MULTI-CLOUD-NETZWERKE MIT VMWARE NSX DATA CENTER

Die Herausforderungen der digitalen Transformation in Unternehmen

Angesichts steigender Infrastrukturanforderungen und des wachsenden Bedarfs an Redundanzplänen verfolgen viele Unternehmen eine Strategie mit mehreren Rechenzentren. Laut einer 2018 von RightScale durchgeführten Cloud-Studie verfügen 81% der Unternehmen über eine Multi-Cloud-Strategie, wobei sie im Durchschnitt beinahe fünf Clouds nutzen.[1] IT-Organisationen sind im Hinblick auf ihre Rechenzentren häufig mit Management-, Schutz-, Verbindungs- und Compliance-Problemen konfrontiert. Diese Rechenzentren erfordern oftmals manuelle Netzwerk-Neukonfigurationen, um Mobilität zwischen Rechenzentrumsstandorten oder Clouds zu gewährleisten.

Unternehmen versuchen, sich für sämtliche Szenarien zu rüsten – von Naturkatastrophen bis hin zu Cyber-Angriffen. Dabei kommen kostspielige Disaster Recovery-Pläne zum Einsatz, um unternehmenskritische Anwendungen zu schützen und potenzielle Umsatzeinbußen oder Beeinträchtigungen für den Geschäftsbetrieb so gering wie möglich zu halten. Laut eines 2016 veröffentlichten Reports liegen die durchschnittlichen Kosten eines Rechenzentrumsausfalls bei 740.357 US-Dollar[2], wobei sich die Kosten anderer bekannt gewordener Ausfälle auf bis zu 150 Millionen US-Dollar beliefen. Business Continuity und Disaster Recovery(BCDR)-Pläne sind für gewöhnlich komplex, betrieblich herausfordernd oder gar nicht existent. Da Anwendungen heutzutage zunehmend verteilt sind, können manuelle Failover-Neukonfigurationen Stunden oder gar Tage in Anspruch nehmen.

Unternehmen setzen Public Clouds für eine verbesserte Agilität und Skalierbarkeit ein, jedoch stoßen sie dabei auf eine Vielzahl von Herausforderungen. Public Clouds verfügen über eigene Netzwerk- und Sicherheitskonstrukte sowie eine eigene Richtlinienverwaltung. Dadurch entstehen neue Technologiesilos, die höhere Kosten, Komplexität und Risiken nach sich ziehen. Aus unterschiedlichen Netzwerktopologien, Sicherheitsmodellen, Managementumgebungen und Softwareversionen entwickeln sich Portabilitäts- und Interoperabilitätsbarrieren, die die Cloud-Einführung ausbremsen und Anwendungsbereiche begrenzen.

„Mithilfe von VMware NSX Data Center konnten wir eine sichere, erstklassige Rechenzentrumsarchitektur entwickeln. Dadurch kann die Genossenschaftsbank ihren Mitgliedern Services der nächsten Generation bereitstellen. Es gibt keine Ausfallzeiten, wir sparen Geld und das Management ist einfacher."

AMY HYSELL
SVP UND CIO
ARIZONA FEDERAL CREDIT UNION

Beseitigen von Netzwerkbarrieren

Um diesen Herausforderungen zu begegnen, benötigt die IT eine moderne Netzwerklösung, die sowohl Netzwerkkonsistenz und -sicherheit für heterogene Standorte als auch Automatisierung für einen optimierten Multi-Cloud-Betrieb bietet.

Mit VMware NSX® Data Center wird der Netzwerkbetrieb von der zugrunde liegenden Hardware auf eine verteilte Virtualisierungsebene abstrahiert. Somit erzielen Sie ein hohes Maß an Agilität, Sicherheit und Einsparungen, das mit physischen Netzwerken undenkbar gewesen wäre. Netzwerkservices wie Switching, Routing, Firewalling und Lastausgleich befinden sich näher an der Anwendung und sind über die gesamte Umgebung verteilt.

Mit der Kombination aus NSX Data Center und VMware NSX® Cloud können IT-Administratoren mehrere Private und Public Cloud-Umgebungen verwalten und verfügen dabei über eine einheitliche Strategie für Netzwerkfunktionen und konsistente Sicherheit. Dadurch entsteht ein Hybrid Cloud-Modell für Netzwerk und Sicherheit. Im Rahmen dieser Lösung lassen sich bei Bedarf Layer 2-Domänen auf mehrere Rechenzentren erweitern. Somit werden die IP-Adressen von Anwendungen beibehalten und standortübergreifende Failover-Szenarien unterstützt. Dadurch entfallen manuelle Netzwerk- und Neukonfigurationen und Sie erreichen eine hohe betriebliche Effizienz durch Netzwerkautomatisierung. Netzwerk- und Sicherheitsrichtlinien sind an den Anwendungskontext gebunden und daher über die gesamte Lebensdauer mit dem individuellen Workload verknüpft.

