Get started with Windows Server

Article • 09/19/2022

Windows Server is the platform for building an infrastructure of connected applications, networks, and web services, from the workgroup to the data center. It bridges on-premises environments with Azure, adding additional layers of security while helping you modernize your applications and infrastructure.

This collection of articles contains detailed information to help you understand and get the most from Windows Server, and help determine if you're ready to move to the latest version. Once you've checked the system requirements, upgrade options, and other information about Windows Server, you're ready to start down the path of installing the best edition and installation option for your needs.

> **Tip**
>
> To download Windows Server, see **Windows Server evaluations** in the Evaluation Center.

> **Note**
>
> If you're looking for information about earlier versions that are no longer supported, see the **Windows previous versions documentation**.

Support and feedback

For the latest news on Windows Server, visit the Windows Server blog to stay up to date on announcements, features, events, and other information from the Windows Server engineering teams. You can also visit the Windows Server Community to share best practices, get latest news, and learn from experts about Windows Server.

Learn

Browse learning paths for Windows Server to help learn new skills and accelerate your deployment with step-by-step guidance. You can learn how to deploy, configure and administer Windows Server, as well as network infrastructure, file servers and storage management, Hyper-V and virtualization, plus much more.

Windows Insider Program

The Windows Insider Program for Windows Server provides preview builds of Windows Server allowing you early access to learn, test, and help shape the future of Windows Server. To learn more, you can get started with the Windows Insider Program for Windows Server and participate in the Windows Server Insiders Community.

Next steps

To get started, find out more from these resources.

- What's new in Windows Server 2022 provides an overview of the latest features in Windows Server.
- Learn about the different servicing channels, which each is used for, and what it means for your workloads and support.
- Compare the differences in the editions in Windows Server 2022.
- Choose the right installation option based on whether you want the Desktop Experience or a minimal Core interface.
- Understand the hardware requirements to run Windows Server.
- Follow the learning path for Windows Server deployment, configuration, and administration.
- If you still need to use Windows Server 2008, Windows Server 2008 R2 (and in future Windows Server 2012, or Windows Server 2012 R2) Extended Security Updates are available to help keep you safe with security updates and bulletins rated critical and important.

What's new in Windows Server 2022

Article • 10/19/2023

> Applies to: Windows Server 2022

This article describes some of the new features in Windows Server 2022. Windows Server 2022 is built on the strong foundation of Windows Server 2019 and brings many innovations on three key themes: security, Azure hybrid integration and management, and application platform.

Azure Edition

Windows Server 2022 Datacenter: Azure Edition helps you use the benefits of cloud to keep your VMs up to date while minimizing downtime. This section describes some of the new features in Windows Server 2022 Datacenter: Azure Edition. Learn more about how Azure Automanage for Windows Server brings these new capabilities to Windows Server Azure Edition in the Azure Automanage for Windows Server services article.

Windows Server 2022 Datacenter: Azure Edition builds on Datacenter Edition to deliver a VM-only operating system that helps to use the benefits of cloud, with advanced features like SMB over QUIC, Hotpatch, and Azure Extended Networking. This section describes some of these new features.

Compare the differences in the editions in Windows Server 2022. You can also learn more about how Azure Automanage for Windows Server brings these new capabilities to Windows Server Azure Edition in the Azure Automanage for Windows Server services article.

April 2023

Hotpatching

Windows Server 2022 Datacenter: Azure Edition Hotpatching is now public preview for the Desktop Experience both in Azure and as a supported guest VM on Azure Stack HCI version 22H2.

September 2022

This section lists the features and improvements that are now available in Windows Server Datacenter: Azure Edition beginning with the 2022-09 Cumulative Update for Microsoft server operating system version 21H2 for x64-based Systems (KB5017381). After you've install the Cumulative Update, the OS build number will be 20348.1070 or higher.

Storage Replica compression for data transfer

This update includes Storage Replica compression for data transferred between the source and destination servers. This new functionality compresses the replication data at the source system, sent over the network and decompressed and saved on the destination. The compression results in fewer network packets to transfer the same amount of data, allowing for more throughput, and less network utilization. Higher data throughput should also result in lowering synchronization time for when you need it most, for example in a disaster recovery scenario.

New Storage Replica PowerShell parameters are available for existing commands, review the Windows PowerShell StorageReplica reference to learn more. For more information about Storage Replica, see the Storage Replica overview.

Support for Azure Stack HCI

With this release you can run Windows Server 2022 Datacenter: Azure Edition as a supported guest VM on Azure Stack HCI version 22H2. With Azure Edition running on Azure Stack HCI, you'll be able to use all the existing features including Hotpatch for Server Core and SMB over QUIC at your datacenter and edge locations.

Begin deploying Windows Server 2022 Datacenter: Azure Edition using the Azure Marketplace on Arc-enabled Azure Stack HCI or using an ISO. You can download the ISO from here:

- Windows Server 2022 Datacenter: Azure Edition (EN-US) ISO
- Windows Server 2022 Datacenter: Azure Edition (ZH-CN) ISO

Your Azure subscription permits you to use Windows Server Datacenter: Azure Edition on any virtual machine instances running on Azure Stack HCI. For more information, see your product terms Product Terms.

Learn more about the latest Azure Stack HCI features in our What's new in Azure Stack HCI, version 22H2 article.

Deploy from Azure Marketplace on Arc-enabled Azure Stack HCI (preview)

Windows Server 2022 Datacenter: Azure Edition images will be available in the Azure Marketplace for Arc-enabled Azure Stack HCI, making it easy to try, buy, and deploy using Azure certified images.

Learn more about the Azure Marketplace integration for Azure Arc-enabled Azure Stack HCI features in our What's new in Azure Stack HCI, version 22H2 article.

Azure Edition (initial release)

This section lists the features and improvements available in Windows Server Datacenter: Azure Edition with the release in September 2021.

Azure Automanage - Hotpatch

Hotpatching, part of Azure Automanage, is a new way to install updates on new Windows Server Azure Edition virtual machines (VMs) that doesn't require a reboot after installation. More information can be found at the Azure Automanage documentation.

SMB over QUIC

SMB over QUIC updates the SMB 3.1.1 protocol to use the QUIC protocol instead of TCP in Windows Server 2022 Datacenter: Azure Edition, Windows 11 and later, and third party clients if they support it. By using SMB over QUIC along with TLS 1.3, users and applications can securely and reliably access data from edge file servers running in Azure. Mobile and telecommuter users no longer need a VPN to access their file servers over SMB when on Windows. More information can be found at the SMB over QUIC documentation and SMB over QUIC management with Automanage machine best practices.

To learn more about QUIC, review RFC 9000.

Extended network for Azure

Azure Extended Network enables you to stretch an on-premises subnet into Azure to let on-premises virtual machines keep their original on-premises private IP addresses when migrating to Azure. To learn more, see Azure Extended Network.

All editions

This section describes some of the new features in Windows Server 2022 across all editions. To learn more about the different editions, review the Comparison of Standard, Datacenter, and Datacenter: Azure Edition editions of Windows Server 2022 article.

Security

The new security capabilities in Windows Server 2022 combine other security capabilities in Windows Server across multiple areas to provide defense-in-depth protection against advanced threats. Advanced multi-layer security in Windows Server 2022 provides the comprehensive protection that servers need today.

Secured-core server

Certified Secured-core server hardware from an OEM partner provides more security protections that are useful against sophisticated attacks. Certified Secured-core server hardware can provide increased assurance when handling mission critical data in some of the most data sensitive industries. A Secured-core server uses hardware, firmware, and driver capabilities to enable advanced Windows Server security features. Many of these features are available in Windows Secured-core PCs and are now also available with Secured-core server hardware and Windows Server 2022. For more information about Secured-core server, see Secured-core server.

Hardware root-of-trust

Used by features such as BitLocker drive encryption, Trusted Platform Module 2.0 (TPM 2.0) secure crypto-processor chips provide a secure, hardware-based store for sensitive cryptographic keys and data, including systems integrity measurements. TPM 2.0 can verify that the server has been started with legitimate code and can be trusted by subsequent code execution, known as a hardware root-of-trust.

Firmware protection

Firmware executes with high privileges and is often invisible to traditional anti-virus solutions, which has led to a rise in the number of firmware-based attacks. Secured-core servers measure and verify boot processes with Dynamic Root of Trust for Measurement (DRTM) technology. Secured-core servers can also isolate of driver access to memory with Direct Memory Access (DMA) protection.

UEFI secure boot

UEFI secure boot is a security standard that protects your servers from malicious rootkits. Secure boot ensures the server boots only firmware and software trusted by the hardware manufacturer. When the server is started, the firmware checks the signature of each boot component including firmware drivers and the OS. If the signatures are valid, the server boots and the firmware gives control to the OS.

Virtualization-based security (VBS)

Secured-core servers support virtualization-based security (VBS) and hypervisor-based code integrity (HVCI). VBS uses hardware virtualization features to create and isolate a secure region of memory from the normal operating system, protecting against an entire class of vulnerabilities used in cryptocurrency mining attacks. VBS also allows for the use of Credential Guard, where user credentials and secrets are stored in a virtual container that the operating system can't access directly.

HVCI uses VBS to significantly strengthen code integrity policy enforcement. Kernel mode integrity prevents unsigned kernel mode drivers or system files from being loaded into system memory.

Kernel Data Protection (KDP) provides read-only memory protection of kernel memory containing non-executable data where memory pages are protected by Hypervisor. KDP protects key structures in the Windows Defender System Guard runtime from being tampered.

Secure connectivity

Transport: HTTPS and TLS 1.3 enabled by default on Windows Server 2022

Secure connections are at the heart of today's interconnected systems. Transport Layer Security (TLS) 1.3 is the latest version of the internet's most deployed security protocol, which encrypts data to provide a secure communication channel between two endpoints. HTTPS and TLS 1.3 is now enabled by default on Windows Server 2022, protecting the data of clients connecting to the server. It eliminates obsolete cryptographic algorithms, enhances security over older versions, and aims to encrypt as much of the handshake as possible. Learn more about supported TLS versions and about supported cipher suites.

Although TLS 1.3 in the protocol layer is now enabled by default, applications and services also need to actively support it. The Microsoft Security blog has more detail in the post Taking Transport Layer Security (TLS) to the next level with TLS 1.3 .

Secure DNS: Encrypted DNS name resolution requests with DNS-over-HTTPS

DNS Client in Windows Server 2022 now supports DNS-over-HTTPS (DoH) which encrypts DNS queries using the HTTPS protocol. DoH helps keep your traffic as private as possible by preventing eavesdropping and your DNS data being manipulated. Learn more about configuring the DNS client to use DoH.

Server Message Block (SMB): SMB AES-256 encryption for the most security conscious

Windows Server now supports AES-256-GCM and AES-256-CCM cryptographic suites for SMB encryption. Windows will automatically negotiate more advanced cipher method when connecting to another computer that also supports it, and it can also be mandated through Group Policy. Windows Server still supports AES-128 for down-level compatibility. AES-128-GMAC signing now also accelerates signing performance.

SMB: East-West SMB encryption controls for internal cluster communications

Windows Server failover clusters now support granular control of encrypting and signing intra-node storage communications for Cluster Shared Volumes (CSV) and the storage bus layer (SBL). When using Storage Spaces Direct, you can now decide to encrypt or sign east-west communications within the cluster itself for higher security.

SMB Direct and RDMA encryption

SMB Direct and RDMA supply high bandwidth, low latency networking fabric for workloads like Storage Spaces Direct, Storage Replica, Hyper-V, Scale-out File Server, and SQL Server. SMB Direct in Windows Server 2022 now supports encryption. Previously, enabling SMB encryption disabled direct data placement; this was intentional, but seriously impacted performance. Now data is encrypted before data placement, leading to far less performance degradation while adding AES-128 and AES-256 protected packet privacy.

More information on SMB encryption, signing acceleration, secure RDMA, and cluster support can be found at SMB security enhancements.

Azure hybrid capabilities

You can increase your efficiency and agility with built-in hybrid capabilities in Windows Server 2022 that allow you to extend your data centers to Azure more easily than ever before.

Azure Arc enabled Windows Servers

Azure Arc enabled servers with Windows Server 2022 brings on-premises and multicloud Windows Servers to Azure with Azure Arc. This management experience is designed to be consistent with how you manage native Azure virtual machines. When a hybrid machine is connected to Azure, it becomes a connected machine and is treated as a resource in Azure. More information can be found at the Azure Arc enables servers documentation.

Add Windows Servers

As of the KB5031364 update, you can now add Windows Servers with an easy, simple process.

To add new Windows Servers, go to the Azure Arc icon in the bottom-right corner of the taskbar and launch the Azure Arc Setup program to install and configure an Azure Connected Machine Agent. Once installed, you can use the Azure Connected Machine Agent at no extra charge to your Azure account. Once you've enabled Azure Arc on your server, you can see the status information in the taskbar icon.

To learn more, see Connect Windows Server machines to Azure through Azure Arc Setup.

Windows Admin Center

Improvements to Windows Admin Center to manage Windows Server 2022 include capabilities to both report on the current state of the Secured-core features mentioned above, and where applicable, allow customers to enable the features. More information on these and many more improvements to Windows Admin Center can be found at the Windows Admin Center documentation.

Application platform

There are several platform improvements for Windows Containers, including application compatibility and the Windows Container experience with Kubernetes.

Some of the new features are:

- Reduced Windows Container image size by up to 40%, which leads to a 30% faster startup time and better performance.
- Applications can now use Azure Active Directory with group Managed Services Accounts (gMSA) without domain joining the container host. Windows Containers now also support Microsoft Distributed Transaction Control (MSDTC) and Microsoft Message Queuing (MSMQ).
- Simple buses can now be assigned to process-isolated Windows Server containers. Applications running in containers that need to talk over SPI, I2C, GPIO, and UART/COM are now able to do so.
- We've enabled support for hardware acceleration of DirectX APIs in Windows containers to support scenarios such as Machine Learning (ML) inference using local graphical processing unit (GPU) hardware. For more information, see the Bringing GPU acceleration to Windows containers blog post.
- There are several other enhancements that simplify the Windows Container experience with Kubernetes. These enhancements include support for host-process containers for node configuration, IPv6, and consistent network policy implementation with Calico.
- Windows Admin Center has been updated to make it easy to containerize .NET applications. Once the application is in a container, you can host it on Azure Container Registry to then deploy it to other Azure services, including Azure Kubernetes Service.
- With support for Intel Ice Lake processors, Windows Server 2022 supports business-critical and large-scale applications that require up to 48 TB of memory and 2,048 logical cores running on 64 physical sockets. Confidential computing with Intel Secured Guard Extension (SGX) on Intel Ice Lake improves application security by isolating applications from each other with protected memory.

To learn more about the new features, see What's new for Windows containers in Windows Server 2022.

Other key features

Remote Desktop IP virtualization

As of the KB5030216 update, you can now use Remote Desktop IP Virtualization.

Remote Desktop IP Virtualization simulates a single-user desktop by supporting per-session and per-program Remote Desktop IP Virtualization for Winsock applications. To learn more, see Remote Desktop IP Virtualization in Windows Server.

Task Scheduler and Hyper-V Manager for Server Core installations

We added two management tools to the App Compatibility Feature on Demand feature package in this version, Task Scheduler (taskschd.msc) and Hyper-V Manager (virtmgmt.msc). For more information, see Server Core App Compatibility Feature on Demand (FOD).

Nested virtualization for AMD processors

Nested virtualization is a feature that allows you to run Hyper-V inside of a Hyper-V virtual machine (VM). Windows Server 2022 brings support for nested virtualization using AMD processors, giving more choices of hardware for your environments. More information can be found at the nested virtualization documentation.

Microsoft Edge browser

Microsoft Edge is included with Windows Server 2022, replacing Internet Explorer. It's built on Chromium open source and backed by Microsoft security and innovation. It can be used with the Server with Desktop Experience installation options. More information can be found at the Microsoft Edge Enterprise documentation. Microsoft Edge, unlike the rest of Windows Server, follows the Modern Lifecycle for its support lifecycle. For details, see Microsoft Edge lifecycle documentation.

Networking performance

UDP performance improvements

UDP is becoming a popular protocol carrying more network traffic due to the increasing popularity of RTP and custom (UDP) streaming and gaming protocols. The QUIC protocol, built on top of UDP, brings the performance of UDP to a level on par with TCP. Significantly, Windows Server 2022 includes UDP Segmentation Offload (USO). USO moves most of the work required to send UDP packets from the CPU to the network adapter's specialized hardware. Complimenting USO is UDP Receive Side Coalescing (UDP RSC), which coalesces packets and reduces CPU usage for UDP processing. In addition, we have also made hundreds of improvements to the UDP data path both

transmit and receive. Windows Server 2022 and Windows 11 both have this new capability.

TCP performance improvements

Windows Server 2022 uses TCP HyStart++ to reduce packet loss during connection start-up (especially in high-speed networks) and RACK to reduce Retransmit TimeOuts (RTO). These features are enabled in the transport stack by default and provide a smoother network data flow with better performance at high speeds. Windows Server 2022 and Windows 11 both have this new capability.

Hyper-V virtual switch improvements

Virtual switches in Hyper-V have been enhanced with updated Receive Segment Coalescing (RSC). RSC allows the hypervisor network to coalesce packets and process as one larger segment. CPU cycles are reduced and segments will remain coalesced across the entire data path until processed by the intended application. RSC results in improved performance for both network traffic from an external host, received by a virtual NIC, and from a virtual NIC to another virtual NIC on the same host.

System Insights disk anomaly detection

System Insights has another capability via Windows Admin Center, 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 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 Windows 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 option with a Windows Recovery Environment partition.

Storage

Storage Migration Service

Enhancements to Storage Migration Service in Windows Server 2022 makes it easier to migrate storage to Windows Server or to Azure from more source locations. Here are the features that are available when running the Storage Migration Server orchestrator on Windows Server 2022:

- Migrate local users and groups to the new server.
- Migrate storage from failover clusters, migrate to failover clusters, and migrate between standalone servers and failover clusters.
- Migrate storage from a Linux server that uses Samba.
- More easily synchronize migrated shares into Azure by using Azure File Sync.
- Migrate to new networks such as Azure.
- Migrate NetApp CIFS servers from NetApp FAS arrays to Windows servers and clusters.

Adjustable storage repair speed

User adjustable storage repair speed is a new feature in Storage Spaces Direct that offers more control over the data resync process. Adjustable storage repair speed enables you to allocate resources to either repair data copies (resiliency) or to run active workloads (performance). Controlling the repair speed helps improve availability and allows you to service your clusters more flexibly and efficiently.

Faster repair and resynchronization

Storage repair and resynchronization after events such as node reboots and disk failures are now twice as fast. Repairs have less variance in time taken so you can be more sure of how long the repairs will take, which has been achieved through adding more granularity to data tracking. Repairs now only move the data that needs to be moved, reducing the system resources used and time taken.

Storage bus cache with Storage Spaces on standalone servers

Storage bus cache is now available for standalone servers. It can significantly improve read and write performance, while maintaining storage efficiency and keeping the operational costs low. Similar to its implementation for Storage Spaces Direct, this feature binds together faster media (for example, NVMe or SSD) with slower media (for

example, HDD) to create tiers. A portion of the faster media tier is reserved for the cache. To learn more, see Enable storage bus cache with Storage Spaces on standalone servers.

ReFS file-level snapshots

Microsoft's Resilient File System (ReFS) now includes the ability to snapshot files using a quick metadata operation. Snapshots are different than ReFS block cloning in that clones are writable, whereas snapshots are read-only. This functionality is especially useful in virtual machine backup scenarios with VHD/VHDX files. ReFS snapshots are unique in that they take a constant time irrespective of file size. Support for snapshots is available in ReFSUtil or as an API.

SMB compression

Enhancement to SMB in Windows Server 2022 and Windows 11 allows a user or application to compress files as they transfer over the network. Users no longer have to manually zip files in order to transfer much faster on slower or more congested networks. For details, see SMB Compression.

What's new in Windows Server 2019

Article • 12/14/2022

This article 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).

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 extra cost beyond Windows and is ready to use in production.

You can install Windows Admin Center on Windows Server 2019 and 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're 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. System Insights allows you to understand how your servers are functioning and helps you reduce the operational expenses associated with reactively managing issues in your Windows Server deployments.

Hybrid Cloud

Server Core App Compatibility Feature on Demand

Server Core App Compatibility Feature on Demand (FOD) significantly improves the app compatibility by including a subset of binaries and components from Windows Server with the Desktop Experience. Server Core is kept it as lean as possible by not adding the Windows Server Desktop Experience graphical environment itself, increasing the functionality and compatibility.

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.

Windows Deployment Services (WDS) Transport Server role added to Server Core

Transport Server contains only the core networking parts of WDS. You can now use Server Core with the Transport Server role to create multicast namespaces that transmit data (including operating system images) from a standalone server. You can also use it if you want to have a PXE server that allows clients to PXE boot and download your own custom setup application.

Remote Desktop Services integration with Azure AD

With Azure AD integration you can use Conditional Access policies, Multifactor Authentication, Integrated authentication with other SaaS Apps using Azure AD, and many more. For more information, see Integrate Azure AD Domain Services with your RDS deployment.

Networking

We made several improvements to the core network stack, such as TCP Fast Open (TFO), Receive Window Autotuning, IPv6, and more. For more information, see the Core Network Stack feature improvement post.

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 enabling you to balance security risk and productivity requirements. Windows Defender Exploit Guard is designed to lock down the device against a wide variety of attack vectors and block behaviors commonly used in malware attacks. The components are:

- Attack Surface Reduction (ASR) 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. We've made deployment easier by including default CI policies. The default policy allows all Windows in-box files and Microsoft applications, such as SQL Server, and blocks 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 using 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.

  Even if the HGS can't be reached, offline mode will allow you to continue to start up your shielded VMs. Offline mode will allow you to start your VMs as long as the VM has started successfully once, and the host's security configuration hasn't 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 useful if you've lost network connectivity to your VM and need to update its configuration to restore access.

  These features don't 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.

Data Deduplication

- **Data Deduplication now supports ReFS** You can now enable Data Deduplication wherever you can enable ReFS, increasing storage efficiency by up to 95% with ReFS.
- **DataPort API for optimized ingress/egress to deduplicated volumes** Developers can now take advantage of the knowledge Data Deduplication has about how to store data efficiently to move data between volumes, servers, and clusters efficiently.

File Server Resource Manager

It's now possible to prevent the File Server Resource Manager service from creating a change journal (also known as a USN journal) on all volumes when the service starts. Preventing the creation of the change journey can conserve space on each volume, but will disable real-time file classification. For more information, see File Server Resource Manager overview.

SMB

- **SMB1 and guest authentication removal** Windows Server no longer installs the SMB1 client and server by default. Additionally, the ability to authenticate as a guest in SMB2 and later is off by default. For more information, review SMBv1 isn't installed by default in Windows 10, version 1709 and Windows Server, version 1709.
- **SMB2/SMB3 security and compatibility** You now have the ability to disable oplocks in SMB2+ for legacy applications, and require signing or encryption on per-connection basis from a client. For more information, review the SMBShare PowerShell module help.

Storage Migration Service

Storage Migration Service is a new technology that makes it easier to migrate servers to a newer version of Windows Server. We've provided a graphical tool that inventories

data on servers, then transfers the data and configuration to newer servers. The Storage Migration Service will also optionally move the identities of the old servers to the new servers, so that apps and users don't need 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's now possible to run Windows and Linux-based containers on the same container host, using the same docker daemon. You can now have a heterogeneous container host environment 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. We've enhanced 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 more API dependencies, there's 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 to speed 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.

Compute improvements

- **VM Start Ordering** VM Start Ordering is also improved with OS and Application awareness, bringing enhanced triggers for when a VM is considered started before starting the next.

- **Storage-class memory support for VMs** enables NTFS-formatted direct access volumes to be created on non-volatile DIMMs and exposed to Hyper-V VMs. Hyper-V VMs can now use the low-latency performance benefits of storage-class memory devices.

- **Persistent Memory support for Hyper-V VMs** To use the high throughput and low latency of persistent memory (also known as storage class memory) in virtual machines, it can now be projected directly into VMs. Persistent memory can help to drastically reduce database transaction latency or reduce recovery times for low latency in-memory databases on failure.

- **Container storage – persistent data volumes** Application containers now have persistent access to volumes. For more info, see Container Storage Support with Cluster Shared Volumes (CSV), Storage Spaces Direct (S2D), SMB Global Mapping.

- **Virtual machine configuration file format (updated)** The VM guest state file (`.vmgs`) has been added for virtual machines with a configuration version of 8.2 and higher. The VM guest state file includes device state information that was previously part of the VM runtime state file.

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. Improved performance lowers the operations and maintenance cost while increasing the available density of your hosts. These new features are:

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

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. LEDBAT consumes bandwidth available while the network isn't in use. The technology is intended for use when 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.

Windows Subsystem for Linux (WSL)

WSL enables server administrators to use existing tools and scripts from Linux on Windows Server. Many improvements showcased in the command line blog are now part of Windows Server, including Background tasks, DriveFS, WSLPath, and much more.

What's new in Windows Server 2016

Article • 11/16/2022

This article describes some of the new features in Windows Server 2016 that are the ones most likely to have the greatest impact as you work with this release.

Compute

The Virtualization area includes virtualization products and features for the IT professional to design, deploy, and maintain Windows Server.

General

Physical and virtual machines benefit from greater time accuracy due to improvements in the Win32 Time and Hyper-V Time Synchronization Services. Windows Server can now host services that are compliant with upcoming regulations that require a 1ms accuracy with regard to UTC.

Hyper-V

- What's new in Hyper-V on Windows Server 2016. This topic explains the new and changed functionality of the Hyper-V role in Windows Server 2016, Client Hyper-V running on Windows 10, and Microsoft Hyper-V Server 2016.
- Windows Containers: Windows Server 2016 container support adds performance improvements, simplified network management, and support for Windows containers on Windows 10. For some additional information on containers, see Containers: Docker, Windows and Trends.

Nano Server

What's New in Nano Server. Nano Server now has an updated module for building Nano Server images, including more separation of physical host and guest virtual machine functionality as well as support for different Windows Server editions.

There are also improvements to the Recovery Console, including separation of inbound and outbound firewall rules as well as the ability to repair the configuration of WinRM.

Shielded Virtual Machines

Windows Server 2016 provides a new Hyper-V-based Shielded Virtual Machine to protect any Generation 2 virtual machine from a compromised fabric. Among the features introduced in Windows Server 2016 are the following:

- A new **Encryption Supported** mode that offers more protections than for an ordinary virtual machine, but less than **Shielded** mode, while still supporting vTPM, disk encryption, Live Migration traffic encryption, and other features, including direct fabric administration conveniences such as virtual machine console connections and PowerShell Direct.
- Full support for converting existing non-shielded Generation 2 virtual machines to shielded virtual machines, including automated disk encryption.
- Hyper-V Virtual Machine Manager can now view the fabrics upon which a shielded virtual is authorized to run, providing a way for the fabric administrator to open a shielded virtual machine's key protector (KP) and view the fabrics it is permitted to run on.
- You can switch Attestation modes on a running Host Guardian Service. Now you can switch on the fly between the less secure but simpler Active Directory-based attestation and TPM-based attestation.
- End-to-end diagnostics tooling based on Windows PowerShell that is able to detect misconfigurations or errors in both guarded Hyper-V hosts and the Host Guardian Service.
- A recovery environment that offers a means to securely troubleshoot and repair shielded virtual machines within the fabric in which they normally run while offering the same level of protection as the shielded virtual machine itself.
- Host Guardian Service support for existing safe Active Directory – you can direct the Host Guardian Service to use an existing Active Directory forest as its Active Directory instead of creating its own Active Directory instance

For more details and instructions for working with shielded virtual machines, see Guarded Fabric and Shielded VMs.

Identity and Access

New features in Identity improve the ability for organizations to secure Active Directory environments and help them migrate to cloud-only deployments and hybrid deployments, where some applications and services are hosted in the cloud and others are hosted on premises.

Active Directory Certificate Services

Active Directory Certificate Services (AD CS) in Windows Server 2016 increases support for TPM key attestation: You can now use Smart Card KSP for key attestation, and devices that are not joined to the domain can now use NDES enrollment to get certificates that can be attested for keys being in a TPM.

Active Directory Domain Services

Active Directory Domain Services includes improvements to help organizations secure Active Directory environments and provide better identity management experiences for both corporate and personal devices. For more information, see What's new in Active Directory Domain Services (AD DS) in Windows Server 2016.

Active Directory Federation Services

What's New in Active Directory Federation Services. Active Directory Federation Services (AD FS) in Windows Server 2016 includes new features that enable you to configure AD FS to authenticate users stored in Lightweight Directory Access Protocol (LDAP) directories. For more information, see What's New in AD FS for Windows Server 2016.

Web Application Proxy

The latest version of Web Application Proxy focuses on new features that enable publishing and pre-authentication for more applications and improved user experience. Check out the full list of new features that includes pre-authentication for rich client apps such as Exchange ActiveSync and wildcard domains for easier publishing of SharePoint apps. For more information, see Web Application Proxy in Windows Server 2016.

Administration

The Management and Automation area focuses on tool and reference information for IT pros who want to run and manage Windows Server 2016, including Windows PowerShell.

Windows PowerShell 5.1 includes significant new features, including support for developing with classes and new security features that extend its use, improve its usability, and allow you to control and manage Windows-based environments more easily and comprehensively. See New Scenarios and Features in WMF 5.1 for details.

New additions for Windows Server 2016 include: the ability to run PowerShell.exe locally on Nano Server (no longer remote only), new Local Users & Groups cmdlets to replace the GUI, added PowerShell debugging support, and added support in Nano Server for security logging & transcription and JEA.

Here are some other new administration features:

PowerShell Desired State Configuration (DSC) in Windows Management Framework (WMF) 5

Windows Management Framework 5 includes updates to Windows PowerShell Desired State Configuration (DSC), Windows Remote Management (WinRM), and Windows Management Instrumentation (WMI).

For more info about testing the DSC features of Windows Management Framework 5, see the series of blog posts discussed in Validate features of PowerShell DSC. To download, see Windows Management Framework 5.1.

PackageManagement unified package management for software discovery, installation, and inventory

Windows Server 2016 and Windows 10 includes a new PackageManagement feature (formerly called OneGet) that enables IT Professionals or DevOps to automate software discovery, installation, and inventory (SDII), locally or remotely, no matter what the installer technology is and where the software is located.

For more info, see https://github.com/OneGet/oneget/wiki.

PowerShell enhancements to assist digital forensics and help reduce security breaches

To help the team responsible for investigating compromised systems - sometimes known as the "blue team" - we've added additional PowerShell logging and other digital forensics functionality, and we've added functionality to help reduce vulnerabilities in scripts, such as constrained PowerShell, and secure CodeGeneration APIs.

For more info, see the PowerShell ♥ the Blue Team blog post.

Networking

The Networking area addresses networking products and features for the IT professional to design, deploy, and maintain Windows Server 2016.

Software-Defined Networking

You can now both mirror and route traffic to new or existing virtual appliances. Together with a distributed firewall and Network security groups, this enables you to dynamically segment and secure workloads in a manner similar to Azure. Second, you can deploy and manage the entire Software-defined networking (SDN) stack using System Center Virtual Machine Manager. Finally, you can use Docker to manage Windows Server container networking, and associate SDN policies not only with virtual machines but containers as well. For more information, see Plan a Software Defined Network Infrastructure.

TCP performance improvements

The default Initial Congestion Window (ICW) has been increased from 4 to 10 and TCP Fast Open (TFO) has been implemented. TFO reduces the amount of time required to establish a TCP connection and the increased ICW allows larger objects to be transferred in the initial burst. This combination can significantly reduce the time required to transfer an Internet object between the client and the cloud.

In order to improve TCP behavior when recovering from packet loss we have implemented TCP Tail Loss Probe (TLP) and Recent Acknowledgment (RACK). TLP helps convert Retransmit TimeOuts (RTOs) to Fast Recoveries and RACK reduces the time required for Fast Recovery to retransmit a lost packet.

Security and Assurance

The Security and Assurance area Includes security solutions and features for the IT professional to deploy in your data center and cloud environment. For information about security in Windows Server 2016 generally, see Security and Assurance.

Just Enough Administration

Just Enough Administration in Windows Server 2016 is security technology that enables delegated administration for anything that can be managed with Windows PowerShell. Capabilities include support for running under a network identity, connecting over PowerShell Direct, securely copying files to or from JEA endpoints, and configuring the

PowerShell console to launch in a JEA context by default. For more details, see JEA on GitHub.

Credential Guard

Credential Guard uses virtualization-based security to isolate secrets so that only privileged system software can access them. See Protect derived domain credentials with Credential Guard.

Remote Credential Guard

Credential Guard includes support for RDP sessions so that the user credentials remain on the client side and are not exposed on the server side. This also provides Single Sign On for Remote Desktop. See Protect derived domain credentials with Windows Defender Credential Guard.

Device Guard (Code Integrity)

Device Guard provides kernel mode code integrity (KMCI) and user mode code integrity (UMCI) by creating policies that specify what code can run on the server. See Introduction to Windows Defender Device Guard: virtualization-based security and code integrity policies.

Windows Defender

Windows Defender Overview for Windows Server 2016. Windows Server Antimalware is installed and enabled by default in Windows Server 2016, but the user interface for Windows Server Antimalware is not installed. However, Windows Server Antimalware will update antimalware definitions and protect the computer without the user interface. If you need the user interface for Windows Server Antimalware, you can install it after the operating system installation by using the Add Roles and Features Wizard.

Control Flow Guard

Control Flow Guard (CFG) is a platform security feature that was created to combat memory corruption vulnerabilities. See Control Flow Guard for more information.

Storage

Storage in Windows Server 2016 includes new features and enhancements for software-defined storage, as well as for traditional file servers. Below are a few of the new features, for more enhancements and further details, see What's New in Storage in Windows Server 2016.

Storage Spaces Direct

Storage Spaces Direct enables building highly available and scalable storage using servers with local storage. It simplifies the deployment and management of software-defined storage systems and unlocks use of new classes of disk devices, such as SATA SSD and NVMe disk devices, that were previously not possible with clustered Storage Spaces with shared disks.

For more info, see Storage Spaces Direct.

Storage Replica

Storage Replica enables storage-agnostic, block-level, synchronous replication between servers or clusters for disaster recovery, as well as stretching of a failover cluster between sites. Synchronous replication enables mirroring of data in physical sites with crash-consistent volumes to ensure zero data loss at the file-system level. Asynchronous replication allows site extension beyond metropolitan ranges with the possibility of data loss.

For more info, see Storage Replica.

Storage Quality of Service (QoS)

You can now use storage quality of service (QoS) to centrally monitor end-to-end storage performance and create management policies using Hyper-V and CSV clusters in Windows Server 2016.

For more info, see Storage Quality of Service.

Failover Clustering

Windows Server 2016 includes a number of new features and enhancements for multiple servers that are grouped together into a single fault-tolerant cluster using the Failover Clustering feature. Some of the additions are listed below; for a more complete listing, see What's New in Failover Clustering in Windows Server 2016.

Cluster Operating System Rolling Upgrade

Cluster Operating System Rolling Upgrade enables an administrator to upgrade the operating system of the cluster nodes from Windows Server 2012 R2 to Windows Server 2016 without stopping the Hyper-V or the Scale-Out File Server workloads. Using this feature, the downtime penalties against Service Level Agreements (SLA) can be avoided.

For more info, see Cluster Operating System Rolling Upgrade.

Cloud Witness

Cloud Witness is a new type of Failover Cluster quorum witness in Windows Server 2016 that leverages Microsoft Azure as the arbitration point. The Cloud Witness, like any other quorum witness, gets a vote and can participate in the quorum calculations. You can configure cloud witness as a quorum witness using the Configure a Cluster Quorum Wizard.

For more info, see Deploy Cloud Witness.

Health Service

The Health Service improves the day-to-day monitoring, operations, and maintenance experience of cluster resources on a Storage Spaces Direct cluster.

For more info, see Health Service.

Application development

Internet Information Services (IIS) 10.0

New features provided by the IIS 10.0 web server in Windows Server 2016 include:

- Support for the HTTP/2 protocol in the Networking stack and integrated with IIS 10.0, allowing IIS 10.0 websites to automatically serve HTTP/2 requests for supported configurations. This allows numerous enhancements over HTTP/1.1 such as more efficient reuse of connections and decreased latency, improving load times for web pages.
- Ability to run and manage IIS 10.0 in Nano Server. See IIS on Nano Server.
- Support for Wildcard Host Headers, enabling administrators to set up a web server for a domain and then have the web server serve requests for any subdomain.
- A new PowerShell module (IISAdministration) for managing IIS.

For more details see IIS.

Distributed Transaction Coordinator (MSDTC)

Three new features are added in Microsoft Windows 10 and Windows Server 2016:

- A new interface for Resource Manager Rejoin can be used by a resource manager to determine the outcome of an in-doubt transaction after a database restarts due to an error. See IResourceManagerRejoinable::Rejoin for details.
- The DSN name limit is enlarged from 256 bytes to 3072 bytes. See IDtcToXaHelperFactory::Create, IDtcToXaHelperSinglePipe::XARMCreate, or IDtcToXaMapper::RequestNewResourceManager for details.
- Improved tracing allowing you to set a registry key to include an image file path in the trace log file name so you can tell which trace log file to check. See How to enable diagnostic tracing for MS DTC on a Windows-based computer for details on configuring tracing for MSDTC.

Windows Server servicing channels

Article • 10/02/2023

Beginning in September 2023 Windows Server has two primary release channels available, the Long-Term Servicing Channel and the Annual Channel. The Long-Term Servicing Channel (LTSC) provides a longer term option focuses on providing a traditional lifecycle of quality and security updates, whereas the Annual Channel (AC) provides more frequent releases. The more frequent releases of the AC enable you to take advantage of innovation more quickly with focus on containers and microservices.

Long-Term Servicing Channel (LTSC)

With the Long-Term Servicing Channel, a new major version of Windows Server is typically released every 2-3 years. Users are entitled to five years of mainstream support and five years of extended support. This channel provides systems with a long servicing option and consistency, and can be installed with Server Core or Server with Desktop Experience installation options.

Annual Channel (AC)

Windows Server Annual Channel for Containers is an operating system to host Windows Server containers. The Annual Channel enables customers who are innovating quickly to take advantage of new operating system capabilities at a faster pace, focused on containers and microservices. To learn more about Windows Server Annual Channel for Containers, see our TechCommunity announcement.

Each release in this channel is supported for 24 months from the initial release. This channel can only be installed with the Server Core installation option. The Annual Channel is available to volume-licensed customers with Software Assurance and loyalty programs such as Visual Studio Subscriptions.

An Annual Channel release isn't an update, it's the next Windows Server release in the Annual Channel. To move to an Annual Channel release you must perform a clean installation.

Releases of Windows Server in the Annual Channel typically occur every 12 months. The 24 month support lifecycle for each release is 18 months of mainstream support, plus 6 months of extended support. To learn more about the lifecycle, see Windows Server 2022 lifecycle. Each release is named based on the release cycle; for example, **version 23H2** is a release in the second half of the year 2023.

Key differences

The following table summarizes the key differences between the channels:

Description	Long-Term Servicing Channel	Annual Channel
Recommended scenarios	General purpose file servers, Microsoft and non-Microsoft workloads, traditional apps, infrastructure roles, software-defined Datacenter, and hyper-converged infrastructure	Containerized applications running on container hosts benefiting from faster innovation
New releases	Typically 2–3 years	Typically 12 months
Support	5 years of mainstream support, plus 5 years of extended support	18 months of mainstream support, plus 6 months of extended support
Activation	All Windows Server activation keys	Windows Server Datacenter activation keys
Licensing	All licensing programs	Software Assurance customers only
Get media	All distribution channels	Volume Licensing Service Center (VLSC) and Visual Studio Subscriptions only
Installation options	Server Core and Server with Desktop Experience	Server Core for a container host only

Device compatibility

The minimum hardware requirements to run the Annual Channel releases are the same as the most recent Long-Term Servicing Channel release of Windows Server. Most hardware drivers continue to function in these releases.

Servicing

Both the Long-Term Servicing Channel and the Annual Channel releases are supported with security updates and nonsecurity updates up to the dates listed in the Microsoft Lifecycle pages. The difference is the length of time that the release is supported, as described in the Annual Channel (AC) section of this article.

Servicing tools

There are many tools with which you 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 Server and Windows client updates and is natively available in the Windows Server operating system. You can defer updates, add an approval layer, and choose to deploy them to specific computers or groups of computers whenever ready.
- **Microsoft Endpoint Configuration Manager** provides the greatest control over servicing. You can defer updates, approve them, and have multiple options for targeting deployments and managing bandwidth usage and deployment times.

You can continue using the same process for Annual Channel Releases; for example, if you already use Configuration Manager to manage updates, you can continue to use it. Similarly, if you're using WSUS, you can continue to use that.

Where to get Annual Channel

You can obtain Annual Channel releases from the following places:

- Volume Licensing Service Center (VLSC): Volume-licensed customers with Software Assurance can obtain this release by going to the Volume Licensing Service Center and select **Sign In**. Finally, select **Downloads and Keys**, search for Annual Channel, then download the media.

- Visual Studio Subscriptions: Visual Studio Subscribers can obtain Annual Channel releases by downloading them from the Visual Studio Subscriber download page. If you aren't already a subscriber, go to Visual Studio Subscriptions to sign up, and then visit the Visual Studio Subscriber downloads page. Releases obtained through Visual Studio Subscriptions are for development and testing only.

Activating Annual Channel releases

You need to activate your installation using your activation keys obtained from the VLSC. If you're using KMS, Annual Channel releases use the same CSVLK of the last LTSC release before their release. For example, an Annual Channel released with or after

Windows Server 2022 would use the Windows Server 2022 CSVLK. For more information, see KMS client setup keys.

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

Long-Term Servicing Channel releases could be released at the same time as a new version of the Annual Channel. To determine whether a server is running Annual Channel release, you must look at the operating system version. The product name doesn't reflect the servicing channel. To determine whether a server is running an LTSC or AC release, you can run the Get-ComputerInfo PowerShell command. The following example is a computer running Windows Server 2022 Datacenter Edition (LTSC).

To determine the operating system version, run the following command:

PowerShell

```
Get-ComputerInfo  | fl WindowsProductName,OSDisplayVersion
```

Here's an example output from a computer running Windows Server LTSC.

Output

```
WindowsProductName : Windows Server 2022 Datacenter
OSDisplayVersion   : 21H2
```

Here's an example output from a computer running Windows Server Annual Channel for Containers.

Output

```
WindowsProductName : Windows Server 2022 Datacenter
OSDisplayVersion   : 23H2
```

Tip

`OSDisplayVersion` only applies to Windows Server 2022 and later. Annual Channel releases do not apply to Windows Server 2019 and earlier. If you're running Windows Server 2019 or earlier, you're running an LTSC release.

The following table lists the Windows Server LTSC and AC releases and their corresponding operating system versions.

Channel	Operating system display version
LTSC	21H2
Annual Channel	23H2

The guidance is intended to help identify and differentiate between LTSC and AC for lifecycle and general inventory purposes only. It isn't 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. To learn more about using programmatically determining the version, see Operating System Version.

What is Azure Edition for Windows Server?

Article • 07/18/2023

Windows Server Datacenter: Azure Edition is an edition of Windows Server focused on innovation and virtualization optimized to run on Azure. Azure Edition features a Long-Term Servicing Channel (LTSC) and yearly product updates, with two major product updates in the first 3 years. Azure Edition also brings new functionality to Windows Server users faster than the Standard and Datacenter editions of Windows Server.

The annual Azure Edition updates are delivered using Windows Update, rather than a full OS upgrade. As part of this annual update cadence, the Azure Edition Insider preview program gives the opportunity to access early builds - leading to general availability. To get started with Azure Edition Insider preview, visit the Azure Edition preview Azure Marketplace offer. Details regarding each preview is shared in release announcements posted to the Windows Server Insiders space on Microsoft Tech Community.

Key differences

The following table summarizes the key differences:

Description	Windows Server Standard, Datacenter	Windows Server Datacenter: Azure Edition
New releases	Typically 2-3 years	Typically 2-3 years
Product updates	With new release	Yearly, with two major updates in the first 3 years
Support	5 years of mainstream support, plus 5 years of extended support	5 years of mainstream support, plus 5 years of extended support
Servicing channels	Long-Term Servicing Channel	Long-Term Servicing Channel
Who can use it?	All customers through all channels	Software Assurance, Windows Server subscription and cloud customers only
Installation options	Server Core, Server with Desktop Experience, Nano Server container image	Server Core and Server with Desktop Experience only. Windows Server containers aren't supported.

Description	Windows Server Standard, Datacenter	Windows Server Datacenter: Azure Edition
Operating system environments (OSE)	Physical or virtual	Virtual only
Associated virtualization rights	2 virtual OSEs for Standard, Unlimited virtual OSEs for Datacenter	None

Capabilities vary by image, see Getting started with Windows Server Datacenter: Azure Edition for more detail.

> **Tip**
>
> For more information, see the **Microsoft Software Licensing Terms**. The licensing terms may vary based on the distribution channel, for example, a Commercial Licensing program, Retail, Original Equipment Manufacturer (OEM), and so on.

Key capabilities

Hotpatch

Beginning with Windows Server 2022 Datacenter: Azure Edition, Hotpatch gives you the ability to apply security updates on your VM without rebooting. When used with Azure, Azure Guest Patching Service, along with Automanage for Window Server, automate the onboarding, configuration, and orchestration of hotpatching. To learn more, see Hotpatch for new virtual machines.

