

Windows Server 2016 – Was ist neu im Komplettueberblick



Agenda

- Hyper-V
- Failover Clustering
- Storage Services
- Remote Desktop Services (RDS)
- Active Directory
- Web Application Proxy
- Netzwerk
- Security

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

- Nano Server
- Windows Server Container (später Hyper-V Container)
- ReFS Accelerated VHDX Operations (Fixed Size Disk + Merge)
- Nested Virtualization (in WS2016 coming – Windows 10?)
- Neues Shared VHDX Funktionen (Dynamic Resize, Replica, Host Backup)
- Virtual TPM – Bitlocker Support
- Linux Secure Boot
- Shielded VMs → Host Guardian Service → Virtual TPM
- Virtual Machine Configuration Changes
- Production VM Checkpoints (Snapshots)
- Hyper-V Replica Unterstützung fuer VHDX Dateien im laufenden Betrieb
- Hot add / remove von Virtual Machine Memory / NIC

Demo

Virtual TPM – Production Checkpoints – Hot Add / Remove RAM / NIC

Hyper-V

- Virtual Network Adapter Identification (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 Konfiguration Files
- Secure Boot Support fuer Linux
- Distributed Storage QoS
- Virtual Machine Storage Resiliency (WS2012-R2 60 Sek. – WS2016 VM Paused)
- Verbessertes Hyper-V Backup
- RemoteFX OpenGL 4.4, OpenCL 1.1)
- Verbessertes Hyper-V Cluster Management (WMI gegen Cluster)
- PowerShell Direct

Demo

CDN - Update-VMVersion – PS Direct - VMCX

Demo

CDN - Update-VMVersion – PS Direct - VMCX

Windows Container

```
Administrator: Windows PowerShell
VHD mount must be synchronized with other running instances of this script.  waiting for exclusive access...
Mounting Windows Server Core VHD for offline processing...
Enabling Containers feature on drive G...
Copying Docker into Windows Server Core VHD...
Copying NSSM into Windows Server Core VHD...
This script uses a third party tool: NSSM service manager. For more information, see https://nssm.cc/usage
Downloading NSSM...
Extracting NSSM from archive...
Writing default unattend.xml...
Copying Install-ContainerHost.ps1 into Windows Server Core VHD...
Dismounting VHD...
Creating VM ws2016-container...
Configuring VM ws2016-container...
Starting VM ws2016-container...
Waiting for VM ws2016-container to boot...
Connected to VM ws2016-container Heartbeat IC.
Waiting for specialization to complete (this may take a few minutes)...
Executing Install-ContainerHost.ps1 inside the VM...
Completing container install...
Querying status of Windows feature: Containers...
Feature Containers is already enabled.
Enabling container networking...
Creating container switch (NAT)...
Creating NAT for 172.16.0.0/12...
The following images are present on this machine:
  ContainerImage (Name = 'WindowsServerCore') [Publisher = 'CN=Microsoft', Version = '10.0.10514.0'].Name

Docker is already installed.
NSSM is already installed
Creating Docker program data...
Configuring NSSM for Docker service...
Waiting for Docker daemon...
Successfully connected to Docker Daemon.
Tagging new base image...
Script complete!
VM ws2016-container is ready for use as a container host.
See http://msdn.microsoft.com/virtualization/windowscontainers for more information about using Containers.
The source code for these installation scripts is available here: https://github.com/Microsoft/Virtualization-Documenta
tion/tree/master/windows-server-container-tools
PS C:\WINDOWS\system32>
```

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)
- Rolling Cluster Upgrade
- Host Resource Protection (Resource Allocation Tracking in VM)
- Cloud Witness
 - Azure VM
- Host Guardian Service (VM Isolation fuer Tenants)
- Site Aware Cluster
 - Failover Affinity, Storage Affinity, Cross-Site Heartbeating
- Verbessertes Cluster Log
 - TimeZone, VerboseDiagnostic EventViewer, Active Memory Dump

