Azure Stack 1803 Update | Microsoft Docs

brenduns

Azure Stack 1803 update

Applies to: Azure Stack integrated systems

This article describes the improvements and fixes in the 1803 update package, known issues for this release, and where 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.

Build reference

The Azure Stack 1803 update build number is **20180329.1**.

Before you begin

[!IMPORTANT]
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.

Prerequisites

- Install the Azure Stack 1802 Update before you apply the Azure Stack 1803 update.
- Install **AzS Hotfix 1.0.180312.1- Build 20180222.2** before you apply the Azure Stack 1803 update. This hotfix updates Windows Defender, and is available when you download updates for Azure Stack.

  To install the hotfix, follow the normal procedures for installing updates for Azure Stack. The name of the update appears as **AzS Hotfix 1.0.180312.1**, and includes the following files:
  - PUPackageHotFix_20180222.2-1.exe
  - PUPackageHotFix_20180222.2-1.bin
  - Metadata.xml

  After uploading these files to a storage account and container, run the install from the Update tile in the admin portal.

  Unlike updates to Azure Stack, installing this update does not change the version of Azure Stack. To confirm this update is installed, view the list of **Installed updates**.

New features

This update includes the following improvements and fixes for Azure Stack.

- **Update Azure Stack secrets** - (Accounts and Certificates). For more information about managing secrets, see Rotate secrets in Azure Stack.
- **Automatic redirect to HTTPS** when you use HTTP to access the administrator and user portals. This improvement was made based on UserVoice feedback for Azure Stack.
- **Access the Marketplace** ? You can now open the Azure Stack Marketplace by using the +New option from within the admin and user portals the same way you do in the Azure portals.
- **Azure Monitor** - Azure Stack adds Azure Monitor to the admin and user portals. This includes new explorers for metrics and activity logs. To access this Azure Monitor from external networks, port **13012** must be open in firewall configurations. For more information about ports required by Azure Stack, see Azure Stack datacenter integration - Publish endpoints.

  Also as part of this change, under **More services**, *Audit logs* now appears as *Activity logs*. The functionality is now consistent with the Azure portal.

- **Sparse files** - When you add a New image to Azure Stack, or add an image through marketplace syndication, the image is converted to a sparse file. Images that were added prior to using Azure Stack version 1803 cannot be converted. Instead, you must use marketplace syndication to resubmit those images to take advantage of this feature.

  Sparse files are an efficient file format used to reduce storage space use, and improve I/O. ?For more information, see Fsutil sparse for Windows Server.

Fixed issues

- Internal Load Balancing (ILB) now properly handles MAC addresses for back-end VMs, which causes ILB to drop packets to the back-end network when using Linux instances on the back-end network. ILB works fine with Windows instances on the back-end network.
- An issue where VPN Connections between Azure Stack would become disconnected due to Azure Stack using different settings for the IKE policy than Azure. The values for SALifetime (Time) and SALiftetime (Bytes) were not compatible with Azure and have changed in 1803 to match the Azure settings. The value for SALifetime (Seconds) prior to 1803 was 14,400 and now changes to 27,000 in 1803. The value for SALifetime (Bytes) prior to 1803 was 819,200 and changes to 33,553,408 in 1803.
- The IP issue where VPN Connections was previously visible in the portal; however enabling or toggling IP Forwarding has no effect. The feature is turned on by default and the ability to change this not yet supported. The control has been removed from the portal.

- Azure Stack does not support Policy Based VPN Gateways, even though the option appears in the Portal. The option has been removed from the Portal.
- Azure Stack now prevents resizing of a virtual machine that is created with dynamic disks.
- Usage data for virtual machines is now separated at hourly intervals. This is consistent with Azure.
- The issue where in the admin and user portals, the Settings blade for vNet Subnets fails to load. As a workaround, use PowerShell and the Get-AzureRmVirtualNetworkSubnetConfig cmdlet to view and manage this information.
- When you create a virtual machine, the message *Unable to display pricing* no longer appears when choosing a size for the VM size.
- Various fixes for performance, stability, security, and the operating system that is used by Azure Stack.

Changes

- The way to change the state of a newly created offer from *private* to *public* or *decommissioned* has changed. For more information, see Create an offer.

Known issues with the update process

During installation of the 1803 update, there can be downtime of the blob service and internal services that use blob service. This includes some virtual machine operations. This down time can cause failures of tenant operations or alerts from services that can't access data. This issue resolves itself when the update completes installation.

