

Engineering Cisco Meraki Solutions

Durée: 4 Jours **Réf de cours: ECMS** **Version: 1.0** **Méthodes d'apprentissage: Classe à distance**

Résumé:

Cette formation permet aux participants d'acquérir les connaissances et les compétences de base nécessaires pour déployer, planifier, concevoir, mettre en œuvre et exploiter des solutions Cisco Meraki complexes. Cette formation combine les formations Engineering Cisco Meraki Solutions Part 1 et 2. Préparez-vous à des rôles axés sur la mise en œuvre, la sécurisation et la gestion des réseaux basés sur Cisco Meraki™ à partir d'un tableau de bord centralisé. Les sujets abordés comprennent les solutions de Cisco Meraki basées sur le cloud, la compréhension des protocoles de sécurité réseau, la conception d'architectures évolutives et l'application de stratégies de dépannage. Cette formation vous prépare à l'examen Cisco Meraki Solutions Specialist (ECMS 500-220). En cas de réussite, vous obtiendrez la certification Cisco Meraki Solutions Specialist.

Cette formation vaut 24 crédits de formation continue (CE) pour la recertification.

Mise à jour : 11.07.2024

Public visé:

Toute personne souhaitant acquérir des connaissances et des compétences de base sur les solutions Cisco Meraki, y compris la gestion du Cloud, la conception, la mise en œuvre, la surveillance, le dépannage et les fonctionnalités complètes de la suite de produits Cisco Meraki. Les personnes souhaitant obtenir la certification de spécialiste en solutions Cisco Meraki.

Objectifs pédagogiques:

- À l'issue de la formation, les participants seront capables de :
- Décrire l'architecture, l'administration, les licences du cloud Cisco Meraki, le matériel et les caractéristiques des familles de produits Cisco Meraki
- Planifier de nouvelles architectures Cisco Meraki et étendre les déploiements existants
- Concevoir le réseau pour une gestion évolutive et une haute disponibilité
- Décrire comment automatiser et mettre à l'échelle les déploiements de Cisco Meraki à l'aide d'outils de tableau de bord
- Utiliser les protocoles de routage dynamique pour étendre les réseaux et améliorer les performances des réseaux étendus (WAN).
- Décrire la qualité de service (QoS), la politique et les configurations de routage basées sur les performances dans un réseau Cisco Meraki et l'optimisation du WAN grâce à la mise en forme du trafic.
- Décrire les topologies de réseaux privés virtuels (VPN) et de réseaux étendus (WAN) et la manière de les intégrer.
- Sécuriser, étendre et façonner le réseau
- Mettre en œuvre les concepts et les pratiques des réseaux commutés, les pratiques et les concepts de configuration sans fils et configurer les réseaux invités
- Décrire les concepts et pratiques de gestion des points d'extrémité à l'aide de Cisco Meraki Systems Manager et les concepts et pratiques de sécurité physique
- Configurer les fonctions de reporting et d'audit dans le tableau de bord de Cisco Meraki et surveiller et résoudre les problèmes à l'aide des outils de Cisco Meraki

Pré-requis:

Il est recommandé aux participants d'avoir les pré-requis suivants :

- Être activement engagé dans la conception, le déploiement, la mise à l'échelle, la configuration et la gestion des réseaux d'entreprise, de l'IPsec et des technologies VPN associées.
- Avoir de l'expérience dans la conception et les meilleures pratiques de la segmentation hiérarchique des réseaux (accès, distribution et couche centrale).
- Une solide connaissance fondamentale des schémas

Test et certification

Recommandé comme préparation aux examens suivants :

- 500-220 - Examen de spécialiste des solutions Cisco Meraki

d'adressage et de sous-réseau du protocole Internet (IP) nécessaires à la construction de réseaux locaux (LAN)

- Une compréhension fondamentale des services d'authentification, d'autorisation et de comptabilité des réseaux

Solides connaissances fondamentales des protocoles de routage dynamique, en particulier de l'OSPF (Open Shortest Path First) et du BGP (Border Gateway Protocol).

- Une compréhension fondamentale des mécanismes de qualité de service (QoS) avec et sans fil, des opérations de mise en file d'attente des paquets et des mises en œuvre pratiques.
- Une compréhension fondamentale des concepts et méthodologies de modélisation des menaces et la capacité de les appliquer pour identifier, analyser et répondre aux menaces en matière de cybersécurité.
- Une compréhension fondamentale des contrôles et des protocoles de sécurité des réseaux, des meilleures pratiques de gestion des réseaux et de la sécurité des données une compréhension fondamentale des contrôles et des protocoles de sécurité des réseaux, des meilleures pratiques de gestion des réseaux et de la sécurité des données.
- Une connaissance fondamentale intermédiaire des concepts, de la terminologie, des principes de conception et des mises en œuvre pratiques des radiofréquences (RF), tels qu'ils s'appliquent aux réseaux sans fil et aux normes sans fil 802.11 actuelles.
- Une compréhension fondamentale des meilleures pratiques en matière de sécurité sans fil, axées sur le contrôle d'accès (802.1x) et la sécurité du spectre par le biais d'un système de détection d'intrusion sans fil (WIDS) et d'un système de prévention (WIPS).
- Une connaissance de base des protocoles standard de journalisation et de surveillance, en particulier du protocole de gestion de réseau simple (SNMP), de syslog et de webhooks, ainsi que des composants ou outils de mise en œuvre correspondants.
- Etre familiarisé avec les interfaces de programmation d'applications (API) et les langages et formats connexes, tels que le transfert d'état représentationnel (REST) et la notation d'objet JavaScript (JSON), et avoir une connaissance de base de ces interfaces.
- CCNA - Mettre en oeuvre et administrer des solutions réseaux Cisco
- ENCOR - Mise en oeuvre et opérations des technologies réseaux Cisco Enterprise

Contenu:

Présentation du Cloud et du tableau de bord Cisco Meraki

- Capacités complètes de Cisco Meraki
- Les appareils Cisco Meraki et le cloud
- Avantages d'une solution dans le Cloud
- Structure organisationnelle et multi-organisationnelle du tableau de bord Cisco Meraki

Présentation des produits et de l'administration de Cisco Meraki

- Appliance de sécurité et SD-WAN Cisco Meraki MX
- Commutateurs Cisco Meraki MS
- AP sans fil Cisco Meraki MR
- Gestion des points d'extrémité Cisco Meraki Systems Manager
- Caméras de sécurité Cisco Meraki MV
- Cisco Meraki Insight - Analyse des applications sur le Web

Introduction au dépannage de Cisco Meraki

- Synchronisation du tableau de bord Cisco Meraki
- Outils de surveillance et de dépannage de Cisco Meraki
- Intégration des outils de surveillance et de dépannage de Cisco Meraki dans les systèmes existants
- Interfaces de programmation d'applications
- Comment travailler avec l'assistance de Cisco Meraki

Planification de nouvelles architectures Cisco Meraki et extension d'un déploiement existant

- Dimensionnement des solutions Cisco Meraki
- Explorer les différentes fonctionnalités de l'interface utilisateur du tableau de bord

Conception d'une gestion évolutive et d'une haute disponibilité

- Accès basé sur les rôles
- Conception et structure des balises
- Haute disponibilité de l'appliance de sécurité Cisco Meraki MX
- Commutateur Cisco Meraki MS haute disponibilité
- Conception sans fil à haute densité

Automatisation et mise à l'échelle des déploiements Cisco Meraki

- RBAC avec SAML
- Configurer SAML et créer des rôles SAML Démonstration
- Cloner un réseau et synchroniser une configuration Démonstration

Conception du routage sur la plateforme Cisco Meraki

- Routage à travers les réseaux Cisco Meraki
- Explorer le routage de couche 3, y compris la création, l'édition et le déplacement de SVI Démo
- Routage dynamique avec OSPF
- BGP pour un routage WAN évolutif et une redondance

Introduction à la QoS et à la conception de la mise en forme du trafic

- Conception de la QoS sans fil et câblée
- Préparer le réseau pour la voix
- Mise en forme du trafic et priorisation sur la plateforme Cisco Meraki MX

Construire des topologies VPN et WAN

- Modes de fonctionnement du VPN Cisco Meraki MX
- Conception et topologies VPN
- VPN automatique
- Concevoir une topologie VPN évolutive
- Explorer la démo du guide de dimensionnement de Cisco Meraki MX
- Intégrer Cisco Meraki vMX dans une architecture Auto VPN
- Fondamentaux du SD-WAN
- Conception SD-WAN
- Explorer les configurations Cisco Meraki vMX et SD-WAN dans la démo du tableau de bord

Sécuriser, étendre et façonner le réseau

- Présentation de la sécurité Cisco Meraki
- Comportement par défaut et ordre de traitement des règles
- Services de sécurité avancés
- Filtrage de contenu
- Intégration de Cisco Umbrella
- Introduction aux concepts et pratiques des réseaux commutés
- Politiques d'accès à l'aide de l'authentification Cisco Meraki
- Clonage des paramètres des commutateurs
- Modèles et profils de commutateur
- Démonstration des profils de commutateur
- Meilleures pratiques en matière d'accès invité au réseau local et au réseau local sans fil