Supported platforms

Hotpatch is supported on the following operating systems for VMs running on Azure and Azure Stack HCI:

- Windows Server 2022 Datacenter: Azure Edition Core
- Windows Server 2022 Datacenter: Azure Edition with Desktop Experience

> **Note**
>
> Hotpatch isn't supported on Windows Server containers base images.

SMB over QUIC

Beginning with Windows Server 2022 Datacenter: Azure Edition, SMB over QUIC offers an "SMB VPN" for telecommuters, mobile device users, and branch offices. SMB over QUIC provides secure, reliable connectivity to edge file servers over untrusted networks like the Internet. QUIC is an IETF-standardized protocol used in HTTP/3, designed for maximum data protection with TLS 1.3 and requires encryption that can't be disabled. SMB behaves normally within the QUIC tunnel, meaning the user experience doesn't change. SMB features like multichannel, signing, compression, continuous availability, and directory leasing work normally.

SMB over QUIC is also integrated with Azure Automanage machine best practices for Windows Server to help make SMB over QUIC management easier. QUIC uses certificates to provide its encryption and organizations often struggle to maintain complex public key infrastructures. Azure Automanage machine best practices ensure that certificates don't expire without warning and that SMB over QUIC stays enabled for maximum continuity of service.

To learn more, see SMB over QUIC and SMB over QUIC management with Automanage machine best practices.

Storage Replica compression for data transfer

Beginning with Update 1 for Windows Server 2022 Datacenter: Azure Edition, you can compress Storage Replica data between source and destination server. The compression results in fewer network packets to transfer the same amount of data, allowing for more throughput, and less network utilization. Higher data throughput should also result in lowering synchronization time for when you need it most, for example in a disaster recovery scenario.

To learn more about Storage Replica features, see Storage Replica features

Extended network for Azure

Beginning with Windows Server 2022 Datacenter: Azure Edition, Azure Extended Network enables you to stretch an on-premises subnet into Azure to let on-premises virtual machines keep their original on-premises private IP addresses when migrating to Azure. To learn more, see
Azure Extended Network.

Get started with Windows Server Datacenter: Azure Edition

To get started using Azure Edition, use your preferred method to create an Azure or Azure Stack HCI VM, and select the *Windows Server Datacenter: Azure Edition* image that you would like to use.

> **Important**
>
> Some capabilities have specific configuration steps to perform during VM creation, and some capabilities that are in preview have specific opt-in and portal viewing requirements. See the individual capability topics to learn more about using that capability with your VM.

To learn more about creating virtual machine using Azure or Azure Stack HCI, see Create a Windows virtual machine in the Azure portal and Deploy Windows Server Azure Edition VMs in Azure Stack HCI.

Next steps

- Comparison of Standard, Datacenter, and Datacenter: Azure Edition editions of Windows Server 2022
- Hotpatch for new virtual machines
- Enable Hotpatch for Azure Edition virtual machines built from ISO (preview)
- SMB over QUIC
- Extend your on-premises subnets into Azure using extended network for Azure

Comparison of Standard, Datacenter, and Datacenter: Azure Edition editions of Windows Server 2022

Article • 10/18/2022

Use this article to compare Standard, Datacenter, and Datacenter: Azure Edition editions of Windows Server 2022 to see which will be most appropriate.

Features generally available

Full Comparison

Features available generally	Windows Server 2022 Standard	Windows Server 2022 Datacenter	Windows Server 2022 Datacenter: Azure Edition
Azure Extended Network	No	No	**Yes**
Best Practices Analyzer	Yes	Yes	Yes
Containers	Yes	Yes	Yes
Direct Access	Yes	Yes	Yes
Dynamic Memory (in virtualization)	Yes	Yes	Yes
Hot Add/Replace RAM	Yes	Yes	Yes
Hotpatching	No	No	**Yes**
Microsoft Management Console	Yes	Yes	Yes
Minimal Server Interface	Yes	Yes	Yes
Network Load Balancing	Yes	Yes	Yes

Features available generally	Windows Server 2022 Standard	Windows Server 2022 Datacenter	Windows Server 2022 Datacenter: Azure Edition
Windows PowerShell	Yes	Yes	Yes
Server Core installation option	Yes	Yes	Yes
Server Manager	Yes	Yes	Yes
SMB Direct and SMB over RDMA	Yes	Yes	Yes (not supported in Azure)
SMB Compression	Yes	Yes	Yes
SMB over QUIC	No	No	**Yes**
Software-defined Networking	No	**Yes**	**Yes**
Storage Migration Service	Yes	Yes	Yes
Storage Replica	Yes, (1 partnership and 1 resource group with a single 2TB volume)	Yes, **unlimited**	Yes, **unlimited**
Storage Replica Compression	No	No	**Yes**
Storage Spaces	Yes	Yes	Yes
Storage Spaces Direct	No	**Yes**	**Yes**
Volume Activation Services	Yes	Yes	Yes, (Cannot Configure as a KMS host)
VSS (Volume Shadow Copy Service) integration	Yes	Yes	Yes
Windows Server Update Services	Yes	Yes	Yes
Server license logging	Yes	Yes	Yes
Inherited activation	As guest if hosted on Datacenter	**Can be a host or a guest**	**Can be a host or a guest**

Features available generally	Windows Server 2022 Standard	Windows Server 2022 Datacenter	Windows Server 2022 Datacenter: Azure Edition
Work Folders	Yes	Yes	Yes

Locks and Limits

Full Comparison

Locks and Limits	Windows Server 2022 Standard	Windows Server 2022 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	48 TB	48 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
Windows Server Containers	Unlimited	Unlimited
Virtual OSE/Hyper-V isolated Containers	2	Unlimited
Server can join a domain	Yes	Yes

Locks and Limits	Windows Server 2022 Standard	Windows Server 2022 Datacenter
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

Full Comparison

Windows Server roles available	Role services	Windows Server 2022 Standard	Windows Server 2022 Datacenter
Active Directory Certificate Services		Yes	Yes
Active Directory Domain Services		Yes	Yes
Active Directory Federation Services		Yes	Yes
Active Directory Lightweight Directory Services		Yes	Yes
Active Directory 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

Windows Server roles available	Role services	Windows Server 2022 Standard	Windows Server 2022 Datacenter
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**
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

Windows Server roles available	Role services	Windows Server 2022 Standard	Windows Server 2022 Datacenter
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 Update Services		Yes	Yes

Features

Full Comparison

Windows Server Features available	Windows Server 2022 Standard	Windows Server 2022 Datacenter
.NET Framework 3.5	Yes	Yes
.NET Framework 4.8	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	Yes
Data Center Bridging	Yes	Yes
Direct Play	Yes, when installed as Server	Yes, when installed as Server

Windows Server Features available	Windows Server 2022 Standard	Windows Server 2022 Datacenter
	with Desktop Experience	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
IP Address Management (IPAM) Server	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
Microsoft Defender Antivirus	Yes	Yes
Multipath I/O	Yes	Yes
MultiPoint Connector	Yes	Yes
Network Load Balancing	Yes	Yes
Network Virtualization	Yes	Yes
Peer Name Resolution Protocol	Yes	Yes
Quality Windows Audio Video Experience	Yes	Yes
RAS Connection Manager Administration Kit (CMAK)	Yes, when installed as Server with Desktop Experience	Yes, when installed as Server with Desktop Experience

Windows Server Features available	Windows Server 2022 Standard	Windows Server 2022 Datacenter
Remote Assistance	Yes, when installed as Server with Desktop Experience	Yes, when installed as Server with Desktop Experience
Remote Differential Compression	Yes	Yes
Remote Server Administration Tools (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	Yes	Yes
SMB Bandwidth Limit	Yes	Yes
SMTP Server	Yes	Yes
SNMP Service	Yes	Yes
Software Load Balancer	Yes	Yes
Storage Migration Service	Yes	Yes
Storage Migration Service Proxy	Yes	Yes
Storage Replica	Yes	Yes
System Data Archiver	Yes	Yes
System Insights	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 Server Features available	Windows Server 2022 Standard	Windows Server 2022 Datacenter
Windows Biometric Framework	Yes, when installed as Server with Desktop Experience	Yes, when installed as Server with Desktop Experience
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	Yes	Yes
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 Migration Tools	Yes	Yes
Windows Standards-Based Storage Management	Yes	Yes
Windows Subsystem for Linux	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	Yes	Yes
XPS Viewer	Yes, installed with Server with Desktop Experience	Yes, installed with Server with Desktop Experience

Comparison of Standard and Datacenter editions of Windows Server 2019

Article • 09/19/2022

Use this article to compare Standard and Datacenter editions of Windows Server 2019 to see which will be most appropriate.

Features generally available

Full Comparison

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

Features available generally	Windows Server 2019 Standard	Windows Server 2019 Datacenter
Storage Replica	Yes, (1 partnership and 1 resource group with a single 2TB volume)	Yes, **unlimited**
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
Server license logging	Yes	Yes
Inherited activation	As guest if hosted on Datacenter	**Can be a host or a guest**
Work Folders	Yes	Yes

Locks and Limits

Full Comparison

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

Locks and Limits	Windows Server 2019 Standard	Windows Server 2019 Datacenter
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

Full Comparison

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
Active Directory Federation Services		Yes	Yes
Active Directory Lightweight Directory Services		Yes	Yes

Windows Server roles available	Role services	Windows Server 2019 Standard	Windows Server 2019 Datacenter
Active Directory 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

Windows Server roles available	Role services	Windows Server 2019 Standard	Windows Server 2019 Datacenter
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**
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 Update Services		Yes	Yes

> **Note**
>
> WDS Transport Server is new to Server Core installations in Windows Server 2019 and also included in the Semi-Annual Channel starting with Windows Server version 1803.

Features

Full Comparison

Windows Server Features available	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
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
IP Address Management (IPAM) Server	Yes	Yes

Windows Server Features available	Windows Server 2019 Standard	Windows Server 2019 Datacenter
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 (CMAK)	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
Remote Server Administration Tools (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

Windows Server Features available	Windows Server 2019 Standard	Windows Server 2019 Datacenter
SMB 1.0/CIFS File Sharing Support	Yes	Yes
SMB Bandwidth Limit	Yes	Yes
SMTP Server	Yes	Yes
SNMP Service	Yes	Yes
Software Load Balancer	Yes	Yes
Storage Migration Service	Yes	Yes
Storage Migration Service Proxy	Yes	Yes
Storage Replica	Yes	Yes
System Data Archiver	Yes	Yes
System Insights	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 Antivirus	Yes	Yes
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	Yes	Yes

Windows Server Features available	Windows Server 2019 Standard	Windows Server 2019 Datacenter
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 Migration Tools	Yes	Yes
Windows Standards-Based Storage Management	Yes	Yes
Windows Subsystem for Linux	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	Yes	Yes
XPS Viewer	Yes, when installed as Server with Desktop Experience	Yes, when installed as Server with Desktop Experience

Comparison of Standard and Datacenter editions of Windows Server 2016

Article • 09/19/2022

Use this article to compare Standard and Datacenter editions of Windows Server 2016 to see which will be most appropriate.

Features generally available

Full Comparison

Features available generally	Windows Server 2016 Standard	Windows Server 2016 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
Nano Server installation option	Yes	Yes
Server Manager	Yes	Yes
SMB Direct and SMB over RDMA	Yes	Yes
Software-defined Networking	No	**Yes**
Storage Replica	No	**Yes**
Storage Spaces	Yes	Yes
Storage Spaces Direct	No	**Yes**

Features available generally	Windows Server 2016 Standard	Windows Server 2016 Datacenter
Volume Activation Services	Yes	Yes
VSS (Volume Shadow Copy Service) integration	Yes	Yes
Windows Server Update Services	Yes	Yes
Server license logging	Yes	Yes
Inherited activation	As guest if hosted on Datacenter	**Can be host or guest**
Work Folders	Yes	Yes

Locks and Limits

Full Comparison

Locks and Limits	Windows Server 2016 Standard	Windows Server 2016 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	65535	65535
Maximum number of 64-bit sockets	64	64
Maximum number of cores	unlimited	unlimited
Maximum RAM	24 TB	24 TB

Locks and Limits	Windows Server 2016 Standard	Windows Server 2016 Datacenter
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

Full Comparison

Windows Server roles available	Role services	Windows Server 2016 Standard	Windows Server 2016 Datacenter
Active Directory Certificate Services		Yes	Yes
Active Directory Domain Services		Yes	Yes
Active Directory Federation Services		Yes	Yes
Active Directory Lightweight Directory Services		Yes	Yes
Active Directory Rights Management Services		Yes	Yes
Device Health Attestation		Yes	Yes
DHCP Server		Yes	Yes

Windows Server roles available	Role services	Windows Server 2016 Standard	Windows Server 2016 Datacenter
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**

Windows Server roles available	Role services	Windows Server 2016 Standard	Windows Server 2016 Datacenter
MultiPoint Services		Yes	Yes
Network Controller		No	**Yes**
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, when installed as Server with Desktop Experience	Yes, when installed as Server with Desktop Experience
Windows Server Essentials Experience		Yes	Yes
Windows Server Update Services		Yes	Yes

Features

Full Comparison

Windows Server Features available	Windows Server 2016 Standard	Windows Server 2016 Datacenter
.NET Framework 3.5	Yes	Yes
.NET Framework 4.6	Yes	Yes
Background Intelligent Transfer Service (BITS)	Yes	Yes

Windows Server Features available	Windows Server 2016 Standard	Windows Server 2016 Datacenter
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 (Windows containers unlimited; Hyper-V containers up to 2)	Yes (all container types unlimited)
Data Center Bridging	Yes	Yes
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

Windows Server Features available	Windows Server 2016 Standard	Windows Server 2016 Datacenter
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
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	Yes	Yes
SMB Bandwidth Limit	Yes	Yes
SMTP Server	Yes	Yes
SNMP Service	Yes	Yes
Software Load Balancer	No	**Yes**
Storage Replica	No	Yes
Telnet Client	Yes	Yes
TFTP Client	Yes, when installed as Server with Desktop Experience	Yes, when installed as Server with Desktop Experience

Windows Server Features available	Windows Server 2016 Standard	Windows Server 2016 Datacenter
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	Yes	Yes
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	Yes	Yes
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 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	Yes	Yes
XPS Viewer	Yes, when installed as Server with Desktop Experience	Yes, when installed as Server with Desktop Experience

Hardware requirements for Windows Server

Article • 12/23/2021

This article outlines the minimum hardware requirements to run Windows Server. 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 hardware requirements apply to all installation options (Server Core and Server with Desktop Experience) and both Standard and Datacenter editions.

> **ⓘ Important**
>
> The highly diverse scope of potential deployments makes it unrealistic to state recommended hardware 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 hardware 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, part of Windows Sysinternals, 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 on which you intend to install this release. 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 addition 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 the keyboard combination `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:\). Then close the command prompt and proceed with Setup.

Storage controller and disk space requirements

Computers that run Windows Server 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 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 2022 using the Server Core installation option, with the Web Services (IIS) server role. A server in Server Core mode is about 4 GB smaller than the same server using the Server with Desktop Experience installation option.
>
> 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 1 gigabit per second 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 only required 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 required 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.

Features removed or no longer developed starting with Windows Server 2022

Article • 11/07/2023

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 2022.

> **Tip**
>
> - You can get early access to Windows Server builds by joining the **Windows Insider Program for Business** - this is a great way to test feature changes.

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

Semi-Annual Channel

As part of our customer-centric approach, we'll move to the Long-Term Servicing Channel (LTSC) as our primary release channel. Current Semi-Annual Channel (SAC) releases will continue through their mainstream support end dates, which are May 10, 2022 for Windows Server version 20H2 and December 14, 2021 for Windows Server version 2004

The focus on container and microservice innovation previously released in the Semi-Annual Channel will now continue with Azure Kubernetes Service (AKS), AKS on Azure Stack HCI, and other platform improvements made in collaboration with the Kubernetes community. And with the Long-Term Servicing Channel, a major new version of Windows Server will be released every 2-3 years, so customers can expect both container host and container images to align with that cadence.

Features we've removed in this release

We're removing the following features and functionalities from the installed product image in Windows Server 2022. Applications or code that depend on these features

won't function in this release unless you use an alternate method.

Feature	Explanation
Internet Storage Name Service (iSNS) Server service	The iSNS Server service has now been removed from Windows Server 2022 after it was considered for removal in Windows Server, version 1709. You can still connect to iSNS servers or add iSCSI targets individually.

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.

Feature	Explanation
Computer Browser	The Computer Browser driver and service are deprecated. The browser (browser protocol and service) is a dated and insecure device location protocol. This protocol, service, and driver were first disabled by default in Windows 10 with the removal of the SMB1 service. For more information on Computer Browser, see MS-BRWS Common Internet File System.
Remote Mailslots	Remote Mailslots are deprecated. The Remote Mailslot protocol, which was initially introduced in MS DOS, is a dated and simple IPC method that is both unreliable and insecure. This protocol was first disabled by default in Windows 11 Insider Preview Build. For more information on Remote Mailslots, see About Mailslots and [MS-MAIL]: Remote Mailslot Protocol.
WebDAV Redirector service	The WebDAV Redirector service is deprecated. The service isn't installed by default in Windows Server. For more information on the WebDAV Redirector service, see WebDAV - Win32 apps.
TLS 1.0 and 1.1	Over the past several years, internet standards and regulatory bodies have deprecated or disallowed TLS versions 1.0 and 1.1 due to various security issues. In a future release of Windows Server, TLS 1.0 and 1.1 will be disabled by default. For more information, see TLS versions 1.0 and 1.1 disablement resources.
Windows Internet Name Service (WINS)	WINS is a legacy computer name registration and resolution service. You should replace WINS with Domain Name System (DNS). For more information, see Windows Internet Name Service (WINS).
Guarded Fabric and Shielded Virtual Machines (VMs)	Windows Server and Azure Stack HCI are aligning with Azure to take advantage of continuing enhancements to Azure Confidential Computing and Azure Security Center. Having this alignment translates to more cloud security offerings being extended to customer data centers (on-premises). Microsoft will continue to provide support for these features, but there will

Feature	Explanation
	be no further development. On client versions of Windows, the Remote Server Administration Tools (RSAT): Shielded VM Tools feature will be removed.
Launching SConfig from a command prompt (CMD) window by running `sconfig.cmd`	Starting with Windows Server 2022, SConfig is launched **by default** when you sign in to a server running Server Core installation option. Moreover, PowerShell is now the default shell on Server Core. If you exit SConfig, you get to a regular interactive PowerShell window. Similarly, you can opt out from SConfig autolaunch. In this case, you'll get a PowerShell window at sign-in. In either scenario, you can launch SConfig from PowerShell by running `SConfig`. If needed, you can launch the legacy command prompt (CMD) from PowerShell as well. But to simplify different transition options, we're going to remove `sconfig.cmd` from the next version of the operating system. If you need to start SConfig from a CMD window, you'll have to launch PowerShell first.
Windows Deployment Services (WDS) boot.wim image deployment	The operating system deployment functionality of WDS is being partially deprecated. Workflows that rely on boot.wim from Windows Server 2022 installation media will show a non-blocking deprecation notice, but the workflows will otherwise not be impacted. Windows 11 workflows and workflows for future versions of Windows Server that rely on boot.wim from installation media will be blocked. Alternatives to WDS, such as Microsoft Endpoint Configuration Manager or the Microsoft Deployment Toolkit (MDT), provide a better, more flexible, and feature-rich experience for deploying Windows images. You're advised to move to one of these solutions instead. WDS PXE boot isn't affected. You can still use WDS to PXE boot devices to custom boot images. You can also still run setup from a network share. Workflows that use custom boot.wim images, such as with Configuration Manager or MDT, will also not be impacted by this change.
LSARPC interface	The named pipe **\PIPE\lsarpc** for accessing EFS encrypted files over the network will be disabled and eventually removed from future versions of Windows. You can still use the named pipe **\PIPE\efsrpc** to access encrypted files.
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	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

Feature	Explanation
	display driver should plan a migration to the WDDM driver model. For more information on implementing remote display indirect display driver see Updates for IddCx versions 1.4 and later.
UCS log collection tool	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.

Features removed or no longer developed starting with Windows Server 2019

Article • 11/28/2022

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.

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

Features we've 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	Explanation
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 **disabled** 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.

Feature	Explanation
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.
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.
Nano Server installation option	Nano Server isn't available as an installable host operating system. Instead, Nano Server is available as a container operating system. To learn more about Nano Server as a container, see Windows Container Base Images.
Server Message Block (SMB) version 1	Starting with this release, Server Message Block (SMB) version 1 is no longer installed by default. For details, see SMBv1 isn't installed by default in Windows 10 version 1709, Windows Server version 1709 and later versions
File Replication Service	File Replication Services, introduced in Windows Server 2003 R2, has been replaced by DFS Replication. You need to migrate any domain controllers that use FRS for the sysvol folder to DFS Replication.
Hyper-V Network Virtualization (HNV)	Network Virtualization is now included in Windows Server as part of the Software Defined Networking (SDN) solution. The SDN solution also includes the Network Controller, Software Load Balancing, User-Defined Routing, and Access Control Lists.

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.

Feature	Explanation
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 virtual machines (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.

Feature	Explanation
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. Host key attestation is 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 extra hardware requirements beyond what Active Directory attestation required, so all existing systems will remain compatible with the new mode. For more information, 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.
IIS 6 Management compatibility	Specific features being considered for replacement are: • IIS 6 Metabase Compatibility (Web-Metabase) • IIS 6 Management Console (Web-Lgcy-Mgmt-Console) • IIS 6 Scripting Tools (Web-Lgcy-Scripting) • IIS 6 WMI Compatibility (Web-WMI) IIS 6 Metabase Compatibility acts as an emulation layer between IIS 6-based metabase scripts and the file-based configuration used by IIS 7 or newer versions. You should start migrating management scripts to target IIS file-based configuration directly, by using tools such as the Microsoft.Web.Administration namespace. You should also start migration from IIS 6.0 or earlier versions, and move to the latest version of IIS, which is always available in the most recent release of Windows Server.

Feature	Explanation
IIS Digest Authentication	This authentication method is planned for replacement. Instead, you should start using other authentication methods such as Client Certificate Mapping (see Configuring One-to-One Client Certificate Mappings) or Windows Authentication (see Application Settings).
Internet Storage Name Service (iSNS)	The Server Message Block (SMB) feature offers essentially the same functionality with more features. See Server Message Block Overview for background information on this feature.
RSA/AES Encryption for IIS	This encryption method is being considered for replacement because the superior Cryptography API: Next Generation (CNG) method is already available. To learn more about CNG encryption, see About CNG.
Windows PowerShell 2.0	This early version of Windows PowerShell has been superseded by several more recent versions. For the best features and performance, migrate to Windows PowerShell 5.0 or later. See PowerShell Documentation for plenty of information.
IPv4/6 Transition Technologies (6to4, ISATAP, and Direct Tunnels)	6to4 has been disabled by default since Windows 10, version 1607 (the Anniversary Update), ISATAP has been disabled by default since Windows 10, version 1703 (the Creators Update), and Direct Tunnels has always been disabled by default. Use native IPv6 support instead.
MultiPoint Services	We're no longer developing the MultiPoint Services role as part of Windows Server. MultiPoint Connector services are available through Feature on Demand for both Windows Server and Windows 10. You can use Remote Desktop Services, in particular the Remote Desktop Services Session Host, to provide RDP connectivity.
Offline symbol packages (Debug symbol MSIs)	We're no longer making the symbol packages available as a downloadable MSI. Instead, the Microsoft Symbol Server is moving to be an Azure-based symbol store. If you need the Windows symbols, connect to the Microsoft Symbol Server to cache your symbols locally or use a manifest file with SymChk.exe on a computer with internet access.
Software Restriction Policies in Group Policy	Instead of using the Software Restriction Policies through Group Policy, you can use AppLocker or Windows Defender Application Control. You can use AppLocker and Windows Defender Application Control to manage which apps users can access and what code can run in the kernel.
Storage Spaces in a Shared configuration using a SAS fabric	Deploy Storage Spaces Direct instead. Storage Spaces Direct supports the use of HLK-certified SAS enclosures, but in a non-shared configuration, as described in the Storage Spaces Direct hardware requirements.

Feature	Explanation
Windows Server Essentials Experience	We're no longer developing the Essentials Experience role for the Windows Server Standard or Windows Server Datacenter SKUs. If you need an easy-to-use server solution for small-to-medium businesses, check out our new Microsoft 365 for business solution, or use Windows Server 2016 Essentials.

Features Removed or Deprecated in Windows Server 2016

Article • 12/23/2021

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 2016.

> **Tip**
>
> - You can get early access to Windows Server builds by joining the **Windows Insider Program for Business** - this is a great way to test feature changes.

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

Features we've removed in this release

We're removing the following features and functionalities from the installed product image in Windows Server 2016. Applications or code that depend on these features won't function in this release unless you use an alternate method.

> **Note**
>
> If you are moving to Windows Server 2016 from a server release prior to Windows Server 2012 R2 or Windows Server 2012, you should also review **Features Removed or Deprecated in Windows Server 2012 R2** and **Features Removed or Deprecated in Windows Server 2012**.

Feature	Explanation
Share and Storage Management snap-in for Microsoft Management Console	If the computer you want to manage is running an operating system older than Windows Server 2016, connect to it with Remote Desktop and use the local version of the Share and Storage Management snap-in. On a computer running Windows 8.1 or earlier, use the Share and Storage Management snap-in from RSAT to view the computer you want to manage. Use Hyper-V on a client computer to run a virtual machine running Windows 7, Windows 8, or Windows 8.1 that has the Share and Storage Management snap-in in RSAT.

Feature	Explanation
Journal.dll	The file `Journal.dll` is removed from Windows Server 2016. There is no replacement.
Security Configuration Wizard	The Security Configuration Wizard is removed. Instead, features are secured by default. If you need to control specific security settings, you can use either Group Policy or Microsoft Security Compliance Manager.
SQM	The opt-in components that manage participation in the Customer Experience Improvement Program have been removed.

Windows Update	The **wuauclt.exe /detectnow** command has been removed and is no longer supported. To trigger a scan for updates, run these PowerShell commands:
	
	`$AutoUpdates = New-Object -ComObject "Microsoft.Update.AutoUpdate"`
	`$AutoUpdates.DetectNow()`

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.

Feature	Explanation
Configuration tools	`scregedit.exe` is deprecated. If you have scripts that depend on scregedit.exe, adjust them to use reg.exe or PowerShell methods.
Sconfig.exe	Use Sconfig.cmd instead.
NetCfg custom APIs	Installation of PrintProvider, NetClient, and ISDN using NetCfg custom APIs is deprecated.
Remote management	WinRM.vbs is deprecated. Instead, use functionality in the WinRM provider of PowerShell.
SMB 2+ over NetBT	SMB 2+ over NetBT is deprecated. Instead, implement SMB over TCP or RDMA.

Windows Server release information

Article • 12/23/2021

Windows Server is moving to the Long-Term Servicing Channel (LTSC) as our primary release channel. The Windows Server Semi-Annual Channel (SAC) was retired on August 9, 2022. There will be no future SAC releases of Windows Server.

The focus on container and microservice innovation previously released in the Semi-Annual Channel will now continue with Azure Kubernetes Service (AKS), AKS on Azure Stack HCI, and other platform improvements made in collaboration with the Kubernetes community. A major new version of Windows Server will continue to be released every 2-3 years, so you can expect both container host and container images to align with that cadence.

Windows Server current versions by servicing option

(All dates are listed in ISO 8601 format: YYYY-MM-DD)

Windows Server release	Servicing option	Editions	Availability	Build	Mainstream support end date	Extended support end date
Windows Server 2022	Long-Term Servicing Channel (LTSC)	Datacenter, Standard	2021-08-18	20348.169	2026-10-13	2031-10-14
Windows Server 2019 (version 1809)	Long-Term Servicing Channel (LTSC)	Datacenter, Essentials, Standard	2018-11-13	17763.107	2024-01-09	2029-01-09
Windows Server 2016 (version 1607)	Long-Term Servicing Channel (LTSC)	Datacenter, Essentials, Standard	2016-10-15	14393.0	End of servicing	2027-01-11

> **Note**
>
> Windows Server is governed by either the **Modern Lifecycle Policy** or the **Fixed Lifecycle Policy**, depending on the version or edition. See the **Windows Lifecycle**

FAQ and **Comparison of servicing channels** for details regarding servicing requirements and other important information. To learn more about which Windows Server versions apply to the Modern Lifecycle Policy, see **Windows Server Releases**.

Extended Security Updates for Windows Server overview

Article • 08/04/2023

The Extended Security Update (ESU) program is a last resort option for customers who need to run certain legacy Microsoft products past the end of support. Windows Server Long Term Servicing Channel (LTSC) has a minimum of 10 years of support: five years for mainstream support and five years for extended support, which includes regular security updates.

However, once products reach the end of support, it also means the end of security updates and bulletins. This scenario can cause security or compliance issues and put business applications at risk. Microsoft recommends that you upgrade to the current version of Windows Server for the most advanced security, performance, and innovation.

> **Tip**
>
> You can find information on support dates on **Microsoft Lifecycle**.

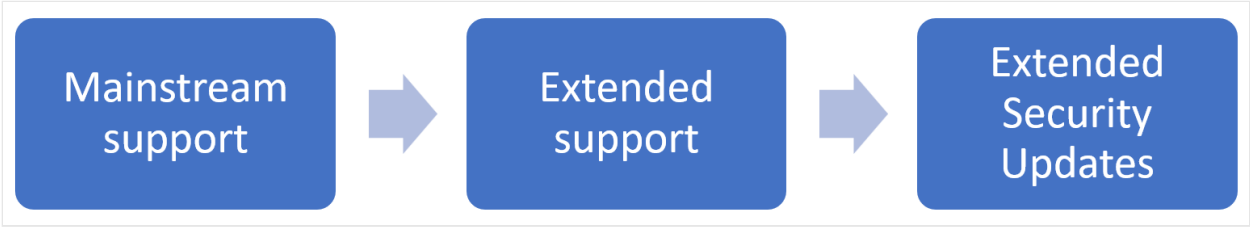
The following versions of Windows Server have reached or are in the process of reaching the end of extended support:

- Extended support for Windows Server 2008 and Windows Server 2008 R2 ended on January 14, 2020.
- Extended support for Windows Server 2012 and Windows Server 2012 R2 will be ending on October 10, 2023.

What are Extended Security Updates?

Extended Security Updates for Windows Server include security updates and bulletins rated *critical* and *important* for a maximum period of time from the end of extended support, depending on the version. They're available free of charge for servers hosted in Azure, and available to purchase for servers not hosted in Azure. Extended Security Updates don't include new features, customer-requested non-security hotfixes, or design change requests. For more information, see Lifecycle FAQ - Extended Security Updates.

With Extended Security Updates, the different phases for these versions of Windows Server are as follows:



If you haven't already upgraded your servers, you can do the following things to protect your applications and data during the transition:

- Migrate the affected existing Windows Server workloads as-is to Azure Virtual Machines (VM). Migrating to Azure automatically provides Extended Security Updates for the defined period. There's no extra charge for Extended Security Updates on top of an Azure VM's cost, and you don't need to do any other configuration.
- Purchase an Extended Security Update subscription for your servers and remain protected until you're ready to upgrade to a newer Windows Server version. When you have an Extended Security Update subscription, Microsoft provides updates for the defined period. Once you purchase a subscription, you must get a product key and install it on each applicable server. For more information, see How to get Extended Security Updates.

When you get the Extended Security Updates depends on which version of Windows Server you're using and where it's hosted. The following table lists the Extended Security Update duration for each version of Windows Server.

Product version	Hosted	ESU duration	ESU end date
Windows Server 2008 Windows Server 2008 R2	Azure*	Four years	January 9, 2024
Windows Server 2008 Windows Server 2008 R2	Not in Azure	Three years	January 10, 2023
Windows Server 2012 Windows Server 2012 R2	Azure*	Three years	October 13, 2026
Windows Server 2012 Windows Server 2012 R2	Not in Azure	Three years	October 13, 2026

* Includes the Azure Stack portfolio of products that extend Azure services and capabilities to your environment of choice.

> ⚠ **Warning**
>
> After the period of Extended Security Updates ends, we'll stop providing updates. We recommend you update your version of Windows Server to a more recent version as soon as possible.

Migrate to Azure

You can migrate your on-premises servers that run a version of Windows Server that has reached or is almost reaching the end of extended support to Azure, where you can continue to run them as virtual machines. When you migrate to Azure, you not only stay compliant with security updates, but also add cloud innovation to your work. The benefits of migrating to Azure include:

- Security updates in Azure.
- Get Windows Server critical and important security updates for a certain period of time, included at no extra charge.
- Upgrades in Azure free of charge.
- Adopt more cloud services whenever you're ready.
- By migrating SQL Server to Azure VMs, you get three more years of Windows Server critical security updates, included at no extra charge. You can also modernize your SQL Server to Azure SQL Managed Instance.
- Benefit from Azure Hybrid Benefit, which lets you use existing Windows Server licenses and SQL Server licenses for cloud savings unique to Azure.

To get started migrating, learn how to upload a generalized VHD and use it to create new VMs in Azure, or use Shared Image Galleries in Azure.

You can also read the Migration Guide for Windows Server for help with the following things:

- Analyze your existing IT resources.
- Assess the current state of your deployment.
- Understand whether moving certain services and applications to the cloud or keeping them on-premises and upgrading to the latest version of Windows Server instead is best for you.

Upgrade on-premises

If you need to keep your servers on-premises instead of migrating to Azure and the cloud, you have two choices for how to proceed:

- Build new servers with a supported version of Windows Server and migrate your applications and data.
- Upgrade in-place to a supported version of Windows Server.

In-place upgrades can typically upgrade Windows Server through at least one version, sometimes even two versions. For example, Windows Server 2012 R2 can upgrade in-place to Windows Server 2019. However, if you're running Windows Server 2008 or Windows Server 2008 R2, there's no direct upgrade path to Windows Server 2016 or later. Instead, you must first upgrade to Windows Server 2012 R2, then upgrade to Windows Server 2016 or Windows Server 2019.

As you upgrade, you can also migrate to Azure at any time. For more information about your on-premises upgrade options, see supported upgrade paths for Windows Server.

Upgrade SQL Server in parallel with your Windows Servers

If you're running a version of SQL Server that reached or is reaching the end of extended support, you can also benefit from Extended Security Updates for SQL Server. For more information, see Extended Security Updates for SQL Server and Windows Server.

Next steps

- Learn how to get Extended Security Updates (ESU) for Windows Server.

Overview of Windows Server upgrades

Article • 07/11/2022

The process of upgrading to a newer version of Windows Server can vary greatly, depending on which operating system you are starting with and the pathway you take. We use the following terms to distinguish between different actions, any of which could be involved in a new Windows Server deployment.

- **Upgrade.** Also known as an "in-place upgrade". You move from an older version of the operating system to a newer version, while staying on the same physical hardware. **This is the method we will be covering in this section.**

  > **Important**
  >
  > In-place upgrades might also be supported by public or private cloud companies; however, you must check with your cloud provider for the details. Additionally, you'll be unable to perform an in-place upgrade on any Windows Server configured to **Boot from VHD**. An in-place upgrade from Windows Storage Server Editions is not supported. You can perform either a **Migration** or **Installation** instead.

- **Installation.** Also known as a "clean installation". You move from an older version of the operating system to a newer version, deleting the older operating system.
- **Migration.** You move from an older version of the operating system to a newer version of the operating system, by transferring to a different set of hardware or virtual machine.
- **Cluster OS Rolling Upgrade.** You upgrade the operating system of your cluster nodes 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. For more information, see Cluster OS Rolling Upgrade
- **License conversion.** 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. We call this "license conversion". For example, if your server is running Standard edition, you can convert it to Datacenter.

Which version of Windows Server should I upgrade to?

We recommend upgrading to the latest version of Windows Server. Running the latest version of Windows Server allows you to use the latest features – including the latest security features – and delivers the best performance.

> **Tip**
>
> You can upgrade to a newer version of Windows Server by up to two versions at a time. For example, Windows Server 2016 can be upgraded to Windows Server 2019 or Windows Server 2022. If you are using the **Cluster OS Rolling Upgrade feature** you can only one version at at time.

In this table you can see the supported upgrade paths, based on the version you're currently on.

Upgrade from / to	Windows Server 2008 R2	Windows Server 2012	Windows Server 2012 R2	Windows Server 2016	Windows Server 2019	Windows Server 2022
Windows Server 2008	Yes	Yes	-	-	-	-
Windows Server 2008 R2	-	Yes	Yes	-	-	-
Windows Server 2012	-	-	Yes	Yes	-	-
Windows Server 2012 R2	-	-	-	Yes	Yes	-
Windows Server 2016	-	-	-	-	Yes	Yes
Windows Server 2019	-	-	-	-	-	Yes

You can also upgrade from an evaluation version of the operating system to a retail version, from an older retail version to a newer version, or, in some cases, from a volume-licensed edition of the operating system to an ordinary retail edition. For more information about upgrade options other than in-place upgrade, see Upgrade and conversion options for Windows Server.

> **Note**

Support for **Windows Server 2008** and **Windows Server 2008 R2** has ended. We recommend you update your version of Windows Server to a more recent version as soon as possible. Learn more about **Extended Security Updates (ESU)** as a last resort.

Next steps

Now that you've ready to upgrade Windows Server, here are some articles that might help you get started:

- Install, upgrade, or migrate to Windows Server
- Upgrade and migrate roles and features in Windows Server
- Upgrade and conversion options for Windows Server
- Perform an in-place upgrade of Windows Server

Install, upgrade, or migrate to Windows Server

Article • 08/10/2022

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

> **Important**
>
> Extended support for Windows Server 2008 R2 and Windows Server 2008 ended in January 2020. Extended Security Updates (ESU) are available, with one option to migrate your on-premises servers to Azure, where you can continue to run them on virtual machines. To find out more, see **Extended Security Updates overview**.

> **Tip**
>
> To download Windows Server 2022, see **Windows Server Evaluations**.

Clean install

Clean install is simplest way to install Windows Server, where you install on a blank server or overwrite an existing operating system, 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 hardware requirements, so be sure to check the details for Windows Server.

In-place upgrade

In-place upgrade enables you to keep the same hardware and all the server roles you have set up without wiping and reinstalling the operating system, by which you go from an older operating system to a newer one, keeping your settings, server roles and features, and data intact. For example, if your server is running Windows Server 2019, you can upgrade it to Windows Server 2022. However, not every older operating system has a pathway to every newer one and some roles or features don't support this or need you to take extra steps. In-place upgrade works best in virtual machines where specific OEM hardware drivers are not needed for a successful upgrade.

For step-by-step guidance and more information on upgrading, review the Windows Server upgrade content and Upgrade and migrate roles and features in Windows Server.

Cluster Operating System rolling upgrade

Cluster Operating System (OS) rolling upgrade gives an administrator the ability to upgrade the operating system of the cluster nodes without stopping the Hyper-V or the Scale-Out File Server workloads. For example, if nodes in your cluster are running Windows Server 2019 you can install Windows Server 2022 on them avoiding downtime to the cluster, which would otherwise impact Service Level Agreements. This feature is discussed in more detail at Cluster OS rolling upgrade.

Migration

Migration of Windows Server 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

License conversion enables you to 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 for some Windows Server releases. For example, if your server is running Windows Server 2022 Standard, you can convert it to Windows Server 2022 Datacenter. Keep in mind that while you can move up from Windows Server 2022 Standard to Windows Server 2022 Datacenter, you are unable to reverse the process and go from Datacenter edition to Standard edition. In some releases of Windows Server, you can also freely convert between OEM, volume-licensed, and retail versions with the same command and the appropriate key.

Server Core vs Server with Desktop Experience install options

Article • 11/26/2021

When you install Windows Server using the setup wizard, you can choose between Server Core or Server with Desktop Experience install options. With Server Core, the standard graphical user interface (the Desktop Experience) is not installed; you manage the server from the command line using PowerShell, the Server Configuration tool (SConfig), or by remote methods. Server with Desktop Experience installs the standard graphical user interface and all tools, including client experience features.

We recommend that you choose the Server Core install option unless you have a particular need for the extra user interface elements and graphical management tools that are included in the Server with Desktop Experience install option.

The setup wizard lists the install options below. In this list, editions without **Desktop Experience** are the Server Core install options:

- Windows Server Standard
- Windows Server Standard with Desktop Experience
- Windows Server Datacenter
- Windows Server Datacenter with Desktop Experience

> **Note**
>
> Unlike some previous releases of Windows Server, you cannot convert between Server Core and Server with Desktop Experience after installation. You will need to do a **clean installation** if you install later decide to use a different option.

Differences

There are some key differences between Server Core and Server with Desktop Experience:

Component	Server Core	Server with Desktop Experience
User interface	Minimal, command line driven (PowerShell, SConfig, cmd)	Standard Windows graphical user interface
Disk space	Smaller requirement	Larger requirement

Component	Server Core	Server with Desktop Experience
Install, configure, uninstall server roles locally	PowerShell	Server Manager or PowerShell
Roles and Features	Some roles and features are not available. For more information, see Roles, Role Services, and Features not in Windows Server - Server Core. Some of the features from Server with Desktop Experience for application compatibility can be installed with the App Compatibility Feature on Demand (FOD).	All roles and features are available, including those for application compatibility.
Remote management	Yes, can be managed remotely using GUI tools, such as Windows Admin Center, Remote Server Administration Tools (RSAT), or Server Manager, or by PowerShell.	Yes, can be managed remotely using GUI tools, such as Windows Admin Center, Remote Server Administration Tools (RSAT), or Server Manager, or by PowerShell.
Potential attack surface	Greatly reduced attack surface	No reduction
Microsoft Management Console	Not installed - can be installed with the App Compatibility Feature on Demand (FOD).	Installed

> **Note**
>
> For RSAT, you must use the version included with Windows 10 or later.

Upgrade and migrate roles and features in Windows Server

Article • 12/23/2021

You can update roles and features to later versions of Windows Server by migrating to a new server, or many also support in-place upgrade where you install the new version of Windows Server over the top of the current one. This article contains links to migration guides as well a table with migration and in-place upgrade information to help you decide which method to use.

You can migrate many roles and features by using Windows Server Migration Tools, a feature built in to Windows Server for migrating roles and features, whereas file servers and storage can be migrated using Storage Migration Service.

The migration guides support migrations of specified roles and features from one server to another (not in-place upgrades). Unless otherwise noted in the guides, migrations are supported between physical and virtual computers, and between installation options of Windows Server with either Server with Desktop Experience or Server Core.

> **Important**
>
> Before you begin migrating roles and features, verify that both source and destination servers are running the most current updates that are available for their operating systems.
>
> Whenever you migrate or upgrade to any version of Windows Server, you should review and understand the **support lifecycle policy** and time frame for that version and plan accordingly. You can **search for the lifecycle information** for the particular Windows Server release that you are interested in.

Windows Server Migration Tools

Windows Server Migration Tools enables you to migrate server roles, features, operating system settings, and other data and shares to servers, including later versions of Windows Server. It is a feature of Windows Server and so it is easily installed using the Add Roles and Features wizard, or PowerShell. Learn more about how to install, use, and remove Windows Server Migration Tools.

> **Note**

Cross-subnet migrations using Windows Server Migration Tools is available with Windows Server 2012 and later releases. Previous versions of Windows Server Migration Tools only support migrations in the same subnet.

Migration guides

Below you can find links to migration guides for specific Windows Roles and Features.

Active Directory

- Active Directory Certificate Services Migration Guide for Windows Server 2012 R2
- Active Directory Certificate Services Migration Guide for Windows Server 2008 R2
- Migrate Active Directory Federation Services Role Service to Windows Server 2012 R2
- Migrate Active Directory Federation Services Role Services to Windows Server 2012
- Active Directory Rights Management Services Migration and Upgrade Guide
- Upgrade Domain Controllers to Windows Server 2012 R2 and Windows Server 2012
- Active Directory Domain Services and Domain Name System (DNS) Server Migration Guide for Windows Server 2008 R2

BranchCache

- BranchCache Migration Guide

DHCP

- Migrate DHCP Server to Windows Server 2012 R2
- Dynamic Host Configuration Protocol (DHCP) Server Migration Guide for Windows Server 2008 R2

Failover Clustering

- Migrate Cluster Roles to Windows Server 2012 R2
- Migrate Clustered Services and Applications to Windows Server 2012

File and Storage Services

- Storage Migration Service

- Migrate File and Storage Services to Windows Server 2012 R2

Hyper-V

- Migrate Hyper-V to Windows Server 2012 R2 from Windows Server 2012
- Migrate Hyper-V to Windows Server 2012 from Windows Server 2008 R2

Network Policy Server

- Migrate Network Policy Server to Windows Server 2012
- Migrate Health Registration Authority to Windows Server 2012

Print and Document Services

- Migrate Print and Document Services to Windows Server 2012

Remote Access

- Migrate Remote Access to Windows Server 2012

Remote Desktop Services

- Migrate Remote Desktop Services
- Migrate Remote Desktop Services to Windows Server 2012 R2
- Migrate MultiPoint Services

Routing and Remote Access

- RRAS Migration Guide

Web Server (IIS)

- Web Server (IIS)

Windows Server Update Services

- Migrate Windows Server Update Services to Windows Server 2012 R2

Other Windows migration guides

- Local User and Group Migration Guide
- IP Configuration Migration Guide

Upgrade and migration matrix

Server Role	Upgradeable in-place?	Migration Supported?	Can migration be completed without downtime?
Active Directory Certificate Services	Yes	Yes	No
Active Directory Domain Services	Yes	Yes	Yes
Active Directory Federation Services	No	Yes	No (new nodes need to be added to the farm)
Active Directory Lightweight Directory Services	Yes	Yes	Yes
Active Directory Rights Management Services	Yes	Yes	No
DHCP Server	Yes	Yes	Yes
DNS Server	Yes	Yes	No
Failover Clustering	Yes with Cluster OS Rolling Upgrade process (Windows Server 2012 R2 and later) or when the server is removed by the cluster for upgrade and then added to a different cluster.	Yes	Yes for Failover Clusters with Hyper-V VMs or Failover Clusters running the Scale-out File Server role. See Cluster OS Rolling Upgrade (Windows Server 2012 R2 and later).

