Azure Stack 1712 Update | Microsoft Docs

brenduns

Azure Stack 1712 update

Applies to: Azure Stack integrated systems

This article describes the improvements and fixes in this update package, known issues for this release, and where to download the update. Known issues are divided into known issues directly related to the update process, and known issues with the build (post-installation).

[!IMPORTANT] This update package is only applicable for Azure Stack integrated systems. Do not apply this update package to the Azure Stack Development Kit.

Build reference

The Azure Stack 1712 update build number is **180106.1**. If a customer has deployed **180103.2** previously, you do not need to apply **180106.1**.

Before you begin

[!IMPORTANT] Do not attempt to create virtual machines during the 1712 update installation process. See manage updates in Azure Stack overview for more details.

Prerequisites

You must first install the Azure Stack 1711 Update before applying this update.

Post-update steps

- After the installation of 1712, install any applicable Hotfixes. For more information view the following knowledge base articles, as well as our Servicing Policy.
  - KB 4103348 - Network Controller API service crashes when you try to install an Azure Stack update
- Update 1712 also requires that you install firmware updates from the OEM partner after you complete the 1712 Azure Stack update installation.

  [!NOTE] Please refer to your OEM partner website to download the updates.

New features and fixes

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

New features

- Test-AzureStack cmdlet to validate Azure Stack Cloud available via privileged endpoint

- Ability to register a disconnected deployment of Azure Stack
- Monitoring alerts for certificate and user account expiration
- Added Set-BmcPassword cmdlet in PEP for BMC password rotation
- Network logging updates to support on-demand logging
- Support reimage operation for Virtual Machine Scales Sets (VMSS)
- Enable kiosk mode on ERCS VM for CloudAdmin login
- Tenants can activate Windows VMs automatically

Fixes

- Fix to show Node Operational Status in maintenance while running repair
- Fix to correct Public IP usage records time/date stamp
- Various other performance, stability and security fixes
- TimeSource and Defender privileged endpoint module bug fixes

Windows Server 2016 new features and fixes

- January, 3rd - 2018 KB4056890 (OS Build 14393.2007)
  - This update includes the software fixes for the industry-wide security issue described by MSRC Security Advisory ADV 180002.

Known issues with the update process

This section contains known issues that you may encounter during the 1712 update installation.

1. **Symptom:** Azure Stack operators may see the following error during the update process: *"Type 'CheckHealth' of Role 'VirtualMachines' raised an exception:Machine health check for -ACS01 produced the following errors.was an error getting VM information from hosts. Exception details:-VM : The operation on computer 'Node03' failed: The WS-Management service cannot process the request. The WMI or the WMI provider returned an unknown error: HRESULT 0x8004106c."*
    1. **Cause:** This issue is caused by a Windows Server issue that is intended to be addressed in subsequent Window server updates.
    2. **Resolution:** Contact Microsoft Customer Service and Support (CSS) for assistance.
2. **Symptom:** Azure Stack operators may see the following error during the update process:*"Enabling the seed ring VM failed on node Host-Node03 with an error: [Host-Node03] Connecting to remote server Host-Node03 failed with the following error message : The WinRM client received an HTTP server error status (500), but the remote service did not include any other information about the cause of the failure."*
    1. **Cause:** This issue is caused by a Windows Server issue that is intended to be addressed in subsequent Window server updates.
    2. **Resolution:** Contact Microsoft Customer Service and Support (CSS) for assistance.

Known issues (post-installation)

This section contains post-installation known issues with build **180106.1**.

Portal

- It may not be possible to view compute or storage resources in the administrator portal. This indicates that an error occurred during the installation of the update and that the update was incorrectly reported as successful. If this issue occurs, please contact Microsoft CSS for assistance.
- You may 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**.
- When you view the properties of a resource group, the **Move** button is disabled. This behavior is expected. Moving resource groups between subscriptions is not currently supported.
- For any workflow where you select a subscription, resource group, or location in a drop-down list, you may experience one or more of the following issues:

  - You may see a blank row at the top of the list. You should still be able to select an item as expected.
  - If the list of items in the drop-down list is short, you may not be able to view any of the item names.
  - If you have multiple user subscriptions, the resource group drop-down list may be empty.

    [!NOTE] To work around the last two issues, you can type the name of the subscription or resource group (if you know it), or you can use PowerShell instead.

- 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 are not able to view permissions to your subscription using the Azure Stack portals. As a workaround, you can verify permissions by using PowerShell.
- 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.

- If you reboot an infrastructure role instance, you may receive a message indicating that the reboot failed. However, the reboot actually succeeded.

Marketplace

- Some marketplace items are being removed in this release due to compatibility concerns. These will be re-enabled after further validation.
- 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

- Users are given the option to create a virtual machine with geo-redundant storage. This configuration causes virtual machine creation to fail.
- You can configure a virtual machine availability set only with a fault domain of one, and an update domain of one.
- There is no marketplace experience to create virtual machine scale sets. You can create a scale set by using a template.
- 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`.

Networking

- You can't create a load balancer with a public IP address by using the portal. As a workaround, you can use PowerShell to create the load balancer.
- You must create a network address translation (NAT) rule when you create a network load balancer. If you don't, you'll receive an error when you try to add a NAT rule after the load balancer is created.
- You can't disassociate a public IP address from a virtual machine (VM) after the VM has been created and associated with that IP address. Disassociation will appear to work, but the previously assigned public IP address remains associated with the original VM. 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. Currently, you must only use new public IP addresses for new VM creation.
- Azure Stack operators may be unable to deploy, delete, modify VNETs or Network Security Groups. This issue is primarily seen on subsequent update attempts of the

same package. This is caused by a packaging issue with an update which is currently under investigation.
- Internal Load Balancing (ILB) improperly handles MAC addresses for back-end VMs which breaks Linux instances.

SQL/MySQL

- It can take up to an hour before tenants can create databases in a new SQL or MySQL SKU.
- Creation of items directly on SQL and MySQL hosting servers that are not performed by the resource provider is not supported and may result in a mismatched state.

  [!NOTE] You should not have impact to your existing SQL or MySQL resource provider users when updating your Azure Stack Integrated Systems to the 1712 version. You can continue to use your current SQL or MySQL resource provider builds until a new Azure Stack update is available.

App Service

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

Identity

In Azure Active Directory Federation Services (ADFS) deployed environments, the **azurestack* account is no longer the owner of the Default Provider Subscription. Instead of logging into the** Admin portal / adminmanagement endpoint** with the **azurestack*, you can use the **azurestack* account, so that you can manage and use the Default Provider Subscription.

[!IMPORTANT] Even though the **azurestack* account is the owner of the Default Provider Subscription in ADFS deployed environments, it does not have permissions to RDP into the host. Continue to use the** azurestack* account or the local administrator account to login, access and manage the host as needed.

Download the update

You can download the Azure Stack 1712 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 1712.

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

See also

- See Manage updates in Azure Stack overview for an overview of the update management in Azure Stack.
- See Apply updates in Azure Stack for more information about how to apply updates with Azure Stack.