Broschüre

HPE aruba networking

Fünf Designprinzipien für ein intelligenteres Rechenzentrum

Weniger Komplexität im Rechenzentrum und schnellere Automatisierung, Integration und Sicherheit – mit Architekturen für verteilte Services.

Hewlett Packard Enterprise | mat

Einleitung

Die Nachfrage, Mehrwert zu generieren, nimmt rapide zu. Daher setzen IT-Führungskräfte für erfolgreiche digitale Initiativen auf die Applikationsmodernisierung und Cloud-Betriebsmodelle. Dazu müssen traditionelle Infrastrukturen modernisiert werden. Das wiederum kann so viele Probleme schaffen, wie es löst. Viele Unternehmen sind darauf nicht vorbereitet und sehen sich Inseln von isoliertem Computing und Datenspeicher, unzusammenhängenden Netzwerk- und Sicherheitsarchitekturen sowie Prozessen ausgesetzt, die eine zentrale IT-Verwaltung, Orchestrierung, Sicherheit, Richtlinien und Transparenz behindern.

Während sich die Netzwerktechnologie für Rechenzentren weiterentwickelt hat, um leistungsstärkere 100/400G-Leaf-Spine-Fabrics bereitzustellen, sind Sicherheits- und Servicearchitekturen nicht entsprechend vorangekommen. Die Netzwerkmodernisierung erfordert Automatisierung und API-basierte Programmierbarkeit für die Integration in Cloud-Orchestrierungs- und Management-Plattformen. Diese Umstellung bedeutet, dass Infrastruktur und Betrieb ebenfalls modernisiert werden müssen, um sie an die Cloud-zentrierten, Microservice-basierten Anwendungsarchitekturen und die agilen IT-Servicebereitstellung anzupassen, die Hyperscale-Rechenzentren seit Jahren nutzen.

Es ist paradox, dass das Netzwerk zwar wichtiger denn je ist, aber gleichzeitig unsichtbar sein soll – die Anwendungsentwicklung oder Geschäftsprozesse nicht behindern soll.

Um dem gerecht zu werden, verwenden viele Unternehmen eine zustandsunabhängige Rechenzentrums-Fabric, die die Netzwerk-Services nicht effizient einbindet und eine komplexe Servicekette anlegt. Die reine Menge, die Geschwindigkeit und die Vielfalt des Datenverkehrs erfordern jedoch eine Umstellung von manuellen, reaktiven und isolierten Prozessen für die Verwaltung von Netzwerkverbindungen und Datenflüssen zu ML/KI-basierten Plattformen, die Verbindungen aufbauen, erweitern und sichern sowie die Infrastruktur verwalten.

Es gibt eine bessere Möglichkeit: Eine Netzwerkarchitektur, die einfacher zu implementieren, bereitzustellen und zu verwalten ist, und die transparent auf die Anforderungen von Anwendungsentwicklern, IT-Betrieb, DevOps und Unternehmen reagiert.

Die Rechenzentrums-Fabrics der nächsten Generation ermöglichen Unternehmen, sich von älteren Architekturen abzulösen und auf der selben Stufe wie Hyperscaler zu konkurrieren. Dazu konsolidieren sie zustandsabhängige Funktionen in der gesamten Fabric und stellen eine Vielzahl von Infrastrukturservices auf neue und integrierte Art und Weise bereit. Die Fabric darf nicht mehr als reine Segmentierungs- und Konnektivitätslösung betrachtet, sondern muss als Lösung verstanden werden, die alle für die Skalierung von Workloads zulässigen Infrastrukturservices unterstützt.

Dieses Dokument untersucht fünf wichtige Designprinzipien, die bei der Gestaltung eines zukünftigen Rechenzentrums zu berücksichtigen sind:

- Modernisierung mit Hardware-beschleunigten DPU-fähigen Switches
- Umstellung auf eine Architektur für verteilte Services der vierten Generation
- Positionierung von Zero Trust dichter an den Anwendungen
- Kombinieren von Netzwerk- und Sicherheits-AIOps
- Nutzung von Edge, Colocation und IaaS

1 – Modernisierung mit DPU-fähigen Switches

Traditionell stellten die reinen CPUs die Rechenleistung für Hyperscale- und Rechenzentren in Unternehmen bereit. In jüngerer Zeit haben GPUs (Grafikprozessoren) eine bedeutende Rolle übernommen. Ursprünglich wurden sie zur Bereitstellung umfangreicher Echtzeitgrafiken eingesetzt, und aufgrund ihrer Parallelverarbeitungsfähigkeiten sind sie ideal geeignet für beschleunigte Computing-Aufgaben, einschließlich Anwendungen für künstliche Intelligenz, Deep Learning und Big-Data-Analysen.

