What's new in Windows Server 2016

Article • 07/31/2024

This article describes some of the new features in Windows Server 2016 that are the ones most likely to have the greatest impact as you work with this release.

Compute

The Virtualization area includes virtualization products and features for the IT professional to design, deploy, and maintain Windows Server.

General

Physical and virtual machines benefit from greater time accuracy due to improvements in the Win32 Time and Hyper-V Time Synchronization Services. Windows Server can now host services that are compliant with upcoming regulations that require a 1ms accuracy regarding UTC.

Hyper-V

Hyper-V network virtualization (HNV) is a fundamental building block of Microsoft's updated Software Defined Networking (SDN) solution and is fully integrated into the SDN stack. Windows Server 2016 includes the following changes for Hyper-V:

- Windows Server 2016 now includes a programmable Hyper-V switch. Microsoft's Network Controller pushes HNV policies down to a Host Agent running on each host using the Open vSwitch Database Management Protocol (OVSDB) as the SouthBound Interface (SBI). The Host Agent stores this policy using a customization of the VTEP schema and programs complex flow rules into a performant flow engine in the Hyper-V switch. The flow engine in the Hyper-V switch is the same one that Azure uses. The entire SDN stack up through the Network Controller and Network Resource provider is also consistent with Azure, making its performance comparable to the Azure public cloud. Within Microsoft's flow engine, the Hyper-V switch is equipped to handle both stateless and stateful flow rules through a simple match action mechanism that defines how packets should be processed within the switch.
- HNV now supports Virtual eXtensible Local Area Network (VXLAN) protocol encapsulation. HNV uses the VXLAN protocol in MAC distribution mode through the Microsoft Network Controller to map tenant overly network IP addresses to the

physical underlay network IP addresses. The NVGRE and VXLAN Task Offloads support third-party drivers for improved performance.

- Windows Server 2016 includes a software load balancer (SLB) with full support for virtual network traffic and seamless interaction with HNV. The performant flow engine implements the SLB in the data plane v-Switch, then the Network Controller controls it for Virtual IP (VIP) or Dynamic IP (DIP) mappings.

- HNV implements correct L2 Ethernet headers to ensure interoperability with third-party virtual and physical appliances that depend on industry-standard protocols. Microsoft ensures that all transmitted packets have compliant values in all fields to guarantee interoperability. HNV requires support for Jumbo Frames (MTU > 1780) in the physical L2 network to account for packet overhead introduced by encapsulation protocols such as NVGRE and VXLAN. Jumbo Frame support ensures that guest Virtual Machines attached to an HNV Virtual Network maintain a 1514 MTU.

- Windows Container support adds performance improvements, simplified network management, and support for Windows containers on Windows 10. For more information, see our Windows Containers Documentation and Containers: Docker, Windows, and Trends ↗.

- Hyper-V is now compatible with Connected Standby. When you install the Hyper-V role on a computer that uses the Always On/Always Connected (AOAC) power model, you can now configure it to use the Connected Standby power state.

- Discrete device assignment lets you give a virtual machine (VM) direct and exclusive access to certain PCIe hardware devices. This feature bypasses the Hyper-V virtualization stack, which results in faster access. For more information, see Discrete device assignment and Discrete Device Assignment - Description and background ↗.

- Hyper-V now supports BitLocker drive encryption for operating system disks in generation 1 VMs. This protection method replaces virtual Trusted Platform Modules (TPMs), which are only available in generation 2 VMs. To decrypt the disk and start the VM, the Hyper-V host must either be part of an authorized guarded fabric or have the private key from one of the VM's guardians. Key storage requires a version 8 VM. For more information, see Upgrade virtual machine version in Hyper-V on Windows or Windows Server.

- Host resource protection prevents VMs from using too many system resources by tracking excessive levels of activity. When monitoring detects an unusually high activity level in a VM, it throttles the amount of resources the VM consumes. You can enable this feature by running the Set-VMProcessor cmdlet in PowerShell.

- You can now use hot add or remove to add or remove network adapters while the VM is running without downtime in generation 2 VMs running either Linux or Windows operating systems. You can also adjust how much memory is assigned to a VM while it's running even if you haven't enabled Dynamic Memory on both generation 1 and 2 VMs running Windows Server 2016 and later or Windows 10 and later.

- Hyper-V Manager now supports the following features:

  - Alternate credentials, which let you use a different set of credentials in Hyper-V Manager when connecting to another Windows Server 2016 or Windows 10 remote host. You can also save these credentials to make signing in easier.

  - You can now manage Hyper-V on machines running Windows Server 2012 R2, Windows Server 2012, Windows 8.1, and Windows 8.

  - Hyper-V Manager now communicates with remote Hyper-V hosts using the WS-MAN protocol, which permits CredSSP, Kerberos, and NTLM authentication. When you use CredSSP to connect to a remote Hyper-V host, you can perform a live migration without enabling constrained delegation in Active Directory. WS-MAN also makes it easier to enable hosts for remote management. WS-MAN connects over port 80, which is open by default.

- Updates to integration services for Windows guests are now distributed through Windows Update. Service providers and private cloud hosts can give tenants who own the VMs control over applying updates. Windows tenants can now upgrade their VMs with all of the latest updates through a single method. For more information about how Linux tenants can use integration services, see Supported Linux and FreeBSD virtual machines for Hyper-V on Windows Server and Windows.

  > ⓘ **Important**
  >
  > Hyper-V for Windows Server 2016 no longer includes the vmguest.iso image file because it's no longer required.

- Linux operating systems running on generation 2 VMs can now boot with the Secure Boot option enabled. The OSes that support Secure Boot on Windows Server 2016 hosts include Ubuntu 14.04 and later, SUSE Linux Enterprise Server 12 and later, Red Hat Enterprise Linux 7.0 and later, and CentOS 7.0 and later. Before you boot the VM for the first time, you must configure it to use the Microsoft UEFI

Certificate Authority in either Hyper-V Manager, Virtual Machine Manager, or by running the Set-VMFirmware cmdlet in PowerShell.

- Generation 2 VMs and Hyper-V hosts can now use significantly more memory and virtual processors. You can also configure hosts with more memory and virtual processors than previous versions. These changes support scenarios such as running large in-memory databases for online transaction processing (OLTP) and data warehousing (DW) for e-commerce. For more information, see Windows Server 2016 Hyper-V large-scale VM performance for in-memory transaction processing. Learn more about version compatibility and supported maximum configurations at Upgrade virtual machine version in Hyper-V on Windows or Windows Server and Plan for Hyper-V scalability in Windows Server.

- The Nested Virtualization feature lets you use a VM as a Hyper-V host and create VMs within the virtualized host. You can use this feature to build development and test environments running at least Windows Server 2016 or Windows 10 with an Intel VT-x capable processor. For more information, see What is Nested Virtualization?.

- You can now set up production checkpoints to comply with support policies for VMs running production workloads. These checkpoints run on backup technology inside the guest device instead of a saved state. Windows VMs use the Volume Snapshot Service (VSS), while Linux VMs flush file system buffers to create checkpoints that are consistent with the file system. You can still use checkpoints based on save states by using standard checkpoints instead. For more information, see Choose between standard or production checkpoints in Hyper-V.

  > ⓘ **Important**
  >
  > New VMs use production checkpoints as the default.

- You can now resize shared virtual hard disks (`.vhdx` files) for guest clustering without downtime. You can also use guest clusters to protect shared virtual hard disks by using Hyper-V Replica for disaster recovery. You can only use this feature on collections in a guest cluster that you've enabled replication through Windows Management Instrumentation (WMI). For more information, see Msvm_CollectionReplicationService class and Virtual Hard Disk Sharing Overview.

  > ⓘ **Note**

> Managing replication of a collection is not possible via PowerShell cmdlets or using the WMI interface.

- When backing up a single virtual machine, we don't recommend using a VM group or snapshot collection regardless of whether the host is clustered or not. These options are intended for backing up guest clusters that use a shared vhdx. Instead, we recommend taking a snapshot using the Hyper-V WMI provider (V2).

