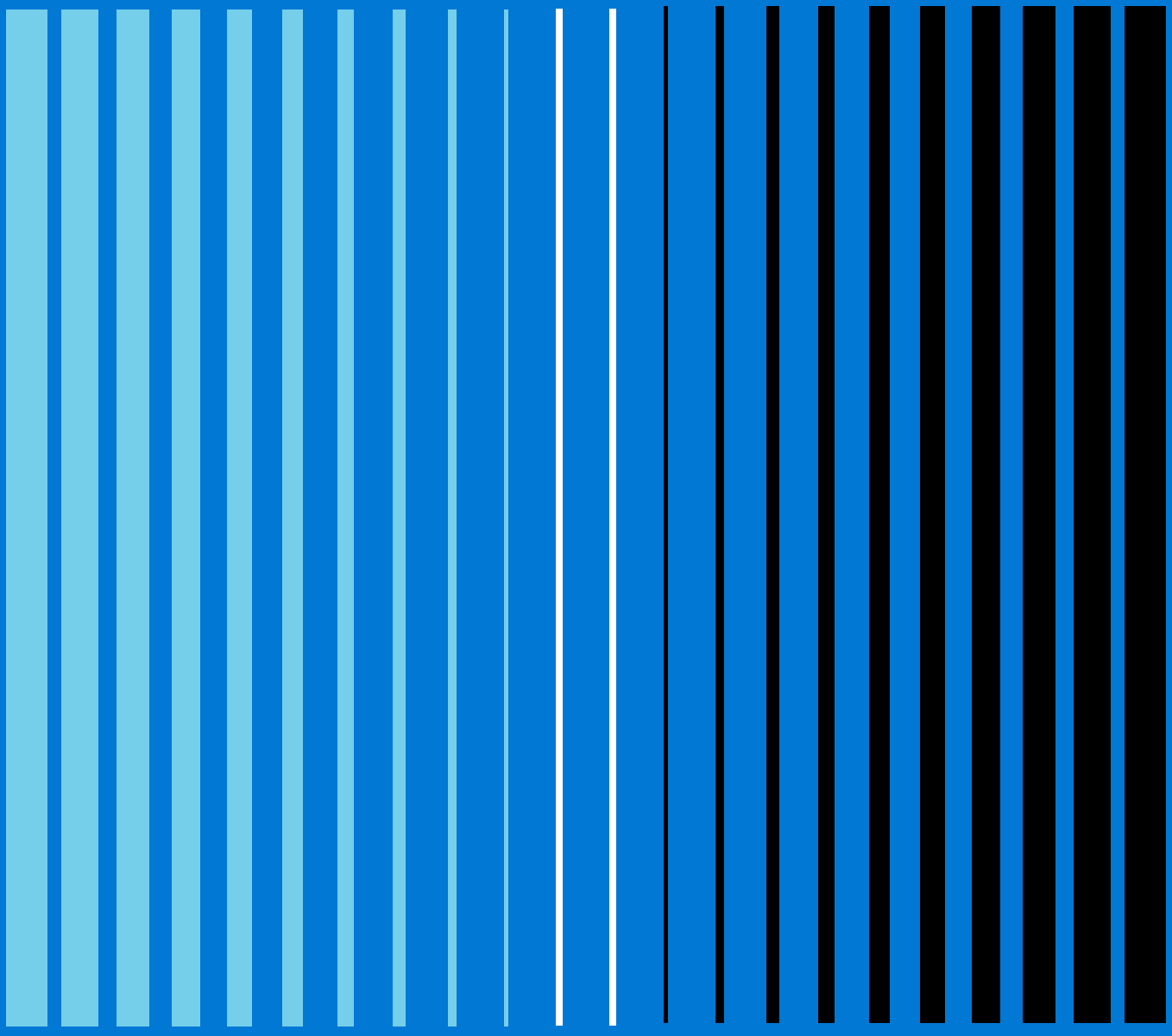
The Ultimate Guide to Windows Server 2022

Microsoft



Windows Server 2022 for today's business challenges

Technical advances and innovation. Escalating customer expectations. Attacks that exploit previously unknown security vulnerabilities. Competitive pressures. Earth-shaking world events.

These are some of the factors that make the world of information technology an exciting, challenging place to work. For more than 20 years, Windows Server has been right there, a server accessible to all organizations, from small businesses to the largest enterprise and government datacenters. As a result, organizations benefited: They gained continuous improvement in security and a robust application platform, systems architecture, and system administration tools. As cloud services grew in importance, Windows Server was there too, providing hybrid capabilities that brought together datacenter investments and new cloud innovations.

