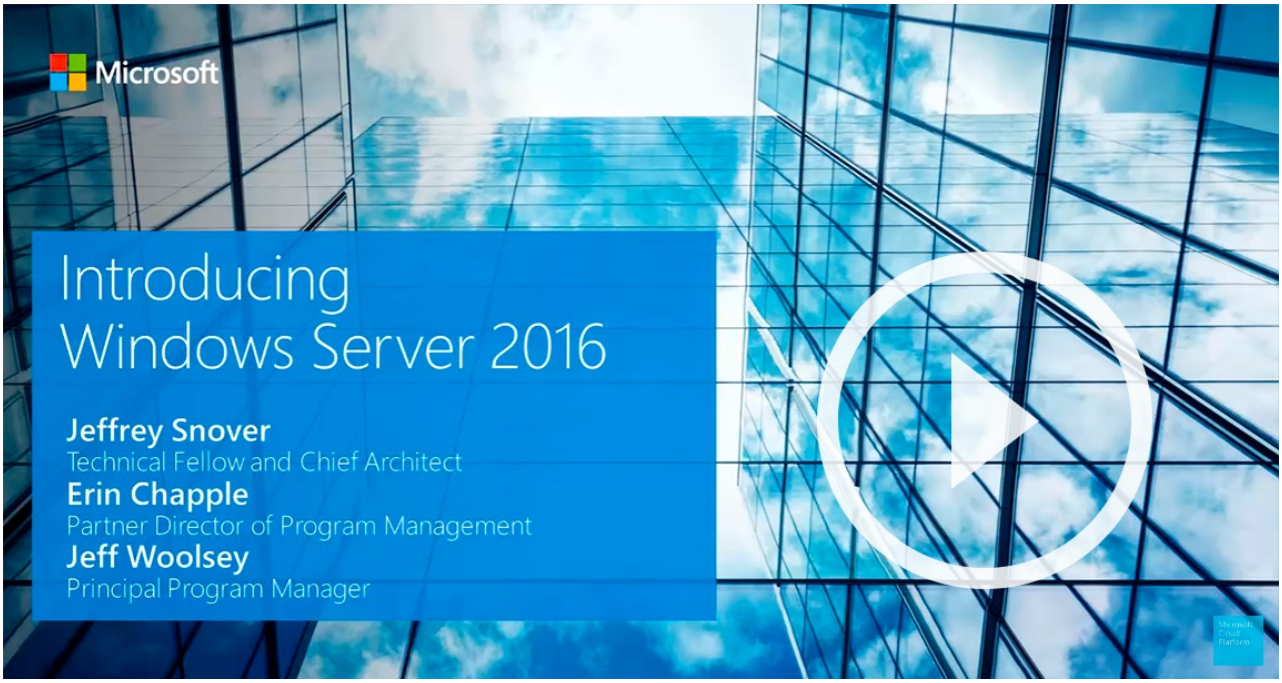
Table of Contents

Windows Server 2016

5/9/2017 • 2 min to read • Edit Online

This library provides info for IT pros to evaluate, plan, deploy, secure, and manage Windows Server 2016.



What's New?

Get Started

Administer

Failover Clustering

Identity and Access

Networking

Remote Access

Security and Assurance

Storage

Virtualization

> **NOTE**
>
> To experience first-hand new features and functionality available in Windows Server 2016, you can download an evaluation version by visiting Windows Server Evaluations.

Windows Server 2016 editions

Windows Server 2016 is available in Standard, Datacenter, and Essentials editions. Windows Server 2016 Datacenter includes unlimited virtualization rights plus new features to build a software-defined datacenter. Windows Server 2016 Standard offers enterprise-class features with limited virtualization rights. Windows Server Essentials is an ideal cloud-connected first server. It has its own extensive documentation—the content here focuses on Standard and Datacenter editions. The following table briefly summarizes the key differences between Standard and Datacenter editions:

FEATURE	DATACENTER	STANDARD
Core functionality of Windows Server	yes	yes
OSEs / Hyper-V containers	unlimited	2
Windows Server containers	unlimited	unlimited
Host Guardian Service	yes	yes
Nano Server installation option	yes	yes
Storage features including Storage Spaces Direct and Storage Replica	yes	no
Shielded Virtual Machines	yes	no
Software Defined Networking Infrastructure (Network Controller, Software Load Balancer, and Multi-tenant Gateway)	yes	no

For more information, see Pricing and licensing for Windows Server 2016 and Compare features in Windows Server versions.

Installation options

Both Standard and Datacenter editions offer three installation options:

- **Server Core:** reduces the space required on disk, the potential attack surface, and especially the servicing requirements. This is the **recommended** option unless you have a particular need for additional user interface elements and graphical management tools.
- **Server with Desktop Experience:** installs the standard user interface and all tools, including client experience features that required a separate installation in Windows Server 2012 R2. Server roles and features are installed with Server Manager or by other methods.
- **Nano Server:** is a remotely administered server operating system optimized for private clouds and datacenters. It is similar to Windows Server in Server Core mode, but significantly smaller, has no local logon capability, and

only supports 64-bit applications, tools, and agents. It takes up far less disk space, sets up significantly faster, and requires far fewer updates and restarts than the other options.

