WAAS Express/APPNAV XE使用aaa命令授权

Contents

Introduction

本文提供配置广域应用程序(WAAS) Express/APPNAV XE细节使用终端访问控制器访问控制系统(TACACS)和认证、授权和认为的(AAA) authorization命令。

Prerequisites

Requirements

Cisco 建议您了解以下主题：

- Cisco WAAS
- AAA授权
- TACACS

Components Used

本文档中的信息基于以下软件和硬件版本：

- WAAS 6.1.1x

- 2900路由器
- 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.

背景信息

WAAS中央管理器要求安全壳SSH和安全的HTTPS为了访问WAAS Express和APPNAV - XE路由器。

安全壳SSH使用初始配置/registratoin。

HTTPS使用持续的配置和监视。

通常HTTPS和AAA配置的组合在设备防止中央管理器正确通信与这些设备。

示例TACACS设置

```
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
```

示例HTTPS配置

```
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
```

命令由在WAAS Express/APPNAV XE的CM负责通过HTTP

这是中央管理器在远端设备需要为了能运作命令的列表。

配置模式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模式CLIs

WAASX -状态

```
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 -配置

```
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 -统计数据

```
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
```

注册

```
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

在终端设备的不正确AAA或HTTP配置能的注册和状态更新故障导致故障。

> Note:简单方法测试，如果有授权问题将设置一本地WAAS用户、本地AAA认证和IP HTTP认证本地。如果此测试配置工作意味着您可能有您的远程user命令授权的一个问题。

在WAAS中央管理器CLI

确认您能从CM CLI的SSH到远端设备。

```
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 (event)在CM的cms调试和在注册时查看**cms.log**和**waasx-audit.log**文件，推出设置和统计数据收集。

```
# 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
```

示例日志条目，当CM不能推进WAAS快速的命令或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.
```

HTTPS

您能登陆到HTTP接口。

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

然后请键入您的命令到 Command 部分。

工作的示例显示invetory命令

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.

失败的示例显示库存命令

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.

调试在WAAS Express路由器

#debug AAA授权

成功Running命令

```
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
```

认证失败

```
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
```