Microsoft

Technical Feature Comparison Guide

Windows Server 2016, Windows Server 2012 R2, and Windows Server 2008 R2

Contents

Take the next step. Learn more at www.microsoft.com/windowsserver

How to use this comparison guide

This feature comparison guide compares selected features of Microsoft Windows Server 2008 R2, Windows Server 2012 R2, and Windows Server 2016. Its goal is to help customers understand the differences between the version they are running today and the latest version available from Microsoft.

> Customers who are innovating quickly can move to the Semi-annual Channel licensing model to get more frequent feature releases for Windows Server. This guide does not currently include details about the new semi-annual releases, but you can find more details here.

The comparison table includes comments about each feature, as well as notation about how well each feature is supported in each release. The legend for this notation is given in the table below.

Level of feature support

Feature name	Not Supported ○	Partially Supported ◑	Fully Supported ●
Feature description			

Windows Server 2016 – The cloud-ready operating system

Windows Server 2016 is the cloud-ready operating system that delivers new layers of security and Azure-inspired innovation for the applications and infrastructure that power your business. Increase security and reduce business risk with multiple layers of protection built into the operating system. Evolve your datacenter to save money and gain flexibility with software-defined datacenter technologies inspired by Microsoft Azure. Innovate faster with an application platform optimized for the applications you run today as well as the cloud-native apps of tomorrow.

Easier hybrid cloud computing

Windows Server 2016 is designed to work well for hybrid environments:

- Benefit from cloud-consistency built into Windows Server 2016 to move workloads from on-premises to the cloud, in virtual machines (VMs) or containers.
- Use familiar management skills and tools, including PowerShell, to manage across your on-premises, hosted, or public cloud environments.
- Use your on-premises Windows Server licenses with Software Assurance to save up to 49 percent when you move workloads to Azure with the Azure Hybrid Benefit. Find out more at www.azure.com/ahub.

Built-in security

Windows Server 2016 includes built-in breach resistance to help thwart attacks on your systems and meet compliance goals. Even if someone finds a way into your environment, the layers of security built into Windows Server 2016 limit the damage they can cause and help detect suspicious activity.

- Help prevent risks associated with compromised administrative credentials. Use new privileged identity management features to limit administrative access by enabling “just enough” and “just-in-time” administration capabilities. Use Credential Guard to prevent administrative credentials from being stolen by Pass-the-Hash attacks.
- Protect your virtual machines using the unique Shielded Virtual Machine feature. A Shielded VM is encrypted using BitLocker and can only run on approved hosts.
- Protect against unknown vulnerabilities by ensuring only permitted binaries are executed using additional security features such as Control Flow Guard and Code Integrity as well as Windows Defender optimized for server roles.
- Use Hyper-V isolation for a unique additional layer of isolation for Windows and Linux containerized applications.

Software-defined infrastructure

Datacenter operations are struggling to reduce costs while handling more data traffic. New applications stretch the operational fabric and create infrastructure backlogs that can slow business. Windows Server 2016 delivers a more flexible and cost-efficient operating system for datacenters, using software-defined compute, storage, and network virtualization features inspired by Azure.

Resilient compute

Run your datacenter with a highly automated, resilient, virtualized server operating system.

- Upgrade infrastructure clusters to Windows Server 2016 with zero downtime for your Hyper-V or scale-out file server workloads, and without requiring new hardware, using Mixed OS Mode cluster upgrades.
- Increase application availability with improved cluster resiliency to transient failures in network and storage.
- Automate server management with PowerShell 5.1 and Desired State Configuration.
- Deploy applications on multiple operating systems with best-in-class support for Linux on Hyper-V.
- Control Windows servers from anywhere using Microsoft Management Console or Server Manager, both of which can be used remotely

Reduced-cost storage

Windows Server 2016 includes expanded capabilities in software-defined storage with an emphasis on resilience, reduced cost, and increased control.

- Build highly available and scalable software-defined storage solutions at a fraction of the cost of SAN or NAS. Storage Spaces Direct uses standard servers with local storage to create converged or hyper-converged storage architectures.
- Create affordable business continuity and disaster recovery among datacenters with Storage Replica synchronous storage replication.
- Ensure application users have priority access to storage resources using Quality-of-Service features.

Agile networking

Windows Server 2016 delivers key networking features inspired by technology in the Azure datacenters to support agility, dynamic security, and hybrid flexibility in your datacenter.

- Deploy and manage workloads with different types of networking policies (isolation, Quality of Service, security, load balancing, switching, routing, gateway, DNS, etc.) across their entire lifecycle in a matter of seconds using a scalable Network Controller.
- Dynamically segment your network based on workload needs using a distributed firewall and network security groups to apply NIC and subnet in enforcement by routing or mirroring traffic to virtualized firewall appliances for even greater levels of security.
- Take control of your hybrid workloads and move them across servers, racks, and clouds using standards-based VXLAN and NVGRE overlay networks and multi-tenanted hybrid gateways.
- Optimize cost/performance by converging RDMA storage traffic and tenant workload traffic on the same teamed NICs, thereby driving down cost while providing performance and Quality of Service (QoS) at 40G and beyond.

Cloud-ready application platform

Windows Server 2016 delivers new ways to deploy and run your applications – whether on-premises, in a hybrid environment, or in any public cloud or hosted environment – using capabilities such as Windows Server containers and Nano Server as the container image.

- Build cloud-native and hybrid apps using containers and microservices architectures.
- Move your traditional applications into a modern DevOps environment with little or no code changes using containers. Windows Server Containers bring the agility and density of containers to the Windows ecosystem, enabling agile application development and management. Use Hyper-V isolation for a unique additional level of security for Linux and Windows containerized applications without any changes to the container image. Use Active Directory identity mapped to your Windows Server Containers.
- Microsoft, Docker Inc. and the Docker Community have partnered to provide the Docker Enterprise Edition with support for new container technologies in Windows Server 2016.
- Use Nano Server as the container image for the agility and flexibility today's application developers need. Optimized for use inside containers, it's the perfect option for working with microservices.
- Run traditional first-party applications such as SQL Server 2016 with best-in-class performance, security and availability.

Windows Server 2016 editions

Windows Server 2016 editions include:

- **Datacenter**: This edition delivers significant value for customers who need unlimited virtualization along with powerful new features including Shielded Virtual Machines, software-defined storage and software-defined networking.
- **Standard**: This edition is ideal for customers who need limited virtualization but require a robust, general purpose server operating system.
- **Essentials**: This edition is designed for small-to-medium sized customers with 25-50 users.

Windows Server 2016 will not have a Foundation edition, but current Foundation customers will find the Essentials edition to be a close match for their requirements.

For the Standard and Datacenter editions, there are two installation options:

- **Server Core**: The Server Core installation option removes the client UI from the server, providing an installation that runs the majority of the roles and features on a lighter install. Server Core does not include Microsoft Management Console (MMC) or Server Manager, which can be used remotely, but does include limited local graphical tools such as Task Manager as well as PowerShell for local or remote management.
- **Server with Desktop Experience**: The Server with Desktop Experience installation option provides an ideal user experience for those that need to run an app that requires local UI or for Remote Desktop Services Host. This option has the full Windows client shell and experience, consistent with Windows 10 Anniversary edition Long Term Servicing Branch (LTSB), with the MMC available locally on the server.

Security

Windows Server 2016 delivers layers of protection that help address emerging threats and meet your compliance needs, making Windows Server 2016 an active participant in your security defenses. These include the new Shielded Virtual Machine feature that protects VMs from attacks and compromised administrators in the underlying fabric, extensive threat resistance components built into the Windows Server 2016 operating system and enhanced auditing events that will help security systems detect malicious activity.

Shielded Virtual Machines	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

Shielded Virtual Machines and Guarded Fabric help provide hosting service providers and private cloud operators the ability to offer their tenants a hosted environment where protection of tenant virtual machine data is strengthened against threats from compromised storage, network and host administrators, and malware. For example: If you are running your domain controllers or sensitive SQL databases as a virtual machine, you would want to shield them from fabric attacks.

A Shielded Virtual Machine is a generation 2 VM (supports Windows Server 2012 and later) that has a virtual TPM, is encrypted using BitLocker and can only run on healthy and approved hosts in the fabric. You can configure to run a Shielded Virtual Machine on any Hyper-V host. For the highest levels of assurance, the host hardware requires TPM 2.0 (or later) and UEFI 2.3.1 (or later).

Credential Guard	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

Credential Guard helps prevent pass the hash attacks by utilizing virtualization-based security to credential artifacts from administrators.. Credential Guard offers better protection against advanced persistent threats by protecting credentials on the system from being stolen by a compromised administrator or malware.

Credential Guard can also be enabled on Remote Desktop Services servers and Virtual Desktop Infrastructure so that the credentials for users connecting to their sessions are protected.

Remote Credential Guard	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

Remote Credential Guard helps you protect your credentials over a Remote Desktop connection by redirecting the Kerberos requests back to the device that's requesting the connection. It also provides single sign on experiences for Remote Desktop sessions. If the target device is compromised, your credentials are not exposed because both credential and credential derivatives are never sent to the target device.

Code Integrity (Device Guard)	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

Code Integrity uses Virtualization Based Security to ensure that only allowed binaries can be run on the system. If the app or driver isn't trusted, it can't run.

Code Integrity can also help protect Remote Desktop Services to lock down what applications can run within the user sessions.

AppLocker	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	◑	●	●

AppLocker can help you protect the digital assets within your organization, reduce the threat of malicious software being introduced into your environment, and improve the management of application control and the maintenance of application control policies. AppLocker and Code Integrity can be used in tandem to provide a wide set of software restriction policies that meets your operational needs.

Control Flow Guard	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

Control Flow Guard (CFG) protects against an attacker corrupting the control flow of a process by changing the addresses of indirect calls. Windows user mode components are created with Control Flow Guard built-in and vendors can also include Control Flow Guard in their binaries using Visual Studio 2015.

Windows Defender: included antimalware	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

Windows Defender is malware protection that actively protects Windows Server 2016 against known malware and can regularly update antimalware definitions through Windows Update. Windows Defender is optimized to run on Windows Server supporting the various server roles and is integrated with PowerShell for malware scanning.

Distributed firewall	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

The distributed firewall is a network layer, 5-tuple (protocol, source and destination port numbers, source and destination IP addresses), stateful, multitenant firewall. When deployed and offered as a service by the service provider, tenant administrators can install and configure firewall policies to help protect their virtual networks from unwanted traffic originating from Internet and intranet networks.

Host Guardian Service	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

Host Guardian Service is a new role in Windows Server 2016 that enables Shielded Virtual Machines and Guarded Fabric.

Guarded Fabric: Shielded VMs can only run on Guarded hosts. These hosts need to pass an attestation check to make sure they are locked down and comply with the policy that enables Shielded VMs to run on them. This functionality is implemented through a **Host Guardian Service** deployed in the environment which will store the keys required for approved Hyper-V hosts that can prove their health to run Shielded VMs.

Device Health Attestation Service	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

For Windows 10-based devices, Microsoft introduces a new public API that will allow Mobile Device Management (MDM) software to access a remote attestation service called Windows Health Attestation Service. A health attestation result, in addition to other elements, can be used to allow or deny access to networks, apps, or services, based on whether devices prove to be healthy.

Privileged Access: Just Enough Administration	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	◑	◑	●

Administrators should only be able to perform their role and nothing more. For example: A file server administrator can restart services, but should not be able to browse the data on the server.

Just Enough Administration (JEA) provides a role based access platform through PowerShell. It allows specific users to perform specific adminstrative tasks on servers without giving them administrator rights.

JEA is built into Windows Server 2016 and you can also use WMF 5.0 to take advantage of JEA on Windows Server 2008 R2 and higher.

Privileged Access: Just-in-Time Administration	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	◑	●	●

The concept of Just-in-Time Administration helps transform administration privileges from perpetual administration to time-based administration. When a user needs to be an administrator, they go through a workflow that is fully audited and provides them with administration privilege for a limited time by adding them to a time-based security group and automatically removing them after that period of time has passed.

The deployment of Just-in-Time Administration includes creating an isolated administration forest, where the controlled administrator accounts will be managed.

Virtualization Based Security	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

Virtualization Based Security (VBS) is a new protected environment that provides isolation from the running operating system so that secrets and control can be protected from compromised administrators or malware. VBS is used by Code Integrity to protect kernel code, Credential Guard for credential isolation and Shielded VMs for the virtual TPM implementation.

