

# Windows Defender Application Control for Azure Stack HCI, version 23H2 (preview)

Article • 11/14/2023

Applies to: Azure Stack HCI, version 23H2 (preview)

This article describes how to use Windows Defender Application Control (WDAC) to reduce the attack surface of Azure Stack HCI.

WDAC is a software-based security layer that reduces attack surface by enforcing an explicit list of software that is allowed to run. WDAC is enabled by default and limits the applications and the code that you can run on the core platform. For more information, see [Windows Defender Application Control](#).

## Important

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

## Enable WDAC policy modes

You can decide to have WDAC enabled during deployment or after deployment. If you want to change the initial selection in the deployment wizard, you can do it after deployment using PowerShell.

Connect to one of the cluster nodes and use the following cmdlets to enable the desired WDAC policy in "Audit" or "Enforced" mode. In this build release there are two cmdlets.

- First cmdlet `Enable-AsWdacPolicy` affects all the nodes in the cluster.
- Second cmdlet `Enable-ASLocalWDACPolicy` only affects the node from where it is run.

Depending on the use case, you should run a global cluster change or a local node change.

This is useful when:

- You started with the default recommended settings. You need to install or run new third party software. You can switch your policy modes to create a supplemental policy.
- You started with WDAC disabled during deployment and now you want to enable WDAC to increase security protection or to validate that your software runs properly.
- Your software or scripts are blocked by WDAC. In this case you can use audit mode to understand and troubleshoot the issue.

#### ⓘ Note

- When your application is blocked, WDAC will create a corresponding event. Review the Event log to understand the details of the policy that's blocking your application. For more information, see the [Windows Defender Application Control operational guide](#).

Follow these steps to switch between WDAC policy modes. These PowerShell commands interact with the Orchestrator to enable the selected modes.

1. Connect to your Azure Stack HCI node.
2. Run the following PowerShell command using local administrator credentials or deployment user credentials.

#### ⓘ Important

Cmdlets interacting with LCM (Lifecycle Manager) requires proper credentials authorization via the security group (PREFIX-ECESG) and CredSSP (when using remote PowerShell) or Console session (RDP)

3. Run the following cmdlet to check the WDAC policy mode that is currently enabled:

PowerShell

```
Get-AsWdacPolicyMode
```

This cmdlet returns an integer:

- 0 – Not deployed
- 1 – Audit

- 2 - Enforced

4. Run the following cmdlet to switch the policy mode:

PowerShell

```
Enable-AsWdacPolicy -Mode <PolicyMode [Audit | Enforced]>
```

For example, to switch the policy mode to audit, run:

PowerShell

```
Enable-AsWdacPolicy -Mode Audit
```

### Warning

The Orchestrator will take up to two to three minutes to switch to the selected mode.

5. Run `Get-ASWDACPolicyMode` again to confirm the policy mode is updated.

PowerShell

```
Get-AsWdacPolicyMode
```

Here's a sample output of these cmdlets:

Azure PowerShell

```
PS C:\> Get-AsWdacPolicyMode
```

```
2
```

```
PS C:\> Enable-AsWdacPolicy -Mode Audit
```

```
VERBOSE: Action plan instance ID specified: a61a1fa2-da14-4711-8de3-0c1cc3a71ff4  
a61a1fa2-da14-4111-8de3-0c1cc3a71ff4
```

```
PS C:\temp> Get-WDACPolicyMode
```

```
1
```

# Create a WDAC policy to enable third party software

While using this preview with WDAC in enforcement mode, for your non-Microsoft signed software to run, you'll need to build on the Microsoft-provided base policy by creating a WDAC supplemental policy. Additional information can be found in our [public WDAC documentation](#).

## ⓘ Note

To run or install new software, you might need to switch WDAC to audit mode first (see steps above), install your software, test that it works correctly, create the new supplemental policy, and then switch WDAC back to enforced mode.

Create a new policy in the Multiple Policy Format as shown below. Then use `Add-ASWDACSupplementalPolicy -Path Policy.xml` to convert it to a supplemental policy and deploy it across nodes in the cluster.

## Create a WDAC supplemental policy

Use the following steps to create a supplemental policy:

1. Before you begin, install the software that will be covered by the supplemental policy into its own directory. It's okay if there are subdirectories. When creating the supplemental policy, you must provide a directory to scan, and you don't want your supplemental policy to cover all code on the system. In our example, this directory is C:\software\codetoscan.
2. Once you have all your software in place, run the following command to create your supplemental policy. Use a unique policy name to help identify it.

Azure PowerShell

```
New-CIPolicy -MultiplePolicyFormat -Level Publisher -FilePath  
c:\wdac\Contoso-policy.xml -UserPEs -Fallback Hash -ScanPath  
c:\software\codetoscan
```

3. Modify the metadata of your supplemental policy.

Azure PowerShell

```
# Set Policy Version (VersionEx in the XML file)
$policyVersion = "1.0.0.1"
Set-CIPolicyVersion -FilePath $policyPath -Version $policyVersion

# Set Policy Info (PolicyName, PolicyID in the XML file)
Set-CIPolicyIdInfo -FilePath c:\wdac\Contoso-policy.xml -PolicyID
"Contoso-Policy_$policyVersion" -PolicyName "Contoso-Policy"
```

#### 4. Deploy the policy.

Azure PowerShell

```
Add-ASWDACSupplementalPolicy -Path c:\wdac\Contoso-supplemental-
policy.xml
```

#### 5. To check the status of the new policy:

Azure PowerShell

```
Get-ASLocalWDACPolicyInfo
```

Here's a sample output of these cmdlets:

Azure PowerShell

```
C:\> Get-ASLocalWDACPolicyInfo
```

```

NodeName      : Node01
PolicyMode    : Enforced
PolicyGuid    : {A6368F66-E2C9-4AA2-AB79-8743F6597683}
PolicyName    : AS_Base_Policy
PolicyVersion : AS_Base_Policy_1.1.4.0
PolicyScope   : Kernel & User
MicrosoftProvided : True
LastTimeApplied : 10/26/2023 11:14:24 AM
```

```

NodeName      : Node01
PolicyMode    : Enforced
PolicyGuid    : {2112036A-74E9-47DC-A016-F126297A3427}
PolicyName    : Contoso-Policy
PolicyVersion : Contoso-Policy_1.0.0.1
PolicyScope   : Kernel & User
MicrosoftProvided : False
LastTimeApplied : 10/26/2023 11:14:24 AM
```

## Next steps

- [Install Azure Stack HCI, version 23H2.](#)

# Security baseline settings for Azure Stack HCI, version 23H2 (preview)

Article • 11/15/2023

Applies to: Azure Stack HCI, version 23H2 (preview)

This article describes the security baseline settings associated with your Azure Stack HCI cluster, the associated drift control mechanism, and baseline management.

Azure Stack HCI is a secure-by-default product and has more than 300 security settings enabled right from the start. These settings provide a consistent security baseline to ensure that the device always starts in a known good state.

## Important

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

## Benefits of the security baseline

The security baseline on Azure Stack HCI:

- Enables you to closely meet Center for Internet Security (CIS) benchmark and Defense Information System Agency (DISA) Security Technical Implementation Guide (STIG) requirements for the operating system (OS) and the Microsoft recommended security baseline.
- Reduces the operating expenditure (OPEX) with its built-in drift protection mechanism and consistent at-scale monitoring via the Azure Arc Hybrid Edge baseline.
- Improves the security posture by disabling legacy protocols and ciphers.

## About security baseline and drift control

When you prepare the Active Directory for Azure Stack HCI and create a dedicated organizational unit (OU), by default, the existing group policies and Group Policy Object (GPO) inheritance are blocked. Blocking these policies ensures that there is no conflict of security settings.

The Azure Stack HCI Supplemental Package deployment then establishes and maintains:

- A new built-in configuration management stack in the operating system.
- A security baseline.
- Secured-core settings for your cluster.

You can monitor and perform drift protection of this default enabled security baseline and secured-core settings during both deployment and runtime. You can also disable the drift protection during the deployment when you configure the security settings.

With drift protection applied, the security settings are refreshed regularly after every 90 minutes. This refresh interval is the same as that for the group policies and ensures that any changes from the desired state are remediated. This continuous monitoring and auto-remediation allows you to have a consistent and reliable security posture throughout the lifecycle of the device.

## Modify drift control

To adjust security hardening as per your requirements, we recommend that you keep a balanced security posture. Use the initial security baseline, stop the drift control, and modify any of the protected security settings that you defined during the deployment.

To toggle drift control, follow these steps.

1. Connect to your Azure Stack HCI node.
2. Run the following PowerShell command using local administrator credentials or deployment user account credentials.
3. To disable drift control:

PowerShell

```
Disable-AzsSecurity -FeatureName DriftControl -Scope <Local | Cluster>
```

- **Local** - Affects local node only. Can be run on a regular remote PowerShell session.
- **Cluster** - Affects all nodes in the cluster using the orchestrator. Requires user to belong to the deployment authorization group (PREFIX-ECESG) and CredSSP or an Azure Stack HCI server using a remote desktop protocol (RDP) connection.

4. To enable drift control:



PowerShell

```
Enable-AzsSecurity -FeatureName DriftControl -Scope <Local | Cluster>
```

- **Local** - Affects local node only. Can be run on a regular remote PowerShell session.
- **Cluster** - Affects all nodes in the cluster using the orchestrator. Requires user to belong to the deployment authorization group (PREFIX-ECESG) and CredSSP or an Azure Stack HCI server using a remote desktop protocol (RDP) connection.

## Manage security baseline

When deploying your cluster via the Supplemental Package, you can modify the drift control settings as well as other security settings that constitute the security baseline. The changes that you make to the security settings are also reflected in the *config.json* that you are create using the deployment tool.

## Configure security during deployment

The following table describes the security settings that can be configured on your Azure Stack HCI cluster during deployment.

Feature area	Feature	Description	Supports drift control?
Governance	<a href="#">Security baseline</a>	Maintains the security defaults on each server. Helps protect against changes.	Yes
Credential protection	<a href="#">Windows Defender Credential Guard</a>	Uses virtualization-based security to isolate secrets from credential-theft attacks.	Yes
Application control	<a href="#">Windows Defender Application control</a>	Controls which drivers and apps are allowed to run directly on each server.	No
Data at-rest encryption	<a href="#">BitLocker for OS boot volume</a>	Encrypts the OS startup volume on each server.	No
Data at-rest encryption	<a href="#">BitLocker for data volumes</a>	Encrypts cluster shared volumes (CSVs) on this cluster	No

Feature area	Feature	Description	Supports drift control?
Data in-transit protection	<a href="#">Signing for external SMB traffic</a>	Signs SMB traffic between this system and others to help prevent relay attacks.	Yes
Data in-transit protection	<a href="#">SMB Encryption for in-cluster traffic</a>	Encrypts traffic between servers in the cluster (on your storage network).	No

## Modify security after deployment

Once the deployment is complete, you can also enable security features while maintaining drift control. Here is a table of the commands used to modify these security features.

As noted, some of these features might require a reboot to take effect. We provide commands to Get, Enable, and Disable security features.

## PowerShell cmdlet properties for `AzureStackOSConfigAgent` module

The following cmdlet properties are for module *AzureStackOSConfigAgent*.

- `Get-AzsSecurity` -Scope: <Local | PerNode | AllNodes | Cluster>
- `Enable-AzsSecurity` -Scope <Local | Cluster>
- `Disable-AzsSecurity` -Scope <Local | Cluster>
  - **Local** - Provides boolean value (true/False) on local node. Can be run on a regular remote PowerShell session.
  - **PerNode** - Provides boolean value (true/False) per node.
  - **Report** - Requires CredSSP or an Azure Stack HCI server using a remote desktop protocol (RDP) connection. AllNodes –Provides boolean value (true/False) computed across nodes- requires CredSSP (when using remote PowerShell) or Console session (RDP). Cluster –Provides boolean value from ECE store. Interacts with the orchestrator and acts to all the nodes in the cluster, requires deployment authorization (PREFIX-ECESG) and either CredSSP (when using remote PowerShell) or Console session (RDP).
  - **FeatureName** - <CredentialGuard | DriftControl | DRTM | HVCI | SideChannelMitigation | SMBEncryption | SMBSigning | VBS>
    - Credential Guard
    - Drift Control

- VBS (Virtualization Based Security)- We only support enable command.
- DRTM (Dynamic Root of Trust for Measurement)
- HVCI (Hypervisor Enforced if Code Integrity)
- Side Channel Mitigation
- SMB Encryption
- SMB Signing

Name	Feature	Supports drift control	Reboot required
Enable	Virtualization Based Security (VBS)	Yes	Yes
Enable Disable	Dynamic Root of Trust for Measurement (DRTM)	Yes	Yes
Enable Disable	Hypervisor-protected Code Integrity (HVCI)	Yes	Yes
Enable Disable	Side channel mitigation	Yes	Yes
Enable Disable	SMB signing	Yes	Yes
Enable Disable	SMB cluster encryption	No, cluster setting	No

## View the settings

With drift protection enabled, you can only modify non-protected security settings. To modify protected security settings that form the baseline, you must first disable drift protection. You can find and download the complete list of security settings at: [SecurityBaseline](#).

## Next steps

- [Understand BitLocker encryption](#)

# BitLocker encryption for Azure Stack HCI, version 23H2 (preview)

Article • 11/15/2023

Applies to: Azure Stack HCI, version 23H2 (preview)

This article describes the BitLocker encryption enabled on Azure Stack HCI and the procedure to retrieve your BitLocker keys if the system needs to be restored.

## Important

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

## About BitLocker encryption

On your Azure Stack HCI cluster, all the data-at-rest is encrypted via BitLocker XTS-AES 256-bit encryption. When you deploy your Azure Stack HCI cluster, you have the option to modify the associated security settings. By default, the data-at-rest encryption is enabled on your data volumes created during deployment. We recommend that you accept the default setting.

## Note

Cluster Shared Volumes created after deployment might need to be encrypted. Use the Powershell cmdlets to [Enable Bitlocker on newly created volumes](#).

Once Azure Stack HCI is successfully deployed, you can retrieve the BitLocker recovery keys. We recommend that you store the BitLocker keys in a secure location outside of the system. The recovery keys help you recover the local data if a system is restored from a backup image.

## Note

It is important that you save the BitLocker keys outside of the system. If the cluster is down and you don't have the key, it could potentially result in data loss.

# Manage BitLocker encryption

You can view, enable, and disable BitLocker encryption settings on your Azure Stack HCI cluster.

## PowerShell cmdlet properties for `AzureStackBitLockerAgent` module

The following cmdlet properties are for BitLocker module: *AzureStackBitLockerAgent*.

- `Get-ASBitLocker` - Scope <Local | PerNode | AllNodes | Cluster>
  - **Local** - Provides BitLocker volume details for the local node. Can be run in a regular remote PowerShell session.
  - **PerNode** - Provides BitLocker volume details per node. Requires CredSSP (when using remote PowerShell) or Console session (RDP).
- `Enable-ASBitLocker` - Scope <Local | Cluster> -VolumeType <BootVolume | ClusterSharedVolume>
- `Disable-ASBitLocker` - Scope <Local | Cluster> -VolumeType <BootVolume | ClusterSharedVolume>

## View BitLocker encryption settings

Use the following steps to view BitLocker encryption settings:

1. Connect to your Azure Stack HCI node.
2. Run the following PowerShell cmdlet using local administrator credentials:

```
PowerShell
```

```
Get-ASBitLocker
```

## Modify BitLocker encryption

Use the following steps to modify BitLocker encryption:

1. Connect to your Azure Stack HCI node.
2. Run the following PowerShell cmdlets using local administrator credentials:

**Enable BitLocker encryption:**

### Important

- Enabling BitLocker on volume type BootVolume requires TPM 2.0.
- While enabling BitLocker on volume type `ClusterSharedVolume` (CSV), the volume will be put in redirected mode and any workload VMs will be paused for a short time. This operation is disruptive; plan accordingly.

PowerShell

```
Enable-ASBitLocker
```

Disable BitLocker encryption:

PowerShell

```
Disable-ASBitLocker
```

## Get BitLocker recovery keys

Use the following steps to get the BitLocker recovery keys for your cluster.

1. Run PowerShell as Administrator on your Azure Stack HCI cluster.
2. Run the following command in PowerShell:

PowerShell

```
Get-AsRecoveryKeyInfo | ft ComputerName, PasswordID, RecoveryKey
```

Here is sample output:

Output

```
PS C:\Users\ashciuser> Get-AsRecoveryKeyInfo | ft ComputerName, PasswordID, RecoveryKey
```

ComputerName	PasswordId	RecoveryKey
-----	-----	-----
ASB88RR10U19	{Password1}	Key1
ASB88RR10U20	{Password2}	Key2
ASB88RR10U21	{Password3}	Key3
ASB88RR10U22	{Password4}	Key4

# Next steps

- [Assess deployment readiness via the Environment Checker.](#)

# Evaluate the deployment readiness of your environment for Azure Stack HCI, version 23H2 (preview)

Article • 11/17/2023

Applies to: Azure Stack HCI, version 23H2 (preview)

This article describes how to use the Azure Stack HCI Environment Checker in a standalone mode to assess how ready your environment is for deploying the Azure Stack HCI solution.

For a smooth deployment of the Azure Stack HCI solution, your IT environment must meet certain requirements for connectivity, hardware, networking, and Active Directory. The Azure Stack HCI Environment Checker is a readiness assessment tool that checks these minimum requirements and helps determine if your IT environment is deployment ready.

## Important

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

## About the Environment Checker tool

The Environment Checker tool runs a series of tests on each server in your Azure Stack HCI cluster, reports the result for each test, provides remediation guidance when available, and saves a log file and a detailed report file.

The Environment Checker tool consists of the following validators:

- **Connectivity validator.** Checks whether each server in the cluster meets the [connectivity requirements](#). For example, each server in the cluster has internet connection and can connect via HTTPS outbound traffic to well-known Azure endpoints through all firewalls and proxy servers.
- **Hardware validator.** Checks whether your hardware meets the [system requirements](#). For example, all the servers in the cluster have the same manufacturer and model.



- **Active Directory validator.** Checks whether the Active Directory preparation tool is run prior to running the deployment.
- **Network validator.** Validates your network infrastructure for valid IP ranges provided by customers for deployment. For example, it checks there are no active hosts on the network using the reserved IP range.
- **Arc integration validator.** Checks if the Azure Stack HCI cluster meets all the prerequisites for successful Arc onboarding.

## Why use Environment Checker?

You can run the Environment Checker to:

- Ensure that your Azure Stack HCI infrastructure is ready before deploying any future updates or upgrades.
- Identify the issues that could potentially block the deployment, such as not running a pre-deployment Active Directory script.
- Confirm that the minimum requirements are met.
- Identify and remediate small issues early and quickly, such as a misconfigured firewall URL or a wrong DNS.
- Identify and remediate discrepancies on your own and ensure that your current environment configuration complies with the [Azure Stack HCI system requirements](#).
- Collect diagnostic logs and get remote support to troubleshoot any validation issues.

## Environment Checker modes

You can run the Environment Checker in two modes:

- **Integrated tool:** The Environment Checker functionality is integrated into the deployment process. By default, all validators are run during deployment to perform pre-deployment readiness checks.
- **Standalone tool:** This light-weight PowerShell tool is available for free download from the Windows PowerShell gallery. You can run the standalone tool anytime, outside of the deployment process. For example, you can run it even before receiving the actual hardware to check if all the connectivity requirements are met.

This article describes how to run the Environment Checker in a standalone mode.

## Prerequisites

Before you begin, complete the following tasks:

- Review [Azure Stack HCI system requirements](#).
- Review [Firewall requirements for Azure Stack HCI](#).
- Make sure you have access to a client computer that is running on the network where you'll deploy the Azure Stack HCI cluster.
- Make sure that the client computer used is running PowerShell 5.1 or later.
- Make sure you have permission to verify the Active Directory preparation tool is run.

## Install Environment Checker

The [Environment Checker](#) works with PowerShell 5.1, which is built into Windows.

You can install the Environment Checker on a client computer, staging server, or Azure Stack HCI cluster node. However, if installed on an Azure Stack HCI cluster node, make sure to [uninstall](#) it before you begin the deployment to avoid any potential conflicts.

To install the Environment Checker, follow these steps:

1. Run PowerShell as administrator (5.1 or later). If you need to install PowerShell, see [Installing PowerShell on Windows](#).
2. Enter the following cmdlet to install the latest version of the PowerShellGet module:

PowerShell

```
Install-Module PowerShellGet -AllowClobber -Force
```

3. After the installation completes, close the PowerShell window and open a new PowerShell session as administrator.
4. In the new PowerShell session, register PowerShell gallery as a trusted repo:

PowerShell

```
Set-PSRepository -Name PSGallery -InstallationPolicy Trusted
```

5. Enter the following cmdlet to install the Environment Checker module:

PowerShell

```
Install-Module -Name AzStackHci.EnvironmentChecker -AllowPrerelease
```

6. If prompted, press **Y** (Yes) or **A** (Yes to All) to install the module.

## Run readiness checks

Each validator in the Environment Checker tool checks specific settings and requirements. You can run these validators by invoking their respective PowerShell cmdlet on each server in your Azure Stack HCI cluster or from any computer on the network where you'll deploy Azure Stack HCI.

You can run the validators from the following locations:

- Remotely via PowerShell session.
- Locally from a workstation or a staging server.
- Locally from the Azure Stack HCI cluster node. However, make sure to uninstall the Environment Checker before you begin the deployment to avoid any potential conflicts.

Select each of the following tabs to learn more about the corresponding validator.

### Connectivity

Use the connectivity validator to check if all the servers in your cluster have internet connectivity and meet the minimum connectivity requirements. For connectivity prerequisites, see [Firewall requirements for Azure Stack HCI](#).

You can use the connectivity validator to:

- Check the connectivity of your servers before receiving the actual hardware. You can run the connectivity validator from any client computer on the network where you'll deploy the Azure Stack HCI cluster.
- Check the connectivity of all the servers in your cluster after you've deployed the cluster. You can check the connectivity of each server by running the validator cmdlet locally on each server. Or, you can remotely connect from a staging server to check the connectivity of one or more servers.

## Run the connectivity validator

To run the connectivity validator, follow these steps.

1. Open PowerShell locally on the workstation, staging server, or Azure Stack HCI cluster node.
2. Run a connectivity validation by entering the following cmdlet:

PowerShell

```
Invoke-AzStackHciConnectivityValidation
```

#### ⓘ Note

Using the `Invoke-AzStackHciConnectivityValidation` cmdlet without any parameter checks connectivity for all the service endpoints that are enabled from your device. You can also pass parameters to run readiness checks for specific scenarios. See examples, below.

Here are some examples of running the connectivity validator cmdlet with parameters.

### Example 1: Check connectivity of a remote computer

In this example, you remotely connect from your workstation or a staging server to check the connectivity of one or more remote systems.

PowerShell

```
$session = New-PSSession -ComputerName remotesystem.contoso.com -  
Credential $credential  
Invoke-AzStackHciConnectivityValidation -PsSession $Session
```

### Example 2: Check connectivity for a specific service

You can check connectivity for a specific service endpoint by passing the `Service` parameter. In the following example, the validator checks connectivity for Azure Arc service endpoints.

PowerShell

```
Invoke-AzStackHciConnectivityValidation -Service Arc
```

### Example 3: Check connectivity if you're using a proxy

If you're using a proxy server, you can specify the connectivity validator to go through the specified proxy and credentials, as shown in the following example:

PowerShell

```
Invoke-AzStackHciConnectivityValidation -Proxy  
http://proxy.contoso.com:8080 -ProxyCredential $proxyCredential
```

#### ⓘ Note

The connectivity validator validates general proxy, it doesn't check if your Azure Stack HCI is configured correctly to use a proxy. For information about how to configure firewalls for Azure Stack HCI, see [Firewall requirements for Azure Stack HCI](#).

### Example 4: Check connectivity and create PowerShell output object

You can view the output of the connectivity checker as an object by using the `-PassThru` parameter:

PowerShell

```
Invoke-AzStackHciConnectivityValidation -PassThru
```

Here's a sample screenshot of the output:

```

PS C:\Users\Administrator> $result = Invoke-AzStackHciConnectivityValidation -PassThru
Log Location (contains PII): C:\Users\Administrator\.AzStackHci\AzStackHciEnvironmentChecker.log
Report Location (contains PII): C:\Users\Administrator\.AzStackHci\AzStackHciEnvironmentReport.json
Invoke-AzStackHciConnectivityValidation completed

PS C:\Users\Administrator> $result |ft name, status

```

Name	Status
AzStackHci_Connectivity_ARC_Notification_Service_Extensions	Succeeded
AzStackHci_Connectivity_ARC_Azure_Resource_Manager	Succeeded
AzStackHci_Connectivity_ARC_Azure_Active_Directory	Succeeded
AzStackHci_Connectivity_ARC_Guest_Config	Succeeded
AzStackHci_Connectivity_ARC_Metadata_Hybrid_Identity	Succeeded
AzStackHci_Connectivity_ARC_Windows_Package_Download	Succeeded
AzStackHci_Connectivity_ARC_Installation_Download_Script	Succeeded
AzStackHci_Connectivity_ARC_Server_Extensions	Succeeded
AzStackHci_Connectivity_ARC_Agent_Telemetry	Succeeded
AzStackHci_Connectivity_ARC_Notification_Service	Succeeded
AzStackHci_Connectivity_ARC_ResourceBridge_Identity_Service	Succeeded
AzStackHci_Connectivity_ARC_ResourceBridge_Container_Registry	Succeeded
AzStackHci_Connectivity_ARC_ResourceBridge_Configuration_Service	Succeeded
AzStackHci_Connectivity_ARC_ResourceBridge_Guest_Notification_Service	Succeeded
AzStackHci_Connectivity_ARC_ResourceBridge_Container_Image_Download	Succeeded
AzStackHci_Connectivity_ARC_ResourceBridge_K8Container_Image_Download	Succeeded
AzStackHci_Connectivity_CloudWitness_Quorum	Succeeded
AzStackHci_Connectivity_Defender_for_cloud	Succeeded
AzStackHci_Connectivity_Defender_for_endpoint_crl	Succeeded
AzStackHci_Connectivity_HCI_Update_Service	Succeeded
AzStackHci_Connectivity_Nuget	Succeeded
AzStackHci_Connectivity_HCI_Azure_Portal	Succeeded
AzStackHci_Connectivity_HCI_Microsoft_Office	Succeeded
AzStackHci_Connectivity_HCI_Kubernetes_Binaries	Succeeded
AzStackHci_Connectivity_HCI_Azure_Cli_Binaries	Succeeded
AzStackHci_Connectivity_HCI_Kubernetes_Images	Succeeded
AzStackHci_Connectivity_HCI_PSGallery	Succeeded
AzStackHci_Connectivity_HCI_Azure_Websites	Succeeded
AzStackHci_Connectivity_HCI_Cloud_Service	Succeeded
AzStackHci_Connectivity_HCI_Azure_Active_Directory	Succeeded
AzStackHci_Connectivity_Observability_Services_Watson	Succeeded
AzStackHci_Connectivity_Observability_Services_Remote_Support	Succeeded
AzStackHci_Connectivity_Observability_Services_Geneva	Succeeded
AzStackHci_Connectivity_Test_Dns	Succeeded
AzStackHci_Connectivity_Collect_Proxy_Diagnostics_winHttp	Succeeded
AzStackHci_Connectivity_Collect_Proxy_Diagnostics_Environment	Succeeded
AzStackHci_Connectivity_Collect_Proxy_Diagnostics_IEProxy	Succeeded

## Connectivity validator attributes

You can filter any of the following attributes and display the connectivity validator result in your desired format:

Attribute name	Description
EndPoint	The endpoint being validated.
Protocol	Protocol used – example https.
Service	The service endpoint being validated.
Operation Type	Type of operation – deployment, update.
Group	Readiness Checks.
System	For internal use.
Name	Name of the individual service.
Title	Service title; user facing name.
Severity	Critical, Warning, Informational, Hidden.
Description	Description of the service name.

Attribute name	Description
Tags	Internal Key-value pairs to group or filter tests.
Status	Succeeded, Failed, In Progress.
Remediation	URL link to documentation for remediation.
TargetResourceID	Unique identifier for the affected resource (node or drive).
TargetResourceName	Name of the affected resource.
TargetResourceType	Type of the affected resource.
Timestamp	The time in which the test was called.
AdditionalData	Property bag of key value pairs for additional information.
HealthCheckSource	The name of the services called for the health check.

## Connectivity validator output

The following samples are the output from successful and unsuccessful runs of the connectivity validator.

To learn more about different sections in the readiness check report, see [Understand readiness check report](#).

### Sample output: Successful test

The following sample output is from a successful run of the connectivity validator. The output indicates a healthy connection to all the endpoints, including well-known Azure services and observability services. Under **Diagnostics**, you can see the validator checks if a DNS server is present and healthy. It collects WinHttp, IE proxy, and environment variable proxy settings for diagnostics and data collection. It also checks if a transparent proxy is used in the outbound path and displays the output.



```
HCi:
> Healthy Microsoft Update Microsoft Update Microsoft Update
> Healthy Nuget Nuget Nuget command line tool
> Healthy Azure Portal Azure portal URL for proxy bypass (https) Azure portal URL for proxy bypass (https)
> Healthy Microsoft Office Microsoft Office Microsoft Office
> Healthy Kubernetes Kubernetes binaries Cloud init service to download Kubernetes binaries
> Healthy Azure CLI Azure CLI Download Windows Admin Center to download Azure CLI
> Healthy Kubernetes Kubernetes Images Kubernetes service to download container images
> Healthy Microsoft Update PowerShell Gallery PowerShell Gallery central repository
> Healthy Azure Websites Azure Websites Web-hosting platform that supports multiple technologies
> Healthy Cloud Service Azure Stack HCI Cloud Service Azure Stack HCI Cloud Service
> Healthy Azure Active Directory Azure Active Directory Azure Active Directory

Observability:
> Healthy Azure Endpoint Observability Services - Watson Observability Services - Watson
> Healthy Azure Endpoint Observability Services - Remote Support Observability Services - Remote Support
> Healthy Azure Endpoint Observability Services - Geneva Observability Services - Geneva Control Plane and Ingestion

Diagnostics:
> DNS - Test DNS Test DNS Resolution
> V-DW -> 127.0.0.1
> Proxy_Setting - WinHttp Proxy Settings Collects proxy configuration for WinHttp
> V-DW -> <Not configured>
> Proxy_Setting - Environment Proxy Settings Collects proxy configuration from environment variables
> V-DW_https_proxy_process -> <Not configured>
> V-DW_https_proxy_process -> <Not configured>
> V-DW_https_proxy_user -> <Not configured>
> V-DW_https_proxy_machine -> <Not configured>
> Proxy_Setting - IE Proxy Settings Collects Proxy configuration from IE
> V-DW -> <Not configured>
> Root CA - System Check - SSL Inspection Detection Well known endpoint for Root CA thumbprint validation
> V-DW -> https://login.microsoftonline.com

Summary
The following is summary of the unique issues found, these issues should be reviewed prior to continuing. Critical issues require remediation and are blocking issues. Warning issues are sub-optimal non-blocking issues. Informational issues are for your information.
> 55 successes

Remediation:
Summary
> 55 / 55 (100%) resources test successfully.

Log Location (contains PII): C:\Users\Administrator\.AzStackHci\AzStackHciEnvironmentChecker.log
Report Location (contains PII): C:\Users\Administrator\.AzStackHci\AzStackHciEnvironmentReport.json
Invoke-AzStackHciConnectivityValidation completed
```

## Sample output: Failed test

If a test fails, the connectivity validator returns information to help you resolve the issue, as shown in the sample output below. The **Needs Remediation** section displays the issue that caused the failure. The **Remediation** section lists the relevant article to help remediate the issue.

```
ARC:
> Needs Remediation Azure Endpoint - Guest Configuration Extension and guest configuration services
> V-Host1 -> https://login.microsoftonline.com
> V-Host1 -> https://doesnotexist.guestconfiguration.azure.com
> Help URL: https://docs.microsoft.com/en-us/azure/azure-arc/servers/network-requirements#urls

> Healthy Azure Endpoint ARC Notification Service Notification service for extensions
> Healthy Azure Endpoint Azure Resource Manager Azure Resource Manager
> Healthy Azure Endpoint Guest Notification service Guest Notification service
> Healthy Azure Endpoint Metadata and Hybrid Identity Metadata and hybrid identity services
> Healthy Azure Endpoint Windows installation package download Windows installation package download
> Healthy Azure Endpoint Installation Download Script Installation Download Script
> Healthy Azure Endpoint Azure Arc-enabled Servers Extensions Download source for Azure Arc-enabled servers extensions
> Healthy Azure Endpoint Agent telemetry Agent telemetry
> Healthy Azure Endpoint Guest Notification service Guest Notification service
> Healthy Azure Endpoint Azure Arc Identity service Azure Arc Identity service
> Healthy Azure Endpoint Microsoft Container Registry Microsoft Container Registry
> Healthy Azure Endpoint Azure Arc Configuration Service Azure Arc configuration service
> Healthy Azure Endpoint Guest Notification service Guest Notification service
> Healthy Kubernetes Resource bridge container image download Resource bridge container image download
> Healthy Kubernetes Azure Arc for K8s container image download Azure Arc for K8s container image download

ARM:
> Healthy Azure Endpoint Azure Resource Manager Azure Resource Manager

CloudWitness:
> Healthy Azure Endpoint Cloud Witness for a Failover Cluster Cloud Witness for a Failover Cluster

Defender:
> Healthy Azure Endpoint Microsoft Defender for Cloud Microsoft Defender for Cloud
> Healthy Azure Endpoint Microsoft Defender for Endpoint Certificate Revocation List Microsoft Defender for Endpoint Certificate Revocation List

HCi:
> Healthy Microsoft Update Microsoft Update Microsoft Update
> Healthy Nuget Nuget Nuget command line tool
> Healthy Azure Portal Azure portal URL for proxy bypass (https) Azure portal URL for proxy bypass (https)
> Healthy Microsoft Office Microsoft Office Microsoft Office
> Healthy Kubernetes Kubernetes binaries Cloud init service to download Kubernetes binaries
> Healthy Azure CLI Azure CLI Download Windows Admin Center to download Azure CLI
> Healthy Kubernetes Kubernetes Images Kubernetes service to download container images
> Healthy Microsoft Update PowerShell Gallery PowerShell Gallery central repository
> Healthy Azure Websites Azure Websites Web-hosting platform that supports multiple technologies
> Healthy Cloud Service Azure Stack HCI Cloud Service Azure Stack HCI Cloud Service
> Healthy Azure Active Directory Azure Active Directory Azure Active Directory

Observability:
> Healthy Azure Endpoint Observability Services - Watson Observability Services - Watson
> Healthy Azure Endpoint Observability Services - Remote Support Observability Services - Remote Support
> Healthy Azure Endpoint Observability Services - Geneva Observability Services - Geneva Control Plane and Ingestion

Diagnostics:
> DNS - Test DNS Test DNS Resolution
> V-HOST1 -> 192.168.200.222
> Proxy_Setting - WinHttp Proxy Settings Collects proxy configuration for WinHttp
> V-HOST1 -> <Not configured>
> Proxy_Setting - Environment Proxy Settings Collects proxy configuration from environment variables
> V-HOST1_https_proxy_process -> <Not configured>
> V-HOST1_https_proxy_process -> <Not configured>
> V-HOST1_https_proxy_user -> <Not configured>
> V-HOST1_https_proxy_user -> <Not configured>
> V-HOST1_https_proxy_machine -> <Not configured>
> V-HOST1_https_proxy_machine -> <Not configured>
> Proxy_Setting - IE Proxy Settings Collects Proxy configuration from IE
> V-HOST1 -> (Enabled)
> Root CA - System Check - SSL Inspection Detection Well known endpoint for Root CA thumbprint validation
> 192.168.200.128 -> https://login.microsoftonline.com

Summary
The following is summary of the unique issues found, these issues should be reviewed prior to continuing. Critical issues require remediation and are blocking issues. Warning issues are sub-optimal non-blocking issues. Informational issues are for your information.
> 1 Critical Issue(s)
> 55 successes

Needs Remediation
> V-Host1->https://doesnotexist.guestconfiguration.azure.com

Remediation:
> https://docs.microsoft.com/en-us/azure/azure-arc/servers/network-requirements#urls

Failed Urls log: C:\Users\Administrator\.AzStackHci\FailedUrls.txt

Log Location (contains PII): C:\Users\Administrator\.AzStackHci\AzStackHciEnvironmentChecker.log
Report Location (contains PII): C:\Users\Administrator\.AzStackHci\AzStackHciEnvironmentReport.json
Invoke-AzStackHciConnectivityValidation completed
```

## Potential failure scenario for connectivity validator



The connectivity validator checks for SSL inspection before testing connectivity of any required endpoints. If SSL inspection is turned on in your Azure Stack HCI system, you get the following error:

```
Invoke-AzStackHciConnectivityValidation v1.2100.2166.62 started.

Unable to continue a diagnostic collection found an unrecoverable error. Message: Expected at least 1 chain certificate subjects to match O=DigiCert or O=Microsoft. 0 matched. Actual subjects CN=tlslsinspection, OU=azs, O=msft, L=wookingham, S=bk, C=gb. SSL decryption and re-encryption detected.. Expected at least 1 chain certificate subjects to match O=DigiCert or O=Microsoft. 0 matched. Actual subjects CN=tlslsinspection, OU=azs, O=msft, L=wookingham, S=bk, C=gb. SSL decryption and re-encryption detected.. Result Object:

EndPoint      : {login.microsoftonline.com, portal.azure.com}
Protocol       : {https}
Service       : 
OperationType  : 
Group         : 
Mandatory     : True
System        : False
Name          : System_Check_SSL_Inspection_Detection
Title         : System Check - SSL Inspection Detection
Severity      : Critical
Description    : Well known endpoint for Root CA thumbprint validation
Tags          : @{Group=System.Object[]; Service=System.Object[]; ExpectedSubject=System.Object[]; Mandatory=True}
Status        : Failed
Remediation    : https://aka.ms/hci-connect-chk
TargetResourceID : login.microsoftonline.com_portal.azure.com
TargetResourceName : login.microsoftonline.com_portal.azure.com
TargetResourceType : External Endpoint
Timestamp     : 08/12/2022 19:16:31
AdditionalData  : @{Detail=Expected at least 1 chain certificate subjects to match O=DigiCert or O=Microsoft. 0 matched. Actual subjects CN=tlslsinspection, OU=azs, O=msft, L=wookingham, S=bk, C=gb. SSL decryption and re-encryption detected.; Status=Failed; TimeStamp=08/12/2022 19:16:29; Resource=https://login.microsoftonline.com; Source=LAPTOP-BFEENPAC}, @{Detail=Expected at least 1 chain certificate subjects to match O=DigiCert or O=Microsoft. 0 matched. Actual subjects CN=tlslsinspection, OU=azs, O=msft, L=wookingham, S=bk, C=gb. SSL decryption and re-encryption detected.; Status=Failed; TimeStamp=08/12/2022 19:16:31; Resource=https://portal.azure.com; Source=LAPTOP-BFEENPAC}}
HealthCheckSource : Import-AzStackHciConnectivityTarget\Get-AzStackHciConnectivityTarget\Invoke-AzStackHciConnectivityValidation
                  \<ScriptBlock>
```

## Workaround

Work with your network team to turn off SSL inspection for your Azure Stack HCI system. To confirm your SSL inspection is turned off, you can use the following examples. After SSL inspection is turned off, you can run the tool again to check connectivity to all the endpoints.

If you receive the certificate validation error message, run the following commands individually for each endpoint to manually check the certificate information:

PowerShell

```
C:\> Import-Module AzStackHci.EnvironmentChecker
C:\> Get-SigningRootChain -Uri <Endpoint-URI> | ft subject
```

For example, if you want to verify the certificate information for two endpoints, say `https://login.microsoftonline.com` and `https://portal.azure.com`, run the following commands individually for each endpoint:

- For `https://login.microsoftonline.com`:

PowerShell

```
C:\> Import-Module AzStackHci.EnvironmentChecker
C:\> Get-SigningRootChain -Uri https://login.microsoftonline.com |
```

```
ft subject
```

Here's a sample output:

```
PowerShell
```

```
Subject
```

```
-----
```

```
CN=portal.office.com, O=Microsoft Corporation, L=Redmond, S=WA, C=US
CN=Microsoft Azure TLS Issuing CA 02, O=Microsoft Corporation, C=US
CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US
```

- For `https://portal.azure.com`:

```
PowerShell
```

```
C:\> Import-Module AzStackHci.EnvironmentChecker
C:\> Get-SigningRootChain -Uri https://portal.azure.com | ft
Subject
```

Here's a sample output:

```
PowerShell
```

```
Subject
```

```
-----
```

```
CN=portal.azure.com, O=Microsoft Corporation, L=Redmond, S=WA, C=US
CN=Microsoft Azure TLS Issuing CA 01, O=Microsoft Corporation, C=US
CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US
```

## Understand readiness check report

Each validator generates a readiness check report after completing the check. Make sure to review the report and correct any issues before starting the actual deployment.

