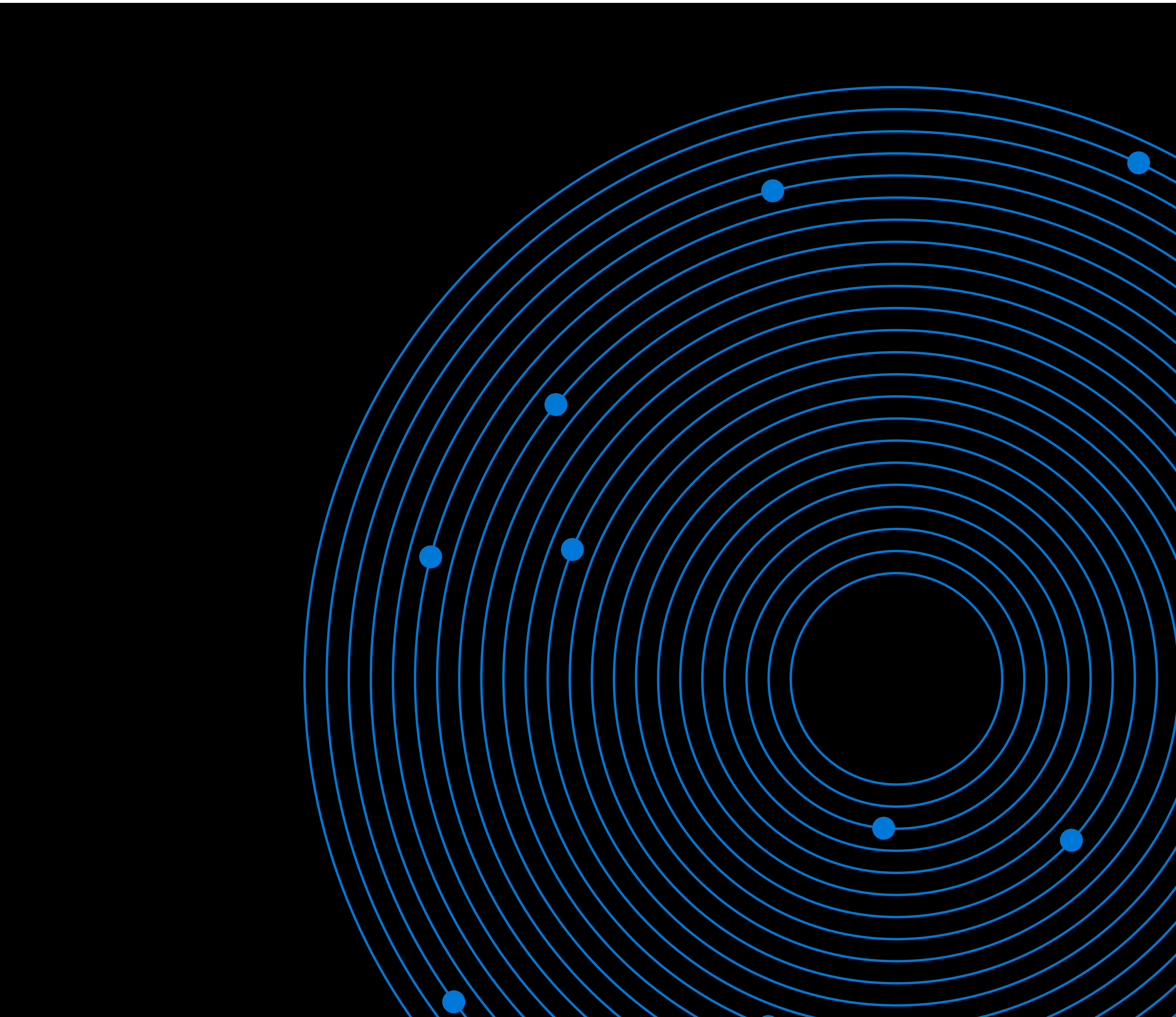
Microsoft

The Ultimate Guide to Windows Server 2019



Why Windows Server 2019

The cloud is a growing source of innovation, but on-premises datacenters aren't going away. The challenge is to blend the strengths of each in a way that meets your organization's needs, using a hybrid strategy. Hybrid cloud enables a future-proof, long-term approach that will play a central role in IT strategies for the foreseeable future.

Benefit from cloud computing on your terms

The latest version of Windows Server has been specifically designed to bridge on-premises and the cloud, to help you benefit from cloud computing on your terms. Organizations are using Windows Server to extend their datacenters to the public cloud. They synchronize file servers, securely connect to cloud services, and perform backups on Azure. And now you can use Windows Admin Center to simplify everyday server management tasks for Windows Server running anywhere—on physical servers, virtual machines, on-premises, and in Azure, Microsoft's cloud offering.

Read this guide to learn more. When you are ready to get started, we'll explain how to quickly start no-cost evaluations of Windows Server 2019 and Windows Admin Center. You also can find links to more in-depth information, including migration and upgrade resources.

What's new and improved in Windows Server 2019

01 **Hybrid cloud**
Extend your on-premises Windows Server environments to Azure and easily integrate high value services.

02 **Security**
Ability to guard against ransomware attacks and help stop malicious virtual machine tampering.

03 **Application development**
New support for Kubernetes and new capabilities to deploy and scale out containers across a hybrid environment.

04 **Hyperconverged infrastructure**
Improvements to Microsoft's hyperconverged platform now power prebuilt solutions that simplify deployment.

