Contents

What is Azure Arc-enabled servers?

9/7/2021 • 4 minutes to read • Edit Online

Azure Arc-enabled servers enables you to manage your Windows and Linux physical servers and virtual machines hosted *outside* of Azure, on your corporate network, or other cloud provider. This management experience is designed to be consistent with how you manage native Azure virtual machines. 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. Now you can benefit from standard Azure constructs, such as Azure Policy and applying tags. Service providers managing a customer's on-premises infrastructure can manage their hybrid machines, just like they do today with native Azure resources, across multiple customer environments using Azure Lighthouse.

To deliver this experience with your hybrid machines, you need to install the Azure Connected Machine agent on each machine. This agent does not deliver any other functionality, and it doesn't replace the Azure Log Analytics agent. The Log Analytics agent for Windows and Linux is required when:

- You want to proactively monitor the OS and workloads running on the machine,
- Manage it using Automation runbooks or solutions like Update Management, or
- Use other Azure services like Azure Security Center.

Supported cloud operations

When you connect your machine to Azure Arc-enabled servers, it enables the ability for you to perform the following operational functions as described in the following table.

OPERATIONS FUNCTION	DESCRIPTION
Govern	
Azure Policy	Assign Azure Policy guest configurations to audit settings inside the machine. To understand the cost of using Azure Policy Guest Configuration policies with Arc-enabled servers, see Azure Policy pricing guide
Protect	
Azure Security Center	Protect non-Azure servers with Microsoft Defender for Endpoint, included through Azure Defender, for threat detection, for vulnerability management, and to proactively monitor for potential security threats. Azure Security Center presents the alerts and remediation suggestions from the threats detected.
Azure Sentinel	Machines connected to Arc-enabled servers can be configured with Azure Sentinel to collect security-related events and correlate them with other data sources.
Configure	

OPERATIONS FUNCTION	DESCRIPTION
Azure Automation	Assess configuration changes about 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.
Azure Automanage	Onboard a set of Azure services when you use Automanage Machine for Arc-enabled servers.
VM extensions	Provides post-deployment configuration and automation tasks using supported Arc-enabled servers VM extensions for your non-Azure Windows or Linux machine.
Monitor	
Azure Monitor	Monitor the connected machine guest operating system performance, and discover application components to monitor their processes and dependencies with other resources using VM insights. Collect other log data, such as performance data and events, from the operating system or workload(s) running on the machine with the Log Analytics 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 for your server.

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

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.

To learn more about how Azure Arc-enabled servers can be used to implement Azure monitoring, security, and update services across hybrid and multicloud environments, see the following video.

Supported regions

For a definitive 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 is affected by an outage, the connected machine is not affected, but management operations using Azure may be unable to complete. If there is a regional outage, and if you have multiple locations that support a geographically redundant service, it is best to connect the machines in each location to a different Azure region.

The following metadata information about the connected machine is collected and stored in the region where the Azure Arc machine resource is configured:

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

For example, if the machine is registered with Azure Arc in the East US region, this data 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 of which hybrid cloud environments hosting VMs are supported, 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 Connected Machine agent sends a regular heartbeat message to the service every 5 minutes. If the service stops receiving these heartbeat messages from a machine, that machine is considered offline and the status will automatically be changed to **Disconnected** in the portal within 15 to 30 minutes. Upon receiving a subsequent heartbeat message from the Connected Machine agent, its status will automatically be changed to **Connected**.

Next steps

- Before evaluating or enabling Azure Arc-enabled servers across multiple hybrid machines, review Connected Machine agent overview to understand requirements, technical details about the agent, and deployment methods.

- Review the Planning and deployment guide to plan for deploying Azure Arc-enabled servers at any scale and implement centralized management and monitoring.

What's new with Azure Arc-enabled servers agent

9/7/2021 • 2 minutes to read • Edit Online

The Azure Arc-enabled servers Connected Machine agent receives improvements on an ongoing basis. To stay up to date with the most recent developments, this article provides you with information about:

- The latest releases
- Known issues
- Bug fixes

This page is updated monthly, so revisit it regularly. If you're looking for items older than six months, you can find them in archive for What's new with Azure Arc-enabled servers agent.

August 2021

Version 1.10

Fixed

- The guest configuration policy agent can now configure and remediate system settings. Existing policy assignments continue to be audit-only. Learn more about the Azure Policy guest configuration remediation options.
- The guest configuration policy agent now restarts every 48 hours instead of every 6 hours.

July 2021

Version 1.9

New features

Added support for the Indonesian language

Fixed

Fixed a bug that prevented extension management in the West US 3 region

Version 1.8

New features

- Improved reliability when installing the Azure Monitor Agent extension on Red Hat and CentOS systems
- Added agent-side enforcement of max resource name length (54 characters)
- Guest Configuration policy improvements:
  - Added support for PowerShell-based Guest Configuration policies on Linux operating systems
  - Added support for multiple assignments of the same Guest Configuration policy on the same server
  - Upgraded PowerShell Core to version 7.1 on Windows operating systems

Fixed

- The agent will continue running if it is unable to write service start/stop events to the Windows application event log

June 2021

Version 1.7

New features

- Improved reliability during onboarding:
  - Improved retry logic when HIMDS is unavailable
  - Onboarding will now continue instead of aborting if OS information cannot be obtained
- Improved reliability when installing the OMS agent extension on Red Hat and CentOS systems

May 2021

Version 1.6

New features

- Added support for SUSE Enterprise Linux 12
- Updated Guest Configuration agent to version 1.26.12.0 to include:
  - Policies are executed in a separate process.
  - Added V2 signature support for extension validation.
  - Minor update to data logging.

April 2021

Version 1.5

New features

- Added support for Red Hat Enterprise Linux 8 and CentOS Linux 8.
- New `-useStderr` parameter to direct error and verbose output to stderr.
- New `-json` parameter to direct output results in JSON format (when used with -useStderr).
- Collect other instance metadata - Manufacturer, model, and cluster resource ID (for Azure Stack HCI nodes).

Next steps

- Before evaluating or enabling Azure Arc-enabled servers across multiple hybrid machines, review Connected Machine agent overview to understand requirements, technical details about the agent, and deployment methods.
- Review the Planning and deployment guide to plan for deploying Azure Arc-enabled servers at any scale and implement centralized management and monitoring.

Archive for What's new with Azure Arc-enabled servers agent

9/1/2021 • 2 minutes to read • Edit Online

The primary What's new in Azure Arc-enabled servers agent? article contains updates for the last six months, while this article contains all the older information.

The Azure Arc-enabled servers Connected Machine agent receives improvements on an ongoing basis. This article provides you with information about:

- Previous releases
- Known issues
- Bug fixes

March 2021

Version 1.4

New features

- Added support for private endpoints, which is currently in limited preview.
- Expanded list of exit codes for azcmagent.
- Agent configuration parameters can now be read from a file with the `--config` parameter.
- Collect new instance metadata to determine if Microsoft SQL Server is installed on the server

Fixed

Network endpoint checks are now faster.

December 2020

Version: 1.3

New features

Added support for Windows Server 2008 R2 SP1.

Fixed

Resolved issue preventing the Custom Script Extension on Linux from installing successfully.

November 2020

Version: 1.2

Fixed

Resolved issue where proxy configuration could be lost after upgrade on RPM-based distributions.

October 2020

Version: 1.1

Fixed

- Fixed proxy script to handle alternate GC daemon unit file location.

- GuestConfig agent reliability changes.
- GuestConfig agent support for US Gov Virginia region.
- GuestConfig agent extension report messages to be more verbose if there is a failure.

September 2020

Version: 1.0 (General Availability)

Plan for change

- Support for preview agents (all versions older than 1.0) will be removed in a future service update.
- Removed support for fallback endpoint `.azure-automation.net`. If you have a proxy, you need to allow the endpoint `*.his.arc.azure.com`.
- If the Connected Machine agent is installed on a virtual machine hosted in Azure, VM extensions can't be installed or modified from the Arc-enabled servers resource. This is to avoid conflicting extension operations being performed from the virtual machine's **Microsoft.Compute** and **Microsoft.HybridCompute** resource. Use the **Microsoft.Compute** resource for the machine for all extension operations.
- Name of guest configuration process has changed, from *gcd* to *gcad* on Linux, and *gcservice* to *gcarcservice* on Windows.

New features

- Added `azcmagent logs` option to collect information for support.
- Added `azcmagent license` option to display EULA.
- Added `azcmagent show --json` option to output agent state in easily parseable format.
- Added flag in `azcmagent show` output to indicate if server is on a virtual machine hosted in Azure.
- Added `azcmagent disconnect --force-local-only` option to allow reset of local agent state when Azure service cannot be reached.
- Added `azcmagent connect --cloud` option to support other clouds. In this release, only Azure is supported by service at time of agent release.
- Agent has been localized into Azure-supported languages.

Fixed

- Improvements to connectivity check.
- Corrected issue with proxy server settings being lost when upgrading agent on Linux.
- Resolved issues when attempting to install agent on server running Windows Server 2012 R2.
- Improvements to extension installation reliability

August 2020

Version: 0.11

- This release previously announced support for Ubuntu 20.04. Because some Azure VM extensions don't support Ubuntu 20.04, support for this version of Ubuntu is being removed.

- Reliability improvements for extension deployments.

Known issues

If you are using an older version of the Linux agent and it's configured to use a proxy server, you need to reconfigure the proxy server setting after the upgrade. To do this, run `sudo azcmagent_proxy add http://proxyserver.local:83`.

Next steps

- Before evaluating or enabling Arc-enabled servers across multiple hybrid machines, review Connected Machine agent overview to understand requirements, technical details about the agent, and deployment methods.

- Review the Planning and deployment guide to plan for deploying Azure Arc-enabled servers at any scale and implement centralized management and monitoring.

Quickstart: Connect hybrid machines with Azure Arc-enabled servers

9/7/2021 • 4 minutes to read • Edit Online

Azure Arc-enabled servers enables you to manage and govern your Windows and Linux machines hosted across on-premises, edge, and multicloud environments. In this quickstart, you'll deploy and configure the Connected Machine agent on your Windows or Linux machine hosted outside of Azure for management by Azure Arc-enabled servers.

Prerequisites

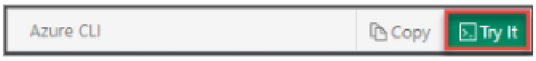
- If you don't have an Azure subscription, create a free account before you begin.
- Deploying the Azure Arc-enabled servers Hybrid Connected Machine agent requires that you have administrator permissions on the machine to install and configure the agent. On Linux, by using the root account, and on Windows, with an account that is a member of the Local Administrators group.
- Before you get started, be sure to review the agent prerequisites and verify the following:
  - Your target machine is running a supported operating system.
  - Your account is granted assignment to the required Azure roles.
  - If the machine connects through a firewall or proxy server to communicate over the Internet, make sure the URLs listed are not blocked.
  - Azure Arc-enabled servers supports only the regions specified here.

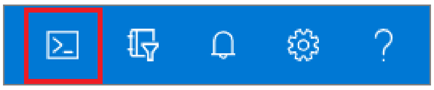
> **WARNING**
>
> The Linux hostname or Windows computer name cannot use one of the reserved words or trademarks in the name, otherwise attempting to register the connected machine with Azure will fail. See Resolve reserved resource name errors for a list of the reserved words.

Use Azure Cloud Shell

Azure hosts Azure Cloud Shell, an interactive shell environment that you can use through your browser. You can use either Bash or PowerShell with Cloud Shell to work with Azure services. You can use the Cloud Shell preinstalled commands to run the code in this article without having to install anything on your local environment.

To start Azure Cloud Shell:

OPTION	EXAMPLE/LINK
Select **Try It** in the upper-right corner of a code block. Selecting **Try It** doesn't automatically copy the code to Cloud Shell.	
Go to https://shell.azure.com, or select the **Launch Cloud Shell** button to open Cloud Shell in your browser.	

OPTION	EXAMPLE/LINK
Select the **Cloud Shell** button on the menu bar at the upper right in the Azure portal.	

To run the code in this article in Azure Cloud Shell:

1. Start Cloud Shell.
2. Select the **Copy** button on a code block to copy the code.
3. Paste the code into the Cloud Shell session by selecting **Ctrl**+**Shift**+**V** on Windows and Linux or by selecting **Cmd**+**Shift**+**V** on macOS.
4. Select **Enter** to run the code.

Register Azure resource providers

Azure Arc-enabled servers depends on the following Azure resource providers in your subscription in order to use this service:

- Microsoft.HybridCompute
- Microsoft.GuestConfiguration

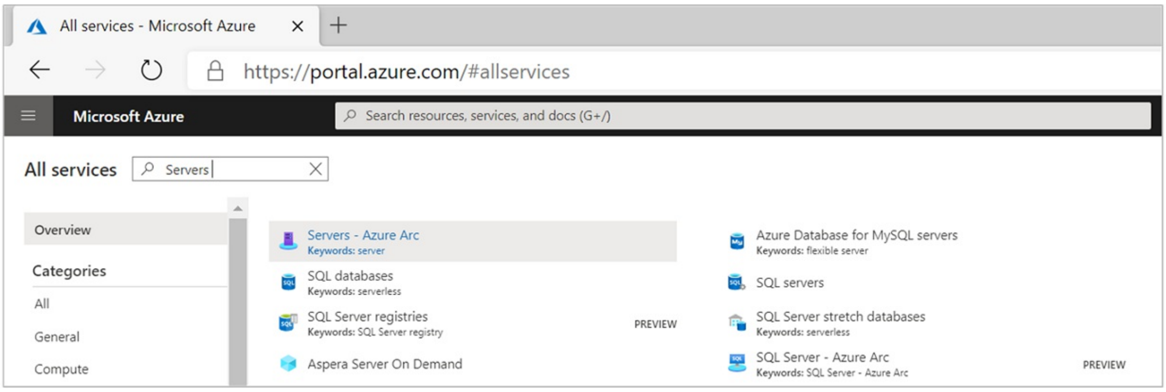
Register them using the following commands:

```
az account set --subscription "{Your Subscription Name}"
az provider register --namespace 'Microsoft.HybridCompute'
az provider register --namespace 'Microsoft.GuestConfiguration'
```

Generate installation script

The script to automate the download, installation, and establish the connection with Azure Arc, is available from the Azure portal. To complete the process, do the following:

1. Launch the Azure Arc service in the Azure portal by clicking **All services**, then searching for and selecting **Servers - Azure Arc**.


All services - Microsoft Azure
https://portal.azure.com/#allservices
Microsoft Azure
Search resources, services, and docs (G+/)
All services
Servers
Overview
Categories
All
General
Compute
Servers - Azure Arc
Keywords: server
SQL databases
Keywords: serverless
SQL Server registries
Keywords: SQL Server registry
PREVIEW
Aspera Server On Demand
Azure Database for MySQL servers
Keywords: flexible server
SQL servers
SQL Server stretch databases
Keywords: serverless
SQL Server - Azure Arc
Keywords: SQL Server - Azure Arc
PREVIEW

2. On the **Servers - Azure Arc** page, select **Add** at the upper left.
3. On the **Select a method** page, select the **Add servers using interactive script** tile, and then select **Generate script**.
4. On the **Generate script** page, select the subscription and resource group where you want the machine to be managed within Azure. Select an Azure location where the machine metadata will be stored. This

location can be the same or different, as the resource group's location.

5. On the **Prerequisites** page, review the information and then select **Next: Resource details**.

6. On the **Resource details** page, provide the following:

   a. In the **Resource group** drop-down list, select the resource group the machine will be managed from.
   b. In the **Region** drop-down list, select the Azure region to store the servers metadata.
   c. In the **Operating system** drop-down list, select the operating system that the script be configured to run on.
   d. If the machine is communicating through a proxy server to connect to the internet, specify the proxy server IP address or the name and port number that the machine will use to communicate with the proxy server. Enter the value in the format `http://<proxyURL>:<proxyport>`.
   e. Select **Next: Tags**.

7. On the **Tags** page, review the default **Physical location tags** suggested and enter a value, or specify one or more **Custom tags** to support your standards.

8. Select **Next: Download and run script**.

9. On the **Download and run script** page, review the summary information, and then select **Download**. If you still need to make changes, select **Previous**.

Install the agent using the script

Windows agent

1. Log in to the server.

2. Open an elevated 64-bit PowerShell command prompt.

3. Change to the folder or share that you copied the script to, and execute it on the server by running the `./OnboardingScript.ps1` script.

Linux agent

1. To install the Linux agent on the target machine that can directly communicate to Azure, run the following command:

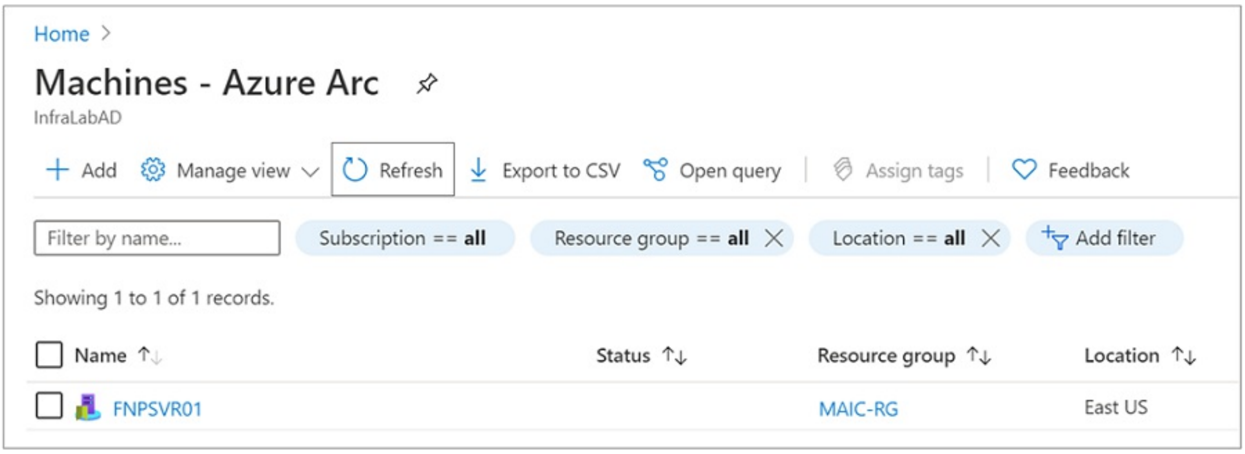
   ```
   bash ~/Install_linux_azcmagent.sh
   ```

   - If the target machine communicates through a proxy server, run the following command:

     ```
     bash ~/Install_linux_azcmagent.sh --proxy "{proxy-url}:{proxy-port}"
     ```

Verify the connection with Azure Arc

After you install the agent and configure it to connect to Azure Arc-enabled servers, go to the Azure portal to verify that the server has successfully connected. View your machine in the Azure portal.



Showing 1 to 1 of 1 records.

□ Name	Status	Resource group	Location
□ FNPSVR01		MAIC-RG	East US

Next steps

Now that you've enabled your Linux or Windows hybrid machine and successfully connected to the service, you are ready to enable Azure Policy to understand compliance in Azure.

To learn how to identify Azure Arc-enabled servers enabled machine that doesn't have the Log Analytics agent installed, continue to the tutorial:

Create a policy assignment to identify non-compliant resources

Tutorial: Create a policy assignment to identify non-compliant resources

9/7/2021 • 4 minutes to read • Edit Online

The first step in understanding compliance in Azure is to identify the status of your resources. Azure Policy supports auditing the state of your Azure Arc-enabled server with guest configuration policies. Azure Policy's guest configuration definitions can audit or apply settings inside the machine. This tutorial steps you through the process of creating and assigning a policy, identifying which of your Azure Arc-enabled servers don't have the Log Analytics agent installed.

At the end of this process, you'll successfully identify machines that don't have the Log Analytics agent for Windows or Linux installed. They're *non-compliant* with the policy assignment.

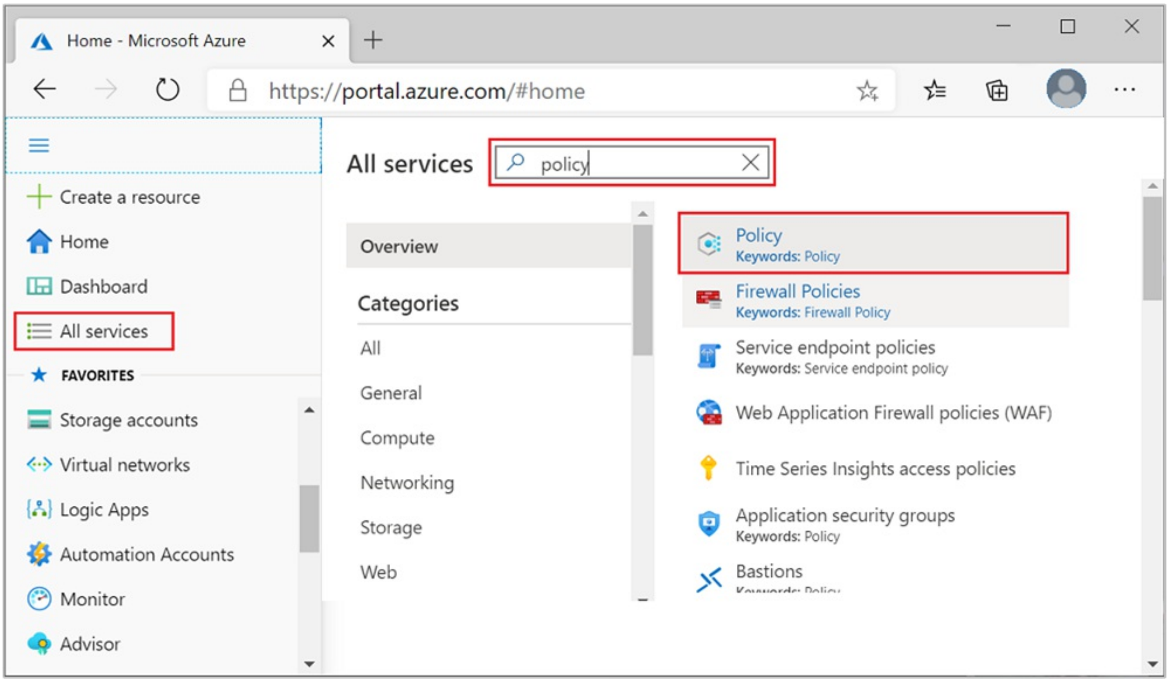
Prerequisites

If you don't have an Azure subscription, create a free account before you begin.

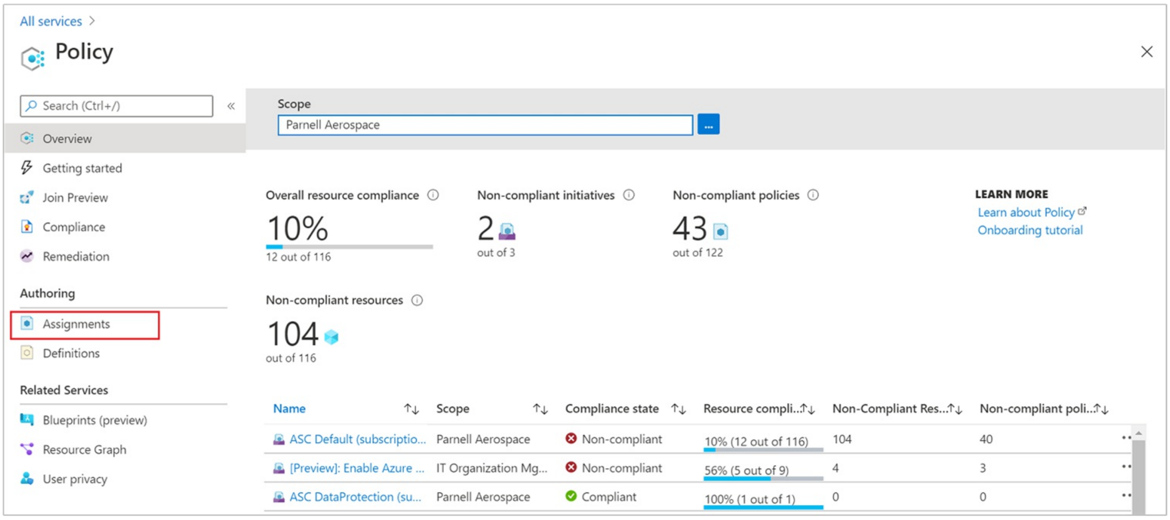
Create a policy assignment

In this tutorial, you create a policy assignment and assign the *[Preview]: Log Analytics agent should be installed on your Linux Azure Arc machines* policy definition.

1. Launch the Azure Policy service in the Azure portal by clicking **All services**, then searching for and selecting **Policy**.



2. Select **Assignments** on the left side of the Azure Policy page. An assignment is a policy that has been assigned to take place within a specific scope.



Scope: Parnell Aerospace

Overall resource compliance: 10% (12 out of 116)

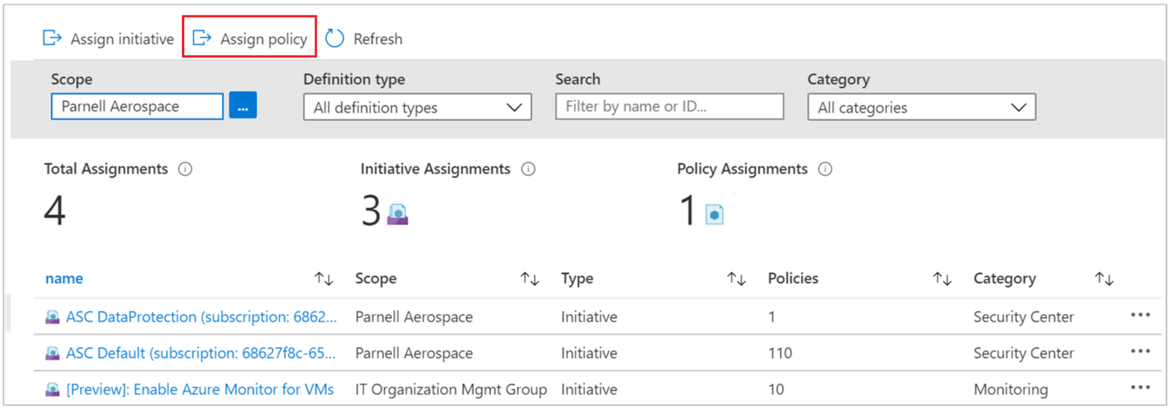
Non-compliant initiatives: 2 (out of 3)

Non-compliant policies: 43 (out of 122)

Non-compliant resources: 104 (out of 116)

Name	Scope	Compliance state	Resource compli...	Non-Compliant Res...	Non-compliant poli...
ASC Default (subscriptio...	Parnell Aerospace	Non-compliant	10% (12 out of 116)	104	40
[Preview]: Enable Azure ...	IT Organization Mg...	Non-compliant	56% (5 out of 9)	4	3
ASC DataProtection (su...	Parnell Aerospace	Compliant	100% (1 out of 1)	0	0

3. Select **Assign Policy** from the top of the **Policy - Assignments** page.



Scope: Parnell Aerospace

Definition type: All definition types

Search: Filter by name or ID...

Category: All categories

Total Assignments: 4

Initiative Assignments: 3

Policy Assignments: 1

name	Scope	Type	Policies	Category
ASC DataProtection (subscription: 6862...	Parnell Aerospace	Initiative	1	Security Center
ASC Default (subscription: 68627f8c-65...	Parnell Aerospace	Initiative	110	Security Center
[Preview]: Enable Azure Monitor for VMs	IT Organization Mgmt Group	Initiative	10	Monitoring

4. On the **Assign Policy** page, select the **Scope** by clicking the ellipsis and selecting either a management group or subscription. Optionally, select a resource group. A scope determines what resources or grouping of resources the policy assignment gets enforced on. Then click **Select** at the bottom of the **Scope** page.

   This example uses the **Parnell Aerospace** subscription. Your subscription will differ.

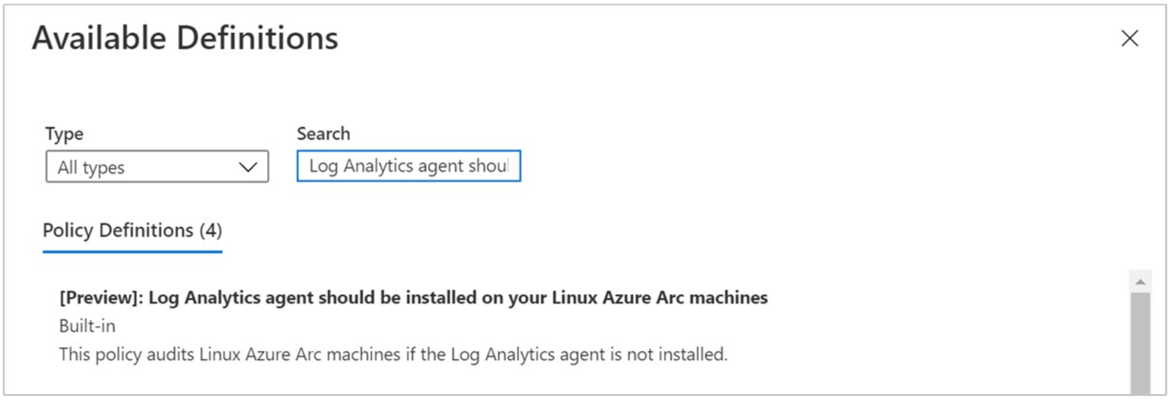
5. Resources can be excluded based on the **Scope**. **Exclusions** start at one level lower than the level of the **Scope**. **Exclusions** are optional, so leave it blank for now.

6. Select the **Policy definition** ellipsis to open the list of available definitions. Azure Policy comes with built-in policy definitions you can use. Many are available, such as:

   - Enforce tag and its value
   - Apply tag and its value
   - Inherit a tag from the resource group if missing

   For a partial list of available built-in policies, see Azure Policy samples.

7. Search through the policy definitions list to find the *[Preview]: Log Analytics agent should be installed on your Windows Azure Arc machines* definition if you have enabled the Arc-enabled servers agent on a Windows-based machine. For a Linux-based machine, find the corresponding *[Preview]: Log Analytics agent should be installed on your Linux Azure Arc machines* policy definition. Click on that policy and click **Select**.



Available Definitions

Type: All types

Search: Log Analytics agent shoul

Policy Definitions (4)

[Preview]: Log Analytics agent should be installed on your Linux Azure Arc machines
Built-in
This policy audits Linux Azure Arc machines if the Log Analytics agent is not installed.

8. The **Assignment name** is automatically populated with the policy name you selected, but you can change it. For this example, leave *[Preview]: Log Analytics agent should be installed on your Windows Azure Arc machines* or *[Preview]: Log Analytics agent should be installed on your Linux Azure Arc machines* depending on which one you selected. You can also add an optional **Description**. The description provides details about this policy assignment. **Assigned by** will automatically fill based on who is logged in. This field is optional, so custom values can be entered.

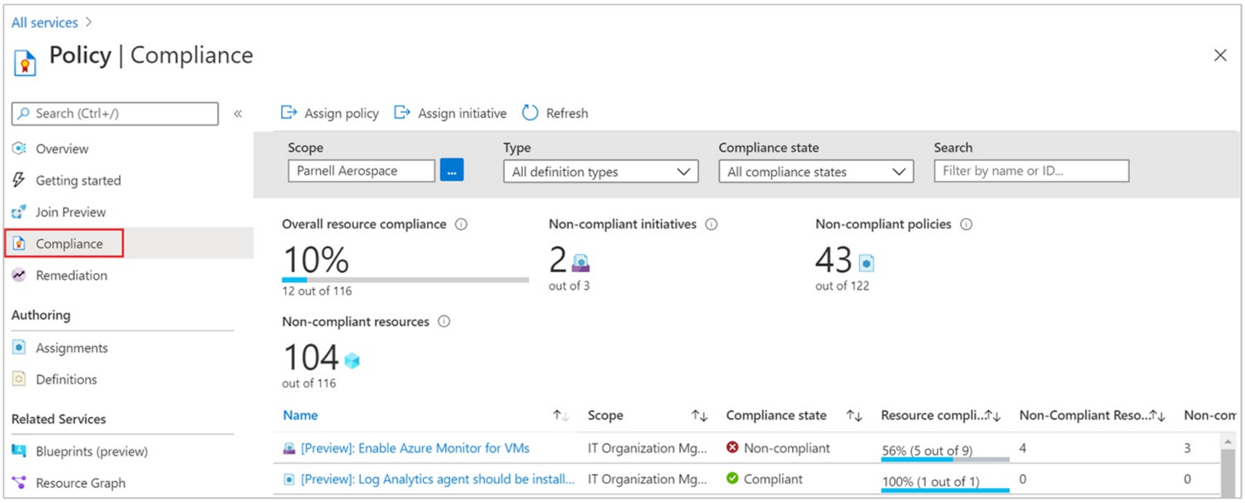
9. Leave **Create a Managed Identity** unchecked. This box *must* be checked when the policy or initiative includes a policy with the deployIfNotExists effect. As the policy used for this quickstart doesn't, leave it blank. For more information, see managed identities and how remediation security works.

10. Click **Assign**.

You're now ready to identify non-compliant resources to understand the compliance state of your environment.

Identify non-compliant resources

Select **Compliance** in the left side of the page. Then locate the **[Preview]: Log Analytics agent should be installed on your Windows Azure Arc machines** or **[Preview]: Log Analytics agent should be installed on your Linux Azure Arc machines** policy assignment you created.



Scope: Parnell Aerospace
Type: All definition types
Compliance state: All compliance states
Search: Filter by name or ID...

Overall resource compliance: 10% (12 out of 116)
Non-compliant initiatives: 2 (out of 3)
Non-compliant policies: 43 (out of 122)
Non-compliant resources: 104 (out of 116)

Name	Scope	Compliance state	Resource compli...	Non-Compliant Reso...	Non-com
[Preview]: Enable Azure Monitor for VMs	IT Organization Mg...	☒ Non-compliant	56% (5 out of 9)	4	3
[Preview]: Log Analytics agent should be install...	IT Organization Mg...	✓ Compliant	100% (1 out of 1)	0	0

If there are any existing resources that aren't compliant with this new assignment, they appear under **Non-compliant resources**.

When a condition is evaluated against your existing resources and found true, then those resources are marked as non-compliant with the policy. The following table shows how different policy effects work with the condition evaluation for the resulting compliance state. Although you don't see the evaluation logic in the Azure portal, the compliance state results are shown. The compliance state result is either compliant or non-compliant.

RESOURCE STATE	EFFECT	POLICY EVALUATION	COMPLIANCE STATE
Exists	Deny, Audit, Append*, DeployIfNotExist*, AuditIfNotExist*	True	Non-Compliant
Exists	Deny, Audit, Append*, DeployIfNotExist*, AuditIfNotExist*	False	Compliant
New	Audit, AuditIfNotExist*	True	Non-Compliant
New	Audit, AuditIfNotExist*	False	Compliant

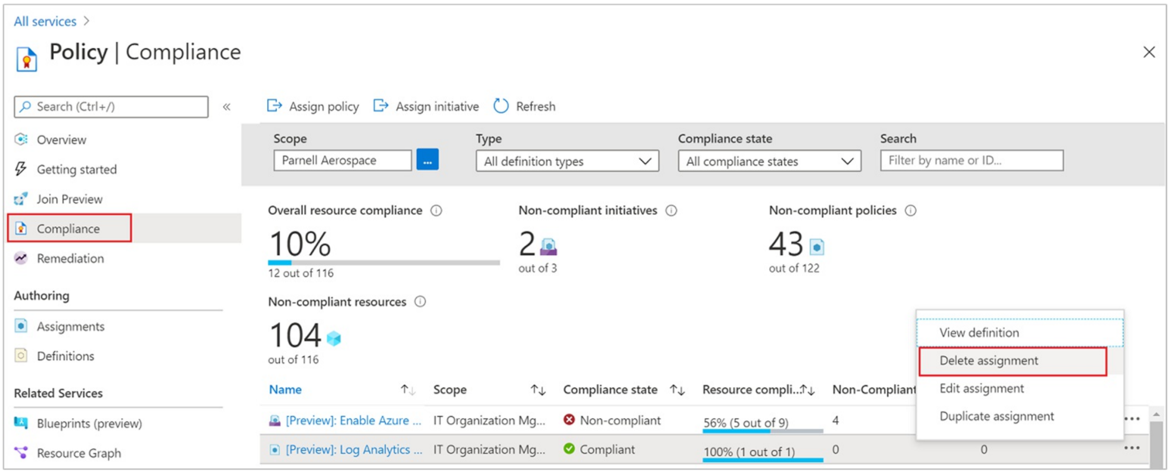
* The Append, DeployIfNotExist, and AuditIfNotExist effects require the IF statement to be TRUE. The effects also require the existence condition to be FALSE to be non-compliant. When TRUE, the IF condition triggers evaluation of the existence condition for the related resources.

Clean up resources

To remove the assignment created, follow these steps:

1. Select **Compliance** (or **Assignments**) in the left side of the Azure Policy page and locate the **[Preview]: Log Analytics agent should be installed on your Windows Azure Arc machines** or **[Preview]: Log Analytics agent should be installed on your Linux Azure Arc machines** policy assignment you created.

2. Right-click the policy assignment and select **Delete assignment**.



Scope: Parnell Aerospace

Type: All definition types

Compliance state: All compliance states

Search: Filter by name or ID...

Overall resource compliance: 10% — 12 out of 116

Non-compliant initiatives: 2 — out of 3

Non-compliant policies: 43 — out of 122

Non-compliant resources: 104 — out of 116

Name	Scope	Compliance state	Resource compli...	Non-Compliant	
[Preview]: Enable Azure ...	IT Organization Mg...	Non-compliant	56% (5 out of 9)	4	
[Preview]: Log Analytics ...	IT Organization Mg...	Compliant	100% (1 out of 1)	0	0

Next steps

In this tutorial, you assigned a policy definition to a scope and evaluated its compliance report. The policy definition validates that all the resources in the scope are compliant and identifies which ones aren't. Now you are ready to monitor your Azure Arc-enabled servers machine by enabling VM insights.

To learn how to monitor and view the performance, running process and their dependencies from your machine, continue to the tutorial:

Enable VM insights

Tutorial: Monitor a hybrid machine with VM insights

9/7/2021 • 2 minutes to read • Edit Online

Azure Monitor can collect data directly from your hybrid machines into a Log Analytics workspace for detailed analysis and correlation. Typically this would entail installing the Log Analytics agent on the machine using a script, manually, or automated method following your configuration management standards. Azure Arc-enabled servers recently introduced support to install the Log Analytics and Dependency agent VM extensions for Windows and Linux, enabling VM insights to collect data from your non-Azure VMs.

This tutorial shows you how to configure and collect data from your Linux or Windows machines by enabling VM insights following a simplified set of steps, which streamlines the experience and takes a shorter amount of time.

Prerequisites

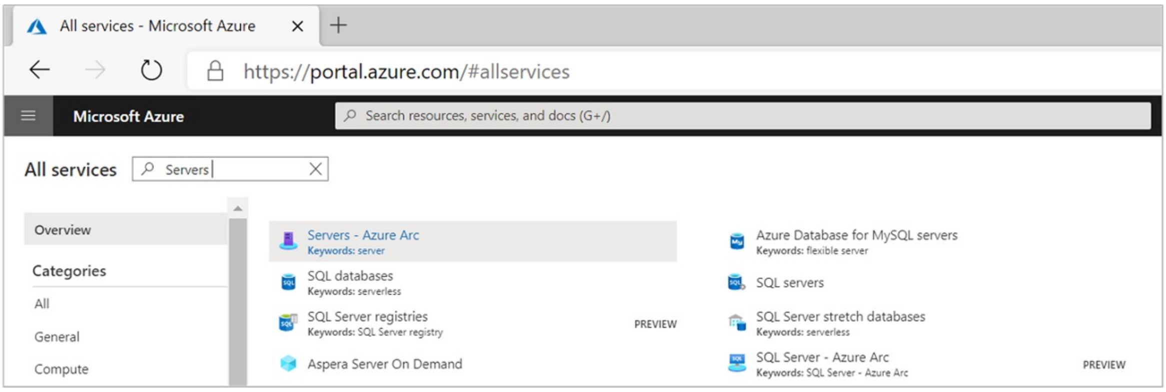
- If you don't have an Azure subscription, create a free account before you begin.
- VM extension functionality is available only inthe list of supported regions.
- See Supported operating systems to ensure that the servers operating system you're enabling is supported by VM insights.
- Review firewall requirements for the Log Analytics agent provided in the Log Analytics agent overview. The VM insights Map Dependency agent doesn't transmit any data itself, and it doesn't require any changes to firewalls or ports.

Sign in to Azure portal

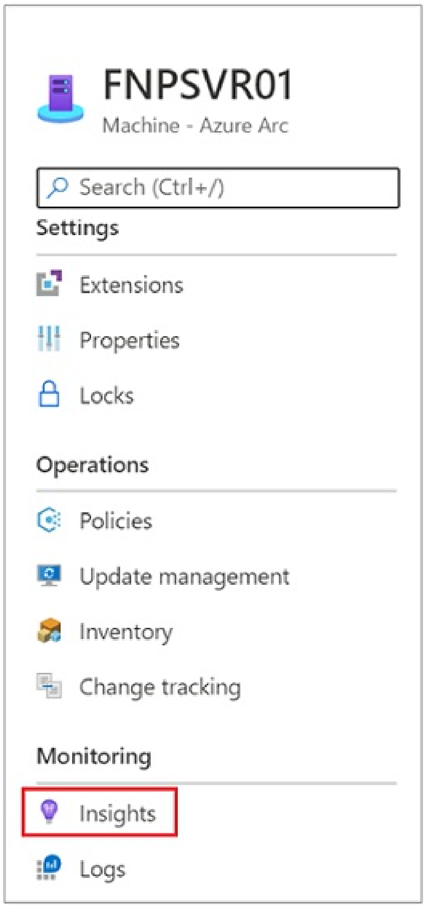
Sign in to the Azure portal.

Enable VM insights

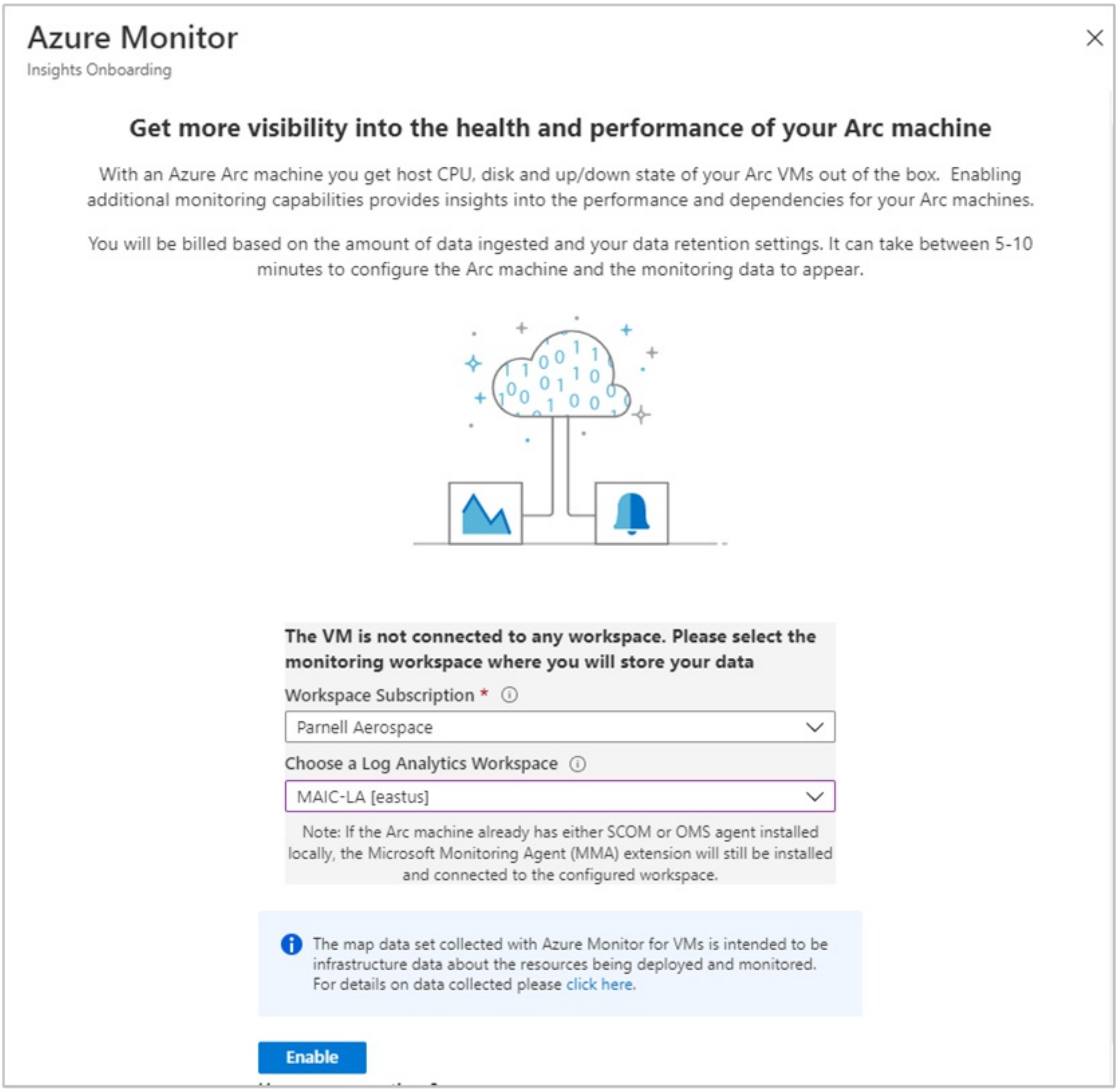
1. Launch the Azure Arc service in the Azure portal by clicking **All services**, then searching for and selecting **Machines - Azure Arc**.


