Configuring TACACS+ for Cisco APIC Access

First Published: October 2019

Version: 1.0

Americas Headquarters

Cisco Systems, Inc.

170 West Tasman Drive

San Jose, CA 95134-1706

USA

http://www.cisco.com

Tel: 408 526-4000

800 553-NETS (6387)

Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers us ed in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Overview

This article provides step by step instructions on how to enable TACACS+ users to access the APIC. It assumes the reader is thoroughly familiar with the *Cisco Application Centric Infrastructure Fundamentals* manual, especially the User Access, Authentication, and Accounting chapter.

You can use RBAC to specify support groups. As a member of a support group, an authenticated user can access to the specific ACI resources with the rights and privileges associated with that support group.

Note In the case of a disaster scenario such as the loss of all but one APIC in the cluster, APIC disables remote authentication. In this scenario, only a local administrator account can log into the fabric devices.

Note Remote users for AAA Authentication with shell:domains=all/read-all/ will not be able to access Leaf switches and Spine switches in the fabric for security purposes. This pertains to all version up to 4.0(1h).

Note: The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Procedure Overview

1. On the APIC:
    a. Create the TACACS+ provider.
    b. *For ACI versions prior to v4*: Create the TACACS+ provider group.
    c. Create the TACACS+ login domain.
2. Configure TACACS+:
    a. Configure the AAA client(s)
    b. Configure the user, and associate user with identity group.
    c. Create the unique ‘Shell Profile’
    d. Create a Service Selection Rule for TACACS+
    e. Create a rule to associate the Identity Group with the Shell Profile.
3. On the APIC, validate the TACACS+ configuration
    a. Log in using the TACACS+ user account.
    b. On an ACI switch, validate that the correct access privileges are enforced

Configuring APIC for TACACS+ Access

Before you begin

- The Cisco Application Centric Infrastructure (ACI) fabric is installed, fabric discovery is complete, Application Policy Infrastructure Controllers (APICs) are online, and the APIC cluster is formed and healthy, there is In-Band/Out-of-Band connectivity to the APIC controllers and fabric switches, and In-Band/Out-of-Band contracts are configured that allow

ICMP and default TACACS ports UDP 49 and TCP 49.

- The TACACS+ server host name or IP address, port, and key are available, and that you can ping your TACACS server from the APICs and fabric switches you are trying to authenticate from.
- The APIC management endpoint group is available.

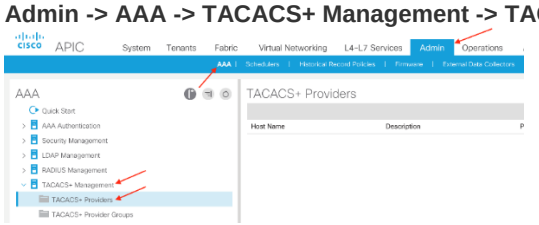
Procedure: Configure the APIC for TACACS+ Access

Step 1 In the APIC, create the **TACACS+ Provider**.

a) On the menu bar, choose **Admin** > **AAA**.

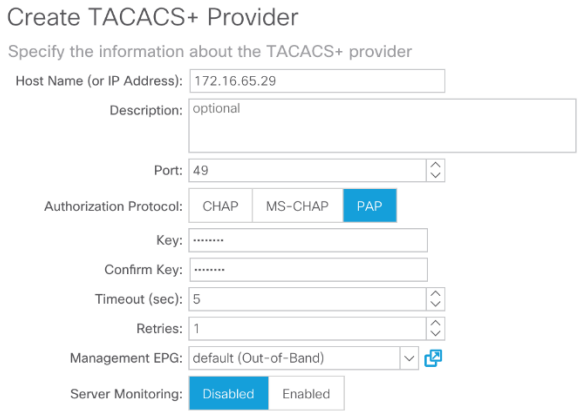
b) In the **Navigation** pane, choose **TACACS+ Management** > **TACACS+ Providers**.

Admin -> AAA -> TACACS+ Management -> TACACS+ Providers



c) In the **Work** pane, choose **Actions** > **Create TACACS+ Provider**.

d) Right click **TACACS+ Providers** and select **Create TACACS+ Provider**



e) Specify the TACACS attributes used to connect to the TACACS server:

- **IP Address**: This is the IP address of the TACACS server
- **Port:** This is the port used to connect to the TACACS server. TACACS default is port 49
- **Authorization Protocol:** This needs to match the configuration on the TACACS server which we will go over later in the ACS and ISE configuration
- **Key:** This needs to match the configuration on the TACACS server which we will go over later in the ACS and ISE configuration
- **Timeout:** The amount of time allowed for a login attempt to occur before giving up (measured in seconds)
- **Retries:** The number of automatic re-try login attempts allowed for a single authentication submission

- **Management EPG:** The management EPG used to connect to the TACACS server. You will want to use the Management EPG which has all the necessary contracts in place
- **Server Monitoring:** Used to determine if the TACACS server is alive. This option uses the TACACS protocol login to check if the TACACS server is alive

Note If the APIC is configured for in-band management connectivity, out-of-band management does not work for authentication. With the APIC release2.1(1x), you can set a global toggle between In-band and out-of-band as the default management connectivity between the APIC and other external management devices.