Unbeatable offers

Running current versions of software enables you to benefit from the latest security, performance, innovation features, and regular security updates. When you take advantage of special offers—including offers exclusively for Windows Server customers—you maximize your license benefits and cost savings, as well as increase deployment flexibility.

Azure Hybrid Benefit

Save money when you extend your datacenter to Azure by using your existing Windows Server licenses. With the Azure Hybrid Benefit, you can use on-premises Windows Server licenses that are covered with active Software Assurance or Windows Server Subscriptions to run Windows Server virtual machines in Azure at a reduced compute rate.

Special Azure Dev/Test pricing in Azure

Increasingly, organizations are using cloud or hybrid cloud for their dev/test environments and DevOps initiatives. With Azure, create dev/test environments in seconds, not weeks. Simplify and speed the process of running a dev/test environment. Provision virtual machines in seconds, instead of days or weeks. Get predictable costs and pay only for the resources you use. Microsoft makes it easy to use Azure cloud services by offering discounted rates on Azure to support your ongoing development and testing.

Windows Server 2008 End of Support options and offers

If you're still running workloads on Windows Server 2008 or 2008 R2, remember end of support is January 14, 2020. With the right planning, end of support can be the start of something better.

- **Build a bridge to the cloud with Windows Server 2019.** When you upgrade, you can more easily bridge on-premises environments with Azure services, adding additional layers of security while helping modernize your applications and infrastructure.
- **Secure on-premises; plan for hybrid.** If you cannot upgrade on-premises servers before the deadline, gain peace of mind by buying Extended Security Updates for your servers running Windows Server or SQL Server 2008 and 2008 R2. Or, rehost your Windows Server 2008 and 2008 R2 workloads in Azure and get three years of Extended Security Updates at no additional charge.

01

Hybrid cloud

Many organizations are accelerating their digital transformation by using public cloud services to build with modern architectures and refresh legacy apps. Most, however, must keep some workloads and data on-premises, for reasons that include technical and regulatory obstacles. Whether you use cloud or on-premises, Windows Server 2019 has you covered. Run it in a virtual machine in Azure, or upgrade on-premises to maximize existing investments with the option to extend your datacenter to the cloud.

Easily manage Windows Server running anywhere

Wherever you're using Windows Server—on a physical server, within a virtual machine, running on Hyper-V or VMware, or in the cloud on Azure—you can use Windows Admin Center as your management hub across your hybrid environment. Download the tool at no additional charge and install in minutes.

Windows Admin Center reimagines systems management by consolidating dozens of familiar admin tools in a single, browser-based, graphical user interface. Manage and troubleshoot servers, virtual machines, as well as traditional and hyperconverged clusters securely from any device.

Windows Admin Center is agentless—all you need to do is install it and point it to a server or virtual machine. It offers a single view, so there's no switching of tools or context, whether you're checking disk space or reconfiguring a cluster.

Server management reimagined

With Windows Admin Center, you can remotely manage Windows Server running anywhere.

- **Individual servers:** Perform backups, monitor events, manage users and groups, configure virtual machines and switches, and much more.
- **Clusters:** Configure and manage disks, networks, nodes, roles, updates, and VMs in both traditional and hyperconverged clusters.
- **Hyperconverged dashboard:** Access a unified view of compute, storage, and networking resources, if you are using hyperconverged infrastructure.

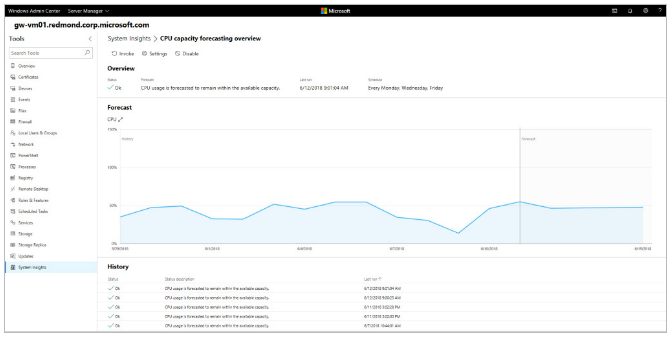
Manage servers and virtual machines remotely

Instead of launching and running multiple tools, you can now complete many administration tasks inside Windows Admin Center:

- Perform day-to-day server management tasks such as viewing and managing processes, services, certificates, devices, events, files, firewall rules, installed applications, users and groups, networks, registry, roles and features, storage, and updates.
- Manage Windows Server roles and features such as Hyper-V Virtual machines and containers, Active Directory, DHCP, DNS, Storage Migration Service, and Storage Replica.
- Use the PowerShell and Remote Desktop web consoles within Windows Admin Center for scripting and other tasks.
- Manage failover clusters by configuring and managing disks, networks, roles, virtual machines, and updates with cluster-aware updating.

The tool's graphical user interface is built on PowerShell, and there's even a button that allows you to view the PowerShell scripts running behind the GUI. This shows what's happening behind the scenes and allows you to copy and paste the script into other tools.

One new Windows Server 2019 capability that really comes alive with Windows Admin Center is System Insights, a new predictive analytics feature built into the operating system. Four default predictive capabilities—each backed by a machine-learning model—locally analyze Windows Server system data, such as performance counters, events, and disk anomalies, providing insight into the functioning of your servers. With this information, you can become more proactive managing issues in your deployments.



