

Contents

[Get started with Windows Server 2019](#)

[What's new in Windows Server 2019](#)

[What's new in Windows Server, versions 1903 and 1909](#)

[Comparison of servicing channels](#)

[Install | Upgrade | Migrate](#)

[Release notes: Important issues in Windows Server 2019](#)

[System requirements](#)

[Windows Server 2019 activation](#)

[Windows Server 2019 VM activation](#)

[Troubleshooting Windows volume activation](#)

[Windows Server 2019 and Microsoft Server Application Compatibility](#)

[Server Core App Compatibility Feature on Demand \(FOD\)](#)

[Standard | Datacenter Editions comparison](#)

[Removed features](#)

[Features removed or planned for replacement in Windows Server](#)

[Features removed or planned for replacement starting in Windows Server 2019](#)

[Features removed or planned for replacement starting in Windows Server, version 1903](#)

[Windows Server release information](#)

[Windows Server license terms](#)

Get started with Windows Server 2019

4/7/2020 • 2 minutes to read • [Edit Online](#)

Applies to: Windows Server 2019

This collection contains detailed information to help you determine if you're ready to move to Windows Server 2019. Once you've checked the system requirements, upgrade options, and other information about moving to Windows Server 2019, you're ready to start down the path of installing the best edition and installation option for your needs. To download Windows Server 2019, see [Windows Server Evaluations](#).

If you're looking for info about Windows Server 2016, see [Get started with Windows Server 2016](#). For even earlier versions, see our [Windows previous versions library](#).

What's new?

Find out what's new in Windows Server 2019.

Servicing channels Better plan your deployment and patching schedules by understanding the difference between our Long Term Servicing Channel (LTSC) and Semi-Annual Channel (SAC) releases.	Install, Upgrade , Migrate You can move to Windows Server 2019 a number of ways. Whether you are newly installing, upgrading in-place, or migrating applications and Server Roles, discover the best approach here.	Release notes Issues that could cause serious problems if you don't avoid or work around them.
System requirements The minimum hardware requirements to install and run Windows Server 2019.	Activation Basic information on activation of Windows Server 2019 itself, and other operating systems, by using Windows Server 2019.	Application Compatibility Need to get SQL working on Windows Server 2019 or find steps to get Exchange running? This topic links to documentation for compatible Microsoft applications.
Features on Demand Features on Demand (FODs) are Windows Server feature packages that can be added at any time.	Standard / Datacenter Editions comparison Windows Server Standard and Datacenter Editions have different capabilities. Find out which one you need.	

What's new in Windows Server 2019

4/3/2020 • 9 minutes to read • [Edit Online](#)

Applies to: Windows Server 2019

This topic describes some of the new features in Windows Server 2019. Windows Server 2019 is built on the strong foundation of Windows Server 2016 and brings numerous innovations on four key themes: Hybrid Cloud, Security, Application Platform, and Hyper-Converged Infrastructure (HCI).

To find out what's new in Windows Server Semi-Annual Channel releases, see [What's New in Windows Server](#).

General

Windows Admin Center

Windows Admin Center is a locally deployed, browser-based app for managing servers, clusters, hyper-converged infrastructure, and Windows 10 PCs. It comes at no additional cost beyond Windows and is ready to use in production.

You can install Windows Admin Center on Windows Server 2019 as well as Windows 10 and earlier versions of Windows and Windows Server, and use it to manage servers and clusters running Windows Server 2008 R2 and later.

For more info, see [Windows Admin Center](#).

Desktop experience

Because Windows Server 2019 is a Long-Term Servicing Channel (LTSC) release, it includes the **Desktop Experience**. (Semi-Annual Channel (SAC) releases don't include the Desktop Experience by design; they are strictly Server Core and Nano Server container image releases.) As with Windows Server 2016, during setup of the operating system you can choose between Server Core installations or Server with Desktop Experience installations.

System Insights

System Insights is a new feature available in Windows Server 2019 that brings local predictive analytics capabilities natively to Windows Server. These predictive capabilities, each backed by a machine-learning model, locally analyze Windows Server system data, such as performance counters and events, providing insight into the functioning of your servers and helping you reduce the operational expenses associated with reactively managing issues in your Windows Server deployments.

Hybrid Cloud

Server Core app compatibility feature on demand

The [Server Core App Compatibility feature on demand \(FOD\)](#) significantly improves the app compatibility of the Windows Server Core installation option by including a subset of binaries and components from Windows Server with the Desktop Experience, without adding the Windows Server Desktop Experience graphical environment itself. This is done to increase the functionality and compatibility of Server Core while keeping it as lean as possible.

This optional feature on demand is available on a separate ISO and can be added to Windows Server Core installations and images only, using DISM.

Security

Windows Defender Advanced Threat Protection (ATP)

ATP's deep platform sensors and response actions expose memory and kernel level attacks and respond by suppressing malicious files and terminating malicious processes.

- For more information about Windows Defender ATP, see [Overview of Windows Defender ATP capabilities](#).
- For more information on onboarding servers, see [Onboard servers to Windows Defender ATP service](#).

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 you to balance security risk and productivity requirements.

- **Attack Surface Reduction(ASR)** is 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** is a set of mitigations for vulnerability exploits (replacing EMET)that can be easily configured to protect your system and applications.

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 have built default CI policies, which allows all Windows in-box files and Microsoft applications, such as SQL Server, and block known executables that can bypass CI.

Security with Software Defined Networking (SDN)

Security with SDN delivers many features to increase customer confidence in running workloads, either on-premises, or as a service provider in the cloud.

These security enhancements are integrated into the comprehensive SDN platform introduced in Windows Server 2016.

For a complete list of what's new in SDN see, [What's New in SDN for Windows Server 2019](#).

Shielded Virtual Machines improvements

• Branch office improvements

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.

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.

• Troubleshooting improvements

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 become available automatically when a shielded VM is placed on a Hyper-V host running Windows Server version 1803 or later.

- **Linux support**

If you run mixed-OS environments, Windows Server 2019 now supports running Ubuntu, Red Hat Enterprise Linux, and SUSE Linux Enterprise Server inside shielded virtual machines.

HTTP/2 for a faster and safer Web

- Improved coalescing of connections to deliver an uninterrupted and properly encrypted browsing experience.
- Upgraded HTTP/2's server-side cipher suite negotiation for automatic mitigation of connection failures and ease of deployment.
- Changed our default TCP congestion provider to Cubic to give you more throughput!

Storage

Here are some of the changes we've made to storage in Windows Server 2019. For details, see [What's new in Storage](#).

Storage Migration Service

Storage Migration Service is a new technology that makes it easier to migrate servers to a newer version of Windows Server. It provides a graphical tool that inventories data on servers, transfers the data and configuration to newer servers, and then optionally moves the identities of the old servers to the new servers so that apps and users don't have to change anything. For more info, see [Storage Migration Service](#).

Storage Spaces Direct

Here's a list of what's new in Storage Spaces Direct. For details, see [What's new in Storage Spaces Direct](#). Also see [Azure Stack HCI](#) for info on acquiring validated Storage Spaces Direct systems.

- **Deduplication and compression for ReFS volumes**
- **Native support for persistent memory**
- **Nested resiliency for two-node hyper-converged infrastructure at the edge**
- **Two-server clusters using a USB flash drive as a witness**
- **Windows Admin Center support**
- **Performance history**
- **Scale up to 4 PB per cluster**
- **Mirror-accelerated parity is 2X faster**
- **Drive latency outlier detection**
- **Manually delimit the allocation of volumes to increase fault tolerance**

Storage Replica

Here's what's new in Storage Replica. For details, see [What's new in Storage Replica](#).

- Storage Replica is now available in Windows Server 2019 Standard Edition.
- Test failover is a new feature that allows mounting of destination storage to validate replication or backup data. For more information, see [Frequently Asked Questions about Storage Replica](#).
- Storage Replica log performance improvements
- Windows Admin Center support

Failover Clustering

Here's a list of what's new in Failover Clustering. For details, see [What's new in Failover Clustering](#).

- **Cluster sets**

- Azure-aware clusters
- Cross-domain cluster migration
- USB witness
- Cluster infrastructure improvements
- Cluster Aware Updating supports Storage Spaces Direct
- File share witness enhancements
- Cluster hardening
- Failover Cluster no longer uses NTLM authentication

Application Platform

Linux containers on Windows

It is now possible to run Windows and Linux-based containers on the same container host, using the same docker daemon. This enables you to have a heterogeneous container host environment while providing flexibility to application developers.

Built-in Support for Kubernetes

Windows Server 2019 continues the improvements to compute, networking and storage from the semi-annual channel releases needed to support Kubernetes on Windows. More details are available in upcoming Kubernetes releases.

- [Container Networking](#) in Windows Server 2019 greatly improves usability of Kubernetes on Windows by enhancing platform networking resiliency and support of container networking plugins.
- Deployed workloads on Kubernetes are able to use network security to protect both Linux and Windows services using embedded tooling.

Container improvements

- **Improved integrated identity**

We've made integrated Windows authentication in containers easier and more reliable, addressing several limitations from prior versions of Windows Server.

- **Better application compatibility**

Containerizing Windows-based applications just got easier: The app compatibility for the existing *windowsservercore* image has been increased. For applications with additional API dependencies, there is now a third base image: *windows*.

- **Reduced size and higher performance**

The base container image download sizes, size on disk and startup times have been improved. This speeds up container workflows

- **Management experience using Windows Admin Center (preview)**

We've made it easier than ever to see which containers are running on your computer and manage individual containers with a new extension for Windows Admin Center. Look for the "Containers" extension in the [Windows Admin Center public feed](#).

Encrypted Networks

[Encrypted Networks](#) - Virtual network encryption allows encryption of virtual network traffic between virtual machines that communicate with each other within subnets marked as **Encryption Enabled**. It also utilizes Datagram Transport Layer Security (DTLS) on the virtual subnet to encrypt packets. DTLS protects against eavesdropping, tampering, and forgery by anyone with access to the physical network.

Network performance improvements for virtual workloads

[Network performance improvements for virtual workloads](#) maximizes the network throughput to virtual machines without requiring you to constantly tune or over-provision your host. This lowers the operations and maintenance cost while increasing the available density of your hosts. These new features are:

- Receive Segment Coalescing in the vSwitch
- Dynamic Virtual Machine Multi-Queue (d.VMMQ)

Low Extra Delay Background Transport

Low Extra Delay Background Transport (LEDBAT) is a latency optimized, network congestion control provider designed to automatically yield bandwidth to users and applications, while consuming the entire bandwidth available when the network is not in use.

This technology is intended for use in deploying large, critical updates across an IT environment without impacting customer facing services and associated bandwidth.

Windows Time Service

The [Windows Time Service](#) includes true UTC-compliant leap second support, a new time protocol called Precision Time Protocol, and end-to-end traceability.

High performance SDN gateways

[High performance SDN gateways](#) in Windows Server 2019 greatly improves the performance for IPsec and GRE connections, providing ultra-high-performance throughput with much less CPU utilization.

