Windows Server 2016

Run workloads for any platform

Microsoft

The best choice for your workloads on any platform

Windows Server 2016 is the strategic choice for businesses focused on digital transformation. Whether on-premises or in the cloud, Windows Server 2016 is designed to run both traditional and cloud-native workloads equally well.

Windows Server 2016 can help resolve many of the issues facing IT for deploying workloads in hybrid and cloud environments. At the top of the list: Security. For many organizations, it is difficult to provide security parity between workloads running in different clouds, on different hosts, and those running on bare metal. Windows Server 2016 addresses these challenges with built-in protection for common security concerns across all platforms.

Developing apps across hosts and cloud services can create difficulties when there is inconsistency in how toolsets work—or don't work—in different environments. That's why Windows Server 2016 also includes features that make it easier to support both traditional app development and in-the-cloud development efforts using a common set of tools, regardless of the underlying platform.

Finally, Windows Server 2016 eliminates the need to use multiple toolsets to manage workload access to data and updates across hybrid and cloud environments. One solution is all you need for storage, disaster recovery, and centralized management across platforms.

For customers looking to upgrade existing Windows Server 2012 R2 (or earlier) deployments, as well as those seeking to develop new apps on-premises and in the cloud, Windows Server 2016 has much to offer. This paper describes the features that make Windows Server 2016 the best choice for running your workloads on any platform, as summarized in Table 1. For Microsoft Azure customers, it also provides an overview of additional capabilities that become available when running workloads on Windows Server 2016 on Azure.

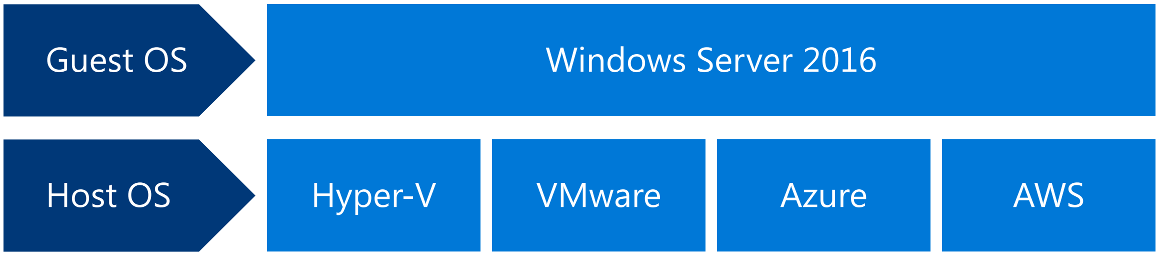

Figure 1. As organizations continue to rely on hybrid environments, they need an operating system that can run smoothly across any host platform. Windows Server 2016 is designed to work across platforms using common technologies and tools.

Table 1. Windows Server 2016 benefits on any platform

Benefits	Features supported on: Hyper-V, VMware, AWS, and Microsoft Azure hosts	Key capabilities
Industry-leading scalability for apps running in virtual machines	• Virtual machine memory and virtual processor support	• See table on page 4.
Built-in security for virtual machines	• Device Guard • Control Flow Guard • Windows Defender • Security auditing • Remote Credential Guard • Just in Time and Just Enough Administration • Risk-based conditional access	• Block compromised software from running. • Prevent memory class corruption attacks. • Automatically block known malware. • Scan audit logs for malicious activity. • Eliminate credential theft in remote desktop sessions. • Help prevent high-value administrator credentials from being compromised. • Make sure devices and users are safe before allowing connections.
Easier, more efficient app development	• Windows Server containers • Active Directory Service Accounts for Windows containers • Server Core • Nano Server • AD FS support for OpenID Connect and OAuth2 clients	• Streamline app development and testing with containers. • Help secure authentication for containers. • Lift and shift apps to the cloud faster and with more stability and security. • Optimize cloud-based app development with "just enough operating system" capabilities. • Make it easier to sign on to websites and SaaS apps.
Improved VDI experiences	• Personal Session Desktops • RemoteFX and Discrete Device Assignment (DDA) • MultiPoint Server role	• Provide personal session desktops in the cloud. • Run modern graphics and 3D apps on virtual desktops. • Deploy MultiPoint virtual machines without paying additional licensing costs.
More cost-effective disaster recovery	• Storage Replica	• Easily replicate virtual machine data between servers and clusters – on-premises or in the cloud.

