Known issues in the Azure Stack HCI 2411 release

Applies to: Azure Stack HCI, version 23H2

This article identifies critical known issues and their workarounds in the Azure Stack HCI 2411 release.

These release notes are continuously updated, and as critical issues requiring a workaround are discovered, they're added. Before you deploy your Azure Stack HCI instance, carefully review the information contained here.

Important

For information about supported update paths for this release, see Release information.

For more information about new features in this release, see What's new in 23H2.

Known issues for version 2411

This software release maps to software version number **2411.0.22**.

Release notes for this version include the issues fixed in this release, known issues in this release, and release note issues carried over from previous versions.

Note

For detailed remediation for common known issues, see the Azure Stack HCI Supportability GitHub repository.

Fixed issues

Feature	Issue	Workaround
Arc VM management	If you try to enable guest management on a migrated VM, the operation fails with the following error: *(InternalError) admission webhook "createupdatevalidationwebhook.infrastructure.azstackhci.microsoft.com" denied the request: OsProfile cannot be changed after resource creation*	

Known issues in this release

The following table lists the known issues in this release:

Feature	Issue	Workaround
Security vulnerability	Microsoft has identified a security vulnerability that could expose the local admin credentials used during the creation of Arc VMs on Azure Stack HCI to non-admin users on the VM and on the hosts. Arc VMs running on releases prior to Azure Stack HCI 2411 release are vulnerable.	To identify the Arc VMs that require this change and to change the account passwords, see detailed instructions in: https://aka.ms/CVE-2024-49060.
Update	With the 2411 release, applying a Solution Builder Extension package requires a separate update run. Solution and Solution Builder Extension update are not combined in a single update run.	
Update	When applying solution update, the update fails at the step "update ARB and extension" error "Clear-AzContext failed with 0 and Exception calling "Initialize" with "1" argument(s): "Object reference not set to an instance of an object."	Follow these steps on each node of the system. 1. Check if Az.Accounts PowerShell module version 3.0.4 is installed. Run the following command: Get-InstalledModule Az.Accounts Verify that the version in output is 3.0.4. 2. Force install Az.Accounts PowerShell module version 3.0.3. Run the following commands:

		Uninstall-Module -Name Az.Accounts -RequiredVersion 3.0.4 -Force Install-Module -Name Az.Accounts -RequiredVersion 3.0.3 -Force 3. Confirm Az.Accounts PowerShell module version 3.0.3 is installed. Run the following command: Get-InstalledModule Az.Accounts. Verify that the version in the output is 3.0.3. 4. Retry the update.

Known issues from previous releases

The following table lists the known issues from previous releases:

Feature	**Issue**	**Workaround**
Repair server	After you repair a node and run the command Set-AzureStackLCMUserPassword, you may encounter the following error: CloudEngine.Actions.InterfaceInvocationFailedException: Type 'ValidateCredentials' of Role 'SecretRotation' raised an exception:	Follow these steps to mitigate the issue: $NewPassword = <Provide new password as secure string> $OldPassword = <Provide the old/current password as secure string> $Identity = <LCM username> $credential = New-Object -TypeName PSCredential -ArgumentList $Identity, $NewPassword 1. Import the necessary module:

	Cannot load encryption certificate. The certificate setting 'CN=DscEncryptionCert' does not represent a valid base-64 encoded certificate, nor does it represent a valid certificate by file, directory, thumbprint, or subject name. at Validate-Credentials	Import-Module "C:\Program Files\WindowsPowerShell\Modules\Microsoft.AS.Infra.Security.SecretRotation\PasswordUtilities.psm1" -DisableNameChecking 2. Check the status of the ECE cluster group: $eceClusterGroup = Get-ClusterGroup \| Where-Object {$_.Name -eq "Azure Stack HCI Orchestrator Service Cluster Group"} if ($eceClusterGroup.State -ne "Online") {Write-AzsSecurityError -Message "ECE cluster group is not in an Online state. Cannot continue with password rotation." -ErrRecord $_} 3. Update the ECE with the new password: Write-AzsSecurityVerbose -Message "Updating password in ECE" -Verbose $eceContainersToUpdate = @("DomainAdmin", "DeploymentDomainAdmin", "SecondaryDomainAdmin", "TemporaryDomainAdmin", "BareMetalAdmin", "FabricAdmin", "SecondaryFabric", "CloudAdmin") foreach ($containerName in $eceContainersToUpdate) {Set-ECEServiceSecret -ContainerName $containerName -Credential $credential 3>$null 4>$null} Write-AzsSecurityVerbose -Message "Finished updating credentials in ECE." -Verbose 4. Update the password in Active Directory: Set-ADAccountPassword -Identity $Identity -OldPassword $OldPassword -NewPassword $NewPassword
Arc VM management	Using an exported Azure VM OS disk as a VHD to create a gallery image	Run the command restart-service mochostagent to restart the mochostagent service.