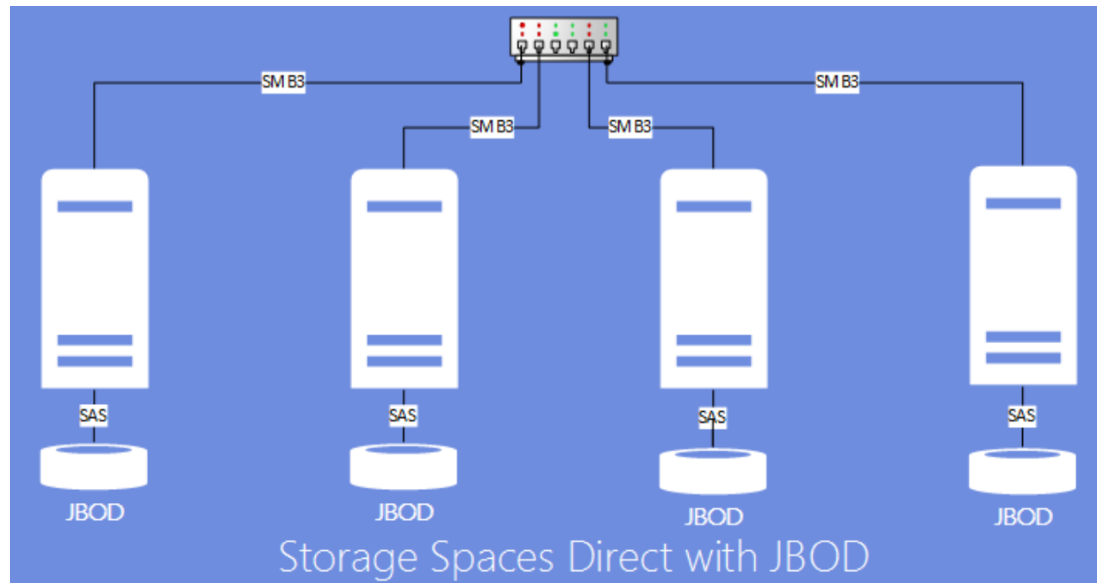
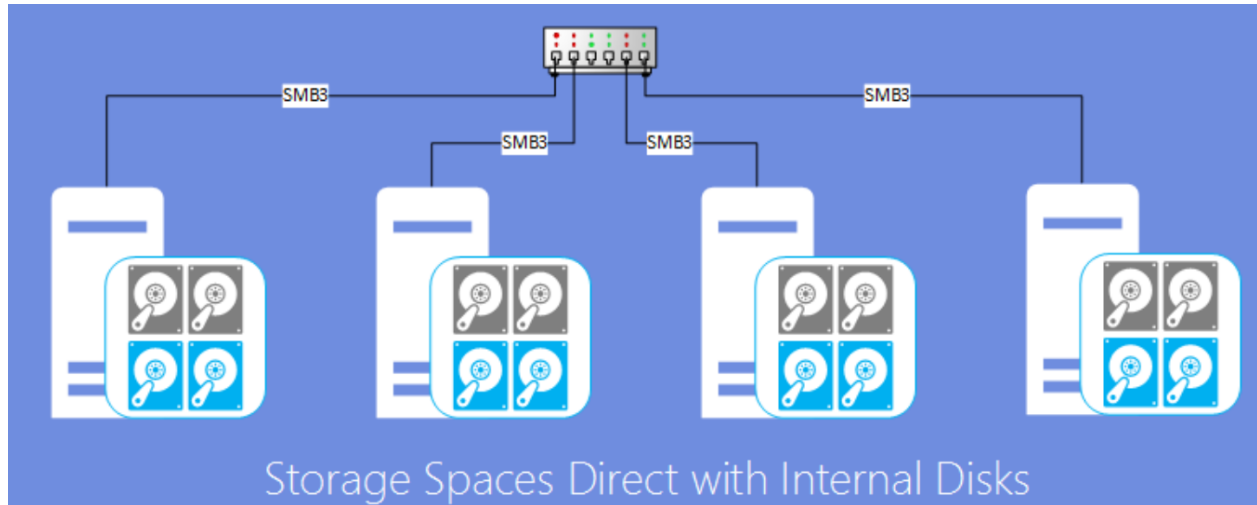
Demo