Server Role	Upgradeable in-place?	Migration Supported?	Can migration be completed without downtime?
File and Storage Services	Yes	Varies by subfeature	No
Hyper-V	Yes with Cluster OS Rolling Upgrade process (Windows Server 2012 R2 and later)	Yes	Yes for Failover Clusters with Hyper-V VMs or Failover Clusters running the Scale-out File Server role. See Cluster OS Rolling Upgrade (Windows Server 2012 R2 and later).
Print and Fax Services	No	Yes (using Printbrm.exe)	No
Remote Desktop Services	Yes, for all subroles, but mixed mode farm is not supported	Yes	No
Web Server (IIS)	Yes	Yes	No
Windows Server Essentials Experience	Yes	Yes	No
Windows Server Update Services	Yes	Yes	No
Work Folders	Yes	Yes	Yes with Cluster OS Rolling Upgrade process (Windows Server 2012 R2 and later).

Upgrade and conversion options for Windows Server

Article • 09/19/2023

You can upgrade or convert installations of Windows Server to newer versions, different editions, or switch between licensing options, such as evaluation, retail, and volume licensed. This article helps explain what the options are to help with your planning.

The process of upgrading or converting installations of Windows Server might vary greatly depending on which version and edition you have installed, how it's licensed, and the pathway you take. We use different terms to distinguish between actions, any of which could be involved in a deployment of Windows Server: clean install, in-place upgrade, cluster operating system (OS) rolling upgrade, migration, and license conversion. You can learn more about these terms at Install, upgrade, or migrate to Windows Server.

Upgrade licensed versions of Windows Server

The following general guidelines are for in-place upgrade paths where Windows Server is **already licensed**, that is, not evaluation:

- Upgrades from 32-bit to 64-bit architectures aren't supported. All releases of Windows Server since Windows Server 2008 R2 are 64-bit only.
- Upgrades from one language to another aren't supported.
- If the server is an Active Directory domain controller, you can't convert it to a retail version. See Upgrade Domain Controllers to Windows Server for important information.
- Upgrades from prerelease versions (previews) of Windows Server aren't supported. Perform a clean installation of Windows Server.
- Upgrades that switch from a Server Core installation to a Server with Desktop Experience installation or vice versa aren't supported.
- Upgrades from a previous Windows Server installation to an evaluation copy of Windows Server aren't supported. Evaluation versions should be installed as clean installations.
- When you upgrade from a previous version to a new version, the default is to retain the existing operating system edition. For example, the default is to upgrade from Standard (previous version) to Standard (new version), from Datacenter (previous version) to Datacenter (new version), or from Datacenter: Azure Edition (previous version) to Datacenter: Azure Edition (new version).

- Alternatively, you can change to certain other editions when upgrading. You can change from Standard to Datacenter or to Datacenter: Azure Edition, or change from Datacenter to Datacenter: Azure Edition. You can't change from Datacenter to Standard edition or from Datacenter: Azure Edition to either Standard or Datacenter editions when upgrading.

> ⓘ **Note**
>
> If your server uses NIC Teaming, disable NIC Teaming prior to upgrade, and then re-enable it after upgrade is complete. See **NIC Teaming Overview** for details.

Convert an evaluation version to a retail version

You can convert evaluation versions and editions of Windows Server to retail versions and editions. For example, if you've installed the evaluation version of Standard (Desktop Experience) edition, you can convert it to the retail version of either the Standard (Desktop Experience) edition or the Datacenter (Desktop Experience) edition.

However, you can't convert all Windows Server evaluation versions and editions to all retail versions or editions. For example, if you've installed the evaluation Datacenter edition, you can convert it only to the retail Datacenter edition, not to the retail Standard edition.

In Windows Server versions after 2016, if you've installed Desktop Experience evaluation versions, you can't convert them to Core retail versions. If you install the Standard Core evaluation version, you can convert it only to retail Datacenter Core, not to retail Standard Core.

It's important to run the `DISM /online /Get-TargetEditions` command as instructed in the following procedure to determine which retail versions you can upgrade to. If the retail version you want isn't listed as a target version, you need to do a fresh install of the retail version you want.

> ⓘ **Note**
>
> To verify that your server is running an evaluation version, you can run either of the following commands at an elevated command prompt:

- Run `DISM /online /Get-CurrentEdition` and make sure the current edition name includes `Eval`.
- Run `slmgr.vbs /dlv` and make sure the output includes `EVAL`.

If you haven't already activated Windows, the bottom right-hand corner of the desktop shows the time remaining in the evaluation period.

Windows Server Standard or Datacenter

If your server is running an evaluation version of Windows Server Standard or Datacenter edition, you can convert it to an available retail version. Run the following commands in an elevated command prompt or PowerShell session.

1. Determine the current edition name by running the following command. The output is an abbreviated form of the edition name. For example, Windows Server Datacenter (Desktop Experience) Evaluation edition is `ServerDatacenterEval`.

   Windows Command Prompt

   ```
   DISM /online /Get-CurrentEdition
   ```

2. Verify which editions the current installation can be converted to by running the following command. From the output, make a note of the edition name you want to upgrade to.

   Windows Command Prompt

   ```
   DISM /online /Get-TargetEditions
   ```

3. Run the following command to save the Microsoft Software License Terms for Windows Server, which you can then review. Replace the `<target edition>` placeholder with the edition name you noted from the previous step.

   Windows Command Prompt

   ```
   DISM /online /Set-Edition:<target edition> /GetEula:C:\license.rtf
   ```

4. Enter the new edition name and corresponding retail product key in the following command. The upgrade process requires you to accept the Microsoft Software License Terms for Windows Server that you saved previously.

Windows Command Prompt

```
DISM /online /Set-Edition:<target edition> /ProductKey:<product key>
/AcceptEula
```

For example:

Windows Command Prompt

```
DISM /online /Set-Edition:ServerDatacenter /ProductKey:ABCDE-12345-
ABCDE-12345-ABCDE /AcceptEula
```

Tip

For more information about Dism.exe, see **DISM Command-line options**.

Important

You can't convert an Active Directory domain controller from an evaluation to a retail version. In this case, install an additional domain controller on a server that runs a retail version, migrate any FSMO roles held, and remove Active Directory Domain Services (AD DS) from the domain controller that runs on the evaluation version. For more information, see **Upgrade Domain Controllers to Windows Server**.

Windows Server Essentials

If the server is running Windows Server Essentials, you can convert it to the full retail version by entering a retail, volume license, or OEM key in the following command at an elevated command prompt:

Windows Command Prompt

```
slmgr.vbs /ipk <license key>
```

Convert Windows Server Standard edition to Datacenter edition

At any time after installing Windows Server, you can convert Windows Server Standard edition to Datacenter edition. You can also run `setup.exe` from the installation media to upgrade or repair the installation, sometimes called in-place repair. If you run `setup.exe` to upgrade or repair in-place on any edition of Windows Server, the result is the same edition you started with.

You can convert the Standard edition of Windows Server to the Datacenter edition as follows:

1. Determine that Windows Server Standard is the current edition name by running the following command. The output is an abbreviated form of the edition name, for example Windows Server Standard (Desktop Experience) edition is `ServerStandard`.

   Windows Command Prompt

   ```
   DISM /online /Get-CurrentEdition
   ```

2. Verify that Windows Server Datacenter is a valid option to convert to by running the following command:

   Windows Command Prompt

   ```
   DISM /online /Get-TargetEditions
   ```

3. Enter `ServerDatacenter` and your retail product key in the following command:

   Windows Command Prompt

   ```
   DISM /online /Set-Edition:ServerDatacenter /ProductKey:<product key>
   /AcceptEula
   ```

Convert between retail, volume-licensed, and OEM licenses

At any time after installing Windows Server, you can freely convert between a retail license, a volume-licensed license, or an OEM license. The edition (Standard or Datacenter) remains the same during this conversion. If you're starting with an evaluation version, convert it to the retail version first and then convert between the versions by running the following command from an elevated command prompt. Provide your volume-license, retail, or OEM product key.

Windows Command Prompt

```
slmgr.vbs /ipk <product key>
```

See also

For more information about upgrading Windows Server, see the following articles:

- Overview of Windows Server upgrades
- Server Core vs Server with Desktop Experience install options
- Perform an in-place upgrade of Windows Server
- In-place upgrade for VMs running Windows Server in Azure

Automatic Virtual Machine Activation in Windows Server

Article • 09/20/2023

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 activate Windows Server virtual machines (VMs) on a Windows Server Hyper-V host that is properly activated, even in disconnected environments. AVMA binds the VM activation to the licensed virtualization host and activates the VM when it starts up. When you use AVMA, you can get real-time reporting on usage and historical data on the license state of the VM. Reporting and tracking data is available on the virtualization host.

Practical applications

On virtualization hosts, AVMA offers several benefits.

Server data center managers can use AVMA to do the following tasks:

- Activate VMs in remote locations.
- Activate VMs with or without an internet connection.
- Track VM usage and licenses from the virtualization host, without requiring any access rights on the virtualized systems.

Service Provider License Agreement (SPLA) partners and other hosting providers don't have to share product keys with tenants or access a tenant's VM to activate it. VM 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

For a virtualization server host to run guest VMs, you must activate it. To do so, obtain keys through the Volume Licensing Service Center or your OEM provider.

> **Note**

In a failover cluster, each virtualization server host in the cluster must be activated for guest VMs to stay activated, regardless of which server they run on.

AVMA requires a Windows Server Datacenter edition with the Hyper-V server host role installed. The Windows Server version of the host determines which versions it can activate in a guest VM. The following table lists the guest VM versions that each host version is able to activate. A host version can access all the editions (Datacenter, Standard, or Essentials) of its eligible guest VM versions.

Server host version	Windows Server 2022 guest VM	Windows Server 2019 guest VM	Windows Server 2016 guest VM	Windows Server 2012 R2 guest VM
Windows Server 2022	X	X	X	X
Windows Server 2019		X	X	X
Windows Server 2016			X	X
Windows Server 2012 R2				X

> **Note**
>
> AVMA does not work with other server virtualization technologies.

How to implement AVMA

To activate VMs with AVMA, you use a generic AVMA key (detailed in AVMA keys) that corresponds to the version of Windows Server that you want to activate. To create a VM and activate it with an AVMA key, follow these steps:

1. On the server that will host the VMs, install and configure the Microsoft Hyper-V Server role. Ensure that the server is successfully activated. For more information, see Install Hyper-V Server.
2. Create a virtual machine and install a supported Windows Server operating system on it.

> **Important**
>
> The **Data Exchange integration service** (also known as Key-Value Pair Exchange) must be enabled in the VM settings for AVMA to work. It is enabled by default for new VMs.

3. After you've finished installing Windows Server on the VM, install the AVMA key on the VM. From PowerShell or an elevated command prompt, run the following command:

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

The VM will automatically activate, providing the virtualization host itself is activated.

> **Tip**
>
> You can also add the AVMA keys in any **Unattend setup file**.

AVMA keys

The following AVMA keys can be used for Windows Server 2022:

Edition	AVMA key
Datacenter	W3GNR-8DDXR-2TFRP-H8P33-DV9BG
Datacenter Azure Edition	F7TB6-YKN8Y-FCC6R-KQ484-VMK3J
Standard	YDFWN-MJ9JR-3DYRK-FXXRW-78VHK

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
Standard	C3RCX-M6NRP-6CXC9-TW2F2-4RHYD
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 Key-Value Pair (KVP) exchange between the virtualization host and the VM provides real-time tracking data for the guest operating systems, including activation information. This activation information is stored in the Windows registry of the VM. Historical data about AVMA requests is logged in Event Viewer on the virtualization host.

See Data Exchange: Using key-value pairs to share information between the host and guest on Hyper-V for more information about KVP.

> **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).

Since the AVMA activation process is transparent, error messages aren't displayed. However, AVMA requests are also logged on the virtualization host in Event Viewer in the Application log with Event ID 12310, and on the VM with Event ID 12309. The following events are captured on the VMs:

Notification	Description
AVMA Success	The VM was activated.
Invalid Host	The virtualization host is unresponsive. This event can happen when the server isn't running a supported version of Windows.
Invalid Data	This event usually results from a failure in communication between the virtualization host and the VM, often caused by corruption, encryption, or data mismatch.
Activation Denied	The virtualization host couldn't activate the guest operating system because the AVMA ID didn't match.

Key Management Services (KMS) activation planning

Article • 12/23/2021

The following information outlines initial planning considerations that you need to review for Key Management Services (KMS) activation.

KMS uses a client-server model to active clients and is used for volume activation. 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 a supported Windows Server or Windows client operating system. A KMS host running on a Windows Server operating system can activate computers running both server and client operating systems, however a KMS host running on a Windows client operating system can only activate computers also running client operating systems.

To use KMS, a KMS host needs a key that activates, or authenticates, the KMS host with Microsoft. This key is sometimes referred to as the KMS host key, but it is formally known as a Microsoft Customer Specific Volume License Key (CSVLK). You can get this key from the Product Keys section of the Volume Licensing Service Center for the following agreements: Open, Open Value, Select, Enterprise, and Services Provider License. You can also get assistance by contacting your local Microsoft Activation Center.

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.

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.

After the first KMS host is activated, the CSVLK that is used on the first host can be used to activate up to five more KMS hosts on your network for a total of six. 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 can request additional activations for your organization's CSVLK - for example, if you have 10 physical locations under one volume licensing agreement and you want each location to have a local KMS host. To request this exception, please contact your local Microsoft Activation Center.

Computers that are running volume licensing editions of Windows Server and Windows client are, by default, KMS clients with no extra configuration needed.

If you are converting a computer from a KMS host, MAK, or retail edition of Windows to a KMS client, you will need to install the applicable KMS client setup key. For more information, see KMS client setup keys.

Network requirements

KMS activation requires TCP/IP connectivity. KMS hosts and clients are configured by default to use Domain Name System (DNS). KMS hosts use DNS dynamic updates 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.

By default, a KMS host is configured to use TCP on port 1688.

Activation versions

The following table summarizes KMS host and client versions for networks that include Windows Server and Windows client devices.

> **Important**
>
> - Windows Updates might be required on the KMS server to support activation of newer clients. If you receive activation errors, check that you have the appropriate updates listed below this table.

CSVLK group	CSVLK can be hosted on	Windows editions activated by this KMS host
Volume License for Windows Server 2022	• Windows Server 2022 • Windows Server 2019 • Windows Server 2016	• Windows Server 2022 (all editions) • Windows Server Semi-Annual Channel • Windows Server 2019 (all editions) • Windows Server 2016 (all editions) • Windows 11 Enterprise/Enterprise N • Windows 11 Professional/Professional N • Windows 11 Professional for Workstations/Professional N for Workstations • Windows 11 for Education/Education N • Windows 10 Enterprise LTSC/LTSC N/LTSB • Windows 10 Enterprise/Enterprise N • Windows 10 Professional/Professional N • Windows 10 Professional for Workstations/Professional N for Workstations • Windows 10 for Education/Education N • 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

CSVLK group	CSVLK can be hosted on	Windows editions activated by this KMS host
Volume License for Windows Server 2019	• Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2	• Windows Server Semi-Annual Channel • Windows Server 2019 (all editions) • Windows Server 2016 (all editions) • Windows 10 Enterprise LTSC/LTSC N/LTSB • Windows 10 Enterprise/Enterprise N • Windows 10 Professional/Professional N • Windows 10 Professional for Workstations/Professional N for Workstations • Windows 10 for Education/Education N • 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 2016 • Windows Server 2012 R2 • Windows Server 2012	• Windows Server Semi-Annual Channel • Windows Server 2016 (all editions) • Windows 10 LTSB (2015 and 2016) • Windows 10 Enterprise/Enterprise N • Windows 10 Professional/Professional N • Windows 10 Professional for Workstations/Professional N for Workstations • Windows 10 Education/Education N • 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

CSVLK group	CSVLK can be hosted on	Windows editions activated by this KMS host
Volume license for Windows 10	• Windows 10 • Windows 8.1 • Windows 7	• 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

KMS host required updates

Depending on which operating system your KMS host is running and which operating systems you want to activate, you might need to install one or more of the updates below. This is required when you want to activate a version of Windows that is newer than the version your KMS host is running.

> ⓘ Note
>
> The updates listed below are the minimum required. Where later cumulative updates or monthly rollups are listed as an option, please install the latest available version for your operating system to benefit from additional security and other fixes.

KMS host OS version	KMS client OS version(s) to activate	Required update
Windows Server 2019	• Windows Server 2022	June 8, 2021—KB5003646 or later cumulative update
Windows Server 2016	• Windows Server 2022 • Windows Server 2019	June 8, 2021—KB5003638 or later cumulative update

KMS host OS version	KMS client OS version(s) to activate	Required update
Windows Server 2016	• Windows Server 2019	December 3, 2018—KB4478877 or later cumulative update
Windows Server 2012 R2	• Windows Server 2019 • Windows Server 2016 • Windows 10	November 27, 2018—KB4467695 (Preview of Monthly Rollup) or later monthly rollup
Windows Server 2012 R2	• Windows Server 2016 • Windows 10	July 2016 update rollup for Windows 8.1 and Windows Server 2012 R2 or later monthly rollup
Windows Server 2012	• Windows Server 2016 • Windows Server 2012 R2 • Windows 10	July 2016 update rollup for Windows Server 2012 or later monthly rollup
Windows Server 2008 R2	• Windows Server 2012 R2 • Windows Server 2012 • Windows 10	Update that enables Windows 7 and Windows Server 2008 R2 KMS hosts to activate Windows 10
Windows 8.1	• Windows 10	July 2016 update rollup for Windows 8.1 and Windows Server 2012 R2 or later monthly rollup
Windows 7	• Windows 10	Update that enables Windows 7 and Windows Server 2008 R2 KMS hosts to activate Windows 10

Server Core App Compatibility Feature on Demand

Article • 03/16/2023

The Server Core App Compatibility Feature on Demand (FOD) is an optional feature package that can be added to Server Core installations of Windows Server installations at any time, beginning with Windows Server 2019.

For more information on other Features on Demand, see Features On Demand.

Why install the App Compatibility FOD?

The App Compatibility Feature on Demand for Server Core improves app compatibility by including a subset of binaries and packages from the Server with Desktop Experience installation option. This optional package is available on a separate ISO, or from Windows Update, but can only be added to Server Core installations and images.

The two primary values the App Compatibility FOD provides are:

- Increases the compatibility of Server Core for server applications already in market or 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)

> **Note**
>
> Failover Cluster Manager requires adding the Failover Clustering Windows Server feature first, which can be done by running the following command from an an elevated PowerShell session:

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

Beginning with Windows Server 2022, the following components are also available (when using the same version of the App Compatibility FOD):

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

Installing the App Compatibility Feature on Demand

> **Important**
>
> - The App Compatibility FOD can only be installed on Server Core. Don't attempt to add the Server Core App Compatibility FOD to the Server with Desktop Experience installation option.
> - For servers running Windows Server 2022, ensure you have installed the **2022-01 Cumulative Update Preview for Microsoft server operating system version 21H2 for x64-based Systems (KB5009608)** or later cumulative update before you install the App Compatibility FOD. You can verify this by checking that the operating system build number is 20348.502 or greater. Prior to this, if you tried to connect to the server using Remote Desktop Protocol (RDP), you could be presented with a black screen and disconnected.

Connected to the internet

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

```
PowerShell

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

Disconnected from the internet

1. If the server can't connect to Windows Update, instead download the Windows Server Languages and Optional Features ISO image file, and copy the ISO to a shared folder on your local network:

   - If you have a volume license, you can download the Windows Server Languages and Optional Features ISO image file from the same portal where the operating system ISO image file is obtained: Volume Licensing Service Center.
   - The Windows Server Languages and Optional Features ISO image file is also available on the Microsoft Evaluation Center or on the Visual Studio portal for subscribers.

   > **Note**
   >
   > The Languages and Optional Features ISO image file is new for Windows Server 2022. Previous versions of Windows Server use the Features on Demand (FOD) ISO.

2. 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 App Compatibility FOD to.

Mount the FOD ISO

1. Use `New-PSDrive` from PowerShell, `net use` from Command Prompt, or some other method, to connect to the location of the FOD ISO. For example, in an elevated PowerShell session run the following command:

```
PowerShell
```

```
$credential = Get-Credential

New-PSDrive -Name FODShare -PSProvider FileSystem -Root
"\\server\share" -Credential $credential
```

2. Copy the FOD ISO to a local folder of your choosing (the copy operation may take some time). Edit the following variables with your folder location and ISO filename, and run the following commands, for example:

```
PowerShell

$isoFolder = "C:\SetupFiles\WindowsServer\ISOs"
$fodIsoFilename = "FOD_ISO_filename.iso"

New-Item -ItemType Directory -Path $isoFolder
Copy-Item -Path "FODShare:\$fodIsoFilename" -Destination $isoFolder -
Verbose
```

3. Mount the FOD ISO by using the following command:

```
PowerShell

$fodIso = Mount-DiskImage -ImagePath "$isoFolder\$fodIsoFilename"
```

4. Run the following command to get the drive letter that the FOD ISO has been mounted to:

```
PowerShell

$fodDriveLetter = ($fodIso | Get-Volume).DriveLetter
```

5. Run the following command (depending on the operating system version):

   For Windows Server 2022:

```
PowerShell

Add-WindowsCapability -Online -Name
ServerCore.AppCompatibility~~~~0.0.1.0 -Source
${fodDriveLetter}:\LanguagesAndOptionalFeatures\ -LimitAccess
```

   For previous versions of Windows Server:

```
PowerShell
```

```
Add-WindowsCapability -Online -Name
ServerCore.AppCompatibility~~~~0.0.1.0 -Source ${fodDriveLetter}:\ -
LimitAccess
```

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

Optionally add Internet Explorer 11 to Server Core

> **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.

> **Note**
>
> Starting with Windows Server 2022, although Internet Explorer 11 can be added to Server Core installations of Windows Server, **Microsoft Edge** should be used instead. Microsoft Edge has **Internet Explorer mode** ("IE mode") built in, so you can access legacy Internet Explorer-based websites and applications straight from Microsoft Edge. Please see **here** for information on the lifecycle policy for Internet Explorer.

1. Sign in as Administrator on the Server Core computer that already has the App Compatibility FOD added and the FOD optional package ISO copied locally.

2. Mount the FOD ISO by using the following command. This step assumes that you've already copied the FOD ISO locally. If not, complete steps 1 and 2 from Mount the FOD ISO. The commands follow on from these two steps. Edit the variables with your folder location and ISO filename, and run the following commands, for example:

PowerShell

```
$isoFolder = "C:\SetupFiles\WindowsServer\ISOs"
$fodIsoFilename = "FOD_ISO_filename.iso"

$fodIso = Mount-DiskImage -ImagePath "$isoFolder\$fodIsoFilename"
```

3. Run the following command to get the drive letter that the FOD ISO has been mounted to:

```PowerShell
$fodDriveLetter = ($fodIso | Get-Volume).DriveLetter
```

4. Run the following commands (depending on your operating system version), using the `$packagePath` variable as the path to the Internet Explorer .cab file:

   For Windows Server 2022:

```PowerShell
$packagePath =
"${fodDriveLetter}:\LanguagesAndOptionalFeatures\Microsoft-Windows-
InternetExplorer-Optional-Package~31bf3856ad364e35~amd64~~.cab"

Add-WindowsPackage -Online -PackagePath $packagePath
```

   For previous versions of Windows Server:

```PowerShell
$packagePath = "${fodDriveLetter}:\Microsoft-Windows-InternetExplorer-
Optional-Package~31bf3856ad364e35~amd64~~.cab"

Add-WindowsPackage -Online -PackagePath $packagePath
```

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

Release notes and suggestions

ⓘ Important

- Packages installed using FoD won't remain in place after an in-place upgrade to a newer Windows Server version. You will have to install them again after the upgrade.
- Alternatively, you can add FoD packages to your upgrade media. Adding packages to your upgrade media ensures that the new version of any FoD package are present after the upgrade completes. For more info, see the

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

- 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, double-clicking to open locally saved .htm files isn't supported. However, you can **right-click** and choose **Open with Internet Explorer**, 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's 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 the PowerShell cmdlet **Install-WindowsFeature** to add IIS Management Console:

  ```
  PowerShell

  Install-WindowsFeature -Name Web-Mgmt-Console
  ```

- As a general point of guidance, when installing applications on Server Core (with or without these optional packages) it's sometimes necessary to use silent install options and instructions.

Adding to an offline WIM Server Core image

1. Download both the Languages and Optional Features ISO and the Windows Server ISO image files to a local folder on a Windows computer. You can complete these steps on a Windows desktop PC, it doesn't need to be running Windows Server with the Server Core installation option.

   - If you have a volume license, you can download the Windows Server Languages and Optional Features ISO image file from the same portal where the operating system ISO image file is obtained: Volume Licensing Service Center.
   - The Windows Server Languages and Optional Features ISO image file is also available on the Microsoft Evaluation Center or on the Visual Studio portal for subscribers.

> **Note**
>
> The Languages and Optional Features ISO image file is new for Windows Server 2022. Previous versions of Windows Server use the Features on Demand (FOD) ISO.

2. Mount both the Languages and Optional Features ISO and the Windows Server ISO by running the following commands in an elevated PowerShell session. Edit the variables with your folder location and ISO filename, and run the following commands, for example::

```PowerShell
$isoFolder = "C:\SetupFiles\WindowsServer\ISOs"
$fodIsoFilename = "FOD_ISO_filename.iso"
$wsIsoFilename = "Windows_Server_ISO_filename.iso"

$fodIso = Mount-DiskImage -ImagePath "$isoFolder\$fodIsoFilename"
$wsIso = Mount-DiskImage -ImagePath "$isoFolder\$wsIsoFilename"
```

3. Run the following command to get the drive letters that the FOD ISO and Windows Server ISO have been mounted to:

```PowerShell
$fodDriveLetter = ($fodIso | Get-Volume).DriveLetter
$wsDriveLetter = ($wsIso | Get-Volume).DriveLetter
```

4. Copy the contents of the Windows Server ISO file to a local folder, for example, **C:\SetupFiles\WindowsServer\Files**. The copy operation may take some time:

```PowerShell
$wsFiles = "C:\SetupFiles\WindowsServer\Files"
New-Item -ItemType Directory -Path $wsFiles

Copy-Item -Path ${wsDriveLetter}:\* -Destination $wsFiles -Recurse
```

5. Get the image name you want to modify within the install.wim file by using the following command. Add your path to the install.wim file to the `$installWimPath` variable, located inside the **sources** folder of the Windows Server ISO file. Note the names of the images available in this install.wim file from the output.

```PowerShell
```

```
$installWimPath =
"C:\SetupFiles\WindowsServer\Files\sources\install.wim"

Get-WindowsImage -ImagePath $installWimPath
```

6. 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 `$installWimPath` variable from the previous command.

   - `$wimImageName` - Enter the name of the image you want to mount from the output of the previous command. The example here uses **Windows Server 2022 Datacenter**.
   - `$wimMountFolder` - Specify an empty folder to use when accessing the contents of the install.wim file.

   PowerShell

   ```
   $wimImageName = "Windows Server 2022 Datacenter"
   $wimMountFolder = "C:\SetupFiles\WindowsServer\WIM"

   New-Item -ItemType Directory -Path $wimMountFolder
   Set-ItemProperty -Path $installWimPath -Name IsReadOnly -Value $false
   Mount-WindowsImage -ImagePath $installWimPath -Name $wimImageName -Path
   $wimMountFolder
   ```

7. Add the capabilities and packages you want to the mounted install.wim image by using the following commands (depending on the version), replacing the sample variable values with your own.

   - `$capabilityName` - Specify the name of the capability to install (in this case, the **AppCompatibility** capability).
   - `$packagePath` - Specify the path to the package to install (in this case, to the **Internet Explorer** cab file).

   For Windows Server 2022:

   PowerShell

   ```
   $capabilityName = "ServerCore.AppCompatibility~~~~0.0.1.0"
   $packagePath =
   "${fodDriveLetter}:\LanguagesAndOptionalFeatures\Microsoft-Windows-
   InternetExplorer-Optional-Package~31bf3856ad364e35~amd64~~.cab"

   Add-WindowsCapability -Path $wimMountFolder -Name $capabilityName -
   Source "${fodDriveLetter}:\LanguagesAndOptionalFeatures" -LimitAccess
   Add-WindowsPackage -Path $wimMountFolder -PackagePath $packagePath
   ```

For previous versions of Windows Server:

```PowerShell
$capabilityName = "ServerCore.AppCompatibility~~~~0.0.1.0"
$packagePath = "${fodDriveLetter}:\Microsoft-Windows-InternetExplorer-Optional-Package~31bf3856ad364e35~amd64~~.cab"

Add-WindowsCapability -Path $wimMountFolder -Name $capabilityName -Source "${fodDriveLetter}:\" -LimitAccess
Add-WindowsPackage -Path $wimMountFolder -PackagePath $packagePath
```

8. Dismount and commit changes to the install.wim file by using the following command, which uses the `$wimMountFolder` variable from previous commands:

```PowerShell
Dismount-WindowsImage -Path $wimMountFolder -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\Files**. This folder now contains the Windows Server installation files with the extra capabilities and optional packages included.

Windows Server 2022 and Microsoft server applications compatibility

Article • 02/08/2023

This table lists Microsoft server applications that support installation and functionality on Window Server 2022. This information is for quick reference and isn't 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.

> **Tip**
>
> 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
Azure DevOps Server 2020.1	Yes*	Yes	Yes	Azure DevOps Server 2020.1 release notes
Configuration Manager (version 2107)	Yes as a managed client and distribution point. No as a site server.	Yes as a site server/site systems and a managed client.	Yes	Support for Windows Server 2022
Exchange Server 2019 CU12 and later	Yes	Yes	Yes	Exchange Server supportability matrix
Host Integration Server 2020	Yes	Yes	Yes	HIS 2020 - What's New, Release Notes, System Requirements, and Installation
Microsoft 365 Apps	No	Yes	Yes	Windows and Office configuration support matrix

Product	Supported on Server Core	Supported on Server with Desktop Experience	Released	Product Web Link
Office Online Server	No	Yes	Yes	Plan Office Online Server
Project Server 2019	No	Yes	Yes	Software requirements for Project Server 2019 - Project Server
Project Server Subscription Edition	Yes	Yes	Yes	Software requirements for Project Server Subscription Edition
SharePoint Server 2019	No	Yes	Yes	Hardware and software requirements for SharePoint Server 2019
SharePoint Server Subscription Edition	Yes	Yes	Yes	System requirements for SharePoint Server Subscription edition
SQL Server 2017	Yes*	Yes	Yes	Hardware and Software Requirements for Installing SQL Server 2017
SQL Server 2019	Yes*	Yes	Yes	Hardware and Software Requirements for Installing SQL Server 2019
System Center Data Protection Manager 2019	Yes as a backup workload. No as a DPM server.	Yes as a backup workload. No as a DPM server.	Yes	Preparing your environment for System Center Data Protection Manager
System Center Data Protection Manager 2022	Yes*	Yes	Yes	Preparing your environment for System Center Data Protection Manager
System Center Operations Manager 2019	Yes as an agent. No as a Management Server**	Yes as an agent. No as a Management Server**.	Yes	System requirements for System Center Operations Manager

Product	Supported on Server Core	Supported on Server with Desktop Experience	Released	Product Web Link
System Center Operations Manager 2022	Yes*	Yes	Yes	System requirements for System Center Operations Manager
System Center Virtual Machine Manager 2022	Yes*	Yes	Yes	System requirements for System Center Virtual Machine Manager

* May have limitations or may require the Server Core App Compatibility Feature on Demand (FOD). For more information, see specific product or Feature on Demand documentation.

** Refer to Product Web Link

Windows Server 2019 and Microsoft server applications compatibility

Article • 12/23/2021

This table lists Microsoft server applications that support installation and functionality on Window 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.

> **Tip**
>
> 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
Azure DevOps Server 2019	Yes*	Yes	Yes	Azure DevOps Server 2019
Azure DevOps Server 2020	Yes*	Yes	Yes	Azure DevOps Server 2020
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
Exchange Server 2019	Yes	Yes	Yes	Exchange Server system requirements
Host Integration Server 2016, CU3	Yes	Yes	Yes	Host Integration Server system requirements
Office Online Server	No	Yes	Yes	Plan Office Online Server
Project Server 2016	No	Yes	Yes	Software requirements for Project Server 2016

Product	Supported on Server Core	Supported on Server with Desktop Experience	Released	Product Web Link
Project Server 2019	No	Yes	Yes	Software requirements for Project Server 2019
Project Server Subscription Edition	Yes	Yes	Yes	Software requirements for Project Server Subscription Edition
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
SharePoint Server Subscription Edition	Yes	Yes	Yes	System requirements for SharePoint Server Subscription edition
Skype for Business 2019	No	Yes	Yes	Install prerequisites for Skype for Business Server
SQL Server 2014	Yes*	Yes	Yes	Hardware and Software Requirements for Installing SQL Server 2014
SQL Server 2016	Yes*	Yes	Yes	Hardware and Software Requirements for Installing SQL Server 2016
SQL Server 2017	Yes*	Yes	Yes	Hardware and Software Requirements for Installing SQL Server 2017
SQL Server 2019	Yes*	Yes	Yes	Hardware and Software Requirements for Installing SQL Server 2019

Product	Supported on Server Core	Supported on Server with Desktop Experience	Released	Product Web Link
System Center Data Protection Manager 2019	No	Yes	Yes	Preparing your environment for System Center Data Protection Manager
System Center Operations Manager 2019	Yes*	Yes	Yes	System requirements for System Center Operations Manager
System Center Virtual Machine Manager 2019	Yes*	Yes	Yes	System requirements for System Center Virtual Machine Manager

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

Windows Server 2016 and Microsoft server applications compatibility

Article • 12/23/2021

This table lists Microsoft server applications that support installation and functionality on Window Server 2016. 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.

> **Tip**
>
> 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	Released	Product Web Link
BizTalk Server 2016	Yes	Microsoft BizTalk Server
Configuration Manager (version 1606)	Yes	What's new in version 1606 of Configuration Manager
Exchange Server 2016	Yes	Updates for Exchange 2016
Host Integration Server 2016	Yes	What's New in HIS 2016
Office Online Server	Yes	Plan Office Online Server
Project Server 2016	Yes	Software requirements for Project Server 2016
Project Server 2019	Yes	Software requirements for Project Server 2019
SharePoint Server 2016	Yes	Hardware and software requirements for SharePoint Server 2016
SharePoint Server 2019	Yes	Hardware and software requirements for SharePoint Server 2019
Skype for Business Server 2015	Yes	How to install Skype for Business Server 2015 on Windows Server 2016
SQL Server 2012	Yes	Hardware and Software Requirements for Installing SQL Server 2012

Product	Released	Product Web Link
SQL Server 2014	Yes	Hardware and Software Requirements for Installing SQL Server 2014
SQL Server 2016	Yes	SQL Server 2016
System Center Virtual Machine Manager 2016	Yes	What's New in System Center
System Center Operations Manager 2016	Yes	What's New in System Center
System Center Data Protection Manager 2016	Yes	What's New in System Center
Visual Studio Team Foundation Server 2017	Yes	Team Foundation Server 2017

Azure Hybrid Benefit for Windows Server

Article • 10/06/2023

Azure Hybrid Benefit enables commercial customers to use their on-premises licenses that also have either active Software Assurance (SA) or a qualifying subscription to get Windows virtual machines (VMs) on Azure at a reduced cost. This article focuses on benefits for Windows Server licenses with SA or a qualifying subscription to get cost savings for Windows Server VMs in Azure, Azure Stack HCI, and Azure Kubernetes Service (AKS) hybrid deployments.

For other Azure hybrid benefits (for example, SQL Server), see Azure Hybrid Benefit.

What qualifies you for Azure Hybrid Benefit?

To qualify for Azure Hybrid Benefit for Windows Server, you need on-premises core licenses for Windows Server with active Software Assurance or qualifying subscription licenses. Software Assurance and qualifying subscription licenses are only available as part of Commercial Licensing agreements. To learn more about Commercial Licensing, see Microsoft Licensing Resources. To learn more about Windows Server core licenses, see Windows Server product licensing.

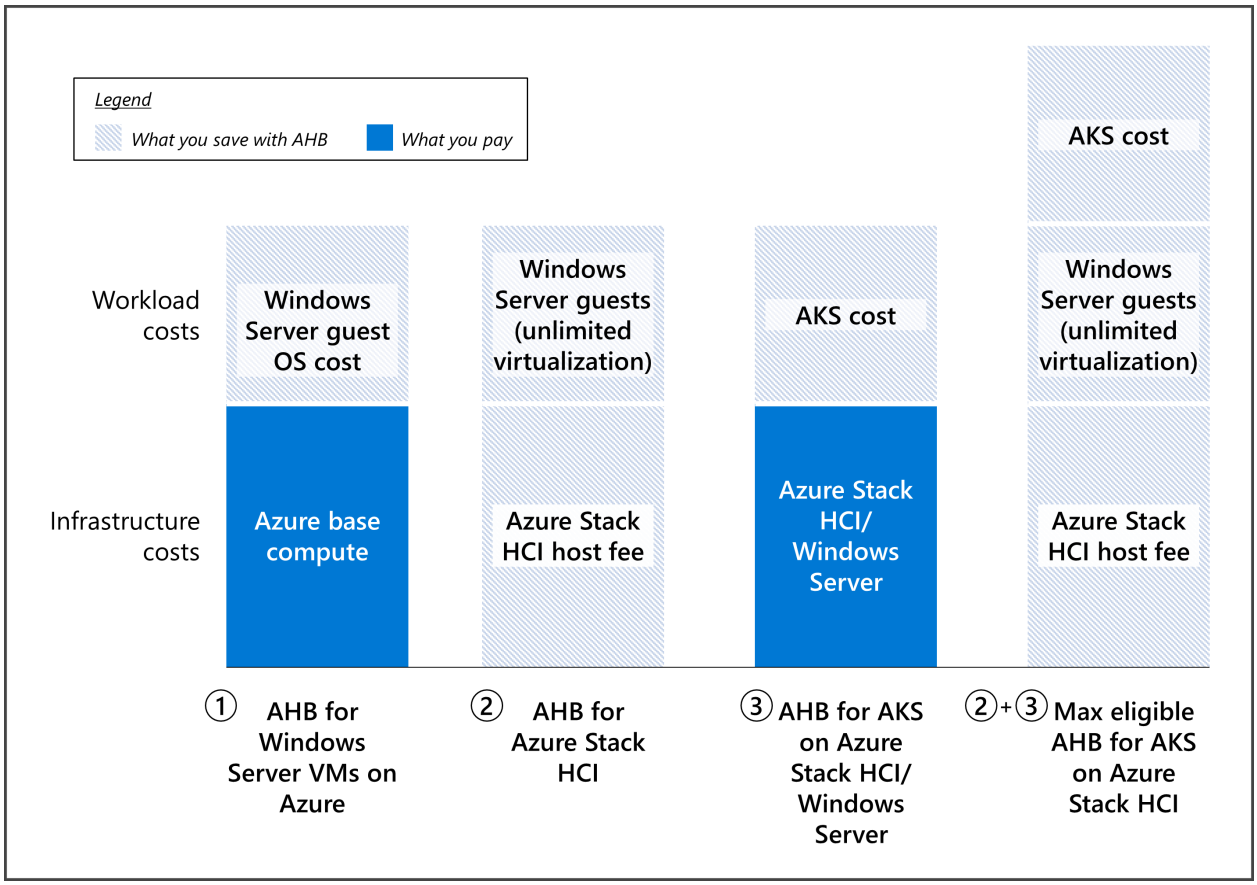
> **Important**
>
> Workloads using Azure Hybrid Benefit can run only during the Software Assurance or subscription license term. When the Software Assurance or subscription license term approaches expiration, you must either renew your agreement with either Software Assurance or a subscription license, disable the hybrid benefit functionality, or deprovision those workloads that are using Azure Hybrid Benefit.

What's included in Azure Hybrid Benefit?

Customers with Windows Server Software Assurance or qualifying subscription licenses can use Azure Hybrid Benefit to further reduce costs in the cloud and in datacenter and edge locations.

Azure Hybrid Benefit includes the following cost savings:

- **Windows Server VMs on Azure:** The license for Windows Server is covered by Azure Hybrid Benefit, so you only need to pay for the base compute rate of the VM. The base compute rate is equal to the Linux rate for VMs.
- **Azure Stack HCI:** The Azure Stack HCI host fee and Windows Server subscription fee are waived with Azure Hybrid Benefit. That is, unlimited virtualization rights are provided at no extra cost. You still pay other costs associated with Azure Stack HCI (for example, customer-managed hardware, Azure services, and workloads). Software Assurance must be active to use this benefit.
- **AKS:** Run AKS on Windows Server and Azure Stack HCI at no extra cost. You still pay for the underlying host infrastructure and any licenses for Windows containers unless you're also eligible for Azure Hybrid Benefit for Azure Stack HCI. With Azure Hybrid Benefit for Azure Stack HCI, you can waive fees for the Azure Stack HCI host and Windows Server subscription.



Pricing for Azure Hybrid Benefit

To evaluate your potential cost savings, you can use these resources:

- **Windows VMs on Azure:** Windows Virtual Machine Pricing. Use the Azure Hybrid Benefit Savings Calculator to estimate cost savings, or compare Windows VM pricing with and without Azure Hybrid Benefit.

- **Azure Stack HCI:** Azure Stack HCI pricing.
- **Azure Kubernetes Service (AKS):** AKS on Azure Stack HCI pricing.

Getting Azure Hybrid Benefit for Windows VMs in Azure

Follow the guidance in this section to get and maintain Azure Hybrid Benefit for your Windows VMs in Azure.

Licensing prerequisites

To qualify for Azure Hybrid Benefit for Windows VMs in Azure, you must meet the following licensing prerequisites.

Types of license

- Windows Server Standard with active Software Assurance.
- Windows Server Datacenter with active Software Assurance.

Number of licenses

You need a minimum of 8 core licenses (Datacenter or Standard edition) per VM. For example, 8 core licenses are still required if you run a 4-core instance. You may also run instances larger than 8 cores by allocating licenses equal to the core size of the instance. For example, 12 core licenses are required for a 12-core instance. For customers with processor licenses, each 2-core processor license is equivalent to 16 core licenses.

Use rights

- **Windows Server Standard edition:** Licenses must be used either on-premises or in Azure, but not at the same time. The only exception is on a one-time basis, for up to 180 days, to allow you to migrate the same workloads to Azure.
- **Windows Server Datacenter edition:** Licenses allow simultaneous usage on-premises and in Azure. Dual Use Rights don't apply for licenses allocated for Unlimited Virtualization Rights.

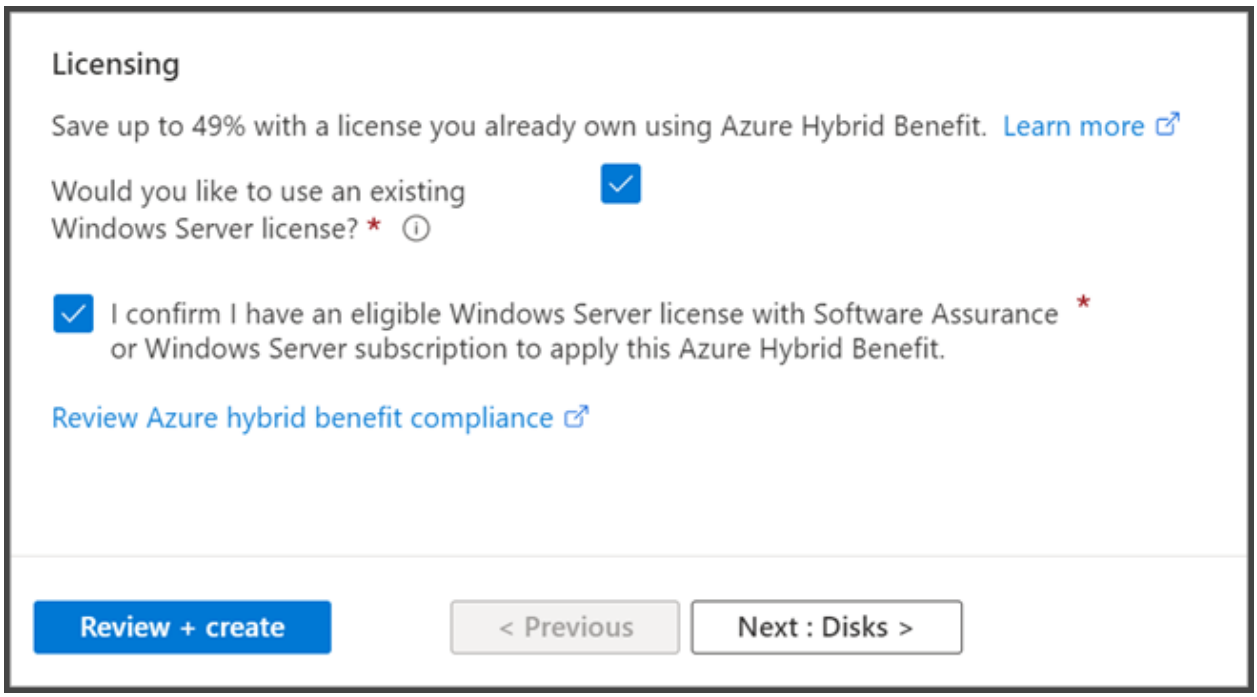
Unlimited virtualization

Unlimited Virtualization Rights refers to the right to use any number of Windows Server VMs on a host.