Virtual TPM: Trusted Platform Module	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

Implemented in Windows Server 2016 Hyper-V, a Generation 2 virtual machine (Windows Server 2012 and later) can now have its own Virtual TPM so that it can use it as a secure crypto-processor chip. The virtual TPM is a new synthetic device that provides TPM 2.0 functionality.

Virtual TPM does not require a physical TPM to be available on the Hyper-V host, and its state is tied to the VM itself rather than the physical host it was first created on so that it can move with the VM. VMs with a virtual TPM can run on a guarded fabric.

The Shielded VM functionality uses the Virtual TPM for BitLocker encryption.

Client machines running on Virtual Desktop Infrastructure can now use a vTPM as well.

BitLocker encryption	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	●	●	●

Windows BitLocker drive encryption provides better data protection for your computer, by encrypting all data stored on the Windows operating system volume and/or data drives.

SMB 3.1.1 security improvements	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

Security improvements to SMB 3.1.1 include pre-authentication integrity and SMB encryption improvements.

Pre-authentication integrity provides improved protection from a man-in-the-middle attacker tampering with SMB's connection establishment and authentication messages. Pre-Auth integrity verifies all the "negotiate" and "session setup" exchanges used by SMB with a strong cryptographic hash (SHA-512). If your client and your server establish an SMB 3.1.1 session, you can be sure that no one has tampered with the connection and session properties.

SMB 3.1.1 offers a mechanism to negotiate the crypto algorithm per connection, with options for AES-128-CCM and AES-128-GCM.

Dynamic Access Control	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	●	●

Apply data governance across your file servers to control who can access information and to audit who has accessed information. Dynamic Access Control lets you:

- Identify data by using automatic and manual classification of files. For example, you could tag data in file servers across the organization.
- Control access to files by applying safety net policies that use central access policies. For example, you could define who can access health information within the organization.
- Audit access to files by using central audit policies for compliance reporting and forensic analysis. For example, you could identify who accessed highly sensitive information.
- Apply Rights Management Services (RMS) protection by using automatic RMS encryption for sensitive Microsoft Office documents. For example, you could configure RMS to encrypt all documents that contain Health Insurance Portability and Accountability Act (HIPAA) information.

AD Rights Management Services	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	●	●	●

AD Rights Management provides information protection for your sensitive information. By using Active Directory Rights Management Services (AD RMS) and the AD RMS client, you can augment an organization's security strategy by protecting information through persistent usage policies, which remain with the information, no matter where it is moved. You can use AD RMS to help prevent sensitive information—such as financial reports, product specifications, customer data, and confidential e-mail messages—from intentionally or accidentally getting into the wrong hands.

Azure Rights Management Connector	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	●	●

Azure Rights Management (RMS) connector lets you quickly enable existing on-premises servers to use their Information Rights Management (IRM) functionality with the cloud-based Microsoft Rights Management service (Azure RMS).

Enhanced auditing for threat detection	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	●	●	●

Based on the Microsoft internal security operation center, Windows Server 2016 includes targeted auditing to better detect malicious behavior. These include auditing access to kernel and sensitive processes as well as new data in the logon events. These events can then be streamed to threat detection systems such as the Microsoft Operations Management Suite to alert on malicious behavior.

PowerShell 5.1 security features	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	◑	◑	●

There are several new security features included in PowerShell 5.1. These include: Script block logging, Antimalware Integration, Constrained PowerShell and transcript logging.

PowerShell 5.1 is also available for install on previous operating systems starting from Windows Server 2008 R2 and on.

Identity

Identity is the new control plane to secure access to on-premises and cloud resources. It centralizes your ability to control user and administrative privileges, both of which are very important when it comes to protecting your data and applications from malicious attack. At the same time, our users are more mobile than ever, and need access to computing resources from anywhere.

Active Directory Domain Services

Active Directory Domain Services (AD DS) stores directory data and manages communication between users and domains, including user logon processes, authentication, and directory searches. An Active Directory domain controller is a server that is running AD DS.

New domain services capabilities	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	◑	●

New in Windows Server 2016:

- **Privileged Access Management.** This capability, which allows organizations to provide time-limited access to administrator accounts, is described in the Security section of this document.
- **Azure Active Directory Join.** There are enhanced identity experiences when devices are joined to Azure Active Directory. These include applying Modern settings to corporate-owned workstations, such as access to the Windows Store with corporate credentials, live tile and notification settings roaming, and backup/restore.
- **Microsoft Passport.** Active Directory Domain Services now supports desktop login from Windows 10 domain joined devices with Microsoft Passport. Microsoft Passport offers stronger authentication than password authentication with device specific and TPM protected credentials.

Active Directory Federation Services

Active Directory Federation Services (AD FS) is a standards-based service that allows the secure sharing of identity information between trusted business partners (known as a federation) across an extranet. The service builds on the extensive AD FS capabilities available in the Windows Server 2012 R2 timeframe. Key enhancements to AD FS in Windows Server 2016 include better sign-on experiences, smoother upgrade and management processes, conditional access, and a wider array of strong authentication options, are described in the topics that follow.

Better sign-on to Azure AD and Office 365	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

One of the most common usage scenarios for AD FS continues to be providing sign-on to Office 365 and other Azure AD based applications using your on-premises Active Directory credentials.

AD FS extends hybrid identity by providing support for authentication based on any LDAP v3 compliant directory, not just Active Directory. This allows you to enable sign in to AD FS resources from:

- Any LDAP v3 compliant directory including AD LDS and third party directories.
- Un-trusted or partially trusted Active Directory domains and forests.

Support for LDAP v3 directories is done by modeling each LDAP directory as a "local" claim that providers trust. This enables the following admin capabilities:

- Restrict the scope of the directory based on OU.
- Map individual attributes to AD FS claims, including login ID.
- Map login suffixes to individual LDAP directories.
- Augment claims for users after authentication by modifying claim rules.

Improved sign-on experience	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

AD FS now allows for **customization of the sign-on experience**. This is especially applicable to organizations that host applications for a number of different customers or brands. 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 per relying party.

Users on Windows 10 devices and computers will be able to **access applications without having to provide additional credentials**, just based on their desktop login, even over the extranet.

Strong authentication options	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

AD FS in Windows Server 2016 provides more ways to authenticate different types of identities and devices. In addition to the traditional Active Directory based logon options (and new LDAP directory support), you can now configure device authentication or Azure MFA as either primary or secondary authentication methods.

Using either the device or Azure Multi-Factor Authentication (MFA) methods, you can create a way for managed, compliant, or domain joined devices to authenticate without the need to supply a password, even from the extranet. In addition to seamless single sign-on based on desktop login, Windows 10 users can sign-on to AD FS applications based on Microsoft Passport credentials, for a more secure and seamless way of authenticating both users and devices.

Simpler upgrade, deployment, and management	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

Previously, **migrating to a new version of AD FS** required exporting configuration from the old farm and importing to a brand new, parallel farm. Now, moving from AD FS on Windows Server 2012 R2 to AD FS on Windows Server 2016 has gotten much easier. The migration can occur like this:

- Add a new Windows Server 2016 server to a Windows Server 2012 R2 farm, and the farm will act at the Windows Server 2012 R2 farm behavior level, so it looks and behaves just like a Windows Server 2012 R2 farm.
- Add new Windows Server 2016 servers to the farm, verify the functionality and remove the older servers from the load balancer.
- Once all farm nodes are running Windows Server 2016, you are ready to upgrade the farm behavior level to 2016 and begin using the new features.

AD FS in Windows Server 2016, **policies are easier to configure** with wizard-based management that allows you to avoid writing claim rules even for conditional access policies. The new access control policy templates enable the following new scenarios and benefits:

- Templates to simplify applying similar policies across multiple applications.
- Parameterized policies to support assigning different values for access control (e.g. Security Group).
- Simpler UI with additional support for many new conditions.
- Conditional Predicates (Security groups, networks, device trust level, require MFA).

AD FS for Windows Server 2016 introduces the ability to have **separation between server administrators and AD FS service administrators**. This means that there is no longer a requirement for the AD FS administrator to be a local server administrator.

In AD FS for Windows Server 2016, it is much easier to consume and **manage audit data**. The number of audits has been reduced from an average of 80 per logon to 3, and the new audits have been schematized.

In AD FS on Windows Server you can now configure **user certificate authentication on standard port 443**.

Conditional access	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

AD FS in Windows Server 2016 builds on our previous device registration capabilities by enabling new scenarios, working with Azure AD, to require compliant devices and either restrict or require multiple factors of authentication, based on management or compliance status.

Azure AD and Intune based conditional access policies enable scenarios and benefits such as:

- Enable Access only from devices that are managed and/or compliant.
- Restrict access to corporate “joined” PCs (including managed devices and domain joined PCs).
- Require multi factor authentication for computers that are not domain joined and devices that are not compliant.

AD FS in Windows Server 2016 can consume the computer or device compliance status, so that you can apply the same policies to your on-premises resources as you do for the cloud.

Compliance is re-evaluated when device attributes change, so that you can always ensure policies are being enforced.

Seamless sign-on from Windows 10 and Microsoft Passport	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

Domain Join in Windows 10 has been enhanced to provide integration with Azure AD, as well as stronger and more seamless Microsoft Passport based authentication. This provides the following benefits after being connected to Azure AD:

- SSO (single-sign-on) to Azure AD resources from anywhere.
- Strong authentication and convenient sign-in with Microsoft Passport and Windows Hello.

AD FS in Windows Server 2016 provides the ability to extend the above benefits and device policies to on-premises resources protected by AD FS.

Developer focus	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	◑	●

AD FS for Windows Server 2016 builds upon the Oauth protocol support to enable the most current and **industry standard-based authentication** flows among web apps, web APIs, browser and native client-based apps. In Windows Server 2016, the following additional protocols and features are supported:

- OpenId Connect support.
- Additional Oauth authorization code grant types.
    - Implicit flow (for single page applications).
    - Resource Owner password (for scripting apps).
- Oauth confidential clients (clients capable of maintaining their own secret, such as app or service running on web server)
- Oauth confidential client authentication methods:
    - Symmetric (shared secret / password).
    - Asymmetric keys.
    - Windows Integrated Authentication (WIA).
- Support for “on behalf of” flows as an extension to basic Oauth support.

Registering modern applications has also become simpler using AD FS in Windows Server 2016. Now instead of using PowerShell to create a client object, modeling the web API as an RP, and creating all of the authorization rules, you can use the new Application Group wizard.

Active Directory Lightweight Directory Services (AD LDS)

AD LDS is a Lightweight Directory Access Protocol (LDAP) directory service that provides flexible support for directory-enabled applications, without the dependencies that are required for Active Directory Domain Services (AD DS). AD LDS provides much of the same functionality as AD DS, but it does not require the deployment of domains or domain controllers.

Active Directory Lightweight Directory Services	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	●	●	●

There are no significant enhancements to AD LDS in Windows Server 2016.

Existing capabilities that continue to be offered in AD LDS include:

- Role support for Server Core installations.
- Ability to back up and restore databases to an existing AD LDS instance.
- Ability to concurrently run multiple instances of AD LDS on a single computer with an independently managed schema for each AD LDS instance.

Web Application Proxy

The Web Application Proxy is a Windows Server service that allows for secure publishing of internal resources to users on the Internet.

Web Application Proxy	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	◑	●

Web Application Proxy supports new features including pre-authentication support with AD FS for HTTP Basic applications such as Exchange Active Sync. Additionally, certificate authentication is now supported.

The following new features build on the existing application publishing capabilities found in the Web Application Proxy:

Pre-authentication for HTTP basic application publishing: HTTP Basic is the authorization protocol used by many protocols, including ActiveSync, to connect rich clients, including smartphones, with your Exchange mailbox. Web Application Proxy traditionally interacts with AD FS using redirections which is not supported on ActiveSync clients.

