Windows Server 2016 Hyper-V

Agenda

- 09:00 – 09:30 – Anmeldung
- 09:30 – 11:00 – Hyper-V Allgemein & Netzwerk
- 11:00 – 11:15 – Kaffeepause
- 11:15 – 12:30 – Hyper-V & Storage
- 12:30 – 13:30 – Mittagspause
- 13:30 – 14:30 – Storage Spaces Direct Hyper-converged
- 14:30 – 14:45 – Kaffeepause
- 14:45 – 15:45 – Hyper-V Security
- 15:45 – 16:30 – System Center Virtual Machine Manager 2016

Wer bin ich?

- Marc Grote
- Seit 1989 hauptberuflich ITler / Seit 1995 Selbststaendig
- Microsoft MVP fuer Hyper-V seit 2014 (MVP Forefront von 2004-2014)
- Microsoft MCT/MCSE Messaging/Security/Server/MCLC /MCITP*/MCTS*/MCSA*/MC*
  MCSE Private Cloud, Server Infrastructure
  MCS Server Virtualization Hyper-V System Center/Azure
  MCITP Virtualization Administrator
- Buchautor und Autor fuer Fachzeitschriften
- Schwerpunkte:
  - Windows Server Clustering/Virtualisierung/PKI
  - System Center SCVMM/SCEP/DPM
  - Exchange Server seit Version 5.0
  - von *.Forefront reden wir nicht mehr ☹

Hyper-V Allgemein & Netzwerk

- Hyper-V Neuerungen
- Management
- Failover Cluster
- Container
- Nano Server
- Netzwerk Neuerungen

Hyper-V

- Nano Server
- Windows Server und Hyper-V Container
- ReFS Accelerated VHDX Operations (Fixed Size Disk + Merge)
- Nested Virtualization
- Neues Shared VHDX Funktionen (Dynamic Resize, Replica, Host Backup)
- Virtual TPM – Bitlocker Support
- Discrete Device Assignment (DDA)
- Shielded VMs –> Host Guardian Service –> Virtual TPM
- Virtual Machine Configuration changes
- Production VM Checkpoints (Snapshots)
- Hyper-V Replica Unterstuetzung fuer VHDX Dateien im laufenden Betrieb
- Hot add / remove von Virtual Machine Memory / NIC

Demo Nano

Nano Server

- Neuer Micro Server
- Full Server, Minimal Shell, Core → Nano
- 93 % weniger Groesse, 92 % weniger kritische Updates, 80 % weniger Reboots
- Nur Emergency Konsole local
- Erstellung per Powershell
- Remote Management per Powershell und WMI, Hyper-V Manager
- Powershell Core
- Nur 64 Bit, keine GUI
- Eingeschraenkte Rollenfunktionalitaet (Web Server, Hyper-V Host, SOFS Server
- Nur CBB Support, kein LTSB

Nano Server Management

- Auf dem Desktop NET START WINRM
- Set-Item WSMan:\localhost\Client\TrustedHosts -Value 192.168.16.87
- Install-PackageProvider NanoServerPackage
- VM: Import-Module NanoServerPackage
- Get-Command -Module NanoServerPackage
- Install-NanoServerPackage -Name Microsoft-NanoServer-IIS-Package -MinimumVersion 10.0.14393.0
- Remote: Enter-PSSession -ComputerName 192.168.16.87 -Credential NANO1\Administrator
- PS Direct: Enter-PSSession -VMName NANO1 -Credential NANO1\Administrator

Demo

Windows- und Hyper-V Container

- Container enthalten eine isolierte Betriebssystem Umgebung zur Ausfuehrung von Anwendungen
- Container sind portabel
- Windows Container isolieren Anwendungen nutzen aber gemeinsame OS-Ressourcen
- Hyper-V Container isolieren Anwendungen und stellen eigene OS-Ressourcen zur Verfuegung
- Windows Container koennen zu Hyper-V Container ohne Datenverlust migriert werden

Windows Container

- Install-Module -Name DockerMsftProvider -Repository PSGallery -Force
- Install-Package -Name docker -ProviderName DockerMsftProvider
- Restart-Computer -Force
- docker pull microsoft/iis
- docker images
- docker run -it –d -p 80:80 microsoft/iis cmd.exe
- docker ps
- Docker stop aa4bc4bcc40b

Hyper-V

- Virtual Network Adapter Identification (like CDN)
- Hyper-V Manager Verbesserungen
- Power Management Verbesserungen (Connected Standby)
- Neuer Virtual Machine Upgrade Prozess (Versionierung)
- Update der IC-Version mit MU/WU
- Binaere VM Konfigurations-Dateien
- Distributed Storage QoS
- Virtual Machine Storage Resiliency
- Verbessertes Hyper-V Backup
- RemoteFX OpenGL 4.4, OpenCL 1.1
- Verbessertes Hyper-V Cluster Management (WMI gegen Cluster)
- PowerShell Direct

