

Netzwerkarchitekturen für Multi-Cloud-Lösungen

SD-WAN, Cloud Connectivity und IT-Security

Cloud-Lösungen sind ein wichtiger Bestandteil der Unternehmens-IT, wobei meist Hybrid-Cloud- und Multi-Cloud-Szenarien Anwendung finden. Somit stellt sich zwangsläufig die Frage, wie man die On-Premises IT idealerweise mit den verschiedenen Clouds vernetzt. Hierbei ist zu unterscheiden zwischen der Client-Server-Anbindung und der Konnektivität zwischen Private und Public Clouds. In beiden Fällen gilt es viele Aspekte zu berücksichtigen.

In diesem Training werden typische SD-WAN-Lösungen und IT-Security-Konzepte beleuchtet, welche eine optimale User Experience beim Zugriff auf die IT Services in Multi-Cloud-Umgebungen schaffen. Des Weiteren werden die unterschiedlichen Cloud-Connect-Varianten vorgestellt und ihre Vor- und Nachteile diskutiert. Detailliert wird auf die speziellen Netzwerkfunktionen und Anbindungsoptionen der sogenannten Hyperscaler - Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform und Alibaba Cloud - eingegangen, die neben Oracle, IBM und SAP beleuchtet werden. Mit diesem Wissen werden interaktiv typische Lösungsszenarien erarbeitet.

Kursinhalt

- Multi-Cloud – Netzwerkaspekte und Herausforderungen
- Anforderungen der Anwendungen
- Spezialfall Office 365
- Aufbau und Limitierungen klassischer WANs
- SD-WAN: Konzepte, Lösungen und Marktübersicht
- Security-Konzepte bei SD-WAN: SASE, zScaler und Cisco Umbrella SIG
- Netzwerk- und Security-Konzepte für Microsoft Azure, AWS, GCP, Alibaba, Oracle, IBM und SAP
- Konnektivitätsoptionen für Microsoft Azure, AWS, GCP, Alibaba, Oracle, IBM und SAP
- Lösungen für den Cloud Exchange – Colocation & Interconnection
- Colocation via Equinix Cloud Exchange (ECX) und NTT Global Data Centers EMEA (ehemals eShelter)
- Interconnection via DE-CIX
- Cloud Exchange über Private Cloud-Anbieter
- Interconnection via Carrier
- Typische Designs, Fallbeispiel und Best Practices
- Ausblick
- Abschlussdiskussion und Feedback-Runde

E-Book Das ausführliche deutschsprachige digitale Unterlagenpaket, bestehend aus PDF und E-Book, ist im Kurspreis enthalten.

Zielgruppe

Dieser Kurs richtet sich an Netzwerker, Security-Spezialisten und IT-Architekten, welche Netzwerk- und Security-Lösungen für Multi-Cloud-Lösungen aufbauen oder optimieren möchten. Er vermittelt neben den möglichen Konnektivitätsoptionen auch die typischen Begriffe und Konzepte, welche auf Seiten der Hyperscaler und großen Cloud-Anbieter in diesem Zusammenhang genutzt werden.

Netzwerkern, Security- und IT-Architekten, die bisher weniger mit diesen Themen beschäftigt waren, liefert der Kurs einen idealen Einstieg in die Welt von SD-WAN, Cloud-Konnektivität und moderner Security-Konzepte.

Voraussetzungen

Ein grundlegendes Verständnis von WAN-Technologien, Cloud Computing und IT-Security wird vorausgesetzt.

Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.de/go/CCML

Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

Training	Preise zzgl. MwSt.	
Termine in Deutschland	3 Tage	€ 2.195,-
Termine in Österreich	3 Tage	€ 2.195,-
Online Training	3 Tage	€ 2.195,-
Termin/Kursort	Kursprache Deutsch	
17.09.-19.09.25 Online	15.12.-17.12.25 Online	
17.09.-19.09.25 Wien	27.04.-29.04.26 Frankfurt	
15.12.-17.12.25 Frankfurt	27.04.-29.04.26 Online	

Stand 23.05.2025



Inhaltsverzeichnis

Netzwerkarchitekturen für Multi-Cloud-Lösungen – SD-WAN, Cloud Connectivity und IT-Security