New Deployment UI and Windows Admin Center extension for SDN

Now, with Windows Server 2019, it's easy to deploy and manage through a new deployment UI and Windows Admin Center extension that enable anyone to harness the power of SDN.

Persistent Memory support for Hyper-V VMs

To leverage the high throughput and low latency of persistent memory (a.k.a. storage class memory) in virtual machines, it can now be projected directly into VMs. This can help to drastically reduce database transaction latency or reduce recovery times for low latency in-memory databases on failure.

What's new in Windows Server, versions 1903 and 1909

1/30/2020 • 6 minutes to read • [Edit Online](#)

Applies to: Windows Server (Semi-Annual Channel)

This topic describes some of the new features in Windows Server, version 1903 which is a Semi-Annual Channel release. These features include enhancements for running and managing containers, tools for working in Server Core installations, and the ability to migrate storage from Linux devices.

Windows Server, version 1909 is the next Semi-Annual Channel release of Windows Server, focused on reliability, performance, and other general improvements, but no new features. Like other Semi-Annual Channel releases, it's supported for 18 months from its first availability. For more info on the support dates of Semi-Annual Channel releases, see [Windows Server release info](#).

To instead find out what's new in other releases of Windows Server, see [What's New in Windows Server](#). Also see [What's new in Windows 10, version 1903 IT Pro content](#).

The system requirements for this release are the same as for Windows Server 2019—see [System requirements](#) for more info. To see what's been removed recently, see [Features Removed or Planned for Replacement starting with Windows Server, version 1903](#)

NOTE

Windows containers must use the same version of Windows as the host server, or an *earlier* version. For example, a host server running the released version of Windows Server, version 1903 (build 18342) can run Windows Server containers with the same or earlier version and build number (even if the container uses an Insider Preview version of Windows). For more info, see [Windows container version compatibility](#).

Enhanced support for non-Microsoft container services

We enhanced platform capabilities to support Azure container services and non-Microsoft container services.

- We integrated CRI-containerd with Host Compute Service (HCS) to support pods of Windows containers and Linux containers on Windows (LCOW) on Azure.
- We worked with the Kubernetes community to enable Windows container support. With the release of Kubernetes v1.14, Windows Server node support officially graduated from beta to stable. For more info, see [Windows containers now supported in Kubernetes](#).
- Tigera Calico for Windows is now generally available as part of Tigera Essentials subscription and offers both non-overlay networking and network policy interoperable across mixed Linux/Windows environments.
- We delivered scalability improvements enhancing overlay networking support for Windows containers, including integration with Kubernetes through the latest release of Flannel and Kubernetes v1.14. For more info, see [Intro to Windows support in Kubernetes](#).

DirectX hardware acceleration in containers

We're enabling support for hardware acceleration of DirectX APIs in Windows containers to support scenarios such as Machine Learning (ML) inferencing using local graphical processing unit (GPU) hardware. For more info, see [Bringing GPU acceleration to Windows containers](#).

Updated container identity and group managed service account documentation

We added more examples and compatibility info to the [Group Managed Service Accounts](#) documentation, and made the [Credential Spec PowerShell module](#) available in the PowerShell Gallery. For more info, see the [What's new for container identity](#) blog post.

Add Task Scheduler and Hyper-V Manager to Server Core installations

As you might know, we recommend using the Server Core installation option when using Windows Server, Semi-Annual Channel in production. However, Server Core by default omits a number of useful management tools. You can add many of the most commonly used tools by installing the App Compatibility feature, but there have still been some missing tools.

So, based on customer feedback, we added two more tools to the App Compatibility feature in this version: Task Scheduler (taskschd.msc) and Hyper-V Manager (virtmgmt.msc).

For more info, see [Server Core app compatibility feature](#).

Storage Migration Service now migrates local accounts, clusters, and Linux servers

Storage Migration Service makes it easier to migrate servers to a newer version of Windows Server. It provides a graphical tool that inventories data on servers and then transfers the data and configuration to newer servers—all without apps or users having to change anything.

When using this version of Windows Server to orchestrate migrations, we've added the following abilities:

- Migrate local users and groups to the new server
- Migrate storage from failover clusters
- Migrate storage from a Linux server that uses Samba
- More easily sync migrated shares into Azure by using Azure File Sync
- Migrate to new networks such as Azure

For more info about Storage Migration Service, see [Storage Migration Service overview](#).

System Insights disk anomaly detection

[System Insights](#) is a predictive analytics feature that locally analyzes Windows Server system data and provides insight into the functioning of the server. It comes with a number of built-in capabilities, but we've added the ability to install additional capabilities via Windows Admin Center, starting with disk anomaly detection.

Disk anomaly detection is a new capability that highlights when disks are behaving *differently* than usual. While different isn't necessarily a bad thing, seeing these anomalous moments can be helpful when troubleshooting issues on your systems.

This capability is also available for servers running Windows Server 2019.

Windows Admin Center enhancements

A new release of Windows Admin Center is out, adding new functionality to Windows Server. For info on the latest features, see [Windows Admin Center](#).

Security baseline for Windows 10 and Windows Server

The draft release of the [security configuration baseline settings](#) for Windows 10 version 1903, and for Windows Server version 1903 is available.

SetupDiag

[SetupDiag](#) version 1.4.1 is available.

SetupDiag is a command-line tool that can help diagnose why a Windows update failed. SetupDiag works by searching Windows Setup log files. When searching log files, SetupDiag uses a set of rules to match known issues. In the current version of SetupDiag there are 53 rules contained in the rules.xml file, which is extracted when SetupDiag is run. The rules.xml file will be updated as new versions of SetupDiag are made available.

Update rollback improvements

Servers can now automatically recover from startup failures by removing updates if the startup failure was introduced after the installation of recent driver or quality updates. When a device is unable to start up properly after the recent installation of Quality of driver updates, Windows will now automatically uninstall the updates to get the device back up and running normally.

This functionality requires the server to be using the Server Core installation option with a [Windows Recovery Environment](#) partition.

Microsoft Defender Advanced Threat Protection (ATP) improvements

Windows Server includes Microsoft Defender Advanced Threat Protection (for more info, see [Windows Defender Antivirus on Windows Server](#)). This release includes the following improvements:

- [Attack surface area reduction](#) – IT admins can configure devices with advanced web protection that enables them to define allow and deny lists for specific URL's and IP addresses.
- [Next generation protection](#) – Controls have been extended to protection from ransomware, credential misuse, and attacks that are transmitted through removable storage.
 - Integrity enforcement capabilities – Enable remote runtime attestation.
 - Tamper-proofing capabilities – Uses virtualization-based security to isolate critical ATP security capabilities away from the OS and attackers.
- Microsoft Defender ATP next-gen protection technologies:
 - **Advanced machine learning**: Improved with advanced machine learning and AI models that enable it to protect against apex attackers using innovative vulnerability exploit techniques, tools and malware.
 - **Emergency outbreak protection**: Provides emergency outbreak protection which will automatically update devices with new intelligence when a new outbreak has been detected.
 - **Certified ISO 27001 compliance**: Ensures that the cloud service has analyzed for threats, vulnerabilities and impacts, and that risk management and security controls are in place.
 - **Geolocation support**: Support geolocation and sovereignty of sample data as well as configurable retention policies.

Windows Server servicing channels: LTSC and SAC

6/30/2020 • 10 minutes to read • [Edit Online](#)

Applies to: Windows Server 2019, Windows Server 2016, Windows Server (Semi-Annual Channel)

There are two primary release channels available to Windows Server customers, the Long-Term Servicing Channel and the Semi-Annual Channel.

You can keep servers on the Long-Term Servicing Channel (LTSC), move them to the Semi-Annual Channel, or have some servers on either track, depending on what works best for your needs.

Long-Term Servicing Channel (LTSC)

This is the release model you're already familiar with (formerly called the "Long-Term Servicing *Branch*") where a new major version of Windows Server is released every 2-3 years. Users are entitled to 5 years of mainstream support and 5 years of extended support. This channel is appropriate for systems that require a longer servicing option and functional stability. Deployments of Windows Server 2019 and earlier versions of Windows Server will not be affected by the new Semi-Annual Channel releases. The Long-Term Servicing Channel will continue to receive security and non-security updates, but it will not receive the new features and functionality.

NOTE

The current LTSC product is **Windows Server 2019**. If you want to stay in this channel, you should install (or continue using) Windows Server 2019, which can be installed in Server Core installation option or Server with Desktop Experience installation option.

Semi-Annual Channel

The Semi-Annual Channel is perfect for customers who are innovating quickly to take advantage of new operating system capabilities at a faster pace, focused in on containers and microservices. Windows Server products in the Semi-Annual Channel will have new releases available twice a year, in spring and fall. Each release in this channel will be supported for 18 months from the initial release.

Most of the features introduced in the Semi-Annual Channel will be rolled up into the next Long-Term Servicing Channel release of Windows Server. The editions, functionality, and supporting content might vary from release to release depending on customer feedback.

The Semi-Annual Channel is available to volume-licensed customers with [Software Assurance](#), as well as via the Azure Marketplace or other cloud/hosting service providers and loyalty programs such as Visual Studio Subscriptions.

NOTE

The current Semi-Annual Channel release is **Windows Server, version 1909**. If you want to put servers in this channel, you should install Windows Server, version 1909, which can be installed in Server Core mode or as Nano Server run in a container. In-place upgrades from a long-term servicing channel release aren't supported because they are in **different release channels**. Semi-Annual Channel releases aren't updates – it's the next Windows Server release in the Semi-Annual Channel.

In this model, Windows Server releases are identified by the year and month of release: for example, in 2017, a

release in the 9th month (September) would be identified as **version 1709**. Fresh releases of Windows Server in the Semi-Annual Channel will occur twice each year. The support lifecycle for each release is 18 months.

Should you keep servers on the LTSC or move them to the Semi-Annual Channel?

These are the key differences to take into account:

- Do you need to step up on new technology on Devops, Containers and Microservices? If so, you should consider **joining the Semi-Annual Channel** by installing **Windows Server, version 1909**. As described in this topic, you will receive new versions twice a year, with 18 months of mainstream production support per release. You get it through volume licensing, Azure, or Visual Studio Subscription Services. Currently, releases in the Semi-Annual Channel require volume licensing and Software Assurance if you intend to run the product in production.
- Do you need stability and predictability? Do you need to run virtual machines and traditional workloads on physical servers? If so, you should consider **keeping those servers on the Long-Term Servicing Channel**. The current LTSC release is **Windows Server 2019**. As described in this topic, you'll have access to new versions every 2-3 years, with 5 years of mainstream support followed by 5 years of extended support per release. LTSC releases are available through all release mechanisms. Releases in the LTSC are available to anyone regardless of the licensing model they are using.