	for provisioning an Arc VM is unsupported.	
Networking	When a node is configured with a proxy server that has capital letters in its address, such as **HTTPS://10.100.000.00:8080**, Arc extensions fail to install or update on the node in existing builds, including version 2408.1. However, the node remains Arc connected.	Follow these steps to mitigate the issue: 1. Set the environment values in lowercase. [System.Environment]::SetEnvironmentVariable("HTTPS_PROXY", "https://10.100.000.00:8080", "Machine"). 2. Validate that the values were set. [System.Environment]::GetEnvironmentVariable("HTTPS_PROXY", "Machine"). 3. Restart Arc services. Restart-Service himds Restart-Service ExtensionService Restart-Service GCArcService 4. Signal the AzcmaAgent with the lowercase proxy information. & 'C:\Program Files\AzureConnectedMachineAgent\azcmagent.exe' config set proxy.url https://10.100.000.00:8080 & 'C:\Program Files\AzureConnectedMachineAgent\azcmagent.exe' config list
Networking	When Arc machines go down, the "**All Clusters**" page, in the new portal experience shows a "**PartiallyConnected**" or "**Not Connected Recently** status. Even when the Arc machines	There's no known workaround for this issue. To check the connectivity status, use the old experience to see if it shows as "**Connected**".

	become healthy, they may not show a "**Connected**" status.	
Security	The SideChannelMitigation security feature may not show an enabled state even if it's enabled.	There's no workaround in this release. If you encounter this issue, contact Microsoft Support to determine next steps.
Arc VM management	The Mochostagent service might appear to be running but can get stuck without updating logs for over a month. You can identify this issue by checking the service logs in `C:\programdata\mochostagent\logs` to see if logs are being updated.	Run the following command to restart the mochostagent service: `restart-service mochostagent`.
Upgrade	When upgrading the stamp from 2311 or prior builds to 2408 or later, add node and repair node operations may fail. For example, you could see an error: `Type 'AddAsZHostToDomain' of Role 'BareMetal' raised an exception`.	There's no workaround in this release. If you encounter this issue, contact Microsoft Support to determine next steps.
Update	When viewing the readiness check results for an Azure Stack HCI instance via the Azure Update Manager, there	There's no known workaround in this release. Select **View details** to view specific information about the readiness check.

	might be multiple readiness checks with the same name.	
Deployment	In some instances, during the registration of Azure Stack HCI machines, this error might be seen in the debug logs: *Encountered internal server error*. One of the mandatory extensions for device deployment might not be installed.	Follow these steps to mitigate the issue: $Settings = @{ "CloudName" = $Cloud; "RegionName" = $Region; "DeviceType" = "AzureEdge" } New-AzConnectedMachineExtension -Name "AzureEdgeTelemetryAndDiagnostics" -ResourceGroupName $ResourceGroup -MachineName $env:COMPUTERNAME -Location $Region -Publisher "Microsoft.AzureStack.Observability" -Settings $Settings -ExtensionType "TelemetryAndDiagnostics" -EnableAutomaticUpgrade New-AzConnectedMachineExtension -Name "AzureEdgeDeviceManagement" -ResourceGroupName $ResourceGroup -MachineName $env:COMPUTERNAME -Location $Region -Publisher "Microsoft.Edge" -ExtensionType "DeviceManagementExtension" New-AzConnectedMachineExtension -Name "AzureEdgeLifecycleManager" -ResourceGroupName $ResourceGroup -MachineName $env:COMPUTERNAME -Location $Region -Publisher "Microsoft.AzureStack.Orchestration" -ExtensionType "LcmController" New-AzConnectedMachineExtension -Name "AzureEdgeRemoteSupport" -ResourceGroupName $ResourceGroup -MachineName $env:COMPUTERNAME -Location $Region -Publisher "Microsoft.AzureStack.Observability" -ExtensionType "EdgeRemoteSupport" -EnableAutomaticUpgrade

