Basisconfiguratie van wijziging van autorisatie in Catalyst 1300 Switch met CLI

Doel

Het doel van dit artikel is om u te tonen hoe u een basisconfiguratie van de eigenschap van de verandering van vergunning (CoA) in Catalyst 1300 switches uit te voeren die de interface van de bevellijn (CLI) gebruiken.

Toepasselijke apparaten en softwareversie

- Catalyst 1300 switches | 4.1.3.36

Inleiding

Wijziging van autorisatie (CoA) is een uitbreiding van het RADIUS-protocol, waarmee u de eigenschappen van een verificatie-, autorisatie- en accounting (AAA) of dot1x-gebruikerssessie kunt wijzigen nadat deze is geverifieerd. Wanneer een beleid voor een gebruiker of groep in AAA verandert, kunnen beheerders RADIUS CoA-pakketten verzenden vanaf de AAA-server, zoals een Cisco Identity Services Engine (ISE), om de verificatie opnieuw te initialiseren en het nieuwe beleid toe te passen.

De Cisco Identity Services Engine (of ISE) is een volledig uitgeruste, op netwerk gebaseerde engine voor toegangscontrole en beleidshandhaving. Het biedt veiligheidsanalyse en handhaving, RADIUS- en TACACS-diensten, beleidsdistributie, en meer. Cisco ISE is momenteel de enige ondersteunde CoA Dynamic Autorisation-client voor Catalyst 1300 switches. Raadpleeg de ISE-beheerhandleiding voor meer informatie.

De CoA ondersteuning is toegevoegd aan Catalyst 1300 switches in firmware versie 4.1.3.36. Dit omvat ondersteuning voor het verbreken van de verbinding met gebruikers en het wijzigen van de machtigingen die van toepassing zijn op een gebruikerssessie. Het apparaat ondersteunt de volgende CoA-acties:

- Sessie verbreken
- Uitschakelen van host-poort CoA-opdracht
- Bounce host-poort CoA-opdracht
- Opdracht Host CoA opnieuw verifiëren

In dit artikel vindt u de opdrachten voor een basis CoA-configuratie in Catalyst 1300 switches met CLI. De stappen kunnen afwijken, afhankelijk van de

gebruikersinstellingen en -vereisten.

Inhoud

Basis CoA-configuratie met CLI

RADIUS-server en RADIUS-accounting instellen

Gebruik de volgende opdrachten om de RADIUS-server te configureren vanuit de globale configuratiemodus:

Stap 1

Gebruik de opdracht radius-server key om de verificatiesleutel voor RADIUS-communicatie tussen het apparaat en de RADIUS-daemon in te stellen.

```
radius-server key
```

Stap 2

Gebruik de opdracht radius-server host om een RADIUS-serverhost te configureren.

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

- Het IP-adres is het IP-adres van de ISE-server.
- toets <key-string> - Specificeert de verificatie- en coderingssleutel voor alle RADIUS-communicatie tussen het apparaat en de RADIUS-server. Deze sleutel moet overeenkomen met de codering die op de RADIUS-daemon wordt gebruikt.
- Prioriteit - Specificeert de volgorde waarin servers worden gebruikt, waarbij 0 de hoogste prioriteit heeft. (bereik:0-65535)
- gebruik dot1.x - specificeert dat de RADIUS-server wordt gebruikt voor 802.1x-poortverificatie.

Stap 3

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

Dynamische autorisatieserver configureren

Stap 1

Voer in de globale configuratiemodus de CoA-configuratiemodus in door de opdracht uit te voeren:

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

Stap 2

Om de RADIUS-toets te configureren die moet worden gedeeld tussen het apparaat en een CoA-client (bereik: 0-128 tekens), gebruikt u de opdrachtserver-key <key-string> in de configuratiemodus voor de dynamische lokale server. De sleutel in het verzoek van de Rekenkamer moet overeenkomen met deze sleutel.

```
server-key
```

> **Note:**
> Voor ISE zal de key-string dezelfde key string zijn die je hebt opgegeven voor de RADIUS server key-string bij het configureren van RADIUS.

Stap 3

Voer het IP-adres van de CoA-clienthost in. Het IP-adres kan een IPv4-, IPv6- of IPv6z-adres zijn.

```
client
```

Stap 4

```
Exit
```

Configureren 802.1x

Gebruik de opdracht dot1x system-auth-control om 802.1X wereldwijd in te schakelen.

