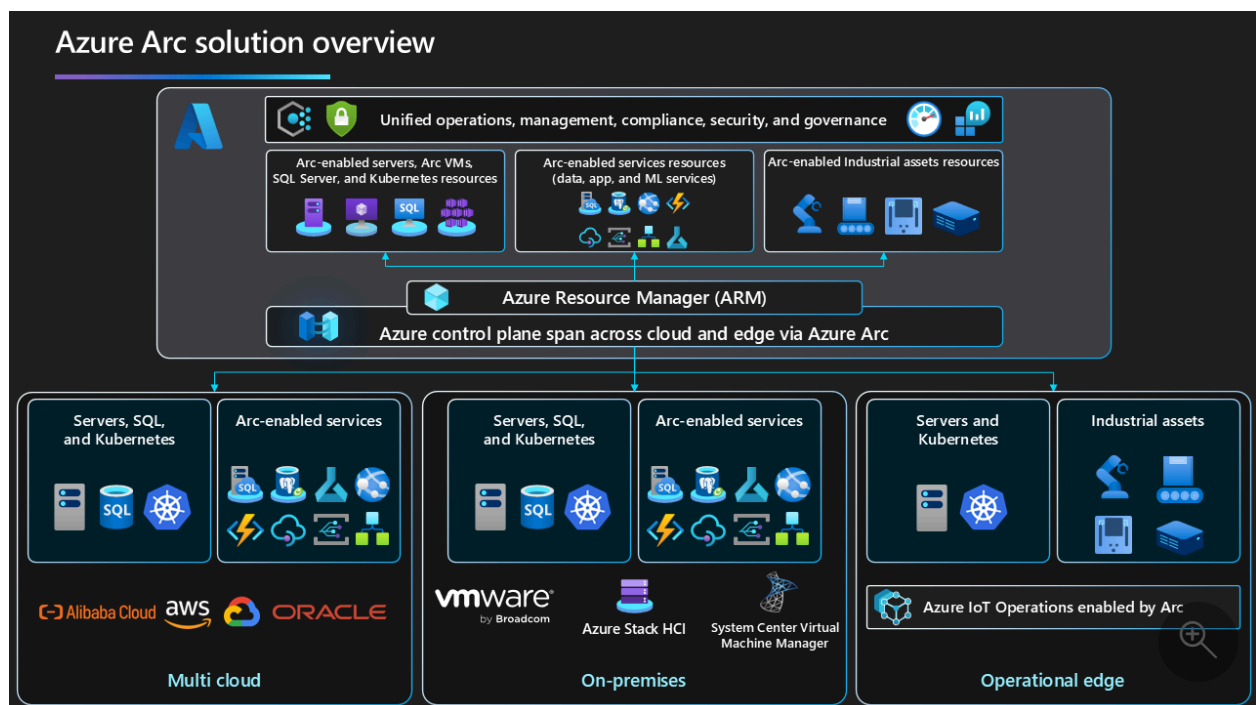
Article • 10/08/2024

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.



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 Stack HCI](#) 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 Azure data services on-premises, at the edge, and in public clouds using Kubernetes and the infrastructure of your choice. SQL Managed Instance and PostgreSQL (preview) services are currently available.
- [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](#).

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 and Azure Database for PostgreSQL server, 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](#), [App services on Azure Arc](#) (including web, function, and logic apps) and [Event Grid on Kubernetes](#).

- Perform virtual machine lifecycle and management operations on [Azure Stack HCI](#) 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](#).

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 Stack HCI.](#)
- 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.](#)

Feedback

Was this page helpful?



[Provide product feedback](#)  | [Get help at Microsoft Q&A](#)

Choosing the right Azure Arc service for machines

Article • 09/19/2024

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 Stack HCI

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.

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
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
Azure Stack HCI VM	Azure Stack HCI
Physical server	Azure Arc-enabled servers
VM on another hypervisor	Azure Arc-enabled servers

If your machine is a...	...connect to Azure with...
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 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.

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 on SCVMM VMs to govern, protect, configure, and monitor them.

Azure Stack HCI

[Azure Stack HCI](#) 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 Stack HCI 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 Stack HCI 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 HCI 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 Stack HCI 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 Stack HCI 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.

Capabilities at a glance

The following table provides a quick way to see the major capabilities of the three 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 Stack HCI
Microsoft Defender for Cloud	✓	✓	✓	✓
Microsoft Sentinel	✓	✓	✓	✓
Azure Automation	✓	✓	✓	✓
Azure Update Manager	✓	✓	✓	✓
VM extensions	✓	✓	✓	✓
Azure Monitor	✓	✓	✓	✓
Extended Security Updates for Windows Server 2012/2012R2 and SQL Server 2012 (11.x)	✓	✓	✓	✓
Discover & onboard VMs to Azure		✓	✓	X
Lifecycle operations (start/stop VMs, etc.)		✓	✓	✓
Self-serve VM provisioning		✓	✓	✓
SQL Server enabled by Azure Arc	✓	✓	✓	✓

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
-

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#)  | [Get help at Microsoft Q&A](#)

Custom locations

Article • 09/19/2024

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](#) and [Azure Arc-enabled PostgreSQL server](#).

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

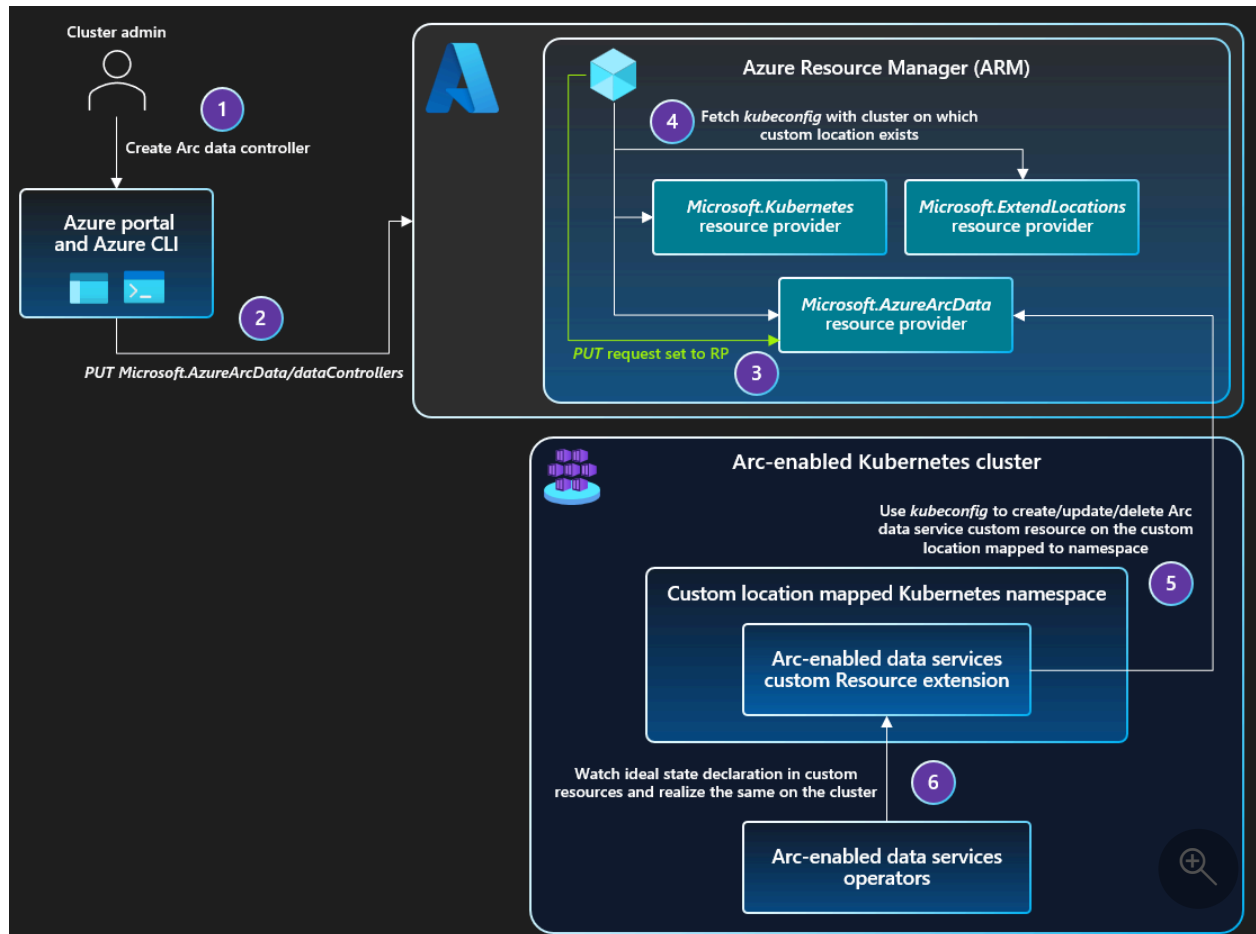
Since the custom location is an Azure Resource Manager resource that supports [Azure role-based access control \(Azure RBAC\)](#), an administrator or operator can determine which users have access to create resource instances on:

- A namespace within a Kubernetes cluster to target deployment of SQL Managed Instance enabled by Azure Arc or Azure Arc-enabled PostgreSQL server.
- The compute, storage, networking, and other vCenter or Azure Stack HCI 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.

The sequence of steps to create the SQL managed instance or PostgreSQL instance are identical to the sequence of steps described above.

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.

Feedback

Was this page helpful?

Yes

No

[Provide product feedback](#)  | [Get help at Microsoft Q&A](#)