> **NOTE**
>
> Unlike some previous releases of Windows Server, you cannot convert between Server Core and Server with Desktop Experience after installation. For example, if you install Server Core and later decide to user Server with Desktop Experience, you should do a fresh installation (and vice versa).

Now that you know which edition and installation option is right for you, click below to get started with Windows Server 2016.

Nano Server -
Lightest weight

Server Core -
Recommended

Desktop Experience -
Full interface

Get Started with Windows Server 2016

4/24/2017 • 1 min to read • Edit Online

Applies To: Windows Server 2016

This collection contains detailed information to help you determine if you're ready to move to Windows Server 2016. Once you've checked the system requirements, upgrade options, and other information about moving to Windows Server 2016, you're ready to go back to the main Windows Server 2016 hub and start down the path to installing the best edition and installation option for your needs.

NOTE

To download Windows Server 2016, see Windows Server Evaluations.

System Requirements

Find out the minimum hardware requirements to install and run Windows Server 2016.

Release Notes: Important Issues in Windows Server

Issues that could cause serious problems if you don't avoid or work around them.

Recommendations for moving to Windows Server 2016

Comprehensive table of available approaches for getting to Windows Server 2016 in various scenarios.

Features Removed or Deprecated in Windows Server 2016

Features that have already been removed from Windows Server 2016 or designated for potential future removal.

Upgrade and Conversion Options

Description of all the ways to move to Windows Server 2016 from whatever you're running today.

Server Role Upgrade and Migration Matrix

Information about additional steps needed to bring particular server roles to Windows Server 2016

Server Application Compatibility Table

Does SQL work on Windows Server 2016? What steps are needed to get Exchange running? This topic explains what you'll need to do.

Server Activation Guide

Basic information on activation of Windows Server 2016 itself and other operating systems by using Windows Server 2016.

Administer Windows Server 2016

5/23/2017 • 1 min to read • Edit Online

Applies To: Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Administration features and tools help IT pros run and manage Windows Server.

Microsoft Server Performance Advisor

With Microsoft Server Performance Advisor (SPA), you can collect metrics to diagnose performance issues on Windows servers unobtrusively without adding software agents or reconfiguring production servers. SPA generates comprehensive performance reports and historical charts with recommendations.

Server Manager

The content in this section describes how to use Server Manager in Windows Server to manage both local and remote Windows-based servers from desktop computers.

Software Inventoy Logging (SIL)

Software Inventory Logging in Windows Server is a feature with a simple set of PowerShell cmdlets that help server administrators retrieve a list of the Microsoft software that is installed on their servers. It also provides the capability to collect and forward this data periodically over the network to a target web server, using the HTTPS protocol, for aggregation. Managing the feature, primarily for hourly collection and forwarding, is also done with PowerShell commands.

User Access Logging (UAL)

User Access Logging aggregates unique client device and user request events that are logged on a computer running Windows Server 2012 or 2016 into a local database. These records are then made available (through a query by a server administrator) to retrieve quantities and instances by server role, by user, by device, by the local server, and by date. In addition, UAL also enables non-Microsoft software developers to instrument their UAL events to be aggregated.

Windows Server Update Services (WSUS)

The content in this section describes how to configure and manage WSUS. In this section you will find information about installing the WSUS Server Role, configuring WSUS servers, as well as managing updates, and managing WSUS client computers and WSUS computer groups.

Windows Commands

The Windows command-line tools are used to perform administrative tasks in Windows. You can use the command

reference to familiarize yourself with the command-line tools, to learn about the command shell, and to automate command-line tasks by using batch files or scripting tools.

See Also

- Manage connections from Windows operating system components to Microsoft services
- Configure Windows telemetry in your organization

Failover Clustering in Windows Server 2016

4/24/2017 • 2 min to read • Edit Online

Applies To: Windows Server 2016

Failover clustering - a Windows Server feature that enables you to group multiple servers together into a fault-tolerant cluster - provides new and improved features for software-defined datacenter customers and many other workloads running clusters on physical hardware or in virtual machines.

A failover cluster is a group of independent computers that work together to increase the availability and scalability of clustered roles (formerly called clustered applications and services). The clustered servers (called nodes) are connected by physical cables and by software. If one or more of the cluster nodes fail, other nodes begin to provide service (a process known as failover). In addition, the clustered roles are proactively monitored to verify that they are working properly. If they are not working, they are restarted or moved to another node.

Failover clusters also provide Cluster Shared Volume (CSV) functionality that provides a consistent, distributed namespace that clustered roles can use to access shared storage from all nodes. With the Failover Clustering feature, users experience a minimum of disruptions in service.

