



**SECURITY**

# **AAA Identity Management Security**

# AAA Identity Management Security

---

Vivek Santuka, CCIE #17621

Premdeep Banga, CCIE #21713

Brandon J. Carroll, CCIE #23837

**Cisco Press**

800 East 96th Street

Indianapolis, IN 46240

# AAA Identity Management Security

## Table of Contents

### Contents

### Introduction

### Chapter 1 Authentication, Authorization, Accounting (AAA)

#### Authentication Overview

##### Authentication Example

#### Authorization Overview

##### Authorization Example

#### Accounting Overview

##### Accounting Example

#### Overview of RADIUS

##### RADIUS in Detail

##### RADIUS Operation

##### RADIUS Encryption

##### RADIUS Authentication and Authorization

##### RADIUS Accounting

#### Overview of TACACS+

##### TACACS+ in Detail

##### TACACS+ Communication

##### TACACS+ Format and Header Values

##### Encrypting TACACS+

##### TACACS+ Operation

##### TACACS+ and Authentication

##### TACACS+ and Authorization

##### TACACS+ Accounting

### Summary

# **Table of Contents**

## **Chapter 2 Cisco Secure ACS**

### **Introduction to ACS**

Overview

AAA Client-Server Framework

### **Cisco Secure Access Control Server Release 4.2 Characteristics and Features**

Policy Model

Platform

Protocol Compliance

Features Available

### **Cisco Secure Access Control System Release 5.1 Characteristics and Features**

Policy Model

Platform

Protocol Compliance

Functions and Features

### **Installing Cisco Secure Access Control Server 4.2**

Installing Cisco Secure Access Control Server for Windows 4.2

Installing Cisco Secure Access Control Server Solution Engine

### **Initial Setup of Cisco Secure Access Control System 5.1**

Cisco Secure Access Control System Appliance 5.1

Installing Cisco Secure Access Control System 5.1

Installing Cisco Secure Access Control System 5.1 on VMware

### **Licensing Model of Cisco Secure Access Control System 5.1**

Type of License

Base License

Add-on License

Evaluation License

Not-For-Resale (NFR) License

# **Table of Contents**

## **Common Problems After Installation**

- ACS Solution Engine Does Not Respond to Pings
- No Proper Cisco Secure Access Control Server GUI Access
- Remote Administration Access to Cisco Secure Access Control Server
- ACS Folder Is Locked During Upgrade or Uninstall
- TACACS+/RADIUS Attributes Do Not Appear Under User/Group Setup
- Key Mismatch Error
- ACS Services Not Starting
- ACS 5.1 Install Failing on VMWare

## **Summary**

## **Chapter 3 Getting Familiar with ACS 4.2**

### **The Seven Services of ACS**

- CSAdmin
- CSAuth
- CSDBSync
- CSLog
- CSMon
- CSRadius
- CSTacacs

### **The Grand Tour of the ACS Interface**

- Administration Control
- Securing Access to ACS
- Network Configuration
- Network Access Profiles
- Interface Configuration
- TACACS+ Settings
- Advanced Options
- User Setup: Managing Users
- Customizing User Attributes
- Group Setup: Managing User Groups

# **Table of Contents**

- System Configuration
- Shared Profile Components
- External User Databases
- Reports and Activity

Summary

## **Chapter 4 Getting Familiar with ACS 5.1**

### **My Workspace**

- Welcome Page
- Task Guide
- My Account

### **Network Resources**

- Network Device Groups
- Network Devices and AAA Clients
- Default Network Device
- External RADIUS Servers

### **Users and Identity Stores**

- Identity Groups
- Adding a User in the Internal Identity Store
- Adding a Host in the Internal Identity Store

### **Policy Elements**

- Session Conditions: Date and Time
- Session Conditions: Custom
- Session Conditions: End Station Filters
- Session Conditions: Device Filters
- Session Conditions: Device Port Filters

### **Access Policies**

- Service Selection Rules
- Access Services
- Creating an Access Service

# **Table of Contents**

- Configuring Identity Policy
- Configuring Authorization Policy
- Creating Service Selection Rules

