NCS Integration with ACS 5.4 Configuration Example

Document ID: 116358

Contributed by Minakshi Kumar, Cisco TAC Engineer.
Aug 23, 2013

Contents

Introduction

This document provides a configuration example for TACACS+ authentication and authorization on the Cisco Prime Network Control System (NCS) Release 1.1.

Prerequisites

Requirements

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

- Define NCS as a client in the Access Control System (ACS).
- Define the IP address and an identical shared−secret key on the ACS and NCS.

Components Used

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

- ACS Version 5.4
- NCS Prime Release 1.1

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.

Configure

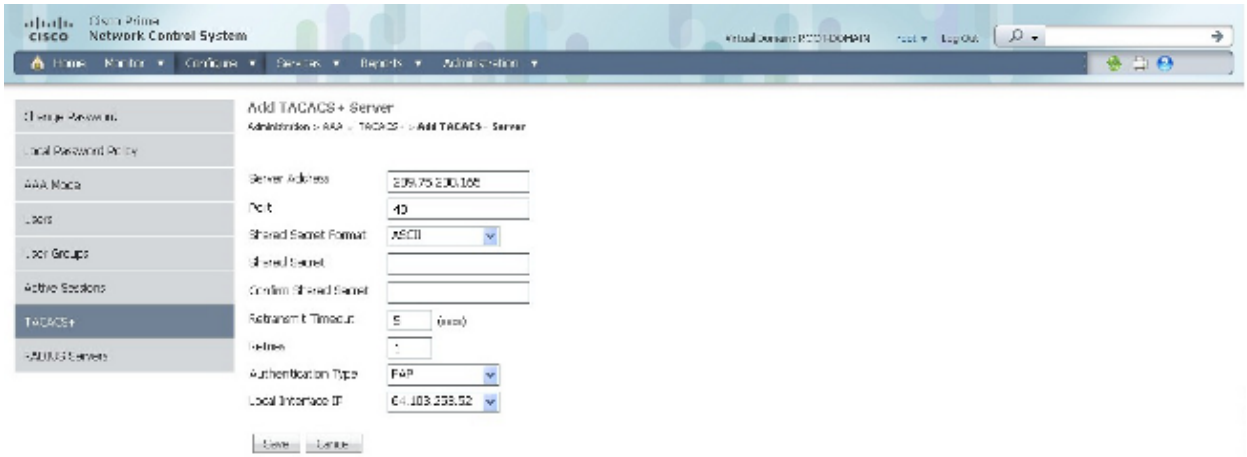
In this section, you are presented with the information used in order to configure the features described in this document.

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

Add ACS as a TACACS Server

Complete these steps in order to add ACS as a TACACS server:

1. Navigate to ***Administration*** > ***AAA***.
2. From the left sidebar menu, choose ***TACACS+***, and this information displays:



   The TACACS+ page shows the IP address, port, retransmit rate, and authentication type.

3. Add the IP address of the ACS server.
4. Enter the TACACS+ shared secret used by the ACS server.
5. Reenter the shared secret in the ***Confirm Shared Secret*** text box.
6. Leave the rest of the fields on their default setting.
7. Click ***Submit***.

AAA Mode Settings

In order to choose an Authentication, Authorization, and Accounting (AAA) mode, complete these steps:

1. Navigate to ***Administration*** > ***AAA***.
2. Choose ***AAA Mode*** from the left sidebar menu, and this information displays:

3. Choose ***TACACS+***.

4. Check the ***Enable Fallback to Local*** check box if you want the administrator to use the local database when the external AAA server (ACS) is down. This is recommended so that authentication still occurs if the TACACS+ server fails. Once the configuration is verified and works, you can make changes, if desired.

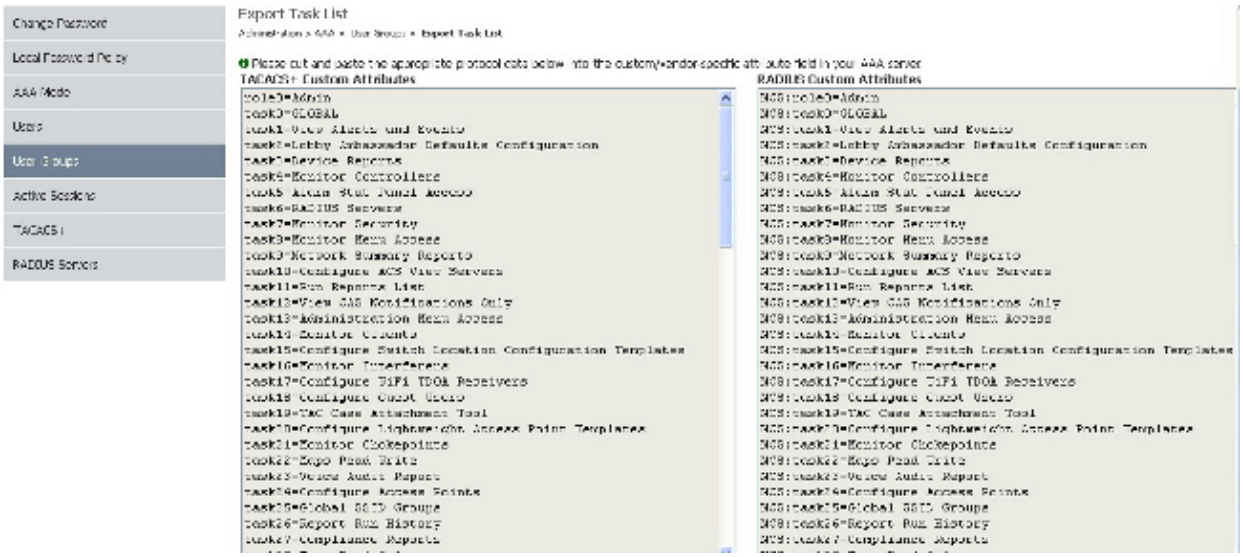
ACS Version 5.4 Configuration

For ACS Version 5.4 configuration, you must complete these steps in order to send attributes from the ACS to the NCS:

1. Retrieve the attributes:

   - Navigate to ***Administration*** > ***AAA*** > ***User Groups***.

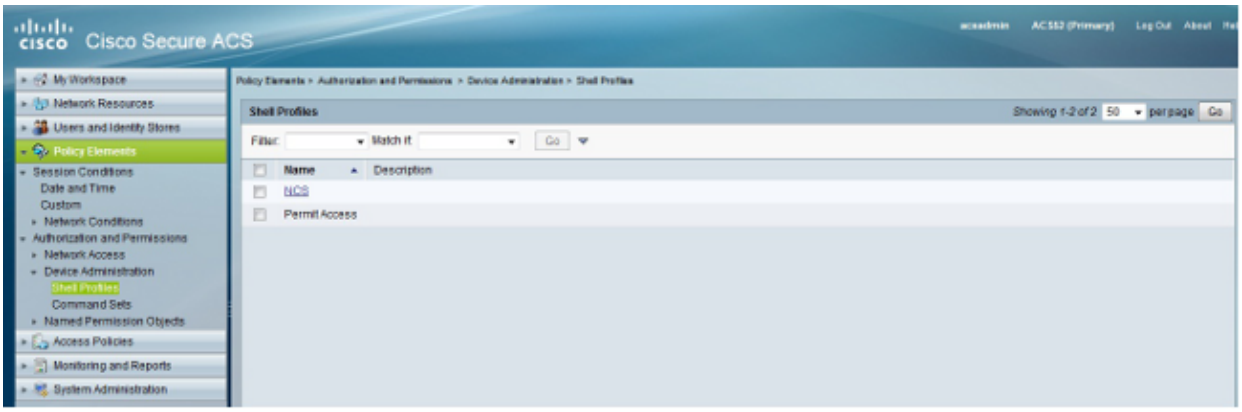
   - This example shows administrator authentication. Look for the ***Admin Group Name*** in the list, and click the ***Task List*** option on the right.



2. Export and save the attributes to the desktop.

3. Log in to the ***ACS Admin GUI***, and navigate to ***Policy Elements > Authentication and Permissions > Device Administration > Shell Profiles*** in order to create a Shell Profile.