Failover Clustering has many practical applications, including:

- Highly available or continuously available file share storage for applications such as Microsoft SQL Server and Hyper-V virtual machines
- Highly available clustered roles that run on physical servers or on virtual machines that are installed on servers running Hyper-V

What's new

Here are some of the new features in Windows Server 2016 - for more details, see What's new in Failover Clustering:

Cluster operating system rolling upgrades

Enables an administrator to upgrade the operating system of the cluster nodes from without stopping the Hyper-V or the Scale-Out File Server workloads.

Cloud Witness for a Failover Cluster

A new type of quorum witness that leverages Microsoft Azure to help determine which cluster node should be considered authoritative if a node goes offline.

Health Service

Improves the day-to-day monitoring, operations, and maintenance experience of Storage Spaces Direct clusters.

Fault Domains

Enables you to define what fault domain to use with a Storage Spaces Direct cluster. A fault domain is a set of hardware that share a single point of failure, such as a server node, server chassis, or rack.

VM load balancing

Helps load be evenly distributed across nodes in a Failover Cluster by identifying busy nodes and live-migrating VMs on these nodes to less busy nodes.

Simplified SMB Multichannel and multi-NIC cluster networks

Enables easier configuration of multiple network adapters in a cluster.

Planning

- Failover Clustering Hardware Requirements and Storage Options
- Validate Hardware for Failover Clustering
- Network Recommendations for a Hyper-V Cluster

Deployment

- Installing the Failover Clustering Feature and Tools
- Validate Hardware for a Failover Cluster
- Prestage Cluster Computer Objects in Active Directory Domain Services
- Creating a Failover Cluster
- Deploy Hyper-V over SMB
- Deploy a Scale-Out File Server
- iSCSI Target Block Storage, How To
- Deploy an Active Directory Detached Cluster
- Using Guest Clustering for High Availability
- Deploy a Guest Cluster using a Shared Virtual Hard Disk
- Building Your Cloud Infrastructure: Scenario Overview

Operations

- Configure and Manage the Quorum in a Failover Cluster
- Use Cluster Shared Volumes in a Failover Cluster
- Cluster-Aware Updating Overview

Tools and settings

- Failover Clustering PowerShell Cmdlets
- Cluster Aware Updating PowerShell Cmdlets

Community resources

- High Availability (Clustering) Forum
- Failover Clustering and Network Load Balancing Team Blog

Identity and Access in Windows Server 2016

4/24/2017 • 1 min to read • Edit Online

Applies To: Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

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

What's new in Active Directory Federation Services for Windows Server 2016

An overview of all of the new features available for AD FS in Windows Server 2016.

What's new in Active Directory Domain Services for Windows Server 2016

Lists all the new features available for AD DS in Windows Server 2016.

Privileged Access Management for Active Directory Domain Services (AD DS)

Privileged Access Management (PAM) for Active Directory Domain Services (AD DS) is a solution that is based on Microsoft Identity Manager (MIM) and Windows Server 2012 R2 and Windows Server 2016.

Windows 10 for the enterprise: Ways to use devices for work

Windows 10 provides you the ability to leverage Azure Active Directory. Windows 10 devices can be connected to Azure AD, and users can sign in to Windows with Azure AD accounts or add their Azure ID to gain access to business apps and resources.

Active Directory Domain Services

Detailed documentation on all of the features available for AD DS in Windows Server 2016.

Active Directory Federation Services

Detailed documentation on all of the features available for AD FS in Windows Server 2016.

Solutions and Scenario Guides

- Secure access to company resources from any location on any device
- Join to Workplace from Any Device for SSO and Seamless Second Factor Authentication Across Company Applications
- Manage Risk with Additional Multi-Factor Authentication for Sensitive Applications

- Manage Risk with Conditional Access Control

Networking

5/19/2017 • 7 min to read • Edit Online

Applies To: Windows Server 2016

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.

When you manage networks as a software defined resource, you can describe an application's infrastructure requirements one time, and then choose where the application runs - on premises or in the cloud.

This consistency means that your applications are now easier to scale, and you can seamlessly run applications - anywhere - with equal confidence about security, performance, quality of service, and availability.

> **NOTE**
> To download Windows Server 2016, see Windows Server Evaluations.

Windows Server 2016 adds the following new networking technologies:

- Software Defined Networking: Network Controller provides a centralized, programmable point of automation to manage, configure, monitor, and troubleshoot virtual and physical network infrastructure in your datacenter. Network Controller allows you to use Network Function Virtualization to easily deploy virtual machines (VMs) for Software Load Balancing (SLB) to optimize network traffic loads for your tenants, and RAS Gateways to provide tenants with the connectivity options they need between Internet, on-prem, and cloud resources. You can also use Network Controller to manage Datacenter Firewall on VMs and Hyper-V hosts.
- Network Platform: Using new features for existing Network Platform technologies, you can use DNS Policy to customize your DNS server responses to queries, use a converged NIC that handles combined Remote Direct Memory Access (RDMA) and Ethernet traffic, use Switch Embedded Teaming (SET) to create Hyper-V Virtual Switches connected to RDMA NICs, and use IP Address Management (IPAM) to manage DNS zones and servers as well as DHCP and IP addresses.