Today, Windows Server 2022 continues this tradition with best-in-class security, an end-to-end hybrid infrastructure, and an application platform that allows you to run existing and new applications with confidence on Azure, on-premises, or on the edge.

Read this guide to learn more about how the Windows Server 2022 operating system helps you deliver three critical business capabilities.

1. Advanced multi-layered security
   Elevate the security posture of your organization starting with the operating system.
2. Hybrid capabilities with Azure
   Extend your datacenter to Azure for greater IT efficiency.
3. Flexible application platform
   Empower developers and IT pros with an application platform designed to build and deploy diverse applications.

Windows Server and Azure — A complete solution

Windows Server 2022 builds on the success of Windows Server 2019, which delivered tools and technologies to bridge the gap between the datacenter and the cloud. Windows Server 2022 delivers an end-to-end hybrid infrastructure and application platform, along with multi-layered security features that protect apps, data, and IT workloads across Azure and the datacenter.

A Secured-core certification program with hardware suppliers provides unprecedented protection from malware targeting firmware and device drivers. Secure connections are at the heart of today's interconnected systems, and new capabilities such as DNS-over-HTTPS and SMB encryption further safeguard network traffic. New management tools like Azure Arc and enhancements to Windows Admin Center increase the efficiency and agility of hybrid computing. Windows containers have also been significantly improved, with greatly reduced image size and faster startup times, along with tools to quickly containerize .NET applications.

Whether you run Windows Server instances on physical servers, virtual machines, on-premises, or in Azure, Microsoft's end-to-end hybrid infrastructure helps manage your servers and services. Azure Arc (discussed in detail later in this guide) extends Azure management and security to Windows Server instances anywhere. Windows Admin Center provides a full suite of tools for managing backup, site recovery, monitoring, and more. Microsoft Entra ID provides consistent and secure identity on-premises and in the cloud.

Read this guide for an overview across all these capabilities. When you're ready for next steps, we'll explain how to quickly start a no-cost evaluation of Windows Server 2022, Azure Arc, and Windows Admin Center. You can also find more in-depth information and resources, including for migration and upgrade efforts.

1 Security

Organizations around the world are embracing digital transformation using technologies across datacenter, cloud, and edge computing to thrive in fast-paced environments. The trend toward remote work continues to push the transformation. Meanwhile, cybercriminals and other bad actors are also innovating, moving to new targets, including the seams between hardware and software that are difficult to monitor for breaches.

Stolen credentials compromise customer data. Servers may be hit with ransomware attacks. To build a strong security strategy, organizations need to track emerging risks and keep up with the latest technologies. They need to understand complex security and privacy regulations that vary from place to place.

Cybersecurity always comes down to people — good and bad. Many companies lack expertise and familiarity with security standards. And even the most security-conscious employees can be susceptible to clever social engineering that tricks users and introduces malware into an organization's networked computers.

Firmware attacks outpace investments targeted at stopping them

83%
Of enterprises have experienced at least one firmware attack in the past two years.

Source: Microsoft-commissioned research by Hypothesis Group, Security Signals, 2021

5x
Increase in attacks against firmware in the last four years.

Source: National Institute of Standards and Technology's (NIST) National Vulnerability Database (NVD)

21%
Of enterprise security decision makers surveyed admit that their firmware data goes unmonitored today.

Source: Microsoft-commissioned research by Hypothesis Group, Security Signals, 2021 and Microsoft Security Team

Advanced multi-layered security for Windows Server

Microsoft builds advanced multi-layered security into Windows Server. Security starts at the hardware level, protects access and credentials, and continues to deepen as you add cloud services that safeguard data and manage risk across your operation. The following figure showcases five pivotal areas that deliver on Microsoft's commitment for advanced multi-layered security.

Critical layers of security

1	Secured operation of workloads	Microsoft Defender workloads		
2	Simplified operational hardening	Privileged Access	Network Security	
3	Trusted system and data security	Encryption and Data Protection	System Security & Zero Trust	
4	Silicon-assisted security	Hardware Root-of-Trust	Secured-core	
5	Enabling regulated customers	Security Assurance	Certification	Secure Supply Chain

Microsoft's commitment to Windows Server security spans datacenter to Azure, starting with protections built into the hardware.

1 Secured operation of workloads

Whether your servers run in the cloud or on-premises, it's critical to have a comprehensive security strategy in place that enables you to secure your servers and protect them against the evolving threat landscape. Microsoft Defender for Cloud is a Cloud Security Posture Management and Cloud Workload Protection solution that helps you securely configure and protect servers against advanced threats across multicloud and hybrid environments. It provides continuous vulnerability assessments and security recommendations, can help you meet compliance standards, and it includes leading endpoint detection and response capabilities to effectively detect and respond to threats. It integrates with Microsoft Sentinel and the tools of your choice to enable easy investigation and remediation workflows.