Azure Resource Graph sample queries for Azure Arc

Article • 09/19/2024

This page is a collection of [Azure Resource Graph](#) sample queries for Azure 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"

```

Next steps

- Learn more about the [query language](#).
- Learn more about how to [explore resources](#).

Feedback

Was this page helpful?

[Provide product feedback](#) | [Get help at Microsoft Q&A](#)

What is Azure Arc resource bridge?

Article • 09/19/2024

Azure Arc resource bridge is a Microsoft managed product that is part of the core Azure Arc platform. It is designed to host other Azure Arc services. In this release, the resource bridge supports VM self-servicing and management from Azure, for virtualized Windows and Linux virtual machines hosted in an on-premises environment on Azure Stack HCI ([Azure Arc VM management](#)), VMware ([Arc-enabled VMware vSphere](#)), and System Center Virtual Machine Manager ([Arc-enabled SCVMM](#)).

Azure Arc resource bridge is a Kubernetes management cluster installed on the customer's on-premises infrastructure as an appliance VM (also known as the Arc appliance). The resource bridge is provided credentials to the infrastructure control plane that allows it to apply guest management services on the on-premises resources. Arc resource bridge enables projection of on-premises resources as ARM resources and management from ARM as "Arc-enabled" Azure resources.

Arc resource bridge delivers the following benefits:

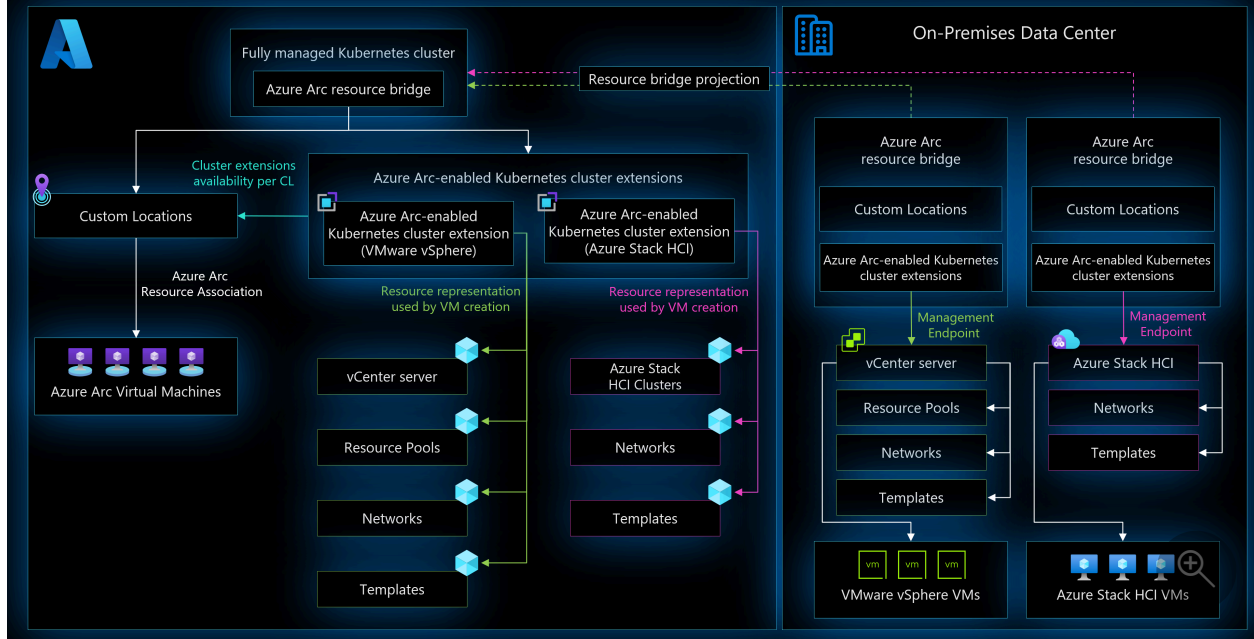
- Enables VM self-servicing from Azure without having to create and manage a Kubernetes cluster.
- Fully supported by Microsoft, including updates to core components.
- Supports deployment to any private cloud hosted on Hyper-V or VMware from the Azure portal or using the Azure Command-Line Interface (CLI).

Overview

Azure Arc resource bridge hosts other components such as [custom locations](#), cluster extensions, and other Azure Arc agents in order to deliver the level of functionality with the private cloud infrastructures it supports. This complex system is composed of three layers:

- The base layer that represents the resource bridge and the Arc agents.
- The platform layer that includes the custom location and cluster extension.
- The solution layer for each service supported by Arc resource bridge (that is, the different type of VMs).

Azure Arc Resource Bridge architecture



Azure Arc resource bridge can host other Azure services or solutions running on-premises. There are two objects hosted on the Arc resource bridge:

- Cluster extension: The Azure service deployed to run on-premises. Currently, it supports three services:
 - Azure Arc VM management on Azure Stack HCI
 - Azure Arc-enabled VMware
 - Azure Arc-enabled System Center Virtual Machine Manager (SCVMM)
- Custom locations: A deployment target where you can create Azure resources. It maps to different resource for different Azure services. For example, for Arc-enabled VMware, the custom locations resource maps to an instance of vCenter, and for Azure Arc VM management on Azure Stack HCI, it maps to an HCI cluster instance.

Custom locations and cluster extension are both Azure resources, which are linked to the Azure Arc resource bridge resource in Azure Resource Manager. When you create an on-premises VM from Azure, you can select the custom location, and that routes that *create action* to the mapped vCenter, Azure Stack HCI cluster, or SCVMM.

Some resources are unique to the infrastructure. For example, vCenter has a resource pool, network, and template resources. During VM creation, these resources need to be specified. With Azure Stack HCI, you just need to select the custom location, network, and template to create a VM.

To summarize, the Azure resources are projections of the resources running in your on-premises private cloud. If the on-premises resource isn't healthy, it can impact the health of the related resources that are projected in Azure. For example, if the resource bridge

is deleted by accident, all the resources projected in Azure by the resource bridge are impacted. The on-premises VMs in your on-premises private cloud aren't impacted, as they're running on vCenter, but you won't be able to start or stop the VMs from Azure. Directly managing or modifying the resource bridge using on-premises applications isn't recommended.

Benefits of Azure Arc resource bridge

Through Azure Arc resource bridge, you can accomplish the following tasks for each private cloud infrastructure from Azure:

Azure Stack HCI

You can provision and manage on-premises Windows and Linux virtual machines (VMs) running on Azure Stack HCI clusters.

VMware vSphere

By registering resource pools, networks, and VM templates, you can represent a subset of your vCenter resources in Azure to enable self-service. Integration with Azure allows you to manage access to your vCenter resources in Azure to maintain a secure environment. You can also perform various operations on the VMware virtual machines that are enabled by Arc-enabled VMware vSphere:

- Start, stop, and restart a virtual machine
- Control access and add Azure tags
- Add, remove, and update network interfaces
- Add, remove, and update disks and update VM size (CPU cores and memory)
- Enable guest management
- Install extensions

System Center Virtual Machine Manager (SCVMM)

You can connect an SCVMM management server to Azure by deploying Azure Arc resource bridge in the VMM environment. Azure Arc resource bridge enables you to represent the SCVMM resources (clouds, VMs, templates etc.) in Azure and perform various operations on them:

- Start, stop, and restart a virtual machine
- Control access and add Azure tags
- Add, remove, and update network interfaces

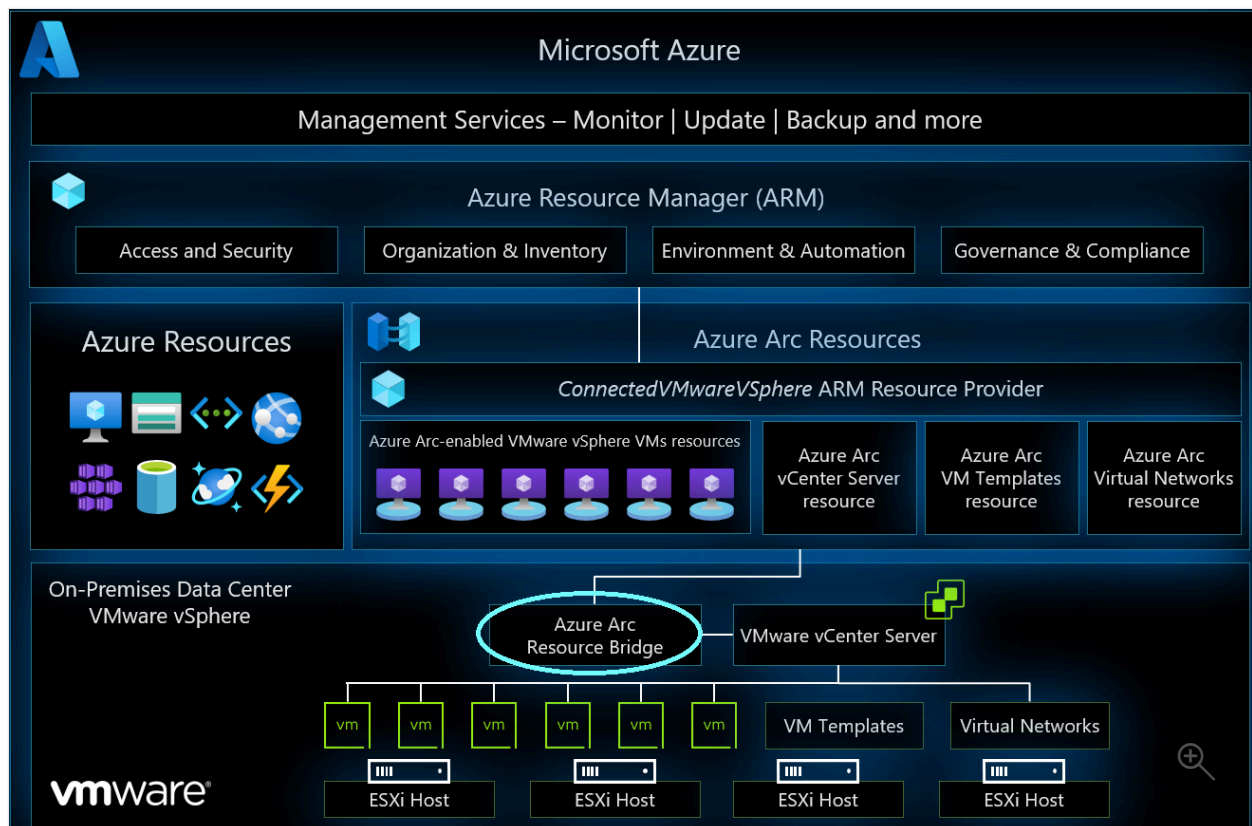
- Add, remove, and update disks and update VM size (CPU cores and memory)
- Enable guest management
- Install extensions

Example scenarios

The following are just two examples of the many scenarios that can be enabled by using Arc resource bridge in a hybrid environment.

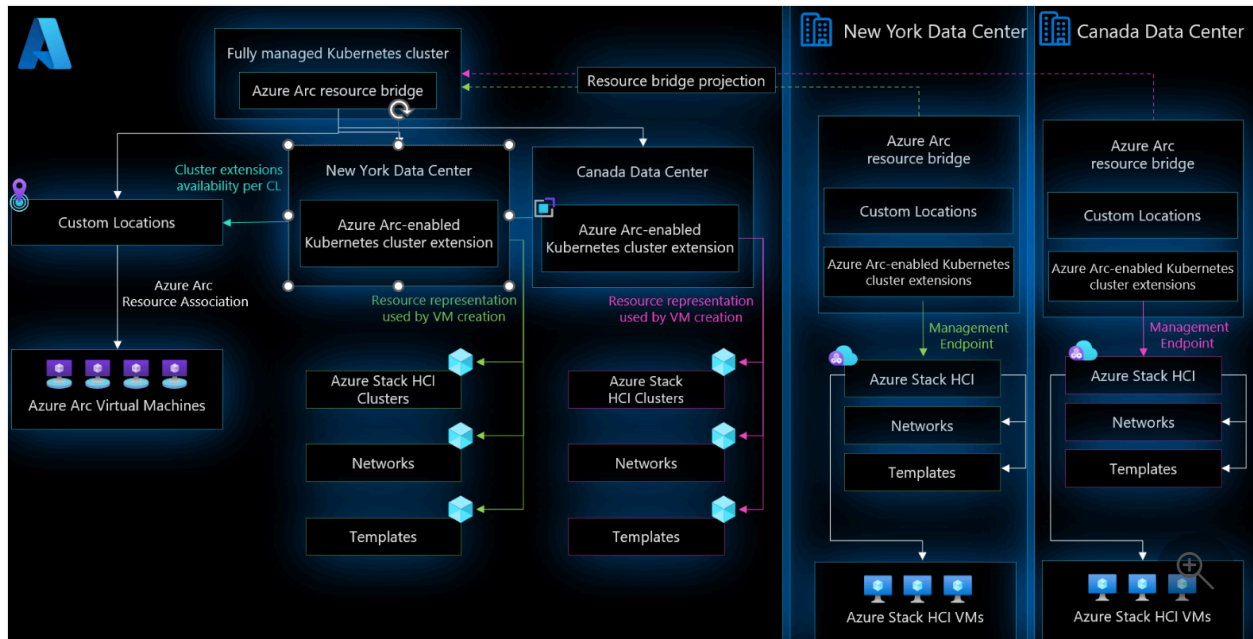
Apply Azure Policy and other Azure services to on-premises VMware VMs

A customer deploys Arc Resource Bridge onto their on-premises VMware environment. They sign into the Azure portal and select the VMware VMs that they'd like to connect to Azure. Now they can manage these on-premises VMware VMs in Azure Resource Manager (ARM) as Arc-enabled machines, alongside their native Azure machines, achieving a single pane of glass to view their resources in a VMware/Azure hybrid environment. This includes deploying Azure services, such as Defender for Cloud and Azure Policy, to keep updated on the security and compliance posture of their on-premises VMware VMs in Azure.



Create physical HCI VMs on-premises from Azure

A customer has multiple datacenter locations in Canada and New York. They install an Arc resource bridge in each datacenter and connect their Azure Stack HCI VMs to Azure in each location. They can then sign into Azure portal and see all their Arc-enabled VMs from the two physical locations together in one central cloud location. From the portal, the customer can choose to create a new VM; that VM is also created on-premises at the selected datacenter, allowing the customer to manage VMs in different physical locations centrally through Azure.



Version and region support

Supported regions

In order to use Arc resource bridge in a region, Arc resource bridge and the Arc-enabled feature for a private cloud must be supported in the region. For example, to use Arc resource bridge with Azure Stack HCI in East US, Arc resource bridge and the Arc VM management feature for Azure Stack HCI must be supported in East US. To confirm feature availability across regions for each private cloud provider, review their deployment guide and other documentation. There could be instances where Arc resource bridge is available in a region where the private cloud feature 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
- Canada Central
- Australia East
- Australia SouthEast
- West Europe
- North Europe
- UK South
- UK West
- Sweden Central
- Japan East
- Southeast Asia
- East Asia
- Central India

Regional resiliency

While Azure has redundancy features at every level of failure, if a service impacting event occurs, Azure Arc resource bridge currently doesn't support cross-region failover or other resiliency capabilities. If the service becomes unavailable, on-premises VMs continue to operate unaffected. Management from Azure is unavailable during that service outage.

Private cloud environments

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

- VMware vSphere version 7.0, 8.0
- Azure Stack HCI
- SCVMM

Supported versions

Generally, the latest released version and the previous three versions (n-3) of Arc resource bridge are supported. For example, if the current version is 1.0.18, then the typical n-3 supported versions are:

- Current version: 1.0.18
- n-1 version: 1.0.17

- n-2 version: 1.0.16
- n-3 version: 1.0.15

There could be instances where supported versions aren't sequential. For example, version 1.0.18 is released and later found to contain a bug; a hot fix is released in version 1.0.19 and version 1.0.18 is removed. In this scenario, n-3 supported versions become 1.0.19, 1.0.17, 1.0.16, 1.0.15.

Arc resource bridge typically releases a new version on a monthly cadence, at the end of the month. Delays might occur that could push the release date further out. Regardless of when a new release comes out, if you are within n-3 supported versions, then your Arc resource bridge version is supported. To stay updated on releases, visit the [Arc resource bridge release notes](#). To learn more about upgrade options, visit [Upgrade Arc resource bridge](#).

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 Stack HCI clusters](#).
- Review the [system requirements](#) for deploying and managing Arc resource bridge.

Feedback

Was this page helpful?

[Provide product feedback](#)  | [Get help at Microsoft Q&A](#)

What's new with Azure Arc resource bridge

Article • 09/19/2024

Azure Arc resource bridge is updated on an ongoing basis. To stay up to date with the most recent developments, this article provides you with information about recent releases.

We generally recommend using the most recent versions of the agents. The [version support policy](#) generally covers the most recent version and the three previous versions (n-3).

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 timeout 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 timeouts 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 handling 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, 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, 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 Timeout 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 timeout 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 Stack HCI - extend `deploy` command timeout 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](#).

Feedback

Was this page helpful?

Yes

No

[Provide product feedback](#)  | [Get help at Microsoft Q&A](#)

Azure Arc resource bridge system requirements

Article • 09/19/2024

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

Arc resource bridge is used with other partner products, such as [Azure Stack HCI](#), [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 Stack HCI, 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 Stack HCI. 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 Stack HCI. 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 separate user account with the necessary roles to view and manage resources in the on-premises infrastructure (such as Arc-enabled VMware vSphere). If so, during creation of the configuration files, the `username` and `password` parameters are required. The account credentials are then stored in a configuration file locally 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 separate 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.

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 made 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.

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](#).

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#)  | [Get help at Microsoft Q&A](#)

Azure Arc resource bridge network requirements

Article • 09/20/2024

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

General network requirements

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, Appliance VM, and Control Plane IP to the required Arc resource bridge URLs.

Firewall/Proxy URL allowlist

 Expand table

Service	Port	URL	Direction	Notes
SFS API endpoint	443	<code>msk8s.api.cdp.microsoft.com</code>	Management machine & Appliance VM IPs need outbound connection.	Download product catalog, product bits, and OS

Service	Port	URL	Direction	Notes
				images from SFS.
Resource bridge (appliance) image download	443	<code>msk8s.sb.tlu.dl.delivery.mp.microsoft.com</code>	Management machine & Appliance VM IPs need outbound connection.	Download the Arc Resource Bridge OS images.
Microsoft Container Registry	443	<code>mcr.microsoft.com</code>	Management machine & Appliance VM IPs need outbound connection.	Download container images for Arc Resource Bridge.
Windows NTP Server	123	<code>time.windows.com</code>	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 Manager	443	<code>management.azure.com</code>	Management machine & Appliance VM IPs need outbound connection.	Manage resources in Azure.
Microsoft Graph	443	<code>graph.microsoft.com</code>	Management machine & Appliance VM IPs need outbound connection.	Required for Azure RBAC.
Azure Resource Manager	443	<code>login.microsoftonline.com</code>	Management machine & Appliance VM IPs need	Required to update ARM tokens.

Service	Port	URL	Direction	Notes
			outbound connection.	
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 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.
Azure Arc agent	443	k8connecthel1m.azureedge.net	Appliance VM IPs need outbound connection.	deploy Azure Arc agent.

Service	Port	URL	Direction	Notes
ADHS telemetry service	443	<code>adhs.events.data.microsoft.com</code>	Appliance VM IPs need outbound connection.	Periodically sends Microsoft required diagnostic data from appliance VM.
Microsoft events data service	443	<code>v20.events.data.microsoft.com</code>	Appliance VM IPs need outbound connection.	Send diagnostic data from Windows.
Log collection for Arc Resource Bridge	443	<code>linuxgeneva-microsoft.azurecr.io</code>	Appliance VM IPs need outbound connection.	Push logs for Appliance managed components.
Resource bridge components download	443	<code>kvamanagementoperator.azurecr.io</code>	Appliance VM IPs need outbound connection.	Pull artifacts for Appliance managed components.
Microsoft open source packages manager	443	<code>packages.microsoft.com</code>	Appliance VM IPs need outbound connection.	Download Linux installation package.
Custom Location	443	<code>sts.windows.net</code>	Appliance VM IPs need outbound connection.	Required for Custom Location.
Azure Arc	443	<code>guestnotificationsservice.azure.com</code>	Appliance VM IPs need outbound connection.	Required for Azure Arc.
Custom Location	443	<code>k8sconnectcsp.azureedge.net</code>	Appliance VM IPs need outbound connection.	Required for Custom Location.

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

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

[Expand table](#)

Service	Port	IP/machine	Direction	Notes
SSH	22	appliance VM IPs and Management machine	Bidirectional	Used for deploying and maintaining the appliance VM.
Kubernetes API server	6443	appliance VM IPs and Management machine	Bidirectional	Management of the appliance VM.
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 control plane (ex: VMware vCenter address).

ⓘ 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

IP Address	Reason for exclusion
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 <code>noProxy</code> list. Use a leading period rather than a wildcard (*) character. In the sample, the addresses <code>.contoso.com</code> excludes addresses <code>prefix1.contoso.com</code> , <code>prefix2.contoso.com</code> , 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](#).
-

Feedback

Was this page helpful?

Yes

No

[Provide product feedback](#)  | [Get help at Microsoft Q&A](#)

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

Was this page helpful?

[Provide product feedback](#)  | [Get help at Microsoft Q&A](#)

Azure Arc resource bridge deployment command overview

Article • 10/03/2024

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

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 Stack HCI VM Management 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 Stack HCI 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 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 will return in the terminal, even though the connection between the ARM resource and on-premises appliance VM is not yet complete. 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](#).

Feedback

Was this page helpful?



Yes



No

[Provide product feedback](#)  | [Get help at Microsoft Q&A](#)

Upgrade Arc resource bridge

Article • 10/03/2024

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

Currently, private cloud providers differ in how they perform Arc resource bridge upgrades. Review the following information to see how to upgrade your Arc resource bridge for a specific provider.

For **Arc-enabled VMware vSphere**, manual upgrade and cloud-managed upgrade are available. Appliances on version 1.0.15 and higher are automatically opted-in to cloud-managed upgrade. Cloud-managed upgrade helps ensure the appliance VM is kept within n-3 supported versions but not the latest version. If you would like to be on the latest version, you need to manual upgrade. In order for either upgrade option to work, [the upgrade prerequisites](#) must be met. Microsoft may attempt to perform a cloud-managed upgrade of your Arc resource bridge at any time if your appliance will soon be out of support. While Microsoft offers cloud-managed upgrade, you're still responsible for ensuring that your Arc resource bridge is within the supported n-3 versions. Disruptions could cause cloud-managed upgrade to fail and you may need to manual upgrade the Arc resource bridge. If your Arc resource bridge is close to being out of support, we recommend a manual upgrade to make sure you maintain a supported version, rather than waiting for cloud-managed upgrade.

For **Azure Arc VM management (preview) on Azure Stack HCI**, appliance version 1.0.15 or higher is only available on Azure Stack HCI build 23H2. In HCI 23H2, the LCM tool manages upgrades across all HCI, Arc resource bridge, and extension components as a "validated recipe" package. Any preview version of Arc resource bridge must be removed before updating from 22H2 to 23H2. Attempting to upgrade Arc resource bridge independent of other HCI environment components may cause problems in your environment that could result in a disaster recovery scenario. For more information, see [About updates for Azure Stack HCI](#).

For **Arc-enabled System Center Virtual Machine Manager (SCVMM)**, the manual upgrade feature 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. Review the steps for [performing the recovery operation](#). This deploys a new resource bridge and reconnects pre-existing Azure resources.

Prerequisites

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

- The appliance VM must be on a General Availability version (1.0.15 or higher). If not, the Arc resource bridge VM needs to be redeployed. If you're using Arc-enabled VMware/AVS, you can [perform disaster recovery](#). If you're using Arc-enabled SCVMM, follow this [disaster recovery guide](#).
- The appliance VM 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 up to date. To test that the credentials within the Arc resource bridge VM are valid, perform an operation on an Arc-enabled VM from Azure. You can also [update the credentials](#) to be certain.
- There must be sufficient space on the management machine (~3.5 GB) and appliance VM (35 GB) to download required images.
- For Arc-enabled VMware, upgrading the resource bridge requires 200 GB of free space on the datastore. A new template is also created.
- The outbound connection from the Appliance VM IPs (`k8snodeippoolstart/end`, VM IP 1/2) to `msk8s.sb.tlu.dl.delivery.mp.microsoft.com`, port 443 must be enabled. Be sure the full list of [required endpoints for Arc resource bridge](#) are also enabled.
- When performing a manual upgrade, run the upgrade command from the management machine used to initially deploy the Arc resource bridge, which should still contain the [appliance configuration files](#). You can also run the upgrade command from a different machine that meets the [management machine requirements](#) and also contains the appliance configuration files.
- Arc resource bridge configured with DHCP can't be upgraded and aren't supported in a production environment. Instead, a new Arc resource bridge should be deployed using [static IP configuration](#).

Overview

The upgrade process deploys a new resource bridge using the reserved appliance VM IP (`k8snodeippoolend` IP, VM IP 2). Once the new resource bridge is up, it becomes the active resource bridge. The old resource bridge is deleted, and its appliance VM IP (`k8snodeippoolstart`, VM IP 1) becomes the new reserved appliance VM IP that will be used in the next upgrade.

Deploying a new resource bridge is a process consisting of several steps: downloading the appliance image (~3.5 GB) from the cloud, using the image to deploy a new appliance VM, verifying the new resource bridge is running, connecting it to Azure, deleting the old appliance VM, and reserving the old IP to be used for a future upgrade.

Overall, the upgrade generally takes at least 30 minutes, depending on network speeds. A short intermittent downtime might happen during the handoff between the old Arc resource bridge to the new Arc resource bridge. Additional downtime can occur if prerequisites aren't met, or if a change in the network (DNS, firewall, proxy, etc.) impacts the Arc resource bridge's network connectivity.

There are two ways to upgrade Arc resource bridge: cloud-managed upgrades managed by Microsoft, or manual upgrades where Azure CLI commands are performed by an admin.

Cloud-managed upgrade

Arc resource bridges on a supported [private cloud provider](#) with an appliance version 1.0.15 or higher are automatically opted into cloud-managed upgrade. With cloud-managed upgrade, Microsoft may attempt to upgrade your Arc resource bridge at any time if it is on an appliance version that will soon be out of support. The upgrade prerequisites must be met for cloud-managed upgrade to work. While Microsoft offers cloud-managed upgrade, you're still responsible for checking that your resource bridge is healthy, online, in a "Running" status, and within the supported n-3 versions. Disruptions could cause cloud-managed upgrades to fail. If your Arc resource bridge is close to being out of support, we recommend a manual upgrade to make sure you maintain a supported version, rather than waiting for cloud-managed upgrade.

To check your resource bridge status and the appliance version, run the `az arcappliance show` command from your management machine or check the Azure resource of your Arc resource bridge. If your appliance VM isn't in a healthy, Running state, cloud-managed upgrade might fail.

Cloud-managed upgrades are handled through Azure. A notification is pushed to Azure to reflect the state of the appliance VM as it upgrades. As the resource bridge progresses through the upgrade, its status might switch back and forth between

different upgrade steps. Upgrade is complete when the appliance VM `status` is `Running` and `provisioningState` is `Succeeded`.

To check the status of a cloud-managed upgrade, check the Azure resource in ARM, or run the following Azure CLI command from the management machine:

```
Azure CLI
```

```
az arcappliance show --resource-group [REQUIRED] --name [REQUIRED]
```

Manual upgrade

Arc resource bridge can be manually upgraded from the management machine. You must meet all upgrade prerequisites before attempting to upgrade. The management machine must have the kubeconfig and [appliance configuration files](#) stored locally, or you won't be able to run the upgrade.

Manual upgrade generally takes between 30-90 minutes, depending on network speeds. The upgrade command takes your Arc resource bridge to the next appliance version, which might not be the latest available appliance version. Multiple upgrades could be needed to reach a [supported version](#). You can check your appliance version by checking the Azure resource of your Arc resource bridge.

Before upgrading, you need the latest Azure CLI extension for `arcappliance`:

```
Azure CLI
```

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

To manually upgrade your resource bridge, use the following command:

```
Azure CLI
```

```
az arcappliance upgrade <private cloud> --config-file <file path to ARBname-appliance.yaml>
```

For example, to upgrade a resource bridge on VMware, run: `az arcappliance upgrade vmware --config-file c:\contosoARB01-appliance.yaml`

To upgrade a resource bridge on SCVMM, run: `az arcappliance upgrade scvmm --config-file c:\contosoARB01-appliance.yaml`

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

Version releases

The Arc resource bridge version is tied to the versions of underlying components used in the appliance image, such as the Kubernetes version. When there's a change in the appliance image, the Arc resource bridge version gets incremented. This generally happens when a new `az arcapppliance` CLI extension version is released. A new extension is typically released on a monthly cadence at the end of the month or early in the month. For detailed release info, see the [Arc resource bridge release notes](#).

Supported versions

Generally, the latest released version and the previous three versions (n-3) of Arc resource bridge are supported. An Arc resource bridge on an unsupported version must be upgraded or redeployed to be in a production support window.

For example, if the current version is 1.0.18, then the typical n-3 supported versions are:

- Current version: 1.0.18
- n-1 version: 1.0.17
- n-2 version: 1.0.16
- n-3 version: 1.0.15

There might be instances where supported versions aren't sequential. For example, version 1.0.18 is released and later found to contain a bug. A hot fix is released in version 1.0.19 and version 1.0.18 is removed. In this scenario, n-3 supported versions become 1.0.19, 1.0.17, 1.0.16, 1.0.15.

Arc resource bridge typically releases a new version on a monthly cadence, at the end of the month, although it's possible that delays could push the release date further out. Regardless of when a new release comes out, if you're within n-3 supported versions, then your Arc resource bridge version is supported. To stay updated on releases, visit the [Arc resource bridge release notes](#).

If a resource bridge isn't upgraded to one of the supported versions (n-3), it falls outside the support window and will be unsupported. It might not always be possible to upgrade an unsupported resource bridge to a newer version, as component services used by Arc resource bridge may no longer be compatible. In addition, the unsupported resource bridge might not be able to provide reliable monitoring and health metrics.

If an Arc resource bridge can't be upgraded to a supported version, you must delete it and deploy a new resource bridge. Depending on which private cloud product you're using, there might be other steps required to reconnect the resource bridge to existing resources. For details, check the partner product's Arc resource bridge recovery documentation.

Notification and upgrade availability

If your Arc resource bridge is at version n-3, you might receive an email notification letting you know that your resource bridge will be out of support once the next version is released. If you receive this notification, upgrade the resource bridge as soon as possible to allow debug time for any issues with manual upgrade, or submit a support ticket if cloud-managed upgrade was unable to upgrade your resource bridge.

To check if your Arc resource bridge has an upgrade available, run the command:

Azure CLI

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

To see the current version of an Arc resource bridge appliance, run `az arcappliance show` or check the Azure resource of your Arc resource bridge.

Next steps

- Learn about [Arc resource bridge maintenance operations](#).
- Learn about [troubleshooting Arc resource bridge](#).

Feedback

Was this page helpful?

Yes

No

[Provide product feedback](#)  | [Get help at Microsoft Q&A](#)

Azure Arc resource bridge maintenance operations

Article • 09/20/2024

To keep your Azure Arc resource bridge deployment online and operational, you need to perform maintenance operations such as updating credentials, monitoring upgrades, and ensuring the appliance VM is online.

Prerequisites

To maintain the on-premises appliance VM, the [appliance configuration files generated during deployment](#) need to be saved in a secure location and made available on the management machine.

The management machine used to perform maintenance operations must meet all of [the Arc resource bridge requirements](#).

The following sections describe the 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](#) (for example, a user account for VMware vCenter) that are used to access the control center of the on-premises infrastructure to view and manage on-premises resources. The credentials used by Arc resource bridge are the same ones provided during deployment of the resource bridge. This allows the resource bridge visibility to on-premises resources for guest management in Azure.

If the credentials change, the credentials stored in the Arc resource bridge must be updated with the [update-fracredentials command](#). This command must be run from the management machine, and it requires a [kubeconfig file](#).

For more information, see [Update the vSphere account credentials](#).

Troubleshoot Arc resource bridge

If you experience problems with the appliance VM, the appliance configuration files can help with troubleshooting. You can include these files when you [open an Azure support request](#).

You might want to [collect logs](#), which requires you to pass credentials to the on-premises control center:

- For VMWare vSphere, use the username and password provided to Arc resource bridge at deployment.
- For Azure Stack HCI, see [Collect logs](#).

Delete Arc resource bridge

You might need to delete Arc resource bridge due to deployment failures, or when the resource bridge is no longer needed. To do so, you need the appliance configuration files.

The [delete command](#) is the recommended way 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.

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](#).

Feedback

Was this page helpful?

[Provide product feedback](#)  | [Get help at Microsoft Q&A](#)

Troubleshoot Azure Arc resource bridge issues

Article • 10/03/2024

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](#).

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 Stack HCI, 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>
```

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.