For more information, see Windows Server 2016 Supported Networking Scenarios.

The following sections provide information about SDN technologies and Network Platform technologies.

Software Defined Networking technologies

Software Defined Networking (SDN)

You can use this topic to learn about the SDN technologies that are provided in Windows Server, System Center, and Microsoft Azure.

> **NOTE**
> For Hyper-V hosts and virtual machines (VMs) that run SDN infrastructure servers, such as Network Controller and Software Load Balancing nodes, you must install Windows Server 2016 Datacenter edition. For Hyper-V hosts that contain only tenant workload VMs that are connected to SDN-controlled networks, you can run Windows Server 2016 Standard edition.

Deploy a Software Defined Network infrastructure using scripts

This guide provides instructions on how to deploy Network Controller with virtual networks and gateways in a test lab environment.

Network Controller

Network Controller provides a centralized, programmable point of automation to manage, configure, monitor, and troubleshoot virtual and physical network infrastructure in your datacenter.

Software Load Balancing (SLB) for SDN

Cloud Service Providers (CSPs) and Enterprises that are deploying Software Defined Networking (SDN) in Windows Server 2016 can use Software Load Balancing (SLB) to evenly distribute tenant and tenant customer network traffic among virtual network resources. The Windows Server SLB enables multiple servers to host the same workload, providing high availability and scalability.

RAS Gateway for SDN

RAS Gateway, which is a software-based, multitenant, Border Gateway Protocol (BGP) capable router in Windows Server 2016, is designed for Cloud Service Providers (CSPs) and Enterprises that host multiple tenant virtual networks using Hyper-V Network Virtualization.

Network Function Virtualization

In 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.

Datacenter Firewall Overview

Datacenter Firewall is a network layer, 5-tuple (protocol, source and destination port numbers, source and destination IP addresses), stateful, multitenant firewall.

Networking Technologies

The following table provides links to some of the networking technologies in Windows Server 2016.

What's New in Networking

You can use the following sections to discover new networking technologies and new features for existing technologies in Windows Server 2016.

BranchCache

BranchCache is a wide area network (WAN) bandwidth optimization technology. To optimize WAN bandwidth when users access content on remote servers, BranchCache fetches content from your main office or hosted cloud content servers and caches the content at branch office locations, allowing client computers at branch offices to access the content locally rather than over the WAN.

Core Network Guide for Windows Server 2016

Learn how to deploy a Windows Server network with the Core Network Guide, as well as add features to your network deployment with Core Network Companion Guides.

DirectAccess

DirectAccess allows connectivity for remote users to organization network resources without the need for

traditional Virtual Private Network (VPN) connections.

DirectAccess documentation is now located in the Remote access and server management section of the Windows Server 2016 table of contents, under Remote Access. For more information, see DirectAccess.

Domain Name System (DNS)

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.

Dynamic Host Configuration Protocol (DHCP)

Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information, such as the subnet mask and default gateway.

Hyper-V Network Virtualization

Hyper-V Network Virtualization (HNV) enables virtualization of customer networks on top of a shared physical network infrastructure.

Hyper-V Virtual Switch

The Hyper-V Virtual Switch is a software-based layer-2 Ethernet network switch that is available in Hyper-V Manager when you install the Hyper-V server role. The switch includes programmatically managed and extensible capabilities to connect virtual machines to both virtual networks and the physical network. In addition, Hyper-V Virtual Switch provides policy enforcement for security, isolation, and service levels.

Hyper-V Virtual Switch documentation is now located in the **Virtualization** section of the Windows Server 2016 table of contents. For more information, see Hyper-V Virtual Switch.

IP Address Management (IPAM)

IP Address Management (IPAM) is an integrated suite of tools to enable end-to-end planning, deploying, managing and monitoring of your IP address infrastructure, with a rich user experience. IPAM automatically discovers IP address infrastructure servers and Domain Name System (DNS) servers on your network and enables you to manage them from a central interface.

Network Load Balancing

Network Load Balancing (NLB) distributes traffic across several servers using the TCP/IP networking protocol. For non-SDN deployments, NLB ensures that stateless applications, such as Web servers running Internet Information Services (IIS), are scalable by adding more servers as the load increases.

Network Offload and Optimization Technologies

Network offload and optimization technologies in Windows Server 2016 include Software Only (SO) features and technologies, Software and Hardware (SH) integrated features and technologies, and Hardware Only (HO) features and technologies.

The following offload and optimization technology documentation is also available.

- Converged Network Interface Card (NIC) Configuration Guide
- Data Center Bridging (DCB)
- Virtual Receive Side Scaling (vRSS)

Network Policy Server

Network Policy Server (NPS) allows you to create and enforce organization-wide network access policies for connection request authentication and authorization.

Network Shell (Netsh)

You can use the Network Shell (netsh) networking utility to manage networking technologies in Windows Server

2016 and Windows 10.