<table>
<tr>
<td>Update</td>
<td>There's an intermittent issue in this release when the Azure portal incorrectly reports the update status as Failed to update or In progress though the update is complete.</td>
<td>Connect to your Azure Stack HCI instance via a remote PowerShell session. To confirm the update status, run the following PowerShell cmdlets:

$Update = get-solutionupdate| ? version -eq "<version string>"

Replace the version string with the version you're running. For example, "10.2405.0.23".

$Update.state

If the update status is Installed, no further action is required on your part. Azure portal refreshes the status correctly within 24 hours.
To refresh the status sooner, follow these steps on one of the cluster nodes.
Restart the Cloud Management cluster group.
Stop-ClusterGroup "Cloud Management"
Start-ClusterGroup "Cloud Management"</td>
</tr>
<tr>
<td>Update</td>
<td>During an initial MOC update, a failure occurs due to the target MOC version not being found in the catalog cache. The follow-up updates and retries show MOC in the target version, without the update succeeding, and as a result the Arc Resource Bridge update fails.

To validate this issue, collect the update logs using Troubleshoot solution updates for Azure Stack HCI,</td>
<td>Follow these steps to mitigate the issue:

1. To find the MOC agent version, run the following command: 'C:\Program Files\AksHci\wssdcloudagent.exe' version.

2. Use the output of the command to find the MOC version from the table below that matches the agent version, and set $initialMocVersion to that MOC version. Set the $targetMocVersion by finding the Azure Stack HCI build you're updating to and get the matching MOC version from the following table. Use these values in the mitigation script provided below:

Expand table
<table><tr><th>Build</th><th>MOC version</th><th>Agent version</th></tr></table></td>
</tr>
</table>

version 23H2. The log files should show a similar error message (current version might differ in the error message):

[ERROR: { "errorCode": "InvalidEntityError", "errorResponse": "{\n\"message\": \"the cloud fabric (MOC) is currently at version v0.13.1. A minimum version of 0.15.0 is required for compatibility\"\n}" }]

2311.2	1.0.24.10106	v0.13.0-6-gf13a73f7, v0.11.0-alph
2402	1.0.25.10203	v0.14.0, v0.13.1, 02/02/2024
2402.1	1.0.25.10302	v0.14.0, v0.13.1, 03/02/2024
2402.2	1.1.1.10314	v0.16.0-1-g04bf0dec, v0.15.1, 03/
2405/2402.3	1.3.0.10418	v0.17.1, v0.16.5, 04/18/2024

For example, if the agent version is v0.13.0-6-gf13a73f7, v0.11.0-alpha.38,01/06/2024, then $initialMocVersion = "1.0.24.10106" and if you are updating to 2405.0.23, then $targetMocVersion = "1.3.0.10418".

3. Run the following PowerShell commands on the first node:

```
$initialMocVersion = "<initial version determined from step 2>"
$targetMocVersion = "<target version determined from step 2>"

# Import MOC module twice
import-module moc
import-module moc
$verbosePreference = "Continue"

# Clear the SFS catalog cache
Remove-Item (Get-MocConfig).manifestCache

# Set version to the current MOC version prior to update, and set state as update failed
Set-MocConfigValue -name "version" -value $initialMocVersion
Set-MocConfigValue -name "installState" -value ([InstallState]::UpdateFailed)

# Rerun the MOC update to desired version
Update-Moc -version $targetMocVersion
```

