Implementing Cisco Secure Access Control System

Duration: 3 Days Course Code: ACS

Overview:

In the Implementing Cisco Secure Access Control System (ACS) 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.

Target Audience:

This course is designed for:Security professionals, architects, and engineers and network administrators responsible for securing their networks to assure authorized access only by authenticated users, with accounting of their activities Cisco channel partners who sell, implement, and maintain Cisco ACS solutions Cisco ACS solutions sales engineers

Objectives:

- Upon completing this course, the learner will be able to meet these overall objectives:
- RADIUS and TACACS+ protocols
- ACS solutions, including ACS Express, ACS Enterprise, ACS on VMware, and appliances such as the CSACS-1120 Series and CSACS-1121 Series
- Major components of ACS
- ACS 5.2 installation best practices
- Configure the ACS from a default install
- License requirements
- How attributes, value types, and predefined values are used
- Types of Authentication, Authorization, and Accounting (AAA) clients and how they access network resources and other AAA clients
- Work with a local identity store and identity store sequence
- Users and identity stores
- Configure an external identity store with LDAP
- 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+)
- Using 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

Prerequisites:

The knowledge and skills that a learner must have before attending this course are as follows:

- CCNA certification or the equivalent knowledge and experience
- Working knowledge of Microsoft Windows
- CCNA Security certification or the equivalent knowledge and experience is recommended

To gain the prerequisite skills and knowledge, Cisco strongly recommends the knowledge of the following courses:

- Interconnecting Cisco Networking Devices Part 1 (ICND1)
- Interconnecting Cisco Networking Devices Part2 (ICND2)
- Implementing Cisco IOS Network Security (IINS)

Content:

Identity Management Solution

- Identity Management Models
- Secure Borderless Network Architecture
- Identity-Enabled Network Use Case Summary

Product Overview and Initial Configuration

- Overview of RADIUS and TACACS+
- RADIUS Basics
- TACACS+ Basics
- RADIUS vs. TACACS+
- ACS 5.2 Overview
- Hardware Platform Solutions
- Software Platform Solutions
- New, Changed, and Supported Features
- ACS 5.2 Installation
- Installation on the CSACS+ Series Appliance
- Installation with VMware ESX Server
- Using Setup Scripts
- Licensing
- ACS Attribute Types
- Attribute Definitions
- Attribute Value Types
- Predefined Values
- Attribute Dictionaries
- Attribute Aliases
- Availability of Attributes Based on Policy
- Adding Network Devices to ACS
- Network Resources
- Types of AAA Clients
- Network Device Groups: Location
- Network Device Groups: Device Type
- Network Devices and AAA Clients
- Local Identity Store and Identity Store Sequence
- Users and Identity Stores
- Internal Identity Store
- External Identity Store
- Certificate Profile
- Internal Identity Stores
- Users
- Groups
- Hosts

Advanced ACS Configuration and Device Management

- External Identity Store with LDAP
- LDAP Overview
- External Identity Stores: OpenLDAP
- Enable LDAP Diagnostics Log
- External Identity Store with Active Directory
- Interface with Active Directory
- DNS Considerations
- NTP Server Considerations
- Considerations of Authenticating Usernames with Domains
- Machine Access Restrictions (MAR)
- Windows 2008 Compatibility and Feature Support
- Testing Connectivity between ACS and AD
- Group Names Differences in ACS 4.x and 5.x
- Identity Store Sequences
- PAP Authentication via Kerberos
- Authentication, Authorization, and Accounting with TACACS+
- Shell Profile
- Command Sets Access Services
- Service Selection Rules
- Default Device Admin: Authorization and Identity
- Monitoring and Troubleshooting ACS
- Cisco Secure ACS View
- Monitoring and Debugging RADIUS Authentication
- Monitoring and Debugging RADIUS Authorization
- Monitoring and Debugging TACACS+ Authentication
- Monitoring and Debugging TACACS+ Authorization
- Debugging TACACS+ Packets and Accounting
- ACS and Certificate Authority
- Certificate-Based Authentication
- Self-Signed Certificates
- Third-Party Digital Certificates

IEEE 802.1x with ACS 5.2

- IEEE 802.1xOverview
- History
- Introduction
- The Port
- EAP
- EAP-TLS
- PEAP
- 802.1x Policy Elements (RADIUS)
- Overview
- Date and Time
- Custom
- Authorization Profiles
- Authorization: Downloadable ACL
- Access Policies
- Service Selection Rules

System Operations

- Distributed Deployment
- ACS Operation Management
- ACS Deployment Structure
- Local Operations
- Distributed System Management
- Distributed Management Operations
- Replication Overview
- Local Operations
- Log Collector
- Change Pass
- ord Flow
- System Administration
- Administrators
- Users
- Operations
- Configuration
- Downloads

- Access Services
- Identity
- 802.1x and Windows XP
- Configure 802.1x
- 802.1x and the Cisco Secure Services Client (SSC)
- Configure 802.1x on the SSC
- Configure 802.1x Single Host Authentication on a Cisco Switch
- Single Host Authentication
- Single Host Authentication Commands
- Cisco Sitch 802.1x Configuration Review
- 802.1x Troubleshooting
- ACS, Switch, and Windows Troubleshooting
- Windows XP and Switch Debug Output
- ACS Monitoring and Reports

Further Information:

For More information, or to book your course, please call us on +254 713 027 191

training@clclearningafrica.com

www.clclearningafrica.com

Computer Learning Centre 2nd Floor Museum Hill Centre, Muthithi Road, Westlands, Nairobi, Kenya