- You can now create shielded Hyper-V VMs that include features that prevent Hyper-V admins on the host or malware from inspecting, tampering with, or stealing data from the shielded VM state. Data and state are encrypted so that Hyper-V admins can't see video output and available disks. You can also restrict the VMs to only run on hosts that a Host Guardian Server has determined are healthy and trustworthy. For more information, see Guarded fabric and shielded VMs overview.

  > ⓘ **Note**
  >
  > Shielded VMs are compatible with Hyper-V Replica. To replicate a shielded virtual machine, you must authorize the host you want to replicate to run that shielded VM.

- The start order priority for clustered virtual machines feature gives you more control over which clustered VMs start or restart first. Deciding start order priority lets you start VMs that provide services before starting VMs that use those services. You can define sets, add VMs to sets, and specify dependencies using PowerShell cmdlets such as New-ClusterGroupSet, Get-ClusterGroupSet, and Add-ClusterGroupSetDependency.

- VM configuration files now use the `.vmcx` file extension format, while runtime state data files use the `.vmrs` file extension format. These new file formats are designed with more efficient reading and writing in mind. The updated formats also decrease the likelihood of data corruption if a storage failure happens.

  > ⓘ **Important**
  >
  > The `.vmcx` file name extension indicates a binary file. Hyper-V for Windows Server 2016 doesn't support editing `.vmcx` or `.vmrs` files.

- We updated version compatibility with version 5 VMs. These VMs are compatible with both Windows Server 2012 R2 and Windows Server 2016. However, version 5 VMs that are compatible with Windows Server 2019 can only run on Windows Server 2016, not Windows Server 2012 R2. If you move or import a Windows Server 2012 R2 VM to a server running a later version of Windows Server, you must manually update the VM configuration to use features for the later versions of Windows Server. For more information about version compatibility and updated features, see Upgrade virtual machine version in Hyper-V on Windows or Windows Server.

- You can now use virtualization-based security features for generation 2 VMs, such as Device Guard and Credential Guard, to protect your OS against malware exploits. These features are available in VMs running version 8 or later. For more information, see Upgrade virtual machine version in Hyper-V on Windows or Windows Server.

- You can now run cmdlets using Windows PowerShell Direct to configure your VM from the host machine as an alternative to VMConnect or Remote PowerShell. You don't need to meet any networking or firewall requirements or have a special remote management configuration in order to start using it. For more information, see Manage Windows virtual machines with PowerShell Direct.

Nano Server

Nano Server now has an updated module for building Nano Server images, including more separation of physical host and guest virtual machine functionality and support for different Windows Server editions. For more information, see Install Nano Server.

There are also improvements to the Recovery Console, including separation of inbound and outbound firewall rules and the ability to repair WinRM configuration.

Shielded Virtual Machines

Windows Server 2016 provides a new Hyper-V-based Shielded Virtual Machine to protect any Generation 2 virtual machine from a compromised fabric. Among the features introduced in Windows Server 2016 are the following:

- A new **Encryption Supported** mode that offers more protections than for an ordinary virtual machine, but less than **Shielded** mode, while still supporting vTPM, disk encryption, Live Migration traffic encryption, and other features, including direct fabric administration conveniences such as virtual machine console connections and PowerShell Direct.

- Full support for converting existing non-shielded Generation 2 virtual machines to shielded virtual machines, including automated disk encryption.

- Hyper-V Virtual Machine Manager can now view the fabrics upon which a shielded virtual is authorized to run, providing a way for the fabric administrator to open a shielded virtual machine's key protector (KP) and view the fabrics it's permitted to run on.

- You can switch Attestation modes on a running Host Guardian Service. Now you can switch on the fly between the less secure but simpler Active Directory-based attestation and TPM-based attestation.

- End-to-end diagnostics tooling based on Windows PowerShell that is able to detect misconfigurations or errors in both guarded Hyper-V hosts and the Host Guardian Service.

- A recovery environment that offers a means to securely troubleshoot and repair shielded virtual machines within the fabric in which they normally run while offering the same level of protection as the shielded virtual machine itself.

- Host Guardian Service support for existing safe Active Directory – you can direct the Host Guardian Service to use an existing Active Directory forest as its Active Directory instead of creating its own Active Directory instance

For more information and instructions for working with shielded virtual machines, see Guarded Fabric and Shielded VMs.

Identity and Access

New features in Identity improve the ability for organizations to secure Active Directory environments and help them migrate to cloud-only deployments and hybrid deployments, where some applications and services are hosted in the cloud and others are hosted on premises.

Active Directory Certificate Services

Active Directory Certificate Services (AD CS) in Windows Server 2016 increases support for TPM key attestation: You can now use Smart Card KSP for key attestation, and devices that aren't joined to the domain can now use NDES enrollment to get certificates that can be attested for keys being in a TPM.

Privileged access management

Privileged access management (PAM) helps mitigate security concerns in Active Directory environments caused by credential theft techniques, such as pass-the-hash, spear phishing, and so on. You can configure this new administrative access solution using Microsoft Identity Manager (MIM), and it introduces the following features:

- The bastion Active Directory forest, provisioned by MIM, has a special PAM trust with an existing forest. Bastion forests are a new type of Active Directory environment that's free of malicious activity due to being isolated from existing forests and only allowing access to privileged accounts.

- New processes in MIM to request administrative privileges, including new workflows for approving requests.

- New shadow security principals, or groups, provisioned in the bastion forest by MIM in response to administrative privilege requests. The shadow security groups have an attribute that references the SID of an administrative group in an existing forest. This allows the shadow group to access resources in existing forests without changing any access control lists (ACLs).

- An expiring links feature, which enables limited time memberships to a shadow group. You can add users to the group for a set amount of time that allows them to perform administrative tasks. The limited time membership is configured by a time-to-live (TTL) value that's propagated to Kerberos ticket lifetime.

  > ⓘ **Note**
  >
  > Expiring links are available on all linked attributes. However, only the *member/memberOF* linked attribute relationship between a group and a user comes preconfigured with PAM to use the expiring links feature.

- Built-in Kerberos Domain Controller (KDC) enhancements allow Active Directory domain controllers to restrict Kerberos ticket lifetimes to the lowest possible TTL value when users have multiple limited-time memberships to administrative groups. For example, if you're a member of time-bound group **A**, then when you sign on, the Kerberos ticket-granting ticket (TGT) lifetime is equal to how much time you have left in group **A**. If you also join time-bound group **B**, which has a lower TTL than group **A**, then your TGT lifetime is equal to how much time you have left in group **B**.

- New monitoring capabilities that let you identify which users requested access, what access the administrators granted to them, and what activities they performed while signed in.

To learn more about PAM, see Privileged Access Management for Active Directory Domain Services.

Microsoft Entra join

Microsoft Entra join enhances identity experiences for enterprise, business, and education customers, as well as including improved capabilities for corporate and personal devices.

- Modern Settings are now available on corporate-owned Windows devices. You no longer need a personal Microsoft account to use core Windows capabilities, and they new run using existing user work accounts to ensure compliance. These services work on PCs joined to an on-premises Windows domain and devices joined to Microsoft Entra. These settings include:
    - Roaming or personalization, accessibility settings, and credentials
    - Back up and restore
    - Access to the Microsoft Store with your work account
    - Live tiles and notifications
- Access organizational resources on mobile devices, such as phones and tablets, that can't be joined to a Windows Domain, whether they're corporate-owned or bring your own device (BYOD).
- Use Single-Sign On (SSO) for Office 365 and other organizational apps, websites, and resources.
- On BYOD devices, add a work account from an on-premises domain or Azure AD to a personally owned device. You can use SSO to access work resources through apps or on the web while remaining compliant with new features such as Conditional Account Control and Device Health attestation.
- Mobile device management (MDM) integration lets you autoenroll devices to your mobile device management (MDM) tool (Microsoft Intune or third-party).
- Set up kiosk mode and shared devices for multiple users in your organization.
- Developer experience lets you build apps that cater to both enterprise and personal contexts with a shared programming stack.
- The imaging option lets you choose between imaging and allowing your users to configure corporate-owned devices directly during the first-run experience.

Windows Hello For Business

Windows Hello for Business is a key-based authentication approach for organizations and consumers that goes beyond passwords. This form of authentication relies on credentials that are resistant to breaches, theft, and phishing.

