

Whitepaper

Software Defined Networking (SDN) mit Windows Server 2016 und System Center Virtual Machine Manager 2016 (SCVMM 2016)

© Gerhard Glenk IT Consulting Josef-Simon-Str. 35 90473 Nürnberg E-Mail: <u>gerhard.glenk@online.de</u>

Version 1.0 – August 2018

Veröffentlicht bei: **Rachfahl** IT-Solutions Rachfahl IT-Solutions GmbH & CO. KG Heiligenhaus 21 59969 Hallenberg Website: https://www.hyper-v-server.de



Inhalt

1	Vor	Vorwort und Motivation		
	1.1	Warum SDN?	. 4	
	1.2	Skript Download	. 4	
2	Die	neue Microsoft SDN-Architektur	. 5	
3	Net	zwerk Controller Funktionalitäten	. 7	
	3.1	Netzwerk Virtualisierung	. 7	
	3.1.	1 Das VXLAN-Protokoll	. 7	
	3.2	Load Balancing	. 8	
	3.3	Remote Access Service (RAS) Multitenant Gateways	. 9	
4	SDN	I-Topologie	10	
	4.1	Logische Netze	10	
	4.2	Hyper-V Hardware	10	
	4.3	Netzwerk Hardware	10	
	4.4	Putting It All Together	11	
	4.5	Weitere Infrastruktursysteme	11	
5	SDN	Deployment	12	
6	Die	SDN Lab Umgebung	13	
	6.1	Hardware	13	
	6.2	Software	13	
	6.3	Die Lab Infrastruktur	13	
	6.3.	1 Virtuelle Maschinen	13	
	6.3.	2 Logische SDN Netze	14	
	6.3.	3 Ein grober Überblick	14	
	6.4	Vorbereitungen	15	
	6.4.	1 SDN-DC01	15	
	6.4.	2 SDN-BGP01	17	
	6.4.	3 SDN-HV01 – SDN-HV04	17	
	6.4.	4 SDN-VMM01	18	
7	Bere	eitstellen der Skripte für das SDN Deployment – VMM Express.ps1	31	
	7.1	Schrittweises Deployment der SDN-Komponenten	38	
8	Star	ten des SDN-Deployments	39	
9	Erfa	hrungen, Tipps und Tricks	39	
	9.1	Hyper-V Switch Deployment	39	
	9.2	REST IP	40	
	9.3	Undo Funktion	40	



9.4	٧N	1MExpress im Debugger ausführen
10	Post I	NC Deployment Schritte und Validierung
10.1	Те	nant Testumgebungen
10	.1.1	Tenant VM Netze
10	.1.2	Tenant Test VMs
10.2	Va	lidierung der Netzwerkisolation mit dem VXLAN-Protokoll
10.3	Ко	nfiguration der Load Balancer Service Instanzen54
10.4	Ко	nfiguration des BGP Routers
10.5	Va	lidierung des Software Load Balancing 58
10	.5.1	Erstellen eines VIP Templates
10	.5.2	Erstellen einer öffentlichen virtuellen IP Adresse (PublicVIP) für ein Tenant VM Netz 61
10	.5.3	Load Balancing Test
10	.5.4	NAT konfigurieren
11	Näch	ste Schritte
Anhang	: Skri	pt Download Details



1 Vorwort und Motivation

Der Microsoft Windows Server 2016 bietet eine Plattform zum Aufbau eines Software-Defined Data Centers (SDDC) basierend auf technischen Innovationen aus Microsoft Azure. Ein kritischer Bestandteil eines SDDC ist dabei das Thema Software Defined Networking (SDN). Microsoft Windows Server 2016 enthält eine Vielzahl an Neuerungen innerhalb des SDN-Stacks wie z.B. Netzwerk Virtualisierung mit dem VXLAN-Protokoll sowie Gateways, Load Balancer und Remote Access Dienste für virtualisierte Netze, welche sich durch den Einsatz von System Center 2016 Virtual Machine Manager effizient bereitstellen und verwalten lassen.

Auf der CDC 2018 in Hanau habe ich zusammen mit Petra Lipp einen Vortrag zum Thema "Software Defined Networking (SDN) mit Windows Server 2016 und System Center Virtual Machine Manager 2016 (SCVMM 2016)" gehalten. Mittlerweile haben wir einige Anfragen bekommen über Details zu den gezeigten Präsentationen und Demoszenarien.

Da keine Mitschnitte von der Veranstaltung existieren, habe ich beschlossen, die wichtigsten technischen Informationen sowie eine Beschreibung zum Aufbau der gezeigten Demoumgebung in einem Whitepaper zusammenzufassen.

1.1 Warum SDN?

In großen Rechenzentren war die Netzwerkverwaltung schon immer eine sehr personal- und zeitaufwendige und damit kostenintensive Aufgabe. Durch die immer stärker zunehmende Server-Virtualisierung entstehen weitere neue Herausforderungen: Netzwerkdienste müssen dynamisch und schnell bereitgestellt werden, die Verwaltung sollte über ein zentrales Werkzeug geschehen und über normierte Schnittstellen (APIs) programmierbar sein, so dass auch eine Automatisierung z.B. durch Skripte möglich wird. Außerdem sind Methoden notwendig, um den Netzwerkverkehr für verschiedene – möglicherweise sogar konkurrierende – Anwendergruppen sicher voneinander zu trennen und damit die jeweiligen Netzwerksegmente zu isolieren. Die Restriktionen der hierfür bislang verwendeten VLAN-Technik sollten beseitigt werden.

SDN Technologien versprechen, all diese Herausforderungen zu lösen.

1.2 Skript Download

In diesem Whitepaper beschreibe ich einige PowerShell Skripte, die ich mir zusätzlich zu den von Microsoft bereitgestellten erstellt habe, um Aktionen, die mit vielen Mausklicks verbunden sind, etwas zu vereinfachen. Diese zusätzlichen Skripte habe ich in einer .ZIP-Datei zusammengestellt, die Sie <u>hier</u> downloaden können. Details zu den Skripten finden Sie am Ende dieses Dokuments.



2 Die neue Microsoft SDN-Architektur

Eigentlich gibt es SDN im Windows Server bereits seit der Version 2012R2. Dort hatte Microsoft die Technologie an verschiedenen Stellen im Betriebssystem und im SCVMM "versteckt". Zur Isolation von Netzen wurde der GRE-Standard (Generic Routing Encapsulation) verwendet. GRE hat sich für diesen Zweck jedoch nicht so recht am Markt durchgesetzt. Die Mehrzahl von Netzwerk-Anbietern setzt mittlerweile auf den VXLAN-Standard (Virtual Extensible LAN), was zur Folge hatte, dass Microsoft dieses Protokoll sowohl in der Microsoft Azure Cloud implementierte und die entsprechenden Komponenten nun auch im Windows Server 2016 bereitstellt.

Anmerkung: VXLAN ist nun das Standard-Protokoll für SDN. Jedoch wird auch weiterhin das GRE-Protokoll unterstützt, so dass bisherige Installationen weiter genutzt werden können. Eine Migration von GRE auf VXLAN ist jedoch nicht vorgesehen und bedeutet eine Neuinstallation.

Werfen wir zunächst einen Blick auf das folgende Architekturbild, das aus der <u>Microsoft TechNet</u> <u>Library</u> stammt.



Im Zentrum der neuen SDN-Architektur steht eine neue Serverrolle, die nur in der Datacenter Edition von Windows Server 2016 verfügbar ist, der *Network Controller*. Wir benötigen dafür entweder physische oder auch virtuelle W2016 Datacenter Systeme, auf denen diese Serverrolle installiert und konfiguriert ist. Und warum die Mehrzahl? Technisch würde eine Instanz des *Network Controllers* genügen. Um aber die Hochverfügbarkeit zu gewährleisten, empfiehlt Microsoft für produktive Umgebungen aber wenigstens 3 Instanzen.

Der Network Controller besitzt zwei Schnittstellen (APIs), die Northbound API und die Southbound API. Über die Southbound API kommuniziert der Network Controller mit den physischen und virtuellen Netzwerkgeräten, also z.B. mit den physischen Switches im Server Rack (Top of Rack – TOR) oder mit den virtuellen Switches in den Hyper-V Hostsystemen. Über die Northbound API erhält der Network Controller von verschiedenen Netzwerk Management Tools Anweisungen bzw. Richtlinien,



wie die über die *Southbound API* verbundenen Netzwerkgeräte den Netzwerkverkehr behandeln sollen.

Für die Kommunikation zwischen dem *Network Controller* und den verschiedenen Netzwerkkomponenten muss in einer Microsoft SDN Plattform das in jedem Rechenzentrum ohnehin vorhandene (logische) Management Netz verwendet werden, das ich in diesem Artikel mit MGMT bezeichnen will.

Anmerkung: Die Einbettung des *Network Controllers* in das MGMT Netz hat nicht zur Folge, dass der Netzwerkverkehr virtueller (Kunden-) Maschinen ebenfalls über dieses Netz läuft. Hierfür werden wir noch weitere logische Netze einführen.

Die Northbound API ist als Representational State Transfer (REST) API ausgelegt, so dass beliebige Management Tools, die dieses Protokoll beherrschen, verwendet werden können, um dem Network Controller Richtlinien zu übermitteln. Darüber hinaus bietet diese API auch die Möglichkeit, das Netzwerk zu überwachen und bei Problemen Informationen fürs Troubbleshooting abzurufen.

Als Management Tools für den *Network Controller* bietet Microsoft aktuell folgende Werkzeuge:

- PowerShell Cmdlets
- den Azure Resource Manager (ARM)
- den System Center 2016 Virtual Machine Manager (SCVMM 2016)

Insbesondere der SCVMM 2016 bietet mit seiner grafischen Benutzeroberfläche eine einfache Möglichkeit zum Konfigurieren des *Network Controllers* und stellt auch alle Funktionen über eigene PowerShell Cmdlets zur Verfügung. Wir werden uns dies später noch genauer ansehen.

Die über die Northbound API erhaltenen Richtlinien verteilt der Network Controller dann über seine Southbound API an die betroffenen Netzwerkgeräte. Bei Hyper-V Hosts ist dies eine neue Hyper-V Switch Erweiterung (Extension) mit dem Namen *Microsoft Azure VFP Switch Extension*. VFP steht für "Virtual Filtering Platform".

Management Ebene Benutzerschnittstelle ARM Beschreibung der Netzwerkrichtlinien SCVMM PowerShel Representational REST **Controller Ebene** State Transfer Standardisierte REST API Übersetzt die Richtlinien für Hyper-V etwork Controlle Eigene virtuelle Maschinen Windows Management WMI **Daten Ebene** Instrumentation Hyper-V Switches VMs VMs VMs VMs mit VFP Extension v-Switch v-Switch v-Switch v-Switch HOST HOST HOST HOST

Die Microsoft SDN-Architektur besteht also aus 3 Ebenen, wie die folgende Abbildung zeigt.



3 Netzwerk Controller Funktionalitäten

Mit dem Netzwerk Controller können nun folgende Funktionalitäten realisiert werden:

3.1 Netzwerk Virtualisierung

Es können für Gruppen von Kunden VMs (häufig auch als "Tenant" VMs bezeichnet) eigene logische virtuelle Netze definiert werden. Diese Netze sind voneinander völlig getrennt, auch wenn sie identische Netzwerkparameter wie IP-Bereiche oder VLANIDs besitzen. Die Isolation des Datenverkehrs innerhalb eines solchen virtuellen Netzes erfolgt durch "Verpacken" der Datenpakete nach dem VXLAN-Protokoll.

3.1.1 Das VXLAN-Protokoll

VMs in einem virtuellen Netz verwenden typischerweise kundenspezifische IP-Adressen ("Customer Addresses" – CAs), die nicht vom Rechenzentrumsbetreiber verwaltet und mit denen die Netzwerkgeräte im Rechenzentrum somit nichts anfangen können. Will nun eine Kunden-VM mit einer anderen kommunizieren, gibt sie ein Ethernet Netzwerkpaket über ihren Netzwerkadapter an einen Switch weiter, in einer Hyper-V Umgebung also an den Hyper-V Switch des Hosts, auf dem sie gerade läuft. Im Hyper-V Switch wird geprüft, ob die Ziel-VM im gleichen Host läuft. Falls ja, wird das Netzwerkpaket vom Switch direkt an die entsprechende VM weitergeleitet.

Falls die Ziel-VM jedoch auf einem anderen Host läuft, wird das Datenpaket in ein neues Netzwerkpaket mit vom RZ-Betreiber verwalteten IP-Adressen ("Provider Addresses" – PAs) gemäß dem VXLAN-Protokoll verpackt und an den Zielhost per UDP weitergeleitet. Dieser kann dann das ursprüngliche Datenpaket wieder auspacken und an die entsprechende VM weiterleiten.

Um die Zuordnung eines verpackten Kunden-Datenpakets zu gewährleisten, wird jedem virtuellen Kundennetz beim Anlegen über den Netzwerk Controller eine eindeutige VXLANID zugewiesen. Diese VXLANID hat eine Länge von 24 Bit. Somit können bis zu 16 Millionen Kundennetze identifiziert werden. Beim Verpacken eines Kunden-Datenpakets wird die VXLANID des Kundennetzes dem Kunden-Datenpaket als Header vorangestellt, so dass beim Auspacken der Daten im Zielhost diese in das entsprechende Kundennetz geleitet werden können.



Für die Kommunikation zwischen den Kunden-VMs benötigen wir also ein (und nur ein) zusätzliches vom Provider verwaltetes logisches Netz, über das die in VXLAN eingepackten Kunden-Datenpakete weitergeleitet werden. Für die weiteren im Netzwerk vorhandenen Geräte wie Switches oder Router sind die Datenpakete der Kunden-VMs also "unsichtbar" und benötigen somit auch keine weiteren Management Aktivitäten.

Zum Vergleich: Bei der bisherigen Methode zur Netzwerk Virtualisierung mit VLANIDs muss hingegen jedes Kundennetz mit einer eindeutigen VLANID vom Provider definiert, verwaltet und an alle Netzwerkgeräte verteilt werden. Da die VLANIDs nur aus 12 Bits bestehen, ist die Anzahl von Kunden-Netzen auf knapp 4096 begrenzt.

Das logische Netzwerk zum Weiterleiten der mit VXLAN verpackten Datenpakete wird in einer Microsoft SDN-Umgebung üblicherweise als HNVPA (<u>Hyper-V N</u>etzwerk <u>V</u>irtualisierung mit <u>P</u>rovider <u>A</u>dressen) Netz bezeichnet.



Die Netzwerk Virtualisierung mit VXLAN vereinfacht also drastisch das Netzwerkmanagement in einem Rechenzentrum, da sich der Provider nicht mehr explizit um die Isolation von Kundennetzen kümmern muss.

3.2 Load Balancing

Für VMs, die in einem virtuellen Kundennetzwerk den gleichen Workload bereitstellen (z.B. Webserver Cluster), kann per Software ein Lastenausgleich ("Software Load Balancing" – SLB) in Form eines SLB-Pools definiert werden. Das Load Balancing wird von eigenständigen über den Netzwerk Controller verwalteten VMs durchgeführt. Die SLB VMs ermöglichen dann auch den Zugriff von außen auf die SLB-Pools in einem virtuellen Kundennetzwerk.

Ein SLB-Pool enthält die virtuellen IP-Adressen der für das Load Balancing vorgesehenen Kunden-VMs (hier als dynamische IP-Adressen – DIPs – bezeichnet). Dem Pool wird dann eine öffentliche IP-Adresse (PublicIP) zugeordnet. PublicVIPs sind typischerweise über das Internet erreichbar, so dass sich Anwender von außen damit verbinden können.

Der Netzwerk Controller übergibt diese Definitionen an die SLB VMs über das MGMT-Netz. Diese wiederum geben die PublicVIPs über das BGP-Protokoll bei einem zentralen BGP-Router bekannt, der die Verbindung zur Außenwelt bereitstellt. Die Kommunikation zwischen den SLB-VMs und dem BGP-Router wird typischerweise über ein eigenes logisches Netz mit dem Namen *Transit* abgewickelt.

Erreicht nun eine Anfrage den BGP-Router zu einer ihm bekannt gemachten öffentliche VIP-Adresse, leitet er diese über das Transit Netzwerk einer SLB-VM zur weiteren Bearbeitung weiter. Da alle SLB-VMs die gleichen Pool-Definitionen enthalten, bestehen also mehrere Wege für diese Weiterleitung. Wir sprechen deshalb hier auch von einem SLB Multiplexer oder SLB-MUX. Bei der Weiterleitung wird die Zieladresse der Anfrage mit der SLB-MUX Adresse im Transit Netz überschrieben.

Der SLB-MUX kann nun in Zusammenspiel mit den SLB Agents in den Hyper-V Switches entscheiden, an welche VM bzw. DIP die Anfrage zur Bearbeitung gegeben wird. In der Anfrage wird dazu die Zieladresse mit der ermittelten DIP überschrieben, das Datenpaket mit VXLAN verpackt und dem entsprechenden Hyper-V Host über das HNVPA-Netz übermittelt. Der Hyper-V Host entpackt das Paket und leitet es an die VM weiter.

Die VM erstellt nun eine Antwort, die als Ziel die ursprüngliche Client Adresse enthält und als Sender die eigene DIP. Der Switch im Hyper-V Host ersetzt diese DIP wieder mit der dem SLB-Pool zugeordneten PublicVIP und sendet das Paket dann über ein Gateway im öffentlichen Netz direkt an den Client, von dem die Anfrage kam. Der Client bekommt also nichts mit von den verschiedenen Weiterleitungsschritten innerhalb der SLB-MUX Umgebung.





3.3 Remote Access Service (RAS) Multitenant Gateways

In der vorstehenden Beschreibung für die Load Balancing Funktion habe ich kurz beschrieben, wie eine Anfrage eines einzelnen Clients aus dem Internet in einer SDN-Umgebung bearbeitet wird. In vielen Fällen wird es jedoch notwendig sein, nicht nur von einem einzelnen Client System eine Verbindung zu den VMs eines Tenants herzustellen, sondern ganze externe Netzwerke mit den virtuellen Systemen eines Tenants zu verbinden.

Hierzu stellt der Netzwerk Controller die Funktion Remote Access Service (RAS) Multitenant Gateway bereit. Es handelt sich dabei (ähnlich den SLB-MUX Systemen) um eigene VMs, die über den Netzwerk Controller verwaltet werden. Damit können dann folgende Remote Szenarien realisiert werden:

- Site-to-Site VPN
- Point-to-Site VPN
- GRE Tunneling
- Dynamic Routing mit dem Border Gateway Protocol (BGP)

In diesem Whitepaper werde ich nicht näher auf diese Themen eingehen, da wir dazu entsprechende Remote Systeme benötigen, die aktuell in unserer Lab-Umgebung nicht verfügbar sind.



4 SDN-Topologie

Nachdem wir nun einige grundlegende Merkmale der Microsoft SDN Architektur geklärt haben, wollen wir uns kurz anschauen, wie dies alles in eine physikalische Umgebung abgebildet werden kann.

4.1 Logische Netze

Fassen wir zusammen, welche logischen Netze in einer SDN-Umgebung notwendig sind:

- NC_Management Dies ist das zentrale Netzwerk, über das alle Systeme in einem "Software Defined Datacenter" (SDDC) verwaltet und konfiguriert werden, also die Netzwerk Controller mit den SDN-Komponenten wie SLB-MUXe und Gateways, die Hyper-V Hosts, aber auch weitere Infrastruktursysteme wie Active Directory, DNS und der SCVMM. Der Netzwerk Controller erhält und verteilt über dieses Netz auch die Anweisungen für die SDN-Komponenten.
- HNVPA Über dieses Netz laufen die mit dem VXLAN-Protokoll verpackten Netzwerkpakete der Tenant VMs zwischen den Hyper-V Hosts.
- Transit Dieses Netz wird verwendet für die Kommunikation zwischen den SLB-MUX Systemen und der Außenwelt, z.B. mit einem BGP-Router, der mit dem Internet verbunden ist.

Diese 3 logischen Netze bilden das Rückgrat von SDN. Sie müssen in allen beteiligten Hyper-V Hosts verfügbar und dort mit den virtuellen Switches verbunden sein. Diese Netze besitzen jeweils einen eigenen IP Adresspool. Zusätzlich können sie optional durch VLANs untereinander isoliert sein, was jedoch kein Muss ist (in der später noch zu beschreibenden Demoumgebung werde ich darauf verzichten).

Für spezielle Szenarien sind gegebenenfalls weitere logische Netze notwendig, die dann aber nicht in den Hyper-V Hosts verfügbar sein müssen:

- PublicVIP Dieses Netz stellt das Tor zum und vom Internet dar. Bei den verwendeten IP-Adressen wird es sich also in der Praxis um öffentliche Adressen handeln und es gibt auch keine Isolation mit VLAN IDs.
- PrivateVIP Dieses Netz enthält private Adressen, über die interne Clients wie z.B. die SLB Manager und andere interne Dienste miteinander kommunizieren können.
- GREVIP Dieses Netz enthält virtuelle IP Adressen für Endpunkte von Site-to-Site (S2S) Verbindungen mit externen (Tenant) Netzen, bei denen das GRE-Protokoll verwendet wird.

Neben diesen SDN-spezifischen logischen Netzen wird es in einem Rechenzentrum weitere logische Netze z.B. für die Storage Anbindung geben, die wir hier aber nicht weiter betrachten wollen.

4.2 Hyper-V Hardware

Für den Aufbau einer SDN-Umgebung benötigen wir eine Reihe von Hyper-V Hosts mit der Windows Server 2016 Datacenter Edition. Es sollten wenigstens 3-4 Systeme verfügbar sein, die idealerweise in einem Hyper-V Failover Cluster zusammengefasst sind. In einer produktiven Umgebung wird man natürlich deutlich mehr Systeme einsetzen.

4.3 Netzwerk Hardware

Eigentlich stellt SDN keine speziellen Anforderungen an die Netzwerkhardware in den Hyper-V Hosts. Jedoch muss man berücksichtigen, dass der gesamte SDN-Netzwerkverkehr über die virtuellen Switches in den Hyper-V Hosts läuft und deshalb eine hohe Bandbreite und Verfügbarkeit erfordert. Deshalb sollte man über Teaming der in den Hyper-V Hosts verbauten Netzwerkadapter als Option nachdenken, was aber nicht zwingend ist.



Für Teaming kann sowohl das "klassische" Teaming auf Basis des Windows Betriebssystems als auch das "Switch Embedded Teaming" (SET) im Hyper-V Switch von Server 2016 zum Einsatz kommen. Letzteres ist natürlich vorzuziehen, wenn dies mit den vorhandenen Netzwerkadaptern möglich ist.

4.4 Putting It All Together

Wenn wir alle vorstehend beschriebenen Komponenten in einer SDN-Umgebung zusammenfassen, dann ergibt sich folgendes Bild für die SDN-Topologie:



Quelle: https://docs.microsoft.com/de-de/windows-server/networking/sdn/plan-plan-a-software-defined-network-infrastructure#network-controller-software-load-balancer-and-ras-gateway-deployment

Die unterste Ebene zeigt das physikalische Netz und die darin eingebetteten logischen SDN-Netze. Mit diesem Netz sind die Netzwerkadapter aller Hyper-V Hosts verbunden, gegebenenfalls auch als Team. Wenn Sie die logischen SDN-Netze als VLANs definiert haben, ist es wichtig, dass für die Ports an den physischen Switches, mit denen die Hyper-V Hosts verbunden sind, der Trunk Mode eingestellt ist. Nur dann sind in den virtuellen Hyper-V Switches alle SDN-Netze verfügbar.

Die virtuellen Hyper-V Switches präsentieren die SDN-Netze den im Host laufenden Infrastruktur VMs wie Netzwerk Controller, SLB-MUXe oder Gateways, so dass sie sich mit virtuellen Netzwerkadaptern damit verbinden können.

Die virtuellen Netzwerkadapter von Tenant VMs sind im Hyper-V Switch mit dem HNVPA Netz verbunden. Das Ver- und Entpacken der Tenant Daten mit dem VXLAN-Protokoll erfolgt dann im virtuellen Hyper-V Switch.

4.5 Weitere Infrastruktursysteme

Außer den Hyper-V Compute Systemen benötigen wir noch einige weitere Infrastruktursysteme:

- Active Directory mit DNS
- Ein System mit dem System Center Virtual Machine Manager (SCVMM) 2016 für das Management der SDN-Umgebung
- Einen BGP-Router, der uns die Verbindung zum öffentlichen Netz bereitstellt.

Auf diese Systeme werde ich später nochmals zurückkommen, wenn wir unsere Lab-Umgebung aufbauen.



5 SDN Deployment

Will man nun eine SDN-Umgebung aufbauen, bietet Microsoft verschiedene Methoden dafür:

• Manuelle Installation mit PowerShell

Diese Methode ist sehr mühsam, kann aber sinnvoll sein, wenn man nur einzelne SDN-Technologien einsetzen will. Details siehe <u>Deploy Software Defined Network Technologies using</u> <u>Windows PowerShell</u> in der Technet Library.

• Installation mit Hilfe vorgefertigter PowerShell Skripte

Diese Methode empfiehlt sich, wenn man eine SDN-Umgebung ohne den System Center Virtual Machine Manager (SCVMM) aufbauen und betreiben will, weil man andere Management Werkzeuge einsetzen will. Details siehe <u>Deploy a Software Defined Network infrastructure using</u> <u>scripts</u> in der Technet Library.

Installation über die Netzwerkfabrik des System Center Virtual Machine Manager 2016 (SCVMM 2016)

Dies ist meiner Meinung nach aktuell die bequemste und übersichtlichste Methode zur Installation einer SDN-Umgebung, insbesondere wenn der SCVMM 2016 sowieso als Management Werkzeug für die virtuelle Welt eingesetzt wird. Wir haben dabei sowohl die Möglichkeit der manuellen Installation über die VMM Konsole (Details siehe <u>Set up a Software</u> <u>Defined Network (SDN) infrastructure in the VMM fabric</u> in der Technet Library) als auch die automatisierte Installation mit PowerShell Skripten, die von Microsoft auf <u>Github</u> bereitgestellt werden.

Ich werde im Folgenden auf die automatisierte SCVMM Installation mit PowerShell Skripten näher eingehen und damit auch eine Lab-Umgebung aufbauen.



6 Die SDN Lab Umgebung

Legen wir also los mit dem Aufbau einer SDN Lab-Umgebung. Klären wir zunächst mal die Voraussetzungen.

6.1 Hardware

In meinem Testlabor habe ich nicht die notwendige Anzahl an Hardware-Systemen zur Verfügung, um eine vollständige SDN-Umgebung auszurollen. Ich werde deshalb das Ganze auf einem einzigen Hyper-V Host aufbauen und mit Nested Virtualisierung arbeiten.

Dieser Hyper-V sollte mindestens 128 GB RAM haben, für Windows Server 2016 Datacenter geeignet bzw. zertifiziert sein und natürlich Hyper-V unterstützen. Zur Not tut es auch ein System mit Windows 10 Pro (Laptop), das aber mindestens 64 GB RAM besitzen sollte. Falls Sie kein solches physisches System zur Verfügung haben, können Sie das Ganze auch in einer einzigen virtuellen Maschine umsetzen, die Sie z.B. in der Microsoft Azure Cloud oder bei einem anderen Service Provider anmieten.

6.2 Software

Sie benötigen folgende Softwarekomponenten für die Installation:

- Windows Server 2016 Data Center
- <u>System Center Virtual Machine Manager (SCVMM) 2016</u> einschließlich <u>SQL Server 2014</u> und <u>Windows Assessment and Deployment Kit</u>
- <u>SCVMM Service Templates und Powershell Skripte f
 ür das SDN Deployment</u>

Da wir hier nur eine Testumgebung aufbauen wollen, genügen die Evaluierungs-Versionen der jeweiligen Komponenten.

Auf das Downloaden und die Verwendung der SCVMM Service Templates und PowerShell Skripte werde ich später noch genauer eingehen.

6.3 Die Lab Infrastruktur

Für die SDN-Umgebung benötigen wir einige virtuelle Maschinen sowie die Parameter der logischen SDN-Netzwerke.

6.3.1 Virtuelle Maschinen

Bei der Infrastruktur der SDN-Umgebung beschränke ich mich auf ein Minimum an virtuellen Maschinen:

• Domain Controller SDN-DC01

Dieses System dient als Active Directory Controller mit integriertem DNS. Darüber hinaus stellt es über File Shares den Storage für unser Hyper-V Failover Cluster bereit.

• BGP-Router SDN-BGP

Dieses System stellt den BGP-Router für unsere Lab-Umgebung dar. Es verwendet dazu die Windows Serverrolle *Remote Access*.

• SDN-VMM01

Auf diesem System ist der System Center Virtual Machine Manager 2016 einschließlich der dafür notwendigen Basiskomponenten wie SQL-Server und Windows Assessment and Deployment Kit installiert. Von diesem System werden wir auch das Deployment der SDN-Umgebung steuern.



• SDN-HV01, SDN-HV02, SDN-HV03 und SDN-HV04

Diese 4 Systeme bilden ein Hyper-V Failover Cluster, in das wir die virtuellen SDN-Systeme wie Network Controller, SLB-MUXs und Gateways sowie auch beispielhaft einige Tenant VMs ausrollen werden.

6.3.2 Logische SDN Netze

Zum Ausrollen der SDN-Umgebung müssen wir auch die Parameter der logischen SDN-Netze festlegen. Die nachstehende Tabelle zeigt die Parameter, wie wir sie später im VMM verwenden werden.

Log. Netz	Subnet	Netzmaske	VLAN	Gateway	DNS	
			(optional)			
NC_Management	192.168.80.0	255.255.255.0	0	192.168.80.1	192.168.80.10	
	Verwendeter IF	P-Bereich: 192.168	8.80.230 – 192	.168.80.254		
	Reserviert für a	ndere Zwecke: 19	2.168.80.230	(IP-Adresse für d	ie REST API)	
HNVPA	10.10.10.0	255.255.255.0	0	10.10.10.1	192.168.80.10	
	Verwendeter IF	P-Bereich: 10.10.1	0.100 – 10.10.	10.199		
Transit	10.10.20.0	255.255.255.0	0	10.10.20.1	192.168.80.10	
	Verwendeter IP-Bereich: 10.10.20.100 – 10.10.20.199					
PrivateVIP	10.10.30.0	255.255.255.0	0	10.10.30.1	192.168.80.10	
	Verwendeter IP-Bereich: 10.10.30.100 – 10.10.30.199					
	Reserviert für L	oad Balancer VIPs	5: 10.10.30.100	0 - 10.10.30.199		
GREVIP	10.10.40.0	255.255.255.0	0	10.10.40.1	192.168.80.10	
	Verwendeter IP-Bereich: 10.10.40.100 – 10.10.40.199					
	Reserviert für L	oad Balancer VIPs	5: 10.10.40.100	0 - 10.10.40.199		
PublicVIP	10.10.50.0	255.255.255.0	0	10.10.50.1	192.168.80.10	
	Verwendeter IP-Bereich: 10.10.50.100 – 10.10.50.199					
	Reserviert für Load Balancer VIPs: 10.10.50.100 – 10.10.50.199					

6.3.3 Ein grober Überblick

Die Infrastruktur der Lab-Umgebung hat also folgendes Aussehen:





6.4 Vorbereitungen

- 1. Installieren Sie auf dem physischen Hyper-V Host die Datacenter Edition von Windows Server 2016 und installieren Sie die Hyper-V Rolle. Für unsere Tests ist keine Windows Aktivierung erforderlich; ersatzweise können Sie auch Windows 10 Pro verwenden.
- 2. Erstellen Sie im Hyper-V Host die 3 folgenden virtuellen Switche entweder über die GUI im Hyper-V Manager oder per PowerShell:

New-VMSwitch -Name "SDN" -SwitchType Internal New-VMSwitch -Name "Public" -SwitchType Internal New-VMSwitch -Name "Private" -SwitchType Internal

 Erzeugen Sie Windows Server 2016 VHDX-Dateien f
ür die verschiedenen zu erzeugenden VMs, z.B. mit dem PowerShell Skript *Convert-WindowsImage.ps1*, das Sie im Verzeichnis <*ISO>/NanoServer/NanoServerImageGenerator* der heruntergeladenen ISO Datei des Windows Server 2016 finden.

cd ' <iso>:\nanoserver\NanoServerImageGenerator'</iso>
\Convert-WindowsImage.ps1
Erzeuge dyn. VHDX für Gen2 Hyper-V VM
mit Windows Server 2016 Datacenter (= Edition4)
Convert-WindowsImage `
-SourcePath ' <iso>:\sources\install.wim' `</iso>
-Edition 4 `
-VHDPath 'E:\Hyper-V\WS2016.vhdx' `
-SizeBytes 80GB `
-VHDFormat VHDX `
-DiskLayout UEFI

4. Erzeugen Sie auf dem physischen Hyper-V Host nun folgende virtuelle Gen 2 Maschinen. Als Festplatte können Sie jeweils die im vorstehenden Schritt erzeugte VHDX-Datei verwenden. Statten Sie die VMs mit den angegebenen Netzwerkadaptern und gegebenenfalls mit den zusätzlichen Datenlaufwerken aus. Verbinden Sie die Netzwerkadapter mit dem jeweils angegebenen virtuellen Switch.

0.0			
6.4.1 SDN-DC01	L		
vCPU	2		
Memory	4 GB		
Netzwerkadapter	NC_Management	Verbunden mit internen Switch SDN	
	IP-Adresse	192.168.80.10	
	Gateway	192.168.80.1	
	DNS	192.168.80.10	
Zusätzliches	1 virt. Festplatte, dynamisch erweiterbar		
Laufwerk	Größe: >= 512 GB		
	Shares:		
	 Hyper-V – Stora 	ge für die HV01 – HV04	
	Cluster-Witness	- Synchronisationsdaten für das Hyper-V	

Installieren und konfigurieren Sie folgende Serverrollen und Features einschließlich der jeweiligen Management Tools:

- Active Directory
 - Domainname: SDNcloud.local

Cluster



- Benutzerkonten:
 - FabAdmin Fabric Admin: Klon des Benutzerkontos Administrator (optional). Ich arbeite normalerweise nur mit diesem Domain User. Damit kann keine Verwechslung mit dem lokalen Administrator-Konto entstehen beim Login an einem Member Server. Sie sollten dieses Konto jedoch auf allen Member Systemen in die lokale Gruppe Administrators aufnehmen, um dort auch alle Aufgaben durchführen zu können.
 - VMM-SVC Service Account für den VMM Service
- Lokale Security Gruppen
 - Network Controller Admins

Mitglieder dieser Sicherheitsgruppe dürfen die Netzwerk Controller Konfiguration verwalten (Kreieren, Löschen und Updaten von NC Komponenten). Für unsere Lab-Umgebung verwende ich die Standardgruppe *Domain Admins* und setze zusätzlich das oben beschriebene Benutzerkonto *FabAdmin* ein.

Network Controller A	Network Controller Admins Properties ? X					
General Members Member Of Managed By						
Members:						
Name	Active Directory Domain Services Folder		r			
Somain Admins	sdncloud.	local/Users local/Fabric/Se	rvices			

- Network Controller Users

Mitglieder dieser Sicherheitsgruppe dürfen nach dem NC-Deployment mit dem Netzwerk Controller über dessen REST-API kommunizieren. Für unsere Lab-Umgebung verwende ich die Standardgruppe Domain Admins und setze zusätzlich das oben beschriebene Benutzerkonto *FabAdmin* ein.

Network	Network Controller Users Properties ? X					×
General	Members	Member Of	Managed By			
Membe	rs:					
Name 🎎 Do 鸄 Fa	Name & Domain Admins & FabAdmin		Active Directory Domain Services Folder sdncloud.local/Users sdncloud.local/Fabric/Services			

- DNS
 - Active Directory integriert
 - definieren Sie ggf. DNS-Forwarders, um Internet Namen auflösen zu können (optional; für einige spätere Testszenarien sinnvoll)

Stellen Sie sicher, dass Sie alle aktuellen Updates und Patches installiert haben.



6.4.2 SDN-BGP01

vCPU	2	
Memory	4 GB	
Netzwerkadapter	NC_Management	Verbunden mit internen Switch SDN
	IP-Adresse	192.168.80.50
	Gateway	192.168.80.1
	DNS	192.168.80.10
	HNVPA	Verbunden mit internen Switch SDN
	IP-Adresse	10.10.10.1
	Transit	Verbunden mit internen Switch SDN
	IP-Adresse	10.10.20.1
	Public	Verbunden mit internen Switch Public
	IP-Adresse	10.10.50.1

Joinen Sie das System als Member Server ins Active Directory.

Installieren und konfigurieren Sie folgende Serverrollen und Features einschließlich der jeweiligen Management Tools:

Remote Access

Es genügen die Rollen Direct Access and VPN sowie Routing

Aktivieren Sie die LAN-Router Funktion oder optional NAT (in meiner Lab-Umgebung arbeite ich mit NAT, da ich über das logische Netz *NC_Management* Internetzugriff habe).

Eine weitere Konfiguration ist zunächst nicht notwendig; sie erfolgt später.

Stellen Sie sicher, dass Sie alle aktuellen Updates und Patches installiert haben.

6.4.3 SDN-HV01 - SDN-HV04

vCPU	Je 4		
Memory	Je 16 GB – dyn. Memory darf nicht aktiviert sein!		
Netzwerkadapter	NC_Management	Verbunden mit internen Switch SDN	
	IP-Adressen	SDN-HV01: 192.168.80.21	
		SDN-HV02: 192.168.80.22	
		SDN-HV03: 192.168.80.23	
		SDN-HV04: 192.168.80.24	
	Gateway	192.168.80.1	
	DNS	192.168.80.10	

- Joinen Sie alle 4 Systeme als Member Server ins Active Directory.

Installieren und konfigurieren Sie folgende Serverrollen und Features einschließlich der jeweiligen Management Tools auf allen 4 VMs:

- Hyper-V

Achtung: Aktivieren Sie Nested Virtualization und MAC Address Spoofing für alle 4 VMs mit PowerShell:

Get-VMProcessor -VMName SDN-HV01 | Set-VMProcessor -ExposeVirtualizationExtensions <u>\$true</u> Get-VMNetworkAdapter -VMName SDN-HV01 | Set-VMNetworkAdapter -MacAddressSpoofing On



Definieren Sie in den Hyper-V Systemen noch keinen virtuellen Switch. Wir werden dies später mit dem SCVMM erledigen.

Setzen Sie im Hyper-V Manager in den Hyper-V Einstellungen die Pfade für virtuelle Maschinen und virtuelle Hard Disks auf den Share, den Sie beim Kreieren des Systems SDN-DC01 angelegt haben.

Hyper-V Settings for SDN-HV01	
 Server Virtual Hard Disks \\SDN-DC01\Hyper-V\ Virtual Machines \\SDN-DC01\Hyper-V\ 	Virtual Hard Disks Specify the default folder to store virtual hard disk files. \\SDN-DC01\Hyper-V\
Hyper-V Settings for SDN-HV01	
 Server Virtual Hard Disks \\SDN-DC01\Hyper-V\ Virtual Machines \\SDN-DC01\Hyper-V\ 	Virtual Machines Specify the default folder to store virtual machine configuration files. \\SDN-DC01\Hyper-V\

- Failover Clustering

Erzeugen Sie ein Hyper-V Failover Cluster mit den 4 Hyper-V Systemen. In meiner Lab-Umgebung verwende ich folgende Parameter:

- Clustername: SDN-HVCL
- Cluster IP: 192.168.80.20

Stellen Sie sicher, dass Sie alle aktuellen Updates und Patches installiert haben.

6.4.4 SDN-VMM01

vCPU	2		
Memory	4 GB		
Netzwerkadapter	NC_Management	Verbunden mit internen Switch SDN	
	IP-Adresse	192.168.80.31 / 24	
	Gateway	192.168.80.1	
	DNS	192.168.80.10	
Zusätzliches	1 virt. Festplatte, dynamisch erweiterbar		
Laufwerk	Größe: >= 512 GB		
Legen Sie Verzeichnisse für die VMM-Library (z.B. D		isse für die VMM-Library (z.B. <i>D:\VMMLibrary</i>)	
	und für die SDN Inst	allationsskripte (z.B. <i>D:\Software</i>) an.	

• Joinen Sie das System als Member Server ins Active Directory.

Downloaden und installieren Sie nun folgende Softwarekomponenten auf den SDN-VMM01:

- <u>Windows Assessment and Deployment Kit</u>
- <u>SQL Server 2014</u> (oder neuer)
- <u>System Center Virtual Machine Manager (SCVMM) 2016</u> einschließlich dem aktuellen <u>Update</u> <u>Rollup UR5</u>
 - Verwenden Sie als Benutzerkonto für den VMM Serverdienst den beim SDN-DC01 erstellten Service Account VMM-SVC.



Stellen Sie sicher, dass Sie alle aktuellen Updates und Patches installiert haben.

Starten Sie nach der vollständigen VMM Installation die VMM Konsole über das Icon auf dem Desktop und führen Sie folgende Basiskonfiguration durch:

• Rufen Sie im Arbeitsbereich *Settings* unter *General* die *Network Settings* auf und deaktivieren Sie das Kontrollkästchen *Create logical networks automatically*.

	Administrator - WAP-VMMULwapcioud.a	ocal - Virtual Machine Manager — 🖉
	Home	
Virtual Machine Manager	Create Create Run Create Servicing User Role As Account Create	Importation Bactup Window Properties
Console	Settings <	Settings (6)
	General	
	👶 User Roles	Name
\	Run As Accounts	Diagnostic and Usage Data Settings
🗉 Connect to Server 🛛 🗖	Servicing Windows	Patabase Connection
	Configuration Providers	Remote Control
		📥 Network Settings
	System Center Settings	V Host Guardian Service Settings
System Center 2016	🐏 Console Add-ins	I Network Settings ×
Virtual Machine Manager Server name: Jocalhost8100 Example: vinmiserver.contoso.com/8100 © Use current Microsoft Windows session identity O Specify credentials User name: Example: contract/domainuser	Microsoft Azure Site Recovery	Network settings Specify the options for logical and virtual switches. Logical network matching Match logical networks by: If the above fails, match by: Another constant by: Another constant by: Automatic constant logical network Interaction of logical networks Interaction the hold network adopter in not associated with a logical network, a new one will be created based on the above choice made for network another Constant logical networks adopter in not associated with a logical network, a new one will be created based on the above choice made for network another
	w VMs and Services	
Password:	Pabric	
	Library	
Automatically connect with these settings	🗈 Jobs	
Automatically connect with these settings	Settings	

 Klicken Sie im Arbeitsbereich Settings mit der rechten Maustaste auf den Eintrag Run As Accounts und rufen den Befehl Create Run As Account auf. Im Dialogfenster geben Sie jetzt ein Benutzerkonto aus dem Active Directory einschließlich Kennwort an, das Domain Admin Rechte besitzt – im Beispiel der FabAdmin aus der Domain sdncloud.

eneral	Name	
un As Accounts		
	Create Run As Account	
E Create Run A	s Account	
Provide March		
Provide the	details for this Run As account	
Name: V	MM Admin	
Description:		
Liser name:	educioud/EabAdmin	
<u>o</u> ser nonier	Example: contoso\domainuser or localuser	
Password:	•••••	
Confirm passw	ord:	
Validate do	main credentials	



• Erstellen einer SDN-Host Gruppe im VMM

Technisch ist dieser Schritt nicht unbedingt erforderlich. Man kann dann jedoch schnell sehen, welche Hosts zu der SDN-Umgebung gehören.

Wechseln Sie in der VMM-Konsole in den Arbeitsbereich *Fabric,* klicken mit der rechten Maustaste unter *Servers* auf *All Hosts* und wählen Sie im Kontextmenü den Befehl *Create Host Group.* Geben Sie als Namen *SDN-Hosts* ein.

Fabric		Hosts (0)	
• 11 Servers		[
All He	Add Hyper-V Hosts and Add VMware ESX Host	d Clusters s and Clusters	
🕴 📥 Networ	🥑 Create Host Group		 Messervers
🕴 🤰 Storage	Move W		All Hosts
	💰 View Networking		► 1.2 Infrastructure
	🗙 Delete		
	Properties		
 WMs and ₩ Fabric ₩ Library ➡ Jobs 	d Services		
Jobs			

• Importieren der Hyper-V Hosts in den VMM

Klicken Sie in der VMM-Konsole im Arbeitsbereich *Fabric* mit der rechten Maustaste auf die soeben erstellte Hostgruppe *SDN-Hosts* und wählen im Kontextmenü den Befehl *Add Hyper-V Hosts and Clusters*.

Es öffnet sich der Add Resource Wizard. Wählen Sie dort die Option Windows Server computers in a trusted Active Directory domain und klicken Sie dann auf Next.



▲				Add Resource Wizard	×
Servers All Hosts SDN-Hoots BNN-Hosts All Hosts Constrained Storage	Image: Second	Name Higher-V Hosts and VIWvare ESX Host te Host Group 2 Networking 2 me erties	Host Status d Clusters s and Clusters	Add Resource Wizard Resource Location Credentials Discovery Scope Target Resources Host Settings Summary	E Location Indicate the Windows computers location Windows Server computers in a trusted Active Directory domain Windows Server computers in a nutrusted Active Directory domain Windows Server computers in a nutrusted Active Directory domain Windows Server computers in a perimeter network Hyou select this option, before you continue, use VMM Setup to install the VMM agent locally on the targeted computers. Ensure that you configure the perimeter network settings during the agent setup. Physical computers to be provisioned as virtual machine hosts Select this option to add bare-metal computers with baseboard management controllers. An agent accessible by the computer might be partitioned during the provisioning process and the data will be loct. Review the online documentation before starting the deployment.
					Previous Next Cancel

Wählen Sie den *Run As Account*, mit dem der Import durchgeführt werden soll, indem Sie auf *Browse* klicken.

Add Resource Wizard	×
🐴 Credenti	als
Resource Location Credentials Discovery Scope Target Resources Host Settings Summary	 Specify the credentials to use for discovery The Run As account or credentials will be used to discover computers and to install the Hyper-V role and the Virtual Machine Manager agent if necessary. Use an existing Run As account Run As account: Manually enter the credentials User name: Example: contoso\domainuser Password: The above provided credentials or Run As account should be a local administrator on the host machines. If a Run As account is provided, then it will be used while adding the host as well as for providing future access to the host during its lifetime. If credentials are entered manually, then they will only be used while adding the host. Once the host has been successfully added, the VMM service account will be added as local administrator on the host and used to provide any future access to it.
	Previous Next Cancel

Wählen Sie in der angezeigten Liste den vorhin angelegten VMM Admin aus und klicken Sie auf OK.



	///	٩
Name	Description	User Role
NT AUTHORITY	System	
NT AUTHORITY	LocalS	
NT AUTHORITY	Netwo	
VMM Admin		Administrator

Zurück im Add Resource Wizard sehen Sie den ausgewählten Run As Account. klicken Sie auf Next.

Add Resource Wizard	×
😭 Credenti	als
Resource Location Credentials Discovery Scope Target Resources Host Settings Summary	 Specify the credentials to use for discovery The Run As account or credentials will be used to discover computers and to install the Hyper-V role and the Virtual Machine Manager agent if necessary. Use an existing Run As account Run As account: VMM Admin Browse Manually enter the credentials User name: Example: contoso\domainuser Password: The above provided credentials or Run As account should be a local administrator on the host machines. If a Run As account is provided, then it will be used while adding the host as well as for providing future access to the host during its lifetime. If credentials are entered manually, then they will only be used while adding the host on the host and used to provide any future access to it.
	Previous Next Cancel

Im nächsten Fenster müssen Sie jetzt die Namen der zu importierenden Hyper-V Hosts bzw. Cluster eingeben, in unserem Fall also den Clusternamen *SDN-HVCL*. Klicken Sie dann wieder auf *Next*.

Jetzt wird Ihnen das Cluster mit den Mitgliedsservern angezeigt. Aktivieren Sie die Checkbox neben dem Clusternamen und klicken Sie auf *Next*.



lesource Location Tredentials	Select the computers that you want to add as hosts Discovered computers:							
Discovery Scope	Computer Name	Operating System	Hypervisor					
larget Resources	SDN-HVCL.sdncloud.local	Windows Server 2016 Datacenter	Hyper-V					
Host Settinos	sdn-hv02.sdncloud.local	Windows Server 2016 Datacenter	Hyper-V					
inosi octorigo	sdn-hv03.sdncloud.local	Windows Server 2016 Datacenter	Hyper-V					
Summary	sdn-hv04.sdncloud.local	Windows Server 2016 Datacenter	Hyper-V					

Wählen Sie jetzt die *Host Group* für den Import aus. Aktivieren Sie auch die Checkbox *Reassociate this host with this VMM environment*. Klicken Sie nochmals auf *Next*.

Add Resource Wizard	
音 Host Set	tings
Resource Location Credentials Discovery Scope	Specify a host group and virtual machine placement path settings for hosts Assign the selected computers to the following host group: Host group: SDN-Hosts
Host Settings	If any of the selected hosts are currently managed by another Virtual Machine Manager (VMM) environment, select this option to reassociate the hosts with this VMM management server.
Samuray	
	Previous Next Cancel



Prüfen Sie in der angezeigten Zusammenfassung nochmals Ihre Angaben und klicken Sie dann auf *Finish*.

Add Resource Wizard	y				
Resource Location Credentials Discovery Scope Target Resources Host Settings Summary	Confirm the settin Resource type: Resource location: Discovery credential Discovery scope: Host settings:	Hyper-V capable Windows Servers Trusted Windows computer s: VMM Admin Computer name based discovery 1 clusters are selected to manage Host group: All Hoste\SDN-Hosts	6		View Script
			Previous	Finish	Cancel

Der Importvorgang startet und Sie können den Fortschritt in der Jobliste des VMM mitverfolgen.

							_
Name	Status	-	Start Time	*	Result Name	Owner	
Refresh host cluster		0 %	02.07.2018 15:21:11		SDN-HVCL.sdncloud.local	sdncloud\FabAdmin	
Add virtual machine host	11111111	50 %	02.07.2018 15:21:11		SDN-HV01.sdncloud.local	sdncloud\FabAdmin	
Add virtual machine host	TTTT MATTER	80 %	02.07.2018 15:21:11		SDN-HV04.sdncloud.local	sdncloud\FabAdmin	
Add virtual machine host		80 %	02.07.2018 15:21:11		SDN-HV03.sdncloud.local	sdncloud\FabAdmin	
Add virtual machine host		80 %	02.07.2018 15:21:10		SDN-HV02.sdncloud.local	sdncloud\FabAdmin	
Ø Create new host cluster	Completed		02.07.2018 15:21:09		SDN-HVCL.sdncloud.local	sdncloud\FabAdmin	
Discover clusters and the	. Completed		02.07.2018 15:21:06		SDN-HVCLsdncloud.local	sdncloud\FabAdmin	
Ohange properties of virt	. Completed		02.07.2018 14:56:50		SDN-Hosts	sdncloud\FabAdmin	
Croate vistual machine h	Completed		03.07.2010 14.55.47		SDN Host	colocioud Esh Admin	

Warten Sie, bis alle Jobs erfolgreich abgeschlossen sind (Anzeige *Completed*). Die angezeigten Warnungen über das nicht aktivierte *Multipath IO* können wir hier ignorieren.



							-
Name	l.	Statu	IS	* Start Time	* Result Name	Owner	-
Refres	sh host cluster	Comp	pleted	02.07.2018 15:21:11	SDN-HVCL.sdncloud.local	sdncloud\FabAdmin	
Add v	irtual machine h	ost Com	leted w/ Info	02.07.2018 15:21:11	SDN-HV01.sdncloud.local	sdncloud\FabAdmin	
Add v	irtual machine h	nost Comp	oleted w/ Info	02.07.2018 15:21:11	SDN-HV04.sdncloud.local	sdncloud\FabAdmin	
Add v	irtual machine h	nost Comp	eleted w/ Info	02.07.2018 15:21:11	SDN-HV03.sdncloud.local	sdncloud\FabAdmin	
Add v	irtual machine h	nost Comp	oleted w/ Info	02.07.2018 15:21:10	SDN-HV02.sdncloud.local	sdncloud\FabAdmin	
Create	e new host clust	er Comp	oleted	02.07.2018 15:21:09	SDN-HVCL.sdncloud.local	sdncloud\FabAdmin	
Disco	ver clusters and	the Comp	oleted	02.07.2018 15:21:06	SDN-HVCLsdncloud.local	sdncloud\FabAdmin	
Ochange properties of virt Completed			pleted	02.07.2018 14:56:50	SDN-Hosts	sdncloud\FabAdmin	
A Crosta with all maching h Completed				02.07.2019 14:55:47	SDAL Harte	colocioud\EshAdmia	
Result nar Started: Duration: Dwner:	SCVMHostC SCVMHostC HV01.sdnck 02.07.2018 00:00:59 sdncloud\Fa	Cluster oud.local 15:21:11 abAdmin	Warning Multipath Recomm Manually wish to p	(26179) I //O is not enabled for know ended Action enable the Multipath I/O fea rovision the host in the Stora	n storage arrays on host SDN-H ture for the host. Do not enable ge Spaces Direct cluster.	/01.sdncloud.local. this feature in case you	
	Details Chan	ne Trackino	Copy Errors				

Schließen Sie das Jobfenster. In der VMM Konsole sind jetzt unser Cluster und die Hyper-V Hosts importiert.

Fabric	<	Hosts (4)					
 ▲ Servers ▲ 🚞 All Hosts 		Name	Host Status	1	Role	Job Status	CPU Average
🖌 🛄 SDN-Hosts		SDN-HV02.sdn	OK		Host	Completed w/ Info	3 %
SDN-HVCL		SDN-HV04.sdn	ОК		Host	Completed w/ Info	3 %
🕨 🛃 Infrastructure		I SDN-HV03.sdn	OK		Host	Completed w/ Info	3 %
🕨 📥 Networking		SDN-HV01.sdn	ОК		Host	Completed w/ Info	74 %
Storage							

Im nächsten Schritt müssen wir dem VMM noch mitteilen, wo die Images für unsere zukünftigen virtuellen Maschinen abgelegt werden sollen.

Wechseln Sie im *Fabric* Arbeitsbereich in die Kategorie *Storage*, klicken mit der rechten Maustaste auf *Providers* und wählen den Befehl *Add Storage Devices*.





Es öffnet sich der Add Storage Devices Wizard. Da wir in dieser Lab-Umgebung für das Ablegen der VM-Images einen File Share mit dem Namen Hyper-V auf unserem Domain Controller SDN-DC01 verwenden wollen, wählen wir als Provider Typ Windows-based file server und klicken auf Next.

🚣 Add Storage Devices Wiz	ard	×
🚣 Select Pro	vider Type	
Select Provider Type Specify Discovery Scope Gather Information Select Storage Devices Summary	Select a storage provider type Before you begin this wizard, you might have to manually install storage provider software. Select the storage provider type that matches the type of device you want to manage. Windows-based file server SAN and NAS devices discovered and managed by a SMI-S provider SAN devices managed by a native SMP provider Fibre Channel fabric discovered and managed by a SMI-S provider 	
	Previous Next Cancel	

Jetzt müssen wir den Servernamen und einen Run As account angeben.



🟝 Add Storage Devices Wiza	rd		×
😫 Specify Dis	covery Sco	ce	
Select Provider Type	Specify the IP	address or FQDN of the Windows-based file server	
Specify Discovery Scope	Provider IP address	s or FQDN:	
Gather Information	SDN-DC01.sdnclo	ud.local	Ŷ
Select Storage Devices	This computer	is in an untrusted Active Directory domain	
Summany	R <u>u</u> n As account:	VMM Admin	<u>B</u> rowse
Summary			
		Previous Next	Cancel

Nach einem Klick auf Next wird uns der SDN-DC01 als Storage Device angezeigt ...

Add Storage Devices Wiz	ormation			
Select Provider Type Specify Discovery Scope	Discover and im	port storage device inforr	nation	Scan Provider
Gather Information	Storage Device	Manufacturer	Model	Capacity
Select Storage Devices	SDN-DC01.sdnctoud	local Microsoft Corporation	Virtual Machine	591,43 G

... und nach einem weiteren Klick auf *Next* die darauf verfügbaren Shares. Wählen Sie den *Hyper-V* Share aus und klicken Sie nochmals auf *Next*.



elect Provider Type ipecify Discovery Scope Sather Information	Select file shares to Bringing file shares under Virtual Machine Manager.	place under management wil	manageme I make them av	nt ailable for use in computers n	nanaged by
elect Storage Devices	Storage Device	Total Capacity	Classification	Host Group	
Summary	SDN-DC01.sdncloud.loca	I 591,43 GB			v
			~		
	NETLOGON				

Es wird eine Zusammenfassung angezeigt. Wenn wir nun auf *Finish* klicken, wird unser File Share als Storage Device importiert.

🟝 Add Storage Devices Wiz	ard		×
📤 Summary			
Select Provider Type Specify Discovery Scope	Confirm the setting	gs	View Script
Gather Information Select Storage Devices Summary	Resource type: Discovery scope: Storage provider type Managed file shares:	Storage device SDN-DC01.sdncloud.local Native Windows WMI Hyper-V File server: SDN-DC01.sdncloud.local Total capacity: Share path: \\SDN-DC01.sdncloud.local\Hyper-V Classification: Remote Storage	
		Previous	Finish Cancel



Über die Jobliste können wir den Vorgang mitverfolgen.

	Jobs					- 0	×
Reci	ant Jobs (13)						45
							9
	Name	Status	Start Time	*	Result Name	Owner	-
0	Sets Storage Provider	Completed	02.07.2018 15:24:32		SDN-DC01	sdncloud\FabAdmin	1
0	Adds Storage Provider	Completed	02.07.2018 15:23:49		SDN-DC01	sdncloud\FabAdmin	

Jetzt müssen wir den gerade importierten Storage Provider noch in den *Properties* unseres Clusters registrieren, damit der VMM weiß, wo er VM Images für dieses Cluster ablegen kann.

Klicken Sie mir der rechten Maustaste auf das Cluster im *Fabric* Arbeitsbereich unter der vorhin angelegten Hostgroup *SDN-Hosts* und rufen Sie im Kontextmenü die *Properties* auf.



Klicken Sie auf der Registerkarte File Share Storage auf die Schaltfläche Add...



eneral	File Share Storage				
atus	The following file shares w	ill be available as storage l	ocations for VMs	deployed to n	odes in this cluster:
vailable Storage	File Share Path	Access Status	Classification	Free Space	Total Capacity
le Share Storage					
nared Volumes					
rtual Switches					
ustom Properties					
			Repa	ir Add	Remove

Im *Add File Share* Dialogfenster können Sie nun den vorher als Storage Provider definierten Pfad *SDN-DC01.sdncloud.local**Hyper-V* in der Klappbox auswählen. Klicken Sie auf *OK* ...

General	File Share Storage				
	The Share Storage				
tatus	The following file shares w	will be available as storage lo	ocations for VMs	deployed to no	odes in this cluster:
wailable Storage	File Share Path	Access Status	Classification	Free Space	Total Capacity
and ble storage	Add File Share			×	
ile Share Storage	Specify a valid SMB	share path to use for	r VM		
hared Volumes	deployment				
irtual Switches	File share path:		-	*	
ustom Properties	To register a file shore to a list or enter the UNC path	-DC01.sdncloud.local\Hyper	r-V a me soure nom a	inc	
	For managed shares, VMN computer account for the management account. For	I grants file share access to virtualization cluster and the unmanaged file shares, ens	the Active Direct e VMM cluster ure that the Acti	ory ve	
	Directory computer accou cluster management acco	nt for the virtualization clust unt have access to the file sh	ter and the VMM nare.		
	To bring a file share into n	anagement: in the VMM co	nsole, open the	Fabric	
	workspace, elect the rioth	acis node, and pren cick. A	so stolage been		
			OK Can	ncel	
			124		
			Repa	ir Add	Remove

... und der Pfad wird in den *File Share Properties* unseres Clusters angezeigt. Durch einen weiteren Klick auf *OK* wird die Änderung übernommen.



eneral	File Share Storage				
tatus	The following file shares w	ill be available as storage lo	ocations for VMs (deployed to nod	les in this cluster:
and the factors	File Share Path	Access Status	Classification	Free Space	Total Capacity
wallable storage	\\SDN-DC01.sdncloud.lo	cal\Hyp	Remote Storag	e 490,77 GB	511,87 GB
ile Share Storage	<				
nared Volumes					
rtual Switches					
ustom Properties					

Damit ist die Basis-Installation und Konfiguration für unsere SDN Lab-Umgebung erstmal abgeschlossen.

7 Bereitstellen der Skripte für das SDN Deployment – VMM Express.ps1

Für das SDN Deployment mit dem SCVMM stellt Microsoft ein eigenes <u>Repository auf GitHub mit</u> <u>Service Templates und Skripten</u> zur Verfügung. Laden Sie dieses Paket als .ZIP-Datei in ein Verzeichnis auf dem Datenlaufwerk des System *SDN-VMM01* (z.B. *D:\Software*).

A https://github.com/Micro	osoft/SDN 🔎 👻 🔒 GitHub, Inc. [US] 🖒	Q GitHub - Microsoft/SDN: T	× ŵ
Features Busines	s Explore Marketplace Pricing	Search	Sign in or Sign
Microsoft / SDN		٥	Watch 77 ★ Star 156 😵 Fork 15
Code (1) Issues 52	Pull requests 4 Projects 0	Insights	
his repo includes PowerSh SDN) Stack using Windows	ell scripts and VMM service templates for s s Server 2016	etting up the Microsoft So	ftware Defined Networking
his repo includes PowerSh iDN) Stack using Windows (P 421 commits	ell scripts and VMM service templates for s s Server 2016 JP 8 branches	etting up the Microsoft So	ftware Defined Networking # 26 contributors
his repo includes PowerSh SDN) Stack using Windows (P 421 commits Branch: master • New pull re	ell scripts and VMM service templates for s s Server 2016 IP 8 branches	etting up the Microsoft So	oftware Defined Networking
his repo includes PowerSh SDN) Stack using Windows (7) 421 commits Branch: master New pull re dcuomo Updated ToC on Tm	ell scripts and VMM service templates for s s Server 2016 8 branches quest stping vGuide	etting up the Microsoft So	Elone with HTTPS ©
his repo includes PowerSh SDN) Stack using Windows	ell scripts and VMM service templates for s s Server 2016	etting up the Microsoft So © 0 releases parameters	Strain Clone with HTTPS Use Git or checkout with SVN using the web URL https://github.com/Hicrosoft/SDN.git

Entsperren und extrahieren Sie die heruntergeladene .ZIP-Datei. Sie erhalten dann folgende Verzeichnisstruktur:



🖸 📴 ╤ VMM Tie Home Share View				- <u>-</u>	1 ×
- 🛶 👻 🕂 🛄 « Software > SDN-r	master > SDN-master > VMM >	~ Ö	Search \	/MM	Q
✓ Software ^	Name	Date mo	dified	Туре	Siz
V SDN-master	scripts	03.07.201	18 16:28	File folder	
✓ SDN-master	🧧 Templates	03.07.201	18 16:28	File folder	
Containers	🔛 VMM SDN Express	03.07.201	18 16:28	File folder	
Diagnostics					
FeatureGuide					
> 🧧 Kubernetes					
NCRESTExamples					
> 🦲 NDKCI					
> 🦲 SDNExpress					
> 🧧 SwitchConfigExamples					
> 🧧 Time					
> 🧧 VMM					
> 😨 SDN-master.zip					

Interessant für unsere weitere Arbeit ist der Unterordner VMM. Er enthält 3 Unterverzeichnisse:

- Scripts PowerShell Beispiel-Skripte für virtuelle Tenant IP-Adressen nach dem SDN Deployment
- Templates VMM Service Templates für Network Controller, SLB und Gateway VMs
- VMM SDN Express PowerShell Skripte für das SDN-Deployment

Werfen wir zunächst einen Blick in das *Templates* Verzeichnis. Es enthält 3 Ordner, je einen für die Netzwerk Controller (*NC*), für die Software Load Balancer(*SLB*) und für die Gateways (*GW*). Im *NC*-Verzeichnis finden wir 4 XML-Dateien für verschiedene Methoden zum Erzeugen der Netzwerk Controller VMs. Der Unterschied: Mit den *Production* Varianten wird ein virtuelles Guest Cluster mit 3 Network Controllern erzeugt, wohingegen die *Standalone* Varianten nur einen einzelnen Network Controller kreieren.

- EdgeDeployment.cr
- NCSetup.cr
- ServerCertificate.cr
- TrustedRootCertificate.cr
- Network Controller Production Generation 1 VM.xml
- Network Controller Production Generation 2 VM.xml
- Retwork Controller Standalone Generation 1 VM.xml
- Network Controller Standalone Generation 2 VM.xml

Für produktive Umgebungen sollten Sie auf jeden Fall die *Production* Varianten einsetzen. Wir werden in unserer Lab-Umgebung ebenfalls damit arbeiten und Gen2 VMs erzeugen.

Bei Bedarf können Sie in den Service Templates die Definitionen für die zu erzeugenden VMs noch anpassen. Öffnen Sie die jeweilige XML-Datei (hier: *Network Controller Production Generation 2 VM.xml*) in einem XML-Editor (z.B. PowerShell ISE). Sie können z.B. die Werte für RAM, Anzahl virtueller CPUs und die TimeZone anpassen:





Für unsere Lab-Umgebung reduziere ich den RAM-Wert auf 4096 und setze die Zeitzone auf den Wert 110 (W. Europe Standard Time). Anm.: Eine Tabelle mit den Indexwerten für Zeitzonen finden Sie z.B. <u>hier</u>.

Analog können Sie auch die Service Templates für die SLBs und Gateways anpassen.

Um die Location Einstellungen der VMs (wie z.B. Tastatur Layout und Datum / Uhrzeit Anzeige in Deutsch) anzupassen, habe ich mir eine eigene *Unattend.xml* Datei erstellt, die ich während des Deployments der Service Templates dem SCVMM "unterjuble".

Nachdem wir die Service Templates gegebenenfalls angepasst haben, können wir uns dem eigentlichen Deployment der SDN-Umgebung zuwenden.

Dazu wechseln wir in das Verzeichnis VMM SDN Express:



In diesem Verzeichnis finden wir eine PowerShell Skriptdatei VMMExpress.ps1 sowie einige PowerShell Datendateien (.PSD1).

VMMExpress.ps1

Dieses PowerShell Skript enthält die komplette Logik zum Ausrollen einer SDN-Umgebung. Es installiert die notwendigen virtuellen Switches in den Hyper-V Systemen, kreiert die weiter oben beschriebenen logischen Netze und erzeugt dann die VMs für die SDN-Komponenten (Network Controller, Software Load Balancer und Gateways).



Das Skript wird über eine Konfigurationsdatei (PowerShell Datendatei – .PSD1-Datei) gesteuert, die beim Aufruf von VMMExpress.ps1 über den Parameter -ConfigurationDataFile angegeben wird. Diese Konfigurationsdatei enthält sowohl Parameter für die SDN-Umgebung wie logische Netze und VMs als auch Ablaufsteuerungsschalter. Letztere ermöglichen entweder einen gesamten Durchlauf für alle Komponenten oder ein schrittweises Deployment der einzelnen Komponenten. So kann festgelegt werden, dass zunächst nur die Netzwerk Controller Instanzen erzeugt werden. In einem weiteren Aufruf von VMMExpress.ps1 werden dann die Software Load Balancer erzeugt und in einem dritten Aufruf schließlich die Gateways. Diese Methode für das schrittweise Deployment der diversen SDN-Komponenten werde ich für unsere Lab-Umgebung verwenden.

Das Verzeichnis VMM SDN Express enthält 2 Beispiele für Konfigurationsdateien. Die Datei Fabricconfig.psd1 stellt ein "leeres" Muster dar. Fabricconfig_Example.psd1 enthält die Parameter für eine von Microsoft erstellte Beispielkonfiguration.

Für unsere SDN Lab-Umgebung habe ich eine eigene Konfigurationsdatei mit den weiter oben beschriebenen Parametern erstellt – *Fabricconfig-SDNcloud-Production.psd1*.

• Fabricconfig-SDNcloud-Production.psd1

Nachstehend finden Sie die vollständige Konfigurationsdatei, um in unserer SDN Lab-Umgebung zunächst nur den Netzwerk Controller und die logischen SDN-Netze zu erzeugen. Speichern Sie diese Datei im gleichen Verzeichnis wie *VMMExpress.ps1* unter dem Namen *Fabricconfig-SDNcloud-Pro1duction.psd1*. Auf die notwendigen Änderungen für das Deployment der SLB- und Gateway-Komponenten werde ich später noch eingehen.





```
#Type of Deployment. The values are :
#Standalone : For single Node
#Production : For 3-node
DeploymentType="Production"
#Higly Available VM. Do you want the infrastructural VMs to be deployed on
#Clustered Host and being higly Available ? If yes pass $true else $false
HighlyAvailableVMs = $true
StorageClassification = "Remote Storage"
#leave it if you want default IPvAddressType to be taken which is static
# else change it to "Dynamic"
IPv4AddressType=""
#Host Group to be Managed by Network Controller
NCHostGroupName="SDN-Hosts"
****
# Section for deploying Logical switch and Logical Network for NC.
#
# Specify IsLogicalSwitchDeployed = $false and
     IsManagementVMNetworkExisting = $false
#
# if VMMExpress.ps1 should try to create a SET switch.
#
# If SET cannot be used you have to deploy Logical Switch and
# Management Network by yourself.
#
# NOTE : This script assumes either you have both logical switch and
# logical Network created and deployed or else you will use the script
# to deploy both.
*****
#Do you have an existing logical switch and the switch is deployed on all
#the hosts you wish to Manage by NC
IsLogicalSwitchDeployed = $false
# IsLogicalSwitchDeployed = $true
#if above is true give the name of logical switch
LogicalSwitch = "NC_LogicalSwitch"
# Do you have existing Management Network that you would like to use
IsManagementVMNetworkExisting = $false
# IsManagementVMNetworkExisting = $true
#if above is true give the name of ManagementVMNetwork
ManagementVMNetwork = "NC Management"
#Uplink Port Profile to be used
UplinkPortProfile = "HV Uplink Port"
# The below set of Parameters are required for creation of Management Logical Network
# and other Logical Networks Managed by NC.
# NOTE : If you already have Management Logical Network Created and switch deployed,
# you don't need to specify any parameters for "NC_Management" LN
#==
     LogicalNetworks = @(
                @{
   Name = "HNVPA"
   Subnets = @(
     @{
       # VLANID = 255
       VLANID = 0
```



```
AddressPrefix = "10.10.10.0/24"
      DNS = @("192.168.80.10")
      Gateways = "10.10.10.1"
      PoolStart = "10.10.10.100"
      PoolEnd = "10.10.10.199"
   }
 )
},
                        @{
  Name = "Transit"
  Subnets = @(
    @{
      # VLANID = 254
      VLANID = 0
      AddressPrefix = "10.10.20.0/24"
      DNS = @("192.168.80.10")
      Gateways = "10.10.20.1"
      PoolStart = "10.10.20.100"
      PoolEnd = "10.10.20.199"
    }
 )
},
@{
 #The first IP address (PoolStart) for this logical network is
  #automatically assigned to the SLB Manager. Other addresses such
  #as the GatewayPublicIPAddress will start after that.
  Name = "PublicVIP"
  Subnets = @(
    @{
      VLANID = 0
      AddressPrefix = "10.10.50.0/24"
      DNS = @("192.168.80.10")
      Gateways = "10.10.50.1"
      PoolStart = "10.10.50.100"
      PoolEnd = "10.10.50.199"
      IsPublic = $true
    }
 )
}
@{
  #The first IP address (PoolStart) for this logical network is
  #automatically assigned to the SLB Manager. Other addresses such
  #as the GatewayPublicIPAddress will start after that.
  Name = "PrivateVIP"
  Subnets = @(
    @{
      # VLANID = 253
      VLANID = 0
      AddressPrefix = "10.10.30.0/24"
      DNS = @("192.168.80.10")
      Gateways = "10.10.30.1"
      PoolStart = "10.10.30.100"
      PoolEnd = "10.10.30.199"
      IsPublic = $false
    }
 )
},
@{
 #This is used for onboarding Gateway
  Name = "GREVIP"
                                    # Don't change this. There should be no LN with this name in VMM
  Subnets = @(
    @{
      VLANID = 0
      AddressPrefix = "10.10.40.0/24"
```


```
DNS = @("192.168.80.10")
       Gateways = "10.10.40.1"
       PoolStart = "10.10.40.100"
       PoolEnd = "10.10.40.199"
       IsPublic = $false
     }
   )
 }
 @{
   #if Management VM Network is not deployed give the ManagementVMNetwork information. Skip
   # this if you already have this created.
   Name = "NC_Management"
   Subnets = @(
     @{
       # VLANID = 811
       VLANID = 0
       AddressPrefix = "192.168.80.0/24"
       DNS = @("192.168.80.10")
       Gateways = "192.168.80.1"
       PoolStart = "192.168.80.230"
       PoolEnd = "192.168.80.254"
       ReservedIPset = "192.168.80.230"
                                               #This IP will be used for NC Rest API
     }
   )
 }
)
# The following set of paremeters are required for importing VMM service Template,
# configuring the Service Template and Deploying the service Template.
# Make this true if self signed certificate is to be used
# Example : $True , $False
IsCertSelfSigned = $true
#The password for server certificate. This sertificate will be installed on the Host
ServerCertificatePassword="Passw0rd!"
# The following are service settings required for configuring and
# deploying the service template imported client security Group Name
ClientSecurityGroupName= "SDNcloud\Network Controller Users"
# Local Admin credentials
# The local admin user name will be .\Administrator
LocalAdminPassword= "Passw0rd!"
# Management Domain Account Which will be used for NC Deployment
ManagementDomainUser="SDNcloud\FabAdmin"
ManagementDomainUserPassword="Passw0rd!"
# This is the domain which NC VMs will join
ManagementDomainFDQN="SDNcloud.local"
#Managemet Security Group Name
ManagementSecurityGroupName="SDNcloud\Network Controller Admins"
# Prefix to be added to infrastructural VMs created. Put the prefix such
# that it makes VM name unique as this is the machine name of VM and should be unique.
ComputerNamePrefix = "SDN"
# RestName = "SDN-NCREST.SDNcloud.local"
RestName = "192.168.80.230"
```



Deoloyment Control Switches # Do you want to deploy NC # DeployNC = \$false DeployNC = \$true #Do you want to create NC managed HNVPA and Transit networks. #These are required if SLB and GW needs to be deployed # createNCManagedNetworks = \$false createNCManagedNetworks = \$true #Do you want to Deploy SLB. Values are \$true , \$false # DeploySLB = \$true DeploySLB = \$false #Do you want to deploy GW. Values are \$true , \$false # DeployGW = \$true DeployGW = \$false };);

7.1 Schrittweises Deployment der SDN-Komponenten

Ich habe bereits erwähnt, dass die Datei *Fabricconfig.psd1* auch Schalter zur Steuerung der von *VMMExpress.ps1* durchzuführenden Aktionen enthält. Ich werde dies für das Deployment unserer SDN Lab-Umgebung nutzen.

Ich sehe damit den Riesenvorteil, dass man jede Komponentenkategorie separat ausrollen und validieren kann. So kann man z.B. vor der Installation der Software Load Balancer sicherstellen, dass die Netzwerk Controller Umgebung korrekt arbeitet und die Netzwerkvirtualisierung mit dem VXLAN-Protokoll funktioniert.

Folgende Schalter stehen zur Verfügung. Sie finden Sie am Ende der Datei Fabricconfig.psd1:

DeployNC = \$true | \$false

Durch Angabe von *\$true* weisen Sie das Skript an, die Netzwerk Controller Instanzen zu erzeugen. Ändern Sie diesen Wert auf *\$false*, wenn Sie nach einer erfolgreichen Installation des Netzwerk Controllers nur die Software Load Balancer bzw. Gateway Instanzen erzeugen wollen.

createNCManagedNetworks = \$true | \$false

Durch Angabe von *\$true* werden durch *VMMExpress.ps1* die für die SDN-Umgebung notwendigen logischen Netze wie *HNVPA*, *Transit*, *PublicVIP*, *GREVIP* und *PrivateVIP* im VMM erzeugt und an die SDN-Switches in den Hyper-V Hosts verteilt. Diese Netze müssen vorhanden sein, um die SLB und Gateway Komponenten erzeugen zu können.

DeploySLB = \$false | \$true

Damit legen Sie fest, dass die Software Load Balancer Komponenten erzeugt werden. Wenn Sie *\$true* angeben, muss sichergestellt sein, dass zuvor der Netzwerk Controller und die logischen SDN-Netze erfolgreich erzeugt wurden.

DeployGW = \$false | \$true



Damit legen Sie fest, dass die Gateway Komponenten erzeugt werden. Wenn Sie *\$true* angeben, muss sichergestellt sein, dass zuvor der Netzwerk Controller, die logischen SDN-Netze sowie die SLB-Komponenten erfolgreich erzeugt wurden.

8 Starten des SDN-Deployments

Wenn Sie die Konfigurationsdatei *Fabricconfig.psd1* mit den zu Ihrer Umgebung passenden Parametern erstellt haben, speichern Sie diese im gleichen Verzeichnis wie das Skript *VMMExpress.ps1* mit einem passenden Namen, z.B. für unsere Lab-Umgebung unter *Fabricconfig-SDNcloud-Production.psd1*.

Dann können Sie das SDN-Deployment mit folgendem Aufruf in einer Powershell Konsole starten:

.\VMMExpress.ps1 -ConfigurationDataFile .\Fabricconfig-SDNcloud-Production.psd1

Tipp: Laden Sie *VMMExpress.ps1* in ein PowerShell ISE Fenster und arbeiten Sie im Debug Modus. Ich werde gleich darauf zurückkommen.

9 Erfahrungen, Tipps und Tricks

9.1 Hyper-V Switch Deployment

In den meisten Fällen kann die Logik in *VMMExpress.ps1* verwendet werden, um in den Hyper-V Hosts einen SDN-kompatiblen Switch zu erzeugen. Dieser wird mit SET (Switch Embedded Teaming) angelegt. Das Skript prüft dazu die in den Hyper-V Hosts vorhandenen physischen Netzwerkadapter und bindet den SDN-Switch an den ersten Adapter, der im Trunk Mode mit dem physischen Netz verbunden ist und dem noch kein logisches Netz zugeordnet ist.

Skript-Ausschnitt Zeile 738:



Wird kein geeigneter Adapter gefunden (<u>\$NetworkAdapter.count -eq 0</u>), gibt das Skript eine Warnung aus. In diesem Fall müssen Sie den logischen SDN-Switch über die VMM-Konsole selbst erzeugen und an die Hyper-V Hosts verteilen.

Ebenso müssen Sie den logischen SDN-Switch selbst erzeugen, wenn Sie SET nicht verwenden wollen (z.B. weil keine geeigneten Netzwerkadapter vorhanden sind oder weil Sie mit "klassischem" Teaming auf Betriebssystemebene in den Hyper-V Hosts arbeiten wollen).

Anmerkung: SET in Verbindung mit geeigneter Hardware bringt zwar deutliche Performance Vorteile, ist aber keine zwingende Voraussetzung für SDN!

Selbst erzeugte Hyper-V Switches müssen vor dem Start von VMMExpress.ps1 definiert und verteilt sein. Setzen Sie in diesem Fall in der Konfigurationsdatei Fabricconfig.psd1 dann folgende Werte:





#if above is true give the name of ManagementVMNetwork ManagementVMNetwork = " NC_Management "

#Uplink Port Profile to be used UplinkPortProfile = "HV Uplink Port"

9.2 REST IP

Wenn Sie die *Production* Variante des Netzwerk Controllers ausrollen wollen, müssen Sie für die REST API des NC eine IP-Adresse in der Konfigurationsdatei angeben. Diese muss eine Adresse aus dem IP-Pool für das Management Netz sein und darf nicht für andere Zwecke verwendet werden. Geben Sie in der Definition für das Managementnetz diese IP-Adresse beim Parameter *ReservedIPset* an:

ReservedIPset = "192.168.80.230"

oder über die VMM Konsole:

3 NC_Management_IPAd	dressPool_0 Properties	×
Name	IP address range	
Network Site	Specify the range of IP addresses from the subnet to be managed by this pool. IP subnet: 192.168.80.0/24	
IP address range	Starting IP address: [192.168.80.230	
Gateway	Enging IP address: 192.168.80.254	
DNS	Iotal addresses: 25	
WINS	VIPs and reserved IP addresses You can specify one or more IP addresses from the address range in the IP subnet to use for creating virtual IP (VIP) addresses or to reserve for other ourcoses. Use commas to separate multiple IP address	ses.
Inactive Addresses	Ranges in the format IP1-IP2 are allowed.	
	ID addresses to be recorded for other user:	
	192.168.80.230	
View Script	OK Cance	I

Damit ist sichergestellt, dass der VMM diese Adresse nicht einem anderen Objekt zuweisen kann.

In der Konfigurationsdatendatei geben Sie dann diese Adresse beim Parameter RestName an:

RestName = "192.168.80.230"

Beim Erzeugen der NC VMs wird dann von *VMMExpress.ps1* diese Adresse für die REST API des NC Guest Clusters konfiguriert.

Bitte verwenden Sie keinen DNS-Namen; dies wird im Deployment für unsere Lab-Umgebung nicht unterstützt.

Wenn Sie für das NC Deployment die *Standalone* Variante definiert haben, werden diese Angaben ignoriert. Als IP-Adresse für die REST API wird dann direkt die IP-Adresse der NC VM verwendet.

9.3 Undo Funktion

VMMExpress.ps1 hat eine eingebaute *Undo*-Funktion, die aufgerufen wird, wenn während der Ausführung des Skripts ein Fehler auftritt. Sie sorgt dafür, dass alle zuvor angelegten Objekte in der richtigen Reihenfolge wieder aus dem VMM entfernt werden. Das funktioniert aber nur, solange der Netzwerk Controller noch nicht im VMM als Netzwerk Service registriert ist. Danach müssen Sie manuell die Umgebung wieder bereinigen. Hilfe dazu erhalten Sie in der <u>Technet-Library</u>.



Tipp: Führen Sie *VMMExpress.ps1* im Debug Modus aus und setzen Sie einen Breakpoint auf den Start der *UndoNCDeployment*-Funktion (ab Zeile 513). Dann können Sie im Fehlerfall die einzelnen Schritte beim Beseitigen fehlerhafter Objekte genauer mitverfolgen und gegebenenfalls manuell eingreifen.

for effective and NCD and a most	
tunction undoinclueployment	
{	
param([Object] <mark>\$node</mark>)	
if (\$NetworkControllerOnBoarder -eq \$false)	

9.4 VMMExpress im Debugger ausführen

Im Zusammenhang mit der *Undo*-Funktion von *VMMExpress.ps1* habe ich Ihnen gerade empfohlen, *VMMExpress.ps1* im Debug Modus der PowerShell ISE auszuführen. Nach meiner Erfahrung hat dies den Vorteil, dass man die einzelnen Schritte bzw. Funktionsblöcke genauer mitverfolgen kann. *VMMExpress.ps1* arbeitet intern mit den CmdLets des PowerShell Moduls für den Virtual Machine Manager. Diese CmdLets starten jeweils einen *Job* im VMM Server, was im *Job*-Fenster der VMM-Konsole mitverfolgt werden kann.

Der folgende Screenshot zeigt eine Situation, als während des Erzeugens der VMs für den Netzwerk Controller ein Problem im Hyper-V Cluster auftrat (Zeile 505 in *VMMExpress.ps1*).

History					-				م
3		Name	Status	Ŧ	Start Time	÷	Result Name	Owner	Ŧ
	0	Refresh a Service Instance	Complet	ed	09.07.2018 18:47:42		NC	sdncloud\VMM-SVC	*
	8	Create Service Instance	Failed		09.07.2018 18:45:33		NC	sdncloud\FabAdmin	
	0	Set Global Setting	Complet	ed	09.07.2018 18:44:12		RestEndPoint	sdncloud\FabAdmin	
	Ø	Set Global Setting	Complet	ed	09.07.2018 18:43:42		ServerCertificatePassword	sdncloud\FabAdmin	
	0	Set Global Setting	Complet	ed	09.07.2018 18:43:41		MgmtSecurityGroup	sdncloud\FabAdmin	
	Ø	Set Global Setting	Complet	ted	09.07.2018 18:43:40		MgmtDomainFQDN	sdncloud\FabAdmin	
	Ø	Set Global Setting	Complet	ted	09.07.2018 18:43:40		MgmtDomainAccountPass	sdncloud\FabAdmin	
	0	Set Global Setting	Complet	ted	09.07.2018 18:43:39		MgmtDomainAccountName	sdncloud\FabAdmin	
	0	Set Global Setting	Complet	ted	09.07.2018 18:43:39		MgmtDomainAccount	sdncloud\FabAdmin	
	0	Create new RunAs Account	Complet	ted	09.07.2018 18:43:38		NC_MgmtAdminRAA	sdncloud\FabAdmin	
	0	Set Global Setting	Complet	ed	09.07.2018 18:43:38		LocalAdmin	sdncloud\FabAdmin	
	0	Create new RunAs Account	Complet	ed	09.07.2018 18:43:38		NC_LocalAdminRAA	sdncloud\FabAdmin	
	0	Set Global Setting	Complet	ed	09.07.2018 18:43:37		ClientSecurityGroup	sdncloud\FabAdmin	
 VMs and Services Fabric Library Jobs Settings 	St Cc Re St Du	Create Service Instance atus: Failed ommand: New-SCService sult name: NC arted: 09.07.2018 18:45: uration: 00:01:51 wner: sdncloud\FabAdm	33 nin	Second Seco	was not successfully deplo ons. d Action nt can be restarted by retry t complete the request. T	ing The	I. Review the event log to dete the job. connection to the agent '*' wa	rmine the cause and	
		Dataila Charrie Tra	-						
	I Sur	mmary Details Change Irac	cking						

Oftmals können Sie die Ursache des Problems sofort beheben und dann einen Restart des fehlgeschlagenen Jobs versuchen (im Kontextmenü des Jobs).





Ich empfehle Ihnen an folgenden Stellen Breakpoints zu setzen und dann die jeweiligen Befehle im Einzelschrittmodus auszuführen:

NC Deployment

Funktion OnBoardNetworkController Zeile 252:

An dieser Stelle können Sie den Connection String für die REST API des Netzwerk Controllers in der Variablen <u>\$ConnectionString</u> überprüfen.

Funktion *importServiceTemplate* Zeile 359:

Dies wäre eine geeignete Stelle, um über den Service Designer in das importierte NC Service Template noch eine eigene *Unattend.xml* einzubringen. Achtung: Der VMM erzeugt selbst eine *Unattend.xml* Datei und mischt sie mit der angegebenen benutzerspezifischen Variante später beim Kreieren der VMs zusammen.

Funktion *configureAndDeployService* Zeile 467:

if(\$ServiceUpdate.deploymenterrorlist -ne \$null)

Überprüfen Sie, ob die Variable wirklich *snull* enthält. Nur dann war die Verteilung der NC VMs auf die Hyper-V Hosts erfolgreich und das Skript kann weiterlaufen. Korrigieren Sie gegebenenfalls das Placement der VMs über den Service Designer in der VMM-Konsole und weisen der Variablen den Wert *snull* zu.

Funktion configureAndDeployService Zeile 505:

\$sc= New-SCService -ServiceConfiguration \$ServiceConfig

Hier können Sie im Service Designer der VMM-Konsole nochmals alle Parameter zum Erzeugen der NC VMs überprüfen.

• SLB Deployment

Funktion *ImportSLBServiceTemplate* Zeile 878:

Dies wäre eine geeignete Stelle, um über den Service Designer in das importierte SLB Service Template noch eine eigene *Unattend.xml* einzubringen. Achtung: Der VMM erzeugt selbst eine *Unattend.xml* Datei und mischt sie mit der angegebenen benutzerspezifischen Variante später beim Kreieren der VMs zusammen.

Funktion *ConfigureAndDeploySLBService* Zeile 917:

if(\$ServiceUpdate.deploymenterrorlist -ne \$null)

Überprüfen Sie die Variable wieder, ob sie *sull* enthält und korrigieren Sie eventuell das Placement der VMs.

Funktion *ConfigureAndDeploySLBService* Zeile 937:

Hier können Sie im Service Designer der VMM-Konsole nochmals alle Parameter zum Erzeugen der SLB VMs überprüfen.

• Gateway Deployment

Funktion *importGatewayTemplate* Zeile 1050:



Dies wäre eine geeignete Stelle, um über den Service Designer in das importierte Gateway Service Template noch eine eigene *Unattend.xml* einzubringen. Achtung: Der VMM erzeugt selbst eine *Unattend.xml* Datei und mischt sie mit der angegebenen benutzerspezifischen Variante später beim Kreieren der VMs zusammen.

Funktion *ConfigureAndDeployGatewayService* Zeile 1091:

if(\$ServiceUpdate.deploymenterrorlist -ne \$null)

Überprüfen Sie die Variable wieder, ob sie *\$null* enthält und korrigieren Sie eventuell das Placement der VMs.

Funktion ConfigureAndDeployGatewayService Zeile 1112:

Hier können Sie im Service Designer der VMM-Konsole nochmals alle Parameter zum Erzeugen der Gateway VMs überprüfen.



10 Post NC Deployment Schritte und Validierung

Wenn Sie das Skript *VMMExpress.ps1* erfolgreich ausgeführt haben, finden Sie zwar alle SDN-Komponenten als virtuelle Maschinen und Services im VMM (der folgende Screenshot zeigt unsere vollständige LAB-Umgebung).

8	Cluster Tools	Virtual Machine Tools	Administrator - SUP	N-VMMUL.sdn	loud.local - Virtua	I Machine Manager			- 0	×
F Home Folder	Host Cluster	Virtual Machine								^
Create Create Virtual Service Create Create Create Create Virtual Create	Create Host Group	Create VM Network	Overview VMs	Services VN Netw	Power	Shell				
VMs and Services	< \	/Ms (9)	30	low	, windo	w				
ch Tanada										٩
() Tenants		Name	Sta	atus 👻 Virtu		Cloud Job St	atus	▼ Owner ▼	Service	Operati
a Clouds	-	SDN-NCVM01.SDN	Icloud.local Ru	nning Runr	ing sdn-hv04	Comple	ted	sdncloud	NC	Windows
🚰 Azure Subscriptions		b SDN-NCVM02.SDN	icloud.local Ru	nning Runr	ing SDN-HV02	. Comple	ted	sdncloud	NC	Windows
🚢 VM Networks		SDN-NCVM03.SDN	Icloud.local Rui	nning Runr	ing SDN-HV01	Comple	ted	sdncloud	NC	Windows
🔁 Storage		腸 SDN-MUXVM02.SE	Ncloud.local Ru	nning Runr	ing SDN-HV03	Comple	ted	sdncloud	Software	Windows
4 🤭 All Usets		腸 SDN-MUXVM01.SE	Ncloud.local Ru	nning Runr	ing SDN-HV03	Comple	ted	sdncloud	Software	Windows
All Hosts		腸 SDN-MUXVM03.SE	Ncloud.local Ru	nning Runr	ing SDN-HV02	. Comple	ted	sdncloud	Software	Windows
A B SDN-HVCL		SDN-GW-VM01.SD	Ncloud.local Ru	nning Runr	ing SDN-HV01	Comple	ted	sdncloud	Gateway	Windows
SDN-HV01		SDN-GW-VM03.SD	Ncloud.local Ru	nning Runr	ing SDN-HV03	Comple	ted	sdncloud	Gateway	Windows
SDN-HV02		SDN-GW-VM02.SD	Ncloud.local Ru	nning Runr	ing SDN-HV02	2 Comple	ted	sdncloud	Gateway	Windows
🕈 sdn-hv04										
	_	SDN-NCVM03.SDI	Ncloud.local							*
		Virtual machine info	rmation	Logica	I networks		Recent jol	b		
		Status: Run	ning	NC_M	inagement		Name:	Refresh virtual ma	chine	
w VMs and Services		Owner: sdn Processors: 4	cloud\FabAdmin	Netwo	rk adapters		Job status:	100 % Completed		
Fabric		Memory: 4,00	GB	00:1D:0	8:B7:1C:24: 192.1	68.80.233				
🧮 Library										
🛅 Jobs		Go to related object	:	Storag	e (1 disks)		Daily perf	ormance (CPU)		
Settings		Host: SDN-HV01.so	dncloud.local	Total st	orage (80,00 GB):				Average	
	_	Service: NC					20			
				40%	ad .					

