Configurazione di base della modifica dell'autorizzazione nello switch Catalyst 1300 con CLI

Obiettivo

Lo scopo di questo articolo è quello di mostrare come eseguire una configurazione di base della funzione di modifica dell'autorizzazione (CoA) sugli switch Catalyst 1300 dall'interfaccia della riga di comando (CLI).

Dispositivi e versione software interessati

- Catalyst 1300 switch | 4.1.3.36

Introduzione

Change of Authorization (CoA) è un'estensione del protocollo RADIUS che consente di modificare le proprietà di un'autenticazione, autorizzazione e accounting (AAA) o di una sessione utente dot1x dopo l'autenticazione. Quando viene modificato un criterio per un utente o un gruppo in AAA, gli amministratori possono trasmettere pacchetti RADIUS CoA dal server AAA, ad esempio Cisco Identity Services Engine (ISE), per reinizializzare l'autenticazione e applicare il nuovo criterio.

Cisco Identity Services Engine (o ISE) è un motore di controllo dell'accesso e applicazione delle policy basato sulla rete completo di tutte le funzionalità. Fornisce analisi e applicazione della sicurezza, servizi RADIUS e TACACS, distribuzione delle policy e altro ancora. Cisco ISE è attualmente l'unico client di autorizzazione dinamica CoA supportato per gli switch Catalyst 1300. Per ulteriori informazioni, consultare la guida per l'amministratore di ISE.

Il supporto CoA è stato aggiunto agli switch Catalyst 1300 nella versione firmware 4.1.3.36. Ciò include il supporto per la disconnessione degli utenti e la modifica delle autorizzazioni applicabili a una sessione utente. Il dispositivo supporta le seguenti azioni CoA:

- Disconnetti sessione
- Disabilita comando CoA porta host
- Comando CoA della porta host di rimbalzo
- Riautentica comando CoA host

In questo articolo, sono riportati i comandi per la configurazione base della CoA sugli switch Catalyst 1300 con CLI. I passaggi possono variare in base alle impostazioni e ai requisiti dell'utente.

Sommario

Configurazione CoA di base tramite CLI

Configurazione del server RADIUS e dell'accounting RADIUS

Per configurare il server RADIUS, dalla modalità di configurazione globale utilizzare i comandi seguenti:

Passaggio 1

Utilizzare il comando radius-server key per impostare la chiave di autenticazione per le comunicazioni RADIUS tra il dispositivo e il daemon RADIUS.

```
radius-server key
```

Passaggio 2

Utilizzare il comando radius-server host per configurare un host server RADIUS.

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

- L'indirizzo IP sarà l'indirizzo IP del server ISE.
- key <key-string>: specifica la chiave di autenticazione e crittografia per tutte le comunicazioni RADIUS tra il dispositivo e il server RADIUS. Questa chiave deve corrispondere alla crittografia utilizzata nel daemon RADIUS.
- Priorità: specifica l'ordine in cui vengono utilizzati i server, dove 0 ha la priorità più alta. (Intervallo: 0-65535)
- usage dot1.x - specifica che il server RADIUS viene utilizzato per l'autenticazione della porta 802.1x.

Passaggio 3

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

Configura server di autorizzazione dinamica

Passaggio 1

In modalità di configurazione globale, accedere alla modalità di configurazione CoA eseguendo il comando:

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

Passaggio 2

Per configurare la chiave RADIUS in modo che venga condivisa tra il dispositivo e un client CoA (intervallo: 0-128 caratteri), utilizzare il comando server-key <stringa-chiave> in modalità di configurazione del server locale con autorizzazione dinamica. La chiave specificata nella richiesta CoA deve corrispondere a questa chiave.

```
server-key
```

> **Note:**
> Per ISE, la stringa della chiave corrisponderà alla stringa della chiave specificata per la stringa della chiave del server RADIUS durante la configurazione di RADIUS.

Passaggio 3

Immettere l'indirizzo IP del client CoA. L'indirizzo IP può essere un indirizzo IPv4, IPv6 o IPv6z.

```
client
```

Passaggio 4

```
Exit
```

Configurazione 802.1x

Per abilitare 802.1X a livello globale, usare il comando dot1x system-auth-control.