All services - Microsoft Azure
https://portal.azure.com/#allservices
Microsoft Azure
Search resources, services, and docs (G+/)
All services
Servers
Overview
Categories
All
General
Compute
Servers - Azure Arc
Keywords: server
SQL databases
Keywords: serverless
SQL Server registries
Keywords: SQL Server registry
PREVIEW
Aspera Server On Demand
Azure Database for MySQL servers
Keywords: flexible server
SQL servers
SQL Server stretch databases
Keywords: serverless
SQL Server - Azure Arc
Keywords: SQL Server - Azure Arc
PREVIEW

2. On the **Machines - Azure Arc** page, select the connected machine you created in the quickstart article.
3. From the left-pane under the **Monitoring** section, select **Insights** and then **Enable**.



4. On the Azure Monitor **Insights Onboarding** page, you are prompted to create a workspace. For this tutorial, we don't recommend you select an existing Log Analytics workspace if you have one already. Select the default, which is a workspace with a unique name in the same region as your registered connected machine. This workspace is created and configured for you.



Azure Monitor

Insights Onboarding

Get more visibility into the health and performance of your Arc machine

With an Azure Arc machine you get host CPU, disk and up/down state of your Arc VMs out of the box. Enabling additional monitoring capabilities provides insights into the performance and dependencies for your Arc machines.

You will be billed based on the amount of data ingested and your data retention settings. It can take between 5-10 minutes to configure the Arc machine and the monitoring data to appear.

The VM is not connected to any workspace. Please select the monitoring workspace where you will store your data

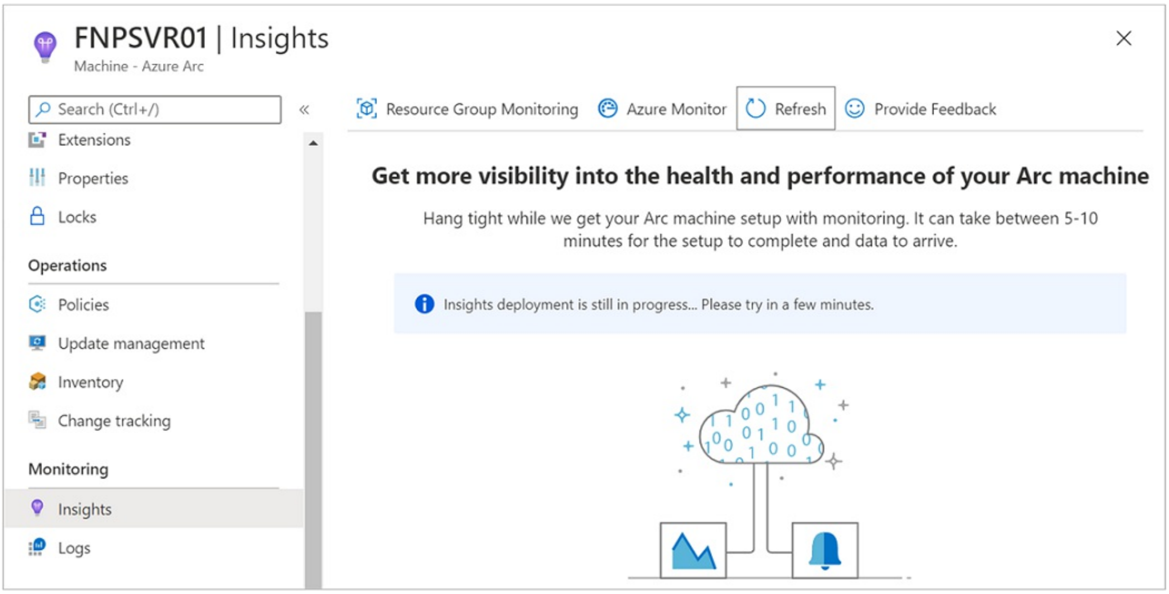
Workspace Subscription * : Parnell Aerospace

Choose a Log Analytics Workspace: MAIC-LA [eastus]

Note: If the Arc machine already has either SCOM or OMS agent installed locally, the Microsoft Monitoring Agent (MMA) extension will still be installed and connected to the configured workspace.

The map data set collected with Azure Monitor for VMs is intended to be infrastructure data about the resources being deployed and monitored. For details on data collected please click here.

5. You receive status messages while the configuration is performed. This process takes a few minutes as extensions are installed on your connected machine.



FNPSVR01 | Insights

Machine - Azure Arc

Get more visibility into the health and performance of your Arc machine

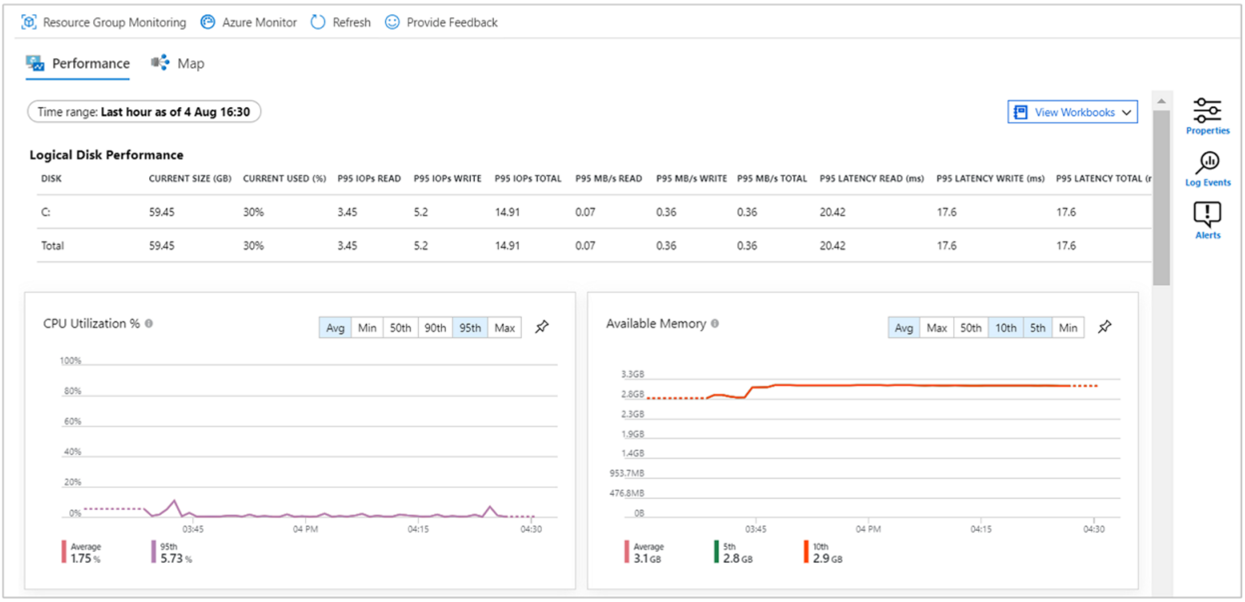
Hang tight while we get your Arc machine setup with monitoring. It can take between 5-10 minutes for the setup to complete and data to arrive.

Insights deployment is still in progress... Please try in a few minutes.

When it's complete, you get a message that the machine has been successfully onboarded and the insight has been successfully deployed.

View data collected

After the deployment and configuration is completed, select **Insights**, and then select the **Performance** tab. On the Performance tab, it shows a select group of performance counters collected from the guest operating system of your machine. Scroll down to view more counters, and move the mouse over a graph to view average and percentiles taken starting from the time when the Log Analytics VM extension was installed on the machine.

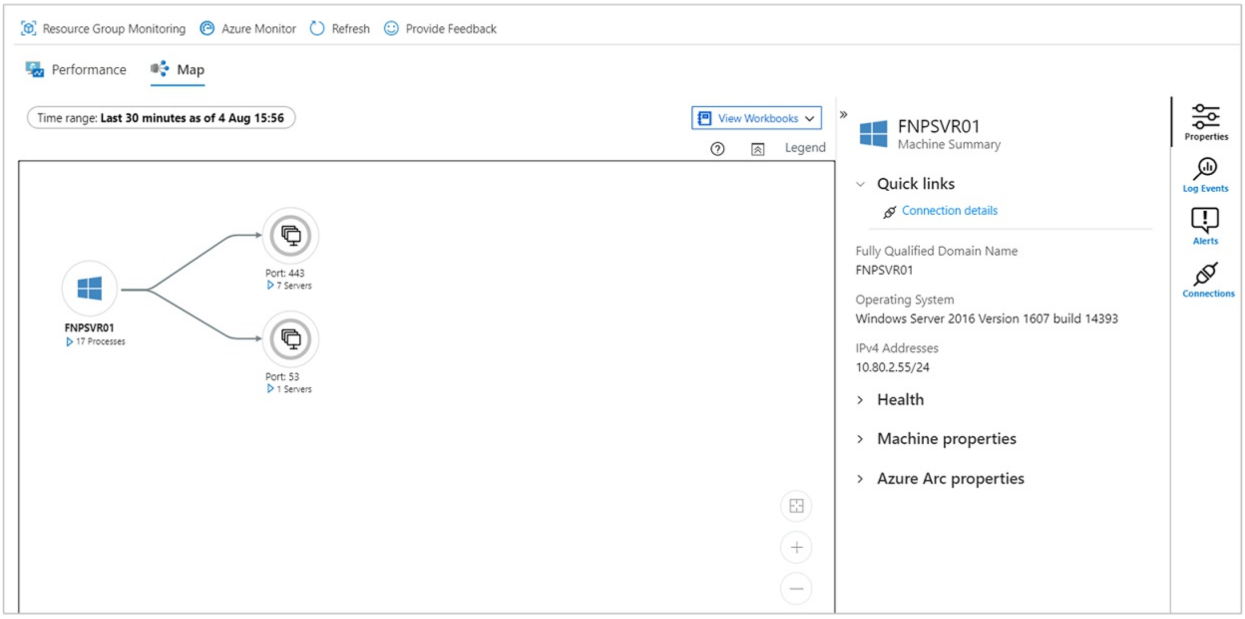


Time range: **Last hour as of 4 Aug 16:30**

Logical Disk Performance

DISK	CURRENT SIZE (GB)	CURRENT USED (%)	P95 IOPs READ	P95 IOPs WRITE	P95 IOPs TOTAL	P95 MB/s READ	P95 MB/s WRITE	P95 MB/s TOTAL	P95 LATENCY READ (ms)	P95 LATENCY WRITE (ms)	P95 LATENCY TOTAL (r
C:	59.45	30%	3.45	5.2	14.91	0.07	0.36	0.36	20.42	17.6	17.6
Total	59.45	30%	3.45	5.2	14.91	0.07	0.36	0.36	20.42	17.6	17.6

Select **Map** to open the maps feature, which shows the processes running on the machine and their dependencies. Select **Properties** to open the property pane if it isn't already open.



Time range: **Last 30 minutes as of 4 Aug 15:56**

FNPSVR01
Machine Summary

Quick links
Connection details

Fully Qualified Domain Name
FNPSVR01

Operating System
Windows Server 2016 Version 1607 build 14393

IPv4 Addresses
10.80.2.55/24

Health

Machine properties

Azure Arc properties

Expand the processes for your machine. Select one of the processes to view its details and to highlight its dependencies.

Select your machine again and then select **Log Events**. You see a list of tables that are stored in the Log Analytics workspace for the machine. This list will be different depending whether you're using a Windows or Linux machine. Select the **Event** table. The **Event** table includes all events from the Windows event log. Log Analytics opens with a simple query to retrieve collected event log entries.

Next steps

To learn more about Azure Monitor, look at the following article:

Azure Monitor overview

Azure Resource Graph sample queries for Azure Arc-enabled servers

9/5/2021 • 4 minutes to read • Edit Online

This page is a collection of Azure Resource Graph sample queries for Azure Arc-enabled servers. For a complete list of Azure Resource Graph samples, see Resource Graph samples by Category and Resource Graph samples by Table.

Sample queries

Get count and percentage of Arc-enabled servers by domain

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

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

- Azure CLI
- Azure PowerShell
- Portal

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

List all extensions installed on an Azure Arc-enabled server

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

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

- Azure CLI
- Azure PowerShell
- Portal

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

List Arc-enabled servers not running latest released agent version

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

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

- Azure CLI
- Azure PowerShell

- Portal

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

Next steps

- Learn more about the query language.
- Learn more about how to explore resources.
- See samples of Starter language queries.
- See samples of Advanced language queries.

Azure Policy Regulatory Compliance controls for Azure Arc-enabled servers

9/3/2021 • 41 minutes to read • Edit Online

Regulatory Compliance in Azure Policy provides Microsoft created and managed initiative definitions, known as *built-ins*, for the **compliance domains** and **security controls** related to different compliance standards. This page lists the **compliance domains** and **security controls** for Azure Arc-enabled servers. You can assign the built-ins for a **security control** individually to help make your Azure resources compliant with the specific standard.

The title of each built-in policy definition links to the policy definition in the Azure portal. Use the link in the **Policy Version** column to view the source on the Azure Policy GitHub repo.

> **IMPORTANT**
>
> Each control below is associated with one or more Azure Policy definitions. These policies may help you assess compliance with the control; however, there often is not a one-to-one or complete match between a control and one or more policies. As such, **Compliant** in Azure Policy refers only to the policies themselves; this doesn't ensure you're fully compliant with all requirements of a control. In addition, the compliance standard includes controls that aren't addressed by any Azure Policy definitions at this time. Therefore, compliance in Azure Policy is only a partial view of your overall compliance status. The associations between controls and Azure Policy Regulatory Compliance definitions for these compliance standards may change over time.

Australian Government ISM PROTECTED

To review how the available Azure Policy built-ins for all Azure services map to this compliance standard, see Azure Policy Regulatory Compliance - Australian Government ISM PROTECTED. For more information about this compliance standard, see Australian Government ISM PROTECTED.

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY (AZURE PORTAL)	POLICY VERSION (GITHUB)
Guidelines for Personnel Security - Access to systems and their resources	415	User identification - 415	Audit Windows machines that have the specified members in the Administrators group	1.0.0
Guidelines for System Hardening - Authentication hardening	421	Single-factor authentication - 421	Windows machines should meet requirements for 'Security Settings - Account Policies'	2.0.0
Guidelines for Personnel Security - Access to systems and their resources	445	Privileged access to systems - 445	Audit Windows machines that have the specified members in the Administrators group	1.0.0

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY	POLICY VERSION
Guidelines for Cryptography - Transport Layer Security	1139	Using Transport Layer Security - 1139	Windows web servers should be configured to use secure communication protocols	3.0.0
Guidelines for Database Systems - Database servers	1277	Communications between database servers and web servers - 1277	Windows web servers should be configured to use secure communication protocols	3.0.0
Guidelines for Personnel Security - Access to systems and their resources	1503	Standard access to systems - 1503	Audit Windows machines that have the specified members in the Administrators group	1.0.0
Guidelines for Personnel Security - Access to systems and their resources	1507	Privileged access to systems - 1507	Audit Windows machines that have the specified members in the Administrators group	1.0.0
Guidelines for Personnel Security - Access to systems and their resources	1508	Privileged access to systems - 1508	Audit Windows machines that have the specified members in the Administrators group	1.0.0
Guidelines for System Hardening - Authentication hardening	1546	Authenticating to systems - 1546	Audit Linux machines that allow remote connections from accounts without passwords	1.0.0
Guidelines for System Hardening - Authentication hardening	1546	Authenticating to systems - 1546	Audit Linux machines that have accounts without passwords	1.0.0

Azure Security Benchmark

The Azure Security Benchmark provides recommendations on how you can secure your cloud solutions on Azure. To see how this service completely maps to the Azure Security Benchmark, see the Azure Security Benchmark mapping files.

To review how the available Azure Policy built-ins for all Azure services map to this compliance standard, see Azure Policy Regulatory Compliance - Azure Security Benchmark.

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY (AZURE PORTAL)	POLICY VERSION (GITHUB)
Identity Management	IM-4	Use strong authentication controls for all Azure Active Directory based access	Authentication to Linux machines should require SSH keys	2.0.1
Data Protection	DP-4	Encrypt sensitive information in transit	Windows web servers should be configured to use secure communication protocols	3.0.0
Logging and Threat Detection	LT-5	Centralize security log management and analysis	Log Analytics agent should be installed on your Linux Azure Arc machines	1.0.0-preview
Logging and Threat Detection	LT-5	Centralize security log management and analysis	Log Analytics agent should be installed on your Windows Azure Arc machines	1.0.0-preview
Posture and Vulnerability Management	PV-4	Sustain secure configurations for compute resources	Linux machines should meet requirements for the Azure compute security baseline	1.1.1-preview
Posture and Vulnerability Management	PV-4	Sustain secure configurations for compute resources	Windows machines should meet requirements of the Azure compute security baseline	1.0.1-preview
Posture and Vulnerability Management	PV-6	Perform software vulnerability assessments	SQL servers on machines should have vulnerability findings resolved	1.0.0
Endpoint Security	ES-2	Use centrally managed modern anti-malware software	Endpoint protection health issues should be resolved on your machines	1.0.0
Endpoint Security	ES-2	Use centrally managed modern anti-malware software	Endpoint protection should be installed on your machines	1.0.0
Endpoint Security	ES-2	Use centrally managed modern anti-malware software	Windows Defender Exploit Guard should be enabled on your machines	1.1.1

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY	POLICY VERSION
Endpoint Security	ES-3	Ensure anti-malware software and signatures are updated	Endpoint protection health issues should be resolved on your machines	1.0.0
Endpoint Security	ES-3	Ensure anti-malware software and signatures are updated	Endpoint protection should be installed on your machines	1.0.0

Azure Security Benchmark v1

The Azure Security Benchmark provides recommendations on how you can secure your cloud solutions on Azure. To see how this service completely maps to the Azure Security Benchmark, see the Azure Security Benchmark mapping files.

To review how the available Azure Policy built-ins for all Azure services map to this compliance standard, see Azure Policy Regulatory Compliance - Azure Security Benchmark.

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY (AZURE PORTAL)	POLICY VERSION (GITHUB)
Network Security	1.11	Use automated tools to monitor network resource configurations and detect changes	Windows machines should meet requirements for 'Administrative Templates - Network'	2.0.0
Network Security	1.11	Use automated tools to monitor network resource configurations and detect changes	Windows machines should meet requirements for 'Security Options - Microsoft Network Server'	2.0.0
Network Security	1.11	Use automated tools to monitor network resource configurations and detect changes	Windows machines should meet requirements for 'Security Options - Network Access'	2.0.0
Network Security	1.11	Use automated tools to monitor network resource configurations and detect changes	Windows machines should meet requirements for 'Security Options - Network Security'	2.0.0
Logging and Monitoring	2.2	Configure central security log management	Audit Windows machines on which the Log Analytics agent is not connected as expected	1.0.0

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY	POLICY VERSION
Logging and Monitoring	2.4	Collect security logs from operating systems	Audit Windows machines on which the Log Analytics agent is not connected as expected	1.0.0
Identity and Access Control	3.3	Use dedicated administrative accounts	Audit Windows machines missing any of specified members in the Administrators group	1.0.0
Identity and Access Control	3.3	Use dedicated administrative accounts	Audit Windows machines that have extra accounts in the Administrators group	1.0.0
Identity and Access Control	3.3	Use dedicated administrative accounts	Audit Windows machines that have the specified members in the Administrators group	1.0.0

Canada Federal PBMM

To review how the available Azure Policy built-ins for all Azure services map to this compliance standard, see Azure Policy Regulatory Compliance - Canada Federal PBMM. For more information about this compliance standard, see Canada Federal PBMM.

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY (AZURE PORTAL)	POLICY VERSION (GITHUB)
Access Control	AC-5	Separation of Duties	Audit Windows machines missing any of specified members in the Administrators group	1.0.0
Access Control	AC-5	Separation of Duties	Audit Windows machines that have the specified members in the Administrators group	1.0.0
Access Control	AC-6	Least Privilege	Audit Windows machines missing any of specified members in the Administrators group	1.0.0

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY	POLICY VERSION
Access Control	AC-6	Least Privilege	Audit Windows machines that have the specified members in the Administrators group	1.0.0
Access Control	AC-17(1)	Remote Access | Automated Monitoring / Control	Audit Linux machines that allow remote connections from accounts without passwords	1.0.0
Identification and Authentication	IA-5	Authenticator Management	Audit Linux machines that do not have the passwd file permissions set to 0644	1.0.0
Identification and Authentication	IA-5	Authenticator Management	Audit Linux machines that have accounts without passwords	1.0.0
Identification and Authentication	IA-5(1)	Authenticator Management | Password-Based Authentication	Audit Windows machines that allow re-use of the previous 24 passwords	1.0.0
Identification and Authentication	IA-5(1)	Authenticator Management | Password-Based Authentication	Audit Windows machines that do not have a maximum password age of 70 days	1.0.0
Identification and Authentication	IA-5(1)	Authenticator Management | Password-Based Authentication	Audit Windows machines that do not have a minimum password age of 1 day	1.0.0
Identification and Authentication	IA-5(1)	Authenticator Management | Password-Based Authentication	Audit Windows machines that do not have the password complexity setting enabled	1.0.0
Identification and Authentication	IA-5(1)	Authenticator Management | Password-Based Authentication	Audit Windows machines that do not restrict the minimum password length to 14 characters	1.0.0

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY	POLICY VERSION
System and Communications Protection	SC-8(1)	Transmission Confidentiality and Integrity | Cryptographic or Alternate Physical Protection	Windows web servers should be configured to use secure communication protocols	3.0.0

CMMC Level 3

To review how the available Azure Policy built-ins for all Azure services map to this compliance standard, see Azure Policy Regulatory Compliance - CMMC Level 3. For more information about this compliance standard, see Cybersecurity Maturity Model Certification (CMMC).

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY (AZURE PORTAL)	POLICY VERSION (GITHUB)
Access Control	AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, and devices (including other information systems).	Audit Linux machines that allow remote connections from accounts without passwords	1.0.0
Access Control	AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, and devices (including other information systems).	Windows machines should meet requirements for 'Security Options - Network Access'	2.0.0
Access Control	AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, and devices (including other information systems).	Windows machines should meet requirements for 'Security Options - Network Security'	2.0.0
Access Control	AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	Audit Linux machines that allow remote connections from accounts without passwords	1.0.0
Access Control	AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	Windows machines should meet requirements for 'Security Options - Network Access'	2.0.0

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY	POLICY VERSION
Access Control	AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	Windows web servers should be configured to use secure communication protocols	3.0.0
Access Control	AC.2.008	Use non-privileged accounts or roles when accessing nonsecurity functions.	Windows machines should meet requirements for 'Security Options - User Account Control'	2.0.0
Access Control	AC.2.008	Use non-privileged accounts or roles when accessing nonsecurity functions.	Windows machines should meet requirements for 'User Rights Assignment'	2.0.0
Access Control	AC.2.013	Monitor and control remote access sessions.	Audit Linux machines that allow remote connections from accounts without passwords	1.0.0
Access Control	AC.2.013	Monitor and control remote access sessions.	Windows machines should meet requirements for 'Security Options - Network Security'	2.0.0
Access Control	AC.2.016	Control the flow of CUI in accordance with approved authorizations.	Windows machines should meet requirements for 'Security Options - Network Access'	2.0.0
Access Control	AC.3.017	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	Audit Windows machines missing any of specified members in the Administrators group	1.0.0
Access Control	AC.3.017	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	Audit Windows machines that have the specified members in the Administrators group	1.0.0
Access Control	AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	Windows machines should meet requirements for 'System Audit Policies - Privilege Use'	2.0.0

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY	POLICY VERSION
Access Control	AC.3.021	Authorize remote execution of privileged commands and remote access to security-relevant information.	Windows machines should meet requirements for 'Security Options - User Account Control'	2.0.0
Access Control	AC.3.021	Authorize remote execution of privileged commands and remote access to security-relevant information.	Windows machines should meet requirements for 'User Rights Assignment'	2.0.0
Configuration Management	CM.2.061	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	Linux machines should meet requirements for the Azure compute security baseline	1.1.1-preview
Configuration Management	CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	Windows machines should meet requirements for 'System Audit Policies - Privilege Use'	2.0.0
Configuration Management	CM.2.063	Control and monitor user-installed software.	Windows machines should meet requirements for 'Security Options - User Account Control'	2.0.0
Configuration Management	CM.2.064	Establish and enforce security configuration settings for information technology products employed in organizational systems.	Windows machines should meet requirements for 'Security Options - Network Security'	2.0.0
Configuration Management	CM.2.065	Track, review, approve or disapprove, and log changes to organizational systems.	Windows machines should meet requirements for 'System Audit Policies - Policy Change'	2.0.0

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY	POLICY VERSION
Identification and Authentication	IA.1.077	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	Audit Linux machines that do not have the passwd file permissions set to 0644	1.0.0
Identification and Authentication	IA.1.077	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	Audit Linux machines that have accounts without passwords	1.0.0
Identification and Authentication	IA.1.077	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	Windows machines should meet requirements for 'Security Options - Network Security'	2.0.0
Identification and Authentication	IA.2.078	Enforce a minimum password complexity and change of characters when new passwords are created.	Audit Linux machines that have accounts without passwords	1.0.0
Identification and Authentication	IA.2.078	Enforce a minimum password complexity and change of characters when new passwords are created.	Audit Windows machines that do not have the password complexity setting enabled	1.0.0
Identification and Authentication	IA.2.078	Enforce a minimum password complexity and change of characters when new passwords are created.	Audit Windows machines that do not restrict the minimum password length to 14 characters	1.0.0
Identification and Authentication	IA.2.078	Enforce a minimum password complexity and change of characters when new passwords are created.	Windows machines should meet requirements for 'Security Options - Network Security'	2.0.0

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY	POLICY VERSION
Identification and Authentication	IA.2.079	Prohibit password reuse for a specified number of generations.	Audit Windows machines that allow re-use of the previous 24 passwords	1.0.0
Identification and Authentication	IA.2.079	Prohibit password reuse for a specified number of generations.	Windows machines should meet requirements for 'Security Options - Network Security'	2.0.0
Identification and Authentication	IA.2.081	Store and transmit only cryptographically-protected passwords.	Audit Windows machines that do not store passwords using reversible encryption	1.0.0
Identification and Authentication	IA.2.081	Store and transmit only cryptographically-protected passwords.	Windows machines should meet requirements for 'Security Options - Network Security'	2.0.0
Identification and Authentication	IA.3.084	Employ replay-resistant authentication mechanisms for network access to privileged and nonprivileged accounts.	Windows web servers should be configured to use secure communication protocols	3.0.0
System and Communications Protection	SC.1.175	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	Windows machines should meet requirements for 'Security Options - Network Access'	2.0.0

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY	POLICY VERSION
System and Communications Protection	SC.1.175	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	Windows machines should meet requirements for 'Security Options - Network Security'	2.0.0
System and Communications Protection	SC.1.175	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	Windows web servers should be configured to use secure communication protocols	3.0.0
System and Communications Protection	SC.3.177	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	Audit Windows machines that do not store passwords using reversible encryption	1.0.0
System and Communications Protection	SC.3.181	Separate user functionality from system management functionality.	Audit Windows machines that have the specified members in the Administrators group	1.0.0
System and Communications Protection	SC.3.183	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	Windows machines should meet requirements for 'Security Options - Network Access'	2.0.0
System and Communications Protection	SC.3.183	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	Windows machines should meet requirements for 'Security Options - Network Security'	2.0.0

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY	POLICY VERSION
System and Communications Protection	SC.3.185	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	Windows web servers should be configured to use secure communication protocols	3.0.0
System and Communications Protection	SC.3.190	Protect the authenticity of communications sessions.	Windows web servers should be configured to use secure communication protocols	3.0.0

FedRAMP High

To review how the available Azure Policy built-ins for all Azure services map to this compliance standard, see Azure Policy Regulatory Compliance - FedRAMP High. For more information about this compliance standard, see FedRAMP High.

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY (AZURE PORTAL)	POLICY VERSION (GITHUB)
Access Control	AC-3	Access Enforcement	Audit Linux machines that have accounts without passwords	1.0.0
Access Control	AC-3	Access Enforcement	Authentication to Linux machines should require SSH keys	2.0.1
Access Control	AC-17	Remote Access	Audit Linux machines that allow remote connections from accounts without passwords	1.0.0
Access Control	AC-17 (1)	Automated Monitoring / Control	Audit Linux machines that allow remote connections from accounts without passwords	1.0.0
Audit and Accountability	AU-6 (4)	Central Review and Analysis	Log Analytics agent should be installed on your Linux Azure Arc machines	1.0.0-preview

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY	POLICY VERSION
Audit and Accountability	AU-6 (4)	Central Review and Analysis	Log Analytics agent should be installed on your Windows Azure Arc machines	1.0.0-preview
Audit and Accountability	AU-6 (5)	Integration / Scanning and Monitoring Capabilities	Log Analytics agent should be installed on your Linux Azure Arc machines	1.0.0-preview
Audit and Accountability	AU-6 (5)	Integration / Scanning and Monitoring Capabilities	Log Analytics agent should be installed on your Windows Azure Arc machines	1.0.0-preview
Audit and Accountability	AU-12	Audit Generation	Log Analytics agent should be installed on your Linux Azure Arc machines	1.0.0-preview
Audit and Accountability	AU-12	Audit Generation	Log Analytics agent should be installed on your Windows Azure Arc machines	1.0.0-preview
Audit and Accountability	AU-12 (1)	System-wide / Time-correlated Audit Trail	Log Analytics agent should be installed on your Linux Azure Arc machines	1.0.0-preview
Audit and Accountability	AU-12 (1)	System-wide / Time-correlated Audit Trail	Log Analytics agent should be installed on your Windows Azure Arc machines	1.0.0-preview
Configuration Management	CM-6	Configuration Settings	Linux machines should meet requirements for the Azure compute security baseline	1.1.1-preview
Configuration Management	CM-6	Configuration Settings	Windows machines should meet requirements of the Azure compute security baseline	1.0.1-preview
Identification and Authentication	IA-5	Authenticator Management	Audit Linux machines that do not have the passwd file permissions set to 0644	1.0.0

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY	POLICY VERSION
Identification and Authentication	IA-5	Authenticator Management	Audit Windows machines that do not store passwords using reversible encryption	1.0.0
Identification and Authentication	IA-5	Authenticator Management	Authentication to Linux machines should require SSH keys	2.0.1
Identification and Authentication	IA-5 (1)	Password-based Authentication	Audit Linux machines that do not have the passwd file permissions set to 0644	1.0.0
Identification and Authentication	IA-5 (1)	Password-based Authentication	Audit Windows machines that allow re-use of the previous 24 passwords	1.0.0
Identification and Authentication	IA-5 (1)	Password-based Authentication	Audit Windows machines that do not have a maximum password age of 70 days	1.0.0
Identification and Authentication	IA-5 (1)	Password-based Authentication	Audit Windows machines that do not have a minimum password age of 1 day	1.0.0
Identification and Authentication	IA-5 (1)	Password-based Authentication	Audit Windows machines that do not have the password complexity setting enabled	1.0.0
Identification and Authentication	IA-5 (1)	Password-based Authentication	Audit Windows machines that do not restrict the minimum password length to 14 characters	1.0.0
Identification and Authentication	IA-5 (1)	Password-based Authentication	Audit Windows machines that do not store passwords using reversible encryption	1.0.0

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY	POLICY VERSION
Risk Assessment	RA-5	Vulnerability Scanning	SQL servers on machines should have vulnerability findings resolved	1.0.0
System and Communications Protection	SC-3	Security Function Isolation	Windows Defender Exploit Guard should be enabled on your machines	1.1.1
System and Communications Protection	SC-8	Transmission Confidentiality and Integrity	Windows web servers should be configured to use secure communication protocols	3.0.0
System and Communications Protection	SC-8 (1)	Cryptographic or Alternate Physical Protection	Windows web servers should be configured to use secure communication protocols	3.0.0
System and Information Integrity	SI-3	Malicious Code Protection	Windows Defender Exploit Guard should be enabled on your machines	1.1.1
System and Information Integrity	SI-3 (1)	Central Management	Windows Defender Exploit Guard should be enabled on your machines	1.1.1
System and Information Integrity	SI-4	Information System Monitoring	Log Analytics agent should be installed on your Linux Azure Arc machines	1.0.0-preview
System and Information Integrity	SI-4	Information System Monitoring	Log Analytics agent should be installed on your Windows Azure Arc machines	1.0.0-preview
System and Information Integrity	SI-16	Memory Protection	Windows Defender Exploit Guard should be enabled on your machines	1.1.1

FedRAMP Moderate

To review how the available Azure Policy built-ins for all Azure services map to this compliance standard, see Azure Policy Regulatory Compliance - FedRAMP Moderate. For more information about this compliance standard, see FedRAMP Moderate.

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY (AZURE PORTAL)	POLICY VERSION (GITHUB)
Access Control	AC-3	Access Enforcement	Audit Linux machines that have accounts without passwords	1.0.0
Access Control	AC-3	Access Enforcement	Authentication to Linux machines should require SSH keys	2.0.1
Access Control	AC-17	Remote Access	Audit Linux machines that allow remote connections from accounts without passwords	1.0.0
Access Control	AC-17 (1)	Automated Monitoring / Control	Audit Linux machines that allow remote connections from accounts without passwords	1.0.0
Audit and Accountability	AU-12	Audit Generation	Log Analytics agent should be installed on your Linux Azure Arc machines	1.0.0-preview
Audit and Accountability	AU-12	Audit Generation	Log Analytics agent should be installed on your Windows Azure Arc machines	1.0.0-preview
Configuration Management	CM-6	Configuration Settings	Linux machines should meet requirements for the Azure compute security baseline	1.1.1-preview
Configuration Management	CM-6	Configuration Settings	Windows machines should meet requirements of the Azure compute security baseline	1.0.1-preview
Identification and Authentication	IA-5	Authenticator Management	Audit Linux machines that do not have the passwd file permissions set to 0644	1.0.0
Identification and Authentication	IA-5	Authenticator Management	Audit Windows machines that do not store passwords using reversible encryption	1.0.0

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY	POLICY VERSION
Identification and Authentication	IA-5	Authenticator Management	Authentication to Linux machines should require SSH keys	2.0.1
Identification and Authentication	IA-5 (1)	Password-based Authentication	Audit Linux machines that do not have the passwd file permissions set to 0644	1.0.0
Identification and Authentication	IA-5 (1)	Password-based Authentication	Audit Windows machines that allow re-use of the previous 24 passwords	1.0.0
Identification and Authentication	IA-5 (1)	Password-based Authentication	Audit Windows machines that do not have a maximum password age of 70 days	1.0.0
Identification and Authentication	IA-5 (1)	Password-based Authentication	Audit Windows machines that do not have a minimum password age of 1 day	1.0.0
Identification and Authentication	IA-5 (1)	Password-based Authentication	Audit Windows machines that do not have the password complexity setting enabled	1.0.0
Identification and Authentication	IA-5 (1)	Password-based Authentication	Audit Windows machines that do not restrict the minimum password length to 14 characters	1.0.0
Identification and Authentication	IA-5 (1)	Password-based Authentication	Audit Windows machines that do not store passwords using reversible encryption	1.0.0
Risk Assessment	RA-5	Vulnerability Scanning	SQL servers on machines should have vulnerability findings resolved	1.0.0

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY	POLICY VERSION
System and Communications Protection	SC-8	Transmission Confidentiality and Integrity	Windows web servers should be configured to use secure communication protocols	3.0.0
System and Communications Protection	SC-8 (1)	Cryptographic or Alternate Physical Protection	Windows web servers should be configured to use secure communication protocols	3.0.0
System and Information Integrity	SI-3	Malicious Code Protection	Windows Defender Exploit Guard should be enabled on your machines	1.1.1
System and Information Integrity	SI-3 (1)	Central Management	Windows Defender Exploit Guard should be enabled on your machines	1.1.1
System and Information Integrity	SI-4	Information System Monitoring	Log Analytics agent should be installed on your Linux Azure Arc machines	1.0.0-preview
System and Information Integrity	SI-4	Information System Monitoring	Log Analytics agent should be installed on your Windows Azure Arc machines	1.0.0-preview
System and Information Integrity	SI-16	Memory Protection	Windows Defender Exploit Guard should be enabled on your machines	1.1.1

HIPAA HITRUST 9.2

To review how the available Azure Policy built-ins for all Azure services map to this compliance standard, see Azure Policy Regulatory Compliance - HIPAA HITRUST 9.2. For more information about this compliance standard, see HIPAA HITRUST 9.2.

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY (AZURE PORTAL)	POLICY VERSION (GITHUB)
Privilege Management	1148.01c2System.78 - 01.c	The organization restricts access to privileged functions and all security-relevant information.	Windows machines should meet requirements for 'Security Options - Accounts'	2.0.0

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY	POLICY VERSION
User Identification and Authentication	11210.01q2Organizational.10 - 01.q	Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records.	Audit Windows machines that have the specified members in the Administrators group	1.0.0
User Identification and Authentication	11211.01q2Organizational.11 - 01.q	Signed electronic records shall contain information associated with the signing in human-readable format.	Audit Windows machines missing any of specified members in the Administrators group	1.0.0
User Identification and Authentication	1123.01q1System.2 - 01.q	Users who performed privileged functions (e.g., system administration) use separate accounts when performing those privileged functions.	Audit Windows machines that have extra accounts in the Administrators group	1.0.0
User Identification and Authentication	1125.01q2System.1 - 01.q	Multi-factor authentication methods are used in accordance with organizational policy, (e.g., for remote network access).	Audit Windows machines that have the specified members in the Administrators group	1.0.0
User Identification and Authentication	1127.01q2System.3 - 01.q	Where tokens are provided for multi-factor authentication, in-person verification is required prior to granting access.	Audit Windows machines missing any of specified members in the Administrators group	1.0.0
Monitoring System Use	12102.09ab1Organizational.4 - 09.ab	The organization shall periodically test its monitoring and detection processes, remediate deficiencies, and improve its processes.	Audit Windows machines on which the Log Analytics agent is not connected as expected	1.0.0
Monitoring System Use	1217.09ab3System.3 - 09.ab	Alerts are generated for technical personnel to analyze and investigate suspicious activity or suspected violations.	Audit Windows machines on which the Log Analytics agent is not connected as expected	1.0.0

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY	POLICY VERSION
Segregation of Duties	1232.09c3Organizational.12 - 09.c	Access for individuals responsible for administering access controls is limited to the minimum necessary based upon each user's role and responsibilities and these individuals cannot access audit functions related to these controls.	Windows machines should meet requirements for 'User Rights Assignment'	2.0.0
Segregation of Duties	1277.09c2Organizational.4 - 09.c	The initiation of an event is separated from its authorization to reduce the possibility of collusion.	Windows machines should meet requirements for 'Security Options - User Account Control'	2.0.0
Network Controls	0858.09m1Organizational.4 - 09.m	The organization monitors for all authorized and unauthorized wireless access to the information system and prohibits installation of wireless access points (WAPs) unless explicitly authorized in writing by the CIO or his/her designated representative.	Windows machines should meet requirements for 'Windows Firewall Properties'	2.0.0
Network Controls	0861.09m2Organizational.67 - 09.m	To identify and authenticate devices on local and/or wide area networks, including wireless networks, the information system uses either a (i) shared known information solution or (ii) an organizational authentication solution, the exact selection and strength of which is dependent on the security categorization of the information system.	Windows machines should meet requirements for 'Security Options - Network Access'	2.0.0

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY	POLICY VERSION
On-line Transactions	0945.09y1Organizational.3 - 09.y	Protocols used to communicate between all involved parties are secured using cryptographic techniques (e.g., SSL).	Audit Windows machines that do not contain the specified certificates in Trusted Root	1.0.1
Control of Operational Software	0605.10h1System.12 - 10.h	Only authorized administrators are allowed to implement approved upgrades to software, applications, and program libraries, based on business requirements and the security implications of the release.	Windows machines should meet requirements for 'Security Options - Audit'	2.0.0
Control of Operational Software	0605.10h1System.12 - 10.h	Only authorized administrators are allowed to implement approved upgrades to software, applications, and program libraries, based on business requirements and the security implications of the release.	Windows machines should meet requirements for 'System Audit Policies - Account Management'	2.0.0
Change Control Procedures	0635.10k1Organizational.12 - 10.k	Managers responsible for application systems are also responsible for the strict control (security) of the project or support environment and ensure that all proposed system changes are reviewed to check that they do not compromise the security of either the system or the operating environment.	Windows machines should meet requirements for 'System Audit Policies - Detailed Tracking'	2.0.0

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY	POLICY VERSION
Change Control Procedures	0636.10k2Organizational.1 - 10.k	The organization formally addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance for configuration management (e.g., through policies, standards, processes).	Windows machines should meet requirements for 'System Audit Policies - Detailed Tracking'	2.0.0
Change Control Procedures	0637.10k2Organizational.2 - 10.k	The organization has developed, documented, and implemented a configuration management plan for the information system.	Windows machines should meet requirements for 'System Audit Policies - Detailed Tracking'	2.0.0
Change Control Procedures	0638.10k2Organizational.34569 - 10.k	Changes are formally controlled, documented and enforced in order to minimize the corruption of information systems.	Windows machines should meet requirements for 'System Audit Policies - Detailed Tracking'	2.0.0
Change Control Procedures	0639.10k2Organizational.78 - 10.k	Installation checklists and vulnerability scans are used to validate the configuration of servers, workstations, devices and appliances and ensure the configuration meets minimum standards.	Windows machines should meet requirements for 'System Audit Policies - Detailed Tracking'	2.0.0

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY	POLICY VERSION
Change Control Procedures	0640.10k2Organizational.1012 - 10.k	Where development is outsourced, change control procedures to address security are included in the contract(s) and specifically require the developer to track security flaws and flaw resolution within the system, component, or service and report findings to organization-defined personnel or roles.	Windows machines should meet requirements for 'System Audit Policies - Detailed Tracking'	2.0.0
Change Control Procedures	0641.10k2Organizational.11 - 10.k	The organization does not use automated updates on critical systems.	Windows machines should meet requirements for 'System Audit Policies - Detailed Tracking'	2.0.0
Change Control Procedures	0642.10k3Organizational.12 - 10.k	The organization develops, documents, and maintains, under configuration control, a current baseline configuration of the information system, and reviews and updates the baseline as required.	Windows machines should meet requirements for 'System Audit Policies - Detailed Tracking'	2.0.0

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY	POLICY VERSION
Change Control Procedures	0643.10k3Organizational.3 - 10.k	The organization (i) establishes and documents mandatory configuration settings for information technology products employed within the information system using the latest security configuration baselines; (ii) identifies, documents, and approves exceptions from the mandatory established configuration settings for individual components based on explicit operational requirements; and (iii) monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.	Windows machines should meet requirements for 'System Audit Policies - Detailed Tracking'	2.0.0
Change Control Procedures	0644.10k3Organizational.4 - 10.k	The organization employs automated mechanisms to (i) centrally manage, apply, and verify configuration settings; (ii) respond to unauthorized changes to network and system security-related configuration settings; and (iii) enforce access restrictions and auditing of the enforcement actions.	Windows machines should meet requirements for 'System Audit Policies - Detailed Tracking'	2.0.0
Control of Technical Vulnerabilities	0709.10m1Organizational.1 - 10.m	Technical vulnerabilities are identified, evaluated for risk and corrected in a timely manner.	Windows machines should meet requirements for 'Security Options - Microsoft Network Server'	2.0.0

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY	POLICY VERSION
Business Continuity and Risk Assessment	1637.12b2Organizational.2 - 12.b	Business impact analysis are used to evaluate the consequences of disasters, security failures, loss of service, and service availability.	Windows machines should meet requirements for 'Security Options - Recovery console'	2.0.0

IRS 1075 September 2016

To review how the available Azure Policy built-ins for all Azure services map to this compliance standard, see Azure Policy Regulatory Compliance - IRS 1075 September 2016. For more information about this compliance standard, see IRS 1075 September 2016.

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY (AZURE PORTAL)	POLICY VERSION (GITHUB)
Access Control	9.3.1.5	Separation of Duties (AC-5)	Audit Windows machines missing any of specified members in the Administrators group	1.0.0
Access Control	9.3.1.5	Separation of Duties (AC-5)	Audit Windows machines that have the specified members in the Administrators group	1.0.0
Access Control	9.3.1.6	Least Privilege (AC-6)	Audit Windows machines missing any of specified members in the Administrators group	1.0.0
Access Control	9.3.1.6	Least Privilege (AC-6)	Audit Windows machines that have the specified members in the Administrators group	1.0.0
Access Control	9.3.1.12	Remote Access (AC-17)	Audit Linux machines that allow remote connections from accounts without passwords	1.0.0
Identification and Authentication	9.3.7.5	Authenticator Management (IA-5)	Audit Linux machines that do not have the passwd file permissions set to 0644	1.0.0

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY	POLICY VERSION
Identification and Authentication	9.3.7.5	Authenticator Management (IA-5)	Audit Linux machines that have accounts without passwords	1.0.0
Identification and Authentication	9.3.7.5	Authenticator Management (IA-5)	Audit Windows machines that allow re-use of the previous 24 passwords	1.0.0
Identification and Authentication	9.3.7.5	Authenticator Management (IA-5)	Audit Windows machines that do not have a maximum password age of 70 days	1.0.0
Identification and Authentication	9.3.7.5	Authenticator Management (IA-5)	Audit Windows machines that do not have a minimum password age of 1 day	1.0.0
Identification and Authentication	9.3.7.5	Authenticator Management (IA-5)	Audit Windows machines that do not have the password complexity setting enabled	1.0.0
Identification and Authentication	9.3.7.5	Authenticator Management (IA-5)	Audit Windows machines that do not restrict the minimum password length to 14 characters	1.0.0
Identification and Authentication	9.3.7.5	Authenticator Management (IA-5)	Audit Windows machines that do not store passwords using reversible encryption	1.0.0
System and Communications Protection	9.3.16.6	Transmission Confidentiality and Integrity (SC-8)	Windows web servers should be configured to use secure communication protocols	3.0.0

ISO 27001:2013

To review how the available Azure Policy built-ins for all Azure services map to this compliance standard, see Azure Policy Regulatory Compliance - ISO 27001:2013. For more information about this compliance standard, see ISO 27001:2013.

