Configuring AAA

This chapter contains the following sections:

Information About AAA

AAA Security Services

Based on a user ID and password combination, authentication, authorization, and accounting (AAA) is used to authenticate and authorize users. A key secures communication with AAA servers. AAA supports IPv4 and IPv6 addresses.

In many circumstances, AAA uses protocols such as RADIUS or TACACS+ to administer its security functions. If your router or access server is acting as a network access server, AAA is the means through which you establish communication between your network access server and your RADIUS or TACACS+ security server.

Although AAA is the primary (and recommended) method for access control, additional features for simple access control are available outside the scope of AAA, such as local username authentication, line password authentication, and enable password authentication. However, these features do not provide the same degree of access control that is possible by using AAA.

Separate AAA configurations are made for the following services:

- User Telnet or Secure Shell (SSH) login authentication
- Console login authentication
- User management session accounting

The following table provides the authentication commands:

AAA Service Configuration Option	Related Command
Telnet or SSH login	aaa authentication login default
Console login	aaa authentication login console

Authentication

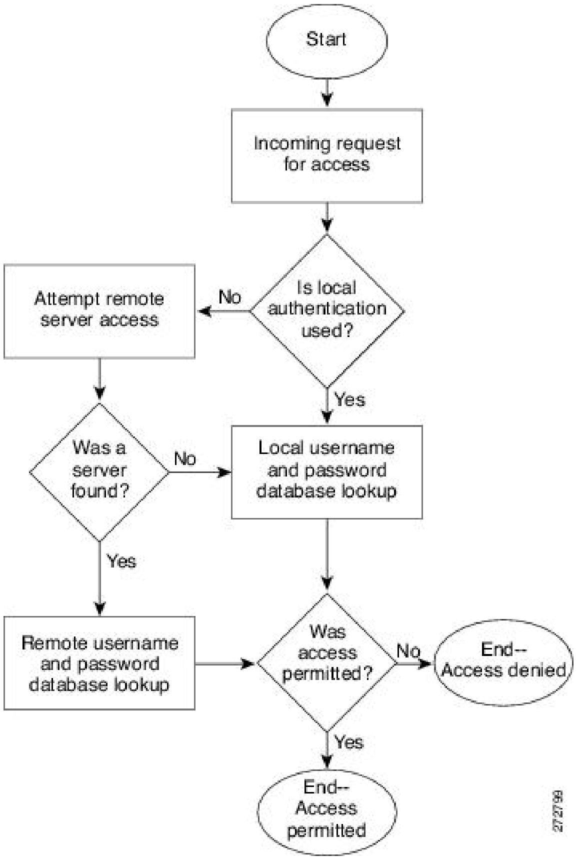
Authentication provides the method of identifying users, including login and password dialog, challenge and response, messaging support, and, depending on the security protocol that you select, encryption. Authentication is the way a user is identified prior to being allowed access to the network and network services. You configure AAA authentication by defining a named list of authentication methods and then applying that list to various interfaces.

Authentication is accomplished as follows:

Authentication Method	Description
Local database	Authenticates the following with a local lookup database of usernames or passwords: • Console login authentication • User login authentication • User management session accounting
Remote RADIUS or TACACS+ server	Authenticates the following with a local lookup database of usernames or passwords: • Console login authentication • User login authentication • User management session accounting
None	Authenticates the following with only a username: • Console login authentication • User login authentication • User management session accounting

The following figure shows a flowchart of the authentication process.

Figure 1: Authenticating User Login


Start
Incoming request for access
Is local authentication used?
No
Attempt remote server access
Yes
Was a server found?
No
Local username and password database lookup
Yes
Remote username and password database lookup
Was access permitted?
No
End-- Access denied
Yes
End-- Access permitted
272799

Note This diagram is applicable only to username password SSH authentication. It does not apply to public key SSH authentication. All username password SSH authentication goes through AAA.

Authorization

Authorization restricts the actions that a user is allowed to perform. It provides the method for remote access control, including one-time authorization or authorization for each service, per-user account list and profile, user group support, and support of IP, IPX, ARA, and Telnet.

Remote security servers, such as RADIUS and TACACS+, authorize users for specific rights by associating attribute-value (AV) pairs, which define those rights, with the appropriate user. AAA authorization works by assembling a set of attributes that describe what the user is authorized to perform. These attributes are compared with the information contained in a database for a given user, and the result is returned to AAA to determine the user's actual capabilities and restrictions.

Accounting

Accounting provides the method for collecting and sending security server information used for billing, auditing, and reporting, such as user identities, start and stop times, executed commands (such as PPP), number of packets, and number of bytes. Accounting enables you to track the services that users are accessing, as well as the amount of network resources that they are consuming.

