Enterprise Wireless

ENGINEERING CISCO MERAKI SOLUTIONS Part 2

ECMS2

Version: 2.1
3 jours

Objectifs

Après avoir suivi ce cours, vous devriez être en mesure de :

- Planifier les déploiements et les intégrations de réseaux à l'aide de la plateforme Meraki.
- Concevoir des architectures Meraki pour la redondance, la haute densité et l'évolutivité
- Mettre en œuvre les fonctionnalités complètes du produit Meraki pour atteindre les objectifs de conception.
- Exploiter les réseaux Meraki et résoudre les incidents réseau complexes à l'aide du tableau de bord et des analyses Meraki.

A qui s'adresse ce cours ?

Ce cours est idéal pour ceux qui déploient ou gèrent régulièrement des réseaux Meraki et qui souhaitent approfondir leur expertise technique et leur compréhension de la suite complète de produits Meraki et de ses fonctionnalités. Il peut s'agir de professionnels occupant des postes ou des rôles tels que :

- Techniciens de déploiement sur le terrain
- Administrateurs réseau
- Ingénieurs avant/après-vente
- Ingénieurs de fournisseurs de services Ingénieurs système
- Professionnels de l'informatique

Prérequis

Avant de vous inscrire au cours ECMS2, il est fortement recommandé d'avoir suivi et terminé le cours Engineering Cisco Meraki Solutions Part 1 (ECMS1) avant de participer à cette formation.

Vous devez également avoir une compréhension générale du réseau, des compétences spécifiques à Meraki et des connaissances dans les domaines suivants :

Réseau général :

- Être activement engagé dans la conception, le déploiement, la mise à l'échelle et la gestion des réseaux d'entreprise.

- Solide connaissance fondamentale des schémas d'adressage et de sous-réseau IP nécessaires à la construction de réseaux locaux

- Solide connaissance fondamentale des protocoles de routage dynamique (accent mis sur l'Open Shortest Path First [OSPF] et le Border Gateway Protocol [BGP]).

- Une compréhension fondamentale des mécanismes de qualité de service (QoS) avec et sans fil, des opérations de file d'attente de paquets et des implémentations pratiques.

- Avoir une expérience de la conception et de la configuration de l'IPsec et des technologies de réseau privé virtuel (VPN) associées.

- Une compréhension fondamentale des contrôles/protocoles de sécurité du réseau, des meilleures pratiques de gestion du réseau et de la sécurité des données.

- Une compréhension fondamentale des principes de conception et des mises en œuvre pratiques des meilleures pratiques en matière de radiofréquence (RF).

- Une connaissance fondamentale des meilleures pratiques de sécurité sans fil centrées sur le contrôle d'accès (802.1x) et la sécurité du spectre par le biais de systèmes de détection des intrusions sans fil (WIDS) et de systèmes de prévention des intrusions sans fil (WIPS).

- Maîtrise fondamentale des protocoles de journalisation et de surveillance standard (en particulier le protocole de gestion de réseau simple [SNMP], syslog et les webhooks) et des composants ou outils de mise en œuvre connexes.

- Connaître et avoir une connaissance de base des interfaces de programmation d'applications (API) et des langages/formats connexes (REST, JavaScript Object Notation [JSON]).

Connaissance de Meraki :

- Compréhension fondamentale de la structure organisationnelle de Dashboard, de la délimitation des privilèges et des processus administratifs primordiaux.

- Être en mesure d'exposer les éléments clés de la licence Meraki (modèle de co-résiliation et période de grâce d'expiration).

- Avoir les connaissances et la capacité de déployer des fonctions de sécurité avancées sur les appareils de sécurité MX (détection/prévention des intrusions, protection avancée contre les logiciels malveillants [AMP], règles de pare-feu des couches 3 et 7).

- Compréhension fondamentale de l'Auto VPN et de son objectif lorsqu'il est utilisé dans un déploiement de réseau étendu défini par logiciel (SD-WAN).

- Être en mesure de décrire les concepts qui sous-tendent une solution WLAN basée sur le cloud et les fonctionnalités qui peuvent être fournies, notamment la mise en forme du trafic de couche 7 et les différentes méthodes d'authentification de l'accès des invités.

- Compréhension fondamentale de la conteneurisation des profils de périphériques et des capacités de gestion à distance, telles que gérées par la plate-forme Systems Manager.

- Compréhension fondamentale de l'architecture périphérique telle qu'elle est mise en œuvre par les caméras de sécurité Meraki MV et de ses implications sur la rétention vidéo grâce à diverses options configurables.

Avantages du cours :

Ce cours vous aidera à :

- Acquérir les compétences et techniques avancées pour planifier, concevoir, mettre en œuvre et exploiter la plateforme complexe Cisco Meraki pour la gestion de réseau basée sur le cloud.
- Vous préparer à passer la ou les prochaines certifications Meraki.

Contenu du cours

- Planification de nouvelles architectures Meraki et extension des déploiements existants
- Conception d'une gestion évolutive et d'une haute disponibilité
- Automatisation et mise à l'échelle des déploiements Meraki
- Conception et pratiques de routage sur la plate-forme Meraki
- Mise en œuvre de la qualité de service (QoS) et conception de la mise en forme du trafic
- Architecture des topologies VPN et WAN
- Sécuriser, étendre et façonner le réseau
- Concepts et pratiques de réseau commuté
- Comprendre les pratiques et les concepts de configuration sans fil
- Comprendre les concepts et pratiques de gestion des points d'extrémité
- Mettre en œuvre les concepts et pratiques de sécurité physique
- Obtenir un aperçu supplémentaire du réseau grâce à la surveillance des applications
- Préparer les services de surveillance, de journalisation et d'alerte
- Configurer les capacités de reporting et d'audit du tableau de bord.
- Obtenir une visibilité et résoudre les problèmes à l'aide des fonctions Meraki et des outils de dépannage intégrés.

Laboratoires

- Création et application
- Tags Configuration de l'agrégation de liens
- Configuration de la mise en miroir des ports
- Établissement d'un VPN automatique
- Configuration des interfaces virtuelles et du routage
- Configuration des routes et de la redistribution
- Configuration de la qualité de service
- Configuration de la mise en forme du trafic
- Configuration de l'équilibrage des charges
- Définition des règles de pare-feu
- Activation de la protection avancée contre les logiciels malveillants
- Activation de la détection et de la protection contre les intrusions
- Activation du filtrage de contenu
- Configuration et application des politiques d'accès
- Configuration de l'accès invité sans fil
- Configuration des identificateurs d'ensembles de services (SSID)
- Mise en œuvre des profils RF
- Mise en œuvre de l'Air Marshal
- Création de System Manager (SM)
- Profils de configuration
- Définition des politiques de sécurité
- Mise en œuvre de la sécurité de bout en bout
- Configuration des alertes de mouvement
- Gestion de la conservation des vidéos
- Déploiement de caméras sans fil
- Activation des alertes Ajout de
- Surveillance et rapports
- Génération de rapports de synthèse
- Gestion des micrologiciels
- Rapports sur l'interconnexion des composants périphériques (PCI)
- Dépannage d'un dispositif hors ligne
- Dépannage du filtrage de contenu
- Dépannage de la connectivité des sites distants