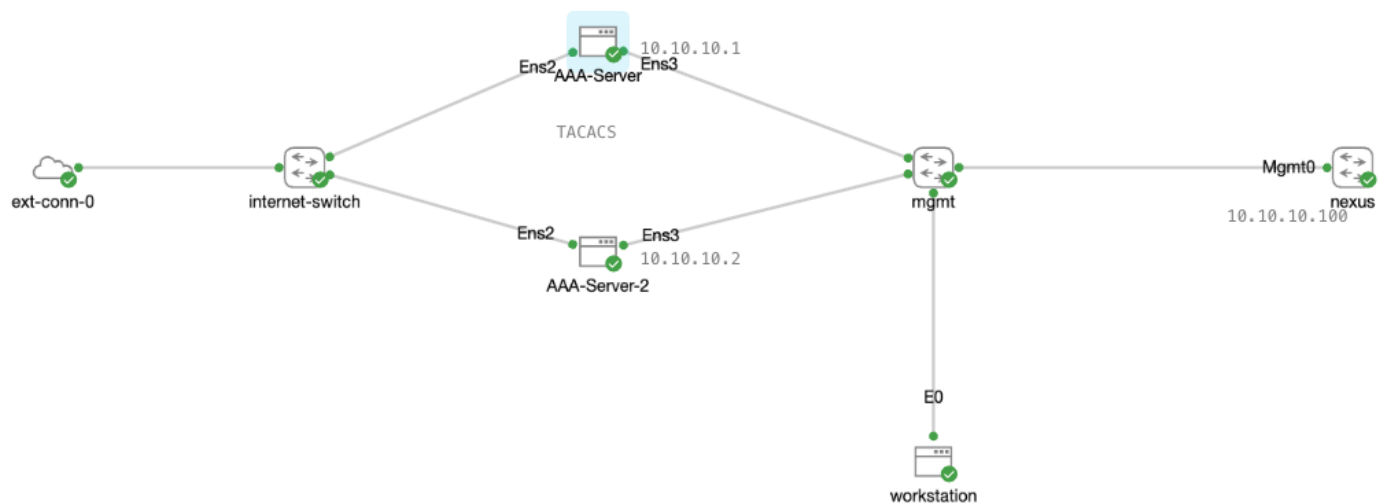


# AAA

AAA remains a key component when it comes to network infrastructure security. The AAA framework enables a verified user via credentials (authentication) to access a network device, perform actions based on their privileges within the system (authorization), and log their actions (accounting) for auditing, compliance, billing, session logging etc.

This lab configures a TACACS+ AAA server on a Linux box using a `tac_plus` daemon. User credentials and their privileges are configured in the `tac_plus.conf` file located in the `/etc/tacacs/` directory. A dedicated management workstation is used to access a Cisco Nexus switch using the credentials that have been configured on the TACACS+ server.

## Lab Topology



## Setting up TACACS+ functionality on Linux

The following packages are required:

```
wget
make
gcc
flex
bison
libwrap0-dev
python3.10-venv
```

Update package manager

```
sudo apt-get update
```

Install the respective packages:

```
sudo apt-get install <package-name>
```

### Configure the TACACS+ Daemon:

Create and open the `tac_plus.conf`

```
sudo nano /etc/tacacs+/tac_plus.conf
```

Setup the the required AAA commands according to your needs. In this lab the users and roles are configured specifically for the Cisco Nexus device.

```
key = tacacsLab123

group = nexus_admin {
    default service = permit
    service = exec {
        priv-lvl = 15
        shell:roles="\network-admin vdc-admin\""
    }
}

group = nexus_operator {
    default service = permit
    service = exec {
        priv-lvl = 1
        shell:roles="\network-operator vdc-operator\""
    }
}

user = lan-admin {
    member = nexus_admin
    login = cleartext dclan123
}

user = lan-operator {
    member = nexus_operator
    login = cleartext dclan123
}
```

The key sets the shared secret that will be used to encrypt communications between the TACACS+ server and clients (network devices).

The groups are created to define administrative access for users that will require access to the network device. The **nexus\_admin** group will be associated to users that require complete read and write access to the entire NXOS system. The **nexus\_operator** in turn is associated to users that require complete read-access only to the NXOS device.

