

# Microsoft EEAP Release Notes

---

Key information	Build validation and feedback	What's new	Bug fixes	Known issues	Breaking changes
-----------------	-------------------------------	------------	-----------	--------------	------------------

## Windows Server LTSC and SAC, preview build 17754.1

---

These release notes describe the new features, bug fixes, known issues, and breaking changes introduced since build 17751.1 of Windows Server 2019 Long-Term Servicing Channel (LTSC).

This build includes the following:

### Long-Term Servicing Channel (LTSC) preview

- Windows Server 2019 Datacenter Edition and Standard Edition with Desktop Experience and Server Core installation options (ISO and VHDX)

### Semi-Annual Channel (SAC) preview

- Windows Server Datacenter Edition and Standard Edition with Core installation options (ISO and VHDX)

### Additional content (LTSC and SAC)

- Nano Server Container
- Server Core Container
- Microsoft Hyper-V Server preview

## Key information

---

This section has key information required for testing the latest build.

Windows Server activation keys	<p>This build and future builds require use of activation keys during setup. The following keys allow for unlimited activations.</p> <table border="1" data-bbox="467 472 1403 638"><tr><td data-bbox="467 472 727 556"><b>Datacenter</b></td><td data-bbox="727 472 1403 556">6XBNX-4JQGW-QX6QG-74P76-72V67</td></tr><tr><td data-bbox="467 556 727 638"><b>Standard</b></td><td data-bbox="727 556 1403 638">MFY9F-XBN2F-TYFMP-CCV49-RMYVH</td></tr></table> <p><b>Note</b> The pre-release activation keys provided for previous preview builds are not valid for build 17751 or later. You may skip the activation key during setup and still have a fully functional build to test with. For upgrades from released operating systems, setup does not allow you to skip entering the key. For upgrade testing, you will need to use build 17744.</p> <p>This Server Insider preview release build will expire on December 14, 2018.</p>	<b>Datacenter</b>	6XBNX-4JQGW-QX6QG-74P76-72V67	<b>Standard</b>	MFY9F-XBN2F-TYFMP-CCV49-RMYVH
<b>Datacenter</b>	6XBNX-4JQGW-QX6QG-74P76-72V67				
<b>Standard</b>	MFY9F-XBN2F-TYFMP-CCV49-RMYVH				
Symbols for debugging	<p>If you need symbols, you can obtain them from the public symbol server. For details, see <a href="#">Using the Microsoft Symbol Server</a>.</p>				
HLK and Certification Guidance	<p>The Windows Hardware Lab Kit (HLK) will be updated to support Windows 10 vNext and Windows Server 2019.</p> <p>The HLK is updated each week and available for download on Microsoft Collaborate, you will see the download locations with your weekly build notifications.</p> <p>The HLK for Windows 10 and Windows Server 2019 will enforce the Windows 10 hardware requirements and policies, which will be posted on MSDN in March, and is designed for testing Windows 10 vNext and Windows Server 2019.</p> <p>The support scenarios identified in the following table will be accepted.</p>				

<b>HLK VERSION</b>	<b>WINDOWS 10 VERSIONS SUPPORTED</b>	<b>DEVICE/COMPONENT SUBMISSIONS ACCEPTED</b>	<b>SYSTEM SUBMISSIONS ACCEPTED</b>
"RS5"	Code named "RS5"	"RS5" client device/component Windows Server 2019 device/component	"vNext" Server systems
1709	1709 - client	1709 client device/component	1709 client systems
1703	1703 - client 1607 - client	1703 client device/component 1607 client device/component	1703 client systems
1607	1607 - client 1607 - Server, Azure Stack, SDDC 1511 - client	1607 client device/component 1607 Server device/component 1511 client device/component	1607 Server systems

When submitting a Windows 10 RS5 and Windows Server 2019 HLK package for validation, you must use Windows 10 vNext and Windows Server 2019, version build TBD or newer on the test device. The submission will otherwise be rejected.

You must continue to use the Windows Hardware Certification Kit (HCK) version 2.1 to certify for following operating systems:

- Windows 7
- Windows 8
- Windows 8.1
- Windows Server 2012
- Windows Server 2012 R2

You must continue to use the Windows Logo Kit (WLK) version 1.6 to certify for following operating systems:

- Windows Server 2008 R2 (x64 and ia64)