Demo

Netzwerk Neuerungen

- Switch Embedded Teaming (SET)
- Virtual Machine Multi Queues (VMMQ)
- Quality of Service (QoS) fuer Software-definierte Netzwerke
- Network Controller
- Hyper-V NAT Switch
- Datacenter Firewall
- Software Load Balancing (SLB)

Switch Embedded Teaming

LBFO/SET Feature comparison						
Feature	**LBFO**	**SET**		**Feature interactions:** works with	**LBFO**	**SET**
Switch independent teaming				Checksum offloads		
Switch dependent teaming: Static				DCB		
Switch dependent teaming: LACP				HNV v1		
Dynamic load distribution				HNV v2		
HyperVPort mode load distribution				IEEE 802.1X		
Address hash load distribution				IPsecTO		
Active/Standby operation				LSO		
Teams of up to ___ members	32	8		RDMA		
VMM managed		RTM		RSC		
Inbox UI managed				RSS		
PowerShell managed				SDN-QoS		
Works in Native stack				SR-IOV		
Works in a VM				TCP Chimney		
Teams different speed NICs				VMMQ		
Teams different NICs				VMQ (filter)		
vNICs/vmNICs affinitized to team members				VMQ (NIC Switch)		
				vmQoS		
				vRSS		

Source: https://gallery.technet.microsoft.com/Windows-Server-2016-839cb607

Quality of Service (QoS)

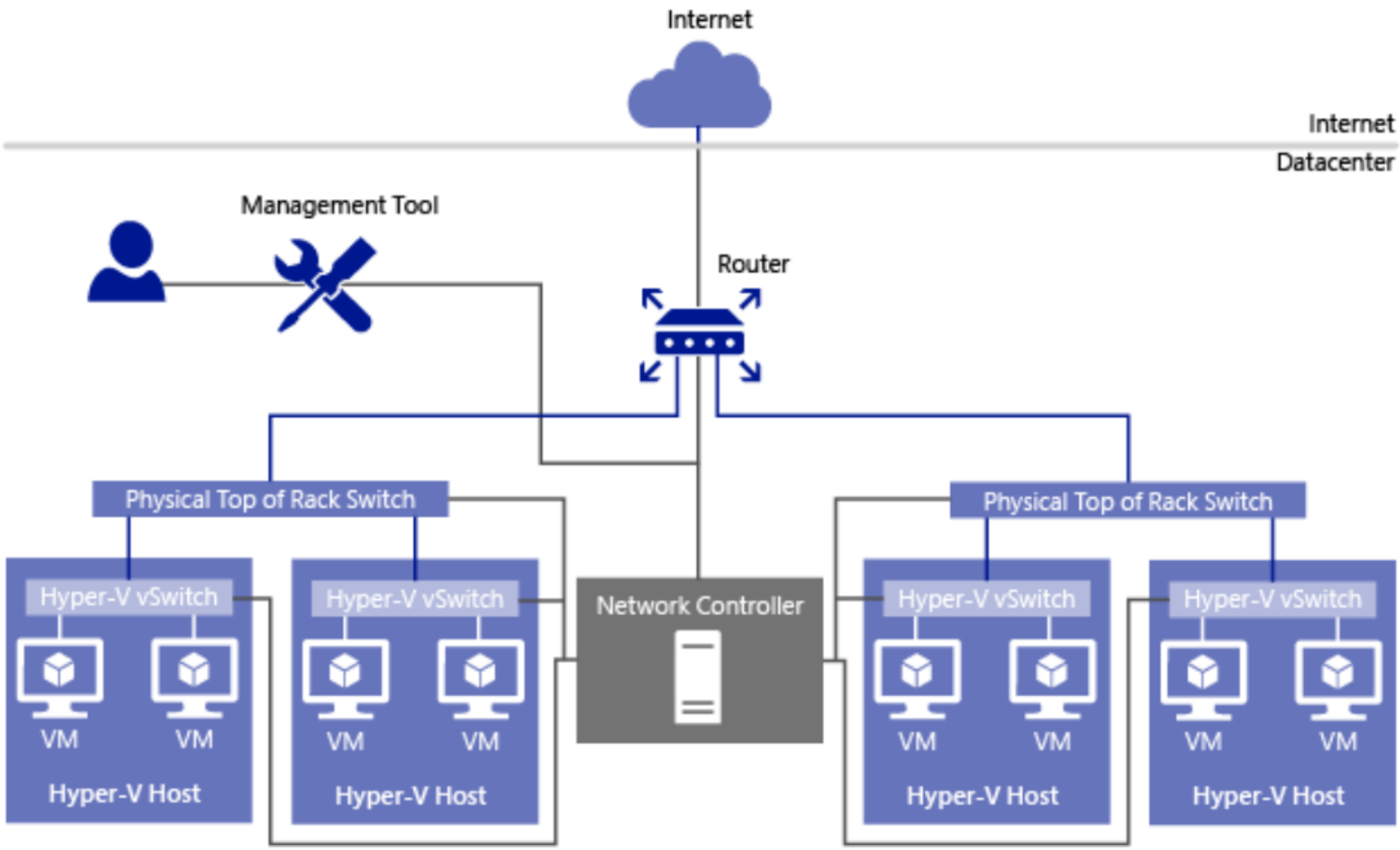
- Storage QoS pro VM manuell oder im Cluster …
- Storage QoS im Cluster fuer SOFS und CSV
- MONITORING
  - Get-VM | Enable-VMResourceMetering
  - Measure-VM –VMName Name der VM oder Get-VM | Measure-VM
- New-StorageQosPolicy -Name ConcatWorkstation -PolicyType Dedicated -MinimumIops 100 -MaximumIops 300
- Get-VM -Name ConcatDesk* | Get-VMHardDiskDrive | Set-VMHardDiskDrive -QoSPolicyID abcdefghijklmnopqrst

