Configuração Básica de Alteração de Autorização no Switch Catalyst 1300 utilizando CLI

Objetivo

O objetivo deste artigo é mostrar como executar uma configuração básica do recurso de alteração de autorização (CoA) nos switches Catalyst 1300 usando a interface de linha de comando (CLI).

Dispositivos aplicáveis e versão de software

- Catalyst 1300 Switches | 4.1.3.36

Introdução

Change of Authorization (CoA) é uma extensão do protocolo RADIUS, que permite alterar as propriedades de uma sessão de usuário de autenticação, autorização e relatório (AAA) ou dot1x após ser autenticada. Quando uma política para um usuário ou grupo em AAA muda, os administradores podem transmitir pacotes RADIUS CoA do servidor AAA, como um Cisco Identity Services Engine (ISE), para reinicializar a autenticação e aplicar a nova política.

O Cisco Identity Services Engine (ou ISE) é um mecanismo completo de controle de acesso baseado em rede e aplicação de políticas. Ele fornece análise e aplicação de segurança, serviços RADIUS e TACACS, distribuição de políticas e muito mais. O Cisco ISE é atualmente o único cliente de autorização dinâmica de CoA suportado para switches Catalyst 1300. Consulte o guia de administração do ISE para obter mais informações.

O suporte a CoA foi adicionado aos switches Catalyst 1300 na versão 4.1.3.36 do firmware. Isso inclui suporte para desconectar usuários e alterar autorizações aplicáveis a uma sessão de usuário. O dispositivo oferece suporte às seguintes ações de CoA:

- Desconectar Sessão
- Desabilitar o comando CoA da porta do host
- comando CoA de porta de host de devolução
- Comando CoA Reauthenticate host

Neste artigo, você encontrará os comandos para uma configuração básica de CoA nos switches Catalyst 1300 que usam CLI. As etapas podem variar de acordo com as configurações e os requisitos do usuário.

Table Of Contents

- Configuração básica de CoA usando CLI
- Outros comandos para a configuração de CoA
- Comandos CLI no modo exec privilegiado

Configuração básica de CoA usando CLI

Configurar Servidor RADIUS e Contabilização RADIUS

Para configurar o servidor RADIUS, no modo de configuração global, use os seguintes comandos:

Passo 1

Use o comando radius-server key para definir a chave de autenticação para comunicações RADIUS entre o dispositivo e o daemon RADIUS.

```
radius-server key
```

Passo 2

Use o comando radius-server host para configurar um host de servidor RADIUS.

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

- O endereço IP será o endereço IP do servidor ISE.
- key <key-string> - Especifica a chave de autenticação e de criptografia para todas as comunicações RADIUS entre o dispositivo e o servidor RADIUS. Essa chave deve corresponder à criptografia usada no daemon RADIUS.
- Prioridade - Especifica a ordem na qual os servidores são usados, onde 0 tem a prioridade mais alta. (Intervalo:0-65535)
- usage dot1.x - especifica que o servidor RADIUS é usado para a autenticação de porta 802.1x.

Etapa 3

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

Configurar Servidor de Autorização Dinâmico

Passo 1

No modo de configuração global, entre no modo de configuração de CoA executando o comando:

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

Passo 2

Para configurar a chave RADIUS a ser compartilhada entre o dispositivo e um cliente CoA (Intervalo: 0-128 caracteres), use o comando server-key <key-string> no modo de configuração do servidor local de autorização dinâmica. A chave fornecida na solicitação de CoA deve corresponder a essa chave.

```
server-key
```

> **Note:**
> Para o ISE, a sequência de chave será a mesma que você especificou para a sequência de chave do servidor RADIUS ao configurar o RADIUS.

Etapa 3

Insira o endereço IP do host do cliente de CoA. O endereço IP pode ser IPv4, IPv6 ou IPv6z.

```
client
```

Passo 4

```
Exit
```

Configurar 802.1x

Para ativar o 802.1X globalmente, use o comando dot1x system-auth-control.

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

Configurar 802.1x em uma porta

Passo 1

Entre na configuração de Interface e selecione o ID da interface usando o comando interface GigabitEthernet<Interface ID>.

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

Passo 2

Para ativar o controle manual do estado de autorização da porta, use o comando dot1x port-control. O modo Automático habilita a autenticação 802.1X na porta e faz com que ela passe para o estado autorizado ou não autorizado, com base na troca de autenticação 802.1X entre o dispositivo e o cliente.

```
dot1x port-control auto
```

Etapa 3

Para iniciar manualmente a reautenticação de todas as portas habilitadas para 802.1X ou da porta habilitada para 802.1X especificada, use o comando dot1x re-authenticate no modo EXEC privilegiado.

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

Passo 4

Para configurar o modo de aprendizado de segurança de porta, use o comando do modo de configuração da interface do modo de segurança de porta (Ethernet, Port Channel). O parâmetro de exclusão na redefinição segura é um modo seguro com aprendizagem limitada de endereços MAC seguros com o tempo de vida da exclusão na redefinição.

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

Etapa 5

Para sair da configuração da interface, digite o seguinte:

```
exit
```

Outros comandos para a configuração de CoA

Aqui estão alguns dos outros comandos CoA que podem ser usados com base na sua configuração e configuração.

- attribute event-timestamp drop-packet - Este comando é usado no modo de configuração de servidor local dynamic authorization para configurar o dispositivo para descartar uma solicitação de Pacote de Desconexão (PoD) ou de CoA que não inclua um atributo event-timestamp.

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

- authentication command bounce-port ignore - Para configurar o dispositