

1 Table of Contents

Contents

- 1 Table of Contents..... 1
- 2 NetEdit TACACS Authentication with ClearPass 2
 - 2.1 Things you need..... 2
- 3 Aruba NetEdit Configuration 3
- 4 ClearPass TACACS Configuration..... 4
 - 4.1 ClearPass Configuration with Local User 4
- 5 Testing 7
 - 5.1 Local user Authentication 7
 - 5.2 AD User Authentication 8

2 NetEdit TACACS Authentication with ClearPass

The main objective of this short technical note is for easy/quick configuration and demo of TACACS authentication between NetEdit and ClearPass Policy Manager (CPPM).

2.1 Things you need

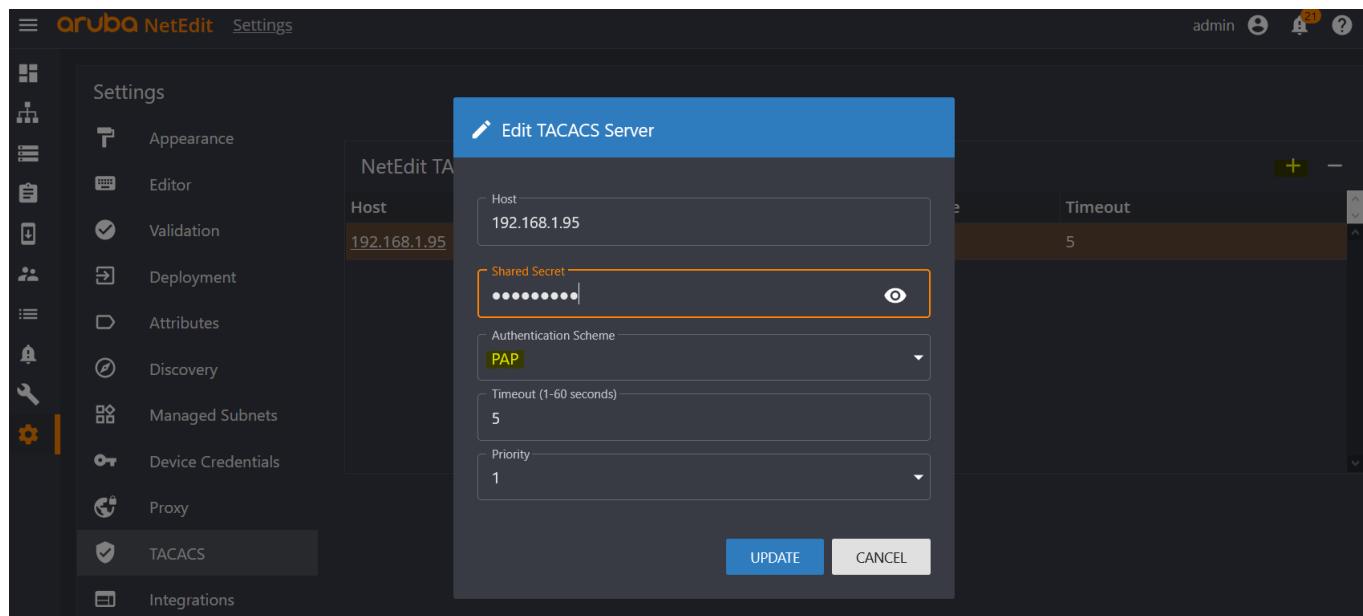
- ClearPass Policy Manager 6.9.x (VM) - 192.168.1.95/24
- NetEdit 2.1.0
- A laptop for Web access to the Aruba NetEdit

We assume that the ClearPass has already joined the AD domain as we'll be using the AD user group to authenticate the TACACS users.

3 Aruba NetEdit Configuration

The NetEdit product is a browser-based client/server application. The NetEdit application provides automation of search, edit, validation, deployment, and audit for network configurations of CX switches.

Here we'll cover the Aruba NetEdit 2.1 TACACS configuration.



Note that PAP is selected for Authentication scheme with ClearPass.

4 ClearPass TACACS Configuration

Here we'll configure ClearPass to be the TACACS+ servers to authenticate users who request access to the NetEdit VM.

4.1 ClearPass Configuration with Local User

First, we ensure the TACACS secret key is configured for NetEdit

Edit Device Details

Device

SNMP Read Settings

SNMP Write Settings

CLI Settings

OnConnect Enforcement

Attributes

Name:

NetEdit

IP or Subnet Address:

192.168.1.90

(e.g., 192.168.1.10 or 192.168.1.1/24 or 192.168.1.1-20 or 2001:db8:a0b:12f0::1)

Description:

RADIUS Shared Secret:

Verify:

TACACS+ Shared Secret:

.....

Verify:

.....

Vendor Name:

Aruba

Enable RADIUS Dynamic Authorization:

☒

Port: 3799

Enable RadSec:

☐

Copy

Save

Cancel

Then we need to create roles and local users for testing.