The following table summarizes the key differences between the channels:

	LONG-TERM SERVICING CHANNEL (WINDOWS SERVER 2019)	SEMI-ANNUAL CHANNEL (WINDOWS SERVER)
Recommended scenarios	General purpose file servers, Microsoft and non-Microsoft workloads, traditional apps, infrastructure roles, software-defined Datacenter, and hyper-converged infrastructure	Containerized applications, container hosts, and application scenarios benefiting from faster innovation
New releases	Every 2–3 years	Every 6 months
Support	5 years of mainstream support, plus 5 years of extended support	18 months
Editions	All available Windows Server editions	Standard and Datacenter editions
Who can use	All customers through all channels	Software Assurance and cloud customers only
Installation options	Server Core and Server with Desktop Experience	Server Core for container host and image and Nano Server container image

Device compatibility

Unless otherwise communicated, the minimum hardware requirements to run the Semi-Annual Channel releases will be the same as the most recent Long-Term Servicing Channel release of Windows Server. For example, **the current Long-Term Servicing Channel release is Windows Server 2019**. Most hardware drivers will continue to function in these releases.

Servicing

Both the Long-Term Servicing Channel and the Semi-Annual Channel releases will be supported with security updates and non-security updates. The difference is the length of time that the release is supported, as described above.

Servicing tools

There are many tools with which IT pros can service Windows Server. Each option has its pros and cons, ranging from capabilities and control to simplicity and low administrative requirements. The following are examples of the servicing tools available to manage servicing updates:

- **Windows Update (stand-alone):** This option is only available for servers that are connected to the Internet and have Windows Update enabled.
- **Windows Server Update Services (WSUS)** provides extensive control over Windows 10 and Windows Server updates and is natively available in the Windows Server operating system. In addition to the ability to defer updates, organizations can add an approval layer for updates and choose to deploy them to specific computers or groups of computers whenever ready.
- **Microsoft Endpoint Configuration Manager** provides the greatest control over servicing. IT pros can defer updates, approve them, and have multiple options for targeting deployments and managing bandwidth usage and deployment times.

You've likely already chosen to use at least one of these options based on your resources, staff, and expertise. You can continue using the same process for Semi-Annual Channel Releases: for example, if you already use Configuration Manager to manage updates, you can continue to use it. Similarly, if you are using WSUS, you can continue to use that.

Where to obtain Semi-Annual Channel releases

Semi-Annual Channel releases should be installed as a clean installation.

- Volume Licensing Service Center (VLSC): Volume-licensed customers with [Software Assurance](#) can obtain this release by going to the [Volume Licensing Service Center](#) and clicking **Sign In**. Then click **Downloads and Keys** and search for this release.
- Semi-Annual Channel releases are also available in [Microsoft Azure](#).
- Visual Studio Subscriptions: Visual Studio Subscribers can obtain Semi-Annual Channel releases by downloading them from the [Visual Studio Subscriber download page](#). If you are not already a subscriber, go to [Visual Studio Subscriptions](#) to sign up, and then visit the [Visual Studio Subscriber download page](#) as above. Releases obtained through Visual Studio Subscriptions are for development and testing only.
- Obtain preview releases through the Windows Insider Program: Testing the early builds of Windows Server helps both Microsoft and its customers because of the opportunity to discover possible issues before release. It also gives customers a unique opportunity to directly influence the functionality in the product. Microsoft depends on receiving feedback throughout the development process so that adjustments may be made as quickly as possible. Early testing and feedback is essential to the rapid release model. To get involved with the Windows Insider Program, see the [Windows Insider Program for Server docs](#).

Activating Semi-Annual Channel releases

- If you're using Microsoft Azure, this release should automatically be activated.
- If you've obtained this release from the Volume Licensing Service Center or Visual Studio Subscriptions, you can activate it by using your Windows Server 2019 CSVLK with your Key Management System (KMS) environment. For more info, see [KMS client setup keys](#).

Semi-Annual Channel releases that were released before Windows Server 2019 use the Windows Server 2016 CSVLK.

Why do Semi-Annual Channel releases offer only the Server Core installation option?

One of the most important steps we take in planning each release of Windows Server is listening to customer feedback – how are you using Windows Server? What new features will have the greatest impact on your Windows Server deployments, and by extension, your day-to-day business? Your feedback tells us that delivering new innovation as quickly and efficiently as possible is a key priority. At the same time, for those customers innovating most quickly, you've told us that you're primarily using command line scripting with PowerShell to manage your datacenters, and as such don't have a strong need for the desktop GUI available in the installation of Windows Server with Desktop Experience, especially now that [Windows Admin Center](#) is available to remotely manage your servers.

By focusing on the Server Core installation option, we're able to dedicate more resources toward those new innovations, while also maintaining traditional Windows Server platform functionality and application compatibility. If you have feedback about this or other issues concerning Windows Server and our future releases, you can make suggestions and comments through the [Feedback Hub](#).

What about Nano Server?

Nano Server is available as a container operating system in the Semi-Annual Channel. See [Changes to Nano Server in Windows Server Semi-Annual Channel](#) for details.

How to tell whether a server is running an LTSC or SAC release

Generally speaking, Long-Term Servicing Channel releases such as Windows Server 2019 are released at the same time as a new version of the Semi-Annual Channel, for example, Windows Server, version 1809. This can make it a little tricky to determine whether a server is running Semi-Annual Channel release. Instead of looking at the build number, you must look at the product name: Semi-Annual Channel releases use the Windows Server Standard or Windows Server Datacenter product name, without a version number, while Long-Term Servicing Channel releases include the version number, for example, Windows Server 2019 Datacenter.

NOTE

The below guidance is intended to help identify and differentiate between LTSC and SAC for lifecycle and general inventory purposes only. It is not intended for application compatibility or to represent a specific API surface. App developers should use guidance elsewhere to properly ensure compatibility as components, APIs, and functionality can be added over the life of a system, or not yet be added. [Operating System Version](#) is a better starting point for App Developers.

Open Powershell and use the `Get-ItemProperty` Cmdlet, or the `Get-ComputerInfo` Cmdlet, to check these properties in the registry. Along with build number, this will indicate LTSC or SAC by the presence, or lack thereof, of the branded year, i.e. 2019. LTSC has this, SAC does not. This will also return the timing of the release with `ReleaseId` or `WindowsVersion`, i.e. 1809, as well as whether the installation is Server Core or Server with Desktop Experience.

Windows Server 2019 Datacenter Edition (LTSC) with Desktop Experience example:

```
Get-ItemProperty -Path "HKLM:\Software\Microsoft\Windows NT\CurrentVersion" | Select ProductName, ReleaseId, InstallationType, CurrentMajorVersionNumber, CurrentMinorVersionNumber, CurrentBuild
```

```
ProductName      : Windows Server 2019 Datacenter
ReleaseId       : 1809
InstallationType : Server
CurrentMajorVersionNumber : 10
CurrentMinorVersionNumber : 0
CurrentBuild    : 17763
```

Windows Server, version 1809 (SAC) Standard Edition Server Core example:

```
Get-ItemProperty -Path "HKLM:\Software\Microsoft\Windows NT\CurrentVersion" | Select ProductName, ReleaseId,
InstallationType, CurrentMajorVersionNumber,CurrentMinorVersionNumber,CurrentBuild
```

```
ProductName      : Windows Server Standard
ReleaseId       : 1809
InstallationType : Server Core
CurrentMajorVersionNumber : 10
CurrentMinorVersionNumber : 0
CurrentBuild    : 17763
```

Windows Server 2019 Standard Edition (LTSC) Server Core example:

```
Get-ComputerInfo | Select WindowsProductName, WindowsVersion, WindowsInstallationType, OsServerLevel,
OsVersion, OsHardwareAbstractionLayer
```

```
WindowsProductName      : Windows Server 2019 Standard
WindowsVersion         : 1809
WindowsInstallationType : Server Core
OsServerLevel          : ServerCore
OsVersion              : 10.0.17763
OsHardwareAbstractionLayer : 10.0.17763.107
```

To query if the new [Server Core App Compatibility FOD](#) is present on a server, use [Get-WindowsCapability](#) Cmdlet and look for:

```
Name      : ServerCore.AppCompatibility~~~~0.0.1.0
State     : Installed
```

Additional References

[Changes to Nano Server in Windows Server Semi-Annual Channel](#)

[Windows Server support lifecycle](#)

[Determining whether Server Core is running](#)

[GetProductInfo function](#)

[Software Inventory Logging Cmdlets](#)

Install, upgrade, or migrate to Windows Server

4/7/2020 • 2 minutes to read • [Edit Online](#)

Applies to: Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008

IMPORTANT

Extended support for Windows Server 2008 R2 and Windows Server 2008 ends in January 2020. [Learn about your upgrade options](#). To download Windows Server 2019, see [Windows Server Evaluations](#).

Is it time to move to a newer version of Windows Server? Depending on what you're running now, you have lots of options to get there.

Clean install

The simplest way to install Windows Server is to perform a clean installation, where you install on a blank server or overwrite an existing operating system. That is the simplest way, but you will need to back up your data first and plan to reinstall your applications. There are a few things to be aware of, such as system requirements, so be sure to check the details for [Windows Server 2019](#), [Windows Server 2016](#), [Windows Server 2012 R2](#), and [Windows Server 2012](#).

In-place upgrade

If you want to keep the same hardware and all the server roles you have set up without flattening the server, you'll want to do an **In-place Upgrade**, by which you go from an older operating system to a newer one, keeping your settings, server roles, and data intact. For example, if your server is running Windows Server 2012 R2, you can upgrade it to Windows Server 2016 or Windows Server 2019. However, not every older operating system has a pathway to every newer one.

For step-by-step guidance on upgrading, review the [Windows Server upgrade content](#).

Cluster OS rolling upgrade

Cluster OS Rolling Upgrade enables an administrator to upgrade the operating system of the cluster nodes from Windows Server 2012 R2 and Windows Server 2016 without stopping the Hyper-V or the Scale-Out File Server workloads. This feature allows you to avoid downtime which could impact Service Level Agreements. This new feature is discussed in more detail at [Cluster operating system rolling upgrade](#).

Migration

Windows Server migration is when you move one role or feature at a time from a source computer that is running Windows Server to another destination computer that is running Windows Server, either the same or a newer version. For these purposes, migration is defined as moving one role or feature and its data to a different computer, not upgrading the feature on the same computer.

License conversion

In some operating system releases, you can convert a particular edition of the release to another edition of the

same release in a single step with a simple command and the appropriate license key. This is called **license conversion**. For example, if your server is running Windows Server 2016 Standard, you can convert it to Windows Server 2016 Datacenter. Keep in mind that while you can move up from Server 2016 Standard to Server 2016 Datacenter, you are unable to reverse the process and go from Datacenter to Standard. In some releases of Windows Server, you can also freely convert among OEM, volume-licensed, and retail versions with the same command and the appropriate key.

Release Notes - Important issues in Windows Server 2019

4/7/2020 • 2 minutes to read • [Edit Online](#)

Applies To: Windows Server 2019

These release notes summarize the most critical issues in the Windows Server 2019 operating system, including ways to avoid or work around the issues, if known. For information about by-design changes, new features, and fixes in this release, see [What's New in Windows Server 2019](#) and announcements from the specific feature teams. Unless otherwise specified, each reported issue applies to all editions and installation options of Windows Server 2019.

