

Configuring TACACS+

This chapter describes how to configure the Terminal Access Controller Access Control System Plus (TACACS+) protocol on Cisco NX-OS devices.

This chapter includes the following sections:

- TACACS+, on page 1
- Prerequisites for TACACS+, on page 5
- Guidelines and limitations for TACACS+, on page 5
- Default settings for TACACS+, on page 6
- One-time password support, on page 7
- Configuring TACACS+, on page 7
- Monitor TACACS+ servers, on page 27
- Clear TACACS+ server statistics, on page 28
- TACACS+ configuration verification commands, on page 28
- Configuration examples for TACACS+, on page 29
- Configure TACACS+ over TLS, on page 30
- TACACS+ over TLS configuration verification, on page 31
- Where to go next, on page 31
- Additional references for TACACS+, on page 31

TACACS+

TACACS+ is a security protocol that provides centralized authentication, authorization, and accounting for users attempting Cisco NX-OS device access. TACACS+ services are maintained in a database on a TACACS+ daemon running, typically, on a UNIX or Windows NT workstation. You must have access to TACACS+ server and must configure it before the configured TACACS+ features on your NX-OS device are available.

TACACS+ provides for separate authentication, authorization, and accounting facilities. TACACS+ allows for a single access control server (the TACACS+ daemon) to provide each service—authentication, authorization, and accounting—independently. Each service can be tied into its own database to take advantage of other services available on that server or on the network, depending on the capabilities of the daemon.

The TACACS+ client/server protocol uses TCP (TCP port 49) for transport. NX-OS devices provide centralized authentication using the TACACS+ protocol.

Beginning with NX-OS release 10.4(3)F, SSH based authorization of X.509 certificates using TACACS+ server can be done using the **aaa authorization ssh-certificate default group** command on the Cisco Nexus

9000 Series platform switches. For configuration details, see Configure X.509 Certificate-Based SSH authorization using TACACS server, on page 24

TACACS+ Advantages

TACACS+ has the following advantages over RADIUS authentication:

- Provides independent AAA facilities. For example, the NX-OS device can authorize access without authenticating.
- Uses the TCP transport protocol to send data between the AAA client and server, making reliable transfers with a connection-oriented protocol.
- Obfuscates the entire protocol payload between the switch and the AAA server to ensure higher data confidentiality. The RADIUS protocol only obfuscates passwords.

TACACS+ Operation for User Login

When a user attempts a Password Authentication Protocol (PAP) login to a Cisco NX-OS device using TACACS+, the following actions occur:

Note TACACS+ allows an arbitrary conversation between the daemon and the user until the daemon receives enough information to authenticate the user. This action is usually done by prompting for a username and password combination, but may include prompts for other items, such as your mother's maiden name.

1. When the Cisco NX-OS device establishes a connection, it contacts the TACACS+ daemon to obtain the username and password.
2. The Cisco NX-OS device will eventually receive one of the following responses from the TACACS+ daemon:

   ACCEPT
   User authentication succeeds and service begins. If the Cisco NX-OS device requires user authorization, authorization begins.
   REJECT
   User authentication failed. The TACACS+ daemon either denies further access to the user or prompts the user to retry the login sequence.
   ERROR
   An error occurred at some time during authentication either at the daemon or in the network connection between the daemon and the Cisco NX-OS device. If the Cisco NX-OS device receives an ERROR response, the Cisco NX-OS device tries to use an alternative method for authenticating the user.

   After authentication, the user also undergoes an additional authorization phase if authorization has been enabled on the Cisco NX-OS device. Users must first successfully complete TACACS+ authentication before proceeding to TACACS+ authorization.
3. If TACACS+ authorization is required, the Cisco NX-OS device again contacts the TACACS+ daemon and it returns an ACCEPT or REJECT authorization response. An ACCEPT response contains attributes that are used to direct the EXEC or NETWORK session for that user and determines the services that the user can access.

   Services include the following:

- Telnet, remote login (rlogin), Point-to-Point Protocol (PPP), Serial Line Internet Protocol (SLIP), or EXEC services
- Connection parameters, including the host or client IP address (IPv4 or IPv6), access list, and user timeouts

Default TACACS+ server obfuscation type and secret key

You must configure the TACACS+ secret key to authenticate the switch to the TACACS+ server. A secret key is a secret text string shared between the Cisco NX-OS device and the TACACS+ server host. The length of the key is restricted to 63 characters and can include any printable ASCII characters (white spaces are not allowed). You can configure a global secret key for all TACACS+ server configurations on the Cisco NX-OS device to use.

You can override the global secret key assignment by explicitly using the **key** option when configuring an individual TACACS+ server.

Command authorization support for TACACS+ servers

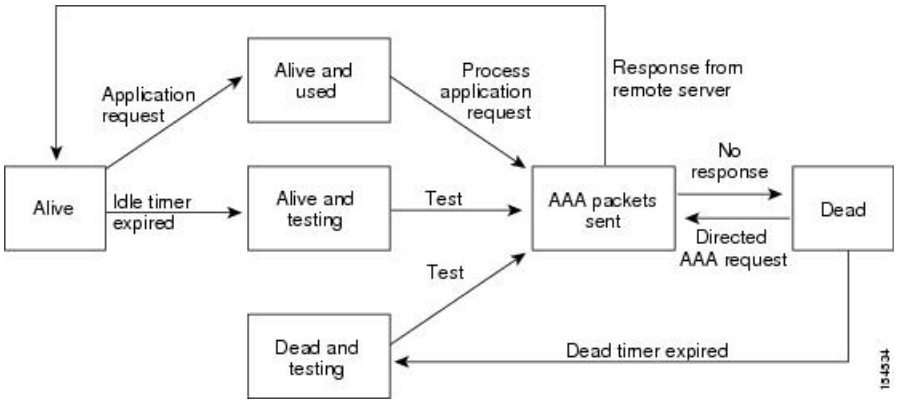
By default, command authorization is done against a local database in the Cisco NX-OS software when an authenticated user enters a command at the command-line interface (CLI). You can also verify authorized commands for authenticated users using TACACS+.