Demo

Hyper-V NAT Switch

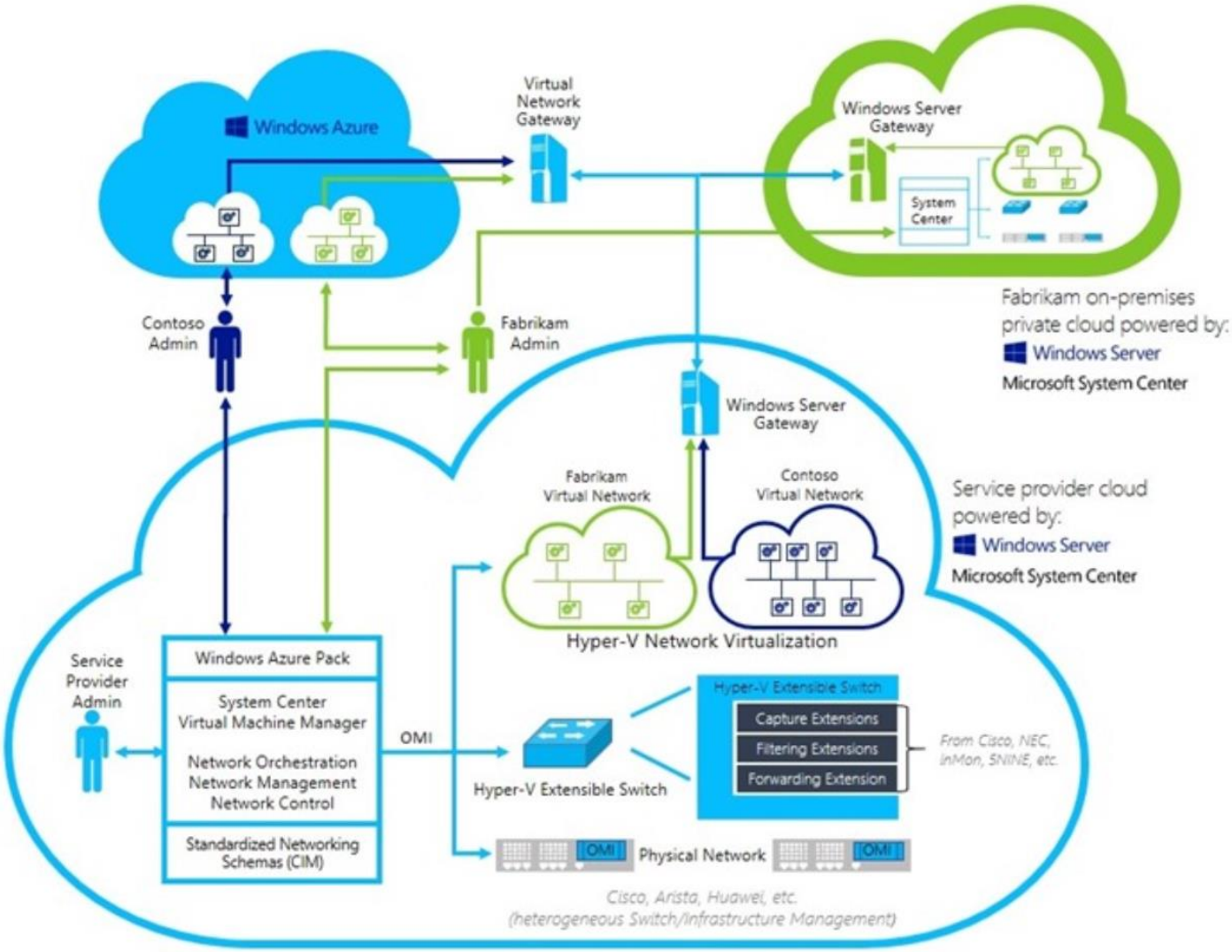
- **Achtung**: Aenderung seit 2016 RTM und W10 Anniversary Update
- New-VMSwitch -Name NATSwitch -SwitchType Internal
- $ifindex = (Get-NetAdapter | where {$_.Name –match “NameDerNIC”}).ifIndex
- New-NetIPAddress -IPAddress 192.168.16.1 -PrefixLength 24 -InterfaceIndex $ifindex
- New-NetNat –Name “NATSwitch” -InternalIPInterfaceAddressPrefix "192.168.16.0/24“
- VM mit NAT Switch verbinden, IP Konfiguration manuell (192.168.16.xxx), Default Gateway auf IP-Adresse des NAT Adapters setzen (192.168.16.1)