	<ul style="list-style-type: none"><li>• Windows Server 2008 (x86, x64 and ia64)</li></ul> <p>Certification for Windows Server 2016, Azure Stack and SDDC must meet the Windows Hardware Compatibility Requirements as stated in version 1607 of the documentation, use the 1607 version of the Windows Server 2016 operating system and use HLK version 1607 build 14393 with matching playlist and supplemental content to generate logs and following the policies stated in the Windows Server Policy. Questions about the Azure Stack or SDDC program or how to submit the results for solution validation should be directed to the appropriate Microsoft contact—a technical account manager or a partner management contact.</p>
Installing kits on released operating systems	<p>If you are installing the Windows 10 kits on a publicly released OS such as Windows 10, version 1703, Windows 10, version 1607, Windows 10, version 1511, Windows 10, Windows 8.1, Windows 8, or Windows 7, you must disable strong name-signing and manually install two additional test certificates. To do this, perform the following installation procedure once for each test computer, using an account with administrator privileges on the controller computer:</p> <ul style="list-style-type: none"><li>• From the <b>KitPreinstall</b> folder, install the <b>TestRoot.cer</b> and <b>TestRoot-SHA2.cer</b> test certificates using the following steps:<ol style="list-style-type: none"><li>1. Download the Kit Pre-install package, <i>KitPreinstallV2.zip</i>, from <a href="https://developer.microsoft.com/en-us/dashboard/collaborate/packages/4778">developer.microsoft.com/en-us/dashboard/collaborate/packages/4778</a>.</li><li>2. On the controller computer, extract the files and right-click the certificate.</li><li>3. Click <b>Install Certificate</b>.</li><li>4. Click <b>Next</b>.</li><li>5. Accept the default for the certificate store, and click <b>Next</b>.</li><li>6. Click <b>Finish</b>.</li></ol></li><li>• From the same folder, disable strong name signing by installing the <b>StrongNameBypass.reg</b> and <b>WOW64StrongNameBypass.reg</b> registry keys, as follows:<ol style="list-style-type: none"><li>1. From the controller computer, right-click the registry key.</li><li>2. Click <b>Merge</b>.</li><li>3. Click <b>Run</b>.</li><li>4. Click <b>Yes</b>.</li></ol></li></ul>

Playlists to support the incremental Windows releases

Due to the change in the policy regarding which versions of Windows 10 that the HLK validates, it is important to note which tests are required with each kit. Playlists must match the version of the HLK being used, not the version of Windows 10 that is under test. For RS5 and Windows Server 2019 Previews, the Preview Playlist is available on Collaborate at:

<https://partner.microsoft.com/en-us/dashboard/collaborate/packages/5733>.

The follow table lists the required playlist pairings.

HLK VERSION	ARCHITECTURE	PLAYLIST
"RS5"	x86 or x64	HLK Version 1709 CompatPlaylist x86_x64
"RS5"	ARM64 desktop	HLK Version 1709 CompatPlaylist ARM64 HLK Version 1709 CompatPlaylist ARM64_x86 on ARM64
1709	x86 or x64	HLK Version 1709 CompatPlaylist x86_x64
1709	ARM64 desktop *	HLK Version 1709 CompatPlaylist ARM64 HLK Version 1709 CompatPlaylist ARM64_x86 on ARM64
1703	x86 or x64	HLK Version 1703 CompatPlaylist
1607	x86 or x64	HLK Version 1607 CompatPlaylist

Testing ARM64 Desktop requires two playlists. For additional information, see the setup instructions in [Step 1: Install Controller and Studio on the test server](#) on Hardware Dev Center.

Symbols for debugging

If you need symbols, you can obtain them from the public symbol server. For details, see [Using the Microsoft Symbol Server](#).

## Build validation and feedback

---

In each preview release, there are two major areas that we would like you to try out:

- **In-place OS Upgrade** (from Windows Server 2012 R2, Windows Server 2016 or a previous preview build).
- **Application compatibility** – please let us know if any server roles or applications stops working or fails to function as it used to.

Please report any issues you find.

In addition, please also validate functionality that was introduced in previous preview releases. For a list of new features introduced in earlier releases, see [aka.ms/ServerInsider-WhatsNew](https://aka.ms/ServerInsider-WhatsNew).

As always, we welcome your feedback.

## What's new

---

This section describes some of the new features that are in this build. For a list of all new features in Windows Server 2019, see [What's New in Windows Server 2019 Insider Preview Builds](#).

### Azure Host Awareness in an IaaS Virtual Machine

Numerous companies run Windows Servers in Azure. A common occurrence is when the host needs some sort of maintenance. Depending on the type of maintenance it is, the IaaS virtual machine can be moved off onto another host to continue production. However, in some cases, the maintenance would be very brief (less than a minute) and the virtual machine is simply frozen while maintenance occurs. In the case of Failover Clusters as an example, this could cause issues with connectivity between the nodes that may result in unexpected failovers or a node being removed from membership. The user is left to guess what had happened.

In Windows Server 2019, we are now letting the users know ahead of time when scheduled

Azure Host Maintenance is to occur through events. Not only that, we have added new parameters you can set to react to this, if desired, ahead of time.