TACACS+ server monitoring

An unresponsive TACACS+ server can delay the processing of AAA requests. A Cisco NX-OS device can periodically monitor a TACACS+ server to check whether it is responding (or alive) to save time in processing AAA requests.

The Cisco NX-OS device marks unresponsive TACACS+ servers as dead and does not send AAA requests to any dead TACACS+ servers. A Cisco NX-OS device periodically monitors dead TACACS+ servers and brings them to the alive state once they are responding. This process verifies that a TACACS+ server is in a working state before real AAA requests are sent its way. Whenever a TACACS+ server changes to the dead or alive state, a Simple Network Management Protocol (SNMP) trap is generated and the Cisco NX-OS device displays an error message that a failure is taking place before it can impact performance.

Figure 1: TACACS+ server states



Note The monitoring interval for alive servers and dead servers are different and can be configured by the user. The TACACS+ server monitoring is performed by sending a test authentication request to the TACACS+ server.

Vendor-specific attributes for TACACS+

The draft standard from the Internet Engineering Task Force (IETF) describes how to communicate vendor-specific attributes (VSAs) between a network access server and a TACACS+ server. Attribute 26 is reserved for vendor-specific attributes. With VSAs, vendors can provide extended attributes intended for unique requirements and not for general use.

Cisco VSA format for TACACS+

The Cisco TACACS+ implementation supports one vendor-specific option using the format recommended in the IETF specification.

The Cisco vendor ID is 9, and the supported option is vendor type 1, which is named cisco-av-pair. The value is a string with the following format:

```
protocol : attribute separator value *
```

The protocol is a Cisco attribute for a particular type of authorization, the separator is = (equal sign) for mandatory attributes, and * (asterisk) indicates optional attributes.

When you use TACACS+ servers for authentication on a Cisco NX-OS device, the TACACS+ protocol directs the TACACS+ server to return user attributes, such as authorization information, along with authentication results. This authorization information is specified through VSAs.

The following VSA protocol options are supported by the Cisco NX-OS software:

- Shell

  Protocol used in access-accept packets to provide user profile information.

- Accounting

  Protocol used in accounting-request packets. If a value contains any white spaces, you should enclose the value within double quotation marks.

The Cisco NX-OS software supports the following attributes:

- roles

  Lists all the roles to which the user belongs. The value field is a string that lists the role names delimited by white space. For example, if the user belongs to roles network-operator and network-admin, the value field would be network-operator network-admin. This subattribute, which the TACACS+ server sends in the VSA portion of the Access-Accept frames, can only be used with the shell protocol value. The following examples show the roles attribute as supported by Cisco ACS:

  ```
  shell:roles=network-operator network-admin
  shell:roles*network-operator network-admin
  ```

Note When you specify a VSA as shell:roles* *network-operator network-admin*, this VSA is flagged as an optional attribute and other Cisco devices ignore this attribute.

- accountinginfo

  Stores accounting information in addition to the attributes covered by a standard TACACS+ accounting protocol. This attribute is sent only in the VSA portion of the Account-Request frames from the TACACS+ client on the switch. It can be used only with the accounting protocol data units (PDUs).

Prerequisites for TACACS+

TACACS+ has the following prerequisites:

- Obtain the IPv4 or IPv6 addresses or hostnames for the TACACS+ servers.
- Obtain the secret keys from the TACACS+ servers, if any.
- Ensure that the Cisco NX-OS device is configured as a TACACS+ client of the AAA servers.

Guidelines and limitations for TACACS+

Use this reference to review the guidelines and limitations for TACACS+.

TACACS+ has the following guidelines and limitations:

- Beginning with Cisco NX-OS Release 10.6(2)F, Cisco Nexus 9000 Series switches support routing TACACS+ (AAA) traffic via the Linux kernel network stack (kstack) in addition to the existing netstack path.
  - If the TACACS+ server IP is configured as a local interface address (ideally a loopback) in the selected VRF, the AAA requests are sent through kstack.
  - For external TACACS+ server IPs, the AAA requests are still sent through netstack.
  - TACACS+ servers configured with IPv4 or IPv6 addresses are supported through kstack. TACACS+ servers configured with hostnames are not supported through kstack. When hostnames are used, the system still relies on netstack for DNS resolution.
  - This feature does not support TACACS-over-TLS functionality over kstack.
  - Only TACACS+ supports kstack; RADIUS and LDAP continue to use netstack.
- Beginning with Cisco NX-OS Release 10.6(1)F, users can use TLS to configure TACACS+ server for a client.

  This feature does not support the AAA functionality when a shared key is enabled.
- TACACS+ authentication fails for usernames containing special characters on N9K-X9636C-R and N9K-X9636Q-R line cards and the N9K-C9508-FM-R fabric module.

- Beginning with Cisco NX-OS Release 10.3(1)F , TACACS+ is supported on the Cisco Nexus 9808 switches.
    - Beginning with Cisco NX-OS Release 10.4(1)F, TACACS+ is supported on Cisco Nexus X98900CD-A and X9836DM-A line cards with Cisco Nexus 9808 switches.
- Beginning with Cisco NX-OS Release 10.4(1)F, TACACS+ is supported on the Cisco Nexus 9804 switches,X98900CD-A and X9836DM-A line cards.
- Beginning with Cisco NX-OS release 10.4(3)F, SSH based authorization of X.509 certificates using TACACS+ server can be done using the aaa authorization ssh-certificate default group command on the Cisco Nexus 9000 Series platform switches.
- The Cisco NX-OS switches do not support custom username/password prompts. If custom prompts are provided to the switch, they will be ignored.

Configuration limitations

- You can configure a maximum of 64 TACACS+ servers on the Cisco NX-OS device.
- If a user account on the local Cisco NX-OS device shares its name with a remote user account on an AAA server, the Cisco NX-OS software applies the user roles from the local account to the remote user, not those configured on the AAA server.
- Cisco recommends that you configure the dead-time interval if more than six servers are configured in a group. If you must configure more than six servers, make sure to set the dead-time interval to a value greater than 0 and enable dead server monitoring by configuring the test username and test password.
- Command authorization on TACACS+ servers is available for console and vty sessions. "Do not use command authorization for console login without first testing it.

