Nexus Integration with ACS 5.2 Configuration Example

Document ID: 115925

Contributed by Minakshi Kumar, Cisco TAC Engineer.
Mar 15, 2013

Contents

Introduction

This document provides an example of TACACS+ authentication configuration on a Nexus switch. By default, if you configure the Nexus switch in order to authenticate through Access Control Server (ACS), you are automatically placed in the network−operator/vdc−operator role, which provides read−only access. In order to be placed in the network−admin/vdc−admin role, you need to create a shell on the ACS 5.2. This document describes that process.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- Define your Nexus switch as a client in ACS.
- Define the IP address and an identical shared secret key on the ACS and Nexus.

Note: Create a checkpoint or a backup on Nexus before you make any changes.

Components Used

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

- ACS 5.2
- Nexus 5000, 5.2(1)N1(1)

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 more information on document conventions.

Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Nexus Device for Authentication and Authorization with ACS 5.2 Configuration

Complete these steps:

1. Create a local user on the Nexus switch with full privileges for fallback:

   ```
   username admin privilege 15 password 0 cisco123!
   ```
2. Enable TACACS+, then provide the IP address of the TACACS+ Server (ACS):

   ```
   feature tacacs+

   tacacs-server host IP-ADDRESS key KEY


   tacacs-server key KEY


   tacacs-server directed-request

   aaa group server tacacs+ ACS

   server IP-ADDRESS


   use-vrf management

   source-interface mgmt0
   ```

   Note: The key must match the shared secret configured on the ACS for this Nexus device.
3. Test the TACACS server availability:

   ```
   test aaa group group-name username password
   ```

   The test authentication should fail with a reject message from the server, since the server has not been configured. This reject message confirms that the TACACS+ server is reachable.
4. Configure login authentications:

   ```
   aaa authentication login default group ACS

   aaa authentication login console group ACS

   aaa accounting default group ACS

   aaa authentication login error-enable
   ```

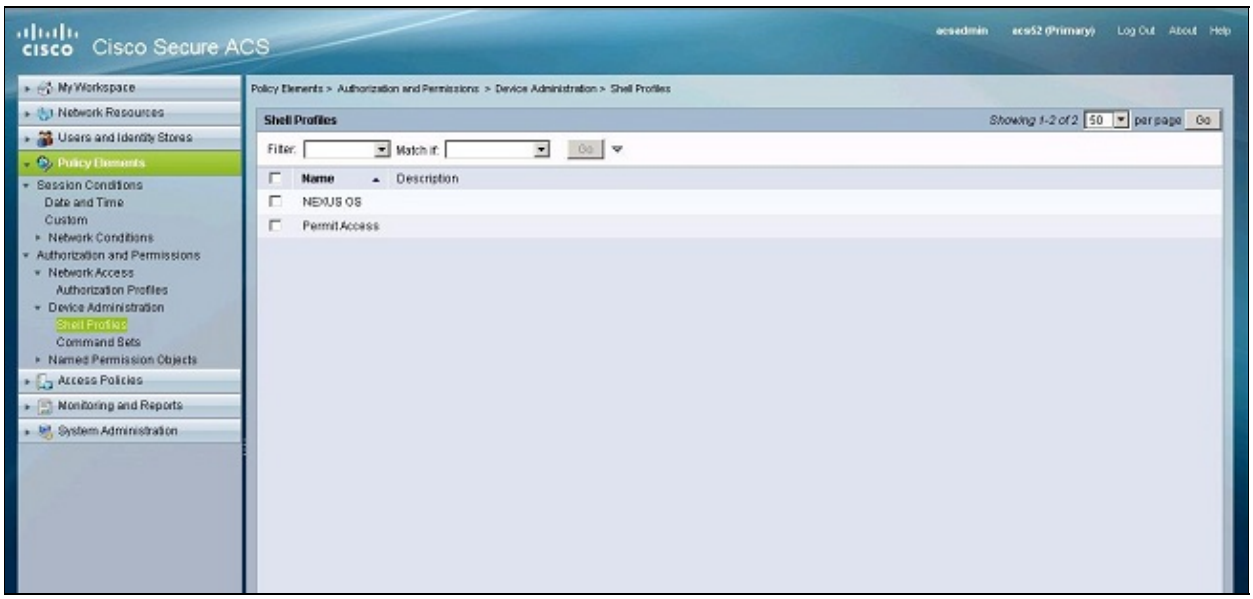
```
aaa authorization commands default local

aaa authorization config-commands default local
```

Note: Nexus uses local authentication if the authentication server is unreachable.

ACS 5.x Configuration

Complete these steps:

1. Navigate to **Policy Elements > Authentication and Permissions > Device Administration > Shell Profiles** in order to create a Shell Profile.

