What's new in Windows Server 2022

Article • 07/10/2024

> 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.

In vSwitch, RSC can also coalesce multiple TCP segments into a larger segment before data traversing the vSwitch. This change also improves networking performance for virtual workloads. RSC is enabled on external virtual switches by default.

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

Windows Server 2022 includes the following Storage updates. Storage is also affected by the updates to System Insights disk anomaly detection and Windows Admin Center.

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.

Containers

Windows Server 2022 includes the following changes to Windows containers.

Server Core image size reduction

We've reduced the size of Server Core images. This smaller image size allows you to deploy containerized applications faster. In Windows Server 2022, the Server Core container image release to manufacturing (RTM) layer at the time of GA clocks in at 2.76 GB uncompressed on disk. Compared to the Windows Server 2019 RTM layer at the time of GA, which clocks in at 3.47 GB uncompressed on disk, that's a 33% reduction in on-disk footprint for that layer. While you shouldn't expect the total image size to be reduced by 33%, a smaller RTM layer size generally means the overall image size will be smaller.

> ⓘ Note
>
> Windows container base images ship as two layers: and RTM layer and a patch layer that contains the latest security fixes for OS libraries and binaries that's overlaid on the RTM layer. The patch layer's size changes over the life of the container image

support cycle depending on how many changes are in the binaries. When you pull a container base image onto a new host, you need to pull both layers.

Longer support cycle for all Windows container images

Windows Server 2022 images, including Server Core, Nano Server, and Server image, have five years of mainstream support and five years of extended support. This longer support cycle ensures you have time to implement, use, and upgrade or migrate when appropriate for your organization. For more information, see Windows containers base image lifecycles and Windows Server 2022 lifecycles.

Virtualized time zone

With Windows Server 2022, Windows containers can now maintain a virtualized time zone configuration separate from the host. All configurations the host time zone typically uses are now virtualized and instanced for each container. To configure the container time zone, you can use the tzutil command utility or the Set-TimeZone PowerShell cmdlet. To learn more, see Virtualized time zone.

Scalability improvements for overlay networking support

Windows Server 2022 aggregates several performance and scale improvements that were already in four earlier Semi-Annual Channel (SAC) releases of Windows Server that hadn't been backported into Windows Server 2019:

- Fixed the issue that caused port exhaustion when using hundreds of Kubernetes services and pods on the same node.
- Improved packet forwarding performance in the Hyper-V virtual switch (vSwitch).
- Increased reliability across Container Networking Interface (CNI) restarts in Kubernetes.
- Improvements in the Host Networking Service (HNS) control plane and in the data plane used by Windows Server containers and Kubernetes networking.

To learn more about the performance and scalability improvements for overlay networking support, see Kubernetes Overlay Networking for Windows.

Direct Server Return routing for overlay and l2bridge networks

Direct Server Return (DSR) is an asymmetric network load distribution in load balanced systems that makes request and response traffic use different network paths. Using different network paths helps avoid extra hops and reduces latency, speeding up response time between the client and service and removing extra load from the load balancer. DSR transparently achieves increased network performance for applications with little to no infrastructure changes.

To learn more, see DSR in Introduction to Windows support in Kubernetes .

gMSA improvements

You can use Group Managed Service Accounts (gMSA) with Windows containers to facilitate Active Directory (AD) authentication. When introduced in Windows Server 2019, gMSA required joining the container host to a domain to retrieve the gMSA credentials from Active Directory. In Windows Server 2022, gMSA for containers with a non-domain joined host uses a portable user identity instead of a host identity to retrieve gMSA credentials. Therefore, manually joining Windows worker nodes to a domain is no longer necessary. After authentication, Kubernetes saves the user identity as a secret. gMSA for containers with a non-domain joined host provides the flexibility of creating containers with gMSA without joining the host node to the domain.

To learn more about the gMSA improvements, see Create gMSAs for Windows containers.

IPv6 support

Kubernetes in Windows now supports the IPv6 dual stack in L2bridge-based networks in Windows Server. IPv6 is dependent on the CNI that Kubernetes uses, and also requires Kubernetes version 1.20 or later to enable end-to-end IPv6 support. For more information, see IPv4/IPv6 in Introduction to Windows support in Kubernetes .

Multi-subnet support for Windows worker nodes with Calico for Windows

The Host Network Service (HNS) now allows you to use more restrictive subnets, such as subnets with a longer prefix length, and also multiple subnets for each Windows worker node. Previously, HNS restricted Kubernetes container endpoint configurations to only use the prefix length of the underlying subnet. The first CNI that makes use of this functionality is Calico for Windows . For more information, see Multiple subnet support in Host Networking Service.

HostProcess containers for node management

HostProcess containers are a new container type that runs directly on the host and extends the Windows container model to enable a wider range of Kubernetes cluster management scenarios. With HostProcess containers, users can package and distribute management operations that require host access while retaining versioning and deployment methods provided by containers. You can use Windows containers for a variety of device plug-in, storage, and networking management scenarios in Kubernetes.

HostProcess containers have the following benefits:

- Cluster users no longer need to sign in and individually configure each Windows node for administrative tasks and management of Windows services.
- Users can utilize the container model to deploy management logic to as many clusters as needed.
- Users can build HostProcess containers on top of existing Windows Server 2019 or later base images, manage them using Windows container runtime, and run as any user available in the domain of the host machine.
- HostProcess containers provide the best way to manage Windows nodes in Kubernetes.

For more information, see Windows HostProcess Containers .

Windows Admin Center improvements

Windows Server 2022 expands on the Containers extension added to Windows Admin Center to containerize existing web applications based on ASP.NET from .NET Framework. You can use static folders or Visual Studio solutions from your developer.

Windows Admin Center includes the following enhancements:

- The Containers extension now supports Web Deploy files, which lets you extract the app and its configuration from a running server and then containerize the application.
- You can validate the image locally and then push that image to Azure Container Registry.
- Azure Container Registry and Azure Container Instance now have basic management functionality. You can now use the Windows Admin Center UI to create and delete registries, manage images, and start and stop new container instances.

Azure Migrate App Containerization tooling

Azure Migrate App Containerization is an end-to-end solution that containerizes and moves existing web applications to the Azure Kubernetes Service. You can assess existing web servers, create a container image, push the image to the Azure Container Registry, create a Kubernetes deployment, and finally deploy it to the Azure Kubernetes Service.

For more information about the Azure Migrate App Containerization tool, see ASP.NET app containerization and migration to Azure Kubernetes Service and Java web app containerization and migration to Azure Kubernetes Service.

Feedback

Was this page helpful? 👍 Yes 👎 No