The information displayed on each readiness check report varies depending on the checks the validators perform. The following table summarizes the different sections in the readiness check reports for each validator:

Section	Description	Available in
Services	Displays the health status of each service endpoint that the connectivity validator checks. Any service endpoint that fails the check is highlighted with the <b>Needs Remediation</b> tag.	Connectivity validator report
Diagnostics	Displays the result of the diagnostic tests. For example, the health and availability of a DNS server. It also shows what information the validator collects for diagnostic purposes, such as WinHttp, IE proxy, and environment variable proxy settings.	Connectivity validator report
Hardware	Displays the health status of all the physical servers and their hardware components. For information on the tests performed on each hardware, see the table under the "Hardware" tab in the <a href="#">Run readiness checks</a> section.	Hardware validator report
AD OU Diagnostics	Displays the result of the Active Directory organization unit test. Displays if the specified organizational unit exists and contains proper sub-organizational units.	Active Directory validator report
Network range test	Displays the result of the network range test. If the test fails, it displays the IP addresses that belong to the reserved IP range.	Network validator report
Summary	Lists the count of successful and failed tests. Failed test results are expanded to show the failure details under <b>Needs Remediation</b> .	All reports
Remediation	Displays only if a test fails. Provides a link to the article that provides guidance on how to remediate the issue.	All reports
Log location (contains PII)	<p>Provides the path where the log file is saved. The default path is:</p> <ul style="list-style-type: none"> <li>- <code>\$HOME\.AzStackHci\AzStackHciEnvironmentChecker.log</code> when you run the Environment Checker in a standalone mode.</li> <li>- <code>C:\CloudDeployment\Logs</code> when the Environment Checker is run as part of the deployment process.</li> </ul> <p>Each run of the validator overwrites the existing file.</p>	All reports
Report Location (contains PII)	<p>Provides the path where the completed readiness check report is saved in the JSON format. The default path is:</p> <ul style="list-style-type: none"> <li>- <code>\$HOME\.AzStackHci\AzStackHciEnvironmentReport.json</code> when you run the Environment Checker in a standalone mode.</li> <li>- <code>C:\CloudDeployment\Logs</code> when the Environment Checker is run as part of the deployment process.</li> </ul> <p>The report provides detailed diagnostics that are collected during each test. This information can be helpful for system integrators</p>	All reports

Section	Description	Available in
	or when you need to contact the support team to troubleshoot the issue. Each run of the validator overwrites the existing file.	
Completion message	At the end of the report, displays a message that the validation check is completed.	All reports

## Environment Checker results

### ⓘ Note

The results reported by the Environment Checker tool reflect the status of your settings only at the time that you ran it. If you make changes later, for example to your Active Directory or network settings, items that passed successfully earlier can become critical issues.

For each test, the validator provides a summary of the unique issues and classifies them into: success, critical issues, warning issues, and informational issues. Critical issues are the blocking issues that you must fix before proceeding with the deployment.

## Uninstall environment checker

The environment checker is shipped with Azure Stack HCI, make sure to uninstall it from all Azure Stack HCI cluster nodes before you begin the deployment to avoid any potential conflicts.

PowerShell

```
Remove-Module AzStackHci.EnvironmentChecker -Force
Get-Module AzStackHci.EnvironmentChecker -ListAvailable | Where-Object
{$_.Path -like "*$($_.Version)*"} | Uninstall-Module -force
```

## Troubleshoot environment validation issues

For information about how to get support from Microsoft to troubleshoot any validation issues that may arise during cluster deployment or pre-registration, see [Troubleshoot environment validation issues](#).

## Next steps

- [Review the deployment checklist.](#)
- [Contact Microsoft Support.](#)

# Azure Stack HCI deployment overview (preview)


Article • 05/31/2023

Applies to: Azure Stack HCI, Supplemental Package

This article is the first in the series of deployment articles that describe how to deploy Azure Stack HCI using a new deployment tool and methods.

You can deploy Azure Stack HCI using a new or existing *config* file interactively or via PowerShell.

## Important

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

## About deployment methods

You can deploy Azure Stack HCI using one of the following methods:

- **Interactive:** Deploy using a new config file interactively. The interactive flow provides a guided, step-by-step experience that helps you create a new configuration file which is then used to deploy and register the cluster. This method should be used when you deploy for the first time and is recommended for most customers.
- **Existing configuration:** Deploy using this option if you already have a configuration file from a prior deployment. This option is recommended when deploying multiple systems.
- **PowerShell:** Deploy using this option if you already have a configuration file. This option is recommended for the partners and when deploying systems at-scale.

## Deployment sequence

Follow this process sequence to deploy Azure Stack HCI in your environment:

- Select one of the [validated network topologies](#) to deploy.
- Read the [prerequisites](#) for Azure Stack HCI.
- Follow the [deployment checklist](#).
- Prepare your [Active Directory](#) environment.
- [Install the English version of Azure Stack HCI, version 22H2](#) on each server.
- Install and run the deployment tool interactively with a [new configuration file](#) or using an [existing configuration file](#).
- If preferred, you can [deploy using PowerShell](#).
- After deployment, [validate deployment](#).
- If needed, [troubleshoot deployment](#).

## Validated network topologies

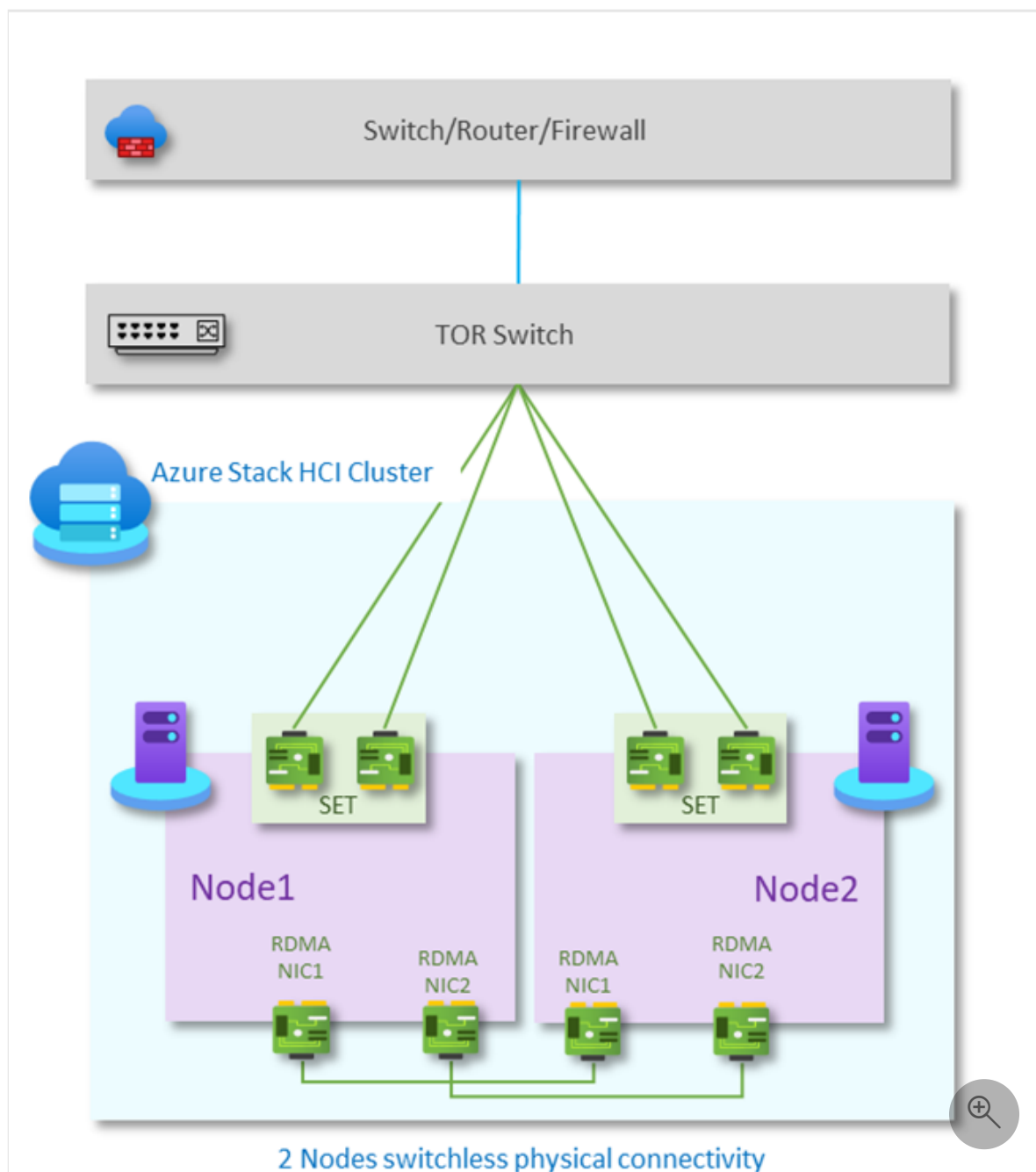
### Important

We recommend that you use one of the validated network topologies for optimum results.

The following network topologies were tested and validated for this release:

- A single physical server connected to a network switch. This is sometimes referred to as a single-node cluster.
- Two physical servers with direct (switchless) storage network connections to an L2 switch.

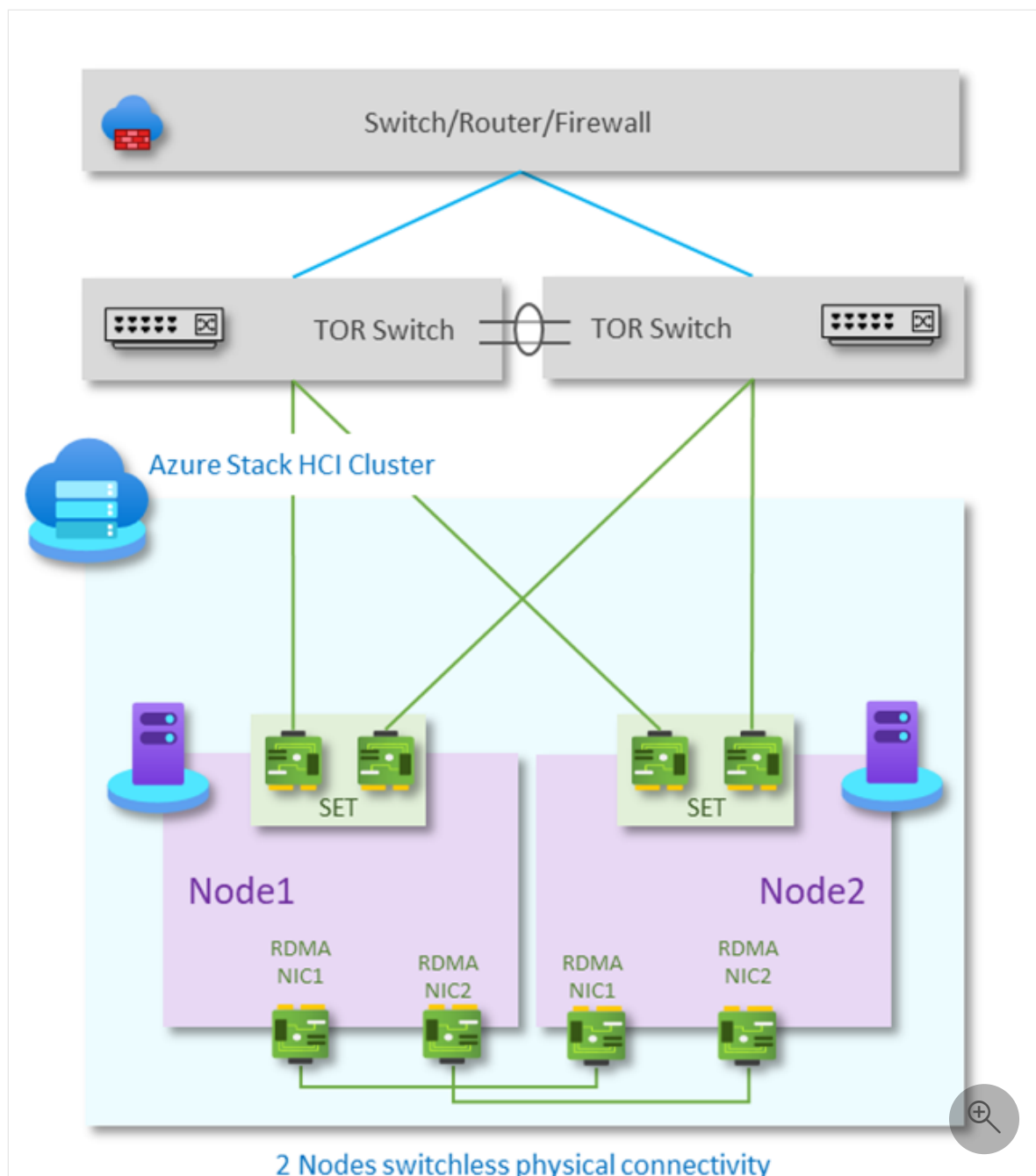
**Configuration 1:** The following diagram shows two physical servers with a directly connected (switchless) storage network and a single TOR switch.



- Two physical servers with direct (switchless) storage network connections to redundant L3 switches.

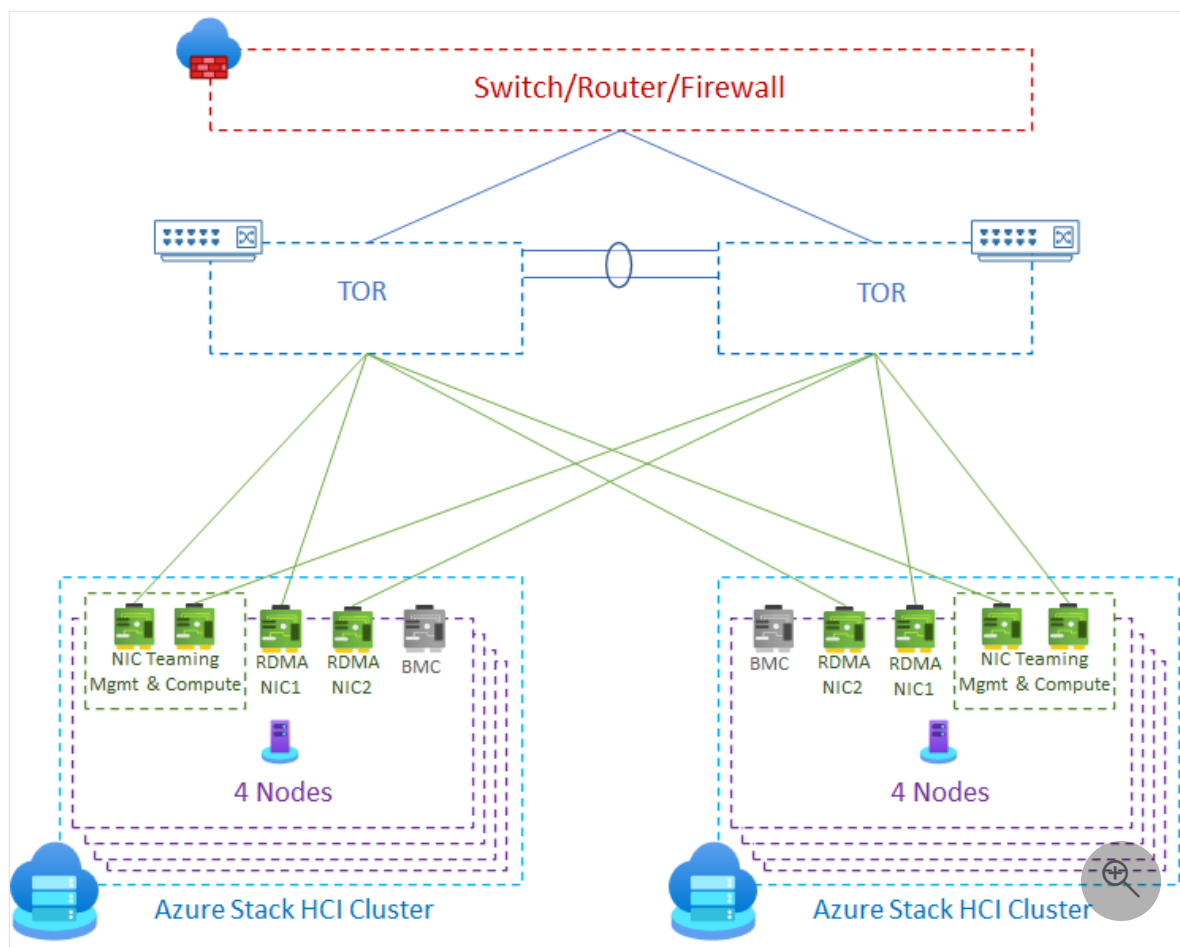
**Configuration 2:** The following diagram shows two physical servers with a directly connected (switchless) storage network and redundant TOR switches.





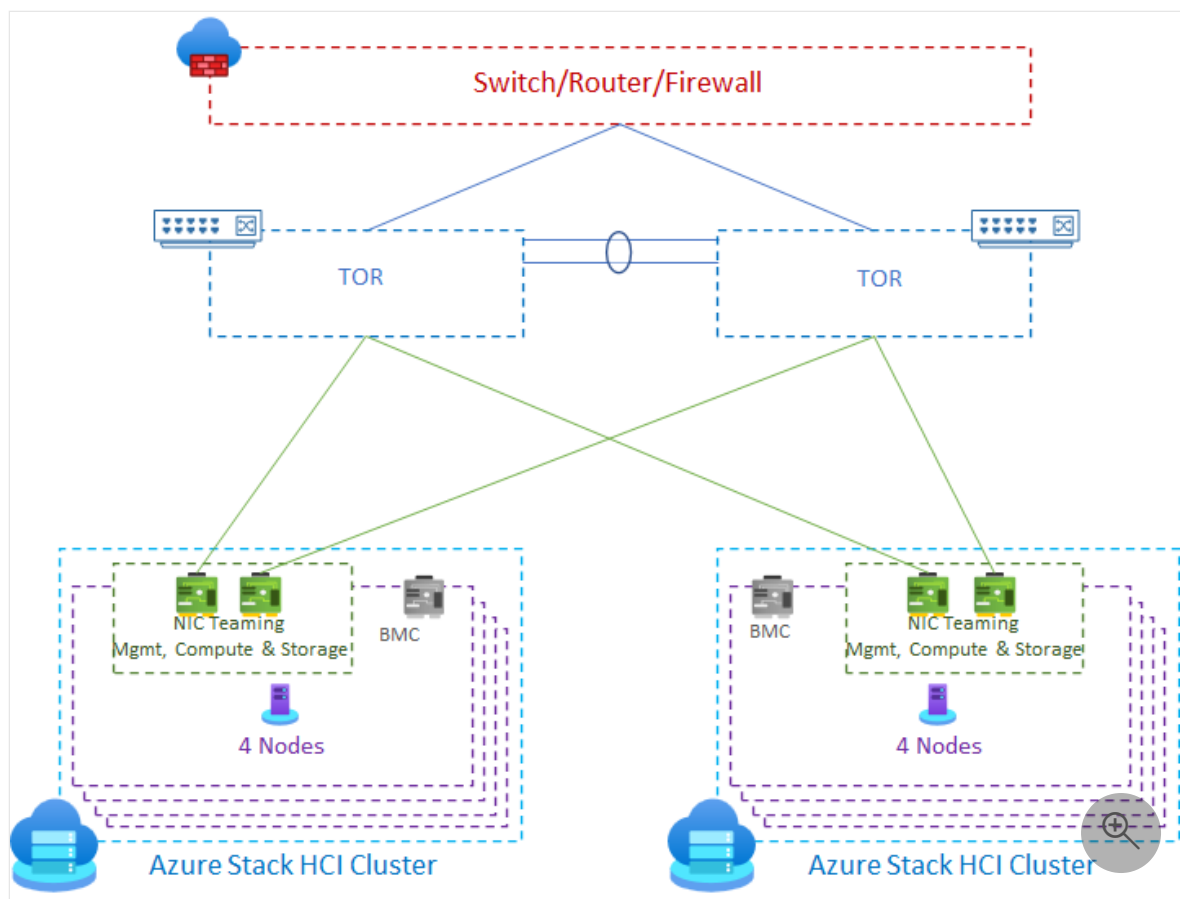
- Four physical servers with storage network connections to an L2-switch.

**Configuration 3:** The following diagram shows four physical servers using a non converged network and with storage network connections to L2 switches.



- Four physical servers deployed using a fully-converged network for compute, storage, and management and with redundant TOR switches.

**Configuration 4:** The following diagram shows four physical servers using a fully converged network (for compute, management, and storage) and with storage network connections to redundant L3 switches.



## Next steps

- Read the [prerequisites](#) for Azure Stack HCI.


# Review deployment prerequisites for Azure Stack HCI (preview)

Article • 05/31/2023

Applies to: Azure Stack HCI, Supplemental Package

This article discusses the security, software, hardware, and networking prerequisites in order to deploy Azure Stack HCI.

## Important

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

## Security considerations

Review the [security considerations](#) for Azure Stack HCI and [assess environment readiness](#) by using the Environment Checker. If you plan to use the standalone version of the Environment Checker on an Azure Stack HCI cluster node, make sure to uninstall it before running the Deployment Tool. This will help you avoid any potential conflicts that could arise during the deployment process.

## Software requirements

The Supplemental Package supports only the English version of the Azure Stack HCI operating system. Therefore, you must install Azure Stack HCI, version 22H2 operating system in English using the instructions in [Deploy Azure Stack HCI, version 22H2 OS](#).

## Hardware requirements

Before you begin, make sure that the physical hardware used to deploy the solution meets the following requirements:

Component	Minimum
-----------	---------

Component	Minimum
CPU	A 64-bit Intel Nehalem grade or AMD EPYC or later compatible processor with second-level address translation (SLAT).
Memory	A minimum of 32 GB RAM.
Host network adapters	At least two network adapters listed in the Windows Server Catalog. Or dedicated network adapters per intent, which does require two separate adapters for storage intent. For more information, see <a href="#">Windows Server Catalog</a> .
BIOS	Intel VT or AMD-V must be turned on.
Boot drive	A minimum size of 200 GB size.
Data drives	At least 3 disks with a minimum capacity of 500 GB (SSD or HDD).
TPM	TPM 2.0 hardware must be present and turned on.
Secure boot	Secure Boot must be present and turned on.

## Network requirements

Before you begin, make sure that the physical network and the host network where the solution is deployed meet the requirements described in:

- [Physical network requirements](#)
- [Host network requirements](#)

## Next steps

- Review the [deployment checklist](#).


# Get the deployment checklist for Azure Stack HCI (preview)

Article • 04/18/2023

Applies to: Azure Stack HCI, Supplemental Package

Use the following checklist to gather the required information ahead of the actual deployment of your Azure Stack HCI cluster.

## Important

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

## Deployment checklist

Component	What is needed
Server names	Unique name for each server you wish to deploy.
Active Directory Cluster name	The name for the new cluster AD object during the <a href="#">Active Directory preparation</a> . This name is also used for the name of the cluster during deployment.
Active Directory Object prefix	The prefix used for all AD objects created for the Azure Stack HCI deployment. The prefix is used during the <a href="#">Active Directory preparation</a> . The prefix must not exceed 8 characters.
Active directory OU	A new organizational unit (OU) to store all the objects for the Azure Stack HCI deployment. The OU is created during the <a href="#">Active Directory preparation</a> .
Active Directory FQDN	Fully-qualified domain name (FQDN) for the Active Directory domain.

Component	What is needed
Active Directory lifecycle manager (LCM) credential	<p>A new username and password that is created with the appropriate permissions for deployment. This account is the same as the user account used by the Azure Stack HCI 22H2 deployment tool.</p> <p>The password must conform to the length and complexity requirements. Use a password that is at least eight characters long. The password must also contain three out of the four requirements: a lowercase character, an uppercase character, a numeral, and a special character.</p> <p>For more information, see <a href="#">password complexity requirements</a>.</p> <p>The name must be unique for each deployment and you can't use <i>admin</i> as the username.</p>
IPv4 network range subnet for management network intent	<p>A subnet used for management network intent. You need an address range for management network with a minimum of 6 available, contiguous IPs in this subnet. These IPs are used for infrastructure services with the first IP assigned to fail over clustering.</p> <p>For more information, see the <b>Provide management network details</b> page in <a href="#">Deploy interactively using a config file</a>.</p>
Storage VLAN ID	<p>Two unique VLAN IDs to be used for the storage networks, from your IT network administrator.</p> <p>We recommend using the default VLANs from Network ATC for storage subnets. If you plan to have two storage subnets, Network ATC will use VLANs from 712 and 711 subnets.</p> <p>For more information, see the <b>Provide storage network details</b> page in <a href="#">Deploy interactively using a config file</a>.</p>
DNS Server	<p>A DNS Server that is used in your environment. The DNS server used must resolve the Active Directory Domain.</p> <p>For more information, see the <b>Provide management network details</b> page in <a href="#">Deploy interactively using a config file</a>.</p>
Azure subscription ID	<p>ID for the Azure subscription used to register the cluster. Make sure that you are a user access administrator on this subscription. This will allow you to manage access to Azure resources, specifically to Arc-enable each server of an Azure Stack HCI cluster.</p>
Azure Storage account	<p>For two-node clusters, a witness is required. For a cloud witness, an <a href="#">Azure Storage account</a> is needed. For more information, see <b>Step 3: Cluster</b> in <a href="#">Deploy interactively using a config file</a>.</p>
Access key for Azure Storage account	<p>To setup a cloud witness, the <a href="#">Access key</a> for the Azure Storage account is needed. For more information, see <b>Step 3: Cluster</b> in <a href="#">Deploy interactively using a config file</a>.</p>
Azure blob service domain	<p>The domain name for the Azure blob service is needed if you choose to use a custom domain when setting up a cloud witness. For more information, see <b>Step 3: Cluster</b> in <a href="#">Deploy interactively using a config file</a>.</p>

Component	What is needed
File share path	For two-node clusters, a witness is required. For a file share witness, the file share path for the witness is needed. For more information, see <b>Step 3: Cluster</b> in <a href="#">Deploy interactively using a config file</a> .
Outbound connectivity	Run the <a href="#">Environment checker</a> to ensure that your environment meets the outbound network connectivity requirements for firewall rules.

## Next steps

- Prepare your [Active Directory](#) environment.



# Prepare Active Directory for new Azure Stack HCI deployment (preview)

Article • 07/14/2023

Applies to: Azure Stack HCI, Supplemental Package

This article describes how to prepare your Active Directory (AD) environment before you deploy Azure Stack HCI. To enable the security model, each component agent on Azure Stack HCI uses a dedicated Group Managed Service Account (gMSA). For an overview of gMSA, see [Group Manager Service Accounts](#).

## Important

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

## Prerequisites

Before you begin, make sure you've done the following:

- Satisfy the [prerequisites](#) for new deployments of Azure Stack HCI.
- Complete the [deployment checklist](#).
- Install the PowerShell module to prepare Active Directory. [Download the module from the PowerShell Gallery](#) and run the following command:

Azure PowerShell

```
Install-Module AsHciADArtifactsPreCreationTool -Repository PSGallery
```

You can also copy the module from the `C:\CloudDeployment\Prepare` folder on your first (staging) server and then import the module. Run this command from the folder where the module is located:

Azure PowerShell

```
Import-Module .\AsHciADArtifactsPreCreationTool.psm1
```

- Obtain domain administrator access to the Active Directory domain server.
- (Only if you deploy Azure Stack HCI via PowerShell) Create a Service Principal with the necessary permissions for Azure Stack HCI registration. For more information, see:
  - [Create an Azure AD app and service principal in the portal.](#)
  - [Assign Azure permissions from the Azure portal.](#)

## Active Directory preparation module

The *AsHciADArtifactsPreCreationTool.ps1* module is used to prepare Active Directory. Here are the required parameters associated with the cmdlet:

Parameter	Description
- <code>AzureStackLCMUserCredential</code>	<p>A new user object that is created with the appropriate permissions for deployment. This account is the same as the user account used by the Azure Stack HCI 22H2 deployment tool.</p> <p>Make sure that only the username is provided. The name should not include the domain name, for example, <code>contoso\username</code>.</p> <p>The password must conform to the length and complexity requirements. Use a password that is at least eight characters long. The password must also contain three out of the four requirements: a lowercase character, an uppercase character, a numeral, and a special character.</p> <p>For more information, see <a href="#">password complexity requirements</a>.</p> <p>The name must be unique for each deployment and you can't use <i>admin</i> as the username.</p>
<code>-AsHciOUName</code>	<p>A new Organizational Unit (OU) to store all the objects for the Azure Stack HCI deployment. Existing group policies and inheritance are blocked in this OU to ensure there's no conflict of settings. The OU must be specified as the distinguished name (DN). For more information, see the format of <a href="#">Distinguished Names</a>.</p>
<code>-AsHciPhysicalNodeList</code>	<p>A list of computer names that are created for the physical cluster servers.</p>
<code>-DomainFQDN</code>	<p>Fully qualified domain name (FQDN) of the Active Directory domain.</p>
<code>-AsHciClusterName</code>	<p>The name for the new cluster AD object.</p>
<code>-AsHciDeploymentPrefix</code>	<p>The prefix used for all AD objects created for the Azure Stack HCI deployment.</p> <p>The prefix must not exceed 8 characters.</p>

Parameter	Description
<code>-Deploy</code>	Select this scenario for a brand new deployment instead of an upgrade of an existing system.

## Prepare Active Directory

When you prepare Active Directory, you create a dedicated Organizational Unit (OU) to place all the Azure Stack HCI related objects such as computer accounts, gMSA accounts, and user groups.

### ⓘ Note

In this release, only the Active Directory prepared via the provided module is supported.

To prepare and configure Active Directory, follow these steps:

1. Sign in to a computer that is joined to your Active Directory domain as a domain administrator.
2. Run PowerShell as administrator.
3. Create a [Microsoft Key Distribution Service root key](#) on the domain controller to generate group [Managed Service Account](#) passwords. Run the following command.

PowerShell

```
Add-KdsRootKey -EffectiveTime ((Get-Date).addhours(-10))
```

Here's the sample output from a successful run of the command:

```
PS C:\Users\Administrator> Add-KdsRootKey -EffectiveTime ((Get-Date).addhours(-10))
```

Guid

----

```
706e1dd7-3601-4f01-f2de-bb04c7b9afc3
```

4. Run the following command to create the dedicated OU.

## PowerShell

```
New-HciAdObjectsPreCreation -Deploy -AzureStackLCMUserCredential (Get-Credential) -AsHciOUName "<OU name or distinguished name including the domain components>" -AsHciPhysicalNodeList @("<Server name>") -DomainFQDN "<FQDN for the Active Directory domain>" -AsHciClusterName "<Cluster name for deployment>" -AsHciDeploymentPrefix "<Deployment prefix>"
```

5. When prompted, provide the username and password for the deployment.
  - a. Make sure that only the username is provided. The name should not include the domain name, for example, `contoso\username`.
  - b. Make sure that the password meets complexity and length requirements. For more information, see [password complexity requirements](#).

Here is a sample output from a successful completion of the script:

```
PS C:\temp> New-HciAdObjectsPreCreation -Deploy -AsHciDeploymentUserCredential (get-credential) -AsHciOUName "OU=oudocs,DC=ASZ1PLab,DC=nttest,DC=microsoft,DC=com" -AsHciPhysicalNodeList @("a6p15140005012", "a4p1074000603b") -DomainFQDN "ASZ1PLab.nttest.microsoft.com" -AsHciClusterName "docspro2cluster" -AsHciDeploymentPrefix "docspro2"
```

```
cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
Credential
```

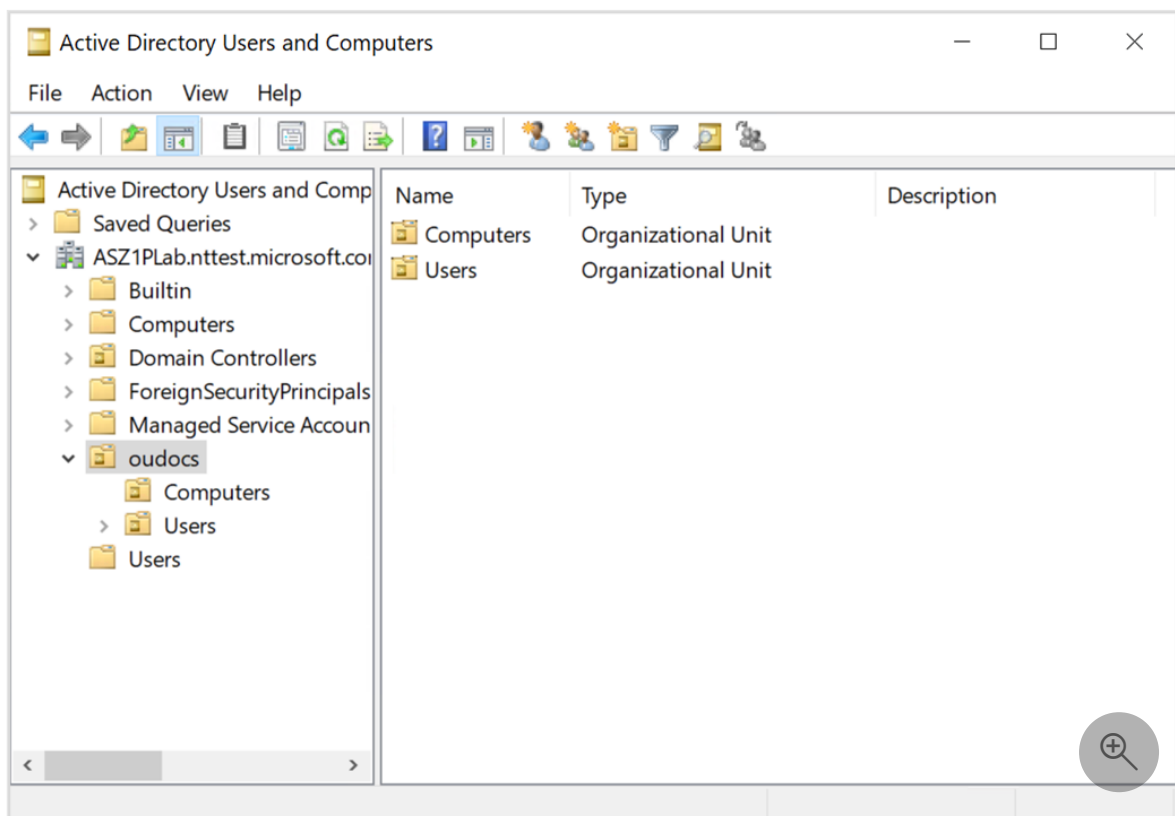
```
ActiveDirectoryRights : ReadProperty
InheritanceType       : All
ObjectType            : 00000000-0000-0000-0000-000000000000
InheritedObjectType   : 00000000-0000-0000-0000-000000000000
ObjectFlags           : None
AccessControlType     : Allow
IdentityReference     : ASZ1PLAB\docspro2cluster$
IsInherited           : False
InheritanceFlags      : ContainerInherit
PropagationFlags      : None
```

```
ActiveDirectoryRights : CreateChild
InheritanceType       : All
ObjectType            : bf967a86-0de6-11d0-a285-00aa003049e2
InheritedObjectType   : 00000000-0000-0000-0000-000000000000
ObjectFlags           : ObjectAceTypePresent
AccessControlType     : Allow
IdentityReference     : ASZ1PLAB\docspro2cluster$
IsInherited           : False
InheritanceFlags      : ContainerInherit
```

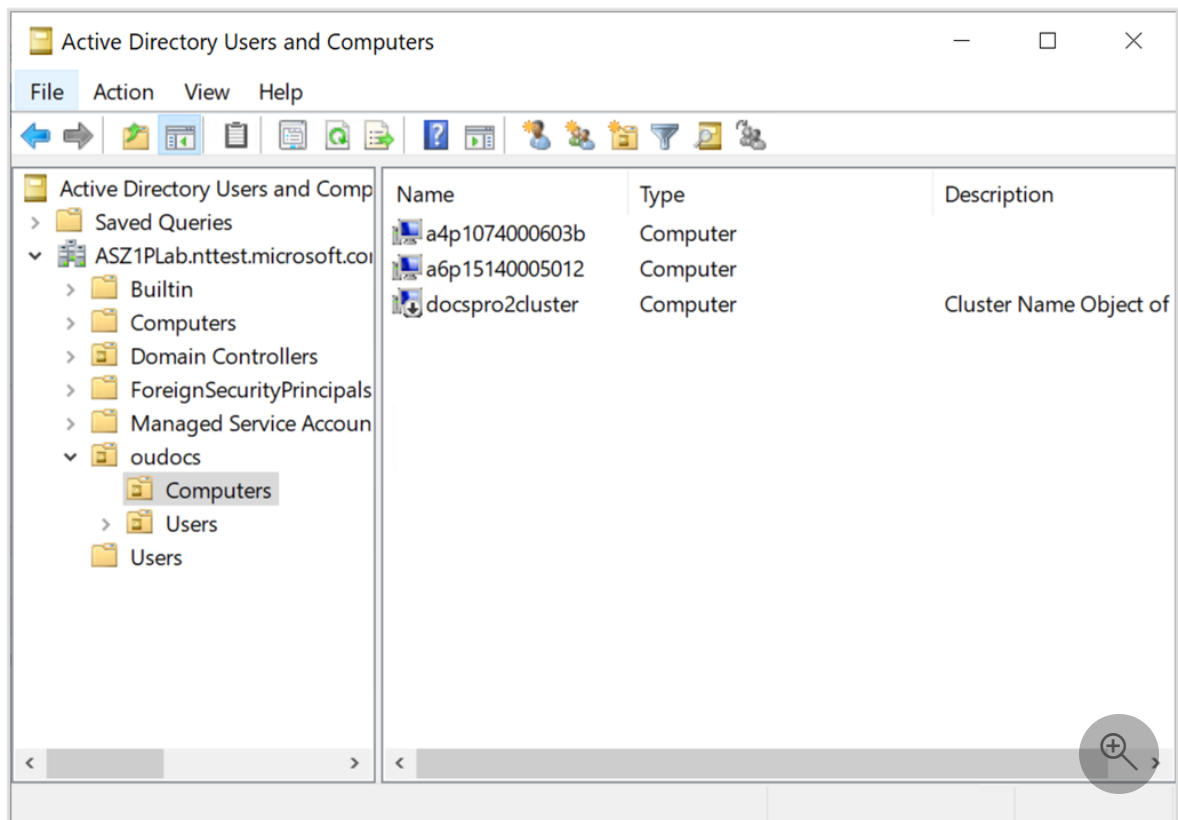
PropagationFlags : None

PS C:\temp>

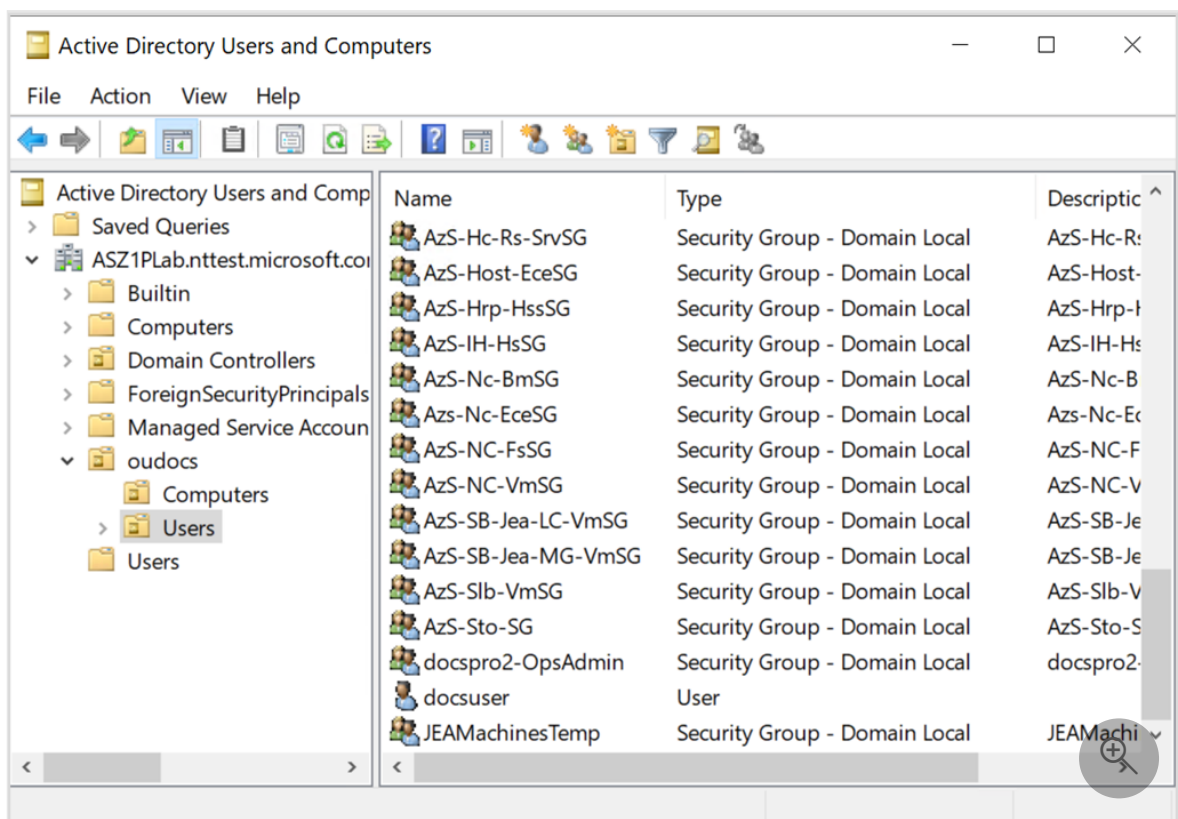
6. Verify that the OU and the corresponding **Computers** and **Users** objects are created. If using a Windows Server client, go to **Server Manager > Tools > Active Directory Users and Computers**.
7. An OU with the specified name should be created and within that OU, you'll see **Computers** and **Users** objects.



