ACS52 (IMPLEMENTING CISCO SECURE ACCESS CONTROL SYSTEM)

Objetivo

Este curso tem como objetivo apresentar a ferramenta Cisco ACS 5.Xem sua versatilidade de emprego em soluções que demandam um controle de acesso centralizado, seguro e monitorado, em soluções de acesso usuário através do emprego de 802.1X e Radius, como para o acesso administrativo pela utilização do protocolo Tacacs+. O aluno vai aprender a fornecer um acesso seguro através do processo AAA, Autenticação, Autorização e Contabilidade (Accounting) através de sua integração tanto em processos de acesso dos usuários da rede, como por exemplo o acesso em uma porta de switch, como pelo emprego na centralização da gerência e controle de acesso administrativo aos equipamentos. Conhecer a diversidade de opções de uso e instalação da linha ACS; Descrição da arquitetura e componentes do Cisco ACS; Entendimento da forma e dos requerimentos para licenciamento; Descrever as políticas que podem ser utilizadas através da implementação de sistemas de controle AAA com ACS; Conhecer as melhores práticas de instalação e emprego do Cisco ACS; Entender como os protocolos Radius e Tacacs+ operam e seus propósitos de emprego nos processos de controle de acesso; Entedimentos das diferentes bases de usuários que podem ser utilizadas e combinadas com o Cisco ACS, como a base interna do produto, e bases externas (LDAP, AD dentre outros); Compreender o protocolo IEEE 802.1X e seu emprego em conjunto com ACS; Repassar conhecimentos em como configurar o Cisco ACS utilizando o protocolo Radius em conjunto com o protocolo IEEE 802.1X em switches; Como preparar o dispositivo do cliente para o acesso, tais como o nativo do sistema Windows XP e 7, e o suplicante da Cisco Anyconnect; Proceder o monitoramento e suporte do produto;

Público Alvo

Administrador de rede ou profissional que necessita implantar o Cisco ACS como uma solução para centralização, gerenciamento e controle do acesso administrativo a equipamentos (exemplos: roteadores e switches com o uso do protocolo Tacacs+), ou o acesso de usuários aos recursos de rede (exemplo: configurar o switch com o protocolo IEEE 802.1X e Radius).

Pré-Requisitos

Conhecimentos básicos de rede, que é proporcionada pelo curso ICND1; Conhecimentos básicos do sistema Windows (XP ou 7); Conhecimentos básicos da linha de comando para configuração de equipamento Cisco, como switch e roteador.

Carga Horária

24 horas (3 dias).

Conteúdo Programático

Course Introduction
Overview
Course Flow

Identity Management Solution Overview
Identity Management Models
Understanding Secure Access Network Architecture
Identity-Enabled Network

Product Overview and Initial Configuration
Introduction to RADIUS and TACACS+
Cisco ACS Overview
Cisco ACS Installation Guidelines
Understanding Cisco ACS Attribute Types and Dictionaries
Adding Network Devices to Cisco ACS
Configuring Local Identity Store
Configuring Identity Store Sequence

Advanced ACS Configuration and Device Management
Configuring LDAP External Identity Store
Configuring AD (Active Diretory) External Identity Store
Configuring AAA (Authentication,Authorization and Accounting) with TACACS+
Configuring Commands and Shell Authorization with TACACS+

Cisco ACS and Certification Authority
Cisco ACS and Self-Signed Certificate
Cisco ACS and CA (Certification Authority)
Cisco ACS Generate Certificate Signing Request
Cisco ACS and EAP-TLS Settings

Monitoring, Reporting and Troubleshooting
Overview
Authentication Records
Portlets and Tabs
Alarms
Configure Thresholds
Configure Syslog
Reports View

IEEE 802.1X and Cisco ACS
Introduction IEEE 802.1X
EAP-TLS and EAP-PEAP
IEEE 802.1X and Cisco ACS Policy Elements
Authorization Profiles and Policies

IEEE 802.1X Clients

802.1x and Windows Native Client
802.1x and Cisco Anyconnect Mobility Client

Cisco ACS and Switch Port Control
Using 802.1X Switch Port-Based Authentication
Configure 802.1x Single Host Authentication on a Cisco Switch
Troubleshooting 802.1X Port Based Authentication

Cisco ACS and Distributed Deployment
Distributed Deployment Overview
Cisco ACS Primary and Secondary Instance
Deployment Distributed Operations
Management Distributed Operations

Administration Cisco ACS
Overview
Administrators
User Account Settings
Configuration and Operations

Roteiro de Laboratório
Lab 1: Verify the Cisco Secure ACS Installation
Lab 2: Set Up AAA Clients in Cisco Secure ACS
Lab 3: User and Local Identity Store
Lab 4: External Identity Store (Active Directory)
Lab 5: Configure Command Authorization
Lab 6: Install a Certificate on the Secure ACS Server
Lab 7: Configure Basic 802.1X Authorization
Lab 8: Configure Advanced 802.1X Authorization
Lab 9: Configure 802.1X VLAN Assignments
Lab 10: Troubleshoot
Lab 11: Distributed Deployment