Microsoft

Server Virtualization

Windows Server 2012

Windows Server 2012

Table of contents

Copyright information

Windows Server 2012 Hyper-V: A more complete virtualization platform

Traditional datacenters were built with physical servers running a dedicated workload. Each server in the datacenter was designed, purchased, deployed, and maintained for the sole purpose of running a single workload. If the workload was later retired or upgraded, the physical server was either repurposed or retired.

This approach had several significant drawbacks, including:

- **High operational costs** due to low server utilization resulting in non-optimized physical space allocation and power consumption.
- **Long deployment cycles** due to lengthy purchase processes for, and manual deployment of, new servers every time the datacenter added new workloads.

Virtualization, however, has enabled a new generation of datacenters. Instead of each workload requiring a dedicated server, virtualization makes it possible to run multiple workloads on the same server. This addresses the issue of low server utilization; it also reduces the total number of physical servers and thus overall power consumption in the datacenter.

With Windows Server 2012 Hyper-V, it is now easier than ever for organizations to take advantage of the cost savings of virtualization and make the optimum use of server hardware investments by consolidating multiple server roles as separate virtual machines. You can use Hyper-V to efficiently run multiple operating systems — Microsoft Windows, Linux, and others — in parallel, on a single server. Windows Server 2012 extends this with more features, greater scalability and built-in reliability mechanisms.

In the datacenter, on the desktop, and now in the cloud, the Microsoft virtualization platform—led by Hyper-V and management tools—offers exceptional value for the money.

More secure multitenancy

A critical requirement of datacenters in today's cloud-based computing and services environment is that they provide a common infrastructure serving multiple groups or customers—all the while keeping each group's data private and secure by enforcing full isolation of each workload from all other groups' workloads. Multitenancy, as it is known, provided a good level of workload isolation between virtual machines in server virtualization, but until Windows Server 2012, the network layer of the virtualized datacenter was still not fully isolated.

Windows Server 2012 incorporates Hyper-V Network Virtualization to provide more secure multitenancy through features such as:

- **Multitenant security and isolation**. This provides the flexibility to restrict any customer's access to a virtual machine on any node while still maintaining network and storage traffic isolation.

- **Extending the Hyper-V Extensible Switch for new capabilities**. The Hyper-V Extensible Switch supports third-party plug-in extensions that can provide enhanced networking and security capabilities tailored to the unique complexities and requirements of your virtual environment.

Flexible infrastructure, when and where you need it

Adding and moving servers is now faster and easier. New features give you the flexibility to place and move servers in your datacenter as needed, with ease. Among these new features and benefits are:

- **Scale beyond VLANs with Hyper-V Network Virtualization**. Network Virtualization provides the flexibility to place a virtual machine on any node regardless of its IP address, even across the cloud.
- **Migrate virtual machines without downtime**. Live migration improvements add the flexibility to move multiple virtual machines without limitation, including outside a clustered environment.
- **Move virtual machine storage with no downtime**. You now have the flexibility to move virtual hard disks without any significant downtime.
- **Reliably import virtual machines**. The Import Wizard for virtualization makes it easier and safer to import multiple servers for virtualization.
- **Merge snapshots while the virtual machine is running**. This feature allows live merging of virtual machine snapshots. You now apply changes or manage a snapshot with little effect on users.
- **Use new automation support for Hyper-V**. IT pros can easily automate Hyper-V management tasks and reduce the administrative overhead in a cloud computing environment. This support provides you with more than 140 Hyper-V cmdlets for Microsoft Windows PowerShell.

Scale, performance, and density

Designing for an increase in datacenter scale requires that various capabilities be considered, such as:

- Virtual machine density.
- Hardware innovations resulting in ever higher performance servers.
- Hardware acceleration technologies, whenever these are beneficial.

Windows Server 2012 Hyper-V includes a significant number of new features that let you take advantage of the latest hardware on servers, network adapters, and storage devices. This all leads to increased scalability of the datacenter and fewer physical servers needed to run more virtual machine workloads. These features include:

- **Hyper-V host scale and scale-up workload support**. With this support, you can configure up to 320 logical processors on hardware, 4 TB of physical memory, 64 virtual processors, and up to 1 TB of memory on a virtual machine. You also can have up to 64 nodes and 4,000 virtual machines in a cluster.
- **Dynamic Memory improvements for Hyper-V**. These improvements dramatically increase virtual machine consolidation ratios and improve reliability for restart operations. This can lead to lower costs, especially in environments that have many idle or low-load virtual machines (such as VDI).
- **Resource Metering in Hyper-V**. Resource Metering provides the ability to track and report the amount of data that is transferred per IP address or virtual machine—helping to ensure accurate showback and chargeback.

- **New virtual hard disk format**. This new format, called VHDX, is designed to better handle current and future workloads. It also addresses the technological demands of an enterprise's evolving needs by increasing storage capacity, protecting data, improving quality performance on 4 KB disks, and providing additional operation-enhancing features.
- **Offloaded Data Transfer support in Hyper-V**. With offloaded data transfer support, the CPU can concentrate on the processing needs of the application rather than networking or storage overhead.
- **Data Center Bridging**. Data Center Bridging (DCB) takes advantage of current innovations to reduce the cost and difficulty of maintaining separate network, management, live migration, and storage traffic by using a modern, converged 10-gigabit (G) local area network (LAN).
- **Virtual Fibre Channel in Hyper-V**. This feature provides the ability to cluster Hyper-V guest operating system over Fibre Channel.
- **Support for 4 KB disk sectors in Hyper-V virtual disks**. Support for 4,096 byte (4 KB) disk sectors lets you take advantage of the emerging innovation in storage hardware that provides increased capacity and reliability.
- **Quality of Service**. Quality of Service (QoS) provides the ability to programmatically adhere to a service level agreement (SLA) by specifying the minimum bandwidth that is available to a virtual machine or a port. It prevents latency issues by allocating maximum bandwidth use for a virtual machine or port.

High availability

Building highly scalable datacenters also implies the need for complete redundancy. No single component in a modern datacenter can be assumed to work forever, but with the right platform support, the datacenter can be designed to:

- Be resilient to failures.
- Increase resiliency for customers who move to a virtualized platform.

To ensure that Windows Server 2012 meets and exceeds these design requirements for high availability, many new features have been developed, including the following:

- **Incremental backups**. This feature permits true differential disk backups of virtual hard disks to help ensure that data is backed up and restored when necessary. It also reduces storage costs because it backs up only what has changed, not the entire disk.
- **Hyper-V Replica**. Asynchronous, application-consistent virtual machine replication is built into Windows Server 2012. It permits replication of Hyper-V virtual machines between two locations for business continuity and failure recovery. Hyper-V Replica works with nearly any server, network, and storage vendors.
- **NIC Teaming**. Servers often require full resiliency. At the network level, this means two network adapters should be teamed together to act as one. If one adapter fails, the other adapter can still provide connectivity to that server. Network Interface Card (NIC) Teaming provides resiliency (failover) in addition to load balancing and aggregation of bandwidth.
- **Hyper-V clustering enhancements**. By clustering your virtualized platform, you can increase availability and enable access to server-based applications during planned or unplanned downtime. Windows Server 2012 provides many new enhancements for your Hyper-V clustered environment.

More secure multitenancy

This section contains a description of the new Hyper-V features in Windows Server 2012 that provide more secure multitenancy in your virtualized environment. The feature sections included are:

- Multitenant security and isolation.
- Extending the Hyper-V Extensible Switch for new capabilities.

Multitenant security and isolation

Virtualized datacenters are becoming more popular and practical every day. IT organizations and hosting providers have begun offering infrastructure as a service (IaaS), which provides more flexible, virtualized infrastructures (“server instances on-demand”) to customers. Because of this trend, IT organizations and hosting providers must offer customers enhanced security and isolation from one another.

If you’re hosting two companies, you must ensure that each company is provided its own privacy and security. Before Windows Server 2012, server virtualization provided isolation between virtual machines, but the network layer of the datacenter was still not fully isolated and implied layer-2 connectivity between different workloads that run over the same infrastructure.

For the hosting provider, isolation in the virtualized environment must be equal to isolation in the physical datacenter, to meet customer expectations and not be a barrier to cloud adoption.

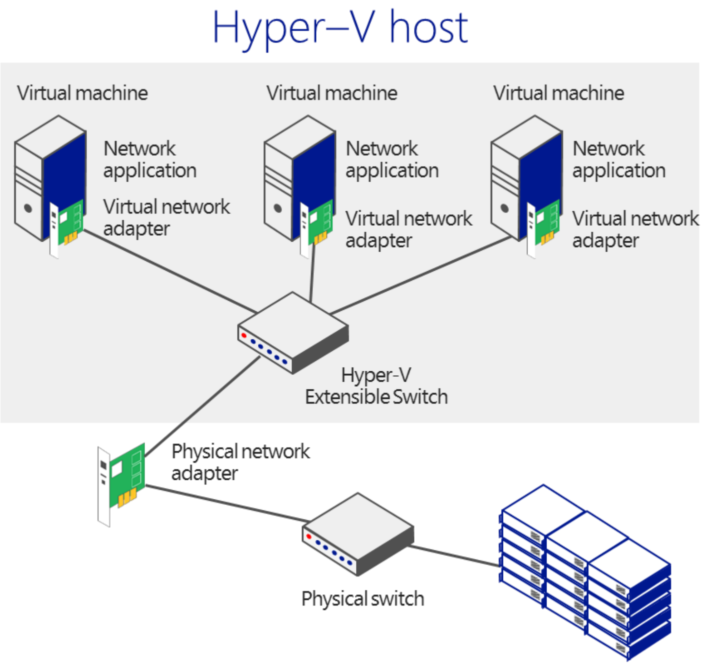
Isolation is almost as important in an enterprise environment. Although all internal departments belong to the same organization, certain workloads and environments (such as finance and human resources systems) must still be isolated from each other. IT departments that offer private clouds and move to an IaaS operational model must consider this requirement and provide a way to isolate such highly sensitive workloads.

Windows Server 2012 contains new security and isolation capabilities through the Hyper-V Extensible Switch.

Technical description

The Hyper-V Extensible Switch is a layer-2 virtual network switch that provides programmatically managed and extensible capabilities to connect virtual machines to the physical network with policy enforcement for security and isolation. The figure on the following page shows a network using the Hyper-V Extensible Switch.

Figure 1: Network with Hyper-V Extensible Switch



With Windows Server 2012, you can configure Hyper-V servers to enforce network isolation among any set of arbitrary isolation groups, which are typically defined for individual customers or sets of workloads.

Windows Server 2012 provides the isolation and security capabilities for multitenancy by offering the following new features:

- Multitenant virtual machine isolation through private virtual LANs (PVLANs).
- Protection from Address Resolution Protocol/Neighbor Discovery (ARP/ND) poisoning (also called spoofing).
- Protection against Dynamic Host Configuration Protocol (DHCP) snooping and DHCP guard.
- Isolation and metering using virtual port access control lists (ACLs).
- The ability to trunk traditional VLANs to virtual machines.
- Monitoring.
- Windows PowerShell/Windows Management Instrumentation (WMI).

Virtual machine isolation with PVLANs

VLAN technology is traditionally used to subdivide a network and provide isolation for individual groups that share a common physical infrastructure. Windows Server 2012 introduces support for PVLANs, a technique used with VLANs that can be used to provide isolation between two virtual machines on the same VLAN.

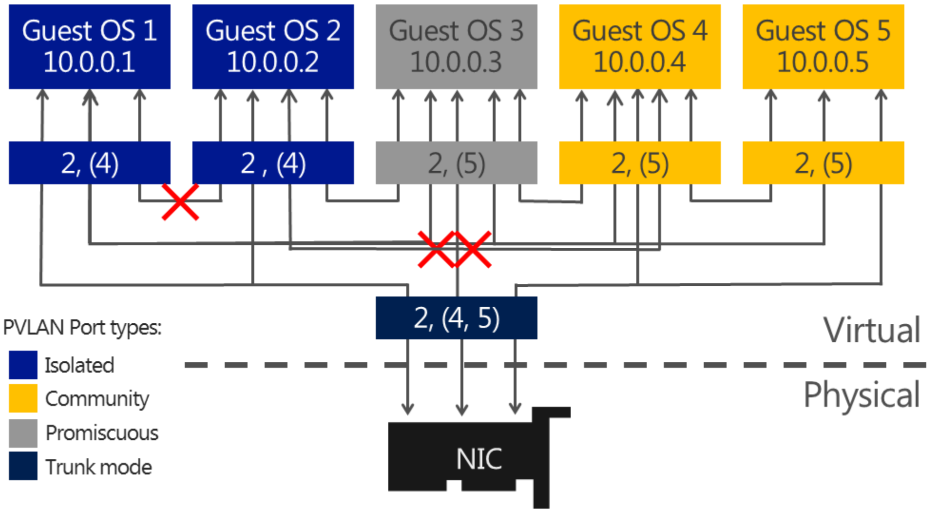
When a virtual machine doesn’t need to communicate with other virtual machines, you can use PVLANs to isolate it from other virtual machines in your datacenter. By assigning each virtual machine in a PVLAN, one primary VLAN ID and one or more secondary VLAN IDs, you can put the secondary PVLANs into one of three modes (as shown in the following table). These PVLAN modes determine which other virtual machines on the PVLAN a virtual machine can talk to. To isolate a virtual machine, put it in isolated mode.

Table 1: PVLAN modes for virtual machine isolation

PVLAN mode	Description
Isolated	Isolated ports cannot exchange packets with each other at layer 2.
Promiscuous	Promiscuous ports can exchange packets with any other port on the same primary VLAN ID.
Community	Community ports on the same VLAN ID can exchange packets with each other at layer 2.

The following figure shows how the three PVLAN modes can be used to isolate virtual machines that share a primary VLAN ID.

Figure 2: Example PVLAN with primary VLAN ID 2



Example PVLAN:
– Primary VLAN ID is 2
– Secondary VLAN IDs are 4 and 5

ARP/ND poisoning and spoofing protection

The Hyper-V Extensible Switch provides protection against a malicious virtual machine stealing IP addresses from other virtual machines through ARP spoofing (also known as ARP poisoning in IPv4). With this type of man-in-the-middle attack, a malicious virtual machine sends a fake ARP message, which associates its own MAC address to an IP address that it doesn’t own. Unsuspecting virtual machines send network traffic targeted to that IP address to the MAC address of the malicious virtual machine instead of the intended destination. For IPv6, Windows Server 2012 provides equivalent protection for ND spoofing.

DHCP Guard protection

In a DHCP environment, a rogue DHCP server could intercept client DHCP requests and provide incorrect address information. The rogue DHCP server could cause traffic to be routed to a malicious intermediary that sniffs all traffic before forwarding it to the legitimate destination. To protect against this particular man-in-the-middle attack, the Hyper-V administrator can designate which Hyper-V Extensible Switch ports can have DHCP servers connected to them. DHCP server traffic from other Hyper-V Extensible Switch ports is automatically dropped. The Hyper-V Extensible Switch now protects against a rogue DHCP server attempting to provide IP addresses that would cause traffic to be rerouted.

Virtual port ACLs for network isolation and metering

Port ACLs provide a mechanism for isolating networks and metering network traffic for a virtual port on the Hyper-V Extensible Switch. By using port ACLs, you can meter the IP addresses or MAC addresses that can (or cannot) communicate with a virtual machine. For example, you can use port ACLs to enforce isolation of a virtual machine by letting it talk only to the Internet, or communicate only with a predefined set of addresses. By using the metering capability, you can measure network traffic going to or from a specific IP address or MAC address, which lets you report on traffic, sent or received from the Internet or from network storage arrays.

You also can configure multiple port ACLs for a virtual port. Each port ACL consists of a source or destination network address, and a permit to deny or meter action. The metering capability also supplies information about the number of instances where traffic was attempted to or from a virtual machine from a restricted (“deny”) address.

Trunk mode to virtual machines

A VLAN makes a set of host machines or virtual machines appear to be on the same local LAN, independent of their actual physical locations. With the Hyper-V Extensible Switch trunk mode, traffic from multiple VLANs can now be directed to a single network adapter in a virtual machine that could previously receive traffic from only one VLAN. As a result, traffic from different VLANs is consolidated, and a virtual machine can listen in on multiple VLANs. This feature can help you shape network traffic and enforce multitenant security in your datacenter.

Monitoring

Many physical switches can monitor the traffic from specific ports flowing through specific virtual machines on the switch. The Hyper-V Extensible Switch also provides this port mirroring, enabling you to designate which virtual ports should be monitored and to which virtual port the monitored traffic should be delivered for further processing. For example, a security-monitoring virtual machine can look for anomalous patterns in the traffic that flows through other specific virtual machines on the switch. In addition, you can diagnose network connectivity issues by monitoring traffic bound for a particular virtual switch port.

Windows PowerShell and WMI

Windows Server 2012 now provides Windows PowerShell cmdlets for the Hyper-V Extensible Switch that lets you build command-line tools or automated scripts for setup, configuration, monitoring, and troubleshooting. These cmdlets can be run remotely. Windows PowerShell also enables third parties to build their own tools to manage the Hyper-V Extensible Switch.

Requirements

Multitenant security and isolation require Windows Server 2012 and the Hyper-V server role.

Summary

Windows Server 2012 multitenant isolation keeps customer virtual machines isolated, even when they are stored on the same physical server. Windows Server 2012 provides better multitenant security for customers on a shared IaaS cloud through the new Hyper-V Extensible Switch, which provides:

- **Security and isolation**. The Hyper-V Extensible Switch provides better security and isolation for IaaS multitenancy with PVLAN support, protection against ARP poisoning and spoofing, protection against DHCP snooping, virtual port ACLs, and VLAN trunk mode support.
- **Monitoring**. With port mirroring, you can run security and diagnostics applications in virtual machines that can monitor virtual machine network traffic. Port mirroring also supports live migration of extension configurations.
- **Manageability**. You can now use Windows PowerShell and WMI support for command-line and automated scripting support, as well as full event logging.

Multitenant isolation in Windows Server 2012 addresses concerns that may have previously prevented organizations from deploying Hyper-V within the datacenters. Two such concerns are:

- Additional management overhead of implementing VLANs on the Ethernet switching infrastructure to ensure isolation between their customers' virtual infrastructures.
- Security risk of a multitenant virtualized environment.

With Hyper-V in Windows Server 2012, you can now use port ACLs to isolate customers' networks from one another and not be required to set up and maintain VLANs. Also, your security needs are met by protection against ARP spoofing and DHCP snooping.

Extending the Hyper-V Extensible Switch for new capabilities

Many enterprises need the ability to extend virtual switch features with their own plug-ins to suit their virtual environment. When IT professionals install virtual switches, they naturally look for the same kind of functionality that they can achieve on physical networks, such as adding firewalls, intrusion detection systems, and network traffic monitoring tools. However, the challenge has been finding easy ways to add virtualized appliances, extensions, and other features and functions to virtual switches. Most virtual switch technology offerings are built around closed systems that make it difficult for enterprise developers and third-party vendors to build solutions and to quickly and easily install new functionality into their virtual switches.

The Hyper-V Extensible Switch changes all that. With the Hyper-V Extensible Switch, IT professionals can easily add more functionality to their virtual machines and networks. At the same time, it gives internal enterprise developers and third-party providers an open platform for creating solutions that extend the basic functionality of the switch. If you're in charge of making IT purchasing decisions at your company, you want to know that the virtualization platform you choose won't lock you in to a small set of compatible features, devices, or technologies.

In Windows Server 2012, the Hyper V Extensible Switch provides new extensibility features.

Technical description

The Hyper-V Extensible Switch in Windows Server 2012 is a layer-2 virtual network switch that provides programmatically managed and extensible capabilities to connect virtual machines to the physical network. The Hyper-V Extensible Switch is an open platform that lets multiple vendors provide extensions written to standard Windows API frameworks. The reliability of extensions is strengthened through the Windows standard framework and reduction of required third-party code for functions, and is backed by the Windows Hardware Quality Labs (WHQL) certification program. You can manage the Hyper-V Extensible Switch and its extensions by using Windows PowerShell, or programmatically with WMI or the Hyper-V Manager UI.

This section focuses on open extensibility and manageability for third-party extensions. For additional capabilities of the Hyper-V Extensible Switch, see the "Quality of Service" and "Multitenant Security and Isolation" sections in this paper.

Extensibility

The Hyper-V Extensible Switch architecture in Windows Server 2012 is an open framework that lets third parties add new functionality such as monitoring, forwarding, and filtering into the virtual switch. Extensions are implemented by using Network Device Interface Specification (NDIS) filter drivers and Windows Filtering Platform (WFP) callout drivers. These two public Windows platforms for extending Windows networking functionality are used as follows:

- **NDIS filter drivers** are used to monitor or modify network packets in Windows. NDIS filters were introduced with the NDIS 6.0 specification.
- **WFP callout drivers**, introduced in Windows Vista and Windows Server 2008, let independent software vendors (ISVs) create drivers to filter and modify TCP/IP packets, monitor or authorize connections, filter IP security (IPsec)-protected traffic, and filter remote procedure calls (RPCs). Filtering and modifying TCP/IP packets provides unprecedented access to the TCP/IP packet processing path. In this path, you can examine or modify outgoing and incoming packets before additional processing occurs. By accessing the TCP/IP processing path at different layers, you can more easily create firewalls, antivirus software, diagnostic software, and other types of applications and services. For more information, see the Windows Filtering Platform.

Extensions may extend or replace three aspects of the switching process:

- Ingress filtering.
- Destination lookup and forwarding.
- Egress filtering.

In addition, by monitoring extensions you can gather statistical data by monitoring traffic at different layers of the switch. Multiple monitoring and filtering extensions can be supported at the ingress and egress portions of the Hyper-V Extensible Switch. Only one instance of the forwarding extension may be used per switch instance, and it overrides the default switching of the Hyper-V Extensible Switch.

