使用CLI更改Catalyst 1300交換機中授權的基本配置

目標

本文的目的是顯示如何使用命令列介面(CLI)在Catalyst 1300交換機中執行授權更改(CoA)功能的基本配置。

適用的裝置和軟體版本

- Catalyst 1300交換器 | 4.1.3.36

簡介

授權變更(CoA)是RADIUS通訊協定的延伸，允許您在驗證之後變更驗證、授權和記帳(AAA)或dot1x使用者作業階段的屬性。當AAA中的使用者或組的策略更改時，管理員可以從AAA伺服器(例如Cisco身份服務引擎(ISE))傳輸RADIUS CoA資料包，以重新初始化身份驗證並應用新策略。

思科身份服務引擎（或ISE）是一個功能全面的基於網路的訪問控制和策略實施引擎。它提供安全分析和實施、RADIUS和TACACS服務、策略分發等。Cisco ISE是目前唯一支援Catalyst 1300交換機的CoA動態授權客戶端。有關詳細資訊，請參閱ISE管理員指南。

韌體版本4.1.3.36中的Catalyst 1300交換機已增加CoA支援。這包括支援中斷使用者連線，以及變更適用於使用者工作階段的授權。裝置支援以下CoA操作：

- 斷開會話
- 停用主機埠CoA命令
- 退回主機埠CoA命令
- 重新驗證主機CoA命令

在本文中，您將使用CLI在Catalyst 1300交換機中找到基本CoA配置的命令。這些步驟可能因使用者設定和要求而異。

目錄

使用CLI進行基本CoA配置

設定RADIUS伺服器和RADIUS記帳

要配置RADIUS伺服器，請在全局配置模式下使用以下命令：

步驟 1

使用radius-server key 命令為裝置和RADIUS守護程式之間的RADIUS通訊設定身份驗證金鑰。

```
radius-server key
```

步驟 2

使用radius-server host 命令配置RADIUS伺服器主機。

```
radius-server host key priority 1 usage dot1.x
```

- IP地址將是ISE伺服器IP地址。
- key <key-string> -為裝置和RADIUS伺服器之間的所有RADIUS通訊指定身份驗證和加密金鑰。此金鑰必須與RADIUS守護程式上使用的加密匹配。
- Priority -指定伺服器的使用順序，其中0具有最高優先順序。(範圍：0-65535)
- usage dot1.x -指定RADIUS伺服器用於802.1x埠身份驗證。

步驟 3

```
aaa accounting dot1x start-stop group radius
```

配置動態授權伺服器

步驟 1

在全局配置模式下，運行以下命令進入CoA配置模式：

```
aaa server radius dynamic-author
```

步驟 2

要配置在裝置和CoA客戶端之間共用的RADIUS金鑰（範圍：0-128個字元），請在動態授權本地伺服器配置模式下使用命令server-key <key-string>。CoA請求中提供的金鑰必須與此金鑰匹配。

```
server-key
```

> Note:
> 對於ISE，金鑰字串將與您在配置RADIUS時為RADIUS伺服器金鑰字串指定的金鑰字串相同。

步驟 3

輸入Coa客戶端主機IP地址。IP地址可以是IPv4、IPv6或IPv6z地址。

```
client
```

步驟 4

```
Exit
```

設定802.1x

要全局啟用802.1X，請使用dot1x system-auth-control命令。

```
dot1x system-auth-control
```

在埠上配置802.1x

步驟 1

輸入介面配置，並使用命令interface GigabitEthernet<Interface ID>選擇介面ID。

```
interface gi1/0/1
```

步驟 2

要啟用埠授權狀態的手動控制，請使用dot1x port-control命令。自動模式會啟用連線埠上的802.1X驗證，並根據裝置與使用者端之間的802.1X驗證交換，使其轉換到授權或未授權狀態。

```
dot1x port-control auto
```

步驟 3

要對啟用802.1X的所有埠或指定的802.1X埠啟動手動重新身份驗證，請在特權EXEC模式下使用dot1x re-authenticate命令。

```
dot1x re-authenticate gi1/0/1
```

步驟 4

要配置埠安全學習模式，請使用port security mode Interface (Ethernet， Port Channel)配置模式命令。Secure delete-on-reset引數是一種安全模式，其學習安全MAC地址有限，且生存壽命為delete-on-reset。

```
port security mode secure delete-on-reset
```

步驟 5

要退出介面配置，請輸入以下命令：

```
exit
```

CoA配置的其他命令

以下是一些可根據您的配置和設定使用的其他CoA命令。

- attribute event-timestamp drop-packet -此命令用於動態授權本地伺服器配置模式，以將裝置配置為丟棄斷開連線資料包(PoD)請求或不包括事件時間戳屬性的CoA請求。

```
attribute event-timestamp drop-packet
```

- authentication command bounce-port ignore -要配置裝置以忽略RADIUS授權更改(CoA)退回埠命令，請在全局配置模式下使用authentication命令bounce-port ignore命令。

```
authentication command bounce-port ignore
```

- authentication command disable-port ignore -要配置裝置以忽略RADIUS CoA disable-port命令，請在全局配置模式下使用此命令。

```
authentication command disable-port ignore
```

- domain delimiter <character> -要配置接收的PoD和CoA請求的使用者名稱域分隔器，請在動態授權本地伺服器配置模式下使用domain delimiter命令。

```
domain delimiter $
```

在本示例中，$字元被配置為分隔符。

- domain stribing [right-to-left] -要啟用和定義已接收的PoD和CoA請求的使用者名稱域剝離行為，請在動態授權本地伺服器配置模式下使用domain stribing命令。

```
domain stripping right-to-left
```

- ignore server-key -此命令用於動態授權本地伺服器配置模式，用於將裝置配置為忽略CoA伺服器

金鑰。

```
ignore server-key
```

特權執行模式下的CLI命令

從特權執行模式，您可以在經過身份驗證的客戶端上運行show命令、清除客戶端計數器以及顯示動態授權伺服器配置。

- 使用show aaa clients顯示AAA (CoA)客戶端的統計資訊。

```
show aaa clients
```

- 使用show aaa server radius dynamic-author命令顯示CoA配置。

```
show aaa server radius dynamic-author
```

- clear aaa counters可用於清除aaa客戶端計數器

```
clear aaa clients counters
```

結論

現在，您已經使用CLI完成了Catalyst 1300交換機中的基本授權更改(CoA)配置。

有關Catalyst 1300交換機的CLI命令的詳細資訊，請參閱Cisco Catalyst 1300交換機系列CLI指南。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。