The user signs in to the device with a biometric or PIN linked to a certificate or an asymmetrical key pair. The Identity Providers (IDPs) validate the user by mapping the public key of the user to IDLocker and provides log on information through One Time Password (OTP), by phone, or a different notification mechanism.

For more information, see Windows Hello for Business.

Deprecation of File Replication Service (FRS) and Windows Server 2003 functional levels

Although File Replication Service (FRS) and the Windows Server 2003 functional levels were deprecated in previous versions of Windows Server, we would like to remind you that AD DS no longer supports Windows Server 2003. You should remove any domain controller that runs Windows Server 2003 from the domain. You should also raise the domain and forest functional level to at least Windows Server 2008.

At the Windows Server 2008 and higher domain functional levels, AD DS uses Distributed File Service (DFS) Replication to replicate SYSVOL folder contents between domain controllers. If you create a new domain at the Windows Server 2008 domain functional level or higher, DFS Replication automatically replicates the SYSVOL folder. If you created the domain at a lower functional level, you must migrate from using FRS to DFS replication for the SYSVOL folder. For more detailed migration steps, see Install, upgrade, or migrate to Windows Server.

For more information, see the following resources:

- Understanding Active Directory Domain Services (AD DS) Functional Levels
- How to raise Active Directory domain and forest functional levels

Active Directory Federation Services

Active Directory Federation Services (AD FS) in Windows Server 2016 includes new features that enable you to configure AD FS to authenticate users stored in Lightweight Directory Access Protocol (LDAP) directories.

Web Application Proxy

The latest version of Web Application Proxy focuses on new features that enable publishing and pre-authentication for more applications and improved user experience. Check out the full list of new features that includes pre-authentication for rich client apps such as Exchange ActiveSync and wildcard domains for easier publishing of SharePoint apps. For more information, see Web Application Proxy in Windows Server 2016.

Administration

The Management and Automation area focuses on tool and reference information for IT pros who want to run and manage Windows Server 2016, including Windows PowerShell.

Windows PowerShell 5.1 includes significant new features, including support for developing with classes and new security features that extend its use, improve its usability, and allow you to control and manage Windows-based environments more easily and comprehensively. See New Scenarios and Features in WMF 5.1 for details.

New additions for Windows Server 2016 include: the ability to run PowerShell.exe locally on Nano Server (no longer remote only), new Local Users & Groups cmdlets to replace the GUI, added PowerShell debugging support, and added support in Nano Server for security logging & transcription and JEA.

Here are some other new administration features:

PowerShell Desired State Configuration (DSC) in Windows Management Framework (WMF) 5

Windows Management Framework 5 includes updates to Windows PowerShell Desired State Configuration (DSC), Windows Remote Management (WinRM), and Windows Management Instrumentation (WMI).

For more info about testing the DSC features of Windows Management Framework 5, see the series of blog posts discussed in Validate features of PowerShell DSC ↗. To download, see Windows Management Framework 5.1.

PackageManagement unified package management for software discovery, installation, and inventory

Windows Server 2016 and Windows 10 includes a new PackageManagement feature (formerly called OneGet) that enables IT Professionals or DevOps to automate software discovery, installation, and inventory (SDII), locally or remotely, no matter what the installer technology is and where the software is located.

For more info, see https://github.com/OneGet/oneget/wiki.

PowerShell enhancements to assist digital forensics and help reduce security breaches

To help the team responsible for investigating compromised systems - sometimes known as the "blue team" - we've added additional PowerShell logging and other digital forensics functionality, and we've added functionality to help reduce vulnerabilities in scripts, such as constrained PowerShell, and secure CodeGeneration APIs.

For more info, see the PowerShell ♥ the Blue Team blog post.

Networking

The Networking area addresses networking products and features for the IT professional to design, deploy, and maintain Windows Server 2016.

Software-Defined Networking

Software-Defined Networking (SDN) is a new Software Defined Datacenter (SDDC) solution that includes the following features:

- Network Controller, which lets you automate the configuration of network infrastructure instead of performing manual configuration of network devices and services. Network Controller uses Representational State Transfer (REST) on its northbound interface with JavaScript Object Notation (JSON) payloads. The Network Controller southbound interface uses Open vSwitch Database Management Protocol (OVSDB).

- New features for Hyper-V:

    - Hyper-V Virtual Switch, which lets you create distributed switching and routing, and a policy enforcement layer that is aligned and compatible with Microsoft Azure. To learn more, see Hyper-V Virtual Switch.

    - Remote direct memory access (RDMA) and switch-embedded teaming (SET) for when you create virtual switches. You can set up RDMA on network adapters bound to a Hyper-V virtual switch regardless of whether you're already using

    SET. SET can give your virtual switches similar capabilities as NIC teaming. For more details, see Host network requirements for Azure Stack HCI.

    - Virtual machine multi-queues (VMMQs) improve on VMQ through put by allocating multiple hardware queues per VM. The default queue becomes a set of queues for a VM and spreads traffic between the queues.

    - Quality of service (QoS) for software-defined networks manages the default class of traffic through the virtual switch within the default class bandwidth.

- Network Function Virtualization (NFV), which lets you mirror or route network functions performed by hardware appliances to virtual appliances, such as load balancers, firewalls, routers, switches, and so on. You can also deploy and manage your entire SDN stack using System Center Virtual Machine Manager. You can manage Windows Server container networking with Docker and associate SDN policies with both virtual machines and containers.

- A Datacenter Firewall that provides granular access control lists (ACLs), enabling you to apply firewall policies at the VM interface level or the subnet level. To learn more, see What is Datacenter Firewall?.

- RAS Gateway, which lets you route traffic between virtual networks and physical networks, including site-to-site VPN connections from your cloud datacenter to your tenants' remote sites. Border Gateway Protocol (BGP) lets you deploy and provide dynamic routing between networks for all gateway scenarios, including Internet Key Exchange version 2 (IKEv2) site-to-site virtual private networks (VPNs), Layer 3 (L3) VPNs, and Generic Routing Encapsulation (GRE) gateways. Gateways now also support gateway pools and M+N redundancy. To learn more, see What is Remote Access Service (RAS) Gateway for Software Defined Networking?.

- Software Load Balancer (SLB) and Network Address Translation (NAT) enhances throughput by supporting Direct Server Return. This allows the return network traffic to bypass the Load Balancing multiplexer, and can be achieved using a north-south and east-west layer 4 load balancer and NAT. To learn more, see What is Software Load Balancer (SLB) for SDN? and Network Function Virtualization.

- Flexible encapsulation technologies that operate at the data plane and support both Virtual Extensible LAN (VxLAN) and Network Virtualization Generic Routing Encapsulation (NVGRE).

For more information, see Plan a Software Defined Network Infrastructure.

Cloud scale fundamentals

Windows Server 2016 includes the following cloud scale fundamentals:

- Converged Network Interface Card (NIC), which lets you use a single network adapter for management, Remote Direct Memory Access (RDMA)-enabled storage, and tenant traffic. A Converged NIC reduces cost for each server in your datacenter because it requires fewer network adapters to manage different types of traffic per server.

- Packet Direct provides a high network traffic throughput and low-latency packet processing infrastructure.

- Switch Embedded Teaming (SET) is a NIC Teaming solution integrated into the Hyper-V Virtual Switch. SET allows the teaming of up to eight physical NICs into a single SET team, which improves availability and provides failover. In Windows Server 2016, you can create SET teams that are restricted to using Server Message Block (SMB) and RDMA. You can also use SET teams to distribute network traffic for Hyper-V Network Virtualization. For more information, see Host network requirements for Azure Stack HCI.

TCP performance improvements

The default Initial Congestion Window (ICW) has been increased from 4 to 10 and TCP Fast Open (TFO) has been implemented. TFO reduces the amount of time required to establish a TCP connection and the increased ICW allows larger objects to be transferred in the initial burst. This combination can significantly reduce the time required to transfer an Internet object between the client and the cloud.

In order to improve TCP behavior when recovering from packet loss, we have implemented TCP Tail Loss Probe (TLP) and Recent Acknowledgment (RACK). TLP helps convert Retransmit TimeOuts (RTOs) to Fast Recoveries and RACK reduces the time required for Fast Recovery to retransmit a lost packet.