This document is continuously updated. As critical issues requiring a workaround are discovered, they are added, as are new workarounds and fixes as they become available.

Release Notes

The following known issues are present in Windows Server 2019.

TITLE	DESCRIPTION
Installation option menu during server setup has truncated German text	<p>When running setup from German server media, on the operating system selection window titled, "Select the operating system you want to install," the description for Desktop Experience installation options will have missing and incorrect characters at the very end of the sentence. Here is the full German text as it should appear:</p> <div data-bbox="821 1294 1433 1444" style="border: 1px solid #ccc; padding: 5px;"><p>Durch diese Option wird die vollständige grafische Umgebung von Windows installiert, wodurch zusätzlicher Speicherplatz verbraucht wird. Sie kann hilfreich sein, wenn Sie den Windows-Desktop verwenden möchten oder über eine App verfügen, die die grafische Umgebung benötigt.</p></div> <p>This only impacts the German media released at Public Availability of Windows Server 2019, Windows Server, version 1809, and Microsoft Hyper-V Server 2019.</p>
Windows Server branding image incorrect during setup of Windows Server, version 1809	<p>During the setup experience for Windows Server, version 1809, the background image on some initial screens shows "Windows Server 2019". As with Windows Server, versions 1709 and 1803, this should simply say "Windows Server". There are no other impacts anywhere else in the product, and there is no impact to the Windows Server 2019 product. The issue is limited to this one image during setup of Windows Server, version 1809, available only to volume license customers accessing the Volume License Service Center.</p>

Copyright

This document is provided as-is. Information and views expressed in this document, including URL and other Internet Web site references, may change without notice.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You

may copy and use this document for your internal, reference purposes.

© 2019 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, Hyper-V, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

This product contains graphics filter software; this software is based in part on the work of the Independent JPEG Group.

1.0

System Requirements

4/7/2020 • 4 minutes to read • [Edit Online](#)

Applies to: Windows Server 2019

This topic outlines the minimum system requirements to run Windows Server® 2019.

Review system requirements

The following are estimated system requirements Windows Server 2019. If your computer has less than the minimum requirements, you will not be able to install this product correctly. Actual requirements will vary based on your system configuration and the applications and features you install.

Unless otherwise specified, these minimum system requirements apply to all installation options (Server Core, Server with Desktop Experience, and Nano Server) and both Standard and Datacenter editions.

IMPORTANT

The highly diverse scope of potential deployments makes it unrealistic to state recommended system requirements that would be generally applicable. Consult documentation for each of the server roles you intend to deploy for more details about the resource needs of particular server roles. For the best results, conduct test deployments to determine appropriate system requirements for your particular deployment scenarios.

Processor

Processor performance depends not only on the clock frequency of the processor, but also on the number of processor cores and the size of the processor cache. The following are the processor requirements for this product:

Minimum:

- 1.4 GHz 64-bit processor
- Compatible with x64 instruction set
- Supports NX and DEP
- Supports CMPXCHG16b, LAHF/SAHF, and PrefetchW
- Supports Second Level Address Translation (EPT or NPT)

[Coreinfo](#) is a tool you can use to confirm which of these capabilities your CPU has.

RAM

The following are the estimated RAM requirements for this product:

Minimum:

- 512 MB (2 GB for Server with Desktop Experience installation option)
- ECC (Error Correcting Code) type or similar technology, for physical host deployments

IMPORTANT

If you create a virtual machine with the minimum supported hardware parameters (1 processor core and 512 MB RAM) and then attempt to install this release on the virtual machine, Setup will fail.

To avoid this, do one of the following:

- Allocate more than 800 MB RAM to the virtual machine you intend to install this release on. Once Setup has completed, you can change the allocation to as little as 512 MB RAM, depending on the actual server configuration. If you've modified the boot image for Setup with additional languages and updates, you may need to allocate more than 800 MB RAM in order to complete the installation
- Interrupt the boot process of this release on the virtual machine with SHIFT+F10. In the command prompt that opens, use Diskpart.exe to create and format an installation partition. Run `Wpeutil createpagefile /path=C:\pf.sys` (assuming the installation partition you created was C:). Close the command prompt and proceed with Setup.

Storage controller and disk space requirements

Computers that run Windows Server 2019 must include a storage adapter that is compliant with the PCI Express architecture specification. Persistent storage devices on servers classified as hard disk drives must not be PATA. Windows Server 2019 does not allow ATA/PATA/IDE/EIDE for boot, page, or data drives.

The following are the estimated **minimum** disk space requirements for the system partition.

Minimum: 32 GB

NOTE

Be aware that 32 GB should be considered an *absolute minimum* value for successful installation. This minimum should allow you to install Windows Server 2019 in Server Core mode, with the Web Services (IIS) server role. A server in Server Core mode is about 4 GB smaller than the same server in Server with a GUI mode.

The system partition will need extra space for any of the following circumstances:

- If you install the system over a network.
- Computers with more than 16 GB of RAM will require more disk space for paging, hibernation, and dump files.

Network adapter requirements

Network adapters used with this release should include these features:

Minimum:

- An Ethernet adapter capable of at least gigabit throughput
- Compliant with the PCI Express architecture specification.

A network adapter that supports network debugging (KDNet) is useful, but not a minimum requirement.

A network adapter that supports the Pre-boot Execution Environment (PXE) is useful, but not a minimum requirement.

Other requirements

Computers running this release also must have the following:

- DVD drive (if you intend to install the operating system from DVD media)

The following items are not strictly required, but are necessary for certain features:

- UEFI 2.3.1c-based system and firmware that supports secure boot
- Trusted Platform Module
- Graphics device and monitor capable of Super VGA (1024 x 768) or higher-resolution
- Keyboard and Microsoft® mouse (or other compatible pointing device)
- Internet access (fees may apply)

NOTE

A Trusted Platform Module (TPM) chip is not strictly required to install this release, though it is necessary in order to use certain features such as BitLocker Drive Encryption. If your computer uses TPM, it must meet these requirements:

- Hardware-based TPMs must implement version 2.0 of the TPM specification.
- TPMs that implement version 2.0 must have an EK certificate that is either pre-provisioned to the TPM by the hardware vendor or be capable of being retrieved by the device during the first boot.
- TPMs that implement version 2.0 must ship with SHA-256 PCR banks and implement PCRs 0 through 23 for SHA-256. It is acceptable to ship TPMs with a single switchable PCR bank that can be used for both SHA-1 and SHA-256 measurements.
- A UEFI option to turn off the TPM is not a requirement.

Windows Server 2019 Activation

6/29/2020 • 6 minutes to read • [Edit Online](#)

Applies To: Windows Server 2019, Windows Server 2016

The following information outlines initial planning considerations that you need to review for Key Management Services (KMS) activation involving Windows Server 2019. For information about KMS activation involving operating systems older than those listed here, see [Step 1: Review and Select Activation Methods](#).

KMS uses a client-server model to activate clients. KMS clients connect to a KMS server, called the KMS host, for activation. The KMS host must reside on your local network.

KMS hosts do not need to be dedicated servers, and KMS can be cohosted with other services. You can run a KMS host on any physical or virtual system that is running Windows 10, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows 8.1, or Windows Server 2012.

A KMS host running on Windows 10 or Windows 8.1 can only activate computers running client operating systems. The following table summarizes KMS host and client requirements for networks that include Windows Server 2016, Windows Server 2019 and Windows 10 clients.

NOTE

- Updates might be required on the KMS server to support activation of any of these newer clients. If you receive activation errors, check that you have the appropriate updates listed below this table.
- If you are working with virtual machines, see [Automatic Virtual Machine Activation](#) for information and AVMA keys.

PRODUCT KEY GROUP	KMS CAN BE HOSTED ON	WINDOWS EDITIONS ACTIVATED BY THIS KMS HOST
-------------------	----------------------	---

PRODUCT KEY GROUP	KMS CAN BE HOSTED ON	WINDOWS EDITIONS ACTIVATED BY THIS KMS HOST
Volume License for Windows Server 2019	Windows Server 2012 R2 Windows Server 2016 Windows Server 2019	Windows Server Semi-Annual Channel Windows Server 2019 (all editions) Windows Server 2016 (all editions) Windows 10 Enterprise LTSC 2019 Windows 10 Enterprise LTSC N 2019 Windows 10 LTSB (2015 and 2016) Windows 10 Professional Windows 10 Enterprise Windows 10 Pro for Workstations Windows 10 Education Windows Server 2012 R2 (all editions) Windows 8.1 Professional Windows 8.1 Enterprise Windows Server 2012 (all editions) Windows Server 2008 R2 (all editions) Windows Server 2008 (all editions) Windows 7 Professional Windows 7 Enterprise
Volume License for Windows Server 2016	Windows Server 2012 Windows Server 2012 R2 Windows Server 2016	Windows Server Semi-Annual Channel Windows Server 2016 (all editions) Windows 10 LTSB (2015 and 2016) Windows 10 Professional Windows 10 Enterprise Windows 10 Pro for Workstations Windows 10 Education Windows Server 2012 R2 (all editions) Windows 8.1 Professional Windows 8.1 Enterprise Windows Server 2012 (all editions) Windows Server 2008 R2 (all editions) Windows Server 2008 (all editions) Windows 7 Professional Windows 7 Enterprise

PRODUCT KEY GROUP	KMS CAN BE HOSTED ON	WINDOWS EDITIONS ACTIVATED BY THIS KMS HOST
Volume license for Windows 10	Windows 7 Windows 8.1 Windows 10	Windows 10 Professional Windows 10 Professional N Windows 10 Enterprise Windows 10 Enterprise N Windows 10 Education Windows 10 Education N Windows 10 Enterprise LTSB (2015) Windows 10 Enterprise LTSB N (2015) Windows 10 Pro for Workstations Windows 8.1 Professional Windows 8.1 Enterprise Windows 7 Professional Windows 7 Enterprise
Volume license for Windows Server 2012 R2 for Windows 10	Windows Server 2008 R2 Windows Server 2012 Standard Windows Server 2012 Datacenter Windows Server 2012 R2 Standard Windows Server 2012 R2 Datacenter	Windows 10 Professional Windows 10 Enterprise Windows 10 Enterprise LTSB (2015) Windows 10 Pro for Workstations Windows 10 Education Windows Server 2012 R2 (all editions) Windows 8.1 Professional Windows 8.1 Enterprise Windows Server 2012 (all editions) Windows Server 2008 R2 (all editions) Windows Server 2008 (all editions) Windows 7 Professional Windows 7 Enterprise

NOTE

Depending on which operating system your KMS server is running and which operating systems you want to activate, you might need to install one or more of these updates:

- Installations of KMS on Windows 7 or Windows Server 2008 R2 must be updated in order to support activation of clients running Windows 10. For more information, see [Update that enables Windows 7 and Windows Server 2008 R2 KMS hosts to activate Windows 10](#).
- Installations of KMS on Windows Server 2012 must be updated in order to support activation of clients running Windows 10 and Windows Server 2016 or Windows Server 2019, or newer client or server operating systems. For more information, see [July 2016 update rollup for Windows Server 2012](#).
- Installations of KMS on Windows 8.1 or Windows Server 2012 R2 must be updated in order to support activation of clients running Windows 10 and Windows Server 2016 or Windows Server 2019, or newer client or server operating systems. For more information, see [July 2016 update rollup for Windows 8.1 and Windows Server 2012 R2](#).
- Windows Server 2008 R2 cannot be updated to support activation of clients running Windows Server 2016, Windows Server 2019, or newer operating systems.
- The KMS installed on Windows Server 2012 R2 must be updated in order to support activation of clients running Windows Server 2019. For more information, see [November 27, 2018—KB4467695 \(Preview of Monthly Rollup\)](#).