8. The **Computers** object should contain one computer account for each server node and one account for the **Cluster Name Object**.



9. The **Users** object should contain one user group corresponding to the user you specified during the creation and one security group - domain local with this name format: *Active Directory object prefix-OpsAdmin*. For example: *docspro2-OpsAdmin*.



ⓘ Note

- To perform a second deployment, run the prepare step with a different prefix and a different OU name.
- If you are repairing a single server, do not delete the existing OU. If the server volumes are encrypted, deleting the OU removes the BitLocker recovery keys.

## Next steps

- [Install Azure Stack HCI version 22H2 operating system](#) on each server in your cluster.

# Install the Azure Stack HCI, version 22H2 operating system (preview)

Article • 11/17/2023

Applies to: Azure Stack HCI, version 23H2 (preview)

The Azure Stack HCI, version 22H2 operating system is installed locally on each server in your cluster. The installation includes a folder that contains the deployment tool used to deploy a cluster.

## Important

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

## Prerequisites

Before you begin, make sure you've done the following:

- Satisfy the [prerequisites](#).
- Complete the [deployment checklist](#).
- Prepare your [Active Directory](#) environment.

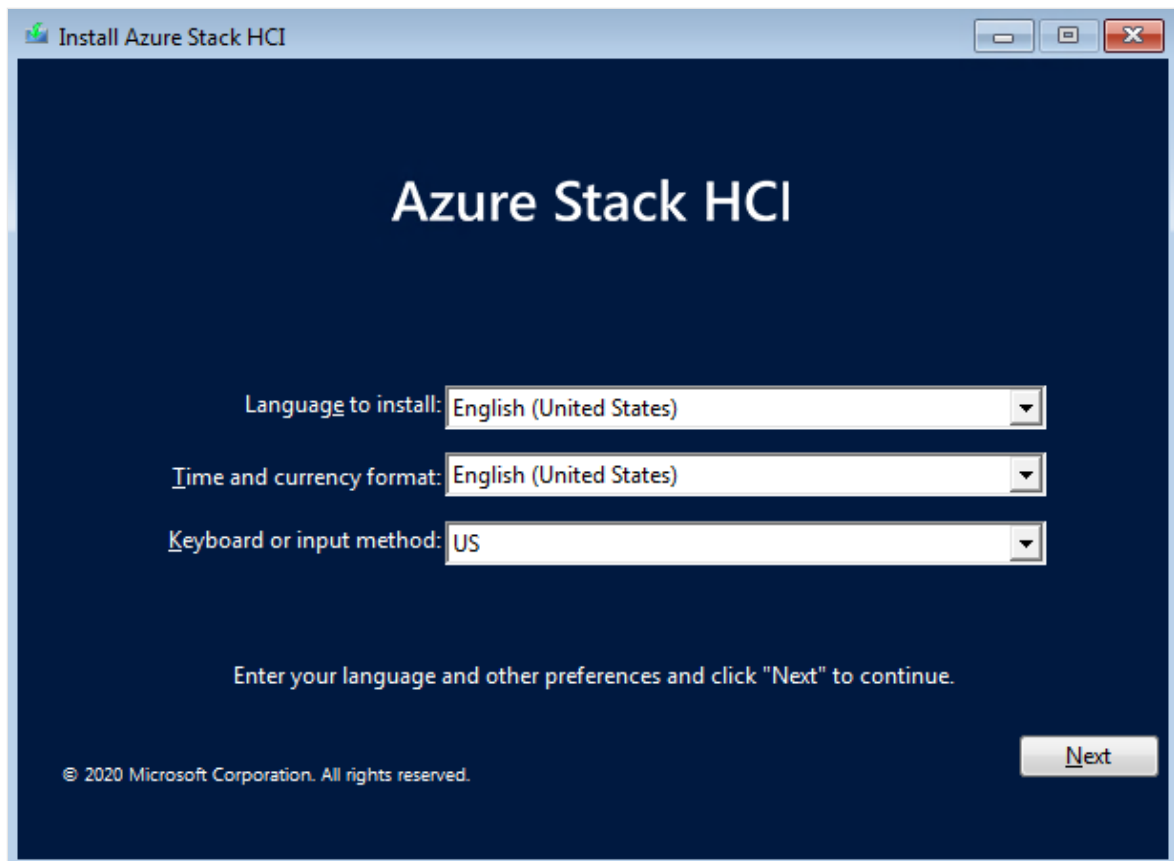
## Boot and install the operating system

The Supplemental package supports only the English version of the Azure Stack HCI operating system.

To install the Azure Stack HCI operating system in English, follow these steps:

1. [Download the Azure Stack HCI operating system from the Azure portal](#). Make sure to select **English** from the **Choose language** dropdown list.
2. Start the **Install Azure Stack HCI** wizard on the system drive of the server where you want to install the operating system.
3. Choose the language to install or accept the default language settings, select **Next**, and then on next page of the wizard, select **Install now**.

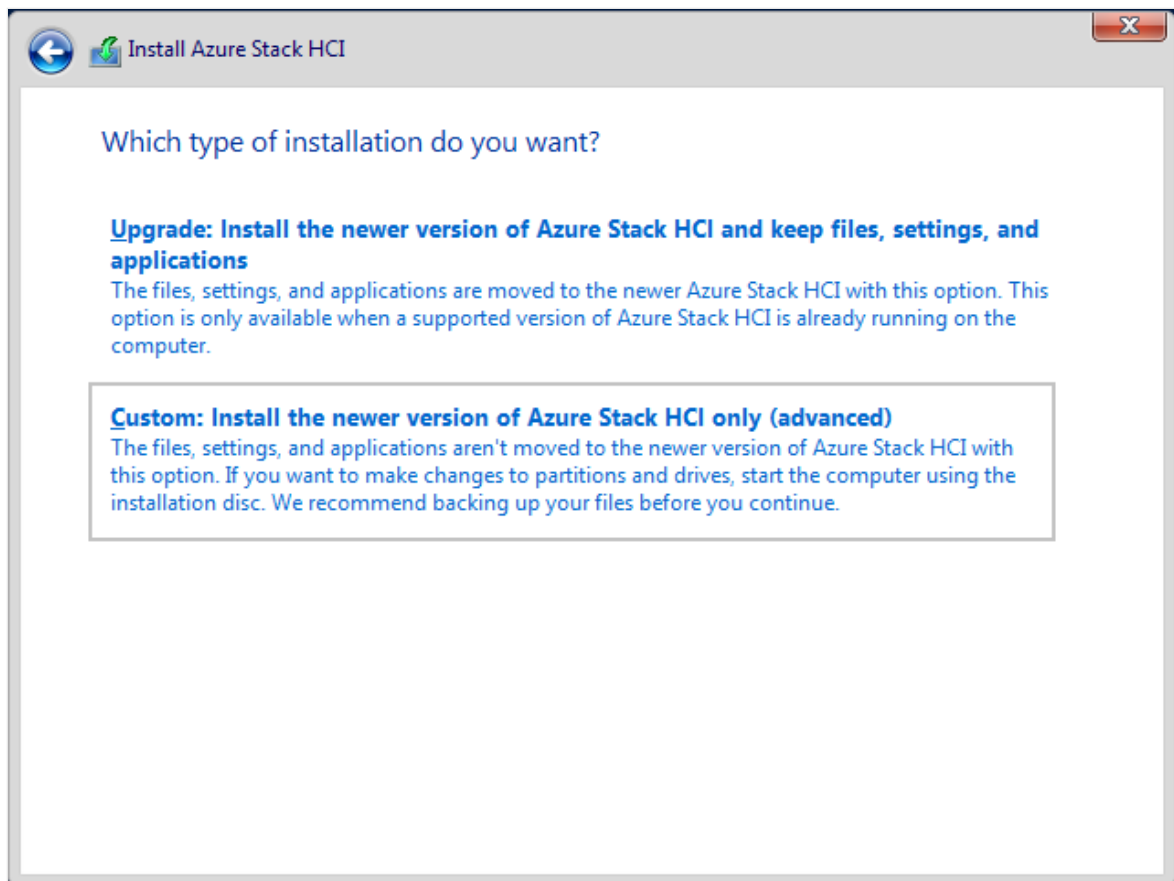




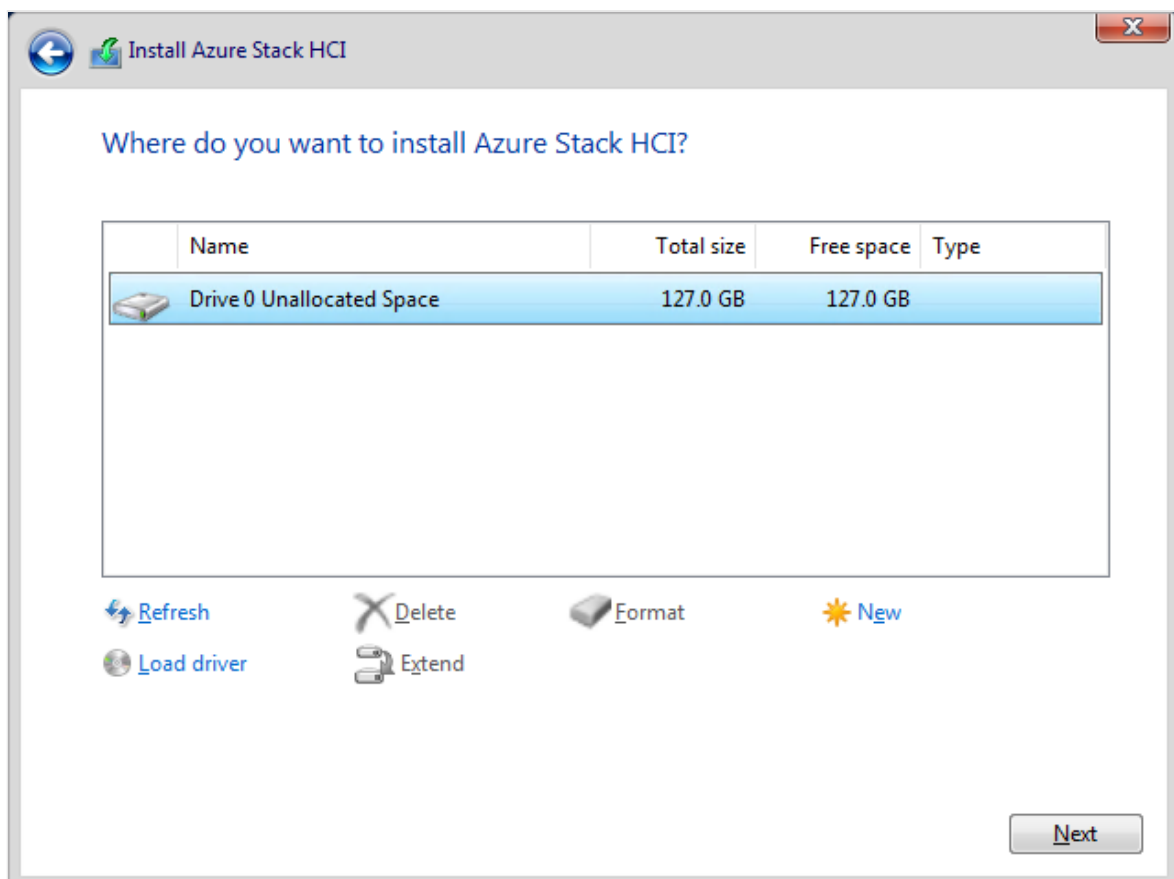
4. On the **Applicable notices and license terms** page, review the license terms, select the **I accept the license terms** checkbox, and then select **Next**.
5. On the **Which type of installation do you want?** page, select **Custom: Install the newer version of Azure Stack HCI only (advanced)**.

ⓘ **Note**

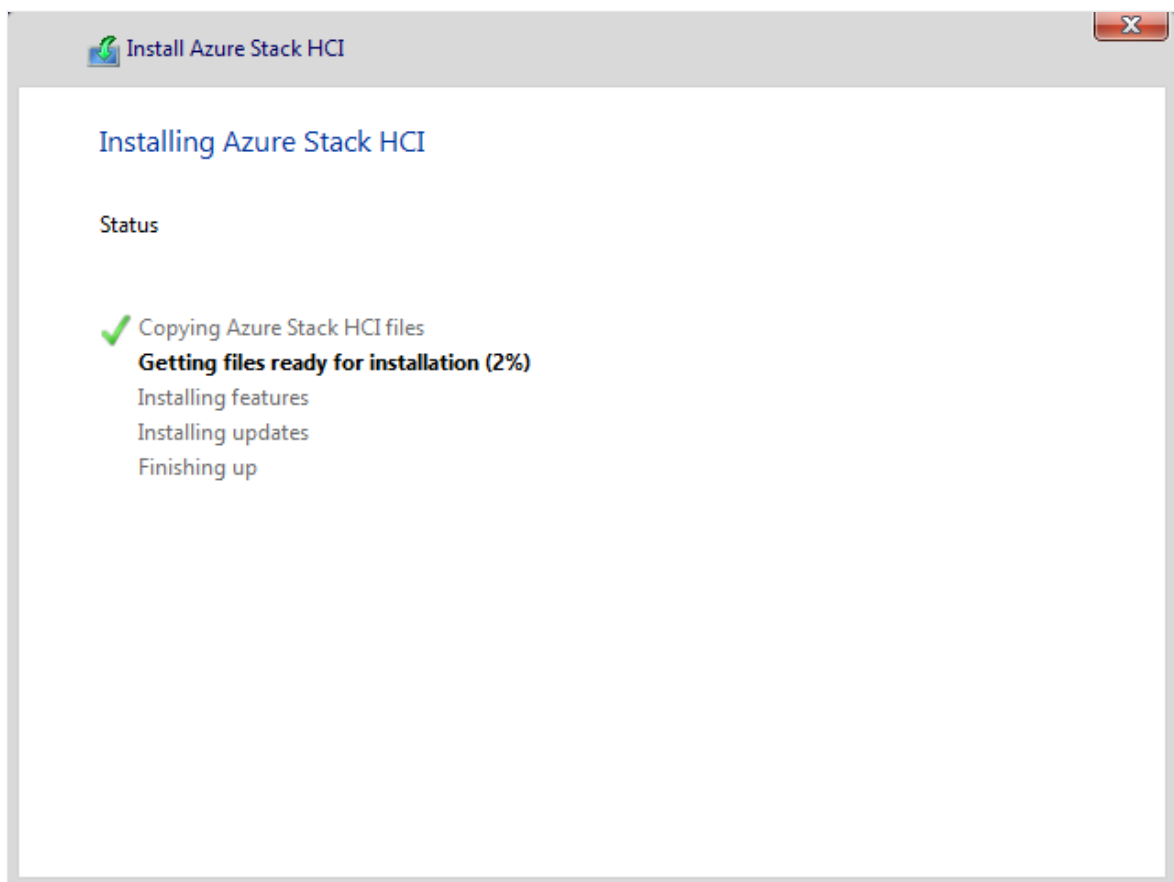
Upgrade installations are not supported in this release of the operating system.



6. On the **Where do you want to install Azure Stack HCI?** page, confirm the drive where the operating system is installed, and then select **Next**.



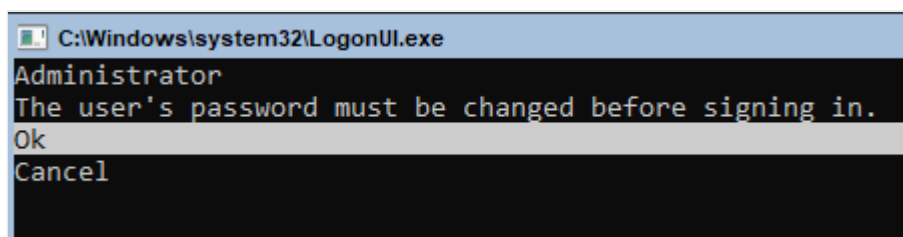
7. The **Installing Azure Stack HCI** page displays to show status on the process.



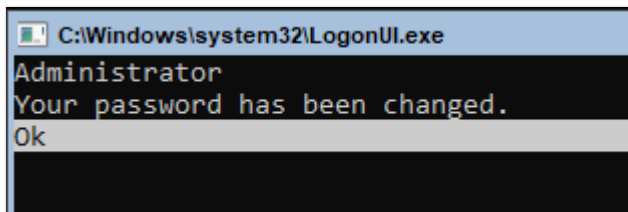
ⓘ **Note**

The installation process restarts the operating system twice to complete the process, and displays notices on starting services before opening an Administrator command prompt.

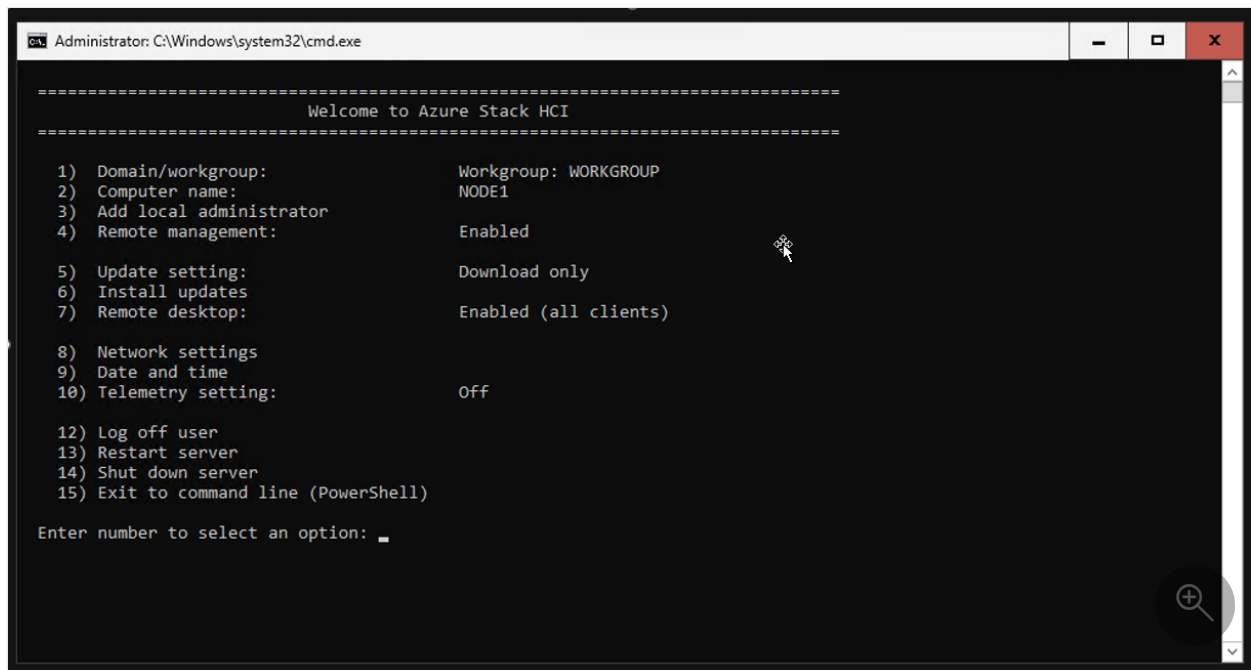
8. At the Administrator command prompt, select **Ok** to change the user's password before signing in, and press **Enter**.



9. At the **Enter new credential** for Administrator prompt, enter a new password. Enter the password again to confirm it, and then press **Enter**.
10. At the **Your password has been changed** confirmation prompt, press **Enter**.



Now you're ready to use the Server Configuration tool (SConfig) to perform important tasks. To use *SConfig*, log on to the server running the Azure Stack HCI operating system. This could be locally via a keyboard and monitor, or using a remote management (headless or BMC) controller, or Remote Desktop. The *SConfig* tool opens automatically when you log on to the server.



## Configure the operating system using SConfig

You can use *SConfig* to configure Azure Stack HCI version 22H2 after installation as follows:

1. Make sure that Windows updates won't be downloaded and installed during the deployment.
2. Configure networking as per your environment.
3. Configure a default valid gateway and a DNS server.
4. Rename the server(s) using option 2 in *SConfig* to match what you have used when preparing Active Directory, as you won't rename the servers later.
5. Restart the servers.

6. Set the local administrator credentials to be identical across all servers.
7. Install the latest drivers and firmware as per the instructions provided by your hardware manufacturer. You can use *SConfig* to run driver installation apps. After the install is complete, restart your servers again.

## Install required Windows roles

1. Install the Hyper-V role. Run the following command:

PowerShell

```
Enable-WindowsOptionalFeature -Online -FeatureName Microsoft-Hyper-V -All
```

Your servers will restart and this will take a few minutes.

2. After the servers have restarted, use the option 15 in *SConfig* to launch the PowerShell session.
3. Skip this step if you're deploying a single server.

- a. On each node, run the following command:

PowerShell

```
winrm quickconfig
```

- b. Enable ICMP. This command is required for the other nodes to access the first node.

Azure PowerShell

```
netsh advfirewall firewall add rule name="ICMP Allow incoming V4 echo request" protocol=icmpv4:8,any dir=in action=allow
```

## Next steps

[Set up the first server in your Azure Stack HCI cluster.](#)

# Set up the first server for new Azure Stack HCI deployment (preview)

Article • 10/05/2023

Applies to: Azure Stack HCI, Supplemental Package

This article describes how to set up the first server in the cluster for a new Azure Stack HCI deployment. The first server listed for the cluster acts as a staging server in the deployment.

The deployment tool is included in the Azure Stack HCI Supplemental Package. You need to install and set up the deployment tool only on the first server in the cluster.

## Important

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

## Prerequisites

Before you begin, make sure you've done the following:

- Satisfy the [prerequisites](#).
- Complete the [deployment checklist](#).
- Prepare your [Active Directory](#) environment.
- [Install version 22H2 OS](#) in English on each server.

## Download the Supplemental Package

The Supplemental Package supports only the English version of the Azure Stack HCI operating system. Make sure that you've installed Azure Stack HCI, version 22H2 OS in English on each server before downloading the Supplemental Package.

## Important

When you try out this new deployment tool, make sure that you do not run production workloads on systems deployed with the Supplemental Package while

it's in preview even with the core operating system Azure Stack HCI 22H2 being generally available. Microsoft Customer Support will supply support services while in preview, but service level agreements available at GA do not apply.

Follow these steps to download the Supplemental Package files:

1. [Download the Azure Stack HCI operating system from the Azure portal](#). Make sure to select **English** from the **Choose language** dropdown list.
2. Download the following Supplemental Package files:

Azure Stack HCI Supplemental Package component	Description
<a href="#">BootstrapCloudDeploymentTool.ps1</a>	Script to extract content and launch the deployment tool. When this script is run with the <code>-ExtractOnly</code> parameter, it will extract the zip file but not launch the deployment tool.
<a href="#">CloudDeployment.zip</a>	Azure Stack HCI, version 22H2 content, such as images and agents.
<a href="#">Verify-CloudDeployment.ps1</a>	Hash used to validate the integrity of zip file.

## Connect to the first server

Follow these steps to connect to the first server:

1. Select the first server listed for the cluster to act as a staging server during deployment.
2. Sign in to the first server using local administrative credentials.
3. Copy the [Supplemental Package that you downloaded previously](#) to a local drive on the first server.

## Set up the deployment tool

1. Run PowerShell as administrator.
2. Run the following command to install the deployment tool:

```
PowerShell
```

```
.\BootstrapCloudDeploymentTool.ps1
```

This step takes several minutes to complete.

### ⚠ Note

If you manually extracted deployment content from the ZIP file previously, you must run `BootstrapCloudDeployment-Internal.ps1` instead.

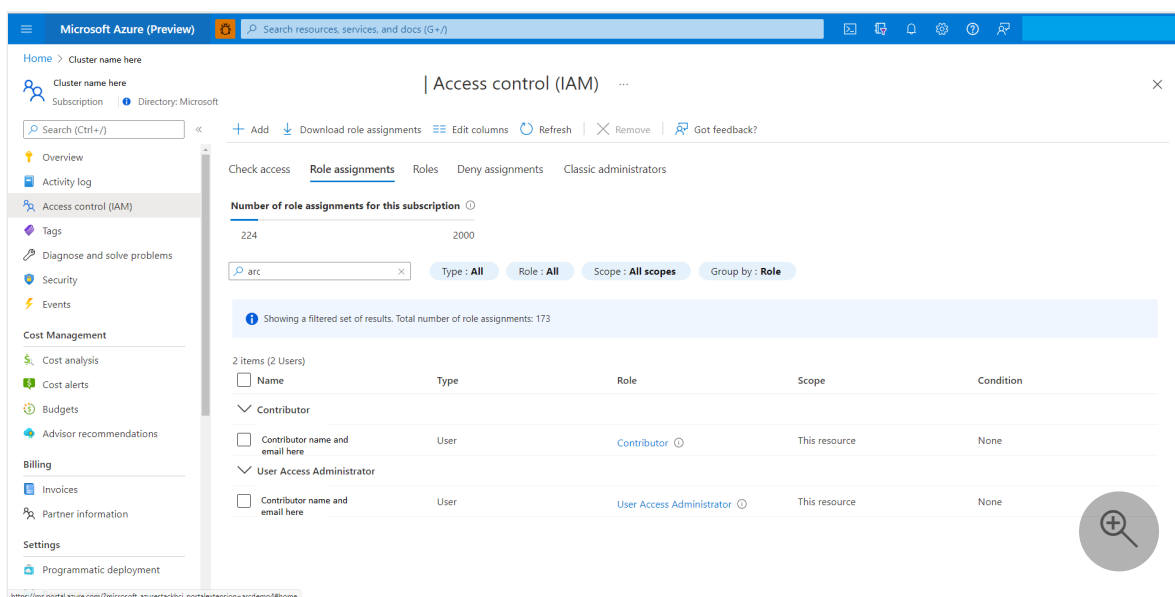
## Assign Azure permissions for deployment

This section describes how to assign Azure permissions for deployment from the Azure portal or using PowerShell.

### Assign Azure permissions from the Azure portal

If your Azure subscription is through an Enterprise Agreement (EA) or Cloud Solution Provider (CSP), ask your Azure subscription admin to assign Azure subscription level privileges of:

- **User Access Administrator** role: Required to Arc-enable each server of an Azure Stack HCI cluster.
- **Contributor** role: Required to register and unregister the Azure Stack HCI cluster.



### Assign Azure permissions using PowerShell



Some admins may prefer a more restrictive option. In this case, it's possible to create a custom Azure role specific for Azure Stack HCI deployment. To create this custom role, you need to be either an Owner or a User Access Administrator on the subscription. For more information about how to create a custom role including the various manage operations, see [Tutorial: Create an Azure custom role using Azure PowerShell](#).

The following procedure provides a typical set of permissions to the custom role.

1. Create a **customHCIRole.json** with the following content. Make sure to change `<subscriptionID>` to your Azure subscription ID. To get your Azure subscription ID, use the [Get-AzSubscription](#) command.

json

```
{
  "id": "/subscriptions/<Azure subscription ID>",
  "properties": {
    "roleName": "Azure Stack HCI 23H2 validator and registration role",
    "description": "Custom Azure role to allow subscription-level access to register Azure Stack HCI",
    "assignableScopes": [
      "/subscriptions/<Azure subscription ID>"
    ],
    "permissions": [
      {
        "Actions": [
          "Microsoft.Resources/subscriptions/resourceGroups/read",
          "Microsoft.Resources/subscriptions/resourceGroups/write",
          "Microsoft.Resources/subscriptions/resourceGroups/delete",
          "Microsoft.AzureStackHCI/register/action",
          "Microsoft.AzureStackHCI/Unregister/Action",
          "Microsoft.AzureStackHCI/clusters/*",
          "Microsoft.Authorization/roleAssignments/write",
          "Microsoft.Authorization/roleAssignments/read",
          "Microsoft.HybridCompute/register/action",
          "Microsoft.GuestConfiguration/register/action",
          "Microsoft.HybridConnectivity/register/action",
          "Microsoft.HybridCompute/machines/extensions/write",
          "Microsoft.HybridCompute/machines/extensions/read",
          "Microsoft.HybridCompute/machines/extensions/delete",
          "Microsoft.HybridCompute/machines/read",
          "Microsoft.HybridCompute/machines/write",
          "Microsoft.HybridCompute/machines/delete",
          "Microsoft.HybridCompute/privateLinkScopes/read",
          "Microsoft.GuestConfiguration/guestConfigurationAssignments/read",
          "Microsoft.ResourceConnector/register/action",
          "Microsoft.ResourceConnector/appliances/read",
          "Microsoft.ResourceConnector/appliances/write",
          "Microsoft.ResourceConnector/appliances/delete",
          "Microsoft.ResourceConnector/locations/operationresults/read",
          "Microsoft.ResourceConnector/locations/operationsstatus/read",
```

```

"Microsoft.ResourceConnector/appliances/listClusterUserCredential/action",
    "Microsoft.ResourceConnector/operations/read",
    "Microsoft.Kubernetes/register/action",
    "Microsoft.KubernetesConfiguration/register/action",
    "Microsoft.ExtendedLocation/register/action",
    "Microsoft.HybridContainerService/register/action",
    "Microsoft.KubernetesConfiguration/extensions/write",
    "Microsoft.KubernetesConfiguration/extensions/read",
    "Microsoft.KubernetesConfiguration/extensions/delete",
    "Microsoft.KubernetesConfiguration/extensions/operations/read",
    "Microsoft.KubernetesConfiguration/namespaces/read",
    "Microsoft.KubernetesConfiguration/operations/read",
    "Microsoft.ExtendedLocation/customLocations/deploy/action",
    "Microsoft.ExtendedLocation/customLocations/read",
    "Microsoft.ExtendedLocation/customLocations/write",
    "Microsoft.ExtendedLocation/customLocations/delete"
  ],
  "notActions": [],
  "dataActions": [],
  "notDataActions": []
}
]
}
}

```

## 2. Create the custom role:

PowerShell

```
New-AzRoleDefinition -InputFile "C:\CustomRoles\customHciRole.json"
```

## 3. Assign the custom role to the user:

PowerShell

```

$user = Get-AzADUser -DisplayName <userdisplayname>
$role = Get-AzRoleDefinition -Name "Azure Stack HCI 23H2 validator and
registration role"
New-AzRoleAssignment -ObjectId $user.Id -RoleDefinitionId $role.Id -
Scope /subscriptions/<Azure Subscription ID>

```

The following table explains why these permissions are required:

Operation	Description
"Microsoft.Resources/subscriptions/resourceGroups/read"	To register
"Microsoft.Resources/subscriptions/resourceGroups/write"	and
"Microsoft.Resources/subscriptions/resourceGroups/delete"	unregister the

Operation	Description
"Microsoft.AzureStackHCI/register/action" "Microsoft.AzureStackHCI/Unregister/Action" "Microsoft.AzureStackHCI/clusters/*" "Microsoft.Authorization/roleAssignments/read"	Azure Stack HCI cluster.
"Microsoft.Authorization/roleAssignments/write" "Microsoft.HybridCompute/register/action" "Microsoft.GuestConfiguration/register/action" "Microsoft.HybridConnectivity/register/action"	To register and unregister the Arc for server resources.
"Microsoft.HybridCompute/machines/extensions/write" "Microsoft.HybridCompute/machines/extensions/read" "Microsoft.HybridCompute/machines/extensions/delete"	To list and enable Arc Extensions on Azure Stack HCI cluster.
"Microsoft.HybridCompute/machines/read" "Microsoft.HybridCompute/machines/write" "Microsoft.HybridCompute/machines/delete"	To enable Arc for Servers on each node of your Azure Stack HCI cluster.
"Microsoft.HybridCompute/privateLinkScopes/read"	To enable private endpoints.
"Microsoft.GuestConfiguration/guestConfigurationAssignments/read" "Microsoft.ResourceConnector/register/action" "Microsoft.ResourceConnector/appliances/read" "Microsoft.ResourceConnector/appliances/write" "Microsoft.ResourceConnector/appliances/delete" "Microsoft.ResourceConnector/locations/operationresults/read" "Microsoft.ResourceConnector/locations/operationsstatus/read" "Microsoft.ResourceConnector/appliances/listClusterUserCredential/action" "Microsoft.ResourceConnector/operations/read" "Microsoft.Kubernetes/register/action" "Microsoft.KubernetesConfiguration/register/action" "Microsoft.ExtendedLocation/register/action" "Microsoft.HybridContainerService/register/action" "Microsoft.KubernetesConfiguration/extensions/write" "Microsoft.KubernetesConfiguration/extensions/read" "Microsoft.KubernetesConfiguration/extensions/delete" "Microsoft.KubernetesConfiguration/extensions/operations/read" "Microsoft.KubernetesConfiguration/namespaces/read" "Microsoft.KubernetesConfiguration/operations/read" "Microsoft.ExtendedLocation/customLocations/deploy/action" "Microsoft.ExtendedLocation/customLocations/read"	For Azure Arc Resource Bridge installation.

Operation	Description
"Microsoft.ExtendedLocation/customLocations/write"	
"Microsoft.ExtendedLocation/customLocations/delete"	

To set more restrictive permissions, see [How do I use a more restricted custom permissions role?](#)

## Next steps

After setting up the first server in your cluster, you're ready to run the deployment tool. You can either create a new deployment configuration file interactively or use an existing configuration file you created:

- [Deploy using a new configuration file.](#)
- [Deploy using an existing configuration file.](#)
- If preferred, you can also [deploy using PowerShell.](#)

# Deploy Azure Stack HCI interactively (preview)


Article • 06/28/2023

Applies to: Azure Stack HCI, Supplemental Package

After you've successfully installed the operating system, you're ready to set up and run the deployment tool. This method of deployment leads you through a guided UI experience to create a configuration (answer) file interactively that is saved.

You can deploy both single server and multi-node clusters using this procedure.

## Important

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

## Prerequisites

Before you begin, make sure you've done the following:

- Satisfy the [prerequisites](#).
- Complete the [deployment checklist](#).
- Prepare your [Active Directory](#) environment.
- [Install version 22H2 OS](#) on each server.
- [Set up the first server](#) in your Azure Stack HCI cluster.
- If deploying as a part of single server recovery, make sure to:
  - Not delete the existing Active Directory OU. If the volumes are encrypted, deletion of the existing OU causes the loss of BitLocker recovery keys.
  - Use the same parameters with which the server was imaged previously.
  - Select the **Use existing drives** option. This option unlocks the encrypted drives using the protector keys stored in your Active Directory.

## Run the deployment tool

This procedure collects deployment parameters from you interactively and saves them to a configuration file as you step through the deployment UI. You deploy single-node

and multi-node clusters similarly.

If you want to use an existing configuration file you have previously created, see [Deploy using a configuration file](#).

1. Open a web browser from a computer that has network connectivity to the staging server.
2. In the URL field, enter *https://your\_staging-server-IP-address*.
3. Accept the security warning displayed by your browser - this is shown because we're using a self-signed certificate.
4. Authenticate using the local administrator credentials of your staging server.
5. In the deployment UI, on the **Get started deploying Azure Stack** page, select **Create a new config file**, then select either **One server** or **Multiple servers** as applicable for your deployment.

Windows Admin Center | Deployment Microsoft

### Get started deploying Azure Stack

These questions define what your setup experience is like. [Learn more](#)

**1. How do you want to deploy?**

☒ Create a new config file  
Gather settings into a file that is applied at the end of the wizard (or later).

☐ Use an existing config file  
Configure your servers with settings loaded from an existing file.

**2. How big is your cluster?**

☐ One server

☒ Multiple servers

[Continue](#)

## Step 1: Initial configuration

1. On step 1.1 **Provide registration details**, enter the following details to authenticate your cluster with Azure:
  - a. Select the **Azure Cloud** to be used. In this release, only Azure public cloud is supported.
  - b. Under **Authentication**, select **Copy** to copy the authentication code for your Azure cloud:

Windows Admin Center | Deployment | Microsoft

## Deploy Azure Stack

1 Initial configuration 2 Networking 3 Cluster 4 Storage 5 Validate and Deploy

### 1.1 Provide registration details

1.2 Configure privacy  
1.3 Add servers  
1.4 Set cluster security  
1.5 Join a domain

#### Provide Azure registration details

This is used to authenticate with Azure and later to create the cluster's Azure resource and set up billing.

**Authentication**

Azure cloud \*

AGUWV9WHU [Copy](#)

Sign in

**Registration**

Azure Active Directory (tenant) ID

Azure subscription

Azure resource group

Azure region

[Back](#) [Next](#) [Exit](#)

c. Select **Sign in**. A new browser window opens. Enter the code that you copied earlier and then provide your Azure credentials. Multi-factor authentication (MFA) is supported.

Microsoft

## Enter code

Enter the code displayed on your app or device.

Code

[Next](#)

d. Go back to the deployment screen and provide the Azure registration details:

Windows Admin Center | Deployment | Microsoft

## Deploy Azure Stack

1 Initial configuration 2 Networking 3 Cluster 4 Storage 5 Validate and Deploy

### 1.1 Provide registration details

1.2 Configure privacy  
1.3 Add servers  
1.4 Set cluster security  
1.5 Join a domain

#### Provide Azure registration details

This is used to authenticate with Azure and later to create the cluster's Azure resource and set up billing.

**Authentication**

Azure cloud \*

Azure account [aszregistration@microsoft.com](#) [Sign out](#)

**Registration**

Azure Active Directory (tenant) ID

Azure subscription

Azure resource group

Azure region

[Back](#) [Next](#) [Exit](#)

- e. From the dropdown, select the **Azure Active Directory ID** or the tenant ID.
- f. Select the associated subscription. This subscription is used to create the cluster resource, register it with Azure Arc and set up billing.

**Note**

Make sure that you are a **user access administrator** on this subscription. This will allow you to manage access to Azure resources, specifically to Arc-enable each server of an Azure Stack HCI cluster.

- g. Select an existing **Azure resource group** from the dropdown to associate with the cluster resource. To create a new resource group, leave the field empty.
  - h. Select an **Azure region** from the dropdown or leave the field empty to use the default.
2. On step 1.2 **Configure privacy**, set the privacy settings as they apply to your organization.

The screenshot shows the 'Deploy Azure Stack' wizard in the Windows Admin Center. The current step is 1.2 'Configure privacy'. The left sidebar lists the steps: 1.1 Provide registration details, 1.2 Configure privacy (selected), 1.3 Add servers, 1.4 Set cluster security, and 1.5 Join a domain. The main content area is titled 'Set privacy settings' and contains three sections: 'Location of your cluster' with radio buttons for 'Europe' and 'Outside of Europe' (selected); 'Diagnostic data' with radio buttons for 'On (Recommended)' and 'Off' (selected); and 'Metrics and telemetry data' with radio buttons for 'On (Recommended)' and 'Off' (selected). Below these sections are links for 'Terms + conditions' and 'Required diagnostic data'. At the bottom, there are 'Back', 'Next', and 'Exit' buttons.