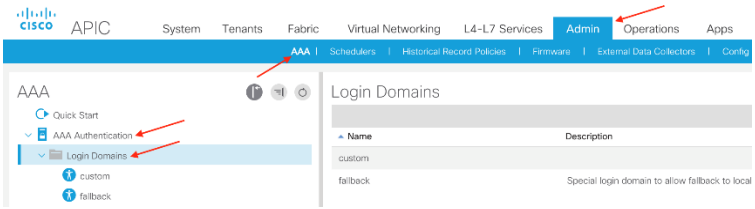
For toggling in-band or out-of-band management in the APIC GUI:

- Prior to Release 2.2(1x): In the **Navigation** pane, choose **Fabric** > **FabricPolicies** > **GlobalPolicies** > **Connectivity Preferences**. In the **Work Pane** select either **inband** or **ooband**.
- For Release 2.2(x) and 2.3(x): In the **Navigation** pane, choose **Fabric** > **Fabric Policies** > **Global Policies** > **APIC Connectivity Preferences**. In the **Work Pane** select either **inband** or **ooband**.
- For Release 3.0(1x) or later: In the **Navigation** pane, choose **System** > **System Settings** > **APIC Connectivity Preferences**. In the **Work Pane** select either **inband** or **ooband**.

Step 2 Create the **Login Domain** for TACACS+.

The final ACI configuration step is to create the Login Domain and associate our newly created TACACS Provider Group. To create a Login Domain navigate to the following APIC web GUI path:

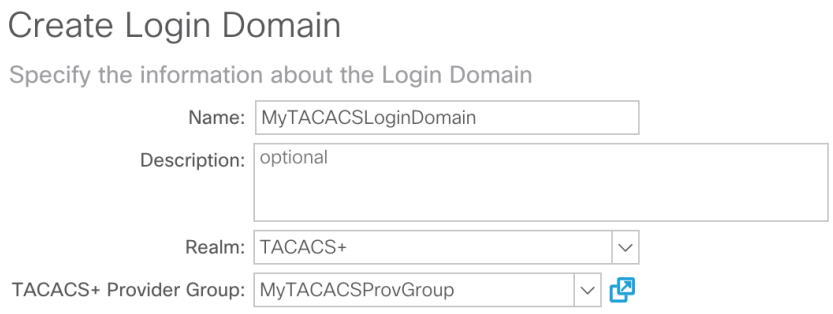
Admin -> AAA -> AAA Authentication -> Login Domains



a) In the **Navigation** pane, choose **AAA Authentication** > **Login Domains**.

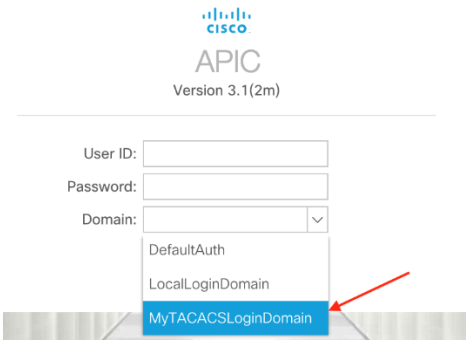
b) In the **Work** pane, choose **Actions** > **Create Login Domain**.

c) Specify the login domain name, description, realm, and provider group as appropriate.



d) Provide a name, realm, and select the newly created TACACS Provider Group.

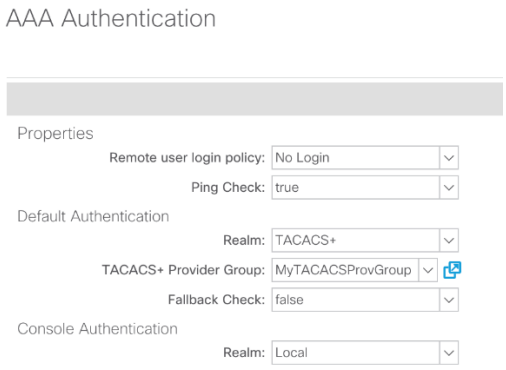
e) Following good practice guidelines, create an additional Login Domain which has a Realm of Local. This local Login Domain will allow users to use local APIC credentials as a fall-back access when the TACACS+ server is unavailable. This Login Domain appears in the Domain drop down list in the APIC GUI login screen.



