Azure Stack 1901 update | Microsoft Docs

Azure Stack 1901 update

Applies to: Azure Stack integrated systems

This article describes the contents of the 1901 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 1901 update build number is **1.1901.0.95** or **1.1901.0.99** after February 26th, 2019. See the following note:

[!IMPORTANT]
Microsoft has discovered an issue that can impact customers updating from 1811 (1.1811.0.101) to 1901, and has released an updated 1901 package to address the issue: build 1.1901.0.99, updated from 1.1901.0.95. Customers that have already updated to 1.1901.0.95 do not need to take further action.

Connected customers that are on 1811 will automatically see the new 1901 (1.1901.0.99) package available in the Administrator portal, and should install it when ready. Disconnected customers can download and import the new 1901 package using the same process described here.

Customers with either version of 1901 will not be impacted when installing the next full or hotfix package.

Hotfixes

Azure Stack releases hotfixes on a regular basis. Be sure to install the latest Azure Stack hotfix for 1811 before updating Azure Stack to 1901.

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

If you already have 1901 and you have not installed any hotfixes yet, you can install 1902 directly, without first installing the 1901 hotfix.

- **1811**: No current hotfix available.
- **1901**: KB 4500636 - Azure Stack hotfix 1.1901.5.109

Prerequisites

[!IMPORTANT] Install the latest Azure Stack hotfix for 1811 (if any) before updating to 1901. If you already have 1901 and you have not installed any hotfixes yet, you can install 1902 directly, without first installing the 1901 hotfix.

- 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 AzsControlPlane, AzsDefenderSummary,
  AzsHostingInfraSummary, AzsHostingInfraUtilization, AzsInfraCapacity,
  AzsInfraRoleSummary, AzsPortalAPISummary, AzsSFRoleSummary,
  AzsStampBMCSummary, AzsHostingServiceCertificates
  ```

- When Azure Stack is managed by System Center Operations Manager (SCOM), be sure to update the Management Pack for Microsoft Azure Stack to version 1.0.3.11 before applying 1901.

New features

This update includes the following new features and improvements for Azure Stack:

- Managed images on Azure Stack enable you to create a managed image object on a generalized VM (both unmanaged and managed) that can only create managed disk VMs going forward. For more information, see Azure Stack Managed Disks.

- **AzureRm 2.4.0**
- **AzureRm.Profile**
  Bug fix - `Import-AzureRmContext` to deserialize the saved token correctly.

- **AzureRm.Resources**
  Bug fix - `Get-AzureRmResource` to query case insensitively by resource type.

- **Azure.Storage**
  AzureRm rollup module now includes the already published version 4.5.0 supporting the **api-version 2017-07-29**.

- **AzureRm.Storage**
  AzureRm rollup module now includes the already published version 5.0.4 supporting

the **api-version 2017-10-01**.

- **AzureRm.Compute**
 Added simple parameter sets in `New-AzureRmVM` and `New-AzureRmVmss`, `-Image` parameter supports specifying user images.

- **AzureRm.Insights**
 AzureRm rollup module now includes the already published version 5.1.5 supporting the **api-version 2018-01-01** for metrics, metric definitions resource types.

- **AzureStack 1.7.1** This a breaking change release. For details on the breaking changes, refer to https://aka.ms/azspshmigration171
- **Azs.Backup.Admin Module**
 Breaking change: Backup changes to cert-based encryption mode. Support for symmetric keys is deprecated.

- **Azs.Fabric.Admin Module**
 `Get-AzsInfrastructureVolume` has been deprecated. Use the new cmdlet `Get-AzsVolume`.
 `Get-AzsStorageSystem` has been deprecated. Use the new cmdlet `Get-AzsStorageSubSystem`.
 `Get-AzsStoragePool` has been deprecated. The `StorageSubSystem` object contains the capacity property.

- **Azs.Compute.Admin Module**
 Bug fix - `Add-AzsPlatformImage`, `Get-AzsPlatformImage`: Calling `ConvertTo-PlatformImageObject` only in the success path.
 BugFix - `Add-AzsVmExtension`, `Get-AzsVmExtension`: Calling ConvertTo-VmExtensionObject only in the success path.

- **Azs.Storage.Admin Module**
 Bug fix - New Storage Quota uses defaults if none provided.

To review the reference for the updated modules, see Azure Stack Module Reference.

Fixed issues

- Fixed an issue in which the portal showed an option to create policy-based VPN gateways, which are not supported in Azure Stack. This option has been removed from the portal.

- Fixed an issue in which after updating your DNS Settings for your Virtual Network from **Use Azure Stack DNS** to **Custom DNS**, the instances were not updated with the new setting.

Fixed an issue in which deploying VMs with sizes containing a **v2** suffix; for example, **Standard_A2_v2**, required specifying the suffix as **Standard_A2_v2** (lowercase v). As with global Azure, you can now use **Standard_A2_V2** (uppercase V).

- Fixed an issue that produced a warning when you used the portal to create virtual machines (VMs) in a premium VM size (DS,Ds_v2,FS,FSv2). The VM was created in a standard storage account. Although this did not affect functionally, IOPs, or billing, the warning has been fixed.

- Fixed an issue with the **Health controller** component that was generating the following alerts. The alerts could be safely ignored:

  - Alert #1:
  - NAME: Infrastructure role unhealthy
  - SEVERITY: Warning
  - COMPONENT: Health controller
  - DESCRIPTION: The health controller Heartbeat Scanner is unavailable. This may affect health reports and metrics.
  - Alert #2:
  - NAME: Infrastructure role unhealthy
  - SEVERITY: Warning
  - COMPONENT: Health controller
  - DESCRIPTION: The health controller Fault Scanner is unavailable. This may affect health reports and metrics.

- Fixed an issue when setting the value of Managed Disks quotas under compute quota types to 0, it is equivalent to the default value of 2048 GiB. The zero quota value now is respected.
- Fixed an issue when using the PowerShell cmdlets **Start-AzsScaleUnitNode** or **Stop-AzsScaleUnitNode** to manage scale units, in which the first attempt to start or stop the scale unit might fail.

- Fixed an issue in which you registered the **Microsoft.Insight** resource provider in the subscription settings, and created a Windows VM with Guest OS Diagnostic enabled, but the CPU Percentage chart in the VM overview page did not show metrics data. The data now correctly displays.

- Fixed an issue in which running the **Get-AzureStackLog** cmdlet failed after running **Test-AzureStack** in the same privileged endpoint (PEP) session. You can now use the same PEP session in which you executed **Test-AzureStack**.

- Fixed issue with automatic backups where the scheduler service would go into disabled state unexpectedly.
- Removed the **Reset Gateway** button from the Azure Stack portal, which threw an error if the button was clicked. This button serves no function in Azure Stack, as Azure

Stack has a multi-tenant gateway rather than dedicated VM instances for each tenant VPN Gateway, so it was removed to prevent confusion.

- Removed the **Effective Security Rules** link from the **Networking Properties** blade as this feature is not supported in Azure Stack. Having the link present gave the impression that this feature was supported but not working. To alleviate confusion, we removed the link.
- Fixed an issue in which after an update was applied to Azure Stack from an OEM, the **Update available** notification did not appear in the Azure Stack administrator portal.

Changes

- Security enhancements in this update result in an increase in the backup size of the directory service role. For updated sizing guidance for the external storage location, see the infrastructure backup documentation. This change results in a longer time to complete the backup due to the larger size data transfer. This change impacts integrated systems.

- Starting in January 2019, you can deploy Kubernetes clusters on Active Directory Federated Services (AD FS) registered, connected Azure Stack stamps (internet access is required). Follow the instructions here to download the new Kubernetes Marketplace item. Follow the instructions here to deploy a Kubernetes cluster. Note the new parameters for indicating whether the target system is ADD or AD FS registered. If it is AD FS, new fields are available to enter the Key Vault parameters in which the deployment certificate is stored.

Note that even with AD FS support, the deployment of Kubernetes clusters requires internet access.

- After installing updates or hotfixes to Azure Stack, new features may be introduced which require new permissions to be granted to one or more identity applications. Granting these permissions requires administrative access to the home directory, and so it cannot be done automatically. For example:

