Microsoft

Microsoft EEAP Release Notes

These release notes describe the new features, bug fixes, known issues, and breaking changes introduced since build 17613.1000 of Windows Server.

Windows Server vNext LTSC Preview, build 17618.1000

This pre-release of Windows Server includes the configurations listed in the following table.

COMPONENT	BUILD NUMBER
Windows Server Datacenter Edition with Desktop Experience and Server Core installation options	17618.1000.180302-1651
Windows Server Standard Edition with Desktop Experience and Server Core installation options	17618.1000.180302-1651

Key information

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

Logo requirements	There are no new feature AQs that are planned for the pre-release version of Windows Server, so no action is required from vendors. However, there are new logo requirements that mention Windows Server, so vendors should take the changed logo requirements as a notice of what will be required for the next Long-Term Servicing Channel (LTSC).

Windows Server activation keys	Pre-release builds of Windows Server are already activated and do not require you to enter activation keys.
HLK and tests	We have a new Windows Hardware Lab Kit (HLK) and tests, and a new OS, but because there are no new major features planned that affect hardware products for Windows Server, there is no action required. However, even though there is no testing or submission for Windows Server, a vendor might want to run the new tests on client OSes, since many tests do not work on Server Core. For example, on products that you have already submitted for Windows Server 2016, make sure that tests are not: • Finding issues on vendor products that the vendor should fix before the next Long-Term Servicing Channel (LTSC). • Incorrectly finding issues (false positives) that Microsoft must fix before the next LTSC. • Finding issues that the vendor may need to fix if an end customer decides to deploy Windows Server.
Certification requirements for Windows Server, Azure Stack, and SDDC	To be certified as a vendor for Windows Server 2016, Azure Stack, and Software-Defined Datacenter (SDDC), you must do the following: • Continue to meet the Windows Hardware Compatibility Requirements for your products, as stated in version 1607 of the documentation. • Use version 1607 (build 14393) of the Windows Hardware Lab Kit (HLK) with matching playlist and supplemental content to generate logs for submissions. • Follow the policies stated in the Windows Server Policy document. For questions about the Azure Stack or SDDC programs, and for instructions for submitting the results for solution validation, contact your Microsoft technical account manager or partner management contact.
Symbols for debugging	If you need symbols, you can obtain them from the public symbol server. For details, see Using the Microsoft Symbol Server.

On a test computer using a publicly released OS, strong name-signing must be disabled, and additional test certificates must be installed	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: • From the **KitPreInstall** folder, install the **TestRoot.cer** and **TestRoot-SHA2.cer** test certificates using the following steps: 1. From the controller computer, right-click the certificate. 2. Click **Install Certificate**. 3. Click **Next**. 4. Accept the default for the certificate store, and click **Next**. 5. Click **Finish**. • From the same folder, disable strong name signing by installing the **StrongNameBypass.reg** and **WOW64StrongNameBypass.reg** registry keys, as follows: 1. From the controller computer, right-click the registry key. 2. Click **Merge**. 3. Click **Run**. 4. Click **Yes**.

What's in this build

For every preview release, we will provide a focus area that we would like you to take a look at and provide us with feedback on. Of course, we are open to, and encourage you to, try out any functionality in the release, and we welcome your feedback.

There are two major areas that we would like you to try out in each preview release and report back any issues:

- **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.

This preview focus area: **Security**

The following sections describe new security functionality that is available in this preview.

Windows Defender Advanced Threat Protection

We provide deep platform sensors, which provide visibility to memory- and kernel-level attacker activities and abilities, and response actions for incidents that affect compromised machines, enabling remote collection of additional forensic data, remediating malicious files, terminating malicious processes, and so on.

If you're already using Windows Defender Advanced Threat Protection (ATP), preview these features by simply installing the latest preview build of Windows Server, and onboard it to Windows Defender ATP.

Otherwise, sign up for the Windows Defender ATP trial on Windows Defender Advanced Threat Protection.

Windows Defender ATP Exploit Guard

Windows Defender ATP Exploit Guard is a new set of host-intrusion prevention capabilities. The four components of Windows Defender Exploit Guard are designed to lock down the device against a wide variety of attack vectors and block behaviors commonly used in malware attacks, while enabling enterprises to balance their security risk and productivity requirements.

- **Attack Surface Reduction (ASR)**: A set of controls that enterprises can enable to prevent malware from getting on the machine by blocking suspicious malicious files (for example, Office files), scripts, lateral movement, ransomware behavior, and email-based threats.

- **Network protection**: Protects the endpoint against web-based threats by blocking any outbound process on the device to untrusted hosts/IP addresses through Windows Defender SmartScreen.

- **Controlled folder access**: Protects sensitive data from ransomware by blocking untrusted processes from accessing your protected folders.

- **Exploit protection**: A set of mitigations for vulnerability exploits (replacing EMET) that can be easily configured to protect your system and applications.

