Contents

Introduction

This document provides details of configuring the Wide Area Application (WAAS) Express/APPNAV-XE using Terminal Access Controller Access Control Systems (TACACS) and Authentication, Authorization and Accounting (AAA) command authorization.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco WAAS
- AAA authorization
- TACACS

Components Used

The information in this document is based on these software and hardware versions:

- WAAS 6.1.1x
- 2900 Routers
- IOS Versoin 15.2(4)M3

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information

The WAAS Central Manager requires Secure Shell (SSH) and Secure HTTPS in order to access WAAS Express and APPNAV - XE routers.

Secure Shell (SSH) is used for initial configuration/registratoin.

HTTPS is used for ongoing configuration and monitoring.

Often the combination of HTTPS and AAA configuration on the device prevents the central manager from communicating with these devices correctly.

Example TACACs setup

```
aaa new-model
!
!
aa group server tacacs+ tacacsgroup
 server name server1
 server name server2

aaa authentication login AUTH group AAA-Servers
aaa authorization commands 1 PRIV1 group AAA-Servers
aaa authorization commands 15 PRIV15 group AAA-Servers
aaa authorization exec AUTHLIST group AAA-Servers
```

Example HTTPS configuration

```
aaa new-model
!
!
aa group server tacacs+ tacacsgroup
 server name server1
 server name server2

aaa authentication login AUTH group AAA-Servers
aaa authorization commands 1 PRIV1 group AAA-Servers
aaa authorization commands 15 PRIV15 group AAA-Servers
aaa authorization exec AUTHLIST group AAA-Servers
```

Commands run by CM on WAAS Express/APPNAV-XE via HTTP

This is a list of the commands that the central manager needs in order to be able to run on the remote device.

Config Mode CLIs

```
aaa new-model
!
```

```
!
aa group server tacacs+ tacacsgroup
 server name server1
 server name server2

aaa authentication login AUTH group AAA-Servers
aaa authorization commands 1 PRIV1 group AAA-Servers
aaa authorization commands 15 PRIV15 group AAA-Servers
aaa authorization exec AUTHLIST group AAA-Servers
```

EXEC Mode CLIs

WAASX - Status

```
aaa new-model
!
!
aa group server tacacs+ tacacsgroup
 server name server1
 server name server2

aaa authentication login AUTH group AAA-Servers
aaa authorization commands 1 PRIV1 group AAA-Servers
aaa authorization commands 15 PRIV15 group AAA-Servers
aaa authorization exec AUTHLIST group AAA-Servers
```

WAASX - Configuration

```
aaa new-model
!
!
aa group server tacacs+ tacacsgroup
 server name server1
 server name server2

aaa authentication login AUTH group AAA-Servers
aaa authorization commands 1 PRIV1 group AAA-Servers
aaa authorization commands 15 PRIV15 group AAA-Servers
aaa authorization exec AUTHLIST group AAA-Servers
```

WAASX - Statistics

```
aaa new-model
!
!
aa group server tacacs+ tacacsgroup
 server name server1
 server name server2

aaa authentication login AUTH group AAA-Servers
aaa authorization commands 1 PRIV1 group AAA-Servers
aaa authorization commands 15 PRIV15 group AAA-Servers
aaa authorization exec AUTHLIST group AAA-Servers
```

Registration

```
aaa new-model
!
!
aa group server tacacs+ tacacsgroup
 server name server1
 server name server2

aaa authentication login AUTH group AAA-Servers
aaa authorization commands 1 PRIV1 group AAA-Servers
aaa authorization commands 15 PRIV15 group AAA-Servers
aaa authorization exec AUTHLIST group AAA-Servers
```

AppNav-XE

```
aaa new-model
!
!
aa group server tacacs+ tacacsgroup
 server name server1
 server name server2

aaa authentication login AUTH group AAA-Servers
aaa authorization commands 1 PRIV1 group AAA-Servers
aaa authorization commands 15 PRIV15 group AAA-Servers
aaa authorization exec AUTHLIST group AAA-Servers
```

Troubleshoot

Incorrect AAA or HTTP configuration on the end device can cause failures in registration and status update failures.

> **Note**: The simplest way to test if there is an authorization issue is to setup a local WAAS user, local AAA authentication and **ip http authentication local**. If this test configuration works it means you likely have an issue with your remote user command authorization.

