Azure Stack 1903 update | Microsoft Docs

Azure Stack 1903 update

Applies to: Azure Stack integrated systems

This article describes the contents of the 1903 update package. The update includes improvements, fixes, and new features for this version of Azure Stack. This article also describes known issues in this release, and includes a link to download the update. Known issues are divided into issues directly related to the update process, and issues with the build (post-installation).

[!IMPORTANT] This update package is only for Azure Stack integrated systems. Do not apply this update package to the Azure Stack Development Kit.

Archived release notes

You can see older versions of Azure Stack release notes on the TechNet Gallery. These archived release notes are provided for reference purposes only and do not imply support for these versions. For further assistance, contact Microsoft Customer Support Services.

Build reference

The Azure Stack 1903 update build number is **1.1903.0.35**.

Update type

The Azure Stack 1903 update build type is **Express**. For more information about update build types, see the Manage updates in Azure Stack article. The expected time it takes for the 1903 update to complete is approximately 16 hours, but exact times can vary. This runtime approximation is specific to the 1903 update and should not be compared to other Azure Stack updates.

[!IMPORTANT] The 1903 payload does not include an ASDK release.

Hotfixes

Azure Stack releases hotfixes on a regular basis. Be sure to install the latest Azure Stack hotfix for 1902 before updating Azure Stack to 1903.

Azure Stack hotfixes are only applicable to Azure Stack integrated systems; do not attempt to install hotfixes on the ASDK.

[!TIP] Subscribe to the following *RSS* or *Atom* feeds to keep up with Azure Stack hotfixes: - RSS - Atom

Azure Stack hotfixes

- **1902**: KB 4500637 - Azure Stack hotfix 1.1902.3.75
- **1903**: KB 4500638 - Azure Stack hotfix 1.1903.2.39

Improvements

- Fixed a bug in networking that prevented changes to the **idle timeout (minutes)** value of a **Public IP Address** from taking effect. Previously, changes to this value were ignored, so that regardless of any changes you made, the value would default to 4 minutes. This setting controls how many minutes to keep a TCP connection open without relying on clients to send keep-alive messages. Note this bug only affected instance level public IPs, not public IPs assigned to a load balancer.
- Improvements to the reliability of the update engine, including auto-remediation of common issues so that updates apply without interruption.
- Improvements to the detection and remediation of low disk space conditions.
- Azure Stack now supports Windows Azure Linux agents greater than version 2.2.35. This support allows customers to maintain consistent Linux images between Azure and Azure Stack. It was added as part of the 1901 and 1902 hotfixes.

Secret management

- Azure Stack now supports rotation of the root certificate used by certificates for external secret rotation. For more information, see this article.
- 1903 contains performance improvements for secret rotation that reduce the time that it takes to execute internal secret rotation.

Prerequisites

[!IMPORTANT] Install the latest Azure Stack hotfix for 1902 (if any) before updating to 1903.

- Make sure to use the latest version of the Azure Stack capacity planner to do your workload planning and sizing. The latest version contains bug fixes and provides new features that are released with each Azure Stack update.
- Before you start installation of this update, run Test-AzureStack with the following parameter to validate the status of your Azure Stack and resolve any operational issues found, including all warnings and failures. Also review active alerts, and resolve any that require action:

```
Test-AzureStack -Group UpdateReadiness
```

- When Azure Stack is managed by System Center Operations Manager, make sure to update the Management Pack for Microsoft Azure Stack to version 1.0.3.11 before applying 1903.

- The package format for the Azure Stack update has changed from **.bin/.exe/.xml** to **.zip/.xml** starting with the 1902 release. Customers with connected Azure Stack scale units will see the **Update available** message in the portal. Customers that are not connected can now simply download and import the .zip file with the corresponding .xml.

Known issues with the update process

- When attempting to install an Azure Stack update, the status for the update might fail and change state to **PreparationFailed**. This is caused by the update resource provider (URP) being unable to properly transfer the files from the storage container to an internal infrastructure share for processing. Starting with version 1901 (1.1901.0.95), you can work around this issue by clicking **Update now** again (not **Resume**). The URP then cleans up the files from the previous attempt, and starts the download again.
- When you run Test-AzureStack, a warning message from the Baseboard Management Controller (BMC) is displayed. You can safely ignore this warning.
- During installation of this update, you might see alerts with the title **Error - Template for FaultType UserAccounts. New is missing.** You can safely ignore these alerts. The alerts close automatically after the installation of this update completes.