Dynamic Host Configuration Protocol (DHCP)

The Dynamic Host Configuration Protocol (DHCP) has the following changes in Windows Server 2016:

- As of Windows 10, version 2004, when you're running a Windows client and connect to the internet using a tethered Android device, the connections are now labeled as metered. The traditional Client Vendor Name that appeared as MSFT 5.0 on certain Windows devices is now MSFT 5.0 XBOX.

- As of Windows 10, version 1803, The DHCP client can now read in and apply option 119, the Domain Search Option, from the DHCP server your system connects to. The Domain Search Option also provides Domain Name Services (DNS) suffixes for DNS lookups of short names. For more information, see RFC 3397.

- DHCP now supports option 82 (sub-option 5). You can use this option to allow DHCP proxy clients and relay agents to request an IP address for a specific subnet. If you're using a DHCP relay agent configured with DHCP option 82 (sub-option 5), the relay agent can request an IP address lease for DHCP clients from a specific IP address range. For more information, see DHCP Subnet Selection Options.

- New logging events for scenarios where DNS record registrations fail on the DNS server. For more information, see DHCP Logging Events for DNS Registrations.

- The DHCP Server role no longer supports Network Access Protection (NAP). DHCP servers don't enforce NAP policies, and DHCP scopes can't be NAP-enabled. DHCP client computers that are also NAP clients send a statement of health (SoH) with the DHCP request. If the DHCP server is running Windows Server 2016, these requests are processed as if no SoH is present. The DHCP server grants a normal DHCP lease to the client. If servers running Windows Server 2016 are Remote Authentication Dial-In User Service (RADIUS) proxies that forward authentication requests to a Network Policy Server (NPS) that supports NAP, the NPS evaluates these clients as non-NAP capable, causing NAP processing to fail. For more information about NAP and NAP deprecation, see Features Removed or Deprecated in Windows Server 2012 R2.

GRE tunneling

RAS Gateway now supports high availability Generic Routing Encapsulation (GRE) tunnels for site-to-site connections and M+N redundancy of gateways. GRE is a lightweight tunneling protocol that encapsulates a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol internetwork. For more information, see GRE Tunneling in Windows Server 2016.

IP Address Management (IPAM)

IPAM has the following updates:

- Enhanced IP address management. IPAM has improved capabilities for scenarios such as handling IPv4 /32 and IPv6 /128 subnets and finding free IP address subnets and ranges in an IP address block.

- You can now run the `Find-IpamFreeSubnet` cmdlet to find available subnets for allocation. This function doesn't allocate the subnets, only reports their availability. However, you can pipe the cmdlet output to the `Add-IpamSubnet` cmdlet to create a subnet. For more information, see Find-IpamFreeSubnet.

- You can now run the `Find-IpamFreeRange` cmdlet to find available IP address ranges within an IP block, prefix length, and number of requested subnets. This cmdlet doesn't allocate the IP address range, only reports their availability. However, you can pipe the output into the `AddIpamRange` cmdlet to create the range. For more information, see Find-IpamFreeRange.

- Enhanced DNS service management:

  - DNS resource records collection for non-DNSSEC DNS servers.

  - Configuring properties and operations on all types of non-DNSSEC Resource Records.

  - DNS zone management for both domain-joined Active Directory-integrated and file-backed DNS servers. You can manage all types of DNS zones, including Primary, Secondary, and Stub zones.

  - Trigger tasks on Secondary and Stub zones regardless of whether they're forward or reverse lookup zones.

  - Role-based access control for supported DNS configurations for records and zones.

  - Conditional forwarders

- Integrated DNS, DHCP, and IP address (DDI) management. You can now view all DNS resource records associated with an IP address in the IP Address Inventory. You can also automatically keep pointer (PTR) records of IP addresses and manage IP address lifecycles for both DNS and DHCP operations.

- Multiple Active Directory Forest support. You can use IPAM to manage the DNS and DHCP servers of multiple Active Directory forests when there's a two-way trust relationship between the forest where you installed IPAM and each of the remote forests. For more information, see Manage Resources in Multiple Active Directory Forests.

- The Purge Utilization Data feature lets you reduce IPAM database size by deleting old IP utilization data. Just specify a date and IPAM deletes all database entries older than or equal to the date you entered. For more information, see Purge Utilization Data.

- You can now use Role Based Access Control (RBAC) to define access scopes for IPAM objects in PowerShell. For more information, see Manage Role Based Access Control with Windows PowerShell and IP Address Management (IPAM) Server Cmdlets in Windows PowerShell.

For more information, see Manage IPAM.

Security and Assurance

The Security and Assurance area Includes security solutions and features for the IT professional to deploy in your data center and cloud environment. For information about security in Windows Server 2016 generally, see Security and Assurance.

Just Enough Administration

Just Enough Administration in Windows Server 2016 is security technology that enables delegated administration for anything that can be managed with Windows PowerShell. Capabilities include support for running under a network identity, connecting over PowerShell Direct, securely copying files to or from JEA endpoints, and configuring the PowerShell console to launch in a JEA context by default. For more information, see JEA on GitHub.

Credential Guard

Credential Guard uses virtualization-based security to isolate secrets so that only privileged system software can access them. For more information, see Protect derived domain credentials with Credential Guard.

Credential Guard for Windows Server 2016 includes the following updates for signed-in user sessions:

- Kerberos and New Technology LAN Manager (NTLM) use virtualization-based security to protect Kerberos and NTLM secrets for signed-in user sessions.

- Credential Manager protects saved domain credentials using virtualization-based security. Signed-in credentials and saved domain credentials don't pass to remote hosts using Remote Desktop.

- You can enable Credential Guard without a Unified Extensible Firmware Interface (UEFI) lock.

Remote Credential Guard

Credential Guard includes support for RDP sessions so that the user credentials remain on the client side and aren't exposed on the server side. This also provides Single Sign On for Remote Desktop. For more information, see Protect derived domain credentials with Windows Defender Credential Guard.

Remote Credential Guard for Windows Server 2016 includes the following updates for signed-in users:

- Remote Credential Guard keeps Kerberos and NTLM secrets for signed-in user credentials on the client device. Any authentication requests from the remote host for assessing network resources as the user require the client device to use the secrets.

- Remote Credential Guard protects supplied user credentials when using Remote Desktop.

Domain protections

Domain protections now require an Active Directory domain.

PKInit Freshness extension support

Kerberos clients now attempt the PKInit freshness extension for public key based sign-ons.

KDCs now support the PKInit freshness extension. However, they don't offer the PKInit freshness extension by default.

For more information, see Kerberos client and KDC support for RFC 8070 PKInit freshness extension.

Rolling public key only user's NTLM secrets

Starting with the Windows Server 2016 domain functional level (DFL), DCs now support rolling the NTLM secrets of a public-key-only user. This feature is unavailable in lower domain functioning levels (DFLs).

> ⚠ Warning
>
> Adding a DC enabled before the November 8, 2016 update to a domain that supports rolling NTLM secrets can cause the DC to crash.

For new domains, this feature is enabled by default. For existing domains, you must configure it in the Active Directory Administrative Center.

From the Active Directory Administrative Center, right-click on the domain in the left pane and select **Properties**. Select the checkbox **Enable rolling of expiring NTLM secrets during sign on for users who are required to use Windows Hello for Business or smart card for interactive logon**. After that, select **OK** to apply this change.

Allowing network NTLM when user is restricted to specific domain-joined devices

DCs can now support allowing network NTLM when a user is restricted to specific domain-joined devices in the Windows Server 2016 DFL and higher. This feature is unavailable in DFLs running an earlier operating system than Windows Server 2016.

To configure this setting, in the authentication policy, select **Allow NTLM network authentication when the user is restricted to selected devices**.

For more information, see Authentication policies and authentication policy silos.

Device Guard (Code Integrity)

Device Guard provides kernel mode code integrity (KMCI) and user mode code integrity (UMCI) by creating policies that specify what code can run on the server. See Introduction to Windows Defender Device Guard: virtualization-based security and code integrity policies.