This new version of Web Application Proxy provides support to publish an app using HTTP basic by enabling the HTTP app to receive a non-claims relying party trust for the application to the Federation Service. For more information on HTTP basic publishing, see Publishing Applications using AD FS Pre-authentication

- **Wildcard Domain publishing of applications:** To support scenarios such as SharePoint 2013, the external URL for the application can now include a wildcard to enable you to publish multiple applications from within a specific domain, for example, https://*.sp-apps.contoso.com. This will simplify publishing of SharePoint apps.
- **HTTP to HTTPS redirection:** In order to make sure your users can access your app, even if they neglect to type HTTPS in the URL, Web Application Proxy now supports HTTP to HTTPS redirection.
- **Publishing of Remote Desktop Gateway Apps:** For more information on RDG in Web Application Proxy, see Publishing Applications with SharePoint, Exchange and RDG.
- **New debug log:** for better troubleshooting and improved service log for complete audit trail and improved error handling. For more information on troubleshooting, see Troubleshooting Web Application Proxy.
- **Administration Console UI improvements.**
- **Propagation of client IP address to backend applications.**

Compute

In this section, the various aspects of server computing are discussed, such as Linux capabilities.

Windows and Linux as a guest OS

With Hyper-V as your hypervisor, you can run a variety of guest operating systems – Windows, Linux, and FreeBSD – in a single virtualization infrastructure. This capability works for Hyper-V and Azure Stack in your datacenter, and also underlies the Linux and FreeBSD capabilities in the Microsoft Azure public cloud. Microsoft works with the Linux and FreeBSD vendors and communities to ensure that these guests achieve production level performance and can take advantage of Hyper-V's sophisticated features such as online backup, dynamic memory, and generation 2 VMs.

Linux and FreeBSD virtual machines for Hyper-V	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	◑	●	●

Hyper-V supports a wide variety of Linux distributions and FreeBSD running in guest virtual machines. While these operating systems can run in emulated mode, the best results are achieved when using the drivers that take advantage of Hyper-V's virtual devices. These drivers are known as the Linux Integration Services (LIS) or FreeBSD Integration Services (BIS). With these integration services, Linux and FreeBSD guests achieve production level performance, integrated management, and use the sophisticated features provided by Hyper-V.

Microsoft has worked with:

- Red Hat to ensure that the LIS drivers are built-in to Red Hat Enterprise Linux (RHEL) releases, and that RHEL is certified by Red Hat for running on Hyper-V.
- CentOS community to ensure that the LIS drivers are built into CentOS releases.
- Debian community to ensure that the LIS drivers are built into Debian GNU/Linux releases.
- Oracle to ensure that the LIS drivers are built into Oracle Linux releases with both the Unbreakable Enterprise Kernel and the Red Hat Compatible Kernel.
- SUSE to ensure that the LIS drivers are built into SUSE Linux Enterprise Server (SLES) releases, and that SLES is certified by SUSE for running on Hyper-V .
- Canonical to ensure that the LIS drivers are built into Ubuntu releases.
- FreeBSD community to ensure that the BIS drivers are built into FreeBSD releases.

Linux Secure Boot	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

Linux operating systems running on generation 2 virtual machines can now boot with the Secure Boot option enabled.

Support Linux versions 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.

PowerShell Desired State Configuration for Linux	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	◑	●

PowerShell Desired State Configuration (DSC) enables you to declaratively specify the configuration of your server, and PowerShell DSC will "make it so." Originally released for Windows, PowerShell DSC is now available for your Linux servers, using the same declarative syntax.

PowerShell on Linux and Mac OS X	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

See the *Management and Automation* section for details on this exciting new capability for Linux and Mac OS X.

Hot add and remove for network adapters	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

You can now add or remove a network adapter while the virtual machine is running, without incurring downtime. This works for generation 2 virtual machines that run either Windows or Linux operating systems.

Manual hot add and remove memory	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

You can now add or remove memory assigned to a virtual machine while the virtual machine is running, without incurring downtime. The "add" or "remove" operation is performed by an IT administrator, and is separate from "Dynamic Memory" functionality, where Hyper-V automatically adds or removes memory from guests in order to meet varying memory demand over time. Manual hot add and remove works for virtual machines that run either Windows or Linux operating systems.

Discrete Device Assignment	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

You can now map some PCI Express devices attached to the Hyper-V host, and map them directly into the address space of a Windows or Linux guest. Applications and libraries running in user space in the guest can directly access the device. For example, Discrete Device Assignment (DDA) can be used to map a physical GPU into a Linux guest so that a High Performance Computing (HPC) application can use it for high-speed computation.

SR-IOV support for Linux Guests	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

SR-IOV is now available for Linux guests, just as it is available for Windows guests. When using physical NICs in the Hyper-V host that are SR-IOV capable, Linux guests can directly access NIC functions in order to achieve higher performance. Like with Windows guests, Linux guests in a Hyper-V cluster can be live-migrated when using SR-IOV, and will automatically fallback to a normal network path if the target Hyper-V host does not have equivalent SR-IOV capability.

Hyper-V Socket support for Linux	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

Hyper-V Sockets provides a secure, general purpose communication channel between Hyper-V host and guest operating systems. Hyper-V Sockets communicates over the VMBus and therefore doesn't require network connectivity between the guest and the Hyper-V host. Applications communicating over Hyper-V Sockets use standard "sockets" as the programming model, and appear in the Windows and Linux operating systems as a new socket address family type.

Storage

Microsoft offers an industry leading portfolio for building on-premises clouds. We embrace your choice of storage for your cloud – be it traditional SAN/NAS or the more cost-effective software-defined storage solutions using Storage Spaces Direct and Storage Spaces with shared JBODs. In Windows Server 2016, we support hyper-converged infrastructure with Storage Spaces Direct. The Microsoft hyper-converged solution offers the following advantages:

- Cloud design points and management with standard servers and local storage. It supports modern device types such as SATA and NVMe SSD. Once deployed management tools are available through System Center Virtual Machine Manager (SCVMM), System Center Operations Manager (SCOM) and PowerShell.
- Reliability, scalability and flexibility: This solution is fault tolerant to drives, servers, or even chassis or rack failures. It scales pools to a large number of drives with simple and fine grained expansion and automatic data rebalancing. VM creation performance and snapshotting has been optimized.
- Simplifies the datacenter by collapsing storage and compute. The storage area network is no longer necessary with a software service acting as a storage controller.

Storage Spaces Direct	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

Storage Spaces Direct enables service providers and enterprises to use industry standard servers with local storage to build highly available and scalable software defined storage. Using servers with local storage decreases complexity, increases scalability, and enables use of storage devices that were not previously possible, such as SATA solid state disks for lower cost flash storage, or NVMe solid state disks for better performance. Storage Spaces Direct removes the need for a shared SAS fabric, simplifying deployment and configuration. Instead it uses the network as a storage fabric, leveraging our investments in SMB3 and SMB Direct (RDMA) for high speed and low latency storage. To scale out, simply add more servers to increase storage capacity and IO performance. Storage Spaces Direct supports both converged and hyper-converged deployment modes enabling customer choice.

- Converged, with storage and compute in separate tiers, for independent scaling and management.
- Hyper-converged, with compute and storage collocated on the same servers, for simple deployment.

Health Service

Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
○	○	●

The Health Service is a new feature in Windows Server 2016 which significantly improves the day-to-day monitoring, operations, and maintenance experience of Storage Spaces Direct. The Health Service is enabled by default. New cmdlets make collecting aggregated performance and capacity metrics simple and fast. Faults and health information bubble up to a single monitoring point per cluster. New included intelligence determines the root cause of faults to reduce chattiness, understand severity, and recommend next steps, including providing helpful physical location and part information for disk replacement. New automation retires failed physical disks, removes them from their pool, and adds their replacements to the same pool, all while kicking off the requisite repair and rebuild jobs.

Resilient File System

Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
○	◑	●

Resilient File System (ReFS) is now the preferred file system for Windows Server 2016. This updated version provides many new capabilities for private cloud workloads. Improvements to ReFS in Windows Server 2016 include:

- **Data integrity**. Checksums protect all filesystem metadata, while optional checksums protect file data. Checksum verification occurs on every read of checksum-protected data during periodic background scrubbing. Healing occurs as soon as corruption is detected. ReFS uses alternate healthy versions to automatically repair corruption.
- **Resiliency and availability**. We designed ReFS to stay online and keep your data accessible. It performs repairs without taking volumes offline. Backups of critical metadata are automatically maintained on the volume. The online repair process consults backups if checksum-based repair fails.
- **Speed and efficiency**. Efficient VM checkpoints and backup are now possible since operations between parent and child VHDX is a ReFS metadata operation. This means reduced IO, increased speed, and lowered time taken. It greatly accelerates fixed and dynamic VHDX creation, lowering VM deployment times. ReFS provides near-instantaneous VM Storage provisioning.

Storage Replica

Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
○	○	●

Storage Replica is a new feature that protects your data in stretch clusters, server-to-server, and cluster-to-cluster scenarios. Capabilities include:

- **Zero data loss, block-level replication**. With synchronous replication, there is no possibility of data loss. With block-level replication, there is no possibility of file locking. Also supports asynchronous replication.
- **Guest and host**. All capabilities of Storage Replica are exposed in both virtualized guest and host-based deployments. This means guests can replicate their data volumes even if running on non-Windows virtualization platforms or in public clouds, as long as they are using Windows Server 2016 in the guest.
- **SMB3-based**. Storage Replica uses the proven and mature technology of SMB 3, first released in Windows Server 2012. This means all of SMB's advanced characteristics - such as multichannel and SMB direct support on RoCE, iWARP, and InfiniBand RDMA network cards – are available to Storage Replica.
- **Simple deployment and management.** Storage Replica has a design mandate for ease of use. Creation of a replication partnership between two servers can be done with only a single PowerShell command. Deployment of stretch clusters is an intuitive wizard in the familiar Failover Cluster Manager tool.

Storage Quality of Service	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

Enables admins to centrally manage and monitor storage performance and control workload access to storage resources. Allows critical workloads to receive higher-priority access to storage resources. Policies define storage I/O minimums and maximums for virtual machines and ensure they are met, providing consistent performance across VMs.

Storage Resiliency	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

Protects VMs from underlying transient storage failures. Monitors the state of storage, gracefully pauses VMs, and then resumes them when storage is available again. Reduces impact and increases availability of workloads running in virtual machines in the event of storage disruption.

Data deduplication	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	◑	●

Deduplication can provide volume space savings of up to 90% to reduce capacity needs and reduce costs.

New features and improvements in the Data Deduplication feature in Windows Server 2016 include integrated support for virtualized backup workloads and major performance improvements to scalability of volume (up to 64TB) and file sizes (up to 1TB with no restrictions).

Cluster OS Rolling Upgrade	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

Cluster OS Rolling Upgrade is a new feature in Windows Server 2016 that enables an administrator to seamlessly upgrade the operating system of nodes in a failover cluster from Windows Server 2012 R2 to Windows Server 2016. When a rolling upgrade of a cluster takes place, there will be a temporary mixture of Windows Server 2012 R2 hosts and Windows Server 2016 hosts. Using this feature, the downtime penalties against Service Level Agreements (SLA) can be avoided for Hyper-V or the scale-out file server workloads. This mechanism can also be used to upgrade your cluster nodes from Windows Server 2012 R2 to Windows Server 2016. Rolling upgrades can also be orchestrated through System Center Virtual Machine Manager (SCVMM).

SMB 3.1.1	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	◑	●

Windows Server 2016 includes updates to our main remote data protocol, known as SMB (Server Message Block).

- **Pre-Authentication Integrity**: Provides improved protection from a man-in-the-middle attacker tampering with SMB's connection establishment and authentication messages. SMB signing protects against an attacker tampering with any packets. SMB encryption protects against an attacker tampering with or eavesdropping on any packets.
- **Encryption performance liprovements**: Default is now AES-128-GCM, which creates a 2X improvement over AES-128-CCM in many scenarios, like copying large files over an encrypted SMB connection. Multiple encryption types now allowed for future-proofing, and full compatibility with Windows Server 2012 R2 SMB encryption.
- **Cluster Dialect Fencing**: Provides support for the Cluster Rolling Upgrade feature. If the cluster is in mixed mode, the SMB server will offer up to version 3.0.2. After upgrading the cluster functional level, the SMB server offers all clients the new 3.1.1 dialect.

Work Folders – overview	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	◑	●

Provides a consistent way for users to access their work files from their PCs and devices.

Ability to maintain control over corporate data by storing files on centrally managed file servers, and optionally specifying user device policies such as encryption and lock-screen passwords.

Ability to deploy Work Folders with the existing deployments of Folder Redirection, Offline Files, and home folders. Work Folders stores user files in a folder on the server called a sync share.

Chkdsk Performance	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	◑	●	●

Ability to run in seconds to fix corrupted data. No offline time when used with CSV. Disk scanning process separated from repair process. Online scanning with volumes and offline repairs.