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY (AZURE PORTAL)	POLICY VERSION (GITHUB)
Access control	9.1.2	Access to networks and network services	Audit Linux machines that allow remote connections from accounts without passwords	1.0.0
Access control	9.1.2	Access to networks and network services	Audit Linux machines that have accounts without passwords	1.0.0
Access control	9.2.4	Management of secret authentication information of users	Audit Linux machines that do not have the passwd file permissions set to 0644	1.0.0
Access control	9.4.3	Password management system	Audit Windows machines that allow re-use of the previous 24 passwords	1.0.0
Access control	9.4.3	Password management system	Audit Windows machines that do not have a maximum password age of 70 days	1.0.0
Access control	9.4.3	Password management system	Audit Windows machines that do not have a minimum password age of 1 day	1.0.0
Access control	9.4.3	Password management system	Audit Windows machines that do not have the password complexity setting enabled	1.0.0
Access control	9.4.3	Password management system	Audit Windows machines that do not restrict the minimum password length to 14 characters	1.0.0
Cryptography	10.1.1	Policy on the use of cryptographic controls	Audit Windows machines that do not store passwords using reversible encryption	1.0.0

New Zealand ISM Restricted

To review how the available Azure Policy built-ins for all Azure services map to this compliance standard, see Azure Policy Regulatory Compliance - New Zealand ISM Restricted. For more information about this compliance standard, see New Zealand ISM Restricted.

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY (AZURE PORTAL)	POLICY VERSION (GITHUB)
Information security monitoring	ISM-4	6.2.6 Resolving vulnerabilities	SQL servers on machines should have vulnerability findings resolved	1.0.0
Access Control and Passwords	AC-4	16.1.40 Password selection policy	Audit Linux machines that have accounts without passwords	1.0.0
Access Control and Passwords	AC-4	16.1.40 Password selection policy	Windows machines should meet requirements for 'Security Settings - Account Policies'	2.0.0
Access Control and Passwords	AC-11	16.4.30 Privileged Access Management	Audit Windows machines missing any of specified members in the Administrators group	1.0.0
Access Control and Passwords	AC-11	16.4.30 Privileged Access Management	Audit Windows machines that have extra accounts in the Administrators group	1.0.0
Access Control and Passwords	AC-11	16.4.30 Privileged Access Management	Audit Windows machines that have the specified members in the Administrators group	1.0.0
Access Control and Passwords	AC-13	16.5.10 Authentication	Audit Linux machines that allow remote connections from accounts without passwords	1.0.0
Cryptography	CR-7	17.4.16 Using TLS	Windows web servers should be configured to use secure communication protocols	3.0.0
Cryptography	CR-9	17.5.7 Authentication mechanisms	Authentication to Linux machines should require SSH keys	2.0.1

NIST SP 800-171 R2

To review how the available Azure Policy built-ins for all Azure services map to this compliance standard, see Azure Policy Regulatory Compliance - NIST SP 800-171 R2. For more information about this compliance standard, see NIST SP 800-171 R2.

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY (AZURE PORTAL)	POLICY VERSION (GITHUB)
Access Control	3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	Audit Linux machines that allow remote connections from accounts without passwords	1.0.0
Access Control	3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	Windows machines should meet requirements for 'Security Options - Network Security'	2.0.0
Access Control	3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	Audit Windows machines missing any of specified members in the Administrators group	1.0.0
Access Control	3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	Audit Windows machines that have the specified members in the Administrators group	1.0.0
Access Control	3.1.12	Monitor and control remote access sessions.	Audit Linux machines that allow remote connections from accounts without passwords	1.0.0
Access Control	3.1.12	Monitor and control remote access sessions.	Windows machines should meet requirements for 'Security Options - Network Security'	2.0.0
Identification and Authentication	3.5.2	Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.	Audit Linux machines that have accounts without passwords	1.0.0

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY	POLICY VERSION
Identification and Authentication	3.5.2	Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.	Windows machines should meet requirements for 'Security Options - Network Security'	2.0.0
Identification and Authentication	3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created.	Audit Linux machines that have accounts without passwords	1.0.0
Identification and Authentication	3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created.	Audit Windows machines that do not have the password complexity setting enabled	1.0.0
Identification and Authentication	3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created.	Audit Windows machines that do not restrict the minimum password length to 14 characters	1.0.0
Identification and Authentication	3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created.	Windows machines should meet requirements for 'Security Options - Network Security'	2.0.0
Identification and Authentication	3.5.8	Prohibit password reuse for a specified number of generations.	Audit Windows machines that allow re-use of the previous 24 passwords	1.0.0
Identification and Authentication	3.5.8	Prohibit password reuse for a specified number of generations.	Windows machines should meet requirements for 'Security Options - Network Security'	2.0.0
Identification and Authentication	3.5.10	Store and transmit only cryptographically-protected passwords.	Audit Linux machines that do not have the passwd file permissions set to 0644	1.0.0

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY	POLICY VERSION
Identification and Authentication	3.5.10	Store and transmit only cryptographically-protected passwords.	Audit Windows machines that do not store passwords using reversible encryption	1.0.0
Identification and Authentication	3.5.10	Store and transmit only cryptographically-protected passwords.	Windows machines should meet requirements for 'Security Options - Network Security'	2.0.0
System and Communications Protection	3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	Windows web servers should be configured to use secure communication protocols	3.0.0
System and Communications Protection	3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	Windows web servers should be configured to use secure communication protocols	3.0.0

NIST SP 800-53 Rev. 4

To review how the available Azure Policy built-ins for all Azure services map to this compliance standard, see Azure Policy Regulatory Compliance - NIST SP 800-53 Rev. 4. For more information about this compliance standard, see NIST SP 800-53 Rev. 4.

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY (AZURE PORTAL)	POLICY VERSION (GITHUB)
Access Control	AC-3	Access Enforcement	Audit Linux machines that have accounts without passwords	1.0.0
Access Control	AC-3	Access Enforcement	Authentication to Linux machines should require SSH keys	2.0.1

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY	POLICY VERSION
Access Control	AC-17	Remote Access	Audit Linux machines that allow remote connections from accounts without passwords	1.0.0
Access Control	AC-17 (1)	Automated Monitoring / Control	Audit Linux machines that allow remote connections from accounts without passwords	1.0.0
Audit and Accountability	AU-6 (4)	Central Review and Analysis	Log Analytics agent should be installed on your Linux Azure Arc machines	1.0.0-preview
Audit and Accountability	AU-6 (4)	Central Review and Analysis	Log Analytics agent should be installed on your Windows Azure Arc machines	1.0.0-preview
Audit and Accountability	AU-6 (5)	Integration / Scanning and Monitoring Capabilities	Log Analytics agent should be installed on your Linux Azure Arc machines	1.0.0-preview
Audit and Accountability	AU-6 (5)	Integration / Scanning and Monitoring Capabilities	Log Analytics agent should be installed on your Windows Azure Arc machines	1.0.0-preview
Audit and Accountability	AU-12	Audit Generation	Log Analytics agent should be installed on your Linux Azure Arc machines	1.0.0-preview
Audit and Accountability	AU-12	Audit Generation	Log Analytics agent should be installed on your Windows Azure Arc machines	1.0.0-preview
Audit and Accountability	AU-12 (1)	System-wide / Time-correlated Audit Trail	Log Analytics agent should be installed on your Linux Azure Arc machines	1.0.0-preview
Audit and Accountability	AU-12 (1)	System-wide / Time-correlated Audit Trail	Log Analytics agent should be installed on your Windows Azure Arc machines	1.0.0-preview

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY	POLICY VERSION
Configuration Management	CM-6	Configuration Settings	Linux machines should meet requirements for the Azure compute security baseline	1.1.1-preview
Configuration Management	CM-6	Configuration Settings	Windows machines should meet requirements of the Azure compute security baseline	1.0.1-preview
Identification and Authentication	IA-5	Authenticator Management	Audit Linux machines that do not have the passwd file permissions set to 0644	1.0.0
Identification and Authentication	IA-5	Authenticator Management	Audit Windows machines that do not store passwords using reversible encryption	1.0.0
Identification and Authentication	IA-5	Authenticator Management	Authentication to Linux machines should require SSH keys	2.0.1
Identification and Authentication	IA-5 (1)	Password-based Authentication	Audit Linux machines that do not have the passwd file permissions set to 0644	1.0.0
Identification and Authentication	IA-5 (1)	Password-based Authentication	Audit Windows machines that allow re-use of the previous 24 passwords	1.0.0
Identification and Authentication	IA-5 (1)	Password-based Authentication	Audit Windows machines that do not have a maximum password age of 70 days	1.0.0
Identification and Authentication	IA-5 (1)	Password-based Authentication	Audit Windows machines that do not have a minimum password age of 1 day	1.0.0

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY	POLICY VERSION
Identification and Authentication	IA-5 (1)	Password-based Authentication	Audit Windows machines that do not have the password complexity setting enabled	1.0.0
Identification and Authentication	IA-5 (1)	Password-based Authentication	Audit Windows machines that do not restrict the minimum password length to 14 characters	1.0.0
Identification and Authentication	IA-5 (1)	Password-based Authentication	Audit Windows machines that do not store passwords using reversible encryption	1.0.0
Risk Assessment	RA-5	Vulnerability Scanning	SQL servers on machines should have vulnerability findings resolved	1.0.0
System and Communications Protection	SC-3	Security Function Isolation	Windows Defender Exploit Guard should be enabled on your machines	1.1.1
System and Communications Protection	SC-8	Transmission Confidentiality and Integrity	Windows web servers should be configured to use secure communication protocols	3.0.0
System and Communications Protection	SC-8 (1)	Cryptographic or Alternate Physical Protection	Windows web servers should be configured to use secure communication protocols	3.0.0
System and Information Integrity	SI-3	Malicious Code Protection	Windows Defender Exploit Guard should be enabled on your machines	1.1.1
System and Information Integrity	SI-3 (1)	Central Management	Windows Defender Exploit Guard should be enabled on your machines	1.1.1
System and Information Integrity	SI-4	Information System Monitoring	Log Analytics agent should be installed on your Linux Azure Arc machines	1.0.0-preview

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY	POLICY VERSION
System and Information Integrity	SI-4	Information System Monitoring	Log Analytics agent should be installed on your Windows Azure Arc machines	1.0.0-preview
System and Information Integrity	SI-16	Memory Protection	Windows Defender Exploit Guard should be enabled on your machines	1.1.1

NIST SP 800-53 Rev. 5

To review how the available Azure Policy built-ins for all Azure services map to this compliance standard, see Azure Policy Regulatory Compliance - NIST SP 800-53 Rev. 5. For more information about this compliance standard, see NIST SP 800-53 Rev. 5.

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY (AZURE PORTAL)	POLICY VERSION (GITHUB)
Access Control	AC-3	Access Enforcement	Audit Linux machines that have accounts without passwords	1.0.0
Access Control	AC-3	Access Enforcement	Authentication to Linux machines should require SSH keys	2.0.1
Access Control	AC-17	Remote Access	Audit Linux machines that allow remote connections from accounts without passwords	1.0.0
Access Control	AC-17 (1)	Monitoring and Control	Audit Linux machines that allow remote connections from accounts without passwords	1.0.0
Audit and Accountability	AU-6 (4)	Central Review and Analysis	Log Analytics agent should be installed on your Linux Azure Arc machines	1.0.0-preview
Audit and Accountability	AU-6 (4)	Central Review and Analysis	Log Analytics agent should be installed on your Windows Azure Arc machines	1.0.0-preview
Audit and Accountability	AU-6 (5)	Integrated Analysis of Audit Records	Log Analytics agent should be installed on your Linux Azure Arc machines	1.0.0-preview

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY	POLICY VERSION
Audit and Accountability	AU-6 (5)	Integrated Analysis of Audit Records	Log Analytics agent should be installed on your Windows Azure Arc machines	1.0.0-preview
Audit and Accountability	AU-12	Audit Record Generation	Log Analytics agent should be installed on your Linux Azure Arc machines	1.0.0-preview
Audit and Accountability	AU-12	Audit Record Generation	Log Analytics agent should be installed on your Windows Azure Arc machines	1.0.0-preview
Audit and Accountability	AU-12 (1)	System-wide and Time-correlated Audit Trail	Log Analytics agent should be installed on your Linux Azure Arc machines	1.0.0-preview
Audit and Accountability	AU-12 (1)	System-wide and Time-correlated Audit Trail	Log Analytics agent should be installed on your Windows Azure Arc machines	1.0.0-preview
Configuration Management	CM-6	Configuration Settings	Linux machines should meet requirements for the Azure compute security baseline	1.1.1-preview
Configuration Management	CM-6	Configuration Settings	Windows machines should meet requirements of the Azure compute security baseline	1.0.1-preview
Identification and Authentication	IA-5	Authenticator Management	Audit Linux machines that do not have the passwd file permissions set to 0644	1.0.0
Identification and Authentication	IA-5	Authenticator Management	Audit Windows machines that do not store passwords using reversible encryption	1.0.0
Identification and Authentication	IA-5	Authenticator Management	Authentication to Linux machines should require SSH keys	2.0.1

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY	POLICY VERSION
Identification and Authentication	IA-5 (1)	Password-based Authentication	Audit Linux machines that do not have the passwd file permissions set to 0644	1.0.0
Identification and Authentication	IA-5 (1)	Password-based Authentication	Audit Windows machines that allow re-use of the previous 24 passwords	1.0.0
Identification and Authentication	IA-5 (1)	Password-based Authentication	Audit Windows machines that do not have a maximum password age of 70 days	1.0.0
Identification and Authentication	IA-5 (1)	Password-based Authentication	Audit Windows machines that do not have a minimum password age of 1 day	1.0.0
Identification and Authentication	IA-5 (1)	Password-based Authentication	Audit Windows machines that do not have the password complexity setting enabled	1.0.0
Identification and Authentication	IA-5 (1)	Password-based Authentication	Audit Windows machines that do not restrict the minimum password length to 14 characters	1.0.0
Identification and Authentication	IA-5 (1)	Password-based Authentication	Audit Windows machines that do not store passwords using reversible encryption	1.0.0
Risk Assessment	RA-5	Vulnerability Monitoring and Scanning	SQL servers on machines should have vulnerability findings resolved	1.0.0
System and Communications Protection	SC-3	Security Function Isolation	Windows Defender Exploit Guard should be enabled on your machines	1.1.1

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY	POLICY VERSION
System and Communications Protection	SC-8	Transmission Confidentiality and Integrity	Windows web servers should be configured to use secure communication protocols	3.0.0
System and Communications Protection	SC-8 (1)	Cryptographic Protection	Windows web servers should be configured to use secure communication protocols	3.0.0
System and Information Integrity	SI-3	Malicious Code Protection	Windows Defender Exploit Guard should be enabled on your machines	1.1.1
System and Information Integrity	SI-4	System Monitoring	Log Analytics agent should be installed on your Linux Azure Arc machines	1.0.0-preview
System and Information Integrity	SI-4	System Monitoring	Log Analytics agent should be installed on your Windows Azure Arc machines	1.0.0-preview
System and Information Integrity	SI-16	Memory Protection	Windows Defender Exploit Guard should be enabled on your machines	1.1.1

UK OFFICIAL and UK NHS

To review how the available Azure Policy built-ins for all Azure services map to this compliance standard, see Azure Policy Regulatory Compliance - UK OFFICIAL and UK NHS. For more information about this compliance standard, see UK OFFICIAL.

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY (AZURE PORTAL)	POLICY VERSION (GITHUB)
Data in transit protection	1	Data in transit protection	Windows web servers should be configured to use secure communication protocols	3.0.0
Identity and authentication	10	Identity and authentication	Audit Linux machines that allow remote connections from accounts without passwords	1.0.0

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY	POLICY VERSION
Identity and authentication	10	Identity and authentication	Audit Linux machines that do not have the passwd file permissions set to 0644	1.0.0
Identity and authentication	10	Identity and authentication	Audit Linux machines that have accounts without passwords	1.0.0
Identity and authentication	10	Identity and authentication	Audit Windows machines that allow re-use of the previous 24 passwords	1.0.0
Identity and authentication	10	Identity and authentication	Audit Windows machines that do not have a maximum password age of 70 days	1.0.0
Identity and authentication	10	Identity and authentication	Audit Windows machines that do not have a minimum password age of 1 day	1.0.0
Identity and authentication	10	Identity and authentication	Audit Windows machines that do not have the password complexity setting enabled	1.0.0
Identity and authentication	10	Identity and authentication	Audit Windows machines that do not restrict the minimum password length to 14 characters	1.0.0

Next steps

- Learn more about Azure Policy Regulatory Compliance.
- See the built-ins on the Azure Policy GitHub repo.

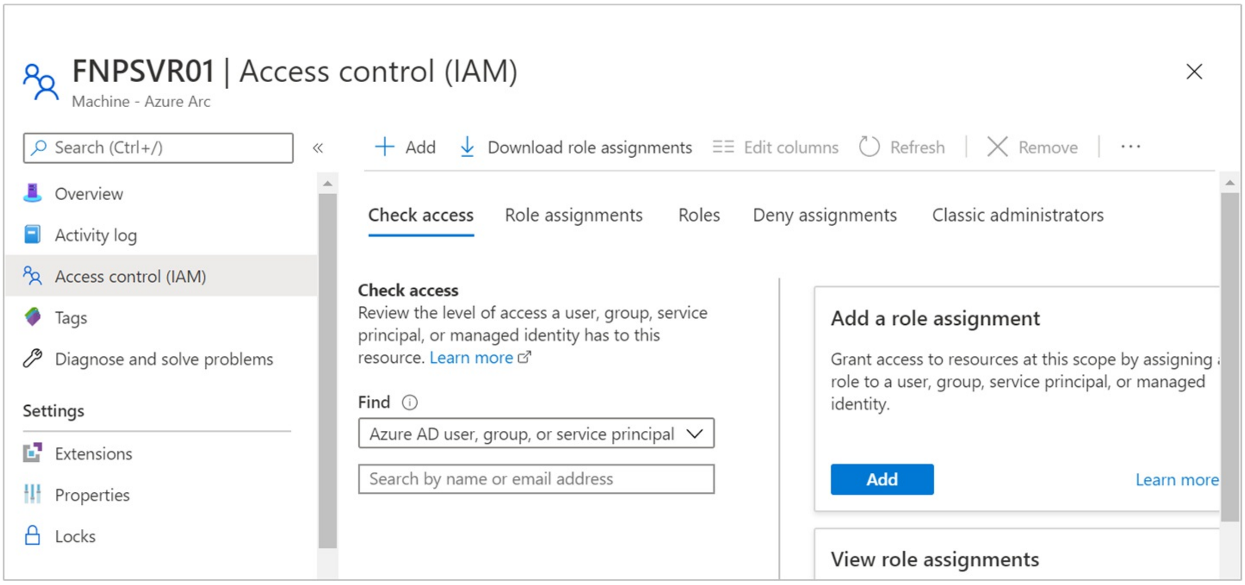
Azure Arc for servers security overview

9/7/2021 • 4 minutes to read • Edit Online

This article describes the security configuration and considerations you should evaluate before deploying Azure Arc-enabled servers in your enterprise.

Identity and access control

Each Azure Arc-enabled server has a managed identity as part of a resource group inside an Azure subscription. That identity represents the server running on-premises or other cloud environment. 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-enabled server.



Check access

Review the level of access a user, group, service principal, or managed identity has to this resource. Learn more

Add a role assignment

Grant access to resources at this scope by assigning a role to a user, group, service principal, or managed identity.

Users and applications granted contributor or administrator role access to the resource can make changes to the resource, including deploying or deleting extensions on the machine. Extensions can include arbitrary scripts that run in a privileged context, so consider any contributor on the Azure resource to be an indirect administrator of the server.

The **Azure Connected Machine Onboarding** role is available for at-scale onboarding, and is only able to read or create new Azure Arc-enabled servers in Azure. It cannot be used to delete servers already registered or manage extensions. As a best practice, we recommend only assigning this role to the Azure Active Directory (Azure AD) service principal used to onboard machines at scale.

Users as a member of the **Azure Connected Machine Resource Administrator** role can read, modify, reonboard, and delete a machine. This role is designed to support management of Azure Arc-enabled servers, but not other resources in the resource group or subscription.

Agent security and permissions

To manage the Azure Connected Machine agent (azcmagent) on Windows, your user account needs to be a member of the local Administrators group. On Linux, you must have root access permissions.

The Azure Connected Machine agent is composed of three services, which run on your machine.

- The Hybrid Instance Metadata Service (himds) service is responsible for all core functionality of Arc. This includes sending heartbeats to Azure, exposing a local instance metadata service for other apps to learn about the machine's Azure resource ID, and retrieve Azure AD tokens to authenticate to other Azure services. This service runs as an unprivileged virtual service account on Windows, and as the **himds** user on Linux.

- The Guest Configuration service (GCService) is responsible for evaluating Azure Policy on the machine.
- The Guest Configuration Extension service (ExtensionService) is responsible for installing, updating, and deleting extensions (agents, scripts, or other software) on the machine.

The guest configuration and extension services run as Local System on Windows, and as root on Linux.

Using a managed identity with Azure Arc-enabled servers

By default, the Azure Active Directory system assigned identity used by Arc can only be used to update the status of the Azure Arc-enabled server in Azure. For example, the *last seen* heartbeat status. You can optionally assign other roles to the identity if an application on your server uses the system assigned identity to access other Azure services. To learn more about configuring a system-assigned managed identity to access Azure resources, see Authenticate against Azure resources with Azure Arc-enabled servers.

While the Hybrid Instance Metadata Service can be accessed by any application running on the machine, only authorized applications can request an Azure AD token for the system assigned identity. On the first attempt to access the token URI, the service will generate a randomly generated cryptographic blob in a location on the file system that only trusted callers can read. The caller must then read the file (proving it has appropriate permission) and retry the request with the file contents in the authorization header to successfully retrieve an Azure AD token.

- On Windows, the caller must be a member of the local **Administrators** group or the **Hybrid Agent Extension Applications** group to read the blob.
- On Linux, the caller must be a member of the **himds** group to read the blob.

To learn more about using a managed identity with Arc-enabled servers to authenticate and access Azure resources, see the following video.

Using disk encryption

The Azure Connected Machine agent uses public key authentication to communicate with the Azure service. After you onboard a server to Azure Arc, a private key is saved to the disk and used whenever the agent communicates with Azure. If stolen, the private key can be used on another server to communicate with the service and act as if it were the original server. This includes getting access to the system assigned identity and any resources that identity has access to. The private key file is protected to only allow the **himds** account access to read it. To prevent offline attacks, we strongly recommend the use of full disk encryption (for example, BitLocker, dm-crypt, etc.) on the operating system volume of your server.

Next steps

- Before evaluating or enabling Azure Arc-enabled servers across multiple hybrid machines, review Connected Machine agent overview to understand requirements, technical details about the agent, and deployment methods.
- Review the Planning and deployment guide to plan for deploying Azure Arc-enabled servers at any scale and implement centralized management and monitoring.

Use Azure Private Link to securely connect networks to Azure Arc

9/7/2021 • 15 minutes to read • Edit Online

Azure Private Link allows you to securely link Azure PaaS services to your virtual network using private endpoints. For many services, you just set up an endpoint per resource. This means you can connect your on-premises or multi-cloud servers with Azure Arc and send all traffic over an Azure ExpressRoute or site-to-site VPN connection instead of using public networks.

Starting with Azure Arc-enabled servers, you can use a Private Link Scope model to allow multiple servers or machines to communicate with their Azure Arc resources using a single private endpoint.

This article covers when to use and how to set up an Azure Arc Private Link Scope (preview).

> **NOTE**
>
> Azure Arc Private Link Scope (preview) is available in all commercial cloud regions, it is not available in the US Government cloud today.

Advantages

With Private Link you can:

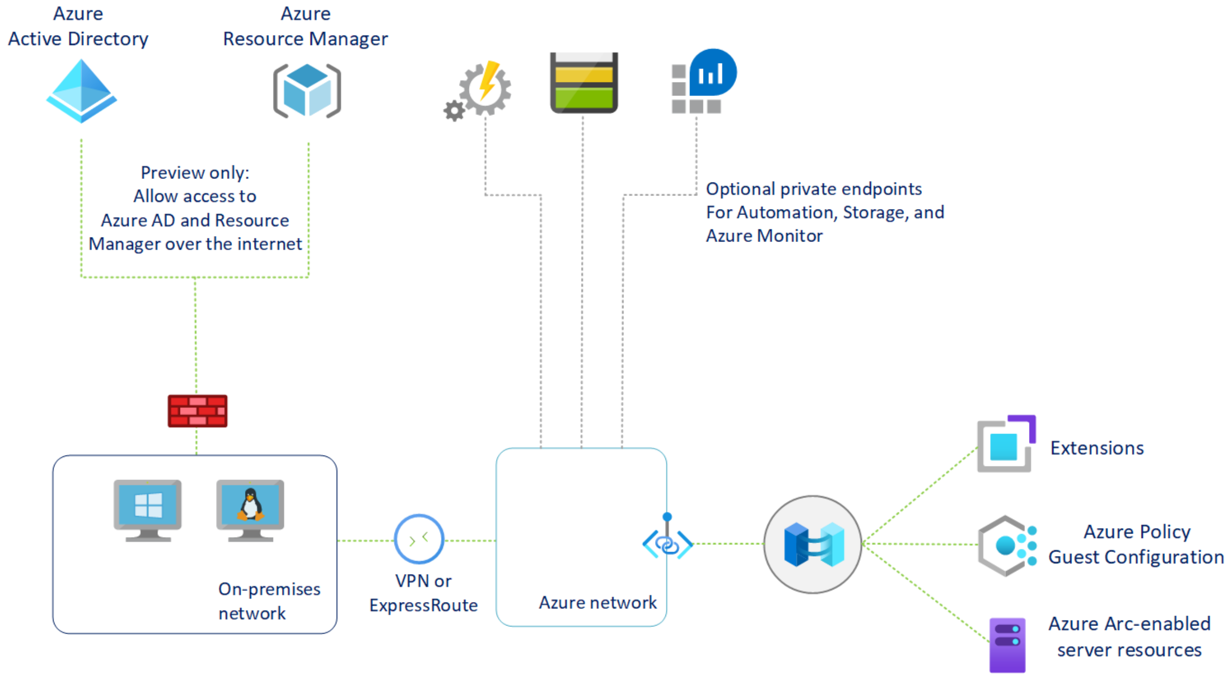
- Connect privately to Azure Arc without opening up any public network access.
- Ensure data from the Azure Arc-enabled machine or server is only accessed through authorized private networks. This also includes data from VM extensions installed on the machine or server that provide post-deployment management and monitoring support.
- Prevent data exfiltration from your private networks by defining specific Azure Arc-enabled servers and other Azure services resources, such as Azure Monitor, that connects through your private endpoint.
- Securely connect your private on-premises network to Azure Arc using ExpressRoute and Private Link.
- Keep all traffic inside the Microsoft Azure backbone network.

For more information, see Key Benefits of Private Link.

How it works

Azure Arc Private Link Scope (preview) connects private endpoints (and the virtual networks they're contained in) to an Azure resource, in this case Azure Arc-enabled servers. When you enable any one of the Azure Arc-enabled servers supported VM extensions, such as Azure Automation Update Management or Azure Monitor, those resources connect other Azure resources. Such as:

- Log Analytics workspace, required for Azure Automation Update Management, Azure Automation Change Tracking and Inventory, Azure Monitor VM insights, and Azure Monitor log collection with Log Analytics agent.
- Azure Automation account, required for Update Management and Change Tracking and Inventory.
- Azure Key Vault
- Azure Blob storage, required for Custom Script Extension.



Connectivity to the other Azure resources from an Azure Arc-enabled server listed earlier require configuring Private Link for each service. For more information, see the following to configure Private Link for Azure Automation, Azure Monitor, Azure Key Vault, or Azure Blob storage.

> **IMPORTANT**
>
> Azure Private Link is now generally available. Both Private Endpoint and Private Link service (service behind standard load balancer) are generally available. Different Azure PaaS will onboard to Azure Private Link at different schedules. See Private Link availability for an accurate status of Azure PaaS on Private Link. For known limitations, see Private Endpoint and Private Link Service.

- The Private Endpoint on your VNet allows it to reach Azure Arc-enabled servers endpoints through private IPs from your network's pool, instead of using to the public IPs of these endpoints. That allows you to keep using your Azure Arc-enabled servers resource without opening your VNet to outbound traffic not requested.
- Traffic from the Private Endpoint to your resources will go over the Microsoft Azure backbone, and not routed to public networks.
- You can configure each of your components to allow or deny ingestion and queries from public networks. That provides a resource-level protection, so that you can control traffic to specific resources.

Restrictions and limitations

The Azure Arc-enabled servers Private Link Scope object has a number of limits you should consider when planning your Private Link setup.

- You can associate at most one Azure Arc Private Link Scope with a virtual network.
- An Azure Arc-enabled machine or server resource can only connect to one Azure Arc-enabled servers Private Link Scope.
- All on-premises machines need to use the same private endpoint by resolving the correct private endpoint information (FQDN record name and private IP address) using the same DNS forwarder. For more information, see Azure Private Endpoint DNS configuration
- The Azure Arc-enabled machine or server, Azure Arc Private Link Scope, and virtual network must be in

the same Azure region.

- Traffic to Azure Active Directory and Azure Resource Manager service tags must be allowed through your on-premises network firewall during the preview.
- Other Azure services that you will use, for example Azure Monitor, requires their own private endpoints in your virtual network.
- Azure Arc-enabled servers Private Link Scope is not currently available in Azure US Government regions.

Planning your Private Link setup

To connect your server to Azure Arc over a private link, you need to configure your network to accomplish the following:

1. Establish a connection between your on-premises network and an Azure virtual network using a site-to-site VPN or ExpressRoute circuit.
2. Deploy an Azure Arc Private Link Scope (preview), which controls which machines or servers can communicate with Azure Arc over private endpoints and associate it with your Azure virtual network using a private endpoint.
3. Update the DNS configuration on your local network to resolve the private endpoint addresses.
4. Configure your local firewall to allow access to Azure Active Directory and Azure Resource Manager. This is a temporary step and will not be required when private endpoints for these services enter preview.
5. Associate the machines or servers registered with Azure Arc-enabled servers with the private link scope.
6. Optionally, deploy private endpoints for other Azure services your machine or server is managed by, such as:
   - Azure Monitor
   - Azure Automation
   - Azure Blob storage
   - Azure Key Vault

This article assumes you have already set up your ExpressRoute circuit or site-to-site VPN connection.

Network configuration

Azure Arc-enabled servers integrates with several Azure services to bring cloud management and governance to your hybrid machines or servers. Most of these services already offer private endpoints, but you need to configure your firewall and routing rules to allow access to Azure Active Directory and Azure Resource Manager over the internet until these services offer private endpoints.

There are two ways you can achieve this:

- If your network is configured to route all internet-bound traffic through the Azure VPN or ExpressRoute circuit, you can configure the network security group (NSG) associated with your subnet in Azure to allow outbound TCP 443 (HTTPS) access to Azure AD and Azure using service tags. The NSG rules should look like the following:

SETTING	AZURE AD RULE	AZURE RULE
Source	Virtual network	Virtual network

SETTING	AZURE AD RULE	AZURE RULE
Source port ranges	*	*
Destination	Service Tag	Service Tag
Destination service tag	AzureActiveDirectory	AzureResourceManager
Destination port ranges	443	443
Protocol	Tcp	Tcp
Action	Allow	Allow
Priority	150 (must be lower than any rules that block internet access)	151 (must be lower than any rules that block internet access)
Name	AllowAADOutboundAccess	AllowAzOutboundAccess

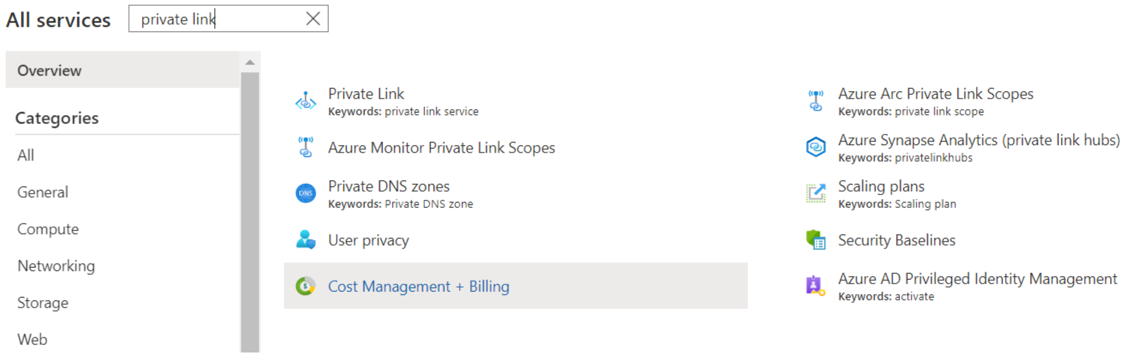
- Configure the firewall on your local network to allow outbound TCP 443 (HTTPS) access to Azure AD and Azure using the downloadable service tag files. The JSON file contains all the public IP address ranges used by Azure AD and Azure and is updated monthly to reflect any changes. Azure ADs service tag is `AzureActiveDirectory` and Azure's service tag is `AzureResourceManager`. Consult with your network administrator and network firewall vendor to learn how to configure your firewall rules.

See the visual diagram under the section How it works for the network traffic flows.

Create a Private Link Scope

1. Sign in to the Azure portal.

2. Go to **Create a resource** in the Azure portal and search for **Azure Arc Private Link Scope**. Or you can use the following link to open the Azure Arc Private Link Scope page in the portal.


All services
private link
Overview
Categories
All
General
Compute
Networking
Storage
Web
Private Link
Keywords: private link service
Azure Monitor Private Link Scopes
Private DNS zones
Keywords: Private DNS zone
User privacy
Cost Management + Billing
Azure Arc Private Link Scopes
Keywords: private link scope
Azure Synapse Analytics (private link hubs)
Keywords: privatelinkhubs
Scaling plans
Keywords: Scaling plan
Security Baselines
Azure AD Privileged Identity Management
Keywords: activate

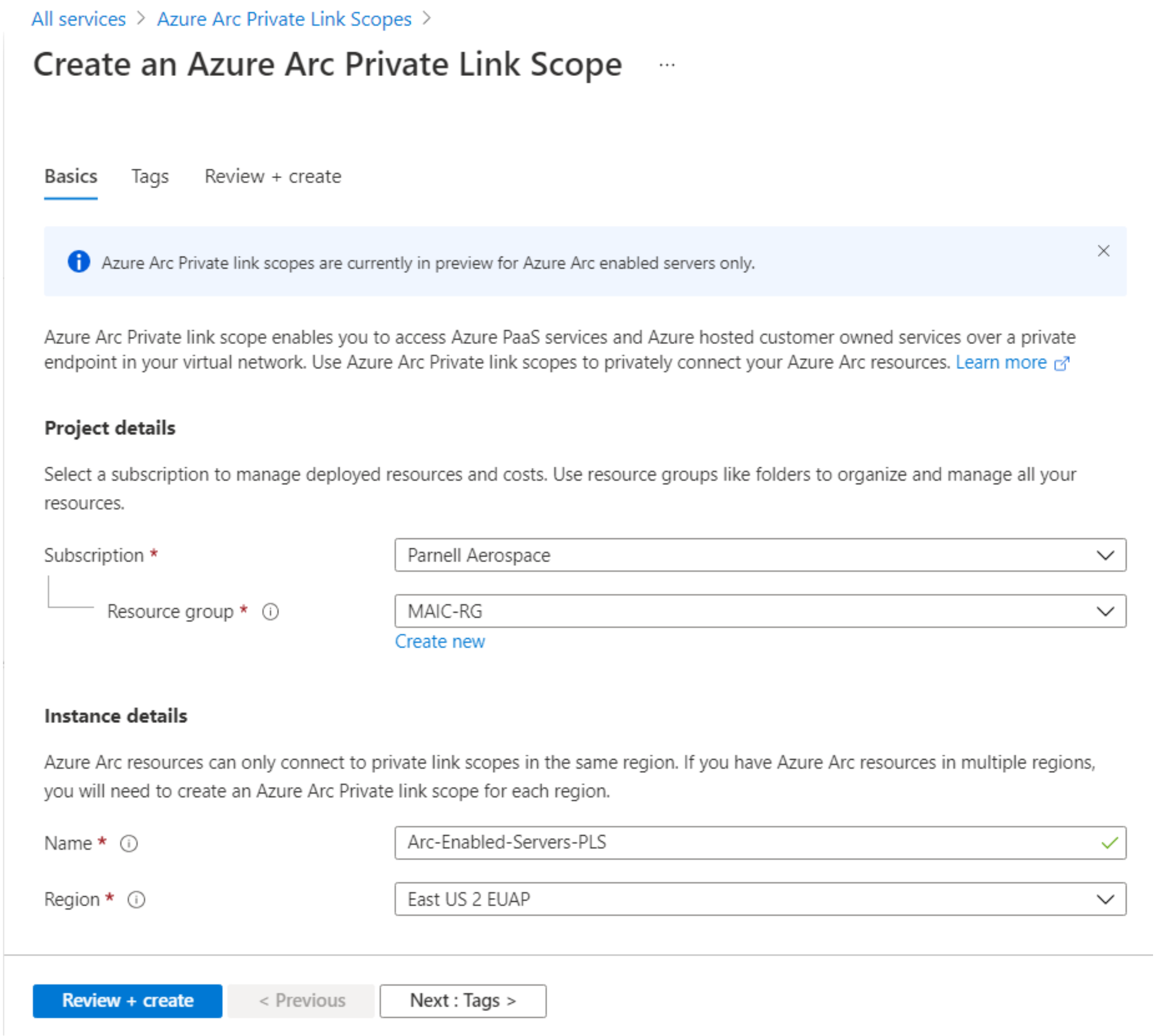
3. Select **Create**.

4. Pick a Subscription and Resource Group. During the preview, your virtual network and Azure Arc-enabled servers must be in the same subscription as the Azure Arc Private Link Scope.

5. Give the Azure Arc Private Link Scope a name. It's best to use a meaningful and clear name.

   You can optionally require every Azure Arc-enabled machine or server associated with this Azure Arc Private Link Scope (preview) to send data to the service through the private endpoint. If you select **Enable public network access**, machines or servers associated with this Azure Arc Private Link Scope (preview) can communicate with the service over both private or public networks. You can change this setting after creating the scope if you change your mind.

6. Select **Review + Create**.



All services > Azure Arc Private Link Scopes >

Create an Azure Arc Private Link Scope ...

Basics | Tags | Review + create

Azure Arc Private link scopes are currently in preview for Azure Arc enabled servers only.

Azure Arc Private link scope enables you to access Azure PaaS services and Azure hosted customer owned services over a private endpoint in your virtual network. Use Azure Arc Private link scopes to privately connect your Azure Arc resources. Learn more

Project details

Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *: Parnell Aerospace

Resource group *: MAIC-RG

Create new

Instance details

Azure Arc resources can only connect to private link scopes in the same region. If you have Azure Arc resources in multiple regions, you will need to create an Azure Arc Private link scope for each region.

Name *: Arc-Enabled-Servers-PLS ✓

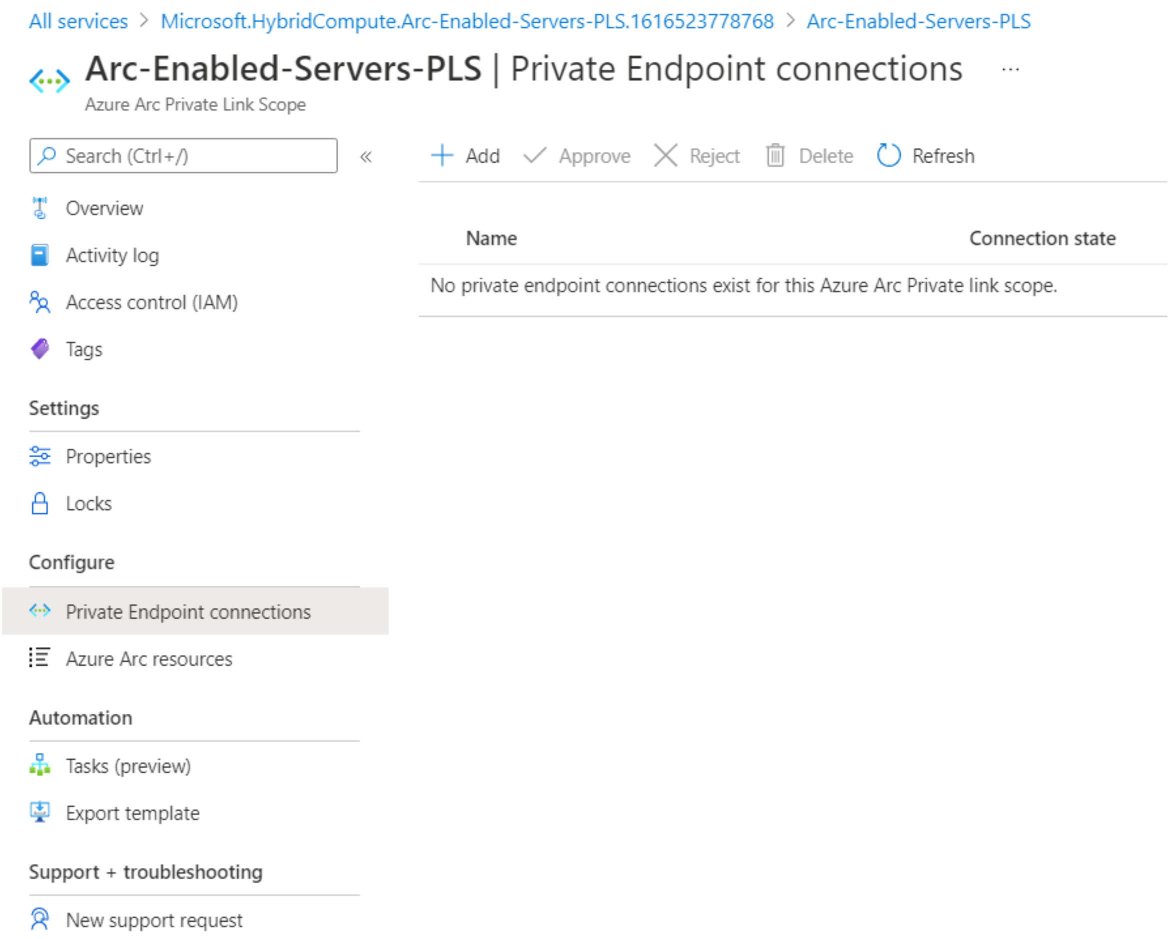
Region *: East US 2 EUAP

7. Let the validation pass, and then select **Create**.

Create a private endpoint

Once your Azure Arc Private Link Scope (preview) is created, you need to connect it with one or more virtual networks using a private endpoint. The private endpoint exposes access to the Azure Arc services on a private IP in your virtual network address space.

1. In your scope resource, select **Private Endpoint connections** in the left-hand resource menu. Select **Add** to start the endpoint create process. You can also approve connections that were started in the Private Link center here by selecting them and selecting **Approve**.


All services > Microsoft.HybridCompute.Arc-Enabled-Servers-PLS.1616523778768 > Arc-Enabled-Servers-PLS
Arc-Enabled-Servers-PLS | Private Endpoint connections
Azure Arc Private Link Scope
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Settings
Properties
Locks
Configure
Private Endpoint connections
Azure Arc resources
Automation
Tasks (preview)
Export template
Support + troubleshooting
New support request
Add
Approve
Reject
Delete
Refresh

Name	Connection state
No private endpoint connections exist for this Azure Arc Private link scope.	

2. Pick the subscription, resource group, and name of the endpoint, and the region it should live in. The region needs to be the same region as the VNet you connect it to.

3. Select **Next: Resource**.

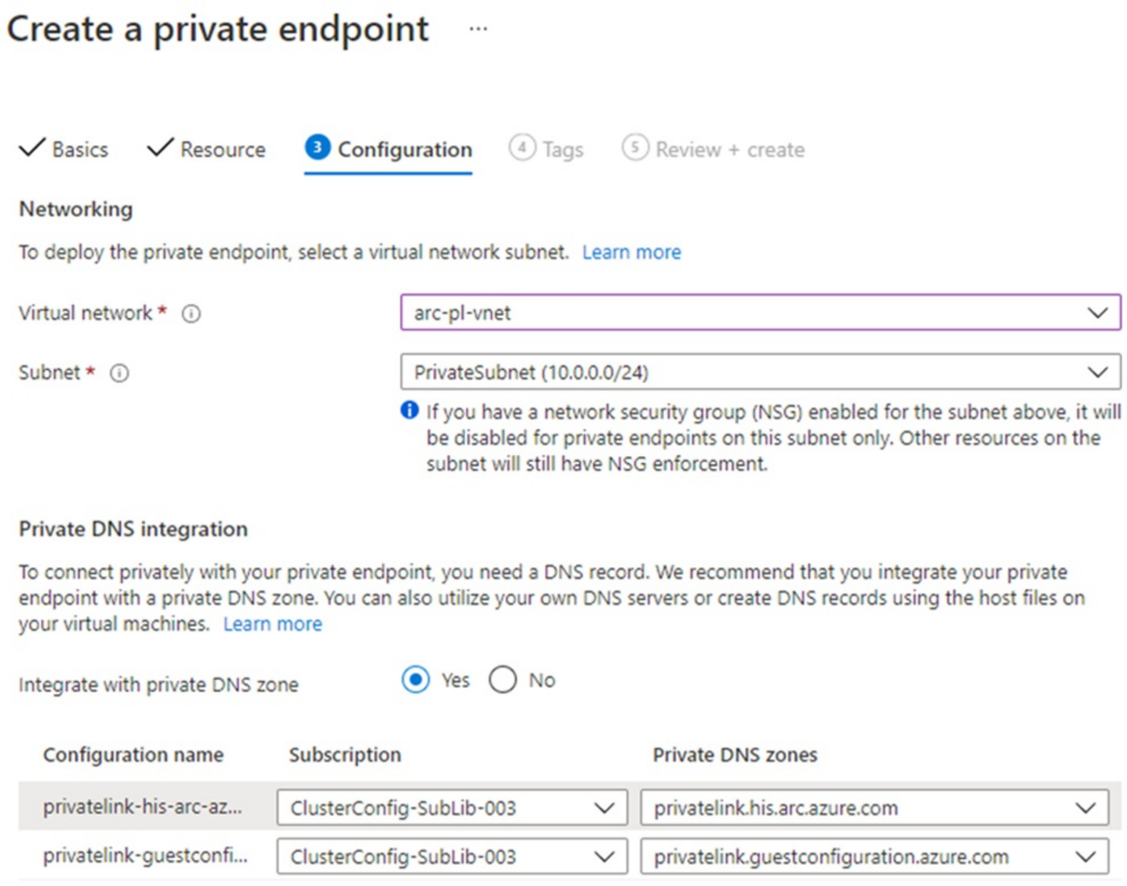
4. On the **Resource** page,

   a. Pick the **Subscription** that contains your Azure Arc Private Link Scope resource.

   b. For **Resource type**, choose **Microsoft.HybridCompute/privateLinkScopes**.

   c. From the **Resource** drop-down, choose your Private Link scope you created earlier.

   d. Select **Next: Configuration >**.



