1 | 17 Sonderdruck für Arista Networks

IT Administrator
Das Magazin für professionelle System- und Netzwerkadministration

Integration von Arista-Switchen in VMware-Infrastrukturen

www.it-administrator.de

Integration von Arista-Switchen in VMware-Infrastrukturen

Schluss mit Handarbeit

von Jens Söldner und Philipp März

VMware unterstützt den Netzwerkbetrieb seines Hypervisors durch zwei virtuelle Switche und bietet mit NSX ein Zusatzprodukt zur Virtualisierung von Netzwerkfunktionen. Doch was bleibt, ist ein hoher manueller Aufwand bei Konfiguration, Administration und Troubleshooting virtueller Netze. Die Kombination mit Switchen aus dem Hause Arista sorgt für Abhilfe.

VMware bietet in vSphere je nach erworbener Lizenz zwei Arten von virtuellen Switchen, die virtuelle Maschinen mit der Außenwelt verbinden. Außerdem fließt darüber jeder Netzwerkverkehr, der für die Verwaltung und den Betrieb des ESXi-Hypervisors benötigt wird. Dazu gehören beispielsweise der Management-Traffic, vMotion für die VM-Livemigration, der Zugriff auf Storage über iSCSI oder NFS sowie Replikation und Fault Tolerance.

Virtuelle Switche in vSphere

Jede vSphere-Lizenz enthält den "vSphere Standard Switch" (vSS), der die elementaren Netzwerkfunktionen abbildet. Deutlich mächtiger und komfortabler ist der "vSphere Distributed Switch" (vDS), der in der Enterprise-Plus-Lizenz (sowie in bestimmten Bundle-Varianten) enthalten ist. Eine Gegenüberstellung der verfügbaren Features zeigt die gleichnamige Tabelle. Sowohl beim Standard Switch als auch beim Distributed Switch handelt es sich um Layer-2-Switche, die die Separierung von Netzwerken via VLANs (802.1Q Tagging) ermöglichen, aber nicht selbst zwischen den über VLANs-separierten Netzwerken routen können. Hierfür verwenden Unternehmen bislang in der Regel physische Layer-3-Switche beziehungsweise virtuelle Maschinen, in denen Routerfunktionen laufen. Letzteres bringt einige Nachteile mit sich, sodass diese Konstellation zumeist nur in Testumgebungen zum Einsatz kommt.

Erst VMwares Netzwerkvirtualisierungsplattform "NSX for vSphere" (NSX-v) erweitert vSphere um Layer-3-Routing-Funktionen sowie Overlay-Networking mittels des "Virtual eXtensible LAN" (VXLAN) Tunneling, Firewalling und einiger Funktionen mehr [1]. NSX-v wendet sich allerdings eher an größere Unternehmen mit hohem Automatisierungsbedarf, wie er beim Betrieb von Cloud-Umgebungen mit "VMware vRealize Automation" (vRA), "VMware Integrated OpenStack" (VIO) oder im Service-Provider-Umfeld mit "vCloud Director for Service Providers" (vCD-SP) anfällt.

Aber auch kleinere Unternehmen ohne interne Cloud und VXLAN-Overlay-Netzwerke profitieren von NSX-v durch die innovativen Firewallfunktionen, die VMware Microsegmentierung nennt. Diese Technologie lässt sich als eine zentral gesteuerte Firewall im Kabel zwischen der VM und dem Switch beschreiben. Vor kurzem hat VMware auch für NSX-v ein abgestuftes Lizenzmodell eingeführt, sodass die von NSX-v bereitgestellten Funktionen analog zu vSphere nun auch von der jeweiligen Lizenz abhängen (Tabelle: "Verfügbare Funktionen der NSX-v-Lizenzen").

Vergleich vSphere Standard Switch und Distributed Switch

Feature	Standard Switch	Distributed Switch
Management	Muss individuell auf Host-Ebene verwaltet werden.	Zentrale Verwaltung und Überwachung aller Hosts, die mit dem Distributed Switch assoziiert sind.
Lizenzierung	In allen vSphere-Versionen enthalten.	Nur in Enterprise-Editionen enthalten.
Erstellen & Konfigurieren	Auf Ebene des ESX/ESXi-Hosts.	Auf vCenter-Ebene.
Layer-2-Switch	Kann Layer-2-Frames weiterleiten.	Kann Layer-2-Frames weiterleiten.
802.1Q-Erkennung	802.1Q-VLAN-Tagging möglich.	802.1Q-VLAN-Tagging möglich.
VLAN-Segmentierung	Ja	Ja
NIC Teaming	Verbindung mehrerer Uplinks möglich.	Verbindung mehrerer Uplinks möglich.
Ausgehenden Datenverkehr modellieren	Ja	Ja
Eingehenden Datenverkehr modellieren	Nein	Ja
VM-Port-Blocking	Nein	Ja
Privates LAN	Nein	Drei VLAN-Typen verfügbar.
Lastbasiertes Teaming	Nein	Ja
Netzwerk-vMotion-Statistik	Nein	Ja
Portspezifische Policies	Policies lassen sich auf Switch- und Portgruppen anwenden.	Policies lassen sich auf Switch- und Portgruppen sowie einzelne Ports anwenden.
NetFlow	Nein	Ja
Port-Spiegelung	Nein	Ja

Herausforderungen beim vSphere-Switch-Management

Unabhängig davon, ob vSphere Standard oder Distributed Switche beziehungsweise gar NSX-v zum Einsatz kommen, stellt das Design, die Konfiguration sowie die Überwachung und Fehlersuche im physischen Netzwerk eine große Herausforderung dar. Um mit vSphere Standard oder Distributed Switchen VLAN-basierte Netzwerke bereitzustellen, müssen Sie mehrfach und in aller Regel manuell tätig werden: Die benötigten VLAN IDs müssen auf allen Switch-Ports, die mit den ESXi-Servern verbunden sind (üblicherweise VLAN-Trunk-Ports), ebenso zugelassen werden wie auf den Trunk-Ports, die die physischen Switche miteinander verbinden. Je nach Größe des Netzwerks und Anzahl der physischen Switche kann dies eine nicht unerhebliche und sehr aufwendige Aufgabe darstellen. Da dies im Regelfall manuell erfolgt, ist die Gefahr von Konfigurationsfehlern sehr wahrscheinlich.

Auf vSphere-Seite müssen Sie pro VLAN eine konsistent bezeichnete Port-Gruppe auf jedem Standard Switch anlegen, die die VLAN ID referenziert. Die Verwendung von Distributed Switch reduziert hier den Aufwand massiv, da dieser Vorgang im Falle eines Distributed Switch nur einmalig anfällt. Die Pflicht zur Konfiguration der physischen Switche kann aber auch ein Distributed Switch nicht lösen, da virtuelle Switche lediglich den Zugriff auf physische Netzwerke (VLANs) aus der VMware Welt heraus ermöglichen.

Neben der aufwendigen Bereitstellung der von den VMs benötigten VLANs in den physischen Switchen stellt wie erwähnt auch die Überwachung und die Fehlersuche im physischen Netzwerk eine große Herausforderung dar. Herstellereigene Netzwerkmanagementlösungen bieten meist keinen übergeordneten und vor allem integrativen Ansatz, um das Netzwerk und die virtuelle Welt gesamtheitlich zu betrachten und zu verwalten. Dies hat zur Folge, dass VMwares Hypervisor sowie die Virtualisierungsadministratoren von der Netzwerk-Welt abgeschirmt sind. Dies vereinfacht sich, wenn der Switch-Hersteller sich mit VMware geschickt integriert.

Switching mit Arista

Genau hier setzt Arista an, ein Hersteller, der sich im Cloud Networking und Software-defined Networking mit tiefgehenden Automatisierungsfunktionen positioniert. Zudem boten seine Produkte frühzeitig eine Integration mit VMware vSphere und der NSX-Plattform. Die von Arista angebotenen Switche versprechen "Ultra-Low Latency", weitgehende Programmierbarkeit, Offenheit, sehr hohe Qualität sowie Erweiterbarkeit und leichte Automatisierbarkeit. Gartner positioniert Arista als führenden Hersteller im Quadranten für "Data Center Networking". Arista setzt bei der Switch-Hardware auf Standard-Chips mehrerer Hersteller, etwa von Broadcom und Intel – weitere Chiphersteller sollen folgen.

Kernstück der Produktpalette ist jedoch Aristas Switch-Betriebssystem "Extensible Operating System" (EOS). Eine Besonderheit ist dabei, dass alle Switche – vom kleinsten 1-GBit-Management-Switch bis hin zum 12-Slot-Chassis mit 432 Ports mit 100 GBit/Port – auf das gleiche Softwareimage setzen, was eine operative Vereinfachung im Vergleich zu anderen Herstellern darstellt, die mehrere Betriebssystemimages für unterschiedliche Geräte benötigen.

EOS bietet als unmodifiziertes Linux-Betriebssystem auf Arista-Switchen die gleichen Möglichkeiten wie Linux im Servereinsatz. Arista lässt den Linux-Kernel unverändert, denn alle Erweiterungen des Herstellers laufen im User Space. Dies kommt beispielsweise der Devops-Community zu Gute, die dieselben Werkzeuge zum Verwalten von Arista-Switchen verwenden kann, wie sie tausendfach in der Serververwaltung helfen. So kann beispielsweise Python eingesetzt werden, um einfach auf Basis der "Aristas EOS API" [2] (eAPI) Skripte zu entwickeln, die die Verwaltung der Switche vereinfachen und automatisie-

Verfügbare Funktionen der NSX-v-Lizenzen			
Feature	**Standard**	**Advanced**	**Enterprise**
Verteiltes Switching und Routing	✓	✓	✓
NSX Edge-Firewall	✓	✓	✓
NAT	✓	✓	✓
SW-L2-Bridging zur physischen Umgebung	✓	✓	✓
Dynamisches Routing mit ECMP (Aktiv/Aktiv)	✓	✓	✓
API-gesteuerte Automatisierung	✓	✓	✓
Integration in vRealize und OpenStack	✓	✓	✓
Automatisierung von Sicherheitsrichtlinien mit vRealize		✓	✓
NSX Edge-Lastausgleich		✓	✓
Verteiltes Firewalling		✓	✓
Integration in Active Directory		✓	✓
Überwachung der Serveraktivität		✓	✓
Service-Integration (Integration von Drittanbieterprodukten)		✓	✓
vCenter-übergreifendes NSX			✓
Standortübergreifende NSX-Optimierungen			✓
VPN (IPsec und SSL)			✓
Remote-Gateway			✓
Integration in Hardware-VTEPs			✓

ren. Darüber hinaus lassen sich dank des Linux-basierten Betriebssystems Standard-RPMs für weitere Funktionen installieren.

Der entscheidende Vorteil von EOS ist allerdings, dass es das momentan einzige Betriebssystem in der Netzwerkwelt ist, das auf "State" (Zustände) anstelle von "Message Passing" setzt. Kern dieser Architektur ist eine kleine Datenbank namens "SysDB", auf die alle Agenten zugreifen, die die Funktionalität des Switch ausmachen (der ASIC-Treiber, BGP, OSPF, SNMP, STP und viele mehr). Die Agenten reden nie direkt miteinander, sondern nur mit der SysDB und registrieren ihren Zustand darin. Sie arbeiten im Publisher/Subscriber-Modell mit der SysDB im Zentrum, um den Zustand anderer Agenten abzufragen.

Diese zustandsbasierte Architektur verleiht Arista hohe Stabilität und vereinfacht es, Agenten zu aktualisieren, da nur der Agent mit seinem Interface zur SysDB im Fokus steht und andere Komponenten nicht berührt werden müssen. Dies steht im Gegensatz zur herkömmlichen Architektur der Switch-Betriebssysteme anderer Hersteller, die auf Message Passing zwischen den Agenten setzen, was zu einem unüberschaubaren und schwer zu wartenden Geflecht von Abhängigkeiten führt.

Im nächsten Schritt ermöglicht Arista die netzwerkweite Erweiterung der SysDB-Datenbanken der einzelnen Arista-Switche zu einer Art "Über"-Datenbank. Der Hersteller nennt diese "NetDB" und baut darauf seine CloudVision-Plattform auf. CloudVision ist ein EOS-Betriebssystem, das in einer virtuellen Maschine (oder als Appliance oder auch als Cluster von VMs) läuft und die Inhalte der SysDBs von allen Arista-Switchen zentral aggregiert und somit den Zustand des kompletten Netzwerks kennt. CloudVision stellt somit einen Integrationspunkt mit Software-defined-Networking-Controllern wie zum Beispiel VMware NSX-v oder auch Cloud-Orchestrierungslösungen anderer Hersteller dar. Wichtig hierbei ist, dass CloudVision sich nicht in der "Data Plane" befindet, sondern nur auf der "Management Plane" aktiv ist – ein Ausfall oder Reboot der CloudVision-Umgebung hat keinerlei negative Auswirkung auf die Verfügbarkeit des Netzwerks.

Vereinfachte VLANs

Arista verbindet mit VMware eine Entwicklungspartnerschaft und enge Kooperation, aus der beispielsweise das VXLAN-Overlay-Protokoll entstand. VXLAN entkoppelt die Netzwerkkommunikation der virtuellen Maschinen vom physischen Netzwerk – VMs können dadurch im Layer-2-Netzwerk kommunizieren, ohne dass die sie ausführenden ESXi-Server eine Layer-2-Verbindung benötigen. Diese Entkopplung des logischen Netzwerks, das die VMs benutzen, vom physischen Netzwerk – definiert durch die Switche – ermöglicht Automatisierung in der Bereitstellung und Verwaltung der Netzwerke sowie ein deut-

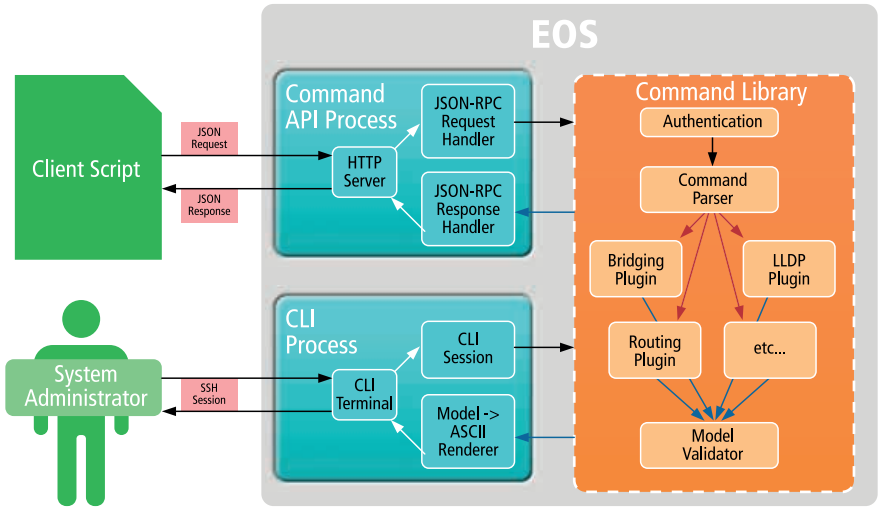

Bild 1: Über Aristas "EOS API" ist eine einfache Administration und Automatisierung der Arista-Switche möglich.

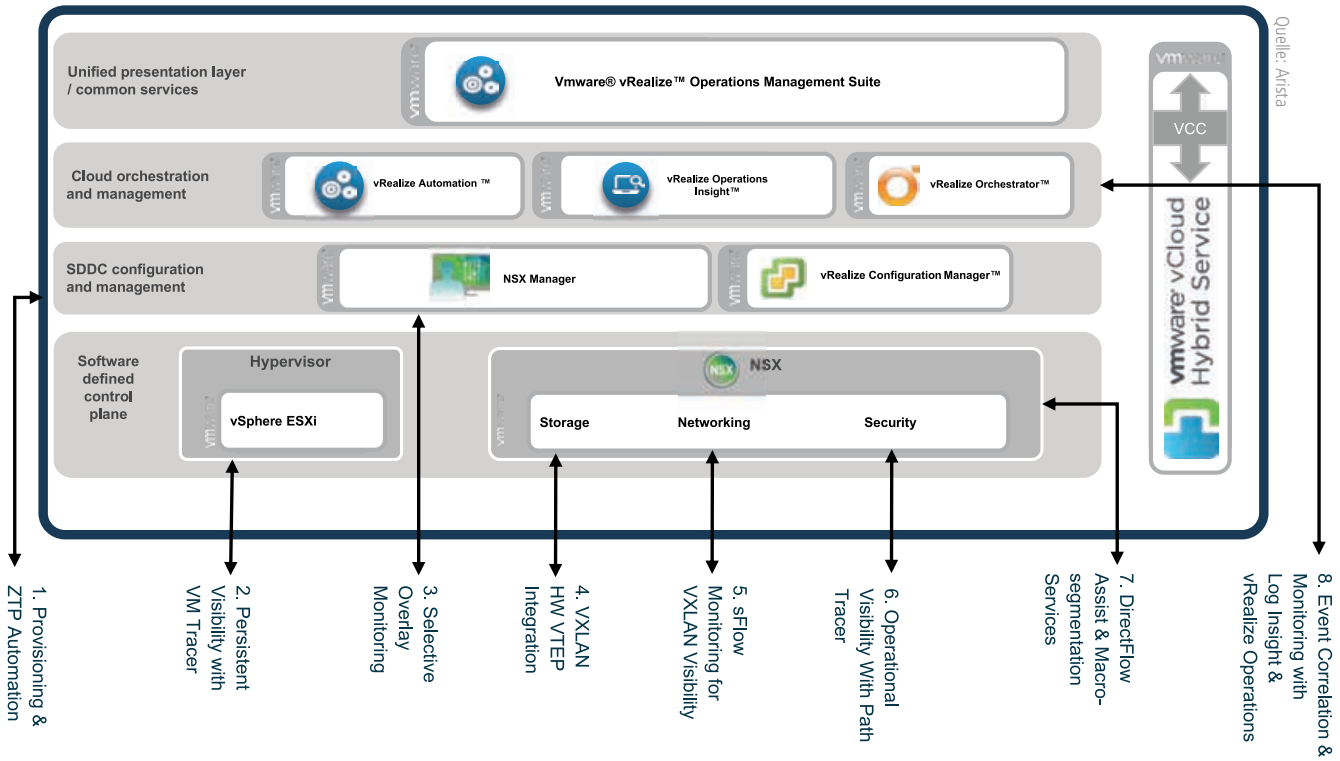

Bild 2: Arista integriert sich über zahlreiche Kontaktpunkte in die VMware-Produktpalette.

lich einfacheres, eleganteres und performanteres Netzwerkdesign.

Durch die Verwendung des VXLAN-Overlay-Protokolls müssen Netzwerkadministratoren deutlich weniger VLANs provisionieren. Allerdings führt die zusätzliche Schicht in der Kommunikation, die das Overlay-Protokoll einführt, auch zu mehr Komplexität bei Überwachung und Troubleshooting. Eine Integration in VMwares Switching-Infrastruktur löst sowohl die Herausforderungen, die bei der Verwendung klassischer VLANs anfallen, als auch die eingeschränkte Einsehbarkeit in das physische Netzwerk bei der Verwendung von NSX-v und dem VXLAN-Protokoll. Bei Arista erfolgt die Integration mit VMware auf mehreren Ebenen (Bild 2): Die Schnittstellen sind dabei die tiefgreifende Integration mit NSX (Punkt 1, 3, 4, 5, 6, 7), der VM Tracer (Punkt 2) sowie die Unterstützung beim Monitoring dank Integration in VMware vRealize Log Insight sowie vRealize Operations.

Der Einsatz von VMware NSX-v vereinfacht die Netzwerkanforderungen, denn die VXLAN-Technologie erlaubt, statt für die VM-Workloads hunderte bis tausende von physischen VLANs (bei VMware-Umgebungen mittlerer und größerer Dimension) in den Switchen bereitzustellen, einen Einsatz eines einzigen gerouteten Transport-VLANs. Dieses nimmt den kompletten VXLAN-Verkehr auf und vereinfacht somit den Netzwerkaufbau. Alle innerhalb von NSX definierten Netzwerke werden dann als VXLAN-basierte Overlay-Netzwerke physisch in das Transport-VLAN eingeschleust.

Bridging zwischen VLAN und physischem Netz

Nicht alle Workloads können (etwa aufgrund von Nicht-x86-Prozessorarchitektur) oder sollen (beispielsweise wegen Lizenzierungshürden) virtualisiert werden und somit in VXLAN-Netzwerke wandern. Daher tritt oftmals die Anforderung auf, die Workloads in VXLAN-Netzwerken mit physischen Maschinen, die in VLANs kommunizieren, in ein Layer-2-Netzwerk zusammenzuführen, sodass diese Maschinen ohne Router direkt miteinander kommunizieren können. Dieses Bridging zwischen VXLAN und VLAN kann zwar prinzipiell in der NSX-v-Plattform Software-basiert durch den "Distributed Logical Router" (DLR) erbracht werden, aber die Performance und die Stabilität sind für dieses Einsatzszenario oftmals nicht ausreichend. Die Lösung hierfür stellen VXLAN-Hardware-Gateways dar, die von VMware ab NSX-v 6.2.4 unterstützt werden. Arista hat dieses Konzept im Zusammenspiel mit VMware mitentwickelt und ist momentan der einzige Hersteller, der ein hochverfügbares VXLAN-Hardware-Gateway für NSX-v im Portfolio hat und bietet dieses mit 10, 25, 40, 50 und 100 GBit/s an.

Die Integration zwischen NSX-V und dem Hardwaregateway erfolgt über das "Open vSwitch Database"-Protokoll (OVSDB) [3]. Dieses umfangreiche Open-Source-Netzwerkmanagement-Protokoll ist vergleichbar mit SNMP aus der klassischen Netzwerkwelt. Der SDN-Pionier Nicira hatte OVSDB vor der Übernahme des Unternehmens durch VMware im Jahr 2012 ursprünglich für Linux-basierte Hypervisoren entwickelt.

Die Architektur der OVSDB-Integration sieht prinzipiell vor, dass ein OVSDB-Server in jedem Hardware-Switch und Hypervisor laufen muss, um die relevanten Zustandsinformationen der Control Plane zwischen der VMware- und der Switching-Welt auszutauschen. Da Arista

dank CloudVision bereits den zentralen Überblick über das Netzwerk durch die Aggregation der einzelnen SysDB Datenbanken hat, lässt sich hier ein deutlich einfacherer Weg beschreiten. CloudVision übernimmt somit die Rolle eines zentralen OVSDB-Servers, was die Integration mit NSX-v vereinfacht und die Komplexität herausnimmt. Neben NSX-v in einer aktuellen Version (6.2.4 oder höher) werden kompatible Arista-Switche (alle aktuellen Leaf-Switche) mit der neuesten Software-Version benötigt. Für einen HA-Modus werden bis zu drei CloudVision-Instanzen implementiert.

Die Integration von CloudVision mit NSX-V ist dann einfach: Zunächst konfiguriert der Systemverantwortliche ESXi-Hypervisoren als sogenannte "Replication Services Nodes", die sich um die Weiterleitung von BUM-Traffic (Broadcast, Unknown Unicast, Multicast) kümmern. Dies ist notwendig für die Verteilung der gelernten MAC-Adressen im Overlay-Netzwerk, was laut Standard mit Multicast erfolgt. Da dies jedoch die Komplexität erhöht, lässt sich mit dem zentralen Replication Node die Verwendung des ungeliebten Multicasts vermeiden.

Der nächste Schritt ist die Einrichtung der Kommunikation zwischen CloudVision und den NSX-Controllern, was mit wenigen Befehlen auf der Kommandozeile und dem Einspielen eines Zertifikats in NSX erledigt ist. Nach dem einmaligen Hinzufügen von CloudVision als zentrale Koordinationsinstanz für alle Arista-Switche kennt NSX dank CloudVision auch das komplette Arista-Switching-Netzwerk.

Danach ist die Grundkonfiguration abgeschlossen – jetzt lassen sich physische Ports auf den Arista-Switchen zu logischen VXLAN-Netzwerken einfach in der NSX GUI zuordnen. Nach einem finalen Test der Funktion ist das Layer-2-Bridging zwischen einem VXLAN-Overlay-Netzwerk und einem VLAN dann einsatzbereit.

Neben dem Hardware-basierten Bridging erleichtert die kombinierte Verwendung von NSX und CloudVision die Verwaltung des Netzwerks ungemein. Dank CloudVision ist die zentrale Verwaltung des gesamten physischen Netzwerks möglich und NSX erfüllt dieselbe Aufgabe für das komplette Software Definied DataCenter (SDDC). Im Zusammenspiel von CloudVision und NSX ist somit ein umfassendes Management sowohl der physischen als auch der virtuellen Welt möglich.

Schnelleres Troubleshooting

Die größte Herausforderung für das Netzwerkteam beim NSX-Betrieb ist herauszufinden, was die eigentliche Ursache von Netzwerkproblemen (geringer Durchsatz, Paketverlust et cetera) in Overlay-Netzwerken ist. Die integrierten Informationen, die standardmäßig von NSX geliefert werden (via LLDP oder TraceFlow), reichen oftmals nicht aus, um das Troubleshooting effektiv und effizient zu gestalten. Erleichterung verspricht hier Aristas "VM Tracer", ein Feature, das Arista schon seit 2010 im Portfolio hat und für die Verwendung mit NSX erweitert hat.

VM Tracer stellt dabei eine Verbindung zwischen den Arista-Switchen und dem vCenter über dessen API her. Darüber wissen die Switche und der Administrator, welche ESXi-Server, vSwitche, virtuelle Maschinen und MAC-Adressen mit den physischen Ports der Arista-Switche verbunden sind – unabhängig davon, ob die VMs in VLANs aktiv sind oder in getunnelten VXLAN-Overlay-Netzwerken, die von NSX verwaltet werden. Des Weiteren kann der Netzwerkadministrator über ein CLI-Kommando erfahren, in welchem Zustand sich die virtuelle Maschine befindet (aktiv oder nicht, wird gerade ein vMotion ausgeführt et cetera). Daneben lässt sich direkt sehen, welchem virtuellen Netz die Maschine angehört, und auch die Trafficstatistiken der vNICs sind direkt sichtbar. Diese zusätzliche Information kann das Troubleshooting des physischen Netzwerks ungemein erleichtern.

Eine weitere Stärke des Tools liegt im automatischen Provisionieren benötigter Netzwerke. Da die Arista-Switche wie erwähnt Einblick in die netzwerkseitigen Aktivitäten des vCenter erhalten, erfahren sie, wenn VLAN-basierte Portgruppen in VMware angelegt werden. Falls ein VLAN auf dem Switch noch nicht existiert, kann VM Tracer es so automatisch anlegen und auch wieder löschen, wenn es nicht mehr benötigt wird. Das sorgt dafür, dass die mittels 802.1Q als VLAN Trunks konfigurierten Switchports nur die minimal benötigten VLANs verwenden, was das Flooding auf Layer-2-Ebene reduziert und somit unnötigen und störenden Broadcast-Verkehr eindämmt.

Für den Einsatz von VM Tracer sind zwei Konfigurationsschritte notwendig, die in Minutenschnelle umgesetzt sind: Zunächst muss sich der Switch beim vCenter authentifizieren, dabei werden bis zu vier vCenter-Systeme pro Switch unterstützt. Nach der Authentifizierung kann VM Tracer die SOAP-API des vCenters abfragen. Im zweiten Schritt versetzt der IT-Verantwortliche die mit den ESXi-Servern verbundenen Switch-Interfaces in den VM-Tracer-Modus. Dies veranlasst die Switche über sogenannte Netzwerk-Discovery-Protokolle wie CDP oder LLDP, die ESXi-Server über die angeschlossenen Ports zu informieren. Die ESXi-Server nehmen diese Discovery-Pakete entgegen und aktualisieren das vCenter mit den darin enthaltenen Informationen. Daraufhin kann VM Tracer die Information erneut aus dem vCenter ziehen und VMs mit ihren virtuellen NICs und deren MAC-Adressen mit den physischen Ports, an denen sie angeschlossen sind, korrelieren.