		4. Resume the update.
AKS on HCI	AKS cluster creation fails with the Error: Invalid AKS network resource id. This issue can occur when the associated logical network name has an underscore.	Underscores aren't supported in logical network names. Make sure to not use underscore in the names for logical networks deployed on your Azure Stack HCI instance.
Update	When viewing the readiness check results for an Azure Stack HCI cluster via the Azure Update Manager, there might be multiple readiness checks with the same name.	There's no known workaround in this release. Select **View details** to view specific information about the readiness check.
Deployment	In some instances, during the registration of Azure Stack HCI servers, this error might be seen in the debug logs: *Encountered internal server error*. One of the mandatory extensions for device deployment might not be installed.	Follow these steps to mitigate the issue: $Settings = @{ "CloudName" = $Cloud; "RegionName" = $Region; "DeviceType" = "AzureEdge" } New-AzConnectedMachineExtension -Name "AzureEdgeTelemetryAndDiagnostics" -ResourceGroupName $ResourceGroup -MachineName $env:COMPUTERNAME -Location $Region -Publisher "Microsoft.AzureStack.Observability" -Settings $Settings -ExtensionType "TelemetryAndDiagnostics" -EnableAutomaticUpgrade New-AzConnectedMachineExtension -Name "AzureEdgeDeviceManagement" -ResourceGroupName $ResourceGroup -MachineName $env:COMPUTERNAME -Location $Region -Publisher "Microsoft.Edge" -ExtensionType "DeviceManagementExtension"

		New-AzConnectedMachineExtension -Name "AzureEdgeLifecycleManager" -ResourceGroupName $ResourceGroup -MachineName $env:COMPUTERNAME -Location $Region -Publisher "Microsoft.AzureStack.Orchestration" -ExtensionType "LcmController" New-AzConnectedMachineExtension -Name "AzureEdgeRemoteSupport" -ResourceGroupName $ResourceGroup -MachineName $env:COMPUTERNAME -Location $Region -Publisher "Microsoft.AzureStack.Observability" -ExtensionType "EdgeRemoteSupport" -EnableAutomaticUpgrade
Update	There's an intermittent issue in this release when the Azure portal incorrectly reports the update status as **Failed to update** or **In progress** though the update is complete.	Connect to your Azure Stack HCI via a remote PowerShell session. To confirm the update status, run the following PowerShell cmdlets: $Update = get-solutionupdate | ? version -eq "<version string>" Replace the version string with the version you're running. For example, "10.2405.0.23". $Update.state If the update status is **Installed**, no further action is required on your part. Azure portal refreshes the status correctly within 24 hours. To refresh the status sooner, follow these steps on one of the cluster nodes. Restart the Cloud Management cluster group. Stop-ClusterGroup "Cloud Management" Start-ClusterGroup "Cloud Management"
Update	During an initial MOC update, a failure occurs due to the target MOC	Follow these steps to mitigate the issue: 1. To find the MOC agent version, run the following

<table>
<tr>
<td></td>
<td>version not being found in the catalog cache. The follow-up updates and retries show MOC in the target version, without the update succeeding, and as a result the Arc Resource Bridge update fails.

To validate this issue, collect the update logs using Troubleshoot solution updates for Azure Stack HCI, version 23H2. The log files should show a similar error message (current version might differ in the error message):

[ERROR: { "errorCode": "InvalidEntityError", "errorResponse": "{\n\"message\": \"the cloud fabric (MOC) is currently at version v0.13.1. A minimum version of 0.15.0 is required for compatibility\"\n}" }]</td>
<td>command: 'C:\Program Files\AksHci\wssdcloudagent.exe' version.

2. Use the output of the command to find the MOC version from the table below that matches the agent version, and set $initialMocVersion to that MOC version. Set the $targetMocVersion by finding the Azure Stack HCI build you're updating to and get the matching MOC version from the following table. Use these values in the mitigation script provided below:

Expand table
<table>
<tr><th>Build</th><th>MOC version</th><th>Agent version</th></tr>
<tr><td>2311.2</td><td>1.0.24.10106</td><td>v0.13.0-6-gf13a73f7, v0.11.0-alp</td></tr>
<tr><td>2402</td><td>1.0.25.10203</td><td>v0.14.0, v0.13.1, 02/02/2024</td></tr>
<tr><td>2402.1</td><td>1.0.25.10302</td><td>v0.14.0, v0.13.1, 03/02/2024</td></tr>
<tr><td>2402.2</td><td>1.1.1.10314</td><td>v0.16.0-1-g04bf0dec, v0.15.1, 0</td></tr>
<tr><td>2405/2402.3</td><td>1.3.0.10418</td><td>v0.17.1, v0.16.5, 04/18/2024</td></tr>
</table>
For example, if the agent version is v0.13.0-6-gf13a73f7, v0.11.0-alpha.38,01/06/2024, then $initialMocVersion = "1.0.24.10106" and if you are updating to 2405.0.23, then $targetMocVersion = "1.3.0.10418".

