Send document comments to nexus5k-docfeedback@cisco.com.

CHAPTER 1

Troubleshooting Security Issues

The Cisco Nexus 5000 NX-OS provides security that protects your network from degradation or failure and from data loss or compromise resulting from intentional attacks or from unintended, damaging mistakes.

This chapter describes how to identify and resolve problems that can occur with security in the Cisco Nexus 5000 Series switch.

This chapter includes the following sections:

Roles

Role assignment fails when user logs in

From the perspective of RBAC, when a user logs in, role assignment fails.

Possible Cause

The AV-pair is not configured properly on TACAC+ or the RADIUS server.

Solution

To complete the role assignment follow these steps:

Step 1 Check the TACACS+ (for example, ACS) server configuration.

- Use the following menu path to access the settings:

  Interface Configuration > TACACS+ (Cisco IOS)

  - Select the User box for Shell (exec)
  - Select the Advanced TACACS+ Features

  Display a window for each service that was selected, where you can enter customized TACACS+ attributes in the Advanced Configuration Options.

- Use the following menu path to access the settings and add a string to the Shell attributes:

  User Setup > Add/Edit “admin” > TACACS+ Settings

  - Select the Shell and Custom attributes boxes

Send document comments to nexus5k-docfeedback@cisco.com.

- Add the following string into the textbox:

  cisco-av-pair=shell:roles="network-admin"

Step 2 Check the RADIUS (for example, ACS) server configuration.

- Use the following menu paths to access the settings:

  Network Configuration > AAA > AAA Servers > svi,20.1.1.2,CiscoSecure ACS

  Network Configuration > AAA > AAA Client > 20.1.1.1 20.1.1.1 RADIUS (Cisco IOS/PIX 6.0) > SharedSecret=test1234, Authenticate Using=RADIUS (Cisco IOS/PIX 6.0)

  Interface Configuration > RADIUS (Cisco IOS/PIX 6.0)

  - Select User for cisco-av-pair.
- Use the following menu path to access the settings and add a string to the RADIUS attributes:

  User Setup > Add/Edit <username> > Cisco IOS/PIX 6.x RADIUS Attributes

  - Check the attribute box.
  - Enter the following string:

    shell:roles="network-admin"

Step 3 Check the RADIUS (for example, RADIUSD) server configuration for settings in the user account.

- Use the following path to access the user account definition:

  .../etc/raddb
- Ensure that the user account definition contains:

  cisco-avpair= "shell: roles = network-admin"

Step 4 Log in the user again.

Step 5 Check the role assignment with the **show user-account** command.

Rules for Role's permit/deny action do not work correctly

When a user-defined role is assigned to a user account, the role's rule policy may not seem to take effect. For example, a rule in the role's configuration is set to deny all interface configuration commands. However, you still can configure interface commands.

Possible Cause

Order of rule configurations for the role is incorrect.

Note The RBAC parser accesses a rule from highest to lowest rule number.

Solution

After identifying the rule that is not working correctly, check to see if any rules preceding it conflict or override it.

For example, if the rule that is not working correctly has a rule ID of 10, then check all the rules that have a rule ID greater than 10 to see if they might conflict with rule 10. To illustrate this example, we can say that rule 15 is found to be overriding rule 10. To resolve this conflict, you would have to modify rule 15 or change the rule ID of rule 10 so that it has a greater rule ID than rule 15.

Send document comments to nexus5k-docfeedback@cisco.com.

Role's interface or VLAN policy does not appear to work correctly

When a user-defined role is assigned to a user account and the role's interface or VLAN policy is set to deny access to a certain interface, the user account can still use **show** commands to display configuration, status, setting, or statistics on the access-denied interface or VLAN.

Possible Cause

You are checking the interface or VLAN role policy with CLI commands, such as **show interface brief** or **show vlan**.

Solution

RBAC does not support filtering when displaying commands. Interface or VLAN role policies only apply to configuration or operational commands.

Possible Cause

You are not assigned to the role properly.

Solution

- Check the user role assignment with the **show user-account** command.
- Verify the role definition with the **show role name** <*name*> command.

Assigning multiple roles to single user does not seem to work correctly

When a user account is assigned to multiple roles, the user can access commands that are denied by one of the roles that it gets assigned to. This gives the appearance that the command parser does not work with multiple roles.

Possible Cause

You might expect that multiple roles on the same user account are parsed sequentially.

Solution

The NX-OS design is to parse multiple roles in a union-to-permit function, that each command is examined and compared to all the roles.

If any of the roles permit the command, then the CLI allows the user to continue.

For example, if the role permits the **interface eth1/1** command, then the CLI allows the you to enter the interface eth1/1 configuration mode.

Each role applies their policies (that is, interface, VLAN, VSAN, and so on) separately. If a role has an interface policy that denies eth1/1 as in the example, then that role would reject the command, but other roles might have a different interface policy allowing the same interface.

Change to role configuration does not get applied

When a user account is assigned to a role and you are logged into the Nexus 5000 switch, any changes made to the role configuration does not get applied immediately.

Possible Cause

While a user account is logged in and has been assigned to role A, the administrator makes some changes to role A with the expectation that the change would immediately affect the user that is logged in. However, the user is not assigned to the role properly.

Send document comments to nexus5k-docfeedback@cisco.com.

Solution

NX-OS does not activate role configuration changes dynamically. You needs to log in again to have the configuration changes to the new role come into effect.

CLI rejects feature-group removal

The CLI rejects the **no role feature-group name** <*group-name*> command when the administrator tries to delete a feature-group.

Possible Cause

A CLI error indicates that the feature group is in use, which means that it is included in one of the role configurations.

Solution

To address the error, perform the following steps:

- Use the **show role | egrep role:|feature-group** command to display which feature group is associated with the role or under which role.
- Detach the association with the **no rule** command within the role configuration mode, and then delete the feature group.

AAA

User cannot login through TACACS+ or RADIUS authentication

With the server group properly configured for the Nexus 5000 switch and the server group is assigned the aaa authentication login default configuration on TACACS+ or RADIUS servers, the Telnet or SSH login fails to authenticate users with the following error:

```
%TACACS-3-TACACS_ERROR_MESSAGE: All servers failed to respond
```

Possible Cause

AAA group is not configured with the correct VRF to access servers.

Solution

Perform the following steps to enable login:

- Check which AAA group is being used for authentication with the **show running-config aaa** and **show aaa authentication** commands.
- For TACACS+, check the VRF association with the AAA group with the **show tacacs-server groups** and **show running-config tacacs+** commands.
- For RADIUS, check the VRF association with the AAA group with the **show radius-server groups** and **show running-config radius** commands.
- Correct the VRF association, then test the VRF setting with the **test aaa group** <*name*> <*username*> <*password*> command.
- If the **test aaa** command returns the error, “user has failed authentication", then the server is accessible but the credentials for the user account are incorrect. Verify that the user configuration is correct on the server.

Send document comments to nexus5k-docfeedback@cisco.com.

Possible Cause

AAA server is not accessible in network.

Solution

If the problem persists after correcting the VRF association and correcting the user-account credentials, then perform the following:

- If the **test aaa** command returns the error, "error authenticating to server", the route to the server might be missing in the configuration. Use the **ping** <*server*> command, if the AAA server is associated with the default VRF. If it is associated with VRF management, use the **ping** <*server*> **vrf management** command.
- If the message "No route to host" appears, then the static route to the server is not configured properly. Reconfigure the IP route in the corresponding VRF context.
- Enter the **ping** <*server*> command again. If the command is successful, then use the **test aaa group** <*name*> <*username*> <*password*> command.
- If the **ping** <*server*> command is unsuccessful, then check the network connectivity, such as if the ARP entry of the nexthop router is displayed in the **show ip arp [vrf management]** command or if the ARP entry of the Nexus 5000 switch exists in the nexthop router's ARP table.

Unable to decode content of packets with Wireshark

AAA packets were captured from the network, but Wireshark was unable to decode the content of the packets.

Possible Cause

AAA packets are encrypted while the host key is enabled.

Solution

Perform the following steps to decode the content:

- Use the no tacacs-server command to delete the TACACS server configuration.
- Reconfigure the TACACS server without specifying any key.
- Reconfigure the AAA client for the Nexus 5000 switch on the Network Configuration page in ACS while removing the host key.
- Re-do the wire tapping. The captured packets now should not be encrypted and the data content should be decoded properly by Wireshark.
- After the packet capturing, the administrator should revert to the host key configuration for better security.

