

Aaa コマンド 許可を使用する WAAS Express/APPNAV XE

目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[例 TACACs 設定](#)

[HTTPS 設定例](#)

[コマンドは HTTP によって WAAS Express/APPNAV XE の CM によって動作します](#)

[コンフィギュレーションモード CLI](#)

[EXEC モード CLI](#)

[WAASX - 状態](#)

[WAASX - 設定](#)

[WAASX - 統計情報](#)

[登録](#)

[AppNav XE](#)

[トラブルシューティング](#)

[WAAS 中央マネージャ CLI](#)

[ブラウザから HTTPS アクセスをテストして下さい](#)

[WAAS Express ルータのデバッグ](#)

概要

この資料はターミナル アクセス コントローラ アクセスコントロールシステム (TACACS) を使用してワイドエリア アプリケーション (WAAS) Express/APPNAV XE の設定の詳細をおよび認証、許可および説明 (AAA) コマンド許可提供したものです。

前提条件

要件

次の項目に関する知識が推奨されます。

- Cisco WAAS
- AAA認証
- TACACS

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- WAAS 6.1.1x
- 2900 人のルータ
- IOS Versoin 15.2(4)M3

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

背景説明

WAAS 中央マネージャはセキュア シェル（SSH）および WAAS Express および APPNAV にアクセスするためにセキュア HTTPS が XE ルータ要求します。

セキュア シェル（SSH）は初期構成/registratoin のために使用されます。

HTTPS は進行中の設定 および モニタリングのために使用されます。

多くの場合デバイスの HTTPS および AAA設定の組み合わせは中央マネージャがこれらのデバイスと正しく交信することを防ぎます。

例 TACACs 設定

```
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 設定例

```
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
```

コマンドは HTTP によって WAAS Express/APPNAV XE の CM によって動作します

これはリモートデバイスで動作できるそのコマンドのリスト中央マネージャ必要があります

o

コンフィギュレーションモード CLI

```
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 モード CLI

WAASX - ステータス

```
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 - 設定

```
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 - 統計情報

```
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
```

登録

```
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
```

トラブルシューティング

端デバイスの不正確な AAA または HTTP 設定により登録およびステータスアップデート失敗で失敗を引き起こす場合があります。

注: 許可問題があればテストする最も簡単な方法はローカル WAAS ユーザ、ローカル AAA認証および ip http authentication ローカルを設定することです。このテスト設定が機能すればそれは多分リモートユーザ コマンド許可においての問題があることを意味します。

WAAS 中央マネージャ CLI

CM CLI からのリモートデバイスに ssh できることを確認して下さい。

```
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
```

CM の cms デバッグを有効にし、登録の間に cms.log および waasx-audit.log ファイルを検討し
ま、構成および統計情報収集を押し出します。

```
# 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
```

CM が WAAS Express か AppNav XE にコマンドを押さない場合の Log エントリ例。

```
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

HTTP インターフェイスにログインできます。

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

Output

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

Exec commands:

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

それからセクションにコマンドを 入力して下さい。

はたらく例は inventory コマンドを示したものです

Command

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: AZS14222OG4

command completed.

失敗の例はコンポーネント コマンドを示したものです

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 AAA認証

うまく働くコマンド

```
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
```

許可障害

```
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
```