Azure Stack 1904 release notes | Microsoft Docs

Azure Stack 1904 update

Applies to: Azure Stack integrated systems

This article describes the contents of the 1904 update package. The update includes what's new improvements, and fixes for this release of Azure Stack. This article contains the following information:

- Description of what's new, improvements, fixes, and security updates
- Update planning

[!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 1904 update build number is **1.1904.0.36**.

Update type

The Azure Stack 1904 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 1904 update to complete is approximately 16 hours, but exact times can vary. This runtime approximation is specific to the 1904 update and should not be compared to other Azure Stack updates.

What's in this update

Improvements

- Significant improvements have been made to the Software Defined Networking (SDN) Stack in 1904. These improvements increase the overall servicing and reliability of the SDN stack in Azure Stack.
- Added a notification in the administrator portal, when the currently logged in user does not have the necessary permissions, which enables the dashboard to load properly. It also contains a link to the documentation that explains which accounts

have the appropriate permissions, depending on the identity provider used during deployment.

- Added improvements to VM resiliency and uptime, which resolves the scenario in which all VMs go offline if the storage volume containing the VM configuration files goes offline.

- Added optimization to the number of VMs evacuated concurrently and placed a cap on bandwidth consumed, to address VM brownouts or blackouts if the network is under heavy load. This change increases VM uptime when a system is updating.

- Improved resource throttling when a system is running at scale to protect against internal processes exhausting platform resources, resulting in failed operations in the portal.

- Improved filtering capabilities enable operators to apply multiple filters at the same time. You can only sort on the **Name** column in the new user interface.

- Improvements to the process of deleting offers, plans, quotas, and subscriptions. You can now successfully delete offers, quotas, plans, and subscriptions from the Administrator portal if the object you want to delete has no dependencies. For more information, see this article.

- Improved syslog message volume by filtering out unnecessary events and providing a configuration parameter to select desired severity level for forwarded messages. For more information about how to configure the severity level, see Azure Stack datacenter integration - syslog forwarding.

- Added a new capability to the **Get-AzureStackLog** cmdlet by incorporating an additional parameter, `-OutputSASUri`. You can now collect Azure Stack logs from your environment and store them in the specified Azure Storage blob container. For more information, see Azure Stack diagnostics.

- Added a new memory check in the **Test-AzureStack** `UpdateReadiness` group, which checks to see if you have enough memory available on the stack for the update to complete successfully.

- Improvements to **Test-AzureStack** for evaluating Service Fabric health.
- Improvements to hardware updates, which reduces the time it takes to complete drive firmware update to 2-4 hours. The update engine dynamically determines which portions of the update need to execute, based on content in the package.
- Added robust operation prechecks to prevent disruptive infrastructure role instance operations that affect availability.
- Improvements to idempotency of infrastructure backup action plan.

- Improvements to Azure Stack log collection. These improvements reduce the time it takes to retrieve the set of logs. Also, the Get-AzureStackLog cmdlet no longer generates default logs for the OEM role. You must execute the Invoke-

AzureStackOnDemandLog cmdlet, specifying the role to retrieve the OEM logs. For more information , see Azure Stack diagnostics.

- Azure Stack now monitors the federation data URL provided for datacenter integration with ADFS. This improves reliability during secret rotation of the customer ADFS instance or farm.

Changes

- Removed the option for Azure Stack operators to shut down infrastructure role instances in the administrator portal. The restart functionality ensures a clean shutdown attempt before restarting the infrastructure role instance. For advanced scenarios, the API and PowerShell functionality remains available.
- There is a new Marketplace management experience, with separate screens for Marketplace images and resource providers. For now, the **Resource providers** window is empty, but in future releases new PaaS service offerings will appear and be managed in the **Resource providers** window.
- Changes to the update experience in the operator portal. There is a new grid for resource provider updates. The ability to update resource providers is not available yet.
- Changes to the update installation experience in the operator portal. To help Azure Stack operators respond appropriately to an update issue, the portal now provides more specific recommendations based on the health of the scale unit, as derived automatically by running **Test-AzureStack** and parsing the results. Based on the result, it will inform the operator to take one of two actions:
- A "soft" warning alert is displayed in the portal that reads "The most recent update needs attention. Microsoft recommends opening a service request during normal business hours. As part of the update process, Test-AzureStack is performed, and based on the output we generate the most appropriate alert. In this case, Test-AzureStack passed."
- A "hard" critical alert is displayed in the portal that reads, "The most recent update failed. Microsoft recommends opening a service request as soon as possible. As part of the update process, Test-AzureStack is performed, and based on the output we generate the most appropriate alert. In this case, Test-AzureStack also failed."
- Updated Azure Linux Agent version 2.2.38.0. This support allows customers to maintain consistent Linux images between Azure and Azure Stack.
- Changes to the update logs in the operator portal. Requests to retrieve successful update logs are no longer available. Failed update logs, because they are actionable for diagnostics, are still available for download.