In this illustration, notice the newly created TACACS+ Login Domain, *MyTACACSLoginDomain*, and the Login Domain, *LocalLoginDomain*, are created for TACACS+ and local authentication. If a Login Domain is not selected, the built in DefaultAuth login domain is used. To make the APIC default to the TACACS+ login domain, change the default Login Domain behavior by navigating to the following APIC web GUI path:

Admin -> AAA -> AAA Authentication

Change the default to TACACS+ and select our newly created TACACS Provider Group:



This enables default TACACS authentication for the APIC GUI and SSH sessions to APICs and fabric switches. To enable TACACS authentication for console sessions to fabric switches, enable the TACACS+ Realm for Console Authentication.

Note: Make sure to leave/set the Fallback Check property to false. Setting the Fallback Check property to true may cause local logins to fail.

If you did not create an additional Login Domain for local authentication, and you forgot your TACACS credentials, ACI includes a fallback Login Domain. The fallback Login Domain cannot be deleted and is set to use local authentication by default. In order to login to the fallback Login Domain you must use this syntax:

APIC GUI: apic:LOGIN_DOMAIN_HERE\\LOCAL_USERNAME_HERE
APIC CLI: apic#LOGIN_DOMAIN_HERE\\LOCAL_USERNAME_HERE

To login to the local admin account you would use the following APIC GUI and CLI syntax's:

APIC GUI: apic:fallback\\admin
APIC CLI: apic#fallback\\admin

This concludes all the necessary ACI configuration for TACACS. Now let's move onto the ACS 5.8 TACACS configuration.

What to Do Next

This completes the APIC TACACS+ configuration steps. Now you need to sue software such as ACS to configure TACACS for authentication and RBAC parameters for ACI access. This document does not provide step-by-step instructions for this task. As an example, a high-level summary of such steps are provided here:

Example of Steps for Configuring TACACS Policies in ACS 5.8:

1. Create Network Device Location
2. Create Network Device Type
3. Create Network Devices and AAA Clients
4. Create Identity Group
5. Create local user on the ACS server
6. Create Shell Profile with AVPair
7. Create Device Administration Authorization Policy

Verify TACACS Authentication on ACI Leaf Switches

This section of the document provides verification/troubleshooting steps for TCACS authentication on ACI leaf switches. We assume that a TACACS domain is configured and is set as the default authentication domain.

The APIC CLI configuration captured below shows that:

- The TACACS group name is '**tacas-1**' configured with a single **tacasplus** provider **192.168.3.129**
- The default login domain is set to TACACS with group '**tacas-1**'
- A login domain named '**tacas**' is configured also using the group '**tacas-1**'

```
fab2-apic1# show running-config aaa
# Command: show running-config aaa
# Time: Mon May 16 11:23:50 2016
  aaa banner 'Application Policy Infrastructure Controller'
  aaa group server TACACSplus tacas-1
    server 192.168.3.129 priority 1
    exit
  aaa authentication login console
    exit
  aaa authentication login default
    realm TACACS
    group tacas-1
    exit
  aaa authentication login domain fallback
    exit
  aaa authentication login domain TACACS
    realm TACACS
    group tacas-1
    exit
fab2-apic1# show running-config all TACACS-server host 192.168.3.129
# Command: show running-config all TACACS-server host 192.168.3.129
# Time: Mon May 16 11:31:36 2016
 TACACS-server host "192.168.3.129"
 retries 1
 timeout 5
 port 49
 protocol pap
 key ""
 exit
```

Verify Login Configuration on Leaf

Below we can see that the tacas-1 group is configured and set as the default AAA authentication mechanism.

```
fab2-leaf101# show TACACS-server groups
total number of groups:1

following TACACS+ server groups are configured:
        group tacas-1:
                server: 192.168.3.129 on port 49
                deadtime is 0

fab2-leaf101# show aaa authentication
         default: group tacas-1
         console: N/A
```

Verify TACACS Server Reachability from a Leaf Switch

APIC currently allows for in-band or out-of-band connectivity to the TACACS server. In this example connectivity is configured for out-of-band. The leaf will check connectivity to the TACACS server via ICMP to mark the server as operable; the leaf/APIC must be able to ping the TACACS server)

```
fab2-leaf101# iping -V management 192.168.3.129
PING 192.168.3.129 (192.168.3.129) from 192.168.3.101: 56 data bytes
64 bytes from 192.168.3.129: icmp_seq=0 ttl=64 time=0.499 ms
64 bytes from 192.168.3.129: icmp_seq=1 ttl=64 time=0.464 ms
64 bytes from 192.168.3.129: icmp_seq=2 ttl=64 time=0.461 ms
64 bytes from 192.168.3.129: icmp_seq=3 ttl=64 time=0.525 ms
64 bytes from 192.168.3.129: icmp_seq=4 ttl=64 time=0.541 ms

--- 192.168.3.129 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.461/0.497/0.541 ms
```

Verify provider is in operation state 'operable' and connecting over the configured EPG (out-of-band in this example)

```
fab2-leaf101# pwd
/mit/uni/userext/TACACSext/TACACSplusprovider-192.168.3.129

fab2-leaf101# cat summary
# TACACS+ Provider
name               : 192.168.3.129
authProtocol       : pap
childAction        :
descr              :
dn                 : uni/userext/TACACSext/TACACSplusprovider-192.168.3.129
epgDn              : uni/tn-mgmt/mgmtp-default/oob-default
key                :
lcOwn              : resolveOnBehalf
modTs              : 2016-05-15T19:57:08.303-04:00
monPolDn           : uni/fabric/monfab-default
monitorServer      : disabled
monitoringPassword :
monitoringUser     : test
operState          : operable
ownerKey           :
ownerTag           :
port               : 49
retries            : 1
rn                 : TACACSplusprovider-192.168.3.129
snmpIndex          : 1
status             :
timeout            : 5
uid                : 15374
vrfName            : management
```

The NGINX process receives updated configuration for TACACS providers and handles monitoring of provider reachability. You can also verify provider reachability in the NGINX logs

```
fab2-leaf101# egrep 192.168.3.129 /var/log/dme/log/nginx.log | more

4852||16-05-16 11:15:13.576-04:00||aaa||DBG4||||Received response from 192.168.3.129 -
notifying callback handler
(IPv4)||../dme/svc/extXMLApi/src/gen/ifc/app/./ping/lib_ifc_ping.cc||756

4852||16-05-16 11:15:13.576-04:00||aaa||DBG4||||Received update on status of
192.168.3.129 (DN uni/userext/TACACSext/TACACSplusprovider-192.168.3.129) - status is
ALIVE||../dme/svc/extXMLApi/src/gen/ifc/app/./pam/PamWorker.cc||1429

<configConfMo dn="uni/userext/TACACSext/TACACSplusprovider-192.168.3.129">

4852||16-05-16 11:15:28.580-04:00||aaa||DBG4||||Received response from 192.168.3.129 -
notifying callback handler
(IPv4)||../dme/svc/extXMLApi/src/gen/ifc/app/./ping/lib_ifc_ping.cc||756

4852||16-05-16 11:15:28.580-04:00||aaa||DBG4||||Received update on status of
192.168.3.129 (DN uni/userext/TACACSext/TACACSplusprovider-192.168.3.129) - status is
ALIVE||../dme/svc/extXMLApi/src/gen/ifc/app/./pam/PamWorker.cc||1429

<configConfMo dn="uni/userext/TACACSext/TACACSplusprovider-192.168.3.129">

4852||16-05-16 11:15:43.573-04:00||aaa||DBG4||||Received response from 192.168.3.129 -
notifying callback handler
(IPv4)||../dme/svc/extXMLApi/src/gen/ifc/app/./ping/lib_ifc_ping.cc||756

4852||16-05-16 11:15:43.573-04:00||aaa||DBG4||||Received update on status of
192.168.3.129 (DN uni/userext/TACACSext/TACACSplusprovider-192.168.3.129) - status is
ALIVE||../dme/svc/extXMLApi/src/gen/ifc/app/./pam/PamWorker.cc||1429

<configConfMo dn="uni/userext/TACACSext/TACACSplusprovider-192.168.3.129">

4852||16-05-16 11:15:58.575-04:00||aaa||DBG4||||Received response from 192.168.3.129 -
notifying callback handler
(IPv4)||../dme/svc/extXMLApi/src/gen/ifc/app/./ping/lib_ifc_ping.cc||756

4852||16-05-16 11:15:58.575-04:00||aaa||DBG4||||Received update on status of
192.168.3.129 (DN uni/userext/TACACSext/TACACSplusprovider-192.168.3.129) - status is
ALIVE||../dme/svc/extXMLApi/src/gen/ifc/app/./pam/PamWorker.cc||1429

<configConfMo dn="uni/userext/TACACSext/TACACSplusprovider-192.168.3.129">

...
```

If TACACS should be the default login domain, verify the `DefaultAuth` object on the leaf.

```
fab2-leaf101# moquery -c aaaDefaultAuth
Total Objects shown: 1

# aaa.DefaultAuth
childAction    :
descr          :
dn             : uni/userext/authrealm/defaultauth
lcOwn          : resolveOnBehalf
modTs          : 2016-05-16T11:23:57.288-04:00
name           :
ownerKey       :
ownerTag       :
providerGroup  : tacas-1
realm          : TACACS
rn             : defaultauth
status         :
uid            : 0
```

SSH to leaf

In this example, the default authentication is set to TACACS (note the name of the TACACS+ login domain is also 'tacas'). However, a user can always specify the login domain they wish to authenticate against. From the ACI fundamentals login guide:

> Login Domains
> `apic:<domain>\<username>`
> From the GUI, use `apic:fallback\\username`.
> From the REST API, use `apic#fallback\\username`.

SSH using the default domain

ssh user1@fab2-leaf101

Important events in the NGINX logs are below. We can see that leaf is defaulting authentication to the TACACS provider group tacas-1 as we configured. Additionally, the provider is reachable over the management VRF. Next, notice that the connection to the TACACS server is successful along with the attributes provided by the TACACS server for the user.

```
6403||16-05-18 13:47:18.755-04:00||aaa||INFO||co=doer:0:0:0xff00000000011467:1||Received
PAM authenticate request from nginx for user
user1||../dme/svc/extXMLApi/src/gen/ifc/app/./imp/aaa/PamAuthenticateImp.cc||81

6403||16-05-18 13:47:18.755-
04:00||aaa||DBG4||co=doer:0:0:0xff00000000011467:1||Performing prefix match check for
input tty 'ssh' - check against platform console tty prefix of
'/dev/ttyS'||../dme/common/src/ifcsec/AaaUtils.cc||1223

6403||16-05-18 13:47:18.755-
04:00||aaa||DBG4||co=doer:0:0:0xff00000000011467:1||DefaultAuthMo specifies realm 2.
Provider Group tacas-1 !||../dme/common/src/ifcsec/AaaUtils.cc||1258
```

6403||16-05-18 13:47:18.755-04:00||aaa||DBG4||co=doer:0:0:0xff00000000011467:1||Decoded username string to Domain: Username: user1 Realm 2, PG tacas-1||../dme/svc/extXMLApi/src/gen/ifc/app/./pam/SecurityMgrPAM.cc||638

6403||16-05-18 13:47:18.755-04:00||aaa||DBG4||co=doer:0:0:0xff00000000011467:1||Adding TacacsProvider 192.168.3.129 to the list, order 1||../dme/svc/extXMLApi/src/gen/ifc/app/./pam/SecurityMgrPAM.cc||567

6403||16-05-18 13:47:18.755-04:00||aaa||DBG4||co=doer:0:0:0xff00000000011467:1||**Input VRF Name management**||../dme/svc/extXMLApi/src/gen/ifc/app/./pam/SecurityMgrPAM.cc||117

6403||16-05-18 13:47:18.755-04:00||aaa||DBG4||co=doer:0:0:0xff00000000011467:1||Obtained VRF Id 2||../dme/svc/extXMLApi/src/gen/ifc/app/./pam/SecurityMgrPAM.cc||141

6405||16-05-18 13:47:18.756-04:00||aaa||DBG4||||transId ca3000000060000 Setting AAA lookup retries = 1, timeout = 5 seconds||../dme/svc/extXMLApi/src/gen/ifc/app/./pam/PamRequest.cc||791

6405||16-05-18 13:47:18.756-04:00||aaa||DBG4||||**Initialized TacacsAuthenticationBroker for lookup of user1** (address 10.150.188.212, hostname ssh)||../dme/svc/extXMLApi/src/gen/ifc/app/./ext/TacacsAuthentication.cc||34

6405||16-05-18 13:47:18.756-04:00||aaa||DBG4||||**Server 192.168.3.129:49**||../dme/svc/extXMLApi/src/gen/ifc/app/./ext/TacacsAuthentication.cc||39

6405||16-05-18 13:47:18.756-04:00||aaa||DBG4|||**|Attempting to start TACACS+ session|**|../dme/svc/extXMLApi/src/gen/ifc/app/./ext/TacacsAuthentication.cc||74

6405||16-05-18 13:47:18.756-04:00||aaa||DBG4||||Creating TACACS+ AUTH START packet for user user1 for remoteAddress 10.150.188.212(../dme/common/src/libTACACS/tplus_pkt.c:528)||../dme/svc/extXMLApi/src/gen/ifc/app/./ext/TacacsAuthentication.cc||256

6405||16-05-18 13:47:18.756-04:00||aaa||DBG4||||Outbound TACACS+ Authen Start packet: Outbound TACACS+ Authen Start packet: Outbound TACACS+ Authen Start packet: Outbound TACACS+ Authen Start packet: Outbound TACA(../dme/common/src/libTACACS/tplus_pkt.c:589)||../dme/svc/extXMLApi/src/gen/ifc/app/./ext/TacacsAuthentication.cc||256

6413||16-05-18 13:47:19.572-04:00||aaa||DBG4||||tplus_decode_author_response: **Attributes count 3**(../dme/common/src/libTACACS/tplus_pkt.c:1467)||../dme/svc/extXMLApi/src/gen/ifc/app/./ext/TacacsAuthentication.cc||256

6413||16-05-18 13:47:19.572-04:00||aaa||DBG4||||tplus_decode_author_response: attribute 0 shell:roles=vdc-admin network-admin(../dme/common/src/libTACACS/tplus_pkt.c:1477)||../dme/svc/extXMLApi/src/gen/ifc/app/./ext/TacacsAuthentication.cc||256