Dashboard

Monitoring

Configuration

Service Templates & Wizards

Services

Authentication

Identity

Single Sign-On (SSO)

Local Users

Endpoints

Static Host Lists

Roles

Role Mappings

Posture

Enforcement

Policies

Profiles

Filter: Name

contains

Go

Clear Filter

#

Name

Description

1.

[AirGroup v1]

Role for an AirGroup protocol version 1 requ

2.

[AirGroup v2]

Role for an AirGroup protocol version 2 requ

3.

all-test-group-member

4.

[Aruba TACACS read-only Admin]

Default role for read-only access to Aruba de

5.

6.

7.

8.

9.

10.

11.

12.

13.

14.

Edit Role

Role ID:

3007

Name:

Netedit

Description:

Save

Cancel

Dashboard

Monitoring

Configuration

Service Templates & Wizards

Services

Authentication

Identity

Single Sign-On (SSO)

Local Users

Endpoints

Static Host Lists

Roles

Role Mappings

Posture

Enforcement

Policies

Profiles

Configuration » Identity » Local Users

Local Users

ClearPass Policy Manager lists all local users in the Local Users page.

Filter: User ID

contains

Go

Clear Filter

Show 20 records

#

User ID

Name

Role

Status

1.

ariya

ariya

MM-Lab-admin

Enabled

2.

dcadmin

dcadmin

MM-DCLab-admin

Enabled

3.

netedit

netedit

Netedit

Enabled

4.

neteditro

neteditro

NeteditRO

Enabled

5.

staff1

staff1

Staff

Enabled

6.

student1

student1

Student

Enabled

Showing 1-6 of 6

Export

Delete

Now that we have configured the users in local database and have assigned their relevant roles. We'll create the TACACS service we need.

Services - Modified Aruba Device Access Service

Summary	Service	Authentication	Roles	Enforcement
Name:	Modified Aruba Device Access Service			
Description:	Service for access to Aruba device			
Type:	TACACS+ Enforcement			
Status:	Enabled			
Monitor Mode:	<input type="checkbox"/> Enable to monitor network access without enforcement			
More Options:	<input type="checkbox"/> Authorization			
Service Rule				
Matches <input checked="" type="radio"/> ANY or <input type="radio"/> ALL of the following conditions:				
Type	Name	Operator	Value	
1.	Click to add...			

Note that we are also adding the AD authentication source as we'll be doing AD lookup for some of the TACACS users.

Summary	Service	Authentication	Roles	Enforcement
Authentication Sources:	<div> <div>[Local User Repository] [Local SQL DB]</div> <div>Ariya AD [Active Directory]</div> <div>Move Up ↑</div> <div>Move Down ↓</div> <div>Remove</div> <div>View Details</div> <div>Modify</div> </div> <div>Add New Authentication Source</div>			
Strip Username Rules:	<input type="checkbox"/> Enable to specify a comma-separated list of rules to strip username prefixes or suffixes			

Summary	Service	Authentication	Roles	Enforcement				
Role Mapping Policy:	--Select-- Add new Role Mapping Policy							
Role Mapping Policy Details								
Description:	-							
Default Role:	-							
Rules Evaluation Algorithm:	-							
<table border="1"> <thead> <tr> <th>Conditions</th> <th>Role</th> </tr> </thead> <tbody> <tr> <td colspan="2"> </td> </tr> </tbody> </table>					Conditions	Role		
Conditions	Role							

Summary	Service	Authentication	Roles	Enforcement										
Use Cached Results:	<input type="checkbox"/> Use cached Roles and Posture attributes from previous sessions													
Enforcement Policy:	Modified Aruba Device Access Policy Add New Enforcement Policy													
Enforcement Policy Details														
Description:	Enforcement policy controlling access to Aruba device													
Default Profile:	[ArubaOS Wireless - TACACS Read-Only Access]													
Rules Evaluation Algorithm:	first-applicable													
<table border="1"> <thead> <tr> <th>Conditions</th> <th>Enforcement Profiles</th> </tr> </thead> <tbody> <tr> <td>1. (Tips:Role MATCHES_ANY [Aruba TACACS root Admin])</td> <td>[ArubaOS Wireless - TACACS Root Access]</td> </tr> <tr> <td>2. (Tips:Role MATCHES_ANY [Aruba TACACS read-only Admin])</td> <td>[ArubaOS Wireless - TACACS Read-Only Access]</td> </tr> <tr> <td>3. (Tips:Role EQUALS Netedit)</td> <td>Ariya TACACS netadmin</td> </tr> <tr> <td>4. (Authorization:Ariya AD:Nested Groups CONTAINS Staff)</td> <td>Ariya TACACS netadmin</td> </tr> </tbody> </table>					Conditions	Enforcement Profiles	1. (Tips:Role MATCHES_ANY [Aruba TACACS root Admin])	[ArubaOS Wireless - TACACS Root Access]	2. (Tips:Role MATCHES_ANY [Aruba TACACS read-only Admin])	[ArubaOS Wireless - TACACS Read-Only Access]	3. (Tips:Role EQUALS Netedit)	Ariya TACACS netadmin	4. (Authorization:Ariya AD:Nested Groups CONTAINS Staff)	Ariya TACACS netadmin
Conditions	Enforcement Profiles													
1. (Tips:Role MATCHES_ANY [Aruba TACACS root Admin])	[ArubaOS Wireless - TACACS Root Access]													
2. (Tips:Role MATCHES_ANY [Aruba TACACS read-only Admin])	[ArubaOS Wireless - TACACS Read-Only Access]													
3. (Tips:Role EQUALS Netedit)	Ariya TACACS netadmin													
4. (Authorization:Ariya AD:Nested Groups CONTAINS Staff)	Ariya TACACS netadmin													

Here is the final Service

Dashboard

Monitoring

Configuration

Service Templates & Wizards

Services

Authentication

Identity

Posture

ClearPass Policy Manager

Menu

Configuration » Services

Services

Filter: Name contains

Go

Clear Filter

Show 20 records

#

Order

Name

Type

Template

Status

1.

1

[Policy Manager Admin Network Login Service]

TACACS

TACACS+ Enforcement

2.

2

[AirGroup Authorization Service]

RADIUS

RADIUS Enforcement (Generic)

3.

3

[Aruba Device Access Service]

TACACS

TACACS+ Enforcement

4.

4

Modified Aruba Device Access Service

TACACS

TACACS+ Enforcement

5.

5

[Guest Operator Logins]

Application

Aruba Application Authentication

6.

6

[Insight Operator Logins]

Application

Aruba Application Authentication

The enforcement policy uses the “Ariya TACACS Netadmin” enforcement profile.

Summary

Profile

Services

Commands

Name:

Ariya TACACS netadmin

Description:

profile for root access to aruba devices

Type:

TACACS

Action:

☒ Accept

☐ Reject

☐ Drop

Device Group List:

--Select--

Remove

View Details

Modify

Add New Device Group

Summary

Profile

Services

Commands

Privilege Level:

15 (Privileged)

Selected Services:

Shell

--Select--

Remove

Export All TACACS+ Services Dictionaries

Authorize Attribute Status:

ADD

Custom Services:

To add new TACACS+ services / attributes, upload the modified dictionary xml - Update TACACS+ Services Dictionary

Service Attributes

Type	Name	=	Value			
1.	Shell	priv-lvl	=	15		
2.	Click to add...					

Summary

Profile

Services

Commands

Service Type:

☒ Shell

☐ PIX Shell

Unmatched Commands:

☐ Enable to permit unmatched commands

Commands

Specify which commands with arguments are permitted/denied

Add

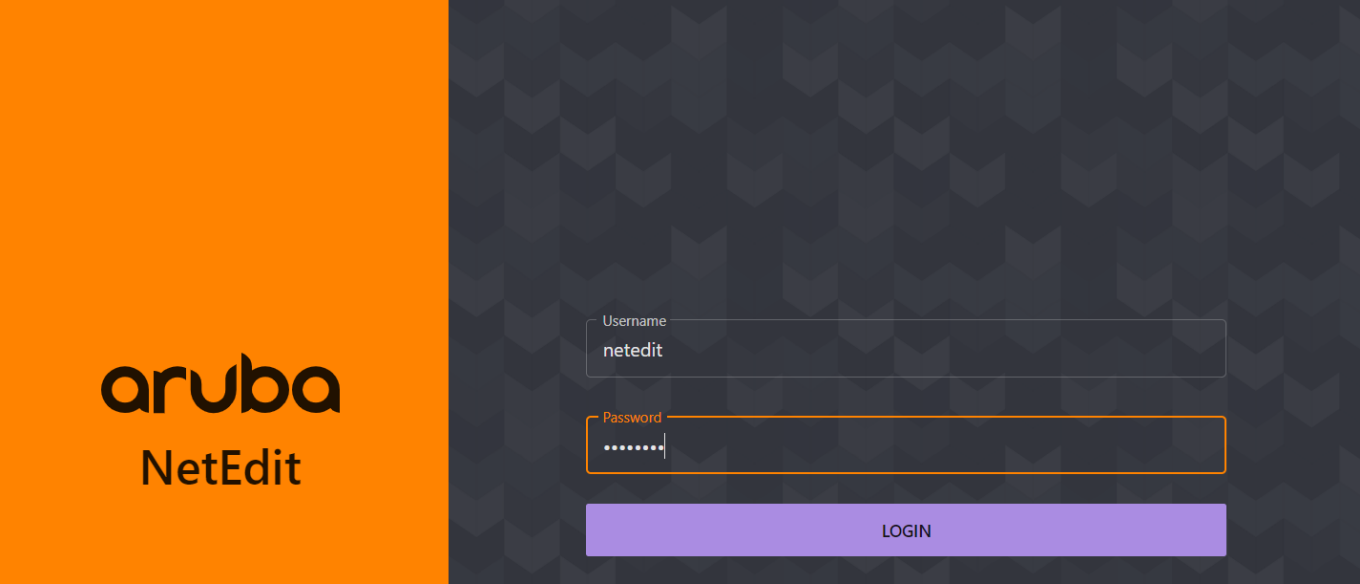
Command	Arguments	Permit Action	Unmatched Arguments
---------	-----------	---------------	---------------------