Industry-leading scalability

The ability to scale your virtual infrastructure is one of the most important factors when selecting an operating system. Windows Server 2016 delivers new industry-leading scalability with support for up to 12 TB of memory and 240 virtual processors per virtual machine as shown in Table 2, helping improve app availability and performance. This is true even for large, data-intensive workloads like SQL Server. For example, Dutch logistics company Danske Fragtmaend was able to run its business intelligence queries 9,521 times faster by moving to SQL Server 2016 on Windows Server 2016 infrastructure.

Table 2. Industry-leading scalability

Feature	Windows Server 2012/2012 R2 Standard and Datacenter	Windows Server 2016 Standard and Datacenter
Virtual machine memory support	Up to 1 TB per virtual machine	Up to 12 TB per virtual machine (12x)
Virtual machine virtual processor support	Up to 64 virtual processors per virtual machine	Up to 240 virtual processors per virtual machine (3.75x)

Built-in operating system-level security

No company or industry is immune to cyberattacks in today's threat environment. Windows Server 2016 is designed to protect against common methods that attackers use to compromise data and disrupt business—such as malware, ransomware, and credential theft—even in virtual environments. Many protections have been added into the base operating system. Simply migrating an existing app to Windows Server 2016 will significantly improve security for that app. These protections include operating system-level defenses, antimalware, credential security, and remote access control.

Block compromised software from running

With Device Guard in Windows Server 2016, organizations gain unprecedented control to prevent unauthorized software from running. System-wide policies can be specified to permit specific binaries to run. Windows Server 2016 will prevent any binary that is not authorized from executing and log the activity to help administrators identify potential breaches. Administrators can use PowerShell to create a policy that lists the binaries allowed to run from a baseline server that has the appropriate software installed.

Prevent memory class corruption attacks

Attackers commonly use a tactic known as memory class corruption to target unpatched vulnerabilities. This might involve sending malicious data to corrupt memory contents with the intention to alter how the program behaves. Attackers leverage these modifications to make the app execute indirect calls to other program areas and seize control of the system. Using Windows Server 2016 helps prevent some classes of memory-based attacks using Control Flow Guard. Lightweight security checks identify and confirm the set of valid functions in an app each time the app is executed. If Control Flow Guard detects an app executing in a non-predetermined or non-viable order, it immediately terminates the program, stopping the exploit attempt in its tracks.

Automatically block malware

Windows Server 2016 virtual machines automatically include the active detection capabilities of Windows Defender to block known malware. Windows Defender is turned on by default, so administrators do not need to take any action to activate protection. This eliminates the effort needed to deploy antimalware software, while also ensuring that IT can immediately meet compliance requirements—even if they decide to use a third-party antimalware solution in the future. Because it is integrated with PowerShell, Windows Defender can also scan for malware before launching any binary code.

Identify malicious activity with security auditing

Windows Server 2016 virtual machines benefit from new audit events that help with the early detection of malicious activity in your datacenter. Events are logged from Control Flow Guard, Device Guard, and other security features in a single location, making it easier for administrators—using monitoring tools you already have in place—to determine what systems may be at risk. New event categories include:

- **Audit Group Membership:** Enables you to audit the group membership information in a user's login token. Events are generated when group memberships are enumerated or queried on the PC where the login session was created.
- **Audit PnP Activity:** Enables you to audit when Plug and Play (PnP) detects an external device that could contain malware. PnP events can be used to track down changes in system hardware.

Eliminate credential theft during remote desktop sessions

A reported 63 percent of all network breaches result from compromised user credentials,[1] making credential security essential to defending your organization against cyberattacks. As part of this effort, Windows Server 2016 helps protect credentials for workers who need to connect to remote desktops for their jobs with Remote Credential Guard.

Previously, Remote Desktop Services required users to log on to their machine locally, then log on again when they connected to the target system hosting their remote desktop. During the second logon, their credentials would pass to the target remote desktop, which could expose them to pass-the-hash or pass-the-ticket attacks.