Guidelines and limitations for TACACS+ on Cisco N9300 smart switches

Beginning with Cisco Nexus Release 10.6(2)F, TACACS+ is supported on the Cisco N9324C-SE1U and Cisco N9348Y2C6D-SE1U Smart switches.

Guidelines and limitations for TACACS+ on Cisco Nexus 9164E-NS4-O switches

Beginning with Cisco Nexus Release 10.6(2n), TACACS+ is supported on the Cisco Nexus 9164E-NS4-O switches.

Default settings for TACACS+

Use this reference to review the default settings for TACACS+.

The default settings for TACACS+ are:

Default settings for TACACS+ information

Table 1: Default TACACS+ parameters settings

Parameters	Default
TACACS+	Disabled
Dead timer interval	0 minutes
Timeout interval	5 seconds
Idle timer interval	0 minutes
Periodic server monitoring username	test
Periodic server monitoring password	test
Privilege level support for TACACS+ authorization	Disabled

One-time password support

A one-time password (OTP) is a password that is valid for a single login session or a transaction. OTPs avoid multiple disadvantages that are associated with the static passwords. OTPs are not at risk to replay attacks. If an intruder manages to record an OTP that was already used to log into a service or to conduct an operation, it cannot be misused because it is no longer valid.

OTPs are applicable only to the RADIUS and TACACS+ protocol daemons. For a RADIUS protocol daemon, you must ensure that you disable the ASCII authentication mode. For a TACACS+ protocol daemon, you must enable the ASCII authentication mode. To enable the ASCII authentication mode, use the **aaa authentication login ascii-authentication** command.

Configuring TACACS+

This section describes how to configure TACACS+ on a Cisco NX-OS device.

Note If you are familiar with the Cisco IOS CLI, be aware that the Cisco NX-OS commands for this feature might differ from the Cisco IOS commands that you would use.

TACACS+ server configuration process

Enable centralized AAA on Cisco NX-OS using TACACS+, so authentication, command authorization, and accounting are handled by external servers with secure shared keys and optional server groups.

Procedure

Step 1 Enable TACACS+.

Step 2 Establish the TACACS+ server connections to the Cisco NX-OS device.

Step 3 Configure the secret keys for the TACACS+ servers.

Step 4 If needed, configure TACACS+ server groups with subsets of the TACACS+ servers for AAA authentication methods.

Step 5 (Optional) Configure the TCP port.

Step 6 (Optional) If needed, configure periodic TACACS+ server monitoring.

Step 7 (Optional) If TACACS+ distribution is enabled, commit the TACACS+ configuration to the fabric.

Related Topics

Enable TACACS+, on page 8

Enable TACACS+

By default, the TACACS+ feature is disabled on the Cisco NX-OS device. You must explicitly enable the TACACS+ feature to access the configuration and verification commands for authentication.

Procedure

Step 1 Use the **feature tacacs+** command to enable TACACS.

Example:

```
switch#configure terminal
switch(config)#feature tacacs+
```

Step 2 Use the **exit** command to exit configuration mode.

Example:

```
switch(config)#exit
switch#
```

Step 3 (Optional) Use the **copy running-config startup-config** command to copy the running configuration to the startup configuration.

Example:

```
switch#copy running-config startup-config
```

Configure TACACS+ server hosts

To access a remote TACACS+ server, you must configure the IP address or the hostname for the TACACS+ server on the Cisco NX-OS device. You can configure as many as 64 TACACS+ servers.

Note By default, when you configure a TACACS+ server IP address or hostname on the Cisco NX-OS device, the TACACS+ server is added to the default TACACS+ server group. You can add the TACACS+ server to another TACACS+ server group.

Before you begin

Enable TACACS+ to allow remote authentication.

Obtain the IPv4 addresses, IPv6 addresses, or hostnames for the remote TACACS+

Procedure

Step 1 Use the **tacacs-server host** {*ipv4-address* | *ipv6-address* | *hostname*} command to specify the IPv4 or IPv6 address or hostname for a TACACS+ server.

Example:

```
switch#configure terminal
switch(config)#tacacs-server host 10.10.2.2
```

Step 2 (Optional) Use the **show tacacs+** {**pending** | **pending-diff**} command to display the TACACS+ configuration pending for distribution.

Example:

```
switch#show tacacs+ pending
```

Step 3 (Optional) Use the **tacacs+ commit** to apply the TACACS+ configuration changes in the temporary database to the running configuration.

Example:

```
switch(config)#tacacs+ commit
```

Step 4 Use the **exit** command to exit configuration mode.

Example:

```
switch(config)#exit
switch#
```

Step 5 (Optional) Use the **show tacacs-server** command to display the TACACS+ server configuration.

Example:

```
switch#show tacacs-server
```

Step 6 (Optional) Use the **copy running-config startup-config** command to copy the running configuration to the startup configuration.

Example:

```
switch#copy running-config startup-config
```

Related Topics

Enable TACACS+, on page 8

Configure TACACS+ server groups, on page 12

Configure global TACACS+ keys

You can configure secret TACACS+ keys at the global level for all servers used by the Cisco NX-OS device. A secret key is a shared secret text string between the Cisco NX-OS device and the TACACS+ server hosts.

Before you begin

Enable TACACS+.

Obtain the secret key values for the remote TACACS+ servers.

Procedure

Step 1 Use the **tacacs-server key** [**0** | **6** | **7**] *key-value* command to specify a TACACS+ key for all TACACS+ server.

Example:

```
switch#configure terminal
switch(config)#tacacs-server key 0 QsEfThUkO
```

Example:

```
switch(config)#tacacs-server key 7 "fewhg"
```

You can specify that the *key-value* is in clear text format (**0**) , is type-6 encrypted (**6**), or is type-7 encrypted (**7**). The Cisco NX-OS software encrypts a clear text key before saving it to the running configuration. The default format is clear text. The maximum length is 63 characters.

By default, no secret key is configured.

Note
If you already configured a shared secret using the **generate type7_encrypted_secret** command, enter it in quotation marks, as shown in the second example. For more information, see Configure the shared secret for RADIUS or TACACS+ .

Step 2 Use the **exit** command to exit configuration mode.

Example:

```
switch(config)#exit
switch#
```

Step 3 (Optional) Use the **show tacacs-server** to display the TACACS+ server configuration.

