Azure Stack 1802 Update | Microsoft Docs

brenduns

Azure Stack 1802 update

Applies to: Azure Stack integrated systems

This article describes the improvements and fixes in the 1802 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 1802 update build number is **20180302.1**.

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 1712 Update before you apply the Azure Stack 1802 update.
- Install **AzS Hotfix 1.0.180312.1- Build 20180222.2** before you apply the Azure Stack 1802 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**.

Post-update steps

After the installation of 1802, install any applicable Hotfixes. For more information view the following knowledge base articles, as well as our Servicing Policy. - Azure Stack hotfix **1.0.180302.4**. KB 4131152 - Existing Virtual Machine Scale Sets may become unusable

This fix also resolves the issues detailed in KB 4103348 - Network Controller API service crashes when you try to install an Azure Stack update.

New features and fixes

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

- **Support is added for the following Azure Storage Service API versions**:
  - 2017-04-17
  - 2016-05-31
  - 2015-12-11
  - 2015-07-08

  For more information, see Azure Stack Storage: Differences and considerations.
- **Support for larger Block Blobs**:
  - The maximum allowable block size is increased from 4 MB to 100 MB.
  - The maximum blob size is increased from 195 GB to 4.75 TB.
- **Infrastructure backup** now appears in the Resource Providers tile, and alerts for backup are enabled. For more information about the Infrastructure Backup Service, see Backup and data recovery for Azure Stack with the Infrastructure Backup Service.
- **Update to the *Test-AzureStack* cmdlet** to improve diagnostics for storage. For more information on this cmdlet, see Validation for Azure Stack.
- **Role-Based Access Control (RBAC) improvements** - You can now use RBAC to delegate permissions to Universal User Groups when Azure Stack is deployed with AD FS. To learn more about RBAC, see Manage RBAC.
- **Support is added for multiple fault domains**. For more information, see High availability for Azure Stack.
- **Support for physical memory upgrades** - You can now expand the memory capacity of Azure Stack integrated system after your initial deployment. For more information, see Manage physical memory capacity for Azure Stack.
- **Various fixes** for performance, stability, security, and the operating system that is used by Azure Stack.

Known issues with the update process

There are no known issues for the installation of update 1802.

Known issues (post-installation)

The following are post-installation known issues for build **20180302.1**

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.

- 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.

- In both the admin portal and user portal, the Overview blade fails to load when you select the Overview blade for storage accounts that were created with an older API version (example: 2015-06-15). This includes system storage accounts like **updateadminaccount** that is used during patch and update.

  As a workaround, use PowerShell to run the **Start-ResourceSynchronization.ps1** script to restore access to the storage account details. The script is available from GitHub, and must run with service administrator credentials on the privileged endpoint.

- The **Service Health** blade fails to load. When you open the Service Health blade in either the admin or user portal, Azure Stack displays an error and does not load information. This is expected behavior. Although you can select and open Service Health, this feature is not yet available but will be implemented in a future version of Azure Stack.

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`.
- You cannot scale up a virtual machine scale set (VMSS) that was created when using Azure Stack prior to version 1802. This is due to the change in support for using availability sets with virtual machine scale sets. This support was added with version 1802. When you attempt to add additional instances to scale a VMSS that was created

prior to this support being added, the action fails with the message *Provisioning state failed*.

This issue is resolved in version 1803. To resolve this issue for version 1802, install Azure Stack hotfix **1.0.180302.4**. For more information, see KB 4131152: Existing Virtual Machine Scale Sets may become unusable.

- Azure Stack supports using only Fixed type VHDs. Some images offered through the marketplace on Azure Stack use dynamic VHDs but those have been removed. Resizing a virtual machine (VM) with a dynamic disk attached to it leaves the VM in a failed state.

  To mitigate this issue, delete the VM without deleting the VM's disk, a VHD blob in a storage account. Then convert the VHD from a dynamic disk to a fixed disk, and then re-create the virtual machine.

- 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.

- Internal Load Balancing (ILB) improperly handles MAC addresses for back-end VMs, which causes ILB to break when using Linux instances on the Back-End network. ILB works fine with Windows instances on the Back-End Network.
- The IP Forwarding feature is visible in the portal, however enabling IP Forwarding has no effect. This feature is not yet supported.
- 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:*

```
Login-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:*

```
Login-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 1802, 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 1710, first apply version 1711, then 1712, and then update to 1802.

The install of update 1802 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.

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 1802 update package from here.

More information

Microsoft has provided a way to monitor and resume updates using the Privileged End Point (PEP) installed with Update 1710.

- See the Monitor updates in Azure Stack using the privileged endpoint documentation.

See also

- 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.