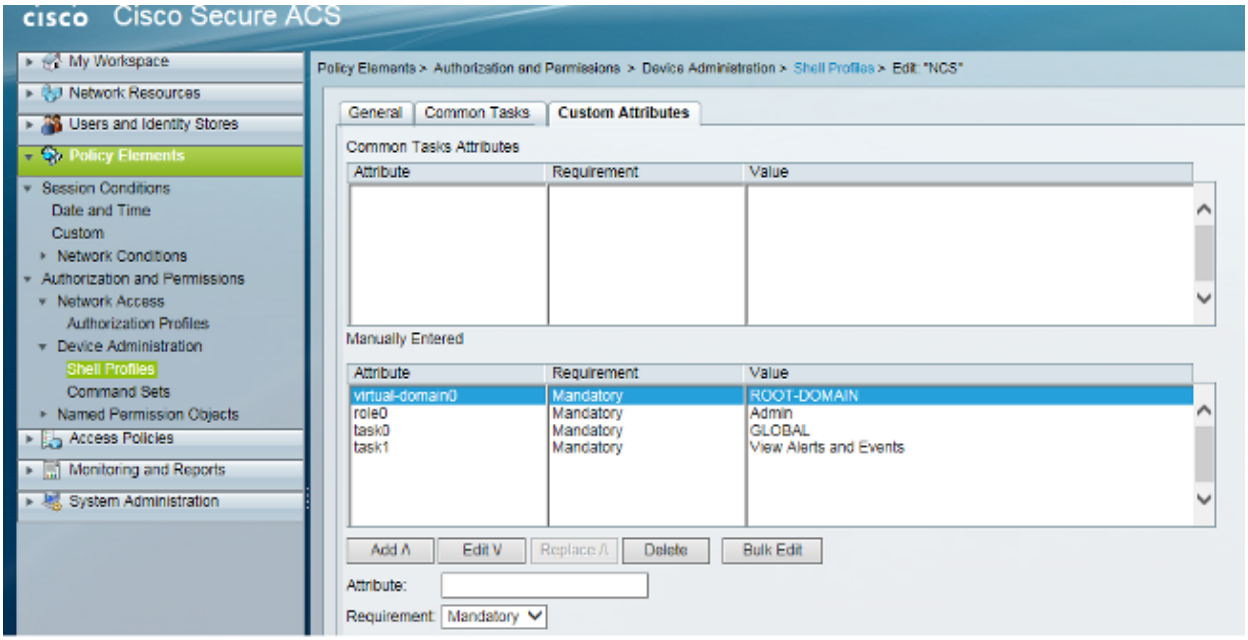
4. Name the profile ***NCS***.



5. From the ***Custom Attributes*** tab, enter these values:

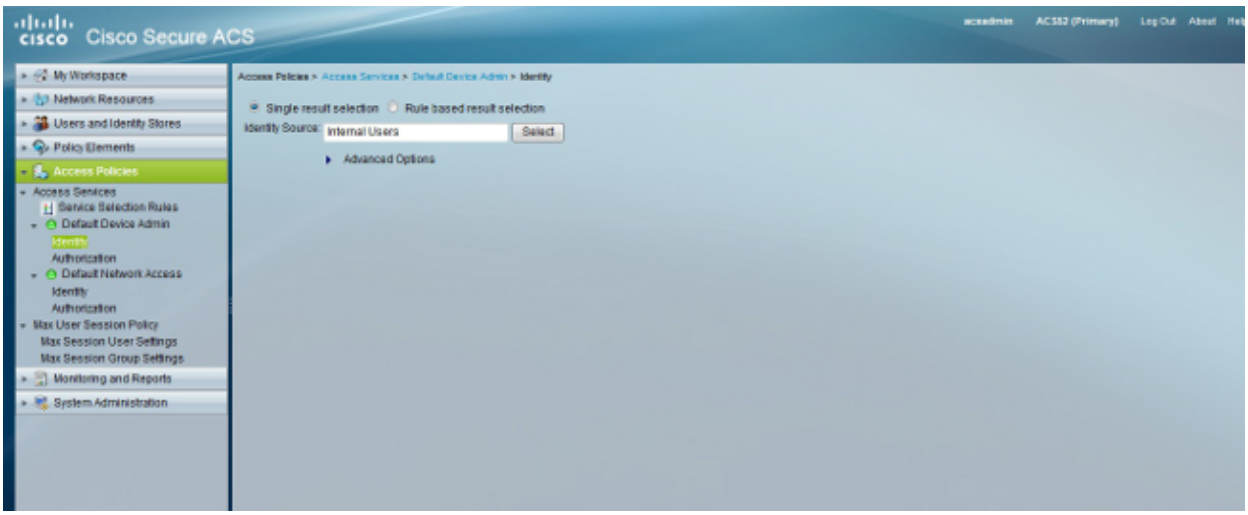
```
Attribute          Requirement    Value
-----------------------------------------------------
role0               Mandatory     Admin
task0               Mandatory     GLOBAL
task1               Mandatory     View Alerts and Events
Virtual-domain0     Mandatory     ROOT-DOMAIN
```