With Remote Credential Guard, users don't have to reenter their user name and password a second time because the system uses the same credentials that were used to log on to the connecting device running the remote desktop session. The result is that attackers will not be able to find—and therefore cannot reuse—exposed privileged credentials, because no credentials have been passed to the target system.

Minimize the impact of compromised administration credentials

After an attacker succeeds in stealing valid administrator credentials, they can use those credentials to launch additional intrusions into the network. Typically, an administrator account has domain-wide privileges, even if the user has a very narrow set of administrative requirements. By providing credential controls, Windows Server 2016 helps limit an attacker's ability to use stolen credentials to gain universal access to network resources.

Windows Server 2016 Just Enough Administration enables organizations to narrowly define administrator access privileges using PowerShell. For example, a DNS administrator can be given access to a limited set of commands available for DNS management. If the administrator's credentials are compromised, the attacker would only be able to access DNS servers—not any SQL database, domain controller, or other high-value target.

Providing administrators with more privileges than they need is especially prevalent in virtualization fabrics—largely because there was previously no way to limit access between virtual machines. Instead, a valid set of administrator credentials equaled access to any virtual machine running in the fabric. Because Just Enough Administration works at the virtual machine level, organizations can now grant or restrict administrator access to an individual Windows Server 2016 instance on a virtual machine, providing security control over what was previously not securable.

You can also use Just in Time Administration, as shown in Figures 2 and 3, which enables administrators to request the specific privileges they need for the exact window of time required to perform system changes. If a DNS administrator needs to make an update to one of their servers, they can request access to manage DNS using Microsoft Identity Manager 2016.

[1] Verizon Data Breach Investigations Report 2016

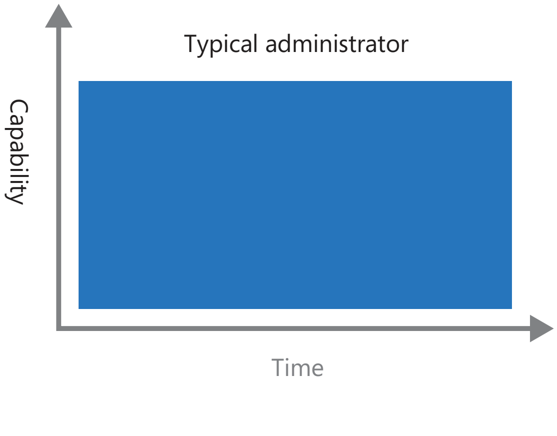

Figure 2. Admin privileges that are too broad and have no time limit create a large window of exposure for attackers searching for credentials.

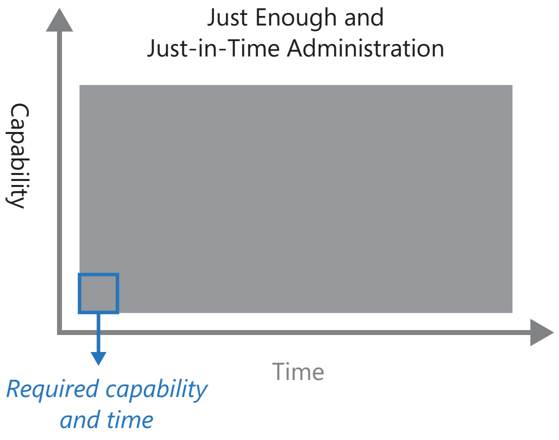
Just Enough and Just-in-Time Administration
Capability
Time
Required capability and time

Figure 3. Just Enough and Just-in-Time Administration reduce the attack surface area for theft of admin credentials.

The request workflow can include an approval process such as two-factor authentication, which can call the administrator's mobile phone to confirm identity before granting the requested privileges. After they're granted, those DNS privileges provide access to the PowerShell role for DNS for a specific time.

Conditional access for federated connections

Windows Server 2016 helps secure access and single sign-on to apps using Active Directory Federation Services (AD FS) by providing conditional access on a per-application basis. Administrators can now configure specific access requirements for sensitive business apps that handle confidential information like credit card numbers or employee salary data. Any highly sensitive apps can be configured to require multifactor authentication, such as a phone call to the user's mobile device or a fingerprint scan, to confirm the user's identity before granting access. AD FS conditional access integrates with Intune mobile device management so you can also define a policy that allows authentication only from enrolled, managed, and compliant devices.

