What's new in Windows Server 2016

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

Compute

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

General

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

Hyper-V

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

- Windows Server 2016 now includes a programmable Hyper-V switch. Microsoft's Network Controller pushes HNV policies down to a Host Agent running on each host using the Open v Switch Database Management Protocol (OVSDB) as the South Bound Interface (SBI). The Host Agent stores this policy using a customization of the VTEP schema and programs complex flow rules into a perform ant flow engine in the Hyper-V switch. The flow engine in the Hyper-V switch is the same one that Azure uses. The entire SDN stack up through the Network Controller and Network Resource provider is also consistent with Azure, making its performance comparable to the Azure public cloud. Within Microsoft's flow engine, the Hyper-V switch is equipped to handle both stateless and state ful flow rules through a simple match action mechanism that defines how packets should be processed within the switch.
- HNV now supports Virtual eXtensible Local Area Network (VXLAN) protocol encapsulation. HNV uses the VXLAN protocol in MAC distribution mode through the Microsoft Network Controller to map tenant overly network IP addresses to the physical underlay network IP addresses. The NVGRE and VXLAN Task Offloads support third-party drivers for improved performance.
- Windows Server 2016 includes a software load balancer (SLB) with full support for virtual network traffic and seamless interaction with HNV. The performant flow engine implements the SLB in the data plane v-Switch, then the Network Controller controls it for Virtual IP (VIP) or Dynamic IP (DIP) mappings.
- HNV implements correct L2 Ethernet headers to ensure interoperability with third-party virtual and physical appliances that depend on industry-standard protocols. Microsoft ensures that all transmitted packets have compliant values in all fields to guarantee interoperability. HNV requires

support for Jumbo Frames (MTU > 1780) in the physical L2 network to account for packet overhead introduced by encapsulation protocols such as NVGRE and VXLAN. Jumbo Frame support ensures that guest Virtual Machines attached to an HNV Virtual Network maintain a 1514 MTU.
- Windows Container support adds performance improvements, simplified network management, and support for Windows containers on Windows 10. For more information, see Containers: Docker, Windows, and Trends.

Nano Server

What's New in Nano Server. Nano Server now has an updated module for building Nano Server images, including more separation of physical host and guest virtual machine functionality and support for different Windows Server editions.

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

Shielded Virtual Machines

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

- A new **Encryption Supported** mode that offers more protections than for an ordinary virtual machine, but less than **Shielded** mode, while still supporting vTPM, disk encryption, Live Migration traffic encryption, and other features, including direct fabric administration conveniences such as virtual machine console connections and PowerShell Direct.
- Full support for converting existing non-shielded Generation 2 virtual machines to shielded virtual machines, including automated disk encryption.
- Hyper-V Virtual Machine Manager can now view the fabrics upon which a shielded virtual is authorized to run, providing a way for the fabric administrator to open a shielded virtual machine's key protector (KP) and view the fabrics it is permitted to run on.
- You can switch Attestation modes on a running Host Guardian Service. Now you can switch on the fly between the less secure but simpler Active Directory-based attestation and TPM-based attestation.
- End-to-end diagnostics tooling based on Windows PowerShell that is able to detect misconfigurations or errors in both guarded Hyper-V hosts and the Host Guardian Service.
- A recovery environment that offers a means to securely troubleshoot and repair shielded virtual machines within the fabric in which they normally run while offering the same level of protection as the shielded virtual machine itself.
- Host Guardian Service support for existing safe Active Directory – you can direct the Host Guardian Service to use an existing Active Directory forest as its Active Directory instead of creating its own Active Directory instance

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

Identity and Access

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

Active Directory Certificate Services

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

Active Directory Domain Services

Active Directory Domain Services includes improvements to help organizations secure Active Directory environments and provide better identity management experiences for both corporate and personal devices. For more information, see What's new in Active Directory Domain Services (AD DS) in Windows Server 2016.

Active Directory Federation Services

Active Directory Federation Services (AD FS) in Windows Server 2016 includes new features that enable you to configure AD FS to authenticate users stored in Lightweight Directory Access Protocol (LDAP) directories. For more information, see What's New in AD FS for Windows Server 2016.

Web Application Proxy

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

Administration

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

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

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

Here are some other new administration features:

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

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

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

Package Management unified package management for software discovery, installation, and inventory

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

PowerShell enhancements to assist digital forensics and help reduce security breaches

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

Networking

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

Software-Defined Networking

You can now both mirror and route traffic to new or existing virtual appliances. Together with a distributed firewall and Network security groups, this enables you to dynamically segment and secure workloads in a manner similar to Azure. Second, you can deploy and manage the entire Software-defined

networking (SDN) stack using System Center Virtual Machine Manager. Finally, you can use Docker to manage Windows Server container networking, and associate SDN policies not only with virtual machines but containers as well. For more information, see Plan a Software Defined Network Infrastructure.

TCP performance improvements

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

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

Security and Assurance

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