Cisco ACI TACACS External Logging

Revised: March 1, 2023

New and Changed Information

The following table provides an overview of the significant changes up to this current release. The table does not provide an exhaustive list of all changes or the new features up to this release.

Table 1: New and Changed Information

Cisco APIC Release	Feature	Description
6.0(2)	TACACS external logging for switches	TACACS can collect AAA data from switches. For more information, see About TACACS External Logging, on page 2.
3.2(1)	This feature was introduced	--

About TACACS External Logging

Terminal Access Controller Access Control System (TACACS) and Terminal Access Controller Access Control System Plus (TACACS+) are simple security protocols that provide centralized validation of users attempting to gain access to network devices. TACACS+ furthers this capability by separating the authentication, authorization, and accounting functions in modules, and encrypting all traffic between the network-attached storage (NAS) and the TACACS+ daemon.

TACACS external logging collects AAA data from a configured fabric-wide TACACS source and delivers it to one or more remote destination TACACS servers, as configured in a TACACS destination group. The collected data includes AAA session logs (`SessionLR`) such as log-ins, log-outs, and time ranges, for every Cisco Application Policy Infrastructure Controller (APIC) user, as well as AAA modifications (`ModLR`) such as the addition of a new user or a password change. Additionally, all configuration changes are logged and include the user ID and time stamp.

Beginning with the Cisco APIC 6.0(2) release, you can enable TACACS external logging for switches. When enabled, the Cisco APIC collects the same types of AAA data from the switches in the chosen TACACS monitoring destination group.

Note TACACS external logging for switches supports CLI modules such as **vsh**, **vsh_lc**, and **ibash**, but it does not support native Linux commands and system binaries.

TACACS External Logging Destination Group

Creating a TACACS External Logging Destination Group and Destinations Using the GUI

AAA log data can be collected and exported to a destination group for delivery to a destination of your choice. The **Create TACACS Monitoring Destination Group** screen contains properties for specifying a TACACS destination group and associated destinations. After you create the destination group, you can associate the group with a TACACS source, either for a fabric policy or an external access policy, that is configured on the Cisco Application Policy Infrastructure Controller (APIC).

A TACACS destination group is used by the Cisco ACI fabric for sending AAA log messages to configured destinations.

Procedure

Step 1 Choose **Admin > External Data Collectors**.

Step 2 In the **Navigation** pane, right-click **Monitoring Destinations** and choose **Create TACACS Monitoring Destination Group**. Alternatively, expand **Monitoring Destinations** in the **Navigation** pane, click **TACACS**, and in the TACACS work pane, click the**Actions** drop-down list, then click **Create TACACS Monitoring Destination Group**.

Step 3 In the **Create TACACS Monitoring Destination Group** dialog, perform the following actions:

a) (Required) Enter a name in the **Name** field.
b) Enter a description in the **Description** field.
c) Click **Next**.

Step 4 In the **Destinations** dialog, click the + symbol above the **Create Destinations** table.

Step 5 In the **Create TACACS Destinations** table editor, perform the following actions:

a) Enter a host name or an IP address of the destination external TACACS log server host in the **Host Name/IP** field.
b) In the **Port** field, enter a port number to be used to send AAA logging data to the destination external TACACS log server.
c) Enter a key or password in the **Key** field. This is the secret shared with the TACACS server.
d) From the **Authentication Protocol** buttons, choose an authentication protocol for the destination.
e) From the **Management EPG** drop-down list, choose an EPG.
f) Click **OK**.

Step 6 Click **Finish**.

Creating a TACACS External Logging Destination Group Using the NX-OS-Style CLI

You can use the NX-OS-style command line interface (CLI) to configure TACACS destination groups and destinations. A TACACS destination group enables you to create a list of remote TACACS server destinations to which AAA logging data is sent. You can create one or more destinations in a group. After you create the destination group, you can associate the group with a TACACS source, either for a fabric policy or an external access policy, that is configured on the Cisco Application Policy Infrastructure Controller (APIC).

Note You must have administrator rights to access the TACACS External Logging commands in the NX-OS-style CLI.

The following example CLI commands show how to configure a TACACS destination group and destination using the NX-OS-style CLI:

Procedure

Step 1 Enter the configuration mode.

Example:

```
apic1# config
```

Step 2 Create a TACACS destination group.

Example:

In the following command, a TACACS destination group named "tacacs-dest-grp-1" is created:

```
apic1(config)# tacacslog-group tacacs-dest-grp-1
```

Step 3 Create a TACACS destination in the new destination group.

Example:

In the following command, a remote TACSCS destination with an IP address of "1.1.1.1" is created and includes the default port number 49:

```
apic1(config-tacacslog-group)# remote-dest 1.1.1.1 port 49
```

Note You can have logs sent to multiple ports on the same IP address by including additional port numbers after the port keyword.

Step 4 Configure specific parameters for the new remote TACACS destination.

Example:

In the following command example, the following characteristics are configured for the new remote destination:

- Authentication key: 12345
- Authentication protocol: MS-CHAP
- Management EPG: Out-of-Band

```
apic1(config-remote-dest)# key
Enter Key: 12345
Enter Key again: 12345
apic1(config-remote-dest)# protocol mschap
apic1(config-remote-dest)# management-epg oob
```

The result of this configuration is the creation of a TACACS destination group containing a remote TACACS server destination. If you want the same AAA logging data sent to multiple remote TACACS servers, you can repeat steps 3 and 4 as many times as needed.

Creating a TACACS External Logging Destination Group Using the REST API

Procedure

Create a TACACS destination group.