Rolling Cluster Update – Cloud Witness

Storage Services

- Virtual Machine Storage Resiliency
- Storages Spaces Direct
- Storage QoS fuer SOFS Cluster
- Bessere stretched Hyper-V Cluster mit Storage Replica

Storage Spaces Direct



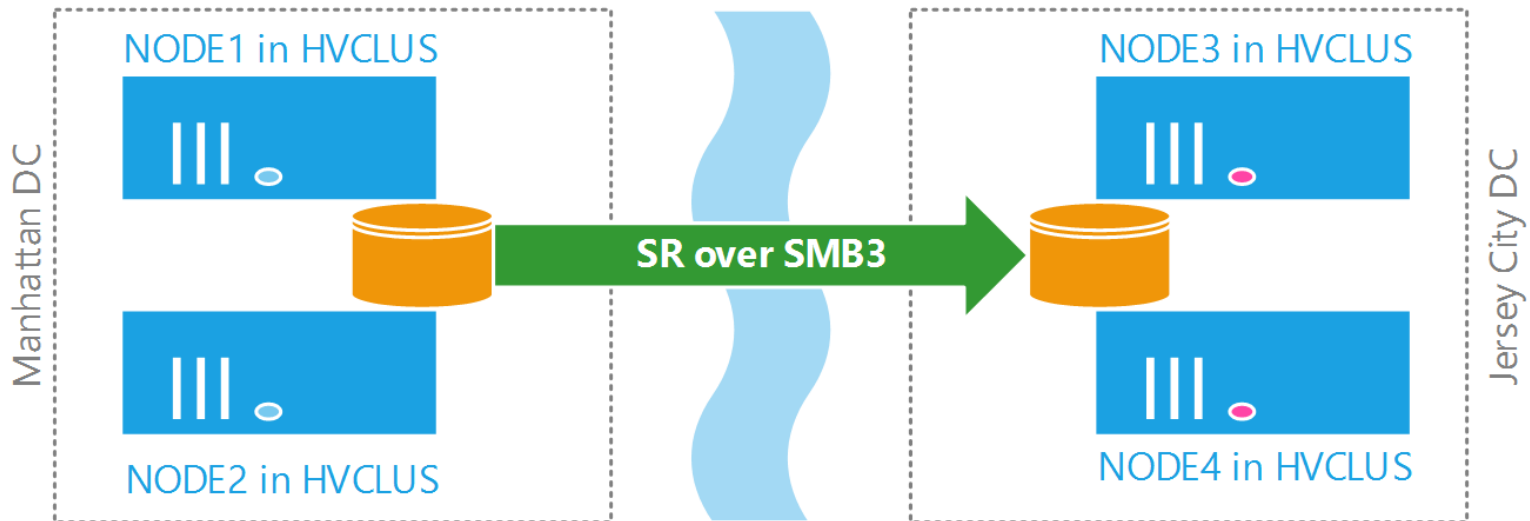
Storage Replica

Server to Server



Figure 1

Stretch Cluster



Remote Desktop Services (RDS)

- Multipoint Server Rolle im OS integriert
- Unterstützung fuer OpenGL 4.4 und OpenCL 1.1 API fuer RemoteFX vGPU
- Generation 2 VM fuer Personal Virtual Desktop
- Personal Session Desktop in Microsoft Azure
- Konfigurierbarer, groesserer, dedizierter Video Speicher.
Konfigurierbarer, groesserer, dedizierter VRAM
- Pen Remoting
- Microsoft Edge in Remote Desktop Session Host
- Geschwindigkeitsverbesserungen,
Stabilitaetsverbesserungen und verbesserte
Anwendungskompatibilitaet