A systemd service for managing the `tac_plus` daemon is required. Create it as follows:

```
#path: /etc/systemd/system/tac_plus.service
```

```
[Unit]
Description=tac_plus Service
After=network.target
[Service]
Type=simple
ExecStart=/tacacs/sbin/tac_plus -G -C /etc/tacacs/tac_plus.conf -d 8 -d 16 -l
/var/log/tac_plus.log
[Install]
WantedBy=multi-user.target
```

By creating this systemd service, administrators can easily manage the `tac_plus` daemon through standard systemd commands such as `start`, `stop`, and `enable`.

Install the ‘`tac_plus`’ TACACS+ server on the Linux system

Download the “`tac_plus`” source code to the `/opt/` directory:

```
wget https://shrubbery.net/pub/tac_plus/tacacs-F4.0.4.28.tar.gz -O
/opt/tacacs-F4.0.4.28.tar.gz
```

Extract the contents of the tarball in the directory where the source code was downloaded.

```
cd /opt && tar -xzf tacacs-F4.0.4.28.tar.gz
```

Compile and install the “`tac_plus`” source code:

```
cd /opt/tacacs-F4.0.4.28 && ./configure --prefix=/tacacs && make && make
install
```

The final step is to enable and start the service:

```
systemctl enable tac_plus
systemctl start tac_plus
```

Monitor the logs generated by the `tac_plus` service in real time on the Linux system.

```
journalctl -fu tac_plus
```

More information can be found here:

<https://github.com/CiscoDevNet/cml-community/tree/master/lab-topologies/aaa-tacacs-exploration>

<https://blogs.cisco.com/learning/exploring-aaa-tacacs-configuration-with-cml>

**Credit:** Hank Preston

# Configure Nexus device as a TACACS+ Client

The AAA configurations for the Nexus device are as follows:

```
feature tacacs
!
tacacs-server key 7 "wwgfusGft123"
!
tacacs-server host 10.10.10.1
tacacs-server host 10.10.10.2
!
aaa group server tacacs+ TACACS
    server 10.10.10.1
    server 10.10.10.2
    use-vrf management
    source-interface mgmt0
!
interface mgmt0
    vrf member management
    ip address 10.10.10.100/24
```

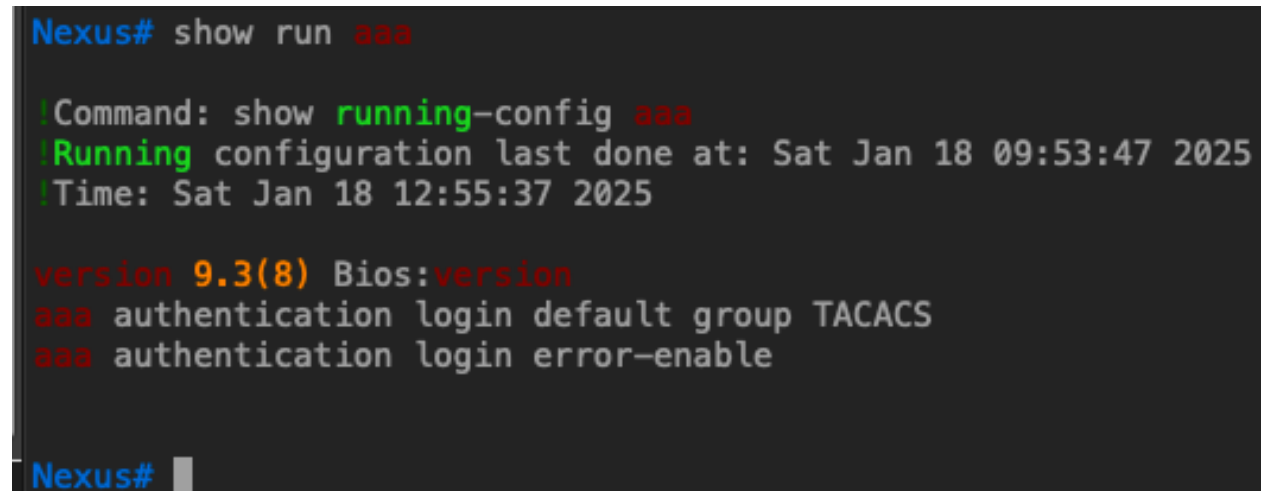
For an extensive list of AAA configurations check the NXOS Security Config Guide:

<https://www.cisco.com/c/en/us/td/docs/dcn/nx-os/nexus9000/105x/configuration/security/cisco-nexus-9000-series-nx-os-security-configuration-guide-release-105x/m-configuring-tacacs.html>

## Verifications and Tests

1. Verify that the correct AAA group is used for authentication.

show run aaa



```
Nexus# show run aaa

!Command: show running-config aaa
!Running configuration last done at: Sat Jan 18 09:53:47 2025
!Time: Sat Jan 18 12:55:37 2025

version 9.3(8) Bios:version
aaa authentication login default group TACACS
aaa authentication login error-enable

Nexus#
```

show aaa authentication

```
Nexus# show aaa authentication
      default: group TACACS
      console: group TACACS
Nexus#
Nexus#
```

2. Check for the VRF association with the AAA group.

show tacacs-server groups

```
Nexus# show tacacs-server groups
total number of groups:1

following TACACS+ server groups are configured:
  group TACACS:
    server 10.10.10.1 on port 49
    server 10.10.10.2 on port 49
    deadtime is 0
    vrf is management
    Source interface mgmt0
Nexus#
```

3. Verify ICMP reachability between the Nexus device and the TACACS+ server.

ping 10.10.10.1 vrf management

```
Nexus# ping 10.10.10.1 vrf management source 10.10.10.100
PING 10.10.10.1 (10.10.10.1) from 10.10.10.100: 56 data bytes
64 bytes from 10.10.10.1: icmp_seq=0 ttl=63 time=2.886 ms
64 bytes from 10.10.10.1: icmp_seq=1 ttl=63 time=1.904 ms
64 bytes from 10.10.10.1: icmp_seq=2 ttl=63 time=4.191 ms
64 bytes from 10.10.10.1: icmp_seq=3 ttl=63 time=2.401 ms
64 bytes from 10.10.10.1: icmp_seq=4 ttl=63 time=2.818 ms

--- 10.10.10.1 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 1.904/2.839/4.191 ms
Nexus#
```

4. Verify authentication of a user against a TACACS+ server group "TACACS"

test aaa group <group-name> <username> <password>

The possible returns of the test aaa command are as follows:

- Authentication successful
- User has failed authentication
- Error authenticating to server

a. Verify authentication using the correct credentials.

```
Nexus# test aaa group TACACS lan-admin dclan123
user has been authenticated
Nexus#
```

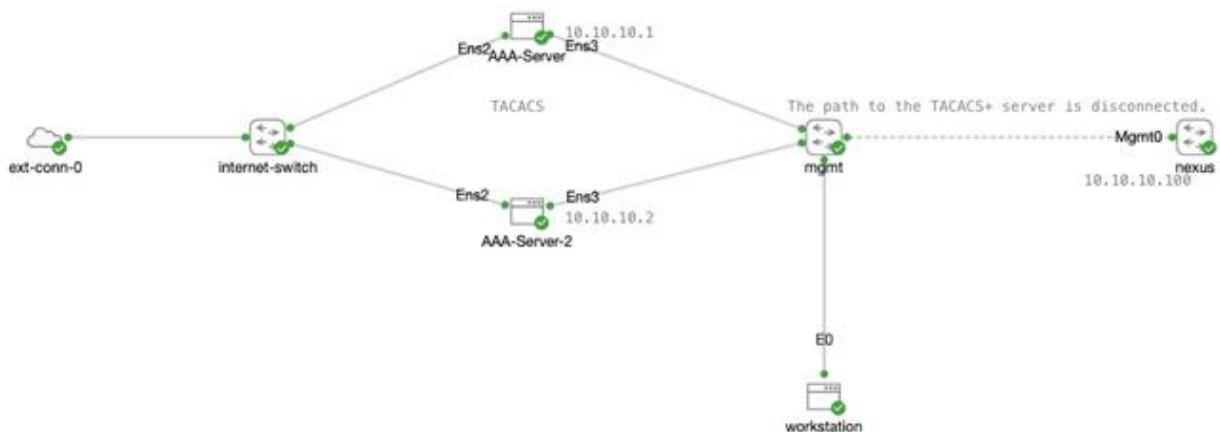
b. Verify authentication using incorrect credentials.