The table on the following page lists the various types of Hyper-V Extensible Switch extensions.

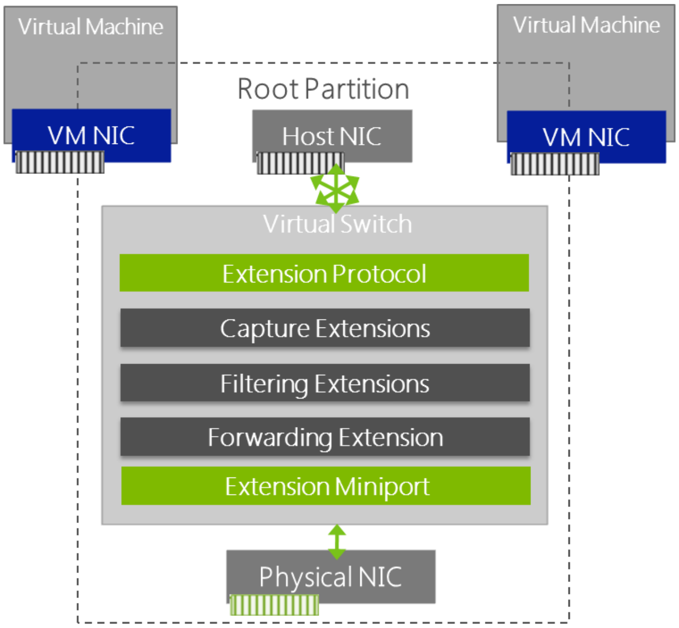
Table 2: Types of Hyper-V Extensible Switch extensions

Extension	Purpose	Examples	Extensibility component
Network Packet Inspection	Inspecting network packets, but not altering them.	sFlow and network monitoring	NDIS filter driver
Network Packet Filter	Injecting, modifying, and dropping network packets.	Security	NDIS filter driver
Network Forwarding	Third-party forwarding that bypasses default forwarding.	OpenFlow, Virtual Ethernet Port Aggregator (VEPA), and proprietary network fabrics	NDIS filter driver
Firewall/ Intrusion Detection	Filtering and modifying TCP/IP packets, monitoring or authorizing connections, filtering IPsec-protected traffic, and filtering RPCs.	Virtual firewall and connection monitoring	WFP callout driver

The Hyper-V Extensible Switch provides an open-switch API that lets enhanced switch and management products work with Hyper-V.

The Hyper-V Extensible Switch architecture in Windows Server 2012 is an open framework that lets third parties add new functionality into the virtual switch. The following figure shows the architecture of the Hyper-V Extensible Switch and the extensibility model.

Figure 3: Architecture of the Hyper-V Extensible Switch



Some other features of Hyper-V Extensible Switch extensibility are:

- **Extension monitoring**. Monitoring extensions lets you gather statistical data by monitoring traffic at different layers of the Hyper-V Extensible Switch. Multiple monitoring and filtering extensions can be supported at the ingress and egress portions of the Hyper-V Extensible Switch.
- **Extension uniqueness**. Extension state/configuration is unique to each instance of an Extensible Switch on a machine.
- **Extensions that learn from virtual machine life cycle**. A virtual machine's activity cycle is similar to that of physical servers, having peak times during various times of the day or night based on its core workloads. Extensions can learn the flow of network traffic based on the workload cycles of your virtual machines, and optimize your virtual network for greater performance.
- **Extensions that can veto state changes**. Extensions can implement monitoring, security, and other features to further improve the performance, management, and diagnostic enhancements of the Hyper-V Extensible Switch. Extensions can help ensure the security and reliability of your system by identifying and blocking implementation of harmful state changes.
- **Multiple extensions on same switch**. Multiple extensions can coexist on the same Hyper-V Extensible Switch.

Manageability

By using the following management features built into the Hyper-V Extensible Switch, you can troubleshoot and resolve problems on Hyper-V Extensible Switch networks:

- **Windows PowerShell and scripting support**. Windows Server 2012 provides Windows PowerShell cmdlets for the Hyper-V Extensible Switch that let you build command-line tools or automated scripts for setup, configuration, monitoring, and troubleshooting. Windows PowerShell also enables third parties to build their own Windows PowerShell–based tools to manage the Hyper-V Extensible Switch.
- **Unified tracing and enhanced diagnostics**. The Hyper-V Extensible Switch includes unified tracing to provide two levels of troubleshooting. At the first level, the Event Tracing for Windows (ETW) provider for the Hyper-V Extensible Switch permits tracing packet events through the Hyper-V Extensible Switch and extensions, making it easier to pinpoint where an issue occurred. The second level permits capturing packets for a full trace of events and traffic packets.

Requirements

Hyper-V Extensible Switch extensibility is built into the Hyper-V server role and requires Windows Server 2012.

Summary

The Hyper-V Extensible Switch is an open platform, so third-party vendors can provide plug-ins that supply additional functionality such as traffic monitoring, firewall filters, and switch forwarding. Plug-in management is unified through Windows PowerShell cmdlets and WMI scripting.

The Hyper-V Extensible Switch permits easier implementation and management of virtualized datacenters by providing the following:

- **Open platform to fuel plug-ins**. The Hyper-V Extensible Switch is an open platform that lets plug-ins sit in the virtual switch between all traffic, including virtual machine–to–virtual machine traffic. Extensions can provide traffic monitoring, firewall filters, and switch forwarding. To jump-start the ecosystem, several partners will announce extensions when the Hyper-V Extensible Switch is released. No “one-switch-only” solution for Hyper-V will occur.

- **Core services provided at no cost**. Core services are provided for extensions. For example, all extensions have live migration support by default, and no special coding for services is required.
- **Windows reliability and quality**. Extensions provide a high level of reliability and quality from the strength of the Windows platform and the Windows logo certification program, both of which set a high bar for extension quality.
- **Unified management**. Managing extensions is integrated into Windows management through Windows PowerShell cmdlets and WMI scripting.
- **Easier support**. Unified tracing makes it quicker and easier to diagnose any issues that arise. This means less downtime and increased availability of services.
- **Live migration support**. The Hyper-V Extensible Switch provides capabilities enabling extensions to participate in Hyper-V live migration.

The Hyper-V Extensible Switch gives third-party vendors the freedom to develop custom solutions for handling network traffic in a Windows Server 2012 virtual network. For example, these solutions can be used to emulate a vendor’s physical switch and its policies, or to monitor and analyze traffic.

Flexible infrastructure, when and where you need it

This section contains a description of new Hyper-V features in Windows Server 2012 which provide flexible infrastructure, when and where you need it. These features enable you to:

- Scale beyond VLANs with Network Virtualization.
- Migrate Virtual Machines without downtime.
- Move Virtual Machine Storage with no downtime.
- Reliably import virtual machines.
- Merge snapshots with minimal downtime.
- Use new automation support for Hyper-V.

Scale beyond VLANs with Hyper-V Network Virtualization

Isolating different departments' or customers' virtual machines can be a challenge on a shared network. When entire networks of virtual machines must be isolated, the challenge becomes even greater. Traditionally, VLANs have been used to isolate networks, but VLANs are very complex to manage on a large scale. The following are the primary drawbacks of VLANs:

- Cumbersome reconfiguration of production switches is required whenever virtual machines or isolation boundaries must be moved. Moreover, frequent reconfigurations of the physical network to add or modify VLANs increases the risk of an outage.
- VLANs have limited scalability because typical switches support no more than 1,000 VLAN IDs (with a maximum of 4,095).
- VLANs cannot span multiple subnets, which limits the number of nodes in a single VLAN and restricts the placement of virtual machines based on physical location.

In addition to these drawbacks, virtual machine IP address assignment presents other key issues when organizations move to the cloud:

- Required renumbering of service workloads.
- Policies that are tied to IP addresses.
- Physical locations that determine virtual machine IP addresses.
- Topological dependency of virtual machine deployment and traffic isolation.

The IP address is the fundamental address that is used for layer-3 network communication because most network traffic is TCP/IP. Unfortunately, when moving to the cloud, the addresses must be changed to accommodate the physical and topological restrictions of the datacenter. Renumbering IP addresses is cumbersome because all associated policies that are based on IP addresses must also be updated.

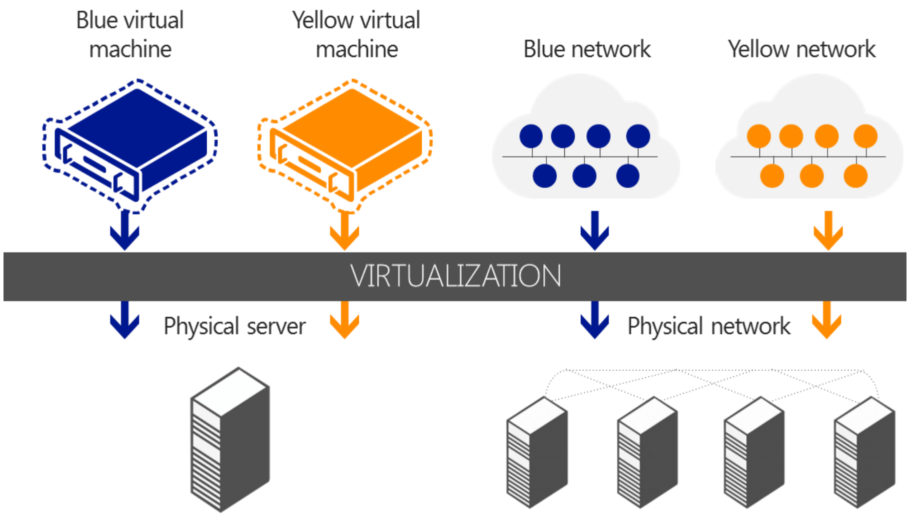
The physical layout of a datacenter influences the permissible potential IP addresses for virtual machines that run on a specific server or blade that is connected to a specific rack in the datacenter. A virtual machine provisioned and placed in the datacenter must adhere to the choices and restrictions regarding its IP address. The typical result is that datacenter administrators assign IP addresses to the virtual machines and force virtual machine owners to adjust all the policies that were based on the original IP address. This renumbering overhead is so high that many enterprises choose to deploy only new services into the cloud and leave legacy applications unchanged.

To solve these problems, Windows Server 2012 introduces Hyper-V Network Virtualization, a new feature that enables you to isolate network traffic from different business units or customers on a shared infrastructure, without having to use VLANs. Network Virtualization also lets you move virtual machines as needed within your virtual infrastructure while preserving their virtual network assignments. You can even use Network Virtualization to transparently integrate these private networks into a preexisting infrastructure on another site.

Technical description

Hyper-V Network Virtualization extends the concept of server virtualization to permit multiple virtual networks, potentially with overlapping IP addresses, to be deployed on the same physical network. With Network Virtualization, you can set policies that isolate traffic in a dedicated virtual network independently of the physical infrastructure. The following figure illustrates how you can use Network Virtualization to isolate network traffic that belongs to two different customers. In the figure, a Blue virtual machine and a Yellow virtual machine are hosted on a single physical network, or even on the same physical server. However, because they belong to separate Blue and Yellow virtual networks, the virtual machines cannot communicate with each other even if the customers assign these virtual machines IP addresses from the same address space.

Figure 4: Hyper-V Network Virtualization



To virtualize the network, Hyper-V Network Virtualization uses the following elements:

- Two IP addresses for each virtual machine.
- Generic Routing Encapsulation (GRE).
- IP address rewrite.
- Policy management server.

IP addresses

Each virtual machine is assigned two IP addresses:

- **Customer Address (CA)** is the IP address that the customer assigns based on the customer's own intranet infrastructure. This address lets the customer exchange network traffic with the virtual machine as if it had not been moved to a public or private cloud. The CA is visible to the virtual machine and reachable by the customer.
- **Provider Address (PA)** is the IP address that the host assigns based on the host's physical network infrastructure. The PA appears in the packets on the wire exchanged with the Hyper-V server hosting the virtual machine. The PA is visible on the physical network, but not to the virtual machine.

The layer of CAs is consistent with the customer's network topology, which is virtualized and decoupled from the underlying physical network addresses, as implemented by the layer of PAs. With Network Virtualization, any virtual machine workload can be executed without modification on any Windows Server 2012 Hyper-V server within any physical subnet, if Hyper-V servers have the appropriate policy settings that can map between the two addresses.

This approach provides many benefits, including cross-subnet live migration, customer virtual machines running IPv4 while the host provider runs an IPv6 datacenter or vice-versa, and using IP address ranges that overlap between customers. But perhaps the biggest advantage of having separate CAs and PAs is that it lets customers move their virtual machines to the cloud with minimal reconfiguration.

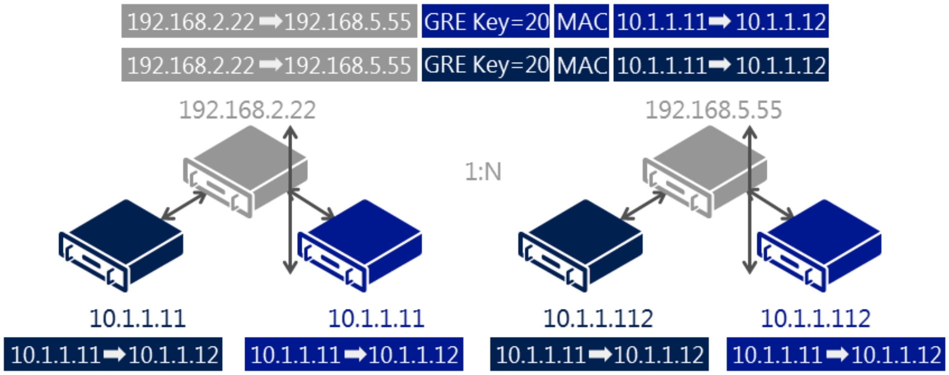
Generic Routing Encapsulation

GRE is a tunneling protocol (defined by RFC 2784 and RFC 2890) that encapsulates various network layer protocols inside virtual point-to-point links over an Internet Protocol network. Hyper-V Network Virtualization in Windows Server 2012 uses GRE IP packets to map the virtual network to the physical network. The GRE IP packet contains the following information:

- One customer address per virtual machine.
- One provider address per host that all virtual machines on the host share.
- A Tenant Network ID embedded in the GRE header Key field.
- Full MAC header.

The following figure illustrates GRE in a Network Virtualization environment.

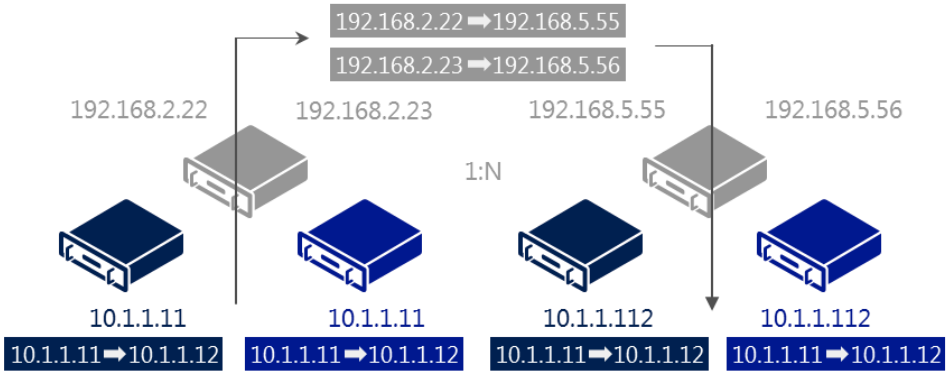
Figure 5: GRE in a Hyper-V Network Virtualization environment



IP Address Rewrite

Hyper-V Network Virtualization uses IP Address Rewrite to map the CA to the PA. Each virtual machine CA is mapped to a unique host PA. This information is sent in regular TCP/IP packets on the wire. With IP Address Rewrite, there is little need to upgrade existing network adapters, switches, and network appliances, and it is immediately and incrementally deployable today with little impact on performance. The following figure illustrates the IP Address Rewrite process.

Figure 6: IP Address Rewrite process



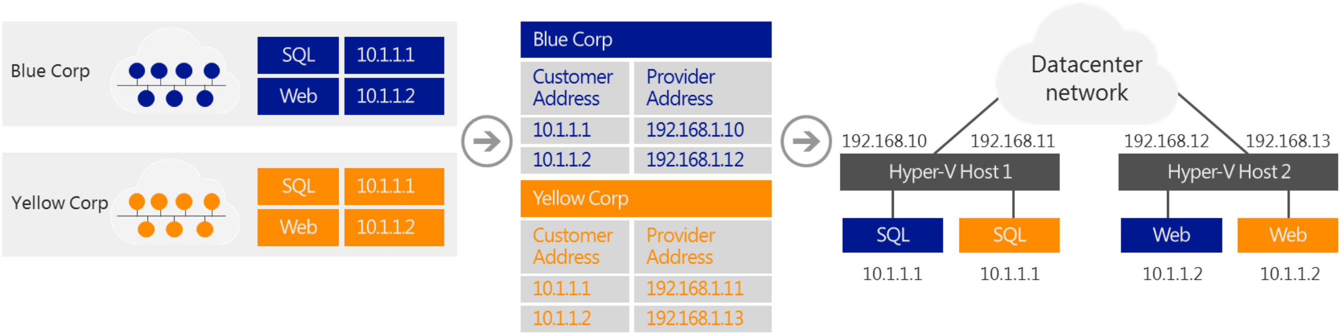
Policy management server

The setting and maintenance of Network Virtualization capabilities require using a policy management server, which may be integrated into the management tools used to manage virtual machines.

Network Virtualization example

Contoso, Ltd. is a service provider that provides cloud services to businesses that need them. Blue Corp and Yellow Corp are two companies that want to move their Microsoft SQL Server infrastructures into the Contoso cloud, but they want to maintain their current IP addressing. Thanks to the new Network Virtualization feature of Hyper-V in Windows Server 2012, Contoso is able to accommodate this customer request, as shown in the following figure.

Figure 7: Companies keep their existing IP addresses—even ones that overlap



Blue Corp	
Customer Address	Provider Address
10.1.1.1	192.168.1.10
10.1.1.2	192.168.1.12

Yellow Corp	
Customer Address	Provider Address
10.1.1.1	192.168.1.11
10.1.1.2	192.168.1.13

Before moving to the hosting provider's shared cloud service:

- Blue Corp ran a SQL Server instance (named SQL) at the IP address 10.1.1.1 and a web server (named WEB) at the IP address 10.1.1.2, which uses its SQL server for database transactions.

- Yellow Corp ran a SQL Server instance, also named SQL and assigned the IP address 10.1.1.1, and a web server, also named WEB and also at the IP address 10.1.1.2, which uses its SQL server for database transactions.

Both Blue Corp and Yellow Corp move their respective SQL and WEB servers to the same hosting provider's shared IaaS service where they run the SQL virtual machines in Hyper-V Host 1 and the WEB virtual machines in Hyper-V Host 2. All virtual machines maintain their original intranet IP addresses (their CAs):

- CAs of Blue Corp virtual machines: SQL is 10.1.1.1, WEB is 10.1.1.2.
- CAs of Yellow Corp virtual machines: SQL is 10.1.1.1, WEB is 10.1.1.2.

Both companies are assigned the following PAs by their hosting provider when the virtual machines are provisioned:

- PAs of Blue Corp virtual machines: SQL is 192.168.1.10, WEB is 192.168.1.12.
- PAs of Yellow Corp virtual machines: SQL is 192.168.1.11, WEB is 192.168.1.13.

The hosting provider creates policy settings that consist of an isolation group for Yellow Corp that maps the CAs of the Yellow Corp virtual machines to their assigned PAs, and a separate isolation group for Blue Corp that maps the CAs of the Blue Corp virtual machines to their assigned PAs. The provider applies these policy settings to both Hyper-V Host 1 and Hyper-V Host 2.

When the Blue Corp WEB virtual machine on Hyper-V Host 2 queries its SQL server at 10.1.1.1, the following occurs:

- Hyper-V Host 2, based on its policy settings, translates the addresses in the packet from:
  Source: 10.1.1.2 (the CA of Blue Corp WEB)
  Destination: 10.1.1.1 (the CA of Blue Corp SQL)
  to
  Source: 192.168.1.12 (the PA for Blue Corp WEB)
  Destination: 192.168.1.10 (the PA for Blue Corp SQL)
- When the packet is received at Hyper-V Host 1, based on its policy settings, Network Virtualization translates the addresses in the packet from:
  Source: 192.168.1.12 (the PA for Blue Corp WEB)
  Destination: 192.168.1.10 (the PA for Blue Corp SQL)
  back to
  Source: 10.1.1.2 (the CA of Blue Corp WEB)
  Destination: 10.1.1.1 (the CA of Blue Corp SQL)
  before delivering the packet to the Blue Corp SQL virtual machine.

When the Blue Corp SQL virtual machine on Hyper-V Host 1 responds to the query, the following happens:

- Hyper-V Host 1, based on its policy settings, translates the addresses in the packet from:
  Source: 10.1.1.1 (the CA of Blue Corp SQL)
  Destination: 10.1.1.2 (the CA of Blue Corp WEB)
  to
  Source: 192.168.1.10 (the PA for Blue Corp SQL)
  Destination: 192.168.1.12 (the PA for Blue Corp WEB)
- When Hyper-V Host 2 receives the packet, based on its policy settings, Network Virtualization translates the addresses in the packet from:
  Source: 192.168.1.10 (the PA for Blue Corp SQL)

Destination: 192.168.1.12 (the PA for Blue Corp WEB)
to
Source: 10.1.1.1 (the CA of Blue Corp SQL)
Destination: 10.1.1.2 (the CA of Blue Corp WEB)
before delivering the packet to the Blue Corp WEB virtual machine.

