Implementing Cisco Secure Access Control System v5.2

ACS

Delivery Type: Classroom
Duration: 5 days

Overview

In this course, you will learn to provide secure access to network resources using the Cisco Secure Access Control System (ACS) 5.2. You'll examine how the ACS has grown by leaps and bounds since 4.x., discover new features, and learn how the 4.x configurations map to 5.x configurations. You will also get a look into future ACS technologies.

You will learn about the role and importance of ACS in Cisco TrustSec, whether TrustSec is deployed as an appliance-based overlay solution or as a network-integrated 802.1x solution. You will learn about user authentication and authorization, posture assessment, device profiling, guest access, data integrity and confidentiality, centralized policy, collaborative monitoring, troubleshooting, and reporting in Cisco TrustSec solutions.

Certification

Recommended preparation for exam(s):
✓ There is no relevant exam or certification at this time

Target Audience

Cisco channel partners who sell, implement, and maintain Cisco ACS solutions and Security professionals, architects, engineers and network administrators responsible for securing their networks to insureaccess is only by authenticated authorized users, with recordsof their activities.

Pre-Requisites
Attendees should meet the following prerequisites:
✓ CCNA Certification ICND1plus ICND2or CCNABC recommended
✓ CCNA Security Certification IINS recommended but not mandatory
✓ Working Knowledge of the Microsoft windows operating system

Objectives
After completing this program, you will be able to:
✓ Understand how the RADIUS and TACACS+ protocols operate and what purpose they serve.
✓ Understand the current ACS solution offering, including ACS Express, ACS Enterprise, ACS on

VMware, and appliances such as the CSACS-1120
- ✓ Series and CSACS-1121 Series
- ✓ Describe the major components of ACS
- ✓ Determine the best installation practices for ACS 5.2
- ✓ Configure the ACS from a default install
- ✓ Understand the Licensing requirements of ACS and how licensing works.
- ✓ Understand how attributes, value types, and predefined values are used
- ✓ Describethe Types of Authentication, Authorization, and Accounting (AAA) clients availalbeand how they access network resources and other AAA clients
- ✓ Work with a local identity store and identity store sequence
- ✓ Understand users and identity stores

- ✓ Configure an external identity store with LDAP
- ✓ Understand the Fundamentals of LDAP
- ✓ Set up LDAP SSL
- ✓ Set up an external identity store with Active Directory
- ✓ Perform AAA with TACACS+
- ✓ Monitor and troubleshoot ACS (AAA with TACACS+)
- ✓ Use a local certificate authority to replace digital certificates self-signed by ACS
- ✓ Introduction to IEEE 802.1x and EAP
- ✓ 802.1x using Windows XP, Windows 7, and AnyConnect 3.x supplicants
- ✓ 802.1x single host authentication
- ✓ 802.1x troubleshooting