Auf dem Markt ist eine neue Art von Prozessor namens DPU (Data Processing Unit) erschienen, der sich schnell zu einem wichtigen Bestandteil der datenorientierten beschleunigten Computing-Reihe entwickelt. Bei DPUs handelt es sich um speziell entwickelte Hardware, die dazu dient, den Datenverkehr so auszulagern, dass rechenintensive Aufgaben auf CPU- und GPU-Ressourcen optimiert werden können.

DPUs verfügen über eigene hardwarebasierte Prozessoren, werden häufig in Hyperscale-Rechenzentrumsservern bereitgestellt und führen eine große Anzahl an beschleunigten Rechen-, Cloud-, Netzwerk-, Sicherheits- und Speicheraufgaben aus, wie unter anderem Verschlüsselung, Firewall, Lastausgleich, NAT und Telemetrie. Diese Funktionen unterstützen die isolierten, Cloud-nativen Bare-Metal-Computing-Plattformen, die die nächste Generation des Computings mit Cloud-Skalierung ausmachen.

Die DPU-Technologie hat sich von einer rein serverbasierten Technologie zu einer Verfügbarkeit in Top-of-Rack-Switches entwickelt. Diese neue Switch-Kategorie für verteilte Services vereint standardbasierte Ethernet/IP-basierte Switches mit integrierter, hardwarebeschleunigter, umfassend programmierbarer DPU-Technologie in einer zentralen leistungsstarken und sicheren Netzwerklösung für das Rechenzentrum und die Cloud.

„HPE Aruba Networking und AMD Pensando haben für die erste Architektur für verteilte Services gesorgt, mit der Unternehmen Netzwerkinfrastrukturen aufbauen und betreiben können, die genauso funktionieren und wachsen, wie bei den Großen der Hyperscale-Infrastruktur.“

Alan Weckel, Founder und Technology Analyst, 650 Group

Damit können Betreiber branchenübliche Leaf-Spine-Netzwerke um zustandsabhängige verteilte Mikrosegmentierung, Ost-West-Firewalling, NAT, Verschlüsselung und Telemetrie-Services erweitern – und zwar dichter an den Stellen, an denen kritischen Computing- und Storage-Workloads am Edge des Computing-Netzwerks verarbeitet werden.

Im Gegensatz zu dedizierten SmartNICs, die im/in Server(n) installiert werden, kann ein Switch für verteilte Services am Server Top-of-Rack bereitgestellt werden und bietet verteilte Services für alle Server und Hosts im Rack.

Switches für verteilte Services erfordern für die Bereitstellung der verteilten Services im großen Maßstab und mit Kabelgeschwindigkeitsleistung keine Änderungen an der Serverhardware oder -software, treffen keine Annahmen über das Betriebssystem eines Servers, erfordern nicht die Installation eines Treibers oder Agenten auf Servern und lassen sich in neue oder bestehende Brownfield-Rechenzentren in Unternehmen und Private Clouds integrieren.

2 – Umstellung auf eine Architektur für verteilte Services der vierten Generation

Dank Hardware und Software können Rechenzentrums-Fabrics heutzutage die Infrastrukturservices bereitstellen, die zur Unterstützung von Workloads im großen Maßstab erforderlich sind, und diese Infrastruktur über eine reine Segmentierungs- und Konnektivitätslösung hinaus erweitern.

Schon vor über einem Jahrzehnt haben Hyperscaler erkannt, dass sie zur Erweiterung ihrer Fabrics die Komplexität beseitigen mussten, die damit einhergeht, dass man für jede Appliance im Rechenzentrum ein anderes Betriebssystem (BS) und einen anderen Service braucht. Statt für jeden Infrastrukturservice einen neuen Anbieter ins Boot zu holen, wurde jede Funktion als einzelnes BS aufgesetzt, das durch einen einzelnen automatisierten Controller verwaltet wird. Durch diese Integration und Vereinfachung lassen sich Millionen von Workloads unterstützen.