3. On step 1.3 **Add servers**, follow these steps:

- a. Provide the local administrator credentials. Make sure that the local administrator credentials are identical across all the servers.



- b. Enter the IP address of each server. Add the servers in the correct sequence, beginning with the first server.

**Note**

The first server is the staging server from which you are currently running the deployment tool.

The screenshot shows the 'Deploy Azure Stack' wizard in the Windows Admin Center. The left sidebar lists steps: 1.1 Provide registration details, 1.2 Configure privacy, 1.3 Add servers (selected), 1.4 Set cluster security, and 1.5 Join a domain. The main area is titled 'Select the servers to cluster'. It includes fields for 'Username' (SetupUser) and 'Password' (masked). Below, there's a section 'Add each server's IP address.' with a text input containing '10.57.51.224' and an 'Add' button. A green checkmark indicates 'Found 'a6p15140005012''. A 'Refresh' button is also present. At the bottom, there's a table with headers: 'Server name or IP address', 'Status', 'Operating system', and 'Model'. The table currently shows 'No records found'. Navigation buttons 'Back', 'Next', and 'Exit' are at the bottom.

4. On step 1.4 Set cluster security, select **Recommended security settings** to use the recommended default settings:

The screenshot shows the 'Deploy Azure Stack' wizard at step 1.4 'Set cluster security'. The left sidebar highlights step 1.4. The main area is titled 'Set the security level of your system's infrastructure'. It states 'You can change this later.' and offers two options: 'Recommended security settings' (selected with a radio button) and 'Customized security settings'. Below, a progress bar shows 'Security settings' at '5 of 5' with a green bar. A green checkmark indicates 'Excellent'. Navigation buttons 'Back', 'Next', and 'Exit' are at the bottom.

or select **Customized security settings**:

Windows Admin Center | Deployment | Microsoft

## Deploy Azure Stack

1 Initial configuration 2 Networking 3 Cluster 4 Storage 5 Validate and Deploy

1.1 Provide registration details  
1.2 Configure privacy  
1.3 Add servers  
1.4 Set cluster security  
1.5 Join a domain

### Set the security level of your system's infrastructure

You can change this later.

☐ Recommended security settings  
☒ Customized security settings

Security settings 5 of 5  
Excellent

#### Recommended security settings

Setting	Description
<input checked="" type="checkbox"/> Security Drift Control	Prevents unnoticed/unmanaged changes over the security defaults. Disable this if you need to customize your security controls beyond the UI options.
<input checked="" type="checkbox"/> App control (WDAC) enforced on host	Provides control to which drivers and applications are allowed or denied to run.
<input checked="" type="checkbox"/> BitLocker for OS boot volume	Provides data protection for the Operating System Volume against data theft or exposure from lost, stolen, or inappropriately decommissioned computers.
<input checked="" type="checkbox"/> BitLocker for data volumes	Provides data protection for Cluster Shared Volumes against data theft or exposure from lost, stolen, or inappropriately decommissioned computers.
<input checked="" type="checkbox"/> SMB Signing Default instance	Protects (using signatures) network SMB connections between your Host and remote shares.

#### Additional hardening settings

Setting	Description
<input type="checkbox"/> SMB Encryption E-W Cluster traffic	Encrypts network SMB connections used by Failover Clustering and/or Storage Spaces Direct to move data between the nodes in the cluster.
<input type="checkbox"/> Credential Guard No Lock	Provides system secrets isolation (Kerberos/NTLM/Cred Manager) so that only privileged system software can access them.

Back Next Exit

For more information on the individual security settings, see:

- [App control \(WDAC\) enforced on host.](#)
- [BitLocker for OS boot volume and BitLocker for data volumes.](#)
- [SMB Signing Default instance.](#)
- [SMB Encryption E-W Cluster traffic.](#)

5. On step 1.5 **Join a domain**, enter the following:

- Provide your **Active Directory domain** name. For example, this would be the fully qualified domain name in `Contoso.com` format.
- Enter the **Computer name prefix** used when you prepared the Active Directory.
- For **OU**, provide the full distinguished name of the organizational unit (including the domain components) that was created for the deployment. For example, the name would be `"OU=Hci001,DC=contoso,DC=com"`.
- Provide the **username** and the **password** for the lifecycle manager (LCM) account that was created during [Prepare the Active Directory](#) step.

Windows Admin Center | Deployment | Microsoft

## Deploy Azure Stack

1 Initial configuration 2 Networking 3 Cluster 4 Storage 5 Validate and Deploy

1.1 Provide registration details  
1.2 Configure privacy  
1.3 Add servers  
1.4 Set cluster security  
1.5 Join a domain

### Join a domain

#### Join an existing Active Directory domain

Active Directory domain \*

Active Directory object prefix \*

Active Directory OU \*

#### Enter the domain account to join

Domain username \*

Domain password \*

When you're ready, select Next.

Back Next: Networking Exit

## Step 2: Networking

1. On step 2.1 **Check network adapters**, consult with your network administrator to ensure you enter the correct network details.

If all the network adapters do not show up and if you have not excluded those, select **Show hidden adapters**. You may also need to check the cabling and the link speeds. While the network interfaces can have identical speeds across the nodes of the cluster, any low speed switch connections could lead to a difference in the overall speed.

The screenshot shows the 'Deploy Azure Stack' wizard in the Windows Admin Center. The 'Networking' step is active, showing a list of network adapters available on all servers. The list includes Port2, Port3, and Port4, all with a speed of 100 Gbps. A 'Show hidden adapters' button is visible at the bottom left of the adapter list. The wizard has a progress bar at the top indicating the current step, and 'Back' and 'Next' buttons at the bottom.

Name	Description	Speed	Exclude
Port2	Intel(R) Ethernet Connection X722 for 10GBASE-T	10 Gbps	<input checked="" type="checkbox"/> Exclude
Port3	Mellanox ConnectX-6 Dx Adapter	100 Gbps	<input checked="" type="checkbox"/> Exclude
Port4	Mellanox ConnectX-6 Dx Adapter	100 Gbps	<input checked="" type="checkbox"/> Exclude

2. On step 2.2 **Define network intents**, consult with your network administrator to ensure you enter the correct network details.

When you define network intents, only the following sets of network intents are supported for this preview release:

- one *Management* + *Compute* intent, one storage intent.
- one fully converged intent that maps to *Management* + *Compute* + *Storage* intent.

The networking intent should match how you've cabled your system. For this release, see the [Validated deployment network patterns](#).

Windows Admin Center | Deployment | Microsoft

## Deploy Azure Stack

Initial configuration **2 Networking** 3 Cluster 4 Storage 5 Validate and Deploy

2.1 Check network adapters  
**2.2 Define network intents**  
 2.3 Provide storage network details  
 2.4 Allocate IP addresses

### Define intents for your network traffic

Specify the intent for your network adapters, indicating the traffic type (management, compute, storage) expected on each set of adapters. We'll configure the same adapters on every server based on what you specify. [Learn more.](#)

- Traffic types can be combined on the same set of adapters
- Assign management and storage traffic only once each (they can be different intents)
- Assign compute and storage traffic to at least one intent

**Intent 1** [Customize network settings](#)

Traffic types \*

Intent name \*

Network adapters \*  [×](#)

[+ Select another adapter for this traffic](#)

**Intent 2** [Customize network settings](#)

Traffic types \*

Intent name \*

Network adapters \*  [×](#)  
 [×](#)

[+ Select another adapter for this traffic](#)

[+ Add an intent](#)

[Back](#) [Next](#) [Exit](#)

3. On step 2.3 **Provide storage network details**, consult with your network administrator to ensure that you enter the correct network details.

Windows Admin Center | Deployment | Microsoft

## Deploy Azure Stack

Initial configuration 2 Networking **3 Cluster** 4 Storage 5 Validate and Deploy

2.1 Check network adapters  
 2.2 Define network intents  
**2.3 Provide storage network details**  
 2.4 Allocate IP addresses

### Provide storage network details

Specify the VLAN for the storage network. These settings are applied to adapters that carry in-cluster storage traffic and VM migrations.

**Storage network**

Storage network	Network adapter	Name	CIDR	VLAN ID
Storage subnet 1	Mellanox ConnectX-6 Dx Adapter	Port3	10.71.1.0/24	5
Storage subnet 2	Mellanox ConnectX-6 Dx Adapter	Port4	10.71.2.0/24	5

[Back](#) [Next](#) [Exit](#)

4. On step 2.4 **Allocate IP addresses**, enter the following input after consulting your network administrator:

- In this release, only the static IPs can be assigned and DHCP isn't supported.
- For the **Starting IP** and the **Ending IP** range, provide a minimum of 6 free, contiguous IPv4 addresses. This range excludes your host IPs. These IPs are used for infrastructure services such as clustering.
- Provide the **Subnet mask** and **Default gateway** for the network.
- Provide the IPv4 address of the **DNS servers** in your environment. DNS servers are required because they're used when your server attempts to communicate

with Azure or to resolve your server by name in your network. The DNS server you configure must be able to resolve the Active Directory domain.

For high availability, we recommend that you configure a preferred and an alternate DNS server.

Windows Admin Center | Deployment | Microsoft

### Deploy Azure Stack

Initial configuration | **Networking** | Cluster | Storage | Validate and Deploy

2.1 Check network adapters  
2.2 Define network intents  
2.3 Provide storage network details  
**2.4 Allocate IP addresses**

#### Allocate IP addresses to the system and services

We need a block of IP addresses on your management network to use for the system and for services such as the Network Controller and Azure Arc. [Learn more.](#)

IP assignment \* ☒ Manual ☐ Automatic (DHCP) - Not available for this release

Starting IP \* 10.57.48.60

Ending IP \* 10.57.48.66

Subnet mask \* 255.255.248.0

Default gateway \* 10.57.48.1

DNS Servers \* 10.57.52.92 [+](#) Add

[Back](#) [Next](#) [Exit](#)

## Step 3: Cluster

For two-node clusters, you'll need to create a cluster witness. A cluster witness helps establish quorum for a two-node cluster if a node goes down. To learn about quorum, see [Understanding quorum](#).

You can either create a cloud witness or a file share witness:

Use a cloud witness if you have internet access and if you use an Azure Storage account to provide a vote on cluster quorum. A cloud witness uses Azure Blob Storage to read or write a blob file and then uses it to arbitrate in split-brain resolution. For more information on cloud witness, see [Deploy a cloud witness for Failover cluster](#).

Use a file share witness if you use a local SMB file share to provide a vote in the cluster quorum. Use a file share witness if all the servers in a cluster have spotty internet connectivity or can't use disk witness as there aren't any shared drives. For more information on file share witness, see [Deploy a file share witness for Failover cluster](#).

### ! Note

For single-server clusters, a witness doesn't apply, so you only need to provide a cluster name for step 3.1 below.

1. On step 3.1 **Provide the cluster name**, enter the cluster name. This must be the cluster name you used when preparing Active Directory.
2. For two-node clusters, select either **Cloud witness** or **File share witness**.
3. For **Cloud witness**, do the following:
  - a. Enter the Azure storage account name.
  - b. Enter the Access key for the storage account.
  - c. For Azure blob service endpoint type, select either **Default** or **Custom domain**.
  - d. If you selected **Custom domain**, enter the domain for the blob service.
  - e. When finished, select **Next: Storage**.

Windows Admin Center | Deployment

Deploy Azure Stack

Initial configuration Networking **3 Cluster** 4 Storage 5 Validate and Deploy

3.1 Provide the cluster name

**Provide the cluster details**

Enter the cluster name used when Active Directory was prepared for this system. You'll use the cluster name later to work with this Azure Stack HCI system instead of directly managing the underlying server or servers. [Learn more](#)

Cluster name \* docspro2cluster

**Cluster Witness**

Witness type \* ☒ Cloud witness ☐ File share witness

Azure storage account name \* myasestoragacct

Access key \* [masked]

Azure blob service endpoint type \* ☒ Default ☐ Custom domain

Blob service [core.windows.net]

Back Next: Storage Exit

4. For **File share witness**, do the following:
  - a. Enter the file share path in `//server/filesshare` format.
  - b. When finished, select **Next: Storage**.

Windows Admin Center | Deployment

Deploy Azure Stack

Initial configuration Networking **3 Cluster** 4 Storage 5 Validate and Deploy

3.1 Provide the cluster name

**Provide the cluster details**

Enter the cluster name used when Active Directory was prepared for this system. You'll use the cluster name later to work with this Azure Stack HCI system instead of directly managing the underlying server or servers. [Learn more](#)

Cluster name \* docspro2cluster

**Cluster Witness**

Witness type \* ☐ Cloud witness ☒ File share witness

File share path \* \\contoso\witnessshare

Back Next: Storage Exit

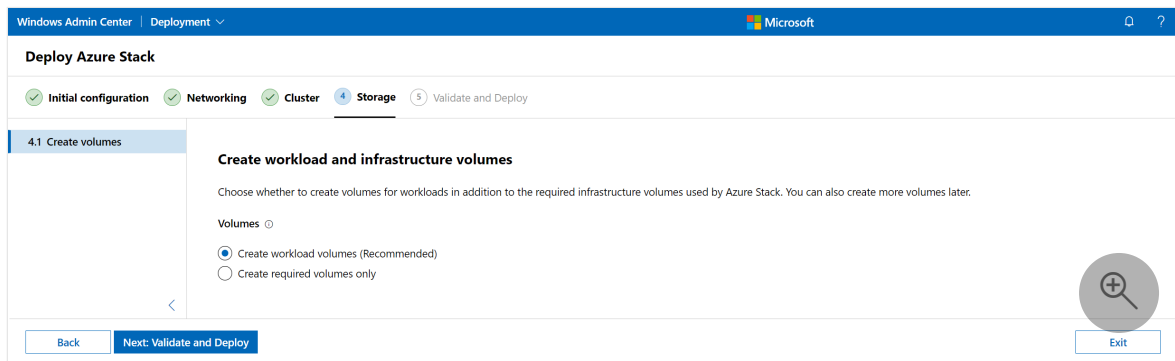
## Step 4: Storage

- On step 4.1 **Create volumes**, select the **Create workload volumes (recommended)** option to create workload volumes in addition to the infrastructure volumes used

by Azure Stack HCI cluster. Choosing this option will create all the volumes with the best resiliency level.

If you select **Create required volumes only**, you will need to create workload volumes yourselves.

Select the **Existing data drives** option only when you are repairing a single server. This option unlocks the encrypted drives using the protector keys stored in your Active Directory.



The screenshot shows the 'Deploy Azure Stack' wizard in the Windows Admin Center. The 'Storage' step is active, showing options to 'Create workload and infrastructure volumes'. The 'Create workload volumes (Recommended)' option is selected. The 'Next: Validate and Deploy' button is visible.

The deployment tool configures your storage according to the best practices based on the number of nodes in the cluster. The tool also configures at least one infrastructure volume that is used by the deployment orchestrator and one or multiple data volumes for your use.

If the resiliency configuration for data volumes does not suit your applications, you can delete these volumes and create these again as per your needs.

#### Important

Do not delete the infrastructure volume used to store content from the Lifecycle Manager.

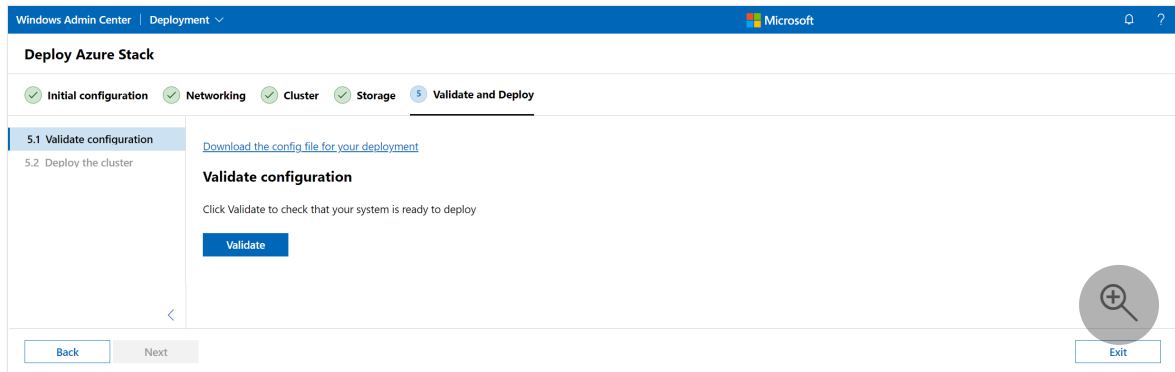
Here is a table summarizing the expected resiliency configuration against the number of nodes in your cluster.

# Node	Volume resiliency	# Infrastructure volumes	# Customer volumes
Single node	Two-way mirror	1	1
Two node	Two-way mirror	1	2
Three node +	Three-way mirror	1	1 per node

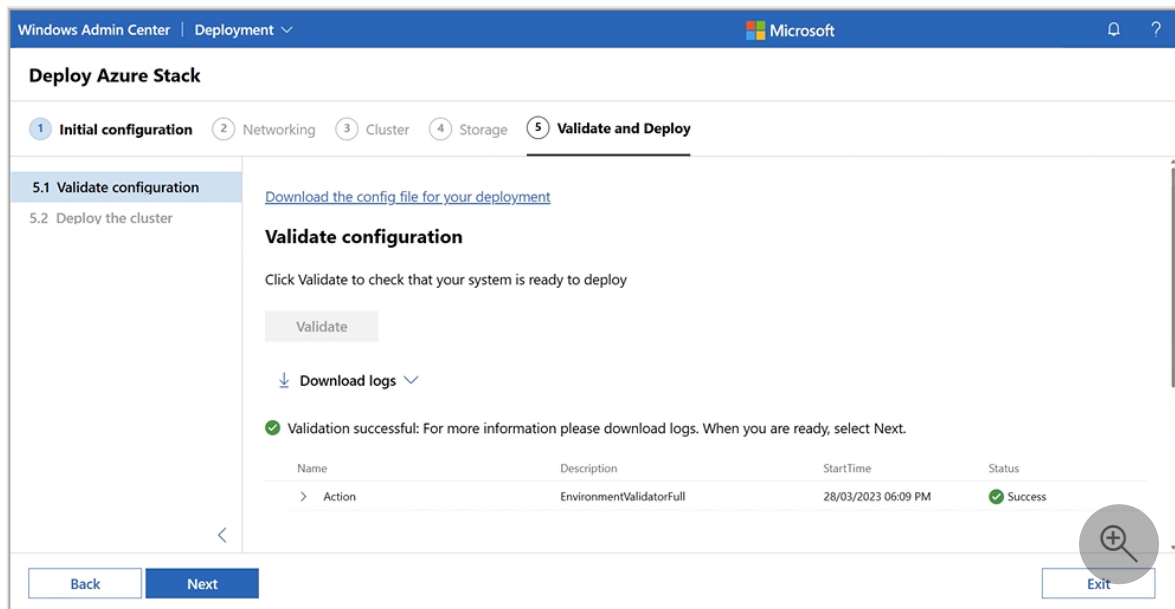
When finished, select **Next: Validate and Deploy** to continue.

## Step 5: Validate and Deploy

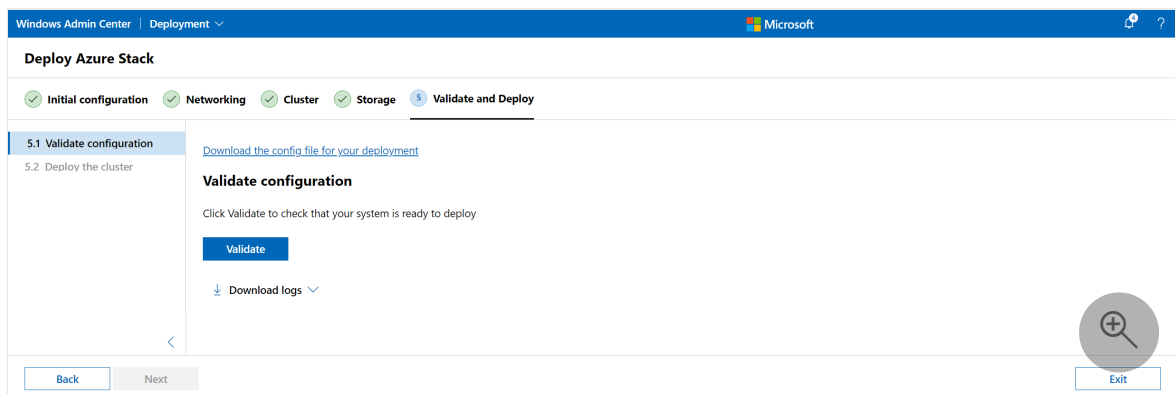
1. On step 5.1 **Validate configuration**, select **Download the config file for your deployment** and then select **Validate** to start validation.



2. If validation has successfully completed, you will receive confirmation. Select **Next** to continue with deployment.



If validation fails, select **Download logs** to view validation conflict details and then select **Validate** again to rerun validation.

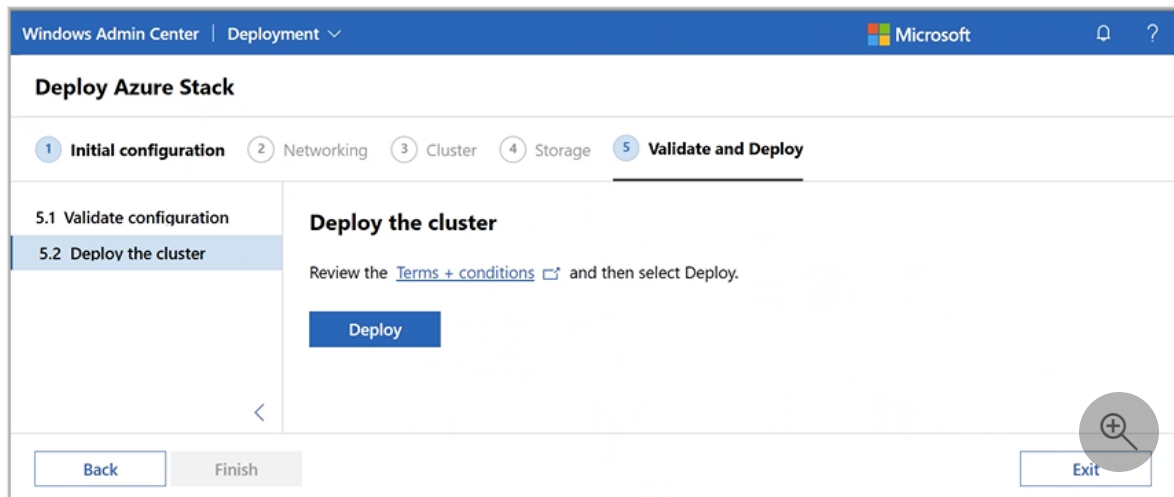




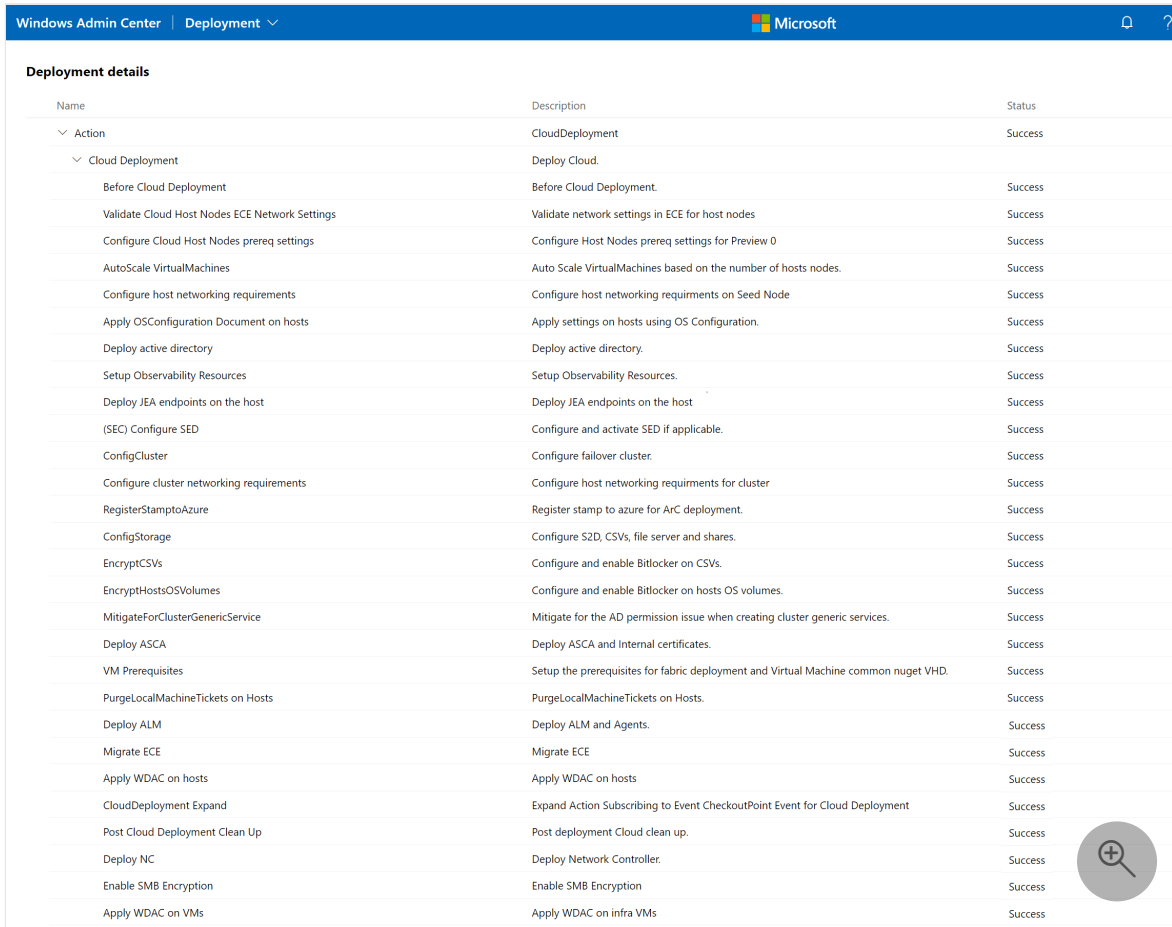
3. On step 5.2 **Deploy the cluster**, select **Deploy**. It can take up to 1.5 hours for deployment to complete.

### Important

The staging server will restart after the deployment starts.



You can monitor your deployment progress in near real time:



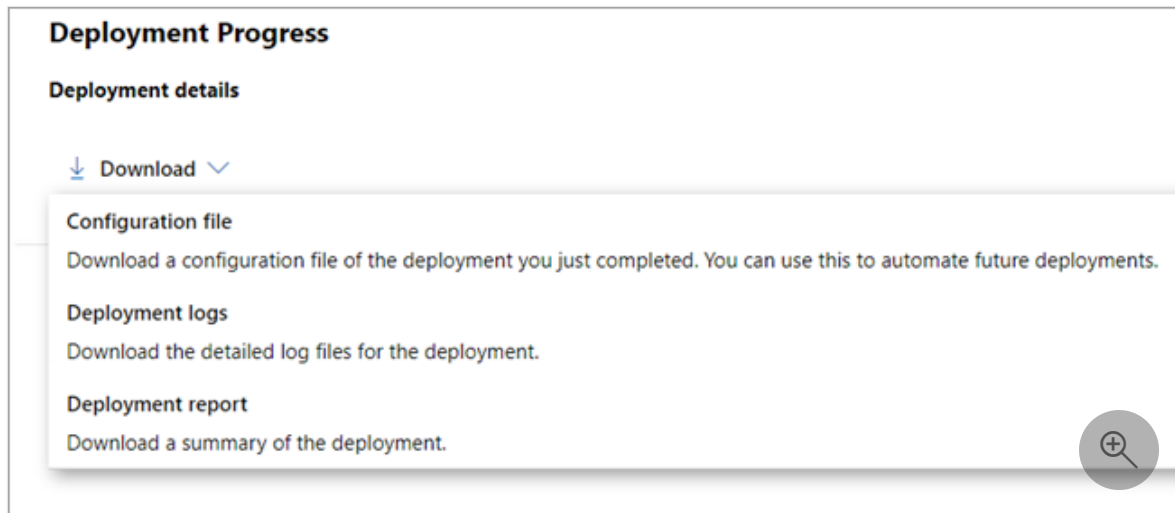
The screenshot shows the 'Deployment details' page in the Windows Admin Center. It displays a table with three columns: Name, Description, and Status. The table lists various deployment actions and their outcomes, all of which are marked as 'Success'. A magnifying glass icon is visible in the bottom right corner of the interface.

Name	Description	Status
✓ Action	CloudDeployment	Success
✓ Cloud Deployment	Deploy Cloud.	
Before Cloud Deployment	Before Cloud Deployment.	Success
Validate Cloud Host Nodes ECE Network Settings	Validate network settings in ECE for host nodes	Success
Configure Cloud Host Nodes prereq settings	Configure Host Nodes prereq settings for Preview 0	Success
AutoScale VirtualMachines	Auto Scale VirtualMachines based on the number of hosts nodes.	Success
Configure host networking requirements	Configure host networking requirements on Seed Node	Success
Apply OSConfiguration Document on hosts	Apply settings on hosts using OS Configuration.	Success
Deploy active directory	Deploy active directory.	Success
Setup Observability Resources	Setup Observability Resources.	Success
Deploy JEA endpoints on the host	Deploy JEA endpoints on the host	Success
(SEC) Configure SED	Configure and activate SED if applicable.	Success
ConfigCluster	Configure failover cluster.	Success
Configure cluster networking requirements	Configure host networking requirements for cluster	Success
RegisterStampToAzure	Register stamp to azure for Arc deployment.	Success
ConfigStorage	Configure S2D, CSVs, file server and shares.	Success
EncryptCSVs	Configure and enable BitLocker on CSVs.	Success
EncryptHostsOSVolumes	Configure and enable BitLocker on hosts OS volumes.	Success
MitigateForClusterGenericService	Mitigate for the AD permission issue when creating cluster generic services.	Success
Deploy ASCA	Deploy ASCA and Internal certificates.	Success
VM Prerequisites	Setup the prerequisites for fabric deployment and Virtual Machine common nuget VHD.	Success
PurgeLocalMachineTickets on Hosts	PurgeLocalMachineTickets on Hosts.	Success
Deploy ALM	Deploy ALM and Agents.	Success
Migrate ECE	Migrate ECE	Success
Apply WDAC on hosts	Apply WDAC on hosts	Success
CloudDeployment Expand	Expand Action Subscribing to Event CheckOutPoint Event for Cloud Deployment	Success
Post Cloud Deployment Clean Up	Post deployment Cloud clean up.	Success
Deploy NC	Deploy Network Controller.	Success
Enable SMB Encryption	Enable SMB Encryption	Success
Apply WDAC on VMs	Apply WDAC on infra VMs	Success

### Note

When you start the deployment, the page may not show actual progress even after the staging server has restarted. Refresh the page once using the browser refresh and then the page will automatically refresh for the remainder of the deployment.

You can select **Download** to download deployment logs and a deployment report. Deployment logs can help you troubleshoot a failed deployment.



## Next steps

- [Validate deployment.](#)
- If needed, [troubleshoot deployment.](#)

# Deploy Azure Stack HCI using an existing configuration file (preview)

Article • 06/29/2023


Applies to: Azure Stack HCI, Supplemental Package

After you have successfully installed the operating system, you are ready to set up and run the deployment tool. This deployment method uses an existing configuration file that you have modified for your environment.

The deployment tool wizard uses your file and further provides an interactive, guided experience that helps you deploy and register the cluster.

You can deploy both single-node and multi-node clusters using this procedure.

## Important

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

## Prerequisites

Before you begin, make sure you have done the following:

- Satisfy the [prerequisites](#).
- Complete the [deployment checklist](#).
- Prepare your [Active Directory](#) environment.
- [Install version 22H2](#) on each server.
- [Set up the first server](#) in your Azure Stack HCI cluster.

## Create the configuration file

Here's a sample configuration file (JSON format) you can modify, save, and use for deployment. One advantage to using your own configuration file is that more settings can be specified than are available when creating a file interactively. For descriptions of each setting, see the reference section later in this article.

JSON

```

{
  "Version": "10.0.0.0",
  "ScaleUnits": [
    {
      "DeploymentData": {
        "SecuritySettings": {
          "HVCIProtection": true,
          "DRTMProtection": true,
          "DriftControlEnforced": true,
          "CredentialGuardEnforced": true,
          "SMBSigningEnforced": true,
          "SMBClusterEncryption": false,
          "SideChannelMitigationEnforced": true,
          "BitlockerBootVolume": true,
          "BitlockerDataVolumes": true,
          "WDACEnforced": true
        },
        "Observability": {
          "StreamingDataClient": true,
          "EULocation": false,
          "EpisodicDataUpload": true
        },
        "Cluster": {
          "Name": "ms169154cluster",
          "WitnessType": "Cloud",
          "WitnessPath": "",
          "CloudAccountName": "myasestoragacct",
          "AzureServiceEndpoint": "core.windows.net"
        },
        "Storage": {
          "ConfigurationMode": "Express"
        },
        "NamingPrefix": "ms169",
        "DomainFQDN": "ASZ1PLab8.nttest.microsoft.com",
        "InfrastructureNetwork": [
          {
            "VlanId": "0",
            "SubnetMask": "255.255.248.0",
            "Gateway": "10.57.48.1",
            "IP Pools": [
              {
                "StartingAddress": "10.57.48.60",
                "EndingAddress": "10.57.48.66"
              }
            ],
            "DNSServers": [
              "10.57.50.90"
            ]
          }
        ],
        "PhysicalNodes": [
          {
            "Name": "ms169host",
            "IPv4Address": "10.57.51.224"
          }
        ]
      }
    ]
  ]
}

```

```

    },
    {
        "Name": "ms154host",
        "IPv4Address": "10.57.53.236"
    }
],
"HostNetwork": {
    "Intents": [
        {
            "Name": "Compute_Management",
            "TrafficType": [
                "Compute",
                "Management"
            ],
            "Adapter": [
                "Port2"
            ],
            "OverrideVirtualSwitchConfiguration": false,
            "VirtualSwitchConfigurationOverrides": {
                "EnableIov": "",
                "LoadBalancingAlgorithm": ""
            },
            "OverrideQoSPolicy": false,
            "QoSPolicyOverrides": {
                "PriorityValue8021Action_Cluster": "",
                "PriorityValue8021Action_SMB": "",
                "BandwidthPercentage_SMB": ""
            },
            "OverrideAdapterProperty": false,
            "AdapterPropertyOverrides": {
                "JumboPacket": "",
                "NetworkDirect": "",
                "NetworkDirectTechnology": ""
            }
        },
        {
            "Name": "Storage",
            "TrafficType": [
                "Storage"
            ],
            "Adapter": [
                "Port3",
                "Port4"
            ],
            "OverrideVirtualSwitchConfiguration": false,
            "VirtualSwitchConfigurationOverrides": {
                "EnableIov": "",
                "LoadBalancingAlgorithm": ""
            },
            "OverrideQoSPolicy": false,
            "QoSPolicyOverrides": {
                "PriorityValue8021Action_Cluster": "",
                "PriorityValue8021Action_SMB": "",
                "BandwidthPercentage_SMB": ""
            }
        },
    ],
}

```

```

        "OverrideAdapterProperty": false,
        "AdapterPropertyOverrides": {
            "JumboPacket": "",
            "NetworkDirect": "",
            "NetworkDirectTechnology": ""
        }
    },
    ],
    "StorageNetworks": [
        {
            "Name": "Storage1Network",
            "NetworkAdapterName": "Port3",
            "VlanId": 5
        },
        {
            "Name": "Storage2Network",
            "NetworkAdapterName": "Port4",
            "VlanId": 5
        }
    ]
},
"ADOUPath":
"OU=ms169,DC=ASZ1PLab8,DC=nttest,DC=microsoft,DC=com"
}
}
]
}

```

## Run the deployment tool

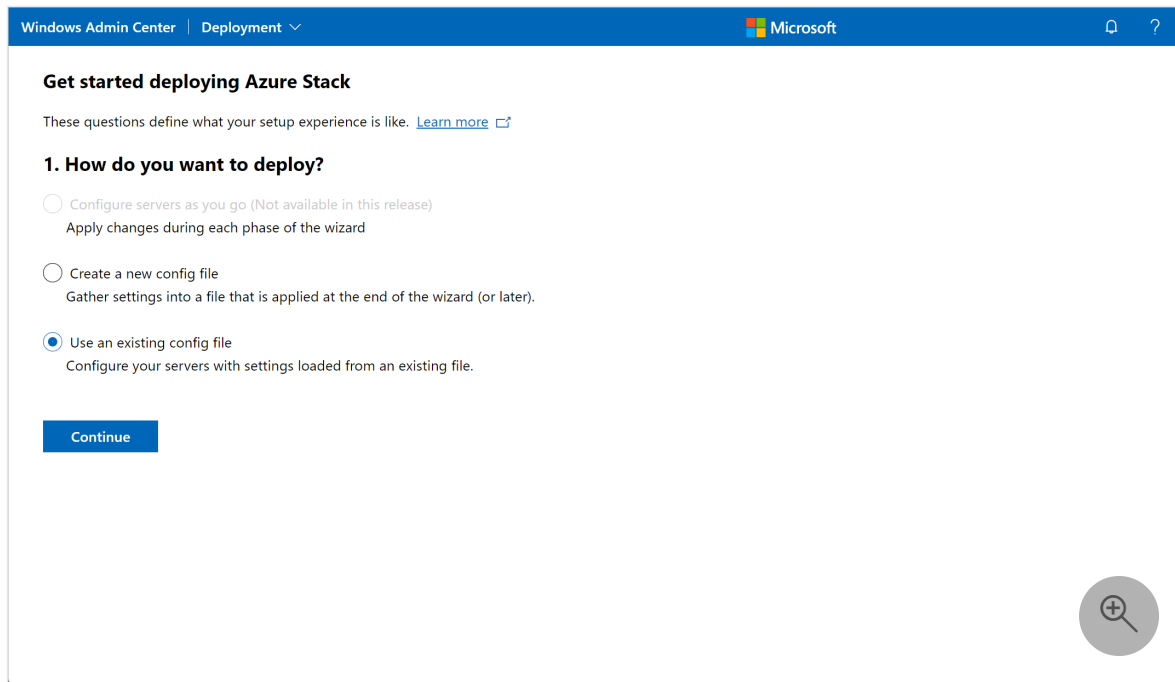
You deploy single-node and multi-node clusters similarly using the interactive flow in the deployment wizard.

### ⓘ Note

You need to install and set up the deployment tool only on the first server in the cluster.

1. Open a web browser from a computer that has network connectivity to the first server also known as the staging server.
2. In the URL field, enter *https://your\_staging-server-IP-address*.
3. Accept the security warning displayed by your browser - this is shown because we're using a self-signed certificate.
4. Authenticate using the local administrator credentials of your staging server.

5. In the deployment wizard, on the **Get started deploying Azure Stack** page, select **Use an existing config file**, then select either **One server** or **Multiple servers** as applicable for your deployment.



The screenshot shows the 'Get started deploying Azure Stack' page in the Windows Admin Center. The page has a blue header with 'Windows Admin Center | Deployment' and the Microsoft logo. Below the header, the title 'Get started deploying Azure Stack' is followed by a sub-header '1. How do you want to deploy?'. There are three radio button options: 'Configure servers as you go (Not available in this release)', 'Create a new config file', and 'Use an existing config file'. The 'Use an existing config file' option is selected. A 'Continue' button is at the bottom left. A search icon is in the bottom right corner.