A similar process for traffic between the Yellow Corp WEB and SQL virtual machines uses the settings in the Yellow Corp isolation group. With Network Virtualization, Yellow Corp and Blue Corp virtual machines interact as if they were on their original intranets, but they are never in communication with each other, even though they are using the same IP addresses. The separate addresses (CAs and PAs), the policy settings of the Hyper-V hosts, and the address translation between CA and PA for inbound and outbound virtual machine traffic, all act to isolate these two sets of servers from each other.

Setting and maintaining Network Virtualization capabilities requires the use of a policy management server, which may be integrated into tools used to manage virtual machines.

Two techniques are used to virtualize the IP address of the virtual machine. The preceding example with Blue Corp and Yellow Corp shows IP Rewrite, which modifies the CA IP address of the virtual machine's packets before they are transferred on the physical network. IP Rewrite can provide better performance because it is compatible with existing Windows networking offload technologies such as VMQs.

The second IP virtualization technique is GRE Encapsulation (RFC 2784). With GRE Encapsulation, all virtual machines packets are encapsulated with a new header before being sent on the wire. GRE Encapsulation provides better network scalability because all virtual machines on a specific host can share the same PA IP address. Reducing the number of PAs means that the load on the network infrastructure associated with learning these addresses (IP and MAC) is greatly reduced.

Requirements

Network Virtualization requires Windows Server 2012 and the Hyper-V server role.

Summary

With Network Virtualization, you now can isolate network traffic from different business units or customers on a shared infrastructure, without having to use VLANs. Network Virtualization also lets you move virtual machines as needed within your virtual infrastructure while preserving their virtual network assignments. Finally, you can use Network Virtualization to transparently integrate these private networks into a pre-existing infrastructure on another site.

Network Virtualization benefits include:

- **Tenant network migration to the cloud with minimum reconfiguration or effect on isolation**. Customers can keep their internal IP addresses while they move workloads onto shared IaaS clouds, minimizing the configuration changes needed for IP addresses, DNS names, security policies, and virtual machine configurations. In software-defined, policy-based datacenter networks, network traffic isolation does not depend on VLANs, but is enforced within Hyper-V hosts, based on multitenant isolation policies. Network administrators can still use VLANs for traffic management of the physical infrastructure if the topology is primarily static.
- **Tenant virtual machine deployment anywhere in the datacenter**. Services and workloads can be placed or migrated to any server in the datacenter while keeping their IP addresses, without being limited to physical IP subnet hierarchy or VLAN configurations.

- **Simplified network and improved server/network resource use**. The rigidity of VLANs, along with the dependency of virtual machine placement on physical network infrastructure, results in overprovisioning and underuse. By breaking this dependency, Virtual Server Virtual Networking increases the flexibility of virtual machine workload placement, thus simplifying network management and improving server and network resource use. Server workload placement is simplified because migration and placement of workloads are independent of the underlying physical network configurations. Server administrators can focus on managing services and servers, while network administrators can focus on overall network infrastructure and traffic management.
- **Works with today's hardware (servers, switches, appliances) to maximize performance**. Network Virtualization can be deployed in today's datacenter, and yet is compatible with emerging datacenter "flat network" technologies, such as TRILL (Transparent Interconnection of Lots of Links), an IETF standard architecture intended to expand Ethernet topologies.
- **Full management through Windows PowerShell and WMI**. You can use Windows PowerShell to script and automate administrative tasks easily. Windows Server 2012 includes Windows PowerShell cmdlets for Network Virtualization that let you build command-line tools or automated scripts for configuring, monitoring, and troubleshooting network isolation policies.

Migrate virtual machines without downtime

To maintain optimal use of physical resources and to add new virtual machines easily, you must be able to move virtual machines whenever necessary—without disrupting your business. Windows Server 2008 R2 introduced live migration, which made it possible to move a running virtual machine from one physical computer to another with no downtime and no service interruption. However, this assumed that the virtual hard disk for the virtual machine remained consistent on a shared storage device such as a Fibre Channel or iSCSI SAN. In Windows Server 2012, live migrations are no longer limited to a cluster and virtual machines can be migrated across cluster boundaries, including to any Hyper-V host server in your environment. Hyper-V builds on this feature, adding support for simultaneous live migrations, enabling you to move several virtual machines at the same time. When combined with features such as Network Virtualization, this feature even allows virtual machines to be moved between local and cloud hosts with ease.

Technical description

Hyper-V live migration makes it possible to move running virtual machines from one physical host to another with no effect on virtual machine availability to users. Hyper-V in Windows Server 2012 introduces faster and simultaneous live migration inside or outside a clustered environment.

As well as providing live migration in the most basic of deployments, this functionality facilitates more advanced scenarios, such as performing a live migration to a virtual machine between multiple, separate clusters to balance loads across an entire datacenter.

Faster and simultaneous migration

If you use live migration in a clustered environment today, you will see that live migrations can now use higher network bandwidths (up to 10 gigabits) to complete migrations faster. You can also perform multiple simultaneous live migrations to quickly move many virtual machines in a cluster.

Live migration outside a clustered environment

Windows Server 2012 Hyper-V live migration lets you perform live migration outside a failover cluster. The two scenarios for this are:

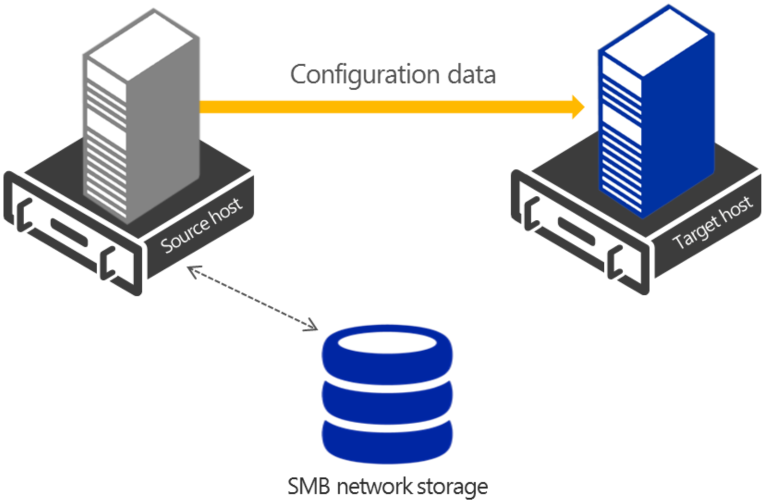
- **SMB-based live migration**. In this instance, each virtual machine's hard disk is stored on a central SMB file share. You then perform a live migration of the virtual machines from one server to another while their storage remains on the central SMB share.
- **"Shared-nothing" live migration**. In this case, the live migration of a virtual machine from one non-clustered Hyper-V host to another begins when the virtual machine's hard drive storage is mirrored to the destination server over the network. Then you perform the live migration of the virtual machine to the destination server while it continues to run and provide network services.

The following subsections walk you through the process of setting up these two types of live migration.

Scenario 1: Setting up a SMB-share-based live migration in Windows Server 2012 Hyper-V

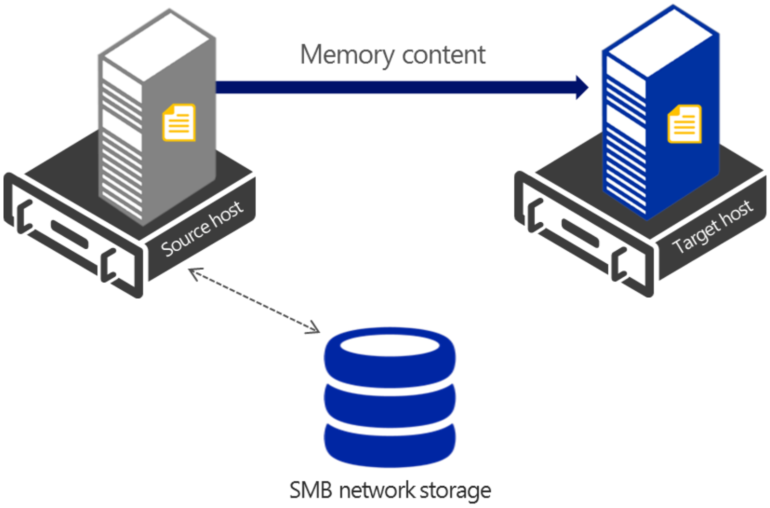
- *Live migration setup*: During the live migration setup stage, the source host creates a TCP connection with the destination host. This connection transfers the virtual machine configuration data to the destination host. A skeleton virtual machine is set up on the destination host, and memory is allocated to the destination virtual machine, as shown in the following figure.

Figure 8: Live migration setup



- *Memory page transfer*: In the second stage of a SMB-based live migration, shown in the following figure, the memory that is assigned to the migrating virtual machine is copied over the network from the source host to the destination host. This memory is referred to as the “working set” of the migrating virtual machine. A page of memory is 4 KB.

Figure 9: Memory pages transferred



For example, suppose that a virtual machine named “Test VM” configured with 1,024 megabytes (MB) of RAM is migrating to another Hyper-V host. The entire 1,024 MB of RAM that is assigned to this virtual machine is in the working set of “Test VM”. The active pages within the “Test VM” working set are copied to the destination Hyper-V host.

In addition to copying the working set of “Test VM” to the destination host, Hyper-V monitors the pages in the working set for “Test VM” on the source host. As “Test VM” modifies the memory pages, it tracks and marks the pages as they are modified. The list of modified pages is simply the list of memory pages that “Test VM” modified after the copy of its working set began.

During this phase of the migration, the migrating virtual machine continues to run. Hyper-V iterates the memory copy process several times, with each iteration requiring a smaller number of modified pages to be copied. After the working set is copied to the destination host, the next stage of the live migration begins.

- *Memory page copy process*: This stage is a memory copy process that duplicates the remaining modified memory pages for “Test VM” to the destination host. The source host transfers the CPU and device state of the virtual machine to the destination host.

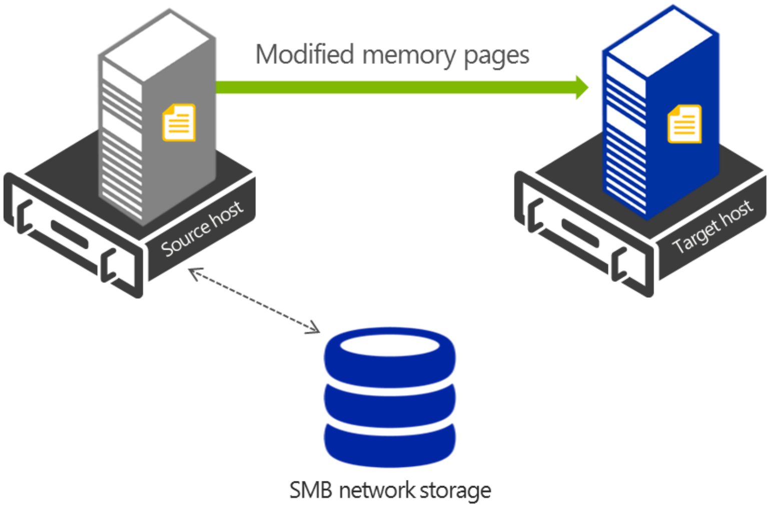
During this stage, the available network bandwidth between the source and destination hosts is critical to the speed of the live migration. Use of a 1-gigabit Ethernet (GbE) or faster connection is important. The faster the source host transfers the modified pages from the migrating virtual machine’s working set, the more quickly live migration is completed.

The number of pages transferred in this stage is determined by how actively the virtual machine accesses and modifies the memory pages. The more modified pages, the longer it takes to transfer all pages to the destination host.

After the modified memory pages are copied to the destination host, the destination host has an up-to-date working set for "Test VM." The working set for "Test VM" is present on the destination host in the exact state as the source host. The memory page copy process is illustrated in the following figure.

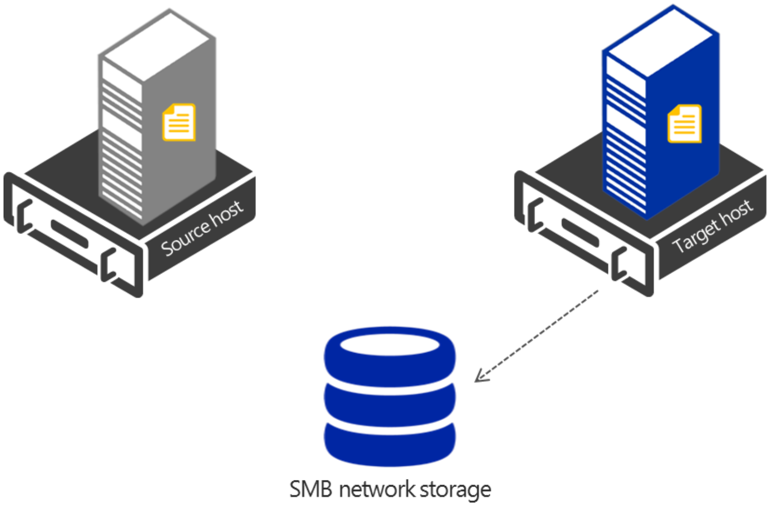
NOTE: You can cancel the live migration process at any time before this stage of the migration.

Figure 10: Modified pages transferred



- *Moving the storage handle from source to destination*: During this stage of a live migration, control of the storage that is associated with "Test VM", such as any virtual hard disk files or physical storage attached through a virtual Fibre Channel adapter, is transferred to the destination host. (Virtual Fibre Channel is also a new feature of Hyper-V. For more information, see "Virtual Fibre Channel in Hyper-V"). The following figure shows this stage.

Figure 11: Storage handle moved



- *Bringing the virtual machine online on the destination server*: In this stage of a live migration, the destination server has the up-to-date working set for "Test VM" and access to any storage that "Test VM" uses. At this time, "Test VM" resumes operation.

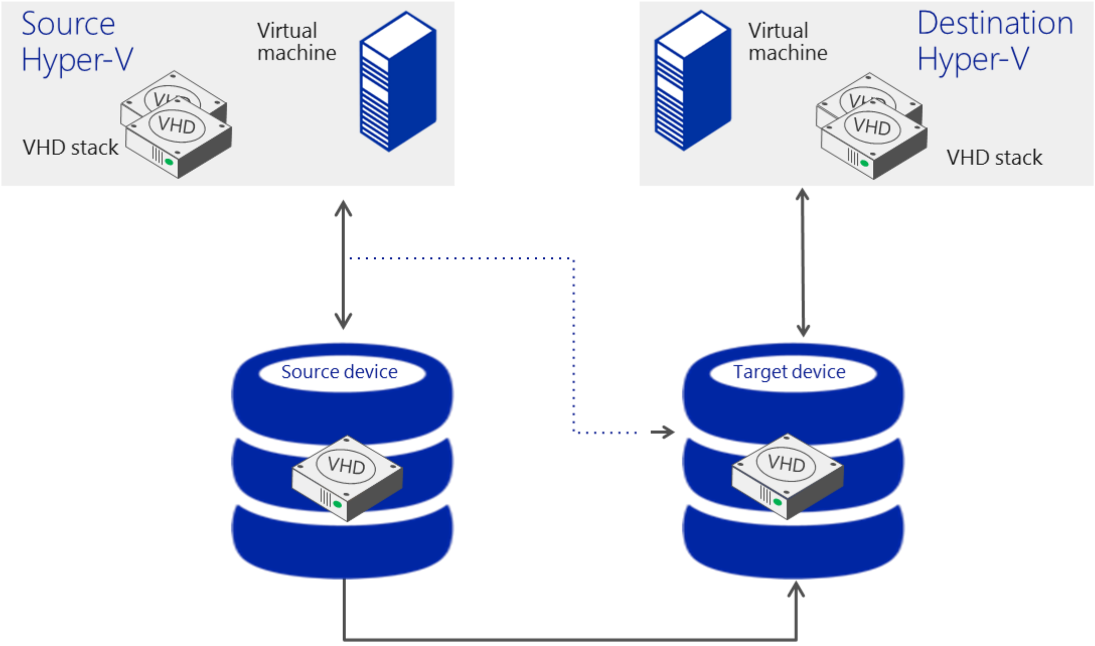
- *Network cleanup*: In the final stage of a live migration, the migrated virtual machine runs on the destination server. At this time, a message is sent to the network switch, which causes it to obtain the new the MAC addresses of the migrated virtual machine so that network traffic to and from "Test VM" can use the correct switch port.

  The live migration process completes in less time than the TCP time-out interval for the virtual machine that is being migrated. TCP time-out intervals vary based on network topology and other factors.

Scenario 2: Setting up a "shared-nothing" live migration in Windows Server 2012 Hyper-V

- *Partial migration of storage*: When you perform a live migration of a virtual machine between two computers that do not share an infrastructure, Hyper-V first performs a partial migration of the virtual machine's storage, as shown in the following figure.

Figure 12: Virtual machine storage partial migration



- *Shared-nothing setup*: Hyper-V then performs the following steps:
  1. Throughout most of the move operation, disk reads and writes go to the source virtual hard disk.
  2. While reads and writes occur on the source virtual hard disk, the disk contents are copied over the network to the new destination virtual hard disk.
  3. After the initial disk copy is complete, disk writes are mirrored to both the source and destination virtual hard disks while outstanding disk changes are replicated.
  4. After the source and destination virtual hard disks are synchronized, the virtual machine live migration is initiated, following the same process that was used for live migration with shared storage.
  5. After the virtual machine's storage is migrated, the virtual machine migrates while it continues to run and provide network services.
  6. After the live migration is complete and the virtual machine is successfully running on the destination server, the files on the source server are deleted.

Requirements

All live migrations in Windows Server 2012 Hyper-V require the following:

- Windows Server 2012.
- Two or more Hyper-V hosts:
  - Servers that support hardware virtualization.
  - Servers that use processors from the same manufacturer (for example, all AMD or all Intel).
- Hyper-V hosts that are part of the same Active Directory domain.
- Virtual machines configured to use virtual hard disks or virtual Fibre Channel disks (no pass-through disks).
- A private network for live migration network traffic.

Live migration in a cluster requires the following:

- The Windows Failover Clustering feature enabled and configured.
- CSV storage in the cluster enabled.

Live migration by using shared storage requires the following:

- All files on a virtual machine (such as virtual hard disks, snapshots, and configuration) stored on a SMB 3 share.
- Permissions on the SMB share configured to grant access to the computer accounts of all Hyper-V hosts.

Live migration with no shared infrastructure has no additional requirements.

Summary

Live migration, which was introduced with Windows Server 2008 R2, was a valuable improvement for cloud management, giving organizations the ability to move virtual machines without shutting them down. As an organization's customer base grows, however, managing the cloud environment becomes more challenging because effective resource use requires administrators to move virtual machines within a cluster and between clusters more frequently.

With the live migration improvements in Windows Server 2012 Hyper-V, organizations can now not only perform live migrations, but also move many virtual machines, quickly and without downtime, between clusters and now even to servers that do not share storage. These improvements significantly increase the flexibility of virtual machine placement by providing truly dynamic mobility of virtual machines across a datacenter. These improvements also increase administrator efficiency and eliminate the user downtime that was previously incurred for migrations across cluster boundaries. In addition to saving time because migration speed is faster, you also save time because you can perform multiple simultaneous live migrations.

Move virtual machine storage with no downtime

Before Windows Server 2012, a virtual machine's storage could be moved only while the virtual machine was shut down. In many organizations, having the flexibility to manage storage without affecting the availability of your virtual machine workloads is a key capability. IT administrators need this flexibility to perform maintenance on storage subsystems, upgrade storage appliance firmware and software, and balance loads as capacity is used. Windows Server 2008 R2 let you move a running instance of a virtual machine by using live migration, but you still could not move the virtual machine's storage while the virtual machine was running.

Hyper-V in Windows Server 2012 introduces live storage migration, which lets you move virtual hard disks attached to a running virtual machine. Through this feature, you can transfer virtual hard disks, with no downtime, to a new location for upgrading or migrating storage, performing backend storage maintenance, or redistributing your storage load. You can perform this operation by using a new wizard in Hyper-V Manager or the new Hyper-V cmdlets for Windows PowerShell. Live storage migration is available for both storage area network (SAN)-based and file-based storage.

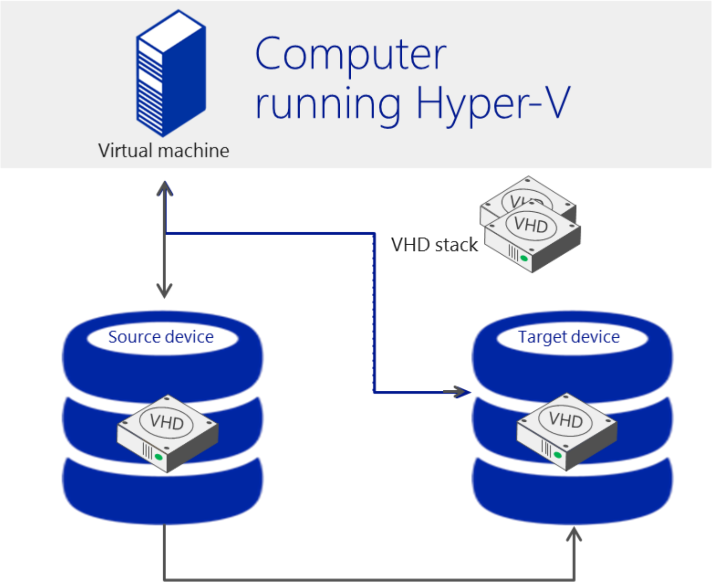
Technical description

When you move a running virtual machine's virtual hard disks, Hyper-V performs the following steps to move storage:

1. Throughout most of the move operation, disk reads and writes go to the source virtual hard disk.
2. While reads and writes occur on the source virtual hard disk, the disk contents are copied to the new destination virtual hard disk.
3. After the initial disk copy is complete, disk writes are mirrored to both the source and destination virtual hard disks while outstanding disk changes are replicated.
4. After the source and destination virtual hard disks are synchronized, the virtual machine switches over to using the destination virtual hard disk.
5. The source virtual hard disk is deleted.