Active Directory

- Azure Active Directory Join
 - SSO, MDM, Kiosk Mode, Shared Devices,
- Microsoft Passport
- FRS entfernt
- Kein Windows Server 2003 Functional Level
- Access Control Policies in AD-FS
- AD-FS Authentifizierung gegen AD-LDS und weitere
- Privileged Access Management (PAM)
 - Bastion Active Directory Forest, provisioniert von MIM
 - Shadow Security Principal Groups
 - Expiring Link feature (time bound Membership in Shadow Group)
 - KDC Erweiterungen um Kerberos Ticket Lifetime zu reduzieren

Privileged Access Management (PAM)

- Mitgliedschaft in administrativen Gruppen auf Zeit
- Multi Faktor Authentifizierung integrierbar
- AD Forest mit Windows Server 2016 erforderlich
- AD Trust zum Produktions Forest erforderlich
- PAM kann separat aktiviert werden → Einstellung irreversibel
- SAM verwaltet Ablaufzeit von Gruppenzugehörigkeiten → Token
- Kerberos TGT erhaelt Ablaufzeit der kuerzesten Gruppenmitgliedschaft
- Provisionierung mit MIM (Microsoft Identity Manager → ehemals FIM (Forefront Identity Manager))
- Administrative Gruppen werden im PAM AD Forest gespiegelt mit MIM → Shadow Security Principals)

Web Application Proxy

- Preauthentication fuer HTTP Basic Anwendungs-Veroeffentlichung
- Wildcard Domain Veroeffentlichung von Anwendungen
- HTTP zu HTTPS Umleitung
- HTTP Veroeffentlichung
- Veroeffentlichung von Remote Desktop Gateway Anwendungen
- Neues Debug Log fuer ein vereinfachtes Troubleshooting
- Administrator Console UI Erweiterungen
- Weiterleitung der Client IP-Adresse zu veroeffentlichen Anwendungen