`UploadError` 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

Networking changes in the infrastructure, environment or cluster can stop the appliance VM from being able to communicate with its counterpart Azure resource. If you're unable to determine what changed, you can reboot the appliance VM, collect logs and submit a support ticket for further investigation.

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 Stack HCI cluster 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.

Resource bridge configurations can't be updated

In this release, all the parameters are specified at time of creation. To update Arc resource bridge, you must delete it and redeploy it again.

For example, if you specify the wrong location or subscription during deployment, resource creation fails. If you only try to recreate the resource without redeploying the resource bridge VM, the status gets stuck at `WaitForHeartBeat`.

To resolve this issue, delete the appliance and update the appliance YAML file. After that, redeploy and create the resource bridge.

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 Stack HCI, 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.

Resource bridge status `offline` and `provisioningState Failed`

When you deploy Arc resource bridge, the bridge might appear to be successfully deployed because no errors were encountered when running `az arcappliance deploy` or `az arcappliance create`. However, when viewing the bridge in Azure portal, you might see status showing as `Offline`, and `az arcappliance show` might show the `provisioningState` as `Failed`. This issue happens when required providers aren't registered before the bridge is deployed.

For Azure Stack HCI, version 23H2 and later, the Arc Resource Bridge is automatically deployed during the cluster deployment and manual installation is no longer required.

If your Arc Resource Bridge is offline, try restarting the Arc Resource Bridge VM. If the issue persists, contact Microsoft Support.

ⓘ Note

Reinstalling the Arc Resource Bridge on Azure Stack HCI could cause issues with your existing Azure resources.

To resolve this problem, delete the resource bridge, register the providers, then redeploy the resource bridge.

1. Delete the resource bridge:

Azure CLI

```
az arcappliance delete <fabric> --config-file <path to appliance.yaml>
```

2. Register the providers:

Azure CLI

```
az provider register --namespace Microsoft.ExtendedLocation --wait  
az provider register --namespace Microsoft.ResourceConnector --wait
```

3. Redeploy the resource bridge.

ⓘ Note

Partner products (such as Arc-enabled VMware vSphere) might have their own required providers to register. For information about these additional providers, see the product's documentation.

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 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.

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\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\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/AA1a73m are
reachable from the Appliance VM. 2. Check firewall/proxy settings\\_\\_\\_ }\\_\\_\\_
}
```

```
{ _errorCode_: _PostOperationsError_, _errorResponse_: _{\n_message\_: \_{\n\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/AA1a73m are
reachable from the Appliance VM. 2. Check firewall/proxy settings\\_\\_\\_\\_\\_}
}
```

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 an error message similar to:

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

This error occurs 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

An error that contains `dial tcp: lookup`

`westeurope.dp.kubernetesconfiguration.azure.com: no such host` while deploying Arc resource bridge means that the configuration data plane is currently unavailable in the specified region. The service may be temporarily unavailable. Wait for the service to be available, then retry the deployment.

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 Stack HCI).
- 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 Stack HCI. 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 Stack HCI). 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 Stack HCI MOC cloud agent. Review [network requirements for Azure Stack HCI](#) and [VMware](#) for Arc resource bridge.
- Appliance VM IP and Control Plane IP need internet access to [these required URLs](#). Azure Stack HCI 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 Stack HCI. 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 Stack HCI. 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. If not, [delete the appliance](#), recreate the Arc resource bridge configuration files with the correct DNS server settings, and then deploy Arc resource bridge using the new configuration files.

Move Arc resource bridge location

Resource move of Arc resource bridge isn't currently supported. Instead, delete the Arc resource bridge and redeploy it to the desired location.

Azure Arc-enabled VMs on Azure Stack HCI issues

For general help resolving issues related to Azure Arc-enabled VMs on Azure Stack HCI, see [Troubleshoot Azure Arc-enabled virtual machines](#).

If you are running Azure Stack HCI, version 23H2 or later, and your Arc Resource Bridge is offline, do not attempt to reinstall or delete the Arc Resource Bridge. Instead, try restarting the Arc Resource Bridge VM to bring it back online. If the issue persists, contact [Microsoft Support](#) [↗] for assistance.

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\n\n\n\_code\_:\n\n\_GuestInternetConnectivityError\_,\n\n\n\n\_message\_:\n\n\_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/AA1a73m 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>"
```

Azure Arc-enabled VMware vCenter issues

errorMessage: error getting the vsphere sdk client

Errors with `errorCode: CreateConfigKvaCustomerError` and `errorMessage: 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.

x509 certificate has expired or isn't yet valid

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
_\n_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/AA1a73m are reachable from the Appliance VM. 2.
Check firewall/proxy settings
```

This error is caused when there's a clock/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 }\" }"
```

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 - not found or does not exist

When you deploy Arc resource bridge, you specify where the appliance VM is deployed. The appliance VM can't be moved from that location path. If the appliance VM moves location and you try to upgrade, you might see errors similar the following:

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

```
{\n  \"code\": \"PreflightcheckError\", \n  \"message\": \"{\\n  \\\"code\\\": \\\"InvalidEntityError\\\", \\n  \\\"message\\\": \\\"The specified vSphere Datacenter '/VxRail-Datacenter' does not exist\\\"\\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.
- 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.
- Delete and [redploy the Arc resource bridge](#).

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\":\n  \"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.](#)
-

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#) | [Get help at Microsoft Q&A](#)

What is Azure Arc-enabled servers?

Article • 09/19/2024

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. For the purposes of Azure Arc, these machines hosted outside of Azure are considered hybrid machines. The management of hybrid machines in Azure Arc is designed to be consistent with how you manage native Azure virtual machines, using standard Azure constructs such as Azure Policy and applying tags. (For additional information about hybrid environments, see [What is a hybrid cloud?](#))

When a hybrid machine is connected to Azure, it becomes a connected machine and is treated as a resource in Azure. Each connected machine has a Resource ID enabling the machine to be included in a resource group.

To connect hybrid machines to Azure, you install the [Azure Connected Machine agent](#) on each machine. This agent doesn't replace the Azure [Azure Monitor Agent](#). The Azure Monitor Agent for Windows and Linux is required in order to:

- Proactively monitor the OS and workloads running on the machine
- Manage it using Automation runbooks or solutions like Update Management
- Use other Azure services like [Microsoft Defender for Cloud](#)

You can install the Connected Machine agent manually, or on multiple machines at scale, using the [deployment method](#) that works best for your scenario.

ⓘ 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.

ⓘ 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. Below are some of the key supported actions for connected machines.

- **Govern:**
 - Assign [Azure machine configurations](#) to audit settings inside the machine. To understand the cost of using Azure Machine Configuration policies with Arc-enabled servers, see Azure Policy [pricing guide](#) [↗].
- **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 [Change Tracking and Inventory](#)
 - Use [Update Management](#) to manage operating system updates for your Windows and Linux servers. Automate onboarding and configuration of a set of Azure services when you use [Azure Automanage \(preview\)](#).
 - Perform post-deployment configuration and automation tasks 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 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](#).

ⓘ Note

At this time, enabling Azure Automation Update Management directly from an Azure Arc-enabled server is not supported. See [Enable Update Management from your Automation account](#) to understand requirements and [how to enable Update Management for non-Azure VMs](#).

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> [↗](#)

Supported regions

For a list of supported regions with Azure Arc-enabled servers, see the [Azure products by region](#) [↗](#) page.

In most cases, the location you select when you create the installation script should be the Azure region geographically closest to your machine's location. Data at rest is stored within the Azure geography containing the region you specify, which may also affect your choice of region if you have data residency requirements. If the Azure region your machine connects to has an outage, the connected machine isn't affected, but management operations using Azure may be unable to complete. If there's a regional outage, and if you have multiple locations that support a geographically redundant service, it's best to connect the machines in each location to a different Azure region.


[Instance metadata information about the connected machine](#) is collected and stored in the region where the Azure Arc machine resource is configured, including the following:

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

For example, if the machine is registered with Azure Arc in the East US region, the metadata is stored in the US region.

Supported environments

Azure Arc-enabled servers support the management of physical servers and virtual machines hosted *outside* of Azure. For specific details about supported hybrid cloud environments hosting VMs, see [Connected Machine agent prerequisites](#).

 **Note**

Azure Arc-enabled servers is not designed or supported to enable management of virtual machines running in Azure.

Agent status

The status for a connected machine can be viewed in the Azure portal under **Azure Arc > Servers**.

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, that machine is considered offline, and its status will automatically be changed to **Disconnected** within 15 to 30 minutes. Upon receiving a subsequent heartbeat message from the Connected Machine agent, its status will automatically be changed back to **Connected**.

If a machine remains disconnected for 45 days, its status may change to **Expired**. An expired machine can no longer connect to Azure and requires a server administrator to disconnect and then reconnect it to Azure to continue managing it with Azure Arc. The exact date upon which a machine expires is determined by the expiration date of the managed identity's credential, which is valid up to 90 days and renewed every 45 days.

Service limits

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


To learn more about resource type limits, see the [Resource instance limit](#) article.

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 region with data residency requirements, customer data is always kept within the same region.

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 [Azure Arc landing zone accelerator for hybrid and multicloud](#).
-

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#)  | [Get help at Microsoft Q&A](#)

What is Azure Arc-enabled Kubernetes?

Article • 10/08/2024

Azure Arc-enabled Kubernetes allows you to attach Kubernetes clusters running anywhere so that you can manage and configure them in Azure. By managing all of your Kubernetes resources in a single control plane, you can enable a more consistent development and operation experience, helping you run cloud-native apps anywhere and on any Kubernetes platform.

When the [Azure Arc agents are deployed to the cluster](#), an outbound connection to Azure is initiated, using industry-standard SSL to secure data in transit.

Clusters that you connect to Azure are represented as their own resources in Azure Resource Manager, and they can be organized using resource groups and tagging.

Supported Kubernetes distributions

Azure Arc-enabled Kubernetes works with any Cloud Native Computing Foundation (CNCF) certified Kubernetes clusters. This includes clusters running on other public cloud providers (such as GCP or AWS) and clusters running on your on-premises data center (such as VMware vSphere or Azure Stack HCI).


The Azure Arc team has worked with key industry partners to [validate conformance of their Kubernetes distributions with Azure Arc-enabled Kubernetes](#).

Scenarios and enhanced functionality

Once your Kubernetes clusters are connected to Azure, at scale you can:


- View all connected Kubernetes clusters for inventory, grouping, and tagging, along with your Azure Kubernetes Service (AKS) clusters.
- Configure clusters and deploy applications using [GitOps-based configuration management](#).
- View and monitor your clusters using [Azure Monitor for containers](#).
- Enforce threat protection using [Microsoft Defender for Kubernetes](#).
- Ensure governance through applying policies with [Azure Policy for Kubernetes](#).

- Grant access and [connect](#) to your Kubernetes clusters from anywhere, and manage access by using [Azure role-based access control \(RBAC\)](#) on your cluster.
- Deploy machine learning workloads using [Azure Machine Learning for Kubernetes clusters](#).
- Deploy and manage Kubernetes applications from Azure Marketplace.
- Deploy services that allow you to take advantage of specific hardware, comply with data residency requirements, or enable new scenarios. Examples of services include:
 - [Azure Arc-enabled data services](#)
 - [Azure Machine Learning for Kubernetes clusters](#)
 - [Event Grid on Kubernetes](#)
 - [App Services on Azure Arc](#)
 - [Open Service Mesh](#)

 **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 Arc-enabled Kubernetes without provisioning a full environment by using the [Azure Arc Jumpstart](#) .
- [Connect an existing Kubernetes cluster to Azure Arc](#).

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#)  | [Get help at Microsoft Q&A](#)

What are Azure Arc-enabled data services?

Article • 09/19/2024

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
- Azure Arc-enabled PostgreSQL (preview)

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 and Azure Arc-enabled PostgreSQL server 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, Azure Data Studio, 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.

At this time, use the [insiders build of Azure Data Studio](#).

Disconnected scenario support

Many of the services such as self-service provisioning, automated backups/restore, and monitoring can run locally in your infrastructure with or without a direct connection to Azure. Connecting directly to Azure opens up additional options for integration with other Azure services such as Azure Monitor and the ability to use the Azure portal and Azure Resource Manager APIs from anywhere in the world to manage your Azure Arc-enabled data services.

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
```



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

Azure PowerShell

[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)

[Create an Azure Database for PostgreSQL server on Azure Arc](#) (requires creation of an Azure Arc data controller first)

Feedback

Was this page helpful?

[Provide product feedback](#) | [Get help at Microsoft Q&A](#)

What is Azure Arc-enabled VMware vSphere?

Article • 09/19/2024

Azure Arc-enabled VMware vSphere is an [Azure Arc](#) service that helps you simplify management of hybrid IT estate distributed across VMware vSphere and Azure. It does so by extending the Azure control plane to VMware vSphere infrastructure and enabling the use of Azure security, governance, and management capabilities consistently across VMware vSphere and Azure.

Arc-enabled VMware vSphere allows you to:

- Discover your VMware vSphere estate (VMs, templates, networks, datastores, clusters/hosts/resource pools) and register resources with 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 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.

ⓘ Note

For more information regarding the different services Azure Arc offers, see [Choosing the right Azure Arc service for machines](#).

Onboard resources to Azure management at scale

Azure services such as Microsoft Defender for Cloud, Azure Monitor, Azure Update Manager, and Azure Policy provide a rich set of capabilities to secure, monitor, patch, and govern off-Azure resources via Arc.

By using Arc-enabled VMware vSphere's capabilities to discover your VMware estate and install the Arc agent at scale, you can simplify onboarding your entire VMware vSphere estate to these services.