When you get the “user has failed authentication” error:

```
Nexus# test aaa group TACACS lan-user sgjdkf
user has failed authentication
Nexus#
```

This means **the server is available, and the AAA group is configured correctly but the credentials don't match.**

c. Disconnect reachability to the server and verify authentication:



```
Nexus# ping 10.10.10.1 vrf management source 10.10.10.100
PING 10.10.10.1 (10.10.10.1) from 10.10.10.100: 56 data bytes
Request 0 timed out
Request 1 timed out
Request 2 timed out
Request 3 timed out
Request 4 timed out
```

When there is no reachability to all the servers in the configured group, you will get the “**error authenticating to the server**”.

```
Nexus# test aaa group TACACS lan-admin dclan123
error authenticating to server, status=7
Nexus#
```

If you get this error when trying to verify authentication, fixing the server's reachability issues is crucial.

5. SSH login from the management workstation to the Nexus device using the credentials configured on the remote AAA server.

```
workstation:~$
workstation:~$ ssh lan-admin@10.10.10.100
User Access Verification
(lan-admin@10.10.10.100) Password:

Cisco NX-OS Software
Copyright (c) 2002-2021, Cisco Systems, Inc. All rights reserved.
```

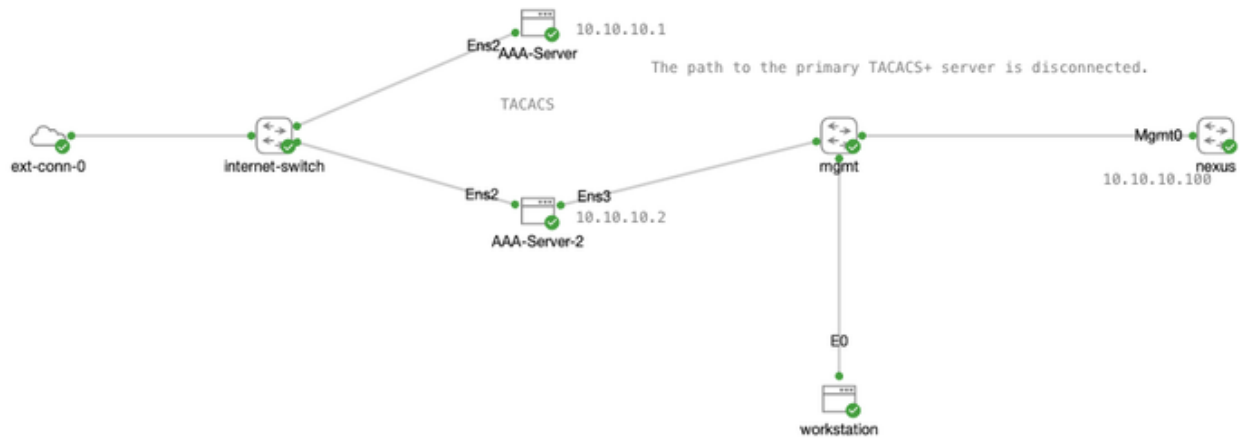
Login to the device is successful

logs from the AAA Server:

```
nas-server tac_plus[34456]: connect from 10.10.10.100 [10.10.10.100]
nas-server tac_plus[34456]: pap-login query for 'lan-admin' pass 0 from 10.10.10.100 accepted
nas-server tac_plus[34457]: connect from 10.10.10.100 [10.10.10.100]
nas-server tac_plus[34457]: Start authorization request
nas-server tac_plus[34457]: do_author: user='lan-admin'
nas-server tac_plus[34457]: user 'lan-admin' found
nas-server tac_plus[34457]: exec authorization request for lan-admin
nas-server tac_plus[34457]: exec is explicitly permitted by line 5
nas-server tac_plus[34457]: nas:service=shell (passed thru)
nas-server tac_plus[34457]: nas:cmd= (passed thru)
nas-server tac_plus[34457]: nas:cisco-av-pair svr:absent/deny -> delete cisco-av-pair* (i)
nas-server tac_plus[34457]: nas:shell:roles svr:shell:roles="network-admin vdc-admin" -> replace with shell:roles="network-admin vdc-admin" (f)
nas-server tac_plus[34457]: nas:absent, server:priv-lvl=15 -> add priv-lvl=15 (k)
nas-server tac_plus[34457]: replaced 2 args
nas-server tac_plus[34457]: authorization query for 'lan-admin' 0 from 10.10.10.100 accepted
```

6. Test for server failure within a TACACS group

Having multiple TACACS+ servers in the same group is crucial for ensuring high availability and fault tolerance. To test redundancy, the link to the primary TACACS+ server is disconnected.