Fixes

- Fixed an issue in which the syslog configuration was not persisted through an update cycle, causing the syslog client to lose its configuration, and the syslog messages to stop being forwarded. Syslog configuration is now preserved.
- Fixed an issue in CRP that blocked deallocation of VMs. Previously, if a VM contained multiple large managed disks, deallocating the VM might have failed with a timeout error.
- Fixed issue with Windows Defender engine impacting access to scale-unit storage.
- Fixed a user portal issue in which the Access Policy window for blob storage accounts failed to load.
- Fixed an issue in both administrator and user portals, in which erroneous notifications about the global Azure portal were displayed.
- Fixed a user portal issue in which selecting the **Feedback** tile caused an empty browser tab to open.
- Fixed a portal issue in which changing a static IP address for an IP configuration that was bound to a network adapter attached to a VM instance, caused an error message to be displayed.
- Fixed a user portal issue in which attempting to **Attach Network Interface** to an existing VM via the **Networking** window caused the operation to fail with an error message.
- Fixed an issue in which Azure Stack did not support attaching more than 4 Network Interfaces (NICs) to a VM instance.
- Fixed a portal issue in which adding an inbound security rule and selecting **Service Tag** as the source, displayed several options that are not available for Azure Stack.
- Fixed the issue in which Network Security Groups (NSGs) did not work in Azure Stack in the same way as global Azure.
- Fixed an issue in Marketplace management, which hides all downloaded products if registration expires or is removed.
- Fixed an issue in which issuing a **Set-AzureRmVirtualNetworkGatewayConnection** command in PowerShell to an existing virtual network gateway connection failed with the error message **Invalid shared key configured...**.
- Fixed an issue that caused the Network Resource Provider (NRP) to be out of sync with the network controller, resulting in duplicate resources being requested. In some cases, this resulted in leaving the parent resource in an error state.
- Fixed an issue in which if a user that was assigned a contributor role to a subscription, but was not explicitly given read permissions, an error was generated that read **...The**

client 'somelogonaccount@domain.com' with object ID {GUID} does not have authorization to perform action... when attempting to save a change to a resource.

- Fixed an issue in which the marketplace management screen was empty if the offline syndication tool was used to upload images, and any one of them was missing the icon URI(s).

- Fixed an issue which prevented products that failed to download from being deleted in marketplace management.

Security updates

This update of Azure Stack does not include security updates to the underlying operating system which hosts Azure Stack. For information, see Azure Stack security updates.

Update planning

Before applying the update, make sure to review the following information:

- Known issues
- Security updates
- Checklist of activities before and after applying the update

[!NOTE] Make sure to use the latest version of the Azure Stack Capacity Planner tool to perform your workload planning and sizing. The latest version contains bug fixes and provides new features that are released with each Azure Stack update.

Download the update

You can download the Azure Stack 1904 update package from the Azure Stack download page.

Hotfixes

Azure Stack releases hotfixes on a regular basis. Be sure to install the latest Azure Stack hotfix for 1903 before updating Azure Stack to 1904.

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

Before applying the 1904 update

The 1904 release of Azure Stack must be applied on the 1903 release with the following hotfixes:

- Azure Stack hotfix 1.1903.2.39

After successfully applying the 1904 update

After the installation of this update, install any applicable hotfixes. For more information, see our Servicing Policy.

- Azure Stack hotfix 1.1904.4.45

Automatic update notifications

Customers with systems that can access the internet from the infrastructure network will see the **Update available** message in the operator portal. Systems without internet access can download and import the .zip file with the corresponding .xml.

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

- RSS
- Atom

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.