Grundlegende Konfiguration der Autorisierungsänderung in Catalyst 1300 Switch über CLI

Ziel

In diesem Artikel wird erläutert, wie Sie eine grundlegende Konfiguration der Funktion zur Autorisierungsänderung (Change of Authorization, CoA) an Catalyst 1300-Switches über die Kommandozeile (Command Line Interface, CLI) durchführen.

Anwendbare Geräte und Softwareversion

- Catalyst Switches der Serie 1300 | 4.1.3.36

Einleitung

Change of Authorization (CoA) ist eine Erweiterung des RADIUS-Protokolls, mit dem Sie die Eigenschaften einer AAA- (Authentication, Authorization, Accounting) oder dot1x-Benutzersitzung nach deren Authentifizierung ändern können. Wenn sich eine Richtlinie für einen Benutzer oder eine Gruppe in AAA ändert, können Administratoren RADIUS-CoA-Pakete vom AAA-Server, z. B. von der Cisco Identity Services Engine (ISE), übertragen, um die Authentifizierung neu zu initialisieren und die neue Richtlinie anzuwenden.

Die Cisco Identity Services Engine (oder ISE) ist eine Network Based Access Control and Policy Enforcement Engine mit vollem Funktionsumfang. Sie bietet Sicherheitsanalysen und -durchsetzung, RADIUS- und TACACS-Services, Richtlinienverteilung und vieles mehr. Die Cisco ISE ist derzeit der einzige unterstützte CoA Dynamic Authorization Client für Catalyst 1300-Switches. Weitere Informationen finden Sie im ISE-Administratorhandbuch.

Die CoA-Unterstützung wurde den Catalyst 1300-Switches in der Firmware-Version 4.1.3.36 hinzugefügt. Dazu gehört die Unterstützung für das Trennen von Benutzern und das Ändern von Berechtigungen für eine Benutzersitzung. Das Gerät unterstützt die folgenden CoA-Aktionen:

- Sitzung trennen
- Host-Port-CoA-Befehl deaktivieren
- CoA-Befehl für Bounce-Host-Port
- CoA-Befehl für Host erneut authentifizieren

In diesem Artikel finden Sie die Befehle für eine grundlegende CoA-Konfiguration in Catalyst 1300-Switches über CLI. Die Schritte können je nach Benutzereinstellungen und -anforderungen variieren.

Inhalt

CoA-Basiskonfiguration mit CLI

RADIUS-Server und RADIUS-Accounting einrichten

Verwenden Sie die folgenden Befehle, um den RADIUS-Server im globalen Konfigurationsmodus zu konfigurieren:

Schritt 1

Verwenden Sie den Befehl radius-server key, um den Authentifizierungsschlüssel für die RADIUS-Kommunikation zwischen dem Gerät und dem RADIUS-Daemon festzulegen.

```
radius-server key
```

Schritt 2

Verwenden Sie den Befehl radius-server host, um einen RADIUS-Serverhost zu konfigurieren.

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

- Bei der IP-Adresse handelt es sich um die IP-Adresse des ISE-Servers.
- key <key-string> - Gibt den Authentifizierungs- und Verschlüsselungsschlüssel für die gesamte RADIUS-Kommunikation zwischen dem Gerät und dem RADIUS-Server an. Dieser Schlüssel muss mit der im RADIUS-Daemon verwendeten Verschlüsselung übereinstimmen.
- Priorität - Gibt die Reihenfolge an, in der Server verwendet werden, wobei 0 die höchste Priorität hat. (Bereich: 0-65535)
- usage dot1.x - gibt an, dass der RADIUS-Server für die 802.1x-Port-Authentifizierung verwendet wird.

Schritt 3

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

Dynamischen Autorisierungsserver konfigurieren

Schritt 1

Wechseln Sie im globalen Konfigurationsmodus in den CoA-Konfigurationsmodus, indem Sie den folgenden Befehl ausführen:

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

Schritt 2

Um den RADIUS-Schlüssel für die gemeinsame Nutzung durch das Gerät und einen CoA-Client (Bereich: 0-128 Zeichen) zu konfigurieren, verwenden Sie den Befehl server-key <key-string> im Konfigurationsmodus für den lokalen Server mit dynamischer Autorisierung. Der in der CoA-Anfrage angegebene Schlüssel muss mit diesem übereinstimmen.

```
server-key
```

> **Note:**
> Bei ISE ist die Schlüsselzeichenfolge die gleiche, die Sie bei der Konfiguration von RADIUS für die Schlüsselzeichenfolge des RADIUS-Servers angegeben haben.

Schritt 3

Geben Sie die IP-Adresse des CoA-Client-Hosts ein. Bei der IP-Adresse kann es sich um eine IPv4-, IPv6- oder IPv6z-Adresse handeln.

```
client
```

Schritt 4

```
Exit
```

Konfigurieren von 802.1x

Um 802.1x global zu aktivieren, verwenden Sie den Befehl dot1x system-auth-control.