6413||16-05-18 13:47:19.572-04:00||aaa||DBG4||||tplus_decode_author_response: attribute 1 priv-

lvl=15(../dme/common/src/libTACACS/tplus_pkt.c:1477)||../dme/svc/extXMLApi/src/gen/ifc/app/./ext/TacacsAuthentication.cc||256

6413||16-05-18 13:47:19.572-04:00||aaa||DBG4||||tplus_decode_author_response: attribute 2
shell:domains=all/admin/(../dme/common/src/libTACACS/tplus_pkt.c:1477)||../dme/svc/extXMLApi/src/gen/ifc/app/./ext/TacacsAuthentication.cc||256

6413||16-05-18 13:47:19.572-04:00||aaa||DBG4||||**Server sent shell:domains=all/admin/**(../dme/common/src/libTACACS/tplus_pkt.c:1491)||../dme/svc/extXMLApi/src/gen/ifc/app/./ext/TacacsAuthentication.cc||256

6403||16-05-18 13:47:19.831-04:00||aaa||DBG4||co=doer:0:0:0xff0000000001146e:1||Checking all UserDomains under remoteuser user1||../dme/svc/extXMLApi/src/gen/ifc/app/./pam/PamRequest.cc||461

6403||16-05-18 13:47:19.831-04:00||aaa||DBG4||co=doer:0:0:0xff0000000001146e:1||Found UserDomain all under remoteuser user1||../dme/svc/extXMLApi/src/gen/ifc/app/./pam/PamRequest.cc||473

6403||16-05-18 13:47:19.831-04:00||aaa||DBG4||co=doer:0:0:0xff0000000001146e:1||Found **UserRole admin with write privileges under UserDomain all - user is an admin user**||../dme/common/src/ifcsec/AaaUtils.cc||532

6403||16-05-18 13:47:19.831-04:00||aaa||DBG4||co=doer:0:0:0xff0000000001146e:1||Found non-admin UserRole admin (write privileges) under UserDomain all||../dme/common/src/ifcsec/AaaUtils.cc||537

6403||16-05-18 13:47:19.831-04:00||aaa||DBG4||co=doer:0:0:0xff0000000001146e:1||Found UserRole admin with write privileges under UserDomain all - user is an admin user||../dme/common/src/ifcsec/AaaUtils.cc||532

6403||16-05-18 13:47:19.831-04:00||aaa||DBG4||co=doer:0:0:0xff0000000001146e:1||Found non-admin UserRole admin (write privileges) under UserDomain all||../dme/common/src/ifcsec/AaaUtils.cc||537

6405||16-05-18 13:47:19.831-04:00||aaa||DBG4||||Received notification of successful remote-user polUpdate||../dme/svc/extXMLApi/src/gen/ifc/app/./pam/PamRequest.cc||597

Note the format of the Cisco-AVPAIR from the TACACS+ server. If the AV pair is not formatted correctly, the leaf may parse an incorrect read/write privilege. Only an admin is allowed access to the leaf; if a non-admin attribute is provided or the AV pair is incorrectly parsed, the user is not be able to SSH to the leaf:

Example of failing attribute pair: `all/aaa/admin(16001)`

- `domain: all`
- `write privilege: aaa`
- `read privilege: admin`

```
18497||16-05-18 17:06:51.338+00:00||aaa||DBG4||||TACACS+ Cisco-avpair
(shell:domains=all/aaa/admin(16001))||../dme/svc/extXMLApi/src/gen/ifc/app/./ext/TacacsA
uthentication.cc||207

...

18487||16-05-18
17:06:51.434+00:00||aaa||DBG4||co=doer:0:0:0xff000000005d535a:1||Checking all
UserDomains under remoteuser
remoteadmin||../dme/svc/extXMLApi/src/gen/ifc/app/./pam/PamRequest.cc||461

18487||16-05-18 17:06:51.434+00:00||aaa||DBG4||co=doer:0:0:0xff000000005d535a:1||Found
UserDomain all under remoteuser
remoteadmin||../dme/svc/extXMLApi/src/gen/ifc/app/./pam/PamRequest.cc||473

18487||16-05-18 17:06:51.434+00:00||aaa||DBG4||co=doer:0:0:0xff000000005d535a:1||Found
non-admin UserRole aaa (write privileges) under UserDomain
all||../dme/common/src/ifcsec/AaaUtils.cc||537

18487||16-05-18 17:06:51.434+00:00||aaa||DBG4||co=doer:0:0:0xff000000005d535a:1||Found
non-admin UserRole admin (read privileges) under UserDomain
all||../dme/common/src/ifcsec/AaaUtils.cc||537

18487||16-05-18 17:06:51.434+00:00||aaa||DBG4||co=doer:0:0:0xff000000005d535a:1||Found
non-admin UserRole aaa (write privileges) under UserDomain
all||../dme/common/src/ifcsec/AaaUtils.cc||537

18487||16-05-18 17:06:51.434+00:00||aaa||DBG4||co=doer:0:0:0xff000000005d535a:1||Found
non-admin UserRole admin (read privileges) under UserDomain
all||../dme/common/src/ifcsec/AaaUtils.cc||537

18487||16-05-18 17:06:51.434+00:00||aaa||DBG4||co=doer:0:0:0xff000000005d535a:1||AAA
Response was authentication successful, but on non IFC platforms, deny login to non-
admin users||../dme/svc/extXMLApi/src/gen/ifc/app/./pam/PamWorker.cc||577

18489||16-05-18 17:06:51.434+00:00||aaa||DBG4||||Received notification of successful
remote-user polUpdate||../dme/svc/extXMLApi/src/gen/ifc/app/./pam/PamRequest.cc||597

18489||16-05-18 17:06:51.434+00:00||aaa||DBG4||||BUT - non admin logins on switch are
denied||../dme/svc/extXMLApi/src/gen/ifc/app/./pam/PamRequest.cc||600
```