Create a private endpoint ...

✓ Basics ✓ Resource ③ Configuration ④ Tags ⑤ Review + create

Networking

To deploy the private endpoint, select a virtual network subnet. Learn more

Virtual network * ⓘ: arc-pl-vnet

Subnet * ⓘ: PrivateSubnet (10.0.0.0/24)

ℹ If you have a network security group (NSG) enabled for the subnet above, it will be disabled for private endpoints on this subnet only. Other resources on the subnet will still have NSG enforcement.

Private DNS integration

To connect privately with your private endpoint, you need a DNS record. We recommend that you integrate your private endpoint with a private DNS zone. You can also utilize your own DNS servers or create DNS records using the host files on your virtual machines. Learn more

Integrate with private DNS zone ● Yes ○ No

Configuration name	Subscription	Private DNS zones
privatelink-his-arc-az...	ClusterConfig-SubLib-003	privatelink.his.arc.azure.com
privatelink-guestconfi...	ClusterConfig-SubLib-003	privatelink.guestconfiguration.azure.com

5. On the **Configuration** page,

a. Choose the **virtual network** and **subnet** that you want to connect to your Azure Monitor resources.

b. Choose **Yes** for **Integrate with private DNS zone**, and let it automatically create a new Private DNS Zone. The actual DNS zones may be different from what is shown in the screenshot below.

> **NOTE**
>
> If you choose **No** and prefer to manage DNS records manually, first complete setting up your Private Link - including this Private Endpoint and the Private Scope configuration. Then, configure your DNS according to the instructions in Azure Private Endpoint DNS configuration. Make sure not to create empty records as preparation for your Private Link setup. The DNS records you create can override existing settings and impact your connectivity with Azure Arc-enabled servers.

c. Select **Review + create**.

d. Let validation pass.

e. Select **Create**.

Configure on-premises DNS forwarding

Your on-premises machines or servers need to be able to resolve the private link DNS records to the private endpoint IP addresses. How you configure this depends on whether you're using Azure private DNS zones to maintain DNS records, or if you're using your own DNS server on-premises and how many servers you're configuring.

DNS configuration using Azure-integrated private DNS zones

If you set up private DNS zones for Azure Arc-enabled servers and Guest Configuration when creating the private endpoint, your on-premises machines or servers need to be able to forward DNS queries to the built-in

Azure DNS servers to resolve the private endpoint addresses correctly. You need a DNS forwarder in Azure (either a purpose-built VM or an Azure Firewall instance with DNS proxy enabled), after which you can configure your on-premises DNS server to forward queries to Azure to resolve private endpoint IP addresses.

The private endpoint documentation provides guidance for configuring on-premises workloads using a DNS forwarder.

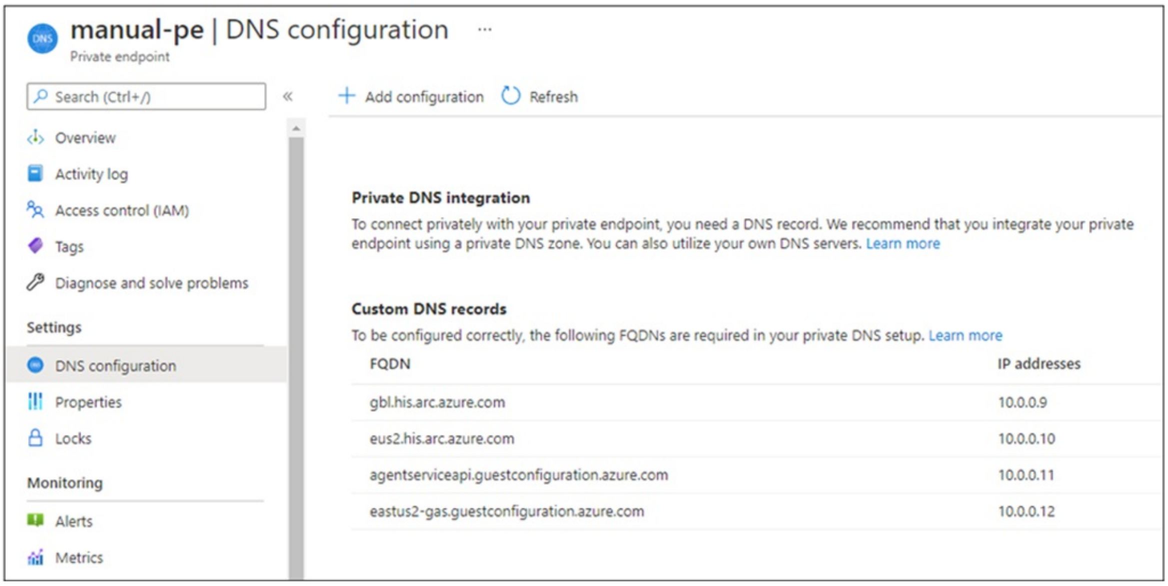
Manual DNS server configuration

If you opted out of using Azure private DNS zones during private endpoint creation, you will need to create the required DNS records in your on-premises DNS server.

1. Go to the Azure portal.

2. Navigate to the private endpoint resource associated with your virtual network and private link scope.

3. From the left-hand pane, select **DNS configuration** to see a list of the DNS records and corresponding IP addresses you'll need to set up on your DNS server. The FQDNs and IP addresses will change based on the region you selected for your private endpoint and the available IP addresses in your subnet.



Private DNS integration

To connect privately with your private endpoint, you need a DNS record. We recommend that you integrate your private endpoint using a private DNS zone. You can also utilize your own DNS servers. Learn more

Custom DNS records

To be configured correctly, the following FQDNs are required in your private DNS setup. Learn more

FQDN	IP addresses
gbl.his.arc.azure.com	10.0.0.9
eus2.his.arc.azure.com	10.0.0.10
agentserviceapi.guestconfiguration.azure.com	10.0.0.11
eastus2-gas.guestconfiguration.azure.com	10.0.0.12

4. Follow the guidance from your DNS server vendor to add the necessary DNS zones and A records to match the table in the portal. Ensure that you select a DNS server that is appropriately scoped for your network. Every machine or server that uses this DNS server now resolves the private endpoint IP addresses and must be associated with the Azure Arc Private Link Scope (preview), or the connection will be refused.

Single server scenarios

If you're only planning to use Private Links to support a few machines or servers, you may not want to update your entire network's DNS configuration. In this case, you can add the private endpoint hostnames and IP addresses to your operating systems **Hosts** file. Depending on the OS configuration, the Hosts file can be the primary or alternative method for resolving hostname to IP address.

Windows

1. Using an account with administrator privileges, open **C:\Windows\System32\drivers\etc\hosts**.

2. Add the private endpoint IPs and hostnames as shown in the table from step 3 under Manual DNS server configuration. The hosts file requires the IP address first followed by a space and then the hostname.

3. Save the file with your changes. You may need to save to another directory first, then copy the file to the original path.

Linux

1. Using an account with the **sudoers** privilege, run `sudo nano /etc/hosts` to open the hosts file.

2. Add the private endpoint IPs and hostnames as shown in the table from step 3 under Manual DNS server configuration. The hosts file asks for the IP address first followed by a space and then the hostname.

3. Save the file with your changes.

Connect to an Azure Arc-enabled servers

> **NOTE**
>
> The minimum supported version of the Azure Arc-connected machine agent with private endpoint is version 1.4. The Azure Arc-enabled servers deployment script generated in the portal downloads the latest version.

Configure a new Azure Arc-enabled server to use Private link

When connecting a machine or server with Azure Arc-enabled servers for the first time, you can optionally connect it to a Private Link Scope. The following steps are

1. From your browser, go to the Azure portal.

2. Navigate to **Servers -Azure Arc**.

3. On the **Servers - Azure Arc** page, select **Add** at the upper left.

4. On the **Add servers with Azure Arc** page, select either the **Add a single server** or **Add multiple servers** depending on your deployment scenario, and then select **Generate script**.

5. On the **Generate script** page, select the subscription and resource group where you want the machine to be managed within Azure. Select an Azure location where the machine metadata will be stored. This location can be the same or different, as the resource group's location.

6. On the **Prerequisites** page, review the information and then select **Next: Resource details**.

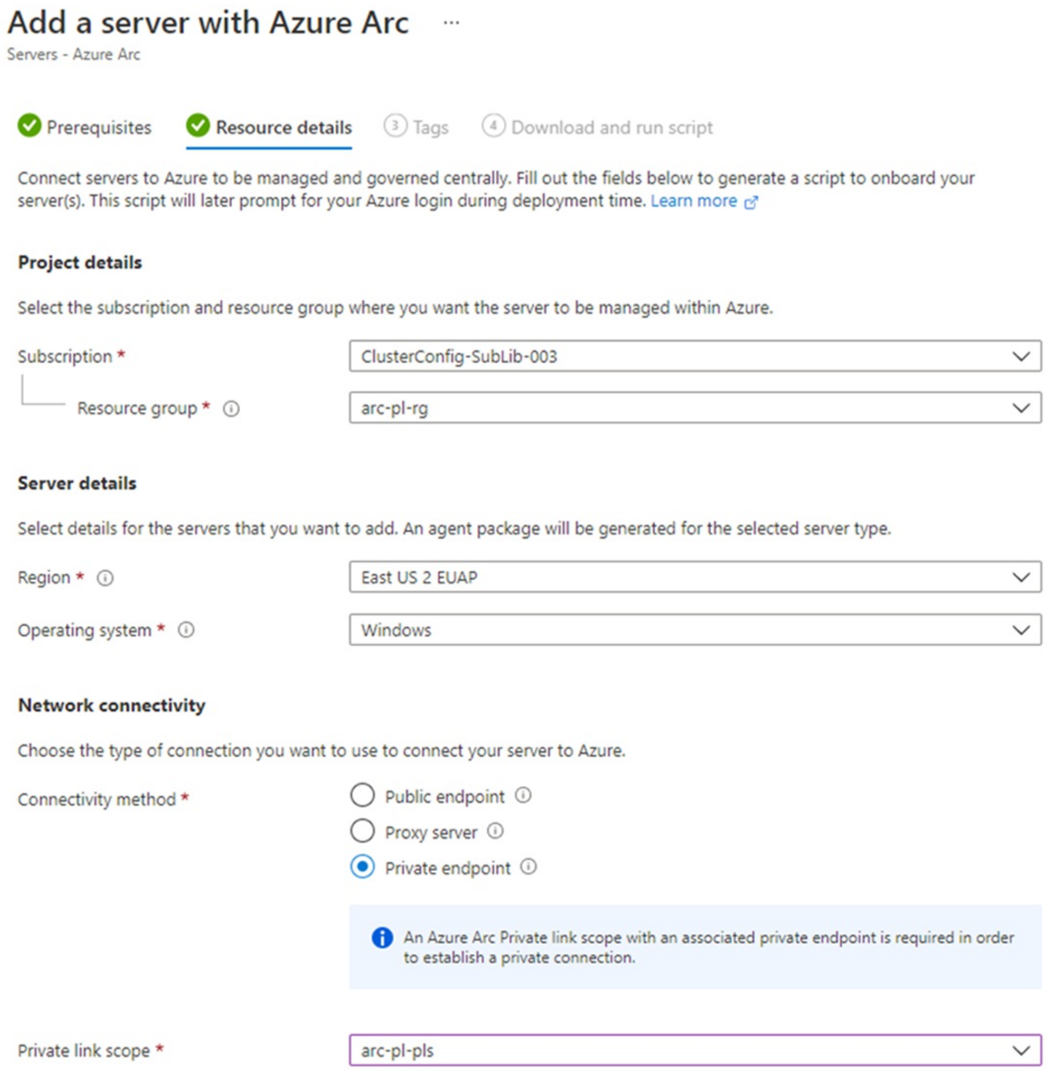
7. On the **Resource details** page, provide the following:

    a. In the **Resource group** drop-down list, select the resource group the machine will be managed from.

    b. In the **Region** drop-down list, select the Azure region to store the machine or server metadata.

    c. In the **Operating system** drop-down list, select the operating system that the script is configured to run on.

    d. Under **Network Connectivity**, select **Private endpoint (preview)** and select the Azure Arc Private Link Scope created in Part 1 from the drop-down list.



Add a server with Azure Arc ...

Servers - Azure Arc

Connect servers to Azure to be managed and governed centrally. Fill out the fields below to generate a script to onboard your server(s). This script will later prompt for your Azure login during deployment time. Learn more

Project details

Select the subscription and resource group where you want the server to be managed within Azure.

Subscription * ClusterConfig-SubLib-003

Resource group * arc-pl-rg

Server details

Select details for the servers that you want to add. An agent package will be generated for the selected server type.

Region * East US 2 EUAP

Operating system * Windows

Network connectivity

Choose the type of connection you want to use to connect your server to Azure.

Connectivity method *

○ Public endpoint

○ Proxy server

● Private endpoint

An Azure Arc Private link scope with an associated private endpoint is required in order to establish a private connection.

Private link scope * arc-pl-pls

e. Select **Next: Tags**.

8. If you selected **Add multiple servers**, on the **Authentication** page, select the service principal created for Azure Arc-enabled servers from the drop down list. If you have not created a service principal for Azure Arc-enabled servers, first review how to create a service principal to familiarize yourself with permissions required and the steps to create one. Select **Next: Tags** to continue.

9. On the **Tags** page, review the default **Physical location tags** suggested and enter a value, or specify one or more **Custom tags** to support your standards.

10. Select **Next: Download and run script**.

11. On the **Download and run script** page, review the summary information, and then select **Download**. If you still need to make changes, select **Previous**.

After downloading the script, you have to run it on your machine or server using a privileged (administrator or root) account. Depending on your network configuration, you may need to download the agent from a computer with internet access and transfer it to your machine or server, and then modify the script with the path to the agent.

The Windows agent can be downloaded from https://aka.ms/AzureConnectedMachineAgent and the Linux agent can be downloaded from https://packages.microsoft.com. Look for the latest version of the **azcmagent** under your OS distribution directory and installed with your local package manager.

The script will return status messages letting you know if onboarding was successful after it completes.

> **NOTE**
>
> If you're deploying the Connected Machine agent on a Linux server, there may be a five minute delay during the network connectivity check followed by an error saying that `you do not have access to login.windows.net`, even if your firewall is configured correctly. This is a known issue and will be fixed in a future agent release. Onboarding should still succeed if your firewall is configured correctly.

Configure an existing Azure Arc-enabled server

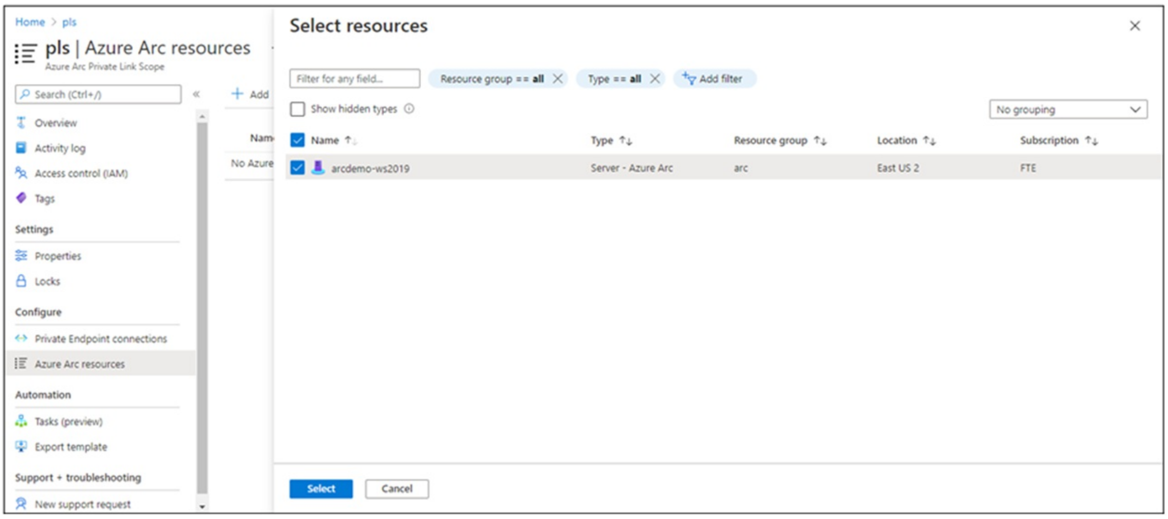
For Azure Arc-enabled servers that were set up prior to your private link scope, you can allow them to start using the Azure Arc-enabled servers Private Link Scope by completing the following steps.

1. In the Azure portal, navigate to your Azure Arc Private Link Scope resource.

2. From the left-hand pane, select **Azure Arc resources** and then **+ Add**.

3. Select the servers in the list that you want to associate with the Private Link Scope, and then select **Select** to save your changes.

   > **NOTE**
   >
   > Only Azure Arc-enabled servers in the same subscription and region as your Private Link Scope is shown.



☑ Name ↑	Type ↑↓	Resource group ↑↓	Location ↑↓	Subscription ↑↓
☑ arcdemo-ws2019	Server - Azure Arc	arc	East US 2	FTE

It may take up to 15 minutes for the Private Link Scope to accept connections from the recently associated server(s).

Troubleshooting

1. Check your on-premises DNS server(s) to verify it is either forwarding to Azure DNS or is configured with appropriate A records in your private link zone. These lookup commands should return private IP addresses in your Azure virtual network. If they resolve public IP addresses, double check your machine or server and network's DNS configuration.

   nslookup gbl.his.arc.azure.com nslookup agentserviceapi.guestconfiguration.azure.com

2. If you are having trouble onboarding a machine or server, confirm that you've added the Azure Active Directory and Azure Resource Manager service tags to your local network firewall. The agent needs to communicate with these services over the internet until private endpoints are available for these services.

Next steps

- To learn more about Private Endpoint, see What is Azure Private Endpoint?.
- If you are experiencing issues with your Azure Private Endpoint connectivity setup, see Troubleshoot Azure Private Endpoint connectivity problems.
- See the following to configure Private Link for Azure Automation, Azure Monitor, Azure Key Vault, or Azure Blob storage.

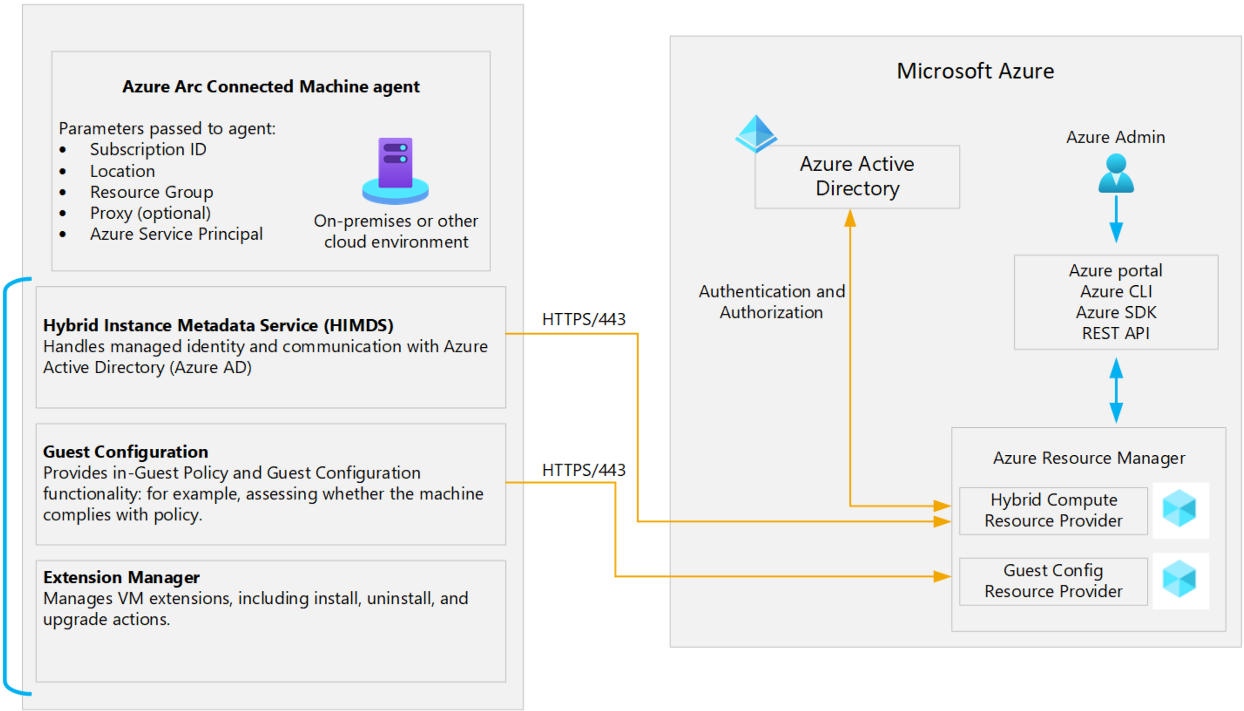
Overview of Azure Arc-enabled servers agent

9/7/2021 • 11 minutes to read • Edit Online

The Azure Arc-enabled servers Connected Machine agent enables you to manage your Windows and Linux machines hosted outside of Azure on your corporate network or other cloud providers. This article provides a detailed overview of the agent, system and network requirements, and the different deployment methods.

> **NOTE**
>
> The Azure Monitor agent (AMA) does not replace the Connected Machine agent. The Azure Monitor agent will replace the Log Analytics agent, Diagnostics extension, and Telegraf agent for both Windows and Linux machines. Review the Azure Monitor documentation about the new agent for more details.

Agent component details



Azure Arc Connected Machine agent
Parameters passed to agent:
Subscription ID
Location
Resource Group
Proxy (optional)
Azure Service Principal
On-premises or other cloud environment
Hybrid Instance Metadata Service (HIMDS)
Handles managed identity and communication with Azure Active Directory (Azure AD)
Guest Configuration
Provides in-Guest Policy and Guest Configuration functionality: for example, assessing whether the machine complies with policy.
Extension Manager
Manages VM extensions, including install, uninstall, and upgrade actions.
HTTPS/443
HTTPS/443
Microsoft Azure
Azure Active Directory
Authentication and Authorization
Azure Admin
Azure portal
Azure CLI
Azure SDK
REST API
Azure Resource Manager
Hybrid Compute Resource Provider
Guest Config Resource Provider

The Azure Connected Machine agent package contains several logical components, which are bundled together.

- The Hybrid Instance Metadata service (HIMDS) manages the connection to Azure and the connected machine's Azure identity.
- The guest configuration agent provides functionality such as assessing whether the machine complies with required policies and enforcing compliance.

  Note the following behavior with Azure Policy guest configuration for a disconnected machine:

  - An Azure Policy assignment that targets disconnected machines is unaffected.
  - Guest assignment is stored locally for 14 days. Within the 14-day period, if the Connected Machine agent reconnects to the service, policy assignments are reapplied.
  - Assignments are deleted after 14 days, and are not reassigned to the machine after the 14-day period.
- The Extension agent manages VM extensions, including install, uninstall, and upgrade. Extensions are downloaded from Azure and copied to the

`%SystemDrive%\%ProgramFiles%\AzureConnectedMachineAgent\ExtensionService\downloads` folder on Windows, and for Linux to `/opt/GC_Ext/downloads`. On Windows, the extension is installed to the following path `%SystemDrive%\Packages\Plugins\<extension>`, and on Linux the extension is installed to `/var/lib/waagent/<extension>`.

Instance metadata

Metadata information about the connected machine is collected after the Connected Machine agent registers with Azure Arc-enabled servers. Specifically:

- Operating system name, type, and version
- Computer name
- Computer manufacturer and model
- Computer fully qualified domain name (FQDN)
- Domain name (if joined to an Active Directory domain)
- Connected Machine agent version
- Active Directory and DNS fully qualified domain name (FQDN)
- UUID (BIOS ID)
- Connected Machine agent heartbeat
- Connected Machine agent version
- Public key for managed identity
- Policy compliance status and details (if using guest configuration policies)
- SQL Server installed (Boolean value)
- Cluster resource ID (for Azure Stack HCI nodes)

The following metadata information is requested by the agent from Azure:

- Resource location (region)
- Virtual machine ID
- Tags
- Azure Active Directory managed identity certificate
- Guest configuration policy assignments
- Extension requests - install, update, and delete.

Download agents

You can download the Azure Connected Machine agent package for Windows and Linux from the locations listed below.

- Windows agent Windows Installer package from the Microsoft Download Center.

- Linux agent package is distributed from Microsoft's package repository using the preferred package format for the distribution (.RPM or .DEB).

The Azure Connected Machine agent for Windows and Linux can be upgraded to the latest release manually or automatically depending on your requirements. For more information, see here.

Prerequisites

Supported environments

Azure Arc-enabled servers support the installation of the Connected Machine agent on any physical server and virtual machine hosted *outside* of Azure. Including virtual machines running on platforms like VMware, Azure

Stack HCI, and other cloud environments. Azure Arc-enabled servers do not support installing the agent on virtual machines running in Azure, or virtual machines running on Azure Stack Hub or Azure Stack Edge as they are already modeled as Azure VMs.

Supported operating systems

The following versions of the Windows and Linux operating system are officially supported for the Azure Connected Machine agent:

- Windows Server 2008 R2 SP1, Windows Server 2012 R2, 2016, 2019, and 2022 (including Server Core)
- Ubuntu 16.04, 18.04, and 20.04 LTS (x64)
- CentOS Linux 7 and 8 (x64)
- SUSE Linux Enterprise Server (SLES) 12 and 15 (x64)
- Red Hat Enterprise Linux (RHEL) 7 and 8 (x64)
- Amazon Linux 2 (x64)
- Oracle Linux 7

> **WARNING**
>
> The Linux hostname or Windows computer name cannot use one of the reserved words or trademarks in the name, otherwise attempting to register the connected machine with Azure will fail. See Resolve reserved resource name errors for a list of the reserved words.

> **NOTE**
>
> While Azure Arc-enabled servers supports Amazon Linux, the following do not support this distro:
>
> - Agents used by Azure Monitor (that is, the Log Analytics and Dependency agent)
> - Azure Automation Update Management
> - VM insights

Software requirements

- NET Framework 4.6 or later is required. Download the .NET Framework.
- Windows PowerShell 5.1 is required. Download Windows Management Framework 5.1..

Required permissions

- To onboard machines, you are a member of the **Azure Connected Machine Onboarding** or Contributor role in the resource group.
- To read, modify, and delete a machine, you are a member of the **Azure Connected Machine Resource Administrator** role in the resource group.
- To select a resource group from the drop-down list when using the **Generate script** method, at a minimum you are a member of the Reader role for that resource group.

Azure subscription and service limits

Before configuring your machines with Azure Arc-enabled servers, review the Azure Resource Manager subscription limits and resource group limits to plan for the number of machines to be connected.

Azure Arc-enabled servers supports up to 5,000 machine instances in a resource group.

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**.

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.

Networking configuration

The Connected Machine agent for Linux and Windows communicates outbound securely to Azure Arc over TCP port 443. If the machine needs to connect through a firewall or proxy server to communicate over the internet, the agent communicates outbound instead using the HTTP protocol. Proxy servers don't make the Connected Machine agent more secure because the traffic is already encrypted.

> **NOTE**
>
> Azure Arc-enabled servers does not support using a Log Analytics gateway as a proxy for the Connected Machine agent.

If outbound connectivity is restricted by your firewall or proxy server, make sure the URLs listed below are not blocked. When you only allow the IP ranges or domain names required for the agent to communicate with the service, you need to allow access to the following Service Tags and URLs.

Service Tags:

- AzureActiveDirectory
- AzureTrafficManager
- AzureResourceManager
- AzureArcInfrastructure
- Storage

URLs:

AGENT RESOURCE	DESCRIPTION
`management.azure.com`	Azure Resource Manager
`login.windows.net`	Azure Active Directory
`login.microsoftonline.com`	Azure Active Directory
`dc.services.visualstudio.com`	Application Insights
`*.guestconfiguration.azure.com`	Guest configuration
`*.his.arc.azure.com`	Hybrid Identity Service
`*.blob.core.windows.net`	Download source for Azure Arc-enabled servers extensions

Preview agents (version 0.11 and lower) also require access to the following URLs:

AGENT RESOURCE	DESCRIPTION
`agentserviceapi.azure-automation.net`	Guest configuration
`*-agentservice-prod-1.azure-automation.net`	Guest configuration

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.

For more information, review Service tags overview.

Register Azure resource providers

Azure Arc-enabled servers depend on the following Azure resource providers in your subscription in order to use this service:

- **Microsoft.HybridCompute**
- **Microsoft.GuestConfiguration**

If they are not registered, you can register them using the following commands:

Azure PowerShell:

```
Login-AzAccount
Set-AzContext -SubscriptionId [subscription you want to onboard]
Register-AzResourceProvider -ProviderNamespace Microsoft.HybridCompute
Register-AzResourceProvider -ProviderNamespace Microsoft.GuestConfiguration
```

Azure CLI:

```
az account set --subscription "{Your Subscription Name}"
az provider register --namespace 'Microsoft.HybridCompute'
az provider register --namespace 'Microsoft.GuestConfiguration'
```

You can also register the resource providers in the Azure portal by following the steps under Azure portal.

Installation and configuration

Connecting machines in your hybrid environment directly with Azure can be accomplished using different methods depending on your requirements. The following table highlights each method to determine which works best for your organization.

> **IMPORTANT**
>
> The Connected Machine agent cannot be installed on an Azure Windows virtual machine. If you attempt to, the installation detects this and rolls back.

METHOD	DESCRIPTION

METHOD	DESCRIPTION
Interactively	Manually install the agent on a single or small number of machines following the steps in Connect machines from Azure portal. From the Azure portal, you can generate a script and execute it on the machine to automate the install and configuration steps of the agent.
At scale	Install and configure the agent for multiple machines following the Connect machines using a Service Principal. This method creates a service principal to connect machines non-interactively.
At scale	Install and configure the agent for multiple machines following the method Using Windows PowerShell DSC. This method uses a service principal to connect machines non-interactively with PowerShell DSC.

Connected Machine agent technical overview

Windows agent installation details

The Connected Machine agent for Windows can be installed by using one of the following three methods:

- Double-click the file `AzureConnectedMachineAgent.msi`.
- Manually by running the Windows Installer package `AzureConnectedMachineAgent.msi` from the Command shell.
- From a PowerShell session using a scripted method.

After installing the Connected Machine agent for Windows, the following system-wide configuration changes are applied.

- The following installation folders are created during setup.

FOLDER	DESCRIPTION
%ProgramFiles%\AzureConnectedMachineAgent	Default installation path containing the agent support files.
%ProgramData%\AzureConnectedMachineAgent	Contains the agent configuration files.
%ProgramData%\AzureConnectedMachineAgent\Tokens	Contains the acquired tokens.
%ProgramData%\AzureConnectedMachineAgent\Config	Contains the agent configuration file `agentconfig.json` recording its registration information with the service.
%ProgramFiles%\ArcConnectedMachineAgent\ExtensionService\GC	Installation path containing the guest configuration agent files.
%ProgramData%\GuestConfig	Contains the (applied) policies from Azure.
%ProgramFiles%\AzureConnectedMachineAgent\ExtensionService\downloads	Extensions are downloaded from Azure and copied here.

- The following Windows services are created on the target machine during installation of the agent.

SERVICE NAME	DISPLAY NAME	PROCESS NAME	DESCRIPTION
himds	Azure Hybrid Instance Metadata Service	himds	This service implements the Azure Instance Metadata service (IMDS) to manage the connection to Azure and the connected machine's Azure identity.
GCArcService	Guest configuration Arc Service	gc_service	Monitors the desired state configuration of the machine.
ExtensionService	Guest configuration Extension Service	gc_service	Installs the required extensions targeting the machine.

- The following environmental variables are created during agent installation.

NAME	DEFAULT VALUE	DESCRIPTION
IDENTITY_ENDPOINT	http://localhost:40342/metadata/identity/oauth2/token	
IMDS_ENDPOINT	http://localhost:40342	

- There are several log files available for troubleshooting. They are described in the following table.

LOG	DESCRIPTION
%ProgramData%\AzureConnectedMachineAgent\Log\himds.log	Records details of the agents (HIMDS) service and interaction with Azure.
%ProgramData%\AzureConnectedMachineAgent\Log\azcmagent.log	Contains the output of the azcmagent tool commands, when the verbose (-v) argument is used.
%ProgramData%\GuestConfig\gc_agent_logs\gc_agent.log	Records details of the DSC service activity, in particular the connectivity between the HIMDS service and Azure Policy.
%ProgramData%\GuestConfig\gc_agent_logs\gc_agent_telemetry.txt	Records details about DSC service telemetry and verbose logging.
%ProgramData%\GuestConfig\ext_mgr_logs	Records details about the Extension agent component.
%ProgramData%\GuestConfig\extension_logs<Extension>	Records details from the installed extension.

- The local security group **Hybrid agent extension applications** is created.

- During uninstall of the agent, the following artifacts are not removed.
  - %ProgramData%\AzureConnectedMachineAgent\Log
  - %ProgramData%\AzureConnectedMachineAgent and subdirectories
  - %ProgramData%\GuestConfig

Linux agent installation details

The Connected Machine agent for Linux is provided in the preferred package format for the distribution (.RPM or .DEB) that's hosted in the Microsoft package repository. The agent is installed and configured with the shell script bundle Install_linux_azcmagent.sh.

After installing the Connected Machine agent for Linux, the following system-wide configuration changes are applied.

- The following installation folders are created during setup.

FOLDER	DESCRIPTION
/var/opt/azcmagent/	Default installation path containing the agent support files.
/opt/azcmagent/	
/opt/GC_Ext	Installation path containing the guest configuration agent files.
/opt/DSC/	
/var/opt/azcmagent/tokens	Contains the acquired tokens.
/var/lib/GuestConfig	Contains the (applied) policies from Azure.
/opt/GC_Ext/downloads	Extensions are downloaded from Azure and copied here.

- The following daemons are created on the target machine during installation of the agent.

SERVICE NAME	DISPLAY NAME	PROCESS NAME	DESCRIPTION
himdsd.service	Azure Connected Machine Agent Service	himds	This service implements the Azure Instance Metadata service (IMDS) to manage the connection to Azure and the connected machine's Azure identity.
gcad.service	GC Arc Service	gc_linux_service	Monitors the desired state configuration of the machine.
extd.service	Extension Service	gc_linux_service	Installs the required extensions targeting the machine.

- There are several log files available for troubleshooting. They are described in the following table.

LOG	DESCRIPTION
/var/opt/azcmagent/log/himds.log	Records details of the agents (HIMDS) service and interaction with Azure.

LOG	DESCRIPTION
/var/opt/azcmagent/log/azcmagent.log	Contains the output of the azcmagent tool commands, when the verbose (-v) argument is used.
/opt/logs/dsc.log	Records details of the DSC service activity, in particular the connectivity between the himds service and Azure Policy.
/opt/logs/dsc.telemetry.txt	Records details about DSC service telemetry and verbose logging.
/var/lib/GuestConfig/ext_mgr_logs	Records details about the Extension agent component.
/var/lib/GuestConfig/extension_logs	Records details from the installed extension.

- The following environmental variables are created during agent installation. These variables are set in `/lib/systemd/system.conf.d/azcmagent.conf`.

NAME	DEFAULT VALUE	DESCRIPTION
IDENTITY_ENDPOINT	http://localhost:40342/metadata/identity/oauth2/token	
IMDS_ENDPOINT	http://localhost:40342	

- During uninstall of the agent, the following artifacts are not removed.
  - /var/opt/azcmagent
  - /opt/logs

Agent resource governance

Azure Arc-enabled servers Connected Machine agent is designed to manage agent and system resource consumption. The agent approaches resource governance under the following conditions:

- The Guest Configuration agent limits up to 5% of the CPU to evaluate policies.
- The Extension Service agent is limited to use up to 5% of the CPU.
  - This only applies to install/uninstall/upgrade operations. Once installed, extensions are responsible for their own resource utilization and the 5% CPU limit does not apply.
  - The Log Analytics agent and Azure Monitor Agent is allowed to use up to 60% of the CPU during their install/upgrade/uninstall operations on Red Hat Linux, CentOS, and other enterprise Linux variants. The limit is higher for this combination of extensions and operating systems to accommodate the performance impact of SELinux on these systems.

Next steps

- To begin evaluating Azure Arc-enabled servers, follow the article Connect hybrid machines with Azure Arc-enabled servers.
- Before deploying the Azure Arc-enabled servers agent and integrate with other Azure management and monitoring services, review the Planning and deployment guide.
- Troubleshooting information can be found in the Troubleshoot Connected Machine agent guide.

Plan and deploy Azure Arc-enabled servers

9/7/2021 • 6 minutes to read • Edit Online

Deployment of an IT infrastructure service or business application is a challenge for any company. In order to execute it well and avoid any unwelcome surprises and unplanned costs, you need to thoroughly plan for it to ensure that you're as ready as possible. To plan for deploying Azure Arc-enabled servers at any scale, it should cover the design and deployment criteria that needs to be met in order to successfully complete the tasks.

For the deployment to proceed smoothly, your plan should establish a clear understanding of:

- Roles and responsibilities.
- Inventory of physical servers or virtual machines to verify they meet network and system requirements.
- The skill set and training required to enable successful deployment and on-going management.
- Acceptance criteria and how you track its success.
- Tools or methods to be used to automate the deployments.
- Identified risks and mitigation plans to avoid delays, disruptions, etc.
- How to avoid disruption during deployment.
- What's the escalation path when a significant issue occurs?

The purpose of this article is to ensure you are prepared for a successful deployment of Azure Arc-enabled servers across multiple production physical servers or virtual machines in your environment.

To learn more about our at-scale deployment recommendations, you can also refer to this video.

Prerequisites

- Your machines run a supported operating system for the Connected Machine agent.
- Your machines have connectivity from your on-premises network or other cloud environment to resources in Azure, either directly or through a proxy server.
- To install and configure the Azure Arc-enabled servers Connected Machine agent, an account with elevated (that is, an administrator or as root) privileges on the machines.
- To onboard machines, you are a member of the **Azure Connected Machine Onboarding** role.
- To read, modify, and delete a machine, you are a member of the **Azure Connected Machine Resource Administrator** role.

Pilot

Before deploying to all production machines, start by evaluating this deployment process before adopting it broadly in your environment. For a pilot, identify a representative sampling of machines that aren't critical to your companies ability to conduct business. You'll want to be sure to allow enough time to run the pilot and assess its impact: we recommend a minimum of 30 days.

Establish a formal plan describing the scope and details of the pilot. The following is a sample of what a plan should include to help get you started.

- Objectives - Describes the business and technical drivers that led to the decision that a pilot is necessary.
- Selection criteria - Specifies the criteria used to select which aspects of the solution will be demonstrated via a pilot.

- Scope - Describes the scope of the pilot, which includes but not limited to solution components, anticipated schedule, duration of the pilot, and number of machines to target.
- Success criteria and metrics - Define the pilot's success criteria and specific measures used to determine level of success.
- Training plan - Describes the plan for training system engineers, administrators, etc. who are new to Azure and it services during the pilot.
- Transition plan - Describes the strategy and criteria used to guide transition from pilot to production.
- Rollback - Describes the procedures for rolling back a pilot to pre-deployment state.
- Risks - List all identified risks for conducting the pilot and associated with production deployment.

Phase 1: Build a foundation

In this phase, system engineers or administrators enable the core features in their organizations Azure subscription to start the foundation before enabling your machines for management by Azure Arc-enabled servers and other Azure services.

TASK	DETAIL	DURATION
Create a resource group	A dedicated resource group to include only Azure Arc-enabled servers and centralize management and monitoring of these resources.	One hour
Apply Tags to help organize machines.	Evaluate and develop an IT-aligned tagging strategy that can help reduce the complexity of managing your Azure Arc-enabled servers and simplify making management decisions.	One day
Design and deploy Azure Monitor Logs	Evaluate design and deployment considerations to determine if your organization should use an existing or implement another Log Analytics workspace to store collected log data from hybrid servers and machines.[1]	One day
Develop an Azure Policy governance plan	Determine how you will implement governance of hybrid servers and machines at the subscription or resource group scope with Azure Policy.	One day
Configure Role based access control (RBAC)	Develop an access plan to control who has access to manage Azure Arc-enabled servers and ability to view their data from other Azure services and solutions.	One day

TASK	DETAIL	DURATION
Identify machines with Log Analytics agent already installed	Run the following log query in Log Analytics to support conversion of existing Log Analytics agent deployments to extension-managed agent: Heartbeat | where TimeGenerated > ago(30d) | where ResourceType == "machines" and (ComputerEnvironment == "Non-Azure") | summarize by Computer, ResourceProvider, ResourceType, ComputerEnvironment	One hour

[1] An important consideration as part of evaluating your Log Analytics workspace design, is integration with Azure Automation in support of its Update Management and Change Tracking and Inventory feature, as well as Azure Security Center and Azure Sentinel. If your organization already has an Automation account and enabled its management features linked with a Log Analytics workspace, evaluate whether you can centralize and streamline management operations, as well as minimize cost, by using those existing resources versus creating a duplicate account, workspace, etc.

Phase 2: Deploy Azure Arc-enabled servers

Next, we add to the foundation laid in phase 1 by preparing for and deploying the Azure Arc-enabled servers Connected Machine agent.

TASK	DETAIL	DURATION
Download the pre-defined installation script	Review and customize the pre-defined installation script for at-scale deployment of the Connected Machine agent to support your automated deployment requirements. Sample at-scale onboarding resources: • At-scale basic deployment script • At-scale onboarding VMware vSphere Windows Server VMs • At-scale onboarding VMware vSphere Linux VMs • At-scale onboarding AWS EC2 instances using Ansible • At-scale deployment using PowerShell remoting (Windows only)	One or more days depending on requirements, organizational processes (for example, Change and Release Management), and automation method used.
Create service principal	Create a service principal to connect machines non-interactively using Azure PowerShell or from the portal.	One hour

TASK	DETAIL	DURATION
Deploy the Connected Machine agent to your target servers and machines	Use your automation tool to deploy the scripts to your servers and connect them to Azure.	One or more days depending on your release plan and if following a phased rollout.

Phase 3: Manage and operate

Phase 3 sees administrators or system engineers enable automation of manual tasks to manage and operate the Connected Machine agent and the machine during their lifecycle.

TASK	DETAIL	DURATION
Create a Resource Health alert	If a server stops sending heartbeats to Azure for longer than 15 minutes, it can mean that it is offline, the network connection has been blocked, or the agent is not running. Develop a plan for how you'll respond and investigate these incidents and use Resource Health alerts to get notified when they start. Specify the following when configuring the alert: **Resource type** = **Azure Arc–enabled servers** **Current resource status** = **Unavailable** **Previous resource status** = **Available**	One hour
Create an Azure Advisor alert	For the best experience and most recent security and bug fixes, we recommend keeping the Azure Arc-enabled servers agent up to date. Out-of-date agents will be identified with an Azure Advisor alert. Specify the following when configuring the alert: **Recommendation type** = **Upgrade to the latest version of the Azure Connected Machine Agent**	One hour
Assign Azure policies to your subscription or resource group scope	Assign the **Enable Azure Monitor for VMs** policy (and others that meet your needs) to the subscription or resource group scope. Azure Policy allows you to assign policy definitions that install the required agents for VM insights across your environment.	Varies
Enable Update Management for your Azure Arc-enabled servers	Configure Update Management in Azure Automation to manage operating system updates for your Windows and Linux virtual machines registered with Azure Arc-enabled servers.	15 minutes

Next steps

- Troubleshooting information can be found in the Troubleshoot Connected Machine agent guide.
- Learn how to simplify deployment with other Azure services like Azure Automation State Configuration and other supported Azure VM extensions.

Connect hybrid machines to Azure from the Azure portal

9/7/2021 • 6 minutes to read • Edit Online

You can enable Azure Arc-enabled servers for one or a small number of Windows or Linux machines in your environment by performing a set of steps manually. Or you can use an automated method by running a template script that we provide. This script automates the download and installation of both agents.

This method requires that you have administrator permissions on the machine to install and configure the agent. On Linux, by using the root account, and on Windows, you are member of the Local Administrators group.

Before you get started, be sure to review the prerequisites and verify that your subscription and resources meet the requirements. For information about supported regions and other related considerations, see supported Azure regions.

If you don't have an Azure subscription, create a free account before you begin.

