

Formation Mettre en œuvre et configurer la solution Cisco Identity Services Engine

Description de la formation Cisco ISE

Cette formation permet d'acquérir les compétences et connaissances nécessaires pour déployer et utiliser IE v2.4 (Cisco Identity Services Engine) une plateforme de contrôle d'accès et d'identité qui simplifie la délivrance de contenus avec un contrôle d'accès sécurisé via des connexions VPN filaires, sans fils et VPN.

Cette formation fournit également les compétences pour mettre en œuvre et utiliser Cisco ISE, tel que les stratégies renforcées, les services de profils, l'authentification Web et les services d'accès invités, BYOD, les services de conformité endpoint et l'administration du périphérique TACACS+.

Au travers d'instructions précises et pratiques, ils apprendront à utiliser Cisco ISE pour obtenir de la visibilité sur ce qui se passe sur le réseau, sur la gestion des stratégies de sécurité et sur leur efficacité opérationnelle.

Les participants seront amenés à travailler en groupe et à partager des équipements.

Objectifs

Concrètement, à l'issue de cette formation Cisco ISE vous serez en mesure de :

- Décrire les déploiements Cisco ISE, y compris les composants du déploiement et comment interagir pour créer une architecture sécurisée cohérente. Décrire les avantages d'un tel déploiement et comment chaque possibilité de Cisco ISE contribue à ces avantages.



ITgate

Training

Your Gateway to Excellence

- Décrire les concepts et configurer les composants liés à 802.1X et à l'authentification MAB (MAC authentication Bypass), gérer les identités et les services de certificats.
- Décrire comment les stratégies Cisco ISE sont utilisés pour mettre en œuvre l'authentification et l'autorisation et comment les aligner aux besoins de l'entreprise.
- Décrire les périphériques d'accès réseau tiers (NADs), Cisco TrustSec et Easy Connect.
- Décrire et configurer l'authentification Web, le fonctionnement des process et les services invités, tels que les composants d'accès invités et les différents scénarios d'accès invités.
- Décrire et configurer les services de profil Cisco ISE et comprendre comment surveiller ces services pour améliorer la surveillance des endpoints connectés au réseau. Décrire les meilleures pratiques pour déployer le service de profils dans votre environnement spécifique.
- Décrire les challenges BYOD, les solutions, les processus et les portails. Configurer une solution BYOD et décrire les relations entre les processus BYOD et leurs composants. Décrire et configurer les différents certificats liés à la solution BYOD.
- Décrire la valeur du portail « My Devices » et comment le configurer.
- Décrire la conformité du endpoint, la conformité des composants et des agents, du déploiement, des licences et du service Cisco ISE.
- Décrire et configure l'administration de TACACS+ via Cisco ISE, tels que les paramètres, les profils et les stratégies. Comprendre le rôle de TACACS+ avec l'authentification, AAA et les différences entre les protocoles RADIUS et ATACS+.
- Migrer les fonctionnalités de ACS (Cisco Secure Access Control System) vers Cisco ISE via un outil de migration.

À qui s'adresse cette formation ?

Public :

Cette formation Cisco ISE cible principalement les ingénieurs en sécurité des réseaux, les administrateurs ISE, les ingénieurs en sécurité des réseaux sans fil ainsi que les intégrateurs et partenaires Cisco.

Prérequis :

Avant de suivre cette formation Cisco ISE il est recommandé, mais non obligatoire, d'être familier avec l'interface de ligne de commande (CLI) du logiciel Cisco IOS, d'avoir des connaissances de base sur le client de mobilité sécurisé Cisco AnyConnect®, et enfin avoir des notions sur les systèmes d'exploitation Microsoft Windows ainsi que sur la norme 802.1X.

Contenu du cours Cisco ISE

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 œuvre de la prise en charge des périphériques d'accès réseau tiers

Présentation de Cisco TrustSec

Configuration 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

Configuration 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+

Administration des dispositifs Cisco ISE TACACS

Configurer l'administration des dispositifs TACACS

Lignes directrices et best practices de la TACACS+ en matière d'administration des dispositifs

Migration de Cisco ACS vers Cisco ISE