使用AAA命令授權的WAAS Express/APPNAV XE

目錄

簡介

本文提供使用終端存取控制器存取控制系統(TACACS)和驗證、授權及計量(AAA)指令授權設定廣域應用(WAAS)Express/APPNAV-XE的詳細資訊。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco WAAS
- AAA授權
- TACACS

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- WAAS 6.1.1x

- 2900路由器
- IOS版本15.2(4)M3

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

WAAS中央管理器需要安全外殼(SSH)和安全HTTPS才能訪問WAAS Express和APPNAV - XE路由器。

安全殼層(SSH)用於初始設定/註冊。

HTTPS用於持續配置和監控。

通常，裝置上的HTTPS和AAA配置組合會阻止中央管理器與這些裝置正確通訊。

TACAC設定示例

```
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
```

HTTPS配置示例

```
ip http server
ip http authentication aaa exec-authorization AUTHLIST
ip http authentication aaa command-authorization 1 PRIV1 ip http authentication aaa command-authorization 15 PRIV15 ip http authentication aaa login-authentication AUTH ip http secure-server
ip http secure-trustpoint TP-self-signed-2945720990
ip http client source-interface GigabitEthernet0/0
ip http client secure-trustpoint TP-self-signed-2945720990
```

CM通過HTTP在WAAS Express/APPNAV-XE上運行的命令

這是中央管理器在遠端裝置上運行所需的命令清單。

配置模式CLI

```
do show running-config | section crypto pki trustpoint
crypto pki export
```

EXEC模式CLI

WAASX — 狀態

```
show waas token | format
show waas status | format
show waas alarms | format
show running-config | section hostname
show ip interface brief | format
show interfaces  | include line protocol | Internet address | address is | *uplex
show running-config brief | include clock timezone
show clock
show crypto pki trustpoints | include Trustpoint
show inventory
```

WAASX — 配置

```
show parameter-map type waas waas_global | format
show class-map type waas | format
show policy-map type waas | format
write memory
```

WAASX — 統計

```
show waas statistics peer | format
show waas statistics application | format
show waas connection brief
show waas statistics accelerator http-express | format
show waas statistics accelerator http-express https | format
show waas statistics accelerator ssl-express | format
show waas statistics class | format
show waas statistics accelerator cifs-express detail | format
```

註冊

```
registration
show waas status extended | format
```

AppNav-XE

```
show service-insertion token | format
show service-insertion status | format
show class-map type appnav | format
show ip int br | format
show service-insertion service-context | format
show service-insertion service-node-group | format
```

```
show service-insertion statistics service-node-group | format
show policy-map type appnav | format
show policy-map target service-context | format
show service-insertion config service-context | format
show service-insertion config service-node-group | format
show service-insertion config appnav-controller-group | format
show service-insertion alarms | format
show ip access-list
show vrf
show running-config | section interface
show running-config | include service-insertion swap src-ip
```

疑難排解

終端裝置上的AAA或HTTP配置不正確可能導致註冊失敗和狀態更新失敗。

> **附註**：測試是否存在授權問題的最簡單方法是設定本地WAAS使用者、本地AAA身份驗證和ip http authentication local。如果此測試配置有效，則意味著您的遠端使用者命令授權可能存在問題。

在WAAS Central Manager CLI上

確認可以從CM CLI通過ssh連線到遠端裝置。

```
#ssh <device-name>
```

在CM上啟用cms調試，並在註冊期間檢視**cms.log**和**waasx-audit.log**檔案，推出配置和統計資訊收集。

```
# 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
```

當CM無法向WAAS-Express或AppNav-XE推送命令時，日誌條目示例。

```
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.
```

HTTPS

您可以登入到HTTP介面。

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

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

然後在部分中鍵入命 Command 令。

工作show inventory命令示例

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.

show Inventory 命令失敗的示例

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.

在WAAS Express路由器上調試

#debug aaa authorization

命令運行成功

```
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
```

授權失敗

```
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
```

命令運行成功

授權失敗