Better, more efficient app development

Virtualization has simplified how businesses create and test apps. Increasingly, however, developers are rethinking these processes, shifting from writing apps for virtual machines to writing apps for the cloud and leveraging microservice architectures. Windows Server 2016 helps developers deliver apps to market faster and with greater impact—in standard virtual machines or leveraging new innovations like containers running a lighter-weight option such as Server Core or Nano Server.

Windows Server containers

Containers deliver on the promise of app mobility and a rapid development cycle. Customers are now deploying new versions of apps on a daily or, in some cases, hourly basis. Containers can help accelerate the development process to meet this timeline—in a way that still ensures high-quality apps. Because containers are virtualizing just the operating system, they provide "just enough virtualization" for rapid app delivery.

Here's how it works: developers can create an image to deploy identically across any environment in seconds, because only the app and the components needed to run the app are included in the image. You can also use an image as a baseline to create another image, making image creation even faster. Multiple containers can share the same image, which means containers start very quickly and use fewer resources. For example, you can use containers to spin up lightweight and portable app components—also known as microservices—for distributed apps, and quickly scale each service separately. With containers, developers can build an app in any language. These apps are completely portable and can run anywhere—server, private cloud, public cloud, or service provider—without any code changes.

Windows Server 2016 offers Windows Server containers and Hyper-V containers. Both work with Windows Server 2016 guest virtual machines and are created and managed identically. Both function in the same way. The difference is the level of isolation between the container, its host, and other containers running on the same host.

Windows Server containers: Multiple container instances can run concurrently on a host with isolation provided through namespace, resource control, and process isolation technologies. They can share the same kernel with the host and with each other, as shown in Figure 4.

Hyper-V containers: Multiple container instances can run concurrently on a host. Each container runs inside a special virtual machine that provides kernel-level isolation between each Hyper-V container and the container host. (Note: This feature does require a Hyper-V host.)

To help developers use the knowledge and experience they have with Linux containers, Microsoft and Docker jointly delivered the Docker container toolset, which allows you to create and manage Windows Server and Hyper-V containers. Microsoft also created a PowerShell module for Docker to extend the Docker experience, which is now open source for community and Docker contributions. The PowerShell module can manage Linux and Windows Server containers locally or remotely using the Docker engine's REST APIs.

Server Core

Server Core is a small-footprint, headless operating system installation option for Windows Server 2016 that removes the desktop UI from the server and runs only required components. It provides greater stability, reduces configuration requirements, and presents a smaller potential attack surface. It also uses less memory and disk space, allowing developers to maximize efficiency on existing hardware. Because the standard user interface is not installed, Server Core is managed using the command line, Windows PowerShell, or by remote methods.

For developers, Server Core is useful as a lighter-weight operating system in a virtual machine or container for traditional apps, such as line-of-business (LOB) apps, that you are lifting and shifting to the cloud. It contains all the operating system functionality that traditional apps need, while also providing efficient use of resources and reducing the maintenance burden.