Network Subsystem Performance Tuning

This topic provides information about choosing the right network adapter for your server workload, ordering network interfaces, network related performance counters, and performance tuning network adapters and related networking technologies, such as Receive Side Scaling (RSS), Receive Side Coalescing (RSC), and others.

NIC Teaming

NIC Teaming allows you to group 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.

Remote Access

You can use Remote Access technologies, such as DirectAccess and Virtual Private Networking (VPN) to provide remote workers with connectivity to internal network resources. In addition, you can use Remote Access for local area network (LAN) routing, and for Web Application Proxy. which provides reverse proxy functionality for web applications inside your corporate network to allow users on any device to access them from outside the corporate network.

Remote Access documentation is now located in the Remote access and server management section of the Windows Server 2016 table of contents. For more information, see Remote Access.

For more information about Web Application Proxy, which is a role service of the Remote Access server role, see Web Application Proxy in Windows Server 2016.

Windows Internet Name Service (WINS)

Windows Internet Name Service (WINS) is a legacy computer name registration and resolution service that maps computer NetBIOS names to IP addresses. Using DNS is recommended over using WINS.

Additional Resources

Networking resources for operating systems earlier than Windows Server 2016 are available at the following locations.

- Windows Server 2012 and Windows Server 2012 R2 Networking Overview
- Windows Server 2008 and Windows Server 2008 R2 Networking
- Windows Server 2003 Windows Server 2003/2003 R2 Retired Content

Remote access and server management

4/24/2017 • 1 min to read • Edit Online

Remote Desktop Services

Remote Desktop Services enables users to access Windows-based programs that are installed on a Remote Desktop Session Host (RD Session Host) server, or to access the full Windows desktop. With Remote Desktop Services, users can access an RD Session Host server from within a corporate network or from the Internet.

Remote Access

The Remote Access server role includes DirectAccess and virtual private network (VPN), local area network (LAN) Routing, and Web Application Proxy. RAS allows you to provide network connectivity to remote employees, site-to-site VPN to connect remote office locations over the Internet, and the RAS Gateway, which has multitenant and Border Gateway Protocol (BGP) capabilities for Enterprises and Cloud Service Providers (CSPs).

Web Application Proxy

Web Application Proxy provides reverse proxy functionality for web applications inside your corporate network to allow users on any device to access them from outside the corporate network safely and securely.

Multipoint Services

Use MultiPoint Services to enable multiple users, each with their own independent and familiar Windows experience, to simultaneously share one computer.

Remote Server Administration Tools

To ease remote server management, you can download and install Remote Server Administration Tools for Windows 10. Remote Server Administration Tools for Windows 10 includes Server Manager, Microsoft Management Console (mmc) snap-ins, consoles, Windows PowerShell cmdlets and providers, and some command-line tools for managing roles and features that run on Windows Server 2016.

Security and Assurance in Windows Server 2016

5/23/2017 • 5 min to read • Edit Online

Applies To: Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

You can rely on new layers of protection built into the operating system to further safeguard against security breaches. Help block malicious attacks and enhance the security of your virtual machines, applications, and data.

Windows Server 2016 Security Blog Post

This blog post from the Windows Server security team highlights many of the improvements in Windows Servers 2016 that increase security for hosting and hybrid cloud environments.

Datacenter and Private Cloud Security Blog

This is the central blog site for technical content from the Microsoft Datacenter and Private Cloud Security team.

Addressing emerging threats and landscape shifts

In this 6-minute video, Anders Vinberg provides an overview of Microsoft's security and assurance strategy, and discusses industry trends and landscape shifts as they relate to security. He then focuses on Microsoft's key initiatives to protect workloads from the underlying fabric, and protect against direct attacks from privileged accounts. Finally, in case of breach, he explains how new detection and forensic capabilities can help better identify the threat.

Protecting Your Datacenter and Cloud from Emerging Threats blog post

This blog post discusses how you can use Microsoft technologies to protect your datacenter and cloud investments from emerging threats.

Security and Assurance Overview session at Ignite 2015

This Ignite session addresses persistent threats, insider breaches, organized cybercrime, and securing the Microsoft Cloud Platform (on-premises and connected services with Azure). It includes scenarios for securing workloads, large enterprise tenants, and service providers.

Secure virtualization with Shielded VMs

Shielded VM in Channel 9

A walkthrough of Shielded VM technology and benefits

Shielded VM Demo

This 4-minute video describes the value of shielded VMs and the differences between a shielded VM and a non-shielded VM.

Shielded Virtual Machines in Windows Server video walkthrough

This video walkthrough shows how the Host Guardian Service, a new role available in Windows Server 2016, enables shielded virtual machines so that sensitive data is protected from unauthorized access by Hyper-V host administrators.

Harden the Fabric: Protecting Tenant Secrets in Hyper-V (Ignite Video)

This Ignite presentation discusses enhancements in Hyper-V, Virtual Machine Manager, and a new Guardian Server role to enable shielded VMs.

Guarded Fabric Deployment Guide

This guide provides installation and validation information for Windows Server 2016 and System Center Virtual Machine Manager for Guarded Fabric Hosts and Shielded VMs.