These steps are illustrated in the following figure.

Figure 13: Moving virtual hard disks from one physical location to another



Just as virtual machines might need to be dynamically moved in a datacenter, allocated storage for running virtual hard disks might sometimes need to be moved for storage load distribution, storage device services, or other reasons.

Updating the physical storage that is available to Hyper-V is the most common reason for moving a virtual machine's storage. You also may want to move virtual machine storage between physical storage devices, at runtime, to take advantage of new, lower-cost storage that is supported in this version of Hyper-V (such as SMB-based storage), or to respond to reduced performance that results from bottlenecks in the storage throughput. Windows Server 2012 provides the flexibility to move virtual hard disks both on shared storage subsystems and on non-shared storage as long as a Windows Server 2012 SMB 3 network shared folder is visible to both Hyper-V hosts.

You can add physical storage to either a stand-alone system or to a Hyper-V cluster, and then move the virtual machine's virtual hard disks to the new physical storage while the virtual machine continues to run.

Storage migration, combined with live migration, also lets you move a virtual machine between hosts on different servers that are not using the same storage. For example, if two Hyper-V servers are each configured to use different storage devices and a virtual machine must be migrated between these two servers, you can use storage migration to a shared folder on a file server that is accessible to both servers and then migrate the virtual machine between the servers (because they both have access to that share). Following the live migration, you can use another storage migration to move the virtual hard disk to the storage that is allocated for the target server, or use "Shared Nothing" live migration.

Requirements

To perform storage live migration you need the following:

- Windows Server 2012.
- Hyper-V server role.
- Virtual machines configured to use virtual hard disks for storage.

Summary

Hyper-V in Windows Server 2012 lets you manage the storage of your cloud environment with greater flexibility and control while you avoid disruption of end user productivity. Storage migration with Hyper-V in Windows Server 2012 gives you the flexibility to perform maintenance on storage subsystems, upgrade storage appliance firmware and software, and balance loads as capacity is used without shutting down virtual machines.

Reliably import virtual machines

Importing a virtual machine from one physical host to another can expose file incompatibilities and other unforeseen complications. Administrators often think of a virtual machine as a single, stand-alone entity that they can move to address their operational needs. In reality, a virtual machine consists of several parts:

- Virtual hard disks, stored as files in the physical storage.
- Virtual machine snapshots, stored as a special type of virtual hard disk file.
- The saved state of the different, host-specific devices.
- The memory file, or snapshot, for the virtual machine.

- The virtual machine configuration file, which organizes the preceding components and arranges them into a working virtual machine.

Each virtual machine, and each snapshot associated with it, use unique identifiers. Additionally, virtual machines store and use some host-specific information, such as the path that identifies the location for virtual hard disk files. When Hyper-V starts a virtual machine, it undergoes a series of validation checks before being started. Problems such as hardware differences that might exist when a virtual machine is imported to another host can cause these validation checks to fail. That, in turn, prevents the virtual machine from starting.

Windows Server 2012 includes an Import wizard that helps you quickly and reliably import virtual machines from one server to another.

Technical description

Hyper-V in Windows Server 2012 introduces a new Import Wizard that detects and fixes more than 40 different types of incompatibilities. You don't have to worry ahead of time about the configuration that is associated with physical hardware, such as memory, virtual switches, and virtual processors. The Import Wizard guides you through the steps to resolving incompatibilities when you import the virtual machine to the new host.

In addition, you no longer need to export a virtual machine to be able to import it. You can simply copy a virtual machine and its associated files to the new host, and then use the Import Wizard to specify the location of the files. This "registers" the virtual machine with Hyper-V and makes it available for use. You also can recover virtual machines if the system drive fails, as long as the data drive that stores the virtual machines is intact.

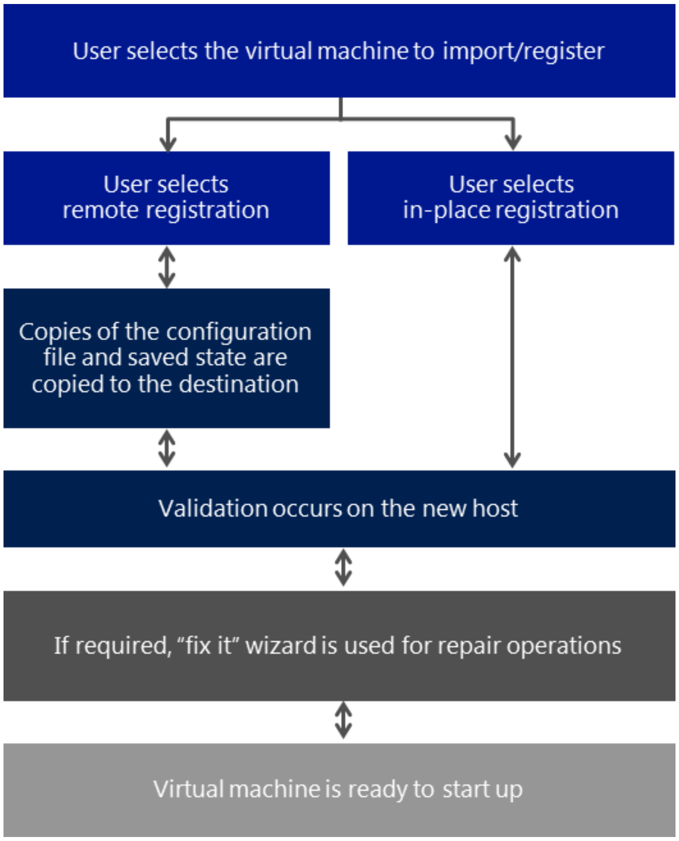
In addition to the new wizard, automation support is available. The new Hyper-V module for Windows PowerShell includes cmdlets for importing virtual machines.

When you import a virtual machine, the wizard does the following:

1. **Creates a copy of the virtual machine configuration file**. This is created as a precaution in case an unexpected restart occurs on the host, such as from a power outage.
2. **Validates hardware**. Information in the virtual machine configuration file is compared to hardware on the new host.
3. **Compiles a list of errors**. This list identifies what needs to be reconfigured and determines which pages appear next in the wizard.
4. **Displays the relevant pages, one category at a time**. The wizard identifies incompatibilities to help you reconfigure the virtual machine so that it is compatible with the new host.
5. **Removes the copy of the configuration file**. After the wizard does this, the virtual machine is ready to start.

The following figure illustrates the Import Wizard process.

Figure 14: Virtual machine import process


User selects the virtual machine to import/register
User selects remote registration
User selects in-place registration
Copies of the configuration file and saved state are copied to the destination
Validation occurs on the new host
If required, "fix it" wizard is used for repair operations
Virtual machine is ready to start up

Requirements

To use the Import Wizard, you need the following:

- Two installations of Windows Server 2012 with the Hyper-V role installed.
- A computer that has processor support for hardware virtualization.
- A virtual machine.
- A user account that belongs to the local Hyper-V Administrators group.

Summary

The new Import Wizard is a simpler, better way to import or copy virtual machines. The wizard detects and fixes potential problems, such as hardware or file differences that might exist when a virtual machine is imported to another host. As an added safety feature, the wizard creates a temporary copy of a virtual machine configuration file in case an unexpected restart occurs on the host, such as from a power outage. Windows PowerShell cmdlets for importing virtual machines let you automate the process.

Merge snapshots while the virtual machine is running

Snapshots have been mainly used for testing changes to existing virtual machine environments, as a way to return to a previous state or time if required. Having an easier way to revert a virtual machine can be very useful if you need to recreate a specific state or condition so that you can troubleshoot a problem.

Under certain circumstances it makes sense to use snapshots in a production environment. For example, you can use snapshots to provide a way to revert a potentially risky operation in a production environment, such as applying an update to the software running in the virtual machine. After successfully testing new changes or updates, many organizations merge their snapshots back into the original parent disk (to reduce storage space and increase virtual machine disk performance). However, this operation would pause the running virtual machine, effectively making it unavailable while the merge takes place.

In Windows Server 2012, the Hyper-V Live Merge feature now allows organizations to merge current snapshots back into the original parent while the virtual machine continues to run.

Technical description

The Hyper-V virtual machine Snapshot feature provides a fast and straightforward way to revert the virtual machine to a previous state. Snapshot data files (the current leaf node of virtual hard disk that is being forked into a read-only parent differential disk) are stored as .avhd files. When a snapshot is deleted, the associated .avhd disks cannot be removed while the virtual machine is running. Windows Server 2012 now provides the ability to merge the associated .avhd disk into the parent while the virtual machine continues to run.

As the process proceeds, I/O is suspended to a small range while data in that range is read from the source and written to the destination. When the leaf is being merged away, further writes to areas that have already been merged are redirected to the merge destination. Upon completion, the online merge fixes the running chain to unlink merged disks and closes those files.

Requirements

The Live Merge feature requires Windows Server 2012 with the Hyper-V role installed.

Summary

Virtual machine snapshots capture the state, data, and hardware configuration of a running virtual machine. Many organizations use snapshots in their current environments for testing updates and patches. However, merging a snapshot into the parent virtual machine requires downtime and virtual machine unavailability. Now, with the Live Merge feature of Windows Server 2012 Hyper-V, you can merge snapshots into the virtual machine parent while the server is running, with little effect on users. Live merging of snapshots provides a faster, easier way to revert a virtual machine to a previous state.

Use new automation support for Hyper-V

Windows PowerShell is the scripting solution for automating tasks in Windows Server. However, in earlier versions of Windows Server, writing scripts for Hyper-V with in-box tools required you to learn WMI, which provides a very flexible set of interfaces designed for developers. IT professionals who are involved with virtualization need ways to easily automate a number of administrative tasks without having to learn developer skills.

Hyper-V in Windows Server 2012 introduces more than 140 Hyper-V cmdlets for Windows PowerShell.

Technical description

The new Hyper-V cmdlets for Windows PowerShell are intentionally designed for IT professionals and let you perform available tasks in the graphic user interface (GUI) of Hyper-V Manager and several tasks exclusively through the cmdlets in Windows PowerShell. This design is reflected in several ways.

Task-oriented interface

Hyper-V cmdlets make it easier for IT professionals to go from *thinking* about the task to actually *performing* the task. The following table shows the task and the associated cmdlet syntax.

Table 3: Tasks and cmdlet syntax

Task	Windows PowerShell command to perform the task
Create a new virtual machine named “test.”	New-VM –Name Test
Get a list of all virtual machines.	Get-VM
Create a new virtual hard disk at d:\VHDs\test.vhd.	New-VHD –Path D:\VHDs\test.vhd
Start all virtual machines whose name begins with “web.”	Start-VM –Name web*
Connect the virtual network adapter on the “test” virtual machine to the “QA” switch.	Connect-VMNetworkAdapter –VMName test –SwitchName QA

Hyper-V administrators often must manage more than just Hyper-V. By using the same verbs as other Windows cmdlets, the Hyper-V cmdlets make it easier for administrators to extend their existing knowledge of Windows PowerShell. For example, administrators who are familiar with managing services by using Windows PowerShell can reuse the same verbs to perform the corresponding tasks on a virtual machine, as shown in the following table.

Table 4: Hyper-V cmdlets

Task	cmdlet for performing task on a service	Hyper-V cmdlet for performing task on a virtual machine
Get	Get-Service	Get-VM
Configure	Set-Service	Set-VM
Create	New-Service	New-VM
Start	Start-Service	Start-VM
Stop	Stop-Service	Stop-VM
Restart	Restart-Service	Restart-VM
Suspend	Suspend-Service	Suspend-VM
Resume	Resume-Service	Resume-VM

There are similar examples with other core Windows PowerShell cmdlets as well, as shown in the following table.

Table 5: Windows PowerShell cmdlets

Core Windows PowerShell cmdlet	Hyper-V cmdlet
Import-Csv	Import-VM
Export-Csv	Export-VM
Enable-PSRemoting	Enable-VMMigration
Checkpoint-Computer	Checkpoint-VM
Measure-Command	Measure-VM

Consistent cmdlet nouns simplify discoverability

There are many cmdlets to learn (more than 140). The nouns of the Hyper-V cmdlets make it easier for you to discover the cmdlets that they need when they need them. All cmdlets in the Hyper-V module use one of three noun prefixes in the following table.

Table 6: Noun prefixes for cmdlets

Prefix	Purpose
VM	Cmdlets for managing virtual machines
VHD	Cmdlets for managing virtual hard disk files
VFD	Cmdlets for managing virtual floppy disk files

Requirements

To use the new Hyper-V cmdlets you need the following:

- Windows Server 2012.
- Computer with processor support for hardware virtualization.
- Hyper-V server role.
- Administrator or Hyper-V Administrator user account.

Optionally, if you want to use the Hyper-V cmdlets remotely, you can install the Hyper-V Windows PowerShell cmdlets feature on a computer running Windows 8, and run the cmdlets as an Administrator or Hyper-V Administrator on the server.

Summary

Before Windows Server 2012, automation of Hyper-V management tasks required writing scripts using WMI, a skill that many datacenter administrators do not have, thus making the automation difficult. Now that Windows Server 2012 provides a rich, powerful, comprehensive, and simple-to-learn set of Windows PowerShell cmdlets, datacenter administrators have an easier time using cmdlets to automate most Hyper-V tasks (such as creating a new virtual machine, importing and exporting virtual machines, and connecting a virtual network adaptor to a virtual machine). You can use these new cmdlets to automate basic and complex datacenter tasks with ease and reduce the administrative overhead in your cloud computing environment.

Scale, performance, and density

This section contains a description of new Hyper-V features in Windows Server 2012 that increase scale, performance, and density of your virtualized environment. These features are:

- Hyper-V host scale and scale-up workload support.
- Dynamic Memory improvements for Hyper-V.
- Resource Metering in Hyper-V.
- New virtual hard disk format.
- Offloaded Data Transfer support in Hyper-V.
- Data Center Bridging (DCB).
- Virtual Fibre Channel in Hyper-V.
- Support for 4 KB disk sectors in Hyper-V virtual disks.
- Quality of Service.

Hyper-V Host scale and scale-up workload support

Hyper-V in Windows Server 2008 R2 supported configuring virtual machines with a maximum of four virtual processors and up to 64 GB of memory. However, IT organizations increasingly want to use virtualization when they deploy mission-critical, tier-1 business applications. Large, demanding workloads such as online transaction processing (OLTP) databases and online transaction analysis (OLTA) solutions typically run on systems with 16 or more processors and demand large amounts of memory. For this class of workloads, more virtual processors and larger amounts of virtual machine memory are a core requirement.

Hyper-V in Windows Server 2012 greatly expands support for host processors and memory. New features include support for up to 64 virtual processors and 1 TB of memory for Hyper-V guests, a new VHDX virtual hard disk format with larger disk capacity of up to 64 TB (see the section, “New virtual hard disk format“), and additional resiliency. These features help ensure that your virtualization infrastructure can support the configuration of large, high-performance virtual machines to support workloads that might need to scale up significantly.

Technical description

Hyper-V in Windows Server 2012 can run on large server systems. It supports the virtualization of high-performance, scale-up workloads with the following changes and features:

- Increased hardware support for the virtualization host.
- Support for large virtual machines.
- Enhanced high availability for your cloud.
- Non-Uniform Memory Access (NUMA) support in a virtual machine.
- Support for Single Root I/O Virtualization (SR-IOV) networking devices.

The following sections describe these new features.

Increased hardware support for the virtualization host

Windows Server 2012 Hyper-V supports running on a host system with up to 320 logical processors on hardware and 4 TB (terabytes) of physical memory. This helps to ensure compatibility with the largest scale-up server systems.

Support for large virtual machines

Hyper-V in Windows Server 2012 lets you configure a virtual machine with up to 64 virtual processors and up to 1 TB of memory.

Enhanced high availability for your cloud

Hyper-V in Windows Server 2012 now supports running up to 4,000 virtual machines on a 64-node failover cluster. This is a significant improvement upon the previous version, which supported a maximum of 16 cluster nodes and 1,000 virtual machines per cluster.

The table below compares the resources available in Windows Server 2008 R2 with Windows Server 2012:

Table 7: Resources available across versions of Windows Server

System	Resource	Maximum number		Improvement factor
		Windows Server 2008 R2	Windows Server 2012	
Host	Logical processors on hardware	64	**320**	5x
	Physical memory	1 TB	**4 TB**	4x
	Virtual processors per host	512	**2,048**	4x
Virtual machine	Virtual processors per virtual machine	4	**64**	16x
	Memory per virtual machine	64 GB	**1 TB**	16x
	Active virtual machines per server	384	**1,024**	2.7x
Cluster	Nodes	16	**64**	4x
	Virtual machines	1,000	**4,000**	4x

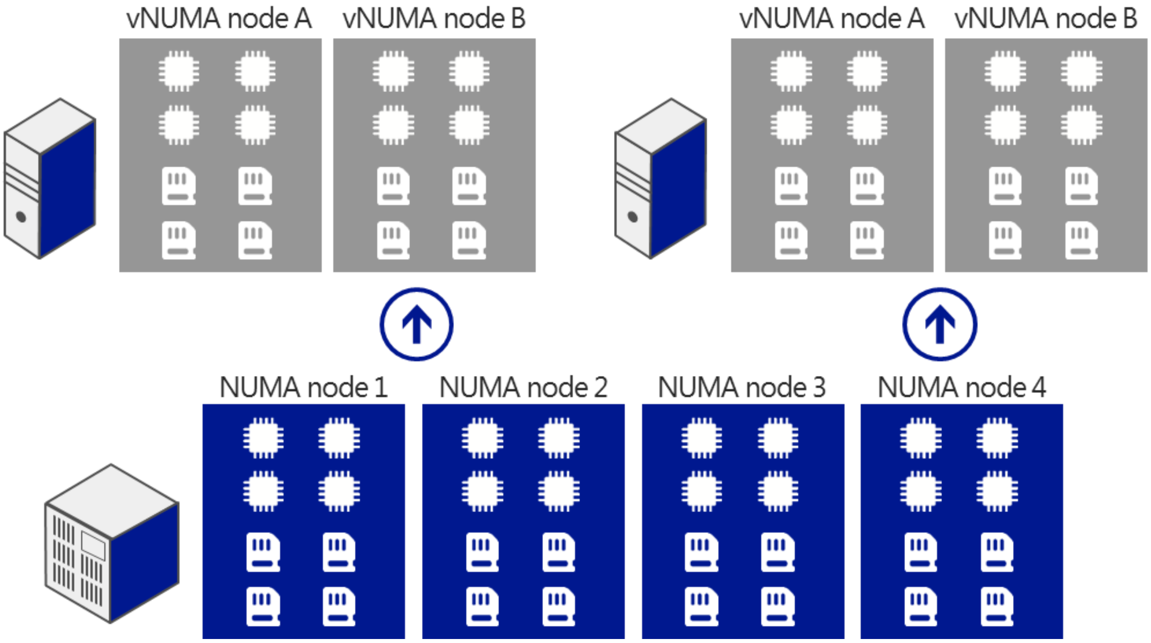
NUMA support in a virtual machine

Windows Server 2012 Hyper-V supports NUMA in a virtual machine. NUMA refers to a computer architecture in multiprocessor systems in which the required time for a processor to access memory depends on the memory’s location relative to the processor.

With NUMA, a processor can access local memory (memory attached directly to the processor) faster than it can access remote memory (memory that is local to another processor in the system). Modern operating systems and high-performance applications such as SQL Server have developed optimizations to recognize the system's NUMA topology and consider NUMA when they schedule threads or allocate memory to increase performance.

Projecting a virtual NUMA topology into a virtual machine provides optimal performance and workload scalability in large virtual machine configurations. It does this by letting the guest operating system and applications such as SQL Server take advantage of their inherent NUMA performance optimizations. The default virtual NUMA topology that is projected into a Hyper-V virtual machine is optimized to match the host's NUMA topology, as shown in the following figure.

Figure 15: Guest NUMA topology by default matching host NUMA topology



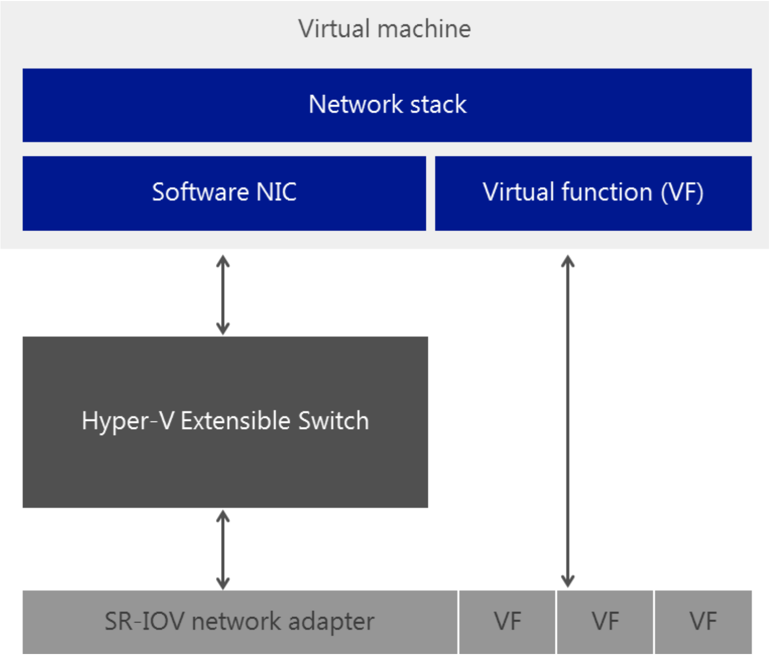
NOTE: If the virtual machine is configured to use Dynamic Memory, only one virtual NUMA node (that is, a flat NUMA topology) is projected into the guest, effectively disabling virtual NUMA support.