Generate the installation script from the Azure portal

The script to automate the download and installation, and to establish the connection with Azure Arc, is available from the Azure portal. To complete the process, perform the following steps:

1. From your browser, go to the Azure portal.
2. On the **Servers - Azure Arc** page, select **Add** at the upper left.
3. On the **Select a method** page, select the **Add servers using interactive script** tile, and then select **Generate script**.
4. On the **Generate script** page, select the subscription and resource group where you want the machine to be managed within Azure. Select an Azure location where the machine metadata will be stored. This location can be the same or different, as the resource group's location.
5. On the **Prerequisites** page, review the information and then select **Next: Resource details**.
6. On the **Resource details** page, provide the following:
   a. In the **Resource group** drop-down list, select the resource group the machine will be managed from.
   b. In the **Region** drop-down list, select the Azure region to store the servers metadata.
   c. In the **Operating system** drop-down list, select the operating system that the script is configured to run on.
   d. If the machine is communicating through a proxy server to connect to the internet, specify the proxy server IP address or the name and port number that the machine will use to communicate with the proxy server. Enter the value in the format `http://<proxyURL>:<proxyport>`.
   e. Select **Next: Tags**.
7. On the **Tags** page, review the default **Physical location tags** suggested and enter a value, or specify one or more **Custom tags** to support your standards.
8. Select **Next: Download and run script**.
9. On the **Download and run script** page, review the summary information, and then select **Download**.

If you still need to make changes, select **Previous**.

Install and validate the agent on Windows

Install manually

You can install the Connected Machine agent manually by running the Windows Installer package *AzureConnectedMachineAgent.msi*. You can download the latest version of the Windows agent Windows Installer package from the Microsoft Download Center.

> **NOTE**
>
> - To install or uninstall the agent, you must have *Administrator* permissions.
> - You must first download and copy the Installer package to a folder on the target server, or from a shared network folder. If you run the Installer package without any options, it starts a setup wizard that you can follow to install the agent interactively.

If the machine needs to communicate through a proxy server to the service, after you install the agent you need to run a command that's described in the steps below. This command sets the proxy server system environment variable `https_proxy`. Using this configuration, the agent communicates through the proxy server using the HTTP protocol.

If you are unfamiliar with the command-line options for Windows Installer packages, review Msiexec standard command-line options and Msiexec command-line options.

For example, run the installation program with the `/?` parameter to review the help and quick reference option.

```
msiexec.exe /i AzureConnectedMachineAgent.msi /?
```

1. To install the agent silently and create a setup log file in the `C:\Support\Logs` folder that exist, run the following command.

   ```
   msiexec.exe /i AzureConnectedMachineAgent.msi /qn /l*v "C:\Support\Logs\Azcmagentsetup.log"
   ```

   If the agent fails to start after setup is finished, check the logs for detailed error information. The log directory is *%ProgramData%\AzureConnectedMachineAgent\log*.

2. If the machine needs to communicate through a proxy server, to set the proxy server environment variable, run the following command:

   ```
   [Environment]::SetEnvironmentVariable("https_proxy", "http://{proxy-url}:{proxy-port}", "Machine")
   $env:https_proxy = [System.Environment]::GetEnvironmentVariable("https_proxy","Machine")
   # For the changes to take effect, the agent service needs to be restarted after the proxy environment
   variable is set.
   Restart-Service -Name himds
   ```

   > **NOTE**
   >
   > The agent does not support setting proxy authentication.

3. After installing the agent, you need to configure it to communicate with the Azure Arc service by running the following command:

```
"%ProgramFiles%\AzureConnectedMachineAgent\azcmagent.exe" connect --resource-group
"resourceGroupName" --tenant-id "tenantID" --location "regionName" --subscription-id "subscriptionID"
```

Install with the scripted method

1. Log in to the server.

2. Open an elevated PowerShell command prompt.

   > **NOTE**
   >
   > The script only supports running from a 64-bit version of Windows PowerShell.

3. Change to the folder or share that you copied the script to, and execute it on the server by running the `./OnboardingScript.ps1` script.

If the agent fails to start after setup is finished, check the logs for detailed error information. The log directory is *%ProgramData%\AzureConnectedMachineAgent\log*.

Install and validate the agent on Linux

The Connected Machine agent for Linux is provided in the preferred package format for the distribution (.RPM or .DEB) that's hosted in the Microsoft package repository. The shell script bundle `Install_linux_azcmagent.sh` performs the following actions:

- Configures the host machine to download the agent package from packages.microsoft.com.

- Installs the Hybrid Resource Provider package.

Optionally, you can configure the agent with your proxy information by including the `--proxy "{proxy-url}:{proxy-port}"` parameter. Using this configuration, the agent communicates through the proxy server using the HTTP protocol.

The script also contains logic to identify the supported and unsupported distributions, and it verifies the permissions that are required to perform the installation.

The following example downloads the agent and installs it:

```
# Download the installation package.
wget https://aka.ms/azcmagent -O ~/Install_linux_azcmagent.sh

# Install the connected machine agent.
bash ~/Install_linux_azcmagent.sh
```

1. To download and install the agent, run the following commands. If your machine needs to communicate through a proxy server to connect to the internet, include the `--proxy` parameter.

   ```
   # Download the installation package.
   wget https://aka.ms/azcmagent -O ~/Install_linux_azcmagent.sh

   # Install the connected machine agent.
   bash ~/Install_linux_azcmagent.sh --proxy "{proxy-url}:{proxy-port}"
   ```

2. After installing the agent, you need to configure it to communicate with the Azure Arc service by running the following command:

```
azcmagent connect --resource-group "resourceGroupName" --tenant-id "tenantID" --location "regionName"
--subscription-id "subscriptionID" --cloud "cloudName"
if [ $? = 0 ]; then echo "\033[33mTo view your onboarded server(s), navigate to
https://portal.azure.com/#blade/HubsExtension/BrowseResource/resourceType/Microsoft.HybridCompute%2Fm
achines\033[m"; fi
```

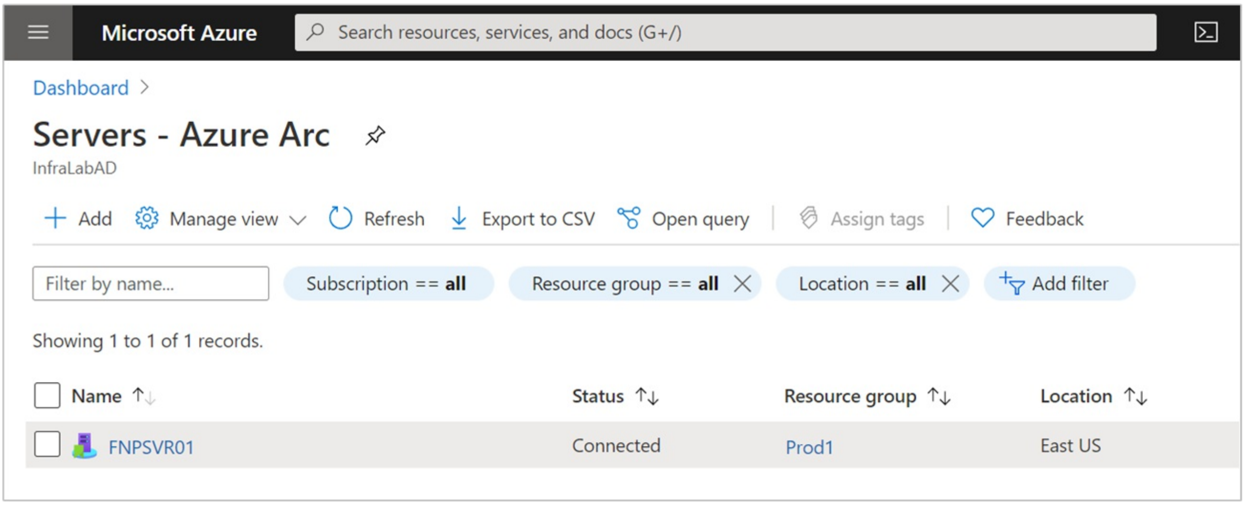
Install with the scripted method

1. Log in to the server with an account that has root access.
2. Change to the folder or share that you copied the script to, and execute it on the server by running the `./OnboardingScript.sh` script.

If the agent fails to start after setup is finished, check the logs for detailed error information. The log directory is *var/opt/azcmagent/log*.

Verify the connection with Azure Arc

After you install the agent and configure it to connect to Azure Arc-enabled servers, go to the Azure portal to verify that the server has successfully connected. View your machines in the Azure portal.



Servers - Azure Arc

InfraLabAD

Subscription == **all**

Resource group == **all**

Location == **all**

Showing 1 to 1 of 1 records.

□ Name ↑↓	Status ↑↓	Resource group ↑↓	Location ↑↓
□ FNPSVR01	Connected	Prod1	East US

Next steps

- Troubleshooting information can be found in the Troubleshoot Connected Machine agent guide.
- Review the Planning and deployment guide to plan for deploying Azure Arc-enabled servers at any scale and implement centralized management and monitoring.
- Learn how to manage your machine using Azure Policy, for such things as VM guest configuration, verify the machine is reporting to the expected Log Analytics workspace, enable monitoring with VM insights, and much more.

Connect hybrid machines to Azure at scale

8/17/2021 • 6 minutes to read • Edit Online

You can enable Azure Arc-enabled servers for multiple Windows or Linux machines in your environment with several flexible options depending on your requirements. Using the template script we provide, you can automate every step of the installation, including establishing the connection to Azure Arc. However, you are required to interactively execute this script with an account that has elevated permissions on the target machine and in Azure.

To connect the machines to Azure Arc-enabled servers, you can use an Azure Active Directory service principal instead of using your privileged identity to interactively connect the machine. A service principal is a special limited management identity that is granted only the minimum permission necessary to connect machines to Azure using the `azcmagent` command. This is safer than using a higher privileged account like a Tenant Administrator, and follows our access control security best practices. The service principal is used only during onboarding, it is not used for any other purpose.

The installation methods to install and configure the Connected Machine agent requires that the automated method you use has administrator permissions on the machines. On Linux, by using the root account and on Windows, as a member of the Local Administrators group.

Before you get started, be sure to review the prerequisites and verify that your subscription and resources meet the requirements. For information about supported regions and other related considerations, see supported Azure regions. Also review our at-scale planning guide to understand the design and deployment criteria, as well as our management and monitoring recommendations.

If you don't have an Azure subscription, create a free account before you begin.

Create a Service Principal for onboarding at scale

You can use Azure PowerShell to create a service principal with the New-AzADServicePrincipal cmdlet. Or you can follow the steps listed under Create a Service Principal using the Azure portal to complete this task.

> **NOTE**
>
> Before you create a service principal, your account must be a member of the **Owner** or **User Access Administrator** role in the subscription that you want to use for onboarding. If you don't have sufficient permissions to configure role assignments, the service principal might be created, but it won't be able to onboard machines.

To create the service principal using PowerShell, perform the following steps.

1. Run the following command. You must store the output of the `New-AzADServicePrincipal` cmdlet in a variable, or you will not be able to retrieve the password needed in a later step.

```
$sp = New-AzADServicePrincipal -DisplayName "Arc-for-servers" -Role "Azure Connected Machine
Onboarding"
$sp
```

```
Secret                : System.Security.SecureString
ServicePrincipalNames : {ad9bcd79-be9c-45ab-abd8-80ca1654a7d1, https://Arc-for-servers}
ApplicationId         : ad9bcd79-be9c-45ab-abd8-80ca1654a7d1
ObjectType            : ServicePrincipal
DisplayName           : Hybrid-RP
Id                    : 5be92c87-01c4-42f5-bade-c1c10af87758
Type                  :
```

2. To retrieve the password stored in the `$sp` variable, run the following command:

```
$credential = New-Object pscredential -ArgumentList "temp", $sp.Secret
$credential.GetNetworkCredential().password
```

3. In the output, find the password value under the field **password** and copy it. Also find the value under the field **ApplicationId** and copy it also. Save them for later in a secure place. If you forget or lose your service principal password, you can reset it using the `New-AzADSpCredential` cmdlet.

The values from the following properties are used with parameters passed to the `azcmagent`:

- The value from the **ApplicationId** property is used for the `--service-principal-id` parameter value
- The value from the **password** property is used for the `--service-principal-secret` parameter used to connect the agent.

NOTE

Make sure to use the service principal **ApplicationId** property, not the **Id** property.

The **Azure Connected Machine Onboarding** role contains only the permissions required to onboard a machine. You can assign the service principal permission to allow its scope to include a resource group or a subscription. To add role assignment, see Assign Azure roles using the Azure portal or Assign Azure roles using Azure CLI.

Generate the installation script from the Azure portal

The script to automate the download and installation, and to establish the connection with Azure Arc, is available from the Azure portal. To complete the process, do the following steps:

1. From your browser, go to the Azure portal.
2. On the **Servers - Azure Arc** page, select **Add** at the upper left.
3. On the **Select a method** page, select the **Add multiple servers** tile, and then select **Generate script**.
4. On the **Generate script** page, select the subscription and resource group where you want the machine to be managed within Azure. Select an Azure location where the machine metadata will be stored. This location can be the same or different, as the resource group's location.
5. On the **Prerequisites** page, review the information and then select **Next: Resource details**.
6. On the **Resource details** page, provide the following:

   a. In the **Resource group** drop-down list, select the resource group the machine will be managed from.
   b. In the **Region** drop-down list, select the Azure region to store the servers metadata.
   c. In the **Operating system** drop-down list, select the operating system that the script is configured to run on.
   d. If the machine is communicating through a proxy server to connect to the internet, specify the proxy

server IP address or the name and port number that the machine will use to communicate with the proxy server. Using this configuration, the agent communicates through the proxy server using the HTTP protocol. Enter the value in the format `http://<proxyURL>:<proxyport>`.

   e. Select **Next: Authentication**.

7. On the **Authentication** page, under the **service principal** drop-down list, select **Arc-for-servers**. Then select, **Next: Tags**.

8. On the **Tags** page, review the default **Physical location tags** suggested and enter a value, or specify one or more **Custom tags** to support your standards.

9. Select **Next: Download and run script**.

10. On the **Download and run script** page, review the summary information, and then select **Download**. If you still need to make changes, select **Previous**.

For Windows, you are prompted to save `OnboardingScript.ps1`, and for Linux `OnboardingScript.sh` to your computer.

Install the agent and connect to Azure

Taking the script template created earlier, you can install and configure the Connected Machine agent on multiple hybrid Linux and Windows machines using your organizations preferred automation tool. The script performs similar steps described in the Connect hybrid machines to Azure from the Azure portal article. The difference is in the final step, where you establish the connection to Azure Arc using the `azcmagent` command using the service principal.

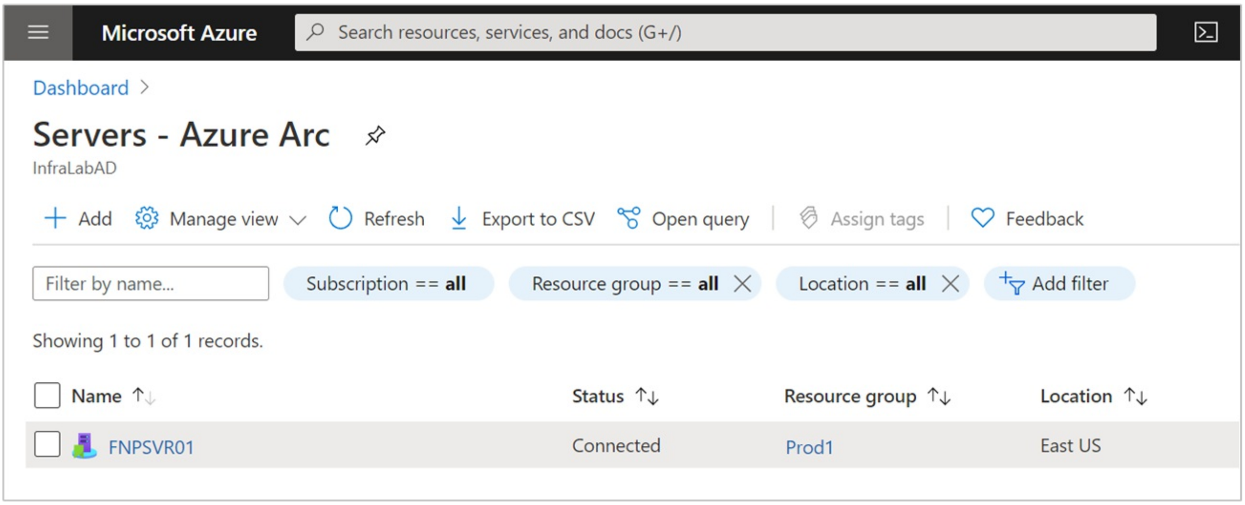
The following are the settings that you configure the `azcmagent` command to use for the service principal.

- `service-principal-id` : The unique identifier (GUID) that represents the application ID of the service principal.
- `service-principal-secret` | The service principal password.
- `tenant-id` : The unique identifier (GUID) that represents your dedicated instance of Azure AD.
- `subscription-id` : The subscription ID (GUID) of your Azure subscription that you want the machines in.
- `resource-group` : The resource group name where you want your connected machines to belong to.
- `location` : See supported Azure regions. This location can be the same or different, as the resource group's location.
- `resource-name` : (*Optional*) Used for the Azure resource representation of your on-premises machine. If you do not specify this value, the machine hostname is used.

You can learn more about the `azcmagent` command-line tool by reviewing the Azcmagent Reference.

> **NOTE**
>
> The Windows PowerShell script only supports running from a 64-bit version of Windows PowerShell.

After you install the agent and configure it to connect to Azure Arc-enabled servers, go to the Azure portal to verify that the server has successfully connected. View your machines in the Azure portal.



Servers - Azure Arc

InfraLabAD

Subscription == **all** | Resource group == **all** | Location == **all**

Showing 1 to 1 of 1 records.

Name	Status	Resource group	Location
FNPSVR01	Connected	Prod1	East US

Next steps

- Troubleshooting information can be found in the Troubleshoot Connected Machine agent guide.
- Review the Planning and deployment guide to plan for deploying Azure Arc-enabled servers at any scale and implement centralized management and monitoring.
- Learn how to manage your machine using Azure Policy, for such things as VM guest configuration, verify the machine is reporting to the expected Log Analytics workspace, enable monitoring with VM insights, and much more.

How to install the Connected Machine agent using Windows PowerShell DSC

9/7/2021 • 3 minutes to read • Edit Online

Using Windows PowerShell Desired State Configuration (DSC), you can automate software installation and configuration for a Windows computer. This article describes how to use DSC to install the Azure Arc-enabled servers Connected Machine agent on hybrid Windows machines.

Requirements

- Windows PowerShell version 4.0 or higher
- The AzureConnectedMachineDsc DSC module
- A service principal to connect the machines to Azure Arc-enabled servers non-interactively. Follow the steps under the section Create a Service Principal for onboarding at scale if you have not created a service principal for Azure Arc-enabled servers already.

Install the ConnectedMachine DSC module

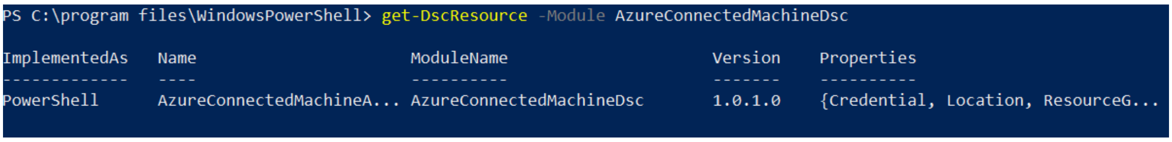
1. To manually install the module, download the source code and unzip the contents of the project directory to the `$env:ProgramFiles\WindowsPowerShell\Modules folder`. Or, run the following command to install from the PowerShell gallery using PowerShellGet (in PowerShell 5.0):

   ```
   Find-Module -Name AzureConnectedMachineDsc -Repository PSGallery | Install-Module
   ```

2. To confirm installation, run the following command and ensure you see the Azure Connected Machine DSC resources available.

   ```
   Get-DscResource -Module AzureConnectedMachineDsc
   ```

   In the output, you should see something similar to the following:



```
PS C:\program files\WindowsPowerShell> get-DscResource -Module AzureConnectedMachineDsc

ImplementedAs   Name                      ModuleName                     Version    Properties
-------------   ----                      ----------                     -------    ----------
PowerShell      AzureConnectedMachineA... AzureConnectedMachineDsc       1.0.1.0    {Credential, Location, ResourceG...
```

Install the agent and connect to Azure

The resources in this module are designed to manage the Azure Connected Machine Agent configuration. Also included is a PowerShell script `AzureConnectedMachineAgent.ps1`, found in the `AzureConnectedMachineDsc\examples` folder. It uses community resources to automate the download and installation, and establish a connection with Azure Arc. This script performs similar steps described in the Connect hybrid machines to Azure from the Azure portal article.

If the machine needs to communicate through a proxy server to the service, after you install the agent you need to run a command that's described here. This sets the proxy server system environment variable `https_proxy`. Instead of running the command manually, you can perform this step with DSC by using the

ComputeManagementDsc module. Using this configuration, the agent communicates through the proxy server using the HTTP protocol.

> **NOTE**
>
> To allow DSC to run, Windows needs to be configured to receive PowerShell remote commands even when you're running a localhost configuration. To easily configure your environment correctly, just run `Set-WsManQuickConfig -Force` in an elevated PowerShell Terminal.

Configuration documents (MOF files) can be applied to the machine using the `Start-DscConfiguration` cmdlet.

The following are the parameters you pass to the PowerShell script to use.

- `TenantId`: The unique identifier (GUID) that represents your dedicated instance of Azure AD.
- `SubscriptionId`: The subscription ID (GUID) of your Azure subscription that you want the machines in.
- `ResourceGroup`: The resource group name where you want your connected machines to belong to.
- `Location`: See supported Azure regions. This location can be the same or different, as the resource group's location.
- `Tags`: String array of tags that should be applied to the connected machine resource.
- `Credential`: A PowerShell credential object with the **ApplicationId** and **password** used to register machines at scale using a service principal.

1. In a PowerShell console, navigate to the folder where you saved the `.ps1` file.
2. Run the following PowerShell commands to compile the MOF document (for information about compiling DSC configurations, see DSC Configurations:

   ```
   .\`AzureConnectedMachineAgent.ps1 -TenantId <TenantId GUID> -SubscriptionId <SubscriptionId GUID> -
   ResourceGroup '<ResourceGroupName>' -Location '<LocationName>' -Tags '<Tag>' -Credential
   <psCredential>
   ```

3. This will create a `localhost.mof file` in a new folder named `C:\dsc`.

After you install the agent and configure it to connect to Azure Arc-enabled servers, go to the Azure portal to verify that the server has been successfully connected. View your machines in the Azure portal.

Adding to existing configurations

This resource can be added to existing DSC configurations to represent an end-to-end configuration for a machine. For example, you might wish to add this resource to a configuration that sets secure operating system settings.

The CompositeResource module from the PowerShell Gallery can be used to create a composite resource of the example configuration, to further simplify combining configurations.

Next steps

- Troubleshooting information can be found in the Troubleshoot Connected Machine agent guide.
- Review the Planning and deployment guide to plan for deploying Azure Arc-enabled servers at any scale and implement centralized management and monitoring.
- Learn how to manage your machine using Azure Policy, for such things as VM guest configuration,

verifying the machine is reporting to the expected Log Analytics workspace, enable monitoring with VM insights, and much more.

Connect hybrid machines to Azure from Windows Admin Center

9/7/2021 • 2 minutes to read • Edit Online

You can enable Azure Arc-enabled servers for one or more Windows machines in your environment by performing a set of steps manually. Or you can use Windows Admin Center to deploy the Connected Machine agent and register your on-premises servers without having to perform any steps outside of this tool.

Prerequisites

- Azure Arc-enabled servers - Review the prerequisites and verify that your subscription, your Azure account, and resources meet the requirements.
- Windows Admin Center - Review the requirements to prepare your environment to deploy and configure Azure integration .
- An Azure subscription. If you don't have one, create a free account before you begin.
- The target Windows servers that you want to manage must have Internet connectivity to access Azure.

Security

This deployment method requires that you have administrator rights on the target Windows machine or server to install and configure the agent. You also need to be a member of the **Gateway users** role.

Deploy

Perform the following steps to configure the Windows server with Azure Arc-enabled servers.

1. Sign in to Windows Admin Center.
2. From the connection list on the **Overview** page, in the list of connected Windows servers, select a server from the list to connect to it.
3. From the left-hand pane, select **Azure hybrid services**.
4. On the **Azure hybrid services** page, select **Discover Azure services**.
5. On the **Discover Azure services** page, under **Leverage Azure policies and solutions to manage your servers with Azure Arc**, select **Set up**.
6. On the **Settings\Azure Arc for servers** page, if prompted authenticate to Azure and then select **Get started**.
7. On the **Connect server to Azure** page, provide the following:

   a. In the **Azure subscription** drop-down list, select the Azure subscription.
   b. For **Resource group**, either select **New** to create a new resource group, or under the **Resource group** drop-down list, select an existing resource group to register and manage the machine from.
   c. In the **Region** drop-down list, select the Azure region to store the servers metadata.
   d. If the machine or server is communicating through a proxy server to connect to the internet, select the option **Use proxy server**. Using this configuration, the agent communicates through the proxy server using the HTTP protocol. Specify the proxy server IP address or the name, and port number that the machine will use to communicate with the proxy server.

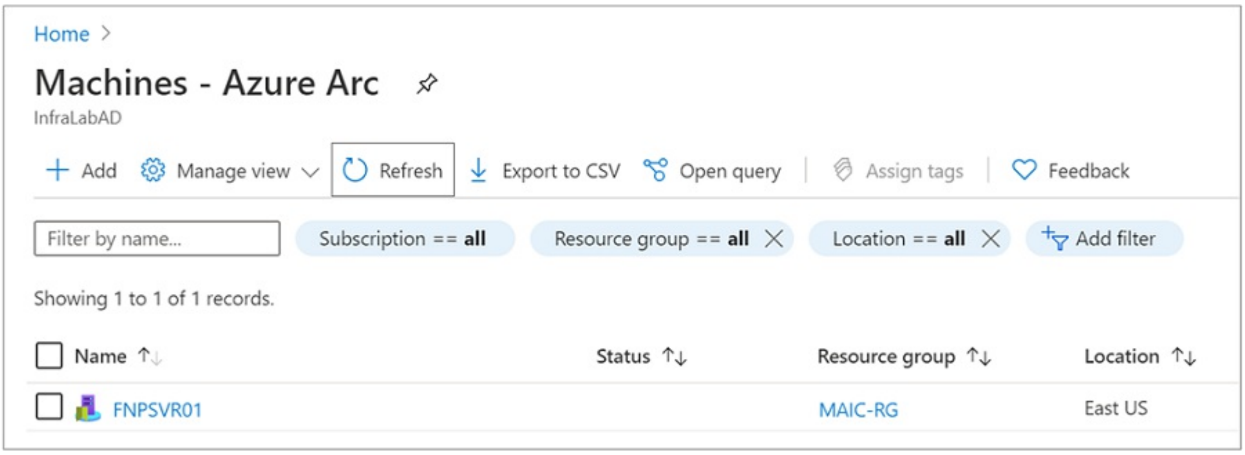
8. Select **Set up** to proceed with configuring the Windows server with Azure Arc-enabled servers.

The Windows server will connect to Azure, download the Connected Machine agent, install it and register with Azure Arc-enabled servers. To track the progress, select **Notifications** in the menu.

To confirm installation of the Connected Machine Agent, in Windows Admin Center select **Events** from the left-hand pane to review *MsiInstaller* events in the Application Event Log.

Verify the connection with Azure Arc

After you install the agent and configure it to connect to Azure Arc-enabled servers, go to the Azure portal to verify that the server has successfully connected. View your machine in the Azure portal.



Subscription == **all** Resource group == **all** Location == **all**

Showing 1 to 1 of 1 records.

Name	Status	Resource group	Location
FNPSVR01		MAIC-RG	East US

Next steps

- Troubleshooting information can be found in the Troubleshoot Connected Machine agent guide.
- Review the Planning and deployment guide to plan for deploying Azure Arc-enabled servers at any scale and implement centralized management and monitoring.
- Learn how to manage your machine using Azure Policy, for such things as VM guest configuration, verifying the machine is reporting to the expected Log Analytics workspace, enable monitoring with VM insights, and much more.

Connect hybrid machines to Azure by using PowerShell

8/17/2021 • 3 minutes to read • Edit Online

For servers enabled with Azure Arc, you can take manual steps to enable them for one or more Windows or Linux machines in your environment. Alternatively, you can use the PowerShell cmdlet Connect-AzConnectedMachine to download the Connected Machine agent, install the agent, and register the machine with Azure Arc. The cmdlet downloads the Windows agent package (Windows Installer) from the Microsoft Download Center, and the Linux agent package from the Microsoft package repository.

This method requires that you have administrator permissions on the machine to install and configure the agent. On Linux, by using the root account, and on Windows, you are member of the Local Administrators group. You can complete this process interactively or remotely on a Windows server by using PowerShell remoting.

Before you get started, review the prerequisites and verify that your subscription and resources meet the requirements. For information about supported regions and other related considerations, see supported Azure regions.

If you don't have an Azure subscription, create a free account before you begin.

Prerequisites

- A machine with Azure PowerShell. For instructions, see Install and configure Azure PowerShell.

You use PowerShell to manage VM extensions on your hybrid servers managed by Azure Arc-enabled servers. Before using PowerShell, install the `Az.ConnectedMachine` module. Run the following command on your server enabled with Azure Arc:

```
Install-Module -Name Az.ConnectedMachine
```

When the installation finishes, you see the following message:

```
The installed extension ``Az.ConnectedMachine`` is experimental and not covered by customer support. Please
use with discretion.
```

Install the agent and connect to Azure

1. Open a PowerShell console with elevated privileges.

2. Sign in to Azure by running the command `Connect-AzAccount`.

3. To install the Connected Machine agent, use `Connect-AzConnectedMachine` with the `-Name`, `-ResourceGroupName`, and `-Location` parameters. Use the `-SubscriptionId` parameter to override the default subscription as a result of the Azure context created after sign-in. Run one of the following commands:

    - To install the Connected Machine agent on the target machine that can directly communicate to Azure, run:

```
Connect-AzConnectedMachine -ResourceGroupName myResourceGroup -Name myMachineName -Location
<region>
```

- To install the Connected Machine agent on the target machine that communicates through a proxy server, run:

  ```
  Connect-AzConnectedMachine -ResourceGroupName myResourceGroup -Name myMachineName -Location
  <region> -Proxy http://<proxyURL>:<proxyport>
  ```

  Using this configuration, the agent communicates through the proxy server using the HTTP protocol.

If the agent fails to start after setup is finished, check the logs for detailed error information. On Windows, check this file: *%ProgramData%\AzureConnectedMachineAgent\Log\himds.log*. On Linux, check this file: */var/opt/azcmagent/log/himds.log*.

Install and connect by using PowerShell remoting

Here's how to configure one or more Windows servers with servers enabled with Azure Arc. You must enable PowerShell remoting on the remote machine. Use the `Enable-PSRemoting` cmdlet to do this.

1. Open a PowerShell console as an Administrator.

2. Sign in to Azure by running the command `Connect-AzAccount`.

3. To install the Connected Machine agent, use `Connect-AzConnectedMachine` with the `-ResourceGroupName`, and `-Location` parameters. The Azure resource names will automatically use the hostname of each server. Use the `-SubscriptionId` parameter to override the default subscription as a result of the Azure context created after sign-in.

   - To install the Connected Machine agent on the target machine that can directly communicate to Azure, run the following command:

     ```
     $sessions = New-PSSession -ComputerName myMachineName
     Connect-AzConnectedMachine -ResourceGroupName myResourceGroup -Location <region> -PSSession
     $sessions
     ```

   - To install the Connected Machine agent on multiple remote machines at the same time, add a list of remote machine names, each separated by a comma.

     ```
     $sessions = New-PSSession -ComputerName myMachineName1, myMachineName2, myMachineName3
     Connect-AzConnectedMachine -ResourceGroupName myResourceGroup -Location <region> -PSSession
     $sessions
     ```

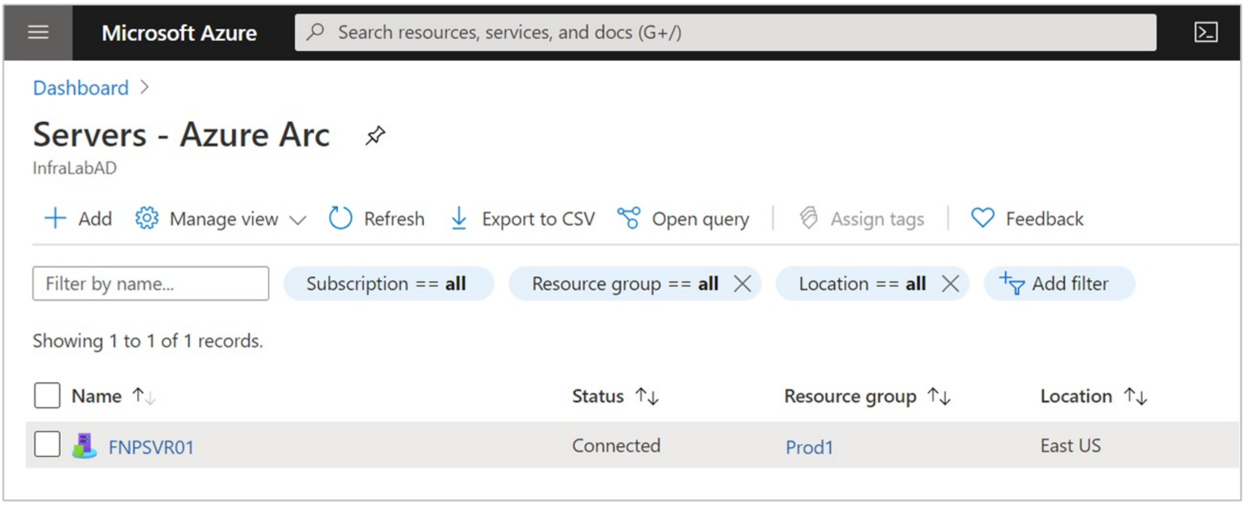
   The following example shows the results of the command targeting a single machine:

```
time="2020-08-07T13:13:25-07:00" level=info msg="Onboarding Machine. It usually takes a few minutes
to complete. Sometimes it may take longer depending on network and server load status."
time="2020-08-07T13:13:25-07:00" level=info msg="Check network connectivity to all endpoints..."
time="2020-08-07T13:13:29-07:00" level=info msg="All endpoints are available... continue onboarding"
time="2020-08-07T13:13:50-07:00" level=info msg="Successfully Onboarded Resource to Azure" VM
Id=f65bffc7-4734-483e-b3ca-3164bfa42941

Name          Location OSName  Status    ProvisioningState
----          -------- ------  ------    -----------------
myMachineName eastus   windows Connected Succeeded
```

Verify the connection with Azure Arc

After you install and configure the agent to register with Azure Arc-enabled servers, go to the Azure portal to verify that the server has successfully connected. View your machine in the Azure portal.



Showing 1 to 1 of 1 records.

□ Name	Status	Resource group	Location
□ FNPSVR01	Connected	Prod1	East US

Next steps

- If necessary, see the Troubleshoot Connected Machine agent guide.
- Review the Planning and deployment guide to plan for deploying Azure Arc-enabled servers at any scale and implement centralized management and monitoring.
- Learn how to manage your machine by using Azure Policy. You can use VM guest configuration, verify that the machine is reporting to the expected Log Analytics workspace, and enable monitoring with VM insights.

Migrate your on-premises or other cloud Azure Arc-enabled server to Azure

9/7/2021 • 4 minutes to read • Edit Online

This article is intended to help you plan and successfully migrate your on-premises server or virtual machine managed by Azure Arc-enabled servers to Azure. By following these steps, you are able to transition management from Azure Arc-enabled servers based on the supported VM extensions installed and Azure services based on its Arc server resource identity.

Before performing these steps, review the Azure Migrate Prepare on-premises machines for migration to Azure article to understand requirements how to prepare for using Azure Migrate.

In this article, you:

- Inventory Azure Arc-enabled servers supported VM extensions installed.
- Uninstall all VM extensions from the Azure Arc-enabled server.
- Identify Azure services configured to authenticate with your Azure Arc-enabled server-managed identity and prepare to update those services to use the Azure VM identity after migration.
- Review Azure role-based access control (Azure RBAC) access rights granted to the Azure Arc-enabled server resource to maintain who has access to the resource after it has been migrated to an Azure VM.
- Delete the Azure Arc-enabled server resource identity from Azure and remove the Azure Arc-enabled server agent.
- Install the Azure guest agent.
- Migrate the server or VM to Azure.

Step 1: Inventory and remove VM extensions

To inventory the VM extensions installed on your Azure Arc-enabled server, you can list them using the Azure CLI or with Azure PowerShell.

With Azure PowerShell, use the Get-AzConnectedMachineExtension command with the `-MachineName` and `-ResourceGroupName` parameters.

With the Azure CLI, use the az connectedmachine extension list command with the `--machine-name` and `--resource-group` parameters. By default, the output of Azure CLI commands is in JSON (JavaScript Object Notation). To change the default output to a list or table, for example, use az configure --output. You can also add `--output` to any command for a one time change in output format.

After identifying which VM extensions are deployed, you can remove them using the Azure portal, using the Azure PowerShell, or using the Azure CLI. If the Log Analytics VM extension or Dependency agent VM extension was deployed using Azure Policy and the VM insights initiative, it is necessary to create an exclusion to prevent re-evaluation and deployment of the extensions on the Azure Arc-enabled server before the migration is complete.

Step 2: Review access rights

List role assignments for the Azure Arc-enabled servers resource, using Azure PowerShell and with other PowerShell code, you can export the results to CSV or another format.

If you're using a managed identity for an application or process running on an Azure Arc-enabled server, you need to make sure the Azure VM has a managed identity assigned. To view the role assignment for a managed identity, you can use the Azure PowerShell `Get-AzADServicePrincipal` cmdlet. For more information, see List role assignments for a managed identity.

A system-managed identity is also used when Azure Policy is used to audit or configure settings inside a machine or server. With Azure Arc-enabled servers, the guest configuration agent service is included, and performs validation of audit settings. After you migrate, see Deploy requirements for Azure virtual machines for information on how to configure your Azure VM manually or with policy with the guest configuration extension.

Update role assignment with any resources accessed by the managed identity to allow the new Azure VM identity to authenticate to those services. See the following to learn how managed identities for Azure resources work for an Azure Virtual Machine (VM).

Step 3: Disconnect from Azure Arc and uninstall agent

Delete the resource ID of the Azure Arc-enabled server in Azure using one of the following methods:

- Running `azcmagent disconnect` command on the machine or server.
- From the selected registered Azure Arc-enabled server in the Azure portal by selecting **Delete** from the top bar.
- Using the Azure CLI or Azure PowerShell. For the `ResourceType` parameter use `Microsoft.HybridCompute/machines`.

Then, remove the Azure Arc-enabled servers Windows or Linux agent following the Remove agent steps.

Step 4: Install the Azure Guest Agent

The VM that is migrated to Azure from on-premises doesn't have the Linux or Windows Azure Guest Agent installed. In these scenarios, you have to manually install the VM agent. For more information about how to install the VM Agent, see Azure Virtual Machine Windows Agent Overview or Azure Virtual Machine Linux Agent Overview.

Step 5: Migrate server or machine to Azure

Before proceeding with the migration with Azure Migration, review the Prepare on-premises machines for migration to Azure article to learn about requirements necessary to use Azure Migrate. To complete the migration to Azure, review the Azure Migrate migration options based on your environment.

Step 6: Deploy Azure VM extensions

After migration and completion of all post-migration configuration steps, you can now deploy the Azure VM extensions based on the VM extensions originally installed on your Azure Arc-enabled server. Review Azure virtual machine extensions and features to help plan your extension deployment.

To resume using audit settings inside a machine with guest configuration policy definitions, see Enable guest configuration.

If the Log Analytics VM extension or Dependency agent VM extension was deployed using Azure Policy and the VM insights initiative, remove the exclusion you created earlier. To use Azure Policy to enable Azure virtual machines, see Deploy Azure Monitor at scale using Azure Policy.

Next steps

Troubleshooting information can be found in the Troubleshoot Connected Machine agent guide.

Virtual machine extension management with Azure Arc-enabled servers

9/7/2021 • 4 minutes to read • Edit Online

Virtual machine (VM) extensions are small applications that provide post-deployment configuration and automation tasks on Azure VMs. For example, if a virtual machine requires software installation, anti-virus protection, or to run a script in it, a VM extension can be used.

Azure Arc-enabled servers enables you to deploy, remove, and update Azure VM extensions to non-Azure Windows and Linux VMs, simplifying the management of your hybrid machine through their lifecycle. VM extensions can be managed using the following methods on your hybrid machines or servers managed by Arc-enabled servers:

- The Azure portal
- The Azure CLI
- Azure PowerShell
- Azure Resource Manager templates

> **NOTE**
>
> Azure Arc-enabled servers does not support deploying and managing VM extensions to Azure virtual machines. For Azure VMs, see the following VM extension overview article.

> **NOTE**
>
> Currently you can only update extensions from the Azure portal. Performing this operation from the Azure CLI, Azure PowerShell, or using an Azure Resource Manager template is not supported at this time.

Key benefits

Azure Arc-enabled servers VM extension support provides the following key benefits:

- Collect log data for analysis with Logs in Azure Monitor by enabling the Log Analytics agent VM extension. Log Analytics makes it useful for doing complex analysis across log data from different kinds of sources.
- With VM insights, it analyzes the performance of your Windows and Linux VMs, and monitors their processes and dependencies on other resources and external processes. This is achieved through enabling both the Log Analytics agent and Dependency agent VM extensions.
- Download and execute scripts on hybrid connected machines using the Custom Script Extension. This extension is useful for post deployment configuration, software installation, or any other configuration or management tasks.
- Automatically refresh of certificates stored in an Azure Key Vault.

Availability

VM extension functionality is available only in the list of supported regions. Ensure you onboard your machine in one of these regions.

Extensions

In this release, we support the following VM extensions on Windows and Linux machines.

To learn about the Azure Connected Machine agent package and details about the Extension agent component, see Agent overview.

NOTE

Recently support for the DSC VM extension was removed for Azure Arc-enabled servers. Alternatively, we recommend using the Custom Script Extension to manage the post-deployment configuration of your server or machine.

Arc-enabled servers support moving machines with one or more VM extensions installed between resource groups or another Azure subscription without experiencing any impact to their configuration. The source and destination subscriptions must exist within the same Azure Active Directory tenant. This support is enabled starting with the Connected Machine agent version `1.8.21197.005`. For more information about moving resources and considerations before proceeding, see Move resources to a new resource group or subscription.

Windows extensions

EXTENSION	PUBLISHER	TYPE	ADDITIONAL INFORMATION
Azure Defender integrated vulnerability scanner	Qualys	WindowsAgent.AzureSecurityCenter	Azure Defender's integrated vulnerability assessment solution for Azure and hybrid machines
Custom Script extension	Microsoft.Compute	CustomScriptExtension	Windows Custom Script Extension
Log Analytics agent	Microsoft.EnterpriseCloud.Monitoring	MicrosoftMonitoringAgent	Log Analytics VM extension for Windows
Azure Monitor for VMs (insights)	Microsoft.Azure.Monitoring.DependencyAgent	DependencyAgentWindows	Dependency agent virtual machine extension for Windows
Azure Key Vault Certificate Sync	Microsoft.Azure.Key.Vault	KeyVaultForWindows	Key Vault virtual machine extension for Windows
Azure Monitor Agent	Microsoft.Azure.Monitor	AzureMonitorWindowsAgent	Install the Azure Monitor agent (preview)

Linux extensions

EXTENSION	PUBLISHER	TYPE	ADDITIONAL INFORMATION
Azure Defender integrated vulnerability scanner	Qualys	LinuxAgent.AzureSecurityCenter	Azure Defender's integrated vulnerability assessment solution for Azure and hybrid machines

EXTENSION	PUBLISHER	TYPE	ADDITIONAL INFORMATION
Custom Script extension	Microsoft.Azure.Extensions	CustomScript	Linux Custom Script Extension Version 2
Log Analytics agent	Microsoft.EnterpriseCloud.Monitoring	OmsAgentForLinux	Log Analytics VM extension for Linux
Azure Monitor for VMs (insights)	Microsoft.Azure.Monitoring.DependencyAgent	DependencyAgentLinux	Dependency agent virtual machine extension for Linux
Azure Key Vault Certificate Sync	Microsoft.Azure.Key.Vault	KeyVaultForLinux	Key Vault virtual machine extension for Linux
Azure Monitor Agent	Microsoft.Azure.Monitor	AzureMonitorLinuxAgent	Install the Azure Monitor agent (preview)

Prerequisites

This feature depends on the following Azure resource providers in your subscription:

- **Microsoft.HybridCompute**
- **Microsoft.GuestConfiguration**

If they aren't already registered, follow the steps under Register Azure resource providers.

Be sure to review the documentation for each VM extension referenced in the previous table to understand if it has any network or system requirements. This can help you avoid experiencing any connectivity issues with an Azure service or feature that relies on that VM extension.

Log Analytics VM extension

The Log Analytics agent VM extension for Linux requires Python 2.x is installed on the target machine.

Azure Key Vault VM extension

The Key Vault VM extension doesn't support the following Linux operating systems:

- CentOS Linux 7 (x64)
- Red Hat Enterprise Linux (RHEL) 7 (x64)
- Amazon Linux 2 (x64)

Deploying the Key Vault VM extension is only supported using:

- The Azure CLI
- The Azure PowerShell
- Azure Resource Manager template

Before you deploy the extension, you need to complete the following:

1. Create a vault and certificate (self-signed or import).

2. Grant the Azure Arc-enabled server access to the certificate secret. If you're using the RBAC preview, search for the name of the Azure Arc resource and assign it the **Key Vault Secrets User (preview)** role. If you're using Key Vault access policy, assign Secret **Get** permissions to the Azure Arc resource's system assigned identity.

Connected Machine agent

Verify your machine matches the supported versions of Windows and Linux operating system for the Azure Connected Machine agent.

The minimum version of the Connected Machine agent that is supported with this feature on Windows and Linux is the 1.0 release.