## **Monitoring and Reports**

- ACS 5.1 Command-Line Interface (CLI)

## **Summary**

# **Chapter 5 Configuring External Databases (Identity Stores) with ACS**

## **External Databases/Identity Stores**

- External Databases/Identity Stores in Cisco Secure Access Control Server 4.2

- External Databases/Identity Stores in Cisco Secure Access Control System 5.1

## **Configuring Active Directory**

- Active Directory Configuration on Cisco Secure Access Control Server 4.2

- Active Directory Configuration on Cisco Secure Access Control System 5.1

## **Configuring LDAP**

- LDAP Configuration on Cisco Secure Access Control Server 4.2

- Domain Filtering

- Common LDAP Configuration

- Primary and Secondary LDAP Server

- LDAP Configuration on Cisco Secure Access Control System 5.1

## **Configuring RSA SecureID**

- RSA SecureID Configuration on Cisco Secure Access Control Server 4.2

- RSA SecureID Configuration on Cisco Secure Access Control System 5.1

## **Group Mapping**

- Group Mapping on Cisco Secure Access Control Server 4.2

# **Table of Contents**

Group Mapping on Cisco Secure Access Control System 5.1

Group Mapping with LDAP Identity Stores

Group Mapping with AD Identity Stores

Group Mapping with RADIUS Identity Stores

Group Mapping Conditions for LDAP, AD, and RADIUS Identity Databases

Summary

## **Chapter 6 Administrative AAA on IOS**

### **Local Database**

Privilege Levels

Lab Scenario #1: Local Authentication and Privilege Levels

Lab Setup

Lab Solution

Lab Verification

### **Using AAA**

Configuring Authentication on IOS Using AAA

Configuring ACS 4.2 and 5.1 for Authentication

Verifying and Troubleshooting Authentication

Authorization of Administrative Sessions

Configuring ACS 4.2 and 5.1 for EXEC Authorization

Verifying and Troubleshooting EXEC Authorization

Command Authorization

Configuring ACS 4.2 and 5.1 for Command Authorization

Verifying and Troubleshooting Command Authorization

Accounting of Administrative Sessions

Configuring ACS for Accounting

### **Lab Scenario #2: Authentication, Authorization, and Accounting of Administrative Sessions Using TACACS+**

Lab Setup

Lab Solution

Lab Verification



# **Table of Contents**

## Lab Scenario #3: Authentication and Authorization of HTTP

### Sessions

Lab Setup

Lab Solution

Lab Verification

### Summary

## Chapter 7 Administrative AAA on ASA/PIX

### Local Database

### Privilege Levels

## Lab Scenario #4: Local Authentication and Privilege Levels on ASA

Lab Setup

Lab Solution

Lab Verification

### Using AAA

Configuring Authentication on ASA Using AAA

Configuring ACS 4.2 and 5.1 for Authentication

Verifying and Troubleshooting Authentication

Authorization of Administrative Sessions

Configuring ACS 4.2 and 5.1 for EXEC Authorization

Verifying and Troubleshooting EXEC Authorization

Command Authorization

Accounting of Administrative Sessions and Commands

## Lab Scenario #5: Authentication, Authorization and Accounting of Administrative Sessions on ASA using TACACS+

Lab Setup

Lab Solution

Lab Verification

### Summary

## Chapter 8 IOS Switches

# **Table of Contents**

## Introduction to 802.1X, EAP, and EAPOL

EAP

EAPOL

Message Exchange in 802.1X

## EAP Types

PEAPv0/EAP-MSCHAPv2

PEAPv1/EAP-GTC

EAP Authentication Type Summary

## 802.1X Configuration on a Cisco Switch

### 802.1X Host Modes

Single-Host Mode

Multiple-Host Mode

Multidomain Authentication Mode

Pre-Authentication Open Access

Multiauthentication Mode

### 802.1X Authentication Features

Guest VLAN

Restricted/Authentication Failed VLAN

MAC Authentication Bypass

VLAN Assignment

### 802.1X Timers

Quiet Period

Switch-to-Client Retransmission Time (tx-period)

