METTRE EN OEUVRE CISCO SECURE ACCESS CONTROL SYSTEM

CODE DE LA FORMATION:
ACS

ÉDITEUR OU CONSTRUCTEUR:
CISCO

VERSION:
5.2

DURÉE:
3 JOURS

A l'issue de la formation, les participants seront capables de sécuriser les accès aux ressources réseau avec Cisco Secure Access Control System (ACS) 5.2. Ils examineront comment ACS a évolué depuis la version 4.x, découvriront les nouvelles fonctionnalités et les nouvelles configurations.
Les participants découvriront également l'importance de ACS dans Cisco TrustSec, quand TrustSec est déployé en tant que solution «appliance-based» ou en tant que solution 802.x intégrée au réseau. L'authentification et l'autorisation, évaluation de posture, profil équipement, l'accès invité, l'intégrité et la confidentialité des données, les stratégies centralisées, la surveillance collaborative, le dépannage…

PRÉREQUIS:
Les participants doivent être certifiés CCNA. La certification CCNA Sécurité est recommandée. Avoir des connaissances du système Windows.

PUBLIC:
Cette formation s’adresse aux architectes, ingénieurs et administrateurs réseaux responsables de la sécurité dans les réseaux.

OBJECTIFS:
- Comprendre comment les protocoles RADIUS et TACACS+ fonctionnent et quels services ils rendent
- Comprendre la solution ACS courante, incluant ACS Express, ACS Enterprise, ACS sur VMware et les appliances tels que CSACS-1120 Series et les CSACS-1121 Series
- Décrire les composants principaux de ACS
- Déterminer les meilleures pratiques pour l’installation de ACS 5.2
- Configurer ACS à partir d’une installation par défaut
- Comprendre les besoins en licences de ACS et comment elles opèrent
- Comprendre comment les attributs, les types de valeurs et les valeurs prédéfinies sont utilisées
- Décrire les types de clients AAA (Authentication, Autorisation, Accounting) disponibles et comment ils accèdent aux ressources réseaux et aux autres clients AAA
- Travailler avec un annuaire d’identité local et séquences d'annuaires
- Comprendre les utilisateurs et les annuaires d'authentification
- Configurer un annuaire d’identification externe avec LDAP
- Comprendre les fondamentaux de LDAP
- Installer LDAP SSL
- Installer un annuaire d’identification externe avec Active Directory
- Implémenter AAA avec TACACS+
- Surveiller et dépanner ACS (AAA avec TACACS+)
- Utiliser une autorité de certification locale pour remplacer les certificats digitaux signés par ACS

- Introduction à IEEE 802.1x et à EAP
- 802.x avec Windows XP, Windows 7 et AnyConnect 3.x supplicant
- Authentification simple de l’hôte 802.1x
- Dépannage de 802.1x

CONTENU:

Solution de gestion des identités

- Modèles de gestion des identités
- Architecture réseau sécurisée
- Etude cas d'un réseau «Identity Enabled»

Vue d'ensemble du produit et configuration initiale

- Vue d’ensemble de RADIUS et TACACS
- Vue d’ensemble de ACS 5.2
- Installation de ACS 5.2
- Types d'attributs ACS
- Ajout de périphériques réseau à ACS
- Annuaire d'identification locale et séquence

Configuration avancée de ACS et gestion des périphériques

- Annuaire d'identification externe LDAP
- Annuaire d'identification avec Active Directory
- AAA (Authentication, Authorization, Accounting) avec TACACS
- Surveillance et dépannage de ACS
- ACS et les certificats d'autorité

IEEE 802.1x avec ACS 5.2

- Vue d'ensemble de IEEE 802.1x
- Eléments de la stratégie 802.1x (RADIUS)
- 802.1x et Windows XP
- 802.1x et le client SCC (Cisco Secure Services Client)
- Configurer l'authentification sur un Switch Cisco d'un équipement 802.1x

Opérations Système

- Déploiement distribué
- Administration système