To upgrade your machine to the version of the agent required, see Upgrade agent.

Next steps

You can deploy, manage, and remove VM extensions using the Azure CLI, Azure PowerShell, from the Azure portal, or Azure Resource Manager templates.

Enable Azure VM extensions from the Azure portal

9/7/2021 • 3 minutes to read • Edit Online

This article shows you how to deploy, update, and uninstall Azure VM extensions supported by Azure Arc enabled servers, on a Linux or Windows hybrid machine using the Azure portal.

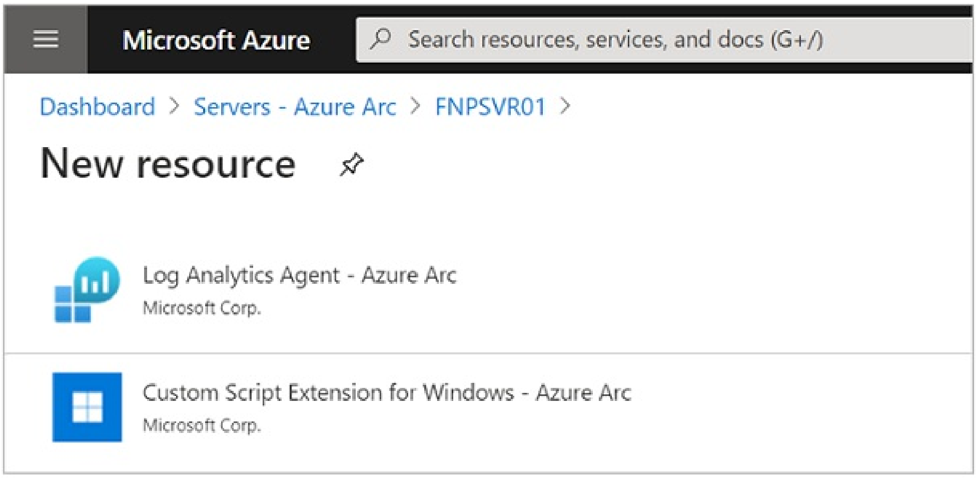
> **NOTE**
>
> The Key Vault VM extension does not support deployment from the Azure portal, only using the Azure CLI, the Azure PowerShell, or using an Azure Resource Manager template.

> **NOTE**
>
> Azure Arc-enabled servers does not support deploying and managing VM extensions to Azure virtual machines. For Azure VMs, see the following VM extension overview article.

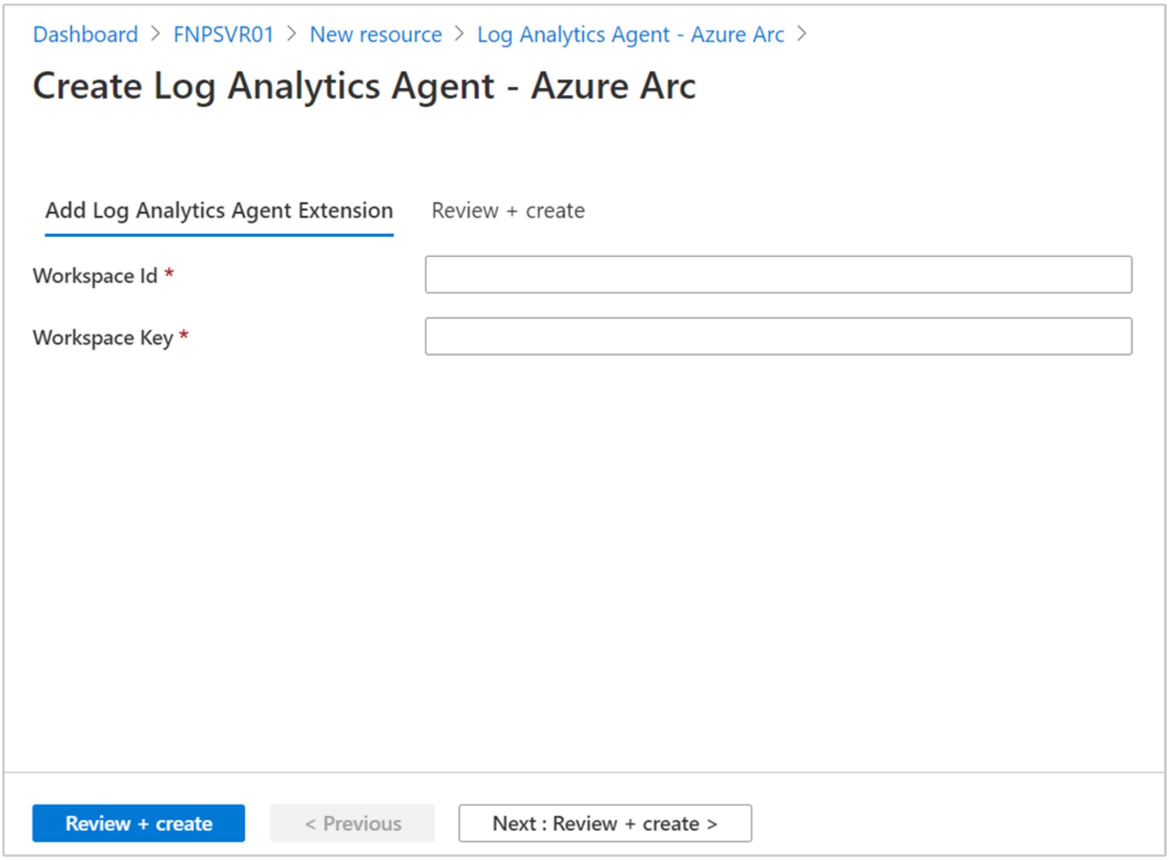
Enable extensions

VM extensions can be applied to your Azure Arc-enabled server-managed machine via the Azure portal.

1. From your browser, go to the Azure portal.
2. In the portal, browse to **Servers - Azure Arc** and select your hybrid machine from the list.
3. Choose **Extensions**, then select **Add**. Choose the extension you want from the list of available extensions and follow the instructions in the wizard. In this example, we will deploy the Log Analytics VM extension.


Microsoft Azure
Search resources, services, and docs (G+/)
Dashboard > Servers - Azure Arc > FNPSVR01 >
New resource
Log Analytics Agent - Azure Arc
Microsoft Corp.
Custom Script Extension for Windows - Azure Arc
Microsoft Corp.

The following example shows the installation of the Log Analytics VM extension from the Azure portal:



Dashboard > FNPSVR01 > New resource > Log Analytics Agent - Azure Arc >

Create Log Analytics Agent - Azure Arc

Add Log Analytics Agent Extension | Review + create

Workspace Id *

Workspace Key *

Review + create | < Previous | Next : Review + create >

To complete the installation, you are required to provide the workspace ID and primary key. If you are not familiar with how to find this information, see obtain workspace ID and key.

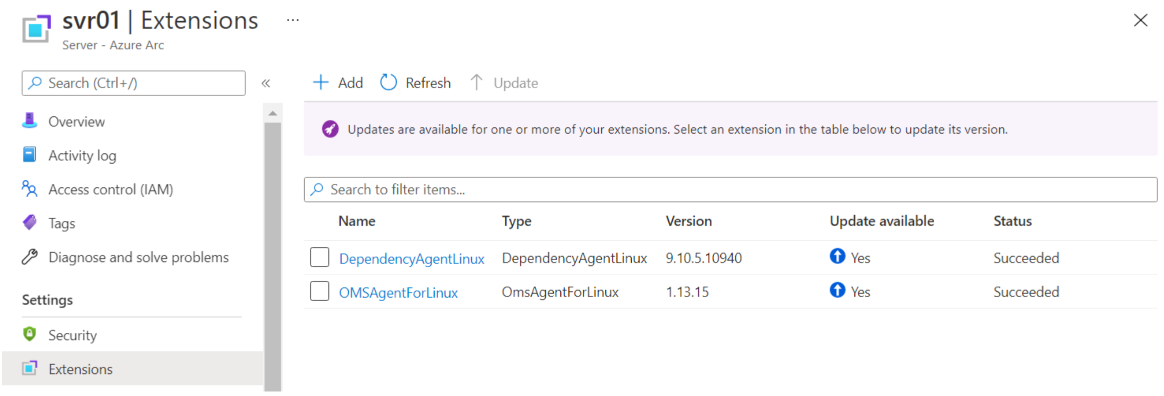
4. After confirming the required information provided, select **Review + Create**. A summary of the deployment is displayed and you can review the status of the deployment.

> **NOTE**
>
> While multiple extensions can be batched together and processed, they are installed serially. Once the first extension installation is complete, installation of the next extension is attempted.

List extensions installed

You can get a list of the VM extensions on your Azure Arc-enabled server from the Azure portal. Perform the following steps to see them.

1. From your browser, go to the Azure portal.
2. In the portal, browse to **Servers - Azure Arc** and select your hybrid machine from the list.
3. Choose **Extensions**, and the list of installed extensions is returned.



svr01 | Extensions
Server - Azure Arc

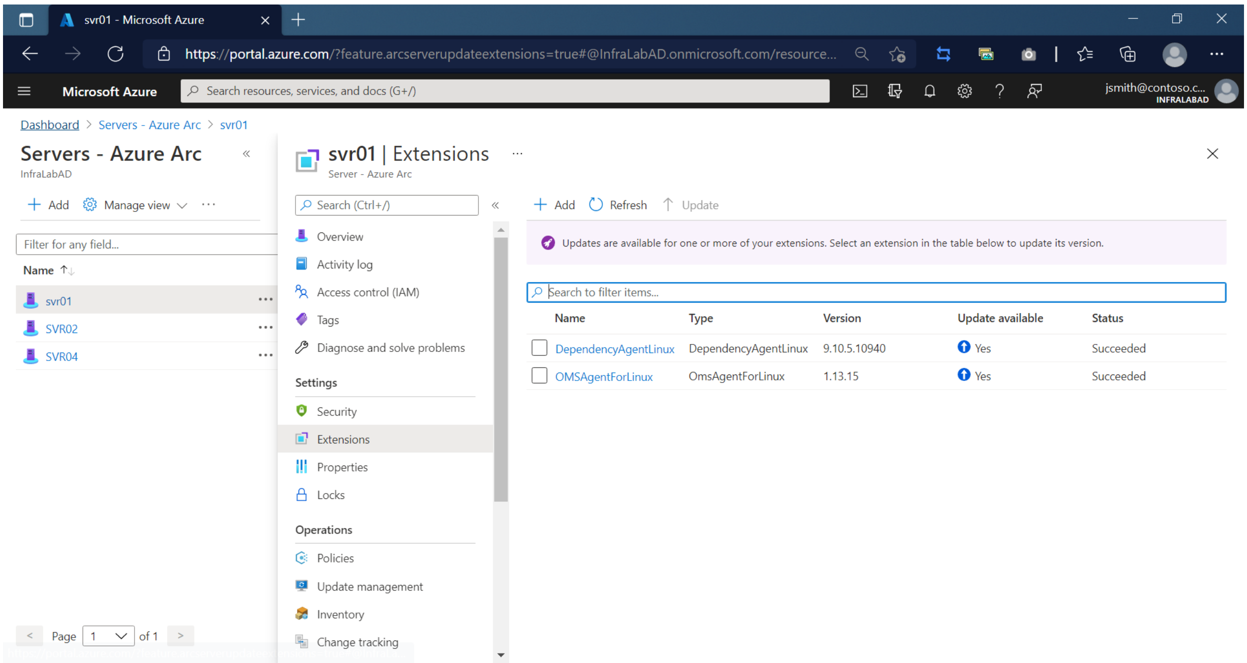
Updates are available for one or more of your extensions. Select an extension in the table below to update its version.

Name	Type	Version	Update available	Status
□ DependencyAgentLinux	DependencyAgentLinux	9.10.5.10940	Yes	Succeeded
□ OMSAgentForLinux	OmsAgentForLinux	1.13.15	Yes	Succeeded

Update extensions

When a new version of a supported extension is released, you can update the extension to that latest release. Arc enabled servers will present a banner in the Azure portal when you navigate to Arc enabled servers, informing you there are updates available for one or more extensions installed on a machine. When you view the list of installed extensions for a selected Arc enabled server, you'll notice a column labeled **Update available**. If a newer version of an extension is released, the **Update available** value for that extension shows a value of **Yes**.

Updating an extension to the newest version does not affect the configuration of that extension. You are not required to respecify configuration information for any extension you update.



Updates are available for one or more of your extensions. Select an extension in the table below to update its version.

Name	Type	Version	Update available	Status
☐ DependencyAgentLinux	DependencyAgentLinux	9.10.5.10940	Yes	Succeeded
☐ OMSAgentForLinux	OmsAgentForLinux	1.13.15	Yes	Succeeded

You can update one or select multiple extensions eligible for an update from the Azure portal by performing the following steps.

> **NOTE**
>
> Currently you can only update extensions from the Azure portal. Performing this operation from the Azure CLI, Azure PowerShell, or using an Azure Resource Manager template is not supported at this time.

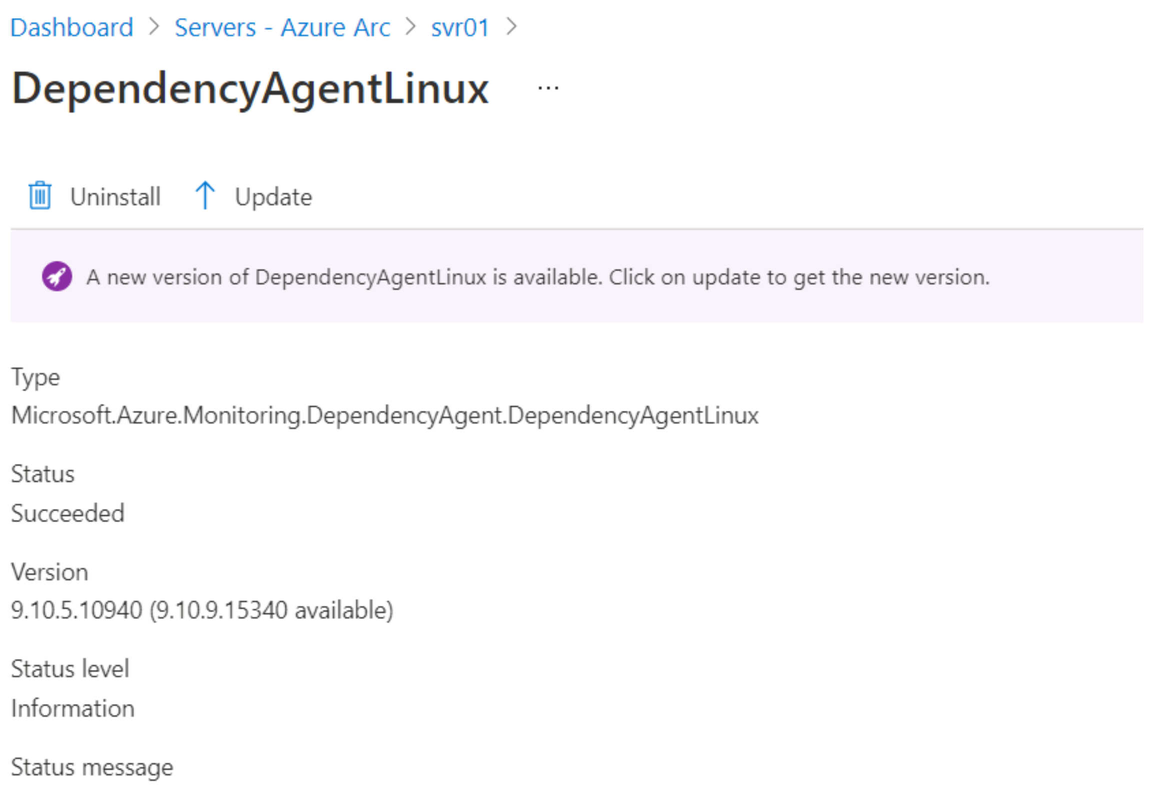
1. From your browser, go to the Azure portal.

2. In the portal, browse to **Servers - Azure Arc** and select your hybrid machine from the list.

3. Choose **Extensions**, and review the status of extensions under the **Update available** column.

You can update one extension by one of three ways:

- By selecting an extension from the list of installed extensions, and under the properties of the extension, select the **Update** option.



Dashboard > Servers - Azure Arc > svr01 >

DependencyAgentLinux ...

Uninstall Update

A new version of DependencyAgentLinux is available. Click on update to get the new version.

Type
Microsoft.Azure.Monitoring.DependencyAgent.DependencyAgentLinux

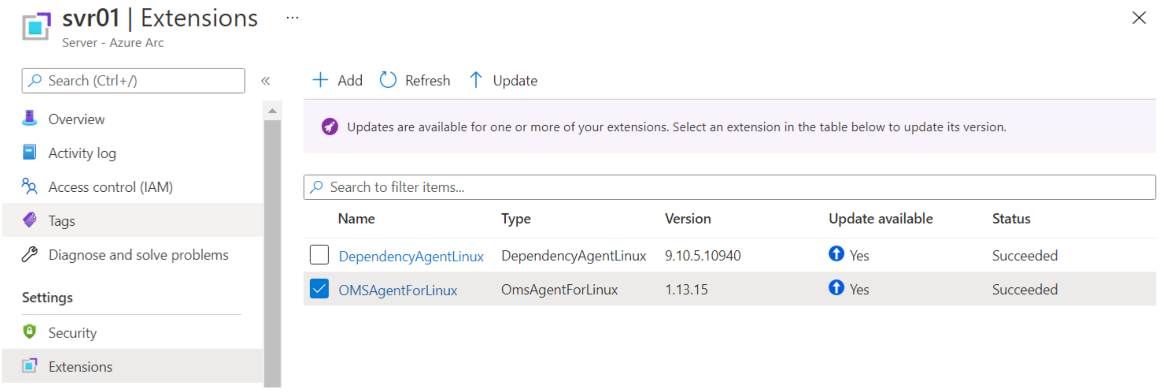
Status
Succeeded

Version
9.10.5.10940 (9.10.9.15340 available)

Status level
Information

Status message

- By selecting the extension from the list of installed extensions, and select the **Update** option from the top of the page.
- By selecting one or more extensions that are eligible for an update from the list of installed extensions, and then select the **Update** option.



svr01 | Extensions ...
Server - Azure Arc

Updates are available for one or more of your extensions. Select an extension in the table below to update its version.

Search to filter items...

	Name	Type	Version	Update available	Status
□	DependencyAgentLinux	DependencyAgentLinux	9.10.5.10940	Yes	Succeeded
☑	OMSAgentForLinux	OmsAgentForLinux	1.13.15	Yes	Succeeded

Uninstall extensions

You can remove one or more extensions from an Azure Arc-enabled server from the Azure portal. Perform the following steps to remove an extension.

1. From your browser, go to the Azure portal.
2. In the portal, browse to **Servers - Azure Arc** and select your hybrid machine from the list.
3. Choose **Extensions**, and then select an extension from the list of installed extensions.
4. Select **Uninstall** and when prompted to verify, select **Yes** to proceed.

Next steps

- You can deploy, manage, and remove VM extensions using the Azure CLI, PowerShell, or Azure Resource Manager templates.

- Troubleshooting information can be found in the Troubleshoot VM extensions guide.

Enable Azure VM extensions using the Azure CLI

9/7/2021 • 2 minutes to read • Edit Online

This article shows you how to deploy and uninstall VM extensions, supported by Azure Arc-enabled servers, to a Linux or Windows hybrid machine using the Azure CLI.

> **NOTE**
>
> Azure Arc-enabled servers does not support deploying and managing VM extensions to Azure virtual machines. For Azure VMs, see the following VM extension overview article.

Prerequisites

- Use the Bash environment in Azure Cloud Shell.

  Launch Cloud Shell

- If you prefer, install the Azure CLI to run CLI reference commands.
  - If you're using a local installation, sign in to the Azure CLI by using the az login command. To finish the authentication process, follow the steps displayed in your terminal. For additional sign-in options, see Sign in with the Azure CLI.
  - When you're prompted, install Azure CLI extensions on first use. For more information about extensions, see Use extensions with the Azure CLI.
  - Run az version to find the version and dependent libraries that are installed. To upgrade to the latest version, run az upgrade.

Install the Azure CLI extension

The ConnectedMachine commands aren't shipped as part of the Azure CLI. Before using the Azure CLI to manage VM extensions on your hybrid server managed by Azure Arc-enabled servers, you need to load the ConnectedMachine extension. Run the following command to get it:

```
az extension add --name connectedmachine
```

Enable extension

To enable a VM extension on your Azure Arc-enabled server, use az connectedmachine extension create with the `--machine-name`, `--extension-name`, `--location`, `--type`, `settings`, and `--publisher` parameters.

The following example enables the Log Analytics VM extension on an Azure Arc-enabled server:

```
az connectedmachine extension create --machine-name "myMachineName" --name "OmsAgentForLinux or
MicrosoftMonitoringAgent" --location "eastus" --settings '{\"workspaceId\":\"myWorkspaceId\"}' --protected-
settings '{\"workspaceKey\":\"myWorkspaceKey\"}' --resource-group "myResourceGroup" --type-handler-version
"1.13" --type "OmsAgentForLinux or MicrosoftMonitoringAgent" --publisher
"Microsoft.EnterpriseCloud.Monitoring"
```

The following example enables the Custom Script Extension on an Azure Arc-enabled server:

```
az connectedmachine extension create --machine-name "myMachineName" --name "CustomScriptExtension" --
location "eastus" --type "CustomScriptExtension" --publisher "Microsoft.Compute" --settings "
{\"commandToExecute\":\"powershell.exe -c \\\"Get-Process | Where-Object { $_.CPU -gt 10000 }\\\"\"}" --
type-handler-version "1.10" --resource-group "myResourceGroup"
```

The following example enables the Key Vault VM extension on an Azure Arc-enabled server:

```
az connectedmachine extension create --resource-group "resourceGroupName" --machine-name "myMachineName" --
location "regionName" --publisher "Microsoft.Azure.KeyVault" --type "KeyVaultForLinux or KeyVaultForWindows"
--name "KeyVaultForLinux or KeyVaultForWindows" --settings '{"secretsManagementSettings": {
"pollingIntervalInS": "60", "observedCertificates": ["observedCert1"] }, "authenticationSettings": {
"msiEndpoint": "http://localhost:40342/metadata/identity" }}'
```

List extensions installed

To get a list of the VM extensions on your Azure Arc-enabled server, use az connectedmachine extension list with the `--machine-name` and `--resource-group` parameters.

Example:

```
az connectedmachine extension list --machine-name "myMachineName" --resource-group "myResourceGroup"
```

By default, the output of Azure CLI commands is in JSON (JavaScript Object Notation). To change the default output to a list or table, for example, use az config set core.output=table. You can also add `--output` to any command for a one time change in output format.

The following example shows the partial JSON output from the `az connectedmachine extension -list` command:

```
[
  {
    "autoUpgradingMinorVersion": "false",
    "forceUpdateTag": null,
    "id":
"/subscriptions/subscriptionId/resourceGroups/resourceGroupName/providers/Microsoft.HybridCompute/machines/S
VR01/extensions/DependencyAgentWindows",
    "location": "eastus",
    "name": "DependencyAgentWindows",
    "namePropertiesInstanceViewName": "DependencyAgentWindows",
```

Remove an installed extension

To remove an installed VM extension on your Azure Arc-enabled server, use az connectedmachine extension delete with the `--extension-name`, `--machine-name` and `--resource-group` parameters.

For example, to remove the Log Analytics VM extension for Linux, run the following command:

```
az connectedmachine extension delete --machine-name "myMachineName" --name "OmsAgentForLinux" --resource-
group "myResourceGroup"
```

Next steps

- You can deploy, manage, and remove VM extensions using the Azure PowerShell, from the Azure portal, or Azure Resource Manager templates.

- Troubleshooting information can be found in the Troubleshoot VM extensions guide.
- Review the Azure CLI VM extension Overview article for more information about the commands.

Enable Azure VM extensions using Azure PowerShell

9/7/2021 • 2 minutes to read • Edit Online

This article shows you how to deploy and uninstall Azure VM extensions, supported by Azure Arc-enabled servers, to a Linux or Windows hybrid machine using Azure PowerShell.

> **NOTE**
>
> Azure Arc-enabled servers does not support deploying and managing VM extensions to Azure virtual machines. For Azure VMs, see the following VM extension overview article.

Prerequisites

- A computer with Azure PowerShell. For instructions, see Install and configure Azure PowerShell.

Before using Azure PowerShell to manage VM extensions on your hybrid server managed by Azure Arc-enabled servers, you need to install the `Az.ConnectedMachine` module. Run the following command on your Azure Arc-enabled server:

`Install-Module -Name Az.ConnectedMachine`.

When the installation completes, the following message is returned:

`The installed extension` Az.ConnectedMachine

`is experimental and not covered by customer support. Please use with discretion.`

Enable extension

To enable a VM extension on your Azure Arc-enabled server, use New-AzConnectedMachineExtension with the `-Name`, `-ResourceGroupName`, `-MachineName`, `-Location`, `-Publisher`, - `ExtensionType`, and `-Settings` parameters.

The following example enables the Log Analytics VM extension on a Azure Arc-enabled Linux server:

```
PS C:\> $Setting = @{ "workspaceId" = "workspaceId" }
PS C:\> $protectedSetting = @{ "workspaceKey" = "workspaceKey" }
PS C:\> New-AzConnectedMachineExtension -Name OMSLinuxAgent -ResourceGroupName "myResourceGroup" -
MachineName "myMachine" -Location "eastus" -Publisher "Microsoft.EnterpriseCloud.Monitoring" -Settings
$Setting -ProtectedSetting $protectedSetting -ExtensionType "OmsAgentForLinux"
```

To enable the Log Analytics VM extension on an Azure Arc-enabled Windows server, change the value for the `-ExtensionType` parameter to `"MicrosoftMonitoringAgent"` in the previous example.

The following example enables the Custom Script Extension on an Azure Arc-enabled server:

```
PS C:\> $Setting = @{ "commandToExecute" = "powershell.exe -c Get-Process" }
PS C:\> New-AzConnectedMachineExtension -Name custom -ResourceGroupName myResourceGroup -MachineName
myMachineName -Location eastus -Publisher "Microsoft.Compute"  -Settings $Setting -ExtensionType
CustomScriptExtension
```

Key Vault VM extension

WARNING

PowerShell clients often add `\` to `"` in the settings.json which will cause akvvm_service fails with error: `[CertificateManagementConfiguration] Failed to parse the configuration settings with:not an object.`

The following example enables the Key Vault VM extension on an Azure Arc-enabled server:

```
# Build settings
    $settings = @{
      secretsManagementSettings = @{
       observedCertificates = @(
        "observedCert1"
       )
      certificateStoreLocation = "myMachineName" # For Linux use
"/var/lib/waagent/Microsoft.Azure.KeyVault.Store/"
      certificateStore = "myCertificateStoreName"
      pollingIntervalInS = "pollingInterval"
      }
    authenticationSettings = @{
     msiEndpoint = "http://localhost:40342/metadata/identity"
     }
    }

    $resourceGroup = "resourceGroupName"
    $machineName = "myMachineName"
    $location = "regionName"

    # Start the deployment
    New-AzConnectedMachineExtension -ResourceGroupName $resourceGRoup -Location $location -MachineName
$machineName -Name "KeyVaultForWindows or KeyVaultforLinux" -Publisher "Microsoft.Azure.KeyVault" -
ExtensionType "KeyVaultforWindows or KeyVaultforLinux" -Setting (ConvertTo-Json $settings)
```

List extensions installed

To get a list of the VM extensions on your Azure Arc-enabled server, use Get-AzConnectedMachineExtension with the `-MachineName` and `-ResourceGroupName` parameters.

Example:

```
Get-AzConnectedMachineExtension -ResourceGroupName myResourceGroup -MachineName myMachineName

Name    Location  PropertiesType        ProvisioningState
----    --------  --------------        -----------------
custom  westus2   CustomScriptExtension Succeeded
```

Remove an installed extension

To remove an installed VM extension on your Azure Arc-enabled server, use Remove-AzConnectedMachineExtension with the `-Name`, `-MachineName` and `-ResourceGroupName` parameters.

For example, to remove the Log Analytics VM extension for Linux, run the following command:

```
Remove-AzConnectedMachineExtension -MachineName myMachineName -ResourceGroupName myResourceGroup -Name
OmsAgentforLinux
```

Next steps

- You can deploy, manage, and remove VM extensions using the Azure CLI, from the Azure portal, or Azure Resource Manager templates.
- Troubleshooting information can be found in the Troubleshoot VM extensions guide.

Enable Azure VM extensions by using ARM template

9/7/2021 • 8 minutes to read • Edit Online

This article shows you how to use an Azure Resource Manager template (ARM template) to deploy Azure VM extensions, supported by Azure Arc-enabled servers.

VM extensions can be added to an Azure Resource Manager template and executed with the deployment of the template. With the VM extensions supported by Azure Arc-enabled servers, you can deploy the supported VM extension on Linux or Windows machines using Azure PowerShell. Each sample below includes a template file and a parameters file with sample values to provide to the template.

> **NOTE**
>
> While multiple extensions can be batched together and processed, they are installed serially. Once the first extension installation is complete, installation of the next extension is attempted.

> **NOTE**
>
> Azure Arc-enabled servers does not support deploying and managing VM extensions to Azure virtual machines. For Azure VMs, see the following VM extension overview article.

Deploy the Log Analytics VM extension

To easily deploy the Log Analytics agent, the following sample is provided to install the agent on either Windows or Linux.

Template file for Linux

```
{
    "$schema": "http://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "vmName": {
            "type": "string"
        },
        "location": {
            "type": "string"
        },
        "workspaceId": {
            "type": "string"
        },
        "workspaceKey": {
            "type": "string"
        }
    },
    "resources": [
        {
            "name": "[concat(parameters('vmName'),'/OMSAgentForLinux')]",
            "type": "Microsoft.HybridCompute/machines/extensions",
            "location": "[parameters('location')]",
            "apiVersion": "2019-08-02-preview",
            "properties": {
                "publisher": "Microsoft.EnterpriseCloud.Monitoring",
                "type": "OmsAgentForLinux",
                "settings": {
                    "workspaceId": "[parameters('workspaceId')]"
                },
                "protectedSettings": {
                    "workspaceKey": "[parameters('workspaceKey')]"
                }
            }
        }
    ]
}
```

Template file for Windows

```
{
    "$schema": "http://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "vmName": {
            "type": "string"
        },
        "location": {
            "type": "string"
        },
        "workspaceId": {
            "type": "string"
        },
        "workspaceKey": {
            "type": "string"
        }
    },
    "resources": [
        {
            "name": "[concat(parameters('vmName'),'/MicrosoftMonitoringAgent')]",
            "type": "Microsoft.HybridCompute/machines/extensions",
            "location": "[parameters('location')]",
            "apiVersion": "2019-08-02-preview",
            "properties": {
                "publisher": "Microsoft.EnterpriseCloud.Monitoring",
                "type": "MicrosoftMonitoringAgent",
                "autoUpgradeMinorVersion": true,
                "settings": {
                    "workspaceId": "[parameters('workspaceId')]"
                },
                "protectedSettings": {
                    "workspaceKey": "[parameters('workspaceKey')]"
                }
            }
        }
    ]
}
```

Parameter file

```
{
    "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentParameters.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "vmName": {
            "value": "<vmName>"
        },
        "location": {
            "value": "<region>"
        },
        "workspaceId": {
            "value": "<MyWorkspaceID>"
        },
        "workspaceKey": {
            "value": "<MyWorkspaceKey>"
        }
    }
}
```

Save the template and parameter files to disk, and edit the parameter file with the appropriate values for your deployment. You can then install the extension on all the connected machines within a resource group with the following command. The command uses the *TemplateFile* parameter to specify the template and the *TemplateParameterFile* parameter to specify a file that contains parameters and parameter values.

```
New-AzResourceGroupDeployment -ResourceGroupName "ContosoEngineering" -TemplateFile
"D:\Azure\Templates\LogAnalyticsAgent.json" -TemplateParameterFile
"D:\Azure\Templates\LogAnalyticsAgentParms.json"
```

Deploy the Custom Script extension

To use the Custom Script extension, the following sample is provided to run on Windows and Linux. If you are unfamiliar with the Custom Script extension, see Custom Script extension for Windows or Custom Script extension for Linux. There are a couple of differing characteristics that you should understand when using this extension with hybrid machines:

- The list of supported operating systems with the Azure VM Custom Script extension is not applicable to Azure Arc-enabled servers. The list of supported OSs for Azure Arc-enabled servers can be found here.
- Configuration details regarding Azure Virtual Machine Scale Sets or Classic VMs are not applicable.
- If your machines need to download a script externally and can only communicate through a proxy server, you need to configure the Connected Machine agent to set the proxy server environmental variable.

The Custom Script extension configuration specifies things like script location and the command to be run. This configuration is specified in an Azure Resource Manager template, provided below for both Linux and Windows hybrid machines.

Template file for Linux

```
{
  "$schema": "http://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "vmName": {
      "type": "string"
    },
    "location": {
      "type": "string"
    },
    "fileUris": {
      "type": "array"
    },
    "commandToExecute": {
      "type": "securestring"
    }
  },
  "resources": [
    {
      "name": "[concat(parameters('vmName'),'/CustomScript')]",
      "type": "Microsoft.HybridCompute/machines/extensions",
      "location": "[parameters('location')]",
      "apiVersion": "2019-08-02-preview",
      "properties": {
        "publisher": "Microsoft.Azure.Extensions",
        "type": "CustomScript",
        "autoUpgradeMinorVersion": true,
        "settings": {},
        "protectedSettings": {
          "commandToExecute": "[parameters('commandToExecute')]",
          "fileUris": "[parameters('fileUris')]"
        }
      }
    }
  ]
}
```

Template file for Windows

```
{
    "$schema": "http://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "vmName": {
            "type": "string"
        },
        "location": {
            "type": "string"
        },
        "fileUris": {
            "type": "string"
        },
        "arguments": {
            "type": "securestring",
            "defaultValue": " "
        }
    },
    "variables": {
        "UriFileNamePieces": "[split(parameters('fileUris'), '/')]",
        "firstFileNameString": "[variables('UriFileNamePieces')[sub(length(variables('UriFileNamePieces')),
1)]]",
        "firstFileNameBreakString": "[split(variables('firstFileNameString'), '?')]",
        "firstFileName": "[variables('firstFileNameBreakString')[0]]"
    },
    "resources": [
        {
            "name": "[concat(parameters('vmName'),'/CustomScriptExtension')]",
            "type": "Microsoft.HybridCompute/machines/extensions",
            "location": "[parameters('location')]",
            "apiVersion": "2019-08-02-preview",
            "properties": {
                "publisher": "Microsoft.Compute",
                "type": "CustomScriptExtension",
                "autoUpgradeMinorVersion": true,
                "settings": {
                    "fileUris": "[split(parameters('fileUris'), ' ')]"
                },
                "protectedSettings": {
                    "commandToExecute": "[concat ('powershell -ExecutionPolicy Unrestricted -File ',
variables('firstFileName'), ' ', parameters('arguments'))]"
                }
            }
        }
    ]
}
```

Parameter file

```
{
  "$schema": "https://schema.management.azure.com/schemas/0.1.2-preview/CreateUIDefinition.MultiVm.json#",
  "handler": "Microsoft.Azure.CreateUIDef",
  "version": "0.1.2-preview",
  "parameters": {
    "basics": [
      {}
    ],
    "steps": [
      {
        "name": "customScriptExt",
        "label": "Add Custom Script Extension",
        "elements": [
          {
            "name": "fileUris",
            "type": "Microsoft.Common.FileUpload",
            "label": "Script files",
            "toolTip": "The script files that will be downloaded to the virtual machine.",
            "constraints": {
              "required": false
            },
            "options": {
              "multiple": true,
              "uploadMode": "url"
            },
            "visible": true
          },
          {
            "name": "commandToExecute",
            "type": "Microsoft.Common.TextBox",
            "label": "Command",
            "defaultValue": "sh script.sh",
            "toolTip": "The command to execute, for example: sh script.sh",
            "constraints": {
              "required": true
            },
            "visible": true
          }
        ]
      }
    ],
    "outputs": {
      "vmName": "[vmName()]",
      "location": "[location()]",
      "fileUris": "[steps('customScriptExt').fileUris]",
      "commandToExecute": "[steps('customScriptExt').commandToExecute]"
    }
  }
}
```

Deploy the Dependency agent extension

To use the Azure Monitor Dependency agent extension, the following sample is provided to run on Windows and Linux. If you are unfamiliar with the Dependency agent, see Overview of Azure Monitor agents.

Template file for Linux

```
{
    "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
    "contentVersion": "1.0.0.0",
  "parameters": {
    "vmName": {
      "type": "string",
      "metadata": {
        "description": "The name of existing Linux machine."
      }
    }
  },
  "variables": {
    "vmExtensionsApiVersion": "2017-03-30"
  },
  "resources": [
    {
      "type": "Microsoft.HybridCompute/machines/extensions",
      "name": "[concat(parameters('vmName'),'/DAExtension')]",
      "apiVersion": "[variables('vmExtensionsApiVersion')]",
      "location": "[resourceGroup().location]",
      "dependsOn": [
      ],
      "properties": {
        "publisher": "Microsoft.Azure.Monitoring.DependencyAgent",
        "type": "DependencyAgentLinux",
        "autoUpgradeMinorVersion": true
      }
    }
  ],
    "outputs": {
    }
}
```

Template file for Windows

```
{
    "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
    "contentVersion": "1.0.0.0",
  "parameters": {
    "vmName": {
      "type": "string",
      "metadata": {
        "description": "The name of existing Windows machine."
      }
    }
  },
  "variables": {
    "vmExtensionsApiVersion": "2017-03-30"
  },
  "resources": [
    {
      "type": "Microsoft.HybridCompute/machines/extensions",
      "name": "[concat(parameters('vmName'),'/DAExtension')]",
      "apiVersion": "[variables('vmExtensionsApiVersion')]",
      "location": "[resourceGroup().location]",
      "dependsOn": [
      ],
      "properties": {
        "publisher": "Microsoft.Azure.Monitoring.DependencyAgent",
        "type": "DependencyAgentWindows",
        "autoUpgradeMinorVersion": true
      }
    }
  ],
    "outputs": {
    }
}
```

Template deployment

Save the template file to disk. You can then deploy the extension to the connected machine with the following command.

```
New-AzResourceGroupDeployment -ResourceGroupName "ContosoEngineering" -TemplateFile
"D:\Azure\Templates\DependencyAgent.json"
```

Deploy Azure Key Vault VM extension (preview)

The following JSON shows the schema for the Key Vault VM extension (preview). The extension does not require protected settings - all its settings are considered public information. The extension requires a list of monitored certificates, polling frequency, and the destination certificate store. Specifically:

Template file for Linux

```
{
    "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "vmName": {
            "type": "string"
        },
        "location": {
            "type": "string"
        },
        "autoUpgradeMinorVersion":{
            "type": "bool"
        },
        "pollingIntervalInS":{
          "type": "int"
        },
        "certificateStoreName":{
          "type": "string"
        },
        "certificateStoreLocation":{
          "type": "string"
        },
        "observedCertificates":{
          "type": "string"
        },
        "msiEndpoint":{
          "type": "string"
        },
        "msiClientId":{
          "type": "string"
        }
},
"resources": [
   {
      "type": "Microsoft.HybridCompute/machines/extensions",
      "name": "[concat(parameters('vmName'),'/KVVMExtensionForLinux')]",
      "apiVersion": "2019-12-12",
      "location": "[parameters('location')]",
      "properties": {
      "publisher": "Microsoft.Azure.KeyVault",
      "type": "KeyVaultForLinux",
      "autoUpgradeMinorVersion": true,
      "settings": {
          "secretsManagementSettings": {
          "pollingIntervalInS": <polling interval in seconds, e.g. "3600">,
          "certificateStoreName": <ignored on linux>,
          "certificateStoreLocation": <disk path where certificate is stored, default:
"/var/lib/waagent/Microsoft.Azure.KeyVault">,
          "observedCertificates": <list of KeyVault URIs representing monitored certificates, e.g.:
"https://myvault.vault.azure.net/secrets/mycertificate"
          },
          "authenticationSettings": {
                "msiEndpoint":  <MSI endpoint e.g.: "http://localhost:40342/metadata/identity">,
                "msiClientId":  <MSI identity e.g.: "c7373ae5-91c2-4165-8ab6-7381d6e75619">
        }
      }
    }
  }
 ]
}
```

Template file for Windows

```
{
    "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "vmName": {
            "type": "string"
        },
        "location": {
            "type": "string"
        },
        "autoUpgradeMinorVersion":{
            "type": "bool"
        },
        "pollingIntervalInS":{
          "type": "int"
        },
        "certificateStoreName":{
          "type": "string"
        },
        "linkOnRenewal":{
          "type": "bool"
        },
        "certificateStoreLocation":{
          "type": "string"
        },
        "requireInitialSync":{
          "type": "bool"
        },
        "observedCertificates":{
          "type": "string"
        },
        "msiEndpoint":{
          "type": "string"
        },
        "msiClientId":{
          "type": "string"
        }
},
"resources": [
   {
      "type": "Microsoft.HybridCompute/machines/extensions",
      "name": "[concat(parameters('vmName'),'/KVVMExtensionForWindows')]",
      "apiVersion": "2019-12-12",
      "location": "[parameters('location')]",
      "properties": {
      "publisher": "Microsoft.Azure.KeyVault",
      "type": "KeyVaultForWindows",
      "autoUpgradeMinorVersion": true,
      "settings": {
        "secretsManagementSettings": {
          "pollingIntervalInS": "3600",
          "certificateStoreName": <certificate store name, e.g.: "MY">,
          "linkOnRenewal": <Only Windows. This feature ensures s-channel binding when certificate renews,
without necessitating a re-deployment.  e.g.: false>,
          "certificateStoreLocation": <certificate store location, currently it works locally only e.g.:
"LocalMachine">,
          "requireInitialSync": <initial synchronization of certificates e..g: true>,
          "observedCertificates": <list of KeyVault URIs representing monitored certificates, e.g.:
"https://myvault.vault.azure.net"
        },
        "authenticationSettings": {
                "msiEndpoint": <MSI endpoint e.g.: "http://localhost:40342/metadata/identity">,
                "msiClientId": <MSI identity e.g.: "c7373ae5-91c2-4165-8ab6-7381d6e75619">
        }
      }
    }
  }
 ]
}
```

NOTE

Your observed certificates URLs should be of the form `https://myVaultName.vault.azure.net/secrets/myCertName`.

This is because the `/secrets` path returns the full certificate, including the private key, while the `/certificates` path does not. More information about certificates can be found here: Key Vault Certificates

Template deployment

Save the template file to disk. You can then deploy the extension to the connected machine with the following command.

NOTE

The VM extension would require a system-assigned identity to be assigned to authenticate to Key vault. See How to authenticate to Key Vault using managed identity for Windows and Linux Azure Arc-enabled servers.

```
New-AzResourceGroupDeployment -ResourceGroupName "ContosoEngineering" -TemplateFile
"D:\Azure\Templates\KeyVaultExtension.json"
```

Deploy the Azure Defender integrated scanner

To use the Azure Defender integrated scanner extension, the following sample is provided to run on Windows and Linux. If you are unfamiliar with the integrated scanner, see Overview of Azure Defender's vulnerability assessment solution for hybrid machines.

Template file for Windows

```
{
  "properties": {
    "mode": "Incremental",
    "template": {
      "contentVersion": "1.0.0.0",
      "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
      "parameters": {
        "vmName": {
          "type": "string"
        },
        "apiVersionByEnv": {
          "type": "string"
        }
      },
      "resources": [
        {
          "type": "Microsoft.HybridCompute/machines/providers/serverVulnerabilityAssessments",
          "name": "[concat(parameters('vmName'), '/Microsoft.Security/default')]",
          "apiVersion": "[parameters('apiVersionByEnv')]"
        }
      ]
    },
    "parameters": {
      "vmName": {
        "value": "resourceName"
      },
      "apiVersionByEnv": {
        "value": "2015-06-01-preview"
      }
    }
  }
}
```

Template file for Linux

```
{
  "properties": {
    "mode": "Incremental",
    "template": {
      "contentVersion": "1.0.0.0",
      "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
      "parameters": {
        "vmName": {
          "type": "string"
        },
        "apiVersionByEnv": {
          "type": "string"
        }
      },
      "resources": [
        {
          "type": "Microsoft.HybridCompute/machines/providers/serverVulnerabilityAssessments",
          "name": "[concat(parameters('vmName'), '/Microsoft.Security/default')]",
          "apiVersion": "[parameters('apiVersionByEnv')]"
        }
      ]
    },
    "parameters": {
      "vmName": {
        "value": "resourceName"
      },
      "apiVersionByEnv": {
        "value": "2015-06-01-preview"
      }
    }
  }
}
```

Template deployment

Save the template file to disk. You can then deploy the extension to the connected machine with the following command.

```
New-AzResourceGroupDeployment -ResourceGroupName "ContosoEngineering" -TemplateFile
"D:\Azure\Templates\AzureDefenderScanner.json"
```

Next steps

- You can deploy, manage, and remove VM extensions using the Azure PowerShell, from the Azure portal, or the Azure CLI.
- Troubleshooting information can be found in the Troubleshoot VM extensions guide.

Authenticate against Azure resources with Azure Arc-enabled servers

9/7/2021 • 4 minutes to read • Edit Online

Applications or processes running directly on an Azure Arc-enabled servers can leverage managed identities to access other Azure resources that support Azure Active Directory-based authentication. An application can obtain an access token representing its identity, which is system-assigned for Azure Arc-enabled servers, and use it as a 'bearer' token to authenticate itself to another service.

Refer to the managed identity overview documentation for a detailed description of managed identities, as well as the distinction between system-assigned and user-assigned identities.

In this article, we show you how a server can use a system-assigned managed identity to access Azure Key Vault. Serving as a bootstrap, Key Vault makes it possible for your client application to then use a secret to access resources not secured by Azure Active Directory (AD). For example, TLS/SSL certificates used by your IIS web servers can be stored in Azure Key Vault, and securely deploy the certificates to Windows or Linux servers outside of Azure.