Damit ist aber die SDN-Konfiguration noch nicht abgeschlossen. Vielmehr sind für die einzelnen SDN-Komponenten noch manuelle Schritte notwendig. Und was natürlich nicht fehlen darf, ist das Durchspielen einiger Testszenarien.

10.1 Tenant Testumgebungen

Wenn der Netzwerk Controller (*Standalone* Variante) bzw. das NC Guest Cluster (*Production* Variante) ausgerollt und als Netzwerk Service im VMM registriert sind, sollten Sie als nächstes 2 Tenant Testumgebungen anlegen. Jede Tenant Umgebung enthält ein *VM Network* mit jeweils 2 Subnetzen. In jedem Tenant *VM Network* gibt es dann jeweils 2 VMs.

10.1.1 Tenant VM Netze

• Erzeugen Sie 2 Tenant VM Netzwerk Umgebungen (*"Red VMNet"* und *"Green VMNet"*) mit identischen Netzwerkdefinitionen:

```
Subnetz 0: "Red VMnet_0" bzw. "Green VMnet_0" – 192.168.0.0/24
IP-Pool 0: "Red IP Pool 0" bzw. "Green IP Pool 0" – 192.168.0.4 - 192.168.0.254
Gateway in den IP Pools: jeweils 192.168.0.1
```

Subnetz 1: *"Red VMnet_1"* bzw. *"Green VMnet_1"* – 192.168.1.0/24 IP-Pool 1: *"Red IP Pool 1"* bzw. *"Green IP Pool 1"* – 192.168.1.4 - 192.168.1.254 Gateway in den IP Pools: jeweils 192.168.1.1



DNS in allen IP Pools: 192.168.80.10 (der Standard DNS-Server in unserer Lab-Umgebung auf dem System SDN-DC01

Sie können dies über die VMM-Konsole oder mit dem weiter unten folgenden PowerShell Skript erledigen.

VMM-Konsole

Klicken Sie im VMM Arbeitsbereich *VMs and Services* mit der rechten Maustaste auf die Kategorie *VM Networks* und wählen Sie im Kontextmenü *Create VM Network.*

Clouds	Name
	GREVIP
Azure Subscriptions	L NC_Management
L VM Networks	
] Storage	Create VM Network

Geben Sie den Namen des anzulegenden VM Netzwerks an und achten Sie darauf, dass in der Klappliste *Logical Network* das HNVPA Netz ausgewählt ist. Klicken Sie auf *Next*.

🌯 Create VM Networ	k Wizard		×
🌲 Name			
Name Isolation VM Subnets Connectivity Summary	Specify a nan Name: Description: Logical network:	ne and description for the VM network	
		Previous	Next Cancel

Lassen Sie im Dialogfenster *Isolation* die Voreinstellung *Isolate using Hyper-V network virtualization* und klicken Sie auf *Next*.





Tragen Sie im Dialogfenster *VM Subnets* die Parameter für die beiden Subnetze ein. Klicken Sie dann wieder auf *Next*.

Name	Specify VM subnets				
VM Subnets	🔛 Add 📼 Remove				
Connectivity	Green VMnet_0 192.168.0.0/24	VM subnet			
Summary	Green VMnet_1 192.168.1.0/24	Give a name to the IP subnet to be virtualized by the VM Network. Enter IP subnets using CIDR notation, for example: 192.168.1.0/24, FD4A:29CD:184F:3A2C::/64. Name:			
		Green VMnet_1			
		Subnet:			

Im Dialog Connectivity lassen Sie die Voreinstellungen und klicken auf Next.



Name	Connectivity					
solation	By default, network virtualizati	on provides an isolated network. Select the options below to add external				
/M Subnets	Connect to another netwo	de through a VPN tunnel				
Connectivity	Enable Border Gateway	/ Protocol (BGP)				
Summary	Connect directly to an additional logical network Direct routing Network address translation (NAT)					
	Select the gateway device to u	se for this connection.				
	Gateway Device: Network Co	ntroller 🧧				
	Device capabilities:	Site to Site VPN Border Gateway Protcol (BGP) Direct routing				
	Remaining capacity:	50 VM networks 250 VPN tunnels				

Sie sehen nun eine Zusammenfassung Ihrer Eingaben.

Create VM Network	Wizard		
Name	Confirm the setting	5	View Script
VM Subnets Connectivity	Name: Description: Border Gateway Protoc	Green VMNet	
Summary	Direct routing:	Disabled	
	·	Pre	vious Finish Cancel

Durch einen Klick auf *Finish* können Sie nun das Anlegen des VM Networks starten. In der *Job*-Liste des VMM können Sie das mitverfolgen.



ant yous (s)					
Name	Status	7	Start Time	7	Result Name
Create VM Subnet	Completed		16.07.2018 14:31:49		Green VMnet_1
Create VM Subnet Create VM Subnet	Completed Completed		16.07.2018 14:31:49 16.07.2018 14:31:46		Green VMnet_1 Green VMnet_0

Nun müssen Sie für jedes Subnetz noch den zugehörigen IP Pool anlegen.

Klicken Sie mit der rechten Maustaste auf das soeben erzeugte VM Network (*Green VMnet*) und wählen Sie im Kontextmenü die Aktion *Create IP Pool*.

	🖂 🚢 Green VMnet	
Azure Subscriptions		Create IP Pool
J VM Networks		Stroperties
		X Delete
storage		View Dependent Resources

Geben Sie den Namen des IP Pools an. Stellen Sie sicher, dass im Feld *VM network* das richtige Tenant VM-Netz und im Feld *VM Subnet* das gewünschte Subnetz ausgewählt sind. Klicken Sie dann auf *Next*.

lame	Specify the	e IP address pool name and VM subnet	
P address range Gateway	Enter the nam want to make	te of the IP address pool and select the VM network and then the VM subne the pool available.	et to which you
ONS	Name:	Green IP Pool 0	
VINS	Description:		
ummary			
	VM network:	Green VMnet	Browse
	VM subnet:	Green VMnet_0 (192.168.0.0/24)	

Die im Dialog *IP address range* angezeigten Werte können Sie für unsere Test-Umgebung durch einen Klick auf Next übernehmen.



Name	IP address range
P address range	Specify the range of IP addresses from the subnet to be managed by this pool.
Jateway	IP subnet: 192.168.0.0/24 Starting IP address: 192.168.0.4
vins Vins iummary	Ending IP address: 192.168.0.254 Total addresses: 251
	VIPs and reserved IP addresses You can specify one or more IP addresses from the address range in the IP subnet to use for creating virtual IP (VIP) addresses or to reserve for other purposes. Use commas to separate multiple IP addresses. Ranges in the format IP1-IP2 are allowed.
	IP addresses reserved for load balancer VIPs:

Geben Sie im Gateway Dialog die Adresse des jeweiligen Gateways ein und klicken Sie auf Next.

Create Static IP Addre	ess Pool Wizard			
🧱 Gateway	Specify default gateway a	ddresses		
P address range Gateway	Gateway addresses must belong t Default gateways:	o the range between 192.168.0.1 and 19	2.168.0.254.	
INS	Gateway Address	Metric		Insert
	192.168.0.1	Automatic	*	Delete
ann na y				
		Previous	Next	Cancel

Im *DNS* Dialog geben Sie die Adresse des DNS-Servers unserer Lab-Umgebung (192.168.80.10) ein und klicken auf *Next*.



lame ^D address range	Specify one or more DNS servers	
lateway	DNS Server Address	Insert
DNS	192.168.80.10	Delete
INS		Move Up
immary	Connection specific DNS suffix: Enter DNS suffix	Move Down
	DNS search suffixes to append (in order):	
	DNS Suffix	Insert
		Delete
		Move Up
		Mous Down

Den *WINS* Dialog können Sie mit *Next* überspringen. Überprüfen Sie in der Zusammenfassung nochmals Ihre Eingaben und klicken Sie dann auf *Finish*, um den IP Pool zu erstellen.

Vame	Confirm the settings		Mary Carlos
P address range			view script
iateway	Name:	Green IP Pool 0	
102.07 4 102	Description:		
INS	IP subnet:	192.168.0.0/24	
VINS	IP address range:	192.168.0.4-192.168.0.254	
umman/	Connection specific DNS	suffix:	
dividity	Network routes:	0 Network routes	
	Gateways:	1 Gateways	
	DNS servers:	1 DNS servers 0 DNS suffixes	
	WINS servers:	0 WINS servers	

In der VMM Jobliste können Sie den Vorgang wieder mitverfolgen.

0	Create static IP address pool	Completed	16.07.2018 14:33:30	Green IP Pool 1
0	Create static IP address pool	Completed	16.07.2018 14:33:29	Green IP Pool 0
0	Create VM Subnet	Completed	16.07.2018 14:33:26	Green VMnet_1
0	Create VM Subnet	Completed	16.07.2018 14:33:24	Green VMnet_0
0	Create VM Network	Completed	16.07.2018 14:33:22	Green VMnet



Erzeugen Sie analog die IP Pools für die anderen Subnetze der Tenants.

PowerShell

Etwas schneller und komfortabler geht das Ganze mit dem nachstehenden PowerShell Skript. Weisen Sie der Variablen <u>\$tenantname</u> den gewünschten Tenant Namen zu und starten das Skript in einer PowerShell Sitzung mit Administrator Rechten.

Create VM network for tenant
\$tenantname = "Red"
\$tenantname = "Green"
Ścubpet0 – "192 168 0 0/24"
Subleto = 152.100.0/24
\$1PrangeEnd() = "102.100.0.4"
SiPrangeendu = 192.168.0.254
Şgatewayû = 192.168.0.1
\$subnet1 = "192.168.1.0/24"
\$IPrangeStart1 = "192.168.1.4"
\$IPrangeEnd1 = "192.168.1.254"
\$gateway1 = "192.168.1.1"
\$DNSserver = "192.168.80.10"
<pre>\$logicalNetwork = Get-SCLogicalNetwork -Name "HNVPA"</pre>
tenant VM net
SymNetwork = New-SCV/MNetwork -Name "Stenantname VMnet" `
JoricalNetwork ClagicalNetwork IcolationType "WindowsNetworkVirtualization"
-CAIPAddressPoolType "IPV4" -PAIPAddressPoolType "IPV4"
tenant subnets
<pre>\$subnetVLan0 = New-SCSubnetVLan -Subnet \$subnet0</pre>
<pre>\$VMsubnet0 = New-SCVMSubnet -Name "\$tenantname VMnet_0" `</pre>
-VMNetwork \$vmNetwork -SubnetVLan \$subnetVLan0
\$subnetVLan1 = New-SCSubnetVLan -Subnet \$subnet1
\$VMsubnet1 = New-SCVMSubnet -Name "Stenantname VMnet 1" `
-VMNetwork \$vmNetwork -SubnetVLan \$subnetVLan1
VMnet_0
Gateways
\dot{s}
SallGateways += New-SCDefaultGateway -IPAddress Sgateway0 -Automatic
DNS servers
$\frac{1}{2} \sum_{i=1}^{n} \frac{1}{2} \sum_{i=1}^{n} \frac{1}$
DNS cuffixoc
fallDracuffiyes - @()
SaliDISSuffixes = @()
\$allWinsServers = @()
New-SCStaticIPAddressPool -Name "\$Tenantname IP Pool 0" -VMSubnet \$VMsubnet0 ` -Subnet \$subnet0 -IPAddressRangeStart \$IPrangeStart0 -IPAddressRangeEnd \$IPrangeEnd0 ` -DefaultGateway \$allGateways -DNSServer \$allDnsServer -DNSSuffix "" ` -DNSSearchSuffix \$allDnsSuffixes
VMnet_1
Gateways
$\hat{s}_{allGateways} = \omega()$
SallGateways += New-SCDefaultGateway -IPAddress Scateway1 -Automatic
DNS convers



\$allDnsServer = @(\$DNSserver)
DNS suffixes
\$allDnsSuffixes = @()
WINS servers
\$allWinsServers = @()
New-SCStaticIPAddressPool -Name "\$Tenantname IP Pool 1" -VMSubnet \$VMsubnet1`
-Subnet Subnet1 - IPAddressRangeStart SIPrangeStart1 - IPAddressRangeEnd SIPrangeEnd1
-DefaultGateway SallGateways -DNSServer SallDnsServer -DNSSuffix ""
-DNSSearchSuffix \$allDnsSuffixes

Den Ablauf des Skripts können Sie wieder über die Jobliste im VMM verfolgen. Als Ergebnis erhalten Sie dann das jeweilige Tenant VM Netzwerk einschließlich der IP Pools.

	🗆 🚢 Green VMnet			
Azure Subscriptions	🚟 Green IP Pool 0	192.168.0.0/24		
🚢 VM Networks	🚟 Green IP Pool 1	192.168.1.0/24		
	🗆 🚢 Red VMnet			
	ared IP Pool 0	192.168.0.0/24		
	a Red IP Pool 1	192.168.1.0/24		

10.1.2 Tenant Test VMs

Erzeugen Sie für jeden der beiden Tenants 2 VMs und verbinden Sie diese wie folgt mit den Subnetzen der beiden VM Netze:

• Red-VM01 – verbunden mit Subnetz 0 von VM Netzwerk Red VMnet

Red-VM01 Properties			×
General	🔚 Save As 🛛 🖷 New 🗙 Remo	ve	
Status	General Processor	Metwork Adapter 1	
Hardware Configuration	2 processors	Connectivity	
Hardware Conliguration	2048 MB	Connected to a VM netwo	ırk
Checkpoints	* Bus Configuration	VM network: Red VM	net Browse
Custom Properties	SCSI Adapter 0 2 Devices attached	VM subnet: Red VM	Inet_0 Y
Settings	WS2016_EN.vhdx 80,00 GB, ID 0	Enable VLAN	v
Actions	Advanced Virtual DVD drive No Media Captured	IP address Dynamic IP	
Servicing Windows	* Network Adapters	Static IP (from a static IP p	lool)
Dependencies	Network Adapter 1 Connected to NC_Lo	MAC address Dynamic	
Validation Errors	Fibre Channel Adapters Advanced	Static: 00:1D:D	8:B7:1C:37
Access	Integration Services Some services offered	Virtual switch Logical Switch	
Ch	Checkpoints	Logical switch: NC_Log	gicalSwitch v

analog:

- Red-VM02 verbunden mit Subnetz 1 von VM Netzwerk Red VMnet
- Green-VM01 verbunden mit Subnetz 0 von VM Netzwerk Green VMnet
- Green-VM02 verbunden mit Subnetz 1 von VM Netzwerk Green VMnet

Installieren Sie in jeder dieser VMs die Serverrolle *Web Server* mit Standardeinstellungen. Modifizieren Sie anschließend das Bild der IIS-Startseite – Datei *iisstart.png* im Verzeichnis *C:\inetpub\wwwroot* – so dass sie den Namen der VM zeigt, z.B.



H Windows Server Red-VM01	H Windows Server Green-VM01
H Windows Server Red-VM02	H Windows Server Green-VM02

Tipp: Das können Sie ganz einfach mit Paint aus dem Windows Zubehör durchführen.

10.2 Validierung der Netzwerkisolation mit dem VXLAN-Protokoll

Nun können Sie folgende Szenarien zur Netzwerkisolation mit dem VXLAN-Protokoll durchspielen.

Melden Sie sich auf dem Tenant System *Red-VM01* an. Im Server Manager können Sie die zugewiesene IP-Adresse überprüfen:



Melden Sie sich jetzt auf dem Tenant System *Red-VM02* an. Der Server Manager wird Ihnen die Adresse 192.168.1.4 anzeigen. Starten Sie den Internet Explorer und geben Sie in die Adresszeile folgende Adresse ein: <u>http://192.168.0.4</u> – Ergebnis:

← <> Mttp://192.168.0.4/		오 - ৫ 🖉 IIS Windows Serv	er X		- 日 × 分☆戀ಅ
🕂 Windows Server Red-VN	01				
Internet Informa	tion Servi	ices			
Welcome Bien	venue Tervetulo	Da			
ょうこそ Benvenuto 歌迎	Bienvenido Ho	s geldiniz ברוכים הבאים		Welkom	
Bem-vindo	Καλώς ορίσατε Vä	ilkommen 환영합니다	Добро пожаловать Ц	Üdvözöljük	
Microsoft	Willkommen Ve	Ikommen	مرحبا Witamy		



Natürlich können Sie auch die umgekehrte Richtung wählen – vom System *Red-VM01* (192.168.0.4) aus die Startseite von *Red-VM02* (192.168.1.4) aufrufen. Entsprechend erhalten Sie:



Die gleichen Spielchen können Sie jetzt auch zwischen den Systemen im *Green-VMnet* ausführen. Sie werden immer nur die Systeme im gleichen VMnet erreichen, können aber nicht auf Systeme in anderen VM Netzen zugreifen.

Erkenntnisse:

Innerhalb eines Tenant VM Netzes werden IP-Pakete zwischen den definierten Subnetzen geroutet. Eine Verbindung zu Systemen in andere Tenant VM Netze ist jedoch nicht möglich, auch wenn die IP-Bereiche identisch sind oder sich überlappen.

10.3 Konfiguration der Load Balancer Service Instanzen

Vom Skript *VMMExpress.ps1* wurden zwar SLB Instanzen als VMs erzeugt. Diese müssen wir aber noch konfigurieren.

• Wechseln Sie in der VMM-Konsole in den *Fabric* Arbeitsbereich und markieren Sie die Kategorie *Network Service*. Klicken Sie mit der rechten Maustaste auf den Eintrag *Network Controller* und rufen die *Properties* auf.

Wechseln Sie in der VMM-Konsole in den *Fabric* Arbeitsbereich und markieren Sie die Kategorie *Network Service*. Klicken Sie mit der rechten Maustaste auf den Eintrag *Network Controller* und rufen die *Porperties* auf.



Fabric	< Network Services (2)				
Servers					
🔺 🚞 All Hosts	Name	Conne	ection String	Manufacturer	Model
🔺 🛄 SDN-Hosts	🗉 🤦 Network Contro	oller server	un i tau ta	14	100 24
SDN-HVCL	🗉 🔛 Load balance	er role	Vie Vie	w Dependent Reso	urces
Infrastructure	🖽 🚩 Gateway		😱 Ref	resh	
🖌 📥 Networking	👰 Microsoft Netw	ork Devic	eA 📼 Rer	move	
The Logical Networks			Prg	vperties	
📕 MAC Address Pools				~J	
🔛 Load Balancers					
VIP Templates					
开 Logical Switches					
Dort Profiles					
Nort Classifications					
🙎 Network Service					
A Storage					
Classifications and Pools					
Providers					
Arrays					
File Servers					
Fibre Channel Fabrics	Network Controller				
GoS Policies					
	Network service inf	formation			Host gi
	Name:	Network C	ontroller		All Host
w VMs and Services	Connection string:	serverurl=h C	ttps://192.16	8.80.230;servicenar	ne=N
😥 Fabric	Description:				

• Wechseln Sie in den *Network Controller Properties* auf die Registerkarte *Services* und markieren die *Load Balancer Role*.