Windows Admin Center | Deployment Microsoft

### Get started deploying Azure Stack

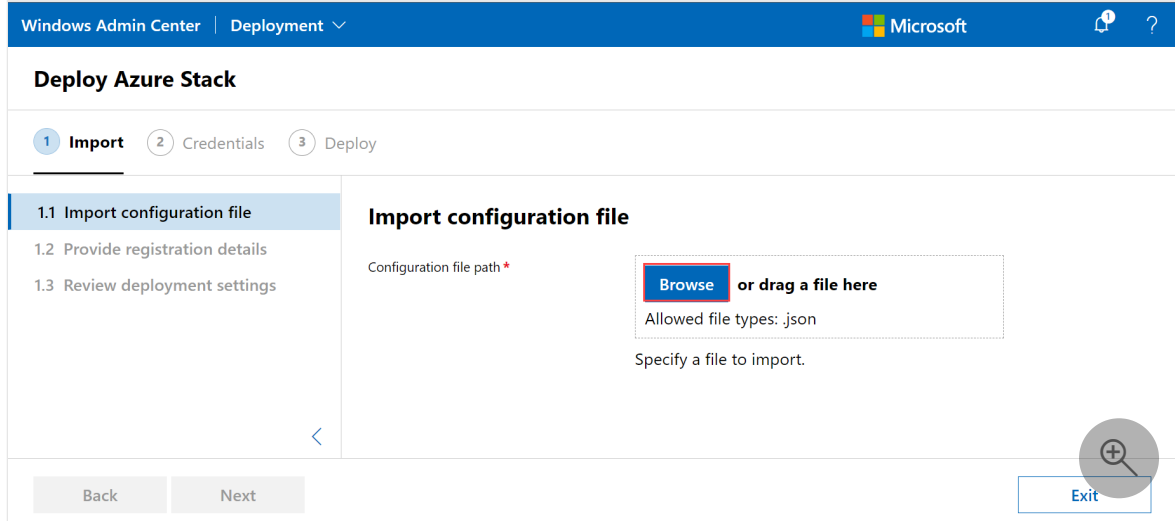
These questions define what your setup experience is like. [Learn more](#)

#### 1. How do you want to deploy?

- ☐ Configure servers as you go (Not available in this release)  
Apply changes during each phase of the wizard
- ☐ Create a new config file  
Gather settings into a file that is applied at the end of the wizard (or later).
- ☒ Use an existing config file  
Configure your servers with settings loaded from an existing file.

Continue

6. On step 1.1 **Import configuration file**, import the existing configuration file you created by selecting **Browse** or dragging the file to the page.



The screenshot shows the 'Deploy Azure Stack' page in the Windows Admin Center. The page has a blue header with 'Windows Admin Center | Deployment' and the Microsoft logo. Below the header, the title 'Deploy Azure Stack' is followed by a progress bar with three steps: '1 Import', '2 Credentials', and '3 Deploy'. The '1 Import' step is selected. Below the progress bar, there are three sub-steps: '1.1 Import configuration file', '1.2 Provide registration details', and '1.3 Review deployment settings'. The '1.1 Import configuration file' sub-step is selected. The main content area is titled 'Import configuration file' and contains a 'Configuration file path' label, a 'Browse' button, and a text box for 'or drag a file here'. Below the text box, it says 'Allowed file types: .json' and 'Specify a file to import.' At the bottom, there are 'Back', 'Next', and 'Exit' buttons. A search icon is in the bottom right corner.

Windows Admin Center | Deployment Microsoft

### Deploy Azure Stack

1 Import 2 Credentials 3 Deploy

#### 1.1 Import configuration file

1.2 Provide registration details  
1.3 Review deployment settings

#### Import configuration file

Configuration file path \*

**Browse** or drag a file here

Allowed file types: .json

Specify a file to import.

Back Next Exit

7. On step 1.2 **Provide registration details**, enter the following details to authenticate your cluster with Azure:

Windows Admin Center | Deployment Microsoft

## Deploy Azure Stack

1 Import 2 Credentials 3 Deploy

1.1 Import configuration file  
**1.2 Provide registration details**  
 1.3 Review deployment settings

### Provide Azure registration details

This is used to authenticate with Azure and later to create the cluster's Azure resource and set up billing.

**Authentication**

Azure cloud\*

Azure account  [Sign out](#)

**Registration**

Azure Active Directory (tenant) ID

Azure subscription

Azure resource group

Azure region

[Back](#) [Next](#) [Exit](#)

- Select the **Azure Cloud** to be used. In this release, only Azure public cloud is supported.
- Copy the authentication code.
- Select **login**. A new browser window opens. Enter the code that you copied earlier and then provide your Azure credentials. Multi-factor authentication (MFA) is supported.
- Go back to the deployment screen and provide the Azure registration details.
- From the dropdown, select the **Azure Active Directory ID** or the tenant ID.
- Select the associated subscription. This subscription is used to create the cluster resource, register it with Azure Arc and set up billing.

#### ⓘ Note

Make sure that you are a **user access administrator** on this subscription. This will allow you to manage access to Azure resources, specifically to Arc-enable each server of an Azure Stack HCI cluster.

- Select an existing **Azure resource group** from the dropdown to associate with the cluster resource. To create a new resource group, leave the field empty.
- Select an **Azure region** from the dropdown or leave the field empty to use the default. import the existing configuration file you created by selecting **Browse** or



dragging the file to the page.

8. On step 1.3 **Review deployment setting**, review the settings stored in the configuration file.

The screenshot shows the 'Deploy Azure Stack' wizard in the Windows Admin Center. The top navigation bar includes 'Windows Admin Center | Deployment' and the Microsoft logo. The wizard has three steps: 1. Import, 2. Credentials, and 3. Deploy. Step 1.3, 'Review deployment settings', is currently selected. On the left, a sidebar lists the steps: 1.1 Import configuration file, 1.2 Provide registration details, and 1.3 Review deployment settings. The main area displays the title 'Review deployment settings' and the filename 'wac-deploy-docspro2cluster (3).json'. Below this, a JSON configuration file is shown with various security and observability settings. At the bottom, there are three buttons: 'Back', 'Next: Credentials' (highlighted with a red border), and 'Exit'.

```
{
  "Version": "3.0.0.0",
  "ScaleUnits": [
    {
      "DeploymentData": {
        "SecuritySettings": {
          "SecurityModeSealed": true,
          "SecuredCoreEnforced": true,
          "VBSProtection": true,
          "HVCIProtection": true,
          "DRTMPProtection": true,
          "KernelDMAProtection": true,
          "DriftControlEnforced": true,
          "CredentialGuardEnforced": false,
          "SMBSigningEnforced": true,
          "SMBClusterEncryption": false,
          "SideChannelMitigationEnforced": true,
          "BitlockerBootVolume": true,
          "BitlockerDataVolumes": true,
          "SEDProtectionEnforced": true,
          "WDACEEnforced": true
        },
        "Observability": {
          "StreamingDataClient": true,
          "EULocation": false,

```

9. On step 2.1 **Credentials**, enter the username and password for the Active Directory account and username and password for the local administrator account.

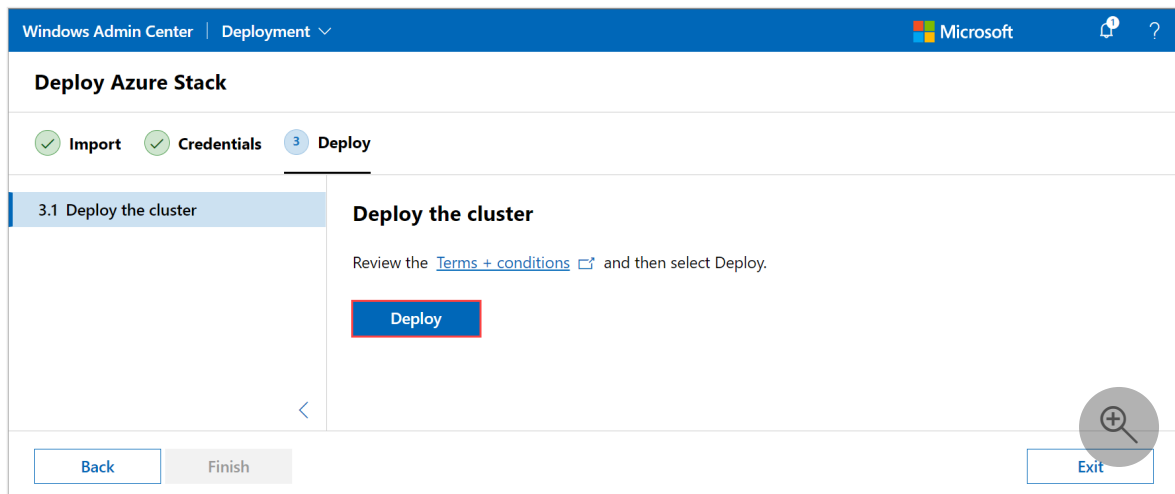
When specifying a username, omit the domain name (don't use *domain\username*). The *Administrator* username isn't supported.

The screenshot shows the 'Deploy Azure Stack' wizard in the Windows Admin Center, now at step 2.1, 'Credentials'. The top navigation bar is the same. The wizard steps are 1. Import, 2. Credentials, and 3. Deploy. Step 2.1 is selected. The sidebar shows '2.1 Credentials'. The main area is titled 'Credentials' and includes a note: 'The configuration file deployment will be kicked off by the orchestrator with the following credentials.' Below this, there are two sections: 'Domain credentials' and 'Local admin credentials'. Under 'Domain credentials', there are fields for 'Domain username' (containing 'docsuser') and 'Domain password' (masked with dots). Under 'Local admin credentials', there are fields for 'Username' (containing 'SetupUser') and 'Password' (masked with dots). At the bottom, there are three buttons: 'Back', 'Next: Deploy' (highlighted with a red border), and 'Exit'.

## Note

Credentials are never collected or stored in the configuration file.

10. On step 3.1 **Deploy the cluster**, select **Deploy** to start deployment of your cluster.



11. It can take up to 1.5 hours for the deployment to complete. You can monitor your deployment progress and the details in near real-time.

The screenshot shows the 'Deployment details' page in the Windows Admin Center. The top navigation bar includes 'Windows Admin Center | Deployment' and the Microsoft logo. The page title is 'Deployment details'. Below the title is a table with three columns: 'Name', 'Description', and 'Status'. The table lists various deployment actions and their status.

Name	Description	Status
✓ Action	CloudDeployment	Success
✓ Cloud Deployment	Deploy Cloud.	
Before Cloud Deployment	Before Cloud Deployment.	Success
Validate Cloud Host Nodes ECE Network Settings	Validate network settings in ECE for host nodes	Success
Configure Cloud Host Nodes prereq settings	Configure Host Nodes prereq settings for Preview 0	Success
AutoScale VirtualMachines	Auto Scale VirtualMachines based on the number of hosts nodes.	Success
Configure host networking requirements	Configure host networking requirements on Seed Node	Success
Apply OSConfiguration Document on hosts	Apply settings on hosts using OS Configuration.	Success
Deploy active directory	Deploy active directory.	Success
Setup Observability Resources	Setup Observability Resources.	Success
Deploy JEA endpoints on the host	Deploy JEA endpoints on the host	Success
(SEC) Configure SED	Configure and activate SED if applicable.	Success
ConfigCluster	Configure failover cluster.	Success
Configure cluster networking requirements	Configure host networking requirements for cluster	Success
RegisterStampToAzure	Register stamp to azure for ArC deployment.	Success
ConfigStorage	Configure S2D, CSVs, file server and shares.	Success
EncryptCSVs	Configure and enable Bitlocker on CSVs.	Success
EncryptHostsOSVolumes	Configure and enable Bitlocker on hosts OS volumes.	Success
MitigateForClusterGenericService	Mitigate for the AD permission issue when creating cluster generic services.	Success
Deploy ASCA	Deploy ASCA and Internal certificates.	Success
VM Prerequisites	Setup the prerequisites for fabric deployment and Virtual Machine common nuget VHD.	Success
PurgeLocalMachineTickets on Hosts	PurgeLocalMachineTickets on Hosts.	Success
Deploy ALM	Deploy ALM and Agents.	Success
Migrate ECE	Migrate ECE	Success
Apply WDAC on hosts	Apply WDAC on hosts	Success
CloudDeployment Expand	Expand Action Subscribing to Event CheckoutPoint Event for Cloud Deployment	Success
Post Cloud Deployment Clean Up	Post deployment Cloud clean up.	Success
Deploy NC	Deploy Network Controller.	Success
Enable SMB Encryption	Enable SMB Encryption	Success
Apply WDAC on VMs	Apply WDAC on infra VMs	Success

A magnifying glass icon is visible in the bottom right corner.

## Reference: Configuration file settings

The following table gives descriptions for the settings listed in the configuration file:

Setting	Description
SecuritySettings	Section name
SecurityModeSealed	This parameter should only be modified based on your OEM guidance. Do not modify this parameter without OEM validation.
SecuredCoreEnforced	This parameter should only be modified based on your OEM guidance. Do not modify this parameter without OEM validation.
VBSProtection	By default, Virtualization-based Security (VBS) is enabled on your Azure Stack HCI cluster. For more information, see <a href="#">Virtualization-based Security</a> .
HVCIProtection	By default, Hypervisor-protected Code Integrity (HVCI) is enabled on your Azure HCI cluster. For more information, see <a href="#">Hypervisor-protected Code Integrity</a> .
DRTMProtection	By default, Secure Boot is enabled on your Azure HCI cluster. This setting is hardware dependent. For more information, see <a href="#">Secure Boot with Dynamic Root of Trust for Measurement (DRTM)</a> .
KernelDMAProtection	By default, Pre-boot Kernel Direct Memory Access (DMA) protection is enabled on your Azure HCI cluster. This setting is hardware dependent. For more information, see <a href="#">Kernel Direct Memory Access protection</a> .
DriftControlEnforced	When set to <code>true</code> , the security baseline is re-applied regularly. For more information, see <a href="#">Security baseline settings for Azure Stack HCI</a>
CredentialGuardEnforced	When set to <code>true</code> , Credential Guard is enabled. For more information, see <a href="#">Manage Windows Defender Credential Guard</a> .
SMBSigningEnforced	When set to <code>true</code> , the SMB default instance requires sign in for the client and server services. For more information, see <a href="#">Overview of Server Message Block signing</a> .
SMBClusterEncryption	When set to <code>true</code> , cluster east-west traffic is encrypted. For more information, see <a href="#">SMB encryption</a> .

Setting	Description
SideChannelMitigationEnforced	When set to <code>true</code> , all the side channel mitigations are enabled, see <a href="#">KB4072698</a> .
BitLockerBootVolume	When set to <code>true</code> , BitLocker XTS_AES 256-bit encryption is enabled for all data-at-rest on the OS volume of your Azure Stack HCI cluster. This setting is TPM-hardware dependent. For more information, see <a href="#">BitLocker encryption for Azure Stack HCI</a> .
BitLockerDataVolumes	When set to <code>true</code> , BitLocker XTS-AES 256-bit encryption is enabled for all data-at-rest on your Azure Stack HCI cluster shared volumes. For more information, see <a href="#">BitLocker encryption for Azure Stack HCI</a> .
SEDProtectionEnforced	Not used for Azure Stack HCI version 22H2.
WDACEnforced	Windows Defender Application Control (WDAC) is enabled by default and limits the applications and the code that you can run on your Azure Stack HCI cluster. For more information, see <a href="#">Windows Defender Application Control</a> .
<b>Observability</b>	Section name
StreamingDataClient	Enables telemetry data to be sent to Microsoft.
EULocation	Location of your cluster. The log and diagnostic data is sent to the appropriate diagnostics servers depending upon where your cluster resides. Setting this to <code>false</code> results in all data sent to Microsoft to be stored outside of the EU.
EpisodicDataUpload	When set to <code>true</code> , collects log data to facilitate quicker issue resolution.
<b>Cluster</b>	Section name
Name	The cluster name provided when preparing Active Directory.
StaticAddress	This value is not used during deployment and will be removed in future releases.

Setting	Description
WitnessType	<p>Specify the witness type as <code>cloud</code> or local <code>fileshare</code> for your Azure Stack HCI cluster.</p> <p>Use a cloud witness if you have internet access and if you use an Azure Storage account to provide a vote on cluster quorum. A cloud witness uses Azure Blob Storage to read or write a blob file and then uses it to arbitrate in split-brain resolution. For more information on cloud witness, see <a href="#">Deploy a cloud witness for Failover cluster</a>.</p> <p>Use a file share witness if you use a local SMB file share to provide a vote in the cluster quorum. You should also use a file share witness if all the servers in a cluster have spotty internet connectivity or can't use disk witness as there aren't any shared drives.</p>
WitnessPath	Specify the fileshare path for the local witness for your Azure Stack HCI cluster.
CloudAccountName	Specify the Azure Storage account name for cloud witness for your Azure Stack HCI cluster.
AzureServiceEndpoint	For Azure blob service endpoint type, select either <b>Default</b> or <b>Custom domain</b> . If you selected <b>**Custom domain</b> , enter the domain for the blob service in this format <code>core.windows.net</code> .
Storage	Section name
ConfigurationMode	By default, this mode is set to <code>Express</code> and your storage is configured as per best practices based on the number of nodes in the cluster. For more information, see step <a href="#">4. 1 Set up cluster storage in Deploy Azure Stack HCI interactively</a> .
OptionalServices	Section name
VirtualSwitchName	This value is not used during deployment and will be removed in future releases.
CSVPath	This value is not used during deployment and will be removed in future releases.
ARBRegion	This value is not used during deployment and will be removed in future releases.
ActiveDirectorySettings	Section name

Setting	Description
NamingPrefix	The prefix used for all AD objects created for the Azure Stack HCI deployment. The prefix must not exceed eight characters.
DomainFQDN	The fully qualified domain name (FQDN) for the Active Directory domain used by your cluster.
ExternalDomainFQDN	This value is not used during deployment and will be removed in future releases.
ADOUPath	The path to the Active Directory Organizational Unit (ADOU) container object prepared for the deployment. Format must be that for a distinguished name (including domain components). For example: "OU=OUName,DC=contoso,DC=com".
DNSForwarder	Name of the server used to forward DNS queries for external DNS names. This value is not used during deployment and will be removed in future releases.
InfrastructureNetwork	Section name
VlanId	Only supported value in version 2210 is 0.
SubnetMask	Subnet mask that matches the provided IP address space.
Gateway	Default gateway that should be used for the provided IP address space.
IP Pools	Range of IP addresses from which addresses are allocated for nodes within a subnet.
StartingAddress	Starting IP address for the management network. A minimum of six free, contiguous IPv4 addresses (excluding your host IPs) are needed for infrastructure services such as clustering.
EndingAddress	Ending IP address for the management network. A minimum of six free, contiguous IPv4 addresses (excluding your host IPs) are needed for infrastructure services such as clustering.

Setting	Description
DNSServers	IPv4 address of the DNS servers in your environment. DNS servers are required as they're used when your server attempts to communicate with Azure or to resolve your server by name in your network. The DNS server you configure must be able to resolve the Active Directory domain.
PhysicalNodes	Section name
Name	NETBIOS name of each physical server on your Azure Stack HCI cluster.
IPv4Address	The IPv4 address assigned to each physical server on your Azure Stack HCI cluster.
HostNetwork	Section name
Intents	The network intents assigned to the network reference pattern used for the deployment. Each intent will define its own name, traffic type, adapter names, and overrides as recommended by your OEM.
Name	Name of the network intent you wish to create.
TrafficType	Type of network traffic. Examples include compute, storage, and management traffic.
Adapter	Array of network interfaces used for the network intent.
OverrideVirtualSwitchConfigurationOverrides	This parameter should only be modified based on your OEM guidance. Do not modify this parameter without OEM validation.
OverrideQoSPolicy	This parameter should only be modified based on your OEM guidance. Do not modify this parameter without OEM validation.
QoSPolicyOverrides	List of QoS policy overrides as specified by your OEM. Do not modify this parameter without OEM validation.
PriorityValue8021Action_Cluster	This parameter should only be modified based on your OEM guidance. Do not modify this parameter without OEM validation.

Setting	Description
PriorityValue8021Action_SMB	This parameter should only be modified based on your OEM guidance. Do not modify this parameter without OEM validation.
BandwidthPercentage_SMB	This parameter should only be modified based on your OEM guidance. Do not modify this parameter without OEM validation.
OverrideAdapterProperty	This parameter should only be modified based on your OEM guidance. Do not modify this parameter without OEM validation.
AdapterPropertyOverrides	List of adapter property overrides as specified by your OEM. Do not modify this parameter without OEM validation.
JumboPacket	This parameter should only be modified based on your OEM guidance. Do not modify this parameter without OEM validation.
NetworkDirect	This parameter should only be modified based on your OEM guidance. Do not modify this parameter without OEM validation.
NetworkDirectTechnology	This parameter should only be modified based on your OEM guidance. Do not modify this parameter without OEM validation.
<b>StorageNetworks</b>	Section name
Name	Name of the storage network.
NetworkAdapterName	Name of the storage network adapter.
VlanID	ID specified for the VLAN storage network. This setting is applied to the network interfaces that route the storage and VM migration traffic. Network ATC uses VLANs 711 and 712 for the first two storage networks. Additional storage networks will use the next VLAN ID on the sequence.

## Next steps

- [Validate deployment.](#)
- If needed, [troubleshoot deployment.](#)



# Deploy Azure Stack HCI using PowerShell (preview)

Article • 07/25/2023

Applies to: Azure Stack HCI, Supplemental Package

In this article, learn how to deploy Azure Stack HCI using PowerShell. Before you begin the deployment, make sure to first install the operating system.

This deployment method uses an existing configuration file that you have modified for your environment.

There are two methods for authenticating your cluster: using a service principal name (SPN) or using multi-factor authentication (MFA).

## ❗ Important

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

## Prerequisites

Before you begin, make sure you have done the following:

- Satisfy the [prerequisites](#).
- Complete the [deployment checklist](#).
- Prepare your [Active Directory](#) environment.
- [Install Azure Stack HCI version 22H2](#) on each server.
- [Set up the first server](#) in your Azure Stack HCI cluster.

## Create the configuration file

Here's a sample configuration file (JSON format) you can modify, save, and use for deployment. One advantage to using your own configuration file is that more settings can be specified than are available when creating a file interactively. For descriptions of each setting, see the reference section later in this article.

JSON

```

{
  "Version": "10.0.0.0",
  "ScaleUnits": [
    {
      "DeploymentData": {
        "SecuritySettings": {
          "HVCIProtection": true,
          "DRTMProtection": true,
          "DriftControlEnforced": true,
          "CredentialGuardEnforced": true,
          "SMBSigningEnforced": true,
          "SMBClusterEncryption": false,
          "SideChannelMitigationEnforced": true,
          "BitlockerBootVolume": true,
          "BitlockerDataVolumes": true,
          "WDACEnforced": true
        },
        "Observability": {
          "StreamingDataClient": true,
          "EULocation": false,
          "EpisodicDataUpload": true
        },
        "Cluster": {
          "Name": "ms169154cluster",
          "WitnessType": "Cloud",
          "WitnessPath": "",
          "CloudAccountName": "myasestoragacct",
          "AzureServiceEndpoint": "core.windows.net"
        },
        "Storage": {
          "ConfigurationMode": "Express"
        },
        "NamingPrefix": "ms169",
        "DomainFQDN": "ASZ1PLab8.nttest.microsoft.com",
        "InfrastructureNetwork": [
          {
            "VlanId": "0",
            "SubnetMask": "255.255.248.0",
            "Gateway": "10.57.48.1",
            "IP Pools": [
              {
                "StartingAddress": "10.57.48.60",
                "EndingAddress": "10.57.48.66"
              }
            ],
            "DNSServers": [
              "10.57.50.90"
            ]
          }
        ],
        "PhysicalNodes": [
          {
            "Name": "ms169host",
            "IPv4Address": "10.57.51.224"
          }
        ]
      }
    ]
  ]
}

```

```

    },
    {
        "Name": "ms154host",
        "IPv4Address": "10.57.53.236"
    }
],
"HostNetwork": {
    "Intents": [
        {
            "Name": "Compute_Management",
            "TrafficType": [
                "Compute",
                "Management"
            ],
            "Adapter": [
                "Port2"
            ],
            "OverrideVirtualSwitchConfiguration": false,
            "VirtualSwitchConfigurationOverrides": {
                "EnableIov": "",
                "LoadBalancingAlgorithm": ""
            },
            "OverrideQoSPolicy": false,
            "QoSPolicyOverrides": {
                "PriorityValue8021Action_Cluster": "",
                "PriorityValue8021Action_SMB": "",
                "BandwidthPercentage_SMB": ""
            },
            "OverrideAdapterProperty": false,
            "AdapterPropertyOverrides": {
                "JumboPacket": "",
                "NetworkDirect": "",
                "NetworkDirectTechnology": ""
            }
        },
        {
            "Name": "Storage",
            "TrafficType": [
                "Storage"
            ],
            "Adapter": [
                "Port3",
                "Port4"
            ],
            "OverrideVirtualSwitchConfiguration": false,
            "VirtualSwitchConfigurationOverrides": {
                "EnableIov": "",
                "LoadBalancingAlgorithm": ""
            },
            "OverrideQoSPolicy": false,
            "QoSPolicyOverrides": {
                "PriorityValue8021Action_Cluster": "",
                "PriorityValue8021Action_SMB": "",
                "BandwidthPercentage_SMB": ""
            }
        },
    ],
}

```

```

        "OverrideAdapterProperty": false,
        "AdapterPropertyOverrides": {
            "JumboPacket": "",
            "NetworkDirect": "",
            "NetworkDirectTechnology": ""
        }
    },
    ],
    "StorageNetworks": [
        {
            "Name": "Storage1Network",
            "NetworkAdapterName": "Port3",
            "VlanId": 5
        },
        {
            "Name": "Storage2Network",
            "NetworkAdapterName": "Port4",
            "VlanId": 5
        }
    ]
},
"ADOUPath":
"OU=ms169,DC=ASZ1PLab8,DC=nttest,DC=microsoft,DC=com"
}
}
]
}

```

## Prepare the configuration file

1. [Connect and sign in to the first server](#) in your Azure Stack HCI cluster as local administrator.
2. Review the [configuration file that you created previously](#) to ensure the provided values match your environment details before you copy it to the first server.
3. Copy the configuration file to the first server by using the following command:

PowerShell

```
Copy-Item -path <Path for your source file> -destination
C:\setup\config.json
```

## Get information for the required parameters

The following parameters are required to run the deployment tool. Consult your network administrator as needed for this information.

Parameter	Description
<code>JSONFilePath</code>	Enter the path to your config file. For example, <code>C:\setup\config.json</code> .
<code>AzureStackLCMUserCredential</code>	Specify the Active Directory account username. The username cannot be <i>Administrator</i> .
<code>LocalAdminCredential</code>	Specify the local administrator credentials.
<code>RegistrationCloudName</code>	Specify the cloud against which you'll authenticate your cluster. In this release, only the <code>AzureCloud</code> corresponding to global Azure is supported.
<code>RegistrationRegion</code>	(Optional) Specify the region that should be used when registering the system with Azure Arc.
<code>RegistrationResourceGroupName</code>	(Optional) Specify the resource group that will be used to hold the resource objects for the system.
<code>RegistrationResourceName</code>	(Optional) Specify the name used for the resource object of the Arc resource name for the cluster.
<code>RegistrationSubscriptionID</code>	Specify the ID for the subscription used to authenticate the cluster to Azure.
<code>RegistrationSPCredential</code>	Specify the credentials including the App ID and the secret for the Service Principal used to authenticate the cluster to Azure.
<code>RegistrationAccountCredential</code>	(Optional for MFA) Specify a credential object which is used to authenticate the Azure subscription. This is an alternative to using a service principal for authentication.
<code>RegistrationArcServerResourceGroupName</code>	(Optional for MFA) Specify a dedicated resource group for the Arc for server objects. This allows separate resource groups between Arc for Servers and Azure Stack HCI clusters.
<code>WitnessStorageKey</code>	Specify the access key for the Azure Storage account used for cloud witness for your Azure Stack HCI cluster.

## Run the deployment tool using a service principal

If you are using a service principal name to authenticate your cluster, use the following steps to deploy Azure Stack HCI via PowerShell.

For more information on creating a service principal, see [Create an Azure service principal with Azure PowerShell](#) and [Create an Azure Active Directory application and service principal that can access resources](#).

1. Connect to the first server in your Azure Stack HCI cluster using Remote Desktop Protocol (RDP).
2. Use option 15 in Server Configuration tool (SConfig) to exit to command line.
3. In the PowerShell window, change the directory to *C:\clouddeployment\setup*.
4. Set the following parameters:

PowerShell

```
$AzureStackLCMUserCred=Get-Credential
$LocalAdminCred=Get-Credential
$SubscriptionID="<Your subscription ID>"
$CloudName="AzureCloud"
$SPNAppID = "<Your App ID>"
$SPNSecret= "<Your SPN Secret>"
$SPNsecStringPassword = ConvertTo-SecureString $SPNSecret -AsPlainText -Force
$SPNCred = New-Object System.Management.Automation.PSCredential
($SPNAppID, $SPNsecStringPassword)
$AzureStorAcctAccessKey = ConvertTo-SecureString '<Azure Storage
account access key in plain text>' -AsPlainText -Force
```

5. Specify the path to your configuration file and run the following command to start the deployment:

PowerShell

```
.\Invoke-CloudDeployment -JSONFilePath <path_to_config_file.json> -
AzureStackLCMUserCredential $AzureStackLCMUserCred -
LocalAdminCredential -$LocalAdminCred -RegistrationSPCredential
$SPNCred -RegistrationCloudName $CloudName -RegistrationSubscriptionID
$SubscriptionID -WitnessStorageKey $AzureStorAcctAccessKey
```

## Run the deployment tool using MFA

If you are using multi-factor authentication (MFA) to authenticate your cluster, complete the following steps to deploy Azure Stack HCI using PowerShell. This method requires a second server in your cluster that has a browser to complete authentication.

1. Connect to the first server in your Azure Stack HCI cluster using Remote Desktop Protocol (RDP).
2. Use option 15 in Server Configuration tool (SConfig) to exit to command line.
3. In the PowerShell window, change the directory to *C:\clouddeployment\setup*.
4. Run the following to import the registration module and configure authentication:

PowerShell

```
$SubscriptionID="<your_subscription_ID>"  
Set-AuthenticationToken -RegistrationCloudName AzureCloud -  
RegistrationSubscriptionID $SubscriptionID
```

5. From a second server in your cluster that has a browser installed, open the browser and navigate to <https://microsoft.com/devicelogin>.
6. Copy the authentication code that is displayed and complete the authentication request.
7. On the first server, start the deployment using PowerShell and run the following command:

PowerShell

```
$DomainCred=Get-Credential  
$LocalCred=Get-Credential  
$AzureStorAcctAccessKey = ConvertTo-SecureString  
'<Azure_Storage_account_access_key_for_cluster_witness_in_plain_text>'  
-AsPlainText -Force  
Invoke-CloudDeployment -JSONFilePath <path_to_config_file.json> -  
AzureStackLCMUserCredential $DomainCred -LocalAdminCredential  
$LocalCred -WitnessStorageKey $AzureStorAcctAccessKey
```

## Reference: Configuration file settings

The following table gives descriptions for the settings listed in the configuration file:

Setting	Description
SecuritySettings	Section name
SecurityModeSealed	This parameter should only be modified based on your OEM guidance. Do not modify this parameter without OEM validation.

Setting	Description
SecuredCoreEnforced	This parameter should only be modified based on your OEM guidance. Do not modify this parameter without OEM validation.
VBSProtection	By default, Virtualization-based Security (VBS) is enabled on your Azure Stack HCI cluster. For more information, see <a href="#">Virtualization-based Security</a> .
HVCIProtection	By default, Hypervisor-protected Code Integrity (HVCI) is enabled on your Azure HCI cluster. For more information, see <a href="#">Hypervisor-protected Code Integrity</a> .
DRTMProtection	By default, Secure Boot is enabled on your Azure HCI cluster. This setting is hardware dependent. For more information, see <a href="#">Secure Boot with Dynamic Root of Trust for Measurement (DRTM)</a> .
KernelDMAProtection	By default, Pre-boot Kernel Direct Memory Access (DMA) protection is enabled on your Azure HCI cluster. This setting is hardware dependent. For more information, see <a href="#">Kernel Direct Memory Access protection</a> .
DriftControlEnforced	When set to <code>true</code> , the security baseline is re-applied regularly. For more information, see <a href="#">Security baseline settings for Azure Stack HCI</a> .
CredentialGuardEnforced	When set to <code>true</code> , Credential Guard is enabled. For more information, see <a href="#">Manage Windows Defender Credential Guard</a> .
SMBSigningEnforced	When set to <code>true</code> , the SMB default instance requires sign in for the client and server services. For more information, see <a href="#">Overview of Server Message Block signing</a> .
SMBClusterEncryption	When set to <code>true</code> , cluster east-west traffic is encrypted. For more information, see <a href="#">SMB encryption</a> .
SideChannelMitigationEnforced	When set to <code>true</code> , all the side channel mitigations are enabled, see <a href="#">KB4072698</a> .
BitLockerBootVolume	When set to <code>true</code> , BitLocker XTS_AES 256-bit encryption is enabled for all data-at-rest on the OS volume of your Azure Stack HCI cluster. This setting is TPM-hardware dependent. For more



Setting	Description
	information, see <a href="#">BitLocker encryption for Azure Stack HCI</a> .
BitLockerDataVolumes	When set to <code>true</code> , BitLocker XTS-AES 256-bit encryption is enabled for all data-at-rest on your Azure Stack HCI cluster shared volumes. For more information, see <a href="#">BitLocker encryption for Azure Stack HCI</a> .
SEDProtectionEnforced	Not used for Azure Stack HCI version 22H2.
WDACEnforced	Windows Defender Application Control (WDAC) is enabled by default and limits the applications and the code that you can run on your Azure Stack HCI cluster. For more information, see <a href="#">Windows Defender Application Control</a> .
<b>Observability</b>	Section name
StreamingDataClient	Enables telemetry data to be sent to Microsoft.
EULocation	Location of your cluster. The log and diagnostic data is sent to the appropriate diagnostics servers depending upon where your cluster resides. Setting this to <code>false</code> results in all data sent to Microsoft to be stored outside of the EU.
EpisodicDataUpload	When set to <code>true</code> , collects log data to facilitate quicker issue resolution.
<b>Cluster</b>	Section name
Name	The cluster name provided when preparing Active Directory.
StaticAddress	This value is not used during deployment and will be removed in future releases.
WitnessType	<p>Specify the witness type as <code>cloud</code> or local <code>fileshare</code> for your Azure Stack HCI cluster.</p> <p>Use a cloud witness if you have internet access and if you use an Azure Storage account to provide a vote on cluster quorum. A cloud witness uses Azure Blob Storage to read or write a blob file and then uses it to arbitrate in split-brain resolution. For more information on cloud witness, see <a href="#">Deploy a cloud witness for Failover cluster</a>.</p> <p>Use a file share witness if you use a local SMB file</p>

Setting	Description
	share to provide a vote in the cluster quorum. You should also use a file share witness if all the servers in a cluster have spotty internet connectivity or can't use disk witness as there aren't any shared drives.
WitnessPath	Specify the fileshare path for the local witness for your Azure Stack HCI cluster.
CloudAccountName	Specify the Azure Storage account name for cloud witness for your Azure Stack HCI cluster.
AzureServiceEndpoint	For Azure blob service endpoint type, select either <b>Default</b> or <b>Custom domain</b> . If you selected <b>**Custom domain</b> , enter the domain for the blob service in this format <code>core.windows.net</code> .
<b>Storage</b>	Section name
ConfigurationMode	By default, this mode is set to <code>Express</code> and your storage is configured as per best practices based on the number of nodes in the cluster. For more information, see step <a href="#">4. 1 Set up cluster storage in Deploy Azure Stack HCI interactively</a> .
<b>OptionalServices</b>	Section name
VirtualSwitchName	This value is not used during deployment and will be removed in future releases.
CSVPath	This value is not used during deployment and will be removed in future releases.
ARBRegion	This value is not used during deployment and will be removed in future releases.
<b>ActiveDirectorySettings</b>	Section name
NamingPrefix	The prefix used for all AD objects created for the Azure Stack HCI deployment. The prefix must not exceed eight characters.
DomainFQDN	The fully qualified domain name (FQDN) for the Active Directory domain used by your cluster.
ExternalDomainFQDN	This value is not used during deployment and will be removed in future releases.
ADOUPath	The path to the Active Directory Organizational Unit (ADOU) container object prepared for the

Setting	Description
	deployment. Format must be that for a distinguished name (including domain components). For example: "OU=OUName,DC=contoso,DC=com".
DNSForwarder	Name of the server used to forward DNS queries for external DNS names. This value is not used during deployment and will be removed in future releases.
InfrastructureNetwork	Section name
VlanId	Only supported value in version 2210 is 0.
SubnetMask	Subnet mask that matches the provided IP address space.
Gateway	Default gateway that should be used for the provided IP address space.
IP Pools	Range of IP addresses from which addresses are allocated for nodes within a subnet.
StartingAddress	Starting IP address for the management network. A minimum of six free, contiguous IPv4 addresses (excluding your host IPs) are needed for infrastructure services such as clustering.
EndingAddress	Ending IP address for the management network. A minimum of six free, contiguous IPv4 addresses (excluding your host IPs) are needed for infrastructure services such as clustering.
DNSServers	IPv4 address of the DNS servers in your environment. DNS servers are required as they're used when your server attempts to communicate with Azure or to resolve your server by name in your network. The DNS server you configure must be able to resolve the Active Directory domain.
PhysicalNodes	Section name
Name	NETBIOS name of each physical server on your Azure Stack HCI cluster.
IPv4Address	The IPv4 address assigned to each physical server on your Azure Stack HCI cluster.
HostNetwork	Section name

Setting	Description
Intents	The network intents assigned to the network reference pattern used for the deployment. Each intent will define its own name, traffic type, adapter names, and overrides as recommended by your OEM.
Name	Name of the network intent you wish to create.
TrafficType	Type of network traffic. Examples include compute, storage, and management traffic.
Adapter	Array of network interfaces used for the network intent.
OverrideVirtualSwitchConfigurationOverrides	This parameter should only be modified based on your OEM guidance. Do not modify this parameter without OEM validation.
OverrideQoSPolicy	This parameter should only be modified based on your OEM guidance. Do not modify this parameter without OEM validation.
QoSPolicyOverrides	List of QoS policy overrides as specified by your OEM. Do not modify this parameter without OEM validation.
PriorityValue8021Action_Cluster	This parameter should only be modified based on your OEM guidance. Do not modify this parameter without OEM validation.
PriorityValue8021Action_SMB	This parameter should only be modified based on your OEM guidance. Do not modify this parameter without OEM validation.
BandwidthPercentage_SMB	This parameter should only be modified based on your OEM guidance. Do not modify this parameter without OEM validation.
OverrideAdapterProperty	This parameter should only be modified based on your OEM guidance. Do not modify this parameter without OEM validation.
AdapterPropertyOverrides	List of adapter property overrides as specified by your OEM. Do not modify this parameter without OEM validation.
JumboPacket	This parameter should only be modified based on your OEM guidance. Do not modify this parameter without OEM validation.

Setting	Description
NetworkDirect	This parameter should only be modified based on your OEM guidance. Do not modify this parameter without OEM validation.
NetworkDirectTechnology	This parameter should only be modified based on your OEM guidance. Do not modify this parameter without OEM validation.
<b>StorageNetworks</b>	Section name
Name	Name of the storage network.
NetworkAdapterName	Name of the storage network adapter.
VlanID	ID specified for the VLAN storage network. This setting is applied to the network interfaces that route the storage and VM migration traffic. Network ATC uses VLANs 711 and 712 for the first two storage networks. Additional storage networks will use the next VLAN ID on the sequence.

## Next steps

- [Validate deployment.](#)
- If needed, [troubleshoot deployment.](#)

# Deploy Azure Stack HCI using non-native VLAN ID for the management network (preview)

Article • 05/10/2023

Applies to: Azure Stack HCI, Supplemental Package

When you deploy Azure Stack HCI using an existing configuration file, by default, a native VLAN ID 0 is used for the management network. However, in some specific scenarios, you may need to use a non-native VLAN ID for the management network.

This article describes how to deploy Azure Stack HCI using a non-native VLAN ID for the management network. This deployment method uses an existing configuration file that you have modified for your environment. For the default deployment scenario using a native VLAN ID, see [Deploy Azure Stack HCI using an existing configuration file \(preview\)](#).

## Prerequisites

Before you begin, make sure you've done the following:

- Satisfy the [prerequisites](#).
- Complete the [deployment checklist](#).
- Prepare your [Active Directory](#) environment.
- [Install version 22H2](#) on each server.
- [Set up the first server](#) in your Azure Stack HCI cluster.

## Deployment workflow

Here are the high-level steps to deploy Azure Stack HCI by using a non-native VLAN ID for the management network:

- [Create a virtual switch on every server in the cluster using the recommended naming convention](#).
- [Configure the management virtual network adapter on every server in the cluster using the required naming convention](#).
- [Configure the required VLAN ID to the management virtual network adapter on every server in the cluster](#).