Security overview

While onboarding your server to Azure Arc-enabled servers, several actions are performed to configure using a managed identity, similar to what is performed for an Azure VM:

- Azure Resource Manager receives a request to enable the system-assigned managed identity on the Azure Arc-enabled server.
- Azure Resource Manager creates a service principal in Azure AD for the identity of the server. The service principal is created in the Azure AD tenant that's trusted by the subscription.
- Azure Resource Manager configures the identity on the server by updating the Azure Instance Metadata Service (IMDS) identity endpoint for Windows or Linux with the service principal client ID and certificate. The endpoint is a REST endpoint accessible only from within the server using a well-known, non-routable IP address. This service provides a subset of metadata information about the Azure Arc-enabled server to help manage and configure it.

The environment of a managed-identity-enabled server will be configured with the following variables on a Windows Azure Arc-enabled server:

- **IMDS_ENDPOINT**: The IMDS endpoint IP address `http://localhost:40342` for Azure Arc-enabled servers.
- **IDENTITY_ENDPOINT**: the localhost endpoint corresponding to service's managed identity `http://localhost:40342/metadata/identity/oauth2/token`.

Your code that's running on the server can request a token from the Azure Instance Metadata service endpoint, accessible only from within the server.

The system environment variable **IDENTITY_ENDPOINT** is used to discover the identity endpoint by applications. Applications should try to retrieve **IDENTITY_ENDPOINT** and **IMDS_ENDPOINT** values and use them. Applications with any access level are allowed to make requests to the endpoints. Metadata responses are handled as normal and given to any process on the machine. However, when a request is made that would expose a token, we require the client to provide a secret to attest that they are able to access data only available to higher-privileged users.

Prerequisites

- An understanding of Managed identities.
- A server connected and registered with Azure Arc-enabled servers.
- You are a member of the Owner group** in the subscription or resource group, in order to perform required resource creation and role management steps.
- An Azure Key Vault to store and retrieve your credential. and assign the Azure Arc identity access to the KeyVault.
    - If you don't have a Key Vault created, see Create Key Vault.
    - To configure access by the managed identity used by the server, see Grant access for Linux or Grant access for Windows. For step number 5, you are going to enter the name of the Azure Arc-enabled server. To complete this using PowerShell, see Assign an access policy using PowerShell.

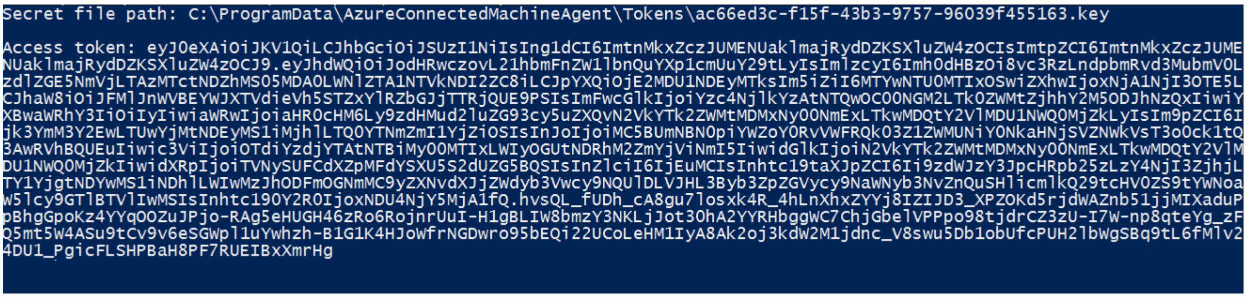
Acquiring an access token using REST API

The method to obtain and use a system-assigned managed identity to authenticate with Azure resources is similar to how it is performed with an Azure VM.

For an Azure Arc-enabled Windows server, using PowerShell, you invoke the web request to get the token from the local host in the specific port. Specify the request using the IP address or the environmental variable **IDENTITY_ENDPOINT**.

```
$apiVersion = "2020-06-01"
$resource = "https://management.azure.com/"
$endpoint = "{0}?resource={1}&api-version={2}" -f $env:IDENTITY_ENDPOINT,$resource,$apiVersion
$secretFile = ""
try
{
    Invoke-WebRequest -Method GET -Uri $endpoint -Headers @{Metadata='True'} -UseBasicParsing
}
catch
{
    $wwwAuthHeader = $_.Exception.Response.Headers["WWW-Authenticate"]
    if ($wwwAuthHeader -match "Basic realm=.+")
    {
        $secretFile = ($wwwAuthHeader -split "Basic realm=")[1]
    }
}
Write-Host "Secret file path: " $secretFile`n
$secret = cat -Raw $secretFile
$response = Invoke-WebRequest -Method GET -Uri $endpoint -Headers @{Metadata='True'; Authorization="Basic
$secret"} -UseBasicParsing
if ($response)
{
    $token = (ConvertFrom-Json -InputObject $response.Content).access_token
    Write-Host "Access token: " $token
}
```

The following response is an example that is returned:



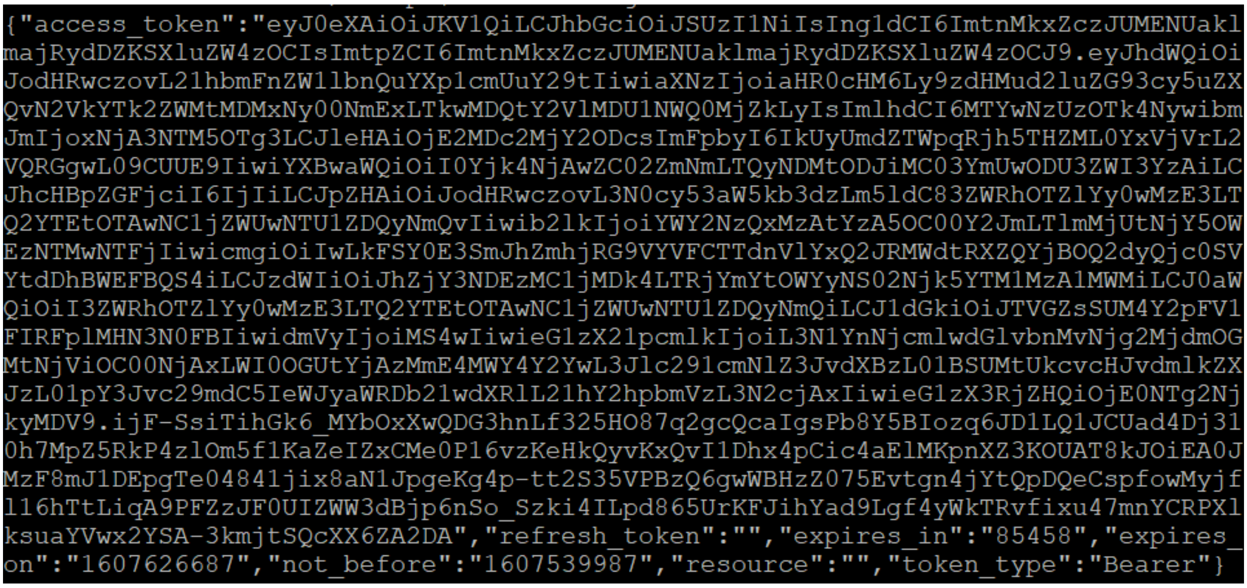
```
Secret file path: C:\ProgramData\AzureConnectedMachineAgent\Tokens\ac66ed3c-f15f-43b3-9757-96039f455163.key

Access token: eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6ImtnMkxZczJUMENUaklmajRydDZKSXluZW4zOCIsImtpZCI6ImtnMkxZczJUME
NUaklmajRydDZKSXluZW4zOCJ9.eyJhdWQiOiJodHRwczovL21hbmFnZW1lbnQuYXp1cmUuY29tLyIsImlzcyI6Imh0dHBzOi8vc3RzLndpbmRvd3MubmV0L
zdlZGE5NmVjLTAzMTctNDZhMS05MDA0LWNlZTA1NTVkNDI2ZC8iLCJpYXQiOjE2MDU1NDEyMTksIm5iZiI6MTYwNTU0MTIxOSwiZXhwIjoxNjA1NjI3OTE5L
CJhaW8iOiJFMlJnWVBEYWJXTVdieVh5STZxYlRZbGJjTTRjQUE9PSIsImFwcGlkIjoiYzc4NjlkYzAtNTQwOC00NGM2LTk0ZWMtZjhhY2M5ODJhNzQxIiwiY
XBwaWRhY3IiOiIyIiwiaWRwIjoiaHR0cHM6Ly9zdHMud2luZG93cy5uZXQvN2VkYTk2ZWMtMDMxNy00NmExLTkwMDQtY2VlMDU1NWQ0MjZkLyIsIm9pZCI6I
jk3YmM3Y2EwLTUwYjMtNDEyMS1iMjhlLTQ0YTNmZmI1YjZiOSIsInJoIjoiMC5BUmNBN0piYWZoY0RvVWFRQk03Z1ZWMUNiY0NkaHNjSVZNWkVsT3o0ck1tQ
3AwRVhBQUEuIiwic3ViIjoiOTdiYzdjYTAtNTBiMy00MTIxLWIyOGUtNDRhM2ZmYjViNmI5IiwidGlkIjoiN2VkYTk2ZWMtMDMxNy00NmExLTkwMDQtY2VlM
DU1NWQ0MjZkIiwidXRpIjoiTVNySUFCdXZpMFdYSXU5S2dUZG5BQSIsInZlciI6IjEuMCIsInhtc19taXJpZCI6Ii9zdWJzY3JpcHRpb25zLzY4NjI3ZjhjL
TY1YjgtNDYwMS1iNDhlLWIwMzJhODFmOGNmMC9yZXNvdXJjZWdyb3Vwcy9NQUlDLVJHL3Byb3ZpZGVycy9NaWNyb3NvZnQuSHlicmlkQ29tcHV0ZS9tYWNoa
W5lcy9GTlBTVlIwMSIsInhtc190Y2R0IjoxNDU4NjY5MjA1fQ.hvsQL_fUDh_cA8gu7losxk4R_4hLnXhxZYYj8IZIJD3_XPZOKd5rjdWAZnb51jjMIXaduP
pBhgGpoKz4YYqOOZuJPjo-RAg5eHUGH46zRo6RojnrUuI-H1gBLIW8bmzY3NKLjJot3OhA2YYRHbggWC7ChjGbelVPPpo98tjdrCZ3zU-I7W-np8qteYg_zF
Q5mt5W4ASu9tCv9v6eSGWpl1uYwhzh-B1G1K4HJoWfrNGDwro95bEQi22UCoLeHM1IyA8Ak2oj3kdW2M1jdnc_V8swu5Db1obUfcPUH2lbWgSBq9tL6fMlv2
4DU1_PgicFLSHPBaH8PF7RUEIBxXmrHg
```

For an Azure Arc-enabled Linux server, using Bash, you invoke the web request to get the token from the local host in the specific port. Specify the following request using the IP address or the environmental variable **IDENTITY_ENDPOINT**. To complete this step, you need an SSH client.

```
ChallengeTokenPath=$(curl -s -D - -H Metadata:true "http://127.0.0.1:40342/metadata/identity/oauth2/token?api-version=2019-11-01&resource=https%3A%2F%2Fmanagement.azure.com" | grep Www-Authenticate | cut -d "=" -f 2 | tr -d "[:cntrl:]")
ChallengeToken=$(cat $ChallengeTokenPath)
if [ $? -ne 0 ]; then
    echo "Could not retrieve challenge token, double check that this command is run with root privileges."
else
    curl -s -H Metadata:true -H "Authorization: Basic $ChallengeToken" "http://127.0.0.1:40342/metadata/identity/oauth2/token?api-version=2019-11-01&resource=https%3A%2F%2Fmanagement.azure.com"
fi
```

The following response is an example that is returned:



```
{"access_token":"eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6ImtnMkxZczJUMENUakl
majRydDZKSXluZW4zOCIsImtpZCI6ImtnMkxZczJUMENUaklmajRydDZKSXluZW4zOCJ9.eyJhdWQiOi
JodHRwczovL21hbmFnZW1lbnQuYXp1cmUuY29tIiwiaXNzIjoiaHR0cHM6Ly9zdHMud2luZG93cy5uZX
QvN2VkYTk2ZWMtMDMxNy00NmExLTkwMDQtY2VlMDU1NWQ0MjZkLyIsImlhdCI6MTYwNzUzOTk4Nywibm
JmIjoxNjA3NTM5OTg3LCJleHAiOjE2MDc2MjY2ODcsImFpbyI6IkUyUmdZTWpqRjh5THZML0YxVjVrL2
VQRGgwL09CUUE9IiwiYXBwaWQiOiI0Yjk4NjAwZC02ZmNmLTQyNDMtODJiMC03YmUwODU3ZWI3YzAiLC
JhcHBpZGFjciI6IjIiLCJpZHAiOiJodHRwczovL3N0cy53aW5kb3dzLm5ldC83ZWRhOTZlYy0wMzE3LT
Q2YTEtOTAwNC1jZWUwNTU1ZDQyNmQvIiwib2lkIjoiYWY2NzQxMzAtYzA5OC00Y2JmLTlmMjUtNjY5OW
EzNTMwNTFjIiwicmgiOiIwLkFSY0E3SmJhZmhjRG9VYVFCTTdnVlYxQ2JRMWdtRXZQYjBOQ2dyQjc0SV
YtdDhBWEFBQS4iLCJzdWIiOiJhZjY3NDEzMC1jMDk4LTRjYmYtOWYyNS02Njk5YTM1MzA1MWMiLCJ0aW
QiOiI3ZWRhOTZlYy0wMzE3LTQ2YTEtOTAwNC1jZWUwNTU1ZDQyNmQiLCJ1dGkiOiJTVGZsSUM4Y2pFV1
FIRFplMHN3N0FBIiwidmVyIjoiMS4wIiwieG1zX21pcmlkIjoiL3N1YnNjcmlwdGlvbnMvNjg2MjdmOG
MtNjViOC00NjAxLWI0OGUtYjAzMmE4MWY4Y2YwL3Jlc291cmNlZ3JvdXBzL01BSUMtUkcvcHJvdmlkZX
JzL01pY3Jvc29mdC5IeWJyaWRDb21wdXRlL21hY2hpbmVzL3N2cjAxIiwieG1zX3RjZHQiOjE0NTg2Nj
kyMDV9.ijF-SsiTihGk6_MYbOxXwQDG3hnLf325HO87q2gcQcaIgsPb8Y5BIozq6JD1LQ1JCUad4Dj31
0h7MpZ5RkP4zlOm5f1KaZeIZxCMe0P16vzKeHkQyvKxQvI1Dhx4pCic4aElMKpnXZ3KOUAT8kJOiEA0J
MzF8mJ1DEpgTe04841jix8aN1JpgeKg4p-tt2S35VPBzQ6gwWBHzZ075Evtgn4jYtQpDQeCspfowMyjf
l16hTtLiqA9PFZzJF0UIZWW3dBjp6nSo_Szki4ILpd865UrKFJihYad9Lgf4yWkTRvfixu47mnYCRPXl
ksuaYVwx2YSA-3kmjtSQcXX6ZA2DA","refresh_token":"","expires_in":"85458","expires_
on":"1607626687","not_before":"1607539987","resource":"","token_type":"Bearer"}
```

The response includes the access token you need to access any resource in Azure. To complete the configuration to authenticate to Azure Key Vault, see Access Key Vault with Windows or Access Key Vault with Linux.

Next steps

- To learn more about Azure Key Vault, see Key Vault overview.
- Learn how to assign a managed identity access to a resource using PowerShell or using the Azure CLI.

Managing and maintaining the Connected Machine agent

9/7/2021 • 12 minutes to read • Edit Online

After initial deployment of the Azure Arc-enabled servers Connected Machine agent for Windows or Linux, you may need to reconfigure the agent, upgrade it, or remove it from the computer. You can easily manage these routine maintenance tasks manually or through automation, which reduces both operational error and expenses.

Before uninstalling agent

Before removing the Connected Machine agent from your Azure Arc-enabled server, consider the following to avoid unexpected issues or costs added to your Azure bill:

- If you have deployed Azure VM extensions to an enabled server, and you remove the Connected Machine agent or you delete the resource representing the Azure Arc-enabled server in the resource group, those extensions continue to run and perform their normal operation.
- If you delete the resource representing the Azure Arc-enabled server in your resource group, but you don't uninstall the VM extensions, when you re-register the machine, you won't be able to manage the installed VM extensions.

For servers or machines you no longer want to manage with Azure Arc-enabled servers, it is necessary to follow these steps to successfully stop managing it:

1. Remove the VM extensions from the machine or server. Steps are provided below.
2. Disconnect the machine from Azure Arc using one of the following methods:
   - Running `azcmagent disconnect` command on the machine or server.
   - From the selected registered Azure Arc-enabled server in the Azure portal by selecting **Delete** from the top bar.
   - Using the Azure CLI or Azure PowerShell. For the `ResourceType` parameter use `Microsoft.HybridCompute/machines`.
3. Uninstall the agent from the machine or server following the steps below.

Renaming a machine

When you change the name of the Linux or Windows machine connected to Azure Arc-enabled servers, the new name is not recognized automatically because the resource name in Azure is immutable. As with other Azure resources, you have to delete the resource and re-create it in order to use the new name.

For Azure Arc-enabled servers, before you rename the machine, it is necessary to remove the VM extensions before proceeding.

NOTE

While installed extensions continue to run and perform their normal operation after this procedure is complete, you won't be able to manage them. If you attempt to redeploy the extensions on the machine, you may experience unpredictable behavior.

WARNING

We recommend you avoid renaming the machine's computer name and only perform this procedure if absolutely necessary.

1. Audit the VM extensions installed on the machine and note their configuration, using the Azure CLI or using Azure PowerShell.
2. Remove VM extensions installed from the Azure portal, using the Azure CLI, or using Azure PowerShell.
3. Use the **azcmagent** tool with the Disconnect parameter to disconnect the machine from Azure Arc and delete the machine resource from Azure. Disconnecting the machine from Azure Arc-enabled servers does not remove the Connected Machine agent, and you do not need to remove the agent as part of this process. You can run azcmagent manually while logged on interactively, or automate using the same service principal you used to onboard multiple agents, or with a Microsoft identity platform access token. If you did not use a service principal to register the machine with Azure Arc-enabled servers, see the following article to create a service principal.
4. Rename the machines computer name.
5. Re-register the Connected Machine agent with Azure Arc-enabled servers. Run the `azcmagent` tool with the Connect parameter complete this step.
6. Redeploy the VM extensions that were originally deployed to the machine from Azure Arc-enabled servers. If you deployed the Azure Monitor for VMs (insights) agent or the Log Analytics agent using an Azure Policy definition, the agents are redeployed after the next evaluation cycle.

Upgrading agent

The Azure Connected Machine agent is updated regularly to address bug fixes, stability enhancements, and new functionality. Azure Advisor identifies resources that are not using the latest version of machine agent and recommends that you upgrade to the latest version. It will notify you when you select the Azure Arc-enabled server by presenting a banner on the **Overview** page or when you access Advisor through the Azure portal.

The Azure Connected Machine agent for Windows and Linux can be upgraded to the latest release manually or automatically depending on your requirements.

The following table describes the methods supported to perform the agent upgrade.

OPERATING SYSTEM	UPGRADE METHOD
Windows	Manually Windows Update
Ubuntu	Apt
SUSE Linux Enterprise Server	zypper

OPERATING SYSTEM	UPGRADE METHOD
RedHat Enterprise, Amazon, CentOS Linux	yum

Windows agent

Update package for the Connected Machine agent for Windows is available from:

- Microsoft Update
- Microsoft Update Catalog
- Windows agent Windows Installer package from the Microsoft Download Center.

The agent can be upgraded following various methods to support your software update management process. Outside of obtaining from Microsoft Update, you can download and run manually from the Command Prompt, from a script or other automation solution, or from the UI wizard by executing `AzureConnectedMachine.msi`.

> **NOTE**
> - To upgrade the agent, you must have *Administrator* permissions.
> - To upgrade manually, you must first download and copy the Installer package to a folder on the target server, or from a shared network folder.

If you are unfamiliar with the command-line options for Windows Installer packages, review Msiexec standard command-line options and Msiexec command-line options.

To upgrade using the Setup Wizard

1. Sign on to the computer with an account that has administrative rights.
2. Execute **AzureConnectedMachineAgent.msi** to start the Setup Wizard.

The Setup Wizard discovers if a previous version exists, and then it automatically performs an upgrade of the agent. When the upgrade completes, the Setup Wizard automatically closes.

To upgrade from the command line

1. Sign on to the computer with an account that has administrative rights.
2. To upgrade the agent silently and create a setup log file in the `C:\Support\Logs` folder, run the following command.

```
msiexec.exe /i AzureConnectedMachineAgent.msi /qn /l*v "C:\Support\Logs\Azcmagentupgradesetup.log"
```

Linux agent

To update the agent on a Linux machine to the latest version, it involves two commands. One command to update the local package index with the list of latest available packages from the repositories, and one command to upgrade the local package.

You can download the latest agent package from Microsoft's package repository.

> **NOTE**
> To upgrade the agent, you must have *root* access permissions or with an account that has elevated rights using Sudo.

Upgrade Ubuntu

1. To update the local package index with the latest changes made in the repositories, run the following

command:

```
apt update
```

2. To upgrade your system, run the following command:

```
apt upgrade
```

Actions of the apt command, such as installation and removal of packages, are logged in the `/var/log/dpkg.log` log file.

Upgrade Red Hat/CentOS/Amazon Linux

1. To update the local package index with the latest changes made in the repositories, run the following command:

```
yum check-update
```

2. To upgrade your system, run the following command:

```
yum update
```

Actions of the yum command, such as installation and removal of packages, are logged in the `/var/log/yum.log` log file.

Upgrade SUSE Linux Enterprise

1. To update the local package index with the latest changes made in the repositories, run the following command:

```
zypper refresh
```

2. To upgrade your system, run the following command:

```
zypper update
```

Actions of the zypper command, such as installation and removal of packages, are logged in the `/var/log/zypper.log` log file.

About the Azcmagent tool

The Azcmagent tool (Azcmagent.exe) is used to configure the Azure Arc-enabled servers Connected Machine agent during installation, or modify the initial configuration of the agent after installation. Azcmagent.exe provides command-line parameters to customize the agent and view its status:

- **Connect** - To connect the machine to Azure Arc
- **Disconnect** - To disconnect the machine from Azure Arc
- **Show** - View agent status and its configuration properties (Resource Group name, Subscription ID, version, etc.), which can help when troubleshooting an issue with the agent. Include the `-j` parameter to output the results in JSON format.
- **Logs** - Creates a .zip file in the current directory containing logs to assist you while troubleshooting.

- **Version** - Shows the Connected Machine agent version.
- **-useStderr** - Directs error and verbose output to stderr. Include the `-json` parameter to output the results in JSON format.
- **-h or --help** - Shows available command-line parameters

  For example, to see detailed help for the **Connect** parameter, type `azcmagent connect -h`.
- **-v or --verbose** - Enable verbose logging

You can perform a **Connect** and **Disconnect** manually while logged on interactively, or automate using the same service principal you used to onboard multiple agents or with a Microsoft identity platform access token. If you did not use a service principal to register the machine with Azure Arc-enabled servers, see the following article to create a service principal.

> **NOTE**
>
> You must have *root* access permissions on Linux machines to run **azcmagent**.

Connect

This parameter specifies a resource in Azure Resource Manager representing the machine is created in Azure. The resource is in the subscription and resource group specified, and data about the machine is stored in the Azure region specified by the `--location` setting. The default resource name is the hostname of the machine if not specified.

A certificate corresponding to the system-assigned identity of the machine is then downloaded and stored locally. Once this step is completed, the Azure Connected Machine Metadata Service and guest configuration agent service begins synchronizing with Azure Arc-enabled servers.

To connect using a service principal, run the following command:

```
azcmagent connect --service-principal-id <serviceprincipalAppID> --service-principal-secret
<serviceprincipalPassword> --tenant-id <tenantID> --subscription-id <subscriptionID> --resource-group
<ResourceGroupName> --location <resourceLocation>
```

To connect using an access token, run the following command:

```
azcmagent connect --access-token <> --subscription-id <subscriptionID> --resource-group <ResourceGroupName> -
-location <resourceLocation>
```

To connect with your elevated logged-on credentials (interactive), run the following command:

```
azcmagent connect --tenant-id <TenantID> --subscription-id <subscriptionID> --resource-group
<ResourceGroupName> --location <resourceLocation>
```

Disconnect

This parameter specifies a resource in Azure Resource Manager representing the machine is deleted in Azure. It does not remove the agent from the machine, you uninstall the agent separately. After the machine is disconnected, if you want to re-register it with Azure Arc-enabled servers, use `azcmagent connect` so a new resource is created for it in Azure.

> **NOTE**
>
> If you have deployed one or more of the Azure VM extensions to your Azure Arc-enabled server and you delete its registration in Azure, the extensions are still installed. It is important to understand that depending on the extension installed, it is actively performing its function. Machines that are intended to be retired or no longer managed by Azure Arc-enabled servers should first have the extensions removed before removing its registration from Azure.

To disconnect using a service principal, run the following command:

```
azcmagent disconnect --service-principal-id <serviceprincipalAppID> --service-principal-secret
<serviceprincipalPassword> --tenant-id <tenantID>
```

To disconnect using an access token, run the following command:

```
azcmagent disconnect --access-token <accessToken>
```

To disconnect with your elevated logged-on credentials (interactive), run the following command:

```
azcmagent disconnect
```

Remove the agent

Perform one of the following methods to uninstall the Windows or Linux Connected Machine agent from the machine. Removing the agent does not unregister the machine with Azure Arc-enabled servers or remove the Azure VM extensions installed. For servers or machines you no longer want to manage with Azure Arc-enabled servers, it is necessary to follow these steps to successfully stop managing it:

1. Remove VM extensions installed from the Azure portal, using the Azure CLI, or using Azure PowerShell that you don't want to remain on the machine.
2. Unregister the machine by running `azcmagent disconnect` to delete the Azure Arc-enabled servers resource in Azure. If that fails, you can delete the resource manually in Azure. Otherwise, if the resource was deleted in Azure, you'll need to run `azcmagent disconnect --force-local-only` on the server to remove the local configuration.

Windows agent

Both of the following methods remove the agent, but they do not remove the *C:\Program Files\AzureConnectedMachineAgent* folder on the machine.

Uninstall from Control Panel

1. To uninstall the Windows agent from the machine, do the following:

   a. Sign in to the computer with an account that has administrator permissions.
   b. In **Control Panel**, select **Programs and Features**.
   c. In **Programs and Features**, select **Azure Connected Machine Agent**, select **Uninstall**, and then select **Yes**.

   > **NOTE**
   >
   > You can also run the agent setup wizard by double-clicking the **AzureConnectedMachineAgent.msi** installer package.

Uninstall from the command line

To uninstall the agent manually from the Command Prompt or to use an automated method, such as a script, you can use the following example. First you need to retrieve the product code, which is a GUID that is the principal identifier of the application package, from the operating system. The uninstall is performed by using the Msiexec.exe command line - `msiexec /x {Product Code}`.

1. Open the Registry Editor.

2. Under registry key `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall`, look for and copy the product code GUID.

3. You can then uninstall the agent by using Msiexec using the following examples:

   - From the command-line type:

```
msiexec.exe /x {product code GUID} /qn
```

- You can perform the same steps using PowerShell:

```
Get-ChildItem -Path HKLM:\Software\Microsoft\Windows\CurrentVersion\Uninstall | `
Get-ItemProperty | `
Where-Object {$_.DisplayName -eq "Azure Connected Machine Agent"} | `
ForEach-Object {MsiExec.exe /x "$($_.PsChildName)" /qn}
```

Linux agent

> **NOTE**
>
> To uninstall the agent, you must have *root* access permissions or with an account that has elevated rights using Sudo.

To uninstall the Linux agent, the command to use depends on the Linux operating system.

- For Ubuntu, run the following command:

```
sudo apt purge azcmagent
```

- For RHEL, CentOS, and Amazon Linux, run the following command:

```
sudo yum remove azcmagent
```

- For SLES, run the following command:

```
sudo zypper remove azcmagent
```

Unregister machine

If you are planning to stop managing the machine with supporting services in Azure, perform the following steps to unregister the machine with Azure Arc-enabled servers. You can perform these steps either before or after you have removed the Connected Machine agent from the machine.

1. Open Azure Arc-enabled servers by going to the Azure portal.

2. Select the machine in the list, select the ellipsis (...), and then select **Delete**.

Update or remove proxy settings

To configure the agent to communicate to the service through a proxy server or remove this configuration after deployment, or use one of the following methods to complete this task. The agent communicates outbound using the HTTP protocol under this scenario.

> **NOTE**
>
> Azure Arc-enabled servers does not support using a Log Analytics gateway as a proxy for the Connected Machine agent.

Windows

To set the proxy server environment variable, run the following command:

```
# If a proxy server is needed, execute these commands with the proxy URL and port.
[Environment]::SetEnvironmentVariable("https_proxy","http://{proxy-url}:{proxy-port}","Machine")
$env:https_proxy = [System.Environment]::GetEnvironmentVariable("https_proxy","Machine")
# For the changes to take effect, the agent service needs to be restarted after the proxy environment
variable is set.
Restart-Service -Name himds
```

To configure the agent to stop communicating through a proxy server, run the following command to remove the proxy server environmental variable and restart the agent service:

```
[Environment]::SetEnvironmentVariable("https_proxy",$null,"Machine")
$env:https_proxy = [System.Environment]::GetEnvironmentVariable("https_proxy","Machine")
# For the changes to take effect, the agent service needs to be restarted after the proxy environment
variable removed.
Restart-Service -Name himds
```

Linux

To set the proxy server, run the following command from the directory you downloaded the agent installation package to:

```
# Reconfigure the connected machine agent and set the proxy server.
bash ~/Install_linux_azcmagent.sh --proxy "{proxy-url}:{proxy-port}"
```

To configure the agent to stop communicating through a proxy server, run the following command to remove the proxy configuration:

```
sudo azcmagent_proxy remove
```

Next steps

- Troubleshooting information can be found in the Troubleshoot Connected Machine agent guide.
- Review the Planning and deployment guide to plan for deploying Azure Arc-enabled servers at any scale and implement centralized management and monitoring.
- Learn how to manage your machine using Azure Policy, for such things as VM guest configuration, verifying the machine is reporting to the expected Log Analytics workspace, enable monitoring with VM insights, and much more.

How to migrate Azure Arc-enabled servers across regions

9/7/2021 • 2 minutes to read • Edit Online

There are scenarios in which you'd want to move your existing Azure Arc-enabled server from one region to another. For example, you realized the machine was registered in the wrong region, to improve manageability, or to move for governance reasons.

To migrate an Azure Arc-enabled server from one Azure region to another, you have to uninstall the VM extensions, delete the resource in Azure, and re-create it in the other region. Before you perform these steps, you should audit the machine to verify which VM extensions are installed.

> **NOTE**
>
> While installed extensions continue to run and perform their normal operation after this procedure is complete, you won't be able to manage them. If you attempt to redeploy the extensions on the machine, you may experience unpredictable behavior.

Move machine to other region

> **NOTE**
>
> During this operation, it results in downtime during the migration.

1. Remove VM extensions installed from the Azure portal, using the Azure CLI, or using Azure PowerShell.
2. Use the **azcmagent** tool with the Disconnect parameter to disconnect the machine from Azure Arc and delete the machine resource from Azure. Disconnecting the machine from Azure Arc-enabled servers does not remove the Connected Machine agent, and you do not need to remove the agent as part of this process. You can run this manually while logged on interactively, or automate using the same service principal you used to onboard multiple agents, or with a Microsoft identity platform access token. If you did not use a service principal to register the machine with Azure Arc-enabled servers, see the following article to create a service principal.
3. Re-register the Connected Machine agent with Azure Arc-enabled servers in the other region. Run the `azcmagent` tool with the Connect parameter complete this step.
4. Redeploy the VM extensions that were originally deployed to the machine from Azure Arc-enabled servers. If you deployed the Azure Monitor for VMs (insights) agent or the Log Analytics agent using an Azure Policy definition, the agents are redeployed after the next evaluation cycle.

Next steps

- Troubleshooting information can be found in the Troubleshoot Connected Machine agent guide.
- Learn how to manage your machine using Azure Policy, for such things as VM guest configuration, verifying the machine is reporting to the expected Log Analytics workspace, enable monitoring with VM insights policy, and much more.

Evaluate Azure Arc-enabled servers on an Azure virtual machine

9/7/2021 • 6 minutes to read • Edit Online

Azure Arc-enabled servers is designed to help you connect servers running on-premises or in other clouds to Azure. Normally, you would not use Azure Arc-enabled servers on an Azure virtual machine because all the same capabilities are natively available for these VMs, including a representation of the VM in Azure Resource Manager, VM extensions, managed identities, and Azure Policy. If you attempt to install Azure Arc-enabled servers on an Azure VM, you'll receive an error message stating that it is unsupported and the agent installation will be canceled.

While you cannot install Azure Arc-enabled servers on an Azure VM for production scenarios, it is possible to configure Azure Arc-enabled servers to run on an Azure VM for *evaluation and testing purposes only*. This article will help you set up an Azure VM before you can enable Azure Arc-enabled servers on it.

Prerequisites

- Your account is assigned to the Virtual Machine Contributor role.
- The Azure virtual machine is running an operating system supported by Azure Arc-enabled servers. If you don't have an Azure VM, you can deploy a simple Windows VM or a simple Ubuntu Linux 18.04 LTS VM.
- Your Azure VM can communicate outbound to download the Azure Connected Machine agent package for Windows from the Microsoft Download Center, and Linux from the Microsoft package repository. If outbound connectivity to the Internet is restricted following your IT security policy, you will need to download the agent package manually and copy it to a folder on the Azure VM.
- An account with elevated (that is, an administrator or as root) privileges on the VM, and RDP or SSH access to the VM.
- To register and manage the Azure VM with Azure Arc-enabled servers, you are a member of the Azure Connected Machine Resource Administrator or Contributor role in the resource group.

Plan

To start managing your Azure VM as an Azure Arc-enabled server, you need to make the following changes to the Azure VM before you can install and configure Azure Arc-enabled servers.

1. Remove any VM extensions deployed to the Azure VM, such as the Log Analytics agent. While Azure Arc-enabled servers support many of the same extensions as Azure VMs, the Azure Arc-enabled servers agent can't manage VM extensions already deployed to the VM.

2. Disable the Azure Windows or Linux Guest Agent. The Azure VM guest agent serves a similar purpose to the Azure Arc-enabled servers Connected Machine agent. To avoid conflicts between the two, the Azure VM Agent needs to be disabled. Once it is disabled, you cannot use VM extensions or some Azure services.

3. Create a security rule to deny access to the Azure Instance Metadata Service (IMDS). IMDS is a REST API that applications can call to get information about the VM's representation in Azure, including its resource ID and location. IMDS also provides access to any managed identities assigned to the machine. Azure Arc-enabled servers provides its own IMDS implementation and returns information about the Azure Arc representation of the VM. To avoid situations where both IMDS endpoints are available and apps have to choose between the two, you block access to the Azure VM IMDS so that the Azure Arc-enabled server

IMDS implementation is the only one available.

After you've made these changes, your Azure VM behaves like any machine or server outside of Azure and is at the necessary starting point to install and evaluate Azure Arc-enabled servers.

When Azure Arc-enabled servers is configured on the VM, you see two representations of it in Azure. One is the Azure VM resource, with a `Microsoft.Compute/virtualMachines` resource type, and the other is an Azure Arc resource, with a `Microsoft.HybridCompute/machines` resource type. As a result of preventing management of the guest operating system from the shared physical host server, the best way to think about the two resources is the Azure VM resource is the virtual hardware for your VM, and let's you control the power state and view information about its SKU, network, and storage configurations. The Azure Arc resource manages the guest operating system in that VM, and can be used to install extensions, view compliance data for Azure Policy, and complete any other supported task by Azure Arc-enabled servers.

Reconfigure Azure VM

1. Remove any VM extensions on the Azure VM.

   In the Azure portal, navigate to your Azure VM resource and from the left-hand pane, select **Extensions**. If there are any extensions installed on the VM, select each extension individually and then select **Uninstall**. Wait for all extensions to finish uninstalling before proceeding to step 2.

2. Disable the Azure VM Guest Agent.

   To disable the Azure VM Guest Agent, you'll need to connect to your VM using Remote Desktop Connection (Windows) or SSH (Linux). Once connected, run the following commands to disable the guest agent.

   For Windows, run the following PowerShell commands:

   ```
   Set-Service WindowsAzureGuestAgent -StartupType Disabled -Verbose
   Stop-Service WindowsAzureGuestAgent -Force -Verbose
   ```

   For Linux, run the following commands:

   ```
   sudo service walinuxagent stop
   sudo waagent -deprovision -force
   sudo rm -rf /var/lib/waagent
   ```

3. Block access to the Azure IMDS endpoint.

   While still connected to the server, run the following commands to block access to the Azure IMDS endpoint. For Windows, run the following PowerShell command:

   ```
   New-NetFirewallRule -Name BlockAzureIMDS -DisplayName "Block access to Azure IMDS" -Enabled True -
   Profile Any -Direction Outbound -Action Block -RemoteAddress 169.254.169.254
   ```

   For Linux, consult your distribution's documentation for the best way to block outbound access to `169.254.169.254/32` over TCP port 80. Normally you'll block outbound access with the built-in firewall, but you can also temporarily block it with **iptables** or **nftables**.

   If your Azure VM is running Ubuntu, perform the following steps to configure its uncomplicated firewall (UFW):

```
sudo ufw --force enable
sudo ufw deny out from any to 169.254.169.254
sudo ufw default allow incoming
```

To configure a generic iptables configuration, run the following command:

```
iptables -A OUTPUT -d 169.254.169.254 -j DROP
```

> **NOTE**
>
> This configuration needs to be set after every reboot unless a persistent iptables solution is used.

If your Azure VM is running CentOS, Red Hat, or SUSE Linux Enterprise Server (SLES), perform the following steps to configure firewalld:

```
firewall-cmd --permanent --direct --add-rule ipv4 filter OUTPUT 1 -p tcp -d 169.254.169.254 -j DROP
firewall-cmd --reload
```

4. Install and configure the Azure Arc-enabled servers agent.

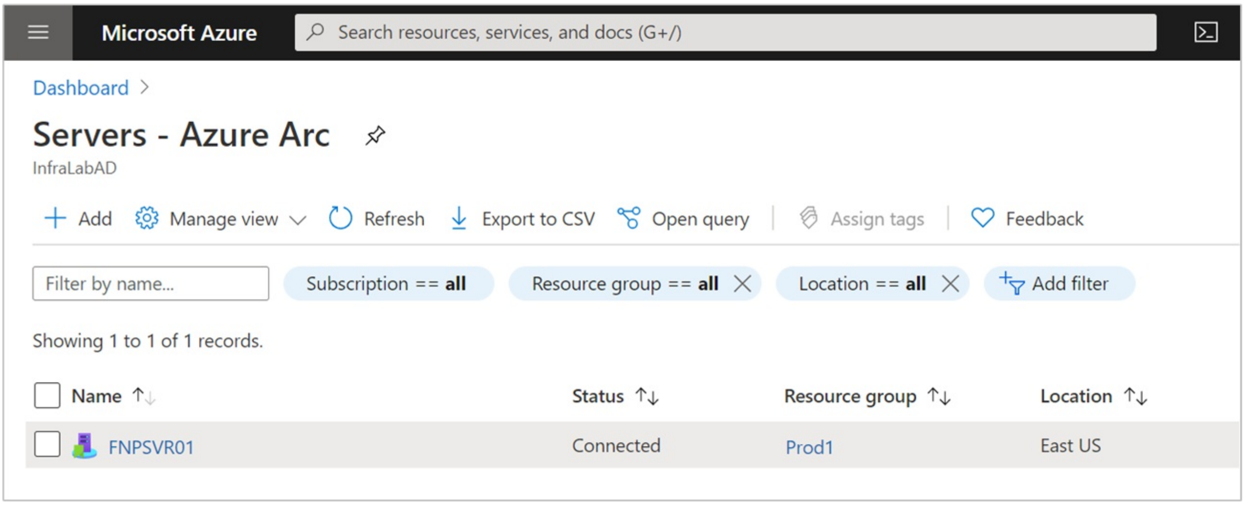
   The VM is now ready for you to begin evaluating Azure Arc-enabled servers. To install and configure the Azure Arc-enabled servers agent, see Connect hybrid machines using the Azure portal and follow the steps to generate an installation script and install using the scripted method.

   > **NOTE**
   >
   > If outbound connectivity to the internet is restricted from your Azure VM, you'll need to download the agent package manually. Copy the agent package to the Azure VM, and modify the Azure Arc-enabled servers installation script to reference the source folder.

If you missed one of the steps, the installation script detects it is running on an Azure VM and terminates with an error. Verify you've completed steps 1-3, and then rerun the script.

Verify the connection with Azure Arc

After you install and configure the agent to register with Azure Arc-enabled servers, go to the Azure portal to verify that the server has successfully connected. View your machine in the Azure portal.



Servers - Azure Arc

InfraLabAD

Showing 1 to 1 of 1 records.

□	Name ↑↓	Status ↑↓	Resource group ↑↓	Location ↑↓
□	FNPSVR01	Connected	Prod1	East US

Next steps

- Learn how to plan and enable a large number of machines to Azure Arc-enabled servers to simplify configuration of essential security management and monitoring capabilities in Azure.
- Learn about our supported Azure VM extensions available to simplify deployment with other Azure services like Automation, KeyVault, and others for your Windows or Linux machine.
- When you have finished testing, see Remove Azure Arc-enabled servers agent.

Onboard Azure Arc-enabled servers to Azure Sentinel

9/7/2021 • 2 minutes to read • Edit Online

This article is intended to help you onboard your Azure Arc-enabled server to Azure Sentinel and start collecting security-related events. Azure Sentinel provides a single solution for alert detection, threat visibility, proactive hunting, and threat response across the enterprise.

Prerequisites

Before you start, make sure that you've met the following requirements:

- A Log Analytics workspace. For more information about Log Analytics workspaces, see Designing your Azure Monitor Logs deployment.
- Azure Sentinel enabled in your subscription.
- You're machine or server is connected to Azure Arc-enabled servers.

Onboard Azure Arc-enabled servers to Azure Sentinel

Azure Sentinel comes with a number of connectors for Microsoft solutions, available out of the box and providing real-time integration. For physical and virtual machines, you can install the Log Analytics agent that collects the logs and forwards them to Azure Sentinel. Azure Arc-enabled servers supports deploying the Log Analytics agent using the following methods:

- Using the VM extensions framework.

  This feature in Azure Arc-enabled servers allows you to deploy the Log Analytics agent VM extension to a non-Azure Windows and/or Linux server. VM extensions can be managed using the following methods on your hybrid machines or servers managed by Azure Arc-enabled servers:

  - The Azure portal
  - The Azure CLI
  - Azure PowerShell
  - Azure Resource Manager templates
- Using Azure Policy.

  Using this approach, you use the Azure Policy Deploy Log Analytics agent to Linux or Windows Azure Arc machines built-in policy to audit if the Azure Arc-enabled server has the Log Analytics agent installed. If the agent is not installed, it automatically deploys it using a remediation task. Alternatively, if you plan to monitor the machines with Azure Monitor for VMs, instead use the Enable Azure Monitor for VMs initiative to install and configure the Log Analytics agent.

We recommend installing the Log Analytics agent for Windows or Linux using Azure Policy.

After your Arc-enabled servers are connected, your data starts streaming into Azure Sentinel and is ready for you to start working with. You can view the logs in the built-in workbooks and start building queries in Log Analytics to investigate the data.

Next steps

Get started detecting threats with Azure Sentinel.

Connect your non-Azure machines to Security Center

8/16/2021 • 5 minutes to read • Edit Online

Security Center can monitor the security posture of your non-Azure computers, but first you need to connect them to Azure.

You can connect your non-Azure computers in any of the following ways:

- Using Azure Arc-enabled servers (**recommended**)
- From Security Center's pages in the Azure portal (**Getting started** and **Inventory**)

Each of these is described on this page.

Add non-Azure machines with Azure Arc

The preferred way of adding your non-Azure machines to Azure Security Center is with Azure Arc-enabled servers.

A machine with Azure Arc-enabled servers becomes an Azure resource and - when you've installed the Log Analytics agent on it - appears in Security Center with recommendations like your other Azure resources.

In addition, Azure Arc-enabled servers provides enhanced capabilities such as the option to enable guest configuration policies on the machine, simplify deployment with other Azure services, and more. For an overview of the benefits, see Supported cloud operations.

NOTE

Security Center's auto-deploy tools for deploying the Log Analytics agent don't support machines running Azure Arc. When you've connected your machines using Azure Arc, use the relevant Security Center recommendation to deploy the agent and benefit from the full range of protections offered by Security Center:

- Log Analytics agent should be installed on your Linux-based Azure Arc machines
- Log Analytics agent should be installed on your Windows-based Azure Arc machines

Learn more about Azure Arc-enabled servers.

