Azure Stack 1809 update | Microsoft Docs

sethmanheim

Azure Stack 1809 update

Applies to: Azure Stack integrated systems

This article describes the contents of the 1809 update package. The update package includes improvements, fixes, and known issues for this version of Azure Stack. This article also 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 1809 update build number is **1.1809.0.90**.

New features

This update includes the following improvements for Azure Stack:

- With this release, Azure Stack integrated systems supports configurations of 4-16 nodes. You can use the Azure Stack Capacity Planner to help in your planning for Azure Stack capacity and configuration.

  Azure Stack syslog client (General Availability) This client allows the forwarding of audits, alerts, and security logs related to the Azure Stack infrastructure to a syslog server or security information and event management (SIEM) software external to Azure Stack. The syslog client now supports specifying the port on which the syslog server is listening.

  With this release, the syslog client is generally available, and it can be used in production environments.

  For more information, see Azure Stack syslog forwarding.

- You can now move the registration resource on Azure between resource groups without having to re-register. Cloud Solution Providers (CSPs) can also move the registration resource between subscriptions, as long as both the new and old subscriptions are mapped to the same CSP partner ID. This does not impact the existing customer tenant mappings.

- Added support for assigning multiple IP addresses per network interface. For more details see Assign multiple IP addresses to virtual machines using PowerShell.

Fixed issues

- On the portal, the memory chart reporting free/used capacity is now accurate. You can now more reliably predict how many VMs you are able to create.
- Fixed an issue in which you created virtual machines on the Azure Stack user portal, and the portal displayed an incorrect number of data disks that can attach to a DS series VM. DS series VMs can accommodate as many data disks as the Azure configuration.
- The following managed disk issues are fixed in 1809, and are also fixed in the 1808 Azure Stack Hotfix 1.1808.9.117:

  - Fixed the issue in which attaching SSD data disks to premium size managed disk virtual machines (DS, DSv2, Fs, Fs_V2) failed with an error: *Failed to update disks for the virtual machine vmname Error: Requested operation cannot be performed because storage account type Premium_LRS is not supported for VM size Standard_DS/Ds_V2/FS/Fs_v2)*.
  - Creating a managed disk VM by using **createOption**: **Attach** fails with the following error: *Long running operation failed with status 'Failed'. Additional Info:'An internal execution error occurred.'* ErrorCode: InternalExecutionError ErrorMessage: An internal execution error occurred.

    This issue has now been fixed.

  Fixed issue in which public IPs that were deployed by using the Dynamic allocation method were not guaranteed to be preserved after a Stop-Deallocate is issued. They are now preserved.

  If a VM was stop-deallocated before 1808 it could not be re-allocated after the 1808 update. This issue is fixed in 1809. Instances that were in this state and could not be started can be started in 1809 with this fix. The fix also prevents this issue from reoccurring.

Changes

- Infrastructure backup service moves from the public infrastructure network to the public VIP network. Customers will need to ensure the service has access the backup storage location from the public VIP network.

[!IMPORTANT]
If you have a firewall that does not allow connections from the public VIP network to the file server, this change will cause infrastructure backups to fail with "Error 53 The network path was not found." This is a breaking change that has no reasonable workaround. Based on customer feedback, Microsoft will revert this change in a hotfix. Please review the post update steps section for more information on available hotfixes for 1809. Once the hotfix is available, make sure to apply it after updating to 1809 only if your network policies do not allow the public VIP

network to access infrastructure resources. in 1811, this change will be applied to all systems. If you applied the hotfix in 1809, there is no further action required.

Common vulnerabilities and exposures

This update installs the following security updates:

- ADV180022
- CVE-2018-0965
- CVE-2018-8271
- CVE-2018-8320
- CVE-2018-8330
- CVE-2018-8332
- CVE-2018-8333
- CVE-2018-8335
- CVE-2018-8392
- CVE-2018-8393
- CVE-2018-8410
- CVE-2018-8411
- CVE-2018-8413
- CVE-2018-8419
- CVE-2018-8420
- CVE-2018-8423
- CVE-2018-8424
- CVE-2018-8433
- CVE-2018-8434
- CVE-2018-8435
- CVE-2018-8438
- CVE-2018-8439
- CVE-2018-8440
- CVE-2018-8442
- CVE-2018-8443
- CVE-2018-8446
- CVE-2018-8449
- CVE-2018-8453
- CVE-2018-8455
- CVE-2018-8462
- CVE-2018-8468
- CVE-2018-8472
- CVE-2018-8475
- CVE-2018-8481
- CVE-2018-8482

- CVE-2018-8484
- CVE-2018-8486
- CVE-2018-8489
- CVE-2018-8490
- CVE-2018-8492
- CVE-2018-8493
- CVE-2018-8494
- CVE-2018-8495
- CVE-2018-8497

For more information about these vulnerabilities, click on the preceding links, or see Microsoft Knowledge Base articles 4457131 and 4462917.