An example of this event is:

```
Log: System
Level: Warning
Event ID: 1139
Description: The cluster service has detected an Azure host maintenance event
has been scheduled. This maintenance event may cause the node hosting the
virtual machine to become unavailable during this time.

Node:
Approximate Time:
Details:
EventStatus: Scheduled Event
Type: Freeze Machine
Type: Virtual Machine
```

As you can see, host maintenance has been scheduled. The event log also tells you what virtual machine will be affected and what will happen to it (as well as the date and time). We have two additional events for this:

- Event ID 1136 – node maintenance is imminent
- Event ID 1140 – node maintenance has been rescheduled

There are also two new cluster properties: **DetectManagedEvents** and **DetectManagedEventsThreshold**.

DetectManagedEvents:

- 0 = Do not log Azure host scheduled events
- 1 = Log Azure host scheduled events (default)
- 2 = Avoid placement and do not move any roles to this node
- 3 = Pause and drain this node when a scheduled event takes place
- 4 = Pause, drain, and failback when a scheduled event is detected

DetectManagedEventsThreshold:

- 60 seconds = amount of time for DetectManagedEvents parameter to execute prior the scheduled event

## Bug fixes

---

The bug fixes described in the following table are new in this build.

WORK ITEM	DESCRIPTION OF BUG FIX
18321838	We resolved an memory leak that affected apps that use the input method editor (IME) for Simplified Chinese.
18248987, 18204211, 18243704, 18291237, 18420214, 18498975	We resolved an issue that could result in garbage characters being displayed in a PowerShell Window, depending on the display language that is configured for the system. Affected display languages included Japanese and Korean.
17854321	We resolved an issue that could result in a system having two COM2 devices, each with different resources, after an affected system running Windows Server 2012 R2 or Windows Server 2016 was upgraded to a recent preview release of the operating system.
17845524	We resolved an issue that caused the back-up GUID Partition Table (GPT) to not be compliant with UEFI on a DirectAccess (DAX) volume.
18688591	<p>We resolved the following issue: After a system running Server Core is transitioned (transmogrified) to Server Datacenter—for example, by running the command <b>dism /online /set-edition:ServerDatacenterCore /ProductKey:product-key/AcceptEula</b>—the operating system is not licensed. On an affected system, the administrator is not instructed to restart the system, and the operating system indicates that it is a retail channel version rather than a Generic Volume License Key (GVLK) version, even when the product key is a GVLK key.</p> <p>To make an affected system licensed, run the following command: <b>cscript c:\Windows\System32\slmgr.vbs /ipkproduct-key</b></p>

WORK ITEM	DESCRIPTION OF BUG FIX
18254122	We resolved the following issue: [NEW] On a system that has <a href="#">Exchange Management Shell</a> installed and operating on a preview release of the operating system, Exchange Management Shell stops working with an error, HTTP 500, following an in-place upgrade of the operating system to a newer preview release.

## Known issues

---

The following known issues are new in this build, or they were not resolved in the last build.

WORK ITEM	DESCRIPTION OF KNOWN ISSUE
18821773	There is a discrepancy in the ProductName entry in the registry: Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName where it reports "Windows Server Datacenter" - systeminfo.exe and WMI value from Win32_OperatingSystem instead of the expected ProductName.
18814123	A container host may become unresponsive due to a deadlock when attempting to mount a volume. On an affected system, Docker hangs on all commands.
18428421, 18034699	The operating system has an unnecessary utility account for Windows Defender Application Guard.
18471696	The Virtual Hard Disk Miniport Driver (Vhdmp.sys) may experience a bug check, SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e).
18314155	When a Windows Defender Application Guard container crashes, the resulting type of dump may be unexpected.

WORK ITEM	DESCRIPTION OF KNOWN ISSUE
18321045, 18306015, 18098973, 18321007	On recent preview builds, database applications might not be able to initialize a database and fail with a stack overflow or insufficient privileges when the database is located on an SMB volume.
18198732	Shielded VMs running Linux do not boot. The loader (LSVMLoad) waits for a passphrase for the boot partition.
17033455	<p>Creating or modifying environment variables by using <b>setx</b> fails on a system running in a Nano Container (that is, Nano Server as a container image). On an affected system, <b>setx</b> requires a specific path in the registry, HKCU\Environment\, to exist by default.</p> <p>You can work around this issue by changing where the variable is stored in the registry, or you can add the expected registry path before executing <b>setx</b> commands. To specify that the variable be set for system-wide use in HKLM rather than in HKCU, the default, add the <b>/M</b> switch to a <b>setx</b> command. To instead add the expected registry path, run <b>reg add HKCU\Environment</b> before executing <b>setx</b> commands.</p>

## Breaking changes

---

No breaking changes are included in this build.