

ECMS2

Engineering Cisco Meraki Solutions Part 2

Der Kurs vertieft Ihr Wissen über die Technologie von Cisco® Meraki™. In diesem technischen Kurs für Fortgeschrittene lernen Sie, wie Sie Netzwerkeinführungen und -integrationen mit der Cisco Meraki-Plattform planen können. Anhand praktischer Anweisungen und Erfahrungen lernen Sie, wie Sie Meraki-Netzwerke betreiben und komplexe Netzwerkvorfälle mit Hilfe des Meraki-Dashboards und der Analysefunktionen beheben.

Sie werden auch lernen, wie Sie Meraki-Architekturen für Redundanz, High-Density und Skalierbarkeit entwerfen, indem Sie umfassende Meraki-Produktfunktionen implementieren, um die Designziele zu erreichen. Dieser Kurs ist der zweite von zwei Kursen, der Sie auf die Cisco Meraki-Zertifizierung vorbereitet.

Kursinhalt

- Planning new Meraki architectures and expanding existing deployments
- Designing for scalable management and high availability
- Automating and scaling Meraki deployments
- Routing design and practices on the Meraki platform
- Implementing Quality of Service (QoS) and traffic shaping design
- Architecting VPN and WAN topologies
- Securing, expanding, and shaping the network
- Switched network concepts and practices
- Understand wireless configuration practices and concepts
- Understand Endpoint management concepts and practices
- Implement physical security concepts and practices
- Gaining additional network insight through application monitoring
- Preparing monitoring, logging, and alerting services
- Setting up Dashboard reporting and auditing capabilities
- Gaining visibility and resolving issues using Meraki features and built-in troubleshooting tools

E-Book Sie erhalten die englischen Original-Unterlagen von Cisco. Diese sind auch als Cisco E-Book verfügbar. Bei der Cisco Digital Learning Version sind die Inhalte der Kursunterlagen stattdessen in die Lernoberfläche integriert.

Zielgruppe

Dieser Kurs ist ideal für diejenigen, die regelmäßig Meraki-Netzwerke einrichten oder verwalten und ihr technisches Fachwissen und Verständnis der gesamten Meraki-Produktpalette und -funktionen vertiefen möchten. Dazu gehören Fachleute mit Berufsbezeichnungen oder in Rollen wie

- Field deployment technicians
- Network administrators
- Pre-/Post-sales engineers
- Service provider engineers
- Systems engineers
- IT professionals

Voraussetzungen

Bevor Sie sich für den ECMS2-Kurs anmelden, wird dringend empfohlen, dass Sie bereits den ECMS1-Kurs besucht haben. Sie sollten auch über ein allgemeines Netzwerkverständnis, Meraki-spezifische Kenntnisse und Kenntnisse in den folgenden Bereichen verfügen:

Allgemeines Netzwerk:

- Sie sollten sich aktiv an der Gestaltung, Bereitstellung, Skalierung und Verwaltung von Unternehmensnetzwerken beteiligen.
- Fundierte Grundkenntnisse der IP-Adressierung und der Subnetz-Schemata, die zum Aufbau lokaler Netzwerke erforderlich sind
- Ausgeprägtes Grundwissen über dynamische Routing-Protokolle (Schwerpunkt/Betonung auf Open Shortest Path First [OSPF] und Border Gateway Protocol [BGP])
- Ein grundlegendes Verständnis der drahtgebundenen und drahtlosen Quality of Service (QoS)-Mechanismen, Paketwarteschlangenoperationen und praktische Implementierungen
- Erfahrung mit dem Entwurf und der Konfiguration von IPsec und damit verbundenen Virtual Private Network (VPN)-Technologien haben
- Netzwerksicherheitskontrollen/-protokollen, bewährten Verfahren der Netzwerkverwaltung und Datensicherheit
- Ein grundlegendes Verständnis der Best-Practice-Konstruktionsprinzipien für Hochfrequenz (HF) und deren praktische Umsetzung
- Ein grundlegendes Wissen über bewährte Verfahren für die drahtlose Sicherheit mit Schwerpunkt auf Zugangskontrolle (802.1x) und Frequenzsicherheit durch Wireless Intrusion Detection Systems (WIDS) und Wireless Intrusion Prevention Systems (WIPS)
- Grundlegende Beherrschung der Standard-Protokollierungs-/Überwachungsprotokolle (Schwerpunkt/Betonung auf Simple Network Management Protocol [SNMP], Syslog und Webhooks) und verwandte Implementierungskomponenten oder Tools
- Mit Application Programming Interfaces (APIs) und verwandten Sprachen/Formaten (REST, JavaScript Object Notation [JSON]) vertraut sein und Grundkenntnisse darüber besitzen