Scale-Out File Server	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	●	●

Scale-Out File Server (SoFS) provides remote file server shares to be used as continuously available file based storage for workloads such as Hyper-V and SQL Server 2012.

- **Support for SMB instances on a scale-out file server.** Provides an additional instance on each cluster node in scale-out file servers specifically for Clustered Shared Volume (CSV) traffic. A default instance can handle incoming traffic from SMB clients that are accessing regular file shares, while another instance only handles inter-node CSV traffic. This feature improves the scalability and reliability of the traffic between cluster nodes.

- **Automatic rebalancing of scale-out file server clients**. Improves scalability and manageability for scale-out file servers. Server message block (SMB) client connections are tracked per file share (instead of per server), and clients are then redirected to the cluster node with the best access to the volume used by the file share. This improves efficiency by reducing redirection traffic between file server nodes. Clients are redirected following an initial connection and when cluster storage is reconfigured.

SMB 3.0	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	●	●

- **SMB Direct (SMB over RDMA).** Improves performance by having SMB3 take advantage of RDMA-enabled network cards, delivering radically improved network performance with little CPU impact. Supports the use of network adapters that have Remote Direct Memory Access (RDMA) capability. Network adapters that have RDMA can function at full speed with very low latency, while using very little CPU. For workloads such as Hyper-V or Microsoft SQL Server, this boosts performance enabling a remote file server to resemble local storage.

- **Improved SMB bandwidth management.** Ability to configure SMB bandwidth limits to control different SMB traffic types. There are three SMB traffic types: default, live migration, and virtual machine.

- **SMB Multichannel.** Enables file servers to use multiple network connections simultaneously. It facilitates aggregation of network bandwidth and network fault tolerance when multiple paths are available between the SMB client and server. This capability allows server applications to take full advantage of all available network bandwidth and makes them resilient to network failures.

iSCSI	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	●	●

- **Virtual disk enhancements.** Includes a redesigned data persistence layer that is based on a new version of the virtual hard disk format called VHDX (VHD 2.0). Provides data corruption protection during power failures and optimizes structural alignments of dynamic and differencing disks to prevent performance degradation on new, large-sector physical disks.
- **Manageability enhancements.** Uses the SMI-S provider with System Center Virtual Machine Manager (SCVMM) to manage iSCSI Target Server in a hosted or private cloud. The new PowerShell cmdlets for iSCSI Target Server enable the exporting and importing of configuration files, and provide the ability to disable remote management when iSCSI Target Server is deployed in a dedicated Windows-based appliance scenario (for example, Windows Storage Server).
- **Improved optimization to allow disk-level caching**. Ability to set the disk cache bypass flag on a hosting disk I/O, through Force Unit Access (FUA), only when the issuing initiator explicitly requests it. This can potentially improve performance.
- **Scalability limits**. Increases the maximum number of sessions per target server to 544, and increases the maximum number of logical units per target server to 256.

Network File System Support (NFS 4.1 Support)	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	●	●

File sharing solution for enterprises with a mixed Windows and UNIX environment.

Ability to reliably store and run VMware ESX virtual infrastructures with file system support on Windows Server 2012, while using the advanced high availability of Windows.

Networking

Networking is a foundational part of the software-defined datacenter (SDDC) platform, and Windows Server 2016 provides new and improved software-defined networking (SDN) technologies to help you move to a fully realized SDDC solution for your organization. Software-defined networking capabilities have been significantly enhanced and revolve around the new Network Controller function.

Networking server roles/features such as DNS, DHCP and IP address management (DDI) provide critical infrastructure services, and have seen important updates as well.

High Performance NIC Offloads: A cost optimized, high-performance data plane

Windows Server 2016 brings a number of enhancements in support of the underlying NIC hardware, specifically taking advantage of the increases in the ability of NICs to offload expensive processing tasks from the server CPUs.

Virtual Machine Queue	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	●	●	●

Virtual Machine Queue (VMQ) enables a Hyper-V host's network adapter to distribute traffic for different VMs into different queues, each of which can be serviced on a different CPU, and which can be optimized for delivery to the VM. VMQ performs CPU load spreading for Hyper-V traffic that RSS does for native stack traffic.

Virtual Machine Multi-Queue	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

Physical NICs that support Virtual Machine Multi-Queue (VMMQ) can offload some of the network traffic processing from virtual RSS into a traffic queue on the physical NIC itself. VMMQ is VMQ integrated with vRSS in the hardware. Ultimately, this means virtual machines can sustain a greater networking traffic load by distributing the processing across multiple cores on the host and multiple cores on the virtual machine. vRSS continues to run on top of VMMQ to do the distribution across the logical processors. The number of queues used in the hardware for VMMQ for traffic for a particular VM has no relationship to the number of RSS queues in that VM.

Virtual Receive-Side Scaling	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	●	●

Receive Side Scaling (RSS) is a capability traditionally enabled in physical network interface cards (NICs) and their driver stacks to allow processing of network traffic to not be constrained by being bound to a single CPU core in the computer. This enables higher network throughput by removing the bottleneck of a single CPU core being fully utilized and unable to keep up with processing incoming network traffic.

In earlier versions of Windows Server, RSS was limited to the NIC in the physical host. In Windows Server 2012 R2, this capability was extended into the virtual NICs of VMs, enabling network processing load distribution across multiple virtual processors in multicore virtual machines, removing a possible bottleneck for traffic processing inside a VM.

Virtual RSS (vRSS) is built on top of VMQ, i.e., the packets arriving in a VMQ for a VM are distributed across the logical processors of that VM using RSS.

Encapsulation task offloads (NVGRE, VXLAN)	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	●	●

Either NVGRE or VXLAN can be used to create a tenant overlay virtual network by encapsulating the tenant's traffic transmitted between Hyper-V VMs. Encapsulation can be an expensive CPU operation for the Hyper-V Host and so the ability to offload these operations to a physical network adapter provides increased throughput performance and decreases CPU host load. The ability to offload these encapsulation operations for NVGRE has been available since Windows Server 2012 R2. Support for VXLAN encapsulation task offloads has been added in Windows Server 2016. This feature is developed in partnership with our NIC vendors who have a supporting driver.

Converged RDMA	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	◑	●

The network platform scenarios allow you to:

- Use a converged NIC to combine both RDMA and Ethernet traffic using a single network adapter, while satisfying needed Quality of Service (QoS) guarantees required for both types of traffic
- Use Switch Embedded Teaming (SET) to spread SMB Direct and RDMA traffic flows between up to two network adapters.

Datacenter Bridging	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	◑	●	●

There is support for hardware compatible with Data Center Bridging (DCB). DCB makes it possible to use a single ultra-high bandwidth NIC while providing QoS and isolation services to support the multitenant workloads expected on private cloud deployments. New in Windows Server 2016 is the ability to use Network QoS (DCB) with a Hyper-V switch.

Network tracing is streamlined and provides more detail	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	●	●

Network traces contain switch and port configuration information that tracks packets through the Hyper-V Virtual Switch, including any forwarding extensions installed. This simplifies network troubleshooting in a virtualized environment.

Software-defined networking, Network Function Virtualization stack

There is a new Azure Inspired software-defined networking stack in Windows Server 2016, which brings in a number of new capabilities – central to which is a scale out Network Controller. Customers gain the ability to drive up agility in deploying complex new workloads, in dynamically securing and segmenting their network to meet workload needs, and hybrid flexibility in moving workloads back and forth between customer datacenters and Azure or other Microsoft-powered clouds.

Network Controller	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

New in Windows Server 2016, the Network Controller provides a centralized, programmable point of automation to manage, configure, monitor, and troubleshoot network infrastructure associated with your workloads in your datacenter. Using the Network Controller, you can automate the configuration of your workloads' network infrastructure requirements, instead of performing manual configuration of physical network devices and services.

You can use Microsoft System Center Virtual Machine Manager or PowerShell scripts to easily automate network configuration across your software defined datacenter.

Virtual Networking with NVGRE	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	●	●

Both Windows Server 2012 R2 and Windows Server 2016 support tenant overlay virtual networks to isolate tenant's network traffic and apply fine-grained network policy on a per-IP (CA) basis. In Windows Server 2012 R2, Hyper-V Network Virtualization (HNV) used the NVGRE encapsulation format to isolate traffic, and this is supported in Windows Server 2016 as well.

These Virtual Networks can be managed through either System Center Virtual Machine Manager or PowerShell scripts to create, read, update, and delete resources through the Network Controller.

Virtual networking with VXLAN	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

Windows Server 2016 supports VXLAN encapsulation for virtual networks. Specifically, VXLAN is the default encapsulation format used for VMs in an overlay to communicate with each other and through Microsoft multi-tenant gateways. VXLAN support for communication through 3rd party VXLAN gateways is not supported.

Software Load Balancer	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

The Software Load Balancer (SLB) is part of the new Software-Defined Networking stack, and is managed through the Network Controller. It enables access to an arbitrary number of load balanced services' IP addresses through a single load-balanced IP address. This load balancing is available for use between services on multiple VMs (East West), or to load balance a set of VMs, making them appear as a single IP address to external users (North South). The load balancing is performed at Layer 4, offering TCP and UDP load balancing.

The load balancer also supports Direct Server Return, which allows return network traffic from the load balanced VM services to bypass the Load Balancing multiplexer. This can significantly reduce the load through the load balancer, improving performance.

Network Address Translation	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	●	●

The load balancer includes Network Address Translation capability, offering an ability to present a single IP address to the public while translating and distributing traffic to workload VMs on private IP addresses.

Network address translation (NAT) allows you to share a connection to the public Internet through a single interface with a single public IP address. The computers on the private network use private, non-routable addresses. NAT maps the private addresses to the public address. This software load balancer feature allows organization employees with single tenant deployments to access Internet resources from behind the gateway. For CSPs, this feature allows applications that are running on tenant VMs to access the Internet. For example, a tenant VM that is configured as a Web server can contact external financial resources to process credit card transactions.

Although the Software Load Balancer function was not present in Windows Server 2012 R2, there was a NAT function available and is why partial support for Windows Server 2012 R2 is shown above.

Distributed firewall	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

The Distributed firewall is a new service included with Windows Server 2016. It is a network layer, 5-tuple (protocol, source and destination port numbers, source and destination IP addresses), stateful, multi-tenant firewall. When deployed and offered as a service by the service provider, tenant administrators can install and configure firewall policies to help protect their virtual networks from unwanted traffic originating from Internet and intranet networks.

The firewall protects the network layer of virtual networks. The policies are enforced at the vSwitch port of each tenant VM. It protects all traffic flows – VM-to-VM and traffic inbound to a VM's network from external networks. The policies are pushed centrally by the Network Controller, which distributes them to all applicable hosts (running the tenant VMs) in your environment. This makes all firewall policies manageable through a single point.

The distributed firewall offers the following advantages for cloud service providers:

- A highly scalable, manageable, and diagnosable software-based firewall solution that can be offered to tenants
- Freedom to move tenant virtual machines to different compute hosts without breaking tenant firewall policies
- Offers protection to tenant virtual machines independent of the tenant guest operating system

The distributed firewall offers the following advantages for tenants:

- Ability to define firewall rules to help protect Internet facing workloads on virtual networks
- Ability to define firewall rules to help protect traffic between virtual machines on the same L2 virtual subnet as well as between virtual machines on different L2 virtual subnets
- Ability to define firewall rules to help protect and isolate network traffic between tenant on premise networks and their virtual networks at the service provider

User-defined routing (route to virtual appliances)	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

In today's software-defined datacenters, network functions that are being performed by hardware appliances (such as load balancers, firewalls, routers, switches, and so on) are increasingly being virtualized as virtual appliances. This "network function virtualization" is a natural progression of server virtualization and network virtualization. Windows Server 2016 supports virtual appliances; they are deployed as pre-built, customized virtual machines, and could come from any vendor an plug into a Hyper-V environment.

With the software-defined networking stack providing the network as a pooled and dynamic resource, facilitating tenant isolation, and providing scale and performance, virtual appliances can naturally plug into this environment. The virtual appliance can be easily moved anywhere in the cloud, and scaled up or down as needed.

Typical virtual appliances include firewalls, Intrusion Detection and Prevention Systems, Anti-malware services, network optimizers, and edge devices like gateways, routers, and proxy servers.

Many of the services described in this section are provided by Microsoft as virtual appliances, such as site-to-site or forwarding gateways, the software load balancer, and the multitenant distributed firewall.