Im Feld Associated Service wählen Sie über die Browse... Schaltfläche unseren Software Load Balancer Service aus.

Wählen Sie für das Feld *Run As Account* einen passenden Account aus (hier: *NC_MgmtAdminRAA*)

In das Feld *SLB Manager VIP* tragen Sie die letzte IP-Adresse aus dem vom Skript *VMMExpress.ps1* erzeugten IP-Pool des logischen Netzes *PrivateVIP* ein (hier also: 10.10.30.199).

Selektieren Sie außerdem in der Liste *SLBM VIP Pools* die IP Pools *PublicVIP_IPAddressPool_0* und *PrivateVIP_IPAddressPool_0*. Diese beiden IP Pools werden dann vom VMM dem SLB Manager zur Verfügung gestellt.



Manufacturer and Model Credentials Connection String Host Group Extensions Services	 Load balancer role 3 active nodes SDN-MUXVM01.S SDN-MUXVM03.S SDN-MUXVM02.S SDN-MUXVM02.S SDN-GW-VM02.S SDN-GW-VM03.S SDN-GW-VM01.S 	Service informatic Associated service: Run As account: SLB Manager VIP: SLBM VIP Pools: PrivateVIPIPAd GREVIPIPAddr PublicVIPIPAd Specify the IP addre Enter IP subnets us FD4A:29CD:184F:34 Datacenter network Destination Prefix	Software Load Balancer NC_MgmtAdminRAA 10.10.30.199 ddressPool_0 (10.10.30.100 - 1 essPool_0 (10.10.40.100 - 10.1 dressPool_0 (10.10.50.100 - 10 ess ranges to exclude from ou ing CIDR notation, for example A2C::/64. k addresses:	Browse Browse 0.10.30.199) 0.40.199) 0.40.199) 0.10.50.199) tbound NAT. e: 192.168.1.0/24, Add
				Remove

 Klicken Sie auf die erste SLB/MUX Instanz SDN-MUXVM01. Geben Sie in das Feld Local ASN eine für Ihre Umgebung geeignete ASN (Autonome System Nummer im Sinne des BGP-Protokolls) ein, hier 65001. Über die Add Schaltfläche fügen Sie nun die Daten des BGP-Routers ein, mit dem diese SLB-Instanz kommunizieren soll. Unser System SDN-DC01 soll ja der BGP-Router werden und er soll die ASN 65000 erhalten. Für die Kommunikation verwenden wir das Transit Netzwerk, in dem das System SDN-DC01 die IP-Adresse 10.10.20.1 besitzt.

Network Controller Properties	ies					Х
Name	Services					
Manufacturer and Model	Load balancer role 3 active nodes	SDN-MUXVN	/01.SDNcloud.lo	cal		
Credentials	SDN-MUXVM01.S	BGP settings	5001			
Connection String	SDN-MUXVM03.S	Provide a list	of devices to peer	with.		
Host Group		Name	IP Address	ASN	Add	
Extensions	SDIN-MUXVMU2.S	BGP	10.10.20.1	65000	Remove	
Services	Gateway manager role 3 active nodes					
	SDN-GW-VM02.S					
1	SDN-GW-VM03.S					
	SDN-GW-VM01.S					
View Script				O	K Cancel	

• Wiederholen Sie diese Schritte für die restlichen SLB-Instanzen



Property Property Network Controller Property	rties				:
Name	Services				
Manufacturer and Model Credentials Connection String Host Group	Load balancer role 3 active nodes SDN-MUXVM01.S SDN-MUXVM03.S	SDN-MUXVM02 BGP settings Local ASN: 6500, Provide a list of d	2 IP Address	cal with.	Add
Extensions Services	 SDN-MOXVMO2.S Gateway manager role 3 active nodes SDN-GW-VM02.S SDN-GW-VM03.S 	BGP	10.10.20.1	65000	Remove
View Script	SDN-GW-VM01.S			ОК	Cancel
Network Controller Proper Name	ties Services				;
Network Controller Proper Name Manufacturer and Model Credentials Connection String	ties Services Coad balancer role 3 active nodes SDN-MUXVM01.S	SDN-MUXVM03. BGP settings Local ASN: 65003	.SDNcloud.loo	cal	
Network Controller Proper Name Manufacturer and Model Credentials Connection String Host Group Extensions	tites Services Services Solution Soluti	SDN-MUXVM03. BGP settings Local ASN: 65003 Provide a list of d Name BGP	SDNcloud.lou a evices to peer IP Address 10.10.20.1	cal with. ASN 65000	Add Remove

Damit ist die Konfiguration der SLB Instanzen abgeschlossen.

10.4 Konfiguration des BGP Routers

Bei der Installation unseres Domain Controllers *SDN-DC01* haben wir unter anderem bereits die Serverrolle *RRAS* installiert, aber nicht weiter konfiguriert. Das werden wir nun nachholen, indem wir die BGP-Funktion dieser Serverrolle aktivieren. Dies muss über PowerShell Befehle geschehen.



Führen Sie auf dem *SDN-DC01* in einer PowerShell Sitzung mit Administratorberechtigung folgenden Befehl aus:

Add-BgpRouter -BgpIdentifier 10.10.20.1 -LocalASN 65000

Hiermit wird die BGP-Router Funktion aktiviert. Dabei wird auch die *lokale ASN* (*Autonome System Nummer*) des BGP-Routers festgelegt. Dies kann ein beliebiger Integer-Wert sein. Üblicherweise werden in SDN-Umgebungen ASNs ab 65000 verwendet, da diese nicht zu Konflikten mit ASNs physischer Geräte führen können. Diese sind typischerweise kleiner 65000.

Als *BgpIdentifier* geben wir die IP-Adresse des BGP-Routers an - in unserem Fall die Adresse des *SDN-DC01* im *Transit* Netz (also 10.10.20.1).

Jetzt können wir die *Peers* definieren, die sich mit dem BGP-Router verbinden und Routen austauschen können. Führen Sie für unsere Lab-Umgebung folgende PowerShell Befehle aus. Bitte vergleichen Sie vorher die Kombinationen *PeerASN / PeerIPAddress* mit den Parametern, die Sie bei der Konfiguration der SLB Service Instanzen festgelegt haben.



Warten Sie, bis sich alle *Peers* mit dem BGP-Router verbunden haben (*ConnectivityStatus* = *Connected*). Dies kann unter Umständen geraume Zeit dauern. Den Verbindungsstatus können Sie mit folgendem Kommando prüfen:

Get-BgpPee	r				
PS C:\Wir	ndows\system32>	Get-BgpPeer			
PeerName	LocalIPAddress	PeerIPAddress	PeerASN	OperationMode	ConnectivityStatus
MUX001 MUX002 MUX003	10.10.20.1 10.10.20.1 10.10.20.1	10.10.20.101 10.10.20.100 10.10.20.102	65001 65002 65003	Mixed Mixed Mixed	Connected Connected Connected

10.5 Validierung des Software Load Balancing

Um den Zugriff auf Tenant VMs mit Hilfe des Software Load Balancing in unserer Lab-Umgebung testen zu können, müssen wir öffentliche virtuelle Adressen (*PublicVIPs*) definieren.

10.5.1 Erstellen eines VIP Templates

In der VMM-Konsole erstellen wir zunächst ein VIP Template. Dazu wechseln Sie in den Fabric Arbeitsbereich, öffnen die Kategorie Networking und klicken mit der rechten Maustaste auf VIP Templates. Wählen Sie im Kontextmenü Create VIP Template.





Geben Sie einen Namen für das VIP Template ein (z.B. *Web VIP Template*) sowie die Ports, zwischen denen die Netzwerkdaten ausgetauscht werden sollen (hier: jeweils Port 80). Klicken Sie auf *Next*.

Name	Specify a nar	e and description for this template	
Type Protocol	A virtual IP temp traffic. The virtua balance.	ste contains load balancer-related configuration settin port is the port that is used for the type of network tra	gs for a specific type of network affic that you want to load
Persistence	Template name:	Web VIP Template	
Load Balancing Health Monitors	Description:		
Summary	Virtual IP port:	80	
	Backend port:	sol]	

Wählen Sie als Template Typ *Specific* und selektieren Sie in der *Manufacturer* Liste *Microsoft* sowie in der *Model* Liste *Microsoft Network Controller*. Klicken Sie auf *Next*.

Name	Specify a template type	
Type Protocol Persistence	Select the type of template to create that best matches your environment. Generic A generic template can be used on any supported load balancer. Specific	
Load balancing Health Monitors Summary	A virtual IP template can be used only on a load balancer of a specific manufacturer and model. Manufacturer: Microsoft Model: Microsoft Network Controller	



Im *Protocol* Dialog wählen Sie die Option *Custom* und geben als *Protokoll Name* den Text *TCP* ein. Klicken Sie wieder auf *Next*.

Name	Specify protocol options
Туре	
Protocol	Select the protocol for which you want to create the virtual IP template. If you select HTTPs, you must specify whether to terminate the HTTPS traffic at the load balancer or to pass it through to the virtual specific selection.
Persistence	О НТТР
.oad Balancing	O HTTPS passthrough
tealth Monitors	Passes through HTTPS traffic without decrypting at load balancers.
rear manual a	O HTTPS terminate
Summary	Terminates HTTPS traffic at load balancers.
	Certificate subject name:
	Re-Encrypt Re-encrypt HTTPS traffic from the load balancer to the server.
	Custom
	Protoco: nome,

Die Seite Persistance können wir direkt mit Next überspringen.

Auf der Seite *Load Balancing* wählen Sie aus der Liste *Load Balancing Method* den Eintrag *Round Robin* und klicken dann auf *Next*.

📳 Load balancer VIP ter	mplate Wizard			×
🔄 Load Ba	lancing			
Name Type Protocol	Specify a load balar Select one of the available Load balancing method:	load balancing method load balancing methods. Round Robin		
Persistence Load Balancing				
Health Monitors Summary				
			Previous	Cancel



Die Seite Health Monitors überspringen wir mit Next und gelangen auf die Summary Seite.

📰 Load balancer VIP tem	nplate Wizard			×
🧧 Summar	y			
Name	Confirm the setti	ngs		View Script
Protocol Persistence Load Balancing Health Monitors Summary	Name: Manufacturer: Model: Protocol: Persistence: Load balancing meti Health monitors:	Web VIP Template Microsoft Microsoft Network Controller Custom Persistence disabled nod: Round Robin 0 monitors		
			Previous Finish	Cancel

Nach dem Klick auf *Finish* wird nun das VIP Template angelegt.

📋 Jobs

Rece	ent Jobs (67)				
	Name	Status	 Start Time	*	Result Name
0	Create load balancer VIP template	Completed	17.07.2018 20:49:16		Web VIP Template

10.5.2 Erstellen einer öffentlichen virtuellen IP Adresse (*PublicVIP*) für ein Tenant VM Netz

Um eine *PublicVIP* für eines unserer *Tenant VM Netze* zu erstellen, müssen wir wieder die PowerShell verwenden. Führen Sie folgendes Skript aus:

param(





[Parameter(Mandatory=\$false)] # The name of the VIP template you created via the VMM Console. \$VipTemplateName = "Web VIP Template",
<pre>[Parameter(Mandatory=\$false)] # Arbitrary but good to match the VIP you're using. \$VipName = "Red-VIP")</pre>
Import-Module virtualmachinemanager
<pre>\$Ib = Get-scLoadBalancer where { \$Service.Name -eq \$LBServiceName}; \$vipNetwork = get-scvmnetwork -Name \$VipNetworkName;</pre>
\$vipMemberNics = @(); foreach (\$vmName in \$VipMemberVMNames)
<pre>\$vm = get-scvirtualmachine -Name \$vmName; # if (\$vm.VirtualNetworkAdapters[0].VMNetwork.ID -ne \$vipNetwork.ID) # {</pre>
<pre># \$vm.VirtualNetworkAdapters[0] set-scvirtualnetworkadapter -VMNetwork \$vipNetwork; # }</pre>
<pre>\$vipMemberNics += \$vm.VirtualNetworkAdapters[0]; }</pre>
<pre>\$existingVip = get-scloadbalancervip -Name \$VipName if (\$existingVip -ne \$null) {</pre>
foreach (\$mem in \$existingVip.VipMembers) # {
\$mem remove-scloadbalancervipmember; # }
<pre>\$existingVip remove-scloadbalancervip; }</pre>
<pre>\$vipt = get-scloadbalancerviptemplate -Name \$VipTemplateName;</pre>
<pre>\$vip = New-SCLoadBalancerVIP -Name \$VipName -LoadBalancer \$Ib -IPAddress \$VipAddress -LoadBalancerVIPTemplate \$vipt -FrontEndVMNetwork \$vipNetwork -BackEndVirtualNetworkAdapters \$vipMemberNics; Write-Output "Created VIP " \$vip;</pre>
<pre>\$vip = get-scloadbalancervip -Name \$VipName; Write-Output "VIP with members " \$vip:</pre>

Anmerkung: Die Parameter dieses Skripts sind so vorbelegt, dass Sie direkt die *PublicVIP* 10.10.50.100 anlegen können, um ein Load Balancing zwischen den VMs *Red-VM01* und *Red-VM02* zu definieren.

Analog können Sie auch eine *PublicVIP* 10.10.50.101 für ein Load Balancing zwischen den Tenant VMs *Green-VM01* und *Green.VM02* zu definieren.

Mit dem CmdLet *Get-SCLoadBalancerVIP* können Sie sich nun eine Liste aller definierten *PublicVIPs* anzeigen lassen.

C:\Windows\system32> Get-SCLoadBalancerVTP



Name	: Green-VIP
Address	: 10.10.50.101
IPAddress	: 10.10.50.101
LoadBalancer	: https://192.168.80.230
Protocol	: TCP
Port	: 80
IsPersistenceEnabled	: False
Persistence	
LoadBalancingMethod	: RoundRobin
HealthMonitors	: ()
VIPMembers	: {192.168.1.4, 192.168.0.4}
state	: Deployed
LoadBalancerConfigurationName	
FrontEndVMNetwork	: PublicVIP
ServerConnection	: Microsoft.SystemCenter.VirtualMachineManager.Remoting.ServerConnection
ID	: 6e0e01ff-76e2-4436-80b8-439a8f802b4d
TsViewOnly	False
ObjectType	LoadBalancerVTP
MarkedForDeletion	Ealse
TsFullyCached	True
Israriyeachea	
Name	: Red-VIP
Address	: 10.10.50.100
IPAddress	: 10.10.50.100
LoadBalancer	: https://192.168.80.230
Protocol	: TCP
Port	: 80
IsPersistenceEnabled	False
Persistence	
LoadBalancingMethod	RoundRobin
HealthMonitors	· 0
VTPMembers	$\{192, 168, 0, 4, 192, 168, 1, 4\}$
state	
LoadBalancerConfigurationName	· beproyed
ErontEndVMNetwork	· public/TP
ServerConnection	. Nicrosoft SystemCenter VirtuelMachineManager Remoting ServerConnection
TD	
ObjectTure	LongPalancon//TD
MankadEanDalation	
ToFullyCached	
ISFUTTycacneu	: mue

10.5.3 Load Balancing Test

Nachdem wir nun für unsere Tenant VMs öffentliche IP-Adressen definiert haben, können wir das Load Balancing einmal ausprobieren.

Starten Sie auf einem System, das Zugriff auf das *PublicVIP* Netz hat – z.B. unser Domain Controller *SDN-DC01* – einen Browser und geben in die Adresszeile *http://10.10.50.100* (die VIP des Red Tenants) ein. Sie sollten folgende Anzeige erhalten:

()	@ http://10.10.50.100/	り → C 🥔 IIS Windows Server	×
	Internet Information	Services	

Starten Sie eine weitere Browser Instanz und geben die gleiche Adresse ein. Ergebnis:



Geben Sie in die Adressleisten der Browser die *PublicVIP* des Green Tenants ein (*http://10.10.50.101*) und Sie erhalten folgende Anzeige:



		5 - Q	Ø IIS Windows Server	×	
🕂 Windows Server	Green-VM01				
Internet Info	ormation S	Services			
		5 - Q	🥖 IIS Windows Server	×	
🚝 Windows Server	Green-VM02				
Internet Info	ormation S	Services			

10.5.4 NAT konfigurieren

Bislang können die Tenant VMs nur in ihrem eigenen VMnet kommunizieren. Nachdem wir die SLB-Instanzen konfiguriert haben, können wir ihnen nun auch den Zugriff auf externe Ressourcen per NAT (Netzwerk Address Translation) einrichten.

Wechseln Sie in der VMM-Konsole in den Arbeitsbereich *VMs and Services*, wählen die Kategorie *VM Networks* und klicken Sie mit der rechten Maustaste auf das VMnet, für das Sie NAT aktivieren wollen. Rufen Sie die *Properties* auf.

VMs and Services	 VM Networks and IP Pool 	ols (7)							
🥵 Tenants									
Clouds	Name	Name							
	🗉 🚢 Green VMnet	🗉 🚣 Green VMnet							
Azure Subscriptions	Green IP Pool C	Green IP Pool 0 192.168							
📥 VM Networks	Green IP Pool 1	I		192.168					
Storage	dREVIP								
a 🧠 ana a	📥 NC_Management								
All Hosts	A PrivateVIP								
	Ju PublicVIP								
	🖂 🎿 Red VMnet		100000-000-000-01						
SDN-HV01 SDN-HV02 SDN-HV03 sdn-hv04	and IP Pool 0	No.	Create IP Pool						
	Ked IP Pool 1		Properties						
	🚢 Transit	^	∧ Delete						
	🔒 View Dependent Resources								
	Red VMnet								
	Red VMnet	tion							
	Red VMnet VM network informa Description:	ition							
	Red VMnet VM network informa Description: Number of VM subnet	ation							
WMs and Services	Red VMnet VM network informa Description: Number of VM subnet VM subnets	ation s: 2 Red V	- /Mnet_0 (192.168.0.0/	(24-0)					
Image: WMs and Services Image: Fabric	Red VMnet VM network informa Description: Number of VM subnet VM subnets	s: 2 Red V Red V	Mnet_0 (192.168.0,0 //Mnet_1 (192.168.1.0/	(24-0) (24-0)					
 WMs and Services Fabric Library 	Red VMnet VM network informa Description: Number of VM subnet VM subnets:	s: 2 Red V Red V	/Mnet_0 (192.168.0.0/ /Mnet_1 (192.168.1.0/	(24-0) (24-0)					
WMs and Services Fabric Library Library	Red VMnet VM network informa Description: Number of VM subnet VM subnets	s: 2 Red V Red V	/Mnet_0 (192.168.0.0/ Mnet_1 (192.168.1.0/	(24-0) (24-0)					
WMs and Services Image: Service services Image: Service ser	Red VMnet VM network informa Description: Number of VM subnet VM subnets:	s: 2 Red V Red V	Mnet_0 (192.168.0.0/ Mnet_1 (192.168.1.0/	(24-0) (24-0)					

Wählen Sie die Registerkarte *Connectivity*. Aktivieren Sie das Kontrollkästchen *Connect directly to an additional logical network* und wählen Sie darunter die Option *Network Address Translation (NAT)* – im linken Bereich erscheint dabei ein Reiter für eine weitere Registerkarte *Network Address…* Stellen Sie sicher, dass im Feld *Gateway Device* der *Network Controller* eingestellt ist.