Windows Defender

Windows Defender Overview for Windows Server 2016. Windows Server Antimalware is installed and enabled by default in Windows Server 2016, but the user interface for Windows Server Antimalware isn't installed. However, Windows Server Antimalware will update antimalware definitions and protect the computer without the user interface. If you need the user interface for Windows Server Antimalware, you can install it after the operating system installation by using the Add Roles and Features Wizard.

Control Flow Guard

Control Flow Guard (CFG) is a platform security feature that was created to combat memory corruption vulnerabilities. See Control Flow Guard for more information.

Storage

Storage in Windows Server 2016 includes new features and enhancements for software-defined storage and traditional file servers.

Storage Spaces Direct

Storage Spaces Direct enables building highly available and scalable storage using servers with local storage. It simplifies deploying and managing software-defined storage systems and lets you use new classes of disk devices, such as SATA SSDs and NVMe disk devices, that previously weren't available with clustered Storage Spaces with shared disks.

For more details, see Storage Spaces Direct.

Storage Replica

Storage Replica enables storage-agnostic, block-level, synchronous replication between servers or clusters for disaster recovery, and lets you stretch a failover cluster between sites. Synchronous replication enables mirroring of data in physical sites with crash-consistent volumes to ensure zero data loss at the file-system level. Asynchronous replication allows site extension beyond metropolitan ranges with the possibility of data loss.

For more info, see Storage Replica.

Storage Quality of Service (QoS)

You can now use storage quality of service (QoS) to centrally monitor end-to-end storage performance and create management policies using Hyper-V and CSV clusters in Windows Server 2016.

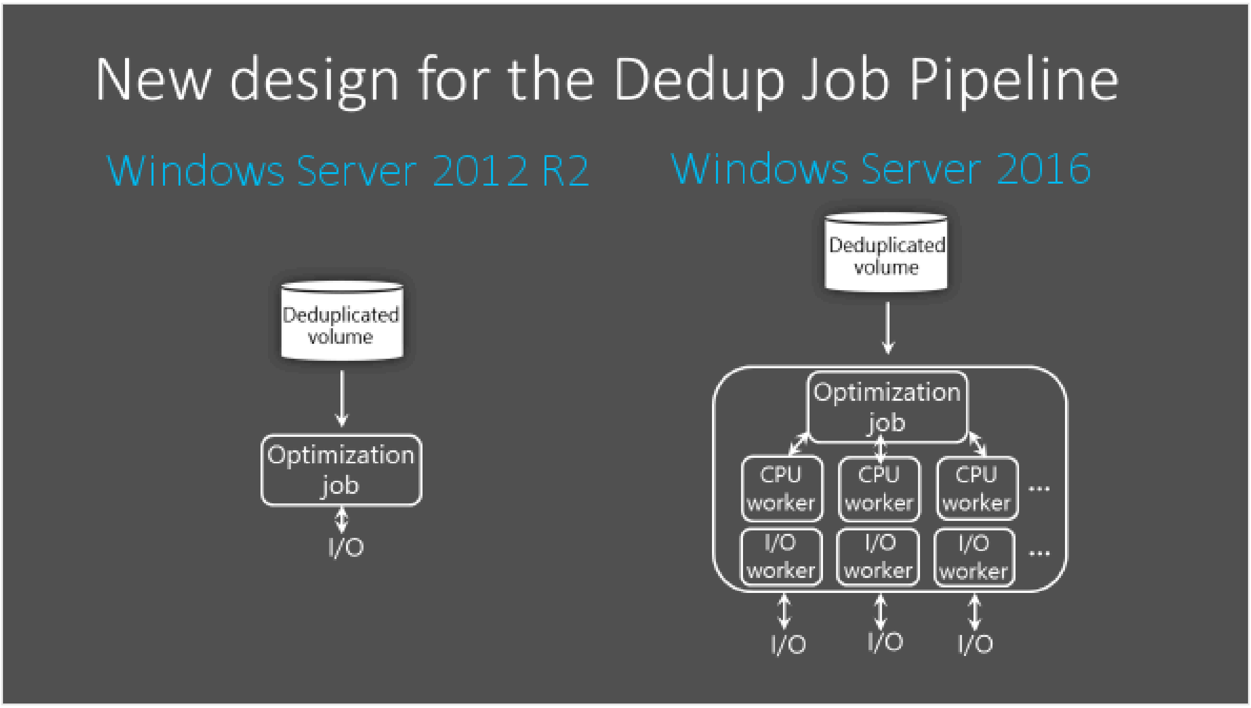
For more info, see Storage Quality of Service.

Data deduplication

Windows Server 2016 includes the following new features for data deduplication.

Support for large volumes

Starting with Windows Server 2016, the Data Deduplication Job pipeline can now run multiple threads in parallel using many I/O queues for each volume. This change increases performance to levels previously only possible by dividing data into several smaller volumes. These optimizations apply to all Data Deduplication Jobs, not just the Optimization Job. The following diagram demonstrates how the pipeline changed between versions of Windows Server.



Because of these performance improvements, on Windows Server 2016, Data Deduplication has high performance on volumes up to 64 TB.

Large file support

As of Windows Server 2016, Data Deduplication uses stream map structures and other improvements to increase optimization throughput and access performance. The Deduplication Processing Pipeline can also resume optimization after failover scenarios instead of starting over from the beginning. This change improves the performance of files up to 1 TB, allowing administrators to apply deduplication savings to a larger range of workloads, such as large files associated with backup workloads.

Support for Nano Server

Nano Server is a headless deployment option in Windows Server 2016 that requires a far smaller system resource footprint, starts up significantly faster, and requires fewer updates and restarts than the Windows Server Core deployment option. Nano Server also fully supports Data Deduplication. For more information about Nano Server, see Container Base Images.

Simplified configuration for Virtualized Backup Applications

Starting with Windows Server 2016, Data Deduplication for Virtualized Backup Applications scenarios are vastly simplified. This scenario is now a predefined Usage Type option. You no longer need to manually tune the deduplication settings, just enable Deduplication for a volume just like you would General Purpose File Server and Virtual Desktop Infrastructure (VDI).

Cluster OS Rolling Upgrade support

Windows Server Failover Clusters running Data Deduplication can have a mix of nodes that run the Windows Server 2012 R2 and Windows Server 2016 versions of Data Deduplication. This mixed-mode cluster feature gives full data access to all deduplicated volumes during cluster rolling upgrades. You can now gradually roll out later versions of Data Deduplications on clusters running earlier versions of Windows Server without any downtime.

You can also now use rolling upgrades on Hyper-V. With Rolling Hyper-V Cluster upgrade, you can now add a node running Windows Server 2019 or Windows Server 2016 to a Hyper-V Cluster with nodes running Windows Server 2012 R2. After you add the node running the later version of Windows Server, you can upgrade the rest of the cluster without downtime. The cluster runs at a Windows Server 2012 R2 feature level until you upgrade all nodes in the cluster and run the Update-ClusterFunctionalLevel in PowerShell to update the cluster functioning level. For more detailed instructions for how the rolling upgrade process works, see Cluster Operating System Rolling Upgrade.

> **Note**
>
> Hyper-V on Windows 10 doesn't support failover clustering.

SMB hardening improvements for SYSVOL and NETLOGON connections

In Windows 10 and Windows Server 2016, client connections to the Active Directory Domain Services used SYSVOL and NETLOGON shares on domain controllers by default. Now these connections require SMB signing and mutual authentication using services such as Kerberos. If SMB signing and mutual authentication are unavailable, a Windows 10 or Windows Server 2016 computer won't process domain-based Group Policy and scripts. This change protects devices from adversary-in-the-middle attacks.

> ⓘ **Note**
>
> The registry values for these settings aren't present by default, but the hardening rules still apply until you override them by editing Group Policy or other registry values.

For more information on these security improvements, see MS15-011: Vulnerability in Group Policy and MS15-011 & MS15-014: Hardening Group Policy.

Work Folders

Windows Server 2016 features improved change notification when the Work Folders server is running Windows Server 2016 and the Work Folders client is Windows 10. When file changes sync to the Work Folders server, the server now immediately notifies Windows 10 clients, then syncs the file changes.