Port mirroring	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	◑	●

Port mirroring allows all traffic that is sent and received on a virtual port to be copied and sent to another port. In Windows Server 2012 R2, this capability is supported on the Hyper-V Virtual Switch and is able to mirror a single port to another single port on the same Virtual Switch.

In Windows Server 2016 this capability is integrated into the SDN infrastructure to allow mirroring of ports on any Hyper-V host controlled by the controller into a single other port on any other host controlled by the controller.

Multi-Tenant Gateway	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	◑	●

The Windows Server 2016 Multi-Tenant Gateway routes network traffic between the physical network and VM network resources, regardless of where the resources are located. You can use the Gateway to route network traffic between physical and virtual networks at the same physical location or at many different physical locations over the Internet.

A single gateway instance is capable of serving multiple tenants with overlapping IP address spaces, maximizing efficiency for the service provider as compared to deploying a separate gateway instance per tenant, while still maintaining isolation between tenants. In Windows Server 2016, a single tenant's traffic can be spread across multiple gateway VMs.

The following are Gateway features in Windows Server 2016. In Windows Server 2012 R2, high availability for the gateway was achieved using guest VM clustering, but in Windows Server 2016, you can deploy the Multi-Tenant Gateway more simply in high availability pools that use some or all of these features at one time:

- **Site-to-site VPN.** This Gateway feature allows you to connect two networks at different physical locations across the Internet by using a site-to-site (S2S)VPN connection. For Cloud Service Providers (CSPs) that host many tenants in their datacenter, RAS Gateway provides a multitenant gateway solution that allows your tenants to access and manage their resources over site-to-site VPN connections from remote sites, and that allows network traffic flow between virtual resources in your datacenter and their physical network.
- **GRE Tunneling.** Generic Routing Encapsulation (GRE) based tunnels enable connectivity between tenant virtual networks and external networks. Since the GRE protocol is lightweight and support for GRE is available on most of network devices it becomes an ideal choice for tunneling where encryption of data is not required. GRE support in Site to Site (S2S) tunnels solves the problem of forwarding between tenant virtual networks and tenant external networks using a multi-tenant gateway. A key scenario that the GRE tunnel enables is providing connectivity to virtual networks when a tenant comes into the cloud over a high-speed link, such as MPLS.
- **L3 (Forwarding) Gateway.** The L3 forwarding functionality provides connectivity between tenant virtual networks and external networks and can be used in all scenarios where GRE tunnels are used. The main difference is that it allows tenant traffic to arrive at the gateway over a VLAN and forwards traffic between VLANs and virtual networks.
- **Dynamic routing with Border Gateway Protocol (BGP).** BGP reduces the need for manual route configuration on routers because it is a dynamic routing protocol, and automatically learns routes between sites that are connected by any of the Windows Server 2016 Gateway functions described in this section. If your organization has multiple sites that are connected by using BGP-enabled routers such as RAS Gateway, BGP allows the routers to automatically calculate and use valid routes to each other in the event of network disruption or failure. For more information, see the BGP topic on TechNet. (http://technet.microsoft.com/en-us/library/mt626647.aspx)
- **SSTP site-to-site VPN**: This feature introdcued in Windows Server 2016 enables firewall traversable site-to-site VPN connectivity by leveraging secure socket tunneling protocol (SSTP) that uses HTTPs (port 443) as transport protocol. This allows administrators or developers to connect to remote networks from deep inside enterprise networks without modifying edge router or firewall configuration. SSTP site-to-site VPN connections cannot be configured through Network Controller, they can only be configured through PowerShell.

In Windows Server 2012 R2, there was support for this function, which is removed from Windows Server 2016:

- **Point-to-site VPN.** This RAS Gateway feature allows organization employees or administrators to connect to your organization's network from remote locations. For multitenant deployments, tenant network administrators can use point-to-site VPN connections to access virtual network resources at the CSP datacenter.

SDN Quality of Service	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	◑	●

SDN Quality of Service (QoS) allows customers to allocate egress bandwidth limits and reservations for traffic from a VM. In addition, ingress bandwidth limit is available as well for Windows Server 2016. This allows for differentiated SLAs for different types of workloads.

Switch Embedded Teaming	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

Switch Embedded Teaming (SET) is an alternative NIC teaming solution that you can use in Windows Server 2016. SET integrates NIC Teaming functionality into the Hyper-V Virtual Switch.

SET allows you to group between one and eight physical Ethernet network adapters into one or more software-based virtual network adapters. These virtual network adapters provide fast performance and fault tolerance in the event of a network adapter failure. SET member network adapters must all be installed in the same physical Hyper-V host to be placed in a team.

For physical switch redundancy, you can connect your teamed NICs to the same physical switch or to different physical switches. If you connect NICs to different switches, both switches must be on the same subnet.

Switch Embedded Teaming is a feature of the physical host – you would use traditional NIC teaming if you wanted to introduce a team into a VM or under a non-Hyper-V stack.

Core network infrastructure services

There are a number of enhancements to the core networking services of DNS and IP Address Management in Windows Server 2016. The key new capability is DNS Server policies, which allows you to provide policy-based answers to DNS clients based on factors like client network location, time of day, or health-based global load balancing.

DHCP Server	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	◑	●	●

DHCP has no significant new features in Windows Server 2016. Two notable changes to DHCP server in Windows Server 2016 as support for link selection suboption (RFC 3527) which has been added for interoperability of Windows DHCP server with Cisco ACI (Application Centric Infrastructure) environments. The other change was do the dynamic DNS registration of IP addresses leases performed by the DHCP server. This change was to improve the reliability and diagnosability of the dynnamic DNS registrations in DHCP server.
Enhancements in DHCP that arrived in Windows Server 2012 and 2012 R2 include DHCP Failover, DHCP policies, DNS registration enhancements, DNS PTR registration options, and PowerShell for DHCP Server management. PowerShell cmdlets are available to perform all DHCP server management tasks.

DHCP Failover provides high availability of DHCP services to clients with DHCP servers running in parallel and replicating lease information between them. DHCP servers can be deployed in a non-clustered failover configuration that includes multi-subnet support.

DNS Server	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	◑	●	●

Domain Name System (DNS) is one of the industry-standard suite of protocols that comprise TCP/IP, and together the DNS Client and DNS Server provide computer name-to-IP address mapping name resolution services to computers and users.

The following are new and updated features of DNS for Windows Server 2016:

- **DNS Policies:** You can now configure DNS policies to specify how a DNS server responds to DNS queries. DNS responses can be based on client IP address (location), time of the day, and several other parameters, and enable location-aware DNS, traffic management, load balancing, split-brain DNS, and other scenarios. These policies allow you to perform sophisticated name resolution, pointing DNS clients to alternate service locations using a more flexible decision-making policy. The policies can be useful in these situations:
  - **Application high availability.** DNS clients are redirected to the healthiest endpoint for a given application.
  - **Traffic Management.** DNS clients are redirected to the closest datacenter.
  - **Split Brain DNS.** DNS records are split into different Zone Scopes, and DNS clients receive a response based on whether they are internal or external clients.
  - **Filtering.** DNS queries from a list of malicious IP addresses or FQDNs are blocked.
  - **Forensics.** Malicious DNS clients are redirected to a sink hole instead of the computer they are trying to reach.
  - **Time of day based redirection.** DNS clients can be redirected to datacenters based on the time of the day
- **Response Rate Limiting:** You can now enable response rate limiting on your DNS servers. By doing this, you avoid the possibility of malicious systems using your DNS servers to initiate a denial of service attack on a target.
- **DNS-based Authentication of Named Entities:** You can now use TLSA (Transport Layer Security Authentication) records to provide information to DNS clients that state what CA they should expect a certificate from for your domain name. DANE prevents man-in-the-middle attacks where someone might corrupt the DNS cache to point to their own website, and provide a certificate they issued from a different CA.
- **Unknown record support:** You can now add records which are not explicitly supported by the Windows DNS server using the unknown record functionality**.**
- **IPv6 root hints:** You can use the native IPv6 root hints support to perform internet name resolution using the IPv6 root servers.
- **PowerShell Support:** New PowerShell cmdlets are available for DNS Server. The cmdlets allow for management of the new DNS server capabilities and some more granular management of existing DNS Server features.

DNS Client service binding improvement for multi-homed systems	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

In Windows Server 2016 (and Windows 10), the DNS Client service offers enhanced support for computers with more than one network interface. For multi-homed computers, DNS resolution is optimized in the following ways:

- When a DNS server that is configured on a specific interface is used to resolve a DNS query, the DNS Client service will bind to this interface before sending the DNS query. By binding to a specific interface, the DNS client can clearly specify the interface where name resolution occurs, enabling applications to optimize communications with the DNS client over this network interface.
- If the DNS server that is used is designated by a Group Policy setting from the Name Resolution Policy Table (NRPT), the DNS Client service does not bind to a specific interface.

Enhanced IP Address Management	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	◑	●

In addition to the previous capabilities of the IP Address Management (IPAM) feature of Windows, there are a number of Windows Server 2016 enhancements. These include:

- **Enhanced DNS service management.** New DNS management features are added allowing administration of a wider range of DNS elements, including resource records, zones, and conditional forwarders. Role-based access control feature has been enhanced to support delegation of granular DNS operations.
- **Multiple Active Directory Forest support.** Now IPAM can manage DNS and DHCP in non-local forests, provided a two-way trust is in place.
- **PowerShell support for role-based access control.** The IPAM PowerShell manageability has been extended to allow for configuration of access scopes against IPAM elements.
- **Integrated DNS, DHCP, and IP Address Management.** Several new experiences and integrated lifecycle management operations are enabled, such as visualizing all DNS resource records that pertain to an IP address, automated inventory of IP addresses based on DNS resource records, and creating or deleting related DNS and DHCP objects from IP address pivot.
- **Handling very small subnets.** IPv4 /32 subnets, and IPv6 /128 subnets are now supported. These are becoming more common for use in point-to-point links between switches or switch loopback addresses.
- **PowerShell cmdlets to find free address ranges and subnets.** New PowerShell cmdlets are added to help find free IP address subnets or ranges in an IP address block or subnet respectively.

Virtualization

Windows Server 2016 can help you reduce costs with improved software-defined datacenter capabilities across storage, networking and compute. Underpinning all of these aspects of consolidation are the virtualization capabilities of Windows Server. In this section, read about the enhancements to the core Hyper-V hypervisor platform.

Hyper-V	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	◑	●	●

The Hyper-V server role in Windows Server enables you to create a virtualized server computing environment where you can create and manage virtual machines. You can run multiple operating systems on one physical computer and isolate the operating systems from each other. With this technology, you can improve the efficiency of your computing resources and free up hardware resources.

New features for Windows Server 2016 include:

- Windows Containers
- Shielded Virtual Machines (see Security section of this document)
- Virtualization Based Security
- Virtual Machine Resiliency
- Production checkpoints
- Cluster OS Rolling Upgrade for Hyper-V clusters
- Storage Quality of Service (QoS)
- PowerShell Direct
- Compatible with Connected Standby
- Discrete device assignment
- Hot add and remove for network adapters
- Hot add and remove for fixed memory

- Hyper-V Manager improvements
- Integration services delivered through Windows Update
- Linux Secure Boot
- Nested virtualization
- Networking features
- Updated virtual machine file formats
- Allow running down-level virtual machines

Windows containers	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

Windows containers provides greater isolation enabling many isolated applications to run on one computer system. They build fast and are highly scalable and portable. Two different types of container runtime are included with the feature, each with a different degree of application isolation. Windows Server containers achieve isolation through namespace and process isolation. Hyper-V isolation encapsulates each container in a lightweight virtual machine.

Here are additional features introduced with Windows containers:

- Nano Server can be the container OS for both types of Windows containers.
- Container data management capabilities are enabled with container shared folders.
- Container resource policies can be implemented.

Virtualization Based Security	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

Virtualization Based Security (VBS) is a new protected environment that provides isolation from the running operating system so that secrets and control can be protected from compromised administrators or malware. VBS is used by Code Integrity to protect kernel code, Credential Guard for credential isolation and Shielded VMs for the virtual TPM implementation.