Prerequisites

- Install the latest Azure Stack Hotfix for 1808 before applying 1809. For more information, see KB 4481066 - Azure Stack Hotfix Azure Stack Hotfix 1.1808.9.117. While Microsoft recommends the latest Hotfix available, the minimum version required to install 1809 is 1.1808.5.110.

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

  - RRS: https://support.microsoft.com/app/content/api/content/feeds/sap/en-us/32d322a8-acae-202d-e9a9-7371dccf381b/rss
  - Atom: https://support.microsoft.com/app/content/api/content/feeds/sap/en-us/32d322a8-acae-202d-e9a9-7371dccf381b/atom

- 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
  ```

- 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 1809.

Known issues with the update process

- When you run Test-AzureStack after the 1809 update, 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. These alerts will close automatically after installation of this update completes.

Do not attempt to create virtual machines during the installation of this update. For more information about managing updates, see Manage updates in Azure Stack overview.

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

Post-update steps

[!Important]
Get your Azure Stack deployment ready for extension host which is enabled by the next update package. Prepare your system using the following guidance, Prepare for extension host for Azure Stack.

After the installation of this update, install any applicable Hotfixes. For more information view the following knowledge base articles, as well as our Servicing Policy.
- KB 4481548 - Azure Stack Hotfix Azure Stack Hotfix 1.1809.12.114

Known issues (post-installation)

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

Portal

- The Azure Stack technical documentation focuses on the latest release. Due to portal changes between releases, what you see when using the Azure Stack portals might vary from what you see in the documentation.
- In the administrator portal, when accessing the details of any user subscription, after closing the blade and clicking on **Recent**, the user subscription name does not appear.
- In both the administrator and user portals, clicking on the portal settings and selecting **Delete all settings and private dashboards** does not work as expected. An error notification is displayed.
- In both the administrator and user portals, under **All services**, the asset **DDoS protection plans** is incorrectly listed. It is not available in Azure Stack. If you try to create it, an error is displayed stating that the portal could not create the marketplace item.
- 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.
- The account you use to sign in to the Azure Stack admin or user portal displays as **Unidentified user**. This message is displayed when the account does not have either a *First* or *Last* name specified. To work around this issue, edit the user account to

provide either the First or Last name. You must then sign out and then sign back in to the portal.

- When you use the portal to create a virtual machine scale set (VMSS), the *instance size* dropdown doesn't load correctly when you use Internet Explorer. To work around this problem, use another browser while using the portal to create a VMSS.
- 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.
- When you install a new Azure Stack environment that runs this version, the alert that indicates *Activation Required* might not display. Activation is required before you can use marketplace syndication.
- 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 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 the following alerts repeatedly appear and then disappear on your Azure Stack system:
  - *Infrastructure role instance unavailable*
  - *Scale unit node is offline*

  Run the Test-AzureStack cmdlet to verify the health of the infrastructure role instances and scale unit nodes. If no issues are detected by Test-AzureStack, you can ignore these alerts. If an issue is detected, you can attempt to start the infrastructure role instance or node using the admin portal or PowerShell.

  This issue is fixed in the latest 1809 hotfix release, so be sure to install this hotfix if you're experiencing the issue.

- 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 and they'll close automatically over time.

- You might see an alert for the **Storage** component that has the following details:

  - NAME: Storage service internal communication error
  - SEVERITY: Critical
  - COMPONENT: Storage
  - DESCRIPTION: Storage service internal communication error occurred when sending requests to the following nodes.

  The alert can be safely ignored, but you need to close the alert manually.

- An Azure Stack operator, if you receive a low memory alert and tenant virtual machines fail to deploy with a **Fabric VM creation error**, it is possible that the Azure Stack stamp is out of available memory. Use the Azure Stack Capacity Planner to best understand the capacity available for your workloads.

Compute

- 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.
- To deploy VMs with sizes containing a **v2** suffix; for example, **Standard_A2_v2**, please 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 you create a new virtual machine (VM) using the Azure Stack portal, and you select the VM size, the USD/Month column is displayed with an **Unavailable** message. This column should not appear; displaying the VM pricing column is not supported in 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 (VM) 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 OS 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 succeed to complete the operation.
- If provisioning an extension on a VM deployment takes too long, users should 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.
- When you register the **Microsoft.Insight** resource provider in Subscription settings, and create a Windows VM with Guest OS Diagnostic enabled, the CPU Percentage chart in the VM overview page doesn't show metrics data.

  To find metrics data, such as the CPU Percentage chart for the VM, go to the Metrics window and show all the supported Windows VM guest metrics.

- 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 1809 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. Click **Resource Providers**, then click **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.

- A Ubuntu 18.04 VM created with SSH authorization enabled will not allow you to use the SSH keys to log in. As a workaround, please 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 blocked.
- 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 their 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 gateway was already created.

App Service

- Users must register the storage resource provider before they create their first Azure Function in the subscription.

Usage

- The public IP address usage meter data shows the same *EventDateTime* value for each record instead of the *TimeDate* stamp that shows when the record was created. Currently, you cannot use this data to perform accurate accounting of public IP address usage.

Download the update

You can download the Azure Stack 1809 update package from here.

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.