Demo

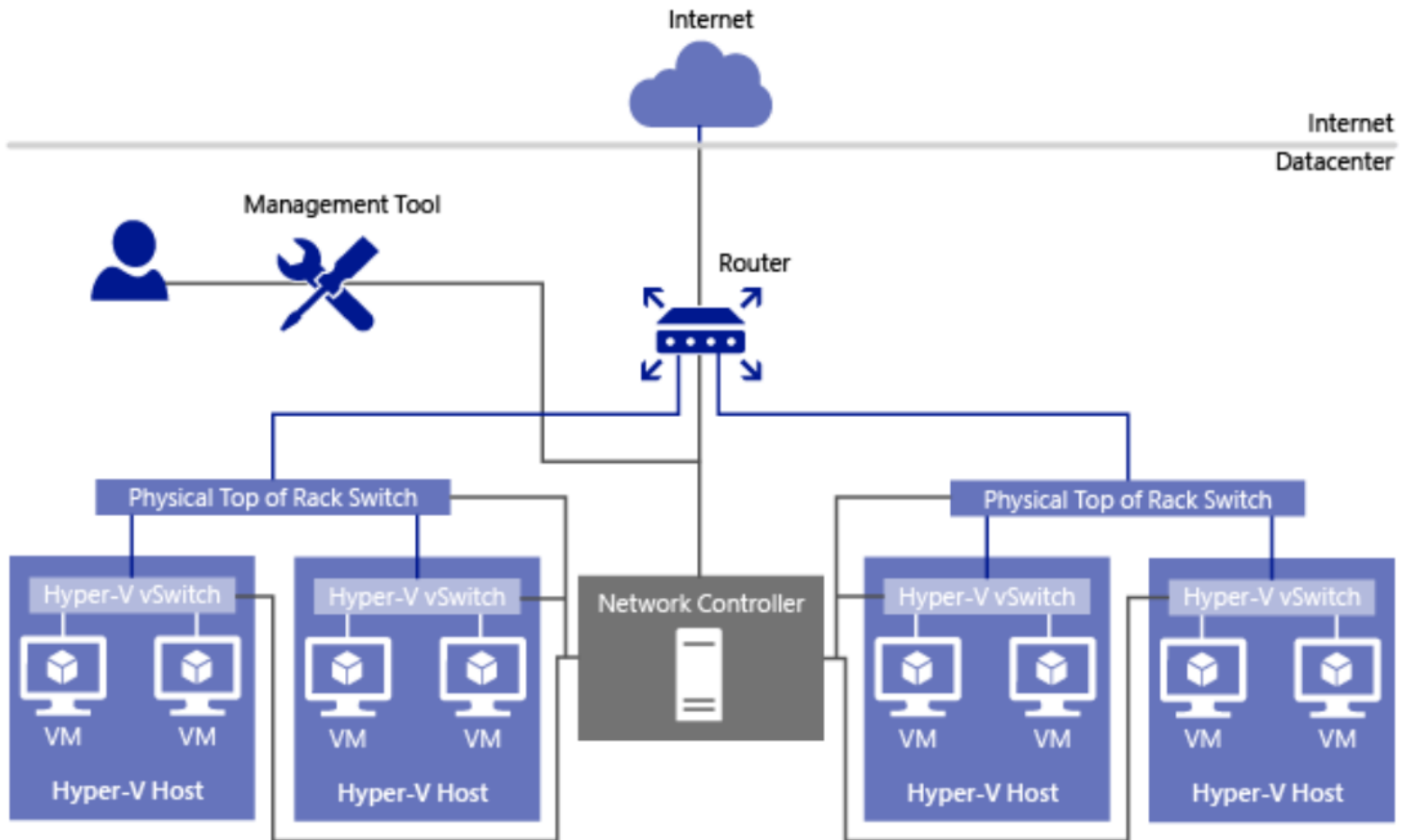
WS2012-DC – WS2016-01 – WS2016-WAP

Netzwerk

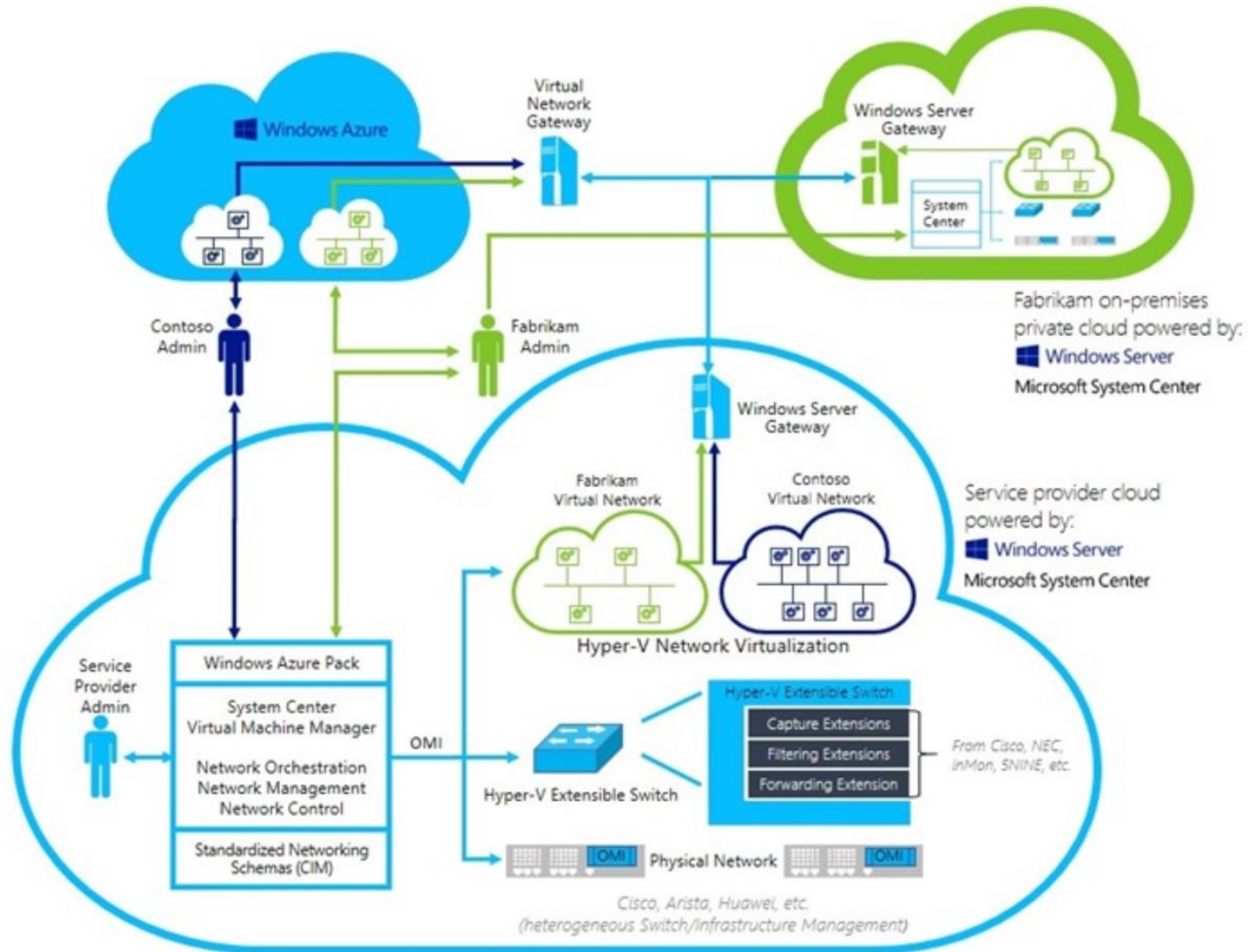
- DNS Client Service Binding
- DNS Server unterstützt DNS Policies
- Neue DNS Server PowerShell cmdlets
- Keine NAP Unterstützung in Windows Server DHCP
- GRE fuer Windows Server Gateway
- Layer 4 Load Balancer
- Network Controller (Konfiguration, Verwaltung und Automatisierung von Datacenter Netzwerkkomponenten – virtualisierter Umgebungen)
- Software Defined Networking (SDN)
- SET (Switch Enabled Teaming)
- Verbessertes IP-Address Management in IPAM (Anzeige, IPv4 / IPv6 Ermittlung, DNS Zonenverwaltung inkl. Standalone DNS)
- Verbessertes DNS Server Management (DNS Policies, Response Rate Limiting, Unknown Record Support, IPv6 Root Hints → Konfig. per PS)
- Converged NIC (RDMA mit 2 NIC)
- PacketDirect auf 40G NIC
- Server Unterstützung fuer HTTP/2