- **Windows Server Datacenter edition:** You can use any number of Windows Server VMs on an Azure dedicated host if you allocate Windows Server Datacenter licenses with active SA or subscription for all the available physical cores on that Azure server.
- **Windows Server Standard edition:** Unlimited Virtualization Rights aren't available.

How to apply Azure Hybrid Benefit for Windows VMs in Azure

To learn how to deploy Windows Server VMs in Azure with Azure Hybrid Benefit, follow the steps in Explore Azure Hybrid Benefit for Windows VMs. One way to activate Azure Hybrid Benefit for a Windows Server VM is to check the box under **Licensing** during VM creation, as shown in the following screenshot.



How to maintain compliance

If you apply Azure Hybrid Benefit to your Windows Server VMs, verify the number of eligible licenses and the Software Assurance (or subscription) coverage period before you activate this benefit. Use the preceding guidelines to make sure you deploy the correct number of Windows Server VMs with this benefit.

If you already have Windows Server VMs running with Azure Hybrid Benefit, perform an inventory to see how many units you're running, and check this number against your

Software Assurance or subscription licenses. You can contact your Microsoft licensing specialist to validate your Software Assurance licensing position.

To see and count all VMs that are deployed with Azure Hybrid Benefit in an Azure subscription, list all VMs and virtual machine scale sets using the steps in Explore Azure Hybrid Benefit for Windows VMs.

You can also look at your Microsoft Azure bill to determine how many VMs with Azure Hybrid Benefit for Windows Server you're running. You can find information about the number of instances with the benefit under **Additional Info**:

JSON


```
"
{"ImageType":"WindowsServerBYOL","ServiceType":"Standard_A1","VMName":"","Us
ageType":"ComputeHR"}"
```


Billing isn't applied in real time. Expect a delay of several hours after you activate a Windows Server VM with Azure Hybrid Benefit before the VM shows on your bill.

To get a comprehensive view of your licensing position, perform an inventory in each of your Azure subscriptions. Confirm that you're fully licensed for the Windows Server VMs running with Azure Hybrid Benefit. You don't need to take any further action.

Perform an inventory regularly to make sure you're using any license benefits that you're entitled to. Regular inventories can help you reduce costs and make sure that you always have enough licenses to cover the Windows Server VMs you've deployed with Azure Hybrid Benefit.

If you don't have enough eligible Windows Server licenses for your deployed VMs, you have three choices:

- Purchase extra Windows Server licenses covered by Software Assurance or subscription through a commercial licensing agreement.
- Disable Azure Hybrid Benefit for some of your VMs and purchase them at regular Azure hourly rates.
- Deallocate some VMs.

> ⓘ **Note**
>
> Microsoft reserves the right to audit customers at any time to verify eligibility for Azure Hybrid Benefit utilization.

Getting Azure Hybrid Benefit for Azure Stack HCI

Use the guidance in this section to get Azure Hybrid Benefit for your Azure Stack HCI infrastructure.

Licensing prerequisites

To qualify for Azure Hybrid Benefit for Azure Stack HCI, you must meet the following licensing prerequisites.

Types of license

- Windows Server Datacenter with active Software Assurance licenses only. Software Assurance must be active to use this benefit.

Number of licenses

- Each Windows Server core license entitles use on one physical core of Azure Stack HCI. You need to allocate enough core licenses for all physical cores on servers in the Azure Stack HCI cluster.

Unlimited virtualization

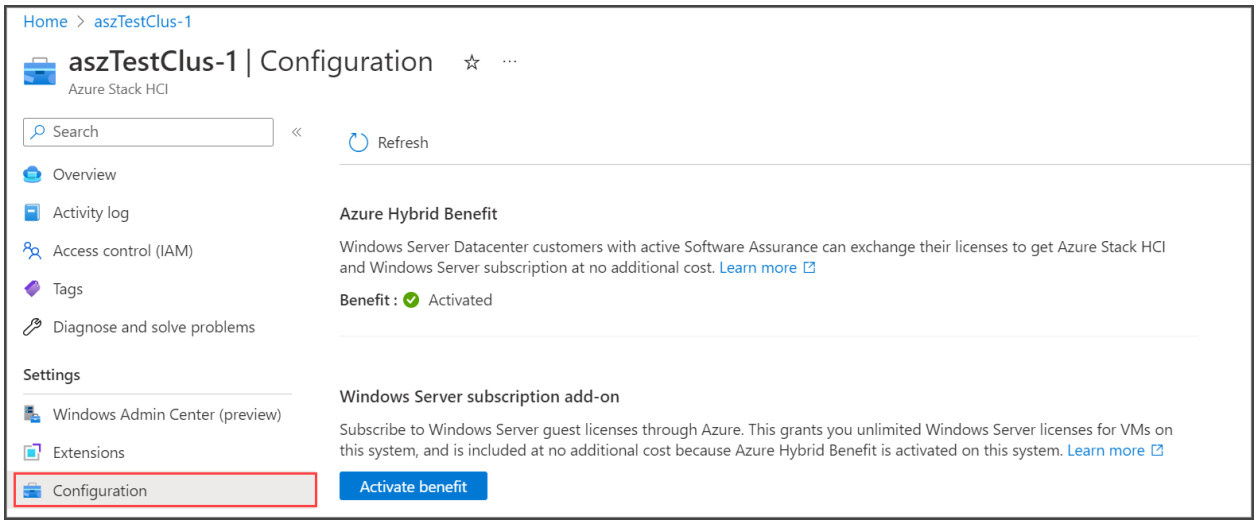
- You can use any number of Windows Server VMs on the Azure Stack HCI cluster if you allocate enough core licenses for all physical cores on servers in the Azure Stack HCI cluster.

Use rights

- Licenses must be used either on-premises or on Azure Stack HCI, but not on both. You have 180 days of concurrent licensing to migrate your servers.

How to apply Azure Hybrid Benefit for Azure Stack HCI

You can learn how to deploy Azure Hybrid Benefit for Azure Stack HCI by following the steps in Azure Stack HCI billing and payment. One method is to activate the benefit from the **Configuration** pane of the Azure Stack HCI resource, as shown in the following screenshot.



Getting Azure Hybrid Benefit for AKS

Follow the guidance in this section to get Azure Hybrid Benefit for AKS.

Licensing prerequisites

To qualify for Azure Hybrid Benefit for AKS, you must meet the following licensing prerequisites.

Eligible hosts

- Windows Server 2019 or later (Datacenter only), or
- Azure Stack HCI

Types of license

- Windows Server Standard with active Software Assurance or subscription.
- Windows Server Datacenter with active Software Assurance or subscription.

Number of licenses

- Each Windows Server core license entitles use on one virtual core of AKS.

Use rights

- Azure Hybrid Benefit for AKS is additive. Core licenses used for Azure Hybrid Benefit for AKS can be used at the same time with on-premises Windows Server licensing, as well as Azure Hybrid Benefit for other workloads in this article.

How to apply Azure Hybrid Benefit for AKS

To get started with Azure Hybrid Benefit for AKS, see Azure Hybrid Benefit for AKS.

FAQ: Azure Hybrid Benefit

Which regions are eligible for Azure Hybrid Benefit?

Azure Hybrid Benefit is available across all Azure regions and sovereign clouds.

What happens to my benefits if my Software Assurance or subscription expires?

To use these benefits, your Software Assurance or qualifying subscription must be active. If you choose not to renew your Software Assurance or subscription when it expires, you need to remove your benefits from your resources in the Azure portal.

What is Software Assurance?

Software Assurance is a comprehensive Volume Licensing program. Software Assurance is only available through Volume Licensing and is purchased when you buy or renew a Volume Licensing agreement. It's included with some agreements and is an optional purchase with others. Software Assurance benefits include new product version rights, support, license mobility rights, and a unique set of technologies and services to maximize your IT investments.

For information about Volume Licensing, see Microsoft Licensing. To learn more about Software Assurance benefits, and how each benefit can help meet your business needs, see Software Assurance benefits.

What is a subscription license?

Subscription licenses are licenses to run the software only during the term of the subscription. Subscription licenses don't include perpetual rights to run the software.

How can customers get Software Assurance?

You can purchase Software Assurance through Volume Licensing. Your Software Assurance benefits are activated in the Volume Licensing Service Center (VLSC). If your

organization has a Microsoft Products and Services Agreement (MPSA), the Business Center is your destination for easy management of your Software Assurance benefits.

See also

- Azure Hybrid Benefit product page
- Explore Azure Hybrid Benefit for Windows VMs
- Azure Hybrid Benefit for Azure Stack HCI

Hotpatch for virtual machines

Article • 10/10/2023

Hotpatching is a way to install OS security updates on supported *Windows Server Datacenter: Azure Edition* virtual machines (VMs) that doesn't require a reboot after installation. It works by patching the in-memory code of running processes without the need to restart the process. This article covers information about hotpatch for supported VMs, which has the following benefits:

- Fewer binaries mean update install faster and consume less disk and CPU resources.
- Lower workload impact with fewer reboots.
- Better protection, as the hotpatch update packages are scoped to Windows security updates that install faster without rebooting.
- Reduces the time exposed to security risks and change windows, and easier patch orchestration with Azure Update Manager.

Supported platforms

Hotpatch is supported only on VMs and Azure Stack HCI created from images with the exact combination of publisher, offer and sku from the below OS images list. Windows Server container base images or Custom images or any other publisher, offer, sku combinations aren't supported.

Publisher	OS Offer	Sku
MicrosoftWindowsServer	WindowsServer	2022-Datacenter-Azure-Edition-Core
MicrosoftWindowsServer	WindowsServer	2022-Datacenter-Azure-Edition-Core-smalldisk
MicrosoftWindowsServer	WindowsServer	2022-Datacenter-Azure-Edition-Hotpatch
MicrosoftWindowsServer	WindowsServer	2022-Datacenter-Azure-Edition-Hotpatch-smalldisk

To get started using Hotpatch, use your preferred method to create an Azure or Azure Stack HCI VM, and select one of the following images that you would like to use. Hotpatch is selected by default when creating an Azure VM in the Azure portal.

- Windows Server 2022 Datacenter: Azure Edition Hotpatch (Desktop Experience)
- Windows Server 2022 Datacenter: Azure Edition Core[1]

[1] Hotpatch is enabled by default on Server Core images.

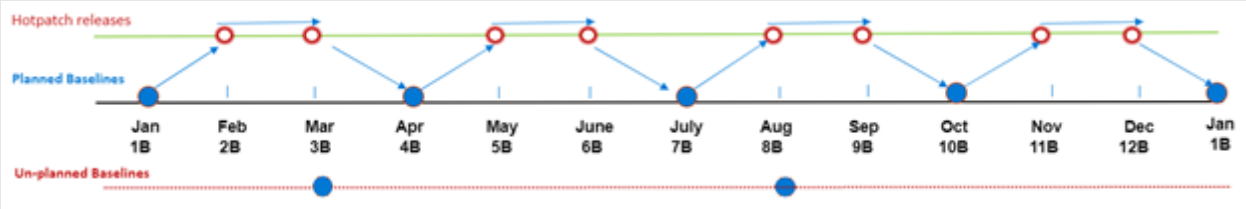
For more information about the available images, see the Windows Server 2022 Datacenter Azure Marketplace product.

How Hotpatch works

Hotpatch works by first establishing a baseline with the current Cumulative Update for Windows Server. Periodically (starting every three months), the baseline is refreshed with the latest Cumulative Update, then hotpatches are released for two months following. For example, if January is a Cumulative Update, February and March would be a hotpatch release. For the hotpatch release schedule, see Release notes for Hotpatch in Azure Automanage for Windows Server 2022.

Hotpatches contains updates that don't require a reboot. Because Hotpatch patches the in-memory code of running processes without the need to restart the process, your applications are unaffected by the patching process. This action is separate from any potential performance and functionality implications of the patch itself.

The following image is an example of an annual three-month schedule (including example unplanned baselines due to zero-day fixes).



There are two types of baselines: **Planned baselines** and **Unplanned baselines**.

- **Planned baselines** are released on a regular cadence, with hotpatch releases in between. Planned baselines include all the updates in a comparable *Latest Cumulative Update* for that month, and require a reboot.
  - The sample schedule illustrates four planned baseline releases in a calendar year (five total in the diagram), and eight hotpatch releases.

- **Unplanned baselines** are released when an important update (such as a zero-day fix) is released, and that particular update can't be released as a hotpatch. When unplanned baselines are released, a hotpatch release is replaced with an unplanned baseline in that month. Unplanned baselines also include all the updates in a comparable *Latest Cumulative Update* for that month, and also require a reboot.
  - The sample schedule illustrates two unplanned baselines that would replace the hotpatch releases for those months (the actual number of unplanned baselines in a year isn't known in advance).

Supported updates

Hotpatch covers Windows Security updates and maintains parity with the content of security updates issued to in the regular (nonhotpatch) Windows update channel.

There are some important considerations to running a supported *Windows Server Azure Edition* VM with hotpatch enabled. Reboots are still required to install updates that aren't included in the hotpatch program. Reboots are also required periodically after a new baseline has been installed. Reboots keep the VM in sync with nonsecurity patches included in the latest cumulative update.

- Patches that are currently not included in the hotpatch program include non security updates released for Windows, .NET updates and non-Windows updates (such as drivers, firmware update etc.). These types of patches may need a reboot during Hotpatch months.

Patch orchestration process

Hotpatch is an extension of Windows Update and typical orchestration processes. Patch orchestration tools vary depending on your platform. To orchestrate Hotpatch:

- **Azure:** Virtual machines created in Azure are enabled for Automatic VM Guest Patching by default with a supported *Windows Server Datacenter: Azure Edition* image. Automatic VM guest patching in Azure:
  - Patches classified as Critical or Security are automatically downloaded and applied on the VM.
  - Patches are applied during off-peak hours in the VM's time zone.
  - Azure manages patch orchestration and patches are applied following availability-first principles.
  - Virtual machine health, as determined through platform health signals, is monitored to detect patching failures.

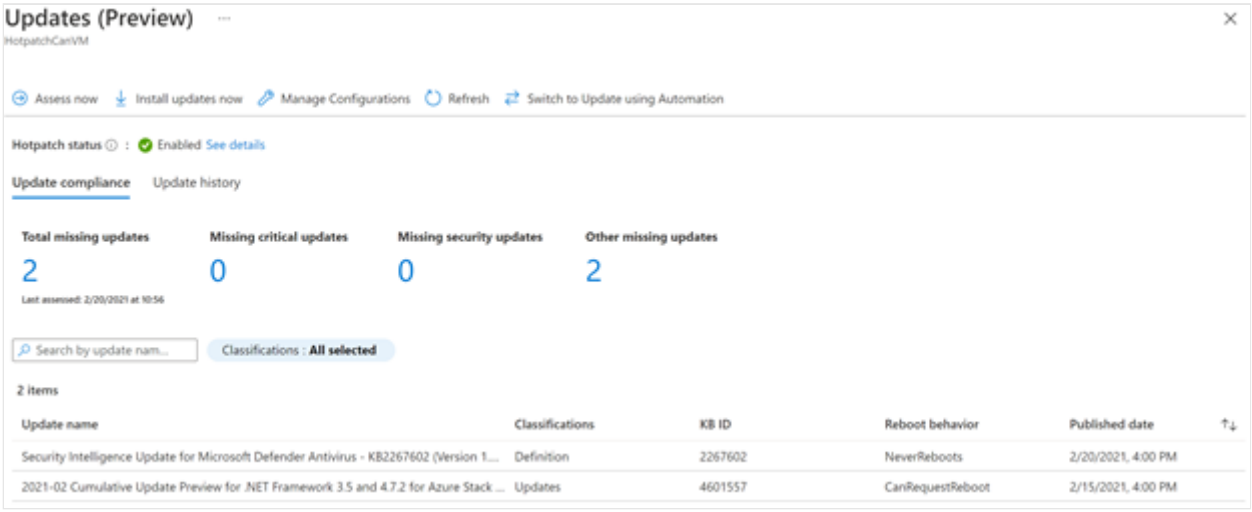
> **Note**
>
> You can't create VM scale sets (VMSS) with Uniform orchestration on Azure Edition images with Hotpatch. To learn more about which features are supported by Uniform orchestration for scale sets, see **A comparison of Flexible, Uniform, and availability sets**.

- **Azure Stack HCI:** Hotpatch updates for virtual machines created on Azure Stack HCI are orchestrated using:
    - Group Policy to configure the Windows Update client settings.
    - Configuring Windows Update client settings, or SCONFIG for Server Core.
    - A third-party patch management solution.

Understand the patch status for your VM in Azure

To view the patch status for your VM, browse to the VM Overview in the Azure portal, under Operations, select **Updates**. Under the **Recommended updates** section, you can view the latest patches and Hotpatch status for your VM.

On this screen, you see the hotpatch status for your VM. You can also review if there any available patches for your VM that haven't been installed. As described in the 'Patch installation' previous section, all security and critical updates are automatically installed on your VM using Automatic VM Guest Patching and no extra actions are required. Patches with other update classifications aren't automatically installed. Instead, they're viewable in the list of available patches under the **Update compliance** tab. You can also view the history of update deployments on your VM through the **Update history**. Update history from the past 30 days is displayed, along with patch installation details.



With automatic VM guest patching, your VM is periodically and automatically assessed for available updates. These periodic assessments ensure that available patches are detected. You can view the results of the assessment on the Updates screen in the previous image, including the time of the last assessment. You can also choose to trigger an on-demand patch assessment for your VM at any time using the 'Assess now' option and review the results after assessment completes.

Similar to on-demand assessment, you can also install patches on-demand for your VM using the 'Install updates now' option. Here you can choose to install all updates under specific patch classifications. You can also specify updates to include or exclude by providing a list of individual knowledge base articles. Patches installed on-demand aren't installed using availability-first principles and may require more reboots and VM downtime for update installation.

You can also view the installed patches using the Get-HotFix PowerShell command or using the Settings app when using the Desktop Experience.

Rollback support on Hotpatching

The installation of Hotpatch or Baseline updates doesn't support automatic rollback. If a VM experiences an issue during or after an update, you'll have to uninstall the latest update and install the last known good baseline update. You'll need to reboot the VM after rollback.

Next steps

- Automatic VM Guest Patching
- Enable Hotpatch for Azure Edition virtual machines built from ISO
- Azure Update Management

What is Secured-core server?

Article • 04/06/2023

> Applies to: Windows Server 2022, Azure Stack HCI version 21H2 and later

Secured-core is a collection of capabilities that offers built-in hardware, firmware, driver and operating system security features. The protection provided by Secured-core systems begins before the operating system boots and continues whilst running. Secured-core server is designed to deliver a secure platform for critical data and applications.

Secured-core server is built on three key security pillars:

- Creating a hardware backed root of trust.
- Defense against firmware level attacks.
- Protecting the OS from the execution of unverified code.

What makes a Secured-core server

The Secured-core initiative started with Windows PCs through a deep collaboration between Microsoft and PC manufacturing partners to provide the most elevated Windows security ever. Microsoft has expanded the partnership further with server manufacturing partners to help ensure Windows Server delivers a secure operating system environment.

Windows Server integrates closely with hardware to provide increasing levels of security:

- Recommended baseline: The recommended minimum for all systems to provide foundational system integrity using TPM 2.0 for a hardware root of trust and Secure Boot. TPM2.0 and Secure boot are required for Windows Server hardware certification. To learn more, see Microsoft raises the security standard for next major Windows Server release
- Secured-core server: Recommended for systems and industries requiring higher levels of assurance. Secured-core server builds on the previous features and uses advanced processor capabilities to provide protection from firmware attacks.

The following table shows how each security concept and feature are used to create a Secured-core server.

Concept	Feature	Requirement	Recommended baseline	Secured-Core server
Create a hardware backed root of trust				
	Secure Boot	Secure Boot is enabled in the Unified Extensible Firmware Interface (UEFI) BIOS by default.	✓	✓
	Trusted Platform Module (TPM) 2.0	Meet the latest Microsoft requirements for the Trusted Computing Group (TCG) specification.	✓	✓
	Certified for Windows Server	Demonstrates that a server system meets Microsoft's highest technical bar for security, reliability and manageability.	✓	✓
	Boot DMA protection	Support on devices that have the Input/Output Memory Management Unit (IOMMU). For example, Intel VT-D or AMD-Vi.		✓
Defend against firmware level attacks				
	System Guard Secure Launch	Enabled in the operating system with Dynamic Root of Trust for Measurement (DRTM) compatible Intel and AMD hardware.		✓
Protect the OS from execution of unverified code				
	Virtualization-based Security (VBS)	Requires the Windows hypervisor, which is only supported on 64-bit	✓	✓

Concept	Feature	Requirement	Recommended baseline	Secured-Core server
		processors with virtualization extensions, including Intel VT-X and AMD-v.		
	Hypervisor Enhanced Code Integrity (HVCI)	Hypervisor Code Integrity (HVCI)-compatible drivers plus VBS requirements.	✓	✓

Create a hardware backed root of trust

UEFI Secure boot is a security standard that protects your servers from malicious rootkits by verifying your systems boot components. Secure boot verifies a trusted author has digitally signed the UEFI firmware drivers and applications. When the server is started, the firmware checks the signature of each boot component including firmware drivers and the OS. If the signatures are valid, the server boots and the firmware gives control to the OS.

To learn more about the boot process, see Secure the Windows boot process.

TPM 2.0 provides a secure, hardware-backed storage for sensitive keys and data. Every component loaded during the boot process is measured and the measurements stored in the TPM. By verifying the hardware root-of-trust it elevates the protection provided by capabilities like BitLocker, which uses TPM 2.0 and facilitates the creation of attestation-based workflows. These attestation-based workflows can be incorporated into zero-trust security strategies.

Learn more about Trusted Platform Modules and how Windows uses the TPM.

Along with Secure Boot and TPM 2.0, Windows Server Secured-core uses Boot DMA protection on compatible processors that have the Input/Output Memory Management Unit (IOMMU). For example, Intel VT-D or AMD-Vi. With boot DMA protection, systems are protected from Direct Memory Access (DMA) attacks during boot and during the operating system runtime.

Defend against firmware level attacks

Endpoint protection and detection solutions usually have limited visibility of firmware, given that firmware runs underneath of the operating system. Firmware has a higher level of access and privilege than operating system and hypervisor kernel, making it an attractive target for attackers. Attacks targeting firmware undermine other security measures implemented by the operating system, making it more difficult to identify when a system or user has been compromised.

Beginning with Windows Server 2022, System Guard Secure Launch protects the boot process from firmware attacks by using hardware capabilities from AMD and Intel. With processor support for Dynamic Root of Trust for Measurement (DRTM) technology, Secured-core servers put firmware in a hardware-backed sandbox helping to limit the effects of vulnerabilities in highly privileged firmware code. System Guard uses the DRTM capabilities that are built into compatible processors to launch the operating system, ensuring the system launches into a trusted stated using verified code.

Protect the OS from execution of unverified code

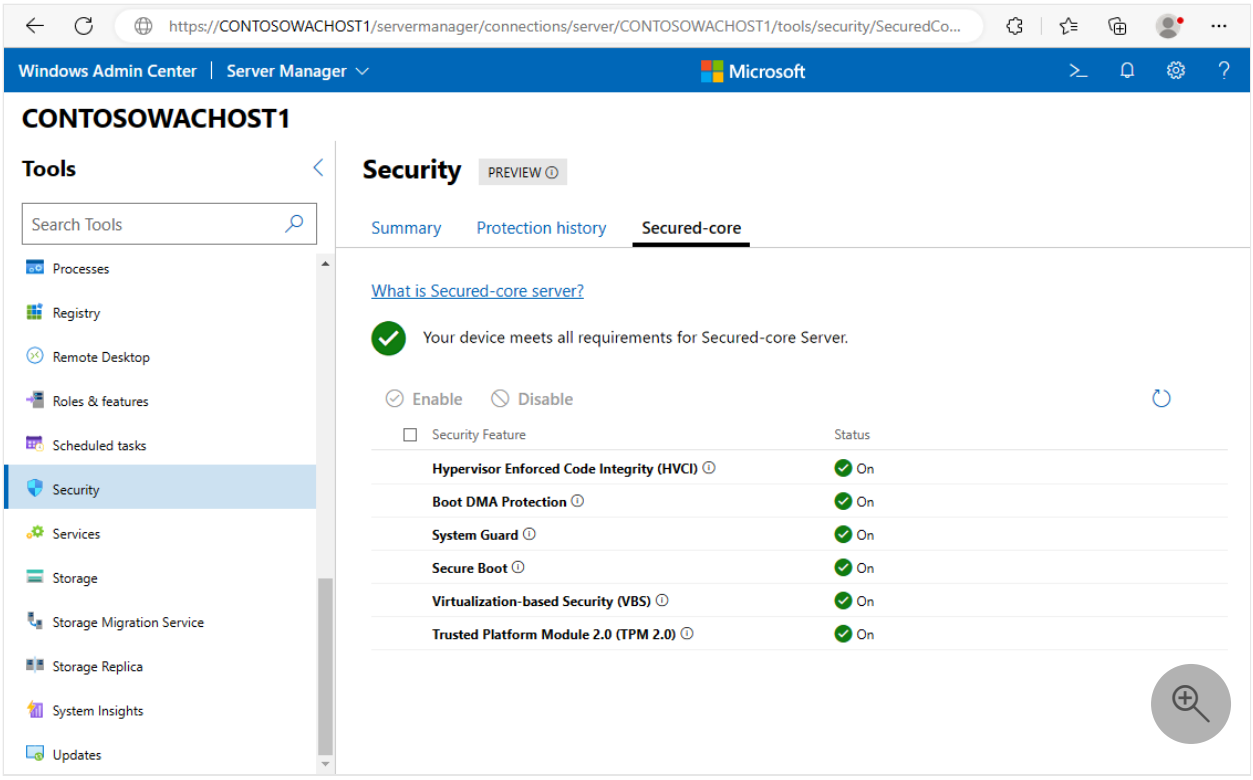
Secured-core server uses Virtualization Based Security (VBS) and hypervisor-protected code integrity (HVCI) to create and isolate a secure region of memory from the normal operating system. VBS uses the Windows hypervisor to create a Virtual Secure Mode (VSM) to offer security boundaries within the operating system, which can be used for other security solutions.

HVCI, commonly referred to as Memory integrity protection, is a security solution that helps ensure that only signed and trusted code is allowed to execute in the kernel. Using only signed and trusted code prevents attacks that attempt to modify the kernel mode code. For example, attacks that modify drivers, or exploits such as WannaCry that attempt to inject malicious code into the kernel.

To learn more about VBS and hardware requirements, see Virtualization-based Security.

Simplified management

You can view and configure the OS security features of Secured-core systems using Windows PowerShell or the security extension in Windows Admin Center. With Azure Stack HCI Integrated Systems, manufacturing partners have further simplified the configuration experience for customers so that Microsoft's best server security is available right out of the box.



Learn more about Windows Admin Center.

Preventative defense

You can proactively defend against and disrupt many of the paths attackers use to exploit systems by enabling Secured-core functionality. Secured-core server enables advanced security features at the bottom layers of the technology stack, protecting the most privileged areas of the system before many security tools are aware of exploits. It also occurs without the need for extra tasks or monitoring by IT and SecOps teams.

Begin your Secured-core journey

You can find hardware certified for Secured-core server from the Windows Server Catalog, and Azure Stack HCI servers in the Azure Stack HCI Catalog. These certified servers come fully equipped with industry-leading security mitigations built into the hardware, firmware, and the operating system to help thwart some of the most advanced attack vectors.

Next steps

Now you understand what Secured-core server is, here are some resources to get you started. Learn about how:

- Configure Secured-core server.

- Microsoft brings advanced hardware security to Server and Edge with Secured-core in the Microsoft Security Blog.
- New Secured-core servers are now available from the Microsoft ecosystem to help secure your infrastructure in the Microsoft Security Blog.
- Building Windows-compatible devices, systems, and filter drivers across all Windows Platforms in Windows Hardware Compatibility Program Specifications and Policies.

How to create a Key Management Services (KMS) activation host

Article • 12/23/2021

KMS uses a client-server model to active Windows clients and is used for volume activation on your local network. KMS clients connect to a KMS server, called the KMS host, for activation. The KMS clients that a KMS host can activate are dependent on the host key used to activate the KMS host. This article walks you through the steps you need to create a KMS host. To learn more about KMS and the initial planning considerations, see Key Management Services (KMS) activation planning.

Prerequisites

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.

KMS hosts do not need to be dedicated servers, and KMS can be co-hosted with other services. You can run a KMS host on any physical or virtual system that is running a supported Windows Server or Windows client operating system.

The version of Windows you use for your KMS host determines the version of Windows you can activate for your KMS clients. Please see the table of activation versions to help you decide which is right for your environment.

By default, KMS hosts automatically publish SRV resource records in DNS. This enables KMS clients to automatically discover the KMS host and activate without the need for any configuration on the KMS client. Automatic publishing can be disabled and the records can be created manually, which is also necessary for automatic activation if the DNS service does not support dynamic updates.

You will need:

- A computer running Windows Server or Windows. A KMS host running on a Windows Server operating system can activate computers running both server and client operating systems, however a KMS host running on a Windows client operating system can only activate computers also running client operating systems.

- The user account you use must be a member of the Administrators group on the KMS host.
- A KMS host key for your organization. You can get this key from the Product Keys section of the Volume Licensing Service Center.

Install and configure a KMS host

1. From an elevated PowerShell session, run the following command to install the Volume Activation Services role:

   ```PowerShell
   Install-WindowsFeature -Name VolumeActivation -IncludeManagementTools
   ```

2. Configure the Windows Firewall to allow the Key Management Service to receive network traffic. You can allow this for any network profiles (default), or for any combination of Domain, Private, and Public network profiles. By default, a KMS host is configured to use TCP on port 1688. In the example below, the firewall rule is configured to allow network traffic for the Domain and Private network profiles only:

   ```PowerShell
   Set-NetFirewallRule -Name SPPSVC-In-TCP -Profile Domain,Private -
   Enabled True
   ```

3. Launch the Volume Activation Tools wizard by running:

   ```PowerShell
   vmw.exe
   ```

4. Select **Next** on the introduction screen. Select **Key Management Service (KMS)** as the activation type and enter `localhost` to configure the local server or the hostname of the server you want to configure.

5. Select **Install your KMS host key** and enter the product key for your organization, then select **Commit**.

6. Once the product key has been installed, you need to activate the product. Click **Next**.

7. Select the product you want to activate from the dropdown menu, then select whether you want to activate online or by phone. In this example, select **Activate online** and then **Commit**.

8. Once activation is successful, the KMS host configuration will be shown. If this is the configuration you want, you can select **Close** to exit the wizard. DNS records will be created and you can start activating KMS clients. See the section below if you need to manually create DNS records. If you want to change the configuration settings, select **Next**.

9. **Optional**: Change the configuration values based on your requirements and select **Commit**.

> ⓘ **Note**
>
> You can now start **activating KMS clients**, however a network must have a minimum number of computers (called the activation threshold). KMS hosts count the number of recent connections and so 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. Windows clients will activate if the count is 25 or higher. Windows Server 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.

Manually create DNS records

If your DNS service does not support dynamic update, the resource records must be manually created to publish the KMS host. Create DNS resource records for KMS manually with your DNS service using the information below (altering the default port number if you changed this in the KMS host configuration):

Property	Value
Type	SRV
Service/Name	_vlmcs
Protocol	_tcp
Priority	0
Weight	0

Property	Value
Port number	1688
Hostname	*FQDN of the KMS host*

You should also disable publishing on all KMS hosts if your DNS service does not support dynamic update to prevent event logs from collecting failed DNS publishing events.

> **Tip**
>
> Manually created resource records can also coexist with resource records that KMS hosts automatically publish in other domains as long as all records are maintained to prevent conflicts.

Disable publishing of DNS records

To disable publishing of DNS records by the KMS host:

1. Launch the Volume Activation Tools wizard by running:

   ```
   PowerShell
   ```

   ```
   vmw.exe
   ```

2. Select **Next** on the introduction screen. Select **Key Management Service (KMS)** as the activation type and enter `localhost` to configure the local server or the hostname of the server you want to configure.

3. Select **Skip to Configuration**, then select **Next**.

4. Uncheck the box for publish DNS records, then select **Commit**.

Key Management Services (KMS) client activation and product keys

Article • 09/05/2023

To use KMS, you need to have a KMS host available on your local network. Computers that activate with a KMS host need to have a specific product key. This key is sometimes referred to as the KMS client key, but it's formally known as a Microsoft Generic Volume License Key (GVLK). Computers that are running volume licensing editions of Windows Server and Windows client are, by default, KMS clients with no extra configuration needed as the relevant GVLK is already there.

There are some scenarios, however, where you'll need to add the GVLK to the computer you wish to activate against a KMS host, such as:

- Converting a computer from using a Multiple Activation Key (MAK)
- Converting a retail license of Windows to a KMS client
- If the computer was previously a KMS host

> **ⓘ Important**
>
> To use the keys listed here (which are GVLKs), you must first have a KMS host available on your local network. If you don't already have a KMS host, please see how to **create a KMS host** to learn more.
>
> If you want to activate Windows without a KMS host available and outside of a volume-activation scenario (for example, you're trying to activate a retail version of Windows client), **these keys will not work**. You will need to use another method of activating Windows, such as using a MAK, or purchasing a retail license. Get help to **find your Windows product key** and learn about **genuine versions of Windows**.

Install a product key

If you're converting a computer from a KMS host, MAK, or retail edition of Windows to a KMS client, install the applicable product key (GVLK) from the list below. To install a client product key, open an administrative command prompt on the client, and run the following command and then press `Enter`:

```
slmgr /ipk <product key>
```

For example, to install the product key for Windows Server 2022 Datacenter edition, run the following command and then press `Enter`:

```
slmgr /ipk WX4NM-KYWYW-QJJR4-XV3QB-6VM33
```

Generic Volume License Keys (GVLK)

In the tables that follow, you'll find the GVLKs for each version and edition of Windows. LTSC is *Long-Term Servicing Channel*, while LTSB is *Long-Term Servicing Branch*.

Windows Server (LTSC versions)

Windows Server 2022

Operating system edition	KMS Client Product Key
Windows Server 2022 Datacenter	WX4NM-KYWYW-QJJR4-XV3QB-6VM33
Windows Server 2022 Datacenter Azure Edition	NTBV8-9K7Q8-V27C6-M2BTV-KHMXV
Windows Server 2022 Standard	VDYBN-27WPP-V4HQT-9VMD4-VMK7H

Windows Server 2019

Operating system edition	KMS Client Product Key
Windows Server 2019 Datacenter	WMDGN-G9PQG-XVVXX-R3X43-63DFG
Windows Server 2019 Standard	N69G4-B89J2-4G8F4-WWYCC-J464C
Windows Server 2019 Essentials	WVDHN-86M7X-466P6-VHXV7-YY726

Windows Server 2016

Operating system edition	KMS Client Product Key
Windows Server 2016 Datacenter	CB7KF-BWN84-R7R2Y-793K2-8XDDG
Windows Server 2016 Standard	WC2BQ-8NRM3-FDDYY-2BFGV-KHKQY
Windows Server 2016 Essentials	JCKRF-N37P4-C2D82-9YXRT-4M63B

Windows Server (Semi-Annual Channel versions)

Windows Server, versions 20H2, 2004, 1909, 1903, and 1809

Operating system edition	KMS Client Product Key
Windows Server Datacenter	6NMRW-2C8FM-D24W7-TQWMY-CWH2D
Windows Server Standard	N2KJX-J94YW-TQVFB-DG9YT-724CC

> **ⓘ Important**
>
> Windows Server, version 20H2 reached end of service on August 9, 2022 and is no longer receiving security updates. This includes the retirement of Windows Server Semi-Annual Channel (SAC) with no future releases.
>
> Customers using Windows Server SAC should move to **Azure Stack HCI**. Alternatively, customers may use the Long-Term Servicing Channel of Windows Server.

Windows 11 and Windows 10 (Semi-Annual Channel versions)

See the Windows lifecycle fact sheet for information about supported versions and end of service dates.

Operating system edition	KMS Client Product Key
Windows 11 Pro Windows 10 Pro	W269N-WFGWX-YVC9B-4J6C9-T83GX
Windows 11 Pro N Windows 10 Pro N	MH37W-N47XK-V7XM9-C7227-GCQG9

Operating system edition	KMS Client Product Key
Windows 11 Pro for Workstations Windows 10 Pro for Workstations	NRG8B-VKK3Q-CXVCJ-9G2XF-6Q84J
Windows 11 Pro for Workstations N Windows 10 Pro for Workstations N	9FNHH-K3HBT-3W4TD-6383H-6XYWF
Windows 11 Pro Education Windows 10 Pro Education	6TP4R-GNPTD-KYYHQ-7B7DP-J447Y
Windows 11 Pro Education N Windows 10 Pro Education N	YVWGF-BXNMC-HTQYQ-CPQ99-66QFC
Windows 11 Education Windows 10 Education	NW6C2-QMPVW-D7KKK-3GKT6-VCFB2
Windows 11 Education N Windows 10 Education N	2WH4N-8QGBV-H22JP-CT43Q-MDWWJ
Windows 11 Enterprise Windows 10 Enterprise	NPPR9-FWDCX-D2C8J-H872K-2YT43
Windows 11 Enterprise N Windows 10 Enterprise N	DPH2V-TTNVB-4X9Q3-TJR4H-KHJW4
Windows 11 Enterprise G Windows 10 Enterprise G	YYVX9-NTFWV-6MDM3-9PT4T-4M68B
Windows 11 Enterprise G N Windows 10 Enterprise G N	44RPN-FTY23-9VTTB-MP9BX-T84FV

Windows 10 (LTSC/LTSB versions)

Windows 10 LTSC 2021 and 2019

Operating system edition	KMS Client Product Key
Windows 10 Enterprise LTSC 2021 Windows 10 Enterprise LTSC 2019	M7XTQ-FN8P6-TTKYV-9D4CC-J462D
Windows 10 Enterprise N LTSC 2021 Windows 10 Enterprise N LTSC 2019	92NFX-8DJQP-P6BBQ-THF9C-7CG2H

Windows 10 LTSB 2016

Operating system edition	KMS Client Product Key
Windows 10 Enterprise LTSB 2016	DCPHK-NFMTC-H88MJ-PFHPY-QJ4BJ
Windows 10 Enterprise N LTSB 2016	QFFDN-GRT3P-VKWWX-X7T3R-8B639

Windows 10 LTSB 2015

Operating system edition	KMS Client Product Key
Windows 10 Enterprise 2015 LTSB	WNMTR-4C88C-JK8YV-HQ7T2-76DF9
Windows 10 Enterprise 2015 LTSB N	2F77B-TNFGY-69QQF-B8YKP-D69TJ

Earlier versions of Windows Server

Windows Server, version 1803

Operating system edition	KMS Client Product Key
Windows Server Datacenter	2HXDN-KRXHB-GPYC7-YCKFJ-7FVDG
Windows Server Standard	PTXN8-JFHJM-4WC78-MPCBR-9W4KR

Windows Server, version 1709

Operating system edition	KMS Client Product Key
Windows Server Datacenter	6Y6KB-N82V8-D8CQV-23MJW-BWTG6
Windows Server Standard	DPCNP-XQFKJ-BJF7R-FRC8D-GF6G4

Windows Server 2012 R2

Operating system edition	KMS Client Product Key
Windows Server 2012 R2 Standard	D2N9P-3P6X9-2R39C-7RTCD-MDVJX
Windows Server 2012 R2 Datacenter	W3GGN-FT8W3-Y4M27-J84CP-Q3VJ9
Windows Server 2012 R2 Essentials	KNC87-3J2TX-XB4WP-VCPJV-M4FWM

Windows Server 2012

Operating system edition	KMS Client Product Key
Windows Server 2012	BN3D2-R7TKB-3YPBD-8DRP2-27GG4
Windows Server 2012 N	8N2M2-HWPGY-7PGT9-HGDD8-GVGGY
Windows Server 2012 Single Language	2WN2H-YGCQR-KFX6K-CD6TF-84YXQ
Windows Server 2012 Country Specific	4K36P-JN4VD-GDC6V-KDT89-DYFKP
Windows Server 2012 Standard	XC9B7-NBPP2-83J2H-RHMBY-92BT4
Windows Server 2012 MultiPoint Standard	HM7DN-YVMH3-46JC3-XYTG7-CYQJJ
Windows Server 2012 MultiPoint Premium	XNH6W-2V9GX-RGJ4K-Y8X6F-QGJ2G
Windows Server 2012 Datacenter	48HP8-DN98B-MYWDG-T2DCC-8W83P
Windows Server 2012 Essentials	HTDQM-NBMMG-KGYDT-2DTKT-J2MPV

Windows Server 2008 R2

Operating system edition	KMS Client Product Key
Windows Server 2008 R2 Web	6TPJF-RBVHG-WBW2R-86QPH-6RTM4
Windows Server 2008 R2 HPC edition	TT8MH-CG224-D3D7Q-498W2-9QCTX
Windows Server 2008 R2 Standard	YC6KT-GKW9T-YTKYR-T4X34-R7VHC
Windows Server 2008 R2 Enterprise	489J6-VHDMP-X63PK-3K798-CPX3Y
Windows Server 2008 R2 Datacenter	74YFP-3QFB3-KQT8W-PMXWJ-7M648
Windows Server 2008 R2 for Itanium-based Systems	GT63C-RJFQ3-4GMB6-BRFB9-CB83V

Windows Server 2008

Operating system edition	KMS Client Product Key
Windows Web Server 2008	WYR28-R7TFJ-3X2YQ-YCY4H-M249D
Windows Server 2008 Standard	TM24T-X9RMF-VWXK6-X8JC9-BFGM2
Windows Server 2008 Standard without Hyper-V	W7VD6-7JFBR-RX26B-YKQ3Y-6FFFJ
Windows Server 2008 Enterprise	YQGMW-MPWTJ-34KDK-48M3W-X4Q6V

Operating system edition	KMS Client Product Key
Windows Server 2008 Enterprise without Hyper-V	39BXF-X8Q23-P2WWT-38T2F-G3FPG
Windows Server 2008 HPC	RCTX3-KWVHP-BR6TB-RB6DM-6X7HP
Windows Server 2008 Datacenter	7M67G-PC374-GR742-YH8V4-TCBY3
Windows Server 2008 Datacenter without Hyper-V	22XQ2-VRXRG-P8D42-K34TD-G3QQC
Windows Server 2008 for Itanium-Based Systems	4DWFP-JF3DJ-B7DTH-78FJB-PDRHK

Earlier versions of Windows

Windows 8.1

Operating system edition	KMS Client Product Key
Windows 8.1 Pro	GCRJD-8NW9H-F2CDX-CCM8D-9D6T9
Windows 8.1 Pro N	HMCNV-VVBFX-7HMBH-CTY9B-B4FXY
Windows 8.1 Enterprise	MHF9N-XY6XB-WVXMC-BTDCT-MKKG7
Windows 8.1 Enterprise N	TT4HM-HN7YT-62K67-RGRQJ-JFFXW

Windows 8

Operating system edition	KMS Client Product Key
Windows 8 Pro	NG4HW-VH26C-733KW-K6F98-J8CK4
Windows 8 Pro N	XCVCF-2NXM9-723PB-MHCB7-2RYQQ
Windows 8 Enterprise	32JNW-9KQ84-P47T8-D8GGY-CWCK7
Windows 8 Enterprise N	JMNMF-RHW7P-DMY6X-RF3DR-X2BQT

Windows 7

Operating system edition	KMS Client Product Key
Windows 7 Professional	FJ82H-XT6CR-J8D7P-XQJJ2-GPDD4
Windows 7 Professional N	MRPKT-YTG23-K7D7T-X2JMM-QY7MG

Operating system edition	KMS Client Product Key
Windows 7 Professional E	W82YF-2Q76Y-63HXB-FGJG9-GF7QX
Windows 7 Enterprise	33PXH-7Y6KF-2VJC9-XBBR8-HVTHH
Windows 7 Enterprise N	YDRBP-3D83W-TY26F-D46B2-XCKRJ
Windows 7 Enterprise E	C29WB-22CC8-VJ326-GHFJW-H9DH4

Windows Vista

Operating system edition	KMS Client Product Key
Windows Vista Business	YFKBB-PQJJV-G996G-VWGXY-2V3X8
Windows Vista Business N	HMBQG-8H2RH-C77VX-27R82-VMQBT
Windows Vista Enterprise	VKK3X-68KWM-X2YGT-QR4M6-4BWMV
Windows Vista Enterprise N	VTC42-BM838-43QHV-84HX6-XJXKV

Connect Windows Server machines to Azure through Azure Arc Setup

Article • 10/15/2023

Windows Server machines can be onboarded directly to Azure Arc through a graphical wizard included in Windows Server. The wizard automates the onboarding process by checking the necessary prerequisites for successful Azure Arc onboarding and fetching and installing the latest version of the Azure Connected Machine (AzCM) agent. Once the wizard process completes, you're directed to your Window Server machine in the Azure portal, where it can be viewed and managed like any other Azure Arc-enabled resource.