Traditionell/Legacy Dritte Generation	Nächste Generation Vierte Generation
• Switching- und Konnektivität-orientiert • Netzwerk-/Sicherheitsservices sind pro VM angelegt • Hoch zentralisierte L4-7-Switches, limitierte Erweiterbarkeit • Hohe Komplexität und Kosten (Geräte, Agenten) • Begrenzte Verfügbarkeit für Automatisierungen aufgrund von Komplexität	• Cloud-orientiertes Betriebsmodell • Vereinheitlichung von Fabric- und Infrastrukturservice • Umfassend verteilte Services für die gesamten Workloads in Rechenzentren • Vereinfachtes Hinzügen von Services in die Rechenzentrums-Fabric • Umfassende Automatisierung, Transparenz und Telemetrie

Abbildung 1. Umstellung auf eine moderne Rechenzentrums-Fabric

Die **vierte Generation** der Architektur des Rechenzentrums führt dieselbe Zusammenlegung zustandsabhängiger Funktionen für die gesamte Fabric ein. Die Fabric ist nicht mehr länger eine zustandsunabhängige Verbindung für Workloads und Services, sondern kann nun eine Vielzahl vereinfachter und integrierter Infrastrukturservices bereitstellen. So lassen sich auch das Design und die Bereitstellung vereinfachen und gleichzeitig sicherstellen, dass zustandsabhängige Services am Fabric-Edge verfügbar sind.

Voraussetzung dafür sind zwei der wichtigsten Funktionen im Rechenzentrum: Ost-West-Sicherheit, die für jede Zero-Trust-Bereitstellung erforderlich ist, und vollständige (nicht stichprobenartige) Netzwerktelemetrie. Beide sind grundlegend für aufgeschlüsselte Workloads. Die Sicherheit innerhalb des Rechenzentrums ist extrem wichtig, um Datenschutzverletzungen zu verhindern. Die Telemetrie eröffnet dabei Möglichkeiten für neue Lösungen, die auf maschinellem Lernen basieren und die Sicherheit und den Netzwerkbetrieb auf eine Weise automatisieren können, die ohne hochpräzise Telemetrie des Rechenzentrums nicht möglich wäre.

Diese neue Architektur räumt auch mit suboptimalen Designoptionen auf, die viele Unternehmen entwickelt haben – und richtet stattdessen Softwareagenten auf den Servern ein, um Mikrosegmentierung bereitzustellen. Durch die Integration dieser Services in die Netzwerk-Fabric haben Betreiber nun eine erstklassige Designoption, die wertvolle Server-CPU-Zyklen freisetzt, die andernfalls durch die notwendige Verarbeitung rechenintensiver Netzwerk-Services verloren gehen würden.

Das Erstellen einer solchen Architektur beim Aufbau neuer Hyperscale-Cloud-Umgebungen von Grund auf kann zwar machbar sein, wie können jedoch bestehende Rechenzentren von dieser top-modernen Technologie profitieren?

Logisch wäre, diese Services zunächst im Top-of-Rack (ToR) Leaf Switch bereitzustellen, um ohne einen teuren, zeitaufwändigen kompletten Austausch auf dem gesamten Rechenzentrum von einer Architektur für verteilte Services zu profitieren. Diese Bereitstellungsstrategie ist sehr attraktiv, da sie Unternehmen ermöglicht, einzelne Server Racks oder PODs im Rechenzentrum unterbrechungsfrei zu migrieren.

Eine Architektur für verteilte Services der vierten Generation kann:

- Latenzen verringern und die Sicherheit verbessern, indem sie Services so dicht wie möglich an den Anwendungen verteilt
- Gerätewildwuchs beseitigen, wodurch die Infrastruktur- und Wartungskosten gesenkt werden
- Die Notwendigkeit verringern oder beseitigen, kostspielige Software-Server-Agenten (für Lizenzierung und CPU-Verarbeitung) bereitzustellen
- Durch Verringern der Latenz über Bereitstellungsservices am Fabric-Edge die Netzwerkleistung und Bandbreite optimieren
- Die betriebliche und Richtlinien-Effizienz von Netzwerk- und Sicherheitsteams steigern helfen

