Azure Stack 1811 update | Microsoft Docs

sethmanheim

Azure Stack 1811 update

Applies to: Azure Stack integrated systems

This article describes the contents of the 1811 update package. The update package 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 so you can 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.

Build reference

The Azure Stack 1811 update build number is **1.1811.0.101**.

Hotfixes

Azure Stack releases hotfixes on a regular basis. Be sure to install the latest Azure Stack hotfix for 1809 before updating Azure Stack to 1811.

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

Azure Stack hotfixes

- **1809**: KB 4481548 – Azure Stack hotfix 1.1809.12.114
- **1811**: No current hotfix available.

Prerequisites

[!IMPORTANT] During installation of the 1811 update, you must ensure that all instances of the administrator portal are closed. The user portal can remain open, but the admin portal must be closed.

- Get your Azure Stack deployment ready for the Azure Stack extension host. Prepare your system using the following guidance: Prepare for extension host for Azure Stack.

- Install the latest Azure Stack hotfix for 1809 before updating to 1811.

- 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
```

If you do not have the extension host requirements met, the `Test-AzureStack` output displays the following message:

```
To proceed with installation of the 1811 update, you will need to import
the SSL certificates required for Extension Host, which simplifies
network    integration and increases the security posture of Azure Stack.
Refer to this    link to prepare for Extension Host:
https://docs.microsoft.com/azure-stack/operator/azure-stack-extension-
host-prepare
```

- The Azure Stack 1811 update requires that you have properly imported the mandatory extension host certificates into your Azure Stack environment. To proceed with installation of the 1811 update, you must import the SSL certificates required for the extension host. To import the certificates, see this section.

  If you ignore every warning and still choose to install the 1811 update, the update will fail in approximately 1 hour with the following message:

  ```
  The required SSL certificates for the Extension Host have not been found.
  The Azure Stack update will halt. Refer to this link to prepare for
  Extension Host: https://docs.microsoft.com/azure-stack/operator/azure-
  stack-extension-host-prepare,   then resume the update.   Exception: The
  Certificate path does not exist: [certificate path here]
  ```

  Once you have properly imported the mandatory extension host certificates, you can resume the 1811 update from the Administrator portal. While Microsoft advises Azure Stack operators to schedule a maintenance window during the update process, a failure due to the missing extension host certificates should not impact existing workloads or services.

  During the installation of this update, the Azure Stack user portal is unavailable while the extension host is being configured. The configuration of the extension host can take up to 5 hours. During that time, you can check the status of an update, or resume a failed update installation using Azure Stack Administrator PowerShell or the privileged endpoint.

- 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 1811.

New features

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

- With this release, the extension host is enabled. The extension host simplifies network integration and improves the security posture of Azure Stack.
- Added support for device authentication with Active Directory Federated Services (AD FS), when using Azure CLI in particular. For more information, see Use API version profiles with Azure CLI in Azure Stack
- Added support for Service Principals using a client secret with Active Directory Federated Services (AD FS). For more information, see Create service principal for AD FS.
- This release adds support for the following Azure Storage Service API versions: **2017-07-29**, **2017-11-09**. Support is also added for the following Azure Storage Resource Provider API versions: **2016-05-01**, **2016-12-01**, **2017-06-01**, and **2017-10-01**. For more information, see Azure Stack storage: Differences and considerations.
- Added new privileged endpoint commands to update and remove service principles for ADFS. For more information, see Create service principal for AD FS.
- Added new Scale Unit Node operations that allow an Azure Stack operator to start, stop, and shut down a scale unit node. For more information, see Scale unit node actions in Azure Stack.
- Added a new region properties blade that displays registration details of the environment. You can view this information by clicking the **Region Management** tile on the default dashboard in the administrator portal, and then selecting **Properties**.
- Added a new privileged endpoint command to update the BMC credential with user name and password, used to communicate with the physical machines. For more information, see Update the baseboard management controller (BMC) credential.
- Added the ability to access the Azure roadmap though the help and support icon (question mark) in the upper right corner of the administrator and user portals, similar to the way it is available in the Azure portal.
- Added an improved Marketplace management experience for disconnected users. The upload process to publish a Marketplace item in a disconnected environment is simplified to one step, instead of uploading the image and the Marketplace package separately. The uploaded product will also be visible in the Marketplace management blade. For more information, see this section.
- This release reduces the required maintenance window for secret rotation by adding the ability to rotate only external certificates during Azure Stack secret rotation.

- Azure Stack PowerShell has been updated to version 1.6.0. The update includes support for the new storage-related features in Azure Stack. For more information, see the release notes for the Azure Stack Administration Module 1.6.0 in the PowerShell Gallery For information about updating or installing Azure Stack PowerShell, see Install PowerShell for Azure Stack.

- Managed Disks is now enabled by default when creating virtual machines using the Azure Stack portal. See the known issues section for the additional steps required for Managed Disks to avoid VM creation failures.

- This release introduces alert **Repair** actions for the Azure Stack operator. Some alerts in 1811 provide a **Repair** button in the alert that you can select to resolve the issue. For more information, see Monitor health and alerts in Azure Stack.

- Updates to the update experience in Azure Stack. The update enhancements include:
  - Tabs that split the Updates from Update history for better tracking updates in progress and completed updates.
  - Enhanced state visualizations in the essentials section with new icons and layout for Current and OEM versions as well as Last updated date.
  - **View** link for the Release notes column takes the user directly to the documentation specific to that update rather than the generic update page.
  - The **Update history** tab used to determine run times for each of the updates as well as enhanced filtering capabilities.

  - Azure Stack scale units that are connected will still automatically receive **Update available** as they become available.
  - Azure Stack scale units that are not connected can import the updates just like before.
  - There are no changes in the process to download the JSON logs from the portal. Azure Stack operators will see expanding steps expressing progress.

  For more information, see Apply updates in Azure Stack.

Fixed issues

- Fixed an issue in which the public IP address usage meter data showed the same **EventDateTime** value for each record instead of the **TimeDate** stamp that shows when the record was created. You can now use this data to perform accurate accounting of public IP address usage.