Shielded VM and Guarded Fabric Operations Guide

This guide provides best practices and recommendations for how to configure your Shielded VM environment, including information specific to Guarded Hosts and tenants.

Shielded VM and Guarded Fabric Troubleshooting Guide

This guide provides information about how to resolve issues you may encounter in your Shielded VM environment.

Shielded VM Article

This white paper provides an overview of how shielded VMs provide increased overall security to prevent tampering.

Privileged Access Management

Securing Privileged Access

A road-map for how you can secure your privileged access. This road-map is built based on the combined expertise of the server security team, Microsoft IT, Azure team and the Microsoft Consulting Services

Just in Time Administration with Microsoft Identity Manager

This article discusses features and capabilities included in Microsoft Identity Manager, including support for Just In Time (JIT) Privileged Access Management.

Protecting Windows and Microsoft Azure Active Directory with Privileged Access Management

This Ignite presentation covers Microsoft's strategy and investments in Windows Server, PowerShell, Active Directory, Identity Manager, and Azure Active Directory for addressing the risks of administrator access through stronger authentication, and managing access using Just in Time and Just Enough Administration (JEA).

Just Enough Administration Article

This document shares the vision and technical details of Just Enough Administration, a PowerShell toolkit designed to help organizations reduce risk by restricting operators to the only access required to perform specific tasks.

Just Enough Administration demo video

Just Enough Administration demo walk through

Credential Protection

Protect derived domain credentials with Credential Guard

Credential Guard uses virtualization-based security to isolate secrets so that only privileged system software can access them. Unauthorized access to these secrets can lead to credential theft attacks, such as Pass-the-Hash or Pass-The-Ticket. Credential Guard prevents these attacks by protecting NTLM password hashes and Kerberos Ticket Granting Tickets.

Protect Remote Desktop credentials with Remote Credential Guard

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. |

Credential Guard demo video

This 5-minute video demos Credential Guard and Remote Credential Guard

Hardening the OS and applications

Device Guard Deployment Guide

Device Guard is a combination of enterprise-related hardware and software security features that, when configured together, will lock a device down so that it can only run trusted applications that you define in your code integrity.

Device Guard demo video

This 7-minute video presents Device Guard and its usage on Windows Server 2016

Control Flow Guard

Control Flow Guard provides built-in protection against some classes of memory corruption attacks.

Windows Defender

Windows Defender provides active detection capabilities to block known malware. Windows Defender is turned on by default and is optimized to support the various server roles in Windows Server 2016.

Detecting and Responding to Threats

Security Threat Analysis Using Microsoft Operations Management Suite

This Ignite presentation discusses how you can use Operational Insights to perform security threat analysis.

Microsoft Operations Management Suite (OMS)

The Microsoft Operations Management Suite (OMS) Security and Audit solution processes security logs and firewall events from on-premises and cloud environments to analyze and detect malicious behavior.

OMS and Windows Server 2016

This 3-minute video shows how OMS can help detect potential malicious behavior that is blocked by Windows Server 2016

Microsoft Advanced Threat Analytics

This blog post discusses Microsoft Advanced Threat Analytics, an on-premises product that uses Active Directory network traffic and SIEM data to discover and alert on potential threats.

Microsoft Advanced Threat Analytics

This 3-minute video presents an overview of how Microsoft is adding threat analytics capabilities in Windows Server 2016. |

Network Security

Datacenter Firewall Overview

This overview discusses Datacenter Firewall, a network layer, 5-tuple (protocol, source and destination port numbers, source and destination IP addresses), stateful, multitenant firewall.

What's New in DNS in Windows Server 2016

This overview topic provides brief descriptions of new capabilities in DNS, along with links for more information.

Mapping security features to compliance regulations

Compliance is an important aspect of security features. We leave the expert advice on how to achieve your compliance and what compliance looks like to your trusted compliance advisers, but we also want to provide initial mapping for you to be able to use when evaluating Windows Server 2016.

- Hyper-V Shielded VMs compliance mapping whitepaper
- JEA and JIT compliance mapping whitepaper
- Device Guard compliance mapping whitepaper
- Credential Guard compliance mapping whitepaper
- Windows Defender compliance mapping whitepaper

Storage in Windows Server 2016

4/24/2017 • 6 min to read • Edit Online

Applies To: Windows Server 2016

Storage in Windows Server 2016 provides new and improved features for software-defined datacenter (SDDC) customers focusing on virtualized workloads. Windows Server also provides extensive support for enterprise customers using file servers with existing workloads.

To find out about what's new in storage, see What's new in storage and What's new in Failover Clustering.

For an overview of storage technologies included in Windows Server, see the following list (categorized by workload).

Software-defined storage for virtualized workloads

Storage Spaces (including the new Storage Spaces Direct)

Storage Spaces now includes support for Storage Spaces Direct - a new architecture for Storage Spaces clusters that uses directly attached local storage - including SATA and NVME devices. Other enhancements include the ability to optimize disk usage after adding new physical disks and faster virtual disk repair times.