3. Run the following PowerShell commands on the first node:

$initialMocVersion = "<initial version determined from step 2>"
$targetMocVersion = "<target version determined from step 2>"

Import MOC module twice
import-module moc
import-module moc</td>
</tr>
</table>

		$verbosePreference = "Continue" # Clear the SFS catalog cache Remove-Item (Get-MocConfig).manifestCache # Set version to the current MOC version prior to update, and set state as update failed Set-MocConfigValue -name "version" -value $initialMocVersion Set-MocConfigValue -name "installState" -value ([InstallState]::UpdateFailed) # Rerun the MOC update to desired version Update-Moc -version $targetMocVersion 4. Resume the update.
AKS on HCI	AKS cluster creation fails with the Error: Invalid AKS network resource id. This issue can occur when the associated logical network name has an underscore.	Underscores aren't supported in logical network names. Make sure to not use underscore in the names for logical networks deployed on your Azure Stack HCI.
Repair server	In rare instances, the Repair-Server operation fails with the HealthServiceWaitForDriveFW error. In these cases, the old drives from the repaired node aren't removed and new disks are stuck in the maintenance mode.	To prevent this issue, make sure that you DO NOT drain the node either via the Windows Admin Center or using the Suspend-ClusterNode -Drain PowerShell cmdlet before you start Repair-Server. If the issue occurs, contact Microsoft Support for next steps.

Repair server	This issue is seen when the single node Azure Stack HCI instance is updated from 2311 to 2402 and then the Repair-Server is performed. The repair operation fails.	Before you repair the single node, follow these steps: 1. Run version 2402 for the *ADPrepTool*. Follow the steps in Prepare Active Directory. This action is quick and adds the required permissions to the Organizational Unit (OU). 2. Move the computer object from **Computers** segment to the root OU. Run the following command: Get-ADComputer <HOSTNAME> | Move-ADObject -TargetPath "<OU path>"
Deployment	If you prepare the Active Directory on your own (not using the script and procedure provided by Microsoft), your Active Directory validation could fail with missing Generic All permission. This is due to an issue in the validation check that checks for a dedicated permission entry for msFVE-RecoverInformationobjects – General – Permissions Full control, which is required for BitLocker recovery.	Use the Prepare AD script method or if using your own method, make sure to assign the specific permission msFVE-RecoverInformationobjects – General – Permissions Full control.
Deployment	There's a rare issue in this release where the DNS record is deleted during the Azure Stack HCI deployment. When that occurs, the following exception is seen:	Check the DNS server to see if any DNS records of the cluster nodes are missing. Apply the following mitigation on the nodes where its DNS record is missing. Restart the DNS client service. Open a PowerShell session and run the following cmdlet on the affected node: Taskkill /f /fi "SERVICES eq dnscache"

	Type 'PropagatePublicRootCertificate' of Role 'ASCA' raised an exception: The operation on computer 'ASB88RQ22U09' failed: WinRM cannot process the request. The following error occurred while using Kerberos authentication: Cannot find the computer ASB88RQ22U09.local. Verify that the computer exists on the network and that the name provided is spelled correctly at PropagatePublicRootCertificate, C:\NugetStore\Microsoft.AzureStack, at Orchestration.Roles.CertificateAuthority.10.2402.0.14\content\Classes\ASCA\ASCA.psm1: line 38, at C:\CloudDeployment\ECEngine\InvokeInterfaceInternal.psm1: line 127,at Invoke-EceInterfaceInternal, C:\CloudDeployment\ECEngine\InvokeInterfaceInternal.psm1: line 123.	

Deployment	In this release, there's a remote task failure on a multi-node deployment that results in the following exception: `ECE RemoteTask orchestration failure with ASRR1N42R01U31 (node pingable - True): A WebException occurred while sending a RestRequest. WebException.Status: ConnectFailure on [https://<URL>](https://<URL>).`	The mitigation is to restart the ECE agent on the affected node. On your machine, open a PowerShell session and run the following command: `Restart-Service ECEAgent`.
Add server	In this release and previous releases, when adding a machine to the cluster, is not possible to update the proxy bypass list string to include the new machine. Updating environment variables proxy bypass list on the hosts will not update the proxy bypass list on Azure Resource Bridge or AKS.	There's no workaround in this release. If you encounter this issue, contact Microsoft Support to determine next steps.
Add/Repair server	In this release, when adding or repairing a machine, a failure is seen when the software load balancer or network controller VM	There's no workaround in this release. If you encounter this issue, contact Microsoft Support to determine next steps.