'admin' write privilege required to access leaf.

If multiple roles are required, separate them with a pipe (|) character. The UID can only be provided after read privilege are assigned. For example:

```
shell:domains=all/aaa|admin/aaa|admin(16001)
- domain: all
- write privilege: aaa and admin
- read privilege: aaa and admin
- UID manually specified: 16001
```

```
The Cisco AV pair format is as follows:


shell:domains =
domainA/writeRole1|writeRole2|writeRole3/readRole1|readRole2,
domainB/writeRole1|writeRole2|writeRole3/readRole1|readRole2
shell:domains =
domainA/writeRole1|writeRole2|writeRole3/readRole1|readRole2,
domainB/writeRole1|writeRole2|writeRole3/readRole1|readRole2(16003)
The first av-pair format has no UNIX user ID, while the second one does. Both are
correct.
The APIC supports the following regexes:


shell:domains\\s*[=:]\\s*((\\S+?/\\S*?/\\S*?)(,\\S+?/\\S*?/\\S*?){0,31})(\\(\\d+\\))$
shell:domains\\s*[=:]\\s*((\\S+?/\\S*?/\\S*?)(,\\S+?/\\S*?/\\S*?){0,31})$
```

SSH manually specifying the domain

ssh apic#TACACS\\user1@fab2-leaf101

The events are the same, but the logs show that the switch derives the domain from the user instead of relying on the DefaultAuthMo object.

```
4848||16-05-16 12:17:16.745-04:00||aaa||INFO||co=doer:0:0:0xff00000000090b8d:1||Received
PAM authenticate request from nginx for user
apic#TACACS\user1||../dme/svc/extXMLApi/src/gen/ifc/app/./imp/aaa/PamAuthenticateImp.cc|
|81

4848||16-05-16 12:17:16.745-04:00||aaa||INFO||co=doer:0:0:0xff00000000090b8d:1||auth-
domain realm = local, lLocalUser user1||../dme/common/src/ifcsec/AaaUtils.cc||1197

4848||16-05-16 12:17:16.745-04:00||aaa||DBG4||co=doer:0:0:0xff00000000090b8d:1||Decoded
username string to Domain: TACACS Username: user1 Realm 2, PG tacas-
1||../dme/svc/extXMLApi/src/gen/ifc/app/./pam/SecurityMgrPAM.cc||638

4848||16-05-16 12:17:16.745-04:00||aaa||DBG4||co=doer:0:0:0xff00000000090b8d:1||Adding
TacacsProvider 192.168.3.129 to the list, order
1||../dme/svc/extXMLApi/src/gen/ifc/app/./pam/SecurityMgrPAM.cc||567

4848||16-05-16 12:17:16.745-04:00||aaa||DBG4||co=doer:0:0:0xff00000000090b8d:1||Input
VRF Name management||../dme/svc/extXMLApi/src/gen/ifc/app/./pam/SecurityMgrPAM.cc||117

4848||16-05-16 12:17:16.745-04:00||aaa||DBG4||co=doer:0:0:0xff00000000090b8d:1||Obtained
VRF Id 2||../dme/svc/extXMLApi/src/gen/ifc/app/./pam/SecurityMgrPAM.cc||141
```