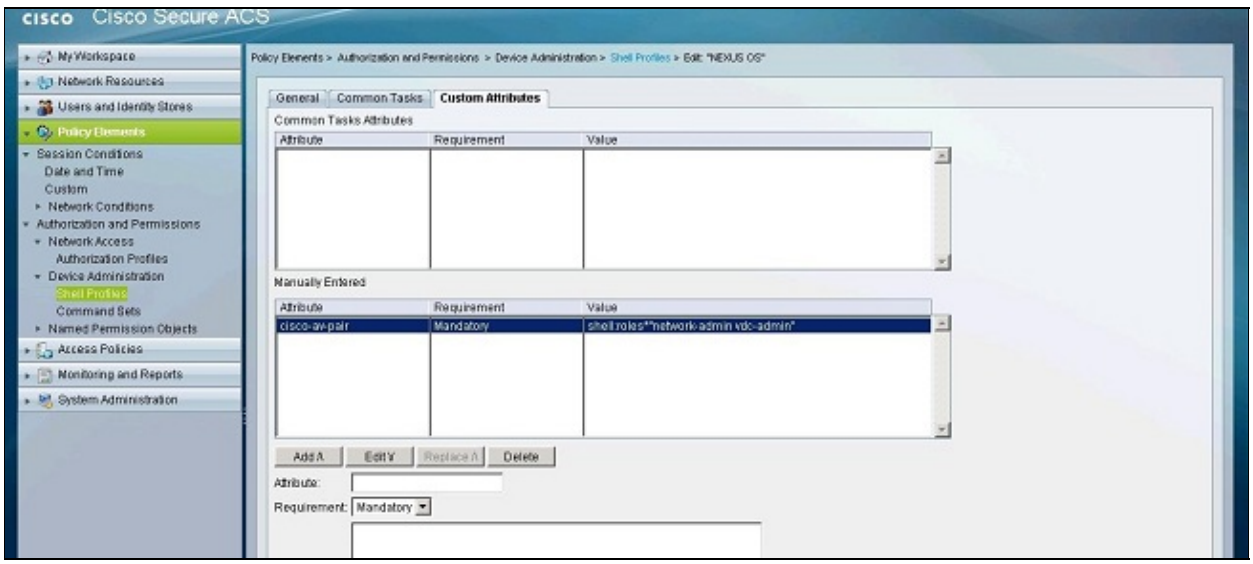


2. Enter a name for the profile.
3. Under the Custom Attributes tab, enter these values:

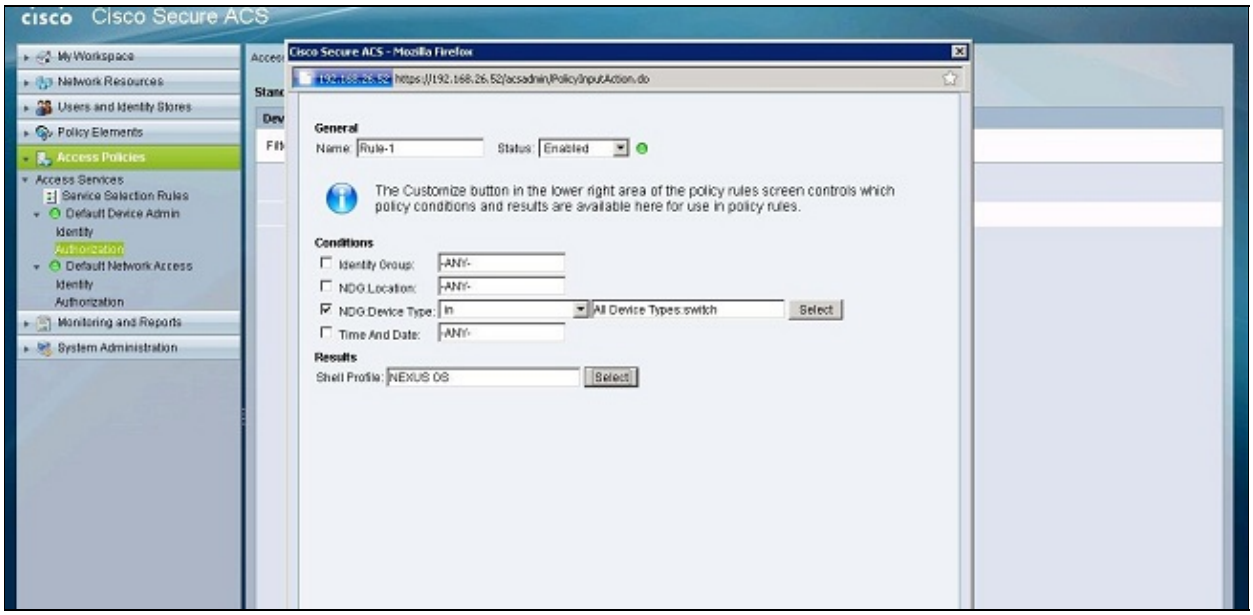
   Attribute: cisco−av−pair

   Requirement: Mandatory

   Value: shell:roles*"network−admin vdc−admin"



4. Submit the changes in order to create an attribute−based role for the Nexus switch.
5. Create a new authorization rule, or edit an existing rule, in the correct access policy. By default, TACACS+ requests are processed by the Default Device Admin access policy.
6. In the Conditions area, choose the appropriate conditions. In the Results area, choose the Nexus OS shell profile.



7. Click **Ok**.

Verify

Use this section to confirm that your configuration works properly.

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

- **show tacacs+** Displays the TACACS+ statistics.
- **show running−config tacacs+** Displays the TACACS+ configuration in the running configuration.
- **show startup−config tacacs+** Displays the TACACS+ configuration in the startup configuration.
- **show tacacs−server** Displays all configured TACACS+ server parameters.

Related Information

- **Technical Support & Documentation − Cisco Systems**

Updated: Mar 15, 2013 Document ID: 115925