Set up self-service access for your teams to use vSphere resources using Azure Arc

Arc-enabled VMware vSphere extends Azure's control plane (Azure Resource Manager) to VMware vSphere infrastructure. This enables you to use Microsoft Entra ID-based identity management, granular Azure RBAC, and Azure Resource Manager (ARM) templates to help your app teams and developers get self-service access to provision and manage VMs on VMware vSphere environment, providing greater agility.

1. Virtualized Infrastructure Administrators/Cloud Administrators can connect a vCenter instance to Azure.
2. Administrators can then use the Azure portal to browse VMware vSphere inventory and register virtual machines resource pools, networks, and templates into Azure.
3. Administrators can provide app teams/developers fine-grained permissions on those VMware resources through Azure RBAC.
4. App teams can use Azure interfaces (portal, CLI, or REST API) to manage the lifecycle of on-premises VMs they use for deploying their applications (CRUD, Start/Stop/Restart).
5. App teams can use Azure Resource Manager (ARM) templates/Bicep (Infrastructure as Code) to deploy VMs as part of CI/CD pipelines.

How does it work?

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 is connected to Azure, an automatic discovery of the inventory of vSphere resources is performed. 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, VM extensions can be installed 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.

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

The easiest way to think of this 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, there can, in fact, not even be a host hypervisor in some cases.
- 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 provides lifecycle management and CRUD (Create, Read, Update, and Delete) operations on a VMware vSphere VM. These lifecycle management capabilities are exposed in the Azure portal and 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 the options, you enjoy the same consistent experience.

Supported VMware vSphere versions

Azure Arc-enabled VMware vSphere currently works with vCenter Server versions 7 and 8.

ⓘ Note

Azure Arc-enabled VMware vSphere supports vCenters with a maximum of 9500 VMs. If your vCenter has more than 9500 VMs, we don't recommend you to use Arc-enabled VMware vSphere with it at this point.

If you're trying to enable Arc for Azure VMware Solution (AVS) private cloud, see [Deploy Arc-enabled VMware vSphere for Azure VMware Solution private cloud](#).

Supported regions

You can use Azure Arc-enabled VMware vSphere in these supported regions:

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

For the most up-to-date information about region availability of Azure Arc-enabled VMware vSphere, see [Azure Products by Region](#) [↗](#) page.

Data Residency

Azure Arc-enabled VMware vSphere doesn't store/process customer data outside the region the customer deploys the service instance in.

Azure Kubernetes Service (AKS) Arc on VMware (preview)


Starting March 2024, Azure Kubernetes Service (AKS) enabled by Azure Arc on VMware is available for preview. AKS Arc on VMware enables you to use Azure Arc to create new

Kubernetes clusters on VMware vSphere. For more information, see [What is AKS enabled by Arc on VMware?](#).

The following capabilities are available in the AKS Arc on VMware preview:

- **Simplified infrastructure deployment on Arc-enabled VMware vSphere:** Onboard VMware vSphere to Azure using a single-step process with the AKS Arc extension installed.
- **Azure CLI:** A consistent command-line experience, with [AKS Arc on Azure Stack HCI 23H2](#), for creating and managing Kubernetes clusters. Note that the preview only supports a limited set of commands.
- **Cloud-based management:** Use familiar tools such as Azure CLI to create and manage Kubernetes clusters on VMware.
- **Support for managing and scaling node pools and clusters.**

Next steps

- Plan your resource bridge deployment by reviewing the [support matrix for Arc-enabled VMware vSphere](#).
- Once ready, [connect VMware vCenter to Azure Arc using the helper script](#).
- Try out Arc-enabled VMware vSphere by using the [Azure Arc Jumpstart](#) .

Feedback

Was this page helpful?

[Provide product feedback](#)  | [Get help at Microsoft Q&A](#)

Overview of Azure Arc-enabled System Center Virtual Machine Manager

Article • 10/18/2024

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 SCVMM extends the Azure control plane to SCVMM managed infrastructure, enabling the use of Azure security, governance, and management capabilities consistently across System Center managed estate and Azure.

Azure Arc-enabled SCVMM 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.

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 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](#).

ⓘ Note

For more information regarding the different services Azure Arc offers, see [Choosing the right Azure Arc service for machines](#).

Onboard resources to Azure management at scale

Azure services such as Microsoft Defender for Cloud, Azure Monitor, Azure Update Manager, and Azure Policy provide a rich set of capabilities to secure, monitor, patch,

and govern off-Azure resources via Arc.

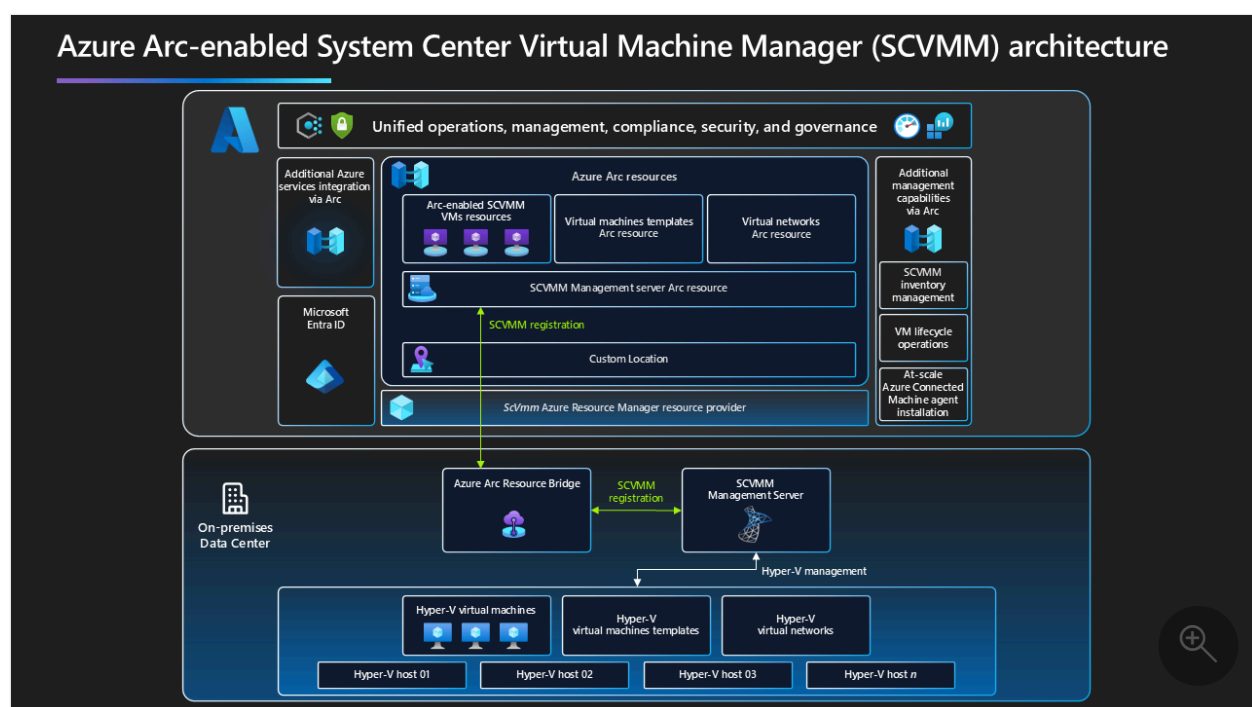
By using Azure Arc-enabled SCVMM's capabilities to discover your SCVMM managed estate and install the Azure Connected Machine agent at scale, you can simplify onboarding your entire System Center estate to these services.

How does it work?

To 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. Azure Arc resource bridge enables you to represent the SCVMM resources (clouds, VMs, templates etc.) in Azure and do various operations on them.

Architecture

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



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, there might, in fact, not even be a host hypervisor 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 provides lifecycle management and CRUD (Create, Read, Update, and Delete) operations on an SCVMM VM. These lifecycle management capabilities are exposed in the Azure portal and look and feel just like a regular Azure VM. Azure Arc-enabled SCVMM 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'll enjoy the same consistent experience.

Supported scenarios

The following scenarios are supported in Azure Arc-enabled SCVMM:

- 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, 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 agents on SCVMM VMs at-scale and install corresponding extensions to use Azure management services like Microsoft Defender for Cloud, Azure Update Manager, Azure Monitor, etc.

ⓘ Note

Azure Arc-enabled SCVMM doesn't support VMware vCenter VMs managed by SCVMM. To onboard VMware VMs to Azure Arc, we recommend you to use [Azure Arc-enabled VMware vSphere](#).

Supported VMM versions

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

Supported regions

Azure Arc-enabled SCVMM is currently supported in the following regions:

- East US
- East US 2
- West US 2
- West US 3
- Central US
- South Central US
- UK South
- North Europe
- West Europe
- Sweden Central
- Southeast Asia
- Australia East

Data Residency

Azure Arc-enabled SCVMM doesn't store/process customer data outside the region the customer deploys the service instance in.

Next steps

- Plan your Azure Arc-enabled SCVMM deployment by reviewing the [support matrix](#).
- Once ready, [connect your SCVMM management server to Azure Arc using the onboarding script](#).

Feedback

Was this page helpful?

[Provide product feedback](#)  | [Get help at Microsoft Q&A](#)

What is Azure Arc VM management?

Article • 02/02/2024

Applies to: Azure Stack HCI, version 23H2

This article provides a brief overview of the Azure Arc VM management feature on Azure Stack HCI including the benefits, its components, and high-level workflow.

About Azure Arc VM management

Azure Arc VM management lets you provision and manage Windows and Linux VMs hosted in an on-premises Azure Stack HCI environment. This feature enables IT admins create, modify, delete, and assign permissions and roles to app owners thereby enabling self-service VM management.

Administrators can manage Arc VMs on their Azure Stack HCI clusters by using Azure management tools, including Azure portal, Azure CLI, Azure PowerShell, and Azure Resource Manager (ARM) templates. Using [Azure Resource Manager](#) templates, you can also automate VM provisioning in a secure cloud environment.

To find answers to frequently asked questions about Arc VM management on Azure Stack HCI, see the [FAQ](#).

Benefits of Azure Arc VM management

While Hyper-V provides capabilities to manage your on-premises VMs, Azure Arc VMs offer many benefits over traditional on-premises tools including:

- Role-based access control via builtin Azure Stack HCI roles ensures that only authorized users can perform VM management operations thereby enhancing security. For more information, see [Azure Stack HCI Arc VM management roles](#).
- Arc VM management provides the ability to deploy with ARM templates, Bicep, and Terraform.
- The Azure portal acts as a single pane of glass to manage VMs on Azure Stack HCI clusters and Azure VMs. With Azure Arc VM management, you can perform various operations from the Azure portal or Azure CLI including:
 - Create, manage, update, and delete VMs. For more information, see [Create Arc VMs](#)

- Create, manage, and delete VM resources such as virtual disks, logical networks, network interfaces, and VM images.
- The self-service capabilities of Arc VM management reduce the administrative overhead.

Components of Azure Arc VM management

Arc VM Management comprises several components including the Arc Resource Bridge, Custom Location, and the Kubernetes Extension for the VM operator.

- **Arc Resource Bridge:** This lightweight Kubernetes VM connects your on-premises Azure Stack HCI cluster to the Azure Cloud. The Arc Resource Bridge is created automatically when you deploy the Azure Stack HCI cluster.

For more information, see the [Arc Resource Bridge overview](#).

- **Custom Location:** Just like the Arc Resource Bridge, a custom location is created automatically when you deploy your Azure Stack HCI cluster. You can use this custom location to deploy Azure services. You can also deploy VMs in these user-defined custom locations, integrating your on-premises setup more closely with Azure.
- **Kubernetes Extension for VM Operator:** The VM operator is the on-premises counterpart of the Azure Resource Manager resource provider. It is a Kubernetes controller that uses custom resources to manage your VMs.

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

Azure Arc VM management workflow

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

1. During the deployment of Azure Stack HCI cluster, one Arc Resource Bridge is installed per cluster and a custom location is also created.
2. [Assign builtin RBAC roles for Arc VM management](#).
3. You can then create VM resources such as:
 - a. [Storage paths](#) for VM disks.
 - b. VM images starting with an [Image in Azure Marketplace](#), in [Azure Storage account](#), or in [Local share](#). These images are then used with other VM resources

to create VMs.

c. [Logical networks](#).

d. [VM network interfaces](#).

4. Use the VM resources to [Create VMs](#).

To troubleshoot issues with your Arc VMs or to learn about existing known issues and limitations, see [Troubleshoot Arc virtual machines](#).

Next steps

- Review [Azure Arc VM management prerequisites](#)

SQL Server enabled by Azure Arc

Article • 04/12/2024

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, or 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](#).