Post-update steps

- After the installation of this update, install any applicable hotfixes. For more information, see Hotfixes, as well as our Servicing Policy.
- Retrieve the data at rest encryption keys and securely store them outside of your Azure Stack deployment. Follow the instructions on how to retrieve the keys.

Known issues (post-installation)

The following are post-installation known issues for this build version.

Portal

- In the user portal dashboard, when you try to click on the **Feedback** tile, an empty browser tab opens. As a workaround, you can use Azure Stack User Voice to file a user voice request.
- In both the administrator and user portals, if you search for "Docker," the item is incorrectly returned. It is not available in Azure Stack. If you try to create it, a blade with an error indication is displayed.
- Plans that are added to a user subscription as an add-on plan cannot be deleted, even when you remove the plan from the user subscription. The plan will remain until the subscriptions that reference the add-on plan are also deleted.
- The two administrative subscription types that were introduced with version 1804 should not be used. The subscription types are **Metering subscription**, and

Consumption subscription. These subscription types are visible in new Azure Stack environments beginning with version 1804 but are not yet ready for use. You should continue to use the **Default Provider** subscription type.

- Deleting user subscriptions results in orphaned resources. As a workaround, first delete user resources or the entire resource group, and then delete the user subscriptions.
- You cannot view permissions to your subscription using the Azure Stack portals. As a workaround, use PowerShell to verify permissions.
- In the user portal, when you navigate to a blob within a storage account and try to open **Access Policy** from the navigation tree, the subsequent window fails to load. To work around this issue, the following PowerShell cmdlets enable creating, retrieving, setting and deleting access policies, respectively:
- New-AzureStorageContainerStoredAccessPolicy
- Get-AzureStorageContainerStoredAccessPolicy
- Set-AzureStorageContainerStoredAccessPolicy
- Remove-AzureStorageContainerStoredAccessPolicy
- In the user portal, when you try to upload a blob using the **OAuth(preview)** option, the task fails with an error message. To work around this issue, upload the blob using the **SAS** option.
- When logged into the Azure Stack portals you might see notifications about the public Azure portal. You can safely ignore these notifications, as they do not currently apply to Azure Stack (for example, "1 new update - The following updates are now available: Azure portal April 2019 update").
- In the user portal dashboard, when you select the **Feedback** tile, an empty browser tab opens. As a workaround, you can use Azure Stack User Voice to file a User Voice request.

Compute

- When creating a new Windows Virtual Machine (VM), the following error may be displayed:

```
'Failed to start virtual machine 'vm-name'. Error: Failed to update serial
output settings for VM 'vm-name'
```

The error occurs if you enable boot diagnostics on a VM but delete your boot diagnostics storage account. To work around this issue, recreate the storage account with the same name as you used previously.

- The Virtual Machine Scale Set creation experience provides CentOS-based 7.2 as an option for deployment. Because that image is not available on Azure Stack Marketplace, either select another operating system for your deployment, or use an

Azure Resource Manager template specifying another CentOS image that has been downloaded prior to deployment from the marketplace by the operator.