Support for SR-IOV networking devices

The SR-IOV standard was introduced by the PCI-SIG, the special interest group that owns and manages PCI specifications as open industry standards. SR-IOV works in conjunction with system chipset support for virtualization technologies that provide remapping of interrupts and DMA and lets SR-IOV–capable devices be assigned directly to a virtual machine.

Hyper-V in Windows Server 2012 enables support for SR-IOV–capable network devices and lets an SR-IOV virtual function of a physical network adapter be assigned directly to a virtual machine. This increases network throughput and reduces network latency while also reducing the host CPU overhead that is required for processing network traffic. The following figure shows the architecture of SR-IOV support in Hyper-V.

Figure 16: SR-IOV support



This configuration increases network throughput and reduces network latency while also reducing the host CPU overhead that is required to process network traffic.

Requirements

To take advantage of the new Hyper-V features for host scale and scale-up workload support, you need the following:

- One or more Windows Server 2012 installations with the Hyper-V role installed. Hyper-V requires a server that provides processor support for hardware virtualization.
- The number of virtual processors that may be configured in a virtual machine depends on the number of processors on the physical machine. You must have at least as many logical processors in the virtualization host as the number of virtual processors required in the virtual machine. For example, to configure a virtual machine with the maximum of 64 virtual processors, you must be running Hyper-V in Windows Server 2012 on a virtualization host that has 64 or more logical processors.

SR-IOV networking requires the following:

- A host system that supports SR-IOV (such as Intel VT-d2), including chipset support for interrupt and DMA remapping and proper firmware support to enable and describe the platform's SR-IOV capabilities to the operating system.
- An SR-IOV–capable network adapter and driver in both the management operating system (which runs the Hyper-V role) and each virtual machine where a virtual function is assigned.

Summary

With the new host scale and scale-up features of Hyper-V in Windows Server 2012, you can scale Hyper-V hosts to 320 logical processors on hardware and 4 terabytes of memory; you can scale guest virtual machines to 64 virtual processors and 1 TB of memory; and you can scale clusters to 64 nodes and 4,000 virtual machines. These new features help ensure that your virtualization infrastructure can support the configuration of large, high-performance virtual machines to support workloads that might need to scale up significantly. You can configure your systems to maximize use of host system processors and memory to effectively handle the most demanding workloads,

Dynamic Memory improvements for Hyper-V

Dynamic Memory, introduced in Windows Server 2008 R2 with SP1, helps you use physical memory more efficiently. With Dynamic Memory, Hyper-V treats memory as a shared resource that can be automatically reallocated among running virtual machines. Dynamic Memory adjusts the amount of memory available to a virtual machine based on changes in memory demand and values that you specify.

In the previous version of Hyper-V, Dynamic Memory included “startup memory,” which is defined as the minimum amount of memory that a virtual machine can have. However, Windows requires more memory during startup than the steady state. Some of the virtual machines are assigned extra memory because earlier versions of Hyper-V cannot reclaim memory from these virtual machines after startup.

The required memory to run an idle virtual machine is less than the required memory to start that virtual machine. By reclaiming unused memory from the idle virtual machines, you can potentially run more virtual machines on one host. To do this, you specify a smaller value for the minimum memory than for the startup memory. However, if you do this in Windows Server 2008 R2 with SP1, a virtual machine cannot restart when the host does not have enough physical memory. This limitation is more problematic in environments where many virtual machines are idle on a host, such as pooled VDI environments and server consolidation environments that are under low load (for example, during the night).

Because a memory upgrade requires shutting down the virtual machine, a common challenge for administrators is upgrading the maximum amount of memory for a virtual machine as demand increases. For example, consider a virtual machine running SQL Server and configured with a maximum of 8 GB of RAM. Because of an increase in the size of the databases, the virtual machine now requires more memory. In Windows Server 2008 R2 with SP1, you must shut down the virtual machine to perform the upgrade, which requires planning for downtime and decreasing business productivity. With Windows Server 2012, you can apply that change while the virtual machine is running.

Fast-growing organizations whose workloads are rapidly expanding often need to add more virtual machines to their host processors. These organizations want to optimize the number of virtual machines they can place on a host server to minimize the number of expensive host servers that they need. With the Hyper-V Dynamic Memory improvements in Windows Server 2012, IT administrators can now allocate virtual machine memory resources more efficiently and dramatically increase virtual machine consolidation ratios.

Technical description

In Windows Server 2012, Dynamic Memory has a new configuration item, “minimum memory.” Minimum memory lets Hyper-V reclaim the unused memory from the virtual machines. This can result in increased virtual machine consolidation numbers, especially in VDI environments.

Windows Server 2012 also introduces Hyper-V Smart Paging for robust virtual machine restart. Although minimum memory increases virtual machine consolidation numbers, it also brings a challenge. If a virtual machine has a smaller amount of memory than its startup memory and it is restarted, Hyper-V needs additional memory to restart the machine. Due to host memory pressure or virtual machines’ states, Hyper-V may not always have additional memory available. This can cause sporadic virtual machine restart failures in customer environments. In Windows Server 2012, Hyper-V Smart Paging is used to bridge the memory gap between minimum memory and startup memory and let virtual machines restart reliably.

In Windows Server 2012, new functionality in Dynamic Memory for Hyper-V lets you:

- Configure a lower minimum memory for virtual machines and have a reliable restart experience.
- Increase the maximum memory and decrease minimum memory on running virtual machines.

Minimum memory configuration with reliable restart operation

As in the earlier version of Dynamic Memory, you can configure minimum memory for your virtual machines and Hyper-V continues to assign this amount to running virtual machines. To provide a reliable restart experience for the virtual machines that are configured with less minimum memory than startup memory, Windows Server 2012 uses Hyper-V Smart Paging.

Hyper-V Smart Paging is a memory management technique that uses disk resources as additional, temporary memory when more memory is required to restart a virtual machine. This approach has both advantages and drawbacks. It provides a reliable way to keep the virtual machines running when no physical memory is available. However, it can degrade virtual machine performance because disk access speeds are much slower than memory access speeds.

To minimize the performance impact of Smart Paging, Hyper-V uses it only when all of the following occur:

- The virtual machine is being restarted.
- No physical memory is available.
- No memory can be reclaimed from other virtual machines that are running on the host.

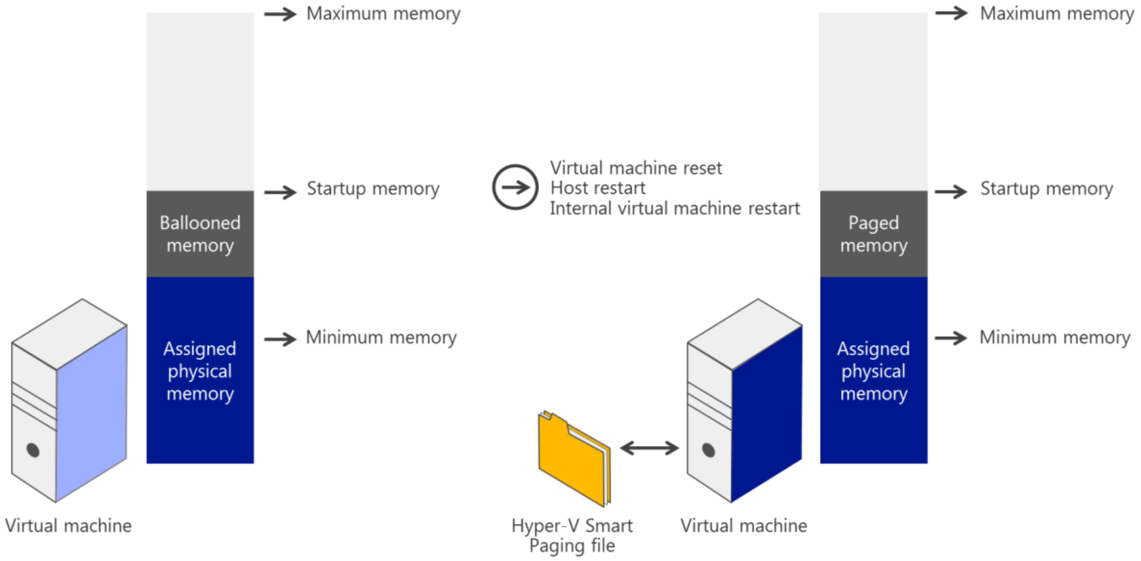
Hyper-V Smart Paging is *not* used when:

- A virtual machine is being started from an off state (instead of a restart).
- Oversubscribing memory for a running virtual machine would result.
- A virtual machine is failing over in Hyper-V clusters.

Hyper-V continues to rely on internal guest paging when host memory is oversubscribed because it is more effective than Hyper-V Smart Paging. With internal guest paging, the paging operation inside virtual machines is performed by Windows Memory Manager. Windows Memory Manager has more information than does the Hyper-V host about memory use within the virtual machine, which means it can provide Hyper-V with better information to use when it chooses the memory to be paged. Because of this, internal guest paging incurs less overhead to the system than Hyper-V Smart Paging.

The figure on the following page shows the mapping of memory for a virtual machine that is being restarted by using Hyper-V Smart Paging.

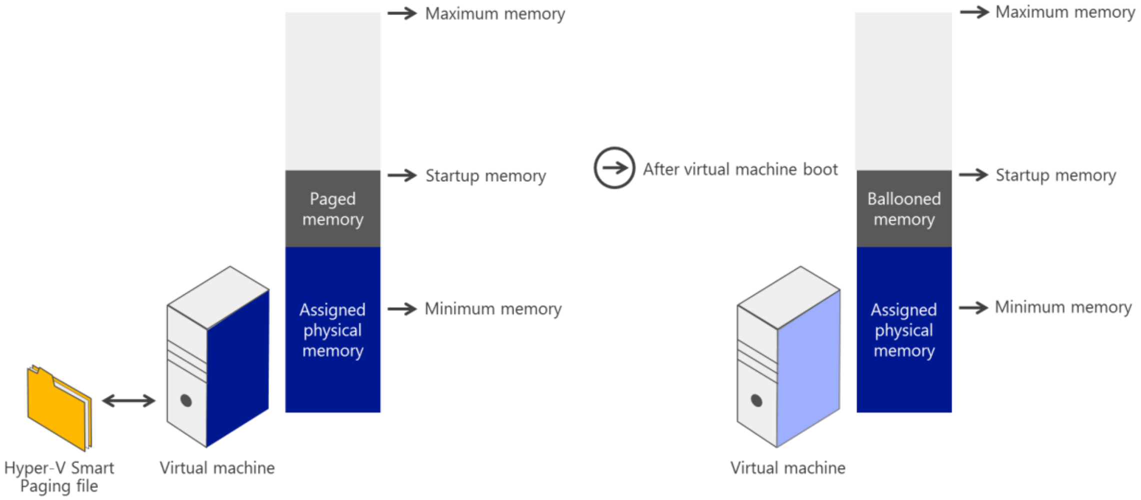
Figure 17: Hyper-V Smart Paging



To further reduce the impact of Hyper-V Smart Paging, after a virtual machine completes the startup process, Hyper-V removes memory from the virtual machine, coordinating with Dynamic Memory components inside the guest (a process sometimes referred to as "ballooning"), so that the virtual machine stops using Hyper-V Smart Paging. With this technique, use of Hyper-V Smart Paging is temporary, and is not expected to be longer than 10 minutes.

The following figure shows Hyper-V removing memory from the virtual machine after it completes the startup process.

Figure 18: Removing paged memory after virtual machine restart



Also note the following about how Hyper-V Smart Paging is used:

- Hyper-V Smart Paging files are created only when needed for a virtual machine.
- After the additional amount of memory is removed, Hyper-V Smart Paging files are deleted.
- Hyper-V Smart Paging is not used for this virtual machine again until another restart occurs and not enough physical memory exists.

Runtime Dynamic Memory configuration changes

Windows Server 2012 Hyper-V enables you to make the following configuration changes to Dynamic Memory when the virtual machine is running:

- Increase the maximum memory.
- Decrease the minimum memory.

Requirements

Dynamic Memory requires the following:

- Windows Server 2012.
- Hyper-V server role.

Summary

Dynamic Memory improvements to Hyper-V in Windows Server 2012 help you reach higher consolidation numbers with improved reliability of Hyper-V operations. You can make memory configuration changes for your virtual machines without shutting down the virtual machines. If you have idle or low-load virtual machines, as in pooled VDI environments, Dynamic Memory additions in Hyper-V let you increase consolidation and improve reliability for restart operations. This can lead to lower costs for customers, especially in environments such as pooled VDI environments that have many idle or low-load virtual machines. With runtime configuration changes for Dynamic Memory, overall IT productivity is expected to increase with reduced downtime and increased agility to respond to requirement changes. You also gain agility in responding to requirement changes with these new capabilities.

Resource Metering in Hyper-V

Your computing resources are limited. You need to know how different workloads draw upon these resources—even when they are virtualized. In Windows Server 2012, Hyper-V introduces Resource Metering, a technology that helps you track historical data on the use of virtual machines and gain insight into the resource use of specific servers. You can use this data to perform capacity planning, to monitor consumption by different business units or customers, or to capture data needed to help redistribute the costs of running a workload. You could also use the information that this feature provides to help build a billing solution, so that customers of your hosting services can be charged appropriately for resource usage.

Technical description

This section describes how Resource Metering works.

Metrics for resource use

Windows Server 2012 offers two ways to obtain historical data on customer usage of virtual machine resources: Hyper-V cmdlets in Windows PowerShell, and the new APIs in the Virtualization WMI Provider.

Hyper-V exposes the metrics in the following table for resource use.

Table 8: Hyper-V metrics

Metric	Units	Description
Average CPU use	Megahertz (MHz)	The average amount of CPU used by a virtual machine over a period of time
Average memory use	Megabytes (MB)	The average amount of physical memory used by a virtual machine over a period of time
Minimum memory use	MB	The lowest amount of physical memory assigned to a virtual machine over a period of time
Maximum memory use	MB	The highest amount of physical memory assigned to a virtual machine over a period of time
Maximum disk allocation	MB	The highest amount of disk space capacity allocated to a virtual machine over a period of time
Incoming network traffic	MB	Total incoming network traffic, for a virtual network adapter over a period of time
Outgoing network traffic	MB	Total outgoing network traffic for a virtual network adapter over a period of time

Use of network metering Port ACLs

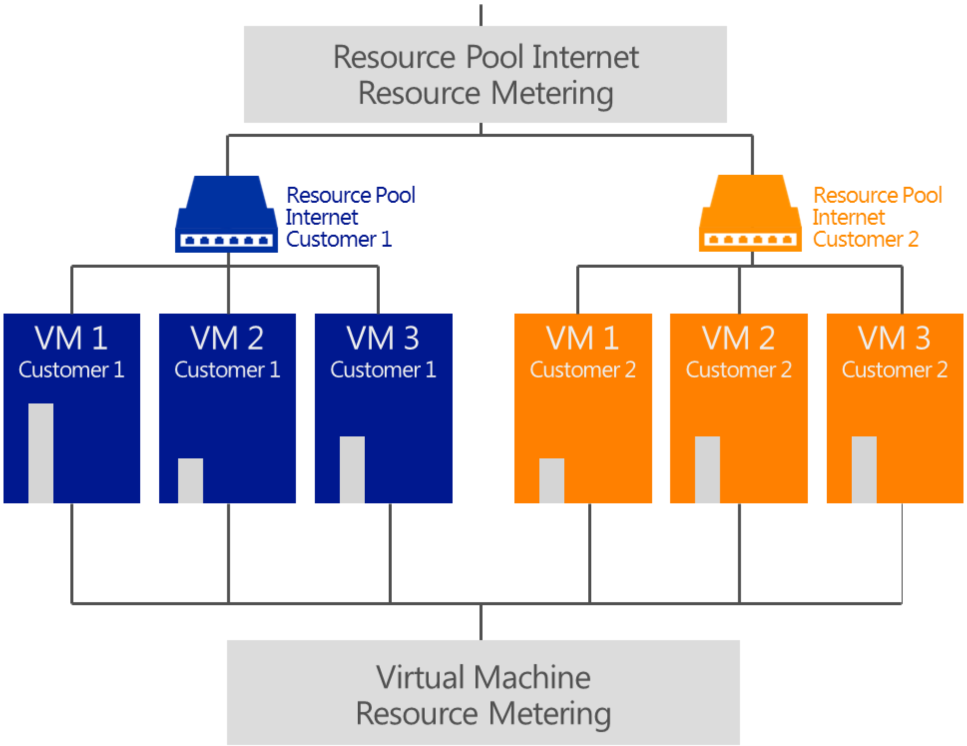
Enterprises pay for the Internet traffic coming into and going out of their datacenters, but not for the network traffic *within* the datacenters. For this reason, providers generally consider Internet and intranet traffic separately for the purposes of billing. To differentiate between Internet and intranet traffic, providers can measure incoming and outgoing network traffic for any IP address range, by using Network Metering Port ACLs.

Metering virtual machine use in a multitenant environment

Hyper-V in Windows Server 2012 lets providers build a multitenant environment in which virtual machines can be served to multiple clients in a more isolated and secure way, as shown in the following figure. Because a single client may have many virtual machines, aggregation of resource use data can be challenging. However, Windows Server 2012 simplifies this task by using resource pools, a feature available in Hyper-V. Resource pools are logical containers that collect resources of virtual machines belonging to one client, permitting single-point querying of the client's overall resource use.

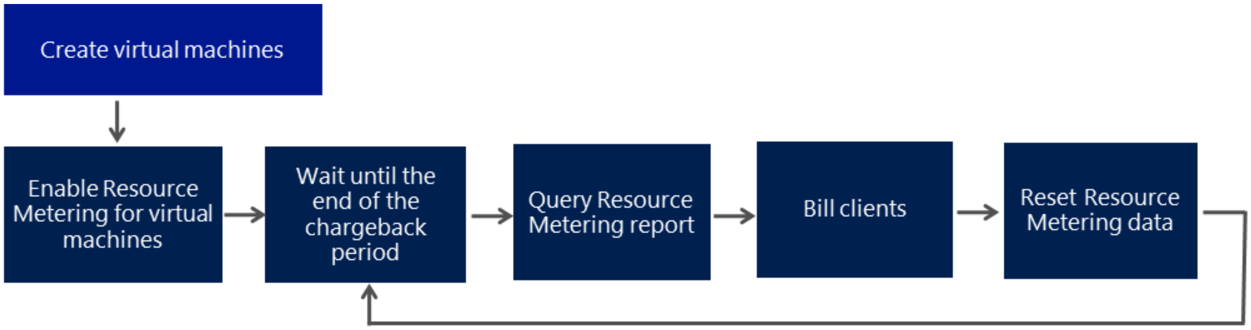
The following figure is an example of Resource Metering in a two-tenant environment that is built with Hyper-V in Windows Server 2012.

Figure 19: Two-tenant environment built with Hyper-V in Windows Server 2012



The following figure shows a basic model of Resource Metering.

Figure 20: Basic model of metering resource use


Create virtual machines
Enable Resource Metering for virtual machines
Wait until the end of the chargeback period
Query Resource Metering report
Bill clients
Reset Resource Metering data

In this model, a hosting provider does the following:

1. Create virtual machines for a customer and enable Resource Metering once for the virtual machines. In a multitenant environment, the provider would enable metering on each resource pool. Hyper-V then tracks resource use for each virtual machine until that virtual machine is deleted.
2. Query resource use data at the end of each chargeback period, and use this data to bill clients as needed.
3. Reset the data at the end of each chargeback period, so that Hyper-V can begin tracking resource use for the new chargeback period.

Resource Metering works with all Hyper-V operations. Movement of virtual machines between Hyper-V hosts (such as through live, offline, or storage migration) does not affect the collected data.

Requirements

You need the following to use the Hyper-V Resource Metering feature:

- Windows Server 2012.
- Hyper-V server role.

Note that Resource Metering is not supported for the following:

- Storage accessed through a virtual Fibre Channel adapter.
- Physical disks attached directly to a virtual machine (sometimes referred to as pass-through disks).
- Network adapters configured with Offload Weight.

NOTE: Network Offload Weight helps ensure that limited hardware resources are dynamically assigned to the right virtual machines. As virtual machines move around inside the datacenter the network offload weight is used to prioritize which virtual machines obtain access to network hardware offloads that have finite limits (such as SR-IOV).

Summary

The Resource Metering feature in Windows Server 2012 Hyper-V makes it easier for you to track historical data about each customer's use of virtual machines. Through resource pools, which are part of this technology, Hyper-V lets providers aggregate usage data in a multitenant environment, in which each customer or business unit may have many virtual machines. With this feature, you can perform capacity planning or monitor resource consumption by various business units or customers. Third-party ISVs can use data provided by this feature to build more reliable, cost-effective, usage-based billing solutions.

New virtual hard disk format

With the evolution of storage systems, and the ever-increasing reliance on virtualized enterprise workloads, the VHD format of Windows Server needed to also evolve. The new format is better suited to address current and future requirements for running enterprise-class workloads, specifically:

- Where the size of the VHD is larger than 2 TB.
- To reliably protect against issues for dynamic and differencing disks during power failures.
- To prevent performance degradation issues on the new, large-sector physical disks.

Hyper-V in Windows Server 2012 contains an update to the VHD format, called VHDX, which has much larger capacity and additional resiliency. VHDX supports up to 64 terabytes of storage. It also provides additional protection against corruption from power failures by logging updates to the VHDX metadata structures, and it prevents performance degradation on large-sector physical disks by optimizing structure alignment.

Technical description

The principal new features of the VHDX format are:

- Support for virtual hard disk storage capacity of up to 64 TB.