	certificates are being copied from the existing nodes. The failure is because these certificates weren't generated during the deployment/update.	
Deployment	In this release, there's a transient issue resulting in the deployment failure with the following exception: Type 'SyncDiagnosticLevel' of Role 'ObservabilityConfig' raised an exception:* *Syncing Diagnostic Level failed with error: The Diagnostic Level does not match. Portal was not set to Enhanced, instead is Basic.	As this is a transient issue, retrying the deployment should fix this. For more information, see how to Rerun the deployment.
Deployment	In this release, there's an issue with the Secrets URI/location field. This is a required field that is marked *Not mandatory* and results in Azure Resource Manager template deployment failures.	Use the sample parameters file in the Deploy Azure Stack HCI, version 23H2 via Azure Resource Manager template to ensure that all the inputs are provided in the required format and then try the deployment. If there's a failed deployment, you must also clean up the following resources before you Rerun the deployment: 1. Delete C:\EceStore. 2. Delete C:\CloudDeployment. 3. Delete C:\nugetstore. 4. Remove-Item HKLM:\Software\Microsoft\LCMAzureStackStampInformation.

Security	For new deployments, Secured-core capable devices won't have Dynamic Root of Measurement (DRTM) enabled by default. If you try to enable (DRTM) using the Enable-AzSSecurity cmdlet, you see an error that DRTM setting isn't supported in the current release. Microsoft recommends defense in depth, and UEFI Secure Boot still protects the components in the Static Root of Trust (SRT) boot chain by ensuring that they're loaded only when they're signed and verified.	DRTM isn't supported in this release.
Networking	An environment check fails when a proxy server is used. By design, the bypass list is different for winhttp and wininet, which causes the validation check to fail.	Follow these workaround steps: 1. Clear the proxy bypass list prior to the health check and before starting the deployment or the update. 2. After passing the check, wait for the deployment or update to fail. 3. Set your proxy bypass list again.
Arc VM management	Deployment or update of Arc Resource Bridge could fail when the automatically generated	Retry the deployment/update. The retry should regenerate the SPN secret and the operation will likely succeed.

	temporary SPN secret during this operation, starts with a hyphen.	

Arc VM management	Arc Extensions on Arc VMs stay in "Creating" state indefinitely.	Sign in to the VM, open a command prompt, and type the following:
		Windows:
		`notepad C:\ProgramData\AzureConnectedMachineAgent\Config\agentconfig.json`
		Linux:
		`sudo vi /var/opt/azcmagent/agentconfig.json`
		Next, find the `resourcename` property. Delete the GUID that is appended to the end of the resource name, so this property matches the name of the VM. Then restart the VM.

Arc VM management	When a new machine is added to an Azure Stack HCI instance, storage path isn't created automatically for the newly created volume.	You can manually create a storage path for any new volumes. For more information, see Create a storage path.
Arc VM management	Restart of Arc VM operation completes after approximately 20 minutes although the VM itself restarts in about a minute.	There's no known workaround in this release.
Arc VM management	In some instances, the status of the logical network shows as Failed in Azure portal. This occurs when you try to delete the logical network without first deleting any resources such as network	If the status of this logical network was *Succeeded* at the time when this network was provisioned, then you can continue to create resources on this network.

	interfaces associated with that logical network. You should still be able to create resources on this logical network. The status is misleading in this instance.	
Arc VM management	In this release, when you update a VM with a data disk attached to it using the Azure CLI, the operation fails with the following error message: *Couldn't find a virtual hard disk with the name*.	Use the Azure portal for all the VM update operations. For more information, see Manage Arc VMs and Manage Arc VM resources.
Update	In rare instances, you may encounter this error while updating your Azure Stack HCI instance: Type 'UpdateArbAndExtensions' of Role 'MocArb' raised an exception: Exception Upgrading ARB and Extension in step [UpgradeArbAndExtensions :Get-ArcHciConfig] UpgradeArb: Invalid applianceyaml = [C:\AksHci\hci-appliance.yaml].	If you see this issue, contact Microsoft Support to assist you with the next steps.