- After applying the 1903 update, you might encounter the following issues when deploying VMs with Managed Disks:
- If the subscription was created before the 1808 update, deploying a VM with Managed Disks might fail with an internal error message. To resolve the error, follow these steps for each subscription:
    1. In the Tenant portal, go to **Subscriptions** and find the subscription. Select **Resource Providers**, then select **Microsoft.Compute**, and then click **Re-register**.
    2. Under the same subscription, go to **Access Control (IAM)**, and verify that **Azure Stack - Managed Disk** is listed.
- If you have configured a multi-tenant environment, deploying VMs in a subscription associated with a guest directory might fail with an internal error message. To resolve the error, follow these steps in this article to reconfigure each of your guest directories.
- An Ubuntu 18.04 VM created with SSH authorization enabled will not allow you to use the SSH keys to sign in. As a workaround, use VM access for the Linux extension to implement SSH keys after provisioning, or use password-based authentication.
- If you do not have a Hardware Lifecycle Host (HLH): before build 1902, you had to set group policy **Computer ConfigurationSettingsSettingsPoliciesOptions** to **Send LM & NTLM - use NTLMv2 session security if negotiated**. Since build 1902, you must leave it as **Not Defined** or set it to **Send NTLMv2 response only** (which is the default value). Otherwise, you won't be able to establish a PowerShell remote session and you will see an **Access is denied** error:

```
powershell    $Session = New-PSSession -ComputerName x.x.x.x -
ConfigurationName PrivilegedEndpoint -Credential $Cred    New-PSSession :
[x.x.x.x] Connecting to remote server x.x.x.x failed with the following error
message : Access is denied. For more information, see the
about_Remote_Troubleshooting Help topic.    At line:1 char:12    + $Session =
New-PSSession -ComputerName x.x.x.x -ConfigurationNa ...    +
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~       +
CategoryInfo          : OpenError:
(System.Manageme....RemoteRunspace:RemoteRunspace) [New-PSSession],
PSRemotingTransportException       + FullyQualifiedErrorId :
AccessDenied,PSSessionOpenFailed
```

- You cannot remove a scale set from the **Virtual Machine Scale Sets** blade. As a workaround, select the scale set that you want to remove, then click the **Delete** button from the **Overview** pane.
- Creating VMs in an availability set of 3 fault domains and creating a virtual machine scale set instance fails with a

FabricVmPlacementErrorUnsupportedFaultDomainSize error during the update process on a 4-node Azure Stack environment. You can create single VMs in an availability set with 2 fault domains successfully. However, scale set instance creation is still not available during the update process on a 4-node Azure Stack.

Networking

- In the Azure Stack portal, when you change a static IP address for an IP configuration that is bound to a network adapter attached to a VM instance, you will see a warning message that states

  ```
  The virtual machine associated with this network interface will be
  restarted to utilize the new private IP address...
  ```

  You can safely ignore this message; the IP address will be changed even if the VM instance does not restart.

- In the portal, if you add an inbound security rule and select **Service Tag** as the source, several options are displayed in the **Source Tag** list that are not available for Azure Stack. The only options that are valid in Azure Stack are as follows:

- **Internet**
- **VirtualNetwork**
- **AzureLoadBalancer**

The other options are not supported as source tags in Azure Stack. Similarly, if you add an outbound security rule and select **Service Tag** as the destination, the same list of options for **Source Tag** is displayed. The only valid options are the same as for **Source Tag**, as described in the previous list.

- Network security groups (NSGs) do not work in Azure Stack in the same way as global Azure. In Azure, you can set multiple ports on one NSG rule (using the portal, PowerShell, and Resource Manager templates). In Azure Stack however, you cannot set multiple ports on one NSG rule via the portal. To work around this issue, use a Resource Manager template or PowerShell to set these additional rules.
- Azure Stack does not support attaching more than 4 Network Interfaces (NICs) to a VM instance today, regardless of the instance size.

App Service

- Tenants must register the storage resource provider before creating their first Azure Function in the subscription.
- Some tenant portal user experiences are broken due to an incompatibility with the portal framework in 1903; principally, the UX for deployment slots, testing in production and site extensions. To work around this issue, use the Azure App Service PowerShell module or the Azure CLI. The portal experience will be restored in the upcoming release of Azure App Service on Azure Stack 1.6 (Update 6).

Syslog

- The syslog configuration is not persisted through an update cycle, causing the syslog client to lose its configuration, and the syslog messages to stop being forwarded. This issue applies to all versions of Azure Stack since the GA of the syslog client (1809). To work around this issue, reconfigure the syslog client after applying an Azure Stack update.

Download the update

You can download the Azure Stack 1903 update package from here.

In connected scenarios only, Azure Stack deployments periodically check a secured endpoint and automatically notify you if an update is available for your cloud. For more information, see managing updates for Azure Stack.

Next steps

- For an overview of the update management in Azure Stack, see Manage updates in Azure Stack overview.
- For more information about how to apply updates with Azure Stack, see Apply updates in Azure Stack.
- To review the servicing policy for Azure Stack integrated systems, and what you must do to keep your system in a supported state, see Azure Stack servicing policy.
- To use the Privileged End Point (PEP) to monitor and resume updates, see Monitor updates in Azure Stack using the privileged endpoint.