Virtual machine resiliency	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

Windows Server 2016 increases virtual machine resiliency to help reduce downtime incurred from transient storage and networking issues:

- **Compute Resiliency:** Compute servers are more resilient to intra-cluster communication issues.
- **Quarantine of unhealthy nodes:** Unhealthy nodes are quarantined and are no longer allowed to join the cluster. This prevents flapping nodes from negatively effecting other nodes and the overall cluster.
- **Storage Resiliency:** In Windows Server 2016, virtual machines are more resilient to transient storage failures. The improved virtual machine resiliency helps preserve tenant virtual machine session states in the event of a storage disruption. This is achieved by intelligent and quick virtual machine response to storage infrastructure issues.

Production checkpoints	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

Production checkpoints allow you to easily create “point in time” images of a virtual machine which can be restored later on in a way that is completely supported for all production workloads. Backup technology inside the guest is used to create the checkpoint, instead of using saved states. For Windows Server virtual machines, the Volume Snapshot Service (VSS) is used. For Linux virtual machines, the file system buffers are flushed to create a file system consistent checkpoint. If you'd rather use checkpoints based on saved states, you can still do that by using standard checkpoints. Production Checkpoints are on by default in Windows Server 2016.

Hot add and remove for network adapters	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

You can now add or remove a network adapter while the virtual machine is running, without incurring downtime. This works for generation 2 virtual machines that run either Windows or Linux operating systems.

Manual hot add and remove memory	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

You can now add or remove memory assigned to a virtual machine while the virtual machine is running, without incurring downtime. The “add” or “remove” operation is performed by an IT administrator, and is separate from “Dynamic Memory” functionality, where Hyper-V automatically adds or removes memory from guests in order to meet varying memory demand over time. Manual hot add and remove works for virtual machines that run either Windows or Linux operating systems.

Discrete Device Assignment	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

You can now map some PCI Express devices attached to the Hyper-V host, and map them directly into the address space of a Windows or Linux guest. Applications and libraries running in user space in the guest can directly access the device. For example, Discrete Device Assignment (DDA) can be used to map a physical GPU into a Linux guest so that a High Performance Computing (HPC) application can use it for high-speed computation.

Allow down-level virtual machines	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	◑	◑	●

With Windows Server 2016, virtual machines created for Windows Server 2012 R2 with configuration version 5 can run on both Windows Server 2012 R2 and Windows Server 2016. Virtual machines with version 8 are compatible with Windows Server 2016, but won't run in Hyper-V on Windows Server 2012 R2. Version 5 virtual machines can be manually upgraded to newer virtual machine versions to leverage new features of Hyper-V.

Previous versions of Hyper-V allow importing of virtual machines from downlevel hosts. In this process the virtual machine is upgraded to match the current host's configuration version and cannot be migrated back to the downlevel host.

PowerShell Direct	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

There is now an easy and reliable way to run PowerShell commands inside a virtual machine from the host operating system. There are no network or firewall requirements, or special configuration. It works regardless of your remote management configuration. To use it, you must run Windows 10 or Windows Server 2016 on the host and the virtual machine guest operating systems.

Shared virtual hard disk	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	◑	●

A shared virtual hard disk enables guest clustering of virtual machines by using shared virtual hard disk (Shared VHDX) files, hosted on Cluster Shared Volume (CSV) or on Server Message Block (SMB)-based scale-out file server file shares. Windows Server 2016 allows resizing Shared VHDX without downtime, support for Hyper-V Replica, and host level backups.

Resize virtual hard disk	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	●	●

This provides the ability to expand or shrink the size of a virtual hard disk while the virtual machine is still running. It also provides the ability to perform maintenance on the virtual hard disk without temporarily shutting down the virtual machine. Note that this is only available for VHDX files that are attached to a SCSI controller.

Hyper-V Live Migration over SMB	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	●	●

Hyper-V Live Migration over SMB provides the ability to perform a live migration of virtual machines by using SMB 3.0 and later as a transport. This enables taking advantage of key SMB features, such as SMB Direct with RDMA enabled network cards and SMB Multichannel, delivering the highest speed virtual machine migration with little CPU utilization impact.

Live Migration with compression	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	●	●

Live Migration with compression provides the ability to first compress the memory content of the virtual machine that is being migrated and then copy it to the destination server over a TCP/IP connection. This is the default setting in Hyper-V in Windows Server 2012 R2 and later.

Live Migration Remote Direct Memory Access	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	●	●

Windows Server 2016 provides the ability to perform faster live migration between Hyper-V hosts by establishing an efficient memory-to-memory transfer of data using Remote Direct Memory Access (RDMA).

Server Message Block Direct (SMB Direct) over RDMA is a technology that, given the hardware (NICs) supporting it, can establish an efficient memory-to-memory transfer of data..

Cross-version live migration	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	◑	●

Cross-version live migration is the ability to support migrating Hyper-V virtual machines between Hyper-V running on different versions of Windows Server. This is dependent on the virtual machine configuration versions that are supported by both hosts participating in the migration.

SR-IOV	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	●	●

When using physical NICs in the Hyper-V host that are SR-IOV capable, Windows and Linux guests can directly access NIC functions in order to achieve higher performance. Guest systems in a Hyper-V cluster can be live-migrated when using SR-IOV, and will automatically fallback to a normal network path if the target Hyper-V host does not have equivalent SR-IOV capability.

Virtual machine generation	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	●	●

Virtual machine generation provides the ability to determine the virtual hardware and functionality that is presented to the virtual machine. The two supported virtual machine generations include:

- **Generation 1**: Provides the same virtual hardware to the virtual machine as in the previous versions of Hyper-V.
- **Generation 2**: Provides the following new functionality on a virtual machine:
  - Secure Boot (enabled by default).
  - Boot from a SCSI virtual hard disk.
  - Boot from a SCSI virtual DVD.
  - Pre-Boot Execution Environment (PXE) boot by using a standard network adapter.
  - Unified Extensible Firmware Interface (UEFI) firmware support.

Live VM Export	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	●	●

Live VM Export provides the ability to export a virtual machine or a virtual machine checkpoint while the virtual machine is running without any downtime.

Highly available virtual machines	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	●	●	●

Virtual machines can be deployed in a highly available fashion on a failover cluster, which provides resiliency to planned and unplanned downtime.

Enhanced session mode	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	●	●

Enhanced session mode provides the ability to redirect local resources in a Virtual Machine Connection session. This enhances the interactive session experience by providing a functionality that is similar to a remote desktop connection while interacting with a virtual machine.

Automatic Virtual Machine Activation	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	●	●

Automatic Virtual Machine Activation provides the ability to install virtual machines on a computer where Windows Server is properly activated without having to manage product keys for each individual virtual machine, even in disconnected environments. It also provides the ability to bind the virtual machine activation to the licensed virtualization server and activate the virtual machine when it starts. This enables real-time reporting on usage and historical data on the license state of the virtual machine.

Local file copies to a VM	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	●	●

Windows Server 2012 R2 and Windows Server 2016 provides the ability to copy files to the virtual machine while the virtual machine is running without using a network connection with Copy-VMFile cmdlet.

Virtual machine drain on shutdown	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	●	●

Virtual machine drain on shutdown enables a Hyper-V host to automatically live migrate running virtual machines if the computer is shut down.

Virtual machine network health detection	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	●	●

Virtual machine network health detection enables a Hyper-V host to automatically live migrate virtual machines if a network disconnection occurs on a protected virtual network.

Shared-nothing live migration	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	●	●

Shared-nothing live migration provides the ability to migrate virtual machines among Hyper-V hosts on different clusters or servers with no storage sharing using Ethernet connection only—with virtually no downtime.

Live storage migration	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	●	●

Live storage migration provides the ability to move virtual hard disks that are attached to a running virtual machine. This supports transfer of virtual hard disks to a new location for upgrading or migrating storage, performing back-end storage maintenance, or redistributing the storage load. It also allows for the ability to add storage to either a stand-alone computer or to a Hyper-V cluster, and then move virtual machines to the new storage while the virtual machines continue to run. A new wizard in Hyper-V Manager or new Hyper-V cmdlets for PowerShell can be used to perform this task.

Live Snapshot Merging	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	●	●

Live Snapshot Merging provides the ability to merge snapshots back into the virtual machine while it continues to run Hyper-V Live Merge.

Non-Uniform Memory Access support	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	●	●

Non-Uniform Memory Access (NUMA) support inside virtual machines provides the ability to project NUMA topology into virtual machines so that guest operating systems and applications can make intelligent NUMA decisions. This functinality is important for scale-up workloads like databases.

Dynamic Memory Run-time Configuration	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	●	●

Dynamic Memory Run-time Configuration provides the ability to make configuration changes to dynamic memory (increasing maximum memory or decreasing minimum memory) when a virtual machine is running. This reduces downtime and increases agility to respond to requirement changes.

VHDX Virtual Disk Format	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	●	●

Provides support for VHDX file format with Hyper-V. VHDX support includes:

- Up to 64 terabytes of storage per *virtual disk*.
- Protection from corruption due to power failures by logging updates to the VHDX metadata structures along with significant performance and scale improvements.
- Prevention of performance degradation on large-sector physical disks through optimizing structure alignment.

Hyper-V Resource Metering	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	●	●

Hyper-V Resource Metering tracks and reports amount of data transferred per IP address or virtual machine. This allows customers to create cost-effective and usage-based billing solutions.

Virtual Fiber Channel	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	●	●

Virtual Fiber Channel provides Fibre Channel ports within the guest operating system. This enables the ability to connect to Fibre Channel and Storage Area Networks (SANs) directly from within virtual machines.

Hyper-V Replica	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	●	●

Hyper-V Replica provides the ability to replicate virtual machines among storage systems, clusters, and datacenters between two sites to provide business continuity and failure recovery.

The Replica server forwards information about the changes that occur on the primary virtual machines to a third server (the extended Replica server). The frequency of replication, which previously was a fixed value, is now configurable for 30 seconds, 5 minutes, and 15 minutes. Access to recovery points in from previous versions was changed from 15 hours to 24 hours.

Simultaneous live migrations	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	◑	●	●

Windows Server Hyper-V enables the migration of several virtual machines with support for simultaneous live migrations at the same time limited only by hardware resources. Live migrations are also not limited to a cluster - virtual machines can be migrated across cluster boundaries and between stand-alone servers that are not part of a cluster.

Hyper-V host and workload support	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	◑	●	●

Hyper-V has the ability to configure up to 320 logical processors on hardware, 4 terabytes of physical memory, 64 virtual processors, and up to 1 terabyte of memory on a virtual machine. Additionally it supports up to 64 nodes and 8,000 virtual machines in a cluster.

Dynamic memory, startup memory, and minimum memory	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	◑	●	●

Dynamic memory, startup memory, and minimum memory help to attain higher consolidation numbers with improved reliability for restart operations. This can lead to lower costs, especially in environments that have many idle or low-load virtual machines, such as pooled VDI environments.

Hyper-V Smart Paging	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	●	●

Hyper-V Smart Paging bridges the gap between the minimum and startup memory if a virtual machine is configured with a lower minimum memory than its startup memory (Hyper-V requires additional memory to restart the virtual machine).

Incremental backup	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	◑	●	●

Hyper-V supports incremental backup (backing up only the differences) of virtual hard disks while the virtual machine is running. Windows Server 2008 R2 provides support for full backups only.

Application monitoring	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	●	●

Provides the ability to monitor health of key services provided by virtual machines. This provides higher availability for workloads not supporting clustering with automatic correction (such as restarting a virtual machine or moving it to a different server).

Hyper-V Sockets	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

Hyper-V Sockets provides a secure, general purpose communication channel between Hyper-V host and guest operating systems. Hyper-V Sockets communicates over the VMBus and therefore doesn't require network connectivity and works with both Linux and Windows Guests.

High availability

Microsoft continues to invest in enhancing and improving the high availability capabilities provided by Windows Server Failover Clustering. In Windows Server 2016, new and improved features simplify your ability to deploy and manage highly available failover clusters.

Cluster infrastructure requirements

Cluster OS Rolling Upgrade	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

Cluster OS Rolling Upgrade is a new feature in Windows Server 2016 that enables an administrator to seamlessly upgrade the operating system of nodes in a failover cluster from Windows Server 2012 R2 to Windows Server 2016. When a rolling upgrade of a cluster takes place, there will be a temporary mixture of Windows Server 2012 R2 hosts and Windows Server 2016 hosts. Using this feature, the downtime penalties against Service Level Agreements (SLA) can be avoided for Hyper-V or the scale-out file server workloads.