2 Simplified operational hardening

Benefit from the expertise Microsoft earned building and running a hyperscale cloud. New features bring the same fundamental capabilities that harden Azure operations to your Windows Server environments.

Privileged Access Management
Restrict privileged access with Just-in-time and Just-enough administration capabilities, integrated with the Microsoft and partner ecosystem, within an existing and isolated Active Directory environment.

Enhanced network security
Gain enhanced network security with improved performance and stability. Network security innovations in Windows Server 2022 include these:

- **Datacenter Firewall.** Offer this highly scalable, manageable, and diagnosable software-based firewall solution to tenants. The Datacenter Firewall protects east-west and north-south traffic flows across the network layer of virtual networks and traditional VLAN networks.
- **TLS security.** Protect data of clients connecting to the server. Windows Server 2022 enables TLS (Transport Security Layer) 1.3 by default and supports HTTP over QUIC (HTTP/3) for faster and more secure HTTPS connections. The Quick UDP connection enables the creation of a TLS 1.3 encrypted tunnel over the internet-friendly UDP port 443.
- **Secure DNS.** Improve DNS security with support for DNS-over-HTTPS (DoH). When DoH is enabled, DNS queries between Windows Server's DNS client and the DNS server pass across a secure HTTPS connection rather than in plain text.

3 Trusted system and data security

To help protect confidential data, Windows Server 2022 delivers hardware-based isolation. This new version includes several key encryption and system security features to protect against unauthorized access.

Encryption and data protection capabilities
The cryptography stack spans Window servers, applications, and services:

- BitLocker Drive Encryption provides data protection integrated with the OS. BitLocker mitigates the threat of data exposure from lost, stolen or inappropriately decommissioned devices.

- Encrypted Hard Drive uses the rapid encryption provided by BitLocker Drive Encryption to enhance security and management.
- SMB Encryption is worth considering for any scenario in which sensitive data needs to be protected from man-in-the-middle attacks. SMB security and performance enhancements in Windows Server include these:
  - SMB AES-256 encryption for the most security conscious.
  - East-West SMB encryption controls for internal cluster communications.
  - Industry-standard encryption that minimizes performance issues using SMB encryption with remote direct memory access (RDMA).

System Security & Zero Trust
Windows Server 2022 delivers zero-trust capability with hardware-based isolation security. Device Health Attestation service, for example, helps verify boot configuration and attributes. When combined with device management, you can create zero-trust policies that ensure only devices that meet a specified posture will be able to connect to protected resources.

Windows Server 2022 enhances other security features first introduced in Windows Server 2016 or 2019.

- Windows Defender Application Control (WDAC), which ensures only verified executables run on the server, has significant improvements to policy configuration and path-based rules.
- Group Managed Service Accounts (gMSAs) now work with Windows containers without having to domain-join the host. Windows Server 2022 introduces a new model where an Active Directory identity protected in a secret store can be used by the un-joined host to retrieve the gMSA password. Removing the need to domain-join the host will make using gMSA in Kubernetes environments more manageable and scalable.

4 Silicon assisted security

Successfully protecting systems requires a holistic approach that builds security from the chip to the cloud across hardware, firmware, and the operating system. Using expertise built in its Azure datacenters and with its Secured-core PC initiative, Microsoft has collaborated with OEM and silicon partners to expand Secured-core certification to Windows Server 2022.

Secured-core
The Secured-core certification program makes it simpler to identify the most secure hardware platforms available for running Windows Server 2022. Certified servers use industry-standard hardware-based root of trust and firmware protections to ensure that only trusted components load in the boot path. Certified devices are suitable for industries that handle intellectual property, customer, or personal data. Functionality spans three key areas.

Hardware root of trust
Trusted Platform Module 2.0 (TPM 2.0) comes standard with Secured-core servers, providing a protected store for sensitive keys and data, such as information verifying components loaded during boot.

Firmware protection
In the last few years, there has been a significant uptick in firmware vulnerabilities, in large part due to the higher level of privileges associated with firmware combined with limited visibility into firmware by traditional anti-virus solutions. Windows Server 2022 supports Unified Extensible Firmware Interface (UEFI) secure boot. When the server is started, the firmware checks the signature of each boot component including firmware drivers and the OS. Secured-core servers go a step further than secure boot. Secured-core servers use advanced processor capabilities to ensure that even if there is a boot

firmware vulnerability, the sensitive contents held in virtualization-based security are not exposed. If the Hyper-V hypervisor loads in its expected configuration and the signatures are valid, the server boots and the firmware passes control to the OS.