Onboarding to Azure Arc is not needed if the Windows Server machine is already running in Azure.

> **Note**
>
> This feature only applies to Windows Server 2022 and later. It was released in the **Cumulative Update of 10/10/2023**.

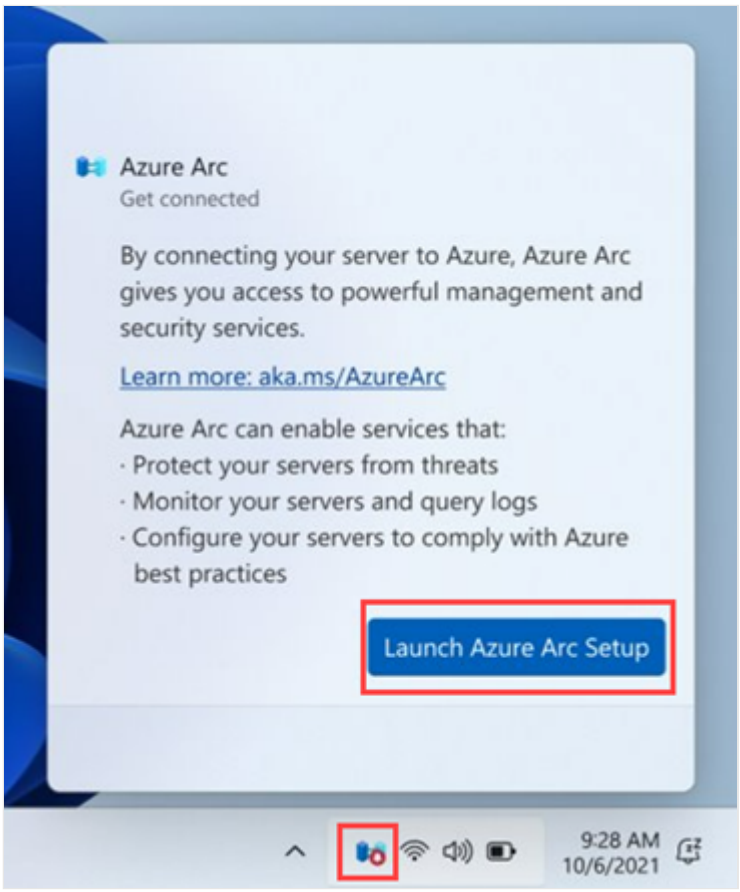
Prerequisites

- Azure Arc-enabled servers - Review the prerequisites and verify that your subscription, your Azure account, and resources meet the requirements.
- An Azure subscription. If you don't have one, create a free account before you begin.
- Modern browser (Microsoft Edge) for authentication to Microsoft Azure. Configuration of the Azure Connected Machine agent requires authentication to your Azure account, either through interactive authentication on a modern browser or device code login on a separate device (if the machine doesn't have a modern browser).

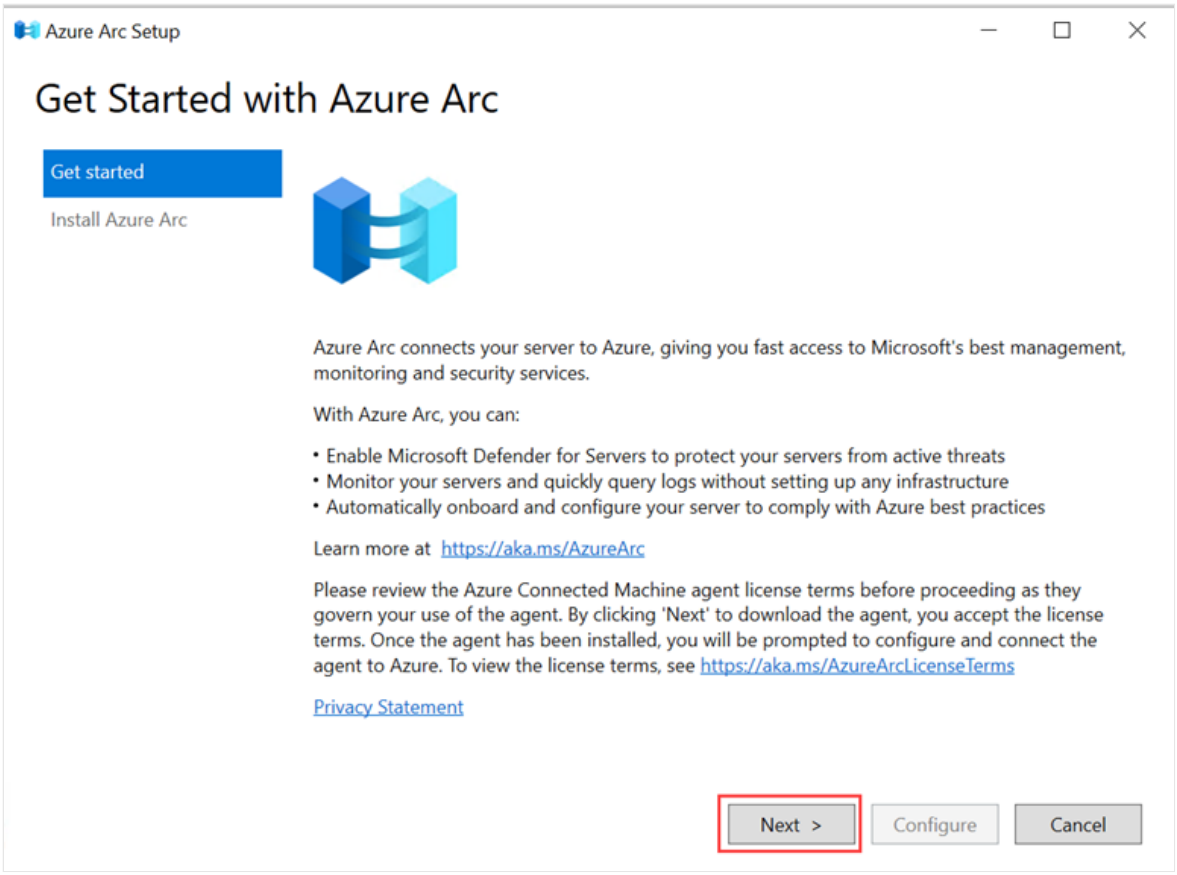
Launch Azure Arc Setup and connect to Azure Arc

The Azure Arc Setup wizard is launched from a system tray icon at the bottom of the Windows Server machine when the Azure Arc Setup feature is enabled. This feature is enabled by default. Alternatively, you can launch the wizard from a pop-up window in the Server Manager or from the Windows Server Start menu.

1. Select the Azure Arc system tray icon, then select **Launch Azure Arc Setup**.



2. The introduction window of the Azure Arc Setup wizard explains the benefits of onboarding your machine to Azure Arc. When you're ready to proceed, click **Next**.

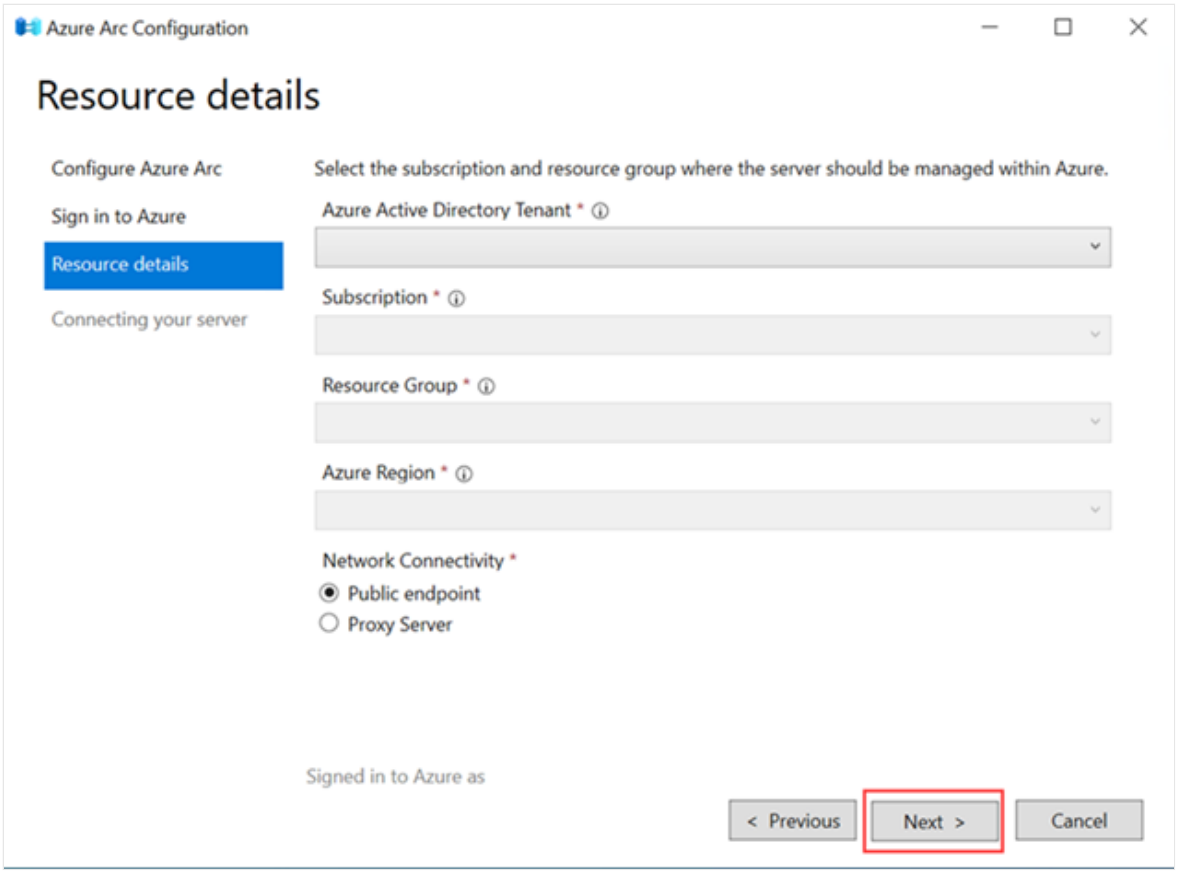


3. The wizard automatically checks for the prerequisites necessary to install the Azure Connected Machine agent on your Windows Server machine. Once this process completes and the agent is installed, select **Configure**.

4. The configuration window details the steps required to configure the Azure Connected Machine agent. When you're ready to begin configuration, select **Next**.

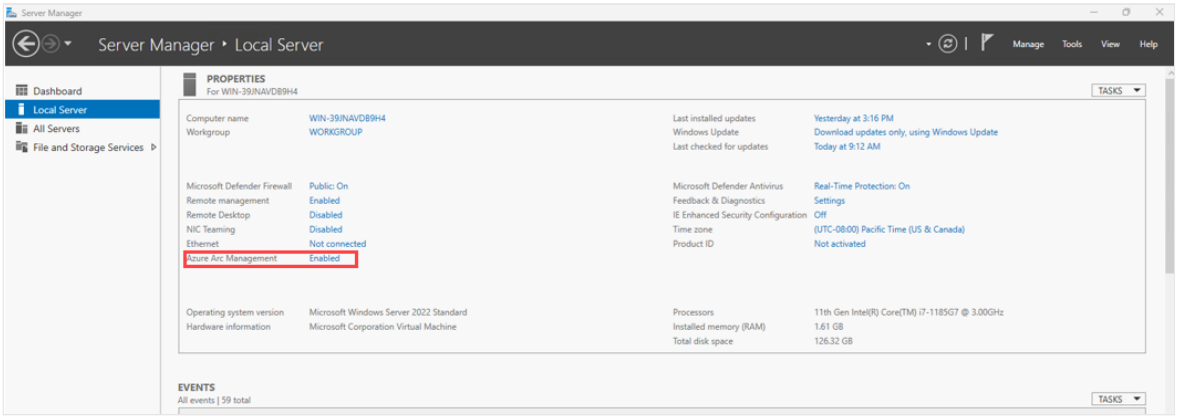
5. Sign-in to Azure by selecting the applicable Azure cloud, and then selecting **Sign in to Azure**. You'll be asked to provide your sign-in credentials.

6. Provide the resource details of how your machine will work within Azure Arc, such as the **Subscription** and **Resource group**, and then select **Next**.



7. Once the configuration completes and your machine is onboarded to Azure Arc, select **Finish**.

8. Go to the Server Manager and select **Local Server** to view the status of the machine in the **Azure Arc Management** field. A successfully onboarded machine has a status of **Enabled**.



Server Manager functions

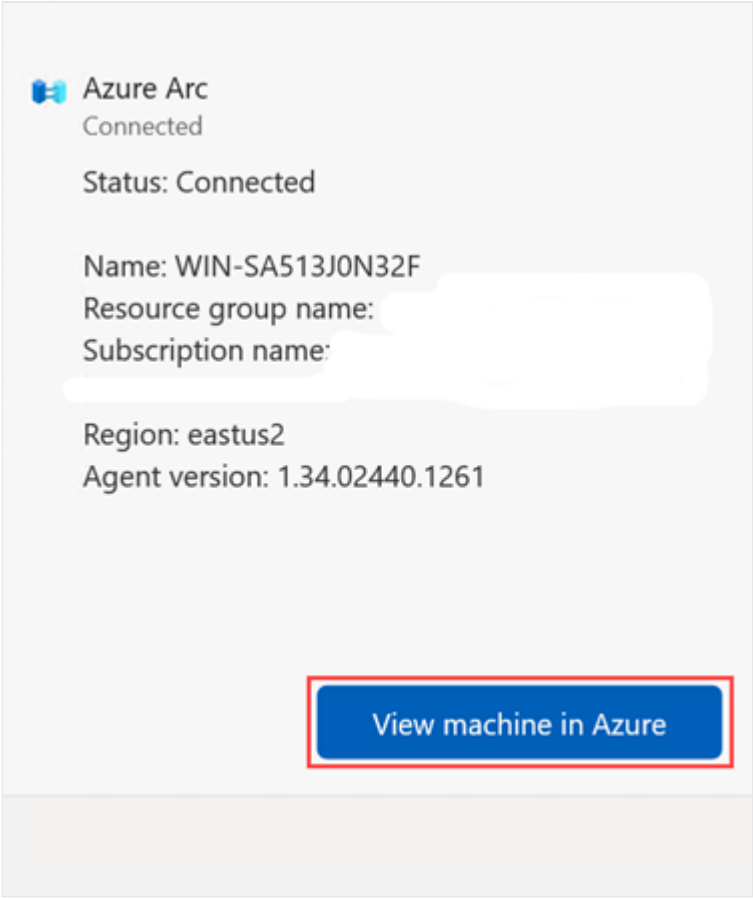
You can select the **Enabled/Disabled** link in the **Azure Arc Management** field of the Server Manager to launch different functions based on the status of the machine:

- If Azure Arc Setup isn't installed, selecting **Enabled/Disabled** launches the **Add Roles and Features Wizard**.

- If Azure Arc Setup is installed and the Azure Connected Machine agent hasn't been installed, selecting **Disabled** launches `AzureArcSetup.exe`, the executable file for the Azure Arc Setup wizard.
- If Azure Arc Setup is installed and the Azure Connected Machine agent is already installed, selecting **Enabled/Disabled** launches `AzureArcConfiguration.exe`, the executable file for configuring the Azure Connected Machine agent to work with your machine.

Viewing the connected machine

The Azure Arc system tray icon at the bottom of your Windows Server machine indicates if the machine is connected to Azure Arc; a red symbol means the machine does not have the Azure Connected Machine agent installed. To view a connected machine in Azure Arc, select the icon and then select **View Machine in Azure**. You can then view the machine in the Azure portal, just as you would other Azure Arc-enabled resources.



Uninstalling Azure Arc Setup

To uninstall Azure Arc Setup, follow these steps:

1. In the Server Manager, navigate to the **Remove Roles and Features Wizard**. (See Remove roles, role services, and features by using the remove Roles and Features

Wizard for more information.)

2. On the Features page, uncheck the box for **Azure Arc Setup**.
3. On the confirmation page, select **Restart the destination server automatically if required**, then select **Remove**.

To uninstall Azure Arc Setup through PowerShell, run the following command:

```PowerShell
Disable-WindowsOptionalFeature -Online -FeatureName AzureArcSetup
```

> **Note**
>
> Uninstalling Azure Arc Setup does not uninstall the Azure Connected Machine agent from the machine. For instructions on uninstalling the agent, see **Managing and maintaining the Connected Machine agent**.

Next steps

- Troubleshooting information can be found in the Troubleshoot Azure Connected Machine agent guide.
- Review the Planning and deployment guide to plan for deploying Azure Arc-enabled servers at any scale and implement centralized management and monitoring.
- Learn how to manage your machine using Azure Policy, for such things as VM guest configuration, verifying the machine is reporting to the expected Log Analytics workspace, enable monitoring with VM insights, and much more.

How to get Extended Security Updates (ESU) for Windows Server

Article • 09/26/2023

Extended Security Updates (ESU) for Windows Server include security updates and bulletins rated *critical* and *important*. Before using ESU, you should read Extended Security Updates for Windows Server Overview to understand what ESUs are, how long they're available for, and what your options are.

How you get ESUs depends on where your server is hosted. You can get access to ESUs through the following options.

- **Azure virtual machines** - Applicable virtual machines (VMs) hosted in Azure are automatically enabled for ESUs and these updates are provided free of charge, there's no need to deploy a MAK key or take any other action. See Extended Security Updates on Azure to learn more.
- **Azure Arc-enabled servers** - If your servers are on-premises or in a hosted environment, you can enroll your Windows Server 2012 and 2012 R2 or SQL Server 2012 machines for Extended Security Updates via the Azure portal, connect through Azure Arc, and you'll be billed monthly via your Azure subscription. See Extended Security Updates enabled by Azure Arc to learn more. [1]
- **Non-Azure physical and virtual machines** - If you can't connect using Azure Arc, use Extended Security Updates on non-Azure VMs, by using a Multiple Activation Key (MAK) and applying it to the relevant servers. This MAK key lets the Windows Update servers know that you can continue to receive security updates. See Access your Multiple Activation Key from the Microsoft 365 Admin Center to learn more. [1]

[1] When using Azure Arc-enabled servers and non-Azure machines you must purchase ESUs. In order to purchase ESUs, you must have Software Assurance through Volume Licensing Programs such as an Enterprise Agreement (EA), Enterprise Agreement Subscription (EAS), Enrollment for Education Solutions (EES), or Server and Cloud Enrollment (SCE).

> **Note**
>
> It may take 3-5 business days for your Multiple Activation Key to become available after purchasing ESUs for on-premises VMs or physical servers. Your organization

may also require time to plan and deploy the new keys. Before purchasing ESUs, you should keep these timelines in mind.

Extended Security Updates on Azure

Applicable virtual machines (VMs) hosted in Azure are automatically enabled for ESU and these updates are provided free of charge. You don't need to configure anything, and there's no extra charge for using ESUs with Azure VMs. ESUs are automatically delivered to Azure VMs if they're configured to receive updates.

> **Note**
>
> Extended Security Updates are also free of charge in other Azure products such as Azure Dedicated Host, Azure VMware Solution, Azure Nutanix Solution, and Azure Stack (Hub, Edge, and HCI), and might require additional configuration. Contact **Microsoft Support** for more help.
>
> Azure Classic VMs (Microsoft.ClassicCompute) also require extra configuration to receive Extended Security Updates since they don't have access to the **Azure Instance Metadata Service** that determines ESUs eligibility.

Extended Security Updates enabled by Azure Arc

ESUs are automatically delivered to Azure Arc-enabled servers if they're connected and enrolled for ESUs through Azure Arc. This can also apply to non-Azure servers connected to Azure Arc.

You can enroll in ESUs at scale by using Azure Policy or Azure portal, there's no upfront charge and you'll be billed monthly via your Azure subscription. You also don't need to activate product keys.

Azure Arc-enabled servers also enable to you to use other Azure services, such as:

- Azure Update Manager.
- Microsoft Defender for Cloud.
- Azure Policy (Machine Configuration).
- Azure Monitor (VM Insights).

From September 2023, you're able to activate Windows Server 2012 and 2012 R2 ESUs through Azure Arc. You can connect Windows Server 2012 and 2012 R2 servers to Azure Arc today, Connect hybrid machines with Azure Arc-enabled servers.

To prepare for activating Windows Server 2012 and 2012R2 ESUs on your Arc-enabled servers, follow these steps:

1. Sign in to the Azure portal.
2. In the search bar, enter *Servers - Azure Arc* and select the matching service entry.
3. Add your existing Windows Server 2012 or 2012 R2 machine to Azure Arc. To learn about getting started with Azure Arc-enabled servers, see Connect hybrid machines with Azure Arc-enabled servers.

To learn more about ESUs with Azure Arc, see Prepare to deliver Extended Security Updates for Windows Server 2012 and Deliver Extended Security Updates for Windows 2012 and 2012 R2.

Access your Multiple Activation Key from the Microsoft 365 Admin Center

Customers who can't connect to Azure Arc to apply ESUs can use Multiple Activation Keys (MAK) through Microsoft 365 Admin Center:

1. Sign in to the Microsoft 365 Admin Center.
2. Select **Your products** > **Volume licensing** > **View contracts**
3. Select your agreement number used to purchase ESUs, the three dots beside it (More Actions icon), then select **View product keys**. All the product keys available to the agreement shown on this page.
4. Once you have your MAK, install the new key on your eligible servers. To learn more about installing and activating your MAK, see our Tech Community blog post Obtaining Extended Security Updates for eligible Windows devices.

Download and installation of Extended Security Updates

Delivery, download, and application of ESUs for Windows Server is no different than other Windows Updates. The updates provided through ESUs are only *Security* updates.

Before you can download and install ESUs, you must have installed the latest Servicing Stack Update (SSU) and the Licensing Preparation Package. To learn more about the steps required to install the latest SSU and Licensing Preparation Package, see KB5031043: Procedure to continue receiving security updates after extended support has ended on October 10, 2023.

You can install the updates using whatever tools and processes you already have in place. The only difference is that the system must be registered using the key generated in the previous section for the updates to download and install.

For VMs hosted in Azure, the process of enabling the server for ESUs is automatically completed for you. Updates should download and install without extra configuration.

Deliver Extended Security Updates for Windows Server 2012

Article • 11/01/2023

This article provides steps to enable delivery of Extended Security Updates (ESUs) to Windows Server 2012 machines onboarded to Arc-enabled servers. You can enable ESUs to these machines individually or at scale.

Before you begin

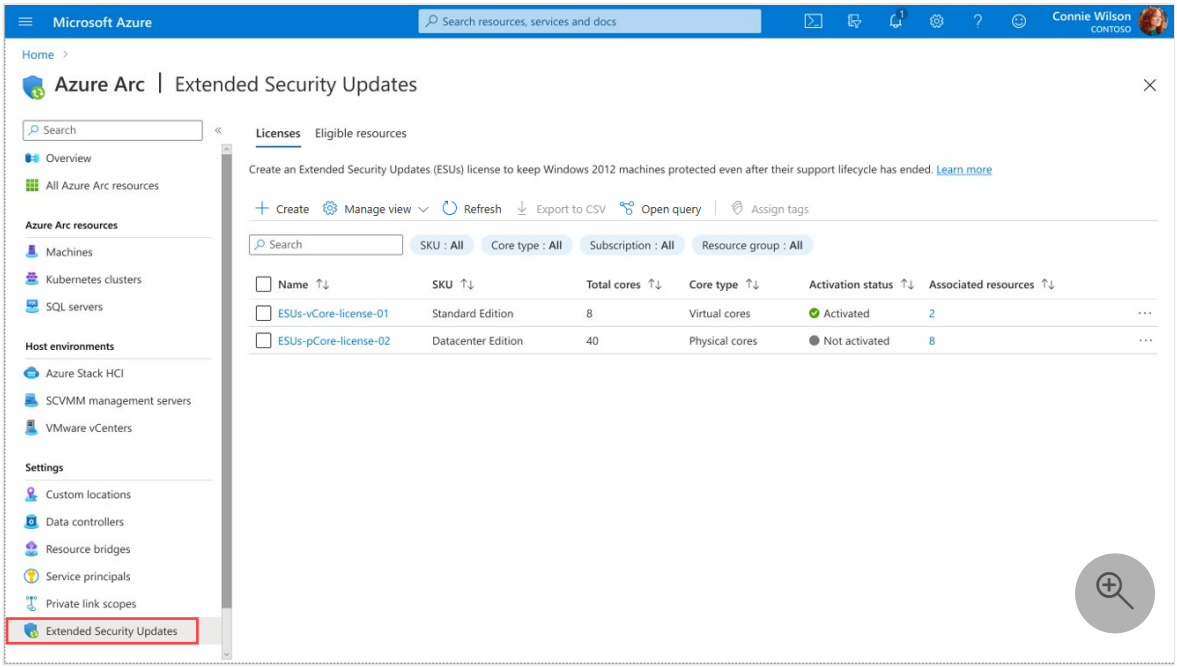
Plan and prepare to onboard your machines to Azure Arc-enabled servers. See Prepare to deliver Extended Security Updates for Windows Server 2012 to learn more.

You'll also need the Contributor role in Azure RBAC to create and assign ESUs to Arc-enabled servers.

Manage ESU licenses

1. From your browser, sign in to the Azure portal.

2. On the **Azure Arc** page, select **Extended Security Updates** in the left pane.



From here, you can view and create ESU **Licenses** and view **Eligible resources** for ESUs.

> **Note**
>
> When viewing all your Arc-enabled servers from the **Servers** page, a banner specifies how many Windows 2012 machines are eligible for ESUs. You can then select **View servers in Extended Security Updates** to view a list of resources that are eligible for ESUs, together with machines already ESU enabled.

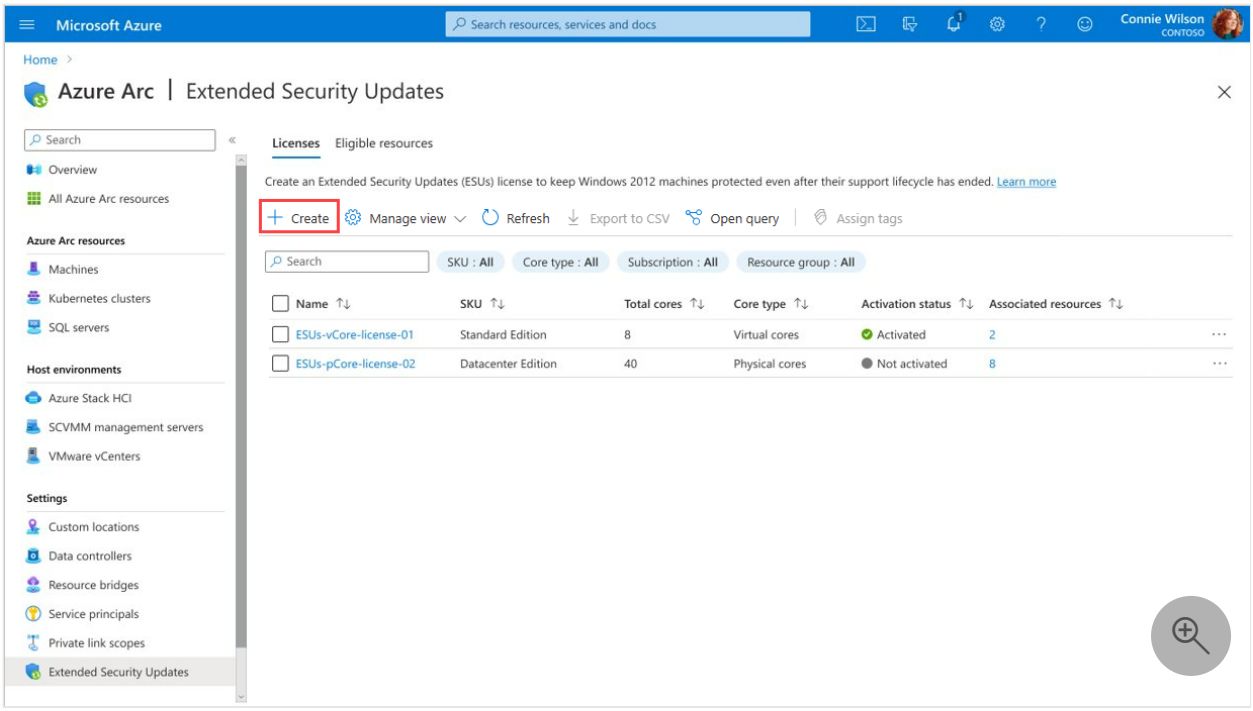
Create Azure Arc WS2012 licenses

The first step is to provision Windows Server 2012 and 2012 R2 Extended Security Update licenses from Azure Arc. You link these licenses to one or more Arc-enabled servers that you select in the next section.

After you provision an ESU license, you need to specify the SKU (Standard or Datacenter), type of cores (Physical or vCore), and number of 16-core and 2-core packs to provision an ESU license. You can also provision an Extended Security Update license in a deactivated state so that it won't initiate billing or be functional on creation. Moreover, the cores associated with the license can be modified after provisioning.

> **Note**
>
> The provisioning of ESU licenses requires you to attest to their SA or SPLA coverage.

The **Licenses** tab displays Azure Arc WS2012 licenses that are available. From here you can select an existing license to apply or create a new license.

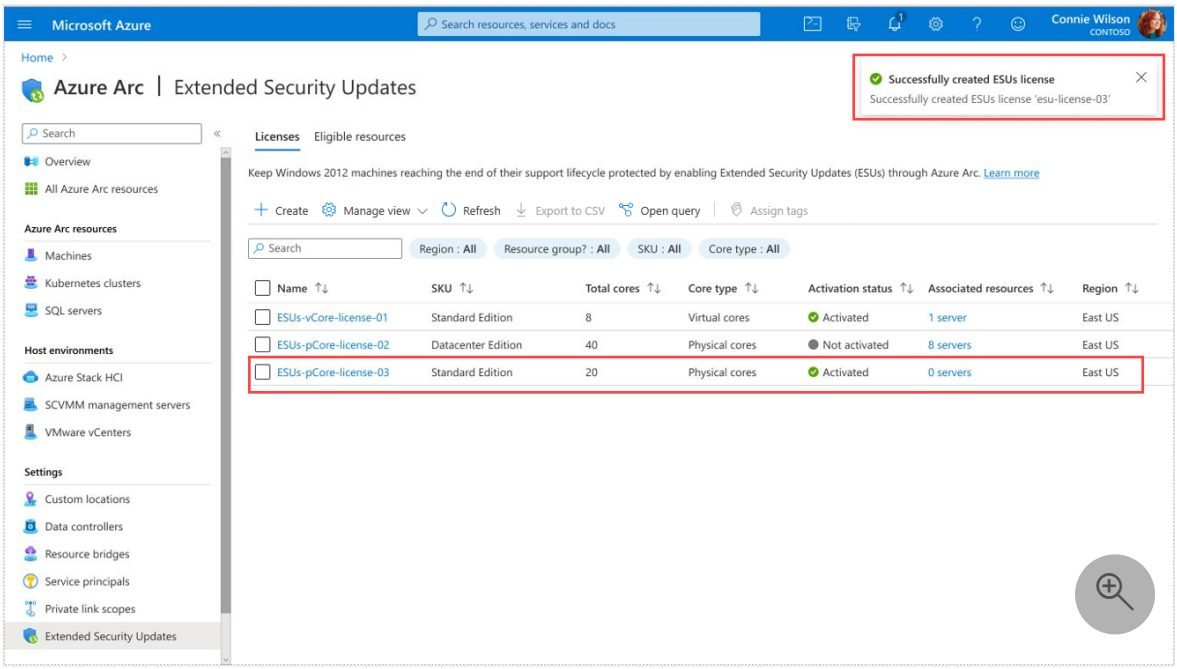


1. To create a new WS2012 license, select **Create**, and then provide the information required to configure the license on the page.

   For details on how to complete this step, see License provisioning guidelines for Extended Security Updates for Windows Server 2012.

2. Review the information provided, and then select **Create**.

   The license you created appears in the list and you can link it to one or more Arc-enabled servers by following the steps in the next section.

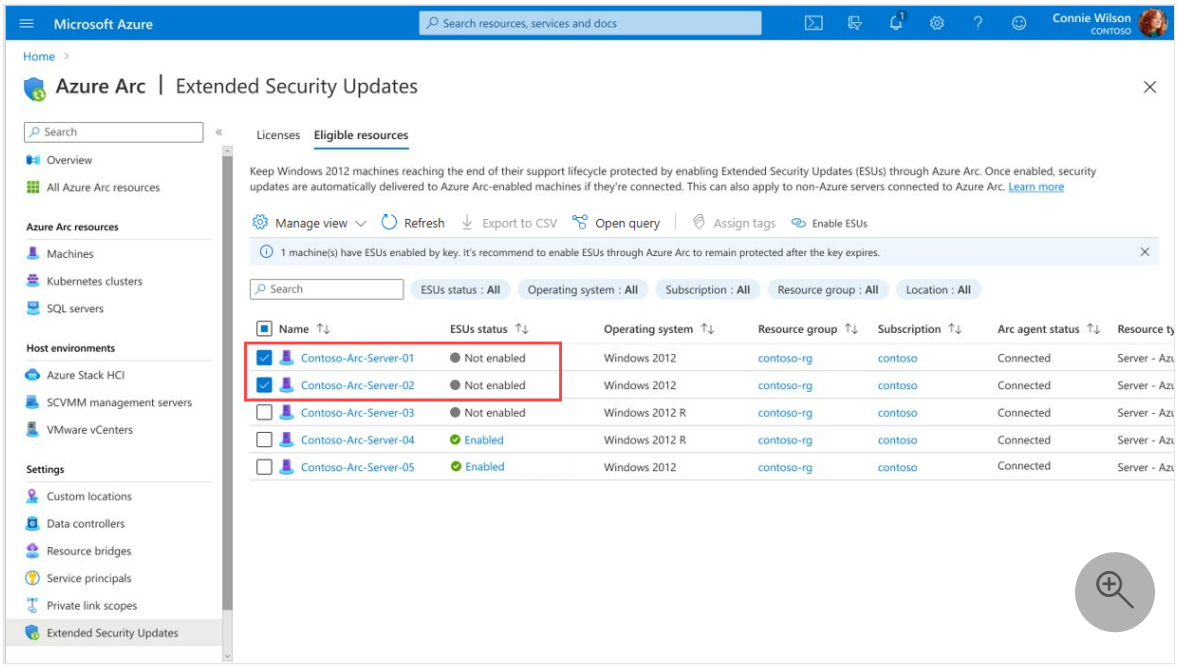


Link ESU licenses to Arc-enabled servers

You can select one or more Arc-enabled servers to link to an Extended Security Update license. Once you've linked a server to an activated ESU license, the server is eligible to receive Windows Server 2012 and 2012 R2 ESUs.

> **Note**
>
> You have the flexibility to configure your patching solution of choice to receive these updates – whether that's **Update Manager**, **Windows Server Update Services**, Microsoft Updates, **Microsoft Endpoint Configuration Manager**, or a third-party patch management solution.

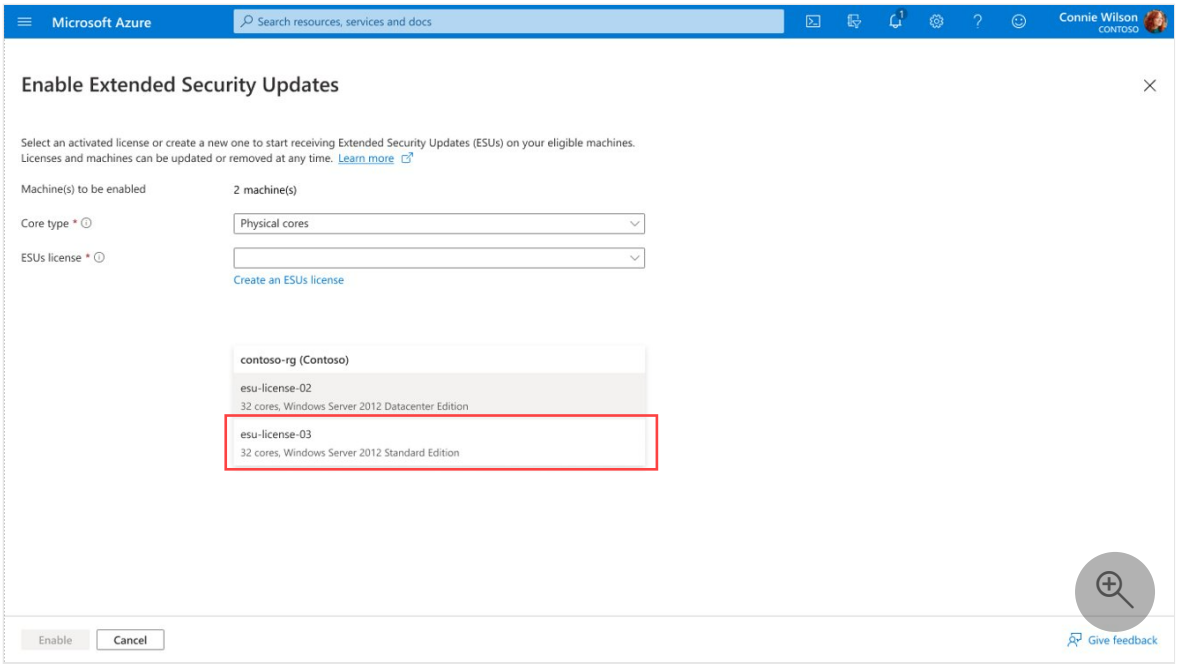
1. Select the **Eligible Resources** tab to view a list of all your Arc-enabled servers running Windows Server 2012 and 2012 R2.



   The **ESUs status** column indicates whether or not the machine is ESUs-enabled.

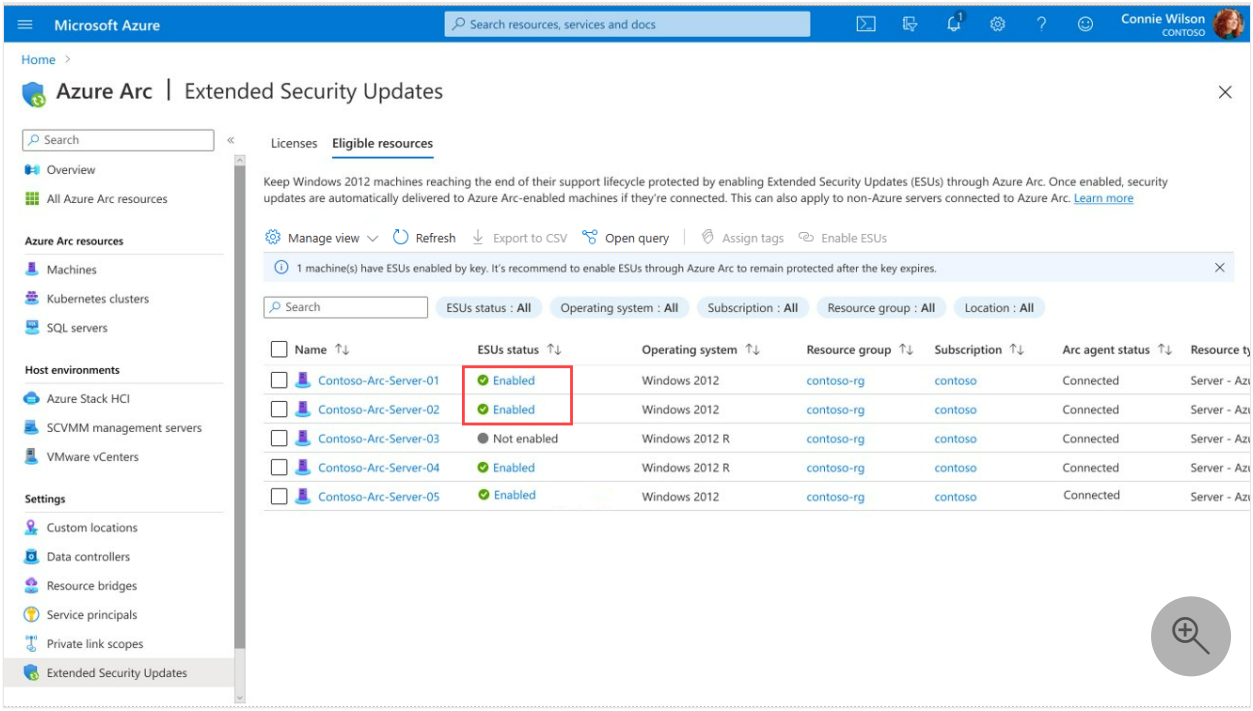
2. To enable ESUs for one or more machines, select them in the list, and then select **Enable ESUs**.

3. On the **Enable Extended Security Updates** page, it shows the number of machines selected to enable ESU and the WS2012 licenses available to apply. Select a license to link to the selected machine(s) and then select **Enable**.



> **Note**
>
> You can also create a license from this page by selecting **Create an ESU license**.

The status of the selected machines changes to **Enabled**.



If any problems occur during the enablement process, see Troubleshoot delivery of Extended Security Updates for Windows Server 2012 for assistance.

Additional scenarios

There are some scenarios in which you may be eligible to receive Extended Security Updates patches at no additional cost. Two of these scenarios supported by Azure Arc include the following:

- Dev/Test (Visual Studio)
- Disaster Recovery (Entitled benefit DR instances from Software Assurance or subscription only)

To qualify for these scenarios, you must have:

1. Provisioned and activated a WS2012 Arc ESU License intended to be linked to regular Azure Arc-enabled servers running in production environments (i.e., normally billed ESU scenarios). This license should be provisioned only for billable cores, not cores that are eligible for free Extended Security Updates.

2. Onboarded your Windows Server 2012 and Windows Server 2012 R2 machines to Azure Arc-enabled servers for the purpose of Dev/Test with Visual Studio subscriptions or Disaster Recovery

To enroll Azure Arc-enabled servers eligible for ESUs at no additional cost, follow these steps to tag and link:

1. Tag both the WS2012 Arc ESU License and the Azure Arc-enabled server with one of the following name-value pairs, corresponding to the appropriate exception:
   a. Name: “ESU Usage”; Value: “WS2012 VISUAL STUDIO DEV TEST”
   b. Name: “ESU Usage”; Value: “WS2012 DISASTER RECOVERY”

   In the case that you're using the ESU License for multiple exception scenarios, mark the license with the tag: Name: “ESU Usage”; Value: “WS2012 MULTIPURPOSE”

2. Link the tagged license to your tagged Azure Arc-enabled Windows Server 2012 and Windows Server 2012 R2 machines. **Do not license cores for these servers**.

   This linking will not trigger a compliance violation or enforcement block, allowing you to extend the application of a license beyond its provisioned cores. The expectation is that the license only includes cores for production and billed servers. Any additional cores will be charged and result in over-billing.

> **Note**
>
> The usage of these exception scenarios will be available for auditing purposes and abuse of these exceptions may result in recusal of WS2012 ESU privileges.

Enable Hotpatch for Azure Edition virtual machines built from ISO

Article • 10/31/2023

Hotpatch for Windows Server 2022 Datacenter: Azure Edition allows you to install security updates on without requiring a reboot after installation. You can use Hotpatch with both Desktop Experience and Server Core. This article will teach you how to configure Hotpatch after installing or upgrading the operating system using an ISO.

> **Note**
>
> If you're using the Azure marketplace, don't follow the steps in this article. Instead, use the following images from Azure Marketplace that are ready for Hotpatching:
>
> - Windows Server 2022 Datacenter: Azure Edition Hotpatch - Gen2
> - Windows Server 2022 Datacenter: Azure Edition Core - Gen2

When using Hotpatch for your ISO deployed machine on Azure Stack HCI, there are a few important differences with the Hotpatch experience compared with using Hotpatch as part of Azure Automanage for Azure VMs.

The differences include:

- Hotpatch configuration isn't available via Azure Update Manager.
- Hotpatch can't be disabled.
- Automatic Patching orchestration isn't available.
- Orchestration must be performed manually (for example, using Windows Update via SConfig).

Prerequisites

To enable Hotpatch, you must have the following prerequisites ready before you start:

- Windows Server 2022 Datacenter: Azure Edition hosted on a supported platform, such as Azure or Azure Stack HCI with Azure benefits enabled.
  - Azure Stack HCI must be version 21H2 or later.
- Review the How hotpatch works section of the Hotpatch for new virtual machines article.

- Outbound network access or an outbound port rule allowing HTTPS (TCP/443) traffic to the following endpoints:
  - `go.microsoft.com`
  - `software-static.download.prss.microsoft.com`

Prepare your computer

Before you can enable Hotpatch for your VM, you must prepare your computer using the following steps:

1. Sign-in to your machine. If you're on Server core, from the SConfig menu, enter option **15**, then press `Enter` to open a PowerShell session. If you're on the desktop experience, remote desktop into your VM and launch PowerShell.