3 – Positionierung von Zero Trust dichter an Ihren Anwendungen

Cybersicherheitsbedrohungen haben sich in den letzten Jahren erheblich verändert. Zero Trust ist eine grundlegende Praxis für Sicherheit im Unternehmen, die Datenschutzverletzungen verhindert und interne laterale Bewegungen reduziert, indem sie davon ausgeht, dass sich der Angreifer in der Umgebung selbst befindet. Im Rechenzentrum bedeutet das, dass jeder Partei und dem gesamten Verkehr im Netzwerk misstraut wird, es sei denn, eine Sicherheitsrichtlinie erlaubt sie ausdrücklich. Die Segmentierung überprüft den gesamten Ost-West-Verkehr im Rechenzentrum zustandsabhängig und wendet Richtlinien an, um zu verhindern, dass sich böswillige Akteure lateral durch das interne Netzwerk bewegen.

Netzwerk-Services müssen eine disaggregierte Skalierung von Anwendungen unterstützen. In der Vergangenheit wurden diese gesamten Services in Form diskreter Appliances oder VMs bereitgestellt, die eine Verbindung mit dem Netzwerk eingingen, aber nicht Teil der Fabric waren. Das führt zu Schwierigkeiten, da verschiedene Anbieter verwaltet werden müssen, der Datenverkehr über die gesamte Fabric verteilt und die Unübersichtlichkeit zwischen dem Netzwerk und den Serviceteams höher ist.

„In unserer Zusammenarbeit mit AMD und HPE Aruba Networking nutzen wir den CX 10000 als Grundkomponente für unsere ‘Sichere Netzwerk-Fabric für DXC’ in Rechenzentren weltweit. Das hat unsere Zero-Trust-Sicherheitsarchitektur für die Rechenzentren und den Edge revolutioniert. Was früher mit unseren Segmentierungs- und Compliance-Anforderungen Hunderte von virtuellen und physischen Firewalls erforderte, wird jetzt nativ inline auf der Plattform bereitgestellt und führt zu prognostizierten TCO-Einsparungen von 83 %.“

- Nitin Jain, Global Network Lead, DXC Technology

Durch die Integration zustandsabhängiger Servicekapazitäten in eine Rechenzentrums-Fabric werden Sicherheit und Transparenz dichter an die Stellen gebracht, an denen Anwendungen und Workloads verarbeitet werden, ohne dass dies Auswirkungen auf die vorhandene Netzwerkarchitektur oder Softwarekonfigurationen hat. Dadurch werden das Sicherheitskonzept und die Transparenz in Rechenzentren verbessert, die Anschaffungskosten gesenkt und der Betrieb vereinfacht. Die Architektur überwacht den Datenverkehr unmittelbar an den Top-of-Rack (ToR)-Switches. Damit entfällt die Notwendigkeit, den Verkehr durch traditionelle zentrale Anwendungen zu lenken, und Netzwerküberlastung und Komplexität werden verringert.

Eine Architektur für verteilte Services dehnt Zero Trust tiefer in das Rechenzentrum aus – an den Edge von Netzwerk-Servern, wo es eine feinkörnige Mikrosegmentierung sowie eine starke Skalierung und Stärkung der Sicherheit geschäftskritischer Workloads bietet – mit einer hundertfachen Skalierung und der zehnfachen Leistung bei einem Drittel der Gesamtbetriebskosten traditioneller Lösungen.

4 – Kombinieren von Netzwerk- und Sicherheits-AIOps

Die Telemetrie dient als zentrale Informationsquelle für Vorgänge im Rechenzentrum. Um jedoch sicherzustellen, dass die Informationen korrekt sind, muss die Telemetrie präzise und im gesamten Rechenzentrum allgegenwärtig sein.

Netzwerkbetriebsteams haben oft damit zu kämpfen, dass ihnen die Telemetrie für Automatisierungen nicht ausreicht, sodass sie mit ihrer begrenzten zur Verfügung stehenden telemetrischen Information einfach Visualisierungen durchführen. Da die heutigen Rechenzentrums-Fabrics keine vollständige Telemetrie leisten können, müssen Untersuchungen des Netzwerks durchgeführt und Software-Agenten eingesetzt werden, um zu wissen, was passiert. Sonden oder Agenten können sehr detaillierte telemetrische Daten liefern, jedoch nur an den Standorten, an denen sie sich befinden. Um eine bessere Transparenz zu erreichen, müssen daher Stichproben von Verkehrsflüssen im gesamten Rechenzentrum genommen werden. Diese Methode erfasst nur Momentaufnahmen des Datenverkehrs und erreicht nicht die Genauigkeit, die heutige ML-basierte Automatisierungslösungen erfordern.