ReFS

The next iteration of ReFS provides support for large-scale storage deployments with diverse workloads, delivering reliability, resiliency, and scalability for your data.

ReFS introduces the following improvements:

- New storage tier functionality, delivering faster performance and increased storage capacity, including the following:
  - Multiple resiliency types on the same virtual disk using mirroring in the performance tier and parity in the capacity tier.
  - Increased responsiveness to drifting working sets.
- Introduces block cloning to improve performance of VM operations, such as `.vhdx` checkpoint merge operations.

- A new ReFS scan tool that can help you recover leaked storage and salvage data from critical corruptions.

Failover Clustering

Windows Server 2016 includes many new features and enhancements for multiple servers that are grouped together into a single fault-tolerant cluster using the Failover Clustering feature.

Cluster Operating System Rolling Upgrade

Cluster Operating System Rolling Upgrade enables an administrator to upgrade the operating system of the cluster nodes from Windows Server 2012 R2 to Windows Server 2016 without stopping the Hyper-V or Scale-Out File Server workloads. You can use this feature to avoid downtime penalties against Service Level Agreements (SLAs).

For more information, see Cluster Operating System Rolling Upgrade.

Cloud Witness

Cloud Witness is a new type of Failover Cluster quorum witness in Windows Server 2016 that leverages Microsoft Azure as the arbitration point. The Cloud Witness, like any other quorum witness, gets a vote and can participate in quorum calculations. You can configure Cloud Witness as a quorum witness using the Configure a Cluster Quorum wizard.

For more information, see Deploy Cloud Witness for a failover cluster.

Virtual Machine resiliency

Windows Server 2016 includes increased virtual machine (VM) compute resiliency to help reduce intra-cluster communication issues in your compute cluster. This increased resiliency includes the following updates:

- You can now configure the following options to define how the VMs should behave during transient failures:
  - **Resiliency Level** defines how your deployment should handle transient failures.
  - **Resiliency Period** defines how long all VMs are allowed to run isolated.

- Unhealthy nodes are quarantined and are no longer allowed to join the cluster. This feature prevents unhealthy nodes from negatively affecting other nodes and the overall cluster.

For more information about compute resiliency features, see Virtual Machine Compute Resiliency in Windows Server 2016 .

Windows Server 2016 VMs also include new storage resiliency features for handling transient storage failures. Improved resiliency helps preserve tenant VM session states in the event of a storage disruption. When a VM disconnects from its underlying storage, it pauses and waits for storage to recover. While paused, the VM retains the context of applications that were running in it at the time of the storage failure. When the connection between the VM and storage is restored, the VM returns to its running state. As a result, the tenant machine's session state is retained on recovery.

The new storage resiliency features also apply to guest clusters.

Diagnostic improvements

To help diagnose issues with failover clusters, Windows Server 2016 includes the following:

- Several enhancements to cluster log files, such as Time Zone Information and DiagnosticVerbose log, make it easier to troubleshoot failover clustering issues. For more information, see Windows Server 2016 Failover Cluster Troubleshooting Enhancements - Cluster Log .

- A new type of active memory dump filters out most memory pages allocated to VMs, making the memory.dmp file much smaller and easier to save or copy. For more information, see Windows Server 2016 Failover Cluster Troubleshooting Enhancements - Active Dump .

Site-aware failover clusters

Windows Server 2016 includes site-aware failover clusters that enable group nodes in stretched clusters based on their physical location, or site. Cluster site-awareness enhances key operations during the cluster lifecycle, such as failover behavior, placement policies, heartbeat between the nodes, and quorum behavior. For more information, see Site-aware Failover Clusters in Windows Server 2016 .

Workgroup and Multi-domain clusters

In Windows Server 2012 R2 and earlier, a cluster can only be created between member nodes joined to the same domain. Windows Server 2016 breaks down these barriers and introduces the ability to create a Failover Cluster without Active Directory dependencies. You can now create failover clusters in the following configurations:

- Single-domain Clusters, which have all their nodes joined to the same domain.
- Multi-domain Clusters, which have nodes that are members of different domains.
- Workgroup Clusters, which have nodes that are member servers or workgroups that aren't domain-joined.

For more information, see Workgroup and Multi-domain clusters in Windows Server 2016

Virtual Machine Load Balancing

Virtual Machine Load Balancing is a new feature in Failover Clustering that seamlessly load balances VMs across the nodes in a cluster. The feature identifies overcommitted nodes based on VM memory and CPU utilization on the node. It then live migrates the VMs from the overcommitted node to nodes with available bandwidth. You can adjust how aggressively the feature balances nodes to ensure optimal cluster performance and utilization. Load Balancing is enabled by default in Windows Server 2016 Technical Preview. However, Load Balancing is disabled when SCVMM Dynamic Optimization is enabled.

Virtual Machine Start Order

Virtual machine Start Order is a new feature in Failover Clustering that introduces start order orchestration for VMs and other groups in a cluster. You can now group VMs into tiers, then create start order dependencies between different tiers. These dependencies ensure that the most important VMs, such as Domain Controllers or Utility VMs, start up first. VMs on lower-priority tiers don't start until after the VMs that they have a dependency on startup.

Simplified SMB Multichannel and Multi-NIC Cluster Networks

Failover cluster networks are no longer limited to a single network interface card (NIC) per subnet or network. With Simplified Server Message Block (SMB) Multichannel and Multi-NIC Cluster Networks, network configuration is automatic and every NIC on the subnet can be used for cluster and workload traffic. This enhancement allows customers to maximize network throughput for Hyper-V, SQL Server Failover Cluster Instance, and other SMB workloads.

For more information, see Simplified SMB Multichannel and Multi-NIC Cluster Networks.

Application development

Internet Information Services (IIS) 10.0

New features provided by the IIS 10.0 web server in Windows Server 2016 include:

- Support for the HTTP/2 protocol in the Networking stack and integrated with IIS 10.0, allowing IIS 10.0 websites to automatically serve HTTP/2 requests for supported configurations. This allows numerous enhancements over HTTP/1.1 such as more efficient reuse of connections and decreased latency, improving load times for web pages.
- Ability to run and manage IIS 10.0 in Nano Server. See IIS on Nano Server.
- Support for Wildcard Host Headers, enabling administrators to set up a web server for a domain and then have the web server serve requests for any subdomain.
- A new PowerShell module (IISAdministration) for managing IIS.

For more details, see IIS .

Distributed Transaction Coordinator (MSDTC)

Three new features are added in Microsoft Windows 10 and Windows Server 2016:

- A new interface for Resource Manager Rejoin can be used by a resource manager to determine the outcome of an in-doubt transaction after a database restarts due to an error. See IResourceManagerRejoinable::Rejoin for details.

- The DSN name limit is enlarged from 256 bytes to 3,072 bytes. See IDtcToXaHelperFactory::Create, IDtcToXaHelperSinglePipe::XARMCreate, or IDtcToXaMapper::RequestNewResourceManager for details.

- Improved tracing allowing you to set a registry key to include an image file path in the Tracelog file name so you can tell which Tracelog file to check. See How to enable diagnostic tracing for MS DTC on a Windows-based computer for details on configuring tracing for MSDTC.

DNS Server

Windows Server 2016 contains the following updates for Domain Name System (DNS) Server.

DNS policies

You can configure DNS policies to specify how a DNS server responds to DNS queries. You can configure DNS responses based on client IP address, time of day, and several other parameters. DNS policies can enable location-aware DNS, traffic management, load balancing, split-brain DNS, and other scenarios. For more information, see the DNS Policy Scenario Guide.

RRL

You can enable Response Rate Limiting (RRL) on your DNS servers to prevent malicious systems from using your DNS servers to initiate a Distributed Denial of Service (DDoS) attack on a DNS client. RRL prevents your DNS server from responding to too many requests at once, which protects it during scenarios when a botnet sends multiple requests at once to try to disrupt server operations.

DANE support

You can use DNS-based Authentication of Named Entities (DANE) support (RFC 6394 and RFC 6698) to specify which certificate authority your DNS clients should expect certificates from for domain names hosted in your DNS server. This prevents a form of man-in-the-middle attack where a malicious actor corrupts a DNS cache and points a DNS name to their own IP address.