```powershell $adminResourceManagerEndpoint = "https://adminmanagement.." $homeDirectoryTenantName = ".onmicrosoft.com" # This is the primary tenant Azure Stack is registered to

Update-AzsHomeDirectoryTenant -AdminResourceManagerEndpoint $adminResourceManagerEndpoint ` -DirectoryTenantName $homeDirectoryTenantName -Verbose ```

- There is a new consideration for accurately planning Azure Stack capacity. With the 1901 update, there is now a limit on the total number of Virtual Machines that can be created. This limit is intended to be temporary to avoid solution instability. The source of the stability issue at higher numbers of VMs is being addressed but a specific timeline for remediation has not yet been determined. With the 1901 update, there is now a per server limit of 60 VMs with a total solution limit of 700. For example, an 8 server Azure Stack VM limit would be 480 (8 * 60). For a 12 to 16 server Azure Stack
```

solution the limit would be 700. This limit has been created keeping all the compute capacity considerations in mind such as the resiliency reserve and the CPU virtual to physical ratio that an operator would like to maintain on the stamp. For more information, see the new release of the capacity planner.
In the event that the VM scale limit has been reached, the following error codes would be returned as a result: VMsPerScaleUnitLimitExceeded, VMsPerScaleUnitNodeLimitExceeded.

- The Compute API version has increased to 2017-12-01.

- Infrastructure backup now requires a certificate with a public key only (.CER) for encryption of backup data. Symmetric encryption key support is deprecated starting in 1901. If infrastructure backup is configured before updating to 1901, the encryption keys will remain in place. You will have at least 2 more updates with backwards compatibility support to update backup settings. For more information, see Azure Stack infrastructure backup best practices.

Common vulnerabilities and exposures

This update installs the following security updates:

- CVE-2018-8477
- CVE-2018-8514
- CVE-2018-8580
- CVE-2018-8595
- CVE-2018-8596
- CVE-2018-8598
- CVE-2018-8621
- CVE-2018-8622
- CVE-2018-8627
- CVE-2018-8637
- CVE-2018-8638
- ADV190001
- CVE-2019-0536
- CVE-2019-0537
- CVE-2019-0545
- CVE-2019-0549
- CVE-2019-0553
- CVE-2019-0554
- CVE-2019-0559
- CVE-2019-0560
- CVE-2019-0561
- CVE-2019-0569
- CVE-2019-0585

- CVE-2019-0588

For more information about these vulnerabilities, click on the preceding links, or see Microsoft Knowledge Base articles 4480977.

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 running Test-AzureStack, if either the **AzsInfraRoleSummary** or the **AzsPortalApiSummary** test fails, you are prompted to run **Test-AzureStack** with the `-Repair` flag. If you run this command, it fails with the following error message: `Unexpected exception getting Azure Stack health status. Cannot bind argument to parameter 'TestResult' because it is null.`

- 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.

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 (VMSS) 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 1901 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 **AzureStack-DiskRP-Client** 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.

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 instances today, regardless of the instance size.

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 1901 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.