There is no reachability towards the 10.10.10.1 server:

```
Nexus# ping 10.10.10.1 vrf management source 10.10.10.100
PING 10.10.10.1 (10.10.10.1) from 10.10.10.100: 56 data bytes
Request 0 timed out
Request 1 timed out
Request 2 timed out
Request 3 timed out
Request 4 timed out

--- 10.10.10.1 ping statistics ---
5 packets transmitted, 0 packets received, 100.00% packet loss
Nexus#
```

There is reachability towards the 10.10.10.2 server:

```
Nexus# ping 10.10.10.2 vrf management source 10.10.10.100
PING 10.10.10.2 (10.10.10.2) from 10.10.10.100: 56 data bytes
64 bytes from 10.10.10.2: icmp_seq=0 ttl=63 time=3.352 ms
64 bytes from 10.10.10.2: icmp_seq=1 ttl=63 time=3.351 ms
64 bytes from 10.10.10.2: icmp_seq=2 ttl=63 time=5.557 ms
64 bytes from 10.10.10.2: icmp_seq=3 ttl=63 time=3.266 ms
64 bytes from 10.10.10.2: icmp_seq=4 ttl=63 time=2.907 ms

--- 10.10.10.2 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 2.907/3.686/5.557 ms
Nexus#
```

From the workstation, try to log in the Nexus device:



If the first remote server (10.10.10.1) in the group fails to respond, the next remote server (10.10.10.2) in the group is tried until one of the servers sends a response

```
workstation:~$ ssh lan-admin@10.10.10.100
User Access Verification
(lan-admin@10.10.10.100) Password:
Cisco NX-OS Software
```

The authentication using the second server in the group succeeds.

## Accounting

The NX-OS software supports TACACS+ methods for accounting. The NX-OS device reports user activity to the TACACS+ servers in the form of accounting records. The accounting records are stored in an accounting log on the AAA server.

The Nexus device is configured with accounting configuration as follows:

```
Nexus# show running-config | in accounting
aaa accounting default group TACACS
Nexus#
Nexus#
Nexus# show aaa accounting
default: group TACACS
Nexus#
```

On the AAA server ; the command `tail -f /var/log/tac_plus.acct` is used to monitor the TACACS+ accounting log file in real-time. This allows you to see TACACS+ accounting records as they are generated, providing real-time visibility into authentication, authorization, and accounting activities

```
tail -f /var/log/tac_plus.acct
```

In this file, the login activity along with user activity on the device can be observed.

```
tail -f /var/log/tac_plus.acct
lan-admin 0 10.10.10.100 stop task_0=10.10.10.100@pts/3 start_time=1737788184 timezone=UTC cmd=modified the configuration for accounting default default (SUCCESS) result=none
lan-admin 0 10.10.10.100 stop task_0=10.10.10.100@pts/3 start_time=1737788184 timezone=UTC cmd=configure terminal ; aaa accounting default group TACACS (SUCCESS) result=none
lan-admin 0 unknown stop task_0=console0 start_time=1737788469 timezone=UTC cmd=configure terminal ; show ip Ethernet1/1 (REDIRECT) result=none
lan-admin 0 unknown stop task_0=console0 start_time=1737788469 timezone=UTC cmd=configure terminal ; show ip Ethernet1/1 (SUCCESS) result=none
lan-admin 0 unknown stop task_0=console0 start_time=1737788472 timezone=UTC cmd=configure terminal ; show ip Ethernet1/2 (REDIRECT) result=none
lan-admin 0 unknown stop task_0=console0 start_time=1737788472 timezone=UTC cmd=configure terminal ; show ip Ethernet1/2 ; shutdown (REDIRECT) result=none
lan-admin 0 unknown stop task_0=console0 start_time=1737788487 timezone=UTC cmd=configure terminal ; shutdown (SUCCESS) result=none
lan-admin 0 unknown stop task_0=console0 start_time=1737788487 timezone=UTC cmd=Performing configuration copy.
admin 0 unknown start task_id=vsh.bin.6698 start_time=1737788488 timezone=UTC result=none
lan-admin 0 unknown stop task_0=console0 start_time=1737788492 timezone=UTC cmd=copy running-config startup-config (SUCCESS) result=none
```

Lab by Titus Majeza