Example:

```
switch#show tacacs-server
```

Note
The secret keys are saved in encrypted form in the running configuration. Use the **show running-config** command to display the encrypted secret keys.

Step 4 (Optional) Use the **copy running-config startup-config** command to copy the running configuration to startup configuration.

Example:

```
switch#copy running-config startup-config
```

Related Topics

Enable TACACS+, on page 8
AES password encryption and primary encryption keys

Configure a key for a specific TACACS+ server

You can configure secret keys for a TACACS+ server. A secret key is a shared secret text string between the Cisco NX-OS device and the TACACS+ server host.

Before you begin

Enable TACACS+.

Obtain the secret key values for the remote TACACS+ servers.

Procedure

Step 1 Use the **tacacs-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **key** [**0** | **6** | **7**] *key-value* command to specify a secret key for a specific TACACS+ server

Example:

```
switch#configure terminal
switch(config)#tacacs-server host 10.10.1.1 key 0 PlIjUhYg
switch(config)#exit
```

Example:

```
switch(config)#tacacs-server host 10.10.1.1 key 7 "fewhg"
```

You can specify that the *key-value* is in clear text format (**0**) , is type-6 encrypted (**6**), or is type-7 encrypted (**7**). The Cisco NX-OS software encrypts a clear text key before saving it to the running configuration. The default format is clear text. The maximum length is 63 characters.

This secret key is used instead of the global secret key.

Note
If you already configured a shared secret using the **generate type7_encrypted_secret** command, enter it in quotation marks, as shown in the second example. For more information, see Configure the shared secret for RADIUS or TACACS+ .

Step 2 (Optional) Use the **show tacacs-server** command to display the TACACS+ server configuration.

Example:

```
switch#show tacacs-server
```

Note
The secret keys are saved in encrypted form in the running configuration. Use the **show running-config** command to display the encrypted secret keys.

Step 3 (Optional) Use the **copy running-config startup-config** command to copy the running configuration to the startup configuration.

Example:

```
switch#copy running-config startup-config
```

Related Topics

AES password encryption and primary encryption keys

Configure TACACS+ server groups

You can specify one or more remote AAA servers to authenticate users using server groups. All members of a group must belong to the TACACS+ protocol. The servers are tried in the same order in which you configure them.

You can configure these server groups at any time but they only take effect when you apply them to an AAA service.

Before you begin

Enable TACACS+.

Procedure

Step 1 Use the **aaa group server tacacs+** *group-name* command to create a TACACS+ server group and enters the TACACS+ server group configuration mode for that group.

Example:

```
switch#configure terminal
switch(config)#aaa group server tacacs+ TacServer
switch(config-tacacs+)#
```

Step 2 Use the **server** {*ipv4-address* | *ipv6-address* | *hostname*} command to configure the TACACS+ server as a member of the TACACS+ server group.

Example:

```
switch(config-tacacs+)#server 10.10.2.2
switch(config-tacacs+)#exit
```

If the specified TACACS+ server is not found, configure it using the **tacacs-server host** command and retry this command.

Step 3 (Optional) Use the **show tacacs-server groups** command to display the TACACS+ server group configuration.

Example:

```
switch#show tacacs-server groups
```

Step 4 (Optional) Use the **copy running-config startup-config** command to copy the running configuration to the startup configuration.

Example:

```
switch#copy running-config startup-config
```

Related Topics

Enable TACACS+, on page 8
Remote AAA services
Configure TACACS+ server hosts, on page 8
Configure the TACACS+ Dead-Time interval, on page 20

Configure the global source interface for TACACS+ server groups

You can configure a global source interface for TACACS+ server groups to use when accessing TACACS+ servers. You can also configure a different source interface for a specific TACACS+ server group. By default, the Cisco NX-OS software uses any available interface.

Procedure

Step 1 Use the **ip tacacs source-interface** *interface* command to configure the global source interface for all TACACS+ server groups configured on the device.

Example:

```
switch#configure terminal
switch(config)#ip tacacs source-interface mgmt 0
switch(config)#exit
```

Step 2 (Optional) Use the **show tacacs-server** command to display the TACACS+ server configuration information.

Example:

```
switch#show tacacs-server
```

Step 3 (Optional) Use the **copy running-config startup config** command to copy the running configuration to the startup configuration.

Example:

```
switch#copy running-config startup-config
```

Related Topics

Enable TACACS+, on page 8
Configure TACACS+ server groups, on page 12

Allowing users to specify a TACACS+ server at login

You can configure the switch to allow the user to specify which TACACS+ server to send the authentication request by enabling the directed-request option. By default, a Cisco NX-OS device forwards an authentication request based on the default AAA authentication method. If you enable this option, the user can log in as *username* **@** *vrfname* **:** *hostname* , where *vrfname* is the VRF to use and *hostname* is the name of a configured TACACS+ server.

Note If you enable the directed-request option, the Cisco NX-OS device uses only the TACACS+ method for authentication and not the default local method.

Note User-specified logins are supported only for Telnet sessions.

Before you begin

Enable TACACS+.

Procedure

Step 1 Use the **tacacs-server directed-request** command for allowing users to specify a TACACS+ server to send the authentication request when logging in.

Example:

```
switch#configure terminal
switch(config)#tacacs-server directed-request
```

By default this command is disabled.

Step 2 (Optional) Use the **show tacacs+** {**pending** | **pending-diff**} command to display pending TACACS+ configuration.

Example:

```
switch#show tacacs+ pending
```

Step 3 (Optional) Use the **tacacs+ commit** command to apply the TACACS+ configuration changes in the temporary database to the running configuration.

Example:

```
switch(config)#tacacs+ commit
switch(config)#exit
```

Step 4 (Optional) Use the **show tacacs-server directed-request** command to display the TACACS+ directed request configuration.

Example:

```
switch#show tacacs-server directed-request
```

Step 5 (Optional) Use the **copy running-config startup-config** command to copy the running configuration to the startup configuration.

Example:

```
switch#copy running-config startup-config
```

Related Topics

Enable TACACS+, on page 8

Configure the timeout interval for a TACACS+ server

You can set a timeout interval that the Cisco NX-OS device waits for responses from a TACACS+ server before declaring a timeout failure. The timeout interval determines how long the Cisco NX-OS device waits for responses from a TACACS+ server before declaring a timeout failure.