Storage Replica (new)

Storage Replica enables storage-agnostic, block-level, synchronous replication between clusters or servers for disaster preparedness and recovery, as well as stretching of a failover cluster across sites for high availability. Synchronous replication enables mirroring of data in physical sites with crash-consistent volumes, ensuring zero data loss at the file system level. Asynchronous replication allows site extension beyond metropolitan ranges.

Storage QoS (new)

Storage Quality of Service (QoS) provides a way to centrally monitor and manage storage performance for virtual machines using Hyper-V and the Scale-Out File Server roles. The feature automatically improves storage resource fairness between multiple virtual machines using the same file server cluster and allows specific minimum and maximum performance goals to be configured in units of normalized IOPs.

Data Deduplication

Data Deduplication is a feature of Windows Server 2016 that can help reduce the impact of redundant data on storage costs. When enabled, Data Deduplication optimizes free space on a volume by examining the data on the volume for duplication. Once identified, duplicated portions of the volume's dataset are stored once and are (optionally) compressed for additional savings. Data Deduplication optimizes redundancies without compromise data fidelity or integrity.

General-purpose file servers

Work Folders

With Work Folders users can store and access work files on personal computers and devices, often referred to as bring-your-own device (BYOD), in addition to corporate PCs. Users gain a convenient location to store work files, and they can access them from anywhere. Organizations maintain control over corporate data by storing the files on centrally managed file servers, and optionally specifying user device policies such as encryption and lock-screen passwords.

Offline Files, Folder Redirection, and Roaming User Profiles

Folder Redirection and Offline Files are used together to redirect the path of local folders (such as the Documents folder) to a network location, while caching the contents locally for increased speed and availability. Roaming User Profiles is used to redirect a user profile to a network location.

DFS Replication

Enables you to efficiently replicate folders (including those referred to by a DFS namespace path) across multiple servers and sites. DFS Replication uses a compression algorithm known as remote differential compression (RDC). RDC detects changes to the data in a file, and it enables DFS Replication to replicate only the changed file blocks instead of the entire file.

DFS Namespaces

Enables you to group shared folders that are located on different servers into one or more logically structured namespaces. Each namespace appears to users as a single shared folder with a series of subfolders. However, the underlying structure of the namespace can consist of numerous file shares that are located on different servers and in multiple sites.

File Classification

File Classification, also known as File Classification Infrastructure (FCI) provides insight into your data by automating classification processes so that you can manage your data more effectively. You can classify files and apply policies based on this classification. Example policies include dynamic access control for restricting access to files, file encryption, and file expiration. Files can be classified automatically by using file classification rules or manually by modifying the properties of a selected file or folder.

File Screens

File screens help you control the types of files that user can store on a file server. You can limit the extension that can be stored on your shared files. For example, you can create a file screen that does not allow files with an MP3 extension to be stored in personal shared folders on a file server.

File Management Tasks

File Management Tasks enables you to apply a conditional policy or action to files based on their classification. The conditions of a file management task include the file location, the classification properties, the date the file was created, the last modified date of the file, or the last time the file was accessed. The actions that a file management task can take include the ability to expire files, encrypt files, or run a custom command.

Quotas

Quotas allow you to limit the space that is allowed for a volume or folder, and they can be automatically applied to new folders that are created on a volume. You can also define quota templates that can be applied to new volumes or folders.

Storage Reports

Storage reports are used to help you identify trends in disk usage and how your data is classified. You can also monitor a selected group of users for attempts to save unauthorized files.

iSCSI Target Server

iSCSI Target Server provides block storage to other servers and applications on the network by using the Internet SCSI (iSCSI) standard.

iSCSI Target Boot

iSCSI Target Server in Windows Server can boot hundreds of computers from a single operating system image that is stored in a centralized location. This improves efficiency, manageability, availability, and security.

File systems, protocols, etc.

ReFS

ReFS is a resilient file system that maximizes data availability, scales efficiently to very large data sets across diverse workloads, and provides data integrity by means of resiliency to corruption (regardless of software or hardware failures).

SMB

The Server Message Block (SMB) protocol is a network file sharing protocol that allows applications on a computer to read and write to files and to request services from server programs in a computer network. The SMB protocol can be used on top of its TCP/IP protocol or other network protocols. Using the SMB protocol, an application (or the user of an application) can access files or other resources at a remote server. This allows applications to read, create, and update files on the remote server. It can also communicate with any server program that is set up to receive an SMB client request.

Storage-class memory

Storage-class memory such as NVDIMM-N devices provide performance similar to computer memory (really fast), but with the data persistence of normal storage drives. Windows treats storage-class memory similary to normal drives (just faster), but there are some differences in the way device health is managed.

BitLocker

BitLocker Drive Encryption stores data on volumes in an encrypted format, even if the computer is tampered with or when the operating system is not running. This helps protect against offline attacks, attacks made by disabling or circumventing the installed operating system, or made by physically removing the hard drive to attack the data separately.