A single KMS host can support an unlimited number of KMS clients. If you have more than 50 clients, we recommend that you have at least two KMS hosts in case one of your KMS hosts becomes unavailable. Most organizations can operate with as few as two KMS hosts for their entire infrastructure.

Addressing KMS operational requirements

KMS can activate physical and virtual computers, but to qualify for KMS activation, a network must have a minimum number of computers (called the activation threshold). KMS clients activate only after this threshold is met. To ensure that the activation threshold is met, a KMS host counts the number of computers that are requesting activation on the network.

KMS hosts count the most recent connections. When a client or server contacts the KMS host, the host adds the machine ID to its count and then returns the current count value in its response. The client or server will activate if the count is high enough. Clients will activate if the count is 25 or higher. Servers and volume editions of Microsoft Office products will activate if the count is five or greater. The KMS only counts unique connections from the past 30 days, and only stores the 50 most recent contacts.

KMS activations are valid for 180 days, a period known as the activation validity interval. KMS clients must renew their activation by connecting to the KMS host at least once every 180 days to stay activated. By default, KMS client computers attempt to renew their activation every seven days. After a client's activation is renewed, the activation validity interval begins again.

Addressing KMS functional requirements

KMS activation requires TCP/IP connectivity. KMS hosts and clients are configured by default to use Domain Name System (DNS). By default, KMS hosts use DNS dynamic update to automatically publish the information that KMS clients need to find and connect to them. You can accept these default settings, or if you have special network and security configuration requirements, you can manually configure KMS hosts and clients.

After the first KMS host is activated, the KMS key that is used on the first host can be used to activate up to five more KMS hosts on your network. After a KMS host is activated, administrators can reactivate the same host up to nine times with the same key.

If your organization needs more than six KMS hosts, you should request additional activations for your organization's KMS key—for example, if you have ten physical locations under one volume licensing agreement and you want each location to have a local KMS host.

NOTE

To request this exception, contact your Activation Call Center. For more information, see [Microsoft Volume Licensing](#).

Computers that are running volume licensing editions of Windows 10, Windows Server 2019, Windows Server 2016, Windows 8.1, Windows Server 2012 R2, Windows Server 2012, Windows 7, Windows Server 2008 R2 are, by default, KMS clients with no additional configuration needed.

If you are converting a computer from a KMS host, MAK, or retail edition of Windows to a KMS client, install the applicable KMS Client Setup Key. For more information, see [KMS Client Setup Keys](#).

Automatic virtual machine activation

4/7/2020 • 3 minutes to read • [Edit Online](#)

Applies to: Windows Server 2019, Windows Server Semi-Annual Channel, Windows Server 2016, Windows Server 2012 R2

Automatic Virtual Machine Activation (AVMA) acts as a proof-of-purchase mechanism, helping to ensure that Windows products are used in accordance with the Product Use Rights and Microsoft Software License Terms.

AVMA lets you install virtual machines on a properly activated Windows server without having to manage product keys for each individual virtual machine, even in disconnected environments. AVMA binds the virtual machine activation to the licensed virtualization server and activates the virtual machine when it starts up. AVMA also provides real-time reporting on usage and historical data on the license state of the virtual machine. Reporting and tracking data is available on the virtualization server.

Practical applications

On virtualization servers that are activated using Volume Licensing or OEM licensing, AVMA offers several benefits.

Server datacenter managers can use AVMA to do the following:

- Activate virtual machines in remote locations
- Activate virtual machines with or without an internet connection
- Track virtual machine usage and licenses from the virtualization server, without requiring any access rights on the virtualized systems

There are no product keys to manage and no stickers on the servers to read. The virtual machine is activated and continues to work even when it is migrated across an array of virtualization servers.

Service Provider License Agreement (SPLA) partners and other hosting providers do not have to share product keys with tenants or access a tenant's virtual machine to activate it. Virtual machine activation is transparent to the tenant when AVMA is used. Hosting providers can use the server logs to verify license compliance and to track client usage history.

System requirements

AVMA requires a Microsoft Virtualization Server running Windows Server 2019 Datacenter, Windows Server 2016 Datacenter, or Windows Server 2012 R2.

Here are the guests that the different version hosts can activate:

SERVER HOST VERSION	WINDOWS SERVER 2019	WINDOWS SERVER 2016	WINDOWS SERVER 2012 R2
Windows Server 2019	X	X	X
Windows Server 2016		X	X
Windows Server 2012 R2			X

Note that these activate all editions (Datacenter, Standard, or Essentials).

This tool does not work with other Virtualization Server technologies.

How to implement AVMA

1. On a Windows Server Datacenter virtualization server, install and configure the Microsoft Hyper-V Server role. For more information, see [Install Hyper-V Server](#).
2. [Create a virtual machine](#) and install a supported server operating system on it.
3. Install the AVMA key in the virtual machine. From an elevated command prompt, run the following command:

```
slmgr /ipk <AVMA_key>
```

The virtual machine will automatically activate the license against the virtualization server.

TIP

You can also employ the AVMA keys in any Unattend.exe setup file.

AVMA keys

The following AVMA keys can be used for Windows Server 2019.

EDITION	AVMA KEY
Datacenter	H3RNG-8C32Q-Q8FRX-6TDXV-WMBMW
Standard	TNK62-RXVTB-4P47B-2D623-4GF74
Essentials	2CTP7-NHT64-BP62M-FV6GG-HFV28

The following AVMA keys can be used for Windows Server, versions 1909, 1903, and 1809.

EDITION	AVMA KEY
Datacenter	H3RNG-8C32Q-Q8FRX-6TDXV-WMBMW
Standard	TNK62-RXVTB-4P47B-2D623-4GF74

The following AVMA keys can be used for Windows Server, version 1803 and 1709.

EDITION	AVMA KEY
Datacenter	TMJ3Y-NTRTM-FJYXT-T22BY-CWG3J
Standard	C3RCX-M6NRP-6CXC9-TW2F2-4RHYD

The following AVMA keys can be used for Windows Server 2016.

EDITION	AVMA KEY
Datacenter	TMJ3Y-NTRTM-FJYXT-T22BY-CWG3J

EDITION	AVMA KEY
Standard	C3RCX-M6NRP-6CXC9-TW2F2-4RH4D
Essentials	B4YNW-62DX9-W8V6M-82649-MHBKQ

The following AVMA keys can be used for Windows Server 2012 R2.

EDITION	AVMA KEY
Datacenter	Y4TGP-NPTV9-HTC2H-7MGQ3-DV4TW
Standard	DBGBW-NPF86-BJVTX-K3WKJ-MTB6V
Essentials	K2XGM-NMBT3-2R6Q8-WF2FK-P36R2

Reporting and tracking

The registry (KVP) on the virtualization server provides real-time tracking data for the guest operating systems. Because the registry key moves with the virtual machine, you can get license information as well. By default the KVP returns information about the virtual machine, including the following:

- Fully qualified domain name
- Operating system and service packs installed
- Processor architecture
- IPv4 and IPv6 network addresses
- RDP addresses

For more information about how to get this information, see [Hyper-V Script: Looking at KVP GuestIntrinsicExchangeItems](#).

NOTE

KVP data is not secured. It can be modified and is not monitored for changes.

IMPORTANT

KVP data should be removed if the AVMA key is replaced with another product key (retail, OEM, or volume licensing key).

Historical data about AVMA requests is available in a log file on the virtualization server (EventID 12310).

Since the AVMA activation process is transparent, error messages are not displayed. However, the following events are captured in a log file on the virtual machines (EventID 12309).

NOTIFICATION	DESCRIPTION
AVMA Success	The virtual machine was activated.

NOTIFICATION	DESCRIPTION
Invalid Host	The virtualization server is unresponsive. This can happen when the server is not running a supported version of Windows.
Invalid Data	This usually results from a failure in communication between the virtualization server and the virtual machine, often caused by corruption, encryption, or data mismatch.
Activation Denied	The virtualization server could not activate the guest operating system because the AVMA ID did not match.

Troubleshooting Windows volume activation

10/4/2019 • 2 minutes to read • [Edit Online](#)

Product activation is the process of validating software after it's installed on a specific computer. Activation confirms that the product is genuine (not a fraudulent copy) and that the product key or serial number is valid and has not been compromised or revoked. Activation also establishes a link or relationship between the product key and the installation.

Volume activation is the process of activating volume-licensed products. To become a volume licensing customer, an organization must set up a volume licensing agreement with Microsoft. Microsoft offers customized volume licensing programs that accommodate the organization's size and purchasing preference. For more information, see the [Microsoft Volume Licensing Service Center](#).

The [Windows Server 2016 Activation Guide](#) focuses on the Key Management Service (KMS) activation technology. This section addresses common issues and provides troubleshooting guidelines for KMS and several other volume activation technologies.

Best practices for volume activation

The following articles provide technical information and best practices for Microsoft's volume activation technologies.

Key Management Service (KMS)

- [Plan for volume activation](#)
- [Understanding KMS](#)
- [Deploying KMS Activation](#)
- [Configuring KMS Hosts](#)
- [Configuring DNS](#)
- [Activate using Key Management Service](#)

Active Directory-based activation (ADBA)

- [Deploy Active-Directory-based Activation](#)
- [Activate using Active Directory-based activation](#)
- [Active Directory-Based Activation overview](#)

Multiple Activation Key (MAK) activation

- [Using MAK Activation](#)
- [Understanding MAK Activation](#)
- [Activating MAK Clients](#)

Subscription activation

- [Windows 10 Subscription Activation](#)
- [Deploy Windows 10 Enterprise licenses](#)
- [Windows 10 Enterprise E3 in CSP](#)

Resources for troubleshooting activation issues

The following articles provide guidelines and information about tools for troubleshooting volume activation issues:

- [Guidelines for troubleshooting the Key Management Service \(KMS\)](#)

- [Slmgr.vbs options for obtaining volume activation information](#)
- [Example: Troubleshooting ADBA clients that do not activate](#)

The following articles provide guidance for addressing more specific activation issues:

- [Resolving common activation error codes](#)
- [KMS activation: known issues](#)
- [MAK activation: known issues](#)
- [Guidelines for troubleshooting DNS-related activation issues](#)
- [How to rebuild the Tokens.dat file](#)

Windows Server 2019 and Microsoft Server application compatibility

4/7/2020 • 2 minutes to read • [Edit Online](#)

Applies To: Windows Server 2019

This table lists Microsoft server applications that support installation and functionality on Windows Server 2019. This information is for quick reference and is not intended to replace the individual product specifications, requirements, announcements, or general communications of each individual server application. Refer to official documentation for each product to fully understand compatibility and options.