Overview

Status	Forecast	Last run	Schedule
✓ Ok	CPU usage is forecasted to remain within the available capacity.	6/12/2018 9:01:04 AM	Every Monday, Wednesday, Friday

History

Status	Status description	Last run ↑
✓ Ok	CPU usage is forecasted to remain within the available capacity.	6/12/2018 9:01:04 AM
✓ Ok	CPU usage is forecasted to remain within the available capacity.	6/12/2018 9:00:25 AM
✓ Ok	CPU usage is forecasted to remain within the available capacity.	6/11/2018 3:02:28 PM
✓ Ok	CPU usage is forecasted to remain within the available capacity.	6/11/2018 3:02:00 PM
✓ Ok	CPU usage is forecasted to remain within the available capacity.	6/7/2018 10:44:01 AM

System Insights dashboard on Windows Admin Center

How Windows Admin Center complements System Center

Windows Admin Center is focused on single server and cluster management and is not designed to replace your System Center tools. Each tool offers powerful capabilities.

Windows Admin Center	System Center
• Comprehensive troubleshooting and management system for single servers and single clusters • No-cost, browser-based management tool • Lights up new platform features of Windows Server • Extensions provide access to Azure services and third-party capabilities	• Powerful management and monitoring system for datacenters • Manages systems at scale • Allows system deployment from bare metal • Provides robust monitoring alerts and notifications

Manage your hybrid environment

Quickly incorporate powerful Azure management services into your datacenter to solve a gamut of IT challenges.

Enterprises need to:	Example	How Windows Admin Center and Azure services help:
Securely connect to the cloud.	A healthcare provider wants to use cloud services, but configuring secure connections is costly.	Use Windows Admin Server and the **Azure Network Adapter** to configure a point-to-site VPN connection between an on-premises Windows Server and an Azure virtual network.
Back up data and virtual machines in a protected off-site environment.	After losing key data, a financial firm struggles to find a more reliable backup strategy.	Use Windows Admin Center to configure **Azure Backup Service** and begin backing up on-premises or Azure virtual machines and servers. Protect data with encryption and apply multifactor authentication.
React quickly to datacenter outages.	With 90 percent of its sales online, a cosmetics firm struggles after a day-long outage.	**Azure Site Recovery** replicates workloads running on physical and virtual machines from a primary site to a secondary location in Azure. When an outage occurs at your primary site, you fail over to secondary location, and access apps from there. After the primary location is running again, you can fail back to it. Also enables replication of Azure Stack VMs, and Azure VMs between Azure regions.
Apply consistent software updates in a hybrid or heterogenous environment.	A pharmaceutical company with Linux and Windows Server VMs on-premises and in the cloud spends too much time updating software.	Through Windows Admin Center, use **Azure Update Management** to assess your update status across your datacenter or hybrid cloud. Manage and automate Windows and Linux virtual machine patching in on-premises environments, in Azure, and in other cloud providers.
Centralize file sharing across geographical regions without compromising performance.	A proliferation of local file servers in seven different locations becomes a major headache for a nationwide insurance firm.	Centralize file shares in **Azure Files**, while keeping your on-premises file server. Azure File Sync transforms Windows Server into a quick (or hot) cache of your Azure file share.
Get a comprehensive view of system activities across multiple datacenters and clouds.	Performance anomalies in a critical web service cause an accounting company's site to repeatedly crash when customers upload large amounts of financial data.	With Windows Admin Server as the front end, **Azure Monitor** collects, analyzes, and acts on telemetry from a variety of resources, including Windows servers and VMs, both on-premises and in the cloud.

02

Security

Cybersecurity attacks continue to increase with higher degrees of sophistication, continually targeting new areas of vulnerability. Security today must address attack vectors such as virtual machines, network traffic of all kinds, cloud services, as well as the human element—phishing, other social engineering exploits, and the acts of disgruntled or careless employees.

Early detection is key

Microsoft research shows that attackers take, on average, just 24-48 hours after infecting the first machine to penetrate an environment and often stay undetected for weeks or months. That's where monitoring and analysis tools like Advanced Threat Protection can play the role of watchdog—detecting and alerting you to threats from inside and outside your organization.

Simply by installing Windows Server 2019, organizations gain protections, because the operating system enables robust security by default. It 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 keeping systems simple to use.

Even if you do nothing else, protect your domain controllers, to limit cybercriminal access to admin privileges that can take down your entire environment. Make sure domain controllers are running the latest version of the operating system and consider these other safeguards:

- To reduce the attack surface, run only the Server Core installation option on domain controllers rather than the full GUI version.
- Enable Device Guard and Windows Defender Application Control.
- Only allow admin sessions (RDP/PowerShell) from known Privileged Access Workstations or Jump Server IP addresses.

If any of these terms are unfamiliar, find links to additional security information at the end of this document.

Below are examples of threats organizations face, and security features within Windows Server 2019 that mitigate those threats. Some features first shipped with Windows Server 2016 but have since been enhanced.