Example:

```
POST https://<apic-name>/api/node/mo/uni/fabric/tacacsgroup-<groupname>.json
```

```
{
  "tacacsGroup": {
    "attributes": {
      "dn": "uni/fabric/tacacsgroup-<groupname>",
      "name": "<groupname>",
      "rn": "tacacsgroup-<groupname>",
      "status": "created"
    },
    "children": [{
      "tacacsTacacsDest": {
        "attributes": {
          "dn": "uni/fabric/tacacsgroup-<groupname>/tacacsdest-<dest-name>-port-<portno>",
         "host": "<dest-name>",
          "rn": "tacacsdest-<dest-name>-port-<portno>",
```

```
            "key": "<server secret>",
            "status": "created"
          },
          "children": [{
            "fileRsARemoteHostToEpg": {
              "attributes": {
                "tDn": "uni/tn-mgmt/mgmtp-default/oob-default",
                "status": "created"
              },
              "children": []
            }
          }]
        }
      }]
    }
  }
```

TACACS External Logging Source

Creating a TACACS External Logging Source Using the GUI

The TACACS monitoring source profile associates a TACACS destination group that identifies destinations where AAA log data should be delivered.

The TACACS source is used by the Cisco ACI Fabric for collecting logged AAA information to send in TACACS messages to TACACS accounting servers.

Procedure

Step 1 Choose **Fabric > Fabric Policies**.

Step 2 In the **Navigation** pane, expand the following:

a) **Policies**
b) **Monitoring**
c) **Common Policy**

Step 3 Click **Callhome/Smart Callhome/SNMP/Syslog/TACACS**.

Step 4 In the **Callhome/Smart Callhome/SNMP/Syslog/TACACS** work pane, click the **TACACS** tab.

Step 5 In the TACACS work pane, click the **Actions** (icon) drop-down list, then click **Create TACACS Source**. Alternatively, right-click **Callhome/Smart Callhome/SNMP/Syslog/TACACS** in the **Navigation** pane and select **Create TACACS Source**.

Step 6 In the **Create TACACS Source** dialog, perform the following actions:

a) Enter a unique name for the policy in the **Name** field.
b) Enter a TACACS destination group, where AAA logging data for this policy will be sent, in the **Destination Group** field.
c) Click **Submit**.

Creating a TACACS External Logging Source Using the NX-OS-Style CLI

You can use the NX-OS-style CLI to configure TACACS sources. In this configuration, the source is associated with a TACACS destination group. Where a TACACS source is created determines which set of AAA logging data is sent. For example, if you create

the TACACS source in Fabric Policies, all AAA logging data for the Cisco Application Centric Infrastructure (Cisco ACI) fabric supported by Cisco Application Policy Infrastructure Controller (Cisco APIC) is sent to the associated TACACS destinations. You can create one or more sources to support different destination groups.

The following example CLI commands show how to configure a TACACS source using the NX-OS-style CLI:

Procedure

Step 1 Enter the configuration mode.

Example:

```
apic1# config
```

Step 2 Create a TACACS source.

Example:

In the following command, a TACSCS source named "tacacs-src-1" is created:

```
apic1(config)# tacacslog-monitoring common tacacslog-src tacacs-src-1
```

Step 3 Associate the TACACS source with a TACACS destination group.

Example:

In the following command, a TACSCS destination group named "tacacs-dest-grp-1" is associated with the new TACACS source:

```
apic1(config-tacacslog-monitoring)# server-group tacacs-dest-grp-1
```

The result of this configuration is the creation of a TACACS source for the entire fabric and the association of a destination group containing a remote TACACS server destination. All AAA logging data for the entire fabric is then sent to the associated TACACS destination(s).

Creating a TACACS External Logging Source Using the REST API

Procedure

Create a TACACS source.

Example:

```
POST https://<apic-name>/api/node/mo/uni/fabric/moncommon/tacacssrc-<src-name>.json

{
  "tacacsSrc": {
    "attributes": {
      "dn": "uni/fabric/moncommon/tacacssrc-<src-name>",
      "incl": "audits,faults",
      "name": "aaa",
      "rn": "tacacssrc-<src-name>",
      "status": "created",
      "incl":"audit,session"
    },
    "children": [{
      "tacacsRsDestGroup": {
        "attributes": {
          "tDn": "uni/fabric/tacacsgroup-<groupname>",
```

```
            "status": "created"
          },
          "children": []
        }
      }]
    }
}
```

TACACS External Logging for Switches

Enabling TACACS External Logging for Switches Using the GUI

Beginning with the Cisco Application Policy Infrastructure Controller (APIC) 6.0(2) release, you can use this procedure to enable TACACS external logging for switches.

Procedure

Step 1 On the menu bar, choose **Fabric** > **Fabric Policies**.

Step 2 In the Navigation pane, choose **Policies** > **Monitoring** > **Common Policy** > **Callhome/Smart Callhome/SNMP/Syslog/TACACS**.

Step 3 In the Work pane, choose **TACACS** > **Actions** > **Create TACACS Source**.

Step 4 In the **Create TACACS Source** dialog, change the name if desired, choose or create the destination group, and for **Switch Tacacs Audit** choose **Enabled**.

Enabling TACACS External Logging for Switches Using the NX-OS-Style CLI

Beginning with the Cisco Application Policy Infrastructure Controller (APIC) 6.0(2) release, you can use this procedure to enable TACACS external logging for switches.

Procedure

Step 1 Enter the configuration mode.

Example:

```
apic1# config
```

Step 2 Create a TACACS source.

The following command creates a TACACS source named "tacacs-src-1" under the common tenant:

Example:

```
apic1(config)# tacacslog-monitoring common tacacslog-src tacacs-src-1
```

Step 3 Enable TACACS external logging for the switches that are in the TACACS source.

Example:

```
apic1(config-tacacslog-monitoring)# switch-audit-enable
```

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.