- Fixed an issue that occurred when creating a new virtual machine (VM) using the Azure Stack portal. Selecting the VM size caused the **USD/Month** column to display an **Unavailable** message. This column no longer appears; displaying the VM pricing column is not supported in Azure Stack.
- Fixed an issue in which the administrator portal, when accessing the details of any user subscription, after closing the blade and clicking on **Recent**, the user subscription name did not appear. The user subscription name now appears.

- Fixed an issue in both the administrator and user portals: clicking on the portal settings and selecting **Delete all settings and private dashboards** did not work as expected and an error notification was displayed. This option now works correctly.
- Fixed an issue in both the administrator and user portals: under **All services**, the asset **DDoS protection plans** was incorrectly listed. It is not available in Azure Stack. The listing has been removed.
- Fixed an issue that occurred when you installed a new Azure Stack environment, in which the alert that indicates **Activation Required** did not display. It now correctly displays.
- Fixed an issue that prevented applying RBAC policies to a user group when using ADFS.
- Fixed an issue with infrastructure backups failing due to an inaccessible file server from the public VIP network. This fix moves the infrastructure backup service back to the public infrastructure network. If you applied the latest Azure Stack hotfix for 1809 that addresses this issue, the 1811 update will not make any further modifications.
- Fixed an issue in which the account you used to sign in to the Azure Stack admin or user portal displayed as **Unidentified user**. This message was displayed when the account did not have either a **First** or **Last** name specified.
- Fixed an issue in which using the portal to create a virtual machine scale set (VMSS) caused the **instance size** dropdown to not load correctly when using Internet Explorer. This browser now works correctly.
- Fixed an issue that generated noisy alerts indicating that an Infrastructure Role Instance was unavailable or Scale Unit Node was offline.
- Fiexed an issue in which the VM overview page cannot correctly show the VM metrics chart.

Changes

- A new way to view and edit the quotas in a plan is introduced in 1811. For more information, see View an existing quota.
- 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.

- The existing PEP cmdlet to retrieve the BitLocker recovery keys is renamed in 1811, from Get-AzsCsvsRecoveryKeys to Get-AzsRecoveryKeys. For more information on how to retrieve the BitLocker recovery keys, see instructions on how to retrieve the keys.

Common vulnerabilities and exposures

This update installs the following security updates:

- CVE-2018-8256

- CVE-2018-8407
- CVE-2018-8408
- CVE-2018-8415
- CVE-2018-8417
- CVE-2018-8450
- CVE-2018-8471
- CVE-2018-8476
- CVE-2018-8485
- CVE-2018-8544
- CVE-2018-8547
- CVE-2018-8549
- CVE-2018-8550
- CVE-2018-8553
- CVE-2018-8561
- CVE-2018-8562
- CVE-2018-8565
- CVE-2018-8566
- CVE-2018-8584

For more information about these vulnerabilities, click on the preceding links, or see Microsoft Knowledge Base articles 4478877.

Known issues with the update process

- When you run the **Get-AzureStackLog** PowerShell cmdlet after running **Test-AzureStack** in the same privileged endpoint (PEP) session, **Get-AzureStackLog** fails. To work around this issue, close the PEP session in which you executed **Test-AzureStack**, and then open a new session to run **Get-AzureStackLog**.

- During installation of the 1811 update, ensure that all instances of the administrator portal are closed during this time. The user portal can remain open, but the admin portal must be closed.

- 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.` This issue will be fixed in a future release.

- During installation of the 1811 update, the Azure Stack use portal is unavailable while the extension host is being configured. The configuration of the extension host can take up to 5 hours. During that time, you can check the status of an update, or resume a failed update installation using Azure Stack Administrator PowerShell or the privileged endpoint.

- During installation of the 1811 update, the user portal dashboard might not be available, and customizations can be lost. You can restore the dashboard to the default setting after the update completes by opening the portal settings and selecting **Restore default settings**.

- 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.

  If you've applied an update to Azure Stack from your OEM, the **Update available** notification may not appear in the Azure Stack administrator portal. To install the Microsoft update, download and import it manually using the instructions located here Apply updates in Azure Stack.

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.

Health and monitoring

- You might see alerts for the **Health controller** component that have the following details:
  - 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.

  Both alerts can be safely ignored. They will close automatically over time.

Compute

- When creating a new Windows Virtual Machine (VM), the **Settings** blade requires that you select a public inbound port in order to proceed. In 1811, this setting is required, but has no effect. This is because the feature depends on Azure Firewall, which is not implemented in Azure Stack. You can select **No Public Inbound Ports**, or any of the other options to proceed with VM creation. The setting will have no effect.

- 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.

- When creating a Dv2 series VM, D11-14v2 VMs allow you to create 4, 8, 16, and 32 data disks respectively. However, the create VM pane shows 8, 16, 32, and 64 data disks.

- Usage records on Azure Stack may contain unexpected capitalization; for example:

  ```
  {"Microsoft.Resources":{"resourceUri":"/subscriptions/<subid>/resourceGro
  ups/ANDREWRG/providers/Microsoft.Compute/
  virtualMachines/andrewVM0002","location":"twm","tags":"null","additionalI
  nfo":
  "{\"ServiceType\":\"Standard_DS3_v2\",\"ImageType\":\"Windows_Server\"}"}
  }
  ```

In this example, the name of the resource group should be **AndrewRG**. You can safely ignore this inconsistency.

- To deploy VMs with sizes containing a **v2** suffix; for example, **Standard_A2_v2**, specify the suffix as **Standard_A2_v2** (lowercase v). Do not use **Standard_A2_V2** (uppercase V). This works in global Azure and is an inconsistency on Azure Stack.
- When using the **Add-AzsPlatformImage** cmdlet, you must use the **-OsUri** parameter as the storage account URI where the disk is uploaded. If you use the local path of the disk, the cmdlet fails with the following error:

  ```
  Long running operation failed with status 'Failed'
  ```

- When you use the portal to create virtual machines (VMs) in a premium VM size (DS,Ds_v2,FS,FSv2), the VM is created in a standard storage account. Creation in a standard storage account does not affect functionally, IOPs, or billing. You can safely ignore the warning that says:

  ```
  You've chosen to use a standard disk on a size that supports premium
  disks. This could impact operating system performance and is not
  recommended. Consider using premium storage (SSD) instead.
  ```

- 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.
- When using the PowerShell cmdlets **Start-AzsScaleUnitNode** or **Stop-AzsScaleunitNode** to manage scale units, the first attempt to start or stop the scale unit might fail. If the cmdlet fails on the first run, run the cmdlet a second time. The second run should successfully complete the operation.
- If provisioning an extension on a VM deployment takes too long, let the provisioning time-out instead of trying to stop the process to deallocate or delete the VM.
- Linux VM diagnostics is not supported in Azure Stack. When you deploy a Linux VM with VM diagnostics enabled, the deployment fails. The deployment also fails if you enable the Linux VM basic metrics through diagnostic settings.
- Managed Disks creates two new compute quota types to limit the maximum capacity of managed disks that can be provisioned. By default, 2048 GiB is allocated for each managed disks quota type. However, you may encounter the following issues:

  - For quotas created before the 1808 update, the Managed Disks quota will show 0 values in the Administrator portal, although 2048 GiB is allocated. You can increase or decrease the value based on your actual needs, and the newly set quota value overrides the 2048 GiB default.
  - If you update the quota value to 0, it is equivalent to the default value of 2048 GiB. As a workaround, set the quota value to 1.
- After applying the 1811 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 the **AzureStack-DiskRP-Client** role 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.

Networking

- Under **Networking**, if you click **Create VPN Gateway** to set up a VPN connection, **Policy Based** is listed as a VPN type. Do not select this option. Only the **Route Based** option is supported in Azure Stack.
- Azure Stack supports a single *local network gateway* per IP address. This is true across all tenant subscriptions. After the creation of the first local network gateway connection, subsequent attempts to create a local network gateway resource with the same IP address are rejected.
- On a virtual network that was created with a DNS server setting of **Automatic**, changing to a custom DNS server fails. The updated settings are not pushed to VMs in that Vnet.
- During Azure Stack *Secret Rotation*, there is a period in which public IP addresses are unreachable for two to five minutes.
- In scenarios where the tenant is accessing virtual machines by using a S2S VPN tunnel, they might encounter a scenario where connection attempts fail if the on-premises subnet was added to the local network gateway after the gateway was already created.

- 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, on the **Networking Properties** blade there is a link for **Effective Security Rules** for each network adapter. If you select this link, a new blade opens that shows the error message `Not Found.` This error occurs because Azure Stack does not yet support **Effective Security Rules**.

- 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.

- The **New-AzureRmIpSecPolicy** PowerShell cmdlet does not support setting **DHGroup24** for the `DHGroup` parameter.

- 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, you cannot set multiple ports on one NSG rule via the portal. To work around this issue, use a Resource Manager template to set these additional rules.

Infrastructure backup

- After enabling automatic backups, the scheduler service goes into disabled state unexpectedly. The backup controller service will detect that automatic backups are disabled and raise a warning in the administrator portal. This warning is expected when automatic backups are disabled.
  - Cause: This issue is due to a bug in the service that results in loss of scheduler configuration. This bug does not change the storage location, user name, password, or encryption key.

  - Remediation: To mitigate this issue, open the backup controller settings blade in the Infrastructure Backup resource provider and select **Enable Automatic Backups**. Make sure to set the desired frequency and retention period.
  - Occurrence: Low

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 1811 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

- 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.
- 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.