Azure Stack 1805 Update | Microsoft Docs

sethmanheim

Azure Stack 1805 update

Applies to: Azure Stack integrated systems

This article describes the improvements and fixes in the 1805 update package, known issues for this version, 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 1805 update build number is **1.1805.1.47**.

[!TIP]
Based on customer feedback, there is an update to the version schema in use for Microsoft Azure Stack. Starting with this update, 1805, the new schema better represents the current cloud version.

The version schema is now *Version.YearYearMonthMonth.MinorVersion.BuildNumber* where the second and third sets indicate the version and release. For example, 1805.1 represents the *release to manufacturing* (RTM) version of 1805.

New features

This update includes the following improvements for Azure Stack. - **Azure Stack now includes a *Syslog* client** as a *preview feature*. This client allows the forwarding of audit and security logs related to the Azure Stack infrastructure to a Syslog server or security information and event management (SIEM) software that is external to Azure Stack. Currently, the Syslog client only supports unauthenticated UDP connections over default port 514. The payload of each Syslog message is formatted in Common Event Format (CEF).

To configure the Syslog client, use the **Set-SyslogServer** cmdlet exposed in the Privileged Endpoint.

With this preview, you might see the following three alerts. When presented by Azure Stack, these alerts include *descriptions* and *remediation* guidance. - TITLE: Code Integrity Off
- TITLE: Code Integrity in Audit Mode - TITLE: User Account Created

While this feature is in preview, it should not be relied upon in production environments.

Fixed issues

- We fixed the issue that blocked opening a new support request from the dropdown from within the admin portal. This option now works as intended.
- **Various fixes** for performance, stability, security, and the operating system that is used by Azure Stack.

Before you begin

Prerequisites

- Install the Azure Stack 1804 update before you apply the Azure Stack 1805 update.
- Install the latest available update or hotfix for version 1804.
- Before you start installation of update 1805, run Test-AzureStack to validate the status of your Azure Stack and resolve any operational issues found. Also review active alerts, and resolve any that require action.

Known issues with the update process

- During installation of the 1805 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 the update to 1805 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.

Post-update steps

After the installation of 1805, install any applicable Hotfixes. For more information view the following knowledge base articles, as well as our Servicing Policy.
- KB 4344102 - Azure Stack Hotfix 1.1805.7.57.

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.
- 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.
- You cannot apply driver updates by using an OEM Extension package with this version of Azure Stack. There is no workaround for this problem.

- When you select **Overview** for a storage account in either the admin or user portals, the information from the *Essentials* pane does not display. The Essentials pane displays information about the account like its *Resource group*, *Location*, and *Subscription ID*. Other options for Overview are accessible, like *Services* and *Monitoring*, as well as options to *Open in Explorer* or to *Delete storage account*.

  To view the unavailable information, use the Get-azureRMstorageaccount PowerShell cmdlet.

- When you select **Tags** for a storage account in either the admin or user portals, the information fails to load and does not display.

  To view the unavailable information, use the Get-AzureRmTag PowerShell cmdlet.

- 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.
- Some administrative subscription types are not available. When you upgrade Azure Stack to this version, the two subscription types that were introduced with version 1804 are not visible in the console. This is expected. The unavailable 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.
- You might not have use of the horizontal scroll bar along the bottom of the admin and user portals. If you can't access the horizontal scroll bar, use the breadcrumbs to navigate to a previous blade in the portal by selecting the name of the blade you want to view from the breadcrumb list found at the top left of the portal.
- 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.

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 #1 and #2 can be safely ignored and they'll close automatically over time.

You might also see the following alert for *Capacity*. For this alert, the percentage of available memory identified in the description can vary:

Alert #3:

- NAME: Low memory capacity
- SEVERITY: Critical
- COMPONENT: Capacity
- DESCRIPTION: The region has consumed more than 80.00% of available memory. Creating virtual machines with large amounts of memory may fail.

In this version of Azure Stack, this alert can fire incorrectly. If tenant virtual machines continue to deploy successfully, you can safely ignore this alert.

Alert #3 does not automatically close. If you close this alert Azure Stack will create the same alert within 15 minutes.

- As 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 selecting a virtual machine size for a virtual machine deployment, some F-Series VM sizes are not visible as part of the size selector when you create a VM. The following VM sizes do not appear in the selector: *F8s_v2*, *F16s_v2*, *F32s_v2*, and *F64s_v2*. As a workaround, use one of the following methods to deploy a VM. In each method, you need to specify the VM size you want to use.

  - **Azure Resource Manager template:** When you use a template, set the *vmSize* in the template to equal the VM size you want to use. For example, the following entry is used to deploy a VM that uses the *F32s_v2* size:

```
"properties": {
"hardwareProfile": {
        "vmSize": "Standard_F32s_v2"
},
```

  - **Azure CLI:** You can use the az vm create command and specify the VM size as a parameter, similar to `--size "Standard_F32s_v2"`.
  - **PowerShell:** With PowerShell you can use New-AzureRMVMConfig with the parameter that specifies the VM size, similar to `-VMSize "Standard_F32s_v2"`.

- 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 DS series VM. DS 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

- You cannot create user-defined routes in either the admin or user portal. As a workaround, use Azure PowerShell.
- 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.
- 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 original VM, and not to the new one.

- If you raise a Quota limit for a Network resource that is part of an Offer and Plan that is associated with a tenant subscription, the new limit is not applied to that subscription. However, the new limit does apply to new subscriptions that are created after the quota is increased.

  To work around this problem, use an Add-On plan to increase a Network Quota when the plan is already associated with a subscription. For more information, see how to make an add-on plan available.

- You cannot delete a subscription that has DNS Zone resources or Route Table resources associated with it. To successfully delete the subscription, you must first delete DNS Zone and Route Table resources from the tenant subscription.
- 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:*

```
Connect-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:*

```
Connect-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

- 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** or **Tier** names when you create a SKU for the SQL and MySQL resource providers.

[!NOTE]
After you update to Azure Stack 1805, 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 1803, first apply version 1804, and then update to 1805.

The install of update 1805 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.
- App Service can only be deployed into the *Default Provider subscription* at this time.

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.

Download the update

You can download the Azure Stack 1805 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.