Packet Capture

In this example, connectivity to the TACACS server is over out-of-band management. A `tcpdump` can be performed on the eth0 interface for out-of-band traffic or `kpm_inb` for in-band traffic.

```
fab2-leaf101# tcpdump -i eth0 "host 192.168.3.129"

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode

listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes

12:22:44.408612 IP 192.168.3.101 > 192.168.3.129: ICMP echo request, id 25269, seq
62421, length 16   <------- ICMP monitor to TACACS server

12:22:44.408952 IP 192.168.3.129 > 192.168.3.101: ICMP echo reply, id 25269, seq 62421,
length 16

12:22:59.407630 IP 192.168.3.101 > 192.168.3.129: ICMP echo request, id 10515, seq
50422, length 16

12:22:59.408295 IP 192.168.3.129 > 192.168.3.101: ICMP echo reply, id 10515, seq 50422,
length 16

12:23:14.408782 IP 192.168.3.101 > 192.168.3.129: ICMP echo request, id 6554, seq 9869,
length 16

12:23:14.409121 IP 192.168.3.129 > 192.168.3.101: ICMP echo reply, id 6554, seq 9869,
length 16

12:23:21.604270 IP 192.168.3.101.50454 > 192.168.3.129.TACACS: Flags [S], seq
1591736023, win 14600, options [mss 1460,sackOK,TS val 14836558 ecr 0,nop,wscale 7],
length 0

12:23:21.604636 IP 192.168.3.129.TACACS > 192.168.3.101.50454: Flags [S.], seq
3678759861, ack 1591736024, win 14480, options [mss 1460,sackOK,TS val 3884607335 ecr
14836558,nop,wscale 7], length 0

12:23:21.604673 IP 192.168.3.101.50454 > 192.168.3.129.TACACS: Flags [.], ack 1, win
115, options [nop,nop,TS val 14836558 ecr 3884607335], length 0

12:23:21.604767 IP 192.168.3.101.50454 > 192.168.3.129.TACACS: Flags [P.], seq 1:50, ack
1, win 115, options [nop,nop,TS val 14836558 ecr 3884607335], length 49

12:23:21.604958 IP 192.168.3.129.TACACS > 192.168.3.101.50454: Flags [.], ack 50, win
114, options [nop,nop,TS val 3884607335 ecr 14836558], length 0

12:23:21.614412 IP 192.168.3.129.TACACS > 192.168.3.101.50454: Flags [P.], seq 1:19, ack
50, win 114, options [nop,nop,TS val 3884607344 ecr 14836558], length 18

12:23:21.614445 IP 192.168.3.101.50454 > 192.168.3.129.TACACS: Flags [.], ack 19, win
115, options [nop,nop,TS val 14836561 ecr 3884607344], length 0

12:23:21.614734 IP 192.168.3.129.TACACS > 192.168.3.101.50454: Flags [F.], seq 19, ack
50, win 114, options [nop,nop,TS val 3884607345 ecr 14836558], length 0

12:23:21.622880 IP 192.168.3.101.50455 > 192.168.3.129.TACACS: Flags [S], seq
1012840409, win 14600, options [mss 1460,sackOK,TS val 14836563 ecr 0,nop,wscale 7],
length 0
```

```
12:23:21.623014 IP 192.168.3.101.50454 > 192.168.3.129.TACACS: Flags [F.], seq 50, ack
20, win 115, options [nop,nop,TS val 14836563 ecr 3884607345], length 0

12:23:21.623123 IP 192.168.3.129.TACACS > 192.168.3.101.50455: Flags [S.], seq
2104245204, ack 1012840410, win 14480, options [mss 1460,sackOK,TS val 3884607353 ecr
14836563,nop,wscale 7], length 0

12:23:21.623158 IP 192.168.3.101.50455 > 192.168.3.129.TACACS: Flags [.], ack 1, win
115, options [nop,nop,TS val 14836563 ecr 3884607353], length 0

12:23:21.623166 IP 192.168.3.129.TACACS > 192.168.3.101.50454: Flags [.], ack 51, win
114, options [nop,nop,TS val 3884607353 ecr 14836563], length 0

12:23:21.623346 IP 192.168.3.101.50455 > 192.168.3.129.TACACS: Flags [P.], seq 1:89, ack
1, win 115, options [nop,nop,TS val 14836563 ecr 3884607353], length 88

12:23:21.623771 IP 192.168.3.129.TACACS > 192.168.3.101.50455: Flags [.], ack 89, win
114, options [nop,nop,TS val 3884607354 ecr 14836563], length 0

12:23:21.630239 IP 192.168.3.129.TACACS > 192.168.3.101.50455: Flags [P.], seq 1:92, ack
89, win 114, options [nop,nop,TS val 3884607360 ecr 14836563], length 91

12:23:21.630260 IP 192.168.3.101.50455 > 192.168.3.129.TACACS: Flags [.], ack 92, win
115, options [nop,nop,TS val 14836565 ecr 3884607360], length 0

12:23:21.630564 IP 192.168.3.129.TACACS > 192.168.3.101.50455: Flags [F.], seq 92, ack
89, win 114, options [nop,nop,TS val 3884607360 ecr 14836563], length 0

12:23:21.630674 IP 192.168.3.101.50455 > 192.168.3.129.TACACS: Flags [F.], seq 89, ack
93, win 115, options [nop,nop,TS val 14836565 ecr 3884607360], length 0

12:23:21.630890 IP 192.168.3.129.TACACS > 192.168.3.101.50455: Flags [.], ack 90, win
114, options [nop,nop,TS val 3884607361 ecr 14836565], length 0
```