Cloud Witness	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

Cloud Witness enables using Azure blob storage as a witness in quorum for a stretched cluster. Cluster witness can now be a Disk Witness, File Share Witness, or Cloud Witness. This feature allows customers to use Azure as a third datacenter hosting the Cloud Witness, without the setup and maintenance overhead associated with running a File Share Witness on a File Server VM in Azure.

Active Directory-independent clusters	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	◑	●

Active Directory-independent clusters provide the ability to deploy a failover cluster with less dependency on Active Directory Domain Services. With Windows Server 2012 R2 the Active Directory-detached clusters feature allows having clusters with names not attached to AD. With Windows Server 2016, failover clusters can be deployed in workgroups and multiple domains.

Cluster resiliency

Windows Server 2016 Cluster Resiliency features	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

Windows Server 2016 introduces new features to improve cluster resiliency.

- **Cluster Quarantine:** Prevents flapping nodes from negatively impacting other nodes and the overall cluster health. Unhealthy nodes are prevented from joining the cluster for a time period. Once quarantined, VMs hosted by the node are gracefully drained to healthy nodes.
- **Site Awareness**: Fault domains with failure and placement policies which are aware and optimized for the physical locations of stretched clusters across sites. Enhances key operations during the cluster lifecycle such as failover behavior, placement policies, heartbeating between the nodes and quorum behavior.
- **Node Fairness**: Identifies idle nodes in a cluster and distributes virtual machines to utilize them, to dynamically load balance the cluster.

Cluster node health detection	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	◑	●

Cluster node health detection ncreases the resiliency to temporary network failures for virtual machines that are running on a Hyper-V cluster.

CSV cache	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	◑	●

CSV Cache provides a write-through cache for unbuffered IO, which significantly boosts virtual machine performance. Scalability improvements to increase the amount of memory that can be allocated as CSV Cache.

The CSV Cache with Windows Server 2016 also has interoperability enhancements, such as being compatible with Tiered Storage Spaces and Deduplication.

CSV interoperability	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	●	●

Adds CSV support for the following Windows Server features:

- Resilient File System (ReFS).
- Deduplication.
- Parity storage spaces.
- Tiered storage spaces.
- Storage Spaces write-back caching.

Management and automation

In order to reap the benefits of a modern platform for running datacenter workloads, it is imperative that capable, scalable, automation-friendly management features are built in. This allows for not only core management and automation to occur, but also allows enterprise tools and utilities to extend and expand these management capabilities.

PowerShell 5.1

PowerShell 5.1 Overview	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
			

PowerShell 5.1 includes significant new features that extend its use, improve its usability, and allow you to control and manage Windows-based environments more easily and comprehensively. PowerShell 5.1 has addded key features to support DevOps, such as Desired State Configuration (DSC), ISE improvements, writing Classes in PowerShell, the Pester test harness, and remote PowerShell debugging.

PowerShell 5.1 is backward-compatible. Cmdlets, providers, modules, snap-ins, scripts, functions, and profiles that were designed for PowerShell 4.0, PowerShell 3.0, and PowerShell 2.0 generally work in PowerShell 5.1 without changes.

PowerShell 5.1 is installed by default on Windows Server® 2016 and Windows 10®. All features of PowerShell 5.1 may be added to Windows 7, Windows Server 2008 R2, Windows Server 2012, Windows 8.1, and Windows Server 2012 R2 by installing the Windows Management Framework (WMF) 5.1.

Desired State Configuration updates	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
			

PowerShell 5.1 makes writing Desired State Configuration (DSC) resources and configurations significantly easier:

- PowerShell 5.1 enables defining DSC resources using classes which reduces the work required to develop new DSC Resources.
- A user can now run a resource under a specified set of credentials by adding the PSDscRunAsCredential attribute to a Node block.
- Composite configurations enable combining multiple steps within a configuration into a separate new DSC resource.
- A new parameter, ThrottleLimit, has been added to cmdlets in the PSDesiredStateConfiguration module.
- Cross-computer synchronization is new in DSC configurations in PowerShell 5.1. By using the built-in WaitFor* commands provides support for dependencies across multiple computers.

Configuration and control of DSC has been added for the Pull Server:

- The DSC pull server is now configurable to support multiple servers as a role, and to allow separation of the configuration and DSC resource repositories from the centralized reporting server.
- With centralized DSC error reporting, rich error information is not only logged in the event log, but it can be sent to a central location for later analysis. You can use this central location to store DSC configuration errors that have occurred for any server in their environment.

Users can now control the DSC processing engine known as the Local Configuration Manager (LCM):

- The DSCLocalConfigurationManager attribute allows configuring the LCM from within a DSC configuration.
- LCM can assemble the configuration for a node from multiple fragments, called Partial Configurations, enabling separate update and maintenance of parts of the system state, and the LCM refresh interval.

- The Get-DSCLocalConfigurationManager cmdlet returns the current state of the LCM as Idle, Busy, Pending Reboot, or PendingConfiguration.

Improvements to PowerShell ISE ease DSC resource authoring. You can now do the following:

- List all DSC resources within a configuration or node block by entering Ctrl+Space on a blank line within the block.
- Automatic completion on resource properties of the enumeration type.
- Automatic completion on the DependsOn property of DSC resources, based on other resource instances in the configuration.
- Improved tab completion of resource property values.

ISE updates	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
			

The PowerShell ISE editor has these enhancements:

- You can now edit remote PowerShell scripts and files in a local copy of PowerShell ISE, by running Enter-PSSession to start a remote session on the computer that's storing the files you want to edit, and then running PSEdit <path and file name on the remote computer>. This feature eases editing PowerShell files that are stored on the Server Core installation option of Windows Server, where PowerShell ISE cannot run.
- The Start-Transcript cmdlet is now supported in PowerShell ISE.
- You can now debug remote scripts in PowerShell ISE.
- A new menu command, Break All (Ctrl+B), breaks into the debugger for both local and remotely-running scripts.

Pester test framework	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
			

Pester is a test automation framework specifically designed for use with PowerShell scripts and code. Developed initially as an open source project, Pester is now built into Windows Server 2016 and Windows 10.
It offers these benefits:

- Pester allows for the development of a standard set of tests for PowerShell code. Pester supports the automatic execution of tests when PowerShell code is written to the framework.
- Eases adding PowerShell scripts, DSC Resources, and DSC Configurations into a CI/CD pipeline.

Package Management and PowerShellGet	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
			

Package Management cmdlets provide a single approach to discover, install, and manage a a range of installer technologies, which aids deployment within a CI/CD pipeline.

- Related PowerShellGet cmdlets enable locating, inspecting, and installing PowerShell code from the PowerShell Gallery, the PowerShell code sharing site hosted by Microsoft.
- PowerShellGet cmdlets support automatically installing dependent modules from the PowerShell Gallery. PowerShell 5 supports multiple versions of the same PowerShell module or DSC resource installed side-by-side.

Develop using classes	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	◑	◑	●

Starting in PowerShell 5.1, you can develop by using classes, by using formal syntax and semantics that are similar to other object-oriented programming languages. Class, Enum, and other keywords have been added to the PowerShell language to support the new feature.

New PowerShell cmdlets	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	◑	◑	●

PowerShell 5.1 adds a number of new cmdlets requested by the community, including:

- The New-FileCatalog cmdlet creates a windows catalog file for set of folders and files that contains hashes for all files in specified paths. User can distribute the set of folders along with corresponding catalog file representing those folders. It can be used by receiver of content to validate if any changes are made to the folders since catalog creation time.
- Get-ComputerInfo allows quick access to commonly-used information about BIOS, Windows, & Windows settings.
- ConvertFrom-String was developed in collaboration with Microsoft Research, and lets you extract and parse structured objects from the content of text strings. For more information, run Get-Help ConvertFrom-String.
- New cmdlets in the Microsoft.PowerShell.Utility module, Get-Runspace, Debug-Runspace, Get-RunspaceDebug, Enable-RunspaceDebug, and Disable-RunspaceDebug, let you set debug options on a runspace, and start and stop debugging on a runspace.
- The new Compress-Archive and Expand-Archive cmdlets ease working with ZIP files.
- Get-Clipboard/Set-Clipboard allow scripting access to the Windows clipboard.
- A new cmdlet, Clear-RecycleBin, has been added to the Microsoft.PowerShell.Management module; this cmdlet empties the Recycle Bin for a fixed drive, which includes external drives.
- A new cmdlet, New-TemporaryFile, lets you create a temporary file as part of scripting. By default, the new temporary file is created in C:\Users\<user name>\AppData\Local\Temp.

Additional parameters and capabilities have been added to cmdlets to make them easier to use:

- Out-File, Add-Content, and Set-Content cmdlets have a new –NoNewline parameter, which omits a new line after the output.
- Get-ChildItem now includes the –Depth parameter. Used in conjunction with the –RecurseNUMA
- parameter, it allows users to control how many levels a recursive action should go.
- Copy-Item now lets you copy files or folders from one PowerShell session to another, meaning that you can copy files to sessions that are connected to remote computers.
- Results of the Get-Command cmdlet now display a Version column, to show support having multiple versions of the same module installed.

PowerShell 5.1 security features	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	◑	◑	●

There are several new security features included in PowerShell 5.1. These include: Script block logging, Antimalware Integration, Constrained PowerShell and transcript logging.

PowerShell 5.1 is also available for install on previous operating systems starting from Windows Server 2008 R2 and on.

Open-source PowerShell and Linux support	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

Beginning in Windows Server 2016, PowerShell enables true cross-platform management by supporting Linux and Mac OS X as well as the existing Windows platforms. PowerShell will be built and maintained as an open-source project, based on the .Net Core CLR, and released for Windows Client, Windows Server, and Linux.

For IT Pros / ITI / Windows admin / *nix admins / Developers, who need to perform their IT operational tasks, Microsoft PowerShell provides the automation and configuration management framework that expedites administrative tasks for Windows and *nix, and enables process automation and configuration management.

This release offers:

- True cross-platform remote administration. Manage Linux from Windows, and Windows from Linux.
- The unique value of PowerShell language experience across Windows and *nix environments, specifically:
    - Powershell is built for handling Structured Objects and converting from Unstructured Data.
    - PowerShell is an extensible tool / solution to manage different Linux distributions in a uniform way
    - PowerShell is a framework which provides unique leverage to developers as well as advantages of metadata driven systems.
- Community-driven open source project provides the basis for future PowerShell plans and improvements

Management

Management Packs for Windows Server 2016 roles	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

System Center Operations Manager Management Packs updated for Windows Server 2016 roles: Windows Server 2016 installation options: Server with Desktop Experience, Server Core, DNS, DHCP, Failover Clustering, NLB, Print Services, IIS, AD DS, DTC Transactions, Windows Defender, Windows Server Essentials, AD RMS, Branch Cache, File and iSCSI Services.

Console host	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

The console host is the underlying code that supports all character-mode applications including the Windows command prompt, the PowerShell prompt, and others has been updated to include several new editing and marking behaviors.

Server Manager	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	●	●	●

Server Manager provides a single point of access to manage snap-ins for virtually all installed roles. It provides the ability to manage a server's identity and system information, display server status, identify problems with server role configuration, and manage virtually all roles installed on the server.

Multi-server management	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	●	●

Windows Server 2012 R2 and Windows Server 2016 support management of multiple servers via roles, services, or customized management groups. It provides a single view for administrators to view events, roles, services, and other important information for virtually all managed servers.

Role and feature deployment to remote servers and offline hard disks	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	●	●

The Server Manager console and PowerShell cmdlets for Server Manager allow the installation of roles and features to local or remote servers, or offline virtual hard disks.

Ability to install multiple roles and features on a single remote server or offline VHD in a single Add Roles and Features Wizard or PowerShell session.

Initial Configuration Tasks	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	●	●	●

The Initial Configuration Tasks provides an integrated console for IT departments to perform initial configuration of a newly installed server.

Group Policy	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	●	●	●

Group Policy provides the ability to specify managed configurations for users and computers through Group Policy settings and Group Policy preferences.

Windows Azure Online Backup (cloud-based backup service)	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	●	●

Windows Azure Online Backup provides offsite protection against data loss from failure with a cloud-based backup solution, which allows files and folders to be backed up and recovered from the cloud.

Group Policy Infrastructure Status	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	●	●

Group Policy Infrastructure Status provides the ability to specify managed configurations for users and computers through Group Policy settings and Group Policy preferences.