Demo

Network Controller



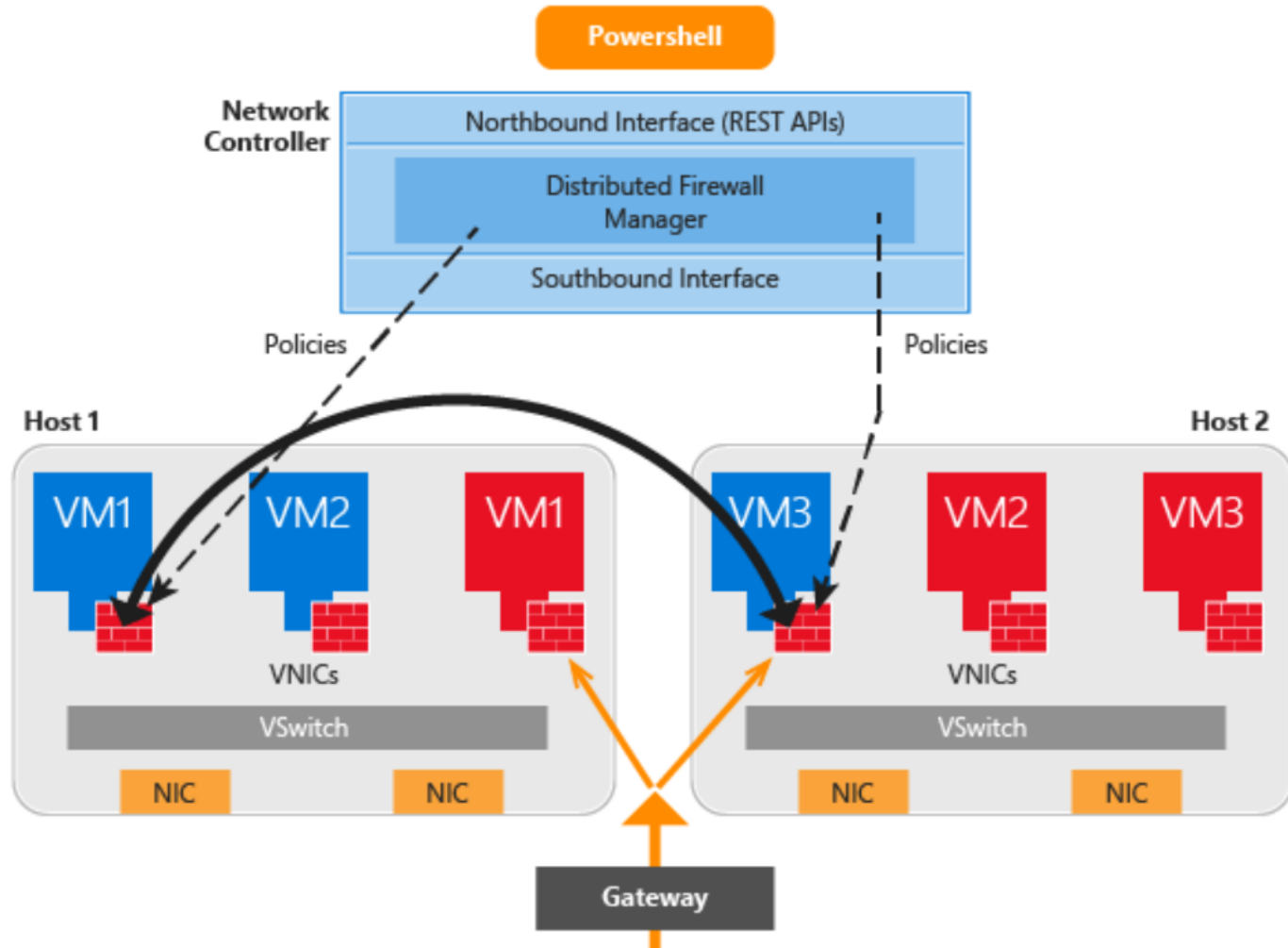
Software Defined Networking



Security

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

Datacenter Firewall



Shielded Virtual Machines

Guarded Fabric Infrastructure

Tenant Infrastructure



Physical server:

- Windows Server Technical Preview
 - Hyper-V role
 - Remote Server Administration tools



Hosting Service Provider Infrastructure

Host Guardian Service
Relecloud.com

Hoster Active Directory
Fabrikam.com

*Relecloud.com trusts
Fabrikam.com*



Physical or Virtual server:

- Windows Server Technical Preview
- Host Guardian Service role
 - Attestation Server
 - Key Protector Server