Network Controller



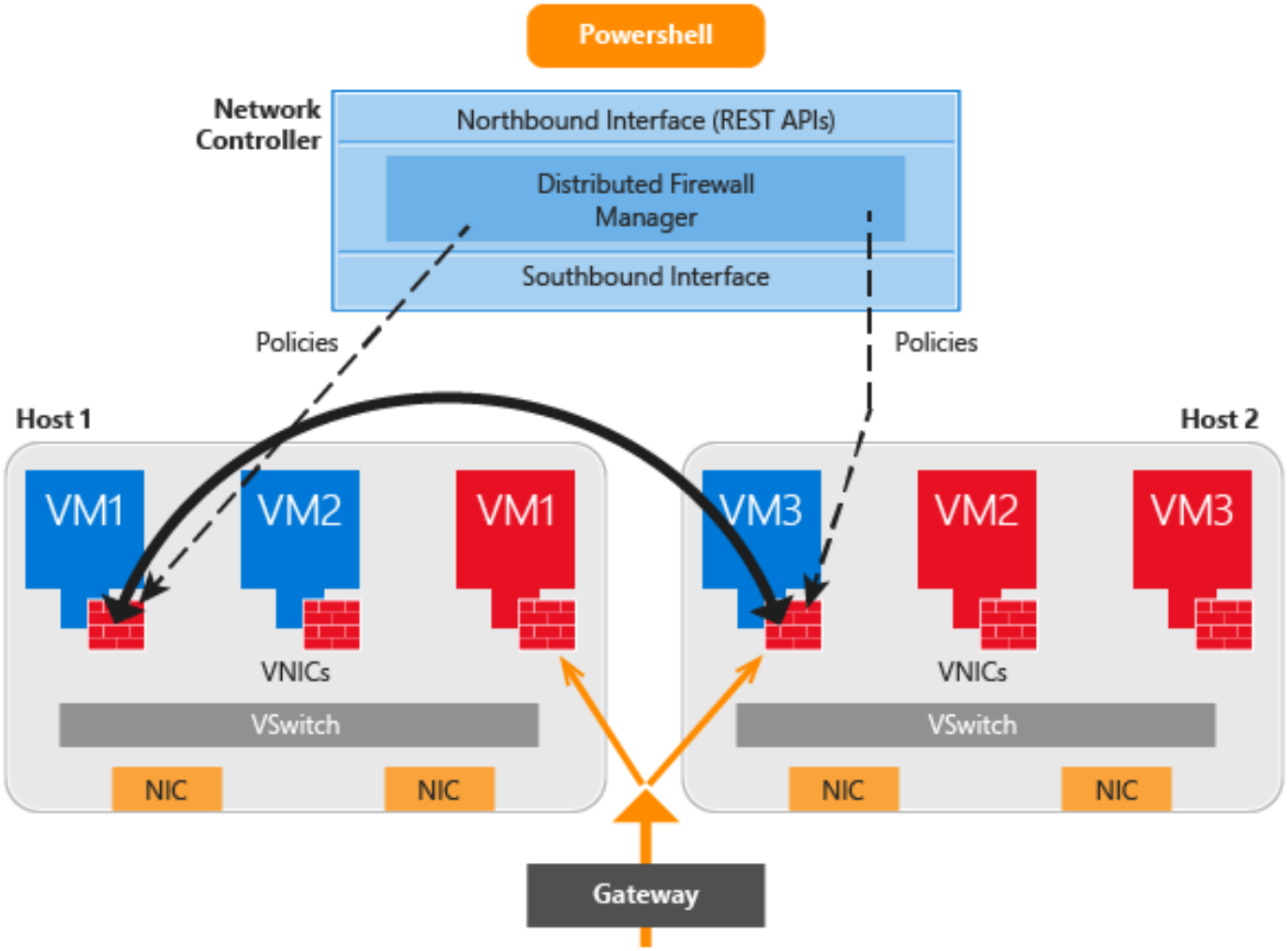
Source: https://technet.microsoft.com/en-us/library/dn859239.aspx

Software Defined Networking



Source: http://blogs.technet.com/b/in_the_cloud/archive/2013/10/31/networking-without-limits-sdn.aspx

Datacenter Firewall



Source: https://technet.microsoft.com/en-us/windows-server-docs/networking/sdn/technologies/network-function-virtualization/datacenter-firewall-overview