If you are a software vendor partner looking for more information on Windows Server compatibility with non-Microsoft applications, visit the [Commercial App Certification portal](#).

PRODUCT	SUPPORTED ON SERVER CORE		SUPPORTED ON SERVER WITH DESKTOP EXPERIENCE	RELEASED?		PRODUCT WEB LINK
Exchange Server 2019	Yes		Yes	Yes		Exchange Server system requirements
Host Integration Server 2016, CU3	Yes		Yes	Yes		Host Integration Server system requirements
Visual Studio Team Foundation Server 2017	Yes*		Yes	Yes		Team Foundation Server 2017
Visual Studio Team Foundation Server 2018	Yes*		Yes	Yes		Team Foundation Server 2018
Microsoft SQL Server 2014	Yes*		Yes	Yes		Hardware and Software Requirements for Installing SQL Server 2014
Microsoft SQL Server 2016	Yes*		Yes	Yes		Hardware and Software Requirements for Installing SQL Server 2016

PRODUCT	SUPPORTED ON SERVER CORE		SUPPORTED ON SERVER WITH DESKTOP EXPERIENCE	RELEASED?		PRODUCT WEB LINK
Microsoft SQL Server 2017	Yes*		Yes	Yes		Hardware and Software Requirements for Installing SQL Server 2017
Microsoft SQL Server 2019	Yes*		Yes	Yes		Hardware and Software Requirements for Installing SQL Server 2019
Configuration Manager (version 1806)	Yes as managed client, No as site server		Yes as managed client, No as site server	Yes		What's new in version 1806 of Configuration Manager current branch
Microsoft System Center Operations Manager 2019	Yes*		Yes	Yes		System requirements for System Center Operations Manager
Microsoft System Center Virtual Machine Manager 2019	Yes*		Yes	Yes		System requirements for System Center Virtual Machine Manager
Microsoft System Center Data Protection Manager 2019	No		Yes	Yes		Preparing your environment for System Center Data Protection Manager
SharePoint Server 2016	No		Yes	Yes		Hardware and software requirements for SharePoint Server 2016
SharePoint Server 2019	No		Yes	Yes		Hardware and software requirements for SharePoint Server 2019

PRODUCT	SUPPORTED ON SERVER CORE		SUPPORTED ON SERVER WITH DESKTOP EXPERIENCE	RELEASED?		PRODUCT WEB LINK
Project Server 2016	No		Yes	Yes		Software requirements for Project Server 2016
Project Server 2019	No		Yes	Yes		Software requirements for Project Server 2019
Skype for Business 2019	No		Yes	Yes		Install prerequisites for Skype for Business Server

*May have limitations or may require the [Server Core App Compatibility Feature on Demand \(FOD\)](#). Please refer to specific product or FOD documentation.

Server Core App Compatibility Feature on Demand (FOD)

4/7/2020 • 7 minutes to read • [Edit Online](#)

Applies to: Windows Server 2019, Windows Server Semi-Annual Channel

The **Server Core App Compatibility Feature on Demand** is an optional feature package that can be added to Windows Server 2019 Server Core installations, or Windows Server Semi-Annual Channel, at any time.

For more information on Features on Demand (FOD), see [Features On Demand](#).

Why install the App Compatibility FOD?

App Compatibility, a Feature on Demand for Server Core, significantly improves the app compatibility of the Windows Server Core installation option by including a subset of binaries and packages from Windows Server with Desktop Experience, without adding the Windows Server Desktop Experience graphical environment. This optional package is available on a separate ISO, or from Windows Update, but can only be added to Windows Server Core installations and images.

The two primary values the App Compatibility FOD provides are:

- Increases the compatibility of Server Core for server applications that are already in market or have already been developed by organizations and deployed.
- Assists with providing OS components and increased app compatibility of software tools used in acute troubleshooting and debugging scenarios.

Operating system components that are available as part of the Server Core App Compatibility FOD include:

- Microsoft Management Console (mmc.exe)
- Event Viewer (Eventvwr.msc)
- Performance Monitor (PerfMon.exe)
- Resource Monitor (Resmon.exe)
- Device Manager (Devmgmt.msc)
- File Explorer (Explorer.exe)
- Windows PowerShell (Powershell_ISE.exe)
- Disk Management (Diskmgmt.msc)
- Failover Cluster Manager (CluAdmin.msc)
 - Requires addition of the Failover Clustering Windows Server feature first.
 - From an elevated PowerShell session:

```
Install-WindowsFeature -Name Failover-Clustering -IncludeManagementTools
```

- To run Failover Cluster Manager, enter **cludmin** at the command prompt.

Servers running Windows Server, version 1903 and later also support the following components (when using the same version of the App Compatibility FOD):

- Hyper-V Manager (virtmgmt.msc)
- Task Scheduler (taskschd.msc)

Installing the App Compatibility FOD

The App Compatibility FOD can only be installed on Server Core. Don't attempt to add the Server Core App Compatibility FOD to a Windows Server installation of Windows Server with Desktop Experience. The same FOD optional packages ISO can be used for either Windows Server 2019 Server Core installations, or Windows Server Semi-Annual Channel installations.

1. If the server can connect to Windows Update, all you have to do is run the following command from an elevated PowerShell session and then restart Windows Server after the command finishes running:

```
Add-WindowsCapability -Online -Name ServerCore.AppCompatibility~~~~0.0.1.0
```

2. If the server can't connect to Windows Update, instead download the Server FOD optional packages ISO, and copy the ISO to a shared folder on your local network:

- If you have a volume license you can download the Server FOD ISO image file from the same portal where the OS ISO image file is obtained: [Volume Licensing Service Center](#).
- The Server FOD ISO image file is also available on the [Microsoft Evaluation Center](#) or on the [Visual Studio portal](#) for subscribers.

3. Sign in with an administrator account on the Server Core computer that is connected to your local network and that you want to add the FOD to.
4. Use **net use**, or some other method, to connect to the location of the FOD ISO.
5. Copy the FOD ISO to a local folder of your choosing.
6. Mount the FOD ISO by using the following command in an elevated PowerShell session:

```
Mount-DiskImage -ImagePath drive_letter:\folder_where_ISO_is_saved\ISO_filename.iso
```

7. Run the following command:

```
Add-WindowsCapability -Online -Name ServerCore.AppCompatibility~~~~0.0.1.0 -Source  
<Mounted_Server_FOD_Drive> -LimitAccess
```

8. After the progress bar completes, restart the operating system.

For more information about DISM commands, see [Use DISM in Windows PowerShell](#)

To optionally add Internet Explorer 11 to Server Core (after adding the Server Core App Compatibility FOD)

NOTE

The Server Core App Compatibility FOD is required for the addition of Internet Explorer 11, but Internet Explorer 11 is not required to add the Server Core App Compatibility FOD.

1. Sign in as Administrator on the Server Core computer that has the App Compatibility FOD already added and the Server FOD optional package ISO copied locally.
2. Start PowerShell by entering **powershell.exe** at a command prompt.
3. Mount the FOD ISO by using the following command:

```
Mount-DiskImage -ImagePath drive_letter:\folder_where_ISO_is_saved\ISO_filename.iso
```

4. Run the following command, using the `$package_path` variable to enter the path to the Internet Explorer cab file:

```
$package_path = D:\Microsoft-Windows-InternetExplorer-Optional-Package~31bf3856ad364e35~amd64~~.cab  
Add-WindowsPackage -Online -PackagePath $package_path
```

5. After the progress bar completes, restart the operating system.

Release notes and suggestions for the Server Core App Compatibility FOD and Internet Explorer 11 optional package

IMPORTANT

FODs installed on Windows Server, version 1809 won't remain in place after an in-place upgrade to Windows Server, version 1903, so you'd have to install them again after the upgrade. Alternatively, you can add FODs to the new Windows Server installation source prior to upgrading. This ensures that the new version of any FODs are present after the upgrade completes. For more info, see the [Adding capabilities and optional packages to an offline WIM Server Core image](#).

- **Important:** Read the Windows Server 2019 release notes for any issues, considerations, or guidance before proceeding with installation and use of the Server Core App Compatibility FOD and Internet Explorer 11 optional package.
- It's possible to encounter flickering with the Server Core console experience when adding the App Compatibility FOD after using Windows Update to install cumulative updates. This issue is resolved with December, 2018 updates. For more info and resolution steps, see [Knowledge Base article 4481610: Screen flickers after you install Server Core App Compatibility FOD in Windows Server 2019 Server Core](#).
- After installation of the App Compatibility FOD and reboot of the server, the command console window frame color will change to a different shade of blue.
- If you choose to also install the Internet Explorer 11 optional package, note that double clicking to open locally saved .htm files is not supported. However, you can **right-click** and choose **Open with IE**, or you can open it directly from Internet Explorer **File -> Open**.
- To further enhance the app compatibility of Server Core with the App Compatibility FOD, the IIS Management Console has been added to Server Core as an optional component. However, it is absolutely necessary to first add the App Compatibility FOD to use the IIS Management Console. IIS Management Console relies on the Microsoft Management Console (mmc.exe), which is only available on Server Core with the addition of the App Compatibility FOD. Use Powershell **Install-WindowsFeature** to add IIS Management Console.
- As a general point of guidance, when installing apps on Server Core (with or without these optional packages) it is sometimes necessary to use silent install options and instructions.
 - As an example, SQL Server Management Studio for SQL Server 2016 and SQL Server 2017 can be

installed on Server Core and is fully functional when the App Compatibility FOD is present. See, [Install SQL Server from the Command Prompt](#).

- o If SQL Server Management Studio is not desired, then it is unnecessary to install the Server Core App Compatibility FOD. See, [Install SQL Server on Server Core](#).