Volume Activation Services	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	◑	●	●

Volume Activation Services is a server role in Windows Server starting with Windows Server 2012 that enables you to automate and simplify the issuance and management of Microsoft software volume licenses for a variety of scenarios and environments. With Volume Activation Services, you can install and configure the Key Management Service (KMS) and enable Active Directory-based Activation.

Remote Desktop Services

Remote Desktop Services (RDS) enables an independent Windows experience for multiple users who remotely access a virtualized Windows desktops and applications from a centralized environment.

RemoteFX vGPU	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	●	●	●

RemoteFX vGPU provides a rich desktop remoting experiencing with Windows Server 2016 Hyper-V and Remote Desktop Services enabling multiple VMs to share the same physical GPU for graphics acceleration. Windows Server 2016 Remote Desktop Services includes the following improvements to RemoteFX vGPU:

- OpenGL 4.4 and OpenCL 1.1 API support
- Up to 1GB dedicated VRAM and up to 1GB of shared memory available in VM
- Up to 4k resolution support
- Windows Server 2016 VM support
- Improved performance

Discrete Device Assignment	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

Discrete Device Assignment (DDA) is a Windows Server 2016 Hyper-V feature that allows some PCI Express devices to be passed through directly to a guest VM (to be controlled by the guest VM). Devices used in this way cannot be used by the host or other VMs.

Windows Server 2016 Remote Desktop Session Hosts can now take advantage of DDA, enabling enhanced graphics performance.

- Full graphics API Support (ex. DirectX, OpenGL, CUDA, OpenCL) (depends on GPU driver)
- Native GPU Driver Support (Intel, AMD, NVIDIA)
- Maximum Performance (1 or more GPUs to 1 VM)
- Multiuser RDSH Support. Multiple sessions can utilize the graphics card assigned to the RDSH VM via DDA

Remote Desktop Protocol graphics compression	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

Windows Server 2016 (and Windows 10) Remote Desktop Protocol (RDP) graphics compression (codec) now implements full-screen AVC 444 mode. This enhancement provides:

- Reduced bandwidth and better experience at higher resolutions
- Hardware offload support.

Scale enhancements	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

In Windows Server 2016 the RD Connection Broker has been enhanced to handle highly concurrent logon scenarios ("logon storms"). The RD Connection Broker was tested at a rate of 2 connections per second up to 10k concurrent connections with significant reductions in connection failures and average connection time.

In previous OS versions the RD Connection Broker required a dedicated SQL Server cluster using Windows authentication for high availability. In Windows Server 2016, SQL authentication is now supported. This enables a database from a shared SQL server cluster to be used, making smaller scale deployments more cost effective.

Cloud optimizations – Azure Active Directory	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	◑	●

Windows Server 2016 Remote Desktop Services can utilize Azure services to provide more cost effective solutions.

Azure Active Directory (AD) Application Proxy allows the RD Web Access and RD Gateway role services to be deployed inside a firewall and published to the Application Proxy service, instead of exposed directly to the public internet. This reduces attack surface and, for small deployments, allows the deployment of RD infrastructure role services on a single machine.

Azure AD Domain Services implements Active Directory Domain Services as a managed service that includes domain join, group policy, Kerberos, etc. This eliminates the need to deploy and manage domain controller VMs, reducing the cost and complexity of an RDS deployment in Azure.

Cloud optimizations – Azure SQL Database	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

Windows Server 2016 Remote Desktop Services can utilize Azure services to provide more cost effective solutions.

In previous OS versions the RD Connection Broker required a dedicated SQL Server cluster using Windows authentication for high availability. In Windows Server 2016, Azure SQL Database using SQL authentication is supported. Azure SQL Database includes high availability, disaster recovery, and upgrade mechanisms. A highly available RDS environment using Azure SQL Database eliminates the need to deploy and manage VMs for SQL Server, reducing the cost and complexity of the RDS deployment.

Other RDS improvements	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

Windows Server 2016 Remote Desktop Services (RDS) provides several improvements over previous versions, including:

- Personal Session Desktop collections which allows each user to be assigned administrative access to a personal RD Session Host VM
- Support for Generation 2 virtual machines
- Pen Remoting support

MultiPoint Services Role	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

MultiPoint Services is a new server role in Windows Server 2016 that is easy to deploy and manage. It enables low-cost per seat desktop computing. MultiPoint leverages the Remote Desktop (RD) Session Host to allow multiple users, each with their own independent Windows 10 desktop experience, to simultaneously share one computer. The unique MultiPoint management tool-set allows monitoring and control of all user sessions on the MultiPoint server.

MultiPoint does not use or require the RD Connection Broker, RD Web Access, and RD Gateway role services. Enabling the Multipoint Services role, installs Remote Desktop Session Host role service which allows users to connect remotely with devices of their choice by using Remote Desktop applications available on Windows, Windows phone, Android, iOS and Mac OS as well as thin clients using the Remote Desktop Protocol (RDP). In addition, MultiPoint enables new types of low cost local user stations based on displays and other devices connected directly to the computer and also MultiPoint USB zero clients connected to the computer over USB.

Application development

Windows Server 2016 resolves the tension between developers and operators by enabling both traditional and container models for application development, with prescribed solutions and artifacts to achieve best practices for developing and operating the application/service.

- The traditional model can be applied across physical, guest, or containers, providing the flexibility to run the application/service in any configuration.
- The container model requires the application/service to be only delivered and managed as a container.

In addition to developing the application/service code, each development and operational model requires a set of artifacts so that operations can benefit from the Windows Server 2016 Cloud Application Platform.

Phase	Traditional model	Container model
Develop	Windows SDK allows targeting the smallest server footprint.	Nano Server SDK allows targeting the smallest container.
Package	Windows Server App (WSA) installer	Container Images
Configure	PowerShell Desired State Configuration	Container Images
Deploy	Package Management (OneGet)	Container Images
Run	In physical, guests, or Windows or Linux containers (Windows Server Containers with or without Hyper-V isolation)	Containers through orchestrators
Test	Pester	Test frameworks
Secure	Just Enough Administration (JEA)	Multiple containers, and JEA

Container model

Microsoft, Docker Inc. and the Docker community have partnered to provide the Docker engine with support for new container technologies in Windows Server 2016. Developers and organizations that want to create container applications using Docker will be able to use either Windows Server or Linux with the same growing Docker ecosystem of users, applications and tools. Windows containers provide operating system level virtualization enabling multiple isolated applications to be run on a single system. There are two different types of container runtimes included with this feature, each with different degrees of application isolation. Both Windows container runtimes are managed by the same API layer providing the same management primitives and utilizing the same configuration format thus enabling customers at runtime to choose the level of isolation required for the specific container instance being started. Both container runtimes can be managed with Docker including a new PowerShell module for Docker.

Windows Server containers	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

Windows Server containers provide operating system level virtualization enabling multiple isolated applications to be run on a single system without interfering with each other. Enabling high portability and maximizing operational agility, Windows Server containers address density and startup performance scenarios achieving isolation through namespace and process isolation.

The process isolation component of Windows Server containers has been constructed upon Windows technology first introduced in Windows NT4 known as Job Objects. Primarily used for applying resource controls on processes it proves a bases for grouping, co-managing and describing related processes. The capabilities of Job Objects have been expanded many times over the life time of Windows and now in Windows Server 2016 they form a solid foundation for Windows Server Containers.

Namespaces isolation describes a form or virtualization where operating system wide or global configuration can be instanced or virtualized to a given set of processes, as referenced by job objects. This enables each container to see a unique and standardized view of the underlying operating system maximizing portability and reducing interference from other processes or configuration. In order for applications inside containers to work properly there are a number of namespaces that must be virtualized, some of the major ones include: storage, registry, networking, object tables and process tables. Each container has a virtualized view of these namespaces limiting its ability to see global properties of the container host or other containers running alongside it.

Hyper-V isolation	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

Hyper-V isolation extends the capabilities of Windows Server containers providing additional isolation and supporting additional variation in kernel versions by encapsulating each container in a specially optimized virtual machine environment. This makes them ideally suited for a wide range of scenarios including regulated workloads, hostile multi-tenancy and hosting environments. Building upon the foundation of the Hyper-V hypervisor and virtualization technology, a specially designed virtual machine was developed providing the same level of isolation that has been trusted for nearly a decade in cloud deployments the world over and pairs it with the speed, density and agility that are the hallmark of containers. Best of all, Windows Server containers with or without Hyper-V isolation are fully interchangeable providing the administrator with the flexibility to choose the right technology for their unique environment. Hyper-V isolation can also be used with Linux containers, enabling these containers to run on a Windows host. This means customers will no longer have to deploy two separate container infrastructures to support both their Windows and Linux-based applications.

Emulated Domain Identity	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

Emulated Domain Identity allows services and scheduled tasks within a container to run using Active Directory identity. It allows applications to authenticate using an Active Directory Group Managed Service Account. For example, an enterprise web application could use Windows Integrated Authentication to connect to a SQL Server instead of using a stored username and password. Domain credentials are not stored in the container image, and are instead provided to the container image as its deployed. That allows the same container to be safely reused in different Active Directory domains to support development, staging and production scenarios.

Traditional model

This section describes the traditional (non-container focused) model for applications.

Desired State Configuration (DSC)	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	●	●

PowerShell Desired State Configuration (DSC) enables cloud scale configuration management. It is a declarative platform used for configuration, deployment, and management of systems. For more information, see the DSC Updates topic in the PowerShell section below.

Pester	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

The Pester test framework was initially developed as an open source project. It is now built into Windows Server 2016 and Windows 10. For more information, see the Pester Test Framework topic in the PowerShell section below.

Just Enough Administration (JEA)	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

Just Enough Administration (JEA) provides a Role-Based Access Control (RBAC) platform through PowerShell. It allows specific users to perform specific tasks without giving them administrator rights. For more information, see the Just Enough Administration topic in the Security section above.

Internet Information Services 10 (IIS 10)

Wildcard Host Headers	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

IIS 10.0 now supports Wildcard Host Headers, enabling admins to setup a webserver for a domain, e.g. contoso.com, and then have the webserver serve requests for any subdomain.

IISAdministration PowerShell module	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

IIS 10.0 introduces IISAdministration, a new PowerShell module for managing IIS.

- IISAdministration will scale better in scripts that take a long time to run with WebAdministration.
- You can now get a direct reference to an instance of Microsoft.Web.Administration.ServerManager object and do anything that you can do in Microsoft.Web.Administration namespace alongside your scripts.
- PowerShell pipeline compatibility was the driving force behind the design of many cmdlets. As such, IISAdministration works much better with PowerShell Pipeline.

HTTP/2	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	○	●

Windows Server 2016 adds support for HTTP/2 protocol. This allows numerous enhancements over HTTP/1.1 such as more efficient reuse of connections and decreased latency, improving web page load times. HTTP/2 support in Windows Server 2016 is added to the Networking stack (HTTP.sys) and integrated with IIS 10.0, allowing IIS 10.0 websites to automatically serve HTTP/2 requests for supported configurations.

Multi-tenant high-density websites	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	●	●

IIS provides a hosting-friendly web server platform with FTP Logon Attempt Restriction and improved site density, centralized SSL certificate support, and server name indication. The following capabilites are provided:

- Increased Internet Information Services (IIS) scalability with SSL scalability, centralized SSL certificate support, and NUMA-aware scalability.
- Binding a more secure site required a unique network endpoint using an IP address and a port in the previous versions of Windows Server, which often meant having a dedicated IP address for each secure site because site owners wanted their secure sites to be running on a standard SSL port.
- Support for increased density of secure sites for greater scalability of sites.

Dynamic IP restrictions	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	○	●	●

Dynamic IP restrictions provide protection against brute force attacks with automatic detection of attacks in- progress and blocking of future requests from the same address. It also supports the ability to modify the number of times FTP will allow users to attempt unsuccessfully to log in within a specified time period before denying access to the IP address.

Multiple language support	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	◑	●	●

IIS contains support for programming languages, such as .NET, PHP, Node.js, and Python. Enhanced support for PHP and MySQL through IIS extensions. IIS provides ASP.NET 4.5 integration and support for the latest HTML5 standards.

Distributed Transaction Coordinator

Microsoft Distributed Transaction Coordinator enhancements	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016
	◑	◑	●

Microsoft Distributed Transaction Coordinator (MSDTC) enhanced features in Windows Server 2016 include:

- New interface and method for Rejoin function in resource manager.
- Enlarged DSN name for XA.
- Include image file path in tracing file name.