Note: Virtual−domain is included in the list in case you use a recent release of NCS. You must define the user Virtual Domain.

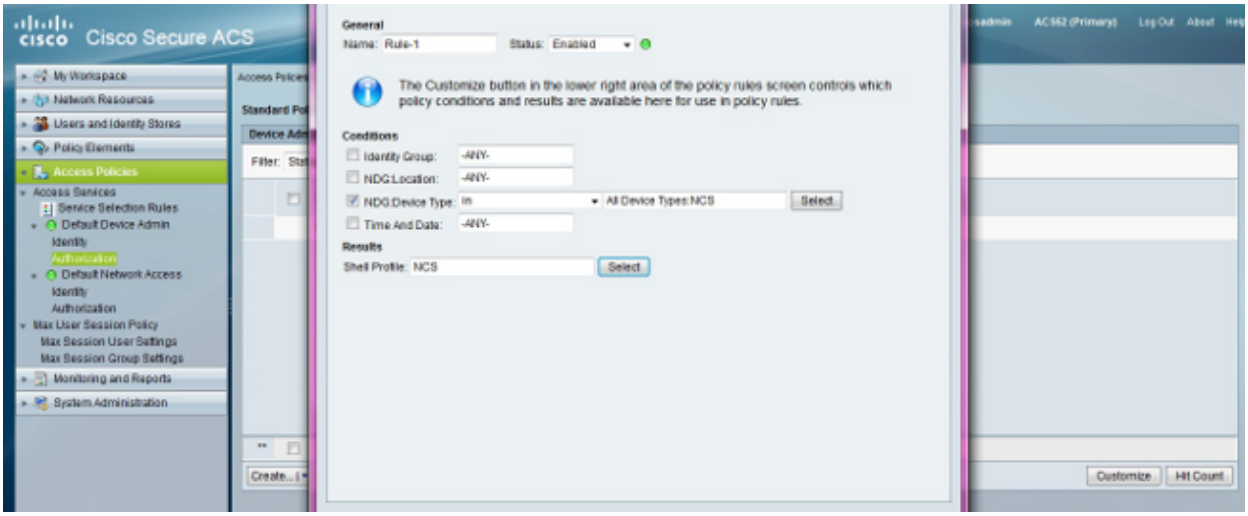


6. Submit the changes in order to create an attribute−based role for the NCS.

7. Navigate to ***Access Policies*** > ***Access Services*** > ***Default Device Admin*** > ***Identity***, and choose ***Internal Users*** for the Identity Source.



8. Create a new authorization rule or edit a rule that already exists in the correct access policy. By default, TACACS+ requests are processed by the ***Default Device Admin*** access policy.



9. In the ***Conditions*** area, choose the appropriate conditions. In the ***Results*** area, choose ***NCS*** for the Shell Profile.

10. Click ***OK***.

Verify

Log into the NCS and confirm that you have the ***Admin*** role.

Troubleshoot

If you cannot log into the NCS, log into the ACS GUI and navigate to ***Monitoring and Reports*** > ***Catalog*** > ***AAA Protocols*** > ***TACACS+ Authentication***. Select the failed authentication, and choose ***Details*** in order to see why the authentication failed or was rejected.

Updated: Aug 23, 2013 Document ID: 116358