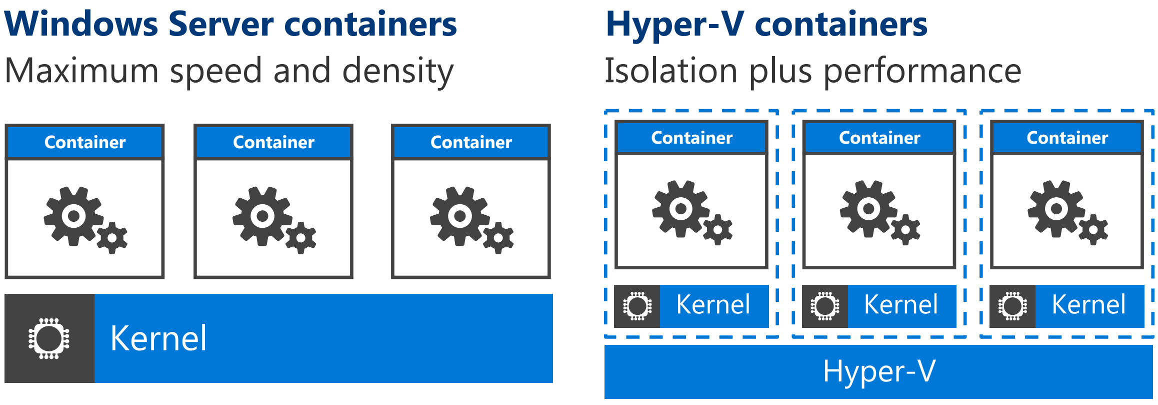

Figure 4. Developers gain an array of new tools, including containers, that make it easier to modernize traditional apps and create high-quality, protected apps. Windows Server containers share the kernel with the host and each other. Hyper-V containers offer kernel-level isolation between each container.

Nano Server

Nano Server is a cutting-edge installation option that provides developers with an extremely small footprint to develop and test new, modern apps. Starting out at 25 times smaller than a full image of Windows Server 2016, it provides "just enough operating system" capabilities, allowing you to add only the roles you need. As a result, its initial boot time is incredibly fast—40 seconds versus 19 minutes—and it is much simpler to operate and maintain.

For developers, Nano Server is particularly useful as a lightweight operating system in a virtual machine or container for born-in-the-cloud apps. It is highly optimized for distributed and cloud-based apps that use containers and microservices architectures, ensuring that more resources are freed up to run apps and services. All management is performed remotely via PowerShell and WMI, with remote management options via existing tools and a new web-based remote management tool.

Authentication for containers using Active Directory

Although they are extremely efficient for app development, containers do present some challenges—one of which is that they cannot be domain-joined. Every time you start them, they look and act brand new, without user names or passwords to authenticate that would allow them to access the systems and services they need to function. How best to address this lack of authentication?

In the Linux world, app developers traditionally include a .txt file in the container with necessary user names and passwords, then use the .txt file as authentication. This results in huge security issues, with the potential to expose not only data, but your entire network, to cyberattacks. Thousands of valid passwords to AWS, Azure, and even internal apps have been found posted inadvertently in places like GitHub that developers use to collaborate.

Windows Server 2016 solves this problem with Active Directory Service Accounts for Windows containers, which allows users and other services to make authenticated connections to your apps—while also helping secure data and prevent unauthorized usage. Windows containers and the services they host can be configured with lightweight directory services by realm-joining them with a group Managed Service Account (gMSA). By assigning a container to use a specific gMSA as its domain identity, any service running as Local System or Network Service can use this container identity just as they use a domain-joined host identity. There is no password or certificate private key stored in the container image that could inadvertently be exposed, and the container can be redeployed to development, test, and production environments without being rebuilt to change stored passwords or certificates.

Single sign-on and authentication for websites and SaaS apps

Windows Server 2016 AD FS adds support for OpenId Connect web sign-on and authentication for OAuth2 confidential clients. By supporting these standards, Windows Server 2016 makes it easier for developers to help secure access to their modern apps and websites. For example, using these common standards, you can allow a user to leverage their Facebook credentials to log on to your app.

Improved virtual desktop infrastructure experiences

When using Windows Server 2016 as a workspace, you can now provide users with a superior user experience whether the operating system is hosted in the cloud or on-premises—including for personal session desktops, graphic-intensive apps, and MultiPoint server deployments.

Provide personal session desktops in the cloud

In Windows Server 2016, Remote Desktop Services (RDS) allows administrators to deploy server-based personal desktops in a cloud computing environment where there is a separation between the fabric Hyper-V servers and the guest virtual machines in Azure. The new personal desktop session extends the session-based desktop deployment scenario to enable an administrator to create a new type of session collection where each user is assigned to their own personal session host with administrative rights that allow them to install their own apps. This scenario is particularly useful for hosting providers (Services Provider License Agreement, or SPLA, partners) who want to offer Windows desktops to end customers, given that the Windows client operating system is not offered under SPLA.

> **Note:** PowerShell is required to set up and configure personal session desktops, because session desktops are not integrated into the RDS Server Manager GUI.

