Azure Stack 1902 update | Microsoft Docs

Azure Stack 1902 update

Applies to: Azure Stack integrated systems

This article describes the contents of the 1902 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 1902 update build number is **1.1902.0.69**.

Update type

The Azure Stack 1902 update build type is **Full**. For more information about update build types, see the Manage updates in Azure Stack article.

Hotfixes

Azure Stack releases hotfixes on a regular basis. Be sure to install the latest Azure Stack hotfix for 1901 before updating Azure Stack to 1902.

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

- **1901**: KB 4500636 - Azure Stack hotfix 1.1901.5.109
- **1902**: KB 4500637 - Azure Stack hotfix 1.1902.3.75

Prerequisites

[!IMPORTANT] You can install 1902 directly from either the **1.1901.0.95** or **1.1901.0.99** release, without first installing any 1901 hotfix. However, if you have installed the older **1901.2.103** hotfix, you must install the newer 1901.3.105 hotfix before proceeding to 1902.

- Before you start installation of this update, run Test-AzureStack with the following parameters 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 -Include AzsDefenderSummary, AzsHostingInfraSummary,
  AzsHostingInfraUtilization, AzsInfraCapacity, AzsInfraRoleSummary,
  AzsPortalAPISummary, AzsSFRoleSummary, AzsStampBMCSummary,
  AzsHostingServiceCertificates
  ```

If the `AzsControlPlane` parameter is included when **Test-AzureStack** is executed, you will see the following failure in the **Test-AzureStack** output: **FAIL Azure Stack Control Plane Websites Summary**. You can safely ignore this specific error.

- When Azure Stack is managed by System Center Operations Manager (SCOM), make sure to update the Management Pack for Microsoft Azure Stack to version 1.0.3.11 before applying 1902.

- 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.

Improvements

- The 1902 build introduces a new user interface on the Azure Stack Administrator portal for creating plans, offers, quotas, and add-on plans. For more information, including screenshots, see Create plans, offers, and quotas.
- Improvements to the reliability of capacity expansion during an add node operation when switching the scale unit state from "Expanding storage" to "Running".
- To improve package integrity and security, as well as easier management for offline ingestion, Microsoft has changed the format of the Update package from .exe and .bin files to a .zip file. The new format adds additional reliability of the unpacking process that at times, can cause the preparation of the update to stall. The same package format also applies to update packages from your OEM.
- To improve the Azure Stack operator experience when running Test-AzureStack, operators can now simply use, "Test-AzureStack -Group UpdateReadiness" as opposed to passing ten additional parameters after an Include statement.

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

- To improve on the overall reliability and availability of core infrastructure services during the update process, the native Update resource provider as part of the update action plan will detect and invoke automatic global remediations as-needed. Global remediation "repair" workflows include:

- Checking for infrastructure virtual machines that are in a non-optimal state and attempt to repair them as-needed.
- Check for SQL service issues as part of the control plan and attempt to repair them as-needed.
- Check the state of the Software Load Balancer (SLB) service as part of the Network Controller (NC) and attempt to repair them as-needed.
- Check the state of the Network Controller (NC) service and attempt to repair it as needed
- Check the state of the Emergency Recovery Console Service (ERCS) service fabric nodes and repair them as needed.
- Check the state of the infrastructure role and repair as needed.

- Check the state of the Azure Consistent Storage (ACS) service fabric nodes and repair them as needed.

- Improvements to Azure stack diagnostic tools to improve log collection reliability and performance. Additional logging for networking and identity services.
- Improvements to the reliability of Test-AzureStack for secret rotation readiness test.
- Improvements to increase AD Graph reliability when communicating with customer's Active Directory environment

- Improvements hardware inventory collection in Get-AzureStackStampInformation.

- To improve reliability of operations running on ERCS infrastructure, the memory for each ERCS instance increases from 8 GB to 12 GB. On an Azure Stack integrated systems installation, this results in a 12 GB increase overall.

- 1902 fixes an issue in the Network Controllers VSwitch Service, in which all VMs on a specific node went offline. The issue caused it to get stuck in a primary loss state, where the primary cannot be contacted but the role has not been failed over to another, healthy instance, which could only be resolved by contacting Microsoft support services.

[!IMPORTANT] To make sure the patch and update process results in the least amount of tenant downtime, make sure your Azure Stack stamp has more than 12 GB of available space in the **Capacity** blade. You can see this memory increase reflected in the **Capacity** blade after a successful installation of the update.

Common vulnerabilities and exposures

This update installs the following security updates:
- ADV190005 - CVE-2019-0595 - CVE-2019-0596 - CVE-2019-0597 - CVE-2019-0598 - CVE-2019-0599 - CVE-2019-0600 - CVE-2019-0601 - CVE-2019-0602 - CVE-2019-0615 - CVE-2019-0616 - CVE-2019-0618 - CVE-2019-0619 - CVE-2019-0621 - CVE-2019-0623 -

CVE-2019-0625 - CVE-2019-0626 - CVE-2019-0627 - CVE-2019-0628 - CVE-2019-0630 - CVE-2019-0631 - CVE-2019-0632 - CVE-2019-0633 - CVE-2019-0635 - CVE-2019-0636 - CVE-2019-0656 - CVE-2019-0659 - CVE-2019-0660 - CVE-2019-0662 - CVE-2019-0663

For more information about these vulnerabilities, click on the preceding links, or see Microsoft Knowledge Base articles 4487006.

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 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

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, 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 1902 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 log in. As a workaround, use VM access for the Linux extension to implement SSH keys after provisioning, or use password-based authentication.

- 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.
- In the user portal, if you attempt to add a **Backend Pool** to a **Load Balancer**, the operation fails with the error message **Failed to update Load Balancer....** To work around this issue, use PowerShell, CLI, or an Azure Resource Manager template to associate the backend pool with a load balancer resource.
- In the user portal, if you attempt to create an **Inbound NAT Rule** for a **Load Balancer**, the operation fails with the error message **Failed to update Load Balancer....** To work around this issue, use PowerShell, CLI, or an Azure Resource Manager template to associate the backend pool with a load balancer resource.
- In the user portal, the **Create Load Balancer** window shows an option to create a **Standard** load balancer SKU. This option is not supported in Azure Stack.

App Service

- You must register the storage resource provider before you create your first Azure Function in the subscription.

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 1902 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.