



Cisco - Offre officielle certifiante

Cisco Identity Services Engine - Implementing and configuring

5 jours (35h00) | ★★★★★ 4,6/5 | SISE | Certification 300-715 (non incluse) | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel

Formations Informatique › Réseaux et Télécoms › Cisco - Offre officielle certifiante

Contenu mis à jour le 13/10/2023. Document téléchargé le 23/05/2024.

Objectifs de formation

A l'issue de cette formation, vous serez capable de :

- Décrire les déploiements Cisco ISE, y compris les composants de base du déploiement et comment ils interagissent pour créer une architecture de sécurité cohésive
- Exposer les avantages d'un tel déploiement et comment chaque capacité Cisco ISE contribue à ces avantages
- Décrire les concepts et configurer les composants liés à l'authentification 802.1X et au MAC Authentication Bypass (MAB), à la gestion d'identité et aux services de certificats
- Représenter comment les stratégies Cisco ISE sont utilisées pour mettre en oeuvre l'authentification et l'autorisation, et comment exploiter cette capacité pour répondre aux besoins de votre organisation
- Décrire les dispositifs d'accès au réseau (NAD) tiers, Cisco TrustSec et Easy Connect
- Reconnaître et configurer l'authentification Web, les processus, le fonctionnement et les services invités, y compris les composants d'accès invités et divers scénarios d'accès invités
- Décrire et configurer les services de profilage Cisco ISE, et surveiller ces services pour améliorer votre connaissance de la situation des points d'extrémité connectés au réseau
- Appliquer les bonnes pratiques pour le déploiement de ce service de profilage dans votre environnement spécifique
- Expliquer les défis, les solutions, les processus et les portails BYOD (Bring Your Own Device)
- Configurer une solution BYOD et expliquer la relation entre les processus BYOD et leurs composantes de configuration connexes
- Décrire et configurer les différents certificats liés à une solution BYOD.

Modalités, méthodes et moyens pédagogiques

Formation délivrée en présentiel ou distanciel* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2i, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

** nous consulter pour la faisabilité en distanciel*

*** ratio variable selon le cours suivi*

Prérequis

Avoir des connaissances de base sur l'interface de ligne de commande (CLI) du logiciel Cisco IOS, sur le client de mobilité sécurisé Cisco AnyConnect, sur les systèmes d'exploitation Microsoft Windows et sur la norme 802.1X. De plus, il est recommandé d'avoir suivi les cours CCNA "Cisco Solutions - Implementing and administering" et SCOR "Cisco Security Core Technologies - Implementing and operating", ou avoir les connaissances équivalentes. Afin d'obtenir la certification CCNP Security, il faut avoir passé l'examen Core 350-701 et l'examen 300-715.

Public concerné

Ingénieurs en sécurité des réseaux (y compris les réseaux sans fil), administrateurs ISE et/ou intégrateurs et partenaires Cisco.

Cette formation :

- Est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par M2i Formation
- Bénéficie d'un suivi de son exécution par une feuille de présence émarginée par demi-journée par les stagiaires et le formateur.

Programme

Présentation de l'architecture et du déploiement de Cisco ISE

- Utilisation de Cisco ISE comme moteur de politique d'accès au réseau
- Cas d'utilisation Cisco ISE
- Description des fonctions de Cisco ISE
- Modèles de déploiement Cisco ISE
- Visibilité du contexte

Application de la politique ISE de Cisco

- Utilisation de 802.1X pour l'accès câblé et sans fil
- Utilisation du contournement de l'authentification MAC pour l'accès câblé et sans fil
- Introduction à la gestion des identités
- Configuration des services de certificats
- Présentation de la politique ISE de Cisco
- Mise en oeuvre de la prise en charge des périphériques d'accès réseau tiers
- Présentation et configuration de Cisco TrustSec
- Easy Connect

Authentification Web et services aux invités

- Introduction de l'accès Web avec Cisco ISE
- Présentation des composants de l'accès invité
- Configuration
 - Des paramètres d'accès invité
 - Des portails de sponsors et d'invités

Cisco ISE Profiler

- Présentation de Cisco ISE Profiler
- Déploiement du profilage et pratiques exemplaires

Cisco ISE BYOD

- Présentation du processus Cisco ISE BYOD
- Description du flux de BYOD
- Configuration du portail "Mes appareils"
- Configuration des certificats dans les scénarios BYOD

Services de conformité des points d'accès Cisco ISE

- Présentation des services de conformité des points d'accès
- Configuration des services de posture client et de provisionnement dans Cisco ISE

Travailler avec des dispositifs d'accès au réseau

- La TACACS+ (Terminal Access Controller Access-Control System Plus)
- Administration des dispositifs Cisco ISE TACACS+
- Configurer l'administration des dispositifs TACACS+
- Lignes directrices et bonnes pratiques de la TACACS+ en matière d'administration des dispositifs
- Migration de Cisco ACS vers Cisco ISE

Certification (en option)

- Prévoir l'achat de la certification en supplément
- Le passage de l'examen se fera (ultérieurement) dans un centre agréé Pearson Vue
- L'examen (en anglais) s'effectue en ligne, et durera en moyenne 1h30

Le contenu de ce programme peut faire l'objet d'adaptation selon les niveaux, prérequis et besoins des apprenants.

Modalités d'évaluation des acquis

- En cours de formation, par des évaluations formatives, à travers des travaux pratiques réalisés sur les labs (à l'issue de chaque module)
- Et/ou, en fin de formation, par une certification (proposée en option)

Les + de la formation

Le support de cours et les labs sont en anglais.

Accessibilité de la formation

Le groupe M2i s'engage pour faciliter l'accessibilité de ses formations. Les détails de l'accueil des personnes en situation de handicap sont consultables sur la page Accueil et Handicap.

Modalités et délais d'accès à la formation

Les formations M2i sont disponibles selon les modalités proposées sur la page programme. Les inscriptions sont possibles jusqu'à 48 heures ouvrées avant le début de la formation. Dans le cas d'une formation financée par le CPF, ce délai est porté à 11 jours ouvrés.