Support modern graphics and 3D apps

RemoteFX, which was introduced in Windows Server 2012 to provide virtual graphics card (GPU) acceleration, now supports Windows Server 2016 virtual machines. With support for OpenGL 4.4 and OpenCL 1.1, it can meet the requirements to run modern graphics and 3D apps, such as Adobe Photoshop, Autodesk AutoCAD, and SOLIDWORKS 3D CAD.

For graphics scenarios where RemoteFX capabilities are not sufficient, **Discrete Device Assignment** (DDA) now allows GPUs on a Hyper-V 2016 host to be directly assigned to a virtual machine, unleashing the full power of available graphics processing to virtual desktops that are using the native driver of the GPU. DDA makes it possible to install graphics drivers inside the virtual machine and leverage GPU proprietary technologies (for example, CUDA or GRID). This is useful for apps like CATIA, NX, and Maya.

> **Note:** Service providers building virtual desktop infrastructure solutions can now use Windows Server 2016 inside tenant virtual machines to provide these improved graphics experiences for their customers through SPLA licensing. Windows 10 licenses are not available through SPLA.

Eliminate MultiPoint Server licensing costs

MultiPoint Server was originally developed for educational institutions to give individual users an independent computing experience on shared classroom, lab, and library computers. Unlike a complete RDS deployment, MultiPoint does not require the Remote Desktop Broker or RD Gateway, making it simpler to deploy in all scenarios where multiple users share hardware, including small to medium-size businesses and retail.

With Windows Server 2016, MultiPoint is now a role, not a separate product, and is included in every Datacenter and Standard edition. Microsoft has also removed the 20 users per MultiPoint Server limit, offering organizations more flexibility in deployments.

More cost-effective disaster recovery

In addition to industry-leading scalability, ground-breaking security features, developer innovations, and VDI improvements, Windows Server 2016 also includes new disaster recovery data protection options. Storage Replica in Windows Server 2016 offers replication of data between servers and clusters to keep all nodes in sync, as shown in Figure 5—regardless of whether they are located on-premises or in the cloud.

Storage Replica offers two methods of replication:

- **Synchronous replication** mirrors data on different racks, floors, buildings, campuses, or cities to ensure zero data loss. All data exists on other servers, so if disaster strikes, you can seamlessly switch access to a workload in a safe location.
- **Asynchronous replication** mirrors data across sites over higher latency networks. Because data is continuously replicated, both sites have identical copies of the data at the time of a failure. This means the post-incident changes tend to be fewer than snapshot-based products.

All capabilities of Storage Replica are exposed in virtualized guest and host-based deployments.

Virtual machines can replicate their data volumes in any public clouds or non-Windows virtualization platform. Because data stays on the virtual machine, it is much easier—and less costly—to deploy than disaster recovery solutions that require either additional software licenses or specialized PaaS components to function appropriately.

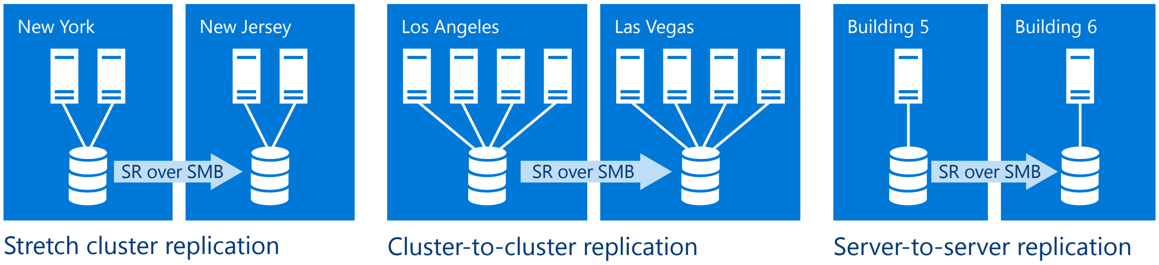

Figure 5. Organizations gain business continuity with Storage Replica, which offers both synchronous and asynchronous replication. Three possible replication scenarios are shown here, including stretch cluster between two sets of storage that are mirrored to allow immediate fail over, cluster to cluster, and server-to-server.