Unknown record support

You can add records that the DNS server doesn't explicitly support by using the unknown record functionality. A record is unknown when the DNS server doesn't recognize its RDATA format. Windows Server 2016 supports unknown record types (RFC 3597), so you can add unknown records to Windows DNS server zones in binary on-wire format. The windows caching resolver can already process unknown record types. Windows DNS server doesn't perform record-specific processing for unknown records, but can send them in response to queries it receives.

IPv6 root hints

Windows DNS server now includes IPv6 root hints published by the Internet Assigned Numbers Authority (IANA). Support for IPv6 root hints lets you make internet queries that use the IPv6 root servers to perform name resolutions.

Windows PowerShell support

Windows Server 2016 includes new commands you can use to configure DNS in PowerShell. For more information, see Windows Server 2016 DnsServer module and Windows Server 2016 DnsClient module.

Nano Server support for file-based DNS

You can deploy DNS servers in Windows Server 2016 on a Nano Server image. This deployment option is available if you're using file-based DNS. By running DNS server on a Nano Server image, you can run your DNS servers with reduced footprint, quick boot up, and minimal patching.

> ⓘ Note
>
> Active Directory integrated DNS is not supported on Nano Server.

DNS client

The DNS client service now offers enhanced support for computers with more than one network interface.

Multi-homed computers can also use DNS client service binding to improve server resolution:

- When you use a DNS server configured on a specific interface to resolve a DNS query, the DNS client binds to the interface before sending the query. This binding lets the DNS client specify the interface where name resolution should take place, optimizing communications between applications and DNS client over the network interface.

- If the DNS server you're using was designated by a Group Policy setting from the Name Resolution Policy Table (NRPT), the DNS client service doesn't bind to the specified interface.

> ⓘ Note

Changes to the DNS Client service in Windows 10 are also present in computers running Windows Server 2016 and later.

Remote Desktop Services

Remote Desktop Services (RDS) made the following changes for Windows Server 2016.

App compatibility

RDS and Windows Server 2016 are compatible with many Windows 10 applications, creating a user experience that's almost identical to a physical desktop.

Azure SQL Database

The Remote Desktop (RD) Connection Broker can now store all deployment information, such as connection states and user-host mappings, in a shared Azure Structured Query Language (SQL) Database. This feature lets you use a highly available environment without having to use an SQL Server Always On Availability Group. For more information, see Use Azure SQL DB for your Remote Desktop Connection Broker high availability environment.

Graphical improvements

Discrete Device Assignment for Hyper-V lets you map graphics processing units (GPUs) on a host machine directly to a virtual machine (VM). Any applications on the VM that need more GPU than the VM can provide can use the mapped GPU instead. We also improved the RemoteFX vGPU, including support for OpenGL 4.4, OpenCL 1.1, 4K resolution, and Windows Server VMs. For more information, see Discrete Device Assignment.

RD Connection Broker improvements

We improved how the RD Connection Broker handles connection during logon storms, which are periods of high sign in requests from users. The RD Connection Broker can now handle over 10,000 concurrent sign in requests! Maintenance improvements also make it easier for you to perform maintenance on your deployment by being able to quickly add servers back into the environment once they're ready to go back online. For more information, see Improved Remote Desktop Connection Broker Performance.

RDP 10 protocol changes

Remote Desktop Protocol (RDP) 10 now uses the H.264/AVC 444 codec, which optimizes across both video and text. This release also includes pen remoting support. These new capabilities allow your remote session to feel more like a local session. For more information, see RDP 10 AVC/H.264 improvements in Windows 10 and Windows Server 2016.

Personal session desktops

Personal session desktops is a new feature that lets you host your own personal desktop in the cloud. Administrative privileges and dedicated session hosts removes the complexity of hosting environments where users want to manage a remote desktop like a local desktop. For more information, see Personal Session Desktops.

Kerberos authentication

Windows Server 2016 includes the following updates for Kerberos authentication.

KDC support for Public Key Trust-based client authentication

Key Distribution Centers (KDCs) now support public key mapping. If you provision a public key for an account, the KDC supports Kerberos PKInit explicitly using that key. Because there's no certificate validation, Kerberos supports self-signed certificates but doesn't support authentication mechanism assurance.

Accounts you've configured to use Key Trust will only use Key Trust regardless of how you configured the UseSubjectAltName setting.

Kerberos client and KDC support for RFC 8070 PKInit Freshness Extension

Starting with Windows 10, version 1607 and Windows Server 2016, Kerberos clients can use the RFC 8070 PKInit freshness extension for public key-based sign-ons. KDCs have the PKInit freshness extension disabled by default, so to enable it you must configure the KDC support for PKInit Freshness Extension KDC administrative template policy on all DCs in your domain.

The policy has the following settings available when your domain is in the Windows Server 2016 domain functional level (DFL):

- **Disabled**: The KDC never offers the PKInit Freshness Extension and accepts valid authentication requests without checking for freshness. Users don't receive the fresh public key identity SID.
- **Supported**: Kerberos supports PKInit Freshness Extension on request. Kerberos clients successfully authenticating with the PKInit Freshness Extension receive the fresh public key identity SID.
- **Required**: PKInit Freshness Extension is required for successful authentication. Kerberos clients that don't support the PKInit Freshness Extension will always fail when using public key credentials.

Domain-joined device support for authentication using public key

If a domain-joined device can register its bound public key with a Windows Server 2016 domain controller (DC), then the device can authenticate with the public key using Kerberos PKInit authentication to a Windows Server 2016 DC.

Domain-joined devices with bound public keys registered with a Windows Server 2016 domain controller can now authenticate to a Windows Server 2016 domain controller using Kerberos Public Key Cryptography for Initial Authentication (PKInit) protocols. To learn more, see Domain-joined Device Public Key Authentication.

Key Distribution Centers (KDCs) now support authentication using Kerberos key trust.

For more information, see KDC support for Key Trust account mapping.

Kerberos clients allow IPv4 and IPv6 address host names in Service Principal Names (SPNs)

Starting with Windows 10 version 1507 and Windows Server 2016, you can configure Kerberos clients to support IPv4 and IPv6 host names in SPNs. For more information, see Configuring Kerberos for IP Addresses.

To configure support for IP address host names in SPNs, create a TryIPSPN entry. This entry doesn't exist in the registry by default. You should place this entry on the following path:

```
text
```