Demo

Failover Clustering

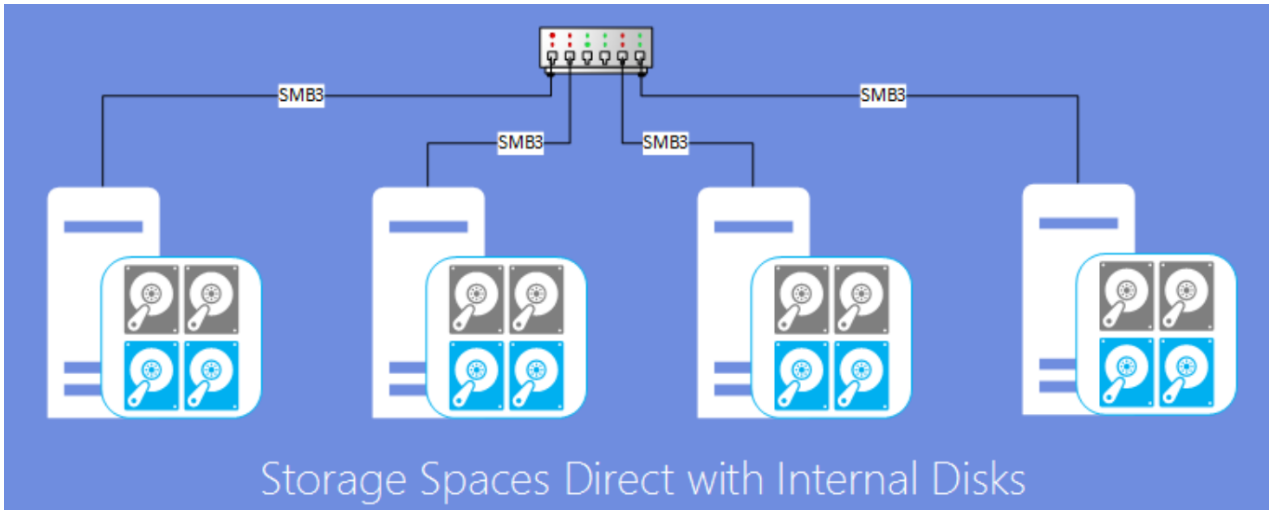
- Virtual Machine Cluster Resiliency
  - Quarantine (Kein Cluster Join fuer 2 Stunden, VM Drain, nicht mehr als 20% Hosts)
  - Isolated (Node kein Active Member, VMs werden weiter gehostet)
  - Konfiguration per PS (Get-Cluster ….)
- Cluster Rolling Upgrade
- Host Resource Protection in VM
- Cloud Witness in Microsoft Azure
- Host Guardian Service (VM Isolation fuer Tenants)
- Start Order Prioritaet fuer VM im Cluster
- Site Aware Cluster
  - Failover Affinity, Storage Affinity, Cross-Site Heartbeating
- Verbessertes Cluster Log
  - TimeZone, VerboseDiagnostic EventViewer, Active Memory Dump

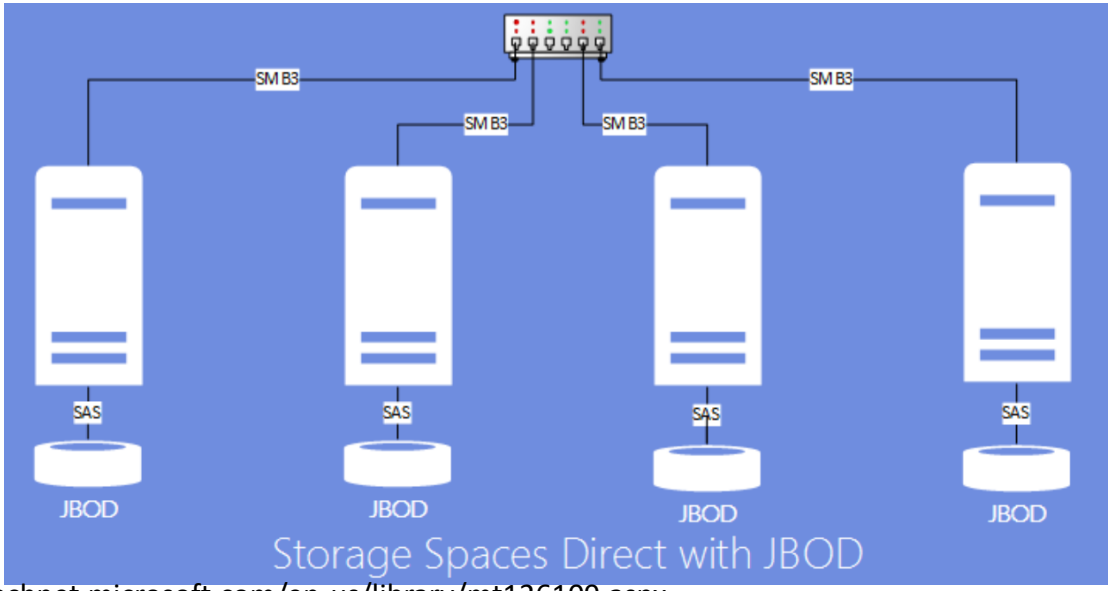
Demo

Hyper-V & Storage

- Distributed Storage QoS
- Rebalancing in Storage Spaces
- Storage Replica
- Virtual Machine Storage Resiliency
- Storage Spaces Direct (S2D)
- Shared VHDX