Das ist ein Problem der bisher verwendeten dritten Generation aufgrund eines fragmentierten Ansatzes.

Eine Architektur für verteilte Services löst diese Herausforderungen, indem sie – nativ – genaue und allgegenwärtige Telemetrie im gesamten Rechenzentrum bereitstellt, ohne Auswirkungen auf den Datenverkehr oder erhöhten Kontaktierungsflecken beim Einführen von Gerätekabeln (Fehlerstellen). Sonden oder Agenten sind nicht mehr notwendig, ebenso wenig wie TAP-Aggregationsnetzwerke zum Sammeln telemetrischer Daten. Da die Telemetrie jetzt Teil der Rechenzentrums-Fabric ist, können Rechenzentrumsbetreiber außerdem das Ausmaß ihrer „blinden Flecken“ bei der Telemetrie verringern.

Architekturen der nächsten Generation bieten mehr Vorteile als nur die Telemetrie, und zwar Folgende:

- Bieten Netzwerkteams eine MTTI (Mean-Time-to-Innocence) – mit einer „Zeitmaschine“, mit der sich der Datenverkehr pro Anwendung für jeden fraglichen Verlauf überprüfen und Ursachen für eine schlechte Anwendungsleistung ermitteln lassen
- Lassen sich über eine Rest API integrieren und stellen Flow-Daten für eine Vielzahl von Sicherheits- und Netzwerkleistungstools bereit, einschließlich Advanced Security ML (XDR), Application Dependency Mapping (ADM), AI/Operations (AIOps), SIEM/SOAR, Firewall-Compliance-Vorschriften und Tools zur Zuordnung von Identitätsgruppen
- Erkennen automatisch Anomalien, gruppieren diese in Vorfälle mit gemeinsamen Wurzeln und benachrichtigen Betriebskonsolen, Ticketsysteme und Automatisierungssysteme mit Streaming-Datenanalysen in Echtzeit, sodass Betriebsteams keine unformatierten telemetrischen Daten visualisieren müssen
- Wechseln von teuren, komplexen TAP-Aggregationsnetzwerken mit begrenzten Einblicken hin zur vollständigen Nutzung von KI/ML-Tools mit umfassender hochgenauer Telemetrie in einer Rechenzentrums-Fabric der vierten Generation

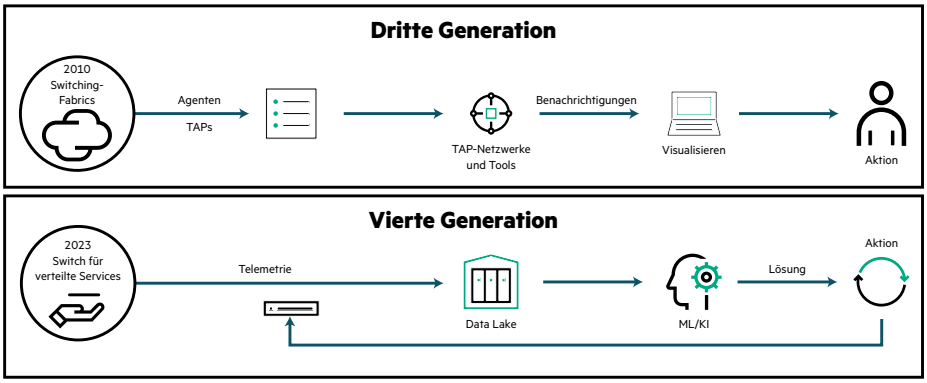


Abbildung 2. Eine neue Ära für den Netzwerkbetrieb

5 – Nutzung von Edge, Colocation und IaaS

Zwei leistungsstarke IT-Trends wachsen zusammen: Die Colocation und eine Infrastructure-as-a-Service vom Edge bis zur Cloud. Die meisten bestehenden Implementierungen basieren auf zentralisierten Architekturen, die Daten in zentralen Rechenzentren, Colocation-Zentren oder in der Cloud sammeln und verarbeiten. In der heutigen Welt wird jedoch eine Fülle von Daten am Edge generiert – an abgelegenen Orten wie Fabrikhallen, Einzelhandelsstandorten, Gesundheitseinrichtungen, intelligenten Gebäuden und Städten.