1 State of the Cloud Report, RightScale Inc., 2018 www.rightscale.com/2018-cloud-report

2 Cost of Data Center Outages, Ponemon Institute, Januar 2016 https://www.ponemon.org/blog/2016-cost-of-data-center-outages

HIGHLIGHTS

- Einheitliches Netzwerk- und Sicherheitsmodell zur Beseitigung manueller Netzwerk- und Neukonfigurationen für eine hohe betriebliche Effizienz durch Netzwerkautomatisierung
- Migration von VMs oder ganzen Rechenzentren von einem Standort zum anderen – bei lediglich minimalen Anwendungsausfallzeiten oder komplett unterbrechungsfrei
- Bereitstellen sicherer und nahtloser Anwendungsmobilität für einfache Migrationen in und aus der Cloud oder zwischen physischen Standorten

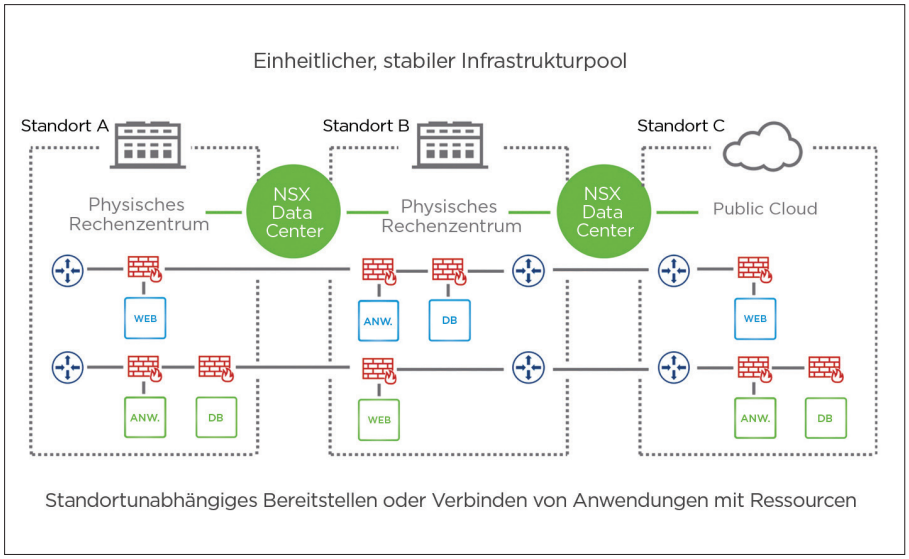

Abbildung 1: Minimale Auswirkungen von Ausfällen dank Multi-Site Pooling

Wichtige Kundenszenarien

Rechenzentrumserweiterung

Mit NSX Data Center und NSX Cloud werden interne Rechenzentren nahtlos auf andere physische Standorte bzw. die Cloud erweitert. Unternehmen profitieren dabei von Skalierbarkeit, Redundanz und Einsparungen. Zudem bietet VMware NSX Hybrid Connect IT-Administratoren eine sichere, nahtlose Anwendungsmobilität zwischen VMware vSphere®-Umgebungen, wodurch sich unterbrechungsfreie Live-Migrationen sowie geplante, umfangreiche Migrationen mit minimalen Ausfallzeiten durchführen lassen.

NSX Data Center verknüpft die Netzwerkservices von Anwendungen (z.B. dieselbe IP-Adresse, Sicherheitsrichtlinie und weitere Services) mit dem jeweiligen Workload und behält diese dadurch bei. Somit werden schnelle Migrations- und Failover-Vorgänge sichergestellt. Folglich bleiben die mit den VM- oder containerbasierten Workloads verknüpften IP-Adressen und Sicherheitsrichtlinien konsistent – auch dann, wenn die Workloads dynamisch zwischen Standorten verschoben werden.

NSX Data Center unterstützt zudem sicheren, verschlüsselten Anwenderzugriff auf private Unternehmensanwendungen (SSL-VPN) sowie standortübergreifende Konnektivität zwischen NSX Edge Gateways und Remote-Standorten (IPsec-VPN) mit optionalen VPN-Gateways oder Hardware-Routern von anderen Anbietern.