Meraki-Wissen:

- Grundlegendes Verständnis der Organisationsstruktur des Dashboards, der Abgrenzung von Privilegien und der übergreifenden Verwaltungsprozesse
- Sie verfügen über das Wissen und die Fähigkeit, fortschrittliche Sicherheitsmerkmale auf MX-Sicherheitsanwendungen zu implementieren (Intrusion Detection/Prevention, Advanced Malware Protection [AMP], Layer 3 & 7 Firewall-Regeln)
- Grundlegendes Verständnis von Auto VPN und dessen Zweck bei Verwendung in einem softwaredefinierten Weitverkehrsnetz (SD-WAN) in der Lage sein, die Konzepte hinter einer Cloud-basierten WLAN-Lösung und die Funktionen zu beschreiben, die bereitgestellt werden können, einschließlich Layer 7 Traffic Shaping und verschiedene Gastzugangs-Authentifizierungsmethoden
- Grundlegendes Verständnis der Containerisierung von Geräteprofilen und Fernverwaltungsfunktionen, wie sie über die Systems Manager-Plattform verwaltet werden
- Grundlegendes Verständnis der Randarchitektur, wie sie von Meraki MV-Sicherheitskameras implementiert wird, und deren Auswirkungen auf die Videoaufbewahrung durch verschiedene konfigurierbare Optionen

Bearbeitungszeit

ca. 18 Stunden

Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.ch/go/ECM2

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.

Cisco Digital Learning & Cisco U.

Die multimodalen Schulungen der Cisco Digital Learning Library beinhalten referenzgeführte HD-Videos mit hinterlegtem durchsuchbarem Text und Untertiteln, Übungen, Labs und erklärenden Text sowie Grafiken. Das Angebot stellen wir Ihnen über unser Lernportal myExperTeach zur Verfügung. Der Zugriff auf die Kurse steht ab der Freischaltung für einen Zeitraum von sechs Monaten zur Verfügung. Bei Paketen (Cisco U.) beträgt dieser Zeitraum zwölf Monate.

Cisco Digital Learning & Cisco U. Preise zzgl. MwSt.
6 Monate Freischaltung **CHF 500,-**

Training	Preise zzgl. MwSt.
Termine in Deutschland	3 Tage CHF 2.855,-
Termine in Österreich	3 Tage CHF 2.855,-
Online Training	3 Tage CHF 2.855,-
Termin/Kursort	Kurssprache Deutsch
22.05.-24.05.24 Online	11.09.-13.09.24 Düsseldorf
22.05.-24.05.24 Wien	11.09.-13.09.24 Online
11.06.-13.06.24 Hamburg	08.10.-10.10.24 Hamburg
11.06.-13.06.24 Online	08.10.-10.10.24 Online
17.07.-19.07.24 München	12.11.-14.11.24 Online
17.07.-19.07.24 Online	12.11.-14.11.24 Wien
14.08.-16.08.24 Frankfurt	11.12.-13.12.24 München
14.08.-16.08.24 Online	11.12.-13.12.24 Online

Stand 07.04.2024



Inhaltsverzeichnis

ECMS2 – Engineering Cisco Meraki Solutions Part 2

Lesson 1: Planning new Meraki architectures and expanding existing deployments

Identify optimal Meraki networks architectures (organization/network sizing and limitations)
Plan for and complete license renewals through the Dashboard

Lesson 2: Designing for scalable management and high availability

Design Meraki organization administrative structure using tags (network and device tags)
Design highly available and redundant networks through the use of MX warm-spares and MS physical stacking technology
Design high density wireless networks (access point calculations and SSID configurations)