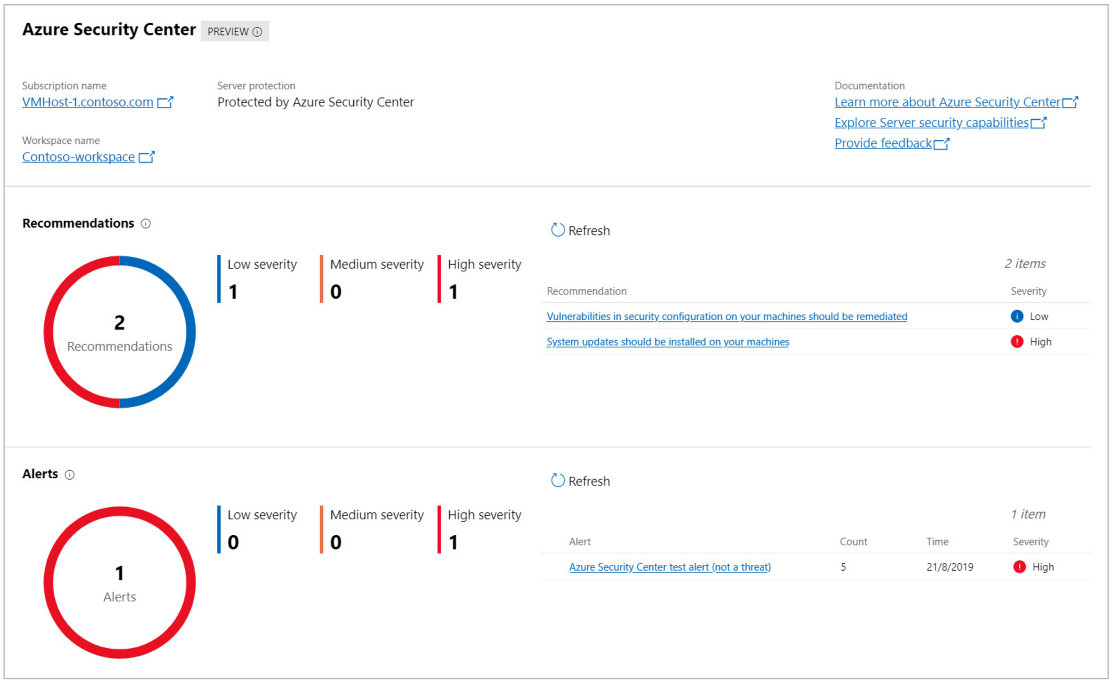
Threat	Scenario Threat	Relevant security feature
Virtual Machine corruption	Using a pass-the-hash attack, a hacker obtains the credentials of a virtual machine administrator. Now he can target a VM and copy it to a remote location. Either with those same credentials or a brute force attack, he inserts malicious code into the VM and reinstalls it in the datacenter. Branch offices typically have less physical security than a datacenter and are at greater risk of having servers and VMs stolen.	**Shielded Virtual Machines** protect against tampering with virtual machines by encrypting them. In Windows Server 2019, both Windows and Linux VMs can be encrypted. For branch office scenarios, Shielded VMs now work in offline mode by caching a special version of the VM TPM key protector on the Hyper-V host. With Windows Guarded Fabric enabled, VMs will only boot if they pass an integrity check. They also can't run on unapproved Hyper-V hosts and can only be accessed using remote network administration tools.
File-less ransomware attacks	An employee is persuaded to open a document or execute a script which contains active code. That code inserts a virus into memory rather than writing to disk. Once in memory, it can access legitimate tools and processes to spread through the network. Traditional antivirus systems are unable to detect it.	**Windows Defender Exploit Guard** is a new set of host intrusion prevention capabilities for Windows 10 and Windows Server 2019 that helps manage and reduce the attack surface of apps through four key components. • Attack Surface Reduction (ASR): Prevent malware from getting on the machine by blocking Office-, script-, 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. • Controlled folder access: Block untrusted processes from accessing protected folders. • Exploit protection: A set of easily-configured exploit mitigations.
Malicious application code	A corporate vice president gets an email pointing to a seemingly legitimate website which actually contains malware. That malware process has the same level of access to data that the user has, allowing a malicious process to corrupt or steal data.	**Windows Defender Application Control (WDAC)** can help mitigate these types of security threats by restricting the applications that users are allowed to run and the code that runs in the kernel. WDAC policies also block unsigned scripts and MSIs, and Windows PowerShell runs in Constrained Language Mode.
Network attacks	A company chooses to avoid implementing network encryption within individual applications and VMs because it's complicated to implement and the overhead of encryption affects performance.	**Virtual Network Encryption** encrypts network traffic between virtual machines. Network encryption is built into the operating system as the basis for application, server, and hypervisor communications, improving performance.

Threat	Scenario Threat	Relevant security feature
Active Directory environment compromised	An admin logs in from an unsecured machine where malware picks up the password string, giving the hacker unlimited access to key datacenter resources.	**Privileged Access Management (PAM)** enables granular access control over privileged admin tasks. It can help protect your organization from breaches that use existing privileged admin accounts. PAM requires users to request just-in-time access to complete elevated and privileged tasks. It also gives organizations more insight into how administrative accounts are used in the environment.
Slow reaction-time to threats	A low-level employee falls for a phishing attack. Malicious code enters the network and spurs a series of subtle lateral attacks undetected for weeks. Applications break, files are stolen, and ultimately Active Directory is compromised.	**Advanced Threat Protection** uses signals from your on-premises Active Directory to stop early threats and identify and respond to breaches. Part of its power comes from cloud security analytics provided by Azure's big-data machine-learning and Microsoft's unique optics across the Windows ecosystem, enterprise cloud products (Azure, Office 365), and online assets. Organizations can use ATP to: • Monitor users, entity behavior, and activities with learning-based analytics. • Protect user identities and credentials stored in Active Directory. • Identify and investigate suspicious user activities and advanced attacks throughout the kill chain. • Provide clear incident information on a simple timeline for fast triage.
NTLM cluster exploits	A user logs in to a compromised server using NTLM. Hackers relay the authentication to another server, granting them permissions to perform operations on the server using the authenticated user's privileges.	**Failover Clusters no longer use NTLM** authentication. Instead Kerberos and certificate-based authentication is used exclusively. There are no changes required by the user, or deployment tools, to take advantage of this security enhancement. It also allows failover clusters to be deployed in environments where NTLM has been disabled.
Man-in-the-middle (eaves-dropping and spoofing) and common ransomware attacks	A machine running the Server Message Block (SMB) networking protocol missing a critical patch is infected by malware that encrypts files on the machine and then displays a ransom notice.	**SMB-1 and guest fallback** are removed from Windows Server 2019 by default. A patch should be applied to older Windows servers.