Running workloads on Windows Server 2016 on Azure

As discussed earlier, organizations can capitalize on considerable security, app, and data protection benefits by running workloads on Windows Server 2016 on-premises (VMware vSphere, Hyper-V host, and so on) or in the cloud (AWS, Google) environment. The next sections of this paper show how these benefits increase even more when you choose Windows Server on Microsoft Azure. New improvements for running apps on Windows Server 2016 on Azure include advanced security for virtual machines, improved resiliency scenarios, more consistent management, and simplified licensing, as detailed in Table 3.

Table 3. Additional Windows Server 2016 benefits available on Azure

Windows Server 2016 on Azure benefits		
Additional security for Azure-based virtual machines	• Credential Guard • Device Guard	• Protect user credentials on virtual machines. • Protect kernel-mode processes and drivers against outside influence.
Improved service levels and resiliency	• Storage Spaces Direct • Cloud Witness	• Create instant shared storage for any clustered workload in the cloud. • Provide high availability clustering without requiring more than three on-premises servers.
More consistent management	• Windows Update • PowerShell	• Centralize virtual machine updates. • Maintain desired state configurations for virtual machines.
Simplified and reduced licensing	• Azure Hybrid Benefit and Azure Reserved Virtual Machine Instances	• Cost-effectively transition workloads to the cloud.

Additional security for Azure-based virtual machines

Windows Server 2016 on Azure provides many of the same operating system-level and credential protections that organizations running their app on a Windows Server Hyper-V host can access.

Protect operating system credentials

When running Windows Server 2016 on Azure, organizations have the option to use Credential Guard. This is the same technology available in Windows 10 to protect credentials from being stolen via pass-the-hash, pass-the-ticket, or similar attacks. By isolating credential information of users logging on to Windows Server 2016 virtual machines, Credential Guard can prevent password hashes or Kerberos tickets from being intercepted.

Credential isolation is achieved with an isolated Local Security Authority (LSA) process within the virtual machine, which is not accessible to the rest of the operating system. All binaries used by the isolated LSA are signed with certificates, which are validated before being launched in the protected environment. Pass-the-hash type attacks become completely ineffective because credentials are locked away.

Enhance kernel mode protections

In Azure (or Hyper-V 2016 host environments), Device Guard can be extended to protect kernel mode processes and drivers against attacks from outside the operating system. This is done by using the Device Guard option called Hypervisor Code Integrity (HVCI), which uses Virtualization Based Security to enforce the Device Guard code integrity policy to all software running in kernel mode.

Improve service levels and resiliency

Windows Server 2016 on Azure provides organizations with new opportunities to create highly available, highly resilient apps in the cloud through shared storage and clustering.

Create instant shared storage for virtual machine clusters

Unlike other public cloud solutions, Windows Server 2016 on Azure provides the ability to create virtual shared storage across clustered virtual machines. Storage Spaces Direct uses industry-standard servers with local-attached drives to create highly available, highly scalable software-defined storage at a fraction of the cost of traditional SAN or NAS arrays. Its converged or hyper-converged architecture radically simplifies procurement and deployment, while features like caching, storage tiers, and erasure coding, together with the latest hardware innovations like RDMA networking and NVMe drives, deliver unrivaled efficiency and performance.

Storage Spaces Direct works especially well in Azure, allowing organizations to build highly available software-defined storage systems using local disks. In the past, there was no way to have shared storage outside of virtual hard disk (VHD) sets, which required special configuration on the host. With Storage Spaces Direct, you can have data disks on the virtual machine and can create instant clustered storage for any cluster workloads that want shared storage.

Leverage the cloud for high availability clustering

Cloud Witness is a new type of failover cluster introduced in Windows Server 2016 that leverages Azure as an arbitration point to resolve when and where to fail over. Organizations—particularly small businesses and highly distributed organizations like big retailers—typically rely on one primary server and one backup server. However, high availability clustering requires at least three servers in a quorum so that if one server goes down, the remaining two servers decide which server should pick up the load. Instead of deploying a third server to fill out the quorum, organizations can use Cloud Witness.