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

Configureer 802.1x op een poort

Stap 1

Voer de interfaceconfiguratie in en selecteer de interface-ID met behulp van de opdrachtinterface Gigabit Ethernet<interface-ID>.

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

Stap 2

Gebruik de opdracht dot1x-poortcontrole om handmatige controle van de poortautorisatiestatus mogelijk te maken. De automatische modus maakt 802.1X-verificatie op de poort mogelijk en zorgt ervoor dat de poort overschakelt naar de geautoriseerde of niet-geautoriseerde status, op basis van de 802.1X-verificatieuitwisseling tussen het apparaat en de client.

```
dot1x port-control auto
```

Stap 3

Gebruik de optie dot1x om de opdracht opnieuw te verifiëren in de geprivilegieerde EXEC-modus om alle 802.1X-enabled poorten of de opgegeven 802.1X-enabled poort handmatig te starten.

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

Stap 4

Om de poortbeveiliging-leermodus te configureren, gebruikt u de opdracht poortbeveiligingsmodus interface (Ethernet, poortkanaal) voor configuratie-modus. Secure Delete-on-reset parameter is een beveiligde modus met beperkte leren beveiligde MAC-adressen met de verwijderbare-on-reset time-of-live.

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

Stap 5

Voer het volgende in om de interfaceconfiguratie te verlaten:

```
exit
```

Andere opdrachten voor CoA-configuratie

Hier zijn enkele andere CoA-opdrachten die kunnen worden gebruikt op basis van uw configuratie en configuratie.

- attribuut event-timestamp drop-pakket - Dit commando wordt gebruikt in de configuratiemodus van de dynamische autorisatie lokale server om het apparaat te configureren om een Packet of Disconnect (PoD) verzoek of CoA verzoek af te wijzen dat geen event-timestamp attribuut bevat.

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

- authenticatieopdracht bounce-port negeren - Gebruik de opdracht bounce-port van de verificatieopdracht in globale configuratiemodus om het apparaat te configureren voor het negeren

van een RADIUS-wijziging van autorisatie (CoA) bounce poortopdracht.

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

- authenticatie opdracht deactiveren-poort negeren - Gebruik deze opdracht in globale configuratie modus om het apparaat te configureren om een RADIUS CoA deactiveren-poortopdracht te negeren.

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

- domeinscheidingsteken <karakter> - Om de gebruikersdomeinscheidingsteken voor ontvangen PoD- en CoA-verzoeken te configureren, gebruikt u de opdracht Domeinscheidingsteken in de configuratiemodus van de lokale server voor dynamische autorisatie.

```
domain delimiter $
```

In dit voorbeeld wordt het $-teken als scheidingsteken ingesteld.

- domein stripping [van rechts naar links] - Om het gedrag voor gebruikersnaam domein stripping voor ontvangen PoD en CoA Verzoeken in te schakelen en te definiëren, gebruikt u de opdracht Domeinstripping in de modus voor dynamische autorisatie lokale serverconfiguratie.

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

- Serversleutel negeren - Deze opdracht wordt gebruikt in de configuratiemodus van de lokale server van de dynamische autorisatie om het apparaat te configureren om de CoA-serversleutel te negeren.

```
ignore server-key
```

CLI-opdrachten in Privilege Exec-modus

Vanuit de privilege exec-modus kunt u de opdrachten op de geverifieerde clients tonen, de clienttellers wissen en de configuratie van de Dynamic Authorisation Server tonen.

- Gebruik de show aaa clients om AAA (CoA) client statistieken te tonen.

```
show aaa clients
```

- Gebruik het bevel van de show aaa serverstraal dynamisch-auteur om CoA configuratie te tonen.

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

- duidelijke aaa tellers kunnen worden gebruikt om de aaa cliënten tellers te ontruimen

```
clear aaa clients counters
```

Conclusie

U hebt nu een fundamentele wijziging van de autorisatie (CoA)-configuratie in Catalyst 1300 switch met CLI voltooid.

Raadpleeg de Cisco Catalyst 1300 Switches Series CLI-handleiding voor meer informatie over de CLI-opdrachten voor de Catalyst 1300-switches .

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.