Red VMnet Properties			×				
Name	Connectivity						
VM Subnets	By default, network virtualization provides an isolated network. Select the options below to add external connectivity to this network.						
Connectivity	Connect to another network through a VPN tunnel Enable Border Gateway Protocol (BGP)						
Network Address	k Address 🗹 Connect directly to an additional logical network						
Access	Direct routing Network address translation (NATI					
	Select the nateway device to use for this connection.						
	Gateway Device: Network Controlle	. *					
	Device capabilities:	Site to Site VPN Border Gateway Protcol (BGP) Direct routing					
	Remaining capacity:	50 VM networks 250 VPN tunnels					
	₽						
View Script		ОК	Cancel				

Klicken Sie jetzt auf den neuen Reiter für die Registerkarte *Network Address…* Im Feld *IP Address Pool* wählen Sie den *PublicVIP_IPAddressPool_0*. Das Feld *IP Address* können Sie freilassen. Vom VMM wird dann eine geeignete IP-Adresse aus dem gewählten Pool eingesetzt. Klicken Sie auf *OK*.

a neu vivinet riopentes						
Name	Network add	lress transla	tion (NAT)			
/M Subnets	In NAT all traffic If you want VMM address column	to external netw I to automatical empty.	vork is routed throug ly pick any available	h single IP, select IP from the select	the IP address pool a ed address pool, leav	and IP below. The IP
Connectivity	IP address pool:	PublicVIP IPAc	idressPool 0 (10.10.5	0.100 - 10.10.50.1	99)	v
Vetwork Address	IP address:					
licress	Specify network	address translat	ion (NAT) rules:			
	Name	Protocol	Incoming Port	Destination IP	Destination P	Add
						Remove
View Script					ОК	Cancel

Zur Kontrolle können Sie nochmals die *Properties des VMnets* aufrufen. Auf der Registerkarte *Network Address* ist jetzt das Feld *IP Address* ausgefüllt (hier: 10.10.50.100).



lame	Network add	Iress translat	tion (NAT)			
/M Subnets	In NAT all traffic t If you want VMM address column	to external netw 1 to automaticall emoty	ork is routed through y pick any available I	h single IP, select P from the select	the IP address pool a ed address pool, leav	nd IP below. e the IP
Connectivity	IP address pool:	PublicVIP_IPAd	dressPool_0 (10.10.5)	0.100 - 10.10.50.1	99)	
Vetwork Address	IP address:	10.10.50.100				
cress	Specify network a	address translati	ion (NAT) rules:			
	Name	Protocol	Incoming Port	Destination IP	Destination P	Add
						Remove

Jetzt könnten Sie von einer VM im *Red VMNet* eine externe Webseite aufrufen. In unserer Lab-Umgebung fehlt jedoch die Verbindung zwischen dem *PublicVIP* Netz und dem öffentlichen Internet. Deshalb können Sie keine externen Ressourcen im Internet ansprechen. Sie können aber beispielsweise versuchen, über die öffentliche VIP eines anderen Tenant Netzes die IIS-Startseite einer VM zu erreichen, z.B.

€ Server Manager ► Local Server							
Dashboard	PROPERTIES For Red-VM01						
Local Server All Servers	Computer name Red-VM01 Workgroup WORKGROUP						
(P ▼ C Ø IIS Windows Server ×						
H Windows Server	Green-VM02						
Internet Information Services							

Jetzt können wir auch noch NAT-Regeln für eingehende Netzwerkpakete von unserer öffentlichen IP-Adresse definieren.

Öffnen Sie wieder die Properties des gewünschten Tenant VMnets und wechseln Sie auf die Registerkarte *Network Address…*

Über die Schaltfläche *Add* können Sie jetzt Regeln für den eingehenden Netzwerkverkehr konfigurieren. Um z.B. eine Remote Desktop Verbindung (RDP) von einem externen System zum System Red-VM01 herstellen zu können, geben Sie folgende Parameter ein:

Name	Geben Sie einen Namen für die eingehende NAT-Verbindung ein,
	z.B. RDP_Red-VM01
Protocol	Wählen Sie das Protokoll (TCP oder UDP) der eingehenden Verbindung.



Incoming Port	Geben Sie die Portnummer für die eingehenden Netzwerkdaten an, hier 3389 (Standard RDP Port)
Destination IP	Geben Sie die IP-Adresse der Tenant VM ein, an die die Daten weitergeben werden sollen, z.B. für die <i>Red-VM01</i> die Adresse 192.168.0.4
Destination Port	Portnummer innerhalb der Tenant VM als Ziel der Datenweiterleitung (RDP- Standard 3389)

Und wenn Sie gerade schon dabei sind, konfigurieren Sie auch gleich eine NAT-Regel für RDP zum System *Red-VM02*. Diesen Datenverkehr erwarten wir auf dem Port 3390 und leiten ihn an den Port 3389 der Ziel-VM weiter.

Name	Geben Sie den Namen der eingehenden NAT-Verbindung ein, z.B. RDP_Red-
	VM02
Protocol	Wählen Sie das Protokoll (TCP oder UDP) der eingehenden Verbindung.
Incoming Port	Geben Sie die Portnummer für die eingehenden Netzwerkdaten an, hier 3390
Destination IP	Geben Sie die IP-Adresse der Tenant VM ein, an die die Daten weitergeben
	werden sollen, z.B. für die <i>Red-VM02</i> die Adresse 192.168.1.4
Destination Port	Portnummer innerhalb der Tenant VM als Ziel der Datenweiterleitung (RDP-
	Standard 3389)

Name	Network add	ress transla	itio	n (NAT)			
VM Subnets	In NAT all traffic to If you want VMM address column e	o external netv to automatica	work	is routed throug ick any available l	h single IP, select t P from the selecte	he IP address pool a d address pool, leav	nd IP below e the IP
Connectivity	IP address pool:	PublicVIP_IPA	ddre	ssPool_0 (10.10.5	0.100 - 10.10.50.19	99)	
Network Address	IP address:	10.10.50.100					
Access	Specify network a	ddress transla	tion	(NAT) rules:			
	Name	Protocol		Incoming Port	Destination IP	Destination P	Add
	RDP_Red-VM02	тср	v	3390	192.168.1.4	3389	Remove
	RDP_Red-VM01	TCP	v	3389	192.168.0.4	3389	
]	

Jetzt können Sie von einem System in unserem *PublicVIP* Netz RDP-Verbindungen zu den Tenant VMs herstellen, z.B. zu *Red-VM01*:

mstsc /v 10.10.50.100:3389

Software Defined Networking (SDN) mit Windows Server 2016 und System Center Virtual Machine Manager 2016 (SCVMM 2016)



Windows Security		×	semote Desktop Connectio	on
Enter your credentials			The identity of the rem	note computer cannot be verified.
,			you want to connect a	nyway?
These credentials will be used to c	onnect to 10.10.50.100.		The remote computer could not be security certificate. It may be unsaf	e authenticated due to problems with its fe to proceed.
Red-VM01\Administrator			Certificate name	
Password			Name in the certificate from Red-VM01	m the remote computer:
Remember me			Certificate errors	
			The following errors were encour computer's certificate:	intered while validating the remote
More choices			The certificate is not from	a trusted certifying authority.
ОК	Cancel		Do you want to connect despite th	ese certificate errors?
			U Uon't ask me again for connect	tions to this computer
			View certificate	<u>Y</u> es <u>N</u> o
10 10 50 100 2200 Berrate Decision Cou				
- 10.10.30.100:3389 - Remote Desktop Cor	inection			
🕋 Server Manager				<u>^</u>
Contract Server Mar	nager + Local Se	arvor		- 3
	lager Local Se			
	PROPERTIES			
Dashboard	For Red-VM01			
Local Server	Computer name	Red V/	401	lact installed und:
All Servers	Workgroup	WORK	GROUP	Windows Update
File and Storage Services ▷				Last checked for u
	Windows Firewall	Drivata	· On	Windows Defende
	Remote management	Enable	d	Feedback & Diagn
	Remote Desktop	Enable	d	IE Enhanced Secur
	NIC Teaming	Disable	ed	Time zone
		102.16		
	Ethernet	192,10	8.0.4, IPv6 enabled	Product ID

Für eine RDP-Verbindung zu *Red-VM02* geben Sie die in der NAT-Regel hinterlegte Portnummer 3390 an:

mstsc /v 10.10.50.100:3390



Windows Security		🗙 🛛 💀 Remote Deskto	op Connection X
Enter your credentials		The identity you want t	y of the remote computer cannot be verified. Do o connect anyway?
These credentials will be used to	connect to 10.10.50.100	The remote compute security certificate.	er could not be authenticated due to problems with its t may be unsafe to proceed.
Red-VM02\Administrator		Certificate name	
Password		Name in the Red-VM02	certificate from the remote computer:
Remember me		Certificate errors	
		The following error computer's certific	rs were encountered while validating the remote ate:
More choices		1 The certifica	ate is not from a trusted certifying authority.
ОК	Cancel	Do you want to con	nect despite these certificate errors?
		Don't ask me an	ain for connections to this computer
			annor connections to this compater
		View certificate	Yes <u>N</u> o
Server Manager	nager • Local Se PROPERTIES For Red-VM02	erver	· ②
E Frank Control			
Local Server	Computer name	Red-VM02	Last installed unda
All Servers	Computer name Workgroup	Red-VM02 WORKGROUP	Last installed upda Windows Update
All Servers	Computer name Workgroup	Red-VM02 WORKGROUP	Last installed upda Windows Update Last checked for u
All Servers File and Storage Services ▷ IIS	Computer name Workgroup	Red-VM02 WORKGROUP	Last installed upda Windows Update Last checked for u
All Server	Computer name Workgroup Windows Firewall	Red-VM02 WORKGROUP Private: On	Last installed upda Windows Update Last checked for u Windows Defende
All Server	Computer name Workgroup Windows Firewall Remote management	Red-VM02 WORKGROUP Private: On Enabled	Last installed upda Windows Update Last checked for u Windows Defende Feedback & Diagn
All Server	Computer name Workgroup Windows Firewall Remote management Remote Desktop	Red-VM02 WORKGROUP Private: On Enabled Enabled	Last installed upda Windows Update Last checked for u Windows Defende Feedback & Diagn JE Enhanced Secur
All Server	Computer name Workgroup Windows Firewall Remote management Remote Desktop NIC Teaming	Red-VM02 WORKGROUP Private: On Enabled Enabled Disabled	Last installed upda Windows Update Last checked for u Windows Defende Feedback & Diagn IE Enhanced Secur Time zone
All Server File and Storage Services ▷ IIS	Computer name Workgroup Windows Firewall Remote management Remote Desktop NIC Teaming Ethernet	Red-VM02 WORKGROUP Private: On Enabled Enabled Disabled 192.168.1.4, IPv6 enabled	Last installed upda Windows Update Last checked for u Windows Defende Feedback & Diagn IE Enhanced Secur Time zone Product ID

Die NAT-Konfiguration und Regeln für ein VMnet können Sie sich auch mit der PowerShell anzeigen lassen:

<pre>\$vnet = Get-SCVMNetwork -Name "Red VMnet"</pre>	
Write-Output "NAT Connections and Rules for VM Network: \$vnet"	
\$NATconn = Get-SCNATConnection -VMNetwork \$vnet	
Write-Output \$NATconn	
\$NATrules = Get-SCNATRule -NATConnection \$NAT	
Write-Output \$NATrules	

NAT Connections and Rules for VM Network: Red VMnet

Name	: Red VMnet_NatConnection
Description	: . Emphlod
MaximumBandwidthTnhoundKhns	. Ellableu
MaximumBandwidthOutboundKbps	
VMNetworkGateway	:
VMNetwork	: Red VMnet
Rules	: {RDP_Red-VM02, RDP_Red-VM01, 10.10.50.100}
ServerConnection	:
Microsoft.SystemCenter.Virtua	1MachineManager.Remoting.ServerConnection
ID	: cab624bb-781c-4507-b858-9841e07db1c5
IsViewOnly	: False
ObjectType	: NATConnection
MarkedForDeletion	: False
IsFullyCached	: True
Name : RDP_Red-V	м02
ExternalIPAddress : 10.10.50.	100



ExternalPort :	3390
InternallPAddress :	192.108.1.4 2200
Protocol	
NATConnection	Red VMnet NatConnection
ServerConnection	Microsoft SystemCenter VirtualMachineManager Remoting ServerConnection
TD	h77e7714-c034-44d5-9abe-680f94139c0f
IsViewOnlv :	False
ObjectType :	: NATRUIE
MarkedForDeletion :	: False
IsFullyCached :	: True
Name	RDP Red-VM01
ExternalIPAddress :	: 10.10.50.100
ExternalPort :	: 3389
InternalIPAddress :	: 192.168.0.4
InternalPort :	: 3389
Protocol :	: TCP
NATConnection :	Red VMnet_NatConnection
ServerConnection :	Microsoft.SystemCenter.VirtualMachineManager.Remoting.ServerConnection
ID :	0821898a-5aee-4+53-b/0c-9218/a331cca
ISV1eWONIY :	
UDJectiype :	
ISFUTTYCached :	. True
Name :	: 10.10.50.100
ExternalIPAddress :	: 10.10.50.100
ExternalPort :	: 0
InternalIPAddress :	
InternalPort :	
Protocol	
NATConnection	Reg VMnet_NatConnection
serverconnection :	The observer connection
ObjectType	
MarkedEorDeletion	
IsFullvCached	



11 Nächste Schritte

In den vorstehenden Abschnitten habe ich versucht, einige der Testszenarien, die Petra Lipp und ich bei unserer Session auf der CDC 2018 präsentiert haben, etwas detaillierter zu beschreiben.

Nun ist das nur ein Bruchteil dessen, was die Microsoft SDN-Technologie bietet. Was wir hier überhaupt nicht weiter betrachtet haben, sind Remote Szenarien, um z.B. ein Unternehmensnetz mit einem *VMnet* in unserer SDN-Umgebung zu verbinden.

Eine weitere Herausforderung wäre auch, wie Service Provider SDN-Technologien ihren Kunden über Self Service Portale anbieten können. Eine Lösung dafür wäre z.B. das gute alte Windows Azure Pack, das sich hervorragend in eine SDN-Umgebung integrieren lässt. Petra und ich haben auf der CDC2018 auch dazu eine Session gehalten und die Implementierung eines Kunden vorgestellt.

Hierzu müssten wir aber unsere Lab-Umgebung jedoch um weitere Infrastruktur- und Remote-Systeme erweitern, was aber irgendwann unsere Ressourcen und den Rahmen dieses Whitepapers sprengen würde.

Bei Bedarf können wir gerne in weiteren Dokumenten und persönlichen Beratungsgesprächen darauf eingehen. Im Moment kann ich Sie nur auf die offizielle Microsoft Dokumentation in der <u>TechNet-Library</u> verweisen, die zugegebenermaßen zumindest in der englischen Originalfassung mal relativ ausführlich und gut verständlich ist. Die (maschinelle) deutsche Übersetzung sollten Sie mit Vorsicht genießen.

Neben dieser offiziellen Dokumentation gibt es auch noch eine Reihe sehr empfehlenswerter Blog-Beiträge verschiedener Microsoft Gurus und MVPs, die mir beim Erstellen und dem Aufbau der Lab-Umgebung wertvolle Informationen geliefert haben. Ohne Anspruch auf Vollständigkeit möchte ich hier auf folgende Artikelserien verweisen (in Englisch):

Schumann Ge's Blog: Deploying SDN on One single physical host using VMM

Larryexchange Blog:

- Step-by-step for deploying a SDNv2 using VMM Part 1-4
- <u>Configure WAP to support new SDN stack on Windows Server 2016</u>

Und die Entwicklung wird weitergehen. Im Herbst dieses Jahres wird die nächste Version von Windows Server unter dem Namen *Windows Server 2019* erscheinen und voraussichtlich einige Neuerungen zum Thema SDN bringen, über die wir natürlich zeitnah berichten werden.

Ich hoffe, dass dieses Whitepaper Ihnen einen Überblick geben konnte zu den Microsoft SDN Technologien mit Windows Server 2016 und dem SCVMM 2016 und Ihnen auch zeigen konnte, wie Sie eine SDN-Umgebung mit Hilfe der von Microsoft auf GitHub bereitgestellten PowerShell Skripte ausrollen können.

Für weitere Fragen, Anregungen und Kommentare stehen wir gerne zur Verfügung.



Anhang: Skript Download Details

In diesem Whitepaper habe ich einige PowerShell Skripte beschrieben, die ich mir zusätzlich zu den von Microsoft auf GitHub bereitgestellten erstellt habe, um Aktionen, die mit vielen Mausklicks verbunden sind, etwas zu vereinfachen. Diese zusätzlichen Skripte habe ich in einer .ZIP-Datei zusammengestellt, die Sie <u>hier</u> downloaden können. Nachstehend finden Sie Details zum Inhalt dieser .ZIP-Datei.

Dateiname: <u>VMM-SDN.zip</u> – Entpacken Sie den Inhalt dieser Datei in das SDN-Master Verzeichnis, das Sie nach dem Download der Microsoft Skripte aus GitHub erstellt haben.

Inhalt:

VMM\scripts\CreateTenantVMnet-Red.ps1 – erzeugt das Red VMnet VMM\scripts\CreateTenantVMnet-Green.ps1 – erzeugt das Green VMnet VMM\scripts\CreateTenantVMnet-Red.ps1 – erzeugt VIP im PublicVIP-Netz für den Red Tenant VMM\scripts\CreateTenantVMnet-Green.ps1 – erzeugt VIP im PublicVIP-Netz für den Green Tenant VMM\VMM SDN Express\Fabricconfig-SDNcloud-Production.psd1 –

Konfigurationsdatendatei für das Deployment der Lab-Umgebung mit VMMexpress.ps1