Accounting tracks and maintains a log of every SVS management session. You can use this information to generate reports for troubleshooting and auditing purposes. You can store accounting logs locally or send them to remote AAA servers.

AAA Server Groups

Remote AAA server groups can provide failovers if one remote AAA server fails to respond, which means that if the first server in the group fails, the next server in the group is tried until a server responds. Multiple server groups can provide failovers for each other in this same way.

If all remote server groups fail, the local database is used for authentication.

Prerequisites for AAA

- At least one TACACS+ or RADIUS server is IP reachable
- The VSM is configured as an AAA server client.
- A shared secret key is configured on the VSM and the remote AAA server.

Guidelines and Limitations

The Cisco Nexus 1000V does not support usernames that have all numeric characters and does not create local usernames that have all numeric characters. If a username that has all numeric characters already exists on an AAA server and is entered during login, the Cisco Nexus 1000V does authenticate the user.

AAA Default Settings

Parameters	**Default**
Console authentication method	local
Default authentication method	local
Login authentication failure messages	Disabled

Configuring AAA

Configuring a Login Authentication Method

If authentication is to be done with TACACS+ server group(s), you must have already added the group(s).

Before you begin

Log in to the CLI in EXEC mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **aaa authentication login** {**console** | **default**} {**group** *group-list* [**none**] | **local** | **none**}	Configures the console or default login authentication method. the keywords and arguments are as follows: • **group**—Specifies that authentication is done by server group(s). • *group-list*—List of server group names separated by spaces. • **none**— Specifies no authentication. • **local**—Specifies that the local database is used for authentication. **Note** Local is the default and is used when no methods are configured or when all the configured methods fail to respond. • **none**—Specifies that authentication is done by username.
Step 3	Required: switch(config)# **exit**	Exits the global configuration mode and returns you to EXEC mode.
Step 4	(Optional) switch# **show aaa authentication**	Displays the configured login authentication method.
Step 5	(Optional) switch# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

This example shows how to configure a login authentication method:

```
switch# configure terminal
switch(config)# aaa authentication login console group tacgroup
switch(config)# exit
switch# show aaa authentication
         default: group tacgroup
         console: group tacgroup
switch# copy running-config startup-config
switch#
```

```
switch# configure terminal
switch(config)# aaa authentication login default group tacacs
switch(config)# aaa authentication login console group tacacs
```

Enabling Login Authentication Failure Messages

You can enable the login authentication failure message to display if the remote AAA servers do not respond.

The following is the Login Authentication Failure message:

```
Remote AAA servers unreachable; local authentication done.
Remote AAA servers unreachable; local authentication failed.
```

Before you begin

Log in to the CLI in EXEC mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **aaa authentication login error-enable**	Enables login authentication failure messages. The default is disabled.
Step 3	switch(config)# **exit**	Exits global configuration mode and returns you to EXEC mode.
Step 4	(Optional) switch# **show aaa authentication login error-enable**	Displays the login failure message configuration.
Step 5	(Optional) switch# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

This example shows how to enable login authentication failure messages:

```
switch# configure terminal
switch(config)# aaa authentication login error-enable
switch(config)# exit
switch# show aaa authentication login error-enable
enabled
```

Verifying the AAA Configuration

Use the following commands to verify the configuration:

Command	Purpose
show aaa authentication [**login** {**error-enable** | **mschap**}]	Displays AAA authentication information.
show aaa groups	Displays the AAA server group configuration.
show running-config aaa [**all**]	Displays the AAA configuration in the running configuration.
show startup-config aaa	Displays the AAA configuration in the startup configuration.

Example: show aaa authentication

```
switch# show aaa authentication login error-enable
disabled
switch#
```

Example: show running config aaa

```
switch# show running-config aaa all
version 4.0(1)
aaa authentication login default local
aaa accounting default local
no aaa authentication login error-enable
no aaa authentication login mschap enable
no radius-server directed-request
no snmp-server enable traps aaa server-state-change
no tacacs-server directed-request
switch#
```

Example: show startup-config aaa

```
switch# show startup-config aaa
version 4.0(1)
```

Configuration Examples for AAA

The following is an AAA configuration example:

```
aaa authentication login default group tacacs
aaa authentication login console group tacacs
```

Feature History for AAA

This table includes only the updates for those releases that have resulted in additions or changes to the feature.

Feature Name	Releases	Feature Information
AAA	4.0(4)SV1(1)	This feature was introduced.

Secure Login Enhancements

Starting with Cisco Nexus 1000V for VMware vSphere Release 5.2(1)SV3(4.1a), you can configure login parameters to enhance secure login to Cisco Nexus 1000V switches.