- [Deploy Azure Stack HCI using the configuration file.](#)

## Create virtual switches using the recommended naming conventions

Azure Stack HCI with Supplemental Package deployment relies on Network ATC to create and configure the virtual switches and virtual network adapters for management, compute, and storage intents. By default, when Network ATC creates the virtual switch for the intents, it uses a specific name for the virtual switch. Although it is not required, we recommend to name your virtual switches with the same naming convention.

Here are the recommended naming conventions for the virtual switches:

Format for the virtual switch name: `"ConvergedSwitch($IntentName)"`

where:

- The name is case-sensitive.
- `$IntentName` inside the parenthesis can be any string you want, preferably indicating the intent type. This string should match the management virtual network adapter name as described later, in the [Configure the management virtual network adapter using the required naming conventions](#) section.

**Example:** The following example shows how to create a virtual switch using the recommended naming convention. Here you create a virtual switch, `ConvergedSwitch(MgmtCompute)` for management and compute traffic types by using two physical network adapters, `NIC1` and `NIC2`. Note the list of network adapter names must be the list of physical network adapters that you plan to use for the management and compute network traffic types.

PowerShell

```
$IntentName = "MgmtCompute"
New-VMSwitch -Name "ConvergedSwitch($IntentName)" -NetAdapterName
"NIC1","NIC2" -EnableEmbeddedTeaming $true -AllowManagementOS $false
```

## Configure the management virtual network adapter using the required naming conventions

After you create the virtual switch, configure the management virtual network adapter on every server in the cluster.

Here are required naming conventions for the virtual network adapter used for the management traffic:

Format for the management virtual network adapter name: `"vManagement($IntentName)"`

where:

- The name is case-sensitive.
- `$IntentName` inside the parenthesis must match the string that you used for the virtual switch.

**Example:** The following example shows how to update the name of the management virtual network adapter:

PowerShell

```
$IntentName = "MgmtCompute"
Add-VMNetworkAdapter -ManagementOS -SwitchName
"ConvergedSwitch($IntentName)" -Name "vManagement($IntentName)"

#NetAdapter needs to be renamed because during creation, Hyper-V adds the
string "vEthernet " to the beginning of the name

Rename-NetAdapter -Name "vEthernet (vManagement($IntentName))" -NewName
"vManagement($IntentName)"
```

## Configure the required VLAN ID to the management virtual network adapter

After you create the virtual switch and the management virtual network adapter, specify the required VLAN ID for this adapter by using the `Set-VMNetworkAdapterIsolation` cmdlet.

### Important

Although there are multiple ways to assign a VLAN ID to a virtual network adapter, we support using the `Set-VMNetworkAdapterIsolation` cmdlet only.



**Example:** The following example shows how to configure the management virtual network adapter to use VLAN ID 8 instead of the native VLAN ID 0.

PowerShell

```
Set-VMNetworkAdapterIsolation -ManagementOS -VMNetworkAdapterName  
"vManagement($IntentName)" -AllowUntaggedTraffic $true -IsolationMode Vlan -  
DefaultIsolationID 8
```

After you configure the required VLAN ID, assign an IP address and gateways to the management virtual network adapter. This verifies that the virtual network adapter has connectivity with other servers, DNS, Active Directory, and internet.

## Deploy Azure Stack HCI using the configuration file

After you finish configuring the networking elements on all the servers, you're ready to deploy Azure Stack HCI using a configuration file that you have modified for your environment. For information about how to create the configuration file and then run the deployment, see [Deploy Azure Stack HCI using an existing configuration file \(preview\)](#).

The following example shows a snippet of the `HostNetwork` configuration section within the configuration file, where the management and compute intent is defined to use the two physical network adapters assigned for these traffic types. There's no reference to the management virtual network adapters created in the previous steps because the deployment tool keeps the network configuration as-is, including the VLAN ID.

JSON

```
"HostNetwork": {  
  "Intents": [  
    {  
      "Name": "MgmtCompute",  
      "TrafficType": [  
        "Management",  
        "Compute"  
      ],  
      "Adapter": [  
        "NIC1",  
        "NIC2"  
      ],  
      "OverrideVirtualSwitchConfiguration": false,  
      "OverrideQoSPolicy": false,  
      "QoSPolicyOverrides": {
```

```

        "PriorityValue8021Action_Cluster": "7",
        "PriorityValue8021Action_SMB": "3",
        "BandwidthPercentage_SMB": "50%"
    },
    "OverrideAdapterProperty": false,
    "AdapterPropertyOverrides": {
        "JumboPacket": "",
        "NetworkDirect": "",
        "NetworkDirectTechnology": ""
    }
},
{
    "Name": "Storage",
    "TrafficType": [
        "Storage"
    ],
    "Adapter": [
        "NIC3",
        "NIC4"
    ],
    "OverrideVirtualSwitchConfiguration": false,
    "OverrideQoSPolicy": false,
    "QoSPolicyOverrides": {
        "PriorityValue8021Action_Cluster": "7",
        "PriorityValue8021Action_SMB": "3",
        "BandwidthPercentage_SMB": "50%"
    },
    "OverrideAdapterProperty": false,
    "AdapterPropertyOverrides": {
        "JumboPacket": "",
        "NetworkDirect": "Enabled",
        "NetworkDirectTechnology": "iWARP"
    }
}
],
"StorageNetworks": [
    {
        "Name": "RDMA1",
        "NetworkAdapterName": "NIC3",
        "VlanId": 711
    },
    {
        "Name": "RDMA2",
        "NetworkAdapterName": "NIC4",
        "VlanId": 712
    }
]
},

```

## Next steps

- [Validate deployment.](#)

- If needed, [troubleshoot deployment](#).

# Deploy a virtual Azure Stack HCI cluster (preview)

Article • 07/11/2023

Applies to: Azure Stack HCI, Supplemental Package

## Important

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

This article describes how to deploy a single-server or multi-node Azure Stack HCI, version 22H2, on a host system running Hyper-V on the Windows Server 2022, Windows 11, or later operating system (OS).

You'll need administrator privileges for the Azure Stack HCI virtual deployment and be familiar with the existing Azure Stack HCI solution. The deployment can take around 2.5 hours to complete.

## Important

A virtual deployment of Azure Stack HCI, version 22H2 is intended for educational and demonstration purposes only. Microsoft Support doesn't support virtual deployments.

## Prerequisites

Here are the software, hardware, and networking prerequisites for the virtual deployment:

## Hardware requirements

Before you begin, make sure that:

- You have access to a host system running Hyper-V on Windows Server 2022, Windows 11, or later. This host would be used to provision a virtual Azure Stack HCI deployment.

- The physical hardware used for the virtual deployment meets the following requirements:

Component	Minimum
Processor	Intel VT-x or AMD-V. Support for nested virtualization. For more information, see <a href="#">Does My Processor Support Intel® virtualization technology?</a> .
Memory	A minimum of 32 GB RAM.
Host network adapters	A single network adapter
Storage	1 TB Solid state drive (SSD)

## Software requirements

Before you begin, make sure that the host system can dedicate the following resources to provision your virtualized Azure Stack HCI. The host operating system must be running Hyper-V on Windows Server 2022, Windows 11, or later.

- A minimum of 4 vCPUs.
- At least 8 GB of RAM.
- At least two network adapters connected to the internal network with MAC, spoofing-enabled.
- At least one boot disk to [install the Azure Stack HCI operating system](#).
- At least six hard disks with a maximum size of 1024 GB for Storage Spaces Direct.
- At least one data disk with 127 GB to store the deployment tool.

## Install the OS

Before you begin, make sure to [install the host operating system](#) - Windows Server 2022, Windows 11, or later.

## Set up the virtual switch

First, create an internal virtual switch with Network Address Translation (NAT) enabled. The use of this switch ensures that the Azure Stack HCI deployment is isolated.

1. On your host computer, run PowerShell as Administrator.
2. Create an internal virtual switch and name the switch *InternalDemo*. Run the following command:

PowerShell

```
New-VMSwitch -SwitchName "InternalDemo" -SwitchType Internal
```

3. Find the interface index of the virtual switch you just created. Use the `Get-NetAdapter` cmdlet to find the interface index:

PowerShell

```
Get-NetAdapter
```

Here is a sample output of the `Get-NetAdapter` cmdlet.

PowerShell

```
PS C:\Users\Administrator> Get-NetAdapter
```

Name	InterfaceDescription	ifIndex	MacAddress	LinkSpeed
vEthernet (InternalDemo)	Hyper-V Virtual Ethernet...	20	Up	00-15-5D-E2-3E-00 10 Gbps
vEthernet (Intel(R) Ethernet Hyper-V Virtual Ethernet	96-E0-69-2F 1 Gbps	9	Up	98-90-
Ethernet (Intel(R) Ethernet	5 Up	98-90-96-E0-69-2F	1 Gbps	
Ethernet 2 ASIX AX88772 USB2.0 to ...	3 Up	00-50-B6-58-05-4A	100 Mbps	

4. From the output of the `Get-NetAdapter` cmdlet, find the adapter that includes the virtual switch name you created in the earlier step. Make a note of the `ifIndex` corresponding to the virtual switch. In the above example, the `ifIndex` is 20.
5. Create the NAT gateway. Provide the NAT gateway IP address, NAT subnet prefix length, and the interface index you determined in the previous step:

PowerShell

```
New-NetIPAddress -IPAddress 192.168.0.1 -PrefixLength 24 -InterfaceIndex <ifIndex from previous step>
```

6. Configure the NAT gateway. Provide a name to describe the name of the NAT network and 192.168.0.0/24 as the NAT subnet prefix:

PowerShell

```
New-NetNat -Name <NAT network name> -  
InternalIPInterfaceAddressPrefix 192.168.0.0/24
```

## Create the virtual host

Create a virtual machine (VM) to serve as the virtual host with the following configuration:

Component	Requirement
Virtual machine type	Secure Boot and Trusted Platform Module (TPM) enabled.
vCPUs	4 cores
Memory	A minimum of 8 GB
Networking	Two network adapters connected to internal network. MAC spoofing must be enabled.
Boot disk	1 disk to install the Azure Stack HCI operating system from ISO.
Hard disks for Storage Spaces Direct	6 dynamic expanding disks. Maximum disk size is 1024 GB.
Data disk	At least 127 GB. Stores the deployment tool.
Time synchronization in integration services	Disabled

You can create this VM using one of the following methods:

- **Use Hyper-V Manager.** For more information, see [Create a virtual machine using Hyper-V Manager](#) to mirror your physical management network.
- **Use PowerShell cmdlets.** Use PowerShell cmdlets to create the VM. Make sure to adjust the VM configuration parameters listed above before you run these cmdlets. For an example output, see the [Appendix](#).

Follow these steps to create a VM via PowerShell cmdlets:

1. Create the VM:

PowerShell

```
new-VHD -Path -SizeBytes 127GB  
New-Vm -Name -MemoryStartupBytes 16GB -VHDPATH -Generation 2 -Path
```

2. Add a second network adapter:

PowerShell

```
Add-VmNetworkAdapter -VmName <VM name>
```

3. Attach both adapters to the virtual switch:

PowerShell

```
Get-VmNetworkAdapter -VmName <VM Name> | Connect-VmNetworkAdapter -  
SwitchName <Internal virtual switch name>
```

4. Enable MAC spoofing on both adapters:

PowerShell

```
Get-VmNetworkAdapter -VmName <VM name> | Set-VmNetworkAdapter -  
MacAddressSpoofing On
```

5. Enable the trunk port (for multi-node deployments only):

PowerShell

```
Get-VmNetworkAdapter -VmName <VM name> | Set-VmNetworkAdapterVlan -  
Trunk -NativeVlanId 0 -AllowedVlanIdList 0-1000
```

6. Enable Trusted Platform Module (TPM):

PowerShell

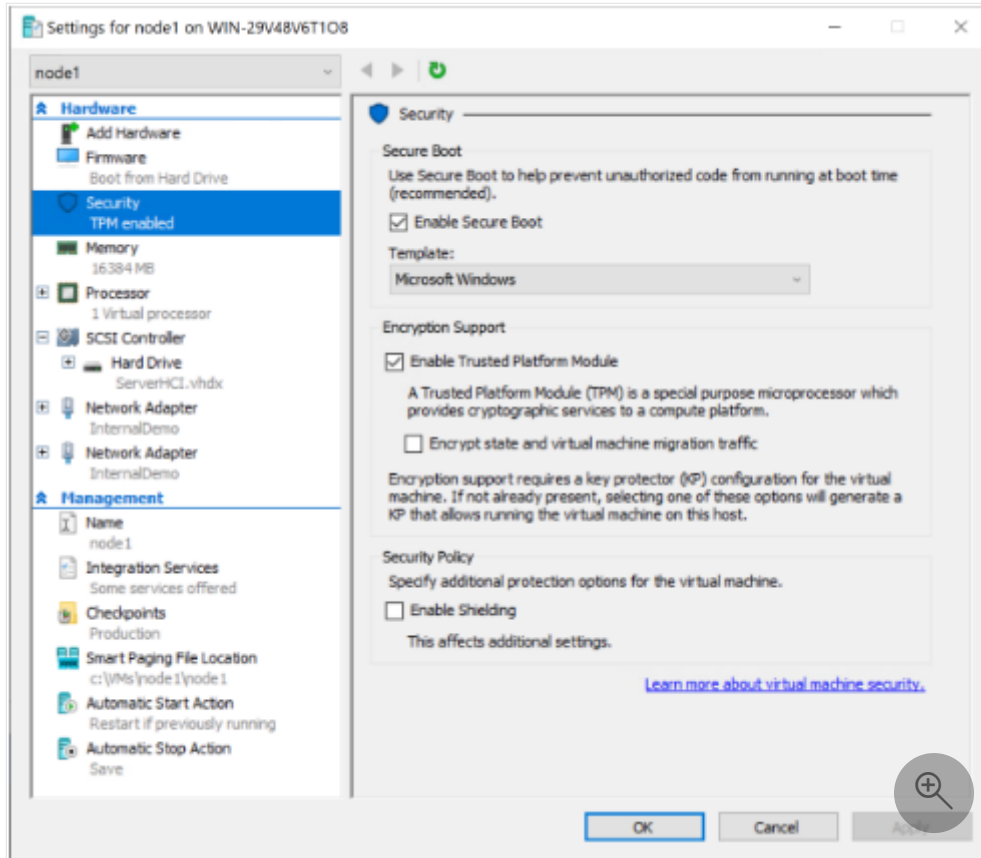
```
Enable-VmTpm -VmName <VM name>
```

If the above step fails, you must enable TPM using Hyper-V Manager as follows:

a. In Hyper-V Manager, select the VM, right-click, and from the context menu, select **Settings**.



- b. Go to **Hardware > Security** and then select the **Enable Trusted Platform Module** option:



7. Change the number of virtual processors to 4:

PowerShell

```
Set-VmProcessor -VmName <VM name> -Count 4
```

8. Create additional drives to be used as the boot disk and hard disks for Storage Spaces Direct:

PowerShell

```
new-VHD -Path <Path to data.vhdx file> -SizeBytes 127GB
new-VHD -Path <Path to s2d1.vhdx file> -SizeBytes 1024GB
new-VHD -Path <Path to s2d2.vhdx file> -SizeBytes 1024GB
new-VHD -Path <Path to s2d3.vhdx file> -SizeBytes 1024GB
new-VHD -Path <Path to s2d4.vhdx file> -SizeBytes 1024GB
new-VHD -Path <Path to s2d5.vhdx file> -SizeBytes 1024GB
new-VHD -Path <Path to s2d6.vhdx file> -SizeBytes 1024GB
```

9. Attach the drives:

PowerShell

```
Add-VMHardDiskDrive -VmName <VM Name> -Path <Path to data.vhdx file>
Add-VMHardDiskDrive -VmName <VM Name> -Path <Path to s2d1.vhdx file>
Add-VMHardDiskDrive -VmName <VM Name> -Path <Path to s2d2.vhdx file>
Add-VMHardDiskDrive -VmName <VM Name> -Path <Path to s2d3.vhdx file>
Add-VMHardDiskDrive -VmName <VM Name> -Path <Path to s2d4.vhdx file>
Add-VMHardDiskDrive -VmName <VM Name> -Path <Path to s2d5.vhdx file>
Add-VMHardDiskDrive -VmName <VM Name> -Path <Path to s2d6.vhdx file>
```

10. Disable time synchronization:

PowerShell

```
Get-VMIntegrationService -VmName node1 |Where-Object {$_.name - like "T*"}|Disable-VMIntegrationService
```

## Enable nested virtualization

If the host processor supports nested virtualization, the Hyper-V role enabled by the Azure Stack HCI deployment will validate.

To enable nested virtualization, run the following command.

PowerShell

```
Set-VmProcessor -VmName node1 -ExposeVirtualizationExtensions $true
```

## Configure NAT inbound rules (optional)

The configuration in this section is optional.

To access the server from your Hyper-V host or any other computer in your network, Network Address Translation (NAT) inbound rules are required.

1. Create the following inbound rules:

Protocol	Port	Description
Remote Desktop Protocol (RDP)	3389	Access the server via Remote Desktop protocol (RDP)
Deployment tool UI	443	Access to the web-based UI for the deployment tool

2. Enable port mapping from port 53389 to 3389. Run the following command:

PowerShell

```
Add-NetNatStaticMapping -NatName MyNATnetwork -ExternalIPAddress 0.0.0.0 -InternalIPAddress 192.168.0.92 -Protocol TCP -ExternalPort 53389 -InternalPort 3389
```

3. Enable port mapping from port 5443 to 443. Run the following command:

PowerShell

```
Add-NetNatStaticMapping -NatName MyNATnetwork -ExternalIPAddress 0.0.0.0 -InternalIPAddress 192.168.0.92 -Protocol TCP -ExternalPort 5443 -InternalPort 443
```

You may receive the following error: *Add-NetNatStaticMapping: The process cannot access the file because it is being used by another process.* To resolve this, change the external port as the one you are trying to use is already allocated.

## Start the deployment

1. Start the virtual host VM using Hyper-V Manager or PowerShell. The VM will take several minutes to boot up. Wait for the boot to complete.

PowerShell

```
Start-Vm <node1>
```

2. [Install the HCI operating system.](#)
3. Update the password since this is the first VM start up.
4. After the password is changed, `Sconfig` is automatically loaded. Select option `15` to exit to the command line and run the next steps from there.

5. Initialize the data disk to store the deployment tool. Ensure that the data disk is assigned the drive letter **D**. Run the following commands from the virtual server:

PowerShell

```
Set-disk 1 -isOffline $false
Set-Disk 1 -isReadOnly $false
Initialize-Disk 1 -PartitionStyle GPT
New-Partition -DiskNumber 1 -UseMaximumSize
Get-Partition -DiskNumber 1 -PartitionNumber 2 | Format-Volume -
FileSystem NTFS
Get-Partition -DiskNumber 1 -PartitionNumber 2 | Set-Partition -
NewDriveLetter D
```

6. Connect to the Windows Server host from the VM and when prompted, provide the credentials:

PowerShell

```
net use \\<Windows Server host IP or FQDN>\C$
```

7. Copy the **cloud** folder that contains the deployment tool from Windows Server to the VM:

PowerShell

```
copy \\<Network path to folder containing deployment tool on Windows
Server> <Destination path on VM on D: drive> -r`
```

Verify that the tool was copied over. Examine the contents of the **cloud** folder.

Here is a sample output:

```
PS C:\Users\Administrator> net use \\WIN-29V48V6T108\C$

Enter the user name for 'WIN-29V48V6T108': <Username>
Enter the password for WIN-29V48V6T108:<Password>
The command completed successfully.
PS C:\Users\Administrator> copy \\WIN-
29V48V6T108\C$\Users\Administrator\Cloud D:\deployment -r

PS C:\Users\Administrator> cd D:\deployment
PS D:\deployment> dir
Directory: D:\deployment
Mode                LastWriteTime         Length Name
----                -
-----
```

```
-a---- 6/28/2022 12:10 AM 18465
BootstrapCloudDeploymentTool.ps1
-a---- 6/28/2022 2:44 PM 21709 CloudDeployment.Metadata.xml
-a---- 6/28/2022 2:41 PM 11420824813
CloudDeployment_10.2206.0.50.zip
PS D:\deployment>
```

8. Launch the Server Configuration Tool (`SConfig`). Run the following command:

```
PowerShell
```

```
SConfig
```

For information on how to use `SConfig`, see [Configure a Server Core installation of Windows Server and Azure Stack HCI with the Server Configuration tool \(SConfig\)](#).

9. Change hostname to `node1`. Use option `2` for **Computer name** in `SConfig`.

The hostname change will result in a restart. When prompted for a restart, enter `yes` and wait for the restart to complete. `SConfig` is launched automatically.

10. Configure IP Address to `192.168.0.92`, subnet mask to `255.255.255.0`, and gateway to `192.168.0.1`. Configure a valid DNS server. Use option `8` for network settings in `SConfig`.

11. Use option `15` and exit to the command line.

12. Choose one of the following methods to deploy Azure Stack HCI:

a. Deploy interactively:

- Switch to the `D:` drive and install the deployment tool as per the instructions in [Step 3A: Deploy Azure Stack HCI interactively](#).
- Afterward, use the **deploy from file** option.

b. Deploy a single-server cluster using PowerShell as per the instructions in [Step 3C: Deploy Azure Stack HCI using PowerShell](#).

## Appendix

Here is an example output for VM creation:

```
PowerShell
```

```
PS C:\Users\Administrator> mkdir c:\users\administrator\vm1\node1
Directory: C:\users\administrator\vm1
```

```

Mode                LastWriteTime         Length Name
----                -
d----- 7/15/2022   9:51 AM node1
PS C:\Users\Administrator> Copy-item c:\users\administrator\image
c:\users\administrator\vm1\node1
PS C:\Users\Administrator> cd c:\users\administrator\vm1\node1
PS C:\users\administrator\vm1\node1> dir
    Directory: C:\users\administrator\vm1\node1
Mode                LastWriteTime         Length Name
----                -
d----- 7/15/2022   9:51 AM image
d----- 7/15/2022  10:54 AM myhcinode1
PS C:\Users\Administrator> new-vm -Name myhcinode1 -MemoryStartupBytes 16GB
-VHDPath
c:\users\administrator\vm1\node1\ServerHCI.vhdx -Generation 2 -Path
c:\users\administrator\vm1\node1

Name      State      CPUUsage(%)  MemoryAssigned (M)  Uptime  Status  Version
----      -
myhcinode1 Off  0              0  00:00:00  Operating normally  9.0

PS C:\Users\Administrator> add-vmnetworkadapter -VMName myhcinode1
PS C:\Users\Administrator> Get-VMNetworkAdapter -VMName myhcinode1 | Connect-
VMNetworkAdapter -SwitchName "InternalDemo"
PS C:\Users\Administrator> Get-VMNetworkAdapter -VMName myhcinode1 | Set-
VMNetworkAdapter -MacAddressSpoofing On
PS C:\Users\Administrator> Enable-VMTPM -VMName myhcinode1

```

## Next steps

- [Review deployment overview.](#)

# Validate Azure Stack HCI deployment (preview)

Article • 04/18/2023

Applies to: Azure Stack HCI, Supplemental Package

Once your deployment has successfully completed, you should verify and validate your deployment.

## Important

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

## Validate registration in Azure portal

The cluster registration completes before the deployment is complete. Follow these steps to validate that your cluster exists and is registered in Azure:

1. Establish a remote PowerShell session with the server node. Run PowerShell as administrator and run the following command:

PowerShell

```
Enter-PSSession -ComputerName <server_IP_address> -Credential  
<username\password for the server>
```

2. Get the information for the cluster you created:

PowerShell

```
Get-AzureStackHCI
```

Here is a sample output:

PowerShell

```
PS C:\Users\Administrator> Enter-PSSession -ComputerName 100.96.113.220  
-Credential localhost\administrator
```

```
[100.96.113.220]: PS C:\Users\Administrator\Documents> Get-
AzureStackHCI

ClusterStatus      : Clustered
RegistrationStatus  : Registered
RegistrationDate    : 7/6/2022 1:01:02 AM
AzureResourceName  : cluster-c0bca4ca3d654d689c7b624732af3727
AzureResourceUri   : /Subscriptions/<Subscription
ID>/resourceGroups/ASZRegistrationRG/providers/Microsoft.AzureStackHCI/
clusters/cluster-c0bca4ca3d654d689c7b624732af3727

ConnectionStatus   : Connected
LastConnected      : 7/6/2022 2:00:02 PM
IMDSAttestation    : Disabled
DiagnosticLevel     : Basic

[100.96.113.220]: PS C:\Users\Administrator\Documents>
```

3. Make a note of the `AzureResourceName` value. You'll need this to do a search in the Azure portal.
4. Sign in to the Azure portal. Make sure that you have used the appropriate Azure account ID and password.
5. In the Azure portal, search for the `AzureResourceName` value, then select the corresponding cluster resource.
6. On the **Overview** page for the cluster resource, view the **Server** information.

The screenshot displays the Azure portal interface for the 'mkclus90' Azure Stack HCI cluster. The left-hand navigation pane shows the 'Overview' tab selected. The main content area is divided into 'Essentials' and 'Servers' sections. The 'Essentials' section provides key cluster information, including the resource group, location, and subscription. The 'Custom location' field is highlighted with a red box, showing 'c104'. The 'Servers' section contains a table of servers, with the first two rows highlighted by a red box, indicating they are connected.

Server	Azure Arc	Manufacturer	Model	Serial number	Cores	Memory
RRN44-13-11	Connected	Dell Inc.	PowerEdge R730xd	9CRV482	20	128 GiB
RRN44-13-15	Connected	Dell Inc.	PowerEdge R730xd	9CRM482	20	128 GiB

## Validate deployment status

After the registration completes, more configuration is needed before the deployment is complete. Once the deployment is complete, remotely connect to the first server via PowerShell.



Follow these steps to verify that the deployment completed successfully:

1. Remotely connect to the first server via PowerShell.
2. Run the following command:

PowerShell

```
([xml](gc C:\ecestore\efb61d70-47ed-8f44-5d63-bed6adc0fb0f\086a22e3-ef1a-7b3a-dc9d-f407953b0f84)) | Select-Xml -XPath "//Action/Steps/Step" | ForEach-Object { $_.Node } | Select-Object FullStepIndex, Status, Name, StartTimeUtc, EndTimeUtc, @{Name="Durration";Expression={new-timespan -Start $_.StartTimeUtc -End $_.EndTimeUtc } } | ft -AutoSize
```

Here's a sample output of the above command:

Output

```
[10.57.51.224]: PS C:\Users\SetupUser\Documents> ([xml](gc C:\ecestore\efb61d70-47ed-8f44-5d63-bed6adc0fb0f\086a22e3-ef1a-7b3a-dc9d-f407953b0f84)) | Select-Xml -XPath "//Action/Steps/Step" | ForEach-Object { $_.Node } | Select-Object FullStepIndex, Status, Name, StartTimeUtc, EndTimeUtc, @{Name="Durration";Expression={new-timespan -Start $_.StartTimeUtc -End $_.EndTimeUtc } } | ft -AutoSize
```

FullStepIndex	Status	Name
Start Time UTC		End Time UTC
-----	-----	-----
-----		---
0	InProgress	Cloud Deployment
2022-09-27T17:23:45.364122Z		
0.1	Success	Before Cloud Deployment
2022-09-27T17:23:54.7859298Z		202
0.1.1	Success	Parallel per-node operation top step
2022-09-27T17:23:54.8328431Z		202
0.1.1.1	Success	OS Configuration Customization
2022-09-27T17:23:54.9734933Z		202
0.1.1.1.10	Success	LiveUpdateWindowsFeatures
2022-09-27T17:23:55.0827964Z		202
0.1.1.1.20	Success	LiveUpdateRegistryKeys
2022-09-27T17:24:32.6803406Z		202
0.1.1.1	Success	OS Configuration Customization
2022-09-27T17:23:54.8797181Z		202
0.1.1.1.10	Success	LiveUpdateWindowsFeatures
2022-09-27T17:23:55.0359952Z		202
0.1.1.1.20	Success	LiveUpdateRegistryKeys
2022-09-27T17:24:47.7428392Z		202
0.1.2	Success	Restart the first server
2022-09-27T17:25:05.7069186Z		202
0.1.3	Success	EnvironmentValidatorFull
2022-09-27T17:26:22.7187521Z		202
0.1.3.0	Success	EnvironmentValidatorFull

2022-09-27T17:26:22.7500568Z 202  
0.1.4 Success Parallel per-node operation top step  
2022-09-27T17:29:28.1542484Z 202  
0.1.4.1 Success Expand Live Update Content  
2022-09-27T17:29:28.29485Z 202  
0.1.4.1 Success Expand Live Update Content  
2022-09-27T17:29:28.2323781Z 202  
0.1.5 Success EnableFirewallPortsOnAllHosts  
2022-09-27T17:33:04.3813397Z 202  
0.1.5.1 Success Parallel per-node operation top step  
2022-09-27T17:33:04.4594369Z 202  
0.1.5.1.1 Success EnableFirewallPorts  
2022-09-27T17:33:04.5375634Z 202  
0.1.5.1.1 Success EnableFirewallPorts  
2022-09-27T17:33:04.4906904Z 202  
0.1.6 Success ResizeSystemDriveOnAllHosts  
2022-09-27T17:33:21.9039183Z 202  
0.1.6.1 Success Parallel per-node operation top step  
2022-09-27T17:33:21.9664168Z 202  
0.1.6.1.1 Success ResizeSystemDrive  
2022-09-27T17:33:22.0757452Z 202  
0.1.6.1.1 Success ResizeSystemDrive  
2022-09-27T17:33:22.0132493Z 202  
0.1.7 Success AddDSCCertificateOnHost  
2022-09-27T17:33:45.8839415Z 202  
0.2 Success Validate network settings for servers  
2022-09-27T17:34:06.437572Z 202  
0.2.1 Success ValidateEceHostNetworkSettings  
2022-09-27T17:34:06.5157117Z 202  
0.3 Success Configure settings on servers  
2022-09-27T17:34:40.8861732Z 202  
0.3.1 Success ConfigureAzureStackHostsPreConfig  
2022-09-27T17:34:40.9642929Z 202  
0.4 Success AutoScale VirtualMachines  
2022-09-27T17:34:48.6407394Z 202  
0.5 Success Configure network settings on servers  
2022-09-27T17:34:48.8750632Z 202  
0.5.1 Success Configure host networking requirements  
2022-09-27T17:34:49.0469906Z 202  
0.6 Success Apply security settings on servers  
2022-09-27T17:45:05.4738632Z 202  
0.6.1 Success Parallel per-node operation top step  
2022-09-27T17:45:05.5363183Z 202  
0.6.1.1 Success Prepare SecurityBaseline Metadata  
2022-09-27T17:45:05.6301162Z 202  
0.6.1.2 Success Enforce SecurityBaseline  
2022-09-27T17:45:12.0051044Z 202  
0.6.1.3 Success Enforce SecuredCore  
2022-09-27T17:45:28.1903232Z 202  
0.6.1.4 Success Configure OSConfig DriftControl  
2022-09-27T17:45:33.5055734Z 202  
0.6.1.1 Success Prepare SecurityBaseline Metadata  
2022-09-27T17:45:05.5988827Z 202  
0.6.1.2 Success Enforce SecurityBaseline  
2022-09-27T17:45:13.8488529Z 202

0.6.1.3 Success Enforce SecuredCore  
2022-09-27T17:45:35.8024458Z 202

0.6.1.4 Success Configure OSConfig DriftControl  
2022-09-27T17:45:43.1461885Z 202

0.7 Success Join servers to a domain  
2022-09-27T17:45:50.3301693Z 202

0.7.1 Success Deploy AD and domain join physical machines  
2022-09-27T17:45:50.4082611Z 202

0.7.1.1 Success Add host to domain  
2022-09-27T17:45:52.0801302Z 202

0.8 Success Setup Observability Resources  
2022-09-27T17:50:42.4434854Z 202

0.8.0 Success Register Observability EventSource  
2022-09-27T17:50:42.5372373Z 202

0.8.1 Success Setup Observability Volume  
2022-09-27T17:51:00.9850708Z 202

0.8.2 Success Create Observability Subfolders and Quotas  
2022-09-27T17:52:27.9143979Z 202

0.8.3 Success Setup UTC Exporter Feature  
2022-09-27T17:52:48.8143452Z 202

0.8.4 Success Install VC Redistributable  
2022-09-27T17:53:11.2112825Z 202

0.8.5 Success Setup uptime scheduled task  
2022-09-27T17:53:26.8353426Z 202

0.8.6 Success Setup census event scheduled task  
2022-09-27T17:53:45.8745538Z 202

0.8.7 Success Setup registration events task  
2022-09-27T17:54:04.6852565Z 202

0.9 Success Deploy JEA endpoints on the host  
2022-09-27T17:54:23.5128828Z 202

0.9.1 Success Parallel per-node operation top step  
2022-09-27T17:54:23.5910102Z 202

0.9.1.1 Success Update Baremetal JEA endpoints  
2022-09-27T17:54:23.809761Z 202

0.9.1.2 Success Update Baremetal JEA endpoints  
2022-09-27T17:54:35.4347618Z 202

0.9.1.2.1 Success Update Baremetal JEA endpoints  
2022-09-27T17:54:35.497264Z 202

0.9.1.1 Success Update Baremetal JEA endpoints  
2022-09-27T17:54:23.6535075Z 202

0.9.1.2 Success Update Baremetal JEA endpoints  
2022-09-27T17:54:40.5128884Z 202

0.9.1.2.1 Success Update Baremetal JEA endpoints  
2022-09-27T17:54:40.5597627Z 202

0.10 Success ConfigCluster  
2022-09-27T17:58:04.5728561Z 202

0.10.1 Success ConfigCluster  
2022-09-27T17:58:04.6353789Z 202

0.11 Success Configure cluster networking requirements  
2022-09-27T18:00:47.4567973Z 202

0.11.1 Success Configure host networking requirements  
2022-09-27T18:00:47.5036695Z 202

0.12 Success Register with Azure  
2022-09-27T18:02:26.499692Z 202

0.12.1 Success RegisterStampToAzure

```

2022-09-27T18:02:26.5621888Z 202
0.13          Success    ConfigStorage
2022-09-27T18:09:53.6289174Z 202
0.13.1        Success    ConfigStorage
2022-09-27T18:09:53.7008911Z 202
0.14          Success    EncryptCSVs
2022-09-27T18:14:46.9273156Z 202
0.15          Success    EncryptHostsOSVolumes
2022-09-27T18:15:28.1432709Z 202
0.16          Success    MitigateForClusterGenericService
2022-09-27T18:15:37.6342017Z 202
0.17          Success    Set up certificates
2022-09-27T18:16:03.9038202Z 202
0.17.0        Success    Install ASCA and Set Up External Certificates
2022-09-27T18:16:03.9662569Z 202
0.17.0.0      Success    StageAndGenerateCertificates
2022-09-27T18:16:07.2006186Z 202
0.17.0.0.0    Success    Add lifecycle manager to certificate Readers
group         2022-09-27T18:16:07.2474936Z 202
0.17.0.0.1    Success    Generate certificates
2022-09-27T18:16:13.932161Z  202
0.17.0.0.2    Success    Remove lifecycle manager to certificate
Readers group 2022-09-27T18:16:47.5523932Z 202
0.17.0.0.3    Success    Publish artifacts
2022-09-27T18:16:50.7242697Z 202
0.18          Success    VM Prerequisites
2022-09-27T18:16:58.3648937Z
0.19          Success    Refresh Active Directory permissions
0.20          Success    Deploy Agent Lifecycle Manager
0.21          Success    Migrate deployment orchestrator service
0.22          Success    Apply WDAC on hosts
0.23          Success    CloudDeployment Expand
0.24          Success    Clean up temporary content
0.25          Success    Deploy the Network Controller service
0.26          Success    Enable SMB Encryption
0.27          Success    Apply security settings on infrastructure
services
0.28          Success    ScheduleTearDown

```

```
[10.57.51.224]: PS C:\Users\SetupUser\Documents>
```

## Validate cluster quorum settings

The cluster quorum should be configured to match the number of nodes in your cluster. We recommend setting up a cluster witness for clusters with two, three, or four nodes. The witness helps the cluster determine which nodes have the most up-to-date cluster data if some nodes can't communicate with the rest of the cluster. For more details, see [Configure the cluster quorum](#).

You can host the cluster witness on a file share located on another server. Follow these steps to create a file share witness:

1. Remotely connect via PowerShell to the first server of your Azure Stack HCI cluster.
2. To validate the cluster quorum configuration, run the following command:

PowerShell

```
Get-ClusterQuorum
```

## Next steps

- If needed, [troubleshoot deployment](#).

# Collect diagnostic logs

Article • 09/20/2023

Applies to: Azure Stack HCI, Supplemental Package; Azure Stack HCI, version 23H2 (preview)

This article describes how to collect diagnostic logs and send them to Microsoft to help identify and fix any issues with your Azure Stack HCI solution.

## Important

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

## Collect logs

Use the `Send-DiagnosticData` cmdlet from any Azure Stack HCI server node to manually collect and send diagnostic logs to Microsoft. When you run this cmdlet, the logs are temporarily copied locally. This copy is parsed, sent to Microsoft, and then deleted from your system. Microsoft retains this diagnostic data for up to 29 days and handles it as per the [standard privacy practices](#).

The `Send-DiagnosticData` cmdlet takes some time to complete based on which roles the logs are collecting, time duration specified, and the number of nodes in your Azure Stack HCI environment.

Here's the syntax of the `Send-DiagnosticData` cmdlet:

PowerShell

```
Send-DiagnosticData [[-FilterByRole] <string[]>] [[-FromDate] <datetime>]  
[[ -ToDate] <datetime>] [[-CollectSddc] <bool>] [<CommonParameters>]
```

where:

- `FromDate` and `ToDate` parameters collect logs for a particular time period. If these parameters aren't specified, logs are collected for the past one hour by default.

- `FilterByRole` parameter collects logs for each role. Currently, you can use the `FilterByRole` parameter to filter log collection by the following roles. This list of roles may change in a future release.
  - ALM
  - ArcAgent
  - AutonomousLogs
  - BareMetal
  - CommonInfra
  - DeploymentLogs
  - ECE
  - Extension
  - FleetDiagnosticsAgent
  - HCICloudService
  - DownloadService
  - Health
  - HostNetwork
  - MOC\_ARB
  - NC
  - ObservabilityAgent
  - ObservabilityLogmanTraces
  - ObservabilityVolume
  - OEMDiagnostics
  - OSUpdateLogs
  - RemoteSupportAgent
  - URP
- `CollectSddc` parameter is set to `$true` by default, which triggers the `Get-SDDCDiagnosticInfo` cmdlet and includes its logs as part of the log collection.

## Examples and sample outputs

Here are some example commands with sample outputs that show how to use the `Send-DiagnosticData` cmdlet with different parameters.