5 Testing

In this section we'll test both the local users we have defined in ClearPass as well as using AD as authentication source.

5.1 Local user Authentication

First, we login with "netedit" credentials.



This is from ClearPass access tracker.

TACACS+ Session Details	
Summary	Request Policies Authorizations
Session ID:	T0000000f-01-60939ae4
Username:	netedit
Time:	May 06, 2021 17:29:41 AEST
Status:	AUTHEN_STATUS_PASS
Authorizations:	1


TACACS+ Session Details	
Summary	Request
Username:	netedit
Session ID:	T0000000f-01-60939ae4
Time:	May 06, 2021 17:29:41 AEST
Status:	AUTHEN_STATUS_PASS
Request Type:	TACACS_AUTHENTICATION
Message:	-
Client IP:	192.168.1.90
Remote IP:	localhost
Computed Attributes	
Authentication:Status	User
Authentication:TacacsAuthService	AUTHEN_SVC_NONE
Connection:NAD-IP-Address	192.168.1.90
Connection:Protocol	TACACS
Tacacs:AuthSource	[Local User Repository]

Summary	Request
Policies Used -	
Service Name:	Modified Aruba Device Access Service
Authentication Source:	[Local User Repository]
Role:	[User Authenticated], Netedit
Profiles:	Ariya TACACS netadmin

TACACS+ Session Details		
Summary	Request	Authorizations
Commands Used	Status	Request Time
shell exec	Pass	May 06, 2021 17:29:41 AEST

5.2 AD User Authentication

Now we login with staff1 credentials that is a member of "Staff" group in AD.



Username
 staff1

Password

LOGIN

<

We have a successful login, lets have a look at ClearPass access tracker.

TACACS+ Session Details	
Summary	Request Policies Authorizations Alerts
Session ID:	T0000000a-01-609a16cc
Username:	staff1
Time:	May 11, 2021 15:31:56 AEST
Status:	AUTHEN_STATUS_PASS
Authorizations:	1

Summary	Request Policies Authorizations Alerts
Username:	staff1
Session ID:	T0000000a-01-609a16cc
Time:	May 11, 2021 15:31:56 AEST
Status:	AUTHEN_STATUS_PASS
Request Type:	TACACS_AUTHENTICATION
Message:	-
Client IP:	192.168.1.90
Remote IP:	localhost
Computed Attributes	
Authentication:Status	User
Authentication:TacacsAuthService	AUTHEN_SVC_NONE
Connection:NAD-IP-Address	192.168.1.90
Connection:Protocol	TACACS
Tacacs:AuthSource	Ariva AD

Summary	Request Policies Authorizations Alerts
Time:	May 11, 2021 15:31:56 AEST
Status:	AUTHEN_STATUS_PASS
Request Type:	TACACS_AUTHENTICATION
Message:	-
Client IP:	192.168.1.90
Remote IP:	localhost
Computed Attributes	
Authorization Attributes	
Authorization:Ariya AD:Account Expires	9223372036854775807
Authorization:Ariya AD:Name	staff1
Authorization:Ariya AD:Nested Groups	Administrators, Staff
Authorization:Ariya AD:UserDN	CN=staff1,CN=Users,DC=wlan,DC=net
Authorization:Ariya AD:memberOf	CN=Administrators,CN=Builtin,DC=wlan,DC=net,CN=Staff,CN=Users,DC=wlan,DC=net

Summary	Request	Policies	Authorizations	Alerts
Policies Used -				
Service Name:	Modified Aruba Device Access Service			
Authentication Source:	Ariya AD			
Role:	Staff, [User Authenticated], Administrators			
Profiles:	Ariya TACACS netadmin			

Summary	Request	Policies	Authorizations	Alerts
Commands Used	Status	Request Time		
shell exec	Pass	May 11, 2021 15:31:56 AEST		

Summary	Request	Policies	Authorizations	Alerts
Authentication Request Messages				
Alerts for this Request:				
Tacacs server	User 'staff1' not present in [Local User Repository](localhost)			