Configuring Login Parameters

Use this task to configure your Cisco Nexus 1000V device for login parameters that help detect suspected DoS attacks and slow down dictionary attacks.

All login parameters are disabled by default. You must enter the **login block-for** command, which enables default login functionality, before using any other login commands. After the **login block-for** command is enabled, the following rule is enforced:

- All login attempts made through Telnet or SSH are denied during the quiet period; that is, no ACLs are exempt from the login period until the **login quiet-mode access-class** command is entered.

Procedure

Step 1 **configure terminal**

Example:

```
Switch# configure terminal
```

Enters global configuration mode.

Step 2 **[no] login block-for** *seconds* **attempts** *tries* **within** *seconds*

Example:

```
Switch(config)# login block-for 100 attempts 2 within 100
```

Configures your Cisco NX-OS device for login parameters that help you detect DoS attack.

Note This command must be issued before any other login command can be used.

Step 3 **[no] login quiet-mode access-class** {*acl-name* | *acl-number*}

Example:

```
Switch(config)# login quiet-mode access-class myacl
```

(Optional) Although this command is optional, it is recommended that it be configured to specify an ACL that is to be applied to the device when the device switches to quiet mode. When the device is in quiet mode, all login requests are denied and the only available connection is through the console.

Step 4 **exit**

Example:

```
Switch(config)# exit
```

Exits to privileged EXEC mode.

Step 5 **show login failures**

Example:

```
Switch# show login failure
```

Displays login parameters.

- **failures** - Displays information related to failed login attempts.

Configuration Examples for Login Parameters

Setting Login Parameters Example

The following example shows how to configure your switch to enter a 100 second quiet period if 15 failed login attempts is exceeded within 100 seconds; all login requests are denied during the quiet period except hosts from the ACL "myacl."

```
Switch(config)# login block-for 100 attempts 15 within 100
Switch(config)# login quiet-mode access-class myacl
```

Showing Login Parameters Example

The following sample output from the **show login** command verifies that secure login parameters have been specified:

```
Switch# show login

No Quiet-Mode access list has been configured, default ACL will be applied.

Switch is enabled to watch for login Attacks.
If more than 2 login failures occur in 45 seconds or less,  logins will be disabled for 70
 seconds.

Switch presently in Normal-Mode.
Current Watch Window remaining time 10 seconds.
Present login failure count 0.
```

The following sample output from the **show login failures** command shows all failed login attempts on the switch:

```
Switch# show login failures

Information about last 20 login failures with the device.
--------------------------------------------------------------------------------
Username                                Line    Source              Appname
TimeStamp
--------------------------------------------------------------------------------
admin                                    pts/0   ws.cisco.com   login
        Wed Jun 10 04:56:16 2015
```

```
admin                                    pts/0   ws.cisco.com   login
        Wed Jun 10 04:56:19 2015
--------------------------------------------------------------------------------
```

The following sample output from the **show login failures** command verifies that no information is presently logged:

```
Switch# show login failures
*** No logged failed login attempts with the device.***
```

The following example shows how to clear the failed login attempts using the clear command:

```
Switch# clear login failures

This command is provided to clear statistics about failure details

Usage:

Nexus 1000v# sh login failures

Information about last 20 login failure's with the device.
------------------------------------------------------------------------------------------
Username                                Line    SourceIPAddr    Appname         TimeStamp
------------------------------------------------------------------------------------------
admin                                   ssh     10.78.184.85    login           Mon Feb 18
 07:38:16 2019
admin                                   ssh     10.78.184.85    login           Mon Feb 18
 07:38:18 2019
------------------------------------------------------------------------------------------
Nexus 1000v#

Nexus 1000v# clear login failures
Nexus 1000v#
Nexus 1000v# sh login failures
```

Guidelines and Limitations

Follow these usage guidelines and limitations while configuring Secure Login Enhancements:

- When the Quite mode is activated and login access is blocked for SSH and Telnet with ACLs, existing login sessions are also stopped. This behavior is consistent with the regular ACL behavior as applied to any interface handling traffic.
- Ensure that ACLs have last entries as “permit ip any any” in order to allow any other permitted protocol traffic to pass through the management interface, other than those handled by ACL entries. Default policy otherwise is to deny such additional IP traffic.
- PNSC access to VSM could get blocked due to ACL. To avoid this issue, configure secure login on VSM such that https access between VSM and PNSC is possible bidirectionally. Corresponding port to be opened for this purpose is 443.
- Secure login feature does not work together with ACLs directly configured with management interface (mgmt0) for VSM. Both are mutually exclusive configurations.