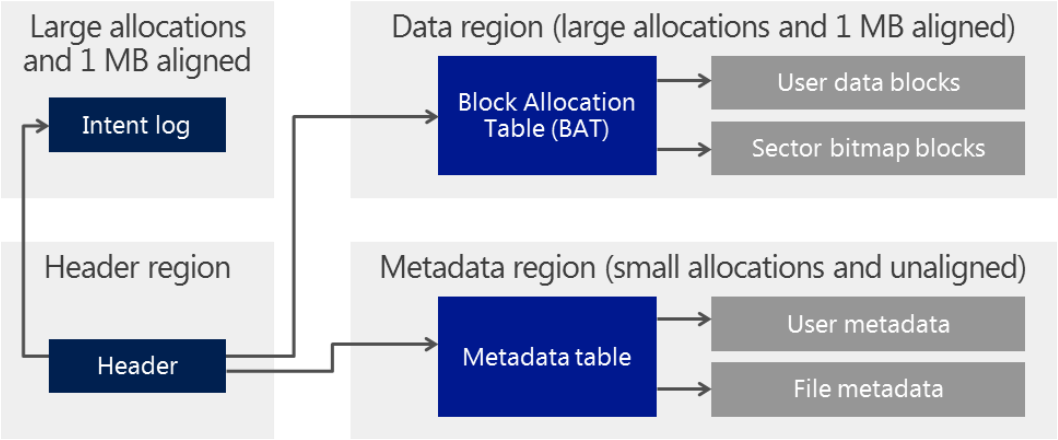
- Protection against corruption during power failures by logging updates to the VHDX metadata structures. The format contains an internal log that is used to capture updates to the metadata of the virtual hard disk file before being written to its final location. In case of a power failure, if the write to the final destination is corrupted, then it is played back from the log to promote consistency of the virtual hard disk file.
- Optimal structure alignment of the virtual hard disk format to suit large sector disks. If unaligned I/Os are issued to these disks, an associated performance penalty is caused by the Read-Modify-Write cycles that are required to satisfy these I/Os. The structures in the format are aligned to help ensure that no unaligned I/Os exist.

The VHDX format also provides:

- Larger block sizes for dynamic and differential disks, which lets these disks attune to the needs of the workload.
- A 4 KB logical sector virtual disk that results in increased performance when applications and workloads that are designed for 4 KB sectors use it.
- The ability to store custom metadata about the file that you might want to record, such as operating system version or patches applied.
- Efficiency (called trim) in representing data, which results in smaller files and lets the underlying physical storage device reclaim unused space. (Trim requires pass-through or SCSI disks and trim-compatible hardware).

The following figure illustrates the VHDX hard disk format.

Figure 21: The VHDX hard disk format


Large allocations and 1 MB aligned
Intent log
Data region (large allocations and 1 MB aligned)
Block Allocation Table (BAT)
User data blocks
Sector bitmap blocks
Header region
Header
Metadata region (small allocations and unaligned)
Metadata table
User metadata
File metadata

As you can see in the figure above, most of the structures are large allocations and are MB aligned. This alleviates the alignment issue associated with virtual hard disks. The different regions of the VHDX format are as follows:

- **Header region**. The header region is the first region of the file and identifies the location of the other structures, including the log, block allocation table (BAT), and metadata region. The header region contains two headers, only one of which is active at a time, to increase resiliency to corruptions.
- **Intent log**. The intent log is a circular ring buffer. Changes to the VHDX metastructures are written to the log before they are written to the final location. If corruption occurs during a power failure while an update is being written to the actual location, on the subsequent open, the change is applied again

from the log, and the VHDX file is brought back to a consistent state. The log does not track changes to the payload blocks, so it does not protect data contained within them.

- **Data region**. The BAT contains entries that point to both the user data blocks and sector bitmap block locations within the VHDX file. This is an important difference from the VHD format, because sector bitmaps are aggregated into their own blocks instead of being appended in front of each payload block.
- **Metadata region**. The metadata region contains a table that points to both user-defined metadata and virtual hard disk file metadata such as block size, physical sector size, and logical sector size.

Based on the workload they are supporting, VHDX files can be large, and the space they consume can grow quickly. Currently, when applications delete content within a virtual hard disk, the Windows storage stacks in both the guest operating system and the Hyper-V host have limitations that prevent this information from being communicated to the virtual hard disk and the physical storage device. This prevents the Hyper-V storage stack from optimizing the space used; it also prevents the underlying storage device from reclaiming the space previously occupied by deleted data.

In Windows Server 2012, Hyper-V now supports unmap notifications, which improves the efficiency with which VHDX files can represent the data they contain. This results in smaller files size, which lets the underlying physical storage device reclaim unused space.

Requirements

To take advantage of the new version of the VHD format, called VHDX, you need the following:

- Windows Server 2012 or Windows 8.
- Hyper-V server role.

To take advantage of the trim feature, you need the following:

- VHDX-based virtual disks connected as virtual SCSI devices or as directly attached physical disks (sometimes referred to as pass-through disks). This optimization also is supported for natively attached VHDX-based virtual disks.
- Trim-capable hardware.

Summary

Designed to handle current and future workloads, VHDX has a much larger storage capacity than earlier VHD formats to address the technological demands of evolving enterprises. Performance-enhancing features in VHDX make it easier to handle large workloads, protect data better during power outages, and optimize structure alignments of dynamic and differential disks to prevent performance degradation on new, large-sector physical disks.

Offloaded data transfer support in Hyper-V

Crucial maintenance tasks for virtual hard disks, such as merge, move, and compact, depend on copying large amounts of data. Storage Area Network (SAN) vendors are working to provide near-instantaneous copying of large amounts of data. This high-speed storage lets the system above the disks specify the move of a specific data set from one location to another, a hardware feature known as a copy offload. In Windows Server 2012, Hyper-V takes advantage of new SAN copy offload innovations to copy large amounts of data from one location to another.

Whenever possible, the speed of your virtualization platform should rival that of physical hardware. Offloaded Data Transfer (ODX) support is a feature of the storage stack of Hyper-V in Windows Server 2012. When used with offload-capable SAN storage hardware, ODX lets a storage device perform a file copy operation without the main processor of the Hyper-V host actually reading the content from one storage place and writing it to another.

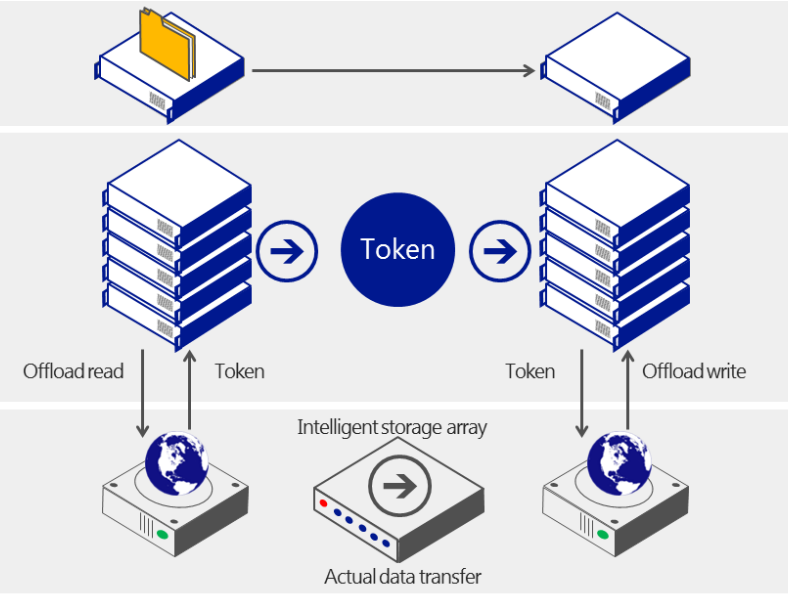
Technical description

The storage stack of Hyper-V in Windows Server 2012 supports ODX operations so that these operations can be passed from the guest operating system to the host hardware, letting the workload use ODX–enabled storage as if it were running in a non-virtualized environment. The Hyper-V storage stack also issues copy offload operations in VHD and VHDX maintenance operations such as merging disks and storage migration meta-operations in which large amounts of data are moved from one virtual hard disk to another virtual hard disk or to another location.

ODX uses a token-based mechanism for reading and writing data within or between intelligent storage arrays. Instead of routing the data through the host, a small token is copied between the source and destination. The token simply serves as a point-in-time representation of the data. As an example, when you copy a file or migrate a virtual machine between storage locations (either within or between storage arrays), a token representing the virtual machine file is copied, which eliminates the need to copy the underlying data through the servers. In a token-based copy operation, the steps are as follows:

1. A user initiates a file copy or move in Windows Explorer, a command-line interface, or a virtual machine migration.
2. Windows Server automatically translates this transfer request into an ODX (if supported by the storage array) and receives a token representation of the data.
3. The token is copied between the source and destination systems.
4. The token is delivered to the storage array.
5. The storage array performs the copy internally and returns progress status.

Figure 22: Token-based copy operation



ODX is especially important in the cloud space when you must provision new virtual machines from virtual machine template libraries, or when virtual hard disk operations are triggered and require large blocks of data to be copied, as in virtual hard disk merges, storage migration, and live migration. These copy operations are then handled by the storage device that must be able to perform offloads (such as an offload-capable iSCSI, Fibre Channel SAN, or a file server based in Windows Server 2012) and frees up the Hyper-V host processors to carry more virtual machine workloads.

Requirements

ODX support in Hyper-V requires the following:

- ODX-capable hardware is required to host virtual hard disk files connected to the virtual machine as virtual SCSI devices or directly attached (sometimes referred to as pass-through disks).
- This optimization is also supported for natively attached, VHDX-based virtual disks.
- VHD- or VHDX-based virtual disks attached to virtual IDE do not support this optimization because integrated development environment (IDE) devices lack ODX support.

Summary

ODX frees up the main processor to handle virtual machine workloads, enabling native-like performance when your virtual machines read from and write to storage.

Feature-level benefits of ODX are:

- Greatly reduced time required to copy large amounts of data.
- Copy operations that don't use processor time.
- A virtualized workload that operates as efficiently as it would in a non-virtualized environment.

All this makes possible faster performance of crucial maintenance tasks for virtual hard drives (such as merge, move, and compact) that depend on copying large amounts of data without using processor time. Enabling ODX support in the Hyper-V storage stack lets you complete these operations in a fraction of the time it would have taken without the support.

Data Center Bridging

Separate isolated connections for network, live migration, and management traffic make managing network switches and other networking infrastructure a challenge. As datacenters evolve, IT organizations look to some of the latest innovations in networking to help solve these issues. The introduction of 10 GigE networks, for example, helps support converged networks that can handle network, storage, live migration, and management traffic through a single connection, reducing IT management requirements and costs.

Data Center Bridging, or DCB, refers to enhancements to Ethernet LANs used in datacenter environments. These enhancements consolidate the various forms of network into a single technology known as a Converged Network Adapter (CNA). In the virtualized environment, Hyper-V in Windows Server 2012 can take advantage of DCB-capable hardware to converge multiple types of network traffic on a single network adapter with a maximum level of service to each.

Technical description

Support for DCB-enabled 10 GigE network adapters is one of the new Quality of Service (QoS) bandwidth management features in Windows Server 2012 that lets hosting providers and enterprises provide services with predictable network performance to virtual machines on a Hyper-V server. See the "Quality of Service" section of this white paper.

DCB is a hardware mechanism which classifies and dispatches network traffic that depends on DCB support on the network adapter, supporting far fewer traffic flows. It converges different types of traffic, including network, storage, management, and live migration traffic. However, it also can classify network traffic that doesn't originate from the networking stack.

A typical scenario involves a CNA that supports iSCSI offload, in which iSCSI traffic bypasses the networking stack and is framed and transmitted directly by the CNA. Because the packet scheduler in the networking stack doesn't process this offloaded traffic, DCB is the only viable choice to enforce minimum bandwidth.

Requirements

In the Hyper-V environment, you need the following to take advantage of DCB:

- Windows Server 2012.
- Hyper-V role.
- DCB-enabled network adaptor.

Summary

The ability to take advantage of the latest innovations in DCB lets users converge network, storage, management, and live migration traffic, and helps ensure that each customer receives the required QoS in a virtualized environment. This approach also makes it easier to change allocations to different traffic flows when needed, because the allocation becomes software controlled and therefore more flexible and easier to modify. This helps reduce costs, and makes it easier to maintain separate connections in the datacenter.

Virtual Fibre Channel in Hyper-V

You need your virtualized workloads to connect to your existing storage arrays with little trouble. Many enterprises have already invested in Fibre Channel SANs, deploying them in their datacenters to address growing storage requirements. Such customers often want the ability to use this storage from within their virtual machines instead of having the storage accessible to and used only by the Hyper-V host.

Virtual Fibre Channel for Hyper-V, a new feature in Windows Server 2012, provides Fibre Channel ports within the guest operating system, enabling direct connections to Fibre Channel directly from within virtual machines.

Technical description

Virtual Fibre Channel lets virtual machines connect directly to Fibre Channel–based storage and presents virtual Fibre Channel host bus adapter (HBA) ports in the guest operating system running on the virtual machine. The key features of Virtual Fibre Channel are:

- Unmediated access to a SAN.
- Hardware-based I/O path to the Windows software virtual hard disk stack.
- Live migration.
- N_Port ID Virtualization (NPIV).
- Single Hyper-V host connected to different SANs with multiple Fibre Channel ports.
- Up to four virtual Fibre Channel adapters on a virtual machine.
- Multipath I/O (MPIO) that helps ensure high availability connections to storage.

Each of these features is described in the following sections.

Unmediated access to a SAN

Virtual Fibre Channel for Hyper-V provides the guest operating system with unmediated access to a SAN by using a standard World Wide Name (WWN) that is associated with a virtual machine. Hyper-V lets you use Fibre Channel SANs to virtualize workloads that require direct access to SAN logical unit numbers (LUNs). Fibre Channel SANs also let you operate in new scenarios, such as running the Windows Failover Clustering feature inside the guest operating system of a virtual machine connected to shared Fibre Channel storage.

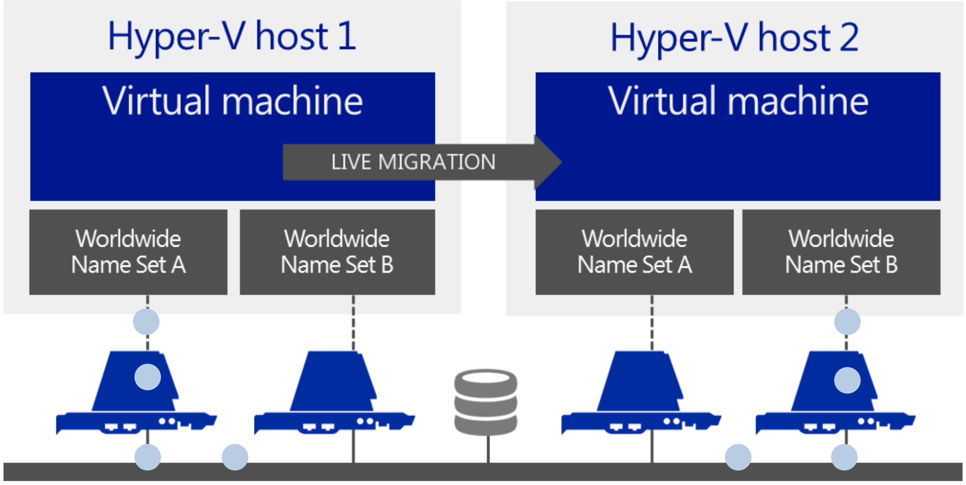
Hardware-based I/O path to the Windows software virtual hard disk stack

Mid-range and high-end storage arrays include advanced storage functionality that helps offload certain management tasks from the hosts to the SANs. Virtual Fibre Channel offers an alternative, hardware-based I/O path to the Windows software virtual hard disk stack. This path lets you use the advanced functionality of your SANs directly from within Hyper-V virtual machines. For example, Hyper-V users can offload storage functionality (such as taking a snapshot of a LUN) to the SAN hardware simply by using a hardware Volume Shadow Copy Service (VSS) provider from within a Hyper-V virtual machine.

Live migration

To support live migration of virtual machines across Hyper-V hosts while maintaining Fibre Channel connectivity, two WWNs, Set A and Set B, are configured for each virtual Fibre Channel adapter. Hyper-V automatically alternates between the Set A and Set B WWN addresses during live migration. This helps ensure that all LUNs are available on the destination host before the migration and that no downtime occurs during the migration. The live migration process that maintains Fibre Channel connectivity is illustrated in the following figure.

Figure 23: Alternating WWN addresses during a live migration



N_Port ID Virtualization (NPIV)

NPIV is a Fibre Channel facility that lets multiple N_Port IDs share a single physical N_Port. This lets multiple Fibre Channel initiators occupy a single physical port, easing hardware requirements in SAN design, especially where virtual SANs are called for. Virtual Fibre Channel for Hyper-V guests uses NPIV (T11 standard) to create multiple NPIV ports on top of the host's physical Fibre Channel ports. A new NPIV port is created on the host each time a virtual HBA is created inside a virtual machine. When the virtual machine stops running on the host, the NPIV port is removed.

Single Hyper-V host connected to different SANs with multiple Fibre Channel ports

Hyper-V lets you define virtual SANs on the host to accommodate scenarios in which a single Hyper-V host is connected to different SANs via multiple Fibre Channel ports. A virtual SAN defines a named group of physical Fibre Channel ports that are connected to the same physical SAN. For example, assume that a Hyper-V host is connected to two SANs—a production SAN and a test SAN. The host is connected to each SAN through two physical Fibre Channel ports. In this example, you might configure two virtual SANs—one named "Production SAN" that has the two physical Fibre Channel ports connected to the production SAN and one named "Test SAN" that has two physical Fibre Channel ports connected to the test SAN. You can use the same technique to name two separate paths to a single storage target.

Up to four virtual Fibre Channel adapters on a virtual machine

You can configure as many as four virtual Fibre Channel adapters on a virtual machine, and associate each one with a virtual SAN. Each virtual Fibre Channel adapter is associated with one WWN address, or two WWN addresses to support live migration. Each WWN address can be set automatically or manually.

MPIO functionality

Hyper-V in Windows Server 2012 uses Microsoft MultiPath I/O (MPIO) functionality to help ensure optimal connectivity to Fibre Channel storage from within a virtual machine. You can use MPIO functionality with Fibre Channel in the following ways:

- Virtualize workloads that use MPIO. Install multiple Fibre Channel ports in a virtual machine, and use MPIO to provide highly available connectivity to the LUNs that the host can access.

- Configure multiple virtual Fibre Channel adapters inside a virtual machine, and use a separate copy of MPIO within the guest operating system of the virtual machine to connect to the LUNs that the virtual machine can access. This configuration can coexist with a host MPIO setup.
- Use different device specific modules (DSMs) for the host or each virtual machine. This approach permits migration of the virtual machine configuration, including the configuration of DSM and connectivity between hosts and compatibility with existing server configurations and DSMs.

Requirements

Virtual Fibre Channel support in Hyper-V requires the following:

- One or more installations of Windows Server 2012 with the Hyper-V role installed. Hyper-V requires a computer with processor support for hardware virtualization.
- A computer with one or more Fibre Channel HBAs, each with an updated HBA driver that supports Virtual Fibre Channel. Check with your HBA vendor for information on whether your HBA supports Virtual Fibre Channel.
- Virtual machines that are configured to use a virtual Fibre Channel adapter, which must use Windows Server 2008, Windows Server 2008 R2, or Windows Server 2012 as the guest operating system.
- Connection *only* to data LUNs. Storage accessed through a virtual Fibre Channel that is connected to a LUN cannot be used as restart media.

Summary

Virtual Fibre Channel lets you access and use Fibre Channel SAN data from your virtual machines instead of having the storage accessible and used only by the Hyper-V host. Support for Fibre Channel in Hyper-V guests also includes support for many related features, such as NPIV, virtual SANs, live migration, and MPIO. This feature protects your investments in Fibre Channel, lets you virtualize workloads that use direct access to Fibre Channel storage, lets you cluster guest operating systems over Fibre Channel, and offers an important new storage option for servers that are hosted on your virtualization infrastructure.

Support for 4 KB disk sectors in Hyper-V virtual disks

Increases in storage density and reliability are among the factors driving the data storage industry to transition the physical format of hard disk drives from 512-byte sectors to 4,096-byte sectors (also known as 4 KB sectors). However, most of the software industry depends on disk sectors of 512 bytes in length. A change in sector size introduces major compatibility issues in many applications. To minimize the impact on the ecosystem, hard drive vendors are introducing transitional “512-byte emulation drives” also known as “512e.” These drives offer some advantages of 4 KB native drives, such as improved format efficiency and an improved scheme for error correction codes (ECC), but with fewer compatibility issues than by exposing a 4 KB sector size at the disk interface.

Hyper-V in Windows Server 2012 supports “512e” and 4 KB disk sectors.

Technical description

In Windows Server 2012, Hyper-V introduces support for 4,096-byte sectors (4 KB disk sectors) in virtual disks, a standard to which the industry will move over the next few years to support increasing storage requirements. Hyper-V in Windows Server 2012 also provides enhanced performance of the transitional standard, 512-byte emulation drives, also known as 512-byte Emulation (512e). Support for 4 KB disk sectors and 512e helps ensure that your virtualization infrastructure keeps pace with industry innovations in storage.