Virtual Machine
Manager Technical
Preview



Hyper-V hosts for
Shielded VMs



Shielded VMs

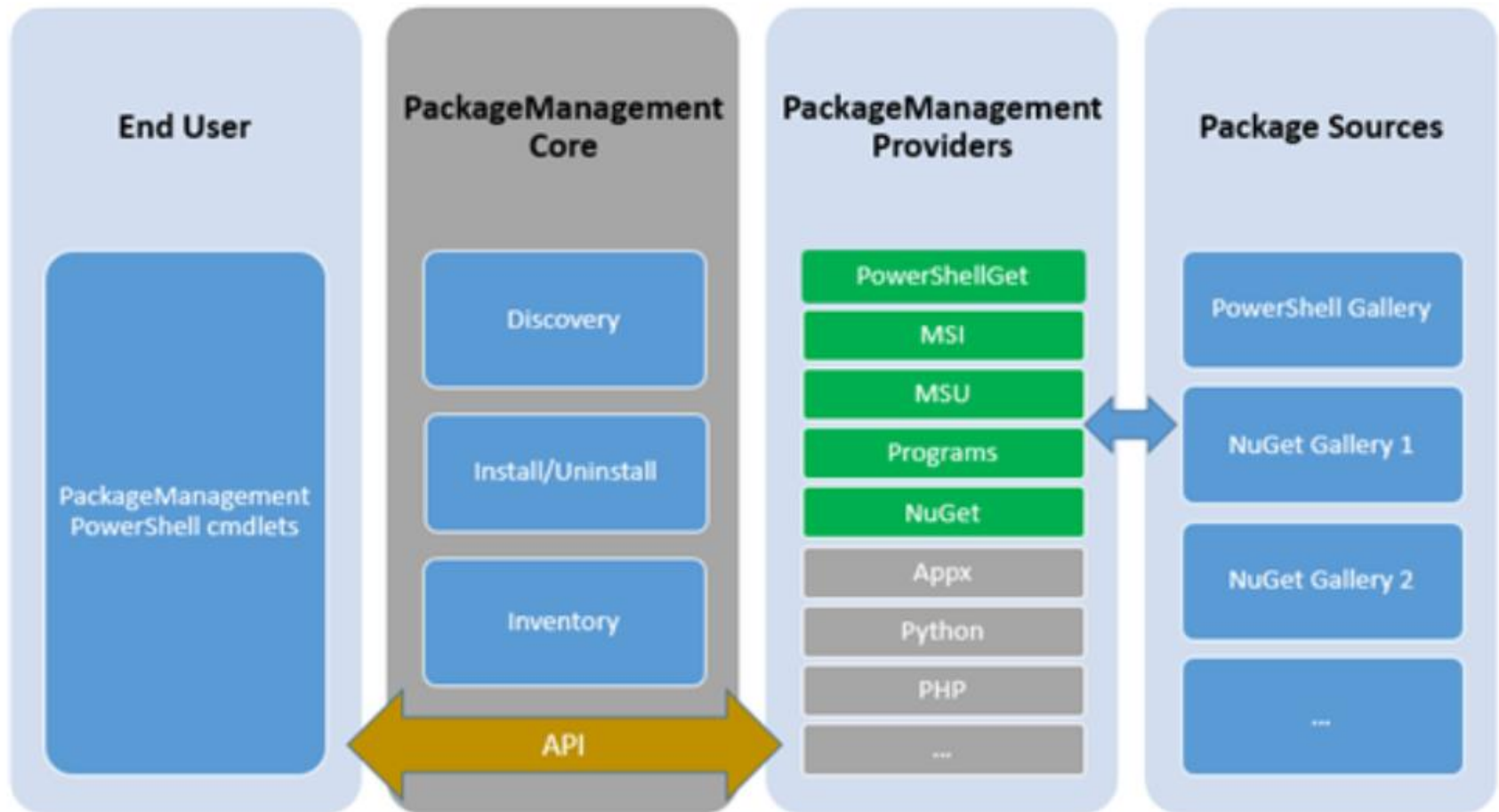


Using Active Directory-based attestation

PowerShell 5.0

- OneGet Framework (Paketmanager)
- Desired State Configuration (DSC) Version 2
- Data Center Abstraction (DAL)
- Verwaltung von Netzwerk-Switchen

Package Management



Fragen?

The image features the word "Fragen?" in a bold, sans-serif font. The word "Fragen" is rendered in a bright orange color, while the question mark is a medium blue. To the right of the text, there is a large, stylized blue question mark icon. This icon is composed of several overlapping, semi-transparent shapes in different shades of blue, creating a layered, 3D effect. The entire graphic is set against a plain white background.

Kontakt

Marc Grote

- E-Mail: grotem@it-training-grote.de
- Web: <http://www.it-training-grote.de>
- Blog: <http://blog.it-training-grote.de>
- XING: [https://www.xing.com/profile/Marc Grote2](https://www.xing.com/profile/Marc_Grote2)
- Mobile: 0176/23380279