Securing servers with Windows Admin Center

In addition to the tools that come with Windows Server, Azure offers a range of advanced security services and technologies you can subscribe to as needed to safeguard your hybrid cloud. Azure provides security services for storage, database, identity and access management, backup and disaster recovery, and networking. Monitoring tools are available, as well as a key vault to store secure secrets such as passwords and connection strings.

Through Windows Admin Center, you can onboard to Azure Security Center to discover active security threats and view recommendations to improve the security posture of your servers. Windows Admin Center also makes it easy to deploy a point-to-site VPN with the Azure Network Adapter, allowing secure access to cloud resources.



Azure Security Center PREVIEW ⓘ

Subscription name
VMHost-1.contoso.com

Workspace name
Contoso-workspace

Server protection
Protected by Azure Security Center

Documentation
Learn more about Azure Security Center
Explore Server security capabilities
Provide feedback

Recommendations ⓘ

2
Recommendations

Low severity	Medium severity	High severity
1	0	1

Refresh

2 items

Recommendation	Severity
Vulnerabilities in security configuration on your machines should be remediated	Low
System updates should be installed on your machines	High

Alerts ⓘ

1
Alerts

Low severity	Medium severity	High severity
0	0	1

Refresh

1 item

Alert	Count	Time	Severity
Azure Security Center test alert (not a threat)	5	21/8/2019	High

Use Windows Admin Center to easily attach servers in your environment to Azure Security Center. With Azure Security Center you can discover active security threats and view recommendations to improve the security posture of your servers.

03

Application development

Microsoft has embraced Linux to give organizations greater AppDev and DevOps flexibility, both on-premises and in the Azure public cloud. Continuing to improve support for Windows and Linux containers has also been a major focus, because containers enable older apps to run on newer versions of Windows and allow you to create apps that can scale up and out, across datacenters and the cloud.

Speed app development with improved support for containers

Major enhancements to the application environment in Windows Server 2019 reflect two realities:

- If your organization is like many, Windows and Linux don't just coexist, they need to work together.
- Developers increasingly are relying on containers to make applications fast, efficient, and portable. Containers package up software code, run-time, and dependencies together in an operating system-level virtualization to provide fast, fully isolated environments on a single system.

Linux support

So what's new in Windows Server 2019? The latest version delivers an improved version of the **Windows Subsystem for Linux (WSL)**. WSL lets your developers run a Linux environment—including most command-line tools, utilities, and applications—directly on Windows, unmodified, without the overhead of managing a virtual machine. Developers can run Bash, the popular shell and command language, as well as tools ranging from awk and sed to programming languages like Ruby and Python.

WSL, first introduced in Windows Server 2016, now adds these capabilities:

- New support for OpenSSH, Curl, Tar, and other common Unix and Linux commands.
- Greater integration of networking, native file system storage, and security controls.
- Ability to see Windows folders from Linux and Linux mounts from Windows.

Kubernetes support

If your organization adopts containers, it won't be long before DevOps has hundreds or thousands of container images to manage, and you don't want to do that manually. Container orchestration platforms like Kubernetes automate the creation, deployment, and management of containers, handling scaling, replication, version updates, and other complex, ongoing tasks. Both the Windows and Azure teams have been integrating Kubernetes into the respective operating environments because orchestration is critical in dynamic, hybrid cloud environments.

Windows Server 2019 includes **built-in support of Kubernetes**, bringing improvements to compute, storage and networking components of Kubernetes clusters. Some specific enhancements include:

- Container networking in Windows Server 2019 has been enhanced to improve the usability of Kubernetes on Windows nodes by increasing platform networking resiliency and strengthening support of container networking plugins.
- Deployed workloads on Kubernetes can use network security to protect both Linux and Windows services using embedded tools.

Additional container capabilities

Beyond improving Linux and Kubernetes support, Windows Server 2019 offers other features that allow containers to play a more central role.

- Use Windows Server Core, the lightest Windows Server deployment option, as a base image to create all your containers, and containerize legacy applications with greater compatibility.
- Run containers on the much smaller **2019 Server Core and Nano Server** base container images, which reduce download time and improve overall performance.
- Achieve higher levels of container density and endpoint creation with **server networking enhancements**.
- Use **Group Managed Service Accounts** (gMSA) to leverage Active Directory domain identities and gain access to network resources. In Windows Server 2019, gMSA delivers greater reliability and scalability for containers.
- Use **Windows Admin Center**, a browser-based server management tool, to view the containers on a Windows Server container host. In the case of a running Windows Server Core container, you can view the event logs and access the command-line interface of the container.