To deploy a default set of Exploit Guard policy on Windows Server, run the following cmdlets:

```
Set-MpPreference -EnableControlledFolderAccess Enabled

Set-MpPreference -EnableNetworkProtection Enabled

Add-MpPreference -AttackSurfaceReductionRules_Ids 75668C1F-73B5-4CF0-BB93-3ECF5CB7CC84 -AttackSurfaceReductionRules_Actions Enabled

Add-MpPreference -AttackSurfaceReductionRules_Ids 3B576869-A4EC-4529-8536-B80A7769E899 -AttackSurfaceReductionRules_Actions Enabled

Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB-401B-4EfC-AADC-AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled

Add-MpPreference -AttackSurfaceReductionRules_Ids D3E037E1-3EB8-44C8-A917-57927947596D -AttackSurfaceReductionRules_Actions Enabled

Add-MpPreference -AttackSurfaceReductionRules_Ids 5BEB7EFE-FD9A-4556-801D-275E5FFC04CC -AttackSurfaceReductionRules_Actions Enabled

Add-MpPreference -AttackSurfaceReductionRules_Ids BE9BA2D9-53EA-4CDC-84E5-9B1EEEE46550 -AttackSurfaceReductionRules_Actions Enabled

Add-MpPreference -AttackSurfaceReductionRules_Ids 92E97FA1-2EDF-4476-BDD6-9DD0B4DDDC7B -AttackSurfaceReductionRules_Actions Enabled

Add-MpPreference -AttackSurfaceReductionRules_Ids D1E49AAC-8F56-4280-B9BA-993A6D77406C -AttackSurfaceReductionRules_Actions Disabled

Add-MpPreference -AttackSurfaceReductionRules_Ids 01443614-cd74-433a-b99e-2ecdc07bfc25 -AttackSurfaceReductionRules_Actions Enabled
```

```
$url = 'https://demo.wd.microsoft.com/Content/ProcessMitigation.xml'

Invoke-WebRequest $url -OutFile ProcessMitigation.xml

Write-Host "Enabling Exploit Protection"

Set-ProcessMitigation -PolicyFilePath ProcessMitigation.xml
```

Windows Defender Application Control

Windows Defender Application Control—also known as *Code Integrity (CI) policy*—was released in Windows Server 2016. Customer feedback has suggested that it is a great concept, but hard to deploy. To address this, we are building default CI policies, which will allow all Windows in-box files and Microsoft applications, such as SQL Server, and block known executables that can bypass CI.

You can download the default policies at: https://developer.microsoft.com/en-us/dashboard/collaborate/packages/4265

The package contains an audit version and an enforced version. If the server doesn't require additional drivers/applications, you can deploy the enforced version. Otherwise, you can use the audit policy, check uncovered executables, and then merge them into the default CI policy.

To deploy the default code integrity policy, run the following commands:

```
Copy-Item C:\CI\ServerDefault-EnforcedCI.bin
C:\Windows\System32\CodeIntegrity\SiPolicy.p7b
```

Reboot the server to allow code integrity service to load the policy.

Failover Cluster removing use of NTLM authentication

Windows Server Failover Clusters no longer use NTLM authentication by exclusively using Kerberos and certificate-based authentication. There are no changes required by the user, or deployment tools, to take advantage of this security enhancement. It also allows failover clusters to be deployed in environments where NTLM has been disabled.

Shielded virtual machines – Offline mode, VMConnect and Linux support

You can now run shielded virtual machines on machines with intermittent connectivity to the Host Guardian Service by leveraging the new fallback HGS and offline mode features. Fallback HGS allows you to configure a second set of URLs for Hyper-V to try if it can't reach your primary HGS server. To see how this can be used in a branch-office scenario, see Improved branch office support for shielded VMs in Windows Server, version 1709 on our blog. Offline mode allows you to continue to start up your shielded VMs, even if HGS can't be reached, as long as the VM has started successfully once, and the host's security configuration has not changed. (To enable offline mode, run the following command on the Host Guardian Service: **Set-HgsKeyProtectionConfiguration –AllowKeyMaterialCaching**.)

We've also made it easier to troubleshoot your shielded virtual machines by enabling support for VMConnect Enhanced Session Mode and PowerShell Direct. These tools are particularly useful if you've lost network connectivity to your VM and need to update its configuration to restore access. These features do not need to be configured, and they will automatically become available when a shielded VM is placed on a Hyper-V host running build 17040 or later.

For customers who run mixed-OS environments, we now support running Ubuntu, Red Hat Enterprise Linux, and SUSE Linux Enterprise Server inside shielded virtual machines. Try it out—Create a Linux shielded VM template disk—and send us your feedback in the Feedback Hub.