To deploy Azure Arc:

- For one machine, follow the instructions in Quickstart: Connect hybrid machines with Azure Arc enabled servers.
- To connect multiple machines at scale to Azure Arc-enabled servers, see Connect hybrid machines to Azure at scale

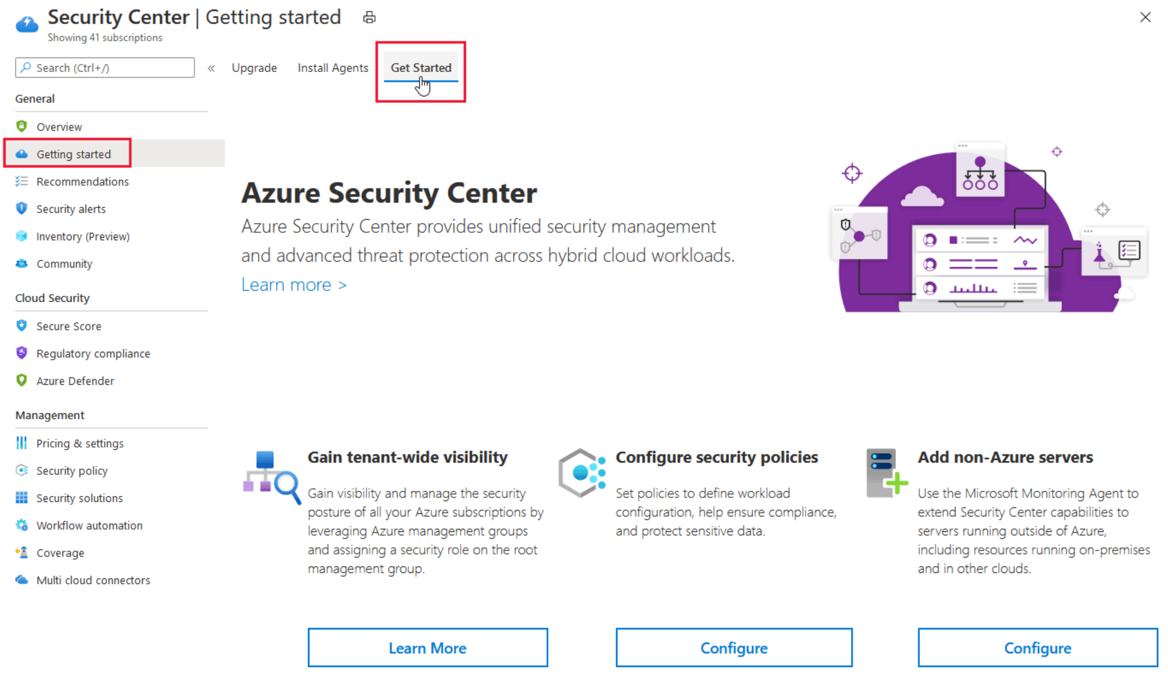
TIP

If you're onboarding machines running on Amazon Web Services (AWS), Security Center's connector for AWS transparently handles the Azure Arc deployment for you. Learn more in Connect your AWS accounts to Azure Security Center.

Add non-Azure machines from the Azure portal

1. From Security Center's menu, open the **Getting started** page.

2. Select the **Get started** tab.



Security Center | Getting started

Showing 41 subscriptions

Azure Security Center

Azure Security Center provides unified security management and advanced threat protection across hybrid cloud workloads.

Learn more >

Gain tenant-wide visibility

Gain visibility and manage the security posture of all your Azure subscriptions by leveraging Azure management groups and assigning a security role on the root management group.

Learn More

Configure security policies

Set policies to define workload configuration, help ensure compliance, and protect sensitive data.

Configure

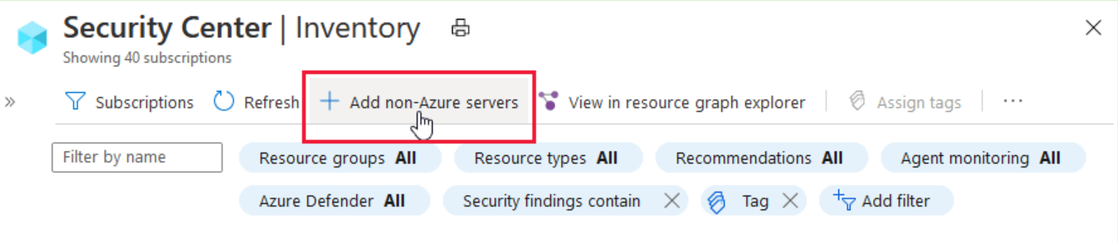
Add non-Azure servers

Use the Microsoft Monitoring Agent to extend Security Center capabilities to servers running outside of Azure, including resources running on-premises and in other clouds.

Configure

3. Below **Add non-Azure servers**, select **Configure** .

> **TIP**
>
> You can also open add machines from the **inventory** page's **Add non-Azure servers** button.



Security Center | Inventory

Showing 40 subscriptions

A list of your Log Analytics workspaces is shown. The list includes, if applicable, the default workspace created for you by Security Center when automatic provisioning was enabled. Select this workspace or another workspace you want to use.

You can add computers to an existing workspace or create a new workspace.

4. Optionally, to create a new workspace, select **Create new workspace**.

5. From the list of workspaces, select **Add Servers** for the relevant workspace. The **Agents management** page appears.

   From here, choose the relevant procedure below depending on the type of machines you're onboarding:

   - Onboard your Azure Stack Hub VMs
   - Onboard your Linux machines
   - Onboard your Windows machines

Onboard your Azure Stack Hub VMs

To add Azure Stack Hub VMs, you need the information on the **Agents management** page and to configure the **Azure Monitor, Update and Configuration Management** virtual machine extension on the virtual machines running on your Azure Stack Hub instance.

1. From the **Agents management** page, copy the **Workspace ID** and **Primary Key** into Notepad.
2. Log into your **Azure Stack Hub** portal and open the **Virtual machines** page.
3. Select the virtual machine that you want to protect with Security Center.

   > **TIP**
   >
   > For information on how to create a virtual machine on Azure Stack Hub, see this quickstart for Windows virtual machines or this quickstart for Linux virtual machines.

4. Select **Extensions**. The list of virtual machine extensions installed on this virtual machine is shown.
5. Select the **Add** tab. The **New Resource** menu shows the list of available virtual machine extensions.
6. Select the **Azure Monitor, Update and Configuration Management** extension and select **Create**. The **Install extension** configuration page opens.

   > **NOTE**
   >
   > If you do not see the **Azure Monitor, Update and Configuration Management** extension listed in your marketplace, please reach out to your Azure Stack Hub operator to make it available.

7. On the **Install extension** configuration page, paste the **Workspace ID** and **Workspace Key (Primary Key)** that you copied into Notepad in the previous step.
8. When you complete the configuration, select **OK**. The extension's status will show as **Provisioning Succeeded**. It might take up to one hour for the virtual machine to appear in Security Center.

Onboard your Linux machines

To add Linux machines, you need the WGET command from the **Agents management** page.

1. From the **Agents management** page, copy the **WGET** command into Notepad. Save this file to a location that can be accessible from your Linux computer.
2. On your Linux computer, open the file with the WGET command. Select the entire content and copy and paste it into a terminal console.
3. When the installation completes, you can validate that the *omsagent* is installed by running the *pgrep* command. The command will return the *omsagent* PID. The logs for the Agent can be found at: */var/opt/microsoft/omsagent/<workspace id>/log/* It might take up to 30 minutes for the new Linux machine to appear in Security Center.

Onboard your Windows machines

To add Windows machines, you need the information on the **Agents management** page and to download the appropriate agent file (32/64-bit).

1. Select the **Download Windows Agent** link applicable to your computer processor type to download the setup file.
2. From the **Agents management** page, copy the **Workspace ID** and **Primary Key** into Notepad.
3. Copy the downloaded setup file to the target computer and run it.
4. Follow the installation wizard (**Next**, **I Agree**, **Next**, **Next**).
   a. On the **Azure Log Analytics** page, paste the **Workspace ID** and **Workspace Key (Primary Key)** that you copied into Notepad.
   b. If the computer should report to a Log Analytics workspace in Azure Government cloud, select **Azure US Government** from the **Azure Cloud** dropdown list.

c. If the computer needs to communicate through a proxy server to the Log Analytics service, select **Advanced** and provide the URL and port number of the proxy server.

d. When you've entered all of the configuration settings, select **Next**.

e. From the **Ready to Install** page, review the settings to be applied and select **Install**.

f. On the **Configuration completed successfully** page, select **Finish**.

When complete, the **Microsoft Monitoring agent** appears in **Control Panel**. You can review your configuration there and verify that the agent is connected.

For further information on installing and configuring the agent, see Connect Windows machines.

Verifying

Congratulations! Now you can see your Azure and non-Azure machines together in one place. Open the asset inventory page and filter to the relevant resource types. These icons distinguish the types:

Non-Azure machine

Azure VM

Azure Arc enabled server

Next steps

This page showed you how to add your non-Azure machines to Azure Security Center. To monitor their status, use the inventory tools as explained in the following page:

- Explore and manage your resources with asset inventory

Troubleshoot Azure Arc-enabled servers agent connection issues

9/7/2021 • 7 minutes to read • Edit Online

This article provides information on troubleshooting and resolving issues that may occur while attempting to configure the Azure Arc-enabled servers Connected Machine agent for Windows or Linux. Both the interactive and at-scale installation methods when configuring connection to the service are included. For general information, see Azure Arc-enabled servers overview.

Agent error codes

If you receive an error when configuring the Azure Arc-enabled servers agent, the following table can help you identify the probable cause and suggested steps to resolve your problem. You will need the `AZCM0000` ("0000" can be any 4 digit number) error code printed to the console or script output to proceed.

ERROR CODE	PROBABLE CAUSE	SUGGESTED REMEDIATION
AZCM0000	The action was successful	N/A
AZCM0001	An unknown error occurred	Contact Microsoft Support for further assistance
AZCM0011	The user canceled the action (CTRL+C)	Retry the previous command
AZCM0012	The access token provided is invalid	Obtain a new access token and try again
AZCM0013	The tags provided are invalid	Check that the tags are enclosed in double quotes, separated by commas, and that any names or values with spaces are enclosed in single quotes: `--tags "SingleName='Value with spaces',Location=Redmond"`
AZCM0014	The cloud is invalid	Specify a supported cloud: `AzureCloud` or `AzureUSGovernment`
AZCM0015	The correlation ID specified is not a valid GUID	Provide a valid GUID for `--correlation-id`
AZCM0016	Missing a mandatory parameter	Review the output to identify which parameters are missing
AZCM0017	The resource name is invalid	Specify a name that only uses alphanumeric characters, hyphens and/or underscores. The name cannot end with a hyphen or underscore.
AZCM0018	The command was executed without administrative privileges	Retry the command with administrator or root privileges in an elevated command prompt or console session.

ERROR CODE	PROBABLE CAUSE	SUGGESTED REMEDIATION
AZCM0041	The credentials supplied are invalid	For device logins, verify the user account specified has access to the tenant and subscription where the server resource will be created. For service principal logins, check the client ID and secret for correctness, the expiration date of the secret, and that the service principal is from the same tenant where the server resource will be created.
AZCM0042	Creation of the Azure Arc-enabled server resource failed	Verify that the user/service principal specified has access to create Azure Arc-enabled server resources in the specified resource group.
AZCM0043	Deletion of the Azure Arc-enabled server resource failed	Verify that the user/service principal specified has access to delete Azure Arc-enabled server resources in the specified resource group. If the resource no longer exists in Azure, use the `--force-local-only` flag to proceed.
AZCM0044	A resource with the same name already exists	Specify a different name for the `--resource-name` parameter or delete the existing Azure Arc-enabled server in Azure and try again.
AZCM0061	Unable to reach the agent service	Verify you are running the command in an elevated user context (administrator/root) and that the HIMDS service is running on your server.
AZCM0062	An error occurred while connecting the server	Review other error codes in the output for more specific information. If the error occurred after the Azure resource was created, you need to delete the Arc server from your resource group before retrying.
AZCM0063	An error occurred while disconnecting the server	Review other error codes in the output for more specific information. If you continue to encounter this error, you can delete the resource in Azure and then run `azcmagent disconnect --force-local-only` on the server to disconnect the agent.
AZCM0064	The agent service is not responding	Check the status of the `himds` service to ensure it is running. Start the service if it is not running. If it is running, wait a minute then try again.
AZCM0065	An internal agent communication error occurred	Contact Microsoft Support for assistance

ERROR CODE	PROBABLE CAUSE	SUGGESTED REMEDIATION
AZCM0066	The agent web service is not responding or unavailable	Contact Microsoft Support for assistance
AZCM0067	The agent is already connected to Azure	Follow the steps in disconnect the agent first, then try again.
AZCM0068	An internal error occurred while disconnecting the server from Azure	Contact Microsoft Support for assistance
AZCM0081	An error occurred while downloading the Azure Active Directory managed identity certificate	If this message is encountered while attempting to connect the server to Azure, the agent won't be able to communicate with the Azure Arc service. Delete the resource in Azure and try connecting again.
AZCM0101	The command was not parsed successfully	Run `azcmagent <command> --help` to review the correct command syntax
AZCM0102	Unable to retrieve the computer hostname	Run `hostname` to check for any system-level error messages, then contact Microsoft Support.
AZCM0103	An error occurred while generating RSA keys	Contact Microsoft Support for assistance
AZCM0104	Failed to read system information	Verify the identity used to run `azcmagent` has administrator/root privileges on the system and try again.

Agent verbose log

Before following the troubleshooting steps described later in this article, the minimum information you need is the verbose log. It contains the output of the **azcmagent** tool commands, when the verbose (-v) argument is used. The log files are written to `%ProgramData%\AzureConnectedMachineAgent\Log\azcmagent.log` for Windows, and Linux to `/var/opt/azcmagent/log/azcmagent.log`.

Windows

The following is an example of the command to enable verbose logging with the Connected Machine agent for Windows when performing an interactive installation.

```
& "$env:ProgramFiles\AzureConnectedMachineAgent\azcmagent.exe" connect --resource-group "resourceGroupName"
--tenant-id "tenantID" --location "regionName" --subscription-id "subscriptionID" --verbose
```

The following is an example of the command to enable verbose logging with the Connected Machine agent for Windows when performing an at-scale installation using a service principal.

```
& "$env:ProgramFiles\AzureConnectedMachineAgent\azcmagent.exe" connect `
  --service-principal-id "{serviceprincipalAppID}" `
  --service-principal-secret "{serviceprincipalPassword}" `
  --resource-group "{ResourceGroupName}" `
  --tenant-id "{tenantID}" `
  --location "{resourceLocation}" `
  --subscription-id "{subscriptionID}"
  --verbose
```

Linux

The following is an example of the command to enable verbose logging with the Connected Machine agent for Linux when performing an interactive installation.

> **NOTE**
>
> You must have *root* access permissions on Linux machines to run **azcmagent**.

```
azcmagent connect --resource-group "resourceGroupName" --tenant-id "tenantID" --location "regionName" --subscription-id "subscriptionID" --verbose
```

The following is an example of the command to enable verbose logging with the Connected Machine agent for Linux when performing an at-scale installation using a service principal.

```
azcmagent connect \
  --service-principal-id "{serviceprincipalAppID}" \
  --service-principal-secret "{serviceprincipalPassword}" \
  --resource-group "{ResourceGroupName}" \
  --tenant-id "{tenantID}" \
  --location "{resourceLocation}" \
  --subscription-id "{subscriptionID}"
  --verbose
```

Agent connection issues to service

The following table lists some of the known errors and suggestions on how to troubleshoot and resolve them.

MESSAGE	ERROR	PROBABLE CAUSE	SOLUTION
Failed to acquire authorization token device flow	`Error occurred while sending request for Device Authorization Code: Post https://login.windows.net/fb84ce97-b875-4d12-b031-ef5e7edf9c8e/oauth2/devicecode?api-version=1.0: dial tcp 40.126.9.7:443: connect: network is unreachable.`	Cannot reach `login.windows.net` endpoint	Verify connectivity to the endpoint.
Failed to acquire authorization token device flow	`Error occurred while sending request for Device Authorization Code: Post https://login.windows.net/fb84ce97-b875-4d12-b031-ef5e7edf9c8e/oauth2/devicecode?api-version=1.0: dial tcp 40.126.9.7:443: connect: network is Forbidden` .	Proxy or firewall is blocking access to `login.windows.net` endpoint.	Verify connectivity to the endpoint and it is not blocked by a firewall or proxy server.
Failed to acquire authorization token device flow	`Error occurred while sending request for Device Authorization Code: Post https://login.windows.net/fb84ce97-b875-4d12-b031-ef5e7edf9c8e/oauth2/devicecode?api-version=1.0: dial tcp lookup login.windows.net: no such host` .	Group Policy Object *Computer Configuration\ Administrative Templates\ System\ User Profiles\ Delete user profiles older than a specified number of days on system restart* is enabled.	Verify the GPO is enabled and targeting the affected machine. See footnote [1] for further details.

MESSAGE	ERROR	PROBABLE CAUSE	SOLUTION
Failed to acquire authorization token from SPN	`Failed to execute the refresh request. Error = 'Post https://login.windows.net/fb84ce97-b875-4d12-b031-ef5e7edf9c8e/oauth2/token?api-version=1.0: Forbidden'`	Proxy or firewall is blocking access to `login.windows.net` endpoint.	Verify connectivity to the endpoint and it is not blocked by a firewall or proxy server.
Failed to acquire authorization token from SPN	`Invalid client secret is provided`	Wrong or invalid service principal secret.	Verify the service principal secret.
Failed to acquire authorization token from SPN	`Application with identifier 'xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx' was not found in the directory 'xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx'. This can happen if the application has not been installed by the administrator of the tenant or consented to by any user in the tenant`	Incorrect service principal and/or Tenant ID.	Verify the service principal and/or the tenant ID.
Get ARM Resource Response	`The client 'username@domain.com' with object id 'xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx' does not have authorization to perform action 'Microsoft.HybridCompute/machines/read' over scope '/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx/resourcegroups/myResourceGroup/providers/Microsoft.HybridCompute/machines/MSJC0 or the scope is invalid. If access was recently granted, please refresh your credentials."}}' Status Code=403`	Wrong credentials and/or permissions	Verify you or the service principal is a member of the **Azure Connected Machine Onboarding** role.
Failed to AzcmagentConnect ARM resource	`The subscription is not registered to use namespace 'Microsoft.HybridCompute'`	Azure resource providers are not registered.	Register the resource providers.
Failed to AzcmagentConnect ARM resource	`Get https://management.azure.com/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx/resourcegroups/myResourceGroup/providers/Microsoft.HybridCompute/machines/MSJC0 api-version=2019-03-18-preview: Forbidden`	Proxy server or firewall is blocking access to `management.azure.com` endpoint.	Verify connectivity to the endpoint and it is not blocked by a firewall or proxy server.

[1] If this GPO is enabled and applies to machines with the Connected Machine agent, it deletes the user profile associated with the built-in account specified for the *himds* service. As a result, it also deletes the authentication certificate used to communicate with the service that is cached in the local certificate store for 30 days. Before the 30-day limit, an attempt is made to renew the certificate. To resolve this issue, follow the steps to unregister the machine and then re-register it with the service running `azcmagent connect`.

Next steps

If you don't see your problem here or you can't resolve your issue, try one of the following channels for additional 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.
- File an Azure support incident. Go to the Azure support site, and select **Get Support**.

Troubleshoot Azure Arc-enabled servers VM extension issues

9/7/2021 • 2 minutes to read • Edit Online

This article provides information on troubleshooting and resolving issues that may occur while attempting to deploy or remove Azure VM extensions on Azure Arc-enabled servers. For general information, see Manage and use Azure VM extensions.

General troubleshooting

Data about the state of extension deployments can be retrieved from the Azure portal.

The following troubleshooting steps apply to all VM extensions.

1. To check the Guest agent log, look at the activity when your extension was being provisioned in `%SystemDrive%\ProgramData\GuestConfig\ext_mgr_logs` for Windows, and for Linux under `/var/lib/GuestConfig/ext_mgr_logs`.

2. Check the extension logs for the specific extension for more details in `%SystemDrive%\ProgramData\GuestConfig\extension_logs\<Extension>` for Windows. Extension output is logged to a file for each extension installed on Linux under `/var/lib/GuestConfig/extension_logs`.

3. Check extension-specific documentation troubleshooting sections for error codes, known issues etc. Additional troubleshooting information for each extension can be found in the **Troubleshoot and support** section in the overview for the extension. This includes the description of error codes written to the log. The extension articles are linked in the extensions table.

4. Look at the system logs. Check for other operations that may have interfered with the extension, such as a long running installation of another application that required exclusive package manager access.

Troubleshooting specific extension scenarios

VM Insights

- When enabling VM Insights for an Azure Arc-enabled server, it installs the Dependency and Log Analytics agent. On a slow machine or one with a slow network connection, it is possible to see timeouts during the installation process. Microsoft is taking steps to address this in the Connected Machine agent to help improve this condition. In the interim, a retry of the installation may succeed.

Log Analytics agent for Linux

- The Log Analytics agent version 1.13.9 (corresponding extension version is 1.13.15) is not correctly marking uploaded data with the resource ID of the Azure Arc-enabled server. Although logs are being sent to the service, when you try to view the data from the selected enabled server after selecting **Logs** or **Insights**, no data is returned. You can view its data by running queries from Azure Monitor Logs or from Azure Monitor for VMs, which are scoped to the workspace.

- Some distributions are not currently supported by the Log Analytics agent for Linux. The agent requires additional dependencies to be installed, including Python 2. Review the support matrix and prerequisites here.

- Error code 52 in the status message indicates a missing dependency. Check the output and logs for more information about which dependency is missing.

- If an installation fails, review the **Troubleshoot and support** section in the overview for the extension. In most cases, there is an error code included in the status message. For the Log Analytics agent for Linux, status messages are explained here, along with general troubleshooting information for this VM extension.

Next steps

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

- File an Azure support incident. Go to the Azure support site, and select **Get Support**.

Azure Arc-enabled servers: Data residency

9/7/2021 • 2 minutes to read • Edit Online

This article explains the concept of data residency and how it applies to Azure Arc-enabled servers.

Azure Arc-enabled servers is **available** in the **United States, Europe, United Kingdom, Australia, and Asia Pacific**.

Data residency

Azure Arc-enabled servers store Azure VM extension configuration settings (that is, property values) the extension requires specifying before attempting to enable on the connected machine. For example, when you enable the Log Analytics VM extension, it asks for the Log Analytics **workspace ID** and **primary key**.

Metadata information about the connected machine is also collected. Specifically:

- Operating system name, type, and version
- Computer name
- Computer fully qualified domain name (FQDN)
- Connected Machine agent version
- Active Directory and DNS fully qualified domain name (FQDN)
- UUID (BIOS ID)
- Connected Machine agent heartbeat
- Connected Machine agent version
- Public key for managed identity
- Policy compliance status and details (if using guest configuration policies)

Azure Arc-enabled servers allow you to specify the region where your data is stored. Microsoft may replicate to other regions for data resiliency, but Microsoft does not replicate or move data outside the geography. This data is stored in the region where the Azure Arc machine resource is configured. For example, if the machine is registered with Arc in the East US region, this data is stored in the US region.

> **NOTE**
>
> For South East Asia, your data is not replicated outside of this region.

For more information about our regional resiliency and compliance support, see Azure geography.

Next steps

Learn more about designing for Azure resiliency.

Azure Policy built-in definitions for Azure Arc-enabled servers

9/3/2021 • 21 minutes to read • Edit Online

This page is an index of Azure Policy built-in policy definitions for Azure Arc-enabled servers. For additional Azure Policy built-ins for other services, see Azure Policy built-in definitions.

The name of each built-in policy definition links to the policy definition in the Azure portal. Use the link in the **Version** column to view the source on the Azure Policy GitHub repo.

Azure Arc-enabled servers

NAME (AZURE PORTAL)	DESCRIPTION	EFFECT(S)	VERSION (GITHUB)
Audit Linux machines that allow remote connections from accounts without passwords	Requires that prerequisites are deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol. Machines are non-compliant if Linux machines that allow remote connections from accounts without passwords	AuditIfNotExists, Disabled	1.0.0
Audit Linux machines that do not have the passwd file permissions set to 0644	Requires that prerequisites are deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol. Machines are non-compliant if Linux machines that do not have the passwd file permissions set to 0644	AuditIfNotExists, Disabled	1.0.0
Audit Linux machines that don't have the specified applications installed	Requires that prerequisites are deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol. Machines are non-compliant if the Chef InSpec resource indicates that one or more of the packages provided by the parameter are not installed.	auditIfNotExists	3.0.0

NAME	DESCRIPTION	EFFECT(S)	VERSION
Audit Linux machines that have accounts without passwords	Requires that prerequisites are deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol. Machines are non-compliant if Linux machines that have accounts without passwords	AuditIfNotExists, Disabled	1.0.0
Audit Linux machines that have the specified applications installed	Requires that prerequisites are deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol. Machines are non-compliant if the Chef InSpec resource indicates that one or more of the packages provided by the parameter are installed.	auditIfNotExists	3.0.0
Audit Windows machines missing any of specified members in the Administrators group	Requires that prerequisites are deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol. Machines are non-compliant if the local Administrators group does not contain one or more members that are listed in the policy parameter.	auditIfNotExists	1.0.0
Audit Windows machines network connectivity	Requires that prerequisites are deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol. Machines are non-compliant if a network connection status to an IP and TCP port does not match the policy parameter.	auditIfNotExists	1.0.0
Audit Windows machines on which the DSC configuration is not compliant	Requires that prerequisites are deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol. Machines are non-compliant if the Windows PowerShell command Get-DSCConfigurationStatus returns that the DSC configuration for the machine is not compliant.	auditIfNotExists	1.0.0

NAME	DESCRIPTION	EFFECT(S)	VERSION
Audit Windows machines on which the Log Analytics agent is not connected as expected	Requires that prerequisites are deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol. Machines are non-compliant if the agent is not installed, or if it is installed but the COM object AgentConfigManager.MgmtSvcCfg returns that it is registered to a workspace other than the ID specified in the policy parameter.	auditIfNotExists	1.0.0
Audit Windows machines on which the specified services are not installed and 'Running'	Requires that prerequisites are deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol. Machines are non-compliant if result of the Windows PowerShell command Get-Service do not include the service name with matching status as specified by the policy parameter.	auditIfNotExists	1.0.0
Audit Windows machines on which Windows Serial Console is not enabled	Requires that prerequisites are deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol. Machines are non-compliant if the machine does not have the Serial Console software installed or if the EMS port number or baud rate are not configured with the same values as the policy parameters.	auditIfNotExists	1.0.0
Audit Windows machines that allow re-use of the previous 24 passwords	Requires that prerequisites are deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol. Machines are non-compliant if Windows machines that allow re-use of the previous 24 passwords	AuditIfNotExists, Disabled	1.0.0

NAME	DESCRIPTION	EFFECT(S)	VERSION
Audit Windows machines that are not joined to the specified domain	Requires that prerequisites are deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol. Machines are non-compliant if the value of the Domain property in WMI class win32_computersystem does not match the value in the policy parameter.	auditIfNotExists	1.0.0
Audit Windows machines that are not set to the specified time zone	Requires that prerequisites are deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol. Machines are non-compliant if the value of the property StandardName in WMI class Win32_TimeZone does not match the selected time zone for the policy parameter.	auditIfNotExists	1.0.0
Audit Windows machines that contain certificates expiring within the specified number of days	Requires that prerequisites are deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol. Machines are non-compliant if certificates in the specified store have an expiration date out of range for the number of days given as parameter. The policy also provides the option to only check for specific certificates or exclude specific certificates, and whether to report on expired certificates.	auditIfNotExists	1.0.0
Audit Windows machines that do not contain the specified certificates in Trusted Root	Requires that prerequisites are deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol. Machines are non-compliant if the machine Trusted Root certificate store (Cert:\LocalMachine\Root) does not contain one or more of the certificates listed by the policy parameter.	auditIfNotExists	1.0.1

NAME	DESCRIPTION	EFFECT(S)	VERSION
Audit Windows machines that do not have a maximum password age of 70 days	Requires that prerequisites are deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol. Machines are non-compliant if Windows machines that do not have a maximum password age of 70 days	AuditIfNotExists, Disabled	1.0.0
Audit Windows machines that do not have a minimum password age of 1 day	Requires that prerequisites are deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol. Machines are non-compliant if Windows machines that do not have a minimum password age of 1 day	AuditIfNotExists, Disabled	1.0.0
Audit Windows machines that do not have the password complexity setting enabled	Requires that prerequisites are deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol. Machines are non-compliant if Windows machines that do not have the password complexity setting enabled	AuditIfNotExists, Disabled	1.0.0
Audit Windows machines that do not have the specified Windows PowerShell execution policy	Requires that prerequisites are deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol. Machines are non-compliant if the Windows PowerShell command Get-ExecutionPolicy returns a value other than what was selected in the policy parameter.	AuditIfNotExists, Disabled	1.0.0
Audit Windows machines that do not have the specified Windows PowerShell modules installed	Requires that prerequisites are deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol. Machines are non-compliant if a module isn't available in a location specified by the environment variable PSModulePath.	AuditIfNotExists, Disabled	2.0.0

NAME	DESCRIPTION	EFFECT(S)	VERSION
Audit Windows machines that do not restrict the minimum password length to 14 characters	Requires that prerequisites are deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol. Machines are non-compliant if Windows machines that do not restrict the minimum password length to 14 characters	AuditIfNotExists, Disabled	1.0.0
Audit Windows machines that do not store passwords using reversible encryption	Requires that prerequisites are deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol. Machines are non-compliant if Windows machines that do not store passwords using reversible encryption	AuditIfNotExists, Disabled	1.0.0
Audit Windows machines that don't have the specified applications installed	Requires that prerequisites are deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol. Machines are non-compliant if the application name is not found in any of the following registry paths: HKLM:SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall, HKLM:SOFTWARE\Wow6432node\Microsoft\Windows\CurrentVersion\Uninstall, HKCU:Software\Microsoft\Windows\CurrentVersion\Uninstall.	auditIfNotExists	1.0.0
Audit Windows machines that have extra accounts in the Administrators group	Requires that prerequisites are deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol. Machines are non-compliant if the local Administrators group contains members that are not listed in the policy parameter.	auditIfNotExists	1.0.0

NAME	DESCRIPTION	EFFECT(S)	VERSION
Audit Windows machines that have not restarted within the specified number of days	Requires that prerequisites are deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol. Machines are non-compliant if the WMI property LastBootUpTime in class Win32_Operatingsystem is outside the range of days provided by the policy parameter.	auditIfNotExists	1.0.0
Audit Windows machines that have the specified applications installed	Requires that prerequisites are deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol. Machines are non-compliant if the application name is found in any of the following registry paths: HKLM:SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall, HKLM:SOFTWARE\Wow6432node\Microsoft\Windows\CurrentVersion\Uninstall, HKCU:Software\Microsoft\Windows\CurrentVersion\Uninstall.	auditIfNotExists	1.0.0
Audit Windows machines that have the specified members in the Administrators group	Requires that prerequisites are deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol. Machines are non-compliant if the local Administrators group contains one or more of the members listed in the policy parameter.	auditIfNotExists	1.0.0

NAME	DESCRIPTION	EFFECT(S)	VERSION
Audit Windows VMs with a pending reboot	Requires that prerequisites are deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol. Machines are non-compliant if the machine is pending reboot for any of the following reasons: component based servicing, Windows Update, pending file rename, pending computer rename, configuration manager pending reboot. Each detection has a unique registry path.	auditIfNotExists	1.0.0
Authentication to Linux machines should require SSH keys	Although SSH itself provides an encrypted connection, using passwords with SSH still leaves the VM vulnerable to brute-force attacks. The most secure option for authenticating to an Azure Linux virtual machine over SSH is with a public-private key pair, also known as SSH keys. Learn more: https://docs.microsoft.com/azure/virtual-machines/linux/create-ssh-keys-detailed.	AuditIfNotExists, Disabled	2.0.1
Configure Dependency agent on Azure Arc enabled Linux servers	Enable VM insights on servers and machines connected to Azure through Arc enabled servers by installing the Dependency agent virtual machine extension. VM insights uses the Dependency agent to collect network metrics and discovered data about processes running on the machine and external process dependencies. See more - https://aka.ms/vminsightsdocs.	DeployIfNotExists, Disabled	2.0.0

NAME	DESCRIPTION	EFFECT(S)	VERSION
Configure Dependency agent on Azure Arc enabled Windows servers	Enable VM insights on servers and machines connected to Azure through Arc enabled servers by installing the Dependency agent virtual machine extension. VM insights uses the Dependency agent to collect network metrics and discovered data about processes running on the machine and external process dependencies. See more - https://aka.ms/vminsightsdocs.	DeployIfNotExists, Disabled	2.0.0
Configure Log Analytics agent on Azure Arc enabled Linux servers	Enable VM insights on servers and machines connected to Azure through Arc enabled servers by installing the Log Analytics agent virtual machine extension. VM insights uses the Log Analytics agent to collect the guest OS performance data, and provides insights into their performance. See more - https://aka.ms/vminsightsdocs.	DeployIfNotExists, Disabled	2.0.0
Configure Log Analytics agent on Azure Arc enabled Windows servers	Enable VM insights on servers and machines connected to Azure through Arc enabled servers by installing the Log Analytics agent virtual machine extension. VM insights uses the Log Analytics agent to collect the guest OS performance data, and provides insights into their performance. See more - https://aka.ms/vminsightsdocs.	DeployIfNotExists, Disabled	2.0.0

NAME	DESCRIPTION	EFFECT(S)	VERSION
[Preview]: Configure machines to receive a vulnerability assessment agent	Azure Defender includes vulnerability scanning for your machines at no extra cost. You don't need a Qualys license or even a Qualys account - everything's handled seamlessly inside Security Center. When you enable this policy, Azure Defender automatically deploys the Qualys vulnerability assessment agent to all supported machines that don't already have it installed.	DeployIfNotExists, Disabled	2.1.0-preview
Configure SQL installed Azure Arc machines to have Arc enabled SQL Server extension enabled.	To ensure SQL Server - Azure Arc resources gets created by default when SQL instance found on Azure Arc enabled windows server, Arc machine should have SQL Server extension enabled. For more information- please visit- https://docs.microsoft.com/en-us/sql/sql-server/azure-arc/overview?view=sql-server-ver15	DeployIfNotExists, Disabled	1.0.0
Configure time zone on Windows machines.	This policy creates a Guest Configuration assignment to set specified time zone on Windows virtual machines.	deployIfNotExists	1.1.0
Endpoint protection health issues should be resolved on your machines	Resolve endpoint protection health issues on your virtual machines to protect them from latest threats and vulnerabilities. Azure Security Center supported endpoint protection solutions are documented here - https://docs.microsoft.com/azure/security-center/security-center-services?tabs=features-windows. Endpoint protection assessment is documented here - https://docs.microsoft.com/azure/security-center/security-center-endpoint-protection.	AuditIfNotExists, Disabled	1.0.0

NAME	DESCRIPTION	EFFECT(S)	VERSION
Endpoint protection should be installed on your machines	To protect your machines from threats and vulnerabilities, install a supported endpoint protection solution.	AuditIfNotExists, Disabled	1.0.0
[Preview]: Linux machines should meet requirements for the Azure compute security baseline	Requires that prerequisites are deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol. Machines are non-compliant if the machine is not configured correctly for one of the recommendations in the Azure compute security baseline.	AuditIfNotExists, Disabled	1.1.1-preview
Linux machines should only have local accounts that are allowed	Requires that prerequisites are deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol. Managing user accounts using Azure Active Directory is a best practice for management of identities. Reducing local machine accounts helps prevent the proliferation of identities managed outside a central system. Machines are non-compliant if local user accounts exist that are enabled and not listed in the policy parameter.	AuditIfNotExists, Disabled	1.0.0
[Preview]: Log Analytics agent should be installed on your Linux Azure Arc machines	This policy audits Linux Azure Arc machines if the Log Analytics agent is not installed.	AuditIfNotExists, Disabled	1.0.0-preview
[Preview]: Log Analytics agent should be installed on your Windows Azure Arc machines	This policy audits Windows Azure Arc machines if the Log Analytics agent is not installed.	AuditIfNotExists, Disabled	1.0.0-preview

NAME	DESCRIPTION	EFFECT(S)	VERSION
SQL servers on machines should have vulnerability findings resolved	SQL vulnerability assessment scans your database for security vulnerabilities, and exposes any deviations from best practices such as misconfigurations, excessive permissions, and unprotected sensitive data. Resolving the vulnerabilities found can greatly improve your database security posture.	AuditIfNotExists, Disabled	1.0.0
Windows Defender Exploit Guard should be enabled on your machines	Windows Defender Exploit Guard uses the Azure Policy Guest Configuration agent. Exploit Guard has four components that are designed to lock down devices against a wide variety of attack vectors and block behaviors commonly used in malware attacks while enabling enterprises to balance their security risk and productivity requirements (Windows only).	AuditIfNotExists, Disabled	1.1.1
Windows machines should meet requirements for 'Administrative Templates - Control Panel'	Windows machines should have the specified Group Policy settings in the category 'Administrative Templates - Control Panel' for input personalization and prevention of enabling lock screens. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol.	AuditIfNotExists, Disabled	2.0.0

NAME	DESCRIPTION	EFFECT(S)	VERSION
Windows machines should meet requirements for 'Administrative Templates - MSS (Legacy)'	Windows machines should have the specified Group Policy settings in the category 'Administrative Templates - MSS (Legacy)' for automatic logon, screen saver, network behavior, safe DLL, and event log. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol.	AuditIfNotExists, Disabled	2.0.0
Windows machines should meet requirements for 'Administrative Templates - Network'	Windows machines should have the specified Group Policy settings in the category 'Administrative Templates - Network' for guest logons, simultaneous connections, network bridge, ICS, and multicast name resolution. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol.	AuditIfNotExists, Disabled	2.0.0
Windows machines should meet requirements for 'Administrative Templates - System'	Windows machines should have the specified Group Policy settings in the category 'Administrative Templates - System' for settings that control the administrative experience and Remote Assistance. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol.	AuditIfNotExists, Disabled	2.0.0

NAME	DESCRIPTION	EFFECT(S)	VERSION
Windows machines should meet requirements for 'Security Options - Accounts'	Windows machines should have the specified Group Policy settings in the category 'Security Options - Accounts' for limiting local account use of blank passwords and guest account status. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol.	AuditIfNotExists, Disabled	2.0.0
Windows machines should meet requirements for 'Security Options - Audit'	Windows machines should have the specified Group Policy settings in the category 'Security Options - Audit' for forcing audit policy subcategory and shutting down if unable to log security audits. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol.	AuditIfNotExists, Disabled	2.0.0
Windows machines should meet requirements for 'Security Options - Devices'	Windows machines should have the specified Group Policy settings in the category 'Security Options - Devices' for undocking without logging on, installing print drivers, and formatting/ejecting media. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol.	AuditIfNotExists, Disabled	2.0.0

NAME	DESCRIPTION	EFFECT(S)	VERSION
Windows machines should meet requirements for 'Security Options - Interactive Logon'	Windows machines should have the specified Group Policy settings in the category 'Security Options - Interactive Logon' for displaying last user name and requiring ctrl-alt-del. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol.	AuditIfNotExists, Disabled	2.0.0
Windows machines should meet requirements for 'Security Options - Microsoft Network Client'	Windows machines should have the specified Group Policy settings in the category 'Security Options - Microsoft Network Client' for Microsoft network client/server and SMB v1. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol.	AuditIfNotExists, Disabled	2.0.0
Windows machines should meet requirements for 'Security Options - Microsoft Network Server'	Windows machines should have the specified Group Policy settings in the category 'Security Options - Microsoft Network Server' for disabling SMB v1 server. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol.	AuditIfNotExists, Disabled	2.0.0

NAME	DESCRIPTION	EFFECT(S)	VERSION
Windows machines should meet requirements for 'Security Options - Network Access'	Windows machines should have the specified Group Policy settings in the category 'Security Options - Network Access' for including access for anonymous users, local accounts, and remote access to the registry. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol.	AuditIfNotExists, Disabled	2.0.0
Windows machines should meet requirements for 'Security Options - Network Security'	Windows machines should have the specified Group Policy settings in the category 'Security Options - Network Security' for including Local System behavior, PKU2U, LAN Manager, LDAP client, and NTLM SSP. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol.	AuditIfNotExists, Disabled	2.0.0
Windows machines should meet requirements for 'Security Options - Recovery console'	Windows machines should have the specified Group Policy settings in the category 'Security Options - Recovery console' for allowing floppy copy and access to all drives and folders. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol.	AuditIfNotExists, Disabled	2.0.0

NAME	DESCRIPTION	EFFECT(S)	VERSION
Windows machines should meet requirements for 'Security Options - Shutdown'	Windows machines should have the specified Group Policy settings in the category 'Security Options - Shutdown' for allowing shutdown without logon and clearing the virtual memory pagefile. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol.	AuditIfNotExists, Disabled	2.0.0
Windows machines should meet requirements for 'Security Options - System objects'	Windows machines should have the specified Group Policy settings in the category 'Security Options - System objects' for case insensitivity for non-Windows subsystems and permissions of internal system objects. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol.	AuditIfNotExists, Disabled	2.0.0
Windows machines should meet requirements for 'Security Options - System settings'	Windows machines should have the specified Group Policy settings in the category 'Security Options - System settings' for certificate rules on executables for SRP and optional subsystems. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol.	AuditIfNotExists, Disabled	2.0.0

NAME	DESCRIPTION	EFFECT(S)	VERSION
Windows machines should meet requirements for 'Security Options - User Account Control'	Windows machines should have the specified Group Policy settings in the category 'Security Options - User Account Control' for mode for admins, behavior of elevation prompt, and virtualizing file and registry write failures. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol.	AuditIfNotExists, Disabled	2.0.0
Windows machines should meet requirements for 'Security Settings - Account Policies'	Windows machines should have the specified Group Policy settings in the category 'Security Settings - Account Policies' for password history, age, length, complexity, and storing passwords using reversible encryption. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol.	AuditIfNotExists, Disabled	2.0.0
Windows machines should meet requirements for 'System Audit Policies - Account Logon'	Windows machines should have the specified Group Policy settings in the category 'System Audit Policies - Account Logon' for auditing credential validation and other account logon events. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol.	AuditIfNotExists, Disabled	2.0.0

NAME	DESCRIPTION	EFFECT(S)	VERSION
Windows machines should meet requirements for 'System Audit Policies - Account Management'	Windows machines should have the specified Group Policy settings in the category 'System Audit Policies - Account Management' for auditing application, security, and user group management, and other management events. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol.	AuditIfNotExists, Disabled	2.0.0
Windows machines should meet requirements for 'System Audit Policies - Detailed Tracking'	Windows machines should have the specified Group Policy settings in the category 'System Audit Policies - Detailed Tracking' for auditing DPAPI, process creation/termination, RPC events, and PNP activity. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol.	AuditIfNotExists, Disabled	2.0.0
Windows machines should meet requirements for 'System Audit Policies - Logon-Logoff'	Windows machines should have the specified Group Policy settings in the category 'System Audit Policies - Logon-Logoff' for auditing IPSec, network policy, claims, account lockout, group membership, and logon/logoff events. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol.	AuditIfNotExists, Disabled	2.0.0

NAME	DESCRIPTION	EFFECT(S)	VERSION
Windows machines should meet requirements for 'System Audit Policies - Object Access'	Windows machines should have the specified Group Policy settings in the category 'System Audit Policies - Object Access' for auditing file, registry, SAM, storage, filtering, kernel, and other system types. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol.	AuditIfNotExists, Disabled	2.0.0
Windows machines should meet requirements for 'System Audit Policies - Policy Change'	Windows machines should have the specified Group Policy settings in the category 'System Audit Policies - Policy Change' for auditing changes to system audit policies. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol.	AuditIfNotExists, Disabled	2.0.0
Windows machines should meet requirements for 'System Audit Policies - Privilege Use'	Windows machines should have the specified Group Policy settings in the category 'System Audit Policies - Privilege Use' for auditing nonsensitive and other privilege use. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol.	AuditIfNotExists, Disabled	2.0.0

NAME	DESCRIPTION	EFFECT(S)	VERSION
Windows machines should meet requirements for 'System Audit Policies - System'	Windows machines should have the specified Group Policy settings in the category 'System Audit Policies - System' for auditing IPsec driver, system integrity, system extension, state change, and other system events. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol.	AuditIfNotExists, Disabled	2.0.0
Windows machines should meet requirements for 'User Rights Assignment'	Windows machines should have the specified Group Policy settings in the category 'User Rights Assignment' for allowing log on locally, RDP, access from the network, and many other user activities. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol.	AuditIfNotExists, Disabled	2.0.0
Windows machines should meet requirements for 'Windows Components'	Windows machines should have the specified Group Policy settings in the category 'Windows Components' for basic authentication, unencrypted traffic, Microsoft accounts, telemetry, Cortana, and other Windows behaviors. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol.	AuditIfNotExists, Disabled	2.0.0

NAME	DESCRIPTION	EFFECT(S)	VERSION
Windows machines should meet requirements for 'Windows Firewall Properties'	Windows machines should have the specified Group Policy settings in the category 'Windows Firewall Properties' for firewall state, connections, rule management, and notifications. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol.	AuditIfNotExists, Disabled	2.0.0
[Preview]: Windows machines should meet requirements of the Azure compute security baseline	Requires that prerequisites are deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol. Machines are non-compliant if the machine is not configured correctly for one of the recommendations in the Azure compute security baseline.	AuditIfNotExists, Disabled	1.0.1-preview
Windows machines should only have local accounts that are allowed	Requires that prerequisites are deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol. This definition is not supported on Windows Server 2012 or 2012 R2. Managing user accounts using Azure Active Directory is a best practice for management of identities. Reducing local machine accounts helps prevent the proliferation of identities managed outside a central system. Machines are non-compliant if local user accounts exist that are enabled and not listed in the policy parameter.	AuditIfNotExists, Disabled	1.0.0

NAME	DESCRIPTION	EFFECT(S)	VERSION
Windows web servers should be configured to use secure communication protocols	To protect the privacy of information communicated over the Internet, your web servers should use the latest version of the industry-standard cryptographic protocol, Transport Layer Security (TLS). TLS secures communications over a network by using security certificates to encrypt a connection between machines.	AuditIfNotExists, Disabled	3.0.0

Next steps

- See the built-ins on the Azure Policy GitHub repo.
- Review the Azure Policy definition structure.
- Review Understanding policy effects.