If you're interested in moving applications to the cloud or modernizing apps using cloud-based services, take a look at the **Azure Kubernetes Service** (AKS). The fully managed service offers serverless Kubernetes, a continuous integration and continuous delivery (CI/CD) experience, and enterprise-grade security and governance. Some of the AKS capabilities include:

- Provision container clusters.
- Minimize infrastructure maintenance using automated upgrades, repair, monitoring, and scaling.
- Elastically provision additional capacity.
- Achieve higher availability and protect applications from datacenter failures using redundancy across nodes.
- Use familiar tools—Visual Studio supports AKS.

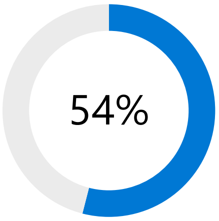
04

Hyperconverged infrastructure

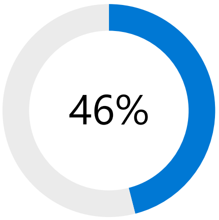
Datacenters are shifting from traditional servers with separate traditional storage arrays, network appliances, and hypervisor hosts, to a hyperconverged infrastructure with software-defined storage and networking. The reason? Less complexity, lower costs, and better performance, reducing both capital expenditure (CapEx) and operating expenses (OpEx).

Hyperconverged infrastructure momentum

Hyperconverged continues to be a fast growing segment of the on-premises server industry.



54% of organizations expect deploying converged/hyperconverged infrastructure to be among their most significant datacenter modernization investments over the next 12-18 months.[1]

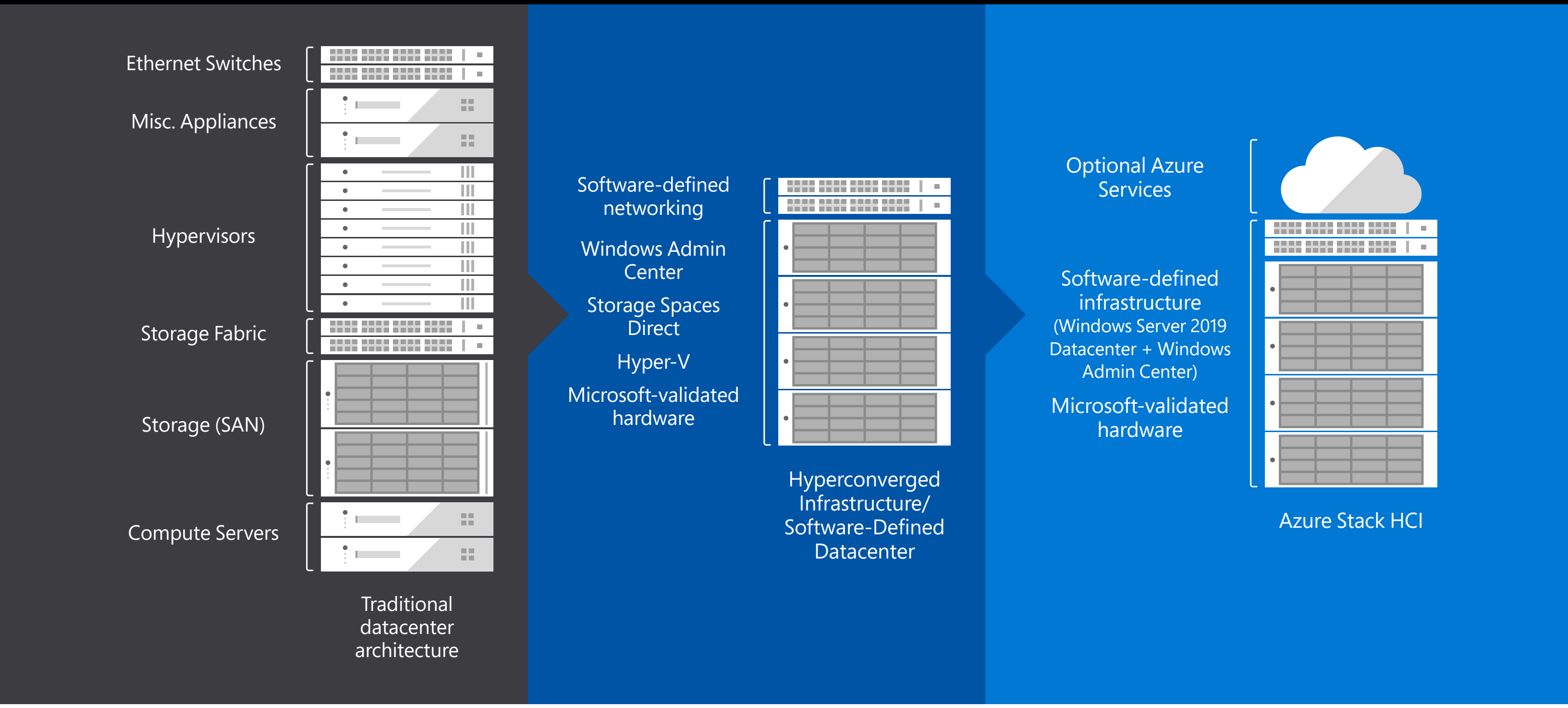


+46% of converged systems investments in Q2 of 2019 were for hyperconverged systems, equal to $1.8 billion in revenue. Hyperconverged systems continue to grow faster than any other converged systems segment.[2]

[1] ESG Data Point of the Week, April 2019 www.esg-global.com/data-point-of-the-week-04-29-19

[2] International Data Corporation (IDC) Worldwide Quarterly Converged Systems Tracker, September 2019 www.idc.com/getdoc.jsp?containerId=prUS45548719