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

Configurazione di 802.1x su una porta

Passaggio 1

Immettere la configurazione dell'interfaccia e selezionare l'ID interfaccia utilizzando il comando interface Gigabit Ethernet<Interface ID>.

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

Passaggio 2

Per abilitare il controllo manuale dello stato di autorizzazione della porta, utilizzare il comando dot1x port-control. La modalità automatica attiva l'autenticazione 802.1X sulla porta e la porta allo stato autorizzato o non autorizzato, in base allo scambio di autenticazione 802.1X tra il dispositivo e il client.

```
dot1x port-control auto
```

Passaggio 3

Per avviare la riautenticazione manuale di tutte le porte abilitate a 802.1X o della porta abilitata a 802.1X specificata, utilizzare il comando dot1x re-authentication in modalità di esecuzione privilegiata.

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

Passaggio 4

Per configurare la modalità di apprendimento per la sicurezza delle porte, utilizzare il comando port security mode Interface (Ethernet, Port Channel) configuration mode. Il parametro eliminazione sicura alla reimpostazione è una modalità protetta con apprendimento limitato degli indirizzi MAC sicuri con il tempo di attività dell'eliminazione alla reimpostazione.

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

Passaggio 5

Per uscire dalla configurazione interfaccia, immettere quanto segue:

```
exit
```

Altri comandi per la configurazione CoA

Di seguito sono riportati alcuni degli altri comandi CoA che possono essere usati in base alla configurazione e alla configurazione.

- attribute event-timestamp drop-packet - Questo comando viene utilizzato nella modalità di configurazione del server locale di autorizzazione dinamica per configurare il dispositivo in modo che ignori una richiesta Packet of Disconnect (PoD) o una richiesta CoA che non include un attributo event-timestamp.

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

- authentication, command bounce-port ignore - Per configurare il dispositivo in modo che ignori un comando RADIUS Change of Authorization (CoA) bounce port, utilizzare il comando authentication bounce-port ignore in modalità di configurazione globale.

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

- authentication command disable-port ignore - Per configurare il dispositivo in modo che ignori un comando RADIUS CoA disable-port, utilizzare questo comando in modalità di configurazione globale.

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

- delimitatore di dominio <carattere> - Per configurare il delimitatore di dominio del nome utente per le richieste PoD e CoA ricevute, utilizzare il comando delimitatore di dominio nella modalità di configurazione del server locale con autorizzazione dinamica.

```
domain delimiter $
```

In questo esempio il carattere $ è configurato come delimitatore.

- domain stripping [right-to-left] - Per abilitare e definire il comportamento per lo stripping del dominio dei nomi utente per le richieste PoD e CoA ricevute, utilizzare il comando stripping del dominio nella modalità di configurazione del server locale con autorizzazione dinamica.

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

- ignore server-key: questo comando viene utilizzato nella modalità di configurazione del server locale con autorizzazione dinamica per configurare il dispositivo in modo che ignori la chiave del server CoA.

```
ignore server-key
```

Comandi CLI in modalità di esecuzione privilegi

In modalità di esecuzione privilegiata è possibile eseguire i comandi show sui client autenticati, cancellare i contatori dei client e visualizzare la configurazione del server di autorizzazione dinamica.

- Utilizzare il comando show aaa client per visualizzare le statistiche dei client AAA (CoA).

```
show aaa clients
```

- Utilizzare il comando show aaa server radius dynamic-author per visualizzare la configurazione del server CoA.

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

- l'opzione clear aaa counters può essere usata per cancellare i contatori dei client aaa

```
clear aaa clients counters
```

Conclusioni

È stata completata una modifica di base alla configurazione dell'autorizzazione (CoA) nello switch Catalyst 1300 con CLI.

Per ulteriori informazioni sui comandi CLI degli switch Catalyst 1300, consultare la guida alla CLI degli switch Cisco Catalyst serie 1300.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).