Cloud Witness uses minimal bandwidth because it watches only the two on-premises servers and communicates its “vote” if and when one of those servers goes down. Most Cloud Witness servers cost less than one cent a month, so businesses get high availability without a third server and have virtually no annual usage fees.

Consistent management

To innovate quickly, IT needs consistent management tools across on-premises, hybrid, and cloud platforms to ensure their workloads run in strict compliance with their expectations. Windows Server 2016 makes it easier to avoid costly surprises by maintaining consistency over virtual machine configuration, updates, and timing in even the largest cloud deployments.

Maintain Desired State Configuration with PowerShell

Being able to establish a template for virtual machine configuration—and enforce it consistently—is critical to ensuring apps work efficiently. PowerShell 5 and PowerShell Desired State Configuration (DSC) provide the platform to support modern DevOps practices. These features that were previously available only via Windows Management Framework (WMF) 5.0 are built into Windows Server 2016. PowerShell DSC allows you to declaratively specify the configuration of your server in code, ensuring that the changes made in the development environment can be checked in, tracked, and applied through preproduction and production environments consistently.

The ability to use PowerShell for automation is not new, but an emphasis on supporting continuous integration and continuous deployment (CI/CD) environments has driven the addition of tools such as the Pester test framework, remote debugging, support for writing classes in PowerShell, and Package Management. By extending the automation platform well-known to IT pros, these features enable developers and IT to work together in migrating to DevOps practices.

Streamline virtual machine updates

In Windows Server 2016, integration services for Windows guests are distributed through Windows Update. This centralizes control of updates for all your guests in Azure, giving you the ability to update your Windows virtual machines by using a single method.

Save up to 49 percent with hybrid licensing

Windows Server 2016 also makes it much easier to support hybrid environments by allowing server licenses to transfer seamlessly—and cost-effectively—between on-premises and cloud deployments.

The Azure Hybrid Benefit gives organizations the ability to use on-premises Windows Server licenses with Software Assurance (SA) to save up to 49 percent on new Windows Server virtual machines in Azure. This gives organizations flexibility to transition to the cloud at their own pace in a very cost-effective manner. For each eligible Windows Server 2016 Standard license, customers can move or add incremental workloads into Azure across two instances, up to 8 cores each, or one instance of up to 16 cores, and pay only base compute pricing. Datacenter Edition customers also earn the lower-cost instances, but can maintain the existing on-premises deployment.

Combine with Azure Reserved Instances to save up to 80 percent

Reduce your total cost of ownership even more when you reserve Windows virtual machines on Azure for one-year or three-year terms with Azure Reserved Virtual Machine Instances. When combined with the Azure Hybrid Benefit, you can save up to 80 percent, which helps you manage costs across predictable and variable workloads.

Conclusion

Wherever you are in your digital transformation, Windows Server 2016 can help you deliver business value through apps and services across multiple platforms, easily and efficiently. Windows Server 2016 security features improve overall app security on implementation and help reduce organizational risk.[2] Equally as important, new capabilities for developers and IT—from containers to the Nano Server installation option—make it easier to modernize and streamline traditional apps. Operational controls, such as centralized updating and data replication, make IT more efficient while protecting critical business assets.

If your organization is transitioning to the cloud, Azure can provide the advantages of seamlessly transitioning workloads between your on-premises datacenter and the cloud—while still ensuring security compliance and a consistent developer, user, and administrator experience. With Windows Server 2016, you can use one of the most powerful operating systems available for running workloads on-premises or in the cloud to create an innovative, protected hybrid environment.

Use Windows Server licenses in Azure

Bring your existing Windows Server licenses to Azure with the Azure Hybrid Benefit. Now you can use on-premises Windows Server licenses that include Software Assurance to run Windows Server virtual machines in Azure at the base compute rate, saving up to 49 percent. Save even more—up to 80 percent—when you also reserve Azure virtual machines for one-year or three-year terms.

Take the next step.

Learn more at
www.microsoft.com/windowsserver2016

[2] For more information about on Windows Server 2016 security compliance capabilities, visit https://www.microsoft.com/en-us/cloud-platform/windows-server-security#compliance.

Index