Role assignment fails when user logs in

Role assignment fails when the user logs in. (From the perspective of the Nexus 5000 switch AAA.)

Possible Cause

Assuming that the ACS or TACACS+ and RADIUS has the Cisco av pair configured correctly, then the problem might be that the internal or local VRF assignment for the user login is not working correctly.

Solution

Send document comments to nexus5k-docfeedback@cisco.com.

Perform the following steps for role assignment:

- Check which AAA group is being used for authentication with the **show running-config aaa** and **show aaa authentication** commands.
- For TACACS+, check the VRF association with the AAA group with the **show tacacs-server groups** and **show running-config tacacs+** commands.
- For RADIUS, check the VRF association with the AAA group with the **show radius-server groups** and **show running-config radius** commands.
- If the above commands show that the association is correct, then use the **debug tacacs+ all** command to enable the trace.
- Log in the user again, and collect the debug trace.

  The trace should contain information for further investigation (as shown in the example).

  Example:

  ```
  tacacs: process_aaa_tplus_request: Group t1 found. corresponding vrf is management
  ```

- Use the **no debug tacacs+ all** command to turn off debug tracing on TACACS+.

No command accounting logs on ACS server when TACACS+ accounting enabled

When TACACS+ accounting is enabled, the command accounting logs on the ACS server are not found.

Possible Cause

The ACS server configuration is wrong or incomplete.

Solution

Perform the following steps:

- In the ACS GUI in Network Configuration, go to the AAA Client Setup for any client. Check the checkbox for **Log Update/Watchdog Packets from this AAA Client**. Click the **Submit + Apply** button.
- Verify CMD Accounting with the following menu path:

  Reports and Activity > TACACS+ Administration

  Open the Tacacs+Administration <active|DATE>.csv file and verify the cmd and timestamp on each row of the file.

aaa authentication login ascii-authentication works only for TACACS+ and not for RADIUS

Possible Cause

From Cisco NX-OS Release 4.2(1)N1(1), the **aaa authentication login ascii-authentication** command is supported only for TACACS+ and not for RADIUS.

Solution

PAP is the default authentication if no other authentication is configured on the switch. Remove the **aaa authentication login ascii-authentication** configuration so that PAP can be configured as the default authentication for both RADIUS and TACACS+.

Send document comments to nexus5k-docfeedback@cisco.com.

Note If you try to configure ASCII authentication for RADIUS with the **aaa authentication login ascii-authentication** command, the following syslog message is displayed during log in.

Example:

```
2016 Jun 14 16:14:15 B21-5596-4 %RADIUS-2-RADIUS_NO_AUTHEN_INFO: ASCII authentication not
supported
2016 Jun 14 16:14:16 B21-5596-4 %AUTHPRIV-3-SYSTEM_MSG: pam_aaa:Authentication failed from
64.103.217.161 - dcos_sshd[16804]
```

Authentication fallback method appears inoperable

The NX-OS supported fallback method for authentication is that if all the AAA remote RADIUS or TACACS+ servers are unreachable, then the log in attempts to authenticate the SSH/Telnet user locally. However, the login to the Nexus 5000 switch might still fail with the local authentication.

Possible Cause

The local user database does not contain the user account that the user is using to login with.

Solution

Perform the following steps to check the authentication fallback method.

- As a best practice, include the **aaa authentication login error-enable** command in the configuration. When it is included in the configuration, the login session sees whether the fallback method is operating correctly. If messages, such as “Remote AAA servers unreachable; local authentication done" or “Remote AAA servers unreachable; local authentication failed", are received, then the fallback method is operating correctly.
- If the remote AAA servers are not accessible, check to see if the local user database has the user credential for local authentication. Use the **show user-account** command to display the credential.

Note By using the **show user-account** command, you can determine which user-account was created through REMOTE authentication. A user account that was created with REMOTE authentication cannot be used for a local (fallback) login.

- Create local user accounts with the **username <username> password <password> role <role name>** command until the remote AAA servers become accessible.

Send document comments to nexus5k-docfeedback@cisco.com.