So kann das Netzwerkteam dank VM Tracer lästige, repetitive und fehleranfällige Konfigurationsschritte automatisieren und die für das Troubleshooting benötigte Zeit

EOS kostenlos ausprobieren

Wollen Sie die Funktionen von Arista Switchen und die einfache Konfiguration testen, lässt sich dies dank "vEOS" [4] kostenlos durchführen. Arista bietet sein Switch-Betriebssystem in einer virtuellen Maschine an, die auf allen gängigen x86-Hypervisoren läuft. Auch der Aufbau komplexer Laborumgebungen und der virtuelle Nachbau von Produktionsumgebungen mit mehreren vEOS-Instanzen ist somit kein Problem – so stellen Sie eine Spine-Leaf-Netzwerkumgebung virtuell nach. Auswirkungen von Konfigurationsänderungen auf die Netzwerkfunktion können dank vEOS sehr einfach simuliert werden.

wird minimiert, da sich nun auf dem Switch oder in CloudVision einsehen lässt, welche VMs mit welchem Switch-Port verbunden sind. Und dies unabhängig davon, ob sie mit NSX in logische Overlay-Netzwerke getunnelt wurden oder über Distributed- oder Standard-Switche in klassischen VLANs kommunizieren.

Fazit

VMwares Distributed Switch vereinfacht bereits VLANs zur Separierung von Layer-2-Netzwerken im Vergleich zu anderen Hypervisoren. Dennoch müssen die Netzwerkadministratoren sicherstellen, dass alle VLANs den richtigen Switch-Ports zugewiesen sind – insbesondere in größeren Umgebungen stellt dies eine manuelle, fehleranfällige und insgesamt undankbare Aufgabe dar. Hier können Features wie VM Tracer, das auf den Arista-Switchen zur Verfügung steht, dem Netzwerk-Team viele Aufgaben abnehmen, indem VLANs automatisch bei Bedarf angelegt werden und zudem aufzeigen, welche VMs an welchen Switch-Ports angeschlossen sind. Noch angenehmer wird das Netzwerkerleben, kommt VMware NSX als SDN-Plattform zum Einsatz. Dadurch sinkt die Anzahl der benötigten VLANs drastisch, indem sich über die standardisierte Overlay-Technologie VXLAN-Netzwerke in Software anlegen, verwalten und wieder entfernen lassen. Auf Switch-Seite wird für Tausende von VXLAN-Netzwerken nur ein Transport-VLAN benötigt.

Jede Lösung zieht allerdings neue Herausforderungen nach sich – nun müssen oftmals physische Workloads in VLANs mit virtuellen Maschinen in VXLAN-Netzwerken in eine Layer-2-Broadcast-Domäne zusammengelegt werden. Dies wird zwar von NSX unterstützt, aber der Durchsatz und die Stabilität dieses Layer-2-Bridgings sind für die meisten IT-Organisationen nicht ausreichend. Hier hilft wiederum der Switch-Hersteller, indem er ermöglicht, die physischen Switche mit NSX via OVSDB zu verheiraten. Arista geht hier einen schlauen Weg und sieht die Koppelung zu NSX über den CloudVision-Ansatz vor. Zudem leistet VM Tracer insbesondere beim Troubleshooting von VXLAN Netzwerken wertvolle Dienste, da durch die VXLAN-Overlay-Technologie von NSX eine weitere Schicht hinzukommt, die sich nur auf der Switch-Ebene komplett einsehen lässt. *(jp)*

Link-Codes

[1] Im Test: VMware NSX 6.2
IT-Administrator Januar 2016, Seite 28 bis 32

[2] Arista eAPI
H1Z81

[3] Open vSwitch Database
H1Z82

[4] vEOS-Download
H1Z83