Support for improved performance of virtual hard disks on 512e disks

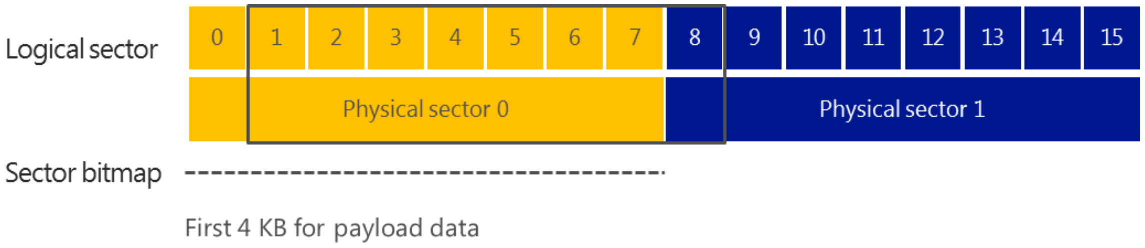
A 512e disk can perform a write only in terms of a physical sector—that is, it cannot directly write a 512-byte sector write that is issued to it. The internal process in the disk which makes this write possible follows these steps:

1. The disk reads the 4 KB physical sector into its internal cache, which contains the 512-byte logical sector that is referred to in the write.
2. Data in the 4 KB buffer is modified to include the updated 512-byte sector.
3. The disk performs a write of the updated 4 KB buffer back to its physical sector on the disk.

This process is called "Read-Modify-Write," or RMW. The RMW process causes performance degradation in virtual hard disks for the following reasons:

- Dynamic and differencing virtual hard disks have a 512-byte sector bitmap in front of their data payload. In addition, footer/header/parent locators all align to a 512-byte sector. It is common for the virtual hard disk drive to issue 512-byte writes to update these structures, resulting in the RMW behavior described earlier.
- Applications commonly issue reads and writes in multiples of 4 KB sizes (the default cluster size of NTFS). Because a 512-byte sector bitmap is in front of the data payload block of dynamic and differencing virtual hard disks, the 4 KB blocks are not aligned to the physical 4 KB boundary, as shown in the following figure.

Figure 24: Virtual hard disk 4 KB block (blue) not aligned with physical 4 KB boundary



Each 4 KB write issued by the current parser—to update the payload data—results in two reads for two blocks on the disk, which are then updated and subsequently written back to the two disk blocks.

The overall performance impact of the RMW process on workloads usually ranged 30 to 80 percent and, at times, was even higher.

Hyper-V in Windows Server 2012 mitigates the performance-degrading effect of 512e disks on the virtual hard disk stack by preparing the previously mentioned structures for alignment to 4 KB boundaries in the VHD format. This avoids the RMW effect when accessing data within the virtual hard disk file and when updating virtual hard disk metadata structures.

Support for hosting virtual hard disks on native 4 KB disks

Hyper-V in Windows Server 2012 makes it possible to store virtual hard disks on 4 KB disks by implementing a software RMW algorithm in the virtual hard disk layer. This algorithm converts 512-byte access-and-update requests to corresponding 4 KB accesses and updates.

Requirements

To take advantage of Hyper-V support for 4 KB disk sectors, you need the following:

- Windows Server 2012.
- Physical disk drives that use the 512e or the native 4 KB format.

Summary

The storage industry is introducing 4 KB physical format drives to provide increased capacity and reliability. Hyper-V in Windows Server 2012 lets you take advantage of this emerging innovation in storage hardware with support for improved performance of virtual hard disks on 512e disks and support for hosting virtual hard disks on native 4 KB disks. Hyper-V 4 KB disk sector support in Windows Server 2012 reduces the performance impact of 512e disks on the virtual hard disk stack, which lets workloads complete disk tasks more quickly.

Quality of Service

Public cloud hosting providers and large enterprises must often run multiple application servers on Hyper-V servers. Hosting providers that host customers on a Hyper-V server must deliver performance that is based on SLAs. Enterprises want to run multiple application servers on a Hyper-V server with the confidence that each application server will perform predictably.

In addition, most hosting providers and enterprises use a dedicated network adapter and a dedicated network for a specific type of workload, such as storage or live migration, to achieve network performance isolation on a Hyper-V server. This strategy works for 1 GbE network adapters but becomes impractical for those using or planning to use 10 GigE network adapters.

For most deployments, one or two 10 GigE network adapters provide enough bandwidth for all the workloads on a Hyper-V server. However, 10 GigE network adapters and switches are considerably more expensive than the 1 GbE counterparts. To optimize the 10 GigE hardware, a Hyper-V server requires new capabilities to manage bandwidth.

Windows Server 2012 expands the power of QoS by introducing the ability to assign a minimum bandwidth to a virtual machine or a service. This feature is important for hosting companies who need to honor SLA clauses that promise a minimum network bandwidth to customers. It’s equally important to enterprises that require predictable network performance when they run virtualized server workloads on shared hardware.

Technical description

In Windows Server 2008 R2, QoS supports the enforcement of maximum bandwidth. This is known as rate limiting. Consider a typical server running Hyper-V in which the following four types of network traffic share a single 10 GigE network adapter:

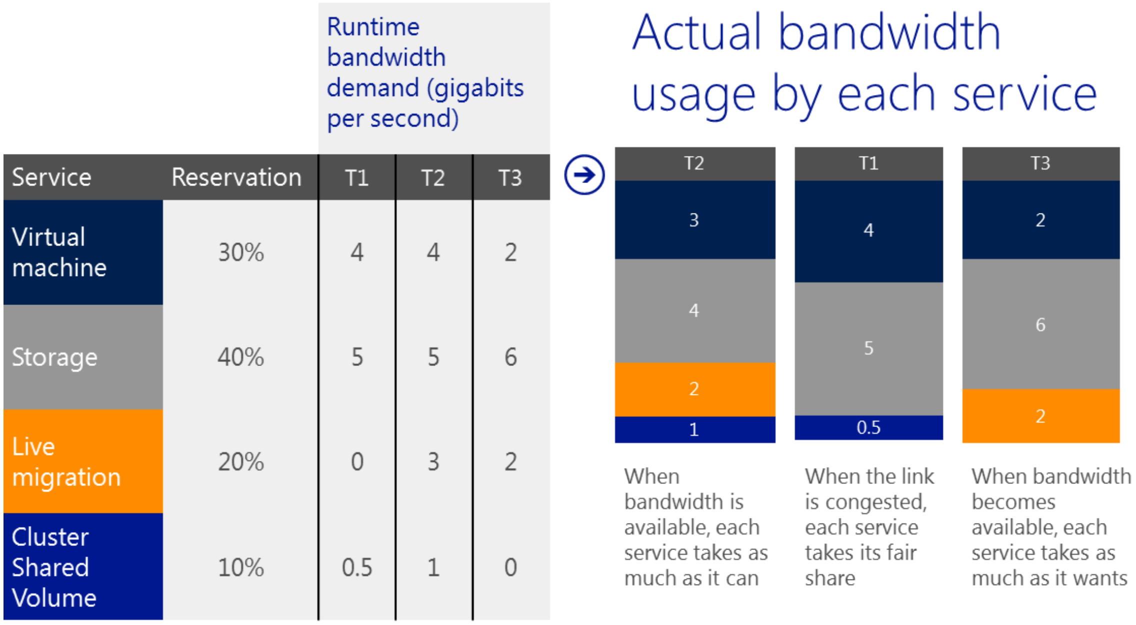
1. Traffic between virtual machines and resources on other servers.
2. Traffic to and from storage.
3. Traffic for live migration of virtual machines between servers running Hyper-V.
4. Traffic to and from a CSV (intercommunication between nodes in a cluster).

If virtual machine data is rate-limited to 3 gigabits per second (Gbps), the sum of the virtual machine data throughputs cannot exceed 3 Gbps at any time, even if other network traffic types don't use the remaining 7 Gbps of bandwidth. However, this also means that the other types of traffic can reduce the actual amount of bandwidth available for virtual machine data to unacceptable levels, depending on how their maximum bandwidths are defined.

Introducing minimum bandwidth

QoS in Windows Server 2012 introduces a new bandwidth management feature: minimum bandwidth. Unlike maximum bandwidth, which is a bandwidth cap, minimum bandwidth is a bandwidth floor. It assigns a certain amount of bandwidth to a given type of traffic. The following figure shows how minimum bandwidth works for each of the four types of network traffic flows in three different time periods: T1, T2, and T3.

Figure 25: Assigning minimum bandwidth to services



		Runtime bandwidth demand (gigabits per second)		
Service	Reservation	T1	T2	T3
Virtual machine	30%	4	4	2
Storage	40%	5	5	6
Live migration	20%	0	3	2
Cluster Shared Volume	10%	0.5	1	0

When bandwidth is available, each service takes as much as it can

When the link is congested, each service takes its fair share

When bandwidth becomes available, each service takes as much as it wants

In this figure, the table on the left shows the configuration of the minimum amount of required bandwidth that a given type of network traffic flow needs. For example, storage is configured to have at least 40 percent of the bandwidth (4 Gbps of a 10 GigE network adapter) at any time. The table on the right shows the actual amount of bandwidth that each type of network traffic has in T1, T2, and T3. In this example, storage is actually sent at 5 Gbps, 4 Gbps, and 6 Gbps, respectively, in the three periods.

The characteristics of minimum bandwidth can be summarized as follows:

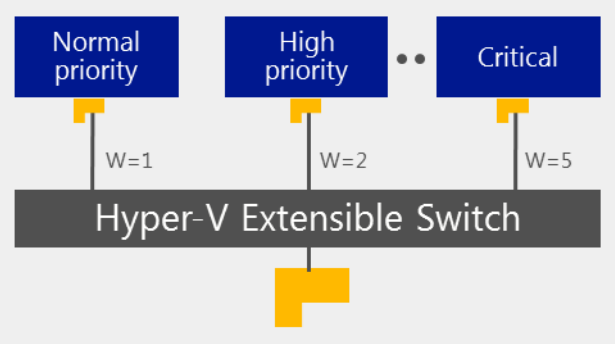
- In the event of congestion, when the desired network bandwidth exceeds the available bandwidth (such as in the T2 period in the figure), minimum bandwidth helps ensure that each type of network traffic receives up to its assigned bandwidth. For this reason, minimum bandwidth is also known as *fair sharing*. This characteristic is essential for converging multiple types of network traffic on a single network adapter.
- If there's no congestion—that is, when sufficient bandwidth is available to accommodate all network traffic (such as in the T1 and T3 periods)—each type of network traffic can exceed its quota and

consume as much bandwidth as is available. This characteristic makes minimum bandwidth superior to maximum bandwidth in using available bandwidth.

Relative minimum bandwidth

If the importance of workloads in virtual machines is relative, you can use relative minimum bandwidth, where you assign a weight to each virtual machine, giving the more important ones a higher weight. You determine the bandwidth fraction that you assign to a virtual machine by dividing the virtual machine's weight by the sum of all the weights of virtual machines that are attached to the Hyper-V Extensible Switch. The following figure illustrates relative minimum bandwidth

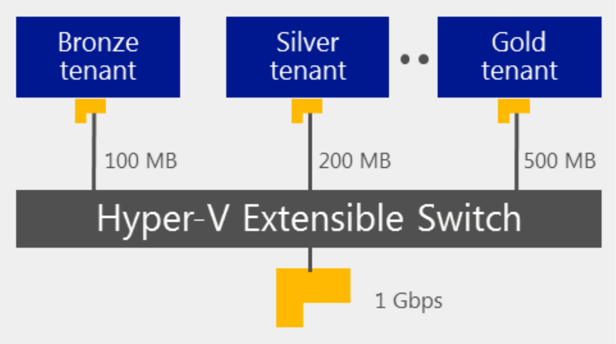
Figure 26: Relative minimum bandwidth



Strict minimum bandwidth

If you want to provide an exact bandwidth, you should use strict minimum bandwidth where you assign an exact bandwidth quota to each virtual machine that is attached to the Hyper-V Extensible Switch.

Figure 27: Strict minimum bandwidth



Minimum bandwidth mechanisms

Windows Server 2012 offers two different mechanisms to enforce minimum bandwidth: one in software (through the newly enhanced packet scheduler in Windows), and the other through the network adapters that support DCB. In both cases, network traffic must be classified first. Windows either classifies a packet itself or gives instructions to a network adapter to classify it. The result of classification is a number of traffic flows in Windows, and a given packet can belong to only one of them.

For example, a traffic flow could be a live migration connection, a file transfer between a server and a client, or a Remote Desktop connection. Based on how the bandwidth policies are configured, either the packet scheduler in Windows or the network adapter dispatches the packets at a rate equal to, or higher than, the minimum bandwidth configured for the traffic flow.

Each of the two mechanisms has its own advantages and disadvantages:

- The software solution, which is built on the new packet scheduler in Windows Server 2012, provides a fine granularity of classification. It is the only viable choice if many traffic flows require minimum bandwidth enforcement. A typical example is a server running Hyper-V hosting many virtual machines, where each virtual machine is classified as a traffic flow.
- The hardware solution, which depends on DCB support on the network adapter, supports far fewer traffic flows. However, it can classify network traffic that doesn't originate from the networking stack. A typical scenario involves a CNA that supports iSCSI offload, in which iSCSI traffic bypasses the networking stack and is framed and transmitted directly by the CNA. Because the packet scheduler in the networking stack doesn't process this offloaded traffic, DCB is the only viable choice to enforce minimum bandwidth.

You can employ both of these mechanisms on the same server. For example, a server running Hyper-V has two physical network adapters: one that binds to a virtual switch and serves virtual machine data, and another that serves the rest of the traffic of the host server. You can enable the software-based minimum bandwidth in Hyper-V to help ensure bandwidth fair sharing among virtual machines, and enable the hardware-based minimum bandwidth on the second network adapter to help ensure bandwidth fair sharing among various types of network traffic from the host server.

It is not recommended that you enable both mechanisms at the same time for a given type of network traffic, however. For example, consider live migration and storage traffic that are configured to use the second network adapter on the server running Hyper-V. If you have already configured the network adapter to allocate bandwidth for live migration and storage traffic using DCB, you shouldn't also configure the packet scheduler in Windows to do the same, and vice versa.

Configuring and managing QoS

In Windows Server 2012, you manage QoS policies and settings dynamically with Windows PowerShell. The new QoS cmdlets support both the QoS functionalities that are available in Windows Server 2008 R2—such as maximum bandwidth and priority tagging—and the new features such as minimum bandwidth that are available in Windows Server 2012.

Requirements

Minimum QoS can be enforced through the following two methods:

- The first method relies on software built into Windows Server 2012 and has no other requirements.
- The second method, which is hardware-assisted, requires a network adapter that supports DCB.

For hardware-enforced minimum bandwidth, you must use a network adapter that supports DCB and the miniport driver of the network adapter must implement the NDIS QoS APIs. A network adapter must support Enhanced Transmission Selection (ETS) and Priority-Based Flow Control (PFC) to pass the NDIS QoS logo test created for Windows Server 2012. Explicit Congestion Notification (ECN) is not required for the logo. The IEEE Enhanced Transmission Selection (ETS) specification includes a software protocol called Data Center Bridging Exchange (DCBX) to let a network adapter and switch exchange DCB configurations. DCBX is also not required for the logo.

Enabling QoS in Windows Server 2012, when it is running as a virtual machine, is not recommended.

Minimum bandwidth enforced by the packet scheduler works optimally on 1 GbE or 10 GigE network adapters.

Summary

To help improve performance in virtualized environments, Windows Server 2012 introduces new QoS bandwidth management features which enable you to assign a minimum bandwidth to a virtual machine or a service. Hosting providers and enterprises can now optimize the number of virtual machines on their Hyper-V servers and have confidence that they will perform as expected.

High availability

This section describes new Hyper-V features in Windows Server 2012 that provide high availability for your mission-critical workloads in new and effective ways. The feature sections included are:

- Incremental Backups.
- Hyper-V Replica.
- Hyper-V Clustering Enhancements.
- NIC Teaming.

Incremental backups

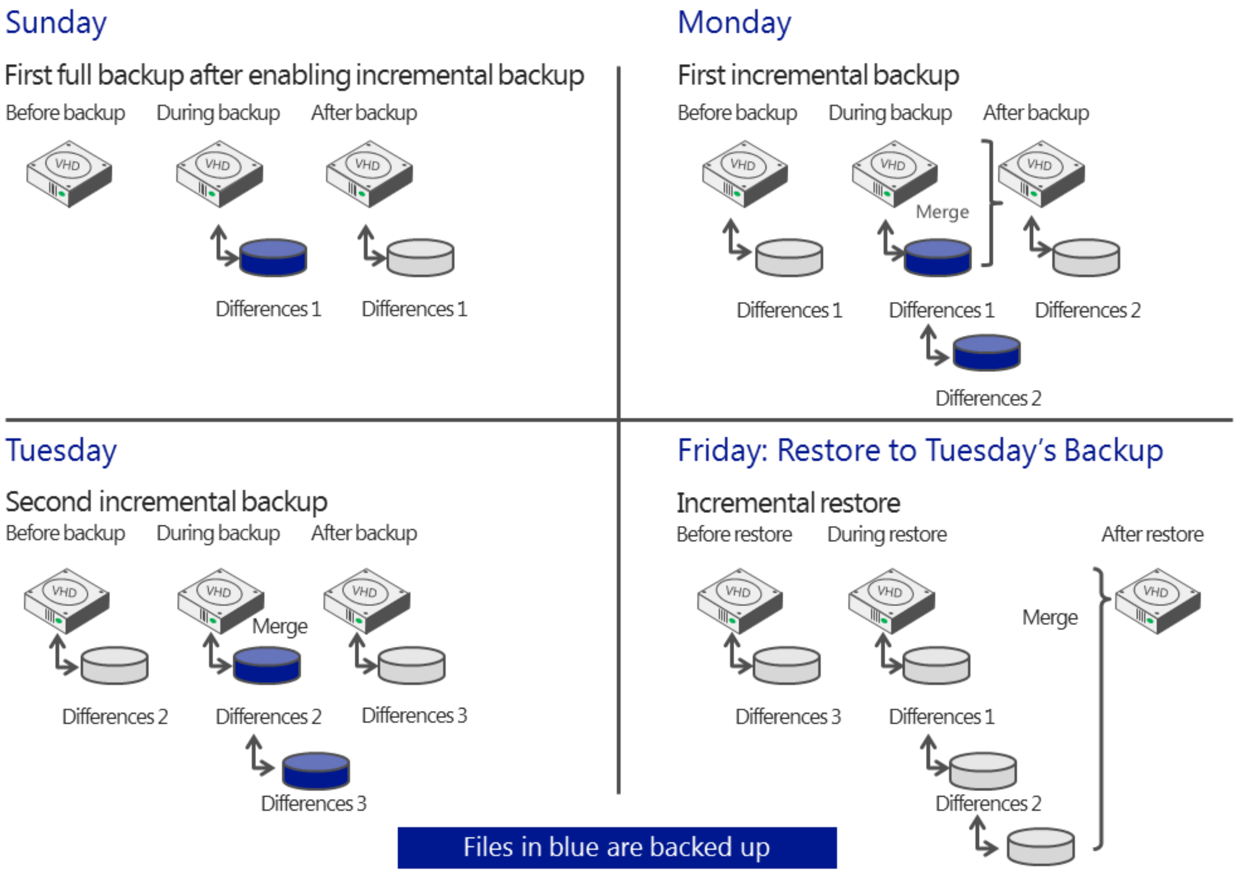
Before Windows Server 2012, backing up data required you to perform full file backups. This meant that you had to either back up the virtual machine and snapshots as flat files when offline, or use Windows Server or third party tools to back up the virtual machine itself with a normal backup of the operating system and data. Windows Server 2012 supports incremental backup of virtual hard disks while the virtual machine is running.

Technical description

Incremental backup of virtual hard disks lets you perform backup operations more quickly and easily, saving network bandwidth and disk space. Because backups are VSS aware, hosting providers can run backups of the Hyper-V environment, backing up tenant virtual machines efficiently and offering additional layers of service to customers without the need for a backup agent inside the virtual machines.

Incremental backup can be independently enabled on each virtual machine through the backup software. Windows Server 2012 uses “recovery snapshots” to track the differences between backups. These are similar to regular virtual machine snapshots, but they are managed directly by Hyper-V software. During each incremental backup, only the differences are backed up (note the blue highlights in the following figure).

Figure 28: Example of incremental backup of a virtual hard disk



The figure above illustrates the incremental backup of a virtual machine with one virtual hard disk and shows 3 days of backups (Sunday, Monday, and Tuesday) followed by a restore (Friday). Of note in this example are the following points:

- To enable change tracking, the virtual machine must be configured to use incremental backup, and a full backup must be performed after incremental backup is enabled (see Sunday).
- During an incremental backup, the virtual machine will briefly be running off of two levels of recovery snapshots. The earlier recovery snapshot is merged into the base virtual hard disk at the end of the backup process.
- The virtual machine's configuration XML files are very small and are backed up often. For simplicity, they are not shown in the figure above.

Requirements

To use incremental backup of virtual hard disks, you need Windows Server 2012 and the Hyper-V role.

Summary

Incremental backup of virtual hard disks saves network bandwidth, reduces backup sizes, saves disk space, and lowers the cost of each backup. It also lets you increase backup frequency because it is now faster and smaller, so backups can be made more often. Because backups are VSS aware, hosting providers can run backups of the entire Hyper-V environment, backing up tenant virtual machines in an efficient way and offering additional layers of service to customers without the need for a backup-agent inside the virtual machines.

Hyper-V Replica

Business continuity depends on fast recovery of business functions after a downtime event, with minimal or no data loss. There are number of reasons why businesses experience outages, including power failure, IT hardware failure, network outage, human errors, IT software failures, and natural disasters. Depending on the type of outage, customers need a high availability solution that simply restores the service.

However, some outages that impact the entire datacenter, such as a natural disaster or an extended power outage, require a disaster recovery solution that restores data at a remote site and brings up the services and connectivity. Organizations need an affordable and reliable business continuity solution that helps them recover from a failure.