NTFS

NTFS—the primary file system for recent versions of Windows and Windows Server—provides a full set of features including security descriptors, encryption, disk quotas, and rich metadata, and can be used with Cluster Shared Volumes (CSV) to provide continuously available volumes that can be accessed simultaneously from multiple nodes of a Failover Cluster.

NFS

Network File System (NFS) provides a file sharing solution for enterprises that have heterogeneous environments that consist of both Windows and non-Windows computers.

See also

- PowerShell cmdlets in Windows Server 2016 and Windows 10
- What's new in storage
- What's new in Failover Clustering
- Azure Storage
- Azure StorSimple

Virtualization

5/8/2017 • 3 min to read • Edit Online

Applies To: Windows Server 2016

Virtualization in Windows Server 2016 is one of the foundational technologies required to create your software defined infrastructure. Along with networking and storage, virtualization features deliver the flexibility you need to power workloads for your customers.

Windows Server 2016 Virtualization technologies include updates to Hyper-V, Hyper-V Virtual Switch, and Guarded Fabric and Shielded Virtual Machines (VMs), that improve security, scalability, and reliability. Updates to failover clustering, networking, and storage make it even easier to deploy and manage these technologies when used with Hyper-V.

Windows Containers is a new technology that offers you another way to deploy flexible, software-based computing power.

> **NOTE**
> To download Windows Server 2016, see Windows Server Evaluations.

The following sections contain brief technology overviews and links to Virtualization documentation.

Guarded Fabric and Shielded VMs

As a cloud service provider or enterprise private cloud administrator, you can use a guarded fabric to provide a more secure environment for VMs. A guarded fabric consists of one Host Guardian Service (HGS) - typically, a cluster of three nodes - plus one or more guarded hosts, and a set of shielded VMs.

For more information, see Guarded Fabric and Shielded VMs.

Hyper-V

The Hyper-V technology provides computing resources through hardware virtualization. Hyper-V creates a software version of computer, called a virtual machine, which you use to run an operating system and applications. You can run multiple virtual machines at the same time, and can create and delete them as needed.

Hyper-V requires specific hardware to create the virtualization environment. For details, see System requirements for Hyper-V on Windows Server 2016.

Hyper-V on Windows Server 2016

Hyper-V is a server role in both Windows Server 2016 Datacenter and Standard editions.

Learn more about Hyper-V, the hardware you need, the operating systems you can run in your virtual machines, and more. If you're new to Hyper-V, start with the Hyper-V Technology Overview.

For more information, see Hyper-V on Windows Server 2016

Hyper-V on Windows 10

Hyper-V is available in some versions of Windows 10, Windows 8.1, and Windows 8.

Hyper-V on Windows is geared toward development and test activities and gives you a quick and easy way to run different operating systems without deploying more hardware.

For more information, see Hyper-V on Windows 10.

Microsoft Hyper-V Server 2016

The Hyper-V technology is also available separately from Windows and Windows Server, as a free, standalone product. Hyper-V Server is commonly used as the host in a virtualized desktop infrastructure (VDI) environment.

For more information, see Microsoft Hyper-V Server 2016.

Hyper-V Virtual Switch

The Hyper-V Virtual Switch is a software-based layer-2 Ethernet network switch that is included in all versions of Hyper-V.

Hyper-V Virtual Switch is available in Hyper-V Manager after you install the Hyper-V server role.

Included in Hyper-V Virtual Switch are programmatically managed and extensible capabilities that allow you to connect virtual machines to both virtual networks and the physical network.

In addition, Hyper-V Virtual Switch provides policy enforcement for security, isolation, and service levels.

Additional Virtualization Technologies for Windows Server 2016 and Windows 10

Following are links to documentation for other Microsoft Windows virtualization technologies.

Windows Containers

You can use Windows Server and Hyper-V containers to provide standardized runtime environments for development, test, and production teams.

Windows Containers provide operating system-level virtualization that allows multiple isolated applications to be run on a single system. Two different types of container runtimes 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 Containers encapsulate each container in a light-weight virtual machine.

For more information, see Windows Containers Documentation on the Microsoft Developer Network (MSDN).

Windows Server technical content

4/24/2017 • 1 min to read • Edit Online

Windows Server is the platform for building an infrastructure of connected applications, networks, and web services, from the workgroup to the data center.

Use the links below to view content for the different versions of Windows Server.

Windows Server 2016

Windows Server 2016 technical content

Windows Server 2012 R2 and Windows Server 2012

Windows Server 2012 R2 and Windows Server 2012 Technical Library

Windows Server 2012 R2 Developer Library on MSDN

Windows Server 2008 R2 and Windows Server 2008

Windows Server 2008 R2 and Windows Server 2008 Technical Library

Windows Server 2008 Developer Library on MSDN

Windows Server 2003

Windows Server 2003 Technical Library - download a PDF version of the archived content

Windows Server 2003 Developer Library on MSDN

Product evaluations

Download Windows Server 2016 Evaluation

Download Windows Server 2012 R2 Trial

Related links

Windows Server 2016 product information