Storage Spaces Direct





Source: https://technet.microsoft.com/en-us/library/mt126109.aspx

Storage Replica

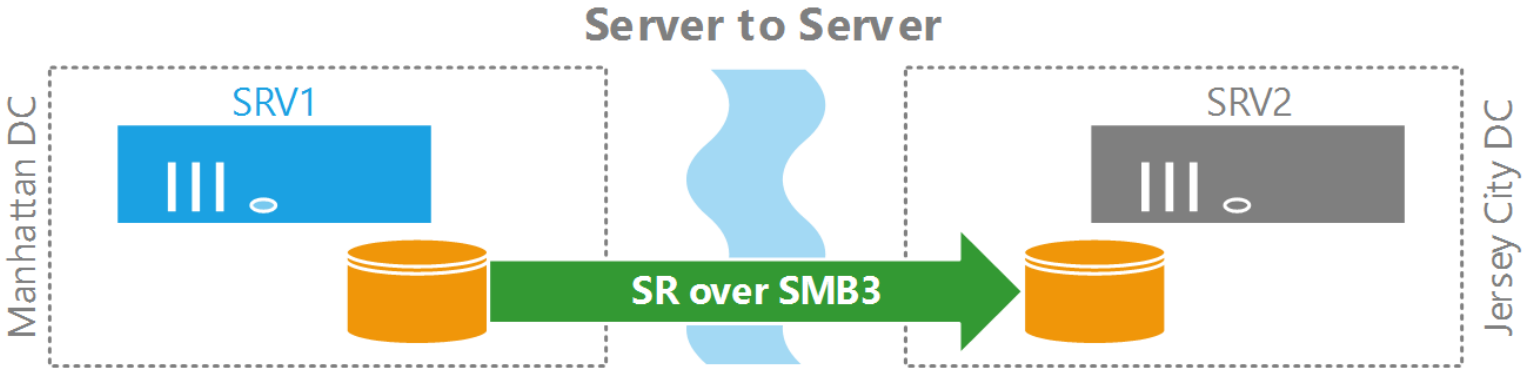
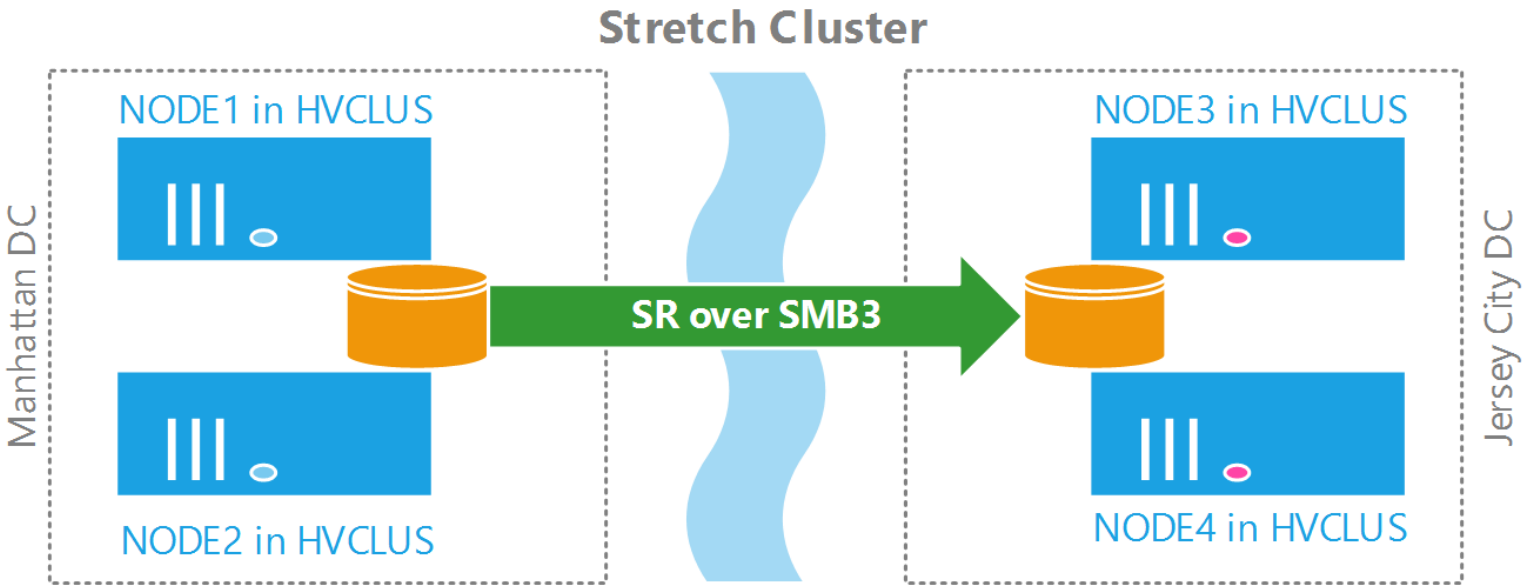


Figure 1



Source: Windows Server Technical Preview Storage Replica Guide.docx

Storage Spaces Direct Hyper-converged

Sicherheit in virtuellen Umgebungen?