### Send diagnostics data with date filtering

In this example, you send diagnostics data with date filtering for log files for the past two hours:

```
PowerShell
```

```
Send-DiagnosticData -FromDate (Get-Date).AddHours(-2) -ToDate (Get-Date)
```

Here's a sample output of this command:

#### Output

```
PS C:\CloudDeployment\logs> Send-DiagnosticData -FromDate (Get-Date).AddHours(-2) -ToDate (Get-Date)
Successfully submitted on-demand. Operation tracking Id: ec0d1a53-f75b-4df5-afb8-cfbf6d4c8118
Current log collection status: Running
Waiting for log collection to complete...
==== CUT ===== CUT =====
Log collection ended with status: Succeeded
PS C:\CloudDeployment\logs>
```

## Send diagnostic data with role filtering

In this example, you send diagnostic data with role filtering for BareMetal and ECE:

#### PowerShell

```
Send-DiagnosticData -FilterByRole BareMetal, ECE
```

Here's a sample output of this command:

#### Output

```
PS C:\Users\docsuser> Send-DiagnosticData -FilterByRole BareMetal, ECE
FromDate parameter not specified. Setting to default value 09/27/2022
17:13:38
ToDate parameter not specified. Setting to default value 09/27/2022 18:13:38
Successfully submitted on-demand. Operation tracking Id: ea5fcb7a-4e54-4de2-b519-88439e0a8149
Current log collection status: Running
Waiting for log collection to complete...
==== CUT ===== CUT =====
Log collection ended with status: Succeeded
PS C:\Users\docsuser>
```

## Get a history of log collection

To get a history of log collections for the last 90 days, enter:

#### PowerShell



## Get-LogCollectionHistory

Here's a sample output of the `Get-LogCollectionHistory` cmdlet:

### Output

```
PS C:\CloudDeployment\logs> Get-LogCollectionHistory
Name                               Value
----                               -
TimeCollected                     9/29/2022 5:08:14 PM +00:00
Status                             Succeeded
CollectionFromDate                 9/29/2022 4:07:57 PM +00:00
CollectionToDate                   9/29/2022 5:07:57 PM +00:00
LogCollectionId                   fdcd94c8-1bd2-4ec6-8612-c92d5abd9a84
Type                               OnDemand
LogUploadSizeMb                    1598
UploadNumberOfFiles                1924
Directory
Location
Error
-----
TimeCollected                     9/27/2022 11:57:25 PM +00:00
Status                             Succeeded
CollectionFromDate                 9/27/2022 9:57:16 PM +00:00
CollectionToDate                   9/27/2022 11:57:16 PM +00:00
LogCollectionId                   f3d8dcc6-901e-4c72-a3cc-210055e6f198
Type                               OnDemand
LogUploadSizeMb                    1069
UploadNumberOfFiles                1941
Directory
Location
Error
PS C:\CloudDeployment\logs>
```

## Save logs to a local file share

You can save diagnostic logs to a local Server Message Block (SMB) share if you want to save data locally or don't have access to send data to Azure. Run the following command on each node of the cluster to collect logs and save them locally:

### PowerShell

```
Send-DiagnosticData -ToSMBShare -BypassObsAgent -SharePath <Path to the SMB share> -ShareCredential <Credentials to connect to the SharePath>
```

If you have outbound connectivity from the SMB share where you saved the logs, you can run the following command to send the logs to Microsoft:

PowerShell

```
Send-DiagnosticData -FromSMBShare -BypassObsAgent -SharePath <Path to the  
SMB share> -ShareCredential <Credentials to connect to the SharePath>
```

## Next steps

- [Contact Microsoft Support](#)
- [Review known issues in Azure Stack HCI](#)

# Troubleshoot environment validation issues (preview)

Article • 09/01/2023

Applies to: Azure Stack HCI, version 23H2 (preview)

This article describes how to get support from Microsoft to troubleshoot validation issues that may arise during the pre-deployment or pre-registration of the Azure Stack HCI cluster.

## Important

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

## Get support from Microsoft

Starting with Azure Stack HCI, version 23H2 (preview) and later, you can get support from Microsoft to troubleshoot any issues that may arise during the environment validation process for Azure Stack HCI.

To troubleshoot environment validation issues, you can begin by filing a support ticket and then do the following:

- Collect diagnostic data locally and submit it to Microsoft to assist with troubleshooting. See [Collect diagnostic data locally and send to Microsoft](#).
- Enable remote support to allow Microsoft Support to connect to your device remotely and provide assistance. See [Get remote support](#).

## Collect diagnostic data locally and send to Microsoft

If the environment validation process fails, you can save diagnostic data to a local Server Message Block (SMB) share and then transmit it to Microsoft for troubleshooting purposes. Microsoft can access that data after you file a support case.

# Save logs on a local file share

You can save diagnostic logs to a local share, typically in the following scenarios:

- **Pre-deployment or pre-registration.** To troubleshoot any validation issues that may arise during the pre-deployment or pre-registration of the cluster.
- **Post-deployment.** If you're normally connected but experiencing connectivity issues, you can save logs locally to help with troubleshooting.

Run the following command on each node of the cluster to collect logs and save them locally:

PowerShell

```
Send-DiagnosticData -ToSMBShare -BypassObsAgent -SharePath <Path to the SMB share> -ShareCredential <Credentials to connect to the SharePath>
```

## Send logs to Microsoft

Microsoft retains the diagnostic data that you send for up to 29 days and handles it as per the [standard privacy practices](#).

You can send logs to Microsoft using `Send-DiagnosticData` and `Send-AzStackHciDiagnosticData` cmdlets, as described in the following sections.

### Send logs using `Send-DiagnosticData`

If the SMB share where you saved the logs has outbound connectivity, you can run the following command to send logs after log collection on all the nodes finishes:

PowerShell

```
Send-DiagnosticData -FromSMBShare -BypassObsAgent -SharePath <Path to the SMB share> -ShareCredential <Credentials to connect to the SharePath>
```

### Send logs using `Send-AzStackHciDiagnosticData`

Use the `Send-AzStackHciDiagnosticData` cmdlet to send logs from any machine with outbound connectivity, outside of the Azure Stack HCI stamp.

The input parameters used to send logs using `Send-AzStackHciDiagnosticData` are the same that are required as part of the deployment process. For description about the

input parameters, see [Deploy Azure Stack HCI using PowerShell \(preview\)](#).

You can use any of the following credentials to send logs:

- \$RegistrationCredential
- \$RegistrationWithDeviceCode
- \$RegistrationSPCCredential
- \$RegistrationWithExistingContext

You can find the parameter values in `C:\Deployment`. Run the following command to see the output:

PowerShell

```
$deployArgs = Import-Clixml -Path C:\Deployment\DeployArguments.xml
```

## Get information for the required parameters

The following parameters are required to use the `Send-AzStackHciDiagnosticData` cmdlet. Consult your network administrator as needed for this information.

- `ResourceGroupName`: Name of the Azure resource group, which must be the same as used during the deployment process. Follow these steps to get the resource group name:

1. Establish a remote PowerShell session with one of the cluster nodes. Run PowerShell as administrator and run the following command:

PowerShell

```
Enter-PsSession -ComputerName <NodeName> -Credential $cred
```

2. Run the following command to get the resource group name:

PowerShell

```
Import-Module
C:\CloudDeployment\ECEngine\EnterpriseCloudEngine.psd1 -
ErrorAction SilentlyContinue
$eceConfig = Get-EceConfiguration -ErrorAction SilentlyContinue
if ($eceConfig.Xml -match "<RegistrationResourceGroupName>(.*?)
</RegistrationResourceGroupName>")
{
    $resourcegroupname = $matches[1].Trim()
}
```

- **SubscriptionId**: Name of the Azure subscription ID, which must be the same as used during the deployment process. Use the following command to get the subscription ID:

PowerShell

```
$subscriptionId = $deployArgs.RegistrationSubscriptionId
```

- **TenantId**: Azure tenant ID, which must be the same as used during the deployment process. Use the following command to get the tenant ID:

PowerShell

```
$cloudName = $deployargs.RegistrationCloudName
Import-Module
"$env:SystemDrive\CloudDeployment\Setup\Common\RegistrationHelpers.psm1"
$RegistrationTenantId = Get-TenantId -AzureEnvironment $CloudName -
SubscriptionId $subscriptionid
```

- **RegistrationRegion**: Registration region, which must be the same as used during the deployment process.
- **Cloud**: Azure cloud name, which must be the same as used during the deployment process.
- **CacheFlushWaitTimeInSec**: Optional wait time in seconds to flush the cache folder. The default value is 600.
- **RegistrationCredential**: Azure credentials to authenticate with Azure. This is mandatory in **DefaultSet** parameter set.
- **DiagnosticLogPath**: Diagnostics log path where logs are stored.
- **RegistrationWithDeviceCode**: The switch that allows Azure authentication with the device code.
- **RegistrationWithExistingContext**: Use this switch if current PowerShell window already had **Connect-AzAccount** executed and use the existing context for Azure authentication.
- **RegistrationSPCredential**: Part of the **ServicePrincipal** parameter set. Use this to send **ServicePrincipal** credential.

## Send logs using different credentials

Based on the type of credentials you have, use one of the following commands to send logs:

- Send logs using registration credentials

PowerShell

```
Send-AzStackHciDiagnosticData -ResourceGroupName <ResourceGroupName> -  
SubscriptionId <SubscriptionId> -TenantId <TenantId> -  
RegistrationCredential <RegistrationCredential> -DiagnosticLogPath  
<LogPath> -RegistrationRegion <RegionName> -Cloud <AzureCloud>
```

Use the following command to set up the registration credentials:

PowerShell

```
$registrationaccountusername = $deployArgs.RegistrationAccountUserName  
$regPassword = $deployArgs.RegistrationAccountPassword  
$registrationCredential = New-Object  
System.Management.Automation.PSCredential -ArgumentList  
$registrationaccountusername, (ConvertTo-SecureString -AsPlainText  
$regPassword -Force) $registrationCredential
```

- Send logs using device code credentials

When you run the following command, you'll be prompted to open a web browser and enter the provided code to proceed with the authentication process.

PowerShell

```
Send-AzStackHciDiagnosticData -ResourceGroupName <ResourceGroupName> -  
SubscriptionId <SubscriptionId> -TenantId <TenantId> -  
RegistrationWithDeviceCode -DiagnosticLogPath <LogPath> -  
RegistrationRegion <RegionName> -Cloud <AzureCloud>
```

- Send logs using service principal name (SPN) credentials

PowerShell

```
Send-AzStackHciDiagnosticData -ResourceGroupName <ResourceGroupName> -  
SubscriptionId <SubscriptionId> -TenantId <TenantId> -  
RegistrationSPCredential <RegistrationSPCredential> -DiagnosticLogPath  
<LogPath> -RegistrationRegion <RegionName> -Cloud <AzureCloud>
```

You can use the following cmdlets to get SPN credentials:

PowerShell

```
$SPNAppID = "<Your App ID>"
$SPNSecret= "<Your SPN Secret>"
$SPNsecStringPassword = ConvertTo-SecureString
$SPNSecret -AsPlainText -Force
$SPNCred = New-Object System.Management.Automation.PSCredential
($SPNAppID, $SPNsecStringPassword)
```

- Send logs using registration with existing context credentials

PowerShell

```
Send-AzStackHciDiagnosticData -ResourceGroupName <ResourceGroupName> -
SubscriptionId <SubscriptionId> -TenantId <TenantId> -
RegistrationWithExistingContext -DiagnosticLogPath <LogPath> -
RegistrationRegion <RegionName> -Cloud <AzureCloud>
```

## Get remote support

In the pre-deployment or pre-registration scenarios, you are prompted to install and enable remote support via the Environment Checker to evaluate the readiness for deployment. If you enable remote support, Microsoft Support can connect to your device remotely and offer assistance. If you want to get remote support post-deployment of the cluster, see [Get remote support for Azure Stack HCI](#).

The high-level workflow to get remote support in the pre-deployment or pre-registration scenario is as follows:

- [Submit a support request](#)
- Enable remote support via PowerShell. This is a one-time configuration.

## Enable remote support

Follow these steps to enable remote support:

1. Establish a remote PowerShell session with the cluster node. Run PowerShell as administrator and run the following command:

PowerShell

```
Enter-PsSession -ComputerName <NodeName> -Credential $cred
```



2. Run the following command to enable remote support. The sample Shared Access Signature (SAS) is provided by the Microsoft support team.

PowerShell

```
Enable-AzStackHciRemoteSupport -AccessLevel <Diagnostics Or  
DiagnosticsRepair> -ExpireInMinutes <1440> -SasCredential <Sample SAS>  
-PassThru
```

### ⓘ Note

When you run the command to enable remote support, you may get the following error:

```
Processing data from remote server <NodeName> failed with the following  
error message: The I/O operation has been aborted because of either a  
thread exit or an application request.
```

This means the Just Enough Administration (JEA) configuration has not been established. When you enable remote support, a service restart is required to activate JEA. During the remote support JEA configuration, the Windows Remote Management (WinRM) restarts twice, which may disrupt the PsSession to the node. To resolve this error, wait for a few minutes before reconnecting to the remote node and then run the `Enable-AzStackHciRemoteSupport` cmdlet again to enable remote support.

For remote support usage scenarios, see [Remote support examples](#).

## Next steps

- [Collect diagnostic logs](#)
- [Contact Microsoft Support](#)

# Troubleshoot Azure Stack HCI deployment (preview)


Article • 06/30/2023

Applies to: Azure Stack HCI, Supplemental Package

This article provides guidance on how to rerun and reset deployment if you encounter issues during your Azure Stack HCI deployment.

Also see [Known issues](#).

## Important

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

## Rerun deployment

To rerun the deployment if there is a failure, follow these steps:

1. Establish a remote desktop protocol (RDP) connection with the first server of your Azure Stack HCI cluster. Use the *option 15* in the *SConfig* to go to the command line. Change the directory to `C:\clouddeployment\setup`.
2. Run the following command on your first (staging) server:

PowerShell

```
.\Invoke-CloudDeployment.ps1 -Rerun -Verbose
```

This command should restart the deployment in verbose mode.

## Update the refresh token

If your authentication token expires and deployment fails, you can update the refresh token. Follow these steps to update the refresh token:

1. Sign in to the first server. To import the registration module, run the following PowerShell cmdlet:

```
PowerShell
```

```
Update-AuthenticationToken
```

2. From a second server that has a browser installed, open the browser and navigate to <https://microsoft.com/devicelogin>.
3. Copy the authentication code that is displayed and complete the authentication request.
4. Resume the deployment using the following cmdlet:

```
PowerShell
```

```
Invoke-CloudDeployment -Rerun
```

## Reset deployment

You may have to reset your deployment if it is in a not recoverable state. For example, if it is an incorrect network configuration, or if rerun doesn't resolve the issue. In these cases, do the following:

1. Back up all your data first.
2. Connect to the first server via remote desktop protocol (RDP). [Reinstall](#) the Azure Stack HCI 22H2 operating system.
3. You'll need to clean the Active Directory objects that were created. Connect to your Active Directory Domain server. Run PowerShell as administrator.
4. Identify the `A` records created for your DNS server. Run the following command to get a list of the `A` records created for your DNS server:

```
Azure PowerShell
```

```
Get-DnsServerResourceRecord -ZoneName "<FQDN for your Active Directory Domain Server>"
```

5. From the list of the records displayed, identify the type `A` records corresponding to the `RecordType` that are associated with your cluster nodes (`RecordData` should

have the cluster node IPs).

6. To remove an **A** record, run the following command:

Azure PowerShell

```
Remove-DnsServerResourceRecord -ZoneName "<FQDN for your Active Directory Domain Server>" -name "<HostName for an A record>" -RRtype A
```

Here's a sample output:

Output

```
PS C:\temp> get-dnsServerResourceRecord -Zonename  
ASZ1PLab.nttest.microsoft.com
```

HostName	RecordType	Type	Timestamp
TimeToLive	RecordData		
-----	-----	----	-----
@	A	1	10/27/2022 1:00:0...
00:10:00	10.57.52.95		
@	NS	2	0
01:00:00	svcclient02vm3.asz1plab.nttest.microsoft.com.		
@	SOA	6	0
01:00:00	[185][svcclient02vm3.asz1plab.nttest.microsoft....		
_msdcs	NS	2	0
01:00:00	svcclient02vm3.asz1plab.nttest.microsoft.com.		
_gc._tcp.Default-First...	SRV	33	10/27/2022 1:00:0...
00:10:00	[0][100][3268][SVCCLIENT02VM3.ASZ1PLab.nttest.m...		
_kerberos._tcp.Default...	SRV	33	10/27/2022 1:00:0...
00:10:00	[0][100][88][SVCCLIENT02VM3.ASZ1PLab.nttest.mic...		
_ldap._tcp.Default-Fir...	SRV	33	10/27/2022 1:00:0...
00:10:00	[0][100][389][SVCCLIENT02VM3.ASZ1PLab.nttest.mi...		
_gc._tcp	SRV	33	10/27/2022 1:00:0...
00:10:00	[0][100][3268][SVCCLIENT02VM3.ASZ1PLab.nttest.m...		
_kerberos._tcp	SRV	33	10/27/2022 1:00:0...
00:10:00	[0][100][88][SVCCLIENT02VM3.ASZ1PLab.nttest.mic...		
_kpasswd._tcp	SRV	33	10/27/2022 1:00:0...
00:10:00	[0][100][464][SVCCLIENT02VM3.ASZ1PLab.nttest.mi...		
_ldap._tcp	SRV	33	10/27/2022 1:00:0...
00:10:00	[0][100][389][SVCCLIENT02VM3.ASZ1PLab.nttest.mi...		
_kerberos._udp	SRV	33	10/27/2022 1:00:0...
00:10:00	[0][100][88][SVCCLIENT02VM3.ASZ1PLab.nttest.mic...		
_kpasswd._udp	SRV	33	10/27/2022 1:00:0...
00:10:00	[0][100][464][SVCCLIENT02VM3.ASZ1PLab.nttest.mi...		
A4P1074000603B	A	1	10/28/2022 10:00:...
00:20:00	10.57.53.236		
A6P15140005012	A	1	10/28/2022 10:00:...
00:20:00	10.57.51.224		
ca-5c55badb-4674-4844-...	A	1	10/21/2022 1:00:0...
00:20:00	10.57.48.71		

docspro2-FS	A	1	10/28/2022 11:00:...
00:20:00	10.57.51.224		
docspro2-FS	A	1	10/28/2022 11:00:...
00:20:00	10.57.53.236		
docspro2cluster	A	1	10/28/2022 10:00:...
00:20:00	10.57.48.60		
DomainDnsZones	A	1	10/27/2022 1:00:0...
00:10:00	10.57.52.95		
_ldap._tcp.Default-Fir...	SRV	33	10/27/2022 1:00:0...
00:10:00	[0][100][389][SVCCLIENT02VM3.ASZ1PLab.nttest.mi...		
_ldap._tcp.DomainDnsZones	SRV	33	10/27/2022 1:00:0...
00:10:00	[0][100][389][SVCCLIENT02VM3.ASZ1PLab.nttest.mi...		
ForestDnsZones	A	1	10/27/2022 1:00:0...
00:10:00	10.57.52.95		
_ldap._tcp.Default-Fir...	SRV	33	10/27/2022 1:00:0...
00:10:00	[0][100][389][SVCCLIENT02VM3.ASZ1PLab.nttest.mi...		
_ldap._tcp.ForestDnsZones	SRV	33	10/27/2022 1:00:0...
00:10:00	[0][100][389][SVCCLIENT02VM3.ASZ1PLab.nttest.mi...		
svcclient02vm3	A	1	0
01:00:00	10.57.52.95		

```
PS C:\temp> Remove-DnsServerResourceRecord -Zonename
ASZ1PLab.nttest.microsoft.com -name docspro2-FS -RRtype A
```

Confirm

Removing DNS resource record set by name docspro2-FS of type A from zone ASZ1PLab.nttest.microsoft.com on SVCCLIENT02VM3 server. Do you want to continue?

[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y

```
PS C:\temp> Remove-DnsServerResourceRecord -Zonename
ASZ1PLab.nttest.microsoft.com -name docspro2cluster -RRtype A
```

Confirm

Removing DNS resource record set by name docspro2cluster of type A from zone ASZ1PLab.nttest.microsoft.com on SVCCLIENT02VM3 server. Do you want to continue?

[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y

```
PS C:\temp> Remove-DnsServerResourceRecord -Zonename
ASZ1PLab.nttest.microsoft.com -name A4P1074000603B -RRtype A
```

Confirm

Removing DNS resource record set by name A4P1074000603B of type A from zone ASZ1PLab.nttest.microsoft.com on SVCCLIENT02VM3 server. Do you want to continue?

[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y

```
PS C:\temp> Remove-DnsServerResourceRecord -Zonename
ASZ1PLab.nttest.microsoft.com -name A6P15140005012 -RRtype A
```

Confirm

Removing DNS resource record set by name A6P15140005012 of type A from zone ASZ1PLab.nttest.microsoft.com on SVCCLIENT02VM3 server. Do you want to continue?

[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y

```
PS C:\temp> get-dnsServerResourceRecord -Zonename
ASZ1PLab.nttest.microsoft.com
```

HostName	RecordType	Type	Timestamp
TimeToLive	RecordData		
@	A	1	10/27/2022 1:00:0...
00:10:00	10.57.52.95		
@	NS	2	0
01:00:00	svcclient02vm3.asz1plab.nttest.microsoft.com.		
@	SOA	6	0
01:00:00	[189][svcclient02vm3.asz1plab.nttest.microsoft....		
_msdcs	NS	2	0
01:00:00	svcclient02vm3.asz1plab.nttest.microsoft.com.		
_gc._tcp.Default-First...	SRV	33	10/27/2022 1:00:0...
00:10:00	[0][100][3268][SVCCLIENT02VM3.ASZ1PLab.nttest.m...		
_kerberos._tcp.Default...	SRV	33	10/27/2022 1:00:0...
00:10:00	[0][100][88][SVCCLIENT02VM3.ASZ1PLab.nttest.mic...		
_ldap._tcp.Default-Fir...	SRV	33	10/27/2022 1:00:0...
00:10:00	[0][100][389][SVCCLIENT02VM3.ASZ1PLab.nttest.mi...		
_gc._tcp	SRV	33	10/27/2022 1:00:0...
00:10:00	[0][100][3268][SVCCLIENT02VM3.ASZ1PLab.nttest.m...		
_kerberos._tcp	SRV	33	10/27/2022 1:00:0...
00:10:00	[0][100][88][SVCCLIENT02VM3.ASZ1PLab.nttest.mic...		
_kpasswd._tcp	SRV	33	10/27/2022 1:00:0...
00:10:00	[0][100][464][SVCCLIENT02VM3.ASZ1PLab.nttest.mi...		
_ldap._tcp	SRV	33	10/27/2022 1:00:0...
00:10:00	[0][100][389][SVCCLIENT02VM3.ASZ1PLab.nttest.mi...		
_kerberos._udp	SRV	33	10/27/2022 1:00:0...
00:10:00	[0][100][88][SVCCLIENT02VM3.ASZ1PLab.nttest.mic...		
_kpasswd._udp	SRV	33	10/27/2022 1:00:0...
00:10:00	[0][100][464][SVCCLIENT02VM3.ASZ1PLab.nttest.mi...		
ca-5c55badb-4674-4844-...	A	1	10/21/2022 1:00:0...
00:20:00	10.57.48.71		
DomainDnsZones	A	1	10/27/2022 1:00:0...
00:10:00	10.57.52.95		
_ldap._tcp.Default-Fir...	SRV	33	10/27/2022 1:00:0...
00:10:00	[0][100][389][SVCCLIENT02VM3.ASZ1PLab.nttest.mi...		
_ldap._tcp.DomainDnsZones	SRV	33	10/27/2022 1:00:0...
00:10:00	[0][100][389][SVCCLIENT02VM3.ASZ1PLab.nttest.mi...		
ForestDnsZones	A	1	10/27/2022 1:00:0...
00:10:00	10.57.52.95		
_ldap._tcp.Default-Fir...	SRV	33	10/27/2022 1:00:0...
00:10:00	[0][100][389][SVCCLIENT02VM3.ASZ1PLab.nttest.mi...		
_ldap._tcp.ForestDnsZones	SRV	33	10/27/2022 1:00:0...
00:10:00	[0][100][389][SVCCLIENT02VM3.ASZ1PLab.nttest.mi...		
svcclient02vm3	A	1	0
01:00:00	10.57.52.95		

```
PS C:\temp>
```

7. Repeat the above steps to remove all the type **A** records.

8. Connect to the first server. You can now [Deploy interactively](#) or [Deploy using an existing config file](#).

## Next steps

- [Collect log data](#) from your deployment.
- View [known issues](#).


# What's the Lifecycle Manager (preview)?

Article • 04/28/2023

Applies to: Azure Stack HCI, Supplemental Package

This article is applicable to version 2303 of the Supplemental Package and later. It describes the Lifecycle Manager, the benefits it provides for an Azure Stack HCI cluster solution, and more.

## Important

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

## About the Lifecycle Manager

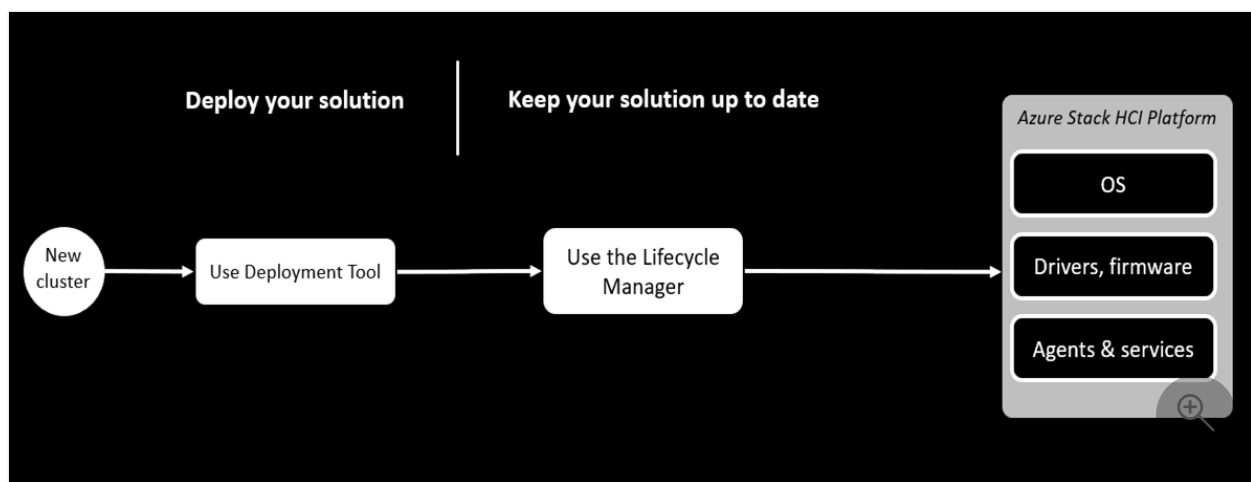
Azure Stack HCI solutions contain many individual features and components. Staying up to date with recent security fixes and feature improvements is important for all pieces of the Azure Stack HCI solution. To stay up to date, you might need to follow different processes to apply updates depending on the services you use.

In past releases of Azure Stack HCI, like 20H2 and 21H2, the operating system (OS) was the primary component being updated. In 22H2, the Supplemental Package introduces new features and components in addition to the OS, including the Lifecycle Manager.

The Lifecycle Manager provides centralized orchestration capabilities for Azure Stack HCI solutions. It's installed as part of and enables the new deployment experience with the management of the OS, core agents and services, and the solution extension. The Lifecycle Manager supports a broad range of updates and sets the foundation for substantial future improvements.

Here's an example of a new cluster deployment using the deployment tool with the Lifecycle Manager:





In this solution the Azure Stack HCI OS, driver, firmware, and agents and services, are automatically updated. Note, some new agents and services can't be updated outside the Lifecycle Manager and availability of those updates depends on the specific feature.

## Benefits of the Lifecycle Manager

The Lifecycle Manager offers many benefits for updating your solution. Some of these benefits include:

- It simplifies update management by consolidating update workflows for various components into a single experience.
- It keeps the system in a well-tested and optimal configuration.
- It helps avoid downtime and effects on workloads with comprehensive health checks before and during an update.
- It improves reliability with automatic retry and the remediation of known issues.
- Whether managed locally or via the Azure portal, the common back-end drives a consistent experience.

## Lifecycle cadence

The Azure Stack HCI platform follows the [Modern Lifecycle policy](#). The Modern Lifecycle policy defines the products and services that are continuously serviced and supported. To stay current with this policy, you must stay within six months of the most recent release. To learn more about the support windows, see [Azure Stack HCI release information](#).

Microsoft might release the following types of updates for the Azure Stack HCI platform:

Update Type	Typical Cadence	Description
Patch Updates	Monthly	Patch updates primarily contain quality and reliability improvements. They might include OS LCUs or hotpatches. Some patches require host system reboots, while others don't. To fix critical or security issues, hotfixes might be released sooner than monthly.
Baseline Updates	Quarterly	Baseline updates include new features and improvements. They typically require host system reboots and might take longer.
Hotfixes	As needed	Hotfixes address blocking issues that could prevent regular patch or baseline updates.
Solution Builder Extension (SBE)	Bi-Annually	Solution Builder Extension provides driver, firmware, and other partner content specific to the system solution used. They might require host system reboots.

Sometimes you might see updates to the latest patch level of your current baseline. If a new baseline is available, you might see the baseline update itself or the latest patch level of the baseline. Your cluster must stay within six months of the most recent baseline to consider it supported.

## Next steps

Learn more about how to [Use Lifecycle Manager for Azure Stack HCI solution updates](#).

# Lifecycle Manager for Azure Stack HCI solution updates (preview)

Article • 11/14/2023

Applies to: Azure Stack HCI, Supplemental Package

This article describes how to keep various pieces of your Azure Stack HCI solution up to date. This article is applicable to software release 2310 for Azure Stack HCI, version 23H2.

## Important

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

## About update the solution

The Lifecycle Manager provides a flexible foundation to integrate and manage more of the solution content in one place. In this release, the Lifecycle Manager allows management of the OS, core agent and services, and the solution extension.

The next sections provide an overview of components, along with methods and links for updating your solution.

## Lifecycle Manager for platform updates

Platform updates managed by the Lifecycle Manager contain new versions of the Azure Stack HCI operating system (OS), the Lifecycle Manager core agents and services, and the solution extension (depending on your cluster's hardware). Microsoft bundles these components into an update release and validates the combination of versions to ensure interoperability.

- **Operating System:** These updates help you stay productive and protected. They provide users and IT administrators with the security fixes they need and protect devices so that unpatched vulnerabilities can't be exploited.
- **Lifecycle Manager agents and services:** The Lifecycle Manager updates its own agents to ensure it has the recent fixes corresponding to the update. To achieve a

successful update of its agents, the Lifecycle Manager:

- Prepares and updates the servicing stack
- Installs new agents and services
- Updates the host OS. Cluster-Aware Updating is used to orchestrate reboots.
- **Solution extension:** Hardware vendors might choose to integrate with the Lifecycle Manager to enhance the update management experience for their customers.
  - If a hardware vendor has integrated with our update validation and release platform, the solution extension content includes the drivers and firmware, and the Lifecycle Manager orchestrates the necessary system reboots within the same maintenance window. You can spend less time searching for updates and experience fewer maintenance windows.

The Lifecycle Manager is the recommended way to update your Azure Stack HCI cluster. Here's a high-level process for platform updates with Lifecycle Manager:

- **Plan for the update.**
  - Discover the update, read the release notes, and determine a good time to update. For example, a time when production workloads aren't in use, or nonpeak hours.
  - Take backups of your deployment.
  - Download the update.
  - If your Solution Builder needs more content, acquire what's needed.
- **Review any precheck warnings or failures and remediate, as necessary.**
  - Execute the update.
- **Monitor the update as it proceeds.**
  - Review the update and system health after completion.
  - Confirm that your storage and workloads are healthy.

## User interfaces for updates

In addition to the Lifecycle Management method used to update your solution, there are two interfaces that can be used to apply your available updates. Here are the interfaces:

- PowerShell (Command line)
- Azure portal

### PowerShell

The PowerShell procedures apply to a single server and multi-server cluster that runs with the Lifecycle Manager installed. For more information, see [Update your Azure Stack HCI solution via PowerShell](#).

## Windows Admin Center

To install feature updates using Azure portal, see [Update your cluster via the Azure Update Manager](#).

## Workload updates

In addition to your cluster updates, there are workload updates that aren't integrated into the Lifecycle Manager that can be applied to your cluster. These workload updates include Azure Kubernetes Service (AKS) hybrid, Azure Arc Virtual Machines (VMs), and Infrastructure Virtual Machines (VMs).

The next sections provide information on these workloads and ways to apply updates.

### Azure Kubernetes Service (AKS) hybrid

Azure Kubernetes Service (AKS) hybrid runs via Virtual Machines (VM) on the Azure Stack HCI system. AKS hybrid tooling orchestrates the workload updates process, which involves bringing up new VMs and moving workloads over in a rolling fashion.

AKS hybrid has two types of updates that can be initiated through PowerShell or Windows Admin Center.

- Host updates
- Workload cluster updates

To update AKS hybrid using Windows Admin Center, see:

- [Upgrade the Azure Kubernetes Service host in AKS hybrid using Windows Admin Center](#).
- [Upgrade the Kubernetes version of Azure Kubernetes Service \(AKS\) workload clusters with Windows Admin Center](#).

To update AKS hybrid using PowerShell, see:

- [Upgrade the Azure Kubernetes Service host in AKS hybrid using PowerShell](#).

- [Upgrade Kubernetes version of Azure Kubernetes Service \(AKS\) workload clusters in AKS hybrid using PowerShell.](#)

## Azure Arc

Azure Arc is a bridge that extends the Azure platform to help you build applications and services with the flexibility to run across datacenters, at the edge, and in multicloud environments. For more information about Azure Arc and applying updates to your Azure Arc agent, see:

- [Azure Arc resource bridge \(preview\) overview.](#)
- [Upgrade the Agent.](#)

## Infrastructure Virtual Machines (VMs)

Software-Defined Networking relies on several Virtual Machines. To update these virtual machines, see [Update SDN infrastructure for Azure Stack HCI](#) for instructions.

Other Microsoft services that rely on Azure Stack HCI VMs may have their own instructions for updates. For example, individually connecting to VMs to upgrade them or swapping a VM's virtual hard disk (VHD).

## Customer apps and workloads

The Azure Stack HCI platform doesn't update customer workloads given the update processes depend on the type of workload. We recommend that you Arc-enable your VMs and keep the Azure Arc agent up to date. For more information, see:

- [Azure Arc-enabled servers.](#)
- [Upgrade the agent.](#)
- [Use Update Management in Azure Automation to manage operating system updates for Azure Arc-enabled servers.](#)

## Next steps

Learn more about the [Phases of an Azure Stack HCI solution update.](#)

# Phases of an Azure Stack HCI solution update (preview)


Article • 04/28/2023

Applies to: Azure Stack HCI, Supplemental Package

This article describes the various phases of solution updates that are applied to your Azure Stack HCI cluster to keep it up-to-date.

The procedure in this article applies to both a single server and a multi-server cluster that is running software versions with Lifecycle Manager installed. For more information, see [What is Lifecycle Manager?](#).

## Important

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

## About update phases

The Azure Stack HCI solution updates can consist of platform, service, and solution extension updates. For more information on each of these types of updates, see [Use Lifecycle Manager to apply solution updates](#).

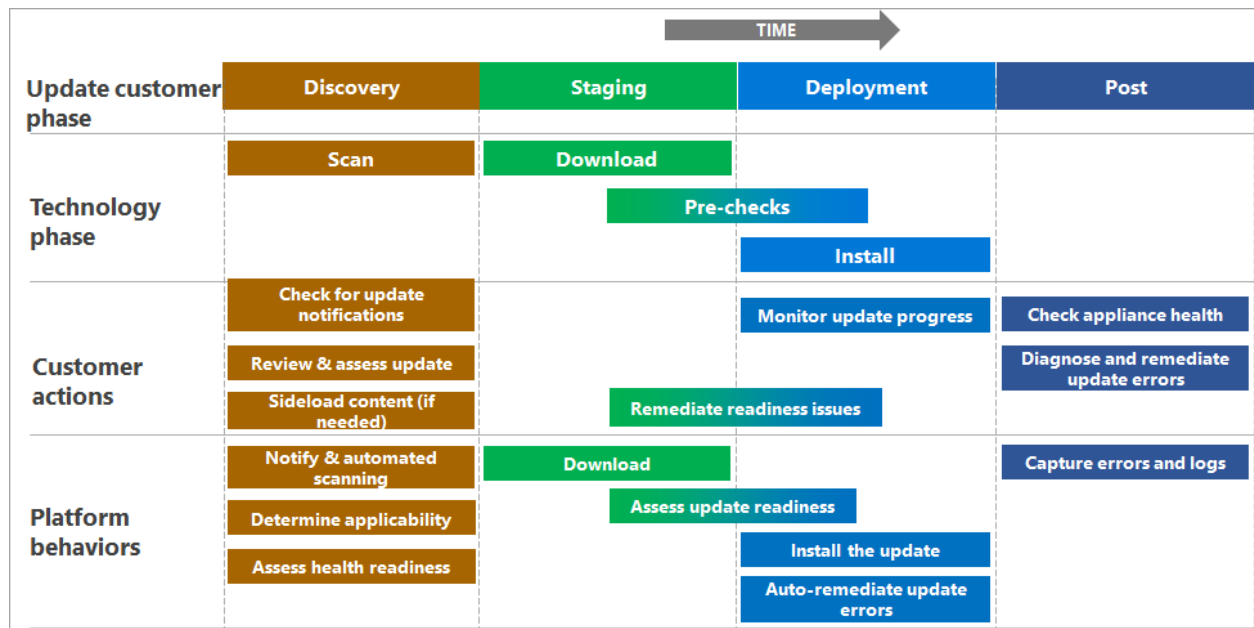
The Lifecycle Manager automates the update process for agents, services, operating system content, and Solution Extension content, with the goal of maintaining availability by shifting workloads around throughout the update process when needed.

The updates can be of the following types:

- **Updates not requiring reboots** - The updates that can be applied to your Azure Stack HCI cluster without requiring any reboots for the servers in the cluster.
- **Updates that require reboots** - The updates may require a reboot of a server in your Azure Stack HCI cluster at a time. If an update requires rebooting the servers in the cluster, the Lifecycle Manager uses the Cluster-Aware Updating to reboot one server at a time. This ensures the availability of the cluster throughout the update process.

The updates consist of several phases: discovering the update, staging the content, deploying the update, and reviewing the installation. Each phase may not require your input but distinct actions occur in each phase.

You can apply these updates via PowerShell or via the Windows Admin Center UI. Regardless of the interface you choose, the subsequent sections summarize what happens within each phase of an update. The following diagram shows what actions you may need to perform during each phase of an update, and what actions the Azure Stack HCI takes throughout the update operation.



## Phase 1: Discovery and acquisition

Before Microsoft releases a new update package, the package is validated as a collection of components. After the validation is complete, the content is released along with the release notes.

The release notes include the update contents, changes, known issues, and links to any external downloads that may be required (for example, drivers and firmware). For more information, see the [Latest release notes](#).

After Microsoft releases the update, your Azure Stack HCI update platform will automatically detect the update. Though you don't need to scan for updates, you must go to the **Updates** page in your management surface to see the new update's details.

Depending on the hardware in your cluster and the scope of an update bundle, you may need to acquire and sideload extra content to proceed with an update. The **operating system** and **agents and services** content are provided by Microsoft, while depending on your specific solution and the OEM, the **Solution Extension** may require an extra



download from the hardware OEM. If this is required, the installation flow prompts you for the content.

## Phase 2: Readiness checks and staging

Before installing a solution update, the Lifecycle Manager runs a series of checks to confirm that your Azure Stack HCI cluster is safe to update. This helps the update go more smoothly.

The following table lists the prechecks performed on your Azure Stack HCI cluster before the updates are applied.

Target component	Precheck description
Storage systems	Check that the storage pools are healthy.
	Check that the Storage services physical disks are healthy and online.
	Check that storage subsystems are healthy and online.
	Check that storage volumes are healthy and online.
	Check that storage virtual disks are healthy and online.
	Check that storage job status is successful.
	Check that storage cluster shared volume is healthy and online.
Failover cluster requirements	Check that the failover cluster is available.
	Check that the failover cluster is running Windows Server 2012 or later.
	Check that the Cluster service is running on all cluster nodes.
	Check that the CAU clustered role is installed on the failover cluster to enable self-updating mode.
	Check that the required versions of .NET Framework and Windows PowerShell are installed on all of the failover cluster nodes.
	Check that the machine proxy on each failover cluster node is set to a local proxy server.
	Check that the automatic updates are not configured to automatically install updates on any failover cluster node.
	Check that the failover cluster nodes are using the same update source.

Target component	Precheck description
Remote management of cluster	Check that remote management is enabled for failover cluster nodes via Windows Management Instrumentation (WMI) version 2.
	Check that Windows PowerShell remoting is enabled on each failover cluster node.
	Check for the presence of a firewall rule that allows remote shutdown. This rule should be enabled on each node in the failover cluster.
Solution Builder Extensions	Check that the Solution Builder Extension status on the cluster is healthy.
	Check that the Solution Builder Extension health status on each cluster node is healthy.

A subset of these checks can be initiated outside the update process. Because new checks can be included in each update, these readiness checks are executed *after* the update content has been downloaded and *before* it begins installing.

Readiness checks can also result in blocking conditions or warnings.

- If the readiness checks detect a blocking condition, the issues must be remediated before the update can proceed.
- Readiness checks can also result in warnings that won't block the updates but may introduce longer update times or impact the workloads. You may need to acknowledge the potential impact and bypass the warning before the update can proceed.

Typically the update platform tries to remediate the issues automatically but sometimes manual intervention is required. Once you remediate the issue, you need to rerun the checks to confirm the update readiness before proceeding.

#### ⓘ Note

In this release, you can only initiate immediate install of the updates. Scheduling of updates is not supported.