Mise en œuvre des pratiques et concepts de configuration sans fil

- Cartes et plans d'étage du tableau de bord Cisco Meraki

Introduction aux concepts et pratiques de sécurité physique

- Architectures Cisco Meraki MV
- Déploiement flexible de caméras avec le sans-fil
- Portefeuille de produits Cisco Meraki MV, caractéristiques et fonctionnalités
- Recherche de mouvement, récapitulation de mouvement, cartes de chaleur de mouvement et démonstration de détection de personne
- Intelligence économique

Obtenir des informations sur le réseau en surveillant les applications

- Présentation de Cisco Meraki Insight
- Cisco Meraki Insight - Mise à l'échelle et licences
- Présentation de Cisco Meraki Insight : Regarder de plus près les applications suivies et la démonstration de la santé du WAN

Préparation, surveillance, journalisation et services d'alerte

- Capacités d'enregistrement
- Examiner les journaux d'événements, de modifications et d'accès vidéo Démonstration
- Outils et services de surveillance
- Examiner les outils et fonctionnalités de surveillance Démonstration
- Alertes prises en charge
- API du tableau de bord Cisco Meraki

Configuration des capacités de rapport et d'audit dans le tableau de bord Cisco Meraki

- Rapports Cisco Meraki
- Gérer les microprogrammes via le tableau de bord
- Audit PCI

Visibilité et résolution des problèmes à l'aide des outils Cisco Meraki

- Méthodes de dépannage
- Capacités de journalisation
- Démonstration de l'aperçu du centre de sécurité Cisco Meraki
- Dépannage sans fil
- Explorer les outils de dépannage sans fil Démonstration
- Dépannage des performances des applications cloud de Cisco Meraki
- Dépannage de l'Auto VPN de Cisco Meraki
- Explorer l'état du VPN, le pare-feu et le transfert de port statique
- Page d'état locale

- Explorer les modèles de configuration
Démonstration
- Approvisionnement du réseau avec les API
- Utiliser Google Sheets et l'éditeur de script avec l'API du tableau de bord Cisco Meraki
Démonstration

- Profils RF
- Chiffrement et authentification sans fil
- Modes SSID pour l'adressage IP du client
- Bluetooth Low Energy
- Démonstration de l'analyse BLE et des clients Bluetooth
- Menaces sans fil

Introduction aux concepts et pratiques de gestion des points d'extrémité

- Présentation de la plateforme Cisco Meraki Systems Manager
- Démonstration de la plate-forme Cisco Meraki Systems Manager
- Méthodologies de déploiement des dispositifs
- Déploiement des profils d'application et de conteneurisation
- Démonstration des politiques de sécurité et des appareils non conformes
- Couplage des politiques de groupe de réseau avec Systems Manager
Démonstration
- Trusted Access

Labs

- Lab 1 : Configurer le tableau de bord Cisco Meraki
- Lab 2 : Activer les fonctions avancées et optimiser le réseau
- Lab 3 : Dépanner le réseau à l'aide du tableau de bord Cisco Meraki
- Lab 4 : Configurer les balises, l'agrégation de liens, la mise en miroir des ports et les SSID à haute densité
- Lab 5 : Établir l'Auto VPN
- Lab 6 : Configurer les interfaces virtuelles et le routage sur les commutateurs Cisco Meraki MS
- Lab 7 : Configurer les routes et la redistribution
- Lab 8 : Configurer la QoS,
- Lab 9 : Configurer la mise en forme du trafic
- Lab 10 : Configurer l'équilibrage de charge
- Lab 11 : Définir les règles du pare-feu
- Lab 12 : Activer la protection avancée contre les logiciels malveillants
- Lab 13 : Activer le filtrage de contenu
- Lab 14 : Configurer et appliquer des politiques d'accès
- Lab 15 : Configurer l'accès invité sans fil
- Lab 16 : Configurer les SSID
- Lab 17 : Implémenter les profils RF
- Lab 18 : Implémenter Air Marshal
- Lab 19 : Créer les profils de configuration de Cisco Meraki Systems Manager
- Lab 20 : Définir les politiques de sécurité
- Lab 21 : Appliquer la sécurité de bout en bout
- Lab 22 : Configurer les alertes de mouvement
- Lab 23 : Déployer des caméras sans fil
- Lab 24 : Gérer la rétention vidéo
- Lab 25 : Activer les alertes
- Lab 26 : Ajouter la surveillance et les rapports
- Lab 27 : Générer et analyser des rapports de synthèse
- Lab 28 : Gérer les microprogrammes
- Lab 29 : Générer un rapport de conformité PCI
- Lab 30 : Dépanner un appareil hors ligne
- Lab 31 : Dépanner le filtrage de contenu
- Lab 32 : Dépanner la connectivité d'un site distant

Méthodes pédagogiques :

Support de cours officiel remis aux participants

Autres moyens pédagogiques et de suivi:

- Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
- Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
- En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de