- Virtuelle Maschinen muessen nicht gehaertet werden, dass Hostsystem ist ja sicher?
- Wer patcht schon seine virtuellen Maschinen?
- Ich kuemmere mich nur um meine VM, das Host-System laeuft einfach so mit
- Wenn mein Host-System kompromittiert wird, betrifft das nicht meine virtuellen Maschinen!

Hyper-V Security

- Windows Server 2016 Core oder Nano!!
  - Reduziertes Attack Surface
  - Reduziertes Footprinting
  - Hoehere Systemverfuegbarkeit durch weniger Updates
- Aktuelle Patchstrategie
- Haerten des Hyper-V Hostsystems
  - Keine Installation zusaetzlicher Anwendungen
  - Windows Firewall
  - Security Configuration Wizard (SCW)
  - Security Compliance Manager (SCM)
- Dedizierte Netzwerkkarte fuer Management und Storage
- Anwendung des Windows Server 2012 Security Guide
- → Was finden Sie noch wichtig?

Best Practice VM in Hyper-V

- Speicherort fuer VHDX, VMCX etc.
- Speicherzuordnung zur VM
- Limit Prozessornutzung
- VM Zugriff nur auf notwendigen Storage
- Zeitsynchronisation in VM (DC?)
- Speichern von VM mit gleichem Schutzbedarf auf der selben Host-Maschine
- Hyper-V Netzwerke
- Sicheres Loeschen von nicht mehr verwendeten VM
- Speichern von Snapshots (AVHD) an einem „sicheren“ Ort
- Firewallkonfiguration
- Third Party Produkte

Gast Sicherheit

- RAM und CPU Monitoring
- VM Limits im Host System setzen
- Virenscanner
- Security Hardening (Hyper-V Sec. Guide)
- Patching
- DoS Angriffe auf VM mit Auswirkung auf Hyper-V Host und andere Gaeste beschraenken
- Host Resource Protection
- Shielded VM

Hyper-V Security

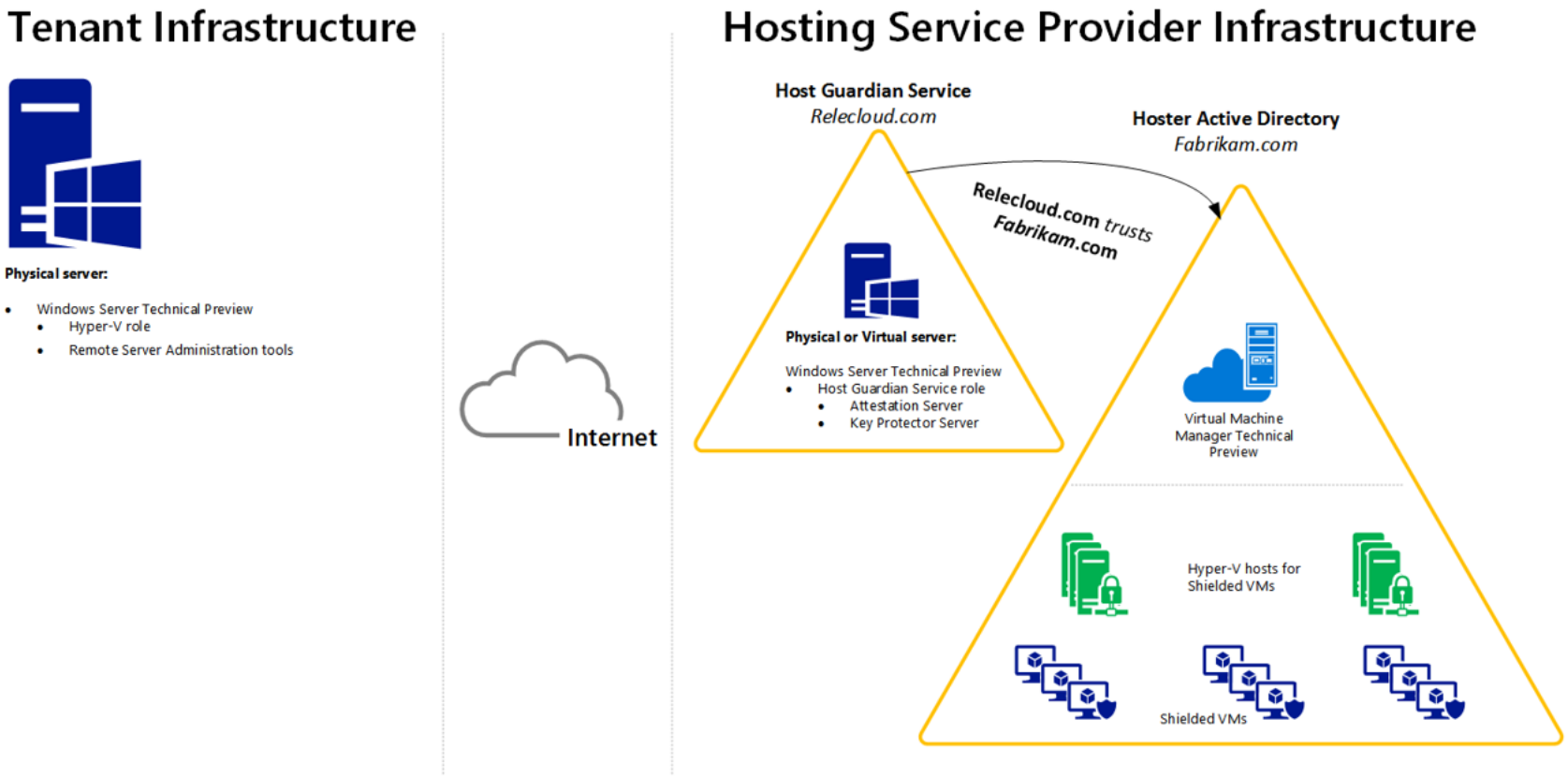
- Datacenter Firewall
- Windows Server Antimalware
- Shielded Virtual Machines mit Host Guardian Service
- Virtual TPM