2. Enable virtualization-based security by running the following PowerShell command to configure the correct registry settings:

   PowerShell

   ```powershell
   $registryPath = "HKLM:\SYSTEM\CurrentControlSet\Control\DeviceGuard"
   $parameters = $parameters = @{
       Path = $registryPath
       Name = "EnableVirtualizationBasedSecurity"
       Value = "0x1"
       Force = $True
       PropertyType = "DWORD"
   }
   New-ItemProperty @parameters
   ```

3. Restart your computer.

4. Configure the Hotpatch table size in the registry by running the following PowerShell command:

   PowerShell

   ```powershell
   $registryPath = "HKLM:\SYSTEM\CurrentControlSet\Control\Session
   Manager\Memory Management"
   $parameters = $parameters = @{
       Path = $registryPath
       Name = "HotPatchTableSize"
       Value = "0x1000"
       Force = $True
       PropertyType = "DWORD"
   }
   New-ItemProperty @parameters
   ```

5. Configure the Windows Update endpoint for Hotpatch in the registry by running the following PowerShell command:

```PowerShell
$registryPath = "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Update\TargetingInfo\DynamicInstalled\Hotpatch.amd64"
$nameParameters = $parameters = @{
    Path = $registryPath
    Name = "Name"
    Value = "Hotpatch Enrollment Package"
    Force = $True
}
$versionParameters = $parameters = @{
    Path = $registryPath
    Name = "Version"
    Value = "10.0.20348.1129"
    Force = $True
}
New-Item $registryPath -Force
New-ItemProperty @nameParameters
New-ItemProperty @versionParameters
```

Now you've prepared your computer, you can install the Hotpatch servicing package.

Install Hotpatch servicing package

> ⓘ **Note**
>
> The Hotpatch Prerequisite KB is currently not published in the Microsoft Update catalog.

To be able to receive Hotpatch updates, you'll need to download and install the Hotpatch servicing package. In your PowerShell session, complete the following steps:

1. Download the (KB5003508) Microsoft Update Standalone Package from the Microsoft Update Catalog and copy it to your computer using the following PowerShell command:

```PowerShell
$parameters = @{
    Uri = "https://go.microsoft.com/fwlink/?linkid=2211714"
    OutFile = ".\KB5003508.msu"
}
Invoke-WebRequest @parameters
```

2. To install the Standalone Package, run the following command:

```
PowerShell

wusa.exe .\KB5003508.msu
```

3. Follow the prompts. Once it's completed, select Finish.

4. To verify the installation, run the following command:

```
PowerShell

Get-HotFix | Where-Object {$_.HotFixID -eq "KB5003508"}
```

> **Note**
>
> When using Server Core, updates are set to be manually installed by default. You can change this setting using the SConfig utility.

Next steps

Now you've set up your computer for Hotpatch, here are some articles that might help you with updating your computer:

- Patch a Server Core installation.
- Learn more about Windows Server Update Services (WSUS).

Perform an in-place upgrade of Windows Server

Article • 09/15/2023

An in-place upgrade allows you to go from an older operating system to a newer one while keeping your settings, server roles, and data intact. This article teaches you how to move to a later version of Windows Server by using an in-place upgrade.

> **Important**
>
> This article covers the in-place Windows Server upgrade process for non-Azure servers and virtual machines (VMs) only. To do an in-place upgrade of Windows Server running in an Azure virtual machine (VM), see **In-place upgrade for VMs running Windows Server in Azure**.

Prerequisites

Before you start upgrading, fulfill the following prerequisites:

- Determine which version of Windows Server to upgrade to.
- Make sure you have a valid product key and activation method. Keys and methods may vary depending on the distribution channel you received Windows Server media from, for example a Commercial Licensing program, Retail, or Original Equipment Manufacturer (OEM).
- Ensure that the install media is ready to use.
- Have a location to store files away from your computer, such as a USB flash drive or network location.
- Review Upgrade and migrate roles and features in Windows Server.
- Review Microsoft server applications compatibility.
- Review any third-party application vendor support requirements.
- Make sure your computer:
  - Meets or exceeds the hardware requirements for Windows Server.
  - Isn't running in Azure.

> **Note**
>
> If you're upgrading a Windows Server 2012 or Windows Server 2012 R2 server with Configuration Manager installed, also follow the pre-upgrade and post-upgrade

instructions at **Upgrade on-premises infrastructure that supports Configuration Manager**.

Collect diagnostic information

We recommend that you collect some information from your devices for diagnostic and troubleshooting purposes in case the upgrade is unsuccessful. We also recommend you store the information somewhere you can get to even if you can't access your device.

To collect your information:

1. Open an elevated PowerShell prompt, make a note of your current directory, and run the following commands.

   PowerShell

   ```
   Get-ComputerInfo -Property WindowsBuildLabEx,WindowsEditionID | Out-File -FilePath .\computerinfo.txt
   systeminfo.exe | Out-File -FilePath systeminfo.txt
   ipconfig /all | Out-File -FilePath ipconfig.txt
   ```

   Tip

   `Get-ComputerInfo` requires PowerShell 5.1 or later. If your Windows Server version doesn't include Powershell, you can find this information in the registry. Open Registry Editor, go to the **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion** key, and then copy and paste the Windows Server **BuildLabEx** and **EditionID** values.

2. Using **File Explorer**, navigate to the directory you noted down, and **copy** the files to a USB flash drive or network location off of your computer.

After you've collected all of your Windows Server-related information, we recommend that you back up your server operating system, apps, and VMs. You must also shut down, quick migrate, or live migrate any VMs currently running on the server. You can't have any VMs running during the in-place upgrade.

Perform the upgrade

Now that you've completed your prerequisites and collected diagnostic information, you're ready to perform the upgrade. In this section, you use Windows Server Setup to select the settings for the upgrade. Windows Server Setup uses these settings to upgrade your version of Windows Server, during which time your computer restarts several times.

To perform the in-place upgrade:

1. Using **File Explorer**, navigate to the Windows Server Setup media. Then open **setup.exe**. For example, if you're using removal media the file path might be *D:\setup.exe*.

   > **Important**
   >
   > Depending on your security settings, User Account Control may prompt you to allow setup to make changes to your device. If you're happy to continue, select **Yes**.

2. By default, setup automatically downloads updates for the installation. If you're okay with the default settings, select **Next** to continue.

   If you don't want Setup to automatically download updates, select **Change how Setup downloads updates**, choose the option appropriate to your environment, and then select **Next**.

3. If prompted, enter your product key and then select **Next**.

4. Select the edition of Windows Server you want to install and then select **Next**.

5. Review the applicable notices and license terms. If you agree to the terms, select **Accept**.

6. Select **Keep personal files and apps** to choose to do an in-place upgrade, and then select **Next**.

7. After Setup finishes analyzing your device, it displays the **Ready to install** screen. To continue the upgrade, select **Install**.

The in-place upgrade starts, and you should see a progress bar. After the upgrade finishes, your server restarts.

Checking if your upgrade was successful

After the upgrade to Windows Server is done, you must make sure the upgrade was successful.

To make sure your upgrade was successful:

1. Open an elevated PowerShell prompt and run the following command to verify that the version and edition matches the media and values you selected during setup.

   ```PowerShell
   Get-ComputerInfo -Property WindowsProductName
   ```

2. Make sure all of your applications are running and that your client connections to the applications are successful.

If your computer isn't working as expected after the upgrade, you can contact Microsoft Support for technical assistance.

Next steps

The following articles can help you prepare for and use your new Windows Server version:

- Install or uninstall roles, role services, or features
- Windows Server management overview
- Get started with Windows Admin Center
- Key Management Services (KMS) activation planning
- Activate using Active Directory-based activation

If you'd like to learn more about deploying and post-installation configuration and activation options, check out the Windows Server deployment, configuration, and administration learning path.

Configure Secured-core server

Article • 09/01/2023

Secured-core is a collection of capabilities that offers built-in hardware, firmware, driver and operating system security features. This article shows you how to configure Secured-core server by using Windows Admin Center, the Windows Server Desktop Experience, and Group Policy.

Secured-core server is designed to deliver a secure platform for critical data and applications. For more information, see What is Secured-core server?

Prerequisites

Before you can configure Secured-core server, you must have the following security components installed and enabled in the BIOS:

- Secure Boot.
- Trusted Platform Module (TPM) 2.0.
- System firmware must meet preboot DMA protection requirements and set appropriate flags in ACPI tables to opt into and enable Kernel DMA Protection. To learn more about Kernel DMA Protection, see Kernel DMA Protection (Memory Access Protection) for OEMs.
- A processor with support enabled in the BIOS for:
  - Virtualization extensions.
  - Input/Output Memory Management Unit (IOMMU).
  - Dynamic Root of Trust for Measurement (DRTM).
  - Transparent Secure Memory Encryption is also required for AMD based systems.

> **ⓘ Important**
>
> Enabling each of the security features in the BIOS can vary based on your hardware vendor. Make sure to check your hardware manufacturer's Secured-core server enablement guide.

You can find hardware certified for Secured-core server from the Windows Server Catalog, and Azure Stack HCI servers in the Azure Stack HCI Catalog.

Enable security features

To configure Secured-core server you need to enable specific Windows Server security features, select the relevant method and follow the steps.

GUI

Here's how to enable Secured-core server using the user interface.

1. From the Windows desktop, open the **Start** menu, select **Windows Administrative Tools**, open **Computer Management**.
2. In Computer management, select **Device Manager**, resolve any device error if necessary.
   a. For AMD based systems, confirm the DRTM Boot Driver device is present before continuing
3. From Windows desktop, open the **Start** menu, select **Windows Security**.
4. Select **Device security** > **Core isolation details**, then enable **Memory Integrity** and **Firmware Protection**.
5. Restart your server when prompted.

Once your server has restarted, your server is enabled for Secured-core server.

Verify Secured-core server configuration

Now that you've configured Secured-core server, select the relevant method to verify your configuration.

GUI

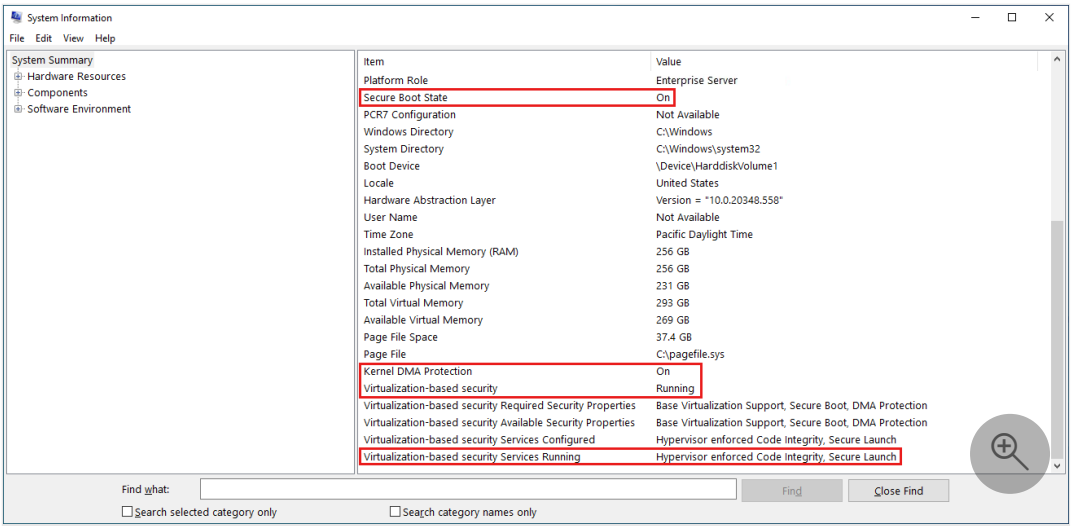
Here's how to verify your Secured-core server is configured using the user interface.

1. From the Windows desktop, open the **Start** menu, type `msinfo32.exe` to open System Information. From the System Summary page, confirm:

   a. **Secure Boot State** and **Kernel DMA Protection** is On.

   b. **Virtualization-based security** is Running.

   c. **Virtualization-based security Services** Running shows **Hypervisor enforced Code Integrity** and **Secure Launch**.



Next steps

Now that you've configured Secured-core server, here are some resources to learn more about:

- Virtualization-based Security (VBS)
- Memory integrity and VBS enablement
- System Guard Secure Launch

Troubleshooting Windows volume activation

Article • 05/19/2022

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

Guidelines for troubleshooting the Key Management Service (KMS)

Article • 09/19/2023

Enterprise customers set up Key Management Service (KMS) as part of their deployment process because it lets them use a simple, straightforward process to activate Windows in their environments. Usually, once you set up the KMS host, the KMS clients connect to the host automatically and activate on their own. However, sometimes the process doesn't work as expected. This article walks you through how to troubleshoot any issues you may encounter.

For more information about event log entries and the `slmgr.vbs` script, see Volume Activation Technical Reference.

Where to begin troubleshooting KMS

Let's start with a quick refresher on how KMS activation works. KMS is a client-server model that has some similarities to Dynamic Host Configuration Protocol (DHCP). However, instead of handing out IP addresses to clients on their request, KMS enables product activation. KMS is also a renewal model, in which the clients try to reactivate on a regular interval. There are two roles: the *KMS host* and the *KMS client*.

- The KMS host runs the activation service and enables activation in the environment. To configure a KMS host, you must install KMS key from the Volume License Service Center (VLSC) and then activate the service.
- The KMS client is the Windows operating system that you deploy in the environment and need to activate. KMS clients can run any edition of Windows that uses volume activation. The KMS clients come with a preinstalled key, called the *Generic Volume License Key (GVLK)* or *KMS Client Setup Key*. The presence of the GVLK is what makes a system a KMS client. The KMS clients use DNS SRV records (`_vlmcs._tcp`) to identify the KMS host. Next, the clients automatically try to discover and use this service to activate themselves. During the 30-day out-of-the-box grace period, they try to activate every two hours. After you activate the KMS clients, they try to renew their activation every seven days.

From a troubleshooting perspective, you may have to look at both the host and client sides to figure out why an issue is happening.

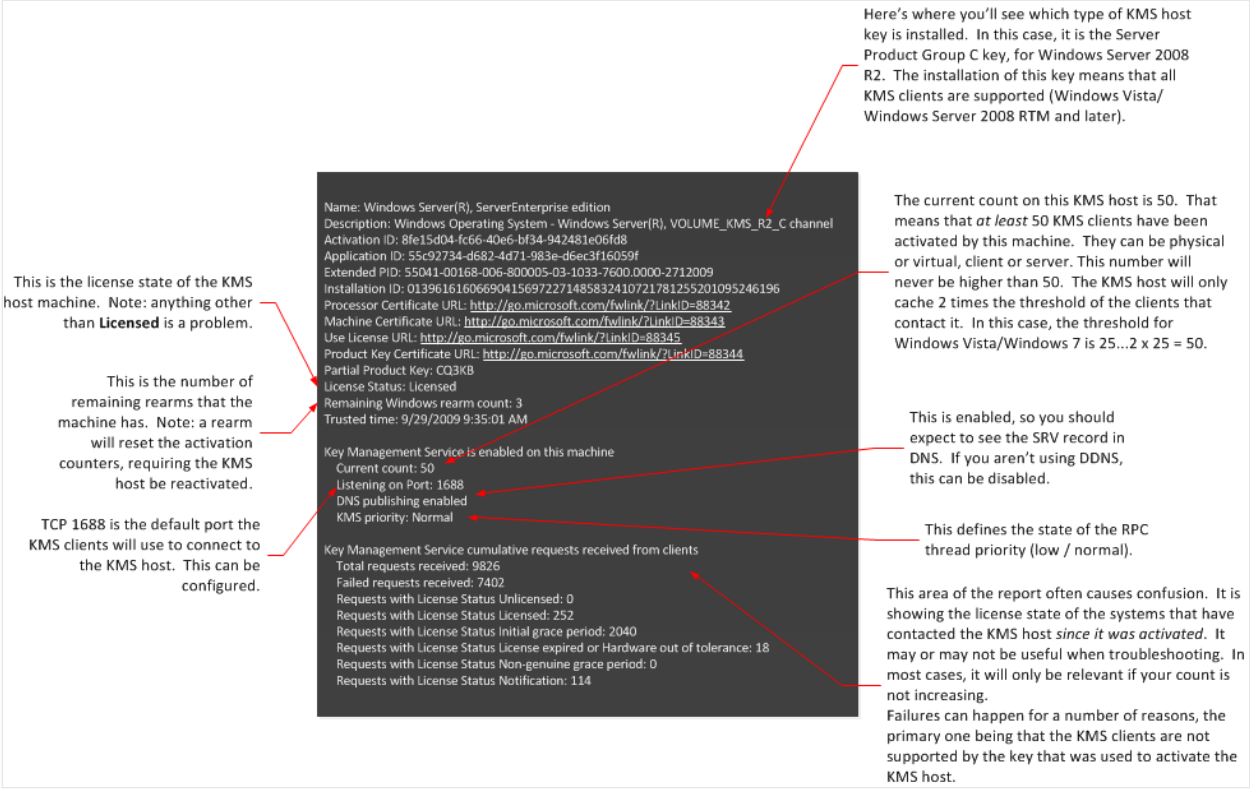
Troubleshooting on the KMS host

When you're examining the KMS host during troubleshooting, there are two areas you should look at:

- Check the status of the host software license service using the `slmgr.vbs` command in a command-line prompt.
- Check the Event Viewer for events related to licensing or activation.

Check the Software Licensing service using the slmgr.vbs command

To see verbose output from the Software Licensing service, open an elevated command prompt window and enter `slmgr.vbs /dlv`. The following screenshot shows the results of running this command on one of our KMS hosts within Microsoft.



Here are some variables you should pay attention to in the output while troubleshooting:

- The *Version Information* is at the top of the `slmgr.vbs /dlv` output. The version information is useful for determining whether the service is up-to-date. Making sure everything's up to date is important because the KMS service supports different KMS host keys. You can use this data to evaluate whether or not the version you're currently using supports the KMS host key you're trying to install. For more information about updates, see An update is available for Windows Vista and for Windows Server 2008 to extend KMS activation support for Windows 7 and for Windows Server 2008 R2.

- The *Name* indicates which edition of Windows is running on the KMS host system. You can use this information to troubleshoot issues that involve adding or changing the KMS host key. For example, you can use this information to verify if the OS edition supports the key you're trying to use.
- The *Description* shows you which key is currently installed. Use this field to verify whether the key that first activated the service was the correct one for the KMS clients you've deployed.
- The *License Status* shows the status of the KMS host system. The value should be **Licensed**. Any other value means you should reactivate the host.
- The *Current Count* displays a count between **0** and **50**. The count is cumulative between operating systems and indicates the number of valid systems that have tried to activate within a 30-day period.

  If the count is **0**, either the service was recently activated or no valid clients have connected to the KMS host.

  The count doesn't increase above **50**, no matter how many valid systems exist in the environment. The count is set to cache only twice the maximum license policy returned by a KMS client. The maximum policy set by the Windows client OS requires a count of **25** or higher from the KMS host to activate itself. Therefore, the highest count the KMS host can have is 2 x 25, or 50. In environments that contain only Windows Server KMS clients, the maximum count on the KMS host is **10**. This limit is because the threshold for Windows Server editions is **5** (2 x 5, or 10).

  A common issue related to the count happens when the environment has an activated KMS host and enough clients, but the count doesn't increase beyond one. When this issue happens, it means the deployed client image wasn't configured correctly, so the systems don't have unique Client Machine IDs (CMIDs). For more information, see KMS client and The KMS current count doesn't increase when you add new Windows Vista or Windows 7-based client computers to the network. One of our Support Escalation Engineers has also blogged about this issue at KMS Host Client Count not Increasing Due to Duplicate CMIDs.

  Another reason why the count may not be increasing is that there are too many KMS hosts in the environment and the count is distributed over all of them.
- **Listening on Port**. Communication with KMS uses anonymous RPC. By default, the clients use the 1688 TCP port to connect to the KMS host. Make sure that this port is open between your KMS clients and the KMS host. You can change or configure the port on the KMS host. During their communication, the KMS host sends the

port designation to the KMS clients. If you change the port on a KMS client, the port designation is overwritten when that client contacts the host.

We often get asked about the *cumulative requests* section of the `slmgr.vbs /dlv` output. Generally, this data isn't helpful for troubleshooting. The KMS host keeps an ongoing record of the state of each KMS client that tries to activate or reactivate. Failed requests indicate the KMS host doesn't support certain KMS clients. For example, if a Windows 7 KMS client tries to activate against a KMS host that was activated by using a Windows Vista KMS key, the activation fails.

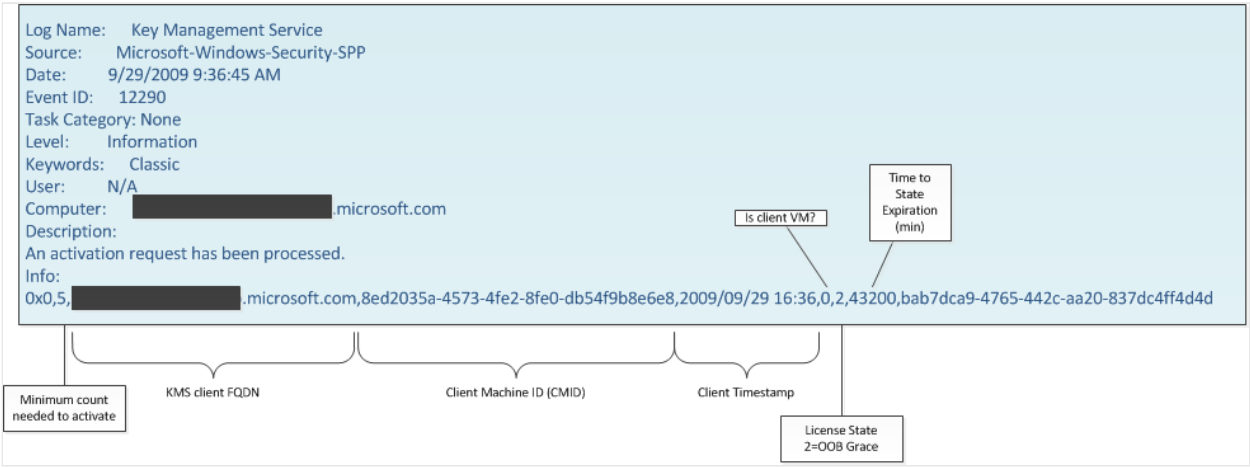
The *Requests with License Status* lines describe all possible license states, past and present. From a troubleshooting perspective, this data is relevant only if the count isn't increasing as expected. In that case, you should see the number of failed requests increasing. To resolve this issue, you should check the product key that was used to first activate the KMS host system. Also, notice that the cumulative request values reset only if you reinstall the KMS host system.

Useful KMS host events

The event IDs described in the following sections are ones you should become familiar with to make troubleshooting host-related issues more efficient.

Event ID 12290

The KMS host creates a log labeled *Event ID 12290* when a KMS client contacts the host when it's trying to activate. Event ID 12290 contains information you can use to figure out what kind of client contacted the host and why a failure occurred. The following segment of an event ID 12290 entry comes from the Key Management Service event log of our KMS host.



The event details include the following information:

- The *Minimum count needed to activate*, which reports that the count from the KMS host must be **5** in order for the client to activate. That means that this OS is a Windows Server OS, although this variable alone doesn't indicate which edition the client is using. If your clients aren't activating, make sure that the host's count allows the client to activate.
- The *Client Machine ID (CMID)*, which is a unique value on each system. If this value isn't unique, it's because the image wasn't correctly configured for distribution using sysprep. To learn more about generalizing your computers, see Sysprep (Generalize) a Windows installation. When you encounter this issue, the KMS host count doesn't increase even though there are enough clients in the environment. For more information, see The KMS current count doesn't increase when you add new Windows Vista or Windows 7-based client computers to the network.
- The *License State and Time to State Expiration*, which is the current license state of the client. This variable can help you tell whether a client is trying to activate for the first time or if it's trying to reactivate. The time entry can also tell you how long the client remains in that state if nothing else changes.

If you're troubleshooting a client and can't find a corresponding event ID 12290 on the KMS host, then the client isn't connecting to the KMS host. Reasons why the event ID 12290 entry is missing can include:

- There's been a network outage.
- The host isn't resolving or isn't registered in DNS.
- The firewall is blocking TCP 1688.
  - The port could also be blocked in other places within the environment, including on the KMS host system itself. By default, the KMS host has a firewall exception for KMS, but this exception isn't automatically enabled. You have to enable the exception manually.
- The event log is full.

KMS clients log two corresponding events: event ID 12288 and event ID 12289. For information about these events, see the KMS client section.

Event ID 12293

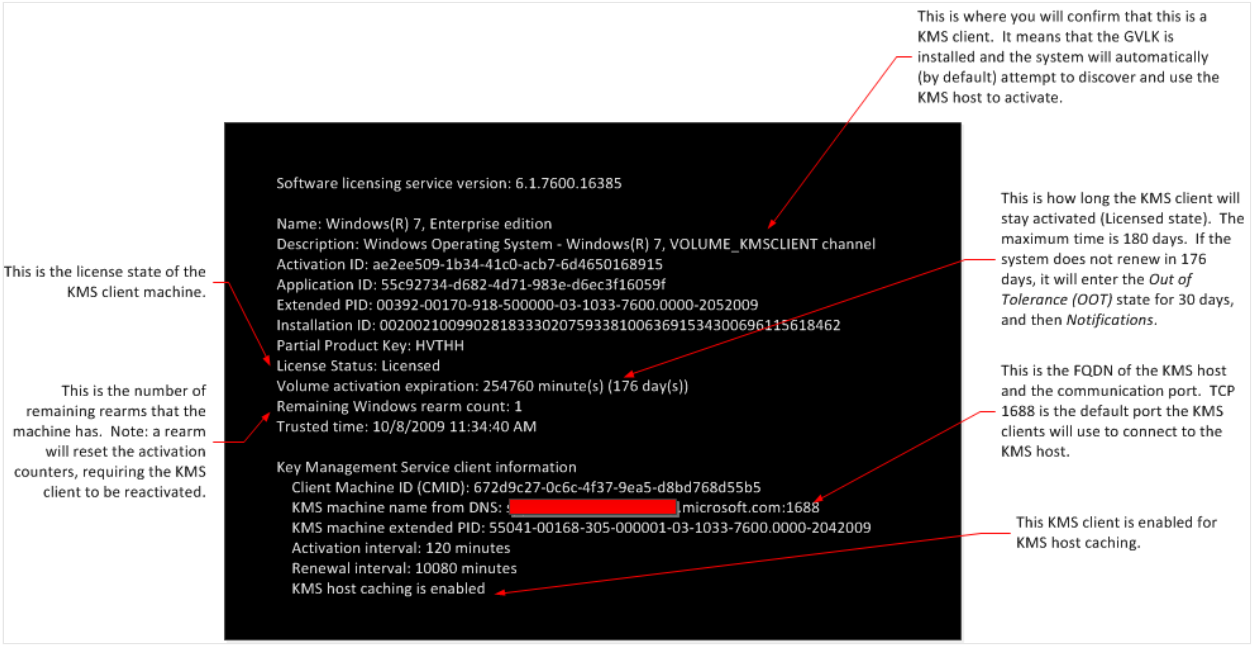
Another relevant event to look for on your KMS host is *Event ID 12293*. This event indicates that the host didn't publish the required records in DNS. This scenario can potentially cause failures, and you should make sure the event isn't there after you set up your host and before you deploy clients. For more information about DNS issues, see Common troubleshooting procedures for KMS and DNS issues.

KMS client

You can also use the `slmgr.vbs` command and Event Viewer to troubleshoot activation on the KMS clients.

Slmgr.vbs and the Software Licensing service

To see verbose output from the Software Licensing service, open an elevated Command Prompt window and enter `slmgr.vbs /dlv` at the command prompt. The following screenshot shows the results of this command on one of our KMS hosts within Microsoft.



Here are some variables you should pay attention to in the output while troubleshooting:

- *Name*, which tells you which edition of Windows the KMS client system is using. You can use this variable to verify that the version of Windows you're trying to activate is compatible with KMS.
- *Description*, which shows you which key was installed. For example, `VOLUME_KMSCLIENT` indicates that the system has installed the KMS Client Setup Key, or GVLK, which is the default configuration for volume license media. A system with a GVLK automatically tries to activate by using a KMS host. If you see a different value here, such as MAK, you must reinstall the GVLK to configure this system as a KMS client. You can manually install the key by following the instructions to run `slmgr.vbs /ipk <GVLK>` in KMS client setup keys, or follow the directions in Volume Activation Management Tool (VAMT) Technical Reference to use the VAMT instead.

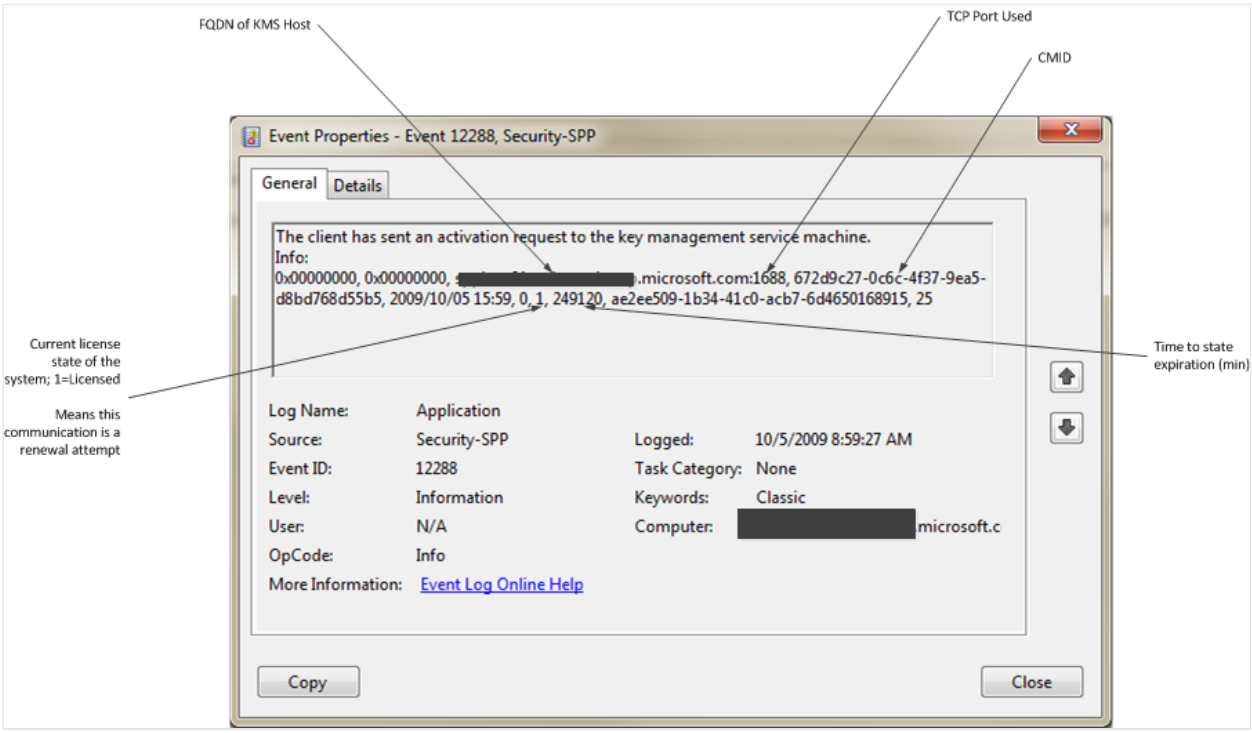
- The *Partial Product Key*, which you can use to determine whether the KMS Client Setup Key matches the operating system the KMS client is using. By default, the correct key is present on systems that are built using media from the Volume License Service Center (VLSC) portal. In some cases, customers may use Multiple Activation Key (MAK) activation until there are enough systems in the environment to support KMS activation. You must install the KMS Client Setup key on these systems to transition them from MAK to KMS. Use VAMT to install this key and make sure you're using the correct key.
- *License Status* shows the status of the KMS client system. For a system activated by KMS, this value should be **Licensed**. Any other value may indicate that there's a problem. For example, if the KMS host is functioning correctly and the KMS client still doesn't activate or is stuck in a **Grace** state, that means something is preventing the client from reaching the host system. This blockage can be a firewall issue, network outage, and so on.
- The *Client Machine ID (CMID)*, which should be unique in every KMS client. As mentioned in Check the Software Licensing service using the slmgr.vbs command, a common issue related to count is if the count doesn't increase beyond one no matter how many KMS hosts or clients you activate in the environment. For more information, see The KMS current count doesn't increase when you add new Windows Vista or Windows 7-based client computers to the network.
- The *KMS Machine Name from DNS*, which shows both the FQDN of the KMS host that the client successfully used for activation and which TCP port it used to communicate.
- *KMS Host Caching*, which shows whether or not caching is enabled. Caching is typically enabled by default. When you enable caching, the KMS client caches the same KMS host that it used for activation and communicates directly with this host instead of querying DNS when it's time to reactivate. If the client can't contact the cached KMS host, it queries DNS to discover a new KMS host.

KMS client events

The following sections describe client events that you should be familiar with to help you troubleshoot potential issues more efficiently.

Event ID 12288 and Event ID 12289

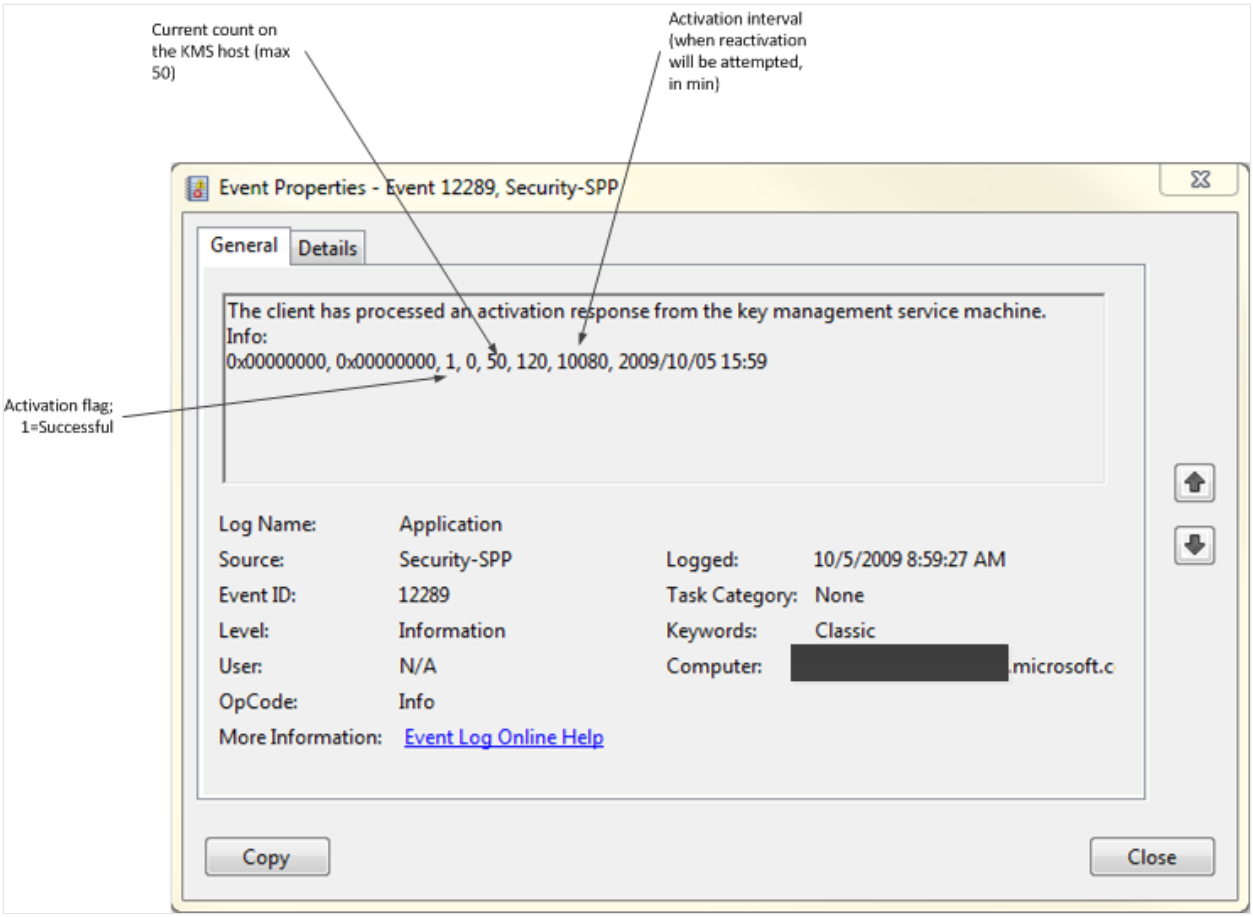
When a KMS client successfully activates or reactivates, the client logs two events: event ID 12288 and event ID 12289. The following screenshot showing a segment of an event ID 12288 entry comes from the Key Management Service event log of our KMS client.



If you see only event ID 12288 without a corresponding event ID 12289, either the KMS client couldn't reach the KMS host, the KMS host didn't respond, or the client didn't receive the host's response. In these cases, you must verify that the KMS host is discoverable and that the KMS clients can contact it.

The most relevant information in event ID 12288 is the data in the *Info* field. For example, Info shows the current state of the client and which FQDN and TCP port the client used when it tried to activate. You can use the FQDN to troubleshoot scenarios where the count on a KMS host doesn't increase. For example, if there are too many KMS hosts available to the clients (either legitimate or unsupported systems), then the count may be distributed over all of them.

An unsuccessful activation doesn't always mean that the client has event ID 12288 and not 12289. A failed activation or reactivation may also have both events. In this case, you have to examine the second event to verify the reason for the failure.



The Info section of event ID 12289 provides the following information:

- *Activation Flag*, which indicates whether the activation succeeded (**1**) or failed (**0**).
- *Current Count on the KMS Host*, which shows the count value on the KMS host when the client tries to activate. If activation fails, it may be because the count is insufficient for this client OS or that there aren't enough systems in the environment to build the count.

What does support ask for?

If your activations aren't working as expected after troubleshooting, you can contact Microsoft Support for technical assistance. The Support Engineer typically asks for the following information:

- `slmgr.vbs /dlv` output from the KMS host and KMS client systems.
- Event logs from both the KMS host (Key Management Service log) and KMS client systems (Application log).

Next steps

- Ask the Core Team: #Activation

Slmgr.vbs options for obtaining volume activation information

Article • 05/19/2022 • Applies to: Windows Server 2012 R2, Windows 10, Windows 8.1

The following describes the syntax of the Slmgr.vbs script, and the tables in this article describe each command-line option.

Windows Command Prompt

```
slmgr.vbs [<ComputerName> [<User> <Password>]] [<Options>]
```

> **Note**
>
> In this article, square brackets [] enclose optional arguments, and angle brackets <> enclose placeholders. When you type these statements, omit the brackets and replace the placeholders by using corresponding values.

> **Note**
>
> For information about other software products that use volume activation, see the documents specifically written for those applications.

Using Slmgr on remote computers

To manage remote clients, use the Volume Activation Management Tool (VAMT) version 1.2 or later, or create custom WMI scripts that are aware of the differences between platforms. For more information about WMI properties and methods for Volume Activation, see WMI Properties and Methods for Volume Activation.

> **Important**
>
> Because of WMI changes in Windows 7 and Windows Server 2008 R2, the Slmgr.vbs script is not intended to work across platforms. Using Slmgr.vbs to manage a Windows 7 or Windows Server 2008 R2 system from the Windows Vista® operating system is not supported. Trying to manage an older system from Windows 7 or Windows Server 2008 R2 will generate a specific version

mismatch error. For example, running **cscript slmgr.vbs <vista_machine_name> /dlv** produces the following output:

> Microsoft (R) Windows Script Host Version 5.8 Copyright (C) Microsoft Corporation. All rights reserved.
>
> The remote machine does not support this version of SLMgr.vbs

General Slmgr.vbs options

Option	Description
[<ComputerName>]	Name of a remote computer (default is local computer)
[<User>]	Account that has the required privilege on the remote computer
[<Password>]	Password for the account that has the required privileges on the remote computer

Global options

Option	Description
/ipk <ProductKey>	Tries to install a 5×5 product key. The product key provided by the parameter is confirmed valid and applicable to the installed operating system. If not, an error is returned. If the key is valid and applicable, the key is installed. If a key is already installed, it is silently replaced. To prevent instability in the license service, the system should be restarted or the Software Protection Service should be restarted. This operation must be run from an elevated Command Prompt window, or the Standard User Operations registry value must be set to allow unprivileged users extra access to the Software Protection Service.

Option	Description
/ato [<Activation ID>]	For retail editions and volume systems that have a KMS host key or a Multiple Activation Key (MAK) installed, **/ato** prompts Windows to try online activation. For systems that have a Generic Volume License Key (GVLK) installed, this prompts a KMS activation attempt. Systems that have been set to suspend automatic KMS activation attempts (**/stao**) still try KMS activation when **/ato** is run. **Note:** Starting in Windows 8 (and Windows Server 2012), the **/stao** option is deprecated. Use the **/act-type** option instead. The parameter <**Activation ID**> expands **/ato** support to identify a Windows edition installed on the computer. Specifying the <**Activation ID**> parameter isolates the effects of the option to the edition associated with that Activation ID. Run **slmgr.vbs /dlv all** to get the Activation IDs for the installed version of Windows. If you have to support other applications, see the guidance provided by that application for further instruction. KMS activation does not require elevated privileges. However, online activation does require elevation, or the Standard User Operations registry value must be set to allow unprivileged users extra access to the Software Protection Service.
/dli [<Activation ID> | All]	Display license information. By default, **/dli** displays the license information for the installed active Windows edition. Specifying the <**Activation ID**> parameter displays the license information for the specified edition that is associated with that Activation ID. Specifying **All** as the parameter displays license information for all applicable installed products. This operation does not require elevated privileges.
/dlv [<Activation ID> | All]	Display detailed license information. By default, **/dlv** displays the license information for the installed operating system. Specifying the <**Activation ID**> parameter displays the license information for the specified edition associated with that Activation ID. Specifying the **All** parameter displays license information for all applicable installed products. This operation does not require elevated privileges.
/xpr [<Activation ID>]	Display the activation expiration date for the product. By default, this refers to the current Windows edition and is primarily useful for KMS clients, because MAK and retail activation is perpetual. Specifying the <**Activation ID**> parameter displays the activation expiration date of the specified edition that is associated with that Activation ID.This operation does not require elevated privileges.

Advanced options

Option	Description
/cpky	Some servicing operations require the product key to be available in the registry during Out-of-Box Experience (OOBE) operations. The **/cpky** option removes the product key from the registry to prevent this key from being stolen by malicious code. For retail installations that deploy keys, best practices recommend running this option. This option is not required for MAK and KMS host keys, because this is the default behavior for those keys. This option is required only for other types of keys whose default behavior is not to clear the key from the registry. This operation must be run in an elevated Command Prompt window.
/ilc <license_file>	This option installs the license file specified by the required parameter. These licenses may be installed as a troubleshooting measure, to support token-based activation, or as part of a manual installation of an on-boarded application. Licenses are not validated during this process: License validation is out of scope for Slmgr.vbs. Instead, validation is handled by the Software Protection Service at runtime. This operation must be run from an elevated Command Prompt window, or the **Standard User Operations** registry value must be set to allow unprivileged users extra access to the Software Protection Service.
/rilc	This option reinstalls all licenses stored in %SystemRoot%\system32\oem and %SystemRoot%\System32\spp\tokens. These are "known-good" copies that were stored during installation. Any matching licenses in the Trusted Store are replaced. Any additional licenses—for example, Trusted Authority (TA) Issuance Licenses (ILs), licenses for applications—are not affected. This operation must be run in an elevated Command Prompt window, or the **Standard User Operations** registry value must be set to allow unprivileged users extra access to the Software Protection Service.
/rearm	This option resets the activation timers. The **/rearm** process is also called by **sysprep /generalize**. This operation does nothing if the **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\SkipRearm** registry entry is set to **1**. See Registry Settings for Volume Activation for details about this registry entry. This operation must be run in an elevated Command Prompt window, or the **Standard User Operations** registry value must be set to allow unprivileged users extra access to the Software Protection Service.
/rearm-app <Application ID>	Resets the licensing status of the specified app.

Option	Description
/rearm-sku <Application ID>	Resets the licensing status of the specified SKU.
/upk [<Application ID>]	This option uninstalls the product key of the current Windows edition. After a restart, the system will be in an Unlicensed state unless a new product key is installed. Optionally, you can use the <**Activation ID**> parameter to specify a different installed product. This operation must be run from an elevated Command Prompt window.
/dti [<Activation ID>]	Displays installation ID for offline activation.
/atp <Confirmation ID>	Activate product by using user-provided confirmation ID.

KMS client options

Option	Description
/skms <Name[:Port] | : port> [<Activation ID>]	This option specifies the name and, optionally, the port of the KMS host computer to contact. Setting this value disables auto-detection of the KMS host. If the KMS host uses Internet Protocol version 6 (IPv6) only, the address must be specified in the format <hostname>:<port>. IPv6 addresses contain colons (:), which the Slmgr.vbs script does not parse correctly. This operation must be run in an elevated Command Prompt window.
/skms-domain <FQDN> [<Activation ID>]	Sets the specific DNS domain in which all KMS SRV records can be found. This setting has no effect if the specific single KMS host is set by using the **/skms** option. Use this option, especially in disjoint namespace environments, to force KMS to ignore the DNS suffix search list and look for KMS host records in the specified DNS domain instead.
/ckms [<Activation ID>]	This option removes the specified KMS host name, address, and port information from the registry and restores KMS auto-discovery behavior. This operation must be run in an elevated Command Prompt window.
/skhc	This option enables KMS host caching (default). After the client discovers a working KMS host, this setting prevents the Domain Name System (DNS) priority and weight from affecting further communication with the host. If the system can no longer contact the working KMS host, the client tries to discover a new host. This operation must be run in an elevated Command Prompt window.