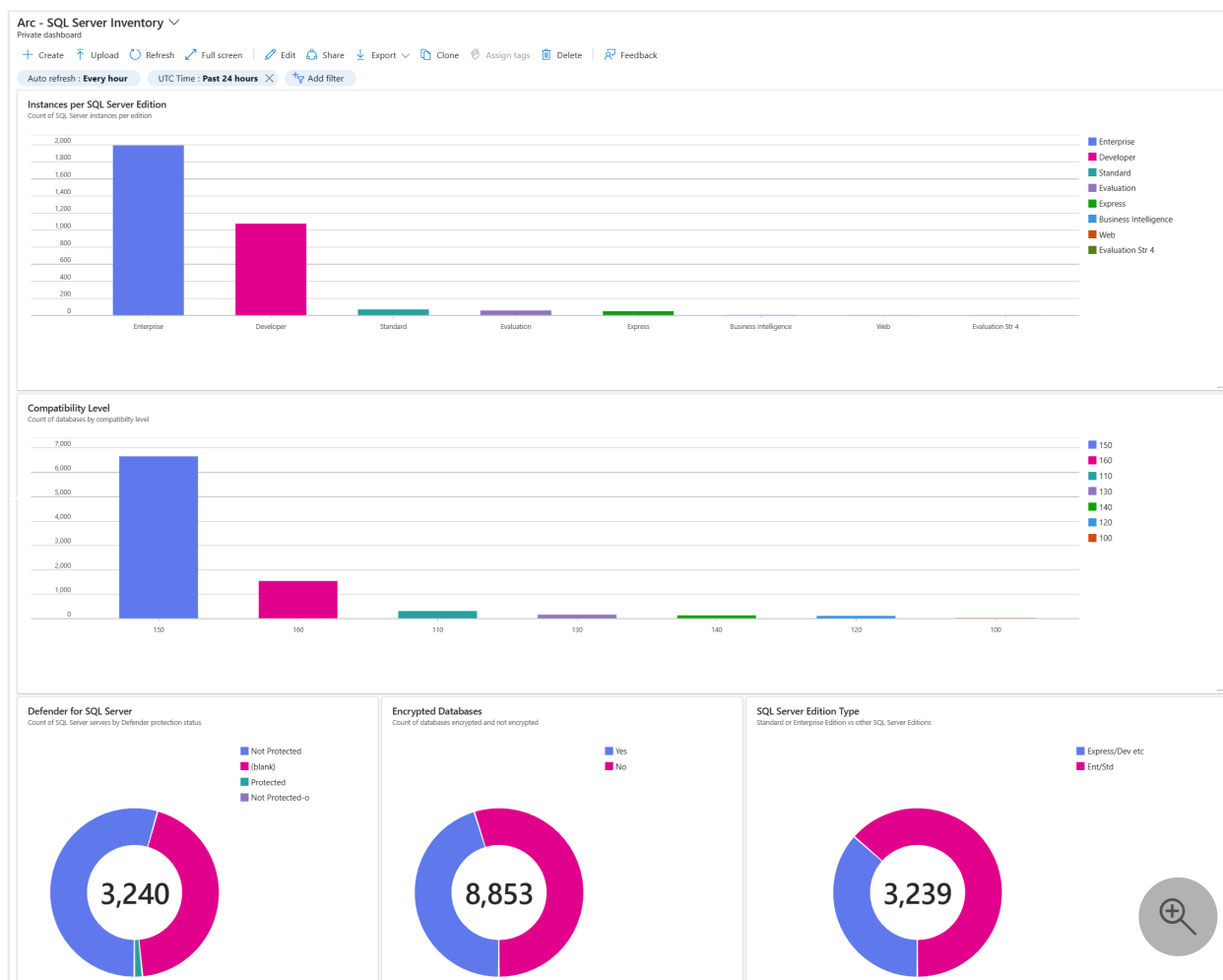
Manage your SQL Server instances at scale from a single point of control

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.

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).

Starting with SQL Server 2022 (16.x), Azure Arc enabled SQL Servers can utilize Microsoft Entra ID for authentication, bringing a modern centralized identity and access management solution to SQL Server. 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

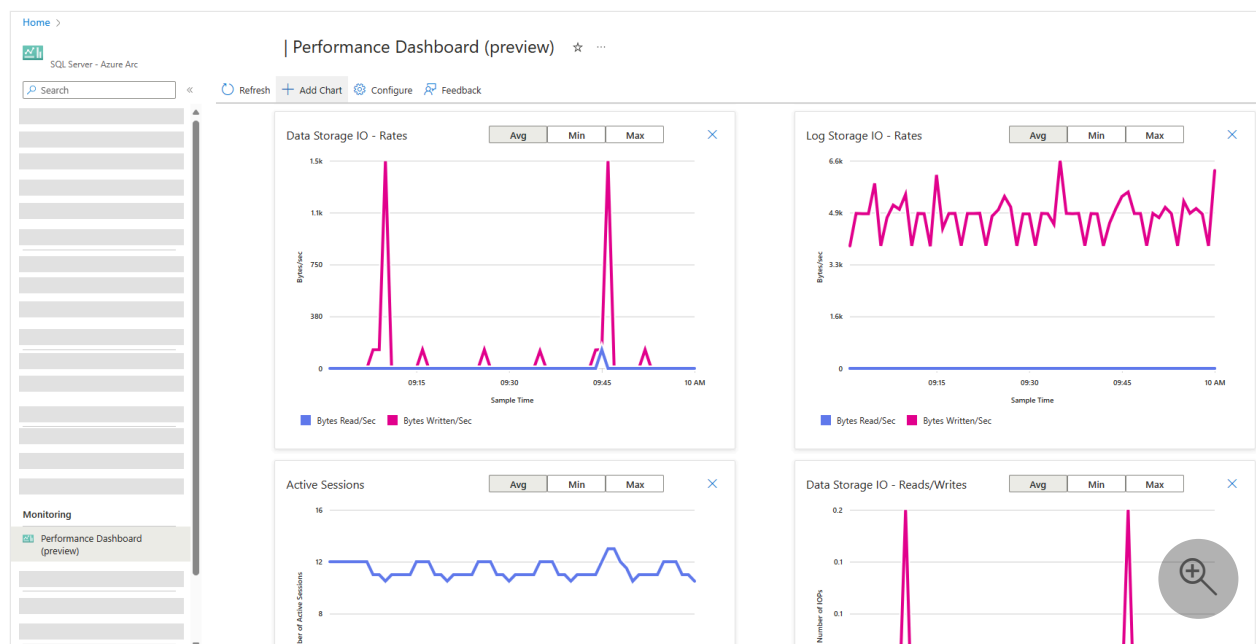
during less busy times. It's also a great option if you only plan to use a SQL Server for a short period of time and then won't need it anymore. Pay-as-you-go, billed through Azure, is now available for all versions of SQL Server from 2012 to 2022.

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 \(preview\)](#).

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](#).

Architecture

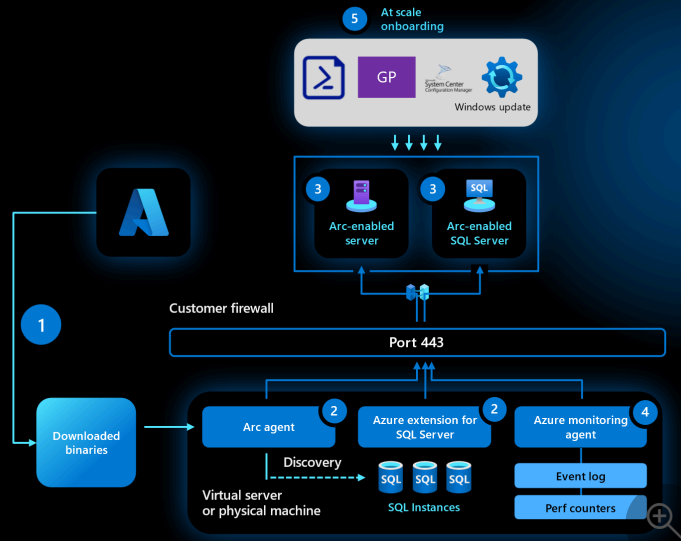
The SQL Server instance that you want to enable with Azure Arc can be installed in a virtual or physical machine running Windows or Linux. The [Azure Connected Machine agent](#) and the Azure Extension for SQL Server securely connect to Azure to establish communication channels with multiple Azure services 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.

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.

SQL Server enabled by Azure Arc architecture

- 1 Generate script & execute on Server
- 2 Local services created
- 3 Arc-enabled server & Arc-enabled SQL Server resources created
- 4 Azure monitoring agent
- 5 Onboard at scale



Feature availability depending on license type

The following table identifies features enabled depending on license type:

[Expand table](#)

Feature	License only ¹	License with Software Assurance or SQL subscription	Pay-as-you-go
Connect to Azure	Yes	Yes	Yes
SQL Server inventory	Yes	Yes	Yes
Best practices assessment	No	Yes	Yes
Migration assessment (preview)	Yes	Yes	Yes
Detailed database inventory	Yes	Yes	Yes
Microsoft Entra ID 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 (preview)	No	Yes	Yes

Feature	License only ¹	License with Software Assurance or SQL subscription	Pay-as-you-go
Automatic updates	No	Yes	Yes
Failover cluster instances	Yes	Yes	Yes
Always On availability groups (preview)	Yes	Yes	Yes
Monitoring (preview)	No	Yes	Yes
Operate with least privilege (preview)	Yes	Yes	Yes

¹ License only includes SQL Server instances that are Developer, Express, Web, or Evaluation Edition and instances using a Server/CAL license.

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
Install Azure extension for SQL Server during setup ¹	Yes	No
Best practices assessment	Yes	No
Migration assessment (preview)	Yes	No
Detailed database 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

Feature	Windows	Linux
SQL Server 2012 extended security updates	Yes	Not applicable
Failover cluster instances	Yes	Not applicable
Always On availability groups (preview)	Yes	Not applicable
Monitoring (preview)	Yes	No
Operate with least privilege (preview)	Yes	No

¹ SQL Server 2022 (16.x) only.

Feature availability by version

The following table identifies features available by SQL Server version:

 Expand table


Feature	2012	2014	2016	2017	2019	2022
Azure pay-as-you-go billing	Yes	Yes	Yes	Yes	Yes	Yes
Best practices assessment	Yes	Yes	Yes	Yes	Yes	Yes
Migration assessment (preview)	Yes	Yes	Yes	Yes	Yes	Yes
Detailed database inventory	Yes	Yes	Yes	Yes	Yes	Yes
Microsoft Entra ID authentication for SQL Server	No	No	No	No	No	Yes
Microsoft Defender for Cloud	Yes	Yes	Yes	Yes	Yes	Yes
Microsoft Purview: DevOps policies	No	No	No	No	No	Yes
Microsoft Purview: data owner policies (preview)	No	No	No	No	No	Yes
Automated backups to local storage (preview)	Yes	Yes	Yes	Yes	Yes	Yes
Point-in-time-restore (preview)	Yes	Yes	Yes	Yes	Yes	Yes
Automatic updates	Yes ¹	Yes	Yes	Yes	Yes	Yes
Failover cluster instances	Yes	Yes	Yes	Yes	Yes	Yes
Always On availability groups (preview)	Yes	Yes	Yes	Yes	Yes	Yes
Monitoring (preview)	Yes	Yes	Yes	Yes	Yes	Yes

Feature	2012	2014	2016	2017	2019	2022
Operate with least privilege (preview)	Yes	Yes	Yes	Yes	Yes	Yes

¹ Requires subscription to [Extended Security Updates \(ESU\) enabled by Azure Arc](#).

Feature availability by edition

The following table identifies features available by SQL Server edition:

 [Expand table](#)

Feature	Enterprise	Standard	Web	Express	Developer	Evaluation
Azure pay-as-you-go billing	Yes	Yes	Not applicable	Not applicable	Not applicable	Not applicable
Best practices assessment	Yes	Yes	Yes	Yes	Yes	Yes
Migration assessment (preview)	Yes	Yes	Yes	Yes	Yes	Yes
Detailed database inventory	Yes	Yes	Yes	Yes	Yes	Yes
Microsoft Entra ID authentication	Yes	Yes	Yes	Yes	Yes	Yes
Microsoft Defender for Cloud	Yes	Yes	Yes	Yes ¹	Yes	Yes
Microsoft Purview: Govern using DevOps and data owner policies	Yes	Yes	Yes	Yes	Yes	Yes
Automated backups to local storage (preview)	Yes	Yes	Yes	Yes	Yes	Yes
Point-in-time-restore (preview)	Yes	Yes	Yes	Yes	Yes	Yes
Automatic updates	Yes	Yes	Yes	Yes	Yes	Yes

Feature	Enterprise	Standard	Web	Express	Developer	Evaluation
Failover cluster instances	Yes	Yes	Not applicable	Not applicable	Yes	Not applicable
Always On availability groups (preview)	Yes	Yes	Not applicable	Not applicable	Yes	Not applicable
Monitoring (preview)	Yes	Yes	No	No	No	No
Operate with least privilege (preview)	Yes	Yes	Yes	Yes	Yes	Yes

¹ [Express LocalDB isn't supported.](#)

Supported configurations

SQL Server version

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

Operating systems

- 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 does not 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)

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

Unsupported configurations

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

- SQL Server running in containers.
- SQL Server roles other than the Database Engine, such as Analysis Services (SSAS), Reporting Services (SSRS), or Integration Services (SSIS).
- 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.

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](#)
- [Automatically connect your SQL Server to Azure Arc](#)

For VMware clusters, review [Support on VMware](#).

Supported Azure regions

Arc-enabled SQL Server 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
- 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

Important

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

Related content

- [Learn about the prerequisites to connect your SQL Server to Azure Arc](#)
- [Automatically connect your SQL Server to Azure Arc](#)
- [Learn more about Microsoft Defender for Cloud](#)
- [Learn more about Microsoft Purview](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#)  | [Get help at Microsoft Q&A](#)

What is Azure Arc site manager (preview)?

Article • 09/19/2024

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

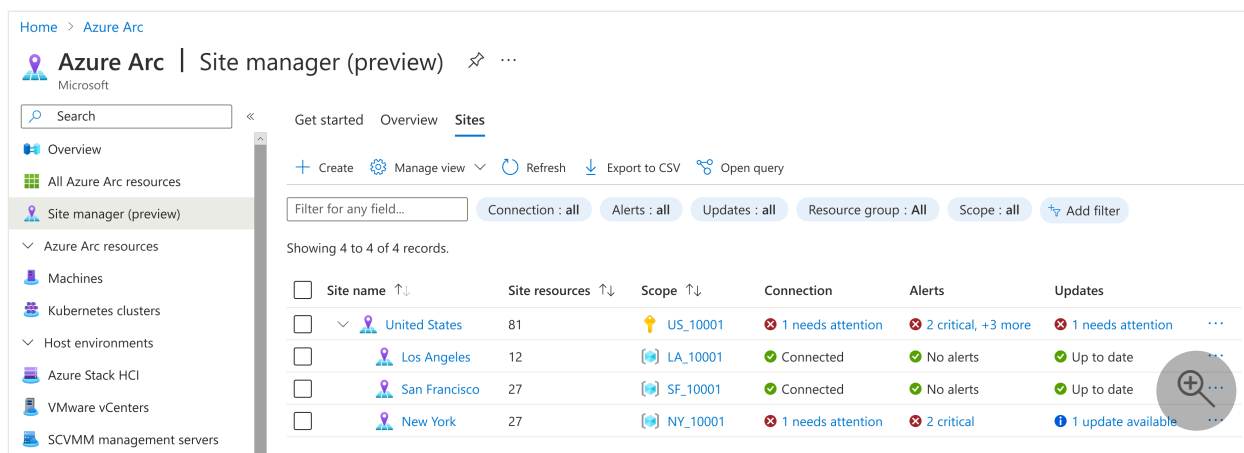
Azure Arc site manager is currently in PREVIEW. See the [Supplemental Terms of Use for Microsoft Azure Previews](#) for legal terms that apply to Azure features that are in beta, preview, or otherwise not yet released into general availability.