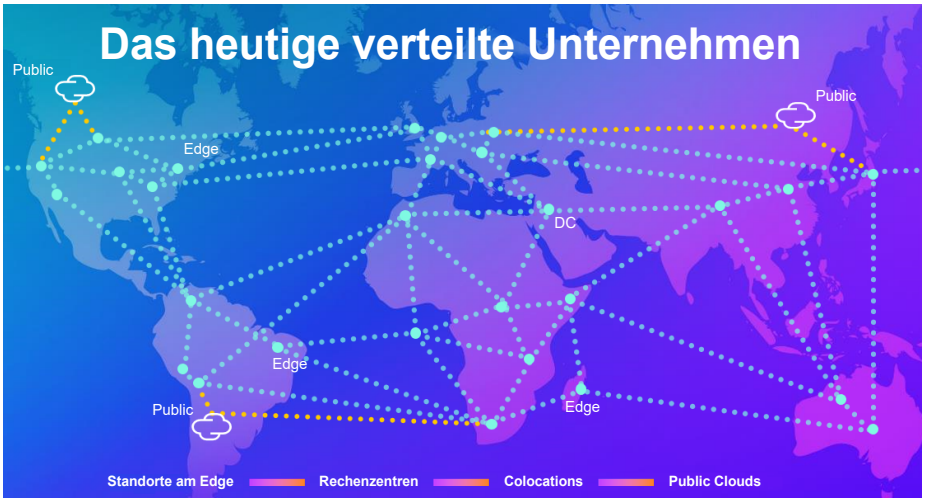


Abbildung 2. Eine neue Ära für den Netzwerkbetrieb

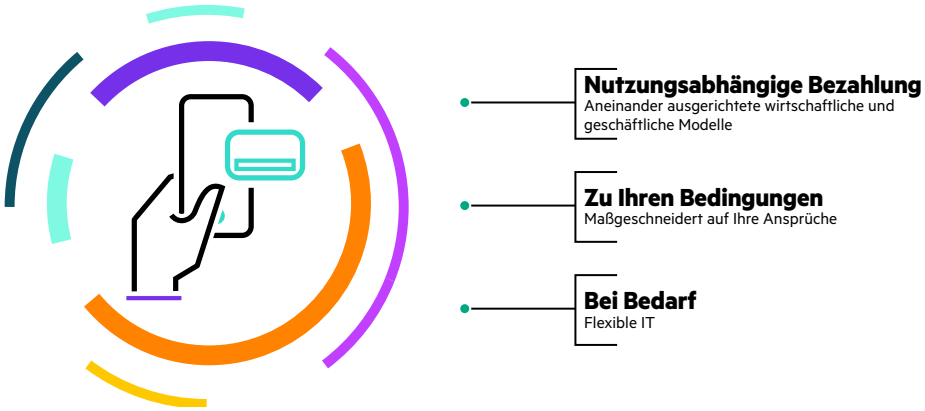
Die Platzierung von Anwendungs-Workloads bestimmt Infrastrukturentscheidungen – und nicht umgekehrt. Die Hybrid Cloud – eine Kombination aus Public Cloud, Edge, Colocation und lokalen Standorten –, ist zum neuen Standard für unternehmenskritische Workloads und unzählige On-Demand-, As-a-Service-Angebote geworden.

Die Colocation in Kombination mit einer As-a-Service-Plattform ist eine großartige Lösung. Die Colocation kann Folgendes bieten:

- Das Beste der Cloud mit nur einem Mandanten bei gleichzeitiger Kontrolle über Anwendungen und Daten
- Geringe Latenz, eine Verbindung mit hoher Bandbreite mit anderen wichtigen Cloud- und Netzwerkanbietern
- Bessere Transaktionsgeschwindigkeit mit direkter Verbindung zu einem breiten Ökosystem von angrenzenden Unternehmen
- Unterstützung für Ihre Nachhaltigkeitsziele durch Vermeidung von Über- oder Unterversorgung sowie energieeffiziente Einrichtungen
- Optimierte IT-Ausgaben ohne Vorabzahlungen, Zahlung nur nach Bedarf und ohne Kosten für ausgehende Daten

Kombinieren Sie diese Vorteile mit einem nutzungsabhängigen Bezahlmodell für Ihre Infrastruktur- und Betriebsanforderungen und Sie erhalten das Beste aus beiden Welten – Public-Cloud-ähnliche Agilität und gemeinsam genutzte Infrastruktur – mit einem einzigen Vertrag, einer einzigen Rechnung und einem einzigen Ansprechpartner. Außerdem bekommen Sie die Möglichkeit, Mitarbeitende vom Betrieb eines Rechenzentrums auf die Arbeit an anderen hochwertigen Tätigkeiten umzustellen.