Option	Description
/ckhc	This option disables KMS host caching. This setting instructs the client to use DNS auto-discovery each time it tries KMS activation (recommended when using priority and weight). This operation must be run in an elevated Command Prompt window.

KMS host configuration options

Option	Description
/sai <Interval>	This option sets the interval in minutes for unactivated clients to try to connect to KMS. The activation interval must be between 15 minutes and 30 days, although the default value (two hours) is recommended. The KMS client initially picks up this interval from registry but switches to the KMS setting after it receives the first KMS response. This operation must be run in an elevated Command Prompt window.
/sri <Interval>	This option sets the renewal interval in minutes for activated clients to try to connect to KMS. The renewal interval must be between 15 minutes and 30 days. This option is set initially on both the KMS server and client sides. The default value is 10,080 minutes (7 days). The KMS client initially picks up this interval from the registry but switches to the KMS setting after it receives the first KMS response. This operation must be run in an elevated Command Prompt window.
/sprt <Port>	This option sets the port on which the KMS host listens for client activation requests. The default TCP port is 1688. This operation must be run from an elevated Command Prompt window.
/sdns	Enable DNS publishing by the KMS host (default). This operation must be run in an elevated Command Prompt window.
/cdns	Disable DNS publishing by the KMS host. This operation must be run in an elevated Command Prompt window.
/spri	Set the KMS priority to normal (default). This operation must be run in an elevated Command Prompt window.
/cpri	Set the KMS priority to low. Use this option to minimize contention from KMS in a co-hosted environment. Note that this could cause KMS starvation, depending on what other applications or server roles are active. Use with care. This operation must be run in an elevated Command Prompt window.

Option	Description
/act-type [<Activation-Type>] [<Activation ID>]	This option sets a value in the registry that limits volume activation to a single type. Activation Type **1** limits activation to Active Directory only; **2** limits it to KMS activation; **3** to token-based activation. The **0** option allows any activation type and is the default value.

Token-based activation configuration options

Option	Description
/lil	List the installed token-based activation issuance licenses.
/ril <ILID> <ILvID>	Remove an installed token-based activation issuance license. This operation must be run from an elevated Command Prompt window.
/stao	Set the **Token-based Activation Only** flag, disabling automatic KMS activation. This operation must be run in an elevated Command Prompt window. This option was removed in Windows Server 2012 R2 and Windows 8.1. Use the **/act–type** option instead.
/ctao	Clear the **Token-based Activation Only** flag (default), enabling automatic KMS activation. This operation must be run in an elevated Command Prompt window. This option was removed in Windows Server 2012 R2 and Windows 8.1. Use the **/act–type** option instead.
/ltc	List valid token-based activation certificates that can activate installed software.
/fta <Certificate Thumbprint> [<PIN>]	Force token-based activation by using the identified certificate. The optional personal identification number (PIN) is provided to unlock the private key without a PIN prompt if you use certificates that are protected by hardware (for example, smart cards).

Active Directory-based activation configuration options

Option	Description

Option	Description
/ad-activation-online <Product Key> [<Activation Object name>]	Collects Active Directory data and starts Active Directory forest activation using the credentials that the command prompt is running. Local administrator access is not required. However, Read/Write access to the activation object container in the root domain of the forest is required.
/ad-activation-get-IID <Product Key>	This option starts Active Directory forest activation in phone mode. The output is the installation ID (IID) that can be used to activate the forest over the telephone if internet connectivity is not available. Upon providing the IID in the activation phone call, a CID is returned that is used to complete activation.
/ad-activation-apply-cid <Product Key> <Confirmation ID> [<Activation Object name>]	When you use this option, enter the CID that was provided in the activation telephone call to complete activation
[/name: <AO_Name>]	Optionally, you can append the **/name** option to any of these commands to specify a name for the activation object stored in Active Directory. The name must not exceed 40 Unicode characters. Use double quotation marks to explicitly define the name string. In Windows Server 2012 R2 and Windows 8.1, you can append the name directly after **/ad-activation-online <Product Key>** and **/ad-activation-apply-cid** without having to use the **/name** option.
/ao-list	Displays all of the activation objects that are available to the local computer.
/del-ao <AO_DN> /del-ao <AO_RDN>	Deletes the specified activation object from the forest.

Additional References

- Volume Activation Technical Reference
- Volume Activation Overview

Resolve Windows activation error codes

Article • 09/19/2023

> **Note**
>
> This article is intended for technical support agents and IT professionals. If you're looking for more information about Windows activation error messages, see **Get help with Windows activation errors**.

This article provides troubleshooting information to help you respond to error messages that you may receive when you try to use a Multiple Activation Key (MAK) or the Key Management Service (KMS) to perform Volume Activation on one or more Windows-based computers. Look for the error code in the following tables, then select the link to see more information about that error code and how to resolve it.

For more information about volume activation, see Plan for volume activation.

For more information about volume activation for current and recent versions of Windows, see Volume Activation [client].

For more information about volume activation for older versions of Windows, see Volume Activation information for Windows Vista, Windows Server 2008, Windows Server 2008 R2 and Windows 7.

You can also try our Virtual Agent, which can help you quickly identify and troubleshoot issues related to KMS and MAK activation.

Diagnostic tool

> **Note**
>
> This tool is intended to resolve Windows activation issues on computers that run Enterprise, Professional, or Server editions of Windows.

Microsoft Support and Recovery Assistant (SaRA) simplifies Windows KMS Activation troubleshooting.

Download the Assistant

The SaRA tool troubleshoots by attempting to start up Windows. If Windows returns an activation error code, the tool then displays targeted solutions for the following known error codes:

- 0xC004F038
- 0xC004F039
- 0xC004F041
- 0xC004F074
- 0xC004C008
- 0x8007007b
- 0xC004C003
- 0x8007232B

Summary of error codes

The following table lists known error codes for Windows Activation, and includes links to relevant sections later in this article that can help you resolve related issues.

Error code	Error message	Activation type
0x8004FE21	`This computer is not running genuine Windows.`	MAK KMS client
0x80070005	`Access denied. The requested action requires elevated privileges.`	MAK KMS client KMS host
0x8007007b	`0x8007007b DNS name does not exist.`	KMS client
0x80070490	`The product key you entered did not work. Check the product key and try again, or enter a different one.`	MAK
0x800706BA	`The RPC server is unavailable.`	KMS client
0x8007232A	`DNS server failure.`	KMS host
0x8007232B	`DNS name does not exist.`	KMS client
0x8007251D	`No records found for DNS query.`	KMS client
0x80092328	`DNS name does not exist.`	KMS client
0xC004B100	`The activation server determined that the computer could not be activated.`	MAK

Error code	Error message	Activation type
0xC004C001	`The activation server determined the specified product key is invalid`	MAK
0xC004C003	`The activation server determined the specified product key is blocked`	MAK
0xC004C008	`The activation server determined that the specified product key could not be used.`	KMS
0xC004C020	`The activation server reported that the Multiple Activation Key has exceeded its limit.`	MAK
0xC004C021	`The activation server reported that the Multiple Activation Key extension limit has been exceeded.`	MAK
0xC004F009	`The Software Protection Service reported that the grace period expired.`	MAK
0xC004F00F	`The Software Licensing Server reported that the hardware ID binding is beyond level of tolerance.`	MAK KMS client KMS host
0xC004F014	`The Software Protection Service reported that the product key is not available`	MAK KMS client
0xC004F02C	`The Software Protection Service reported that the format for the offline activation data is incorrect.`	MAK KMS client
0xC004F035	`The Software Protection Service reported that the computer could not be activated with a Volume license product key.`	KMS client KMS host
0xC004F038	`The Software Protection Service reported that the computer could not be activated. The count reported by your Key Management Service (KMS) is insufficient. Please contact your system administrator.`	KMS client
0xC004F039	`The Software Protection Service reported that the computer could not be activated. The Key Management Service (KMS) is not enabled.`	KMS client
0xC004F041	`The Software Protection Service determined that the Key Management Server (KMS) is not activated. KMS needs to be activated.`	KMS client
0xC004F042	`The Software Protection Service determined that the specified Key Management Service (KMS) cannot be used.`	KMS client

Error code	Error message	Activation type
0xC004F050	`The Software Protection Service reported that the product key is invalid.`	MAK KMS KMS client
0xC004F051	`The Software Protection Service reported that the product key is blocked.`	MAK KMS
0xC004F064	`The Software Protection Service reported that the non-genuine grace period expired.`	MAK
0xC004F065	`The Software Protection Service reported that the application is running within the valid non-genuine period.`	MAK KMS client
0xC004F06C	`The Software Protection Service reported that the computer could not be activated. The Key Management Service (KMS) determined that the request timestamp is invalid.`	KMS client
0xC004F074	`The Software Protection Service reported that the computer could not be activated. No Key Management Service (KMS) could be contacted. Please see the Application Event Log for additional information.`	KMS client

Causes and resolutions

This section describes the causes of each error message and troubleshooting steps you can take to resolve them.

0x8004FE21 This computer isn't running genuine Windows

When you receive this error, you see the following output:

Output

```
This computer is not running genuine Windows.
```

0x8004FE21 Causes

This issue can occur for several reasons:

- A user or program installed language packs (MUI) on computers running editions of Windows not licensed for extra language packs.

  > **Note**
  >
  > This issue doesn't necessarily indicate tampering. Some applications can install multilingual support even when that edition of Windows isn't licensed for those language packs.

- When malware modifies Windows in order to install more features.
- Certain system files are corrupted.

Solution: reinstall operating system

To resolve this issue, you must reinstall the operating system.

0x80070005 Access denied

The full text of this error message says, "Access denied. The requested action requires elevated privileges."

0x80070005 Cause

User Account Control (UAC) prohibits activation processes from running in a non-elevated Command Prompt window.

Solution: run slmgr.vbs

To resolve this issue:

1. Open the **Start menu** and search for **Command prompt**.
2. Right-click **Command prompt**.
3. Select **Run as administrator**.
4. In the command prompt, run `slmgr.vbs`.

0x8007007b DNS name doesn't exist

When you encounter this error, you see the following output:

```
Output
```

```
DNS name does not exist.
```

0x8007007b Cause

This issue can occur if the KMS client can't find the KMS SRV resource records in DNS.

Resolution: check the documentation

For more information about troubleshooting such DNS-related issues, see Common troubleshooting procedures for KMS and DNS issues.

0x80070490 The product key didn't work

When you encounter this issue, you see an error message that says, "The product key that you entered didn't work. Check the product key and try again, or enter a different one."

Possible cause

There are two reasons why you may encounter this issue:

- The Multiple Activation Key (MAK) wasn't valid.
- A known issue in Windows Server 2019 interfered with authenticating the product key.

Solution: run a command on an elevated command prompt

To work around this issue and activate the computer:

1. Open the **Start menu** and search for **Command prompt**.
2. Right-click **Command prompt**.
3. Select **Run as administrator**.
4. In the command prompt, run the following command:

   Windows Command Prompt

   ```
   slmgr -ipk <5x5 key>
   ```

0x800706BA The RPC server is unavailable

When you encounter this error, you see the following output:

```
Output

The RPC server is unavailable.
```

0x800706BA cause

You can encounter this issue because of the following things:

- The KMS host doesn't have configured firewall settings.
- DNS SRV records are stale.

Solution 1: inspect the firewall

On the KMS host, make sure you've enabled the firewall exception for the Key Management Service on TCP port 1688.

Solution 2: inspect DNS SRV records

Check your DNS SRV records and make sure they point to a valid KMS host.

Solution 3: Troubleshoot network connections

If you still see this error after performing solutions 1 and 2, check your network connections to make sure you can access the server.

You can also follow the instructions in Common troubleshooting procedures for KMS and DNS issues.

0x8007232A DNS server failure

When you encounter this issue, you see the following output:

```
Output

DNS server failure.
```

0x8007232A cause

You can encounter this issue when the system has network or DNS issues.

Solution: troubleshoot network connections and DNS

To resolve this issue, troubleshoot your network connections and DNS by following the instructions in Common troubleshooting procedures for KMS and DNS issues.

0x8007232B DNS name doesn't exist

When you encounter this error, you see the following output:

Output

```
DNS name does not exist
```

0x8007232B cause

This error message appears when the KMS client can't find KMS server resource records (SRV RRs) in DNS.

Solution 1: point the KMS client to the correct KMS host

Make sure you've installed a KMS and the DNS publishing is enabled (default). If the DNS isn't available, point the KMS client to the KMS host by opening an elevated command-prompt and running the following command:

Windows Command Prompt

```
slmgr.vbs /skms <kms_host_name>
```

Solution 2: get a MAK

If you don't have a KMS host, get and install an MAK, then try activating the system again.

If these solutions don't resolve the issue, see the instructions in Common troubleshooting procedures for KMS and DNS issues.

0x8007251D No records found for DNS query

When you encounter this error, you see this error message:

```
Output

No records found for DNS query.
```

0x8007251D cause

This error message appears when the KMS client can't find the KMS SRV records in the DNS.

Solution: troubleshoot network connections and connection with DNS

To resolve this issue, follow the instructions in Common troubleshooting procedures for KMS and DNS issues to troubleshoot your network connections and DNS.

0x80092328 DNS name doesn't exist

When you encounter this error, you see this error message:

```
Output

DNS name does not exist.
```

0x80092328 cause

You can encounter this issue if the KMS client can't find the KMS SRV resource records in DNS.

Solution: troubleshoot connections

To resolve this issue, follow the instructions in Common troubleshooting procedures for KMS and DNS issues to troubleshoot your network connections and DNS.

0xC004B100 The activation server determined that the computer couldn't be activated

When you encounter this error, you see this error message:

Output

```
The activation server determined that the computer could not be activated.
```

0xC004B100 cause

You can encounter this issue when Microsoft doesn't support the MAK you're using.

Solution: verify that the MAK is valid

To troubleshoot this issue, verify that the MAK you're using is the same MAK that Microsoft provided to you. To verify that the MAK is valid, contact the Microsoft Licensing Activation Centers.

0xC004C001 The activation server determined the specified product key is invalid

When you encounter this error, you see this error message:

Output

```
The activation server determined the specified product key is invalid.
```

0xC004C001 cause

You can encounter this issue when the MAK you enter isn't valid.

Solution: reenter the MAK key and verify it's valid

You can try reentering the MAK to make sure you entered the correct information. Otherwise, verify the MAK you're using is valid by contacting the Microsoft Licensing Activation Centers.

0xC004C003 The activation server determined the specified product key is blocked

When you encounter this error, you see this error message:

Output

```
The activation server determined the specified product key is blocked.
```

0xC004C003 cause

You can encounter this issue if the MAK is blocked on the activation server.

Solution: get a new MAK

To obtain a new MAK, contact the Microsoft Licensing Activation Centers. After you obtain the new MAK, try installing and activating Windows again.

0xC004C008 The activation server determined that the specified product key couldn't be used

When you encounter this error, you see this error message:

Output

```
The activation server determined that the specified product key could not be used.
```

0xC004C008 cause

This error message appears when the KMS key has exceeded its activation limit. You can only activate KMS host keys up to 10 times on no more than six different computers.

Solution: request more activations for activation server permission

If you require more activations, contact the Microsoft Licensing Activation Centers.

0xC004C020 The activation server reported that the Multiple Activation Key has exceeded its limit

When you encounter this error, you see this error message:

Output

```
The activation server reported that the Multiple Activation Key has exceeded its limit.
```

0xC004C020 cause

This error message appears when the MAK exceeds its activation limit. By design, you can only activate a MAK a limited number of times.

Solution: request more activations to increase limit

If you require more activations, contact the Microsoft Licensing Activation Centers.

0xC004C021 Multiple Activation Key extension limit exceeded

When you encounter this error, you see this error message:

Output

```
The activation server reported that teh Multiple Activation Key extension
limit has been exceeded.
```

0xC004C021 cause

This error message appears when the MAK exceeds its activation limit. By design, you can only activate a MAK a limited number of times.

Solution: request more activations to increase extension limit

If you need more activations, contact the Microsoft Licensing Activation Centers.

0xC004F009 The Software Protection Service reported that the grace period expired

When you encounter this error, you see this error message:

Output

```
The Software Protection Service reported that the grace period expired.
```

0xC004F009 cause

This error message appears when the grace period expires before you activate the system. The system is currently in the Notifications state.

Solution: contact the Microsoft Licensing Activation Centers

For assistance, contact the Microsoft Licensing Activation Centers.

0xC004F00F hardware ID binding is beyond level of tolerance

When you encounter this error, you see this error message:

Output

```
The Software Licensing Server reported that the Hardware ID binding is
beyond level of tolerance.
```

0xC004F00F cause

This error message appears when the system hardware changes or its drivers update.

Solution 1: reactivate the system during the grace period

If you're using MAK activation, reactivate the system phone by using either online or phone activation during the Out of Tolerance (OOT) grace period.

Solution 2: restart Windows or run a command

If you're using KMS activation, try one of the following things:

- Restart Windows.
- Open an elevated command-prompt and run the following command:

  Windows Command Prompt

  ```
  slmgr.vbs /ato
  ```

0xC004F014 The Software Protection Service reported that the product key isn't available

When you encounter this error, you see this error message:

Output

```
The Software Protection Service reported that the product key is not
available.
```

0xC004F014 cause

This issue happens when no product keys are installed on the system.

Resolution: install product keys

If you're using MAK activation, install a MAK product key.

If you're using KMS activation:

1. Check the **Pid.txt** file located on the installation media in the \sources folder for a KMS Setup key.
2. Install the key.

0xC004F02C the format for the offline activation data is incorrect

When you encounter this error, you see this error message:

Output

```
The Software Protection Service reported that the format for the offline
activation data is incorrect.
```

0xC004F02C cause

This error message appears when the system detects the data entered during phone activation isn't valid.

Solution: reenter your caller ID

To resolve this issue, make sure you entered the caller ID (CID) correctly.

0xC004F035 Invalid Volume License Key

When you encounter this error, an error message appears that says, "Error: Invalid Volume License Key. In order to activate, you need to change your product key to a valid Multiple Activation Key (MAK) or Retail key. You must have a qualifying operating system license AND a Volume license Windows 7 upgrade license, or a full license for Windows 7 from a retail source. ANY OTHER INSTALLATION OF THIS SOFTWARE IS IN VIOLATION OF YOUR AGREEMENT AND APPLICABLE COPYRIGHT LAW."

This error message indicates that the computer doesn't have a Windows marker in its BIOS that identifies it as an OEM system running a qualifying edition of Windows. In short, this message means the Volume License Key is invalid. This information is required for KMS client activation.

0xC004F035 cause

Microsoft only licenses Windows 7 Volume editions for upgrade. Microsoft doesn't support installing a Volume operating system on a computer that doesn't already have a qualifying operating system installed.

Solution: activate your Volume License Key

To activate your Volume License Key:

1. Change your product key to a valid Multiple Activation Key (MAK) or Retail key. To change your key, you must have both a qualifying operating system license and a Volume license Windows 7 upgrade license, or a full license for Windows 7 from a retail source.
2. Try to activate your key again.

If you see error message 0x80072ee2 when you attempt to activate your key again, you need to activate your key by phone.

To activate your key by phone:

1. Open a command prompt and run `slmgr /dti`, then record the value of the Installation ID.
2. Contact the Microsoft Licensing Activation Center and provide the Installation ID in order to receive a Confirmation ID.
3. To activate by using the Confirmation ID, run `slmgr /atp <Confirmation ID>`.

0xC004F038 The count reported by your Key Management Service (KMS) is insufficient

When you encounter this issue, an error message appears that says, "The Software Protection Service reported that the computer couldn't be activated. The count reported by your Key Management Service (KMS) is insufficient. Please contact your system administrator."

0xC004F038 cause

You normally encounter this issue when the count on the KMS host isn't high enough. For Windows Server, the KMS count must be greater than or equal to five. For Windows (client), the KMS count must be greater than or equal to 25.

Solution: add computers to the KMS pool

Before you can use KMS to activate Windows, you must have more computers in the KMS pool. To obtain the current count on the KMS host, run `Slmgr.vbs /dli`.

0xC004F039 The Key Management Service (KMS) isn't enabled

When you encounter this issue, an error message appears that says, "The Software Protection Service reported that the computer couldn't be activated. The Key Management Service (KMS) isn't enabled."

0xC004F039 cause

This issue occurs when KMS doesn't respond to a KMS request.

Solution: troubleshoot the KMS connection

To resolve this issue, troubleshoot the network connection between the KMS host and the client. Make sure that a firewall isn't blocking or otherwise filtering TCP port 1688 (default).

0xC004F041 The Software Protection Service determined that the Key Management Server (KMS) isn't activated

When you encounter this issue, an error message appears that says, "The Software Protection Service determined that the Key Management Server (KMS) isn't activated. KMS needs to be activated."

0xC004F041 cause

This issue occurs when the KMS host hasn't been activated.

Solution: activate the KMS host

To resolve this issue, activate the KMS host by using either online or telephone activation.

0xC004F042 the specified Key Management Service (KMS) can't be used

When you encounter this error, you see this error message:

Output

```
The Software Protection Service determined that teh specified Key Management
Service cannot be read.
```

0xC004F042 cause

You may encounter this issue when the KMS client tried to contact a KMS host that couldn't activate the client software. This scenario is common in mixed environments with application-specific and operating system-specific KMS hosts.

Solution: make sure the KMS client connects to the correct host

To resolve this issue, make sure your KMS clients are connection to the correct hosts, especially if you're using specific KMS hosts to activate specific applications or OSes.

0xC004F050 The Software Protection Service reported that the product key is invalid

When you encounter this error, you see this error message:

Output

```
The Software Protection Service reported that the product key is invalid
```

0xC004F050 cause

You can encounter an issue if there was a typo or if you try to use a Beta key on a generally available version of the operating system.

Solution: make sure you're using the right key

To resolve this issue, make sure you're installing the correct KMS key on the corresponding version of Windows. Make sure you've entered the correct characters and numbers. If you're copying and pasting the key, make sure the Clipboard didn't replace the hyphens with em-dashes.

0xC004F051 The Software Protection Service reported that the product key is blocked

When you encounter this error, you see this error message:

Output

```
The Software Protection Service reported that the product key is blocked.
```

0xC004F051 cause

This error message appears when Microsoft blocks the product key.

Solution: get a new MAK or KMS key

To resolve this issue, get a new MAK or KMS key, install it on the system, then try activating again.

0xC004F064 The Software Protection Service reported that the non-genuine grace period expired

When you encounter this error, you see this error message:

Output

```
The Software Protection Service reported that teh non-genuine grace period
expired.
```

0xC004F064 cause

This error occurs when Windows Activation Tools (WAT) determines that a system that's trying to be activated isn't authentic.

Solution: contact assistance

To resolve this issue, contact the Microsoft Licensing Activation Centers for assistance.

0xC004F065 the application is running within the valid non-genuine period

When you encounter this error, you see this error message:

Output

```
The Software Protection Service reported that the application is running
within the valid non-genuine period.
```

0xC004F065 cause

You may encounter this error message because WAT has determined the system trying to activate isn't genuine. However, because of the Non-Genuine Grace Period, the system continues to run.

Solution: get and install a genuine product key before the grace period ends

To resolve this issue, you must get and install a genuine product key, then activate the system before the grace period ends. If you don't, the system goes into the Notification state at the end of the grace period.

0xC004F06C The request timestamp is invalid

When you encounter this issue, an error message appears that says, "The Software Protection Service reported that the computer couldn't be activated. The Key Management Service (KMS) determined that the request timestamp is invalid."

0xC004F06C cause

You can encounter this issue if the system time on the client computer is too different from the time on the KMS host. Time synchronization is important to system and

network security, so desynchronization can cause issues to occur.

Solution: change the system times of the client to match the KMS host

To resolve this issue, you need to change the system time on the client to match the KMS host. We recommend you use a Network Time Protocol (NTP) time source or Active Directory Domain Services for time synchronization. This issue uses UTP time, so time zone selection doesn't affect it.

0xC004F074 No Key Management Service (KMS) could be contacted

When you encounter this issue, an error message appears that says, "The Software Protection Service reported that the computer couldn't be activated. No Key Management Service (KMS) could be contacted. Please see the Application Event Log for additional information."

0xC004F074 cause

This issue occurs when all the KMS host systems your client tires to contact return errors.

Solution: troubleshoot all returned errors

To resolve this issue:

1. Open the **Application Event Log**.
2. Identify each event associated with the activation attempt that has an Event ID of 12288.
3. Troubleshoot each of these errors by following the instructions in Common troubleshooting procedures for KMS and DNS issues.

KMS activation: known issues

Article • 08/22/2022

Try our Virtual Agent - It can help you quickly identify and fix common issues related to KMS and MAK activation

This article describes common questions and issues that can arisse during Key Management Service (KMS) activations, and provides guidance for addressing the issues.

> ⓘ **Note**
>
> If you suspect that your issue is related to DNS, see **Common troubleshooting procedures for KMS and DNS issues**.

Should I back up KMS host information?

Backup is not required for KMS hosts. However, if you use a tool to routinely clean up event logs, the activation history stored in the logs can be lost. If you use the event log to track or document KMS activations, periodically export the Key Management Service event log from the Applications and Services Logs folder of Event Viewer.

If you use System Center Operations Manager, the System Center Data Warehouse database stores event log data for reporting, therefore you do not have to back up the event logs separately.

Is the KMS client computer activated?

On the KMS client computer, open the **System** control panel, and look for the **Windows is activated** message. Alternatively, run Slmgr.vbs and use the the **/dli** command-line option.

The KMS client computer does not activate

Verify that the KMS activation threshold is met. On the KMS host computer, run Slmgr.vbs and use the **/dli** command-line option to determine the host's current count. Until the KMS host has a count of 25, Windows 7 client computers cannot be activated.

Windows Server 2008 R2 KMS clients require a KMS count of 5 for activation. For more information about KMS requirements, see the Volume Activation Planning Guide.

On the KMS client computer, look in the Application event log for event ID 12289. Check this event for the following information:

- Is the result code **0**? Anything else is an error.
- Is the KMS host name in the event correct?
- Is the KMS port correct?
- Is the KMS host accessible?
- If the client is running a non-Microsoft firewall, does the outbound port have to be configured?

On the KMS host computer, look in the KMS event log for event ID 12290. Check this event for the following information:

- Did the KMS host log a request from the client computer? Verify that the name of the KMS client computer is listed. Verify that the client and KMS host can communicate. Did the client receive the response?
- If no event is logged from the KMS client, the request did not reach the KMS host or the KMS host was unable to process it. Make sure that routers do not block traffic using TCP port 1688 (if the default port is used) and that stateful traffic to the KMS client is allowed.

What does this error code mean?

Except for KMS events that have event ID 12290, Windows logs all activation events to the Application event log under the event provider name Microsoft-Windows-Security-SPP. Windows logs KMS events to the Key Management Service log in the Applications and Services folder. IT pros can run Slui.exe to display a description of most activation-related error codes. The general syntax for this command is as follows:

Windows Command Prompt

```
slui.exe 0x2a ErrorCode
```

For example, if event ID 12293 contains error code 0x8007267C, you can display a description of that error by running the following command:

Windows Command Prompt

```
slui.exe 0x2a 0x8007267C
```

For more information about specific error codes and how to address them, see Resolving common activation error codes.

Clients are not adding to the KMS count

To reset the client computer ID (CMID) and other product-activation information, run **sysprep /generalize** or **slmgr /rearm**. Otherwise, each client computer looks identical, and the KMS host does not count them as separate KMS clients.

KMS hosts are unable to create SRV records

Domain Name System (DNS) may restrict Write access or may not support dynamic DNS (DDNS). In this case, give the KMS host Write access to the DNS database, or create the service (SRV) resource record (RR) manually. For more information about KMS and DNS issues, see Common troubleshooting procedures for KMS and DNS issues.

Only the first KMS host is able to create SRV records

If the organization has more than one KMS host, the other hosts might not able to update the SRV RR unless the SRV default permissions are changed. For more information about KMS and DNS issues, see Common troubleshooting procedures for KMS and DNS issues.

I installed a KMS key on the KMS client

KMS keys should be installed only on KMS hosts, not on KMS clients. Run **slmgr.vbs -ipk <SetupKey>**. For tables of keys that you can use to configure the computer as a KMS client, see KMS client setup keys. These keys are publicly known and are edition-specific. Remember to delete any unnecessary SRV RRs from DNS, and then restart the computers.

A KMS host failed

If a KMS host fails, you must install a KMS host key on a new host and then activate the host. Make sure that the new KMS host has an SRV RR in the DNS database. If you install the new KMS host using the same computer name and IP address as the failed KMS host, the new KMS host can use the DNS SRV record of the failed host. If the new host

has a different computer name, you can manually remove the DNS SRV RR of the failed host or (if scavenging is enabled in DNS) let DNS automatically remove it. If the network is using DDNS, the new KMS host automatically creates a new SRV RR on the DNS server. The new KMS host then starts collecting client renewal requests and begins activating clients as soon as the KMS activation threshold is met.

If your KMS clients use auto-discovery, they automatically select another KMS host if the original KMS host does not respond to renewal requests. If the clients do not use auto-discovery, you must manually update the KMS client computers that were assigned to the failed KMS host by running **slmgr.vbs /skms**. To avoid this scenario, configure the KMS clients to use auto-discovery. For more information, see the Volume Activation Deployment Guide.

MAK activation: known issues

Article • 08/22/2022

Try our Virtual Agent - It can help you quickly identify and fix common issues related to KMS and MAK activation

This article describes common issues that can occur during Multiple Activation Key (MAK) activations, and provides guidance for addressing those issues.

How can I tell whether my computer is activated?

On the computer, open the **System** control panel and look for **Windows is activated**. Alternatively, run Slmgr.vbs and use the **/dli** command-line option.

The computer does not activate over the internet

Make sure that the required ports are open in the firewall. For a list of ports, see the Volume Activation Deployment Guide.

Internet and telephone activation fail

Contact a local Microsoft Activation Center. For the telephone numbers of Microsoft Activation Centers worldwide, go to Microsoft Licensing Activation Centers worldwide telephone numbers. Make sure to provide the Volume License agreement information and proof of purchase when you call.

Slmgr.vbs /ato returns an error code

If Slmgr.vbs returns a hexadecimal error code, determine the corresponding error message by running the following script:

Windows Command Prompt

```
slui.exe 0x2a 0x <ErrorCode>
```

For more information about specific error codes and how to address them, see Resolving common activation error codes.

Guidelines for troubleshooting DNS-related activation issues

Article • 05/19/2022

You may have to use some of these methods if one or more of the following conditions are true:

- You use volume-licensed media and a Volume License generic product key to install one of the following operating systems:
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012 R2
  - Windows Server 2012
  - Windows Server 2008 R2
  - Windows Server 2008
  - Windows 10
  - Windows 8.1
  - Windows 8
- The activation wizard cannot connect to a KMS host computer.

When you try to activate a client system, the activation wizard uses DNS to locate a corresponding computer that's running the KMS software. If the wizard queries DNS and does not find the DNS entry for the KMS host computer, the wizard reports an error.

Review the following list to find an approach that fits your circumstances:

- If you cannot install a KMS host or if you cannot use KMS activation, try the Change the product key to an MAK procedure.
- If you have to install and configure a KMS host, use the Configure a KMS host for the clients to activate against procedure.
- If the client cannot locate your existing KMS host, use the following procedures to troubleshoot your routing configurations. These procedures are arranged from the simplest to the most complex.
  - Verify basic IP connectivity to the DNS server
  - Verify the KMS host configuration
  - Determine the type of routing issue
  - Verify the DNS configuration
  - Manually create a KMS SRV record
  - Manually assign a KMS host to a KMS client
  - Configure the KMS host to publish in multiple DNS domains

Change the product key to an MAK

If you cannot install a KMS host or, for some other reason, you cannot use KMS activation, change the product key to an MAK. If you downloaded Windows images from the Microsoft Developer Network (MSDN), or from TechNet, the stock-keeping units (SKUs) that are listed below the media are generally volume licensed-media, and the product key that's provided is an MAK key.

To change the product key to an MAK, follow these steps:

1. Open an elevated Command Prompt window. To do this, press the Windows logo key+X, right-click **Command Prompt**, and then select **Run as administrator**. If you are prompted for an administrator password or for confirmation, type the password or provide confirmation.
2. At the command prompt, run the following command:

   Windows Command Prompt

   ```
   slmgr -ipk xxxxx-xxxxx-xxxxx-xxxxx-xxxxx
   ```

   > ⓘ **Note**
   >
   > The **xxxxx-xxxxx-xxxxx-xxxxx-xxxxx** placeholder represents your MAK product key.

Return to the procedure list.

Configure a KMS host for the clients to activate against

KMS activation requires that a KMS host be configured for the clients to activate against. If there are no KMS hosts configured in your environment, install and activate one by using an appropriate KMS host key. After you configure a computer on the network to host the KMS software, publish the Domain Name System (DNS) settings.

For information about the KMS host configuration process, see Activate using Key Management Service and Install and Configure VAMT.

Return to the procedure list.

Verify basic IP connectivity to the DNS server

Verify basic IP connectivity to the DNS server by using the ping command. To do this, follow these steps on both the KMS client that is experiencing the error and the KMS host computer:

1. Open an elevated Command Prompt window.
2. At the command prompt, run the following command:

```
Windows Command Prompt

ping <DNS_Server_IP_address>
```

> **Note**
>
> If the output from this command does not include the phrase "Reply from," there is a network problem or DNS issue that you must resolve before you can use the other procedures in this article. For more information about how to troubleshoot TCP/IP issues if you cannot ping the DNS server, see **Advanced troubleshooting for TCP/IP issues**.

Return to the procedure list.

Verify the configuration of the KMS host

Check the registry of the KMS host server to determine whether it is registering with DNS. By default, a KMS host server dynamically registers a DNS SRV record one time every 24 hours.

> **Important**
>
> Follow the steps in this section carefully. Serious problems might occur if you modify the registry incorrectly. Before you modify it, **back up the registry for restoration** in case problems occur.

To check this setting, follow these steps:

1. Start Registry Editor. To do this, right-click **Start**, select **Run**, type **regedit**, and then press Enter.

2. Locate the **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform** subkey (previously **SL** instead of **SoftwareProtectionPlatform** in Windows Server 2008 and Windows Vista), and check the value of the **DisableDnsPublishing** entry. This entry has the following possible values:

   - **0** or undefined (default): The KMS host server registers a SRV record once every 24 hours.
   - **1**: The KMS host server does not automatically register SRV records. If your implementation does not support dynamic updates, see Manually create a KMS SRV record.

3. If the **DisableDnsPublishing** entry is missing, create it (the type is DWORD). If dynamic registration is acceptable, leave the value undefined or set it to **0**.

Return to the procedure list.

Determine the type of routing issue

You can use the following commands to determine whether this is a name resolution issue or an SRV record issue.

1. On a KMS client, open an elevated Command Prompt window.

2. At the command prompt, run the following commands:

   Windows Command Prompt

   ```
   cscript \windows\system32\slmgr.vbs -skms <KMS_FQDN>:<port>
   cscript \windows\system32\slmgr.vbs -ato
   ```

   > **Note**
   >
   > In this command, <KMS_FQDN> represents the fully qualified domain name (FQDN) of the KMS host computer and <port> represents the TCP port that KMS uses.

   If these commands resolve the problem, this is an SRV record issue. You can you can troubleshoot it by using one of the commands that are documented in the Manually assign a KMS host to a KMS client procedure.

3. If the problem persists, run the following commands:

Windows Command Prompt

```
cscript \windows\system32\slmgr.vbs -skms <IP Address>:<port>
cscript \windows\system32\slmgr.vbs -ato
```

> **Note**
>
> In this command, <IP Address> represents the IP address of the KMS host computer and <port> represents the TCP port that KMS uses.

If these commands resolve the problem, this is most likely a name resolution issue. For additional troubleshooting information, see the Verify the DNS configuration procedure.

4. If none of these commands resolves the problem, check the computer's firewall configuration. Any activation communications that occur between KMS clients and the KMS host use the 1688 TCP port. The firewalls on both the KMS client and the KMS host must allow communication over port 1688.

Return to the procedure list.

Verify the DNS configuration

> **Note**
>
> Unless otherwise stated, follow these steps on a KMS client that has experienced the applicable error.

1. Open an elevated Command Prompt window
2. At the command prompt, run the following command:

Windows Command Prompt

```
IPCONFIG /all
```

3. From the command results, note the following information:

   - The assigned IP address of the KMS client computer
   - The IP address of the Primary DNS server that the KMS client computer uses
   - The IP address of the default gateway that the KMS client computer uses
   - The DNS suffix search list that the KMS client computer uses

4. Verify that the KMS host SRV records are registered in DNS. To do this, follow these steps:
   a. Open an elevated Command Prompt window.
   b. At the command prompt, run the following command:

```
Windows Command Prompt

nslookup -type=all _vlmcs._tcp>kms.txt
```

   c. Open the KMS.txt file that the command generates. This file should contain one or more entries that resemble the following entry:

```
_vlmcs._tcp.contoso.com SRV service location:
priority = 0
weight = 0
port = 1688 svr hostname = kms-server.contoso.com
```

> **Note**
>
> In this entry, contoso.com represents the domain of the KMS host.

   i. Verify the IP address, host name, port, and domain of the KMS host.
   ii. If these **_vlmcs** entries exist, and if they contain the expected KMS host names, go to Manually assign a KMS host to a KMS client.

> **Note**
>
> If the **nslookup** command finds the KMS host, it does not mean that the DNS client can find the KMS host. If the **nslookup** command finds the KMS host, but you still cannot activate by using the KMS host, check the other DNS settings, such as the primary DNS suffix and the search list of the DNS suffix.

5. Verify that the search list of the primary DNS suffix contains the DNS domain suffix that is associated with the KMS host. If the search list does not include this information, go to the Configure the KMS host to publish in multiple DNS domains procedure.

Return to the procedure list.

Manually create a KMS SRV record

To manually create an SRV record for a KMS host that uses a Microsoft DNS server, follow these steps:

1. On the DNS server, open DNS Manager. To open DNS Manager, select **Start**, select **Administrative Tools**, and then select **DNS**.
2. Select the DNS server on which you have to create the SRV resource record.
3. In the console tree, expand **Forward Lookup Zones**, right-click the domain, and then select **Other New Records**.
4. Scroll down the list, select **Service Location (SRV)**, and then select **Create Record**.
5. Type the following information:

    - Service: **_VLMCS**
    - Protocol: **_TCP**
    - Port number: **1688**
    - Host offering the service: **<*FQDN of the KMS host*>**

6. When you are finished, select **OK**, and then select **Done**.

To manually create an SRV record for a KMS host that uses a BIND 9.x-compliant DNS server, follow the instructions for that DNS server, and provide the following information for the SRV record:

- Name: **_vlmcs._TCP**
- Type: **SRV**
- Priority: **0**
- Weight: **0**
- Port: **1688**
- Hostname: **<*FQDN or A-Name of the KMS host*>**

To configure a BIND 9.x-compatible DNS server to support KMS auto-publishing, configure the DNS server to enable resource record updates from KMS hosts. For example, add the following line to the zone definition in Named.conf or in Named.conf.local:

Windows Command Prompt

```
allow-update { any; };
```

Manually assign a KMS host to a KMS client

By default, the KMS clients use the automatic discovery process. According to this process, a KMS client queries DNS for a list of servers that have published `_vlmcs` SRV

records within the membership zone of the client. DNS returns the list of KMS hosts in a random order. The client picks a KMS host and tries to establish a session on it. If this attempt works, the client caches the name of the KMS host and tries to use it for the next renewal attempt. If the session setup fails, the client randomly picks another KMS host. We highly recommend that you use the automatic discovery process.

However, you can manually assign a KMS host to a particular KMS client. To do this, follow these steps.

1. On a KMS client, open an elevated Command Prompt window.
2. Depending on your implementation, follow one of these steps:

    - To assign a KMS host by using the FQDN of the host, run the following command:

      Windows Command Prompt

      ```
      cscript \windows\system32\slmgr.vbs -skms <KMS_FQDN>:<port>
      ```

    - To assign a KMS host by using the version 4 IP address of the host, run the following command:

      Windows Command Prompt

      ```
      cscript \windows\system32\slmgr.vbs -skms <IPv4Address>:<port>
      ```

    - To assign a KMS host by using the version 6 IP address of the host, run the following command:

      Windows Command Prompt

      ```
      cscript \windows\system32\slmgr.vbs -skms <IPv6Address>:<port>
      ```

    - To assign a KMS host by using the NETBIOS name of the host, run the following command:

      Windows Command Prompt

      ```
      cscript \windows\system32\slmgr.vbs -skms <NETBIOSName>:<port>
      ```

    - To revert to automatic discovery on a KMS client, run the following command:

      Windows Command Prompt

      ```
      cscript \windows\system32\slmgr.vbs -ckms
      ```

> **Note**
>
> These commands use the following placeholders:
>
> - **<KMS_FQDN>** represents the fully qualified domain name (FQDN) of the KMS host computer
> - **<IPv4Address>** represents the IP version 4 address of the KMS host computer
> - **<IPv6Address>** represents the IP version 6 address of the KMS host computer
> - **<NETBIOSName>** represents the NETBIOS name of the KMS host computer
> - **<port>** represents the TCP port that KMS uses.

Configure the KMS host to publish in multiple DNS domains

> **Important**
>
> Follow the steps in this section carefully. Serious problems might occur if you modify the registry incorrectly. Before you modify it, **back up the registry for restoration** in case problems occur.

As described in Manually assign a KMS host to a KMS client, KMS clients typically use the automatic discovery process to identify KMS hosts. This process requires that the `_vlmcs` SRV records must be available in the DNS zone of the KMS client computer. The DNS zone corresponds to either the primary DNS suffix of the computer or to one of the following:

- For domain-joined computers, the computer's domain as assigned by the DNS system (such as Active Directory Domain Services (AD DS) DNS).
- For workgroup computers, the computer's domain as assigned by the Dynamic Host Configuration Protocol (DHCP). This domain name is defined by the option that has the code value of 15 as defined in Request for Comments (RFC) 2132.

By default, a KMS host registers its SRV records in the DNS zone that corresponds to the domain of the KMS host computer. For example, assume that a KMS host joins the contoso.com domain. In this scenario, the KMS host registers its `_vlmcs` SRV record

under the contoso.com DNS zone. Therefore, the record identifies the service as `_VLMCS._TCP.CONTOSO.COM`.

If the KMS host and KMS clients use different DNS zones, you must configure the KMS host to automatically publish its SRV records in multiple DNS domains. To do this, follow these steps:

1. On the KMS host, start Registry Editor.
2. Locate and then select the **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform** subkey (previously **SL** instead of **SoftwareProtectionPlatform** in Windows Server 2008 and Windows Vista).
3. In the **Details** pane, right-click a blank area, select **New**, and then select **Multi-String Value**.
4. For the name of the new entry, enter **DnsDomainPublishList**.
5. Right-click the new **DnsDomainPublishList** entry, and then select **Modify**.
6. In the **Edit Multi-String** dialog box, type each DNS domain suffix that KMS publishes on a separate line, and then select **OK**.

   > ⓘ **Note**
   >
   > For Windows Server 2008 R2, the format for **DnsDomainPublishList** differs. For more information, see the Volume Activation Technical Reference Guide.

7. Use the Services administrative tool to restart the Software Protection service (previously the Software Licensing service in Windows Server 2008 and Windows Vista). This operation creates the SRV records.
8. Verify that by using a typical method, the KMS client can contact the KMS host that you configured. Verify that the KMS client correctly identifies the KMS host both by name and by IP address. If either of these verifications fails, investigate this DNS client resolver issue.
9. To clear any previously cached KMS host names on the KMS client, open an elevated Command Prompt window on the KMS client, and then run the following command:

   Windows Command Prompt

   ```
   cscript C:\Windows\System32\slmgr.vbs -ckms
   ```

Rebuild the Tokens.dat file

Article • 05/19/2022

When you troubleshoot Windows activation issues, you may have to rebuild the Tokens.dat file. This article describes in detail how to do this.

Resolution

To rebuild the Tokens.dat file, follow these steps:

1. Open an elevated Command Prompt window: **For Windows 10**
   a. Open the **Start** menu, and enter **cmd**.
   b. In the search results, right-click **Command Prompt**, and the select **Run as administrator**.

   For Windows 8.1
   a. Swipe in from the right edge of the screen, and then tap **Search**. Or, if you are using a mouse, point to the lower-right corner of the screen, and then select **Search**.
   b. In the search box, enter **cmd**.
   c. Swipe across or right-click the displayed **Command Prompt** icon.
   d. Tap or click **Run as administrator**.

   For Windows 7
   a. Open the **Start** menu, and enter **cmd**.
   b. In the search results, right-click **cmd.exe**, and the select **Run as administrator**.