Before you begin

Enable TACACS+.

Procedure

Step 1 Use the **tacacs-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **timeout** *seconds* command to specify the timeout interval for a specific server. The default is the global value.

Example:

```
switch#configure terminal
switch(config)#tacacs-server host server1 timeout 10
```

Note
The timeout interval value specified for a TACACS+ server overrides the global timeout interval value specified for all TACACS+ servers.

Step 2 (Optional) Use the **show tacacs+** {**pending** | **pending-diff**} command to display the TACACS+ configuration pending for distribution.

Example:

```
switch#show tacacs+ pending
```

Step 3 (Optional) Use the **tacacs+ commit** command to apply the TACACS+ configuration changes in the temporary database to the running configuration.

Example:

```
switch(config)#tacacs+ commit
switch(config)#exit
```

Step 4 (Optional) Use the **show tacacs-server** command to display the TACACS+ server configuration.

Example:

```
switch#show tacacs-server
```

Step 5 (Optional) Use the **copy running-config startup-config** command to copy the running configuration to the startup configuration.

Example:

```
switch#copy running-config startup-config
```

Related Topics

Enable TACACS+, on page 8

Configure TCP ports

You can configure another TCP port for the TACACS+ servers if there are conflicts with another application. By default, Cisco NX-OS devices use port 49 for all TACACS+ requests.

Before you begin

Enable TACACS+.

Procedure

Step 1 Use the **tacacs-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **port** *tcp-port* command to specify the TCP port to use for TACACS+ messages to the server. The default TCP port is 49. The range is from 1 to 65535.

Example:

```
switch#configure terminal
switch(config)#tacacs-server host 10.10.1.1 port 2
```

Step 2 (Optional) Use the **show tacacs+** {**pending** | **pending-diff**} command to display the TACACS+ configuration pending for distribution.

Example:

```
switch#show tacacs+ distribution pending
```

Step 3 (Optional) Use the **tacacs+ commit** command to apply the TACACS+ configuration changes in the temporary database to the running configuration.

Example:

```
switch(config)#tacacs+ commit
switch(config)#exit
```

Step 4 (Optional) Use the **show tacacs-server** command to display the TACACS+ server configuration.

Example:

```
switch#show tacacs-server
```

Step 5 (Optional) Use the **copy running-config startup-config** commad to copy the running configuration to the startup configuration.

Example:

```
switch#copy running-config startup-config
```

Related Topics

Enable TACACS+, on page 8

Configure global periodic TACACS+ server monitoring

You can monitor the availability of all TACACS+ servers without having to configure the test parameters for each server individually. Any servers for which test parameters are not configured are monitored using the global level parameters.

Note Test parameters that are configured for individual servers take precedence over global test parameters.

The global configuration parameters include the username and password to use for the servers and an idle timer. The idle timer specifies the interval in which a TACACS+ server receives no requests before the Cisco NX-OS device sends out a test packet. You can configure this option to test servers periodically, or you can run a one-time only test.

Note The test parameters are distributed across switches. If even one switch in the fabric is running an older release, the test parameters are not distributed to any switch in the fabric.

Note To protect network security, we recommend that you use a username that is not the same as an existing username in the TACACS+ database.

Note The default idle timer value is 0 minutes. When the idle time interval is 0 minutes, periodic TACACS+ server monitoring is not performed.

Note The username **test** on a Nexus switch cannot be disabled but can be changed if needed; to avoid the TACACS server being marked DEAD and ALIVE periodically, ensure the TACACS server always sends a response (Access-Accept or Access-Reject) to the **test** user request packet.

Before you begin

Enable TACACS+.

Procedure

Step 1 Use the **tacacs-server test** {**idle-time** *minutes* | **password** *password* [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time** *minutes*]]} command to specify parameters for global server monitoring. The default username is test, and the default password is test. The default value for the idle timer is 0 minutes, and the valid range is from 0 to 1440 minutes.

Example:

```
switch#configure terminal
switch(config)#tacacs-server test username user1 password Ur2Gd2BH idle-time 3
```

Note
For periodic TACACS+ server monitoring, the idle timer value must be greater than 0.

Step 2 Use the **tacacs-server dead-time** *minutes* command to specify the number of minutes before the Cisco NX-OS device checks a TACACS+ server that was previously unresponsive. The default value is 0 minutes, and the valid range is from 0 to 1440 minutes.

Example:

```
switch(config)#tacacs-server dead-time 5
switch(config)#exit
```

Step 3 (Optional) Use the **show tacacs-server** command to display the TACACS+ server configuration.

Example:

```
switch#show tacacs-server
```

Step 4 (Optional) Use the **copy running-config startup-config** command to copy the running configuration to the startup configuration.

Example:

```
switch#copy running-config startup-config
```

Related Topics

Configure periodic TACACS+ server monitoring on individual servers, on page 18

Configure periodic TACACS+ server monitoring on individual servers

You can monitor the availability of individual TACACS+ servers. The configuration parameters include the username and password to use for the server and an idle timer. The idle timer specifies the interval in which a TACACS+ server receives no requests before the Cisco NX-OS device sends out a test packet. You can configure this option to test servers periodically, or you can run a one-time only test.

Note Test parameters that are configured for individual servers take precedence over global test parameters.

Note To protect network security, we recommend that you use a username that is not the same as an existing username in the TACACS+ database.

Note The default idle timer value is 0 minutes. When the idle time interval is 0 minutes, periodic TACACS+ server monitoring is not performed.

Note The test parameters are distributed across switches. The test parameters are not distributed to any switch in the fabric.

Before you begin

Enable TACACS+.

Add one or more TACACS+ server hosts.

Procedure

Step 1 **configure terminal**

Example:

```
switch#configure terminal
switch(config)#
```

Enters global configuration mode.

Step 2 Use the **tacacs-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **test** {**idle-time** *minutes* | **password** *password* [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time** *minutes*]]} command to specify parameters for individual server monitoring. The default username is test, and the default password is test. The default value for the idle timer is 0 minutes, and the valid range is from 0 to 1440 minutes.

Example:

```
switch(config)#tacacs-server host 10.10.1.1 test username user1 password Ur2Gd2BH idle-time
 3
```

Note
For periodic TACACS+ server monitoring, the idle timer value must be greater than 0.

Step 3 Use the **tacacs-server dead-time** *minutes* command to specify the number of minutes before the Cisco NX-OS device checks a TACACS+ server that was previously unresponsive. The default value is 0 minutes, and the valid range is from 0 to 1440 minutes.

Example:

```
switch(config)#tacacs-server dead-time 5
switch(config)#exit
```

Step 4 (Optional) Use the **show tacacs-server** to display the TACACS+ server configuration.

Example:

```
switch#show tacacs-server
```

Step 5 (Optional) Use the **copy running-config startup-config** command to copy the running configuration to the startup configuration.

Example:

```
switch#copy running-config startup-config
```

Related Topics

Configure TACACS+ server hosts, on page 8
Configure global periodic TACACS+ server monitoring, on page 16

Configure the TACACS+ Dead-Time interval

You can configure the dead-time interval for all TACACS+ servers. The dead-time interval specifies the time that the Cisco NX-OS device waits, after declaring a TACACS+ server is dead, before sending out a test packet to determine if the server is now alive.

Note When the dead-timer interval is 0 minutes, TACACS+ servers are not marked as dead even if they are not responding. You can configure the dead-timer per group.

Before you begin

Enable TACACS+.

Procedure

Step 1 Use the **tacacs-server deadtime** *minutes* command to configure the global dead-time interval. The default value is 0 minutes. The range is from 1 to 1,440 minutes.

Example:

```
switch#configure terminal
switch(config)#tacacs-server deadtime 5
```

Step 2 (Optional) Use the **show tacacs+** {**pending** | **pending-diff**} command to display the pending TACACS+ configuration.

Example:

```
switch#show tacacs+ pending
```

Step 3 (Optional) Use the **tacacs+ commit** command to apply the TACACS+ configuration changes in the temporary database to the running configuration.

Example:

```
switch(config)#tacacs+ commit
switch(config)#exit
```

Step 4 (Optional) Use the **show tacacs-server** command to display the TACACS+ server configuration.

Example:

```
switch#show tacacs-server
```

Step 5 (Optional) Use the **copy running-config startup-config** command to copy the running configuration to the startup configuration.

Example:

```
switch#copy running-config startup-config
```

Configure ASCII authentication

You can enable ASCII authentication on the TACACS+ server.

Before you begin

Enable TACACS+.

Procedure

Step 1 Use the **aaa authentication login ascii-authentication** command to enable ASCII authentication. The default is disabled.

Example:

```
switch#configure terminal
switch(config)#aaa authentication login ascii-authentication
```

Step 2 (Optional) Use the **show tacacs+** {**pending** | **pending-diff**} command to display the pending TACACS+ configuration.

Example:

```
switch#show tacacs+ pending
```

Step 3 (Optional) Use the **tacacs+ commit** command to apply the TACACS+ configuration changes in the temporary database to the running configuration.

Example:

```
switch(config)#tacacs+ commit
switch(config)#exit
```

Step 4 (Optional) Use the **show tacacs-server** command to display the TACACS+ server configuration.

Example:

```
switch#show tacacs-server
```

Step 5 (Optional) Use the **copy running-config startup-config** command to copy the running configuration to the startup configuration.

Example:

```
switch#copy running-config startup-config
```

Configure command authorization on TACACS+ servers

You can configure authorization for commands on TACACS+ servers.



Caution Command authorization disables user role-based authorization control (RBAC), including the default roles.

Note If you use a console to log in to the server, command authorization is disabled. Authorization is available for both non-console and console sessions. By default, command authorization is disabled for console sessions even if it is configured for default (non-console) sessions. You must explicitly configure a AAA group for the console to enable command authorization for console sessions.

Note By default, context-sensitive help and command tab completion show only the commands supported for a user as defined by the assigned roles. When you enable command authorization, the Cisco NX-OS software displays all commands in the context sensitive help and in tab completion, regardless of the role assigned to the user.

Before you begin

Enable TACACS+.

Procedure

Step 1 Use the **aaa authorization** {**commands** | **config-commands**} {**console** | **default**} {**group** *group-list* [**local**] | **local**} command to configure the command authorization method for specific roles on a TACACS+ server.

Example:

```
switch#configure terminal
switch(config)#aaa authorization commands
default group TacGroup
Per command authorization will disable RBAC for all
users. Proceed (y/n)?
```

The **commands** keyword configures authorization sources for all EXEC commands, and the **config-commands** keyword configures authorization sources for all configuration commands.

The **console** keyword configures command authorization for a console session, and the **default** keyword configures command authorization for a non-console session.

The *group-list* argument consists of a space-delimited list of TACACS+ server group names. Servers belonging to this group are contacted for command authorization. The **local** method uses the local role-based database for authorization.

The **local** method is used only if all the configured server groups fail to respond and you have configured **local** as the fallback method. The default method is **local** .

If you have not configured a fallback method after the TACACS+ server group method, authorization fails if all server groups fail to respond.

If you press **Enter** at the confirmation prompt, the default action is *n* .

Step 2 (Optional) Use the **show tacacs+** {**pending** | **pending-diff**} command to display the pending TACACS+ configuration.

Example:

```
switch#show tacacs+ pending
```

Step 3 (Optional) Use the **tacacs+ commit** command to apply the TACACS+ configuration changes in the temporary database to the running configuration.

Example:

```
switch(config)#tacacs+ commit
switch(config)#exit
```

Step 4 (Optional) Use the **show aaa authorization** [**all**] command to display the AAA authorization configuration. The **all** keyword displays the default values.

Example:

```
switch#show aaa authorization
```

Step 5 (Optional) Use the **copy running-config startup-config** command to copy the running configuration to the startup configuration.

Example:

```
switch#copy running-config startup-config
```

Related Topics

Enable TACACS+, on page 8
Testing command authorization on TACACS+ servers, on page 23

Testing command authorization on TACACS+ servers

You can test the command authorization for a user on the TACACS+ servers.

Note You must send correct commands for authorization or else the results may not be reliable.

Note The **test** command uses the default (non-console) method for authorization, not the console method.