Disaster Avoidance und Recovery

Ein modernes Rechenzentrumsdesign erfordert eine verbesserte Redundanz sowie BCDR bei Ausfällen. Unternehmen mit hohen Anforderungen an die Anwendungsverfügbarkeit setzen auf eine Disaster Avoidance-Strategie (Aktiv/Aktiv-Bereitstellung). Im Gegensatz dazu steht die Disaster Recovery-Strategie (Aktiv/Passiv-Bereitstellung).

NSX Data Center stellt konsistente logische Netzwerk- und Sicherheitsfunktionen für geschützte und Recovery-Standorte bereit, wodurch Recovery Time Objective(RTO)-Intervalle bei Ausfällen verkürzt werden. Da sich Netzwerk- und Sicherheitsfunktionen konsistent über mehrere Standorte erstrecken, können Anwendungen am Recovery-Standort wiederhergestellt und die jeweiligen Netzwerk- (IP-) und Sicherheitskonfigurationen beibehalten werden. Zudem lassen sich mit NSX Data Center ganz einfach Testnetzwerke erstellen, mit denen Recovery-Pläne ohne Beeinträchtigung der Produktionsumgebung getestet werden können.

Im Zusammenhang mit Disaster Avoidance werden durch Multi-Site Pooling einheitliche, nahtlose und stabile Infrastrukturpools erstellt, um Anwendungen rechenzentrumsübergreifend sowie in der Cloud mithilfe einer zentralen konsistenten Netzwerkplattform auszuführen. Ebenso können Anwendungen standortunabhängig bereitgestellt und standortübergreifend mit Ressourcen verbunden werden, um der Disaster Avoidance-Strategie, geplanten sowie ungeplanten Ausfällen oder einer besseren Ressourcenauslastung Rechnung zu tragen.

Workload-Mobilität

Workloads müssen oftmals aus den unterschiedlichsten Gründen und nach Bedarf zwischen Standorten verschoben werden. Zu diesen Gründen zählen u.a. Rechenzentrumsmigrationen, -konsolidierungen, -Upgrades und Sicherheits-Patches sowie Cloud-Onboarding, Cloud-Bursting und Disaster Avoidance.

NSX Data Center und NSX Cloud bieten eine nahtlose Workload-Mobilität, indem sie dieselbe virtualisierte Netzwerk- und Sicherheitsplattform in die Cloud erweitern, die IT-Organisationen für ihre interne Infrastruktur verwenden. Dies führt zu einer einheitlichen Netzwerk- und Sicherheitskonfiguration für Private und Public Cloud-Ressourcen. Dadurch können sich Unternehmen auf den zunehmenden Public Cloud-Betrieb vorbereiten und gleichzeitig Mobilität und Konsistenz sowohl von Workloads als auch den zugehörigen Richtlinien in den verschiedenen Umgebungen sicherstellen.

Produktionsanwendungen können in die Public Cloud verschoben werden, um native Cloud-Services ohne komplexe Konvertierungen oder Umstrukturierungen zu nutzen. Mit NSX Hybrid Connect können Migrationen zwischen vSphere-basierten Clouds noch schneller durchgeführt werden. Zudem werden umfangreiche und unterbrechungsfreie Migrationen sowie kontinuierliches Netzwerk-Routing zwischen Standorten unterstützt.

Unternehmen können Workloads nahtlos von einem Standort zum anderen verschieben – zwischen Rechenzentren oder vom Rechenzentrum in die Cloud – und müssen sich dabei keine Sorgen um die Kompatibilität von VM-Formaten machen. NSX Hybrid Connect bietet automatische Image-Konvertierungen in das gewünschte Cloud-Format, sodass VMs ganz einfach platziert oder migriert werden können.

Zusammenfassung

VMware stellt eine moderne Netzwerkvirtualisierungslösung für konsistente Netzwerk- und Sicherheitsfunktionen an heterogenen Standorten bereit. Dadurch unterstützt NSX Data Center eine Vielzahl von Multi-Cloud-Anwendungsbereichen – von nahtloser Rechenzentrumserweiterung über Multi-Data Center Pooling bis hin zu schneller Workload-Mobilität. Kunden weltweit setzen auf die NSX Data Center-Lösung und ihre Multi-Cloud-Netzwerkfunktionen, um zuverlässige, flexible, agile und hochverfügbare Rechenzentrumsumgebungen zum optimalen Ausführen Tausender Workloads aufzubauen.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com Zweigniederlassung Deutschland Willy-Brandt-Platz 2 81829 München Telefon: +49 89 370 617 000 Fax: +49 89 370 617 333 www.vmware.com/de