Setup Authentication via TACACS+ Server

Setup SSH Authentication via TACACS+ Server

From Release 11.5(1), DCNM provides **appmgr** command to set up authentication for ssh access via TACACS+. For SSH access to DCNM, the credentials are sent to previously configured TACACS+ server, to determine if access is allowed. In case of success, SSH access to DCNM is allowed. When the TACACS+ server is not reachable, the system reverts to local authentication.

DCNM permits SSH access for the following three users—sysadmin, poap, root. The **sysadmin** user has general SSH access to DCNM. SSH access to the **root** user is disabled by default. However, the DCNM Primary and Secondary servers communicate with each other through SSH, using the **root** user with passwordless access, for Native HA setup and maintenance. The **poap** user is employed for SSH/SCP access of information between the DCNM and NX-OS switches. This is typically used for functions such as POAP, and Image management. When you enable TACACS+ authentication for SSH access on the DCNM, you must create three users (sysadmin, poap, root) on the Remote AAA server, and enable TACACS+. Later, any SSH access to the DCNM is authenticated and the TACACS+ server audit logs track all SSH access to DCNM.

Remote authentication is supported only for SSH sessions. The **su** command always uses local authentication. Log in from DCNM console always uses local authentication, to prevent users from system lock-out.

Note For a DCNM Setup in Cluster mode, you must enable and configure remote authentication on all nodes, namely, Primary, Secondary, and all Compute nodes.

Removing Remote Authentication

To remove remote authentication, use the following command:

appmgr remote-auth set none

Note The **appmgr remote-auth set** command always replaces the old configuration with the new one.

Configuring Remote Authentication using TACACS+

To configure remote authentication using TACACS+, use the following command:

appmgr remote-auth set tacacs [**auth** {**pap** | **chap** | **ascii** }] {**server** *<address>* *<secret>* }

Where,

- **auth** defines the Authentication type. If omitted, the default is PAP. ASCII and MSCHAP are also supported.
- *address* is the address of a server. The server address can be hostname, IPv4 address or IPv6 address format. You can also specify a port number. For example: **my.tac.server.com:2049**

  The IPv6 address must a fully qualified IPv6 format as per RFC2732. The IPv6 address must be enclosed in [ ] or the feature won’t function properly.

  For example:

  - [2001:420:1201:2::a] – *correct*
  - 2001:420:1201:2::a – *incorrect*

- *secret* is the secret shared between DCNM and the TACACS+ server. Secrets with spaces aren’t allowed/supported.

Enabling or Disabling Remote Authentication

To enable or disable remote authentication, use the following command.

appmgr remote-auth { **enable** | **disable** }

Viewing Remote Authentication Password

To view the remote authentication password, use the following command:

appmgr remote-auth show

Sample output:

```
dcnm# appmgr remote-auth show
Remote Authentication is DISABLED
```

```
dcnm# appmgr remote-auth show
Remote Authentication is ENABLED
Protocol: tacacs+
Server: 172.28.11.77, secret: ********
Authentication type: ascii
dcnm#
```

By default, shared secrets aren’t displayed in clear-text unless [-S or --show-secret] keyword is used.

Examples

1. Configure and enable 172.28.11.77 as remote authentication server with cisco123 as shared secret.

```
dcnm# appmgr remote□auth set tacacs server 172.28.11.77 cisco123
dcnm# appmgr remote□auth enable
```

2. Configure 172.28.11.77 as remote authentication server with cisco 123 as share secret using MSCHAP as authentication type.

```
dcnm# appmgr remote-auth set tacacs auth mschap 172.28.11.77 cisco123
dcnm# appmgr remote-auth enable
```

3. Configure three servers with different shared secrets.

```
dcnm# appmgr remote-auth set tacacs server tac1.cisco.com:2049 cisco123 server
                  tac2.cisco.com Cisco_123 server tac3.cisco.com C1sco_123
dcnm# appmgr remote-auth enable
```

4. Disable and removes authentication configuration.

```
dcnm# appmgr remote-auth set tacacs none
```

5. Disable remote-authentication without removing the configuration.

```
dcnm# appmgr remote-auth disable
```

6. Enable current remote-authentication configuration.

```
dcnm# appmgr remote-auth enable
```

Remote authentication & POAP

When remote authentication is enabled, the local password of **poap** user must be the same as the password on TACACS server; POAP fails otherwise.

To synchronize local poap password, after setting or changing the password on the TACACS server, use the following command:

appmgr change_pwd ssh poap

In Cisco DCNM Native HA setup, execute this command on the Primary node only.

Remote authentication in DCNM Native HA setup

For scenarios in which a standalone DCNM needs to be converted to a native HA setup, ensure that remote authentication if enabled, should be disabled prior to adding a secondary HA node, and before running **appmgr update ssh-peer-trust** command.