Beginning with Windows Server 2008 R2, Hyper-V and Failover Clustering could be used together to make a virtual machine highly available and minimize disruptions. Administrators could seamlessly migrate virtual machines to a different host in the cluster in the event of outage or to load balance their virtual machines without impacting virtualized applications.

While these measures could protect virtualized workloads from a local host failure or scheduled maintenance of a host in a cluster, they did not protect businesses from outages of an entire datacenter. While Failover Clustering can be used with hardware-based SAN replication across datacenters, these are typically expensive. Hyper-V Replica, a new feature in Windows Server 2012, now offers an affordable in-box disaster recovery solution.

Hyper-V Replica provides asynchronous replication of virtual machines for the purposes of business continuity and disaster recovery. In the event of failures (such as a power failure, fire, or natural disaster) at the primary site, an administrator can manually fail over the production virtual machines to the Hyper-V server at the recovery site.

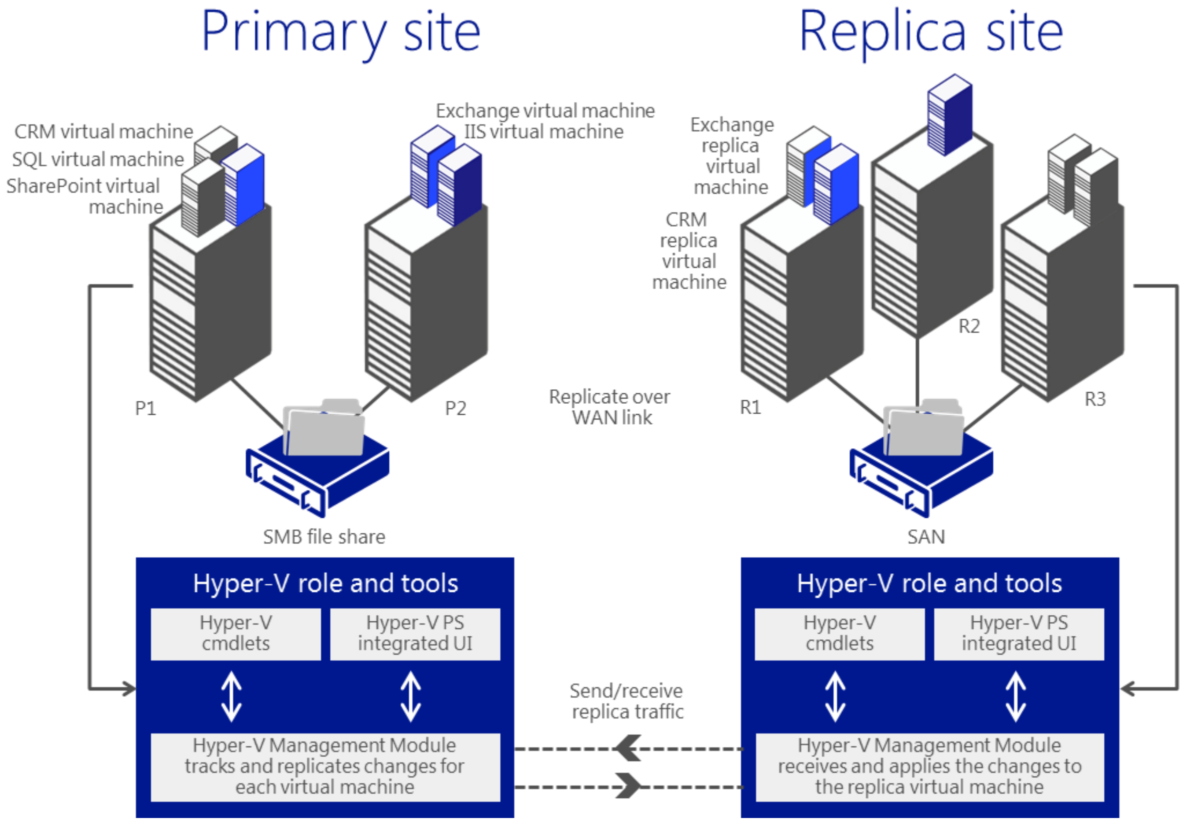
During failover, the virtual machines are brought back to a consistent point in time, and within minutes they can be accessed by the rest of the network with minimal impact to the business. Once the primary site comes back, the administrator can manually revert the virtual machines to the Hyper-V server at the primary site.

Technical description

Hyper-V Replica is a new feature in Windows Server 2012. It lets you replicate your Hyper-V virtual machines over a network link from one Hyper-V host at a primary site to another Hyper-V host at a Replica site without reliance on storage arrays or other software replication technologies.

The following figure shows secure replication of virtual machines from different systems and clusters to a remote site over a WAN.

Figure 29: Replicating virtual machines from several systems to a remote site over a WAN


Primary site
Replica site
CRM virtual machine
SQL virtual machine
SharePoint virtual machine
Exchange virtual machine
IIS virtual machine
P1
P2
SMB file share
Replicate over WAN link
Exchange replica virtual machine
CRM replica virtual machine
R1
R2
R3
SAN
Hyper-V role and tools
Hyper-V cmdlets
Hyper-V PS integrated UI
Hyper-V Management Module tracks and replicates changes for each virtual machine
Send/receive replica traffic
Hyper-V role and tools
Hyper-V cmdlets
Hyper-V PS integrated UI
Hyper-V Management Module receives and applies the changes to the replica virtual machine

Hyper-V Replica tracks the write operations on the primary virtual machine and replicates these changes to the Replica server efficiently over a WAN. The network connection between the two servers uses the HTTP or HTTPS protocol and supports both Windows-integrated and certificate-based authentication. For an encrypted connection, you should choose certificate-based authentication. Hyper-V Replica can also be closely integrated with Windows Failover Clustering, and provides easier replication across different migration scenarios in the primary and Replica servers.

Hyper-V Replica includes the following tools to simplify management:

- Integrated UI with Hyper-V Manager and the Failover Clustering Manager snap-in for Microsoft Management Console (MMC).
- Extensible WMI interface.
- Windows PowerShell command-line interface scripting capability.

Requirements

To use Hyper-V Replica, you need two physical computers configured with:

- Windows Server 2012.
- Hyper-V server role.
- Hardware that supports the Hyper-V role.
- Sufficient storage to host the files that virtualized workloads use (additional storage on the Replica server based on replication configuration settings may be necessary).

- Sufficient network bandwidth among the locations that host the primary and Replica servers and sites.
- Firewall rules to permit replication between the primary and Replica servers and sites.
- Failover Clustering feature (if you want to use Hyper-V Replica on a clustered virtual machine).

Summary

With Hyper-V Replica, you can implement a more affordable and efficient failure recovery solution that automatically replicates Hyper-V virtual machines across your storage systems, networks, and clusters.

You can use Hyper-V Replica to provide a virtual machine-level replication solution that efficiently replicates data over a network link to a remote site without reliance on storage arrays or other software replication technologies. Hyper-V Replica provides a storage-agnostic and workload-agnostic solution that replicates more efficiently, periodically, and asynchronously over IP-based networks, typically to a remote site. It also lets you easily test the Replica virtual machine with little disruption to the ongoing replication. If a failure occurs at the primary site, you can restore business operations by bringing up the replicated virtual machine at the Replica site. Hyper-V Replica provides a virtual machine-level, more affordable, more reliable, and more manageable replication solution that is integrated with Hyper-V Manager and the Failover Clustering feature in Windows Server 2012.

Hyper-V Replica is a software replication solution that works across domains and networks, so businesses can enable replication from their datacenters to a remote hosting provider's datacenter. Because Hyper-V Replica is application-agnostic and works at the granularity level of a virtual machine, it enables hosting providers to manage their virtual machines without knowing intimate details about the workloads within the virtual machines.

NIC Teaming

The failure of an individual Hyper-V port or virtual network adapter can cause a loss of connectivity for a virtual machine. Using multiple virtual network adapters in a Network Interface Card (NIC) Teaming solution can prevent connectivity loss and, when multiple adapters are connected, multiply throughput.

To increase reliability and performance in virtualized environments, Windows Server 2012 includes built-in support for NIC Teaming-capable network adapter hardware. Although NIC Teaming in Windows Server 2012 is not a Hyper-V feature, it is important for business-critical Hyper-V environments because it can provide increased reliability and performance for virtual machines. NIC Teaming is also known as "network adapter teaming technology" and "load balancing failover" (LBFO).

Technical description

NIC Teaming in Windows Server 2012 lets a virtual machine have virtual network adapters that are connected to more than one virtual switch and still have connectivity even if the network adapter under that virtual switch is disconnected. This is particularly important when working with features such as SR-IOV traffic, which does not go through the Hyper-V Extensible Switch and thus cannot be protected by a network adapter team that is under a virtual switch.

With the virtual machine teaming option, you can set up two virtual switches, each connected to its own SR-IOV–capable network adapter. NIC Teaming then works in one of the following ways:

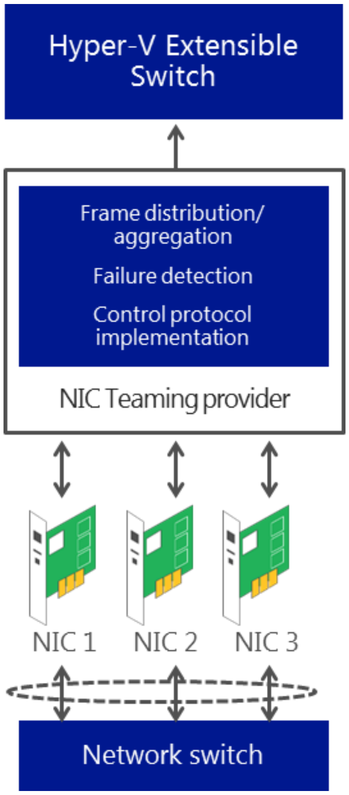
- Each virtual machine can install a virtual function from one or both SR-IOV network adapters and, if a network adapter disconnection occurs, fail over from the primary virtual function to the back-up virtual function.

- Each virtual machine may have a virtual function from one network adapter and a non-virtual function interface to the other switch. If the network adapter associated with the virtual function becomes disconnected, the traffic can fail over to the other switch without losing connectivity.

Because failover between network adapters in a virtual machine might result in traffic being sent with the MAC address of the other interface, each virtual switch port associated with a virtual machine using NIC Teaming must be set to permit MAC spoofing.

The Windows Server 2012 implementation of NIC Teaming supports up to 32 network adapters in a team. As shown in the following figure, the Hyper-V Extensible Switch can take advantage of the native provider support for NIC Teaming, allowing high availability and load balancing across multiple physical network interfaces.

Figure 30: Hyper-V Extensible Switch and native provider support for NIC Teaming


Hyper-V Extensible Switch
Frame distribution/ aggregation
Failure detection
Control protocol implementation
NIC Teaming provider
NIC 1
NIC 2
NIC 3
Network switch

Requirements

To implement NIC Teaming for a virtual machine, you need:

- Windows Server 2012.
- At least one network adapter or two or more network adapters of the same speed.
- Two or more network adapters (if you are seeking bandwidth aggregation or failover protection).
- One or more network adapters (if you are seeking VLAN segregation for the network stack).

Summary

The NIC Teaming feature in Windows Server 2012 gives you the benefit of network fault tolerance on physical servers and virtual machines by using at least two receive-side scaling (RSS)-capable network adapters from any vendor, without the need for a third-party teaming solution. This combination of two or more network adapters lets you obtain twice the throughput (or better), and have the ability to maintain network connection when one of the network adapters fails.

Hyper-V clustering enhancements

Clustering has provided organizations with protection against:

- Application and service failure.
- System and hardware failures (for example, CPUs, drives, memory, network adapters, and power supplies).
- Site failure (which could be caused by natural disaster, power outages, or connectivity outages).

Clustering enables high-availability solutions for many workloads, and has included Hyper-V support since its initial release. By clustering your virtualized platform, you can increase availability and enable access to server-based applications during planned or unplanned downtime.

Technical description

Windows Server 2012 clustering support for Hyper-V adds many new features, including:

- **Support for guest clustering via Fibre Channel.** Windows Server 2012 provides virtual Fibre Channel adapters within the virtual machine, giving your workloads access to storage area networks using Fibre Channel fabric. In addition, a virtual Fibre Channel enables you to:
  - Cluster guest operating systems over Fibre Channel providing HA for workloads within virtual machines.
  - Use Windows MPIO for high-availability and load balancing on the storage path.

  By employing MPIO and Failover Clustering together as complimentary technologies, users can mitigate the risk of a system outage at both the hardware and application levels.
- **Live migration enhancements**. Live migrations have been enhanced to use more available network bandwidth, which dramatically increases the performance of Live Migration and enables concurrent Live Migrations with no limits. The number of Live Migrations possible depends on how much you want to invest in your network infrastructure.
- **Massive Scale.** Windows Server 2012 now supports up to 64 nodes and up to 4,000 virtual machines in a cluster.
- **Encrypted cluster volumes**. Hyper-V, Failover Clustering, and Microsoft BitLocker now work in concert to create an ideal, highly secure platform for private cloud infrastructure. Windows Server 2012 Cluster disks encrypted using BitLocker Drive Encryption enable better physical security for deployments outside secure datacenters, providing a critical safeguard for the cloud and helping protect against data leaks.

- **Cluster Shared Volume 2.0 (CSV).** CSV has been greatly enhanced in a number of ways. From a usability standpoint:
    - CSV is now a core Failover Clustering feature (no longer a separate component that needs to be enabled).
    - Enabling CSV on a disk is now a single right click with the mouse.
    - CSV disks are now included in the Failover Cluster Manager Storage view easing management.

  To support up to 64 nodes in a cluster, CSV has been improved in both performance and scalability. In terms of integrating with Microsoft partners, CSV has specifically been enhanced to work out of the box with storage filter drivers such as those used by third-party anti-virus, data protection, backup and storage replication software products.
- **Hyper-V application monitoring.** With Windows Server 2012, Hyper-V and Failover Clustering work together to bring higher availability to workloads that do not support clustering. They do this by providing a lightweight, simple solution to monitor applications running on virtual machines and integrating with the host. By monitoring services and event logs inside the virtual machine, Hyper-V and Failover Clustering can detect whether the key services that a virtual machine provides are healthy, and if necessary provide automatic corrective action such as restarting the virtual machine or restarting a service within the virtual machine.
- **Virtual machine failover prioritization.** Virtual machine priorities can now be configured to control the order in which specific virtual machines fail over or start. This ensures that high-priority virtual machines get the resources they need, and that lower-priority virtual machines are given resources as they become available.
- **Inbox live migration queuing.** Administrators can now perform large multi-select actions to queue live migrations of multiple virtual machines easily and efficiently.
- **Affinity (and anti-affinity) virtual machine rules.** Administrators can now configure partnered virtual machines so that at failover, the partnered machines are migrated simultaneously. For example, administrators can configure a SharePoint virtual machine and the partnered SQL Server virtual machine to always fail over together to the same node. Administrators can also specify that two specific virtual machines cannot coexist on the same node in a failover scenario.
- **File server transparent failover.** You can now more easily perform hardware or software maintenance of nodes in a File Server cluster (for example, storage virtual machine files such as configuration files, virtual hard disk files, and snapshots in file shares over the SMB 3 protocol) by moving file shares between nodes with little interruption to server applications that are storing data on these file shares. Also, if a hardware or software failure occurs on a cluster node, SMB 3 transparent failover lets file shares fail over to another cluster node with little interruption to server applications that are storing data on these file shares.

Requirements

- Windows Server 2012 with the Hyper-V role installed.
- Network infrastructure that connects the nodes (servers) in the cluster. In this network infrastructure, avoid having single points of failure.
- Storage that is attached to all nodes in the cluster.
- Device controllers or appropriate adapters for the storage. These can be Serial Attached SCSI (SAS), Fibre Channel, or iSCSI.

Scenario

Contoso, Ltd. has used clustering in the past for their virtual machines to increase availability through planned and unplanned downtime events. With Windows Server 2012, Contoso now can deploy more virtual machines into these nodes so that in a downtime event, high-priority virtual machines are migrated first and required resources are available to them. Through their existing investment in Fibre Channel, Contoso can also increase its storage performance via direct access through their virtual machine guests, as well as using BitLocker so that offsite and cloud-based clusters are more secure.

Summary

Windows Server 2012 enhances the clustered environment to fully extend its features to a new level, supporting greater access to storage, faster failover and migration of nodes, and better integrated data security for offsite clusters.

Conclusion

Virtualization technologies help customers reduce costs and deliver greater agility and economies of scale. As either a stand-alone product or an integrated part of Windows Server, Hyper-V is a leading virtualization platform for today and provides a transformational opportunity with cloud computing.

In the datacenter, on the desktop, and now in the cloud, the Microsoft virtualization platform—led by Hyper-V and management tools—makes great sense and offers exceptional value for the money.

Appendix: Hyper-V before Windows Server 2012

Beginning with Windows Server 2008, server virtualization via Hyper-V technology has been an integral part of the operating system. A new version of Hyper-V was included as a part of Windows Server 2008 R2, and it was updated in the release of Service Pack 1 (SP1).

There are two manifestations of the Microsoft Hyper-V technology:

- The hypervisor-based virtualization feature of Windows Server 2008 R2, installed as a Windows Server role.
- Microsoft Hyper-V Server, a free stand-alone product containing only the Windows Hypervisor, Windows Server driver model, and virtualization components.

Hyper-V is a powerful virtualization technology that enables businesses to take advantage of virtualization's benefits, such as reducing costs, increasing hardware utilization, optimizing business infrastructure, and improving server availability. Ideal for server consolidation in both the datacenter and remote sites, it empowers organizations to make more efficient use of their hardware resources. It also enables IT organizations to enhance their administrative productivity and to rapidly deploy new servers to address changing business needs.

Hyper-V uses 64-bit hypervisor-based technology, which vastly increases performance for virtual machines running Windows Server 2008 R2, Windows Server 2008, Windows Server 2003, specific Linux distributions, and Xen-enabled Linux, by giving them the ability to work as closely as possible with CPUs and memory in a shared environment.

Since its release, Hyper-V included numerous improvements for creating dynamic virtual datacenters, including:

- **Increased availability for moving virtual machines**. One of the most important aspects of any datacenter is providing the highest possible availability for systems and applications. Virtual datacenters are no exception to the need for high availability. Hyper-V in Windows Server 2008 R2 included Live Migration, which enabled users to move a virtual machine between server nodes on a cluster or servers using shared storage, with minimal interruption of service.
- **Increased availability for addition and removal of virtual machine storage**. Windows Server 2008 R2 Hyper-V supported hot plug-in and hot removal of virtual machine storage. By supporting the addition or removal of virtual hard disk files and pass-through disks while a virtual machine is running, Windows Server 2008 R2 Hyper-V enabled faster reconfiguration of virtual machines to meet changing requirements.
- **Improved management of virtual datacenters**. Even with all the efficiency gains made possible by virtualization, virtual machines still must be managed. The number of virtual machines tends to proliferate much faster than physical computers (because virtual machines typically do not require a

hardware acquisition), making efficient management of virtual datacenters even imperative than ever before. Windows Server 2008 R2 included the following management tools:

  - A Hyper-V management console, which simplifies day-to-day Hyper-V administrative tasks.
  - System Center Virtual Machine Manager, which improves management of multiple Hyper-V servers in a virtual datacenter environment.

- **Simplified method for physical and virtual computer deployments**. Historically, deploying operating systems and applications to physical and virtual computers used different methods. For virtual computers, the .vhd file format has become a de facto standard for deploying and interchanging preconfigured operating systems and applications. Windows Server 2008 R2 also supported the ability to boot a computer from a .vhd file stored on a local hard disk. This lets you use preconfigured .vhd files to deploy virtual and physical computers. This helped reduce the number of images users needed to manage, and provided an easier method for testing deployments before rolling them out to a production environment.
- **Hyper-V processor compatibility mode for live migration**. As the scope of virtualization increases rapidly in today's enterprise, customers chafe against hardware restrictions when they perform virtual machine migrations across physical hosts. Windows Server 2008 R2 Hyper-V introduced a new capability called "processor compatibility mode for live migration," which enabled live migrations across hosts with differing CPU architectures.
- **Improved virtual networking performance**. Hyper-V took advantage of several networking technologies in Windows Server 2008 R2 to improve overall virtual machine networking performance. Two key examples of this were support for Jumbo Frames, and support for the Virtual Machine Queue (VMQ).

  Support for Jumbo Frames was introduced with Windows Server 2008. Hyper-V in Windows Server 2008 R2 extended this capability to virtual machines. So just like in physical network scenarios, Jumbo Frames added the same basic performance enhancements to virtual networking, including up to six times larger payloads per packet for improved overall throughput and reduced CPU usage during large file transfers.

  VMQ allowed the host's network adapter to deliver Direct Memory Access (DMA) packets directly into individual virtual machine memory stacks. Each virtual machine device buffer is assigned a VMQ, which avoids needless packet copies and route lookups in the virtual switch. Essentially, VMQ allowed the host's single network adapter to appear as multiple network adapters to the virtual machines, allowing each virtual machine its own dedicated network adapter. The result was less data in the host's buffers and an overall performance improvement in I/O operations.
- **Improved virtual machine memory management**. Windows Server 2008 R2 SP1 introduced Hyper-V Dynamic Memory, which enabled customers to better utilize the memory resources of Hyper-V hosts by balancing how memory is distributed between virtual machines running on a network. Memory can be dynamically reallocated between different virtual machines in response to the changing workloads on these machines. Dynamic Memory thus made possible more efficient use of memory while maintaining consistent workload performance and scalability. Implementing Dynamic Memory thus enabled higher levels of server consolidation with minimal impact on performance.

List of charts, tables, and figures

Tables

Figures