使用CLI对Catalyst 1300交换机的授权更改进行基本配置

目标

本文旨在向您展示如何使用命令行界面(CLI)在Catalyst 1300交换机中执行授权更改(CoA)功能的基本配置。

适用设备和软件版本

- Catalyst 1300 交换机 | 4.1.3.36

简介

授权更改(CoA)是RADIUS协议的扩展，允许您在身份验证、授权和记帐(AAA)或dot1x用户会话之后，更改其属性。当AAA中用户或组的策略更改时，管理员可以从AAA服务器（例如思科身份服务引擎[ISE]）传输RADIUS CoA数据包，以重新初始化身份验证并应用新策略。

思科身份服务引擎（或ISE）是一个功能全面的基于网络的访问控制和策略实施引擎。它提供安全分析和实施、RADIUS和TACACS服务、策略分发等。思科ISE目前是Catalyst 1300交换机唯一支持的CoA动态授权客户端。有关详细信息，请参阅ISE管理员指南。

固件版本4.1.3.36中的Catalyst 1300交换机已添加了CoA支持。这包括支持断开用户连接以及更改适用于用户会话的授权。设备支持以下CoA操作：

- 断开会话
- 禁用主机端口CoA命令
- 退回主机端口CoA命令
- 重新验证主机CoA命令

在本文中，您将使用CLI查找Catalyst 1300交换机中的基本CoA配置的命令。这些步骤可能因用户设置和要求而异。

目录

使用CLI进行基本CoA配置

设置RADIUS服务器和RADIUS记帐

要从全局配置模式配置RADIUS服务器，请使用以下命令：

第 1 步

请使用radius-server key命令设置设备与RADIUS后台程序之间RADIUS通信的身份验证密钥。

```
radius-server key
```

步骤 2

使用radius-server host命令配置RADIUS服务器主机。

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

- IP地址将是ISE服务器的IP地址。
- key <key-string> -为设备和RADIUS服务器之间的所有RADIUS通信指定身份验证和加密密钥。此密钥必须与RADIUS守护程序上使用的加密相匹配。
- Priority -指定服务器的使用顺序，其中0具有最高优先级。(范围：0-65535)
- usage dot1.x -指定RADIUS服务器用于802.1x端口身份验证。

步骤 3

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

配置动态授权服务器

第 1 步

在全局配置模式下，运行命令进入CoA配置模式：

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

步骤 2

要配置在设备与CoA客户端之间共享的RADIUS密钥（范围：0-128个字符），请在动态授权本地服务器配置模式下使用命令server-key <key-string>。CoA请求中提供的密钥必须与此密钥匹配。

```
server-key
```

> Note:
> 对于ISE，密钥字符串与您配置RADIUS时为RADIUS服务器key-string指定的密钥字符串相同。

步骤 3

输入CoA客户端主机IP地址。IP地址可以是IPv4、IPv6或IPv6z地址。

```
client
```

步骤 4

```
Exit
```

配置802.1x

要全局启用802.1X，请使用dot1x system-auth-control命令。

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

在端口上配置802.1x

第 1 步

输入接口配置，然后使用命令interface GigabitEthernet<Interface ID>选择接口ID。

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

步骤 2

要启用端口授权状态的手动控制，请使用dot1x port-control命令。根据设备和客户端之间的802.1X身份验证交换，自动模式在端口上启用802.1X身份验证，并使其转换到授权或未经授权状态。

```
dot1x port-control auto
```

步骤 3

要启动所有启用802.1X的端口或指定的启用802.1X的端口的手动重新身份验证，请在特权EXEC模式下使用dot1x re-authenticate命令。

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

步骤 4

要配置端口安全学习模式，请使用端口安全模式接口（以太网、端口通道）配置模式命令。Secure delete-on-reset参数是一种安全模式，其学习安全MAC地址有限，并且存在重置时删除。

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

步骤 5

要退出接口配置，请输入以下命令：

```
exit
```

用于CoA配置的其他命令

以下是一些可根据您的配置和设置使用的其他CoA命令。

- attribute event-timestamp drop-packet -此命令用于动态授权本地服务器配置模式，以配置设备放弃不包括event-timestamp属性的Packet of Disconnect (PoD)请求或CoA请求。

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

- authentication command bounce-port ignore -要配置设备以忽略RADIUS授权更改(CoA)退回端口命令，请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 -要配置设备以忽略RADIUS CoA disable-port命令，请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请求的用户名域分隔符，请在动态授权本地服务器配置模式下使用domain delimiter命令。

```
domain delimiter $
```

在本示例中，$字符被配置为分隔符。

- domain stripping [right-to-left] -要启用和定义所接收PoD和CoA请求的用户名域剥离行为，请在动态授权本地服务器配置模式下使用domain stripping命令。

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

- ignore server-key -此命令用于动态授权本地服务器配置模式，将设备配置为忽略CoA服务器密钥

。

```
ignore server-key
```

特权执行模式下的CLI命令

从特权EXEC模式，您可以在通过身份验证的客户端上运行show命令，清除客户端计数器，并显示动态授权服务器配置。

- 使用show aaa clients显示AAA (CoA)客户端的统计信息。

```
show aaa clients
```

- 使用show aaa server radius dynamic-author命令显示CoA配置。

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

- clear aaa counters可用于清除aaa客户端计数器

```
clear aaa clients counters
```

结论

现在，您已经使用CLI在Catalyst 1300交换机中完成了基本的授权更改(CoA)配置。

有关Catalyst 1300交换机CLI命令的详细信息，请参阅Cisco Catalyst 1300交换机系列CLI指南。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。