On WAAS Central Manager CLI

Confirm that you can ssh from the CM CLI to the remote device.

```
aaa new-model
!
!
aa group server tacacs+ tacacsgroup
 server name server1
 server name server2

aaa authentication login AUTH group AAA-Servers
aaa authorization commands 1 PRIV1 group AAA-Servers
aaa authorization commands 15 PRIV15 group AAA-Servers
aaa authorization exec AUTHLIST group AAA-Servers
```

enable cms debug on CM and review the **cms.log** and **waasx-audit.log** files during registration, pushing out config and statistic gathering.

```
# debug cms waasx-regis
# debug cms router-config
# debug cms stats
(config)# logging disk priority 7
  # cd errorlog
```
 # type-tail cms.log follow
 # type-tail waasx-audit.log follow

Example log entries when the CM fails to push commands to WAAS-Express or AppNav-XE.

```
05/27/2016 00:14:03.760 [I] cdm(RtrSync-40) Configuration commands failed on the device
CeConfig_2875943/USNY25W39-R02. Not Taking backup of complete device configuration.
05/27/2016 00:14:03.774 [W] cdm(RtrSync-64) 700001 Failed configuration commands are ...
05/27/2016 00:14:03.774 [W] cdm(RtrSync-64) 700001
class-map type appnav match-any HTTPS
CLI:class-map type appnav match-any HTTPS
Status:8
Output:Command authorization failed.
```

Test HTTPS access from browser

You can log in to the HTTP interface.

https://<IP_ADDRESS>/level/15/exec/-/

Home   Exec   Configure

Command [   ]

Output

Command base-URL was: /level/15/exec/-
Complete URL was:/level/15/exec/-

Exec commands:
NUMBER   1-1   [   ]

        Slot Number
access-enable
        Create a temporary Access-List entry
access-profile
        Apply user-profile to interface
access-template
        Create a temporary Access-List entry
archive
        manage archive files

Then type your commands into the `Command` section.

Example of a working **show invetory** command

Home   Exec   Configure

Command `show inventory`

Output

```
Command base-URL was: /level/15/exec/-
Complete URL was:/level/15/exec/-/show/inventory/CR
Command was: show inventory
```

```
NAME: "CISCO2911/K9", DESCR: "CISCO2911/K9 chassis, Hw Serial#: FTX1425A1AA, Hw
PID: CISCO2911/K9       , VID: V01 , SN: FTX1425A1AA

NAME: "High Speed Wan Interface Card with 4 serial ports(HWIC-4T) on Slot 0 SubS
PID: HWIC-4T            , VID: V01 , SN: FOC09023M5F

NAME: "Services Module with Services Ready Engine on Slot 1", DESCR: "Services M
PID: SM-SRE-900-K9      , VID: V03, SN: FOC15324NOL

NAME: "C2911 AC Power Supply", DESCR: "C2911 AC Power Supply"
PID: PWR-2911-AC        , VID: V01 , SN: AZS142220G4
```

command completed.

Example of a failing **show Inventory** command

Home   Exec   Configure

Command

Output

```
Command base-URL was: /level/15/exec/-
Complete URL was:/level/15/exec/-/show/inv/CR
Command was: show inv
```

```
Command authorization failed.
```

Debug on WAAS Express router

#debug aaa authorization

Command running successfully

```
Jul  5 07:09:19.161: AAA/AUTHOR/TAC+: (2935402750): user=waasx
Jul  5 07:09:19.161: AAA/AUTHOR/TAC+: (2935402750): send AV service=shell
Jul  5 07:09:19.161: AAA/AUTHOR/TAC+: (2935402750): send AV cmd=show
Jul  5 07:09:19.161: AAA/AUTHOR/TAC+: (2935402750): send AV cmd-arg=vrf
Jul  5 07:09:19.161: AAA/AUTHOR/TAC+: (2935402750): send AV cmd-arg=
Jul  5 07:09:19.365: AAA/AUTHOR (2935402750): Post authorization status = PASS_ADD
```

Authorization failure

```
Jul  5 07:08:32.485: AAA/AUTHOR/TAC+: (819547031): user=waasx
Jul  5 07:08:32.485: AAA/AUTHOR/TAC+: (819547031): send AV service=shell
Jul  5 07:08:32.485: AAA/AUTHOR/TAC+: (819547031): send AV cmd=show
Jul  5 07:08:32.485: AAA/AUTHOR/TAC+: (819547031): send AV cmd-arg=inventory
Jul  5 07:08:32.485: AAA/AUTHOR/TAC+: (819547031): send AV cmd-arg=
Jul  5 07:08:32.685: AAA/AUTHOR (819547031): Post authorization status = FAIL
```