Networking	There's an infrequent DNS client issue in this release that causes the deployment to fail on a two-node cluster with a DNS resolution error: *A WebException occurred while sending a RestRequest. WebException.Status: NameResolutionFailure*. As a result of the bug, the DNS record of the second node is deleted soon after it's created resulting in a DNS error.	Restart the machine. This operation registers the DNS record, which prevents it from getting deleted.
Azure portal	In some instances, the Azure portal might take a while to update and the view might not be current.	You might need to wait for 30 minutes or more to see the updated view.
Arc VM management	Deleting a network interface on an Arc VM from Azure portal doesn't work in this release.	Use the Azure CLI to first remove the network interface and then delete it. For more information, see Remove the network interface and see Delete the network interface.
Deployment	Providing the OU name in an incorrect syntax isn't detected in the Azure portal. The incorrect syntax includes unsupported characters such as &,",',<,>. The incorrect syntax is detected at a later step	Make sure that the OU path syntax is correct and doesn't include unsupported characters.

	during cluster validation.	
Deployment	Deployments via Azure Resource Manager time out after 2 hours. Deployments that exceed 2 hours show up as failed in the resource group though the cluster is successfully created.	To monitor the deployment in the Azure portal, go to the Azure Stack HCI instance resource and then go to new **Deployments** entry.
Azure Site Recovery	Azure Site Recovery can't be installed on an Azure Stack HCI instance in this release.	There's no known workaround in this release.

Update	When updating the Azure Stack HCI instance via the Azure Update Manager, the update progress and results may not be visible in the Azure portal.	To work around this issue, on each cluster node, add the following registry key (no value needed):
		
		`New-Item -Path "HKLM:\SYSTEM\CurrentControlSet\Services\HciCloudManagementSvc\Parameters" -force`
		
		Then on one of the cluster nodes, restart the Cloud Management cluster group.
		
		`Stop-ClusterGroup "Cloud Management"`
		
		`Start-ClusterGroup "Cloud Management"`
		
		This won't fully remediate the issue as the progress details may still not be displayed for a duration of the update process. To get the latest update details, you can Retrieve the update progress with PowerShell.

Update	In rare instances, if a failed update is stuck in	To resume the update, run the following PowerShell command: `Get-SolutionUpdate|Start-SolutionUpdate`.

	an *In progress* state in Azure Update Manager, the **Try again** button is disabled.	
Update	In some cases, SolutionUpdate commands could fail if run after the Send-DiagnosticData command.	Make sure to close the PowerShell session used for Send-DiagnosticData. Open a new PowerShell session and use it for SolutionUpdate commands.
Update	In rare instances, when applying an update from 2311.0.24 to 2311.2.4, cluster status reports *In Progress* instead of expected *Failed to update*.	Retry the update. If the issue persists, contact Microsoft Support.
Update	Attempts to install solution updates can fail at the end of the CAU steps with: There was a failure in a Common Information Model (CIM) operation, that is, an operation performed by software that Cluster-Aware Updating depends on. This rare issue occurs if the Cluster Name or Cluster IP Address resources fail to start after a node reboot and is most typical in small clusters.	If you encounter this issue, contact Microsoft Support for next steps. They can work with you to manually restart the cluster resources and resume the update as needed.

Update	When applying a cluster update to 10.2402.3.11 the `Get-SolutionUpdate` cmdlet may not respond and eventually fails with a RequestTimeoutException after approximately 10 minutes. This is likely to occur following an add or repair server scenario.	Use the `Start-ClusterGroup` and `Stop-ClusterGroup` cmdlets to restart the update service.
		
		`Get-ClusterGroup -Name "Azure Stack HCI Update Service Cluster Group" | Stop-ClusterGroup`
		
		`Get-ClusterGroup -Name "Azure Stack HCI Update Service Cluster Group" | Start-ClusterGroup`
		
		A successful run of these cmdlets should bring the update service online.

Cluster aware updating	Resume node operation failed to resume node.	This is a transient issue and could resolve on its own. Wait for a few minutes and retry the operation. If the issue persists, contact Microsoft Support.
Cluster aware updating	Suspend node operation was stuck for greater than 90 minutes.	This is a transient issue and could resolve on its own. Wait for a few minutes and retry the operation. If the issue persists, contact Microsoft Support.

Next steps

Read the Deployment overview.