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Kerberos\Para
meters
```

After creating the entry, change its DWORD value to 1. If this value isn't configured, Kerberos won't attempt IP address host names.

Kerberos authentication only succeeds if the SPN is registered in Active Directory.

KDC support for Key Trust account mapping

Domain controllers now support Key Trust account mapping and fallback to existing AltSecID and User Principal Name (UPN) in the SAN behavior. You can configure the UseSubjectAltName variable to the following settings:

- Setting the variable to 0 makes explicit mapping required. Users must use either a Key Trust or set an ExplicitAltSecID variable.
- Setting the variable to 1, which is the default value, allows implicit mapping.
  - If you configure a Key Trust for an account in Windows Server 2016 or later, then KDC uses the KeyTrust for mapping.
  - If there's no UPN in the SAN, KDC attempts to use the AltSecID for mapping.
  - If there's a UPN in the SAN, KDC attempts to use the UPN for mapping.

Active Directory Federation Services (AD FS)

AD FS for Windows Server 2016 contains the following updates.

Sign in with Microsoft Entra multifactor authentication

AD FS 2016 builds upon the multifactor authentication (MFA) capabilities of AD FS in Windows Server 2012 R2. You can now allow sign-on that only requires a Microsoft Entra multifactor authentication code instead of a username or password.

- When you configure Microsoft Entra multifactor authentication as the primary authentication method, AD FS prompts the user for their username and the one-time password (OTP) code from the Azure Authenticator app.
- When you configure Microsoft Entra multifactor authentication as the secondary or extra authentication method, the user provides primary authentication credentials. Users can sign in by using Windows Integrated Authentication, which can request

their username and password, smart card, or a user or device certificate. Next, the user sees a prompt for their secondary credentials, such as text, voice, or OTP-based Microsoft Entra multifactor authentication sign-in.

- The new built-in Microsoft Entra multifactor authentication adapter offers simpler setup and configuration for Microsoft Entra multifactor authentication with AD FS.
- Organizations can use Microsoft Entra multifactor authentication without needing an on-premises Microsoft Entra multifactor authentication server.
- You can configure Microsoft Entra multifactor authentication for intranet, extranet, or as part of any access control policy.

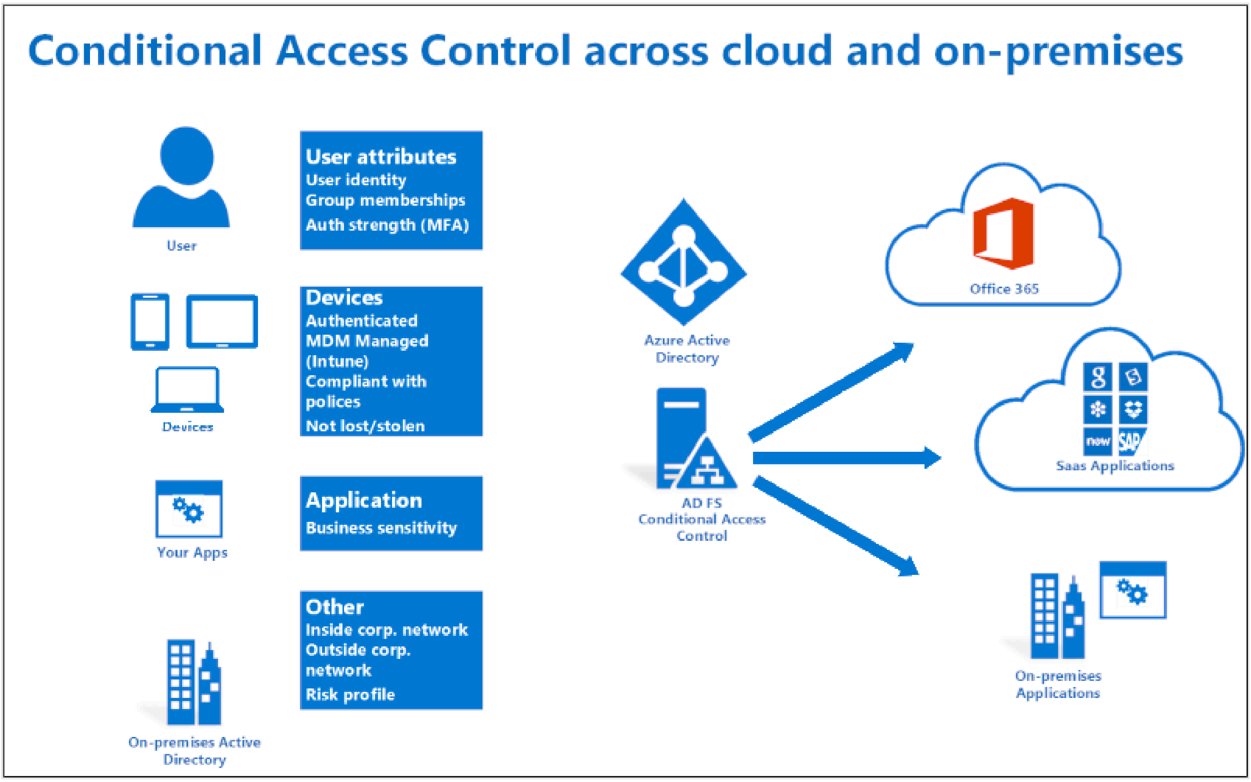
For more information about Microsoft Entra multifactor authentication with AD FS, see Configure AD FS 2016 and Microsoft Entra multifactor authentication.

Passwordless access from compliant devices

AD FS 2016 builds on previous device registration capabilities to enable sign-on and access control on devices based on their compliance status. Users can sign on using the device credential, and AD FS reevaluates compliance whenever device attributes change to ensure policies are being enforced. This feature enables the following policies:

- Enable Access only from devices that are managed and/or compliant.
- Enable Extranet Access only from devices that are managed and/or compliant.
- Require multifactor authentication for computers that aren't managed or compliant.

AD FS provides the on-premises component of conditional access policies in a hybrid scenario. When you register devices with Azure AD for conditional access to cloud resources, you can also use the device identity for AD FS policies.



For more information about using device based conditional access in the cloud, see Azure Active Directory Conditional Access.

For more information about using device based conditional access with AD FS, see Planning for Device Based Conditional Access with AD FS and Access Control Policies in AD FS.

Sign in with Windows Hello for Business

Windows 10 devices introduce Windows Hello and Windows Hello for Business, replacing user passwords with strong device-bound user credentials protected by a user's gesture, such as entering a PIN, a biometric gesture like a fingerprint, or facial recognition. With Windows Hello, users can sign in to AD FS applications from an intranet or extranet without requiring a password.

For more information about using Windows Hello for Business in your organization, see Enable Windows Hello for Business in your organization.

Modern authentication

AD FS 2016 supports the latest modern protocols that provide a better user experience for Windows 10 and the latest iOS and Android devices and apps.

For more information, see AD FS Scenarios for Developers.

Configure access control policies without having to know claim rules language

Previously, AD FS administrators had to configure policies by using the AD FS claim rule language, making it difficult to configure and maintain policies. With access control policies, administrators can use built-in templates to apply common policies. For example, you can use templates to apply the following policies:

- Permit intranet access only.
- Permit everyone and require MFA from extranet.
- Permit everyone and require MFA from a specific group.

The templates are easy to customize. You can apply extra exceptions or policy rules, and you can apply these changes to one or more applications for consistent policy enforcement.

For more information, see Access control policies in AD FS.

Enable sign on with non-AD LDAP directories

Many organizations combine Active Directory with third-party directories. AD FS support for authenticating users stored in Lightweight Directory Access Protocol (LDAP) v3-compliant directories means you can now use AD FS in the following scenarios:

- Users in third party, LDAP v3-compliant directories.
- Users in Active Directory forests that don't have a configured Active Directory two-way trust.
- Users in Active Directory Lightweight Directory Services (AD LDS).

For more information, see Configure AD FS to authenticate users stored in LDAP directories.

Customize sign in experience for AD FS applications

Previously, AD FS in Windows Server 2012 R2 provided a common sign-on experience for all relying party applications, with the ability to customize a subset of text-based content per application. With Windows Server 2016, you can customize not only the messages, but images, logo and web theme per application. Additionally, you can create new, custom web themes and apply these themes per relying party.

For more information, see AD FS user sign-in customization.

Streamlined auditing for easier administrative management

In previous versions of AD FS, a single request could generate many audit events. Relevant information about sign-in or token issuance activities were often absent or spread across multiple audit events, making issues harder to diagnose. As a result, audit events were turned off by default. However, in AD FS 2016, the auditing process is more streamlined and relevant information easier to find. For more information, see Auditing enhancements to AD FS in Windows Server 2016.

Improved interoperability with SAML 2.0 for participation in confederations

AD FS 2016 contains more SAML protocol support, including support for importing trusts based on metadata that contains multiple entities. This change enables you to configure AD FS to participate in confederations such as InCommon Federation and other implementations conforming to the eGov 2.0 standard.

For more information, see Improved interoperability with SAML 2.0.

Simplified password management for federated Microsoft 365 users

You can configure AD FS to send password expiry claims to any relying party trusts or applications that it protects. How these claims appear varies between applications. For example, with Office 365 as your relying party, updates have been implemented to Exchange and Outlook to notify federated users of their soon-to-be-expired passwords.

For more information, see Configure AD FS to send password expiry claims.

Moving from AD FS in Windows Server 2012 R2 to AD FS in Windows Server 2016 is easier

Previously, migrating to a new version of AD FS required exporting the configuration settings from your Windows Server farm to a new, parallel server farm. AD FS on Windows Server 2016 makes the process easier by removing the requirement to have a parallel server farm. When you add a Windows Server 2016 server to a Windows Server 2012 R2 server farm, the new server behaves just like a Windows Server 2012 R2 server.

When you're ready to upgrade and have removed the older servers, you can change the operational level to Windows Server 2016. For more information, see Upgrading to AD FS in Windows Server 2016.

Feedback

Was this page helpful? 👍 Yes 👎 No