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 Stack HCI	✓	✓	✓ (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.

Next steps

[Quickstart: Create a site in Azure Arc site manager \(preview\)](#)

Feedback

Was this page helpful?

[Provide product feedback](#) | [Get help at Microsoft Q&A](#)

What is Multicloud connector enabled by Azure Arc (preview)?

Article • 10/18/2024

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, AWS public cloud environments are supported.


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 and AWS resources with a certain tag, you can do so. The **Inventory** solution will scan 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 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 and AWS resources together.

For more information about how the multicloud connector works, including Azure and AWS prerequisites, see [Add a public cloud with the multicloud connector in the Azure portal](#).

The multicloud connector can work side-by-side with the [AWS connector in Defender for Cloud](#). If you choose, you can use both of these connectors.

Important

Multicloud connector enabled by Azure Arc 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.

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, 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).

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

Scanned AWS 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 cloud, the multicloud connector queries the AWS resource APIs several times a day. These read-only API calls incur no charges in AWS, but they *are* registered in CloudTrail if you've enabled a trail for read events.

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](#).

Feedback

Was this page helpful?

[Provide product feedback](#) | [Get help at Microsoft Q&A](#)

Overview of Azure Arc-enabled service validation

Article • 09/19/2024

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, SQL engine versions, and PostgreSQL server 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](#)
-

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#)  | [Get help at Microsoft Q&A](#)

Azure Arc-enabled Kubernetes validation

Article • 09/19/2024

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 haven't been validated through conformance tests and are not listed on this page.

Validated distributions

The following Microsoft-provided Kubernetes distributions and infrastructure providers have successfully passed the conformance tests for Azure Arc-enabled Kubernetes:

 Expand table

Distribution and infrastructure provider	Version
Cluster API Provider on Azure	Release version: 0.4.12 ; Kubernetes version: 1.18.2
AKS on Azure Stack HCI	Release version: December 2020 Update ; Kubernetes version: 1.18.8
K8s on Azure Stack Edge	Release version: Azure Stack Edge 2207 (2.2.2037.5375); Kubernetes version: 1.22.6
AKS Edge Essentials	Release version 1.0.406.0 ; Kubernetes version 1.24.3

The following providers and their corresponding Kubernetes distributions have successfully passed the conformance tests for Azure Arc-enabled Kubernetes:

 Expand table

Provider name	Distribution name	Version
RedHat	OpenShift Container Platform	4.10.23 , 4.11.0-rc.6 , 4.13.4 , 4.15.0
VMware	Tanzu Kubernetes Grid	TKGs 2.2; upstream K8s 1.25.7+vmware.3 TKGm 2.3; upstream K8s v1.26.5+vmware.2 TKGm 2.2; upstream K8s v1.25.7+vmware.2 TKGm 2.1.0; upstream K8s v1.24.9+vmware.1
Canonical	Charmed Kubernetes	1.24 , 1.28
SUSE Rancher	Rancher Kubernetes Engine	RKE CLI version: v1.3.13 ; Kubernetes versions: 1.24.2, 1.23.8
SUSE Rancher	K3s	v1.27.4+k3s1 , v1.26.7+k3s1 , v1.25.12+k3s1
Nutanix	Nutanix Kubernetes Engine	Version 2.5 ; upstream K8s v1.23.11
Kublr	Kublr Managed K8s Distribution	Kublr 1.26.0 ; Upstream K8s Versions: 1.21.3, 1.22.10, 1.22.17, 1.23.17, 1.24.13, 1.25.6, 1.26.4
Mirantis	Mirantis Kubernetes Engine	MKE Version 3.6.0 MKE Version 3.5.5 MKE Version 3.4.7
Wind River	Wind River Cloud Platform	Wind River Cloud Platform 24.09; Upstream K8s version: 1.28.4 Wind River Cloud Platform 22.12; Upstream K8s version: 1.24.4 Wind River Cloud Platform 22.06; Upstream K8s version: 1.23.1

The Azure Arc team also ran the conformance tests and validated Azure Arc-enabled Kubernetes scenarios on the following public cloud providers:

[Expand table](#)

Public cloud provider name	Distribution name	Version
Amazon Web Services	Elastic Kubernetes Service (EKS)	v1.18.9
Google Cloud Platform	Google Kubernetes Engine (GKE)	v1.17.15

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.

Feedback

Was this page helpful?

[Provide product feedback](#) | [Get help at Microsoft Q&A](#)

Azure Arc-enabled data services

Kubernetes validation

Article • 09/19/2024

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, SQL engine versions, and PostgreSQL server 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.

Azure Arc-enabled PostgreSQL server is available for preview in select regions.

Partners

DataON

[Expand table](#)

Solution and version	Kubernetes version	Azure Arc-enabled data services version	SQL engine version	PostgreSQL server version
DataON AZS-6224	1.24.11	1.20.0_2023-06-13	16.0.5100.7242	14.5 (Ubuntu 20.04)

Dell

[Expand table](#)

Solution and version	Kubernetes version	Azure Arc-enabled data services version	SQL engine version	PostgreSQL server version
PowerStore 4.0	1.28.10	1.30.0_2024-06-11	16.0.5349.20214	Not validated
Unity XT	1.24.3	1.15.0_2023-01-10	16.0.816.19223	Not validated
PowerFlex	1.25.0	1.21.0_2023-07-11	16.0.5100.7242	14.5 (Ubuntu 20.04)

Hitachi

Expand table

Solution and version	Kubernetes version	Azure Arc-enabled data services version	SQL engine version	PostgreSQL server version
Hitachi UCP with Microsoft AKS-HCI	1.27.3	1.29.0_2024-04-09*	16.0.5290.8214	14.5 (Ubuntu 20.04)
Hitachi UCP with Red Hat OpenShift	1.25.11	1.25.0_2023-11-14	16.0.5100.7246	Not validated
Hitachi Virtual Storage Software Block software-defined storage (VSSB)	1.24.12	1.20.0_2023-06-13	16.0.5100.7242	14.5 (Ubuntu 20.04)
Hitachi Virtual Storage Platform (VSP)	1.24.12	1.19.0_2023-05-09	16.0.937.6221	14.5 (Ubuntu 20.04)

*: 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	PostgreSQL server version
HPE Superdome Flex 280	1.25.12	1.22.0_2023-08-08	16.0.5100.7242	Not validated
HPE Apollo 4200 Gen10 Plus	1.22.6	1.11.0_2022-09-13	16.0.312.4243	12.3 (Ubuntu 12.3-1)

Kublr

[Expand table](#)

Solution and version	Kubernetes version	Azure Arc-enabled data services version	SQL engine version	PostgreSQL server 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	14.5 (Ubuntu 20.04)
Kublr 1.21.2	1.22.10	1.9.0_2022-07-12	16.0.312.4243	12.3 (Ubuntu 12.3-1)

Lenovo

[Expand table](#)

Solution and version	Kubernetes version	Azure Arc-enabled data services version	SQL engine version	PostgreSQL server version
Lenovo ThinkEdge SE455 V3	1.26.6	1.24.0_2023-10-10	16.0.5100.7246	Not validated
Lenovo ThinkAgile MX1020	1.26.6	1.24.0_2023-10-10	16.0.5100.7246	Not validated
Lenovo ThinkAgile MX3520	1.22.6	1.10.0_2022-08-09	16.0.312.4243	12.3 (Ubuntu 12.3-1)

Nutanix


[Expand table](#)

Solution and version	Kubernetes version	Azure Arc-enabled data services version	SQL engine version	PostgreSQL server version
Karbon 2.2 AOS: 5.19.1.5 AHV: 20201105.1021	1.19.8-0	1.0.0_2021-07-30	15.0.2148.140	12.3 (Ubuntu 12.3-1)

Solution and version	Kubernetes version	Azure Arc-enabled data services version	SQL engine version	PostgreSQL server version
PC: Version pc.2021.3.02				



PureStorage

 Expand table

Solution and version	Kubernetes version	Azure Arc-enabled data services version	SQL engine version	PostgreSQL server version
Portworx Enterprise 3.1 	1.28.7	1.30.0_2024-06-11	16.0.5349.20214	Not validated
Portworx Enterprise 2.7 1.22.5	1.20.7	1.1.0_2021-11-02	15.0.2148.140	Not validated
Portworx Enterprise 2.9	1.22.5	1.1.0_2021-11-02	15.0.2195.191	12.3 (Ubuntu 12.3-1)

Red Hat

 Expand table

Solution and version	Kubernetes version	Azure Arc-enabled data services version	SQL engine version	PostgreSQL server version
OpenShift 4.15.0 	1.28.6	1.27.0_2024-02-13	16.0.5100.7246	Not validated
OpenShift 4.13.4 	1.26.5	1.21.0_2023-07-11	16.0.5100.7242	14.5 (Ubuntu 20.04)
OpenShift 4.10.16	1.23.5	1.11.0_2022-09-13	16.0.312.4243	12.3 (Ubuntu 12.3-1)



VMware

 Expand table

Solution and version	Kubernetes version	Azure Arc-enabled data services version	SQL engine version	PostgreSQL server version
TKGs 2.2	1.25.7	1.23.0_2023-09-12	16.0.5100.7246	14.5 (Ubuntu 20.04)
TKGm 2.3	1.26.5	1.23.0_2023-09-12	16.0.5100.7246	14.5 (Ubuntu 20.04)
TKGm 2.2	1.25.7	1.19.0_2023-05-09	16.0.937.6223	14.5 (Ubuntu 20.04)
TKGm 2.1.0	1.24.9	1.15.0_2023-01-10	16.0.816.19223	14.5 (Ubuntu 20.04)

Wind River

 Expand table

Solution and version	Kubernetes version	Azure Arc-enabled data services version	SQL engine version	PostgreSQL server version
Wind River Cloud Platform 24.09 	1.28.4	1.33.0_2024-09-10	16.0.5409	Not validated
Wind River Cloud Platform 22.12 	1.24.4	1.26.0_2023-12-12	16.0.5100.7246	Not validated
Wind River Cloud Platform 22.06	1.23.1	1.9.0_2022-07-12	16.0.312.4243	12.3 (Ubuntu 12.3-1)

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

v1.22.5+vmware.1

- [Azure Data CLI \(azdata\)](#)
- [kubectl](#) 

- [Azure Data Studio - Insider build](#) 

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](#)
3. Deploy [Azure Arc-enabled PostgreSQL server](#)

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](#).

Feedback

Was this page helpful?

 Yes

 No

Azure Arc network requirements

Article • 09/19/2024

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.

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 Arc-enabled App services
- 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` to function. For `*.servicebus.windows.net`, websockets need to be enabled for outbound access on firewall and proxy.

 Expand table

Endpoint (DNS)	Description
<code>https://management.azure.com</code>	Required for the agent to connect to Azure and register the cluster.

Endpoint (DNS)	Description
<code>https://<region>.dp.kubernetesconfiguration.azure.com</code>	Data plane endpoint for the agent to push status and fetch configuration information.
<code>https://login.microsoftonline.com</code> <code>https://<region>.login.microsoft.com</code> <code>login.windows.net</code>	Required to fetch and update Azure Resource Manager tokens.
<code>https://mcr.microsoft.com</code> <code>https://*.data.mcr.microsoft.com</code>	Required to pull container images for Azure Arc agents.
<code>https://gbl.his.arc.azure.com</code>	Required to get the regional endpoint for pulling system-assigned Managed Identity certificates.
<code>https://*.his.arc.azure.com</code>	Required to pull system-assigned Managed Identity certificates.
<code>https://k8connecthelm.azureedge.net</code>	<code>az connectedk8s connect</code> uses Helm 3 to deploy Azure Arc agents on the Kubernetes cluster. This endpoint is needed for Helm client download to facilitate deployment of the agent helm chart.
<code>guestnotificationsservice.azure.com</code> <code>*.guestnotificationsservice.azure.com</code> <code>sts.windows.net</code> <code>https://k8sconnectcsp.azureedge.net</code>	For Cluster Connect and for Custom Location based scenarios.
<code>*.servicebus.windows.net</code>	For Cluster Connect and for Custom Location based scenarios.
<code>https://graph.microsoft.com/</code>	Required when Azure RBAC is configured.
<code>*.arc.azure.net</code>	Required to manage connected clusters in Azure portal.
<code>https://<region>.obo.arc.azure.com:8084/</code>	Required when Cluster Connect is configured.
<code>https://linuxgeneva-microsoft.azurecr.io</code>	Required if using Azure Arc-enabled Kubernetes extensions .