Encrypted Network in SDN

Network traffic going out from a VM host can be snooped on and/or manipulated by anyone with access to the physical fabric. While shielded VMs protect VM data from theft and manipulation, similar protection is required for network traffic to and from a VM. While the tenant can setup protection such as IPSEC, this is difficult due to configuration complexity and heterogeneous environments.

Encrypted Networks is a feature which provides simple to configure DTLS-based encryption using the Network Controller to manage the end-to-end encryption and protect data as it travels through the wires and network devices between the hosts It is configured by the Administrator on a per-subnet basis. This enables the VM to VM traffic within the VM subnet to be automatically encrypted as it leaves the host and prevents snooping and manipulation of traffic on the wire. This is done without requiring any configuration changes in the VMs themselves. Try it out—Configure Encryption for a Virtual Subnet—and send us your feedback in the Feedback Hub.

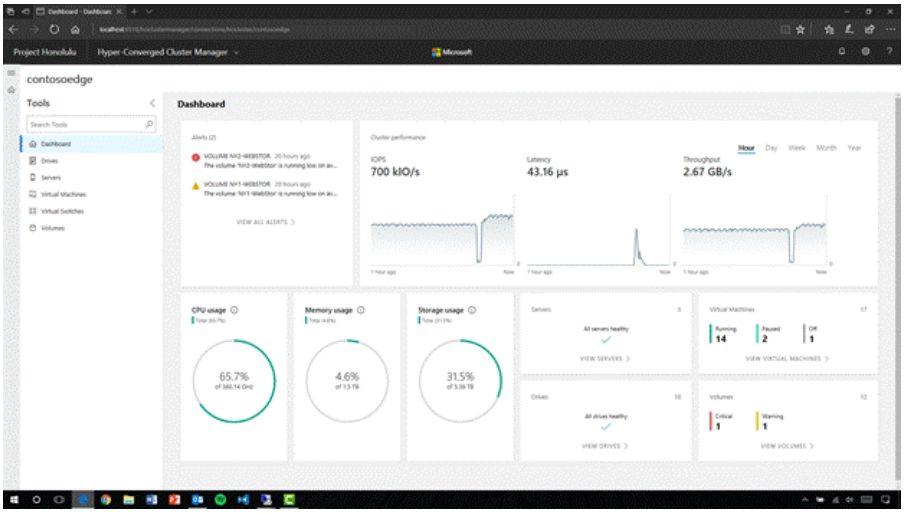
If you are using Storage Spaces Direct, take a look at another area to explore for this release: performance history for Storage Spaces Direct.

Performance history for Storage Spaces Direct

Administrators of Storage Spaces Direct can now get easy access to historical performance and capacity data from their cluster. *Did CPU usage spike last night? When did this drive become slow? Which virtual machine used the most memory last month? Is network activity trending up or down? The cluster is pushing 1,000,000 IOPS – is that my new record?* Previously, you'd need external tooling to answer these questions. No more!

Beginning in build 17090, beautiful new charts in Project Honolulu (and new PowerShell cmdlets, for those so inclined) empower you to answer these questions. There's nothing to install, configure, or start—it's built-in and always-on. Learn more at https://aka.ms/clusterperformancehistory.

Figure 1. New charts in Project Honolulu, powered by built-in cluster performance history.



Bug fixes

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

WORK ITEM	DESCRIPTION OF BUG FIX
15953324	We resolved an issue that could cause a bug check, DRIVER_VERIFIER_DMA_VIOLATION (e6), when reading from an NVM Express (NVMe) device that is connected via the PCI root port. On an affected system, this issue may occur when VT-d virtualization is enabled.
14668563	We fixed the following issue: When BitLocker is enabled and a system is started, the system prompts the user for the BitLocker PIN. Upon providing the correct PIN the first time, the system says the PIN is incorrect; however, if the user presses Enter a second time, the PIN is accepted.
15488106	We fixed the following issue: When the administrator enters the product key for Windows Server, Datacenter Edition, the administrator is not given an option to choose either Server Datacenter (Full Experience) or Server Datacenter (Core Experience).
15685027	We fixed the following issue: After installing the operating system, the system prompts the administrator to enter a password. After the password is entered, the system displays an error message: "The remote procedure call failed." However, the password is accepted as expected.
15832101	We fixed the following issue: A long-running service request in the TPM device driver (TPM.sys) causes a bug check (0x9F) in the watchdog timer for the deferred procedure call.

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
00000000	**In-place OS upgrade: Domain Controllers.** During an in-place OS upgrade, Active Directory (AD) Domain Controllers (DC) might not be upgraded correctly. So, back up any AD DCs before performing an in-place OS upgrade.
12139737	Editing or creating policies for AppLocker can cause the MMC snap-in to crash when generated rules for a packaged app.
16060707	After upgrading the operating system, the AppX database may have corrupted entries, which causes problems for components that use those entries.
13551533	Testing of the Windows core may fail because of a timeout while attempting to load the test libraries.

Breaking changes

No breaking changes are included in this build.