2. Enter the list of commands that is appropriate for your operating system.

   For Windows 10, Windows Server 2016 and later versions of Windows, enter the following commands in sequence:

   Windows Command Prompt

   ```
   net stop sppsvc
   cd %Systemdrive%\Windows\System32\spp\store\2.0\
   ren tokens.dat tokens.bar
   net start sppsvc
   cscript.exe %windir%\system32\slmgr.vbs /rilc
   ```

   For Windows 8.1, Windows Server 2012 and Windows Server 2012 R2, enter the following commands in sequence:

Windows Command Prompt

```
net stop sppsvc
cd %Systemdrive%\Windows\System32\spp\store\
ren tokens.dat tokens.bar
net start sppsvc
cscript.exe %windir%\system32\slmgr.vbs /rilc
```

For Windows 7, Windows Server 2008 and Windows Server 2008 R2, enter the following commands in sequence:

Windows Command Prompt

```
net stop sppsvc
cd
%Systemdrive%\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Mi
crosoft\SoftwareProtectionPlatform
ren tokens.dat tokens.bar
net start sppsvc
cscript.exe %windir%\system32\slmgr.vbs /rilc
```

3. Restart the computer.

More information

After you rebuild the Tokens.dat file, you must reinstall your product key by using one of the following methods:

- At the same elevated prompt command, type the following command, and then press Enter:

  Windows Command Prompt

  ```
  cscript.exe %windir%\system32\slmgr.vbs /ipk <Product key>
  ```

  > **ⓘ Important**
  >
  > Do not use the **/upk** switch to uninstall a product key. To install a product key over an existing product key, use the **/ipk** switch.

- Right-click **My Computer**, select **Properties**, and then select **Change product key**.

For more information about KMS client setup keys, see KMS client setup keys.

Example: Troubleshooting Active Directory Based Activation (ADBA) clients that do not activate

Article • 05/19/2022

> **Note**
>
> This article was originally published as a TechNet blog on March 26, 2018.

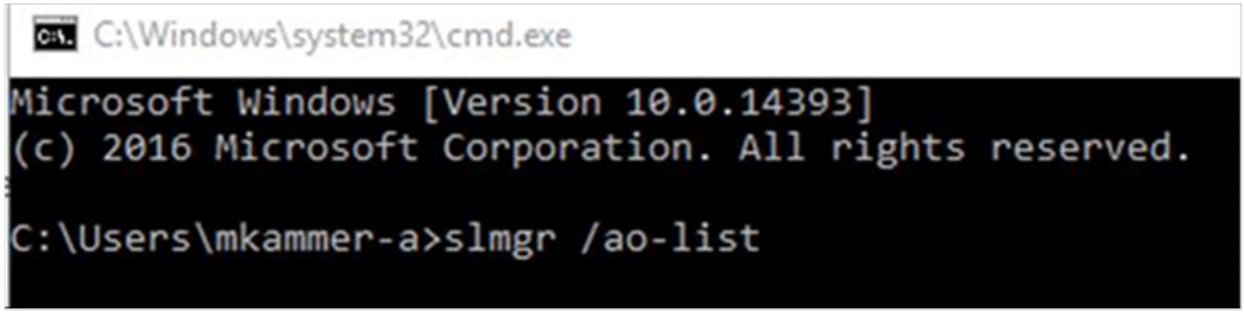
Hello everyone! My name is Mike Kammer, and I have been a Platforms PFE with Microsoft for just over two years now. I recently helped a customer with deploying Windows Server 2016 in their environment. We took this opportunity to also migrate their activation methodology from a KMS Server to Active Directory Based Activation.

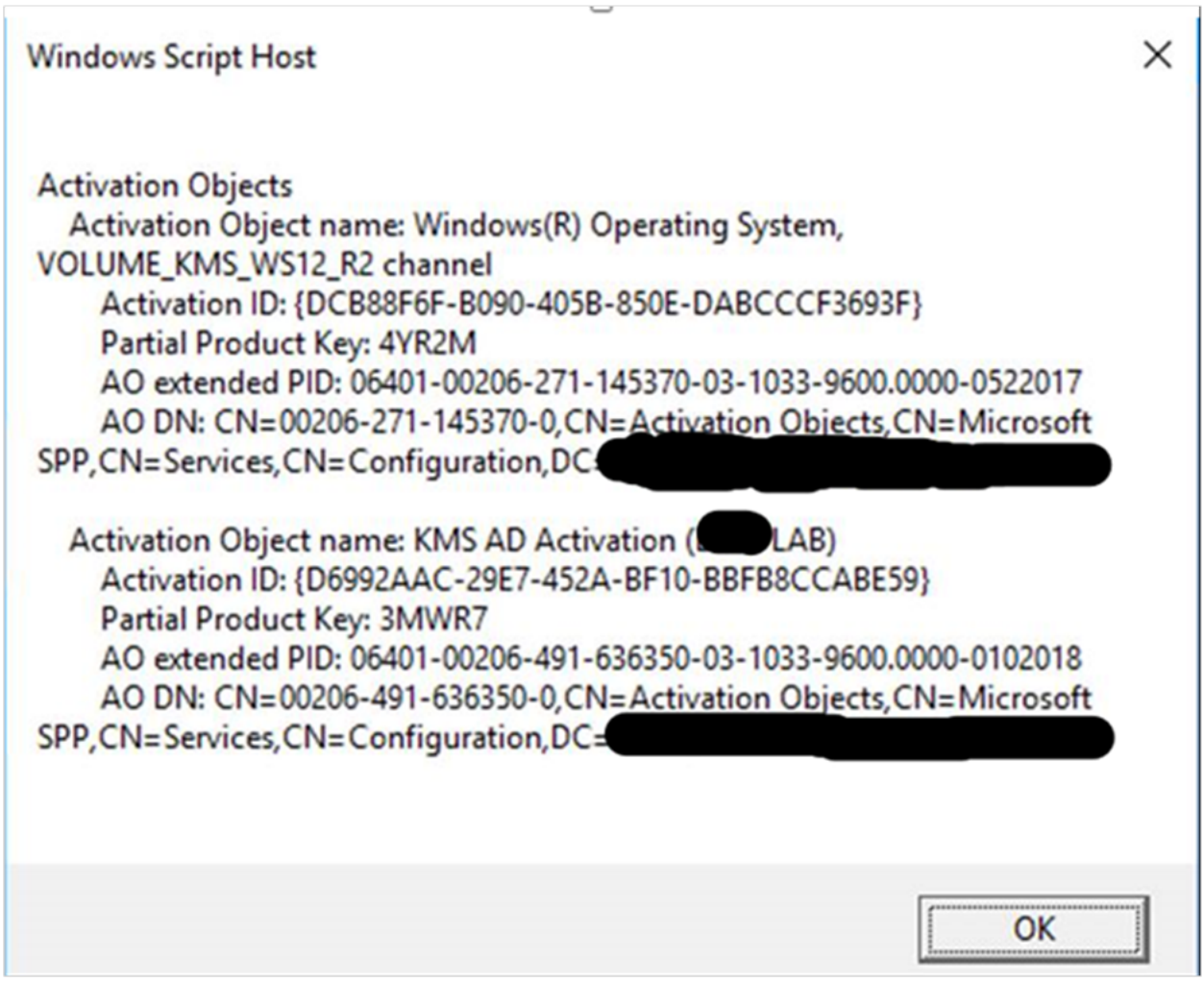
As proper procedure for making all changes, we started our migration in the customer's test environment. We began our deployment by following the instructions in this excellent blog post by Charity Shelbourne, Active Directory-Based Activation vs. Key Management Services. The domain controllers in our test environment were all running Windows Server 2012 R2, so we did not need to prep our forest. We installed the role on a Windows Server 2012 R2 Domain Controller and chose Active Directory Based Activation as our volume activation method. We installed our KMS key and gave it a name of "KMS AD Activation (** LAB)". We pretty much followed the blog post step by step.

We started by building four virtual machines, two Windows 2016 Standard and two Windows 2016 Datacenter. At this point everything was great, and everyone was happy. We built a physical server running Windows 2016 Standard, and the machine activated properly. And that's where our story ends.

Haha! Just kidding! Nothing is ever that easy. Truthfully, the set up and configuration were super easy, so that part was simple and straight forward. I came back into the office on Monday, and all the virtual machines I had built the week prior showed that they weren't activated. Hey! That's not right! I went back to the physical machine and it was fine. I went to the customer to discuss what had happened. Of course, the first question was "What changed over the weekend?" And as usual the answer was "nothing." This time, nothing really had been changed, and we had to figure out what was going on.

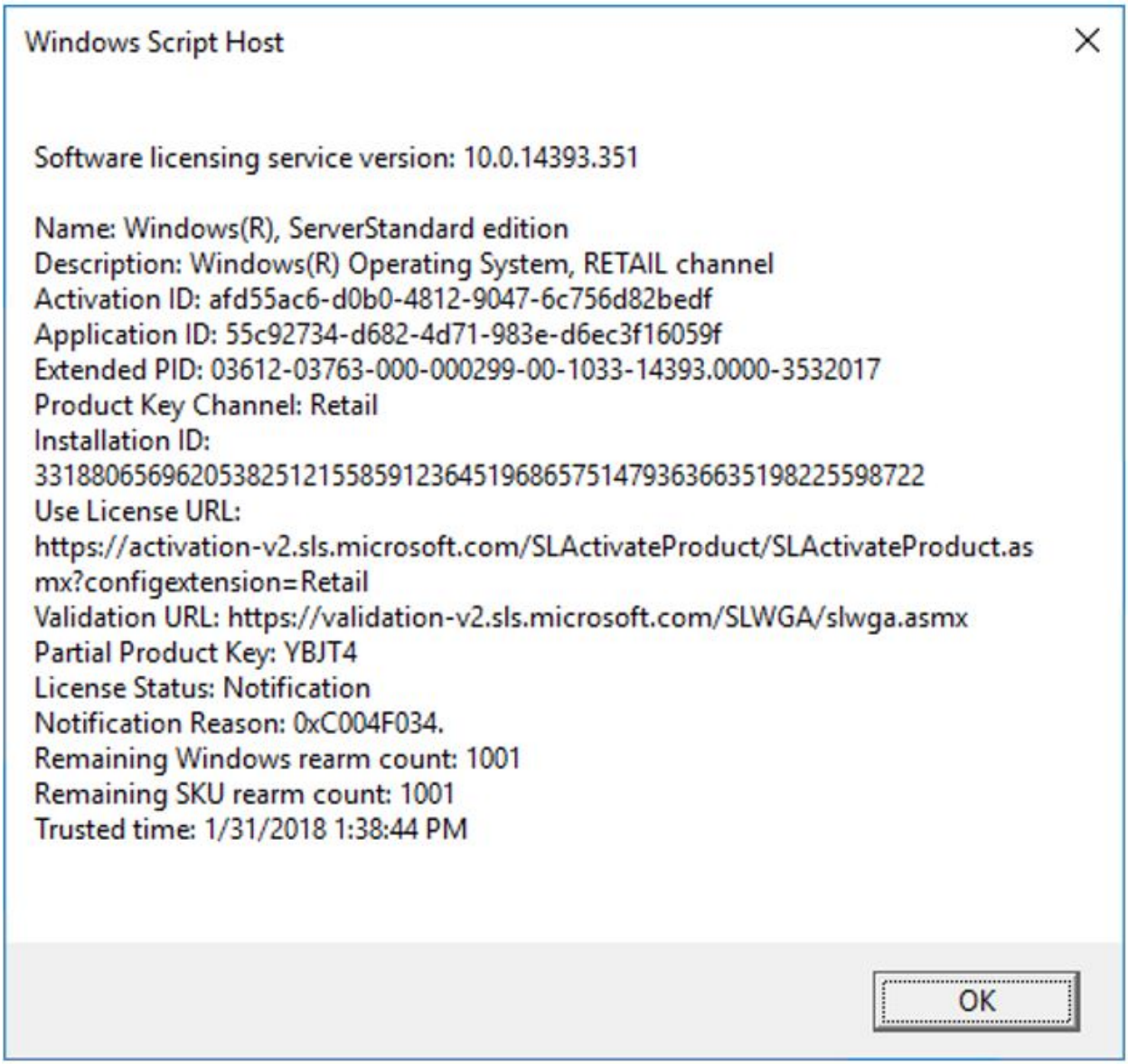
I went to one of my problem servers, opened a command prompt, and checked my output from the **slmgr /ao-list** command. The **/ao-list** switch displays all activation objects in Active Directory.





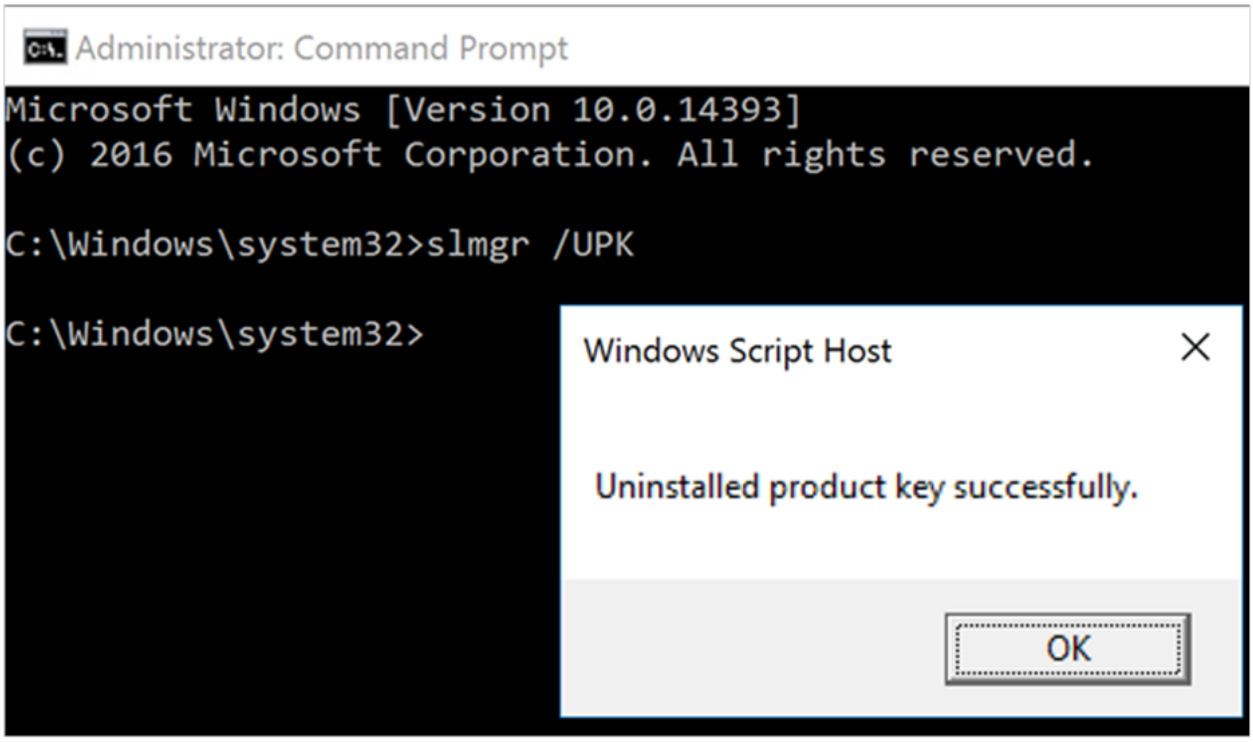
The results show that we have two Activation Objects: one for Server 2012 R2, and our newly created KMS AD Activation (** LAB) which is our Windows Server 2016 license. This confirms our Active Directory is correctly configured to activate Windows KMS Clients

Knowing that the **slmgr** command is my friend for license activation, I continued with different options. I tried the **/dlv** switch, which will display detailed license information. This looked fine to me, I was running the Standard version of Windows Server 2016, there's an Activation ID, an Installation ID, a validation URL, even a partial Product Key.

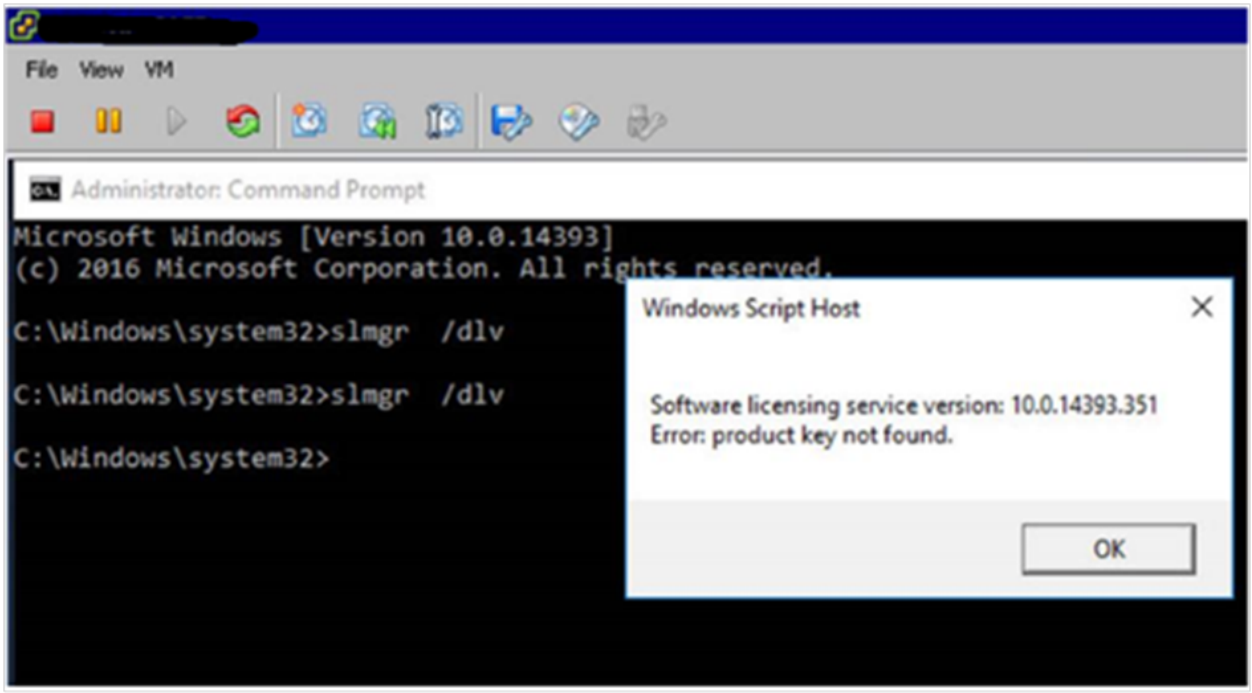


Does anyone see what I missed at this point? We'll come back to it after my other troubleshooting steps but suffice it to say the answer is in this screenshot.

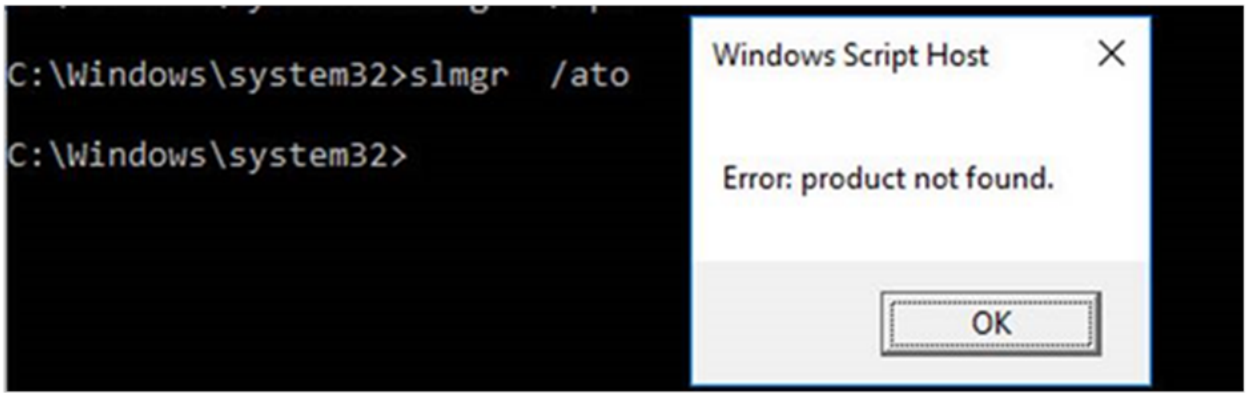
My thinking now is that for some reason the key is broken, so I use the **/upk** switch, which uninstalls the current key. While this was effective in removing the key, it is generally not the best way to do it. Should the server get rebooted before getting a new key it may leave the server in a bad state. I found that using the **/ipk** switch (which I do later in my troubleshooting) overwrites the existing key and is a much safer route to take. Learn from my missteps!



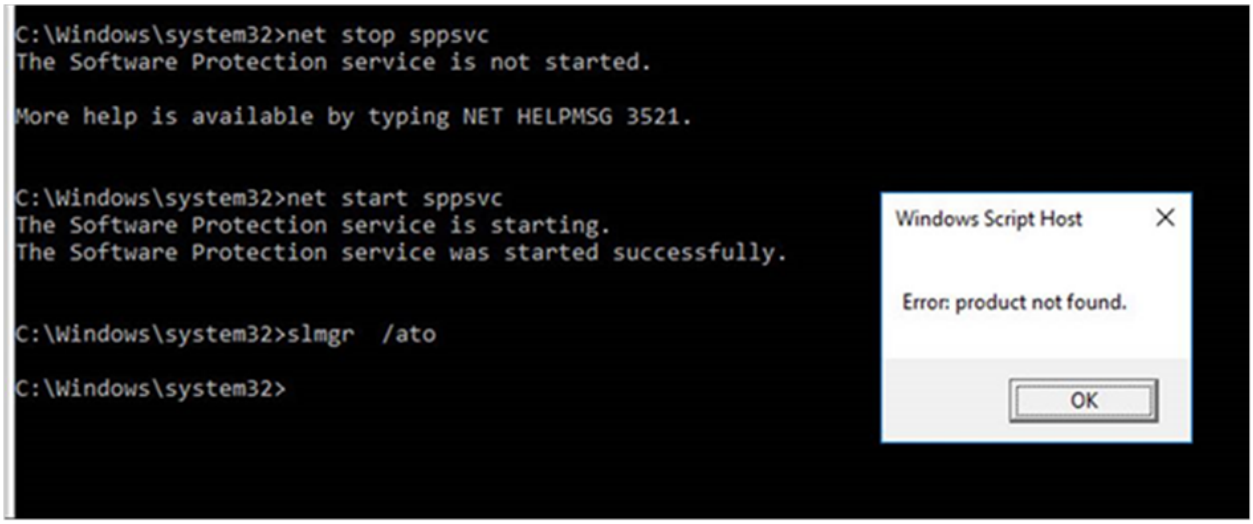
I ran the **/dlv** switch again, to see the detailed license information. Unfortunately for me that didn't give me any helpful information, just a product key not found error. Because, of course, there's no key since I just uninstalled it!



I figured it was a long shot, but I tried the **/ato** switch, which should activate Windows against the known KMS servers (or Active Directory as the case may be). Again, just a product not found error.

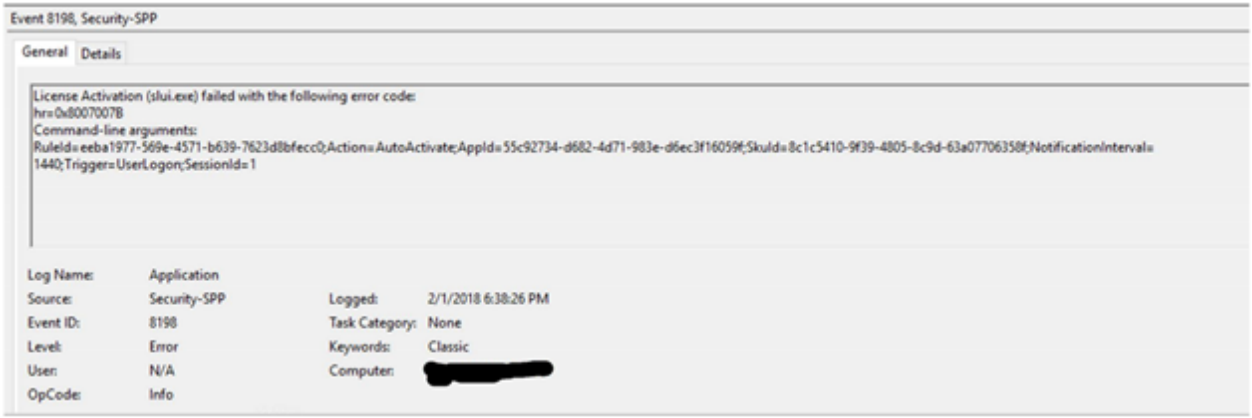


My next thought was that sometimes stopping and starting a service does the trick, so I tried that next. I need to stop and start the Microsoft Software Protection Platform Service (SPPSvc service). From an administrative command prompt, I use the trusty **net stop** and **net start** commands. I notice at first that the service isn't running, so I think this must be it!



But no. After starting the service and attempting to activate Windows again, I still get the product not found error.

I then looked at the Application Event Log on one of the trouble servers. I find an error related to License Activation, Event ID 8198, that has a code of 0x8007007B.



While looking up this code, I found an article that says my error code means that the file name, directory name, or volume label syntax is incorrect. Reading through the methods described in the article, it didn't seem that any of them fit my situation. When I ran the **nslookup -type=all _vlmcs._tcp** command, I found the existing KMS server (still lots of Windows 7 and Server 2008 machines in the environment, so it was necessary to keep it around), but also the five domain controllers as well. This indicated that it was not a DNS problem and my issues were elsewhere.

```
nslookup -type=all _vlmcs._tcp>kms.txt

Server:  labdns1.CONTOSO.COM
Address:  10.10.14.11

_vlmcs._tcp.CONTOSO.COM    SRV service location:
          priority       = 0
          weight         = 0
          port           = 1688
          svr hostname   = labKMS.CONTOSO.COM

_tcp.CONTOSO.COM   nameserver = labDC2.CONTOSO.COM
_tcp.CONTOSO.COM   nameserver = remDC1.CONTOSO.COM
_tcp.CONTOSO.COM   nameserver = labDC4.CONTOSO.COM
_tcp.CONTOSO.COM   nameserver = labDC1.CONTOSO.COM
_tcp.CONTOSO.COM   nameserver = labDC3.CONTOSO.COM
labKMS.CONTOSO.COM  internet address = 10.10.14.100
labDC1.CONTOSO.COM   internet address = 10.10.14.26
remDC1.CONTOSO.COM   internet address = 10.10.20.88
labDC4.CONTOSO.COM   internet address = 10.10.14.27
labDC3.CONTOSO.COM   internet address = 10.10.14.34
labDC2.CONTOSO.COM   internet address = 10.10.14.44
```

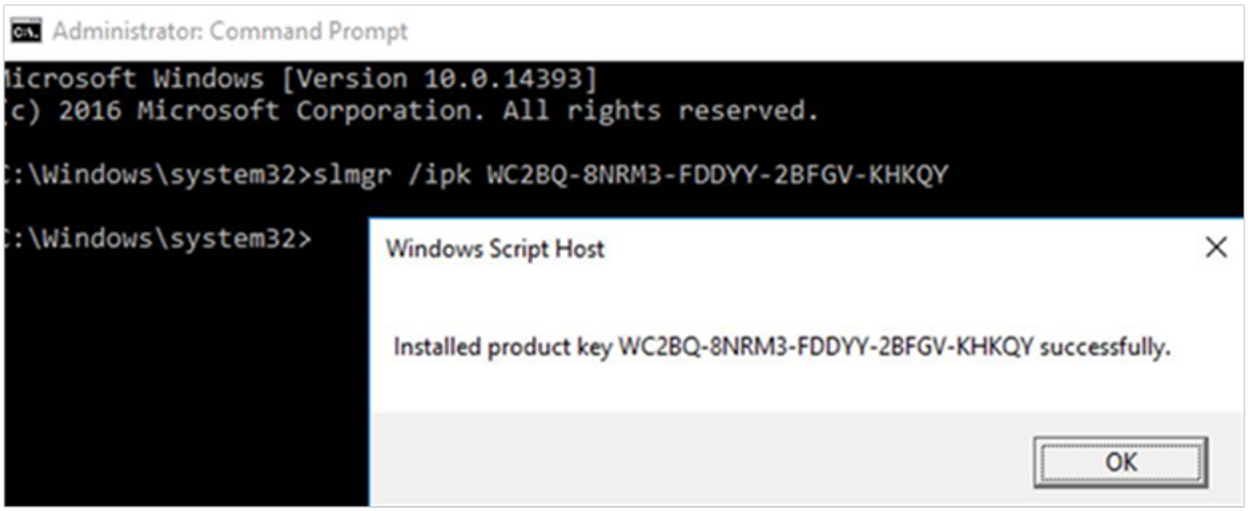
So I know DNS is fine. Active Directory is properly configured as a KMS activation source. My physical server has been activated properly. Could this be an issue with just VMs? As an interesting side note at this point, my customer informs me that someone in a different department has decided to build more than a dozen virtual Windows Server 2016 machines as well. So now I assume I've got another dozen servers to deal with that won't be activating. But no! Those servers activated just fine.

Well, I headed back to my **slmgr** command to figure out how to get these monsters activated. This time I'm going to use the **/ipk** switch, which will allow me to install a product key. I went to this site to get the appropriate keys for my Standard version of Windows Server 2016. Some of my servers are Datacenter, but I need to fix this one first.

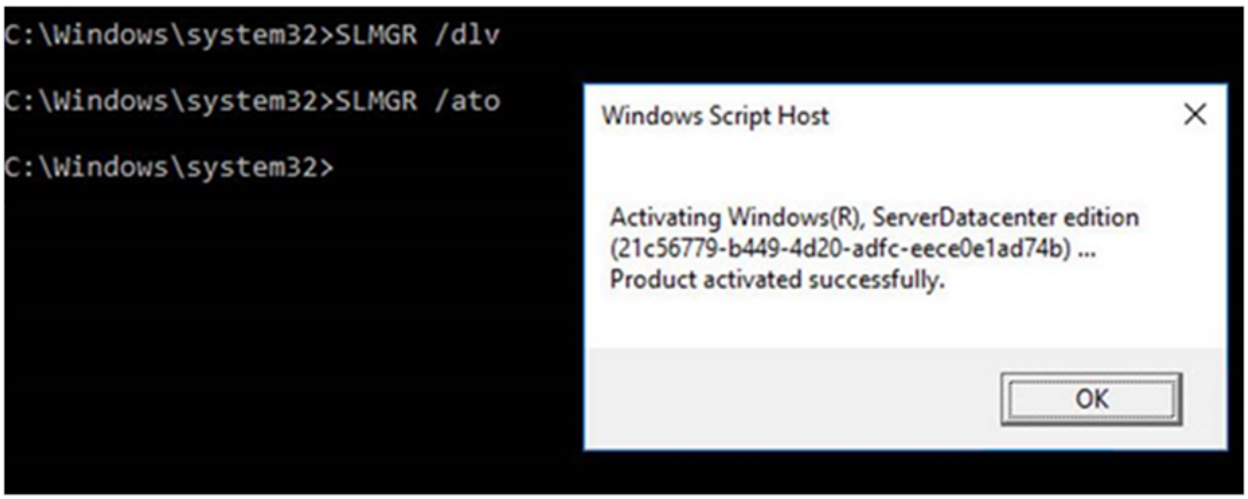
Windows Server 2016

Operating system edition	KMS Client Setup Key
Windows Server 2016 Datacenter	CB7KF-BWN84-R7R2Y-793K2-8XDDG
Windows Server 2016 Standard	WC2BQ-8NRM3-FDDYY-2BFGV-KHKQY
Windows Server 2016 Essentials	JCKRF-N37P4-C2D82-9YXRT-4M63B

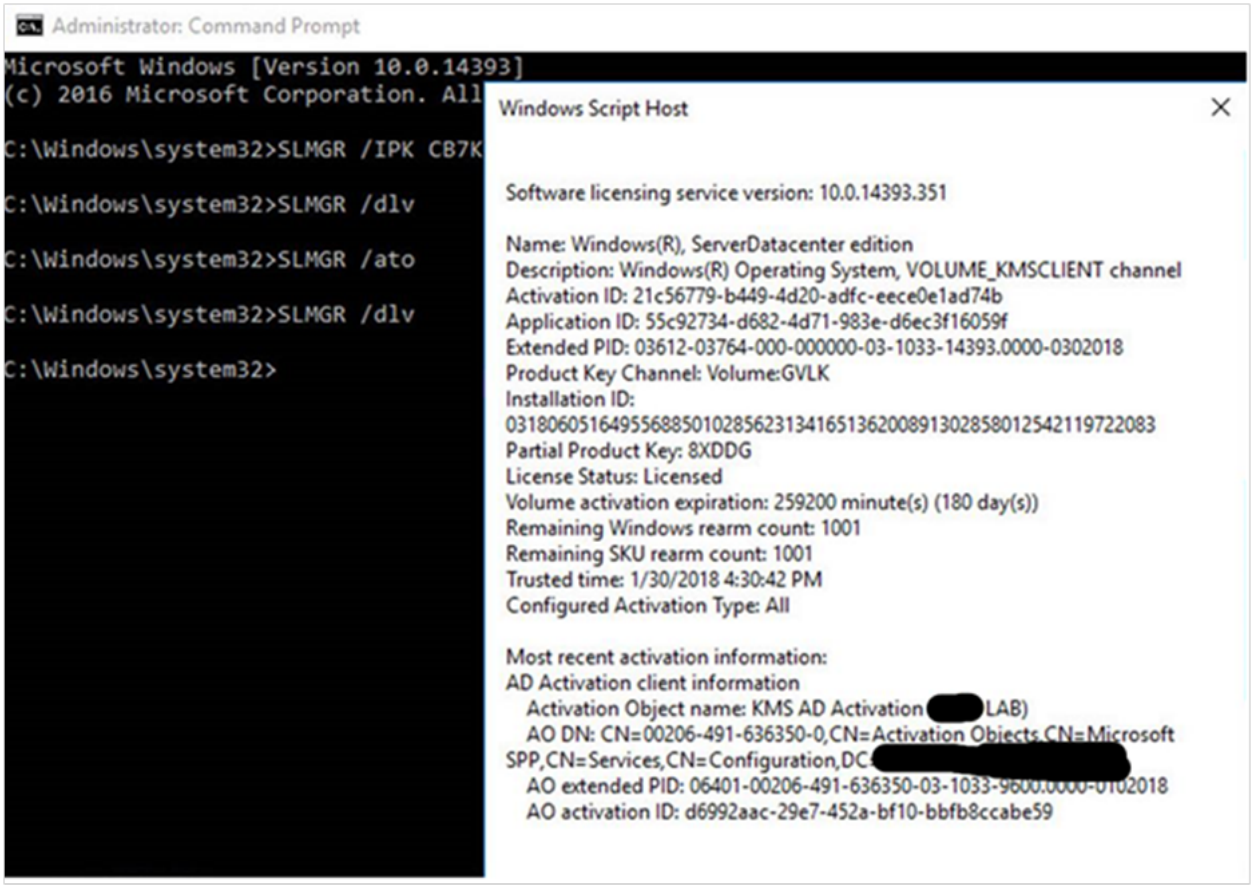
I used the **/ipk** switch to install a product key, choosing the Windows Server 2016 Standard key.



From here on out I only captured results from my Datacenter experiences, but they were the same. I used the **/ato** switch to force the activation. We get the awesome message that the product has been activated successfully!

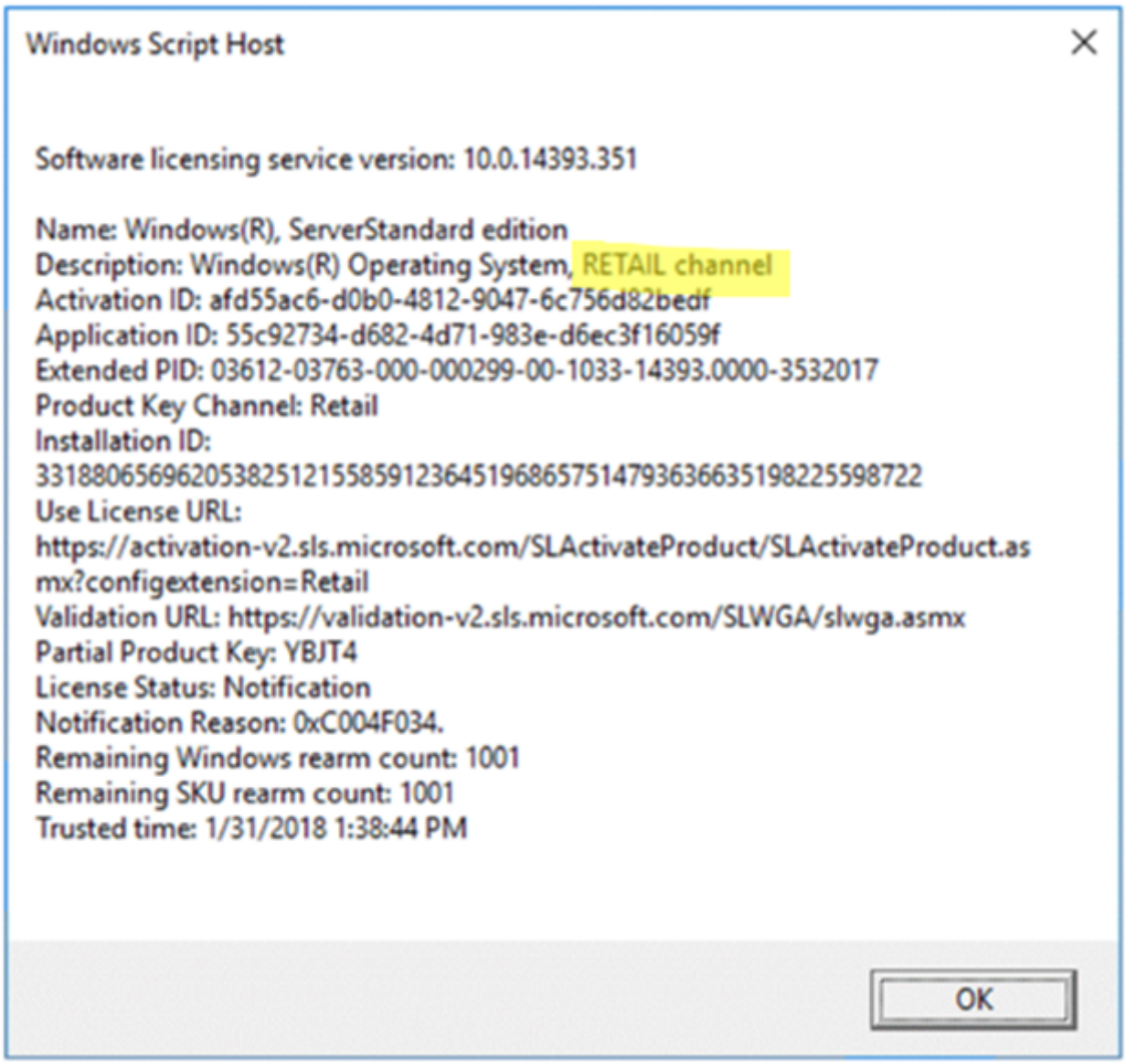


Using the **/dlv** switch again, we can see that now we have been activated by Active Directory.

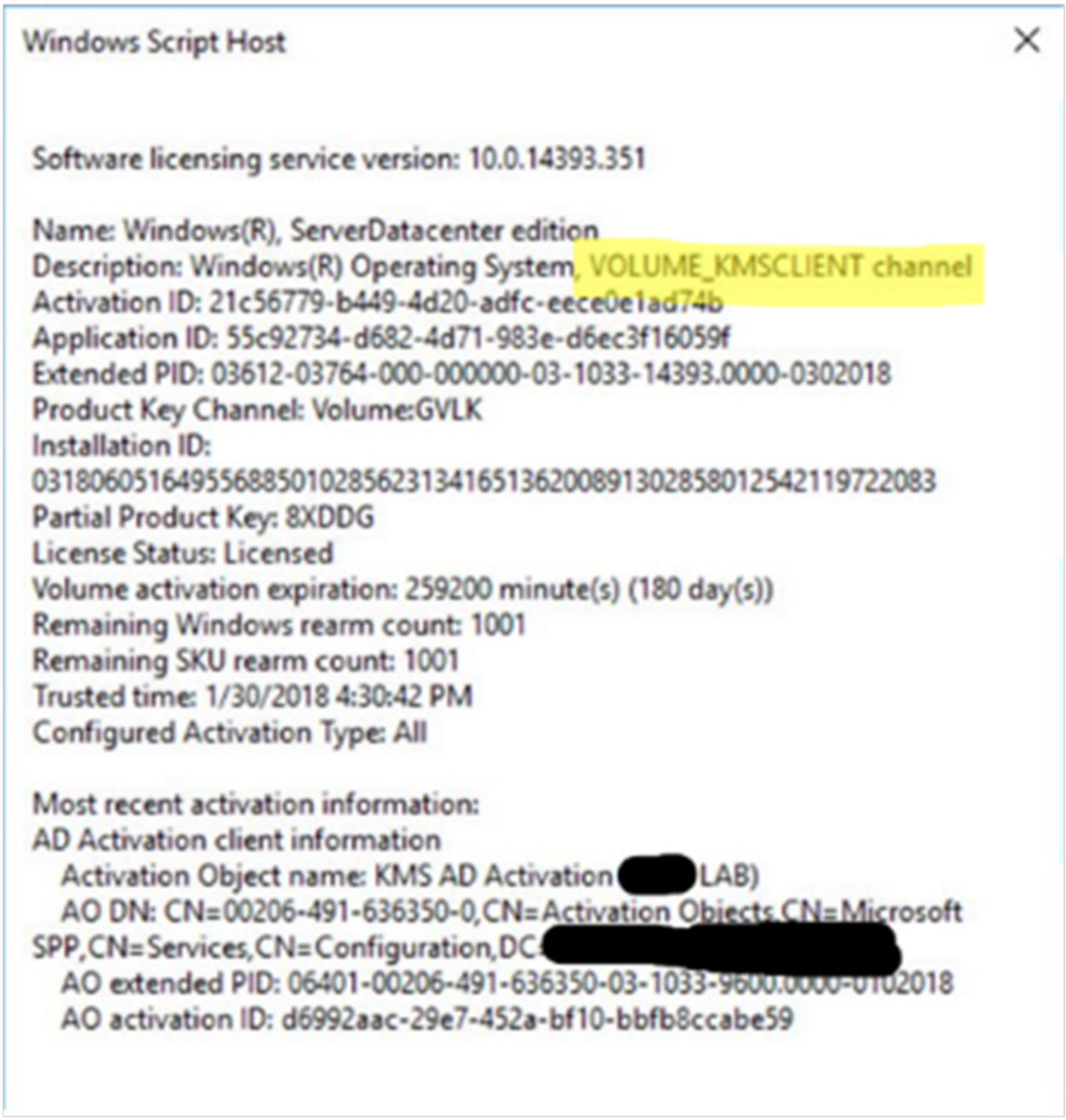


Now, what had gone wrong? Why did I have to remove the installed key and add those generic keys to get these machines to activate properly? Why did the other dozen or so machines activate with no issues? As I said earlier, I missed something key in the initial stages of looking at the issue. I was thoroughly confused, so reached out to Charity from the initial blog post to see if she could help me. She saw the problem right away and helped me understand what I had missed early on.

When I ran the first **/dlv** switch, in the description was the key. The description was Windows® Operating System, RETAIL Channel. I had looked at that and thought that RETAIL Channel meant that it had been purchased and was a valid key.



When we look at the output of the **/dlv** switch from a properly activated server, notice the description now states VOLUME_KMSCLIENT channel. This lets us know that it is indeed a volume license.



So what does that RETAIL channel mean then? Well, it means the media that was used to install the operating system was an MSDN ISO. I went back to my customer and asked if, by some chance, there was a second Windows Server 2016 ISO floating around the network. Turns out that yes, there was another ISO on the network, and it had been used to create the other dozen machines. They compared the two ISOs and sure enough the one that was given to me to build the virtual servers was, in fact, an MSDN ISO. They removed that MSDN ISO from their network and now we have all our existing servers activated and no more worries about the activation failing on future builds.

I hope this has been helpful and may save you some time going forward!

Mike

Windows release health

Official information on Windows releases and servicing milestones, plus resources, tools, and news about known issues and safeguards to help you plan your next update. Want the latest Windows release health updates? Follow @WindowsUpdate on X (formerly known as Twitter).

GET STARTED
How to get the Windows 11 2023 Update

WHAT'S NEW
Explore the most personal Windows 11...

WHAT'S NEW
How to get the latest Windows 11 innovations

REFERENCE
Get updates as soon as they're available for...

REFERENCE
Windows 11 release information

OVERVIEW
Understanding Windows monthly...

Message center

- Windows Server 2012/R2: Extended Security Updates
- Simplify your Windows 11 upgrade experience with Intune
- Windows 11 2023 Update available

See more >

Windows 11, version 23H2

- Known issues
- Resolved issues
- Windows 11 release information
- How to get Windows 11, version 23H2
- Tools for IT pros

Windows 11, version 22H2

- Known issues
- Resolved issues
- Release notes
- Windows 11 release information
- How to get Windows 11, version 22H2

Windows 11, version 21H2

- Known issues
- Resolved issues
- Release notes
- Windows 11 release information
- How to get Windows 11

Windows 10, version 22H2

- Known issues
- Resolved issues
- Release notes
- Windows 10 release information
- How to get Windows 10, version 22H2

Windows 10, version 21H2

- Known issues
- Resolved issues
- Release notes
- Windows 10 release information
- How to get Windows 10, version 21H2

Windows Server 2022

- Known issues
- Resolved issues
- Release notes
- Windows Server release information
- What's new in Windows Server 2022

Additional versions

See details on known and resolved issues for other supported versions of Windows and Windows Server.

- Known issues: earlier versions

Questions? Join office hours!

Get customized guidance, tips and tricks, and answers to your questions.

Submit feedback

Share your thoughts on existing features -- or ideas for new ones through the feedback Hub.

Get help

Find resources to help you troubleshoot common issues and get support from Microsoft.

Windows Server - License Terms

Article • 03/31/2022

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