Switch-to-Client Retransmission Time for EAP-Request Frames  
(supp-timeout)

Switch-to-Authentication-Server Retransmission Time for Layer 4 Packets  
(server-timeout)

Switch-to-Client Frame Retransmission Number (max-reauth-req)

## Configuring Accounting

## Certificate Installation on ACS

# **Table of Contents**

Certificate Installation on ACS 4.2

Certificate Installation on ACS 5.1

## **Configuring EAP-MD5 on ACS**

EAP-MD5 Configuration on ACS 4.2

EAP-MD5 Configuration on ACS 5.1

## **Configuring PEAP on ACS**

PEAP Configuration on ACS 4.2

PEAP Configuration on ACS 5.1

## **Configuring EAP-TLS on ACS**

EAP-TLS Configuration on ACS 4.2

EAP-TLS Configuration on ACS 5.1

## **Dynamic VLAN Assignment: ACS Configuration**

Dynamic VLAN Assignment for ACS 4.2

Dynamic VLAN Assignment for ACS 5.1

## **Lab Scenario #7: Configuring Switch, ACS, and Windows XP for 802.1X Authentication Using EAP-MD5**

Lab Setup

Lab Solution

ACS 4.2 Configuration Requirement

ACS 5.1 Configuration Requirement

Switch Configuration Requirements

Client Configuration Requirements

## **Lab Scenario #8: Configuring Switch, ACS, and Windows XP for 802.1X Authentication Using PEAP**

Lab Solution

## **Lab Scenario #9: Configuring Switch, ACS, and Windows XP for 802.1X Authentication Using EAP-TLS**

Lab Solution

## **Useful show Commands**

# **Table of Contents**

Troubleshooting 802.1X

Summary

## **Chapter 9 Access Points**

Configuring Wireless NAS for 802.1X Authentication on an AP

Configuring Wireless NAS for 802.1X Authentication on a WLC

Configuring ACS 4.2 for LEAP

Configuring ACS 5.1 for LEAP

Configuring ACS 4.2 for EAP-FAST

Configuring ACS 5.1 for EAP-FAST

Lab Scenario #10: Configure WLC, ACS and Cisco Secure Services

Client for 802.1X Authentication Using LEAP

Lab Setup

Lab Solution

ACS 4.2 Configuration Requirements

ACS 5.1 Configuration Requirements

WLC Configuration Requirements

Client Configuration Requirements

Lab Scenario #11: Configure WLC, ACS, and Cisco Secure Services

Client for 802.1X Authentication Using EAP-FAST

Lab Solution

ACS 4.2 Configuration Requirements

ACS 5.1 Configuration Requirements

Client Configuration Requirements

Troubleshooting 802.1X

Summary

## **Chapter 10 Cut-Through Proxy AAA on PIX/ASA**

Cut-Through Proxy Authentication

Virtual Telnet, Virtual HTTP, and HTTP Redirection

# **Table of Contents**

Virtual Telnet

Virtual HTTP

HTTP Redirection

uauth Timer

Configuring ACS for Cut-Through Proxy Authentication

Verifying and Troubleshooting Cut-Through Proxy Authentication

Lab Scenario #12: Authenticating Cut-Through Traffic on ASA

Lab Setup

Lab Verification

Lab Solution

Cut-Through Proxy Authorization

Configuring ACS 4.2 and 5.1 for Cut-Through Proxy Authorization Using  
TACACS+

Configuring ACS 4.2 for Cut-Through Proxy Authorization Using RADIUS

Configuring ACS 5.1 for Cut-Through Proxy Authorization Using RADIUS

Verifying and Troubleshooting Cut-Through Proxy Authorization

Cut-Through Proxy Accounting

Lab Scenario #13: Cut-Through Proxy Authentication,  
Authorization, and Accounting