1 Multi-Cloud – Netzwerkaspekte und Herausforderungen	2.4.7 Palo Alto: Prisma SD-WAN	3.3.1 Logischer Aufbau
1.1 Definition: Cloud Computing	2.4.8 Juniper Secure Vector Routing	3.3.2 Google Direct und Carrier Peering
1.1.1 Service-Modelle des Cloud Computings	2.5 Cloud Network as a Service (CNaas)	3.3.3 Cloud Interconnect
1.1.2 Cloud-Varianten – Private Cloud, Public Cloud, ...	2.6 Teridion – Lösungen und Umsetzung	3.3.4 Anbindung Google Cloud mittels Transit VPC
1.2 Client/Server-Kommunikation	2.7 Security-Konzepte bei SD-WAN	3.3.5 Anbindung Google Cloud mittels Transit VPC
1.3 Server/Server-Kommunikation	2.7.1 Routing zu sicheren Zielen	3.4 Alibaba Cloud
1.4 Edge Computing	2.7.2 Lokale Perimeter Security	3.4.1 VPN Gateway
1.5 SLAs: Shared Responsibility	2.7.3 Regionaler Access	3.4.2 Smart Access Gateway – Eigene SD-WAN-Lösung
1.6 Anforderungen der Anwendungen	2.7.4 Secure Service Edge (SSE)	3.4.3 Express Connect
1.7 Öffentliche IP Services	2.8 SSE und SASE – Herstellerüberblick	3.5 Oracle Cloud
1.8 Spezialfall Microsoft 365	2.8.1 Cisco Secure Access	3.5.1 Oracle Aufbau
1.9 Veränderung der IP-Verkehrsflüsse in Unternehmen	2.8.2 Meraki SASE – Cisco Secure Connect	3.5.2 VPN Connect
1.10 Konnektivitätsoptionen für Multi-Cloud-Lösungen	2.8.3 Fortinet SASE	3.5.3 Fast Connect
1.10.1 Public Internet Peering	2.8.4 Netskope Security Cloud	3.6 IBM Cloud
1.10.2 IP VPN	2.8.5 Palo Alto Networks Prisma Access	3.6.1 IBM Cloud Direct Link Exchange und Cloud Exchange for Equinix
1.10.3 Dedicated WAN	2.8.6 Zscaler	3.6.2 IBM Cloud Direct Link Connect
1.10.4 SD-WAN	2.9 Vom Hybrid WAN zu Internet-only	3.6.3 IBM Cloud Direct Link Dedicated
1.10.5 Cloud Exchange	3 Cloud-Konnektivität im Detail	3.6.4 IBM Cloud Direct Link Dedicated Hosting
1.10.6 Cross-Cloud Interconnect	3.1 Microsoft Azure	3.7 SAP HANA Enterprise Cloud
1.10.7 Cloud-Anbieter als Carrier	3.1.1 Azure Netzwerkstrukturen für IT-Architekten	3.7.1 VPN
1.11 Erreichbarkeit von Services in der Cloud	3.1.2 IP-Adressierung in Azure	3.7.2 Direct Connection – MPLS
1.12 Applikationsmigration in die Cloud	3.1.3 Verschlüsselung beim Datentransport	3.7.3 SAP Cloud Peering
1.13 Security in Cloud-Umgebungen	3.1.4 Gateways (für VPN etc.) in Azure	4 Cloud Exchange
1.14 Landing Zone	3.1.5 Lastausgleich	4.1 Cloud Exchange – Colocation & Interconnection
1.14.1 Cloud-Strategie	3.1.6 N-schichtige Windows-Anwendung in Azure	4.2 Google Cross-Cloud Interconnect
1.14.2 Weiterentwicklung: Landing Zone Lifecycle	3.1.7 Routing in Microsoft Cloud-Umgebungen	4.3 Equinix Cloud Exchange (ECX)
1.14.3 Best Practices	3.1.8 Public Internet Peering	4.3.1 Service Level Agreements
2 SD-WAN und Security in Multi-Cloud-Umgebungen	3.1.9 MS ExpressRoute	4.3.2 Ports, Virtual Connections und Connectors
2.1 Klassisches WAN	3.1.10 ExpressRoute – Verschlüsselung	4.4 NTT Global Data Centers
2.2 SD-WAN: Arbeitsweise	3.1.11 MS ExpressRoute – Tarifierung	4.4.1 Multi-Service-Konzept mittels MSIP Port
2.2.1 SD-WAN: Kundennutzen	3.1.12 ExpressRoute Gateways	4.4.2 Cloud Connect - Virtuelle Dienste
2.2.2 Lokaler Break-out	3.1.13 Geography	4.5 Cloud Exchange via DE-CIX
2.3 SD-WAN Marktübersicht	3.1.14 MS ExpressRoute – Anbieter	4.5.1 Umsetzung von AWS Direct Connect via DE-CIX DirectCloud
2.4 SD-WAN – Hersteller-Übersicht	3.1.15 Azure ExpressRoute – Big Picture	5 Fallbeispiel und Zusammenfassung
2.4.1 Cisco Catalyst SD-WAN (Viptela)	3.1.16 IP VPN	5.1 Fallstudie
2.4.2 Cisco SD-WAN powered by Meraki	3.1.17 Azure Virtual WAN	5.2 Zusammenfassung, Diskussion und Feedback
2.4.3 Velocloud SD-WAN – Broadcom	3.2 Amazon Web Services – Basics	
2.4.4 Fortinet Secure SD-WAN	3.2.1 VPCs und Subnetze	
2.4.5 Versa Networks	3.2.2 AWS Landing Zone	
2.4.6 HPE Aruba EdgeConnect (SilverPeak)	3.2.3 Konnektivität VPC zu VPC	
	3.2.4 Hybrid-Konnektivität	
	3.2.5 Public Internet Peering	
	3.2.6 AWS Direct Connect	
	3.2.7 DNS, NAT und Security	
	3.3 Google Cloud Platform	