Lesson 3: Automation and scaling Meraki deployments

Utilize SAML for scalable role-based access control
Explain the capabilities and limitations of Templates and Network Cloning
Explain and identify ideal use cases for the Dashboard API

Lesson 4: Routing design and practices on the Meraki platform

Design proper static and dynamic routing topologies based on network needs
Explain dynamic routing capabilities on the MX appliance platform
Explain dynamic routing capabilities on the MS switch platform
Configure OSPF across the network as the dynamic routing protocol
Leverage BGP to expand networks and improve WAN performance

Lesson 5: QoS and traffic shaping design

Identify the configurable quality of service (QoS) mechanisms across the LAN and WLAN
Prepare for VoIP and video traffic using class of service (CoS), DSCP tags, and wireless traffic shaping
Configure policy and performance-based routing on the MX appliance platform

Lesson 6: Architecting VPN and WAN topologies

Design highly scalable VPN architectures (full mesh, hub-and-spoke)
Explain the underlying mechanisms of Meraki Auto VPN (VPN registry, UDP hole punching)
Explain the fundamentals of Meraki SD-WAN and its

processing algorithm
Design Meraki SD-WAN architecture with performance-based routing
Extend networks and services into the public cloud (Azure and AWS)

Lesson 7: Securing the network with Advanced Security features

Explain the default traffic flow and layer 3/layer 7 rules processing order of the MX appliance platform
Identify the security intelligence engines and definition databases the MX appliance platform leverages for network protection services (Cisco AMP, Threat Grid, Snort)
Identify and enable content filtering at various levels for desired traffic refinement

Lesson 8: Switched network concepts and practices

Prepare access policies (802.1x) using Meraki authentication
Properly utilize templates, cloning, and switch profiles
Design guest access for LAN/WLAN utilizing Meraki best practices

Lesson 9: Wireless concepts and practices

Configure Dashboard maps and floor plans
Formulate RF profiles to prepare for challenging/variable RF deployments
Configure WLAN access control options based on design requirements
Enable the network for Bluetooth scanning and BLE beaconing
Utilize Air Marshal for intrusion detection and mitigation

Lesson 10: Endpoint management concepts and practices

Explain the different device enrollment and profile deployment methods
Design a native containerization strategy to separate work from personal data on endpoints
Identify and implement various application deployment methods
Assemble and implement security policies which cater to various restriction requirements
Construct a network deployment that leverages SM Sentry

Lesson 11: Physical security concepts and practices

Explain the MV platform's edge architecture and underlying video delivery mechanism (local vs. remote video access)
Design a retention policy using various local or cloud-based storage strategies
Configure MV cameras for wireless deployments

Explain and demonstrate how to effectively utilize advanced analytics and MV camera APIs

Lesson 12: Gaining additional network insight through application monitoring

Explain how Meraki Insight is able to provide network assurance through the use of performance metrics and scores
Qualify and properly size Meraki Insight licenses
Configure, monitor, and track predefined and custom web application thresholds

Lesson 13: Preparing and setting up monitoring, logging, and alerting services

Explain Dashboard's integrated historical log databases (event vs. change logs) to be leveraged for effective activity analysis
Identify the various monitoring tools within Dashboard (native analytics, Topology)
Demonstrate effective network-wide alerting best practices
Utilize the Dashboard API to monitor and maintain Meraki networks

Lesson 14: Setting up Dashboard reporting and auditing capabilities

Generate and interpret on-demand or recurring Summary Reports for key performance metrics
Track and manage firmware releases and prepare for staged upgrades
Recommend proper actions to meet PCI DSS (2.0 and 3.0) compliance

Lesson 15: Gaining visibility and resolving issues using Meraki features and built-in troubleshooting tools

Interpret event and change logs to troubleshoot client and network issues
Classify and compare security threats via the Security Center
Assess wireless intrusions, failures, and network access issues through Dashboard's RF tools (Wireless Health, Air Marshal)
Assess root cause of application performance issues with Meraki Insight
Explain the detailed VPN tunnel information and the VPN Registry found on the VPN Status page
Utilize the Local Status Page as an alternate connectivity method to perform local troubleshooting