Virtualization-based security (VBS)
Secured-core servers support VBS and hypervisor-based code integrity (HVCI). VBS and HVCI isolate privileged parts of the OS, like the kernel, from the rest of the system. This helps to ensure that servers can securely run critical workloads and helps protect related applications and data from attack and exfiltration.

5 Enabling regulated customers

Organizations in regulated industries require tight control over security. Microsoft builds the Windows Server operating system in compliance with the industry's most rigorous policies and procedures, which helps protect devices and users before the device is even turned on. Microsoft uses a combination of red-team, green-team practices along with the Secure development lifecycle to design and develop products with solid security fundamentals:

- Certification and adherence to international standards and certification programs such as FIPS 140 and Common Criteria.
- Secure Supply Chain best practices.
- Security Assurance with the support of the Microsoft Security Response Center, part of the defender community and on the front line of security response evolution.

Balancing tighter security and operational simplicity

Simply by upgrading to Windows Server 2022, organizations gain significant protection because the operating system enables robust security by default. Upgrading to Windows Server 2022 means your servers include all the latest security updates as well as the assurance you'll receive additional updates for years to come when new exploits are uncovered. As discussed in this section, Windows Server 2022 also provides a large suite of additional multi-layer security features worth activating. Each organization needs to prioritize which security issues to address and balance tightening security and operational simplicity. Windows Server 2022 helps advance both objectives.

Azure is the only cloud platform built by a security vendor

8,500
Security experts at Microsoft and $1B annual investment in security

25B+
Brute force authentication attacks blocked in 2021

More than
24 trillion
signals analyzed by Microsoft every 24 days

2 Hybrid

Across every industry and around the world, companies are working hard to keep pace with evolving business needs by building on existing digital investments. According to a 2021 survey sponsored by Microsoft, organizations are increasing investments in hybrid and multicloud to solve complex business needs.

The hybrid approach, which combines on-premises and cloud environments working together, can improve business agility. Yet IT teams can struggle to ensure compliance and manage resources at scale across diverse environments.

- Operating costs typically increase without a unified approach to managing hybrid, multicloud, and edge deployments.
- Organizations find themselves with duplicated cloud platform utilities for network, identity, governance, security, and operations.

Moving toward unified operations with hybrid security, management

Microsoft has built capabilities in Windows Server 2022 and Azure to expand and strengthen the connections between the customer datacenter, Azure, and other clouds. As a result, customers can unify operations with an intentional approach that includes maintaining one set of tools and processes to consistently manage each cloud provider. By using a common set of governance and operations management practices, organizations draw closer to operating seamlessly across on-premises, datacenter, edge environments, other clouds, and Azure.

Azure is the only cloud with end-to-end hybrid infrastructure and consistent security, identity, and management features. If you use Active Directory, for example, adding Microsoft Entra ID helps you manage and secure identities across environments. But you can do a lot more to streamline hybrid operations:

- Extend Azure services such as Microsoft Defender for Cloud, Microsoft Sentinel, and Storage Migration to Windows Server on-premises by using Azure Arc.
- Quickly and easily enable services such as Azure Backup, Azure Site Recovery, and Azure Monitor using Windows Admin Center.
- Simplify IT management and enhance security with Azure Automanage, and take advantage of Azure best practices, such as patching Windows Server VMs running on Azure without requiring a reboot.

Customers build on existing investments with strategic use of cloud

A 2021 survey found 86 percent of all respondents plan to increase investment in hybrid or multicloud environments. And 95 percent say those technologies have already been critical to their success. The survey, conducted by The Harris Poll and sponsored by Microsoft, targeted business decisions makers, IT professionals and IT decision makers in medium to large U.S. companies.

The survey defines hybrid as a mix of on-premises and one or more public clouds. It defines multicloud as an approach with multiple public clouds. Nearly all survey respondents agreed they need to be able to adopt cloud in some areas of business while retaining other data, workloads, and apps on-premises, primarily for regulatory reasons.

Companies surveyed report they are using clouds strategically, often for specific purposes such as data backup or access to sophisticated services such as security monitoring or artificial intelligence.

As hybrid computing has evolved, Windows Server and Azure have become more tightly integrated. Systems like Azure Arc enable management tools to span the datacenter, cloud, and edge devices. As Windows Server continues to evolve to meet business needs, IT pros benefit from powerful tools to design, configure, manage, and troubleshoot complex hybrid cloud environments. Microsoft offers several foundational tools for IT admins working with hybrid computing, which this section will discuss.