Adding capabilities and optional packages to an offline WIM Server Core image

1. Download the Windows Server and Server FOD ISO image files to a local folder on a Windows computer.
 - If you have a volume license you can download the Windows Server and Server FOD ISO image files from the [Volume Licensing Service Center](#).
 - The Server FOD ISO image file is also available for Long-Term Servicing Channel releases on the [Microsoft Evaluation Center](#) or on the [Visual Studio portal](#) for subscribers.
2. Open a PowerShell session as an administrator and then use the following commands to mount the image files as drives:

```
Mount-DiskImage -ImagePath Path_To_ServerFOD_ISO
Mount-DiskImage -ImagePath Path_To_Windows_Server_ISO
```

3. Copy the contents of the Windows Server ISO file to a local folder (for example, *C:\SetupFiles\WindowsServer*).
4. Get the image name you want to modify within the Install.wim file by using the following command. Use the `$install_wim_path` variable to enter the path to the Install.wim file, located inside the \Sources folder of the ISO file.

```
$install_wim_path = C:\SetupFiles\WindowsServer\sources\install.wim
Get-WindowsImage -ImagePath $install_wim_path
```

5. Mount the Install.wim file in a new folder by using the following command replacing the sample variable values with your own, and reusing the `$install_wim_path` variable from the previous command.
 - `$image_name` - Enter the name of the image you want to mount.
 - `$mount_folder variable` - Specify the folder to use when accessing the contents of the Install.wim file.

```
$image_name = Windows Server Datacenter
$mount_folder = c:\test\offline
Mount-WindowsImage -ImagePath $install_wim_path -Name $image_name -path $mount_folder
```

6. Add capabilities and packages you want to the mounted Install.wim image by using the following commands, replacing the sample variable values with your own.
 - `$capability_name` - Specify the name of the capability to install (in this case, the AppCompatibility capability).
 - `$package_path` - Specify the path to the package to install (in this case, Internet Explorer).
 - `$fod_drive` - Specify the drive letter of the mounted Server FOD image.

```
$capability_name = ServerCore.AppCompatibility~~~~0.0.1.0
$package_path = D:\Microsoft-Windows-InternetExplorer-Optional-Package~31bf3856ad364e35~amd64~~.cab
$fod_drive = d:\

Add-WindowsCapability -Path $mount_folder -Name $capability_name -Source $fod_drive -LimitAccess
Add-WindowsPackage -Path $mount_folder -PackagePath $package_path
```

7. Dismount and commit changes to the Install.wim file by using the following command, which uses the `$mount_folder` variable from previous commands:

```
Dismount-WindowsImage -Path $mount_folder -Save
```

You can now upgrade your server by running `setup.exe` from the folder you created for the Windows Server installation files (in this example: `C:\SetupFiles\WindowsServer`). This folder now contains the Windows Server installation files with the additional capabilities and optional packages included.

Comparison of Standard and Datacenter editions of Windows Server 2019

10/21/2019 • 5 minutes to read • [Edit Online](#)

Applies To: Windows Server 2019

Locks and Limits

LOCKS AND LIMITS	WINDOWS SERVER 2019 STANDARD	WINDOWS SERVER 2019 DATACENTER
Maximum number of users	Based on CALs	Based on CALs
Maximum SMB connections	16,777,216	16,777,216
Maximum RRAS connections	unlimited	unlimited
Maximum IAS connections	2,147,483,647	2,147,483,647
Maximum RDS connections	65,535	65,535
Maximum number of 64-bit sockets	64	64
Maximum number of cores	unlimited	unlimited
Maximum RAM	24 TB	24 TB
Can be used as virtualization guest	Yes; 2 virtual machines, plus one Hyper-V host per license	Yes; unlimited virtual machines , plus one Hyper-V host per license
Server can join a domain	yes	yes
Edge network protection/firewall	no	no
DirectAccess	yes	yes
DLNA codecs and web media streaming	Yes, if installed as Server with Desktop Experience	Yes, if installed as Server with Desktop Experience

Server roles

WINDOWS SERVER ROLES AVAILABLE	ROLE SERVICES	WINDOWS SERVER 2019 STANDARD	WINDOWS SERVER 2019 DATACENTER
Active Directory Certificate Services		Yes	Yes
Active Directory Domain Services		Yes	Yes

WINDOWS SERVER ROLES AVAILABLE	ROLE SERVICES	WINDOWS SERVER 2019 STANDARD	WINDOWS SERVER 2019 DATACENTER
Active Directory Federation Services		Yes	Yes
AD Lightweight Directory Services		Yes	Yes
AD Rights Management Services		Yes	Yes
Device Health Attestation		Yes	Yes
DHCP Server		Yes	Yes
DNS Server		Yes	Yes
Fax Server		Yes	Yes
File and Storage Services	File Server	Yes	Yes
File and Storage Services	BranchCache for Network Files	Yes	Yes
File and Storage Services	Data Deduplication	Yes	Yes
File and Storage Services	DFS Namespaces	Yes	Yes
File and Storage Services	DFS Replication	Yes	Yes
File and Storage Services	File Server Resource Manager	Yes	Yes
File and Storage Services	File Server VSS Agent Service	Yes	Yes
File and Storage Services	iSCSI Target Server	Yes	Yes
File and Storage Services	iSCSI Target Storage Provider	Yes	Yes
File and Storage Services	Server for NFS	Yes	Yes
File and Storage Services	Work Folders	Yes	Yes
File and Storage Services	Storage Services	Yes	Yes
Host Guardian Service		Yes	Yes
Hyper-V		Yes	Yes; including Shielded Virtual Machines
Network Controller		No	Yes

WINDOWS SERVER ROLES AVAILABLE	ROLE SERVICES	WINDOWS SERVER 2019 STANDARD	WINDOWS SERVER 2019 DATACENTER
Network Policy and Access Services		Yes, when installed as Server with Desktop Experience	Yes, when installed as Server with Desktop Experience
Print and Document Services		Yes	Yes
Remote Access		Yes	Yes
Remote Desktop Services		Yes	Yes
Volume Activation Services		Yes	Yes
Web Services (IIS)		Yes	Yes
Windows Deployment Services		Yes*	Yes*
Windows Server Essentials Experience		No	No
Windows Server Update Services		Yes	Yes

*WDS Transport Server is new to Server Core installations in Windows Server 2019 (also in the semi-annual channel starting with Windows Server, version 1803)

Features

WINDOWS SERVER FEATURES INSTALLABLE WITH SERVER MANAGER (OR POWERSHELL)	WINDOWS SERVER 2019 STANDARD	WINDOWS SERVER 2019 DATACENTER
.NET Framework 3.5	Yes	Yes
.NET Framework 4.7	Yes	Yes
Background Intelligent Transfer Service (BITS)	Yes	Yes
BitLocker Drive Encryption	Yes	Yes
BitLocker Network Unlock	Yes, when installed as Server with Desktop Experience	Yes, when installed as Server with Desktop Experience
BranchCache	Yes	Yes
Client for NFS	Yes	Yes
Containers	Yes (unlimited Windows containers; up to two Hyper-V containers)	Yes (unlimited Windows and Hyper-V containers)
Data Center Bridging	Yes	Yes

WINDOWS SERVER FEATURES INSTALLABLE WITH SERVER MANAGER (OR POWERSHELL)	WINDOWS SERVER 2019 STANDARD	WINDOWS SERVER 2019 DATACENTER
Direct Play	Yes, when installed as Server with Desktop Experience	Yes, when installed as Server with Desktop Experience
Enhanced Storage	Yes	Yes
Failover Clustering	Yes	Yes
Group Policy Management	Yes	Yes
Host Guardian Hyper-V Support	No	Yes
I/O Quality of Service	Yes	Yes
IIS Hostable Web Core	Yes	Yes
Internet Printing Client	Yes, when installed as Server with Desktop Experience	Yes, when installed as Server with Desktop Experience
IPAM Server	Yes	Yes
iSNS Server service	Yes	Yes
LPR Port Monitor	Yes, when installed as Server with Desktop Experience	Yes, when installed as Server with Desktop Experience
Management OData IIS Extension	Yes	Yes
Media Foundation	Yes	Yes
Message Queueing	Yes	Yes
Multipath I/O	Yes	Yes
MultiPoint Connector	Yes	Yes
Network Load Balancing	Yes	Yes
Peer Name Resolution Protocol	Yes	Yes
Quality Windows Audio Video Experience	Yes	Yes
RAS Connection Manager Administration Kit	Yes, when installed as Server with Desktop Experience	Yes, when installed as Server with Desktop Experience
Remote Assistance	Yes, when installed as Server with Desktop Experience	Yes, when installed as Server with Desktop Experience
Remote Differential Compression	Yes	Yes

WINDOWS SERVER FEATURES INSTALLABLE WITH SERVER MANAGER (OR POWERSHELL)	WINDOWS SERVER 2019 STANDARD	WINDOWS SERVER 2019 DATACENTER
RSAT	Yes	Yes
RPC over HTTP Proxy	Yes	Yes
Setup and Boot Event Collection	Yes	Yes
Simple TCP/IP Services	Yes, when installed as Server with Desktop Experience	Yes, when installed as Server with Desktop Experience
SMB 1.0/CIFS File Sharing Support	Installed	Installed
SMB Bandwidth Limit	Yes	Yes
SMTP Server	Yes	Yes
SNMP Service	Yes	Yes
Software Load Balancer	Yes	Yes
Storage Replica	Yes	Yes
Telnet Client	Yes	Yes
TFTP Client	Yes, when installed as Server with Desktop Experience	Yes, when installed as Server with Desktop Experience
VM Shielding Tools for Fabric Management	Yes	Yes
WebDAV Redirector	Yes	Yes
Windows Biometric Framework	Yes, when installed as Server with Desktop Experience	Yes, when installed as Server with Desktop Experience
Windows Defender features	Installed	Installed
Windows Identity Foundation 3.5	Yes, when installed as Server with Desktop Experience	Yes, when installed as Server with Desktop Experience
Windows Internal Database	Yes	Yes
Windows PowerShell	Installed	Installed
Windows Process Activation Service	Yes	Yes
Windows Search Service	Yes, when installed as Server with Desktop Experience	Yes, when installed as Server with Desktop Experience
Windows Server Backup	Yes	Yes

WINDOWS SERVER FEATURES INSTALLABLE WITH SERVER MANAGER (OR POWERSHELL)	WINDOWS SERVER 2019 STANDARD	WINDOWS SERVER 2019 DATACENTER
Windows Server Migration Tools	Yes	Yes
Windows Standards-Based Storage Management	Yes	Yes
Windows TIFF IFilter	Yes, when installed as Server with Desktop Experience	Yes, when installed as Server with Desktop Experience
WinRM IIS Extension	Yes	Yes
WINS Server	Yes	Yes
Wireless LAN Service	Yes	Yes
WoW64 support	Installed	Installed
XPS Viewer	Yes, when installed as Server with Desktop Experience	Yes, when installed as Server with Desktop Experience

FEATURES AVAILABLE GENERALLY	WINDOWS SERVER 2019 STANDARD	WINDOWS SERVER 2019 DATACENTER
Best Practices Analyzer	Yes	Yes
Direct Access	Yes	Yes
Dynamic Memory (in virtualization)	Yes	Yes
Hot Add/Replace RAM	Yes	Yes
Microsoft Management Console	Yes	Yes
Minimal Server Interface	Yes	Yes
Network Load Balancing	Yes	Yes
Windows PowerShell	Yes	Yes
Server Core installation option	Yes	Yes
Server Manager	Yes	Yes
SMB Direct and SMB over RDMA	Yes	Yes
Software-defined Networking	No	Yes
Storage Migration Service	Yes	Yes
Storage Replica	Yes, (1 partnership and 1 resource group with a single 2TB volume)	Yes, unlimited

FEATURES AVAILABLE GENERALLY	WINDOWS SERVER 2019 STANDARD	WINDOWS SERVER 2019 DATACENTER
Storage Spaces	Yes	Yes
Storage Spaces Direct	No	Yes
Volume Activation Services	Yes	Yes
VSS (Volume Shadow Copy Service) integration	Yes	Yes
Windows Server Update Services	Yes	Yes
Windows System Resource Manager	Yes	Yes
Server license logging	Yes	Yes
Inherited activation	As guest if hosted on Datacenter	Can be a host or a guest
Work Folders	Yes	Yes

Features removed or planned for replacement in Windows Server

6/26/2020 • 2 minutes to read • [Edit Online](#)

Applies to: Windows Server 2019, Windows Server 2016, Windows Server (Semi-Annual Channel)

You can find the removed and deprecated features for each of these Windows Server releases.