Post-update steps

- After the installation of 1803, install any applicable Hotfixes. For more information view the following knowledge base articles, as well as our Servicing Policy.
  - KB 4344115 - Azure Stack Hotfix 1.0.180427.15.
- After installing this update, review your firewall configuration to ensure necessary ports are open. For example, this update introduces *Azure Monitor* which includes a change of Audit logs to Activity logs. With this change, port 13012 is now used and must also be open.

Known issues (post-installation)

The following are post-installation known issues for build **20180323.2**.

Portal

- When you use AD FS for your Azure Stack identity system and update to this version of Azure Stack, the default owner of the default provider subscription is reset to the built-in **CloudAdmin** user.
  Workaround: To resolve this issue after you install this update, use step 3 from the

Trigger automation to configure claims provider trust in Azure Stack procedure to reset the owner of the default provider subscription.

- The ability to open a new support request from the dropdown from within the administrator portal isn't available. Instead, use the following link:
  - For Azure Stack integrated systems, use https://aka.ms/newsupportrequest.
- In the admin portal, it is not possible to edit storage metrics for Blob service, Table service, or Queue service. When you go to Storage, and then select the blob, table, or queue service tile, a new blade opens that displays a metrics chart for that service. If you then select Edit from the top of the metrics chart tile, the Edit Chart blade opens but does not display options to edit metrics.
- It might not be possible to view compute or storage resources in the administrator portal. The cause of this issue is an error during the installation of the update that causes the update to be incorrectly reported as successful. If this issue occurs, contact Microsoft Customer Support Services for assistance.
- You might see a blank dashboard in the portal. To recover the dashboard, select the gear icon in the upper right corner of the portal, and then select **Restore default settings**.
- 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.
- In the dashboard of the admin portal, the Update tile fails to display information about updates. To resolve this issue, click on the tile to refresh it.
- In the admin portal, you might see a critical alert for the *Microsoft.Update.Admin* component. The Alert name, description, and remediation all display as:
  - *ERROR - Template for FaultType ResourceProviderTimeout is missing.*

  This alert can be safely ignored.

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.

Marketplace

- Users can browse the full marketplace without a subscription and can see administrative items like plans and offers. These items are non-functional to users.

Compute

- Scaling settings for virtual machine scale sets are not available in the portal. As a workaround, you can use Azure PowerShell. Because of PowerShell version differences, you must use the `-Name` parameter instead of `-VMScaleSetName`.

- When you create an availability set in the portal by going to **New** > **Compute** > **Availability set**, you can only create an availability set with a fault domain and update domain of 1. As a workaround, when creating a new virtual machine, create the availability set by using PowerShell, CLI, or from within the portal.

- When you create virtual machines on the Azure Stack user portal, the portal displays an incorrect number of data disks that can attach to a D series VM. All supported D series VMs can accommodate as many data disks as the Azure configuration.

- When a VM image fails to be created, a failed item that you cannot delete might be added to the VM images compute blade.

  As a workaround, create a new VM image with a dummy VHD that can be created through Hyper-V (New-VHD -Path C:.vhd -Fixed -SizeBytes 1 GB). This process should fix the problem that prevents deleting the failed item. Then, 15 minutes after creating the dummy image, you can successfully delete it.

  You can then try to redownload the VM image that previously failed.

- 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.

Networking

- After a VM is created and associated with a public IP address, you can't disassociate that VM from that IP address. Disassociation appears to work, but the previously assigned public IP address remains associated with the original VM.

  Currently, you must use only new public IP addresses for new VMs you create.

This behavior occurs even if you reassign the IP address to a new VM (commonly referred to as a *VIP swap*). All future attempts to connect through this IP address result in a connection to the originally associated VM, and not to the new one.

- 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.
- Azure Stack does not support adding additional network interfaces to a VM instance after the VM is deployed. If the VM requires more than one network interface, they must be defined at deployment time.
- You cannot use the admin portal to update rules for a network security group.

  Workaround for App Service: If you need to remote desktop to the Controller instances, you modify the security rules within the network security groups with PowerShell. Following are examples of how to *allow*, and then restore the configuration to *deny*:

  - *Allow:*

```
Add-AzureRmAccount -EnvironmentName AzureStackAdmin

$nsg = Get-AzureRmNetworkSecurityGroup -Name "ControllersNsg" -
ResourceGroupName "AppService.local"

$RuleConfig_Inbound_Rdp_3389 =  $nsg | Get-
AzureRmNetworkSecurityRuleConfig -Name "Inbound_Rdp_3389"

##This doesn't work. Need to set properties again even in case of
edit

#Set-AzureRmNetworkSecurityRuleConfig -Name "Inbound_Rdp_3389" -
NetworkSecurityGroup $nsg -Access Allow

Set-AzureRmNetworkSecurityRuleConfig -NetworkSecurityGroup $nsg `
  -Name $RuleConfig_Inbound_Rdp_3389.Name `
  -Description "Inbound_Rdp_3389" `
  -Access Allow `
  -Protocol $RuleConfig_Inbound_Rdp_3389.Protocol `
  -Direction $RuleConfig_Inbound_Rdp_3389.Direction `
  -Priority $RuleConfig_Inbound_Rdp_3389.Priority `
  -SourceAddressPrefix
$RuleConfig_Inbound_Rdp_3389.SourceAddressPrefix `
```

```
  -SourcePortRange $RuleConfig_Inbound_Rdp_3389.SourcePortRange `
  -DestinationAddressPrefix
$RuleConfig_Inbound_Rdp_3389.DestinationAddressPrefix `
  -DestinationPortRange
$RuleConfig_Inbound_Rdp_3389.DestinationPortRange

# Commit the changes back to NSG
Set-AzureRmNetworkSecurityGroup -NetworkSecurityGroup $nsg
```

- *Deny:*

```
Add-AzureRmAccount -EnvironmentName AzureStackAdmin

$nsg = Get-AzureRmNetworkSecurityGroup -Name "ControllersNsg" -
ResourceGroupName "AppService.local"

$RuleConfig_Inbound_Rdp_3389 =  $nsg | Get-
AzureRmNetworkSecurityRuleConfig -Name "Inbound_Rdp_3389"

##This doesn't work. Need to set properties again even in case of
edit

#Set-AzureRmNetworkSecurityRuleConfig -Name "Inbound_Rdp_3389" -
NetworkSecurityGroup $nsg -Access Allow

Set-AzureRmNetworkSecurityRuleConfig -NetworkSecurityGroup $nsg `
  -Name $RuleConfig_Inbound_Rdp_3389.Name `
  -Description "Inbound_Rdp_3389" `
  -Access Deny `
  -Protocol $RuleConfig_Inbound_Rdp_3389.Protocol `
  -Direction $RuleConfig_Inbound_Rdp_3389.Direction `
  -Priority $RuleConfig_Inbound_Rdp_3389.Priority `
  -SourceAddressPrefix
$RuleConfig_Inbound_Rdp_3389.SourceAddressPrefix `
  -SourcePortRange $RuleConfig_Inbound_Rdp_3389.SourcePortRange `
  -DestinationAddressPrefix
$RuleConfig_Inbound_Rdp_3389.DestinationAddressPrefix `
  -DestinationPortRange
$RuleConfig_Inbound_Rdp_3389.DestinationPortRange

# Commit the changes back to NSG
Set-AzureRmNetworkSecurityGroup -NetworkSecurityGroup $nsg
```

SQL and MySQL

- Before proceeding, review the important note in before you begin near the start of these release notes.

- It can take up to one hour before users can create databases in a new SQL or MySQL deployment.
- Only the resource provider is supported to create items on servers that host SQL or MySQL. Items created on a host server that are not created by the resource provider might result in a mismatched state.
- Special characters, including spaces and periods, are not supported in the **Family** name when you create a SKU for the SQL and MySQL resource providers.

[!NOTE]
After you update to Azure Stack 1803, you can continue to use the SQL and MySQL resource providers that you previously deployed. We recommend you update SQL and MySQL when a new release becomes available. Like Azure Stack, apply updates to SQL and MySQL resource providers sequentially. For example, if you use version 1711, first apply version 1712, then 1802, and then update to 1803.

The install of update 1803 does not affect the current use of SQL or MySQL resource providers by your users. Regardless of the version of the resource providers you use, your users data in their databases is not touched, and remains accessible.

App Service

- Users must register the storage resource provider before they create their first Azure Function in the subscription.
- In order to scale out infrastructure (workers, management, front-end roles), you must use PowerShell as described in the release notes for Compute.

Usage

- Usage 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 can't use this data to perform accurate accounting of public IP address usage.

Downloading Azure Stack Tools from GitHub

- When using the *invoke-webrequest* PowerShell cmdlet to download the Azure Stack tools from Github, you receive an error:
  - *invoke-webrequest : The request was aborted: Could not create SSL/TLS secure channel.*

  This error occurs because of a recent GitHub support deprecation of the Tlsv1 and Tlsv1.1 cryptographic standards (the default for PowerShell). For more information, see Weak cryptographic standards removal notice.

  To resolve this issue, add `[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12` to the top of the script to force the PowerShell console to use TLSv1.2 when downloading from GitHub repositories.

Download the update

You can download the Azure Stack 1803 update package from here.

See also

- 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.