1 Ensure compliance and manage resources at scale

Unify operations with Azure Arc, a set of technologies that bring Azure security and cloud-native services to hybrid and multicloud environments. Use Azure Arc to enroll Windows Servers, Linux servers, and other resources as Azure resources. Once they are Azure resources, you can organize, govern, and secure on-premises machines the same way as Azure-hosted virtual machines.

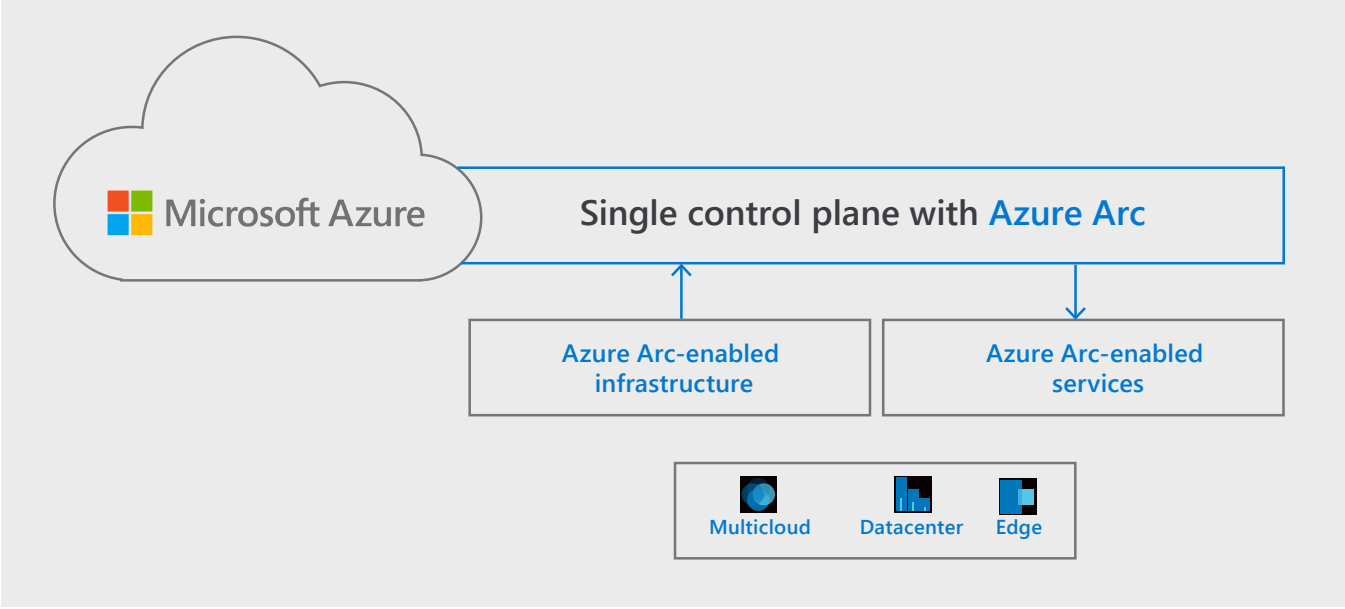
With Azure Arc, you can control infrastructure running outside of Azure using Microsoft Defender for Cloud, Microsoft Sentinel, Hotpatch as part of Azure Automanage for Windows Server, and Storage Migration Services to help make servers secure and reliable.

Here's a look at each:

Harden hybrid cloud resources
Microsoft Defender for Cloud helps you track your security posture, protect against cyberattacks, and streamline security management. Configure customized threat intelligence and prioritized alerts according to your environment, which includes your Arc-enabled Windows Server machines.

To provide an even higher level of security, consider using Microsoft Sentinel to automate the analysis and response to alerts generated by Defender for Cloud and other security monitoring systems.

Unify operations with Azure Arc



Bring Azure security and cloud-native services to hybrid environments with Azure Arc. Connect and operate hybrid resources, including Windows servers and Kubernetes clusters, as native Azure resources. Run Azure services anywhere, including data services and machine learning.

Detect and respond to security events

As an enterprise grows, the increasingly sophisticated attacks and volumes of alerts can overwhelm IT resources. Microsoft Sentinel brings together the value of two types of solutions: a security information and event management (SIEM) system and a security orchestration, automation, and response (SOAR) system. Sentinel uses information from Microsoft Defender for Cloud and many other sources to consolidate, analyze, and respond to security-related situations. Identify real threats to your Windows Server machines and other resources. Reduce noise from legitimate events with built-in machine learning and knowledge based on analyzing trillions of signals daily.