Lab Setup

Lab Solution

Lab Verification

Summary

## **Chapter 11 Router**

Prerequisites for Authentication Proxy

Authenticating HTTP Sessions

Authenticating FTP Sessions

Authenticating Telnet Sessions

# **Table of Contents**

Configuring ACS for Authentication Proxy

Viewing and Maintaining Authentication Proxy Cache

Verifying and Troubleshooting Authentication Proxy

Authentication Proxy Authorization

- Configuring ACS 4.2 for Authorization Using TACACS+

- Configuring ACS 5.1 for Authorization Using TACACS+

- Configuring ACS 4.2 for Authorization Using RADIUS

- Configuring ACS 5.1 for Authorization Using RADIUS

- Verifying and Troubleshooting Authentication Proxy Authorization

Authentication Proxy Accounting

Lab Scenario #14: Authentication Proxy

Lab Setup

Lab Solution

Lab Verification

Summary

## **Chapter 12 AAA of VPN and PPP Sessions on IOS**

Authenticating VPN Sessions

- Authenticating IPsec Remote Access Sessions

- Authenticating SSL VPN Sessions

- Configuring ACS 4.2 and 5.1 for IPsec and SSL VPN Authentication

Verifying and Troubleshooting VPN Authentication

Authorizing VPN Sessions

- Authorizing IPsec Remote Access Sessions

- Configuring ACS 4.2 and ACS 5.1 for IPsec Remote Access Authorization

- Authorizing SSL VPN Sessions

- Configuring ACS 4.2 and ACS 5.1 for SSL VPN Authorization

Verifying and Troubleshooting VPN Authorization

Accounting for IPsec Remote Access and SSL VPN

# **Table of Contents**

## **Lab Scenario #15: VPN AAA**

Lab Setup

Lab Solution

Lab Verification

## **Authenticating PPP Sessions**

Configuring ACS for PPP Authentication

## **Verifying and Troubleshooting PPP Authentication**

## **Authorizing PPP Sessions**

Configuring ACS 4.2 and 5.1 for PPP Authorization

## **Verifying and Troubleshooting PPP Authorization**

## **Accounting for PPP Sessions**

## **Summary**

## **Chapter 13 AAA of VPN on ASA**

### **Authenticating Remote Access IPsec VPN (EzVPN Remote) and SSL VPN Using RADIUS**

Configuring ACS for IPsec Remote Access and SSL VPN Authentication

Verifying and Troubleshooting VPN RADIUS Authentication

### **Authorizing IPsec Remote Access and SSL VPN Using RADIUS**

Configuring ACS 4.2 and 5.1 for IPsec and SSL VPN Authorization

Verifying and Troubleshooting VPN Authorization

### **Accounting for IPsec and SSL VPN Using RADIUS**

### **Lab Scenario # 16: VPN AAA Using RADIUS**

Lab Setup

Lab Solution

Lab Verification

### **Authenticating IPsec and SSL VPN Using LDAP**

Verifying and Troubleshooting VPN Authentication Using LDAP

### **Authorizing IPsec and SSL VPN Using LDAP**

# **Table of Contents**

Verifying and Troubleshooting VPN Authorization with LDAP

## **Lab Scenario # 17: VPN Authentication and Authorization Using LDAP**

Lab Setup

Lab Solution

Lab Verification

Summary

## **Chapter 14 ACS 4.2 Advanced Configuration**

Network Access Restrictions

Backup and Restore

Manual Backups

Scheduled Backups

Recovering ACS from a Backup file

Database Replication

Understanding Database Replication

Replication Versus Backup

Configuring the Primary Server for Replication

Configuring a Secondary Server

RDBMS Synchronization

accountActions Format

Performing RDBMS Synchronization

Network Access Profiles

Classification of Network Request

Policies

Local Password Management

Remote Logging

Log File Management

CSUtil Database Utility

Summary



# **Table of Contents**

## **Chapter 15 ACS 5.1**

### **Replication**

Activating Secondary Servers

### **Dictionaries**

### **Remote Logging**

Defining a Remote Log Target

Specifying a Remote Log Target Under a Logging Category

### **Importing Network Resources and Users**

### **Managing System Administrators**

### **Backup and Restore**

Software Repositories

Backing Up a Database

### **Scheduled Backups**

Restoring Databases

### **Summary**

## **Index**