Implementing Cisco Secure Access Control System (ACS)

Duration 3 Days

COURSE CONTENT

This 3-day course teaches students how to provide secure access to network resources using the Cisco Secure Access Control System (ACS) 5.2, interoperating with security features in Cisco IOS Software. Students will gain a thorough understanding of the operation of the Cisco Secure ACS to control access to network services and devices. Course subjects include the principles of authentication, to restrict user access to networks, services, and devices; authorization, to restrict the functions users can perform on services and devices; and accounting, to track the activities of users. The RADIUS, TACACS+, Extensible Authentication Protocol (EAP), and 802.1x protocols are discussed in theory and practice as the basis of network security. Specific methods and configurations are shown that can be used in your production networks to achieve targeted and detailed restrictions. The course includes hands-on labs to provide personal experience in configuring Cisco ACS and Cisco network devices.

COURSE OBJECTIVES

Upon completing this course, the learner will be able to meet these overall objectives:

- Understand how the RADIUS and TACACS+ protocols operate and what purpose they serve.
- Be familiar with all present ACS Solutions, including ACS Express, ACS Enterprise, ACS on VMware and Appliances like the CSACS-1120 Series and CSACS-1121 Series Appliances.
- How Licensing works with the ACS.
- Understand how Attributes, Value Types and Predefined Values are used.
- The different types of AAA Clients and how they access Network Resources and AAA Clients.
- How to work with a Local Identity Store & Identity Store Sequence.
- Replacing digital certificates self-signed by ACS using a local Certificate Authority.
- Introduction to IEEE 802.1x and EAP Extensible Authentication Protocol.
- Troubleshooting.

COURSE OUTLINE

This course teaches students how to provide secure access to network resources using the Cisco Secure Access Control System (ACS) 5.2, interoperating with security features in Cisco IOS Software. Students will gain a thorough understanding of the operation of the Cisco Secure ACS to control access to network services and devices. Course subjects include the principles of authentication, to restrict user access to networks, services, and devices; authorization, to restrict the functions users can perform on services and devices; and accounting, to track the activities of users. The RADIUS, TACACS+, Extensible Authentication Protocol (EAP), and 802.1x protocols are discussed in theory and practice as the basis of network security. Specific methods and configurations are shown that can be used in your production networks to achieve targeted and detailed restrictions. The course includes hands-on labs to provide personal experience in configuring Cisco ACS and Cisco network devices.

WHO SHOULD ATTEND

Channel Partner / Reseller, Customer, Employee

PREREQUISITES

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

- Cisco Certified Network Associate (CCNA) certification or the equivalent in knowledge and experience.
- Working knowledge of the Microsoft Windows operating system.
- Though not mandatory, students should also attend: * Implementing Cisco IOS Network Security (IINS) certification or the equivalent in knowledge and experience.