Before you begin

Enable TACACS+.

Ensure that you have configured command authorization for the TACACS+ servers.

Procedure

Use the **test aaa authorization command-type** {**commands** | **config-commands**} **user** *username* **command** *command-string* command to test a user's authorization for a command on the TACACS+ servers.

Example:

```
switch#test aaa authorization command-type commands
user TestUser command reload
```

The **commands** keyword specifies only EXEC commands and the **config-commands** keyword specifies only configuration commands.

Note
Put double quotes (") before and after the *command-string* argument if it contains spaces.

Related Topics

Enable TACACS+, on page 8
Configure command authorization on TACACS+ servers, on page 21
Configuring User Accounts and RBAC

Enable and disable command authorization verification

You can enable and disable command authorization verification on the command-line interface (CLI) for the default user session or for another username.

Note The commands do not execute when you enable authorization verification.

Procedure

Step 1 Use the **terminal verify-only** [**username** *username*] command to enable command authorization verification. After you enter this command, the Cisco NX-OS software indicates whether the commands you enter are authorized or not.

Example:

```
switch#terminal verify-only
```

Step 2 Use the **terminal no verify-only** [**username** *username*] command to disable command authorization verification.

Example:

```
switch#terminal no verify-only
```

Configure X.509 Certificate-Based SSH authorization using TACACS server

Beginning with Cisco NX-OS release 10.4(3)F, you can configure SSH-based authorization of x509v3-certificates using a TACAC+ server on the Cisco Nexus switches.

To configure X.509 certificate-based SSH-authorization using a TACAC+ server, follow these steps:

Procedure

Step 1 Use the **aaa authorization ssh-certificate default group** *tacacs-group-name* command to configure the default AAA authorization method for the TACAC+ servers.

Example:

```
switch#configure terminal
switch(config)#aaa authorization ssh-certificate default group tac
switch(config)#exit
switch#
```

The **ssh-certificate** keyword configures TACACS or local authorization with certificate authentication. The default authorization is local authorization, which is the list of authorized commands for the user's assigned role.

Note

- Ensure that the *tacacs-group-name* is configured under the TACACS-server configuration using the **aaa group server tacacs+** *tacacs-group-name* command.
- To support SSH certificate-based authentication, configure a crypto trustpoint and install the root CA. For more details, see the Configuring PKI section.

Step 2 (Optional) Use the **show aaa authorization** [**all**] command to display the AAA authorization configuration. The **all** keyword displays the default values.

Example:

```
switch#show aaa authorization
```

Step 3 (Optional) Use the **copy running-config startup-config** command to copy the running configuration to the startup configuration.

Example:

```
switch#copy running-config startup-config
```

Permitting or denying commands for users of privilege roles

As a network administrator, you can modify the privilege roles to permit users to execute specific commands or to prevent users from running those commands.

You must follow these guidelines when changing the rules of privilege roles:

- You cannot modify the priv-14 and priv-15 roles.
- You can add deny rules only to the priv-0 role.
- These commands are always permitted for the priv-0 role: **configure** , **copy** , **dir** , **enable** , **ping** , **show** , **ssh** , **telnet** , **terminal** , **traceroute** , **end** , and **exit** .

Procedure

Step 1 Use the [**no**] **role name priv-** *n* command to enable or disable a privilege role and enters role configuration mode. The *n* argument specifies the privilege level and is a number between 0 and 13.

Example:

```
switch#configure terminal
switch(config)#role name priv-5
switch(config-role)#
```

Step 2 Use the **rule** *number* {**deny** | **permit**} **command** *command-string* command to configure a command rule for users of privilege roles. These rules permit or deny users to execute specific commands. You can configure up to 256 rules for each role. The rule number determines the order in which the rules are applied. Rules are applied in descending order. For example, if a role has three rules, rule 3 is applied before rule 2, which is applied before rule 1.

Example:

```
switch(config-role)# rule 2 permit command pwd
switch(config-role)#exit
```

The *command-string* argument can contain spaces.

Note
Repeat this command for as many rules as needed.

Step 3 (Optional) Use the **copy running-config startup-config** command to copy the running configuration to the startup configuration.

Example:

```
switch#copy running-config startup-config
```

Related Topics

Configure user roles and rules

Manually monitoring TACACS+ servers or groups

You can manually issue a test message to a TACACS+ server or to a server group.

Before you begin

Enable TACACS+.

Procedure

Step 1 Use the **test aaa server tacacs+** {*ipv4-address* | *ipv6-address* | *hostname*} [**vrf** *vrf-name*] *username password* command to send a test message to a TACACS+ server to confirm availability.

Example:

```
switch#test aaa server tacacs+ 10.10.1.1 user1 Ur2Gd2BH
```

Step 2 Use the **test aaa group** *group-name username password* command to send a test message to a TACACS+ server group to confirm availability.

Example:

```
switch#test aaa group TacGroup user2 As3He3CI
```

Related Topics

Configure TACACS+ server hosts, on page 8
Configure TACACS+ server groups, on page 12

Disable TACACS+

You can disable TACACS+.

Caution When you disable TACACS+, all related configurations are automatically discarded.

Procedure

Step 1 Use the **no feature tacacs+** command to disable TACACS+.

Example:

```
switch#configure terminal
switch(config)#no feature tacacs+
switch(config)#exit
```

Step 2 (Optional) Use the **copy running-config startup-config** command to copy the running configuration to the startup configuration.

Example:

```
switch#copy running-config startup-config
```

Monitor TACACS+ servers

You can monitor the statistics that the Cisco NX-OS device maintains for TACACS+ server activity.

Before you begin

Configure TACACS+ servers on the Cisco NX-OS device.

Procedure

Use the **show tacacs-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*} command to display the TACACS+ statistics.

Example:

```
switch#show tacacs-server statistics 10.10.1.1
```

Related Topics

Configure TACACS+ server hosts, on page 8
Clear TACACS+ server statistics, on page 28

Clear TACACS+ server statistics

You can display the statistics that the Cisco NX-OS device maintains for TACACS+ server activity.

Before you begin

Configure TACACS+ servers on the Cisco NX-OS device.

