Filter by title
Get started with Windows Server
Overview
What's new in Windows Server
Windows Server 2022
Windows Server versions 2004 and 20H2
Windows Server versions 1903 and 1909
Windows Server 2019
Windows Server 2016
Servicing channels comparison
Editions feature comparison
Hardware requirements
Features removed or no longer developed
Release information
Extended Security Updates
Upgrade Windows Server
Concepts
How-to guides
Troubleshooting
Resources



# What's new in Windows Server 2019

Article • 09/05/2022 • 9 minutes to read • 4 contributors

Feedback

This article describes some of the new features in Windows Server 2019. Windows Server 2019 is built on the 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 PCs. It comes at no additional cost beyond Windows and is ready to use in production.

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

For more info, see Windows Admin Center.

### Desktop experience

Because Windows Server 2019 is a Long Term Servicing Channel (LTSC) release, it includes the **Desktop Experience**. Semi-Annual Channel (SAC) releases don't include the Desktop Experience by design, they are optimized for cloud-native, containerized, and infrastructure workloads. Windows Server 2016, during setup of the operating system you can choose between Server Core installations or Server with Desktop Experience installations.

### System Insights

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

## Hybrid Cloud

### Server Core App Compatibility Feature on Demand

The Server Core App Compatibility Feature on Demand (FOD) significantly improves the app compatibility of the Windows Server Core installation option by including a subset of binaries and components from Windows Server with the Desktop Experience, without adding the Windows Server Desktop Experience graphical environment itself. The FOD aims to increase the functionality and compatibility of Server Core while keeping it as lean as possible.

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

## Security

### Windows Defender Advanced Threat Protection (ATP)

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

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

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

- Attack Surface Reduction(ASR) is set of controls that enterprises can enable to prevent malware from getting on the machine by blocking suspicious malicious files (for example, Office files), scripts, lateral movement, ransomware behavior, and email based threats.
- Network protection protects the endpoint against web based threats by blocking any outbound process on the device to untrusted hosts/IP addresses through Windows Defender SmartScreen.
- Controlled folder access* protects sensitive data from ransomware by blocking untrusted processes from accessing your protected folders.
- Exploit protection is a set of mitigations for vulnerability exploits leveraging EMET(that can be easily configured to your system and applications.
- Windows Defender Application Control (also known as Code Integrity Enforcement) introduced in Windows Server 2016. Customer feedback has suggested that it is a great concept, but hard to deploy. To address this, we have built default D1 policies, which allows all Windows in-box files and Microsoft applications, such as SQL Server, and block known executables that can bypass D1.

### 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.

  Offline mode allows you to continue to start up your shielded VMs, even if HGS can't be reached, as long as the VM has started successfully once, and the host's security configuration has not changed.

- **Troubleshooting improvements**

  We've also made it easier to troubleshoot your shielded virtual machines by enabling support for VMConnect Enhanced Session Mode and PowerShell Direct. These tools are particularly useful if you've lost network connectivity to your VM and need to update its configuration to restore access.

  These features do not need to be configured, and they become available automatically when a shielded VM is placed on a Hyper-V host running Windows Server version 1803 or later.

- **Linux support**

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

### HTTP/2 for a faster and safer Web

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

## Storage

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

### Storage Migration Service

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

### Storage Spaces Direct

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

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

### Storage Replica

Here's what's new in Storage Replica: For details, see What's new in Storage Replica.

- Storage Replica is now available in Windows Server 2019 Standard Edition.
- Test failover is a new feature that allows mounting of destination storage to validate replication in 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
- Cluster dashboard enhancements
- VM resiliency improvements
- Failover Cluster no longer uses NTLM authentication

## Application Platform

### Linux containers on Windows

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

### Built-in support for Kubernetes

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

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

### Container improvements

- **Improved integrated identity**

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

- **Better application compatibility**

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

- **Reduced size and higher performance**

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

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

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

### Encrypted Networks

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

### Network performance improvements for virtual workloads

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

- Dynamic Virtual Machine Multi-Queue (UVMMQ)
- 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, while consuming the entire bandwidth available when the network is not in use. This technology is intended for use in deploying large, critical customer services in an environment without impacting customer facing services and associated bandwidth.

### Windows Time Service

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

### High performance SDN gateways

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

### New Deployment UI and Windows Admin Center extension for SDN

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

### Persistent Memory support for Hyper-V VMs

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

## Recommended content

**What's new in Windows Server 2016**
Find out what is new in Windows Server 2016. Learn about Windows Server 2016 that are the ones most likely to have the greatest impact as you work with this release.

**Hardware requirements for Windows Server**
What are the minimum hardware requirements for storage, CPU, network, memory, RAM for Windows Server.

**What's new in Windows Server 2022**
Find out what is new in Windows Server 2022.

**Install, upgrade, or migrate to Windows Server**
How to clean install, or clean upgrade or migrate to Windows Server.

Show more

## Feedback

Submit and view feedback for

This product | This page

View all page feedback



In this article
General
Hybrid Cloud
Security
Storage
Show more