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

Konfigurieren von 802.1x auf einem Port

Schritt 1

Geben Sie die Schnittstellenkonfiguration ein, und wählen Sie die Schnittstellen-ID mithilfe der Befehlsschnittstelle GigabitEthernet<Schnittstellen-ID> aus.

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

Schritt 2

Um die manuelle Steuerung des Port-Autorisierungsstatus zu aktivieren, verwenden Sie den Befehl dot1x port-control. Der Auto-Modus aktiviert die 802.1X-Authentifizierung am Port und veranlasst, dass diese basierend auf dem 802.1X-Authentifizierungsaustausch zwischen dem Gerät und dem Client in den autorisierten oder nicht autorisierten Status wechselt.

```
dot1x port-control auto
```

Schritt 3

Um eine manuelle Neuauthentifizierung aller 802.1X-aktivierten Ports oder des angegebenen 802.1X-aktivierten Ports zu initiieren, verwenden Sie den Befehl dot1x re-Authenticate im privilegierten EXEC-Modus.

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

Schritt 4

Um den Port-Sicherheitslernmodus zu konfigurieren, verwenden Sie den Konfigurationsmodusbefehl port security mode Interface (Ethernet, Port Channel). Der Parameter für sicheres Löschen beim Zurücksetzen ist ein sicherer Modus mit eingeschränktem Lernen und sicheren MAC-Adressen mit der Lebensdauer für das Löschen beim Zurücksetzen.

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

Schritt 5

Geben Sie zum Beenden der Schnittstellenkonfiguration Folgendes ein:

```
exit
```

Weitere Befehle für die CoA-Konfiguration

Im Folgenden sind einige weitere CoA-Befehle aufgeführt, die je nach Konfiguration und Einrichtung verwendet werden können.

- attribute event-timestamp drop-packet - Dieser Befehl wird im Konfigurationsmodus für den

lokalen Server mit dynamischer Autorisierung verwendet, um das Gerät so zu konfigurieren, dass es eine PoD-Anforderung (Packet of Disconnect) oder CoA-Anforderung verwirft, die kein Ereignis-timestamp-Attribut enthält.

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

- authentication-Befehl bounce-Port ignore - Um das Gerät so zu konfigurieren, dass ein RADIUS-Befehl zum Ändern der Autorisierung (CoA) des Bounce-Ports ignoriert wird, verwenden Sie den Befehl authentication bounce-port ignore im globalen Konfigurationsmodus.

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

- authentication-Befehl disable-port ignore - Verwenden Sie diesen Befehl im globalen Konfigurationsmodus, um das Gerät so zu konfigurieren, dass ein RADIUS CoA-Befehl disable-port ignoriert wird.

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

- domain deliter <Zeichen> - Verwenden Sie den Befehl domain deliter im Konfigurationsmodus des lokalen Servers mit dynamischer Autorisierung, um das Trennzeichen der Domäne für empfangene PoD- und CoA-Anforderungen zu konfigurieren.

```
domain delimiter $
```

In diesem Beispiel wird das Zeichen $ als Trennzeichen konfiguriert.

- Domain-Stripping [von rechts nach links] - Verwenden Sie im Konfigurationsmodus des lokalen Servers mit dynamischer Autorisierung den Befehl "Domain-Stripping", um das Verhalten für das User-Name-Domain-Stripping für empfangene PoD- und CoA-Anfragen zu aktivieren und zu definieren.

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

- ignore server-key (Serverschlüssel ignorieren) - Dieser Befehl wird im Konfigurationsmodus für den lokalen Server mit dynamischer Autorisierung verwendet, um das Gerät so zu konfigurieren, dass der CoA-Serverschlüssel ignoriert wird.

```
ignore server-key
```

CLI-Befehle im exec-Modus mit Berechtigungen

Im privilegierten exec-Modus können Sie show-Befehle auf den authentifizierten Clients ausführen, die Client-Zähler löschen und die Konfiguration des Dynamic Authorization Servers anzeigen.

- Verwenden Sie show aaaa clients, um die Statistiken des AAA (CoA)-Clients anzuzeigen.

```
show aaa clients
```

- Verwenden Sie den Befehl show aaa server radius dynamic-author, um die CoA-Konfiguration anzuzeigen.

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

- Clear AAA-Zähler können zum Löschen der AAA-Client-Zähler verwendet werden.

```
clear aaa clients counters
```

Schlussfolgerung

Sie haben jetzt mithilfe der CLI eine grundlegende Änderung der Autorisierungskonfiguration (Basic Change of Authorization, CoA) für den Catalyst 1300-Switch durchgeführt.

Weitere Informationen zu den CLI-Befehlen für die Catalyst 1300 Switches finden Sie im CLI-Leitfaden für Cisco Catalyst Switches der Serie 1300.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.