Long-Term Servicing Channel (LTSC) releases:

- [Features removed or planned for removal in Windows Server 2019](#)
- [Features Removed or Deprecated in Windows Server 2016](#)

Semi-Annual Channel releases:

- [Features removed or planned for replacement starting with Windows Server, version 1903](#)
- [Features removed or planned for replacement starting with Windows Server, version 1803](#)
- [Features removed or planned for replacement starting with Windows Server, version 1709](#) (Out of support as of April 9, 2019)

Windows Server Semi-Annual Channel releases deliver new operating system capabilities at a faster pace. A new release comes out every six months and is supported for 18 months. Check [Windows Server release information](#) and [Lifecycle Support Page](#) for support dates and always use the latest release if possible.

Additional References

- [What's new in Windows Server](#)

Features removed or planned for replacement starting Windows Server 2019

4/7/2020 • 3 minutes to read • [Edit Online](#)

Applies to: Windows Server 2019

Each release of Windows Server adds new features and functionality; we also occasionally remove features and functionality, usually because we've added a better option. Here are the details about the features and functionalities that we removed in Windows Server 2019.

TIP

- You can get early access to Windows Server builds by joining the [Windows Insider program](#) - this is a great way to test feature changes.
- Have questions about other releases? Check out [Features removed or planned for replacement in Windows Server](#).

The list is subject to change and might not include every affected feature or functionality.

Features we removed in this release

We're removing the following features and functionalities from the installed product image in Windows Server 2019. Applications or code that depend on these features won't function in this release unless you use an alternate method.

FEATURE	INSTEAD YOU CAN USE...
Business Scanning, also called Distributed Scan Management (DSM)	We're removing this secure scanning and scanner management capability - there are no devices that support this feature.
Print components - now optional component for Server Core installations	In previous releases of Windows Server, the print components were <i>disabled</i> by default in the Server Core installation option. We changed that in Windows Server 2016, enabling them by default. In Windows Server 2019, those print components are once again disabled by default for Server Core. If you need to enable the print components, you can do so by running the Install-WindowsFeature Print-Server cmdlet.
Remote Desktop Connection Broker and Remote Desktop Virtualization Host in a Server Core installation	Most Remote Desktop Services deployments have these roles co-located with the Remote Desktop Session Host (RDSH), which requires Server with Desktop Experience; to be consistent with RDSH we're changing these roles to also require Server with Desktop Experience. These RDS roles are no longer available for use in a Server Core installation . If you need to deploy these roles as part of your Remote Desktop infrastructure , you can install them on Windows Server with Desktop Experience . These roles are also included in the Desktop Experience installation option of Windows Server 2019.

FEATURE	INSTEAD YOU CAN USE...
RemoteFX 3D Video Adapter (vGPU)	We're developing new graphics acceleration options for virtualized environments. You can also use Discrete Device Assignment (DDA) as an alternative.

Features we're no longer developing

We're no longer actively developing these features and may remove them from a future update. Some features have been replaced with other features or functionality, while others are now available from different sources.

If you have feedback about the proposed replacement of any of these features, you can use the [Feedback Hub app](#).

FEATURE	INSTEAD YOU CAN USE...
Key Storage Drive in Hyper-V	We're no longer working on the Key Storage Drive feature in Hyper-V. If you're using generation 1 VMs, check out Generation 1 VM Virtualization Security for information about options going forward. If you're creating new VMs use Generation 2 virtual machines with TPM devices for a more secure solution.
Trusted Platform Module (TPM) management console	The information previously available in the TPM management console is now available on the Device security page in the Windows Defender Security Center .
Host Guardian Service Active Directory attestation mode	We're no longer developing Host Guardian Service Active Directory attestation mode - instead we've added a new attestation mode, host key attestation , that's far simpler and equally as compatible as Active Directory based attestation. This new mode provides equivalent functionality with a setup experience, simpler management and fewer infrastructure dependencies than the Active Directory attestation. Host key attestation has no additional hardware requirements beyond what Active Directory attestation required, so all existing systems will remain compatible with the new mode. See Deploy guarded hosts for more information about your attestation options.
OneSync service	The OneSync service synchronizes data for the Mail, Calendar, and People apps. We've added a sync engine to the Outlook app that provides the same synchronization.
Remote Differential Compression API support	Remote Differential Compression API support enabled synchronizing data with a remote source using compression technologies, which minimized the amount of data sent across the network.
WFP lightweight filter switch extension	The WFP lightweight filter switch extension enables developers to build simple network packet filtering extensions for the Hyper-V virtual switch . You can achieve the same functionality by creating a full filtering extension. As such, we'll be removing this extension in the future.

Features removed or planned for replacement starting with Windows Server, version 1903 and 1909

11/12/2019 • 2 minutes to read • [Edit Online](#)

Applies to: Windows Server, version 1903 and 1909

The following is a list of features and functionalities in Windows Server, version 1903 and 1909 that have either been removed from the product in that release or are starting to be considered for potential replacement in subsequent releases. It is intended for IT professionals who are updating operating systems in a commercial environment. **This list is subject to change in subsequent releases and might not include every affected feature or functionality.**

Also see [Features removed or planned for replacement in Windows Server](#).

Features we're no longer developing

We're no longer actively developing these features and may remove them from a future update. Some features have been replaced with other features or functionality, while others are now available from different sources.

If you have feedback about the proposed replacement of any of these features, you can use the [Feedback Hub app](#).

FEATURE	INSTEAD YOU CAN USE
Hyper-V vSwitch on LBFO	In a future release, the Hyper-V vSwitch will no longer have the capability to be bound to an LBFO team. Instead, it must be bound via Switch Embedded Teaming (SET) .
XDDM-based remote display driver (new)	Starting with this release the Remote Desktop Services uses a Windows Display Driver Model (WDDM) based Indirect Display Driver (IDD) for a single session remote desktop. The support for Windows 2000 Display Driver Model (XDDM) based remote display drivers will be removed in a future release. Independent Software Vendors that use XDDM-based remote display driver should plan a migration to the WDDM driver model. For more information on implementing remote display indirect display driver ISVs can reach out to rdsdev@microsoft.com .
UCS log collection tool (new)	The UCS log collection tool, while not explicitly intended for use with Windows Server, is nonetheless being replaced by the Feedback hub on Windows 10.
Key Storage Drive in Hyper-V	We're no longer working on the Key Storage Drive feature in Hyper-V. If you're using generation 1 VMs, check out Generation 1 VM Virtualization Security for information about options going forward. If you're creating new VMs use Generation 2 virtual machines with TPM devices for a more secure solution.
Trusted Platform Module (TPM) management console	The information previously available in the TPM management console is now available on the Device security page in the Windows Defender Security Center .

FEATURE	INSTEAD YOU CAN USE
Host Guardian Service Active Directory attestation mode	<p>We're no longer developing Host Guardian Service Active Directory attestation mode - instead we've added a new attestation mode, host key attestation, that's far simpler and equally as compatible as Active Directory based attestation. This new mode provides equivalent functionality with a setup experience, simpler management and fewer infrastructure dependencies than the Active Directory attestation. Host key attestation has no additional hardware requirements beyond what Active Directory attestation required, so all existing systems will remain compatible with the new mode. See Deploy guarded hosts for more information about your attestation options.</p>
OneSync service	<p>The OneSync service synchronizes data for the Mail, Calendar, and People apps. We've added a sync engine to the Outlook app that provides the same synchronization.</p>
Remote Differential Compression API support	<p>Remote Differential Compression API support enabled synchronizing data with a remote source using compression technologies, which minimized the amount of data sent across the network.</p>
WFP lightweight filter switch extension	<p>The WFP lightweight filter switch extension enables developers to build simple network packet filtering extensions for the Hyper-V virtual switch. You can achieve the same functionality by creating a full filtering extension. As such, we'll be removing this extension in the future.</p>

Windows Server release information

4/14/2020 • 2 minutes to read • [Edit Online](#)

Microsoft has updated its servicing model. The Semi-Annual Channel is a twice-per-year feature update release with 18-month servicing timelines for each release. This page is designed to help you determine the end of support date for the Semi-Annual Channel releases.

The Semi-Annual Channel provides opportunity for customers who are innovating quickly to take advantage of new operating system capabilities at a faster pace, both in applications - particularly those built on containers and microservices. For more information see the [Comparison of servicing channels](#). Customers also have the option to continue using the Long-Term Servicing Channel releases, which continue to be released every 2-3 years. Each Long-Term Servicing Channel release is supported for 5 years of mainstream support and 5 years of extended support.

Windows Server current versions by servicing option

WINDOWS SERVER RELEASE	VERSION	OS BUILD	AVAILABILITY	MAINSTREAM SUPPORT END DATE	EXTENDED SUPPORT END DATE
Windows Server, version 1909 (Semi-Annual Channel) (Datacenter Core, Standard Core)	1909	18363.418.1910 07-0143	11/12/2019	05/11/2021	Review note
Windows Server, version 1903 (Semi-Annual Channel) (Datacenter Core, Standard Core)	1903	18362.30.19040 1-1528	5/21/2019	12/08/2020	Review note
Windows Server 2019 (Long-Term Servicing Channel) (Datacenter, Essentials, Standard)	1809	17763.107.1010 129-1455	11/13/2018	01/09/2024	01/09/2029
Windows Server, version 1809 (Semi-Annual Channel) (Datacenter Core, Standard Core)	1809	17763.107.1010 129-1455	11/13/2018	11/10/2020	Review note
Windows Server 2016 (Long-Term Servicing Channel)	1607	14393.0	10/15/2016	01/11/2022	01/11/2027

IMPORTANT

End of service for Windows Server, version 1809 has been delayed due to the ongoing public health crisis. For more information, see [our Support article](#).

NOTE

Windows Server, version 1803 and later are governed by the [Modern Lifecycle Policy](#). See the [Windows Lifecycle FAQ](#) and [Comparison of servicing channels](#) for details regarding servicing requirements and other important information.

Windows Server - License Terms

9/27/2019 • 2 minutes to read • [Edit Online](#)

Review our Windows Server-related license terms.

- [Additional software for Windows Server 2016](#)
- [Windows Server Technical Preview Expiration](#)
- [Windows Server 2016 Technical Preview License Terms](#)
- [Microsoft Software License Terms - MICROSOFT.WINDOWSSERVER.SYSTEMINSIGHTS](#)
- [Microsoft Software License Terms - MICROSOFT.WINDOWSSERVER.SYSTEMINSIGHTS.CAPABILITIES](#)
- [Windows Admin Center - License Terms](#)