Shielded Virtual Machines

- VSM – Virtual Secure Mode
- Shielded VM – Neue Schaltflaeche in Gen 2 VM
- Hyper-V Host sollte TPM 2.0 und UEFI 2.3.1 verwenden (sonst dedizierter AD Forest notwendig)
- Nutzung von Virtual TPM in VM
- Bitlocker Verschluesselung in VM
- Verschluesselter Live Migration Traffic
- Ausfuehrung der VM nur auf Trusted Hosts
- Kein Zugriff durch nicht erlaubte Hyper-V / VMM Administratoren moeglich
- HGS (Host Guardian Service) muss dedizierten Active Directory Forest verwenden, wenn auf den Hyper-V Hosts kein TPM 2.0 und UEFI 2.3.1 verfuegbar ist
- HGS fuehrt Host-Validierung und Schluesselverteilung durch

Shielded Virtual Machines

Guarded Fabric Infrastructure



Using Active Directory-based attestation

Source: Shielded VM and Guarded Fabric Deployment Guide for TP3.docx

System Center Virtual Machine Manager 2016

- Loesung zur Verwaltung eines virtualisierten Rechenzentrums
- Multi Hypervisor-Verwaltung
- Fabric und Storage Management
- Verwaltung von virtuellen Maschinen
- Netzwerkmanagement
- Update und Compliance Management
- Library Management
- Integration in SCOM
- Resource Optimization (DO - PO)
- Baremetal Provisioning

Neuerungen in VMM 2016

- Guarded Hosts and Shielded VMs
- Network Controller Support
- Verbessertes Logic Switch Management
  - Konvertieren von Standard Switch zu Logical Switch
  - Logical Switch Deployment auf einzelne Hosts inkl. Revert
- Mixed Cluster Management
- Hot add/remove RAM und NIC

Neuerungen in VMM 2016

- Verbessertes Storage Provisoning
  - Storage QoS auf Cluster
  - Storage Tiers
  - Storage Spaces Direct
  - SOFS Cluster from BareMetal
- Production Checkpoints in VM
- Azure Subscription in VMM
  - Basic Azure VM Management

VMM-Grundkonfiguration

- Ausfuehrungskonton
- VMM Verwaltungs-Gruppen
- Allgemeine Einstellungen
- Hostgruppen
- VMM Agents
- Bibliothekserver
- Fabric Management
  - Logische Switche
  - Update Server / Bibliothekserver
  - Speicher
- Vorlagen (Hardware, Gast-OS ..)

VMM Administration

- Host Administration
  - Maintenance
  - PO / DO
- VM Administration
  - Connect, Einstellungen, Shutdown
  - Live Migration, Quick Migration, Storage Migration
  - Store in Library
- Auftragsververwaltung
- Cloud Einrichtung
- Azure Subscription

Demo

Update von VMM 2012/R2 auf 2016

- Alle Verbindungen schließen (Konsolen, PowerShell)
- Datensicherung VMM-Server und VMM-Datenbank
- Update ADK auf aktuelle Version (altes ADK vorher deinstallieren)
- Inplace Update moeglich
- Wenn DKM verwendet wird, kann VMM auf einem anderen Server installiert werden
- Verwendung des gleichen VMM-Dienstkonto
- Best Practice: SQL-DB auf anderem Server
- VMM wird beim Update deinstalliert, Option DB beibehalten waehlen

Fragen??

Kontakt

Marc Grote

- E-Mail: marc.grote@it-consulting-grote.de
- Web: http://www.it-consulting-grote.de
- Blog: http://blog.it-consulting-grote.de
- XING: https://www.xing.com/profile/Marc_Grote2
- Mobile: +4917623380279