TACACS+ in Nexus 4005I Configuration Example

Document ID: 112006

Contents

Introduction
Prerequisites
Requirements
Components Used
Conventions
Configurations
Step−by−Step Instructions

TACACS+ CLI Configuration
Verify
Troubleshoot
Related Information

Introduction

This document describes how to configure Terminal Access Controller Access Control System (TACACS+) in a Nexus 4000 series switch. The TACACS+ authentication varies slightly in the Nexus 4000 series than a Cisco Catalyst Switch.

Prerequisites

Requirements

Cisco recommends that you have knowledge of this topic: Cisco Nexus 7000 Series NX−OS Fundamentals Commands.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Nexus 4005I Switch
- Cisco Secure Access Control Server (ACS) 5.x

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to the Cisco Technical Tips Conventions for information on document conventions.

Configurations

The configuration example in this section describes how to configure a Nexus 4005I switch and a TACACS+ server.

Step−by−Step Instructions

Complete these steps in order to configure the Nexus switch and the TACACS+ server:

1. Enable TACACS+ protocol feature.

   The IP address of the ACS server must be configured with the preshared key. If there are more than one ACS server, both hosts must be configured.
2. Enable the AAA concept and the AAA server group.

   In this configuration example, the name of the AAA group name is "ACS."

TACACS+ CLI Configuration

ASA

```

!−−− Enable TACACS+ on the device.

feature tacacs+
tacacs−server host 10.0.0.1 key 7 Cisco
tacacs−server host 10.0.0.2 key 7 Cisco
tacacs−server directed−request


!−−− Provide the name of your ACS server.

aaa group server tacacs+ ACS

!−−− Mention the IP address of the tacacs−servers
!−−− referred to in the "tacacs−server host" command.

server 10.0.0.1
server 10.0.0.2

!−−− Telnet and ssh sessions.

aaa authentication login default group ACS local

!−−− Console sessions.

aaa authentication login console group ACS local

!−−− Accounting command.

aaa accounting default group ACS
```

Note: Use the same preshared key "Cisco" in the ACS server for authentication between the Nexus 4000 series and ACS server.

Note: If the TACACS+ server is down, you can fall back to authenticate locally by configuring the user name and password in the switch.

The Nexus operating system does not use the concept of *privilege* levels instead it uses *roles*. By default you are placed in the *network−operator* role. If you want a user to have full permissions, you must place them in the *network−admin* role, and you must configure the TACACS server to push down an attribute when the user logs in. For TACACS+, you pass back a TACACS custom attribute with a value of `roles="roleA"`. For a full access user, you use: `cisco−av−pair*shell:roles="network−admin"`

```
cisco-av-pair*shell:roles="network-admin"(The
         * makes it optional)

shell:roles="network-admin"
```

Verify

Use the commands in this section in order to verify the TACACS+ server configuration:

- **show tacacs−server** Displays the TACACS+ server configuration.
- **show aaa authentication [login {error−enable | mschap}]** Displays configured authentication information.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- **Configuring AAA**
- **Configuring TACACS+**
- **Technical Support & Documentation − Cisco Systems**

Updated: Jun 01, 2010 Document ID: 112006