Moderne Architekturen der vierten Generation nutzen das Potential der Bereitstellungsflexibiliät und der Verbrauchsmodelle von Serviceangeboten für As-a-Service- und Colocation-Rechenzentren voll aus.



In einer Forrester-Studie berichteten Kunden, die HPE GreenLake bereitgestellt hatten, von einer bis zu 80 % schnelleren Markteinführungszeit bei der Bereitstellung komplexer globaler IT-Projekte.

Fazit

Der Wandel von zentralisierten zu verteilten modernen Edge-to-Cloud-Rechenzentren schreitet weiter voran. Daher werden neue Architekturen benötigt, um sichere Konnektivität bereitzustellen und Benutzern und Anwendungen eine einzigartige Erfahrung zu bieten. Diese nächste Welle der Konnektivität von Rechenzentren erfordert leistungsfähigere Fabrics, verteilte Services und flexible Verbrauchsoptionen.

In der neuen Ära der Rechenzentren werden Infrastrukturservices in einer Fabric der vierten Generation zusammengefasst, wodurch man sich nicht mehr auf separate Hardware-Appliances und Softwareagenten verlassen muss, die in stark zentralisierten, suboptimalen Architekturen bereitgestellt werden.

Mit einem vereinfachten Verbrauchsmodell, beschleunigten Netzwerkservices und der Wahl, wie und wo Workloads platziert werden sollen, ist der Zugriff auf die Einfachheit und Skalierbarkeit, die zuvor Hyperscalern vorbehalten war, jetzt allgemein verfügbar.

Die Software und Hardware sorgen jetzt für die Bereitstellung aller Fabric-Services des Rechenzentrums – zustandsunabhängig und zustandsabhängig – über eine gemeinsame Plattform. Zu guter Letzt stehen allen Kunden die Möglichkeiten und der Umfang zur Verfügung, die sie für ihr Unternehmen benötigen.

HPE Aruba Networking

Im Jahr 2022 schlossen sich HPE Aruba Networking und AMD Pensando™ zusammen und brachten den branchenweit ersten Switch für verteilte Services heraus. Der Switch der HPE Aruba Networking CX 10000 Serie ist eine neue Switch-Kategorie für Rechenzentren, die erstklassiges L2/3-Ethernet-Switching mit der integrierten AMD Pensando DPU-Technologie kombiniert.

Damit können Rechenzentrumsbetreiber zustandsabhängige Services nahtlos auf verteilte Art und Weise in ihre Netzwerke einfügen, was wiederum das Design von Rechenzentrumsnetzwerken vereinfacht und die Sicherheit erhöht.

Switches der nächsten Generation für das Rechenzentrum von HPE Aruba Networking verändern alles. Unternehmen sorgen für großartige digitale Erlebnisse für die Kunden und Mitarbeiter mit neuer Skalierbarkeit, Leistung und betrieblicher Effizienz.

HPE GreenLake ist ein Portfolio von Cloud- und As-a-Service-Lösungen, das dazu beiträgt, Ihren Geschäftsbetrieb zu vereinfachen und zu beschleunigen. Es bietet ein Cloud-Erlebnis, wo immer sich Ihre Anwendungen und Daten auch befinden – ob am Edge, im Rechenzentrum, in Colocations oder in Public Clouds. HPE GreenLake basiert auf einem nutzungsabhängigen Bezahlmodell, wird auf einer offenen und sichereren Edge-to-Cloud-Plattform ausgeführt und bietet Ihnen die nötige Flexibilität, um sich neue Möglichkeiten zu erschließen.

Wo erhalten Sie weitere Informationen?

IDC betrachtet, wie Sie den Bedarf an hoher Leistung und Sicherheit mit einer modernen Rechenzentrums-Fabric erfüllen

Weitere Informationen zur Modernisierung von Rechenzentren mit HPE Aruba Networking

Besuchen Sie **ArubaNetworks.com**

BR_SmartDataCenter_RVK_101123

Hewlett Packard Enterprise