Procedure

Step 1 (Optional) Use the **show tacacs-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*} command to display the TACACS+ server statistics on the Cisco NX-OS device.

Example:

```
switch#show tacacs-server statistics 10.10.1.1
```

Step 2 Use the **clear tacacs-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*} command to clear the TACACS+ server statistics.

Example:

```
switch#clear tacacs-server statistics 10.10.1.1
```

Related Topics

Configure TACACS+ server hosts, on page 8

TACACS+ configuration verification commands

Use this reference to verify the TACACS+ configuration.

To display the TACACS+ configuration, perform one of the following tasks:

TACACS+ configuration verification commands information

Table 2: TACACS+ configuration verification commands

Command	Purpose
show tacacs+ {**status** | **pending** | **pending-diff**}	Displays the TACACS+ Cisco Fabric Services distribution status and other details.
show running-config tacacs [**all**]	Displays the TACACS+ configuration in the running configuration.
show startup-config tacacs	Displays the TACACS+ configuration in the startup configuration.
show tacacs-server [*host-name* | *ipv4-address* | *ipv6-address*] [**directed-request** | **groups** | **sorted** | **statistics**]	Displays all configured TACACS+ server parameters.

Configuration examples for TACACS+

The following example shows how to configure a TACACS+ server host and server group:

```
feature tacacs+
tacacs-server key 7 "ToIkLhPpG"
tacacs-server host 10.10.2.2 key 7 "ShMoMhTl"
aaa group server tacacs+ TacServer
    server 10.10.2.2
```

The following example shows how to configure and use command authorization verification:

```
switch#terminal verify-only
switch#show interface ethernet 7/2 brief
%Success
switch#terminal no verify-only
switch#show interface ethernet 7/2 brief
--------------------------------------------------------------------------------
Ethernet      VLAN   Type Mode   Status  Reason                   Speed     Port
Interface                                                                  Ch #
--------------------------------------------------------------------------------
Eth7/2        1      eth  access down    SFP not inserted           auto(D) --
```

The following example shows how to permit all users with roles priv-5 and above to execute the **pwd** command:

```
switch#configure terminal
switch(config)#role name priv-5
switch(config-role)#rule 1 permit command pwd
```

The following example shows how to deny the **show running-config** command to all users with roles below priv-5. First, you must remove the permission to execute this command from the priv-0 role; then you must permit the command at role priv-5 so that users with roles priv-5 and above have permission to run the command.

```
switch#configure terminal
switch(config)#role name priv-0
switch(config-role)#rule 2 deny command show running-config
switch(config-role)#exit
```

```
switch(config)#role name priv-5
switch(config-role)#rule 3 permit command show running-config
switch(config-role)#exit
```

Configure TACACS+ over TLS

Beginning with Cisco NX-OS Release 10.6(1)F, a TACACS+ client can initiate a TCP connection to the TLS-enabled TACACS+ server on a predesignated port. Once the TCP connection is established, the client starts the TLS negotiation before sending any TACACS+ data. Peers use TLS certificates to authenticate each other. Each peer must validate the certificate path of the other peer, including revocation checks. If peer certificate validation succeeds, then the connection is allowed.

After the TLS connection is set up, all TACACS+ data is exchanged according to the switch's TACACS+ configuration and transmitted as TLS encrypted application data. The TLS connection stays active until the TACACS+ connection is closed. If the closure results from a TLS error, the TACACS+ session becomes invalid.

Procedure

Step 1 Use the **feature tacacs+** command to enable TACACS+

Example:

```
switch#configure terminal
switch(config)#feature tacacs+
```

Step 2 Use the **tacacs-server secure tls** command to globally enable TLS1.3 for connections to all TACACS+ servers configured with the tls parameter.

Example:

```
switch(config)#tacacs-server secure tls
```

Step 3 Use the **tacacs-server host** *tacacs-server-name* **port** *port-number* command to define a destination TACACS+ server and TCP port number to connect to. Ensure that the TACACS+ server is configured to listen on the same port.

Example:

```
switch(config)#tacacs-server host 10.0.0.1 port 449
```

For TSL connection, use the port configured for TACAC TLS in the AAA server.

Step 4 Use the **tacacs-server host** *tacacs-server-name* **tls client-trustpoint** *trustpoint-name* command to specify the trust point containing the client certificates to be used when authenticating with the specified TACACS+ server.

Example:

```
switch(config)#tacacs-server host 10.0.0.1 tls client-trustpoint trusttplus
```

Step 5 Use the **aaa group server tacacs+** *server-pool-name* command to define a pool of AAA TACACS+ servers.

Example:

```
switch(config)#aaa group server tacacs+ tac1
```

Step 6 Use the **server** *tacacs-server-name* command to add the defined server to the AAA server pool.

Example:

```
switch(config-tacacs+)#server 10.0.0.1
```

Step 7 Use the **use-vrf** *vrf-name* command to configure VRF member.

Example:

```
switch(config-tacacs+)#use-vrf management
```

TACACS+ over TLS configuration verification

Use this reference to verify the TACACS+ over TLS configuration.

To verify the TACACS+ over TLS feature is enabled use the following command:

```
!Command: show running-config tacacs+
                !Running configuration last done at: Wed Apr 23 00:21:38 2025
                !Time: Wed Apr 23 00:21:43 2025
                version 10.6(1) Bios:version 05.52
                feature tacacs+
                tacacs-server secure tls
                tacacs-server host 10.0.0.1 port 449
                tacacs-server host 10.0.0.1 tls client-trustpoint trusttplus
                aaa group server tacacs+ tac1
                server 10.0.0.1
                use-vrf management
```

Where to go next

You can now configure AAA authentication methods to include the server groups.

Additional references for TACACS+

Use this reference to find additional references for TACACS+.

This section includes additional information related to implementing TACACS+.

Related Documents

Table 3: Related documents

Related Topic	Document Title
Cisco NX-OS licensing	*Cisco NX-OS Licensing Guide*
VRF configuration	*Cisco NX-OS 9000 Series NX-OS Unicast Routing Configuration Guide*

Standards

Table 4: Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

Table 5: MIBs

MIBs	MIBs Link
MIBs related to TACACS+	To locate and download supported MIBs, go to the following URL: https://example.com/cisco-mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html