To translate the `*.servicebus.windows.net` wildcard into specific endpoints, use the command:

```
rest
```

```
GET https://guestnotificationsservice.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
```

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

```
Azure PowerShell
```

```
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	<code>arcdataservicesrow1.azurecr.io</code>	Outbound	Provisions the Azure Arc data controller bootstrapper and cluster level objects, such as custom resource definitions, cluster roles, and cluster role bindings, is

Service	Port	URL	Direction	Notes
				pulled from an Azure Container Registry.
Azure monitor APIs ¹	443	*.ods.opinsights.azure.com *.oms.opinsights.azure.com *.monitoring.azure.com	Outbound	Azure Data Studio and Azure CLI connect to the Azure Resource Manager APIs to send and retrieve data to and from 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 from Azure Data Studio to the Kubernetes API server uses the Kubernetes authentication and encryption that you have established. Each user that is using Azure Data Studio or 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 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 does not support using a [Log Analytics gateway](#) as a proxy for the Connected Machine agent. At the same time, Azure Monitor Agent supports Log Analytics gateway.

If outbound connectivity is restricted by your firewall or proxy server, make sure the URLs and Service Tags listed below are not blocked.

Service tags

Be sure to allow access to the following Service Tags:

- AzureActiveDirectory
- AzureTrafficManager
- AzureResourceManager
- AzureArcInfrastructure
- Storage
- WindowsAdminCenter (if [using Windows Admin Center to manage 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 containing each

Azure Service and the IP ranges it uses. This 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, then the **AzureCloud** Service Tag should be used to allow access to all Azure services. Do not 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, do not include the IP ranges used by global components of the service. The specific IP address resolved for these endpoints may change over time within the documented ranges, so just using a lookup tool to identify the current IP address for a given endpoint and allowing access to that will not be sufficient to ensure reliable access.

For more information, see [Virtual network service tags](#).

URLs

The table below lists the URLs that must be available in order to install and use the Connected Machine agent.

Azure Cloud

ⓘ Note

When configuring the Azure 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 which endpoints can be configured 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 endpoint if a private link scope is assigned.

 Expand table

Agent resource	Description	When required	Private link capable
<code>aka.ms</code>	Used to resolve the download script during installation	At installation time, only	Public
<code>download.microsoft.com</code>	Used to download the Windows installation package	At installation time, only	Public
<code>packages.microsoft.com</code>	Used to download the Linux installation package	At installation time, only	Public
<code>login.windows.net</code>	Microsoft Entra ID	Always	Public
<code>login.microsoftonline.com</code>	Microsoft Entra ID	Always	Public
<code>pas.windows.net</code>	Microsoft Entra ID	Always	Public
<code>management.azure.com</code>	Azure Resource Manager - to create or delete the Arc server resource	When connecting or disconnecting a server, only	Public, unless a resource management private link is also configured
<code>*.his.arc.azure.com</code>	Metadata and hybrid identity services	Always	Private
<code>*.guestconfiguration.azure.com</code>	Extension management and guest configuration services	Always	Private
<code>guestnotificationsservice.azure.com</code> , <code>*.guestnotificationsservice.azure.com</code>	Notification service for extension and	Always	Public

Agent resource	Description	When required	Private link capable
	connectivity scenarios		
<code>azgn*.servicebus.windows.net</code>	Notification service for extension and connectivity scenarios	Always	Public
<code>*.servicebus.windows.net</code>	For Windows Admin Center and SSH scenarios	If using SSH or Windows Admin Center from Azure	Public
<code>*.waconazure.com</code>	For Windows Admin Center connectivity	If using Windows Admin Center	Public
<code>*.blob.core.windows.net</code>	Download source for Azure Arc-enabled servers extensions	Always, except when using private endpoints	Not used when private link is configured
<code>dc.services.visualstudio.com</code>	Agent telemetry	Optional, not used in agent versions 1.24+	Public
<code>*.<region>.arcdataservices.com</code> ¹	For Arc SQL Server. Sends data processing service, service telemetry, and performance monitoring to Azure. Allows TLS 1.3.	Always	Public
<code>www.microsoft.com/pkiops/certs</code>	Intermediate certificate updates for ESUs (note: uses HTTP/TCP 80 and HTTPS/TCP 443)	If using ESUs enabled by Azure Arc. Required always for automatic updates, or temporarily if	Public

Agent resource	Description	When required	Private link capable
		downloading certificates manually.	

¹ 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 with [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://guestnotificationsservice.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 may 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


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

Azure PowerShell

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

Transport Layer Security 1.2 protocol

To ensure the security of data in transit to Azure, we strongly encourage you to configure machine to use Transport Layer Security (TLS) 1.2. Older versions of TLS/Secure Sockets Layer (SSL) have been found to be vulnerable and while they still currently work to allow backwards compatibility, they are **not recommended**.

 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 your version of OpenSSL is supported.
Windows Server 2012 R2 and higher	Supported, and enabled by default.	To confirm that you are still using the default settings .


Subset of endpoints for ESU only

If you're using 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

 Expand table

Agent resource	Description	When required	Endpoint used with private link
<code>aka.ms</code>	Used to resolve the download script during installation	At installation time, only	Public
<code>download.microsoft.com</code>	Used to download the Windows installation package	At installation time, only	Public

Agent resource	Description	When required	Endpoint used with private link
<code>login.windows.net</code>	Microsoft Entra ID	Always	Public
<code>login.microsoftonline.com</code>	Microsoft Entra ID	Always	Public
<code>management.azure.com</code>	Azure Resource Manager - to create or delete the Arc server resource	When connecting or disconnecting a server, only	Public, unless a resource management private link is also configured
<code>*.his.arc.azure.com</code>	Metadata and hybrid identity services	Always	Private
<code>*.guestconfiguration.azure.com</code>	Extension management and guest configuration services	Always	Private
<code>www.microsoft.com/pkiops/certs</code>	Intermediate certificate updates for ESUs (note: uses HTTP/TCP 80 and HTTPS/TCP 443)	Always for automatic updates, or temporarily if downloading certificates manually.	Public
<code>*.<region>.arcdataservices.com</code>	Azure Arc data processing service and service telemetry.	SQL Server ESUs	Public
<code>*.blob.core.windows.net</code>	Download Sql Server Extension package	SQL Server ESUs	Not required if using Private Link

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, Appliance VM, and Control Plane IP to the required Arc resource bridge URLs.

Firewall/Proxy URL allowlist

 Expand table

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

Service	Port	URL	Direction	Notes
			outbound connection on UDP	
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	443	*.blob.core.windows.net, ecpacr.azurecr.io	Appliance VM IPs need outbound connection.	Required to pull container images.

Service	Port	URL	Direction	Notes
image download				
Managed Identity	443	<code>*.his.arc.azure.com</code>	Appliance VM IPs need outbound connection.	Required to pull system-assigned Managed Identity certificates.
Azure Arc for Kubernetes container image download	443	<code>azurearcfork8s.azurecr.io</code>	Appliance VM IPs need outbound connection.	Pull container images.
Azure Arc agent	443	<code>k8connecthelm.azureedge.net</code>	Appliance VM IPs need outbound connection.	deploy Azure Arc agent.
ADHS telemetry service	443	<code>adhs.events.data.microsoft.com</code>	Appliance VM IPs need outbound connection.	Periodically sends Microsoft required diagnostic data from appliance VM.
Microsoft events data service	443	<code>v20.events.data.microsoft.com</code>	Appliance VM IPs need outbound connection.	Send diagnostic data from Windows.
Log collection for Arc Resource Bridge	443	<code>linuxgeneva-microsoft.azurecr.io</code>	Appliance VM IPs need outbound connection.	Push logs for Appliance managed components.
Resource bridge components download	443	<code>kvamanagementoperator.azurecr.io</code>	Appliance VM IPs need outbound connection.	Pull artifacts for Appliance managed components.
Microsoft open source	443	<code>packages.microsoft.com</code>	Appliance VM IPs need	Download Linux

Service	Port	URL	Direction	Notes
packages manager			outbound connection.	installation package.
Custom Location	443	sts.windows.net	Appliance VM IPs need outbound connection.	Required for Custom Location.
Azure Arc	443	guestnotificationsservice.azure.com	Appliance VM IPs need outbound connection.	Required for Azure Arc.
Custom Location	443	k8sconnectcsp.azureedge.net	Appliance VM IPs need outbound connection.	Required for Custom Location.
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	Manage cluster from Azure portal.

Service	Port	URL	Direction	Notes
			outbound connection.	
Azure CLI & Extension	443	<code>*.blob.core.windows.net</code>	Management machine needs outbound connection.	Download Azure CLI Installer and extension.
Azure Arc Agent	443	<code>*.dp.kubernetesconfiguration.azure.com</code>	Management machine needs outbound connection.	Dataplane used for Arc agent.
Python package	443	<code>pypi.org</code> , <code>*.pypi.org</code>	Management machine needs outbound connection.	Validate Kubernetes and Python versions.
Azure CLI	443	<code>pythonhosted.org</code> , <code>*.pythonhosted.org</code>	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.

[Expand table](#)

Service	Port	IP/machine	Direction	Notes
SSH	22	<code>appliance VM IPs</code> and <code>Management machine</code>	Bidirectional	Used for deploying and maintaining the appliance VM.
Kubernetes API server	6443	<code>appliance VM IPs</code> and <code>Management machine</code>	Bidirectional	Management of the appliance VM.

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 control plane (ex: VMware vCenter address).

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.
Azure CLI and Azure CLI Extensions	443	*.blob.core.windows.net	Management machine needs outbound connection.	Download Azure CLI Installer and Azure CLI extensions.

Service	Port	URL	Direction	Notes
Azure Resource Manager	443	<code>management.azure.com</code>	Management machine needs outbound connection.	Required to create/update resources in Azure using ARM.
Helm Chart for Azure Arc Agents	443	<code>*.dp.kubernetesconfiguration.azure.com</code>	Management machine needs outbound connection.	Data plane endpoint for downloading the configuration information of Arc agents.
Azure CLI	443	- <code>login.microsoftonline.com</code> - <code>aka.ms</code>	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](#)
-

Feedback

Was this page helpful?



[Provide product feedback](#)  | [Get help at Microsoft Q&A](#)

az arcappliance

Reference

ⓘ Note

This reference is part of the **arcappliance** extension for the Azure CLI (version 2.51.0 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 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

Name	Description	Type	Status
az arcpliance delete	Command group for deletion of an Arc resource bridge on-premises appliance VM and its Azure resource.	Extension	GA
az arcpliance delete hci	Command to delete the on-premises appliance VM on Azure Stack HCI and Arc resource bridge Azure resource.	Extension	GA
az arcpliance delete scvmm	Command to delete the on-premises appliance VM on SCVMM and Azure resource.	Extension	GA
az arcpliance delete vmware	Command to delete the on-premises appliance VM and Azure resource for Arc resource bridge (Arc-enabled VMware).	Extension	GA
az arcpliance deploy	Command group for deployment of the Arc resource bridge on-premises appliance VM and creation of its corresponding Azure resource.	Extension	GA
az arcpliance 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
az arcpliance 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 arcpliance deploy vmware	Command to deploy the Arc resource bridge's on-premises appliance VM on VMWare and its corresponding Azure resource.	Extension	GA
az arcpliance get-credentials	Command to get the on-premises infrastructure credentials used by Arc resource bridge to manage on-premises resources.	Extension	GA
az arcpliance get-upgrades	Command to fetch the available upgrades for an Appliance.	Extension	GA
az arcpliance list	Command to list Arc resource bridge resources.	Extension	GA
az arcpliance logs	Command group for collecting logs for Arc resource bridge. Run get-credentials command before running logs command.	Extension	GA
az arcpliance logs hci	Command to collect logs for an Appliance on Azure Stack HCI.	Extension	GA
az arcpliance logs scvmm	Command to collect logs for Arc resource bridge on SCVMM (Arc-enabled SCVMM).	Extension	GA

Name	Description	Type	Status
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
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

Name	Description	Type	Status
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-infracredentials hci	Command to update the on-premises infrastructure credentials for Azure Stack HCI used by Arc resource bridge.	Extension	GA
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

Name	Description	Type	Status
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 [--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

--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.

Accepted values: false, true

Default value: False

--partner

Returns the credentials used by private cloud RP/service to access Arc Resource Bridge. Default: customer user credentials.

Accepted values: false, true

Default value: False

--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.

Accepted values: false, true

Default value: False

▼ Global Parameters

--debug

Increase logging verbosity to show all debug logs.

--help -h

Show this help message and exit.

--only-show-errors

Only show errors, suppressing warnings.

--output -o

Output format.

Accepted values: json, jsonc, none, table, tsv, yaml, yamlc

Default value: json

--query

JMESPath query string. See <http://jmespath.org/> for more information and examples.

--subscription

Name or ID of subscription. You can configure the default subscription using `az`

```
account set -s NAME_OR_ID.
```

--verbose

Increase logging verbosity. Use `--debug` for full debug logs.

az arcappliance get-upgrades

Command to fetch the available upgrades for an Appliance.

Azure CLI

```
az arcappliance get-upgrades --name  
                             --resource-group
```

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>`.

▼ Global Parameters

--debug

Increase logging verbosity to show all debug logs.

--help -h

Show this help message and exit.

--only-show-errors

Only show errors, suppressing warnings.

--output -o

Output format.

Accepted values: json, jsonc, none, table, tsv, yaml, yamlc

Default value: json

--query

JMESPath query string. See <http://jmespath.org/> for more information and examples.

--subscription

Name or ID of subscription. You can configure the default subscription using `az account set -s NAME_OR_ID`.

`--verbose`

Increase logging verbosity. Use `--debug` for full debug logs.

az 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

`--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.

`--help -h`

Show this help message and exit.

--only-show-errors

Only show errors, suppressing warnings.

--output -o

Output format.

Accepted values: json, jsonc, none, table, tsv, yaml, yamlc

Default value: json

--query

JMESPath query string. See <http://jmespath.org/> for more information and examples.

--subscription

Name or ID of subscription. You can configure the default subscription using `az`

```
account set -s NAME_OR_ID.
```

--verbose

Increase logging verbosity. Use `--debug` for full debug logs.

az arcappliance notice

Command to display the EULA & Notice File link for Arc resource bridge.

```
Azure CLI
```

```
az arcappliance notice
```

Examples

Displays the EULA & Notice File link for Arc resource bridge.

```
Azure CLI
```

```
az arcappliance notice
```

▼ Global Parameters

--debug

Increase logging verbosity to show all debug logs.

--help -h

Show this help message and exit.

--only-show-errors

Only show errors, suppressing warnings.

--output -o

Output format.

Accepted values: json, jsonc, none, table, tsv, yaml, yamlc

Default value: json

--query

JMESPath query string. See <http://jmespath.org/> for more information and examples.

--subscription

Name or ID of subscription. You can configure the default subscription using `az`

```
account set -s NAME_OR_ID.
```

--verbose

Increase logging verbosity. Use `--debug` for full debug logs.

az 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.

--help -h

Show this help message and exit.

--only-show-errors

Only show errors, suppressing warnings.

--output -o

Output format.

Accepted values: json, jsonc, none, table, tsv, yaml, yamlc

Default value: json

--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.