Simplify data migration

Migrating data can be a headache when upgrading to new hardware, moving servers to the cloud or onto virtual machines, or upgrading from one operating system to another. How can you be sure that you've transferred all the data and that all links or file paths still work? Storage Migration Service makes it easier to migrate storage, including NetApp FAS storage systems, to Windows Server machines or to Azure. The service provides a graphical tool that inventories data and then transfers the data to newer servers or to Azure virtual machines.

...

Lastly, no overview of Microsoft management tools would be complete without Windows Admin Center, which replaces numerous management tools such as Server Manager and Microsoft Management Console (MMC) and can be used alongside Azure Arc and Microsoft System Center. Windows Admin Center helps customers take advantage of cloud innovation to streamline management of on-premises servers.

2 Quickly and easily enable hybrid services

Remotely manage Windows Server machines running anywhere — physical, virtual, on-premises, in Azure, or in a hosted environment — with Windows Admin Center. The browser-based tool is available as a free download or can be accessed from the Azure portal. Many customers use it to streamline time-consuming, single-machine management tasks. Perhaps more importantly, built-in integration with Azure helps you connect on-premises servers to useful cloud services that can solve business problems and streamline hybrid operations.

Tools to help you manage and govern Windows servers

Windows Admin Center and Azure Arc work together — there's no reason to choose one or the other. Use Windows Admin Center for deep server administration of Windows Server, Azure Stack HCI, and Azure Kubernetes Service (AKS) on Azure Stack HCI.

Windows Admin Center is free to download and ready to use in coordination with Azure Arc. It combines common server management tools in a single interface, including Remote Desktop Connection, PowerShell, and purpose-built interfaces for managing roles and features. OEMs and ISVs also offer extensions that allow Windows Admin Center to manage hardware and third-party software.

Azure Arc complements Windows Admin Center. Arc is a single control plane for IT estate management — allowing you to ensure security, governance, and compliance for servers, Kubernetes clusters, data services, and more.

Here are some services that streamline hybrid operations:

- **Azure Site Recovery** replicates workloads running on physical and virtual machines from a primary site to a secondary location in Azure.
- **Azure Backup Service** backs up on-premises or Azure virtual machines and servers.
- **Azure Monitor** collects monitoring telemetry from a variety of on-premises and Azure sources, storing it in a log data store optimized for cost and performance.
- **Azure Files** centralizes file shares in the cloud while leaving on-premises file servers in place

And if Azure Arc and Windows Admin Center help you govern and manage servers, Azure Automanage makes it easy to automate operations and apply consistent best practices across your Windows Server and Linux virtual machines in Azure.

3 Reduce the pain of updates for cloud-based servers

Systems with unpatched security holes are a dirty secret in IT organizations. Organizations are sometimes reluctant to install security patches because they often require lengthy reboots and sometimes disrupt the stability of previously smooth-running systems.

Hotpatch as part of Azure Automanage for Windows Server is currently available exclusively on Windows Server 2022 Datacenter: Azure Edition. Keep your Windows Server virtual machines on Azure up to date without rebooting, enabling higher availability with faster and more secure delivery of updates.

Spanish company boosts security, eases management of servers at scale with Azure Arc

Prosegur, a Spanish security company, acquired a variety of IT practices from other companies after it grew rapidly and expanded globally. Prosegur adopted Microsoft Azure Arc and other security solutions to easily manage its hybrid, multicloud environment. Since then the company has onboarded 700 on-premises datacenter servers to Azure Arc and plans to ultimately move 5,000 servers: 3,500 Windows servers and 1,500 Linux servers.

Azure Arc helped Prosegur improve scalability and security. The company's IT team is now able to monitor infrastructure from one place, saving time and effort.

> We have the flexibility in Azure Arc to manage on-premises infrastructure similarly to the cloud in terms of updating security, performance, and log analytics in our web-based console …. We were always challenged with consistent management before. Now with Azure Arc and our ecosystem of Microsoft security solutions, we have a common layer to manage our infrastructure globally without thinking about which tool to use for a specific task in a specific datacenter."
>
> **Iñigo Martinez Lasala**
> Director of Technology and Systems
> Prosegur

3 Application Platform

A flexible application platform empowers developers and IT pros to build and deploy diverse applications. Windows Server 2022 delivers. Microsoft continues to improve the operating system's container-focused capabilities, which gives organizations the flexibility to scale both up and down and modernize fast. Windows Server 2022 simplifies and speeds container application deployment, accelerates modernization of .NET applications with a new containerization tool, and improves container orchestration with Kubernetes enhancements.

Speed up app modernization with container enhancements

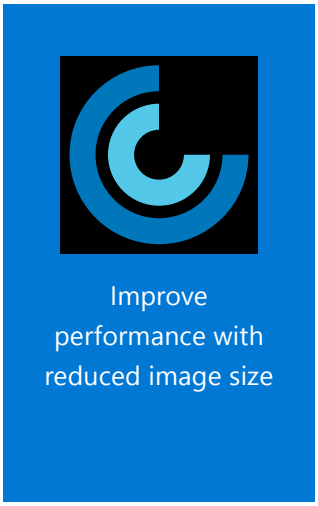
Containers enable you to package apps with everything they need to run so that your apps work the same way in the cloud and on-premises. All containers are created from container images. A container image is a bundle of files organized into a stack of layers that reside on your local machine or in a remote container registry. Larger images typically support more system features and native APIs, but typically have longer start-up times than smaller images.

Windows Server 2022 includes improvements that reduce image sizes and add support for additional Windows capabilities.

Reduced Server Core image size
Containers running on Server Core start faster and run faster in Windows Server 2022 than in previous versions, because Windows Server 2022 significantly reduces the image size.

Longer support cycle
Window Server 2022 container images now come with five years of mainstream support and an offering of an additional five years of extended support, which provides a long-term, stable base for containers dependent on these images. The longer support cycle helps ensure you have time to implement, use, and upgrade or migrate when appropriate for your organization.

Improved authentication
Facilitate Active Directory (AD) authentication using Group Managed Service Accounts (gMSAs) with Windows containers. In Windows Server 2022, use gMSA for containers with a non-domain-joined host



to authenticate via a portable user identity instead of a host identity. Container integration with gMSA helps eliminate the overhead required to manually join Windows worker nodes to a domain and manually manage passwords.

More compatibility
Windows containers now support Microsoft Distributed Transaction Control (MSDTC) and Microsoft Message Queuing (MSMQ), allowing more compatibility with existing applications and operating environments.

1 Accelerate modernization of .NET applications

Many existing Windows Server customers run legacy ASP.NET applications written before the broad adoption of containers. Windows Admin Center, discussed in the Hybrid section, and Azure provide tools to efficiently containerize existing ASP.NET apps so they can be used and managed just like apps written natively for containers.

Local container administration
Administer containers locally and integrate them with the Azure Container Registry with Windows Admin Center. Use the container extension in Windows Admin Center to simplify the containerization of existing web applications based on ASP.Net from the .NET Framework.

Azure-native solution for containerization
Move containers to Azure with Windows Admin Center or Azure Migrate: App Containerization. App Containerization, available from the Azure Migrate hub, provides an end-to-end solution to containerize and migrate existing web applications to Azure Kubernetes Service (AKS). Containerizing ASP.NET applications and migrating them to AKS doesn't require access to the codebase. The tool works by using the running state of the applications on a server to determine the application components and helps package them as a container image.

Watch a demo that walks through the process to move legacy apps to Azure with Azure Migrate.

2 Leverage Kubernetes enhancements

Orchestrators like AKS help you grow and manage containerized apps at scale. Use the service to deploy large numbers of containers, schedule workloads, monitor health, perform failover, and handle networking. The growing popularity of Kubernetes has spurred a vast amount of innovation, and Windows Server 2022 delivers several in-demand Kubernetes features to ease configuration headaches and improve overall reliability.

Run Azure Kubernetes Service on Windows Server 2019 Datacenter, Windows Server 2022 Datacenter, and Azure Stack HCI and get started hosting Windows containers in your datacenter.

Azure Kubernetes Service simplifies the process of setting up Kubernetes on Azure Stack HCI and Windows Server 2019 or 2022 Datacenter, and includes the following features:

- A Windows Admin Center wizard to help set up Azure Kubernetes Service and its dependencies.
- A Windows Admin Center wizard to help create Kubernetes clusters to run your containerized applications.
- PowerShell cmdlets to help set up Kubernetes and create Kubernetes clusters, in case you'd rather script the host setup and Kubernetes cluster creation.

Kubernetes dual-stack support
As more networking environments switch from IPv4 to IPv6, organizations need dual-stack support. Windows Server now includes IPv4/IPv6 dual stack support. Kubernetes assigns a unique network address (IP) to each workload instance (Pod) running on it. With IPv4/IPv6 dual stack support, each workload will get both an IPv4 and IPv6 address, reducing connection issues and configuration headaches in a mixed environment.

Multi-subnet support
Gain more flexibility with network addresses with multi-subnet support for Windows worker nodes via improvements to the Host Network Service (HNS). More restrictive subnets, such as subnets with a longer prefix length, are now allowed, and multiple subnets can now be assigned to each Windows worker node. Previously, HNS restricted the Kubernetes container endpoint configurations to using the prefix length of the underlying subnet. The first Container Networking Interface (CNI) that can use this functionality is Calico for Windows. Calico Network Policies is an open-source network and network security solution founded by Tigera.

Expanded cluster management scenarios
A new container type extends the Windows container model and enables a wider range of Kubernetes cluster management scenarios. With HostProcess

Introduction to containers

Containers are a technology for packaging and running Windows and Linux applications across diverse environments on-premises and in the cloud.

Containers start and stop quickly, making them ideal for apps that need to rapidly adapt to changing demand. The lightweight nature of containers also makes them a useful tool for increasing the density and utilization of your infrastructure.

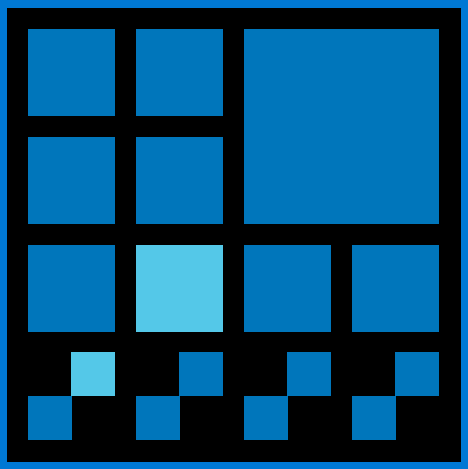
Containers run application code and run on top of server images. The type of server image can change depending on the container's requirements.

containers, users can package and distribute management operations that require host access while retaining versioning and deployment methods provided by containers. This allows you to use Windows containers for a variety of device plug-in, storage, and networking management scenarios in Kubernetes.

3 Support massive applications and databases

Deploy business-critical, large-scale applications and implementations of SQL Server with Windows Server 2022 running on Ice Lake-based servers. Take advantage of up to 48TB of memory and 2,048 logical cores running on 64 physical sockets.

Confidential computing capabilities enabled by Intel Secured Guard Extension (SGX) improve application security by isolating applications from each other with protected memory.



Introduction to orchestrators

While you can manage a few containers manually using Docker and Windows, apps often make use of five, ten, or even hundreds of containers, which is where orchestrators come in. Container orchestrators were built to help manage containers at scale and in production. Microsoft offers the poplular Kubernetes orchestrator on two platforms:

- Azure Kubernetes Service (AKS) — a managed Azure Kubernetes service.
- Azure Kubernetes Service (AKS) on Azure Stack HCI — for Azure Kubernetes Service on-premises, running on hyperconverged infrastructure or a Windows Server Datacenter edition host.

Get started

Whether you're experimenting with hybrid computing or you want to extend your capabilities to the next level, Windows Server 2022 delivers a high level of flexibility, innovation, performance, and security. Here's how to get started.

Download Windows Server 2022
Try the latest version of Windows Server for yourself — in Azure or in your datacenter.

Try Windows Server 2022 in the cloud with an Azure free account
Set up a Windows Server virtual machine in the cloud. Choose between Standard, Datacenter, and Datacenter: Azure Edition installation options.

Plan your migration to Windows Server 2022
Visit the Azure migration and modernization center for guidance and access to Azure engineers, tools and partner services.

Learn more about Azure Arc for servers and Kubernetes
Azure Arc is offered at no additional cost when managing Azure Arc-enabled servers and Azure Arc-enabled Kubernetes. See the Azure Arc pricing page for details.

Remotely manage Windows Server anywhere with Windows Admin
Learn how Windows Admin Center, available with your Windows Server license at no additional charge, consolidates and reimagines Windows Server utilities and tools in a single, browser-based, graphical user interface.

Prepare for Windows Server 2012 and 2012 R2 end of support in October 2023
Understand your options to keep workloads protected when regular security updates end for Windows Server 2012 and 2012 R2.

Windows Server resources

Learn about Windows Server 2022

What's new in Windows Server 2022

Compare Windows Server 2022 with earlier version

Compare Windows Server 2022 editions

Windows Server 2022 pricing and licensing

News and best practices from Windows Server team

Azure Arc overview

Windows Admin Center overview

Windows Server security documentation

Windows Server management documentation

Windows Server Extended Security Updates

Introduction to the hybrid and multicloud scenario

Windows containers in Windows Server 2022

Microsoft