## Phase 3: Installation progress and monitoring

While the update installs, you can monitor the progress via your chosen interface. Steps within the update are shown within a hierarchy. This hierarchy corresponds to the actions the Lifecycle Manager takes throughout the workflow. Steps may be dynamically generated throughout the workflow, so the list of steps may change. For more information, see examples of [Monitoring progress via PowerShell](#).

## Failures and diagnosis

The Lifecycle Manager includes retry and remediation logic. It attempts to fix issues in a non-disruptive way, such as retrying a CAU run. If an update run can't be remediated automatically, it fails. You can retry the update or visit the Azure Support Center to evaluate the next steps.

## Collecting logs

If you encounter failures during the update process, collect diagnostic logs to help Microsoft identify and fix the issues. For more information, see how to [Collect diagnostic logs for Azure Stack HCI, version 22H2 \(preview\)](#).

## Next steps

Learn more about how to [Troubleshoot updates](#).

# Update your Azure Stack HCI solution via PowerShell (preview)

Article • 06/12/2023


Applies to: Azure Stack HCI, Supplemental Package

This article describes how to apply a solution update to your Azure Stack HCI cluster via PowerShell.

The procedure in this article applies to both a single server and multi-server cluster that is running software versions with Lifecycle Manager installed. If your cluster was created via a new deployment of Azure Stack HCI, Supplemental Package, then Lifecycle Manager was automatically installed as part of the deployment.

For information on how to apply solution updates to clusters that were created with older versions of Azure Stack HCI that didn't have Lifecycle Manager installed, see [Update existing Azure Stack HCI clusters](#).

## Important

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

## About solution updates

The Azure Stack HCI solution updates can consist of platform, service, and solution extension updates. For more information on each of these types of updates, see [Use the Lifecycle Manager to apply solution updates](#).

When you apply a solution update, here are the high-level steps that you take:

1. Make sure that all the prerequisites are completed.
2. Identify the software version running on your cluster.
3. Connect to your Azure Stack HCI cluster via remote PowerShell.
4. Verify that your cluster is in good health using the [Environment Checker](#).
5. Discover the updates that are available and filter the ones that you can apply to your cluster.

6. Download the updates, assess the update readiness of your cluster and once ready, install the updates on your cluster. Track the progress of the updates. If needed, you can also monitor the detailed progress.
7. Verify the version of the updates installed.

The time taken to install the updates may vary based on the following factors:

- Content of the update.
- Load on your cluster.
- Number of nodes in your cluster.
- Type of the hardware used.
- Solution Builder Extension used.

The approximate time estimates for a typical single server and 4-server cluster are summarized in the following table:

<b>Cluster/Time</b>	<b>Time for health check <i>hh:mm:ss</i></b>	<b>Time to install update <i>hh:mm:ss</i></b>
Single server	0:01:44	1:25:42
4-node cluster	0:01:58	3:53:09

## Prerequisites

Before you begin, make sure that:

- You have access to an Azure Stack HCI cluster that is running 2303 or higher. The cluster should be registered in Azure.
- You have access to a client that can connect to your Azure Stack HCI cluster. This client should be running PowerShell 5.0 or later.
- You have access to the solution update package over the network. You sideload or copy these updates to the nodes of your cluster.

## Connect to your Azure Stack HCI cluster

Follow these steps on your client to connect to one of the nodes of your Azure Stack HCI cluster.

1. Run PowerShell as administrator on the client that you're using to connect to your cluster.

2. Open a remote PowerShell session to a node on your Azure Stack HCI cluster. Run the following command and provide the credentials of your node when prompted:

PowerShell

```
$cred = Get-Credential  
Enter-PSSession -ComputerName "<Computer IP>" -Credential $cred
```

#### ⚠ Note

You should sign in using your Lifecycle Manager account credentials.

Here's an example output:

Console

```
PS C:\Users\Administrator> $cred = Get-Credential  
  
cmdlet Get-Credential at command pipeline position 1  
Supply values for the following parameters:  
Credential  
PS C:\Users\Administrator> Enter-PSSession -ComputerName  
"100.100.100.10" -Credential $cred  
[100.100.100.10]: PS C:\Users\Administrator\Documents>
```

## Step 1: Identify the stamp version on your cluster

Before you discover the updates, make sure that the cluster was deployed using the Azure Stack HCI, 2303 Supplemental Package.

1. Make sure that you're connected to the cluster node using the Lifecycle Manager account. Run the following command:

PowerShell

```
whoami
```

2. To ensure that the cluster was deployed using the Supplemental Package, run the following command on one of the nodes of your cluster:

PowerShell

## Get-StampInformation

Here's a sample output:

### Console

```
PS C:\Users\lcmuser> Get-StampInformation
Deployment ID      : b4457f25-6681-4e0e-b197-a7a433d621d6
OemVersion        : 2.1.0.0
PackageHash       :
StampVersion      : 10.2303.0.31
InitialDeployedVersion : 10.2303.0.26
PS C:\Users\lcmuser>
```

3. Make a note of the `StampVersion` on your cluster. The stamp version reflects the solution version that your cluster is running.

## Step 2: Optionally validate system health

Before you discover the updates, you can manually validate the system health. This step is optional as the Lifecycle Manager always assesses update readiness prior to applying updates.

### ⓘ Note

Any faults that have a severity of *critical* will block the updates from being applied.

1. Connect to a node on your Azure Stack HCI cluster using the Lifecycle Manager account.
2. Run the following command to validate system health via the [Environment Checker](#).

### PowerShell

```
$result=Test-EnvironmentReadiness
$result|ft Name,Status,Severity
```

Here's a sample output:

### Console

```
PS C:\Users\lcmuser> whoami
rq2205\lcmuser
PS C:\Users\lcmuser> $result=Test-EnvironmentReadiness
VERBOSE: Looking up shared vhd product drive letter.
WARNING: Unable to find volume with label Deployment
VERBOSE: Get-Package returned with Success:True
VERBOSE: Found package
Microsoft.AzureStack.Solution.Deploy.EnterpriseCloudEngine.Client.Deplo
yment with version 10.2303.0.31 at
C:\NugetStore\Microsoft.AzureStack.Solution.Deploy.EnterpriseCloudEngin
e.Client.Deployment.10.2303.0.31\Microsoft.Azure
Stack.Solution.Deploy.EnterpriseCloudEngine.Client.Deployment.nuspec.
03/29/2023 15:45:58 : Launching StoragePools
03/29/2023 15:45:58 : Launching StoragePhysicalDisks
03/29/2023 15:45:58 : Launching StorageMapping
03/29/2023 15:45:58 : Launching StorageSubSystems
03/29/2023 15:45:58 : Launching TestCauSetup
03/29/2023 15:45:58 : Launching StorageVolumes
03/29/2023 15:45:58 : Launching StorageVirtualDisks
03/29/2023 15:46:05 : Launching OneNodeEnvironment
03/29/2023 15:46:05 : Launching NonMigratableWorkload
03/29/2023 15:46:05 : Launching FaultSummary
03/29/2023 15:46:06 : Launching SBEHealthStatusOnNode
03/29/2023 15:46:06 : Launching StorageJobStatus
03/29/2023 15:46:07 : Launching StorageCsv
WARNING: There aren't any faults right now.
03/29/2023 15:46:09 : Launching SBEPrecheckStatus
WARNING: rq2205-cl: There aren't any faults right now.
VERBOSE: Looking up shared vhd product drive letter.
WARNING: Unable to find volume with label Deployment
VERBOSE: Get-Package returned with Success:True
VERBOSE: Found package Microsoft.AzureStack.Role.SBE with version
4.0.2303.66 at
C:\NugetStore\Microsoft.AzureStack.Role.SBE.4.0.2303.66\Microsoft.Azure
Stack.Role.SBE.nuspec.
VERBOSE: SolutionExtension module supports Tag
'HealthServiceIntegration'.
VERBOSE: SolutionExtension module SolutionExtension at
C:\ClusterStorage\Infrastructure_1\Shares\SU1_Infrastructure_1\CloudMed
ia\SBE\Installed\Content\Configuration\SolutionExtension is valid.
VERBOSE: Looking up shared vhd product drive letter.
WARNING: Unable to find volume with label Deployment
VERBOSE: Get-Package returned with Success:True
VERBOSE: Found package Microsoft.AzureStack.Role.SBE with version
4.0.2303.66 at
C:\NugetStore\Microsoft.AzureStack.Role.SBE.4.0.2303.66\Microsoft.Azure
Stack.Role.SBE.nuspec.
VERBOSE: SolutionExtension module supports Tag
'HealthServiceIntegration'.
VERBOSE: SolutionExtension module SolutionExtension at
C:\ClusterStorage\Infrastructure_1\Shares\SU1_Infrastructure_1\CloudMed
ia\SBE\Installed\Content\Configuration\SolutionExtension is valid.
PS C:\Users\lcmuser> $result|ft Name,Status,Severity
```



Name	Status	Severity
----	-----	-----
Storage Pool Summary	SUCCESS	CRITICAL
Storage Services Physical Disks Summary	SUCCESS	CRITICAL
Storage Services Physical Disks Summary	SUCCESS	CRITICAL
Storage Services Physical Disks Summary	SUCCESS	CRITICAL
Storage Services Physical Disks Summary	SUCCESS	CRITICAL
Storage Services Physical Disks Summary	SUCCESS	CRITICAL
Storage Services Physical Disks Summary	SUCCESS	CRITICAL
Storage Services Physical Disks Summary	SUCCESS	CRITICAL
Storage Services Physical Disks Summary	SUCCESS	CRITICAL
Storage Services Physical Disks Summary	SUCCESS	CRITICAL
Storage Services Physical Disks Summary	SUCCESS	CRITICAL
Storage Services Physical Disks Summary	SUCCESS	CRITICAL
Storage Services Physical Disks Summary	SUCCESS	CRITICAL
Storage Services Physical Disks Summary	SUCCESS	CRITICAL
Storage Services Physical Disks Summary	SUCCESS	CRITICAL
Storage Services Physical Disks Summary	SUCCESS	CRITICAL
Storage Services Physical Disks Summary	SUCCESS	CRITICAL
Storage Services Physical Disks Summary	SUCCESS	CRITICAL
Storage Services Physical Disks Summary	SUCCESS	CRITICAL
Storage Services Physical Disks Summary	SUCCESS	CRITICAL
Storage Services Physical Disks Summary	SUCCESS	CRITICAL
Storage Services Summary	SUCCESS	CRITICAL
Storage Services Summary	SUCCESS	CRITICAL
Storage Services Summary	SUCCESS	CRITICAL
Storage Subsystem Summary	SUCCESS	CRITICAL
Test-CauSetup	SUCCESS	INFORMATIONAL
Test-CauSetup	SUCCESS	INFORMATIONAL
Test-CauSetup	SUCCESS	INFORMATIONAL
Test-CauSetup	SUCCESS	INFORMATIONAL
Test-CauSetup	SUCCESS	CRITICAL
Test-CauSetup	SUCCESS	INFORMATIONAL
Test-CauSetup	SUCCESS	INFORMATIONAL
Test-CauSetup	SUCCESS	INFORMATIONAL
Test-CauSetup	FAILURE	INFORMATIONAL
Test-CauSetup	FAILURE	INFORMATIONAL
Test-CauSetup	FAILURE	INFORMATIONAL
Storage Volume Summary	SUCCESS	CRITICAL
Storage Volume Summary	SUCCESS	CRITICAL
Storage Volume Summary	SUCCESS	CRITICAL
Storage Volume Summary	SUCCESS	CRITICAL
Storage Virtual Disk Summary	SUCCESS	CRITICAL
Storage Virtual Disk Summary	SUCCESS	CRITICAL
Storage Virtual Disk Summary	SUCCESS	CRITICAL
Storage Virtual Disk Summary	SUCCESS	CRITICAL
Get-OneNodeRebootRequired	SUCCESS	WARNING
Test-NonMigratableVMs	SUCCESS	WARNING
Faults	SUCCESS	INFORMATIONAL
Test-SBEHealthStatusOnNode	Success	Informational
Test-SBEHealthStatusOnNode	Success	Informational
Storage Job Summary	SUCCESS	CRITICAL
Storage Cluster Shared Volume Summary	SUCCESS	CRITICAL
Storage Cluster Shared Volume Summary	SUCCESS	CRITICAL
Storage Cluster Shared Volume Summary	SUCCESS	CRITICAL

```
Test-SBEPrecheckStatus
```

```
Success Informational
```

```
PS C:\Users\lcmuser>
```

#### ⓘ Note

In this release, the informational failures for `Test-CauSetup` are expected and will not impact the updates.

3. Review any failures and resolve those before you proceed to the discovery step.

## Step 3: Discover the updates

You can discover updates in one of the following two ways:

- **Discover updates online** - This is the recommended option when your cluster has good internet connectivity. The solution updates are discovered via the online update catalog.
- **Sideload and discover updates** - This is an alternative to discovering updates online and should be used for scenarios with unreliable or slow internet connectivity, or when using solution extension updates provided by your hardware vendor. In these instances, you download the solution updates to a central location. You then sideload the updates to an Azure Stack HCI cluster and discover the updates locally.

## Discover solution updates online (recommended)

Discovering solution updates using the online catalog is the *recommended* method. Follow these steps to discover solution updates online:

1. Connect to a node on your Azure Stack HCI cluster using the Lifecycle Manager account.
2. Verify that the update package was discovered by the Update service.

```
PowerShell
```

```
Get-SolutionUpdate | ft DisplayName, State
```

3. Optionally review the versions of the update package components.

```
PowerShell
```

```
$Update=Get-SolutionUpdate  
$Update.ComponentVersions
```

Here's an example output:

Console

```
PS C:\Users\lcmuser> $Update = Get-SolutionUpdate  
PS C:\Users\lcmuser> $Update.ComponentVersions  
  
PackageType Version      LastUpdated  
-----  
Services    10.2303.0.31  
Platform    10.2303.0.31  
SBE         4.1.2.3  
PS C:\Users\lcmuser>
```

You can now proceed to [Download and install the updates](#).

## Sideload and discover solution updates

If you're using solution extension updates from your hardware, you would need to sideload those updates. Follow these steps to sideload and discover your solution updates.

1. Connect to a node on your Azure Stack HCI cluster using the Lifecycle Manager account.
2. Go to the network share and acquire the update package that you use. Verify that the update package that you sideload contains the following files:
  - *SolutionUpdate.xml*
  - *SolutionUpdate.zip*
  - *AS\_Update\_10.2303.4.1.zip*

If a solution builder extension is part of the update package, you should also see the following files:

- *SBE\_Content\_4.1.2.3.xml*
- *SBE\_Content\_4.1.2.3.zip*
- *SBE\_Discovery\_Contoso.xml*

3. Create a folder for discovery by the update service at the following location in the infrastructure volume of your cluster.

PowerShell

**New-Item**

```
C:\ClusterStorage\Infrastructure_1\Shares\SU1_Infrastructure_1\sideload  
-ItemType Directory
```

4. Copy the update package to the folder you created in the previous step.
5. Manually discover the update package using the Update service. Run the following command:

PowerShell

**Add-SolutionUpdate -SourceFolder**

```
C:\ClusterStorage\Infrastructure_1\Shares\SU1_Infrastructure_1\sideload
```

6. Verify that the update package is discovered by the Update service and is available to start preparation and installation.

PowerShell

**Get-SolutionUpdate** | ft DisplayName, Version, State

Here's an example output:

Console

```
PS C:\Users\lcmuser> Get-SolutionUpdate | ft DisplayName, Version,  
State
```

DisplayName	Version	State
Azure Stack HCI 2303 bundle	10.2303.0.31	Ready

```
PS C:\Users\lcmuser>
```

7. Optionally check the version of the update package components. Run the following command:

PowerShell

```
$Update = Get-SolutionUpdate  
$Update.ComponentVersions
```

Here's an example output:

#### Console

```
PS C:\Users\lcmuser> $Update = Get-SolutionUpdate
PS C:\Users\lcmuser> $Update.ComponentVersions

PackageType Version          LastUpdated
-----
Services    10.2303.0.31
Platform    10.2303.0.31
SBE         4.1.2.3
PS C:\Users\lcmuser>
```

## Step 4: Download, check readiness, and install updates

You can download the updates, perform a set of checks to verify the update readiness of your cluster, and start installing the updates.

1. You can only download the update without starting the installation or download and install the update.

- To download and install the update, run the following command:

#### PowerShell

```
Get-SolutionUpdate | Start-SolutionUpdate
```

- To only download the updates without starting the installation, use the `-PrepareOnly` flag with `Start-SolutionUpdate`.

2. To track the update progress, monitor the update state. Run the following command:

#### PowerShell

```
Get-SolutionUpdate | ft Version,State,UpdateStateProperties,HealthState
```

When the update starts, the following actions occur:

- Download of the updates begins. Depending on the size of the download package and the network bandwidth, the download may take several minutes.

Here's an example output when the updates are being downloaded:

#### Console

```
PS C:\Users\lcmuser> Get-SolutionUpdate|ft
Version,State,UpdateStateProperties,HealthState

Version          State UpdateStateProperties HealthState
-----
10.2303.4.1 Downloading                                     InProgress
```

- Once the package is downloaded, readiness checks are performed to assess the update readiness of your cluster. For more information about the readiness checks, see [Update phases](#). During this phase, the **State** of the update shows as **HealthChecking**.

#### Console

```
PS C:\Users\lcmuser> Get-SolutionUpdate|ft
Version,State,UpdateStateProperties,HealthState

Version          State UpdateStateProperties HealthState
-----
10.2303.4.1 HealthChecking                                     InProgress
```

- When the system is ready, updates are installed. During this phase, the **State** of the updates shows as **Installing** and **UpdateStateProperties** shows the percentage of the installation that was completed.

#### Important

During the install, the cluster nodes may reboot and you may need to establish the remote PowerShell session again to monitor the updates. If updating a single node, your Azure Stack HCI will experience a downtime.

Here's a sample output while the updates are being installed.

#### Console

```
PS C:\Users\lcmuser> Get-SolutionUpdate|ft
Version,State,UpdateStateProperties,HealthState

Version          State UpdateStateProperties HealthState
-----
10.2303.4.1 Installing 6% complete.                          Success
```

```

PS C:\Users\lcmuser> Get-SolutionUpdate|ft
Version,State,UpdateStateProperties,HealthState

Version          State UpdateStateProperties HealthState
-----
10.2303.4.1 Installing 25% complete.          Success

PS C:\Users\lcmuser> Get-SolutionUpdate|ft
Version,State,UpdateStateProperties,HealthState

Version          State UpdateStateProperties HealthState
-----
10.2303.4.1 Installing 40% complete.          Success

PS C:\Users\lcmuser> Get-SolutionUpdate|ft
Version,State,UpdateStateProperties,HealthState

Version          State UpdateStateProperties HealthState
-----
10.2303.4.1 Installing 89% complete.          Success

```

Once the installation is complete, the **State** changes to **Installed**. For more information on the various states of the updates, see [Installation progress and monitoring](#).

## Step 5: Verify the installation

After the updates are installed, verify the solution version of the environment and the version of the operating system.

1. After the update is in **Installed** state, check the environment solution version. Run the following command:

PowerShell

```
Get-SolutionUpdateEnvironment | ft State, CurrentVersion
```

Here's a sample output:

Console

```
PS C:\Users\lcmuser> Get-SolutionUpdateEnvironment | ft State,
CurrentVersion
```

```

State          CurrentVersion
-----
AppliedSuccessfully 10.2303.0.31

```

2. Check the operating system version to confirm it matches the recipe you installed.

Run the following command:

```
PowerShell
```

```
cmd /c ver
```

Here's a sample output:

```
Console
```

```
PS C:\Users\lcmuser> cmd /c ver
```

```
Microsoft Windows [Version 10.0.20349.1547]
```

```
PS C:\Users\lcmuser>
```

## Next steps

Learn more about how to [Update existing Azure Stack HCI clusters](#) when the Lifecycle Manager isn't installed.




# Troubleshoot Azure Stack HCI solution update (preview)

Article • 04/28/2023

Applies to: Azure Stack HCI, Supplemental Package

This article describes how to troubleshoot solution updates that are applied to your Azure Stack HCI cluster to keep it up-to-date.

## Important

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

## About troubleshooting updates

The Lifecycle Manager includes retry and remediation logic. This logic attempts to fix update issues in a non-disruptive way, such as retrying a CAU run. If an update run can't be remediated automatically, it fails. When an update fails, you can retry the update.

## Collect update logs

You can also collect diagnostic logs to help Microsoft identify and fix the issues. To collect logs for the update failures, follow these steps on the client that you're using to access your cluster:

1. Establish a remote PowerShell session with the server node. Run PowerShell as administrator and run the following command:

PowerShell

```
Enter-PSSession -ComputerName <server_IP_address> -Credential  
<username\password for the server>
```

2. Get all the solutions updates and then filter the solution updates corresponding to a specific version. The version used corresponds to the version of solution update that failed to install.

PowerShell

```
$Update = Get-SolutionUpdate | ? version -eq "<Version string>" -verbose
```

3. Identify the action plan for the failed solution update run.

PowerShell

```
$Failure = $update|Get-SolutionUpdateRun
```

4. Identify the `ResourceID` for the Update.

PowerShell

```
$Failure
```

Here's a sample output:

Output

```
PS C:\Users\lcmuser> $Update = Get-SolutionUpdate | ? version -eq
"10.2303.1.7" -verbose
PS C:\Users\lcmuser> $Failure = $Update|Get-SolutionUpdateRun
PS C:\Users\lcmuser> $Failure

ResourceId      : redmond/Solution10.2303.1.7/2c21b859-e063-4f24-a4db-
bc1d6be82c4e
Progress       :
Microsoft.AzureStack.Services.Update.ResourceProvider.UpdateService.Models.Step
TimeStarted    : 4/21/2023 10:02:54 PM
LastUpdatedTime : 4/21/2023 3:19:05 PM
Duration       : 00:16:37.9688878
State          : Failed
```

Note the `ResourceID` GUID. This corresponds to the `ActionPlanInstanceId`.

5. Copy the logs for the `ActionPlanInstanceId` that you noted earlier, to a text file named *log.txt*. Use Notepad to open the text file.

PowerShell

```
Get-ActionplanInstance -ActionplanInstanceId <Action Plan Instance ID>
>log.txt
notepad log.txt
```

Here's sample output:

#### Output

```
PS C:\Users\lcmuser> Get-ActionplanInstance -actionplaninstanceid  
2c21b859-e063-4f24-a4db-bc1d6be82c4e >log.txt
```

```
PS C:\Users\lcmuser>notepad log.txt
```

## Next steps

Learn more about how to [Run updates via PowerShell](#).

# Add a server on your Azure Stack HCI (preview)

Article • 11/14/2023

Applies to: Azure Stack HCI, version 23H2 (preview)

This article describes how to manage capacity by adding a server (often called scale-out) to your Azure Stack HCI cluster.

## Important

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

## About add servers

You can easily scale the compute and storage at the same time on your Azure Stack HCI by adding servers to an existing cluster. Your Azure Stack HCI cluster supports a maximum of up to 16 servers.

Each new physical server that you add to your cluster must closely match the rest of the servers in terms of CPU type, memory, number of drives, and the type and size of the drives.

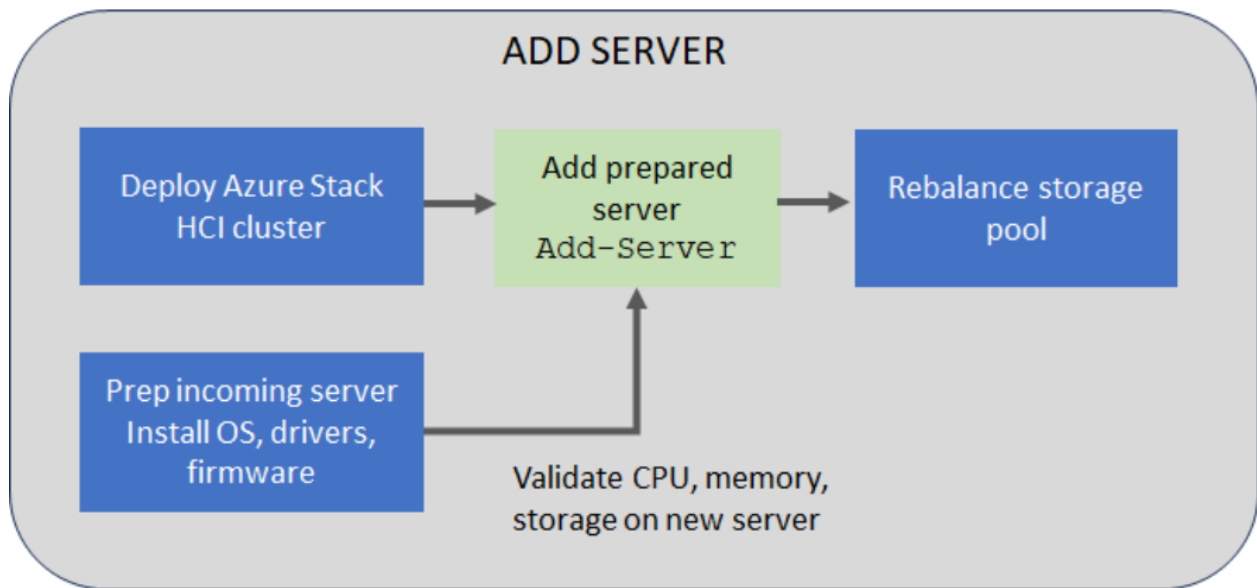
You can dynamically scale your Azure Stack HCI cluster from 1 to 16 servers. In response to the scaling, the orchestrator (also known as Lifecycle Manager) adjusts the drive resiliency, network configuration including the on-premises agents such as orchestrator agents, and Arc registration. The dynamic scaling may require the network architecture change from connected without a switch to connected via a network switch.

## Important

- In this preview release, you can only add one server at any given time. You can however add multiple servers sequentially so that the storage pool is rebalanced only once.
- It is not possible to permanently remove a server from a cluster.

# Add server workflow

The following flow diagram shows the overall process to add a server:



To add a server, follow these high-level steps:

1. Install the operating system, drivers, and firmware on the new cluster server that you plan to add. For more information, see [Install OS](#).
2. Add the prepared server via the `Add-server` PowerShell cmdlet.
3. When adding a server to the cluster, the system validates that the new incoming server meets the CPU, memory, and storage (drives) requirements before it actually adds the server.
4. Once the server is added, cluster is also validated to ensure that it's functioning normally. Next, the storage pool is automatically rebalanced. Storage rebalance is a low priority task that doesn't impact actual workloads. The rebalance can run for multiple days depending on number of the servers and the storage used.

## Supported scenarios

For adding a server, the following scale-out scenarios are supported:

Start scenario	Target scenario	Resiliency settings	Storage network architecture	Witness settings
Single-server	Two-server cluster	Two-way mirror	Configured with and without a switch	Witness required for target scenario.
Two-server cluster	Three-server cluster	Three-way mirror	Configured with a switch only	Witness optional for target scenario.

Start scenario	Target scenario	Resiliency settings	Storage network architecture	Witness settings
Three-server cluster	N-server cluster	Three-way mirror	Switch only	Witness optional for target scenario.

When upgrading a cluster from two to three servers, the storage resiliency level is changed from a two-way mirror to a three-way mirror.

## Resiliency settings

In this preview release, for add server operation, specific tasks aren't performed on the workload volumes created after the deployment.

For add server operation, the resiliency settings are updated for the required infrastructure volumes and the workload volumes created during the deployment. The settings remain unchanged for other workload volumes that you created after the deployment (since the intentional resiliency settings of these volumes aren't known and you may just want a 2-way mirror volume regardless of the cluster scale).

However, the default resiliency settings are updated at the storage pool level and so any new workload volumes that you created after the deployment will inherit the resiliency settings.

## Hardware requirements

When adding a server, the system validates the hardware of the new, incoming server and ensures that the server meets the hardware requirements before it's added to the cluster.

Component	Compliance check
CPU	Validate the new server has the same number of or more CPU cores. If the CPU cores on the incoming node don't meet this requirement, a warning is presented. The operation is however allowed.
Memory	Validate the new server has the same amount of or more memory installed. If the memory on the incoming node doesn't meet this requirement, a warning is presented. The operation is however allowed.
Drives	Validate the new server has the same number of data drives available for Storage Spaces Direct. If the number of drives on the incoming node don't meet this requirement, an error is reported and the operation is blocked.

# Prerequisites

Before you add a server, you would need to complete the hardware and software prerequisites.

## Hardware prerequisites

Make sure to complete the following prerequisites:

1. The first step is to acquire the new Azure Stack HCI hardware from your original OEM. Always refer to your OEM-provided documentation when adding new server hardware for use in your cluster.
2. Place the new physical server in the predetermined location, for example, a rack and cable it appropriately.
3. Enable and adjust physical switch ports as applicable in your network environment.

## Software prerequisites

Make sure to complete the following prerequisites:

- `AzureStackLCMUser` is active in Active Directory. For more information, see [Prepare the Active Directory](#).
- Signed in as `AzureStackLCMUser` or another user with equivalent permissions.
- Credentials for the `AzureStackLCMUser` haven't changed.

# Add a server

This section describes how to add a server using PowerShell, monitor the status of the `Add-Server` operation and troubleshoot, if there are any issues.

## Add a server using PowerShell

Make sure that you have reviewed and completed the [prerequisites](#).

On the new server that you plan to add, follow these steps.

1. Install the operating system and required drivers on the new server that you plan to add. Follow the steps in [Install the Azure Stack HCI, version 23H2 Operating System](#).

ⓘ Note

You must also Install required Windows Roles.

On a server that already exists on your cluster, follow these steps:

1. Sign in with the domain user credentials that you provided during the deployment of the cluster.
2. Before you add the server, make sure to get an updated authentication token. Run the following command:

PowerShell

```
Update-AuthenticationToken
```

3. Run the following command to add the new incoming server:

PowerShell

```
$HostIpv4 = "<IPv 4 for the new server>"  
$Cred = Get-Credential  
Add-Server -Name "< Name of the new server>" -HostIpv4 $HostIpv4 -  
LocalAdminCredential $Cred
```

4. Make a note of the operation ID as output by the `Add-Server` command. You use this operation ID later to monitor the progress of the `Add-Server` operation.

## Monitor operation progress

To monitor the progress of the add server operation, follow these steps:

1. Run the following cmdlet and provide the operation ID from the previous step.

PowerShell

```
$ID = "<Operation ID>"  
Start-MonitoringActionplanInstanceToComplete -actionPlanInstanceID $ID
```

2. After the operation is complete, the background storage rebalancing job will continue to run. Wait for the storage rebalance job to complete. To verify the progress of this storage rebalancing job, use the following cmdlet:

PowerShell



If the storage rebalance job is complete, the cmdlet won't return an output.

The newly added server shows in the Azure portal in your Azure Stack HCI cluster list after several hours. To force the server to show up in Azure portal, run the following command:

PowerShell

```
Sync-AzureStackHCI
```

## Recovery scenarios

Following recovery scenarios and the recommended mitigation steps are tabulated for adding a server:

Scenario description	Mitigation	Supported?
Added a new server out of band without using the orchestrator.	Remove the added server. Use the orchestrator to add the server.	No
Added a new server with orchestrator and the operation failed.	To complete the operation, investigate the failure. Rerun the failed operation using <code>Add-Server -Rerun</code> .	Yes
Added a new server with orchestrator. The operation succeeded partially but had to start with a fresh operating system install.	In this scenario, orchestrator has already updated its knowledge store with the new server. Use the repair server scenario.	Yes

## Troubleshoot issues

If you experience failures or errors while adding a server, you can capture the output of the failures in a log file. On a server that already exists on your cluster, follow these steps:

- Sign in with the domain user credentials that you provided during the deployment of the cluster. Capture the issue in the log files.

PowerShell

```
Get-ActionPlanInstance -ActionPlanInstanceID $ID | out-file log.txt
```

- To rerun the failed operation, use the following cmdlet:

```
PowerShell
```

```
Add-Server -Rerun
```

## Next steps

Learn more about how to [Repair a server](#).

# Repair a server on your Azure Stack HCI (preview)

Article • 11/14/2023

Applies to: Azure Stack HCI, version 23H2 (preview)

This article describes how to repair a server on your Azure Stack HCI cluster.

## Important

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

## About repair servers

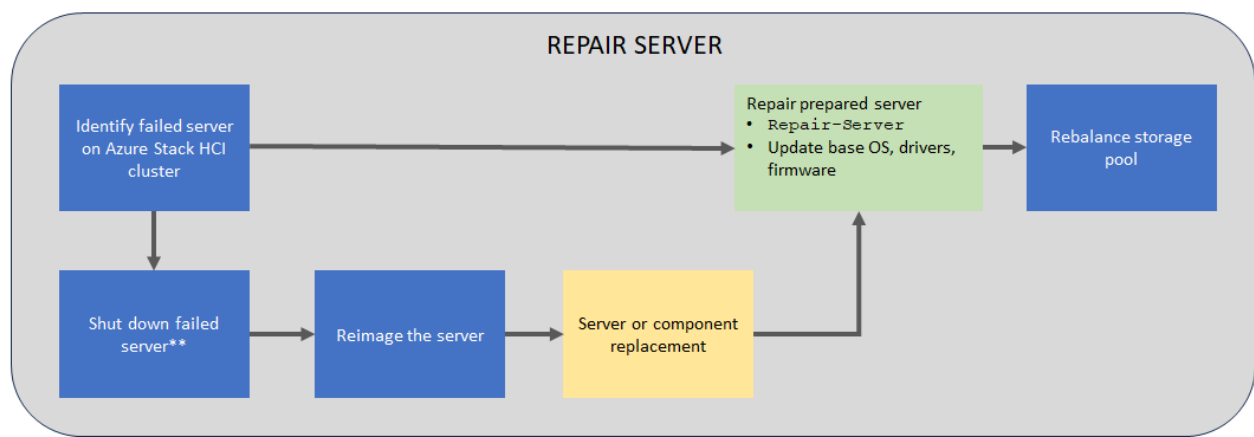
Azure Stack HCI is a hyperconverged system that allows you to repair servers from existing clusters. You may need to repair a server in a cluster if there's a hardware failure.

Before you repair a server, make sure to check with your solution provider, which components on the server are field replacement units (FRUs) that you can replace yourself and which components would require a technician to replace.

Parts that support hot swap typically do not require you to reimage the server unlike the non hot-swappable components such as motherboard do. Consult your hardware manufacturer to determine which component replacements would require you to reimage the server. For more information, see [Component replacement](#).

## Repair server workflow

The following flow diagram shows the overall process to repair a server.



*\*Server may not be in a state where shutdown is possible or necessary*

To repair an existing server, follow these high-level steps:

1. If possible, shut down the server that you want to repair. Depending on the state of the server, a shutdown may not be possible or necessary.
2. Reimage the server that needs to be repaired.
3. Run the repair server operation. The Azure Stack HCI operating system, drivers, and firmware are updated as part of the repair operation.

The storage is automatically rebalanced on the reimaged server. Storage rebalance is a low priority task that can run for multiple days depending on number of the servers and the storage used.

## Supported scenarios

Repairing a server reimages a server and brings it back to the cluster with the previous name and configuration.

Repairing a single server results in a redeployment with the option to persist the data volumes. Only the system volume is deleted and newly provisioned during deployment.

### Important

Make sure that you always have backups for your workloads and do not rely on the system resiliency only. This is especially critical in single-server scenarios.

## Resiliency settings

In this preview release, for repair server operation, specific tasks aren't performed on the workload volumes that you created after the deployment. For repair server operation,

only the required infrastructure volumes and the workload volumes are restored and surfaced as cluster shared volumes (CSVs).

The other workload volumes that you created after the deployment are still retained and you can discover these volumes by running `Get-VirtuaDisk` cmdlet. You'll need to manually unlock the volume (if the volume has BitLocker enabled), and create a CSV (if needed).

## Hardware requirements

When repairing a server, the system validates the hardware of the new, incoming server and ensures that the server meets the hardware requirements before it's added to the cluster.

Component	Compliance check
CPU	Validate the new server has the same number of or more CPU cores. If the CPU cores on the incoming node don't meet this requirement, a warning is presented. The operation is however allowed.
Memory	Validate the new server has the same amount of or more memory installed. If the memory on the incoming node doesn't meet this requirement, a warning is presented. The operation is however allowed.
Drives	Validate the new server has the same number of data drives available for Storage Spaces Direct. If the number of drives on the incoming node don't meet this requirement, an error is reported and the operation is blocked.

## Server replacement

You may replace the entire server:

- With a new server that has a different serial number compared to the old server.
- With the current server after you reimage it.

The following scenarios are supported during server replacement:

Server	Disk	Supported
New server	New disks	Yes
New server	Current disks	Yes
Current server (reimaged)	Current disks reformatted *	No
Current server (reimaged)	New disks	Yes

Server	Disk	Supported
Current server (reimaged)	Current disks	Yes

\*\*Disks that have been used by Storage Spaces Direct, require proper cleaning. Reformatting isn't sufficient. See how to [Clean drives](#).

### Important

If you replace a component during server repair, you don't need to replace or reset data drives. If you replace a drive or reset it, then the drive won't be recognized once the server joins the cluster.

## Component replacement

On your Azure Stack HCI cluster, non hot-swappable components include the following items:

- Motherboard/baseboard management controller (BMC)/video card
- Disk controller/host bus adapter (HBA)/backplane
- Network adapter
- Graphics processing unit
- Data drives (drives that don't support hot swap, for example PCI-e add-in cards)

The actual replacement steps for non hot-swappable components vary based on your original equipment manufacturer (OEM) hardware vendor. See your OEM vendor's documentation if a server repair is required for non hot-swappable components.

## Prerequisites

Before you repair a server, you must ensure that:

- `AzureStackLCMUser` is active in Active Directory. For more information, see [Prepare the Active Directory](#).
- Signed in as `AzureStackLCMUser` or another user with equivalent permissions.
- Credentials for the `AzureStackLCMUser` haven't changed.
- If needed, take the server that you have identified for repair offline. Follow the steps here:
  - [Verify the server is healthy prior to taking it offline](#).
  - [Pause and drain the server](#).

- [Shut down the server.](#)

## Repair a server

This section describes how to repair a server using PowerShell, monitor the status of the `Repair-Server` operation and troubleshoot, if there are any issues.

Make sure that you have reviewed the [prerequisites](#).

Follow these steps on the sever you are trying to repair.

1. Install the operating system and required drivers. Follow the steps in [Install the Azure Stack HCI, version 23H2 Operating System](#).

### ⓘ Note

You must also **Install required Windows Roles**.

Follow these steps on another sever that is a member of the same Azure Stack HCI cluster.

1. Before you add the server, make sure to get an updated authentication token. Run the following command:

PowerShell

```
Update-AuthenticationToken
```

2. Sign into the server that is already a member of the cluster, with the domain user credentials that you provided during the deployment of the cluster. Run the following command to repair the incoming server:

PowerShell

```
$Cred = Get-Credential  
Repair-Server -Name "< Name of the new server>" -LocalAdminCredential  
$Cred
```

3. Make a note of the operation ID as output by the `Repair-Server` command. You use this later to monitor the progress of the `Repair-Server` operation.

## Monitor operation progress

To monitor the progress of the add server operation, follow these steps:

1. Run the following cmdlet and provide the operation ID from the previous step.

PowerShell

```
$ID = "<Operation ID>"  
Start-MonitoringActionplanInstanceToComplete -actionPlanInstanceID $ID
```

2. After the operation is complete, the background storage rebalancing job will continue to run. Wait for the storage rebalance job to complete. To verify the progress of this storage rebalancing job, use the following cmdlet:

PowerShell

```
Get-VirtualDisk | Get-StorageJob
```

If the storage rebalance job is complete, the cmdlet won't return an output.

## Recovery scenarios

Following recovery scenarios and the recommended mitigation steps are tabulated for repairing a server:

Scenario description	Mitigation	Supported ?
Repair server operation failed.	To complete the operation, investigate the failure. Rerun the failed operation using <code>Add-Server - Rerun</code> .	Yes
Repair server operation succeeded partially but had to start with a fresh operation system install.	In this scenario, the orchestrator (also known as Lifecycle Manager) has already updated its knowledge store with the new server. Use the repair server scenario.	Yes

## Troubleshooting

If you experience failures or errors while repairing a server, you can capture the output of the failures in a log file.

- Sign in with the domain user credentials that you provided during the deployment of the cluster. Capture the issue in the log files.



PowerShell

```
Get-ActionPlanInstance -ActionPlanInstanceID $ID |out-file log.txt
```

- To rerun the failed operation, use the following cmdlet:

PowerShell

```
Repair-Server -Rerun
```

## Next steps

Learn more about how to [Add a server](#).