From traditional to out-of-the-box hyperconverged nodes


Ethernet Switches
Misc. Appliances
Hypervisors
Storage Fabric
Storage (SAN)
Compute Servers
Traditional datacenter architecture
Software-defined networking
Windows Admin Center
Storage Spaces Direct
Hyper-V
Microsoft-validated hardware
Hyperconverged Infrastructure/ Software-Defined Datacenter
Optional Azure Services
Software-defined infrastructure (Windows Server 2019 Datacenter + Windows Admin Center)
Microsoft-validated hardware
Azure Stack HCI

Windows Server 2019 supports traditional datacenter architectures as well as newer server systems based on a hyperconverged infrastructure. Customers can configure their own HCI systems or buy them preconfigured from partners. An Azure Stack HCI cluster can begin with as few as two nodes.

Build your own or buy prebuilt hyperconverged infrastructure

Using internal expertise and resources, some organizations use Windows Server 2019 to build hyperconverged infrastructure. Other organizations turn to Microsoft partners to help them realize HCI benefits faster.

You can build your own hyperconverged infrastructure or, with Azure Stack HCI, you can quickly onboard prebuilt hyperconverged nodes via more than 150 solutions from more than 15 partners. These solutions use Microsoft-validated industry-standard x86 hardware to ensure high performance and reliability and include support for cloud-inspired technologies such as Non-Volatile Memory Express (NVMe) drives, persistent memory, and remote-direct memory access (RDMA) networking. The Windows Admin Center management UI provides a simple and centralized way to manage all resources.

Learn more about 150 pre-validated HCI solutions from Microsoft partners.

HCI use cases

Refresh aging hardware:
Replace older servers and storage infrastructure and run Windows and Linux virtual machines on-premises using existing IT skills and tools.

Consolidate virtual workloads:
Consolidate legacy apps on an architecture known for lightning-fast I/O and very low latency—perfect for running virtual machines. Tap into the same types of cloud efficiencies Microsoft uses to run Azure.

Connect to hybrid cloud services:
With Windows Admin Center, streamline access to management and security services in Azure, such as offsite backup, site recovery, and cloud-based monitoring.

Benefit from HCI capabilities

Enhanced hyperconverged infrastructure capabilities in Windows Server 2019 help drive breakthrough performance. It starts with Storage Spaces Direct architecture, which uses industry standard servers with local-attached drives to create highly available, scalable storage at a fraction of the cost of typical SAN or NAS arrays.

In fact, solid-state storage devices are so fast today that capacity is no longer the big issue—it's now about increased speed and reduced latency. Even technologies like SATA, PCI, and Fiber Channel become the choke point between storage devices and the processor. Persistent Memory, supported in Windows Server 2019, has the speed of DRAM and is located adjacent to the CPU to reduce latency. But unlike conventional DRAM, it can retain its content through power cycles. The DRAM can even be partitioned between persistent and conventional memory. In a recent test, a 12-node Windows Server 2019 cluster with Intel® Optane™ DC persistent memory delivered breakthrough performance of 13,798,674 IOPS with only 40 millionths of a second of latency. Additional examples of enhancements in Windows Server 2019 follow.

Example enhancements in Windows Server 2019	
Deduplication and compression for ReFS	The Resilient File System (ReFS) is Microsoft's recommended file system for HCI. With deduplication and compression, disk space savings can go as high as 90 percent.
Increase storage capacity	The maximum total raw storage capacity per cluster has increased from 1 PB in 2016 to 4 PB in Windows Server 2019.
Speed networking	Windows Server 2019 capabilities boost the maximum speed of a single SDN gateway to 18 Gbps from 4 Gbps in Windows Server 2016.
Understand performance history	It's now easy to get historical data and displays of over 50 performance counters with nothing to install or configure.
Reduce clustering security risks	Core failover clustering has become more secure by removing dependency on NTLM.
Orchestrate cluster upgrades	Cluster Aware Updating is now more deeply integrated with Storage Spaces Direct and allows coordinated restart of servers for planned maintenance.
Improve cluster resiliency	Nested resiliency keeps you up and running in the event of having both a driver and server failure at the same time, even in a two-node cluster.

Move files and unstructured data more easily

Even if 13 million IOPS is well beyond your organization’s needs, it shows the benefit of moving to a newer platform. Microsoft has a variety of migration and upgrade services that make these moves easier. Read more about one such service in this section, and you can find additional resources at the end of this document.

Traditionally, one of the most difficult parts of any migration is moving files to a new platform. Whether you choose an Azure Stack HCI prebuilt solution or build your own, you can take advantage of Storage Migration Service, new in Windows Server 2019. The service helps you migrate file servers from any Windows Server version going back to Windows Server 2003. Migrate data into physical or virtual machines running in the datacenter or on Azure. Use the graphical workflow available in Windows Admin Center to step through the process. The workflow manages all the complexity, keeping track of file attributes, permissions, share names, and network settings. It even manages files that are in use and files the operator isn’t authorized to access. Storage Migration Service operates in three phases.

Storage Migration Service phases	
Inventory	Admin selects nodes to migrate. Storage Migration Service orchestrator node interrogates storage, network, security, SMB share settings, and data to migrate.
Transfer	Admin creates pairings of source and destinations from that inventory list. Admin decides what data to transfer and performs one or more transfers.
Cutover	Admin assigns the source networks to the destinations and the new servers take over the identity of the old servers. The old servers enter a maintenance state where they are unavailable to users and applications for later decommissioning. The new servers use the subsumed identities to carry on all duties.

Improve cluster flexibility with Windows Server 2019

Introduced in Windows Server 2016 and enhanced in Windows Server 2019, **cluster sets** enable customers to scale out to thousands of cluster nodes. These loosely coupled groups of clusters can include compute-intensive servers, storage servers, or hyperconverged systems where compute and storage are combined. Individual clusters require the same hardware for all servers, but cluster sets can be made up of clusters with different hardware configurations. With cluster sets, it’s easy to add just a compute node to the cluster (or just a storage node), take down nodes, and to patch nodes with zero downtime by migrating workloads among cluster set members. Cluster sets create a unified storage namespace, enabling you to migrate virtual machines across member clusters of a cluster set.

Streamline management of hyperconverged datacenter with Windows Admin Center

Windows Admin Center, which provides a central hub for server and cluster management, also includes built-in capabilities to streamline management of a hyperconverged infrastructure with simplified workflows of common tasks.

- Create and manage Storage Spaces Direct and Hyper-V virtual machines with radically simple workflows that allow you to, among other things:
  - Create, open, resize, and delete volumes.
  - Create, start, connect to, and move virtual machines.
- Monitor resources cluster-wide with a Windows Admin Center dashboard that graphs memory and CPU usage, storage capacity, IOPS, throughput, and latency in real-time, across every server in the cluster, with clear alerts when something's not right.
- Manage and monitor virtual networks, subnets, connect virtual machines to virtual networks, and monitor your Software Defined Networking infrastructure.

Add experiences by extending Windows Admin Center

Windows Admin Center is not just an application, but an extensible platform for integrating additional capabilities for hardware, application management, and monitoring through third-party extensions. Use it to streamline your server management experience by installing only the features you need. An array of third-party extensions mean you won't have to wait for a new version of Windows Admin Center to get new tools.

Microsoft partners such as Dell-EMC, Lenovo, and DataON have released extensions for managing their server and Azure Stack HCI solutions. Squared Up and BiitOps offer extensions for monitoring and tracking changes across your datacenter.

dataON DELLEMC FUJITSU Hewlett Packard Enterprise

Lenovo \Orchestrating a brighter world NEC PURESTORAGE QCT

THOMAS KRENN® BIITOPS BUSINESS INTELLIGENCE FOR IT OPERATIONS SquaredUp

Get started

For businesses considering the next step in their journey to the cloud, Windows Server 2019 helps bridge on-premises operations with innovative Azure services that help fast track digital transformation initiatives and create new opportunities. Why wait?

Download Windows Admin Center

Windows Admin Center is the new central hub for system administration of Windows servers and hyperconverged systems. It makes hybrid operations easier with built-in integration to Azure for cloud services on demand. Download and install it in minutes at microsoft.com/WindowsAdminCenter.

Try Windows Server 2019 on Azure, for free

If you want to try Windows Server 2019 without a lot of hassle, create a free Azure account and set up a Windows Server virtual machine in the cloud. Choose between Windows Server Datacenter, Datacenter with Containers, and Datacenter Server Core installation options.

Prepare for Windows Server 2008 end of support January 2020

Understand your options to keep workloads protected when regular security updates end for Windows Server 2008 and 2008 R2, including migration to Windows Server 2019. For continued protection beyond the deadline, buy Extended Security Updates (ESUs) or move your workloads to Azure and get three additional years of Extended Security Updates at no additional cost. To take advantage of Azure Hybrid Benefit, use existing Windows Server and SQL Server licenses to save on Azure virtual machines.

Plan your migration to Windows Server 2019

- Download the Migration Guide for Windows Server and learn which options are best for your organization: install, upgrade, or migrate.
- Visit the Azure Migration Center to learn why it might make sense to move applications, data, and virtual machines to Windows Server 2019 on Azure.
- Use Storage Migration Service introduced in Windows Server 2019 to move unstructured data from older servers to Windows Server 2019.

Windows Server resources

Learn about Windows Server 2019	www.microsoft.com/cloud-platform/windows-server
Learn about Windows Admin Center	www.microsoft.com/cloud-platform/windows-admin-center
Download Windows Server free trial	www.microsoft.com/cloud-platform/windows-server-trial
Compare features of Windows Server versions	www.microsoft.com/cloud-platform/windows-server-comparison
Review pricing and licensing for Windows Server 2019	www.microsoft.com/cloud-platform/windows-server-pricing
Get started with Windows Server 2019	docs.microsoft.com/windows-server/get-started-19/get-started-19
Learn about Windows Server on Azure	www.azure.com/windowsserver
Connect Windows Server to Azure hybrid services	docs.microsoft.com/windows-server/manage/windows-admin-center/azure/index
Learn about Azure Stack HCI solutions	microsoft.com/hci
Learn about Azure Kubernetes Service	azure.microsoft.com/services/kubernetes-service
Review Windows Server 2019 application compatibility	docs.microsoft.com/windows-server/get-started-19/app-compat-19
Join the Windows Server Tech Community	techcommunity.microsoft.com/t5/Windows-Server/ct-p/Windows-Server
Read the Windows Server blog	cloudblogs.microsoft.com/windowsserver/
Learn about Windows Server 2008 end of support	www.microsoft.com/cloud-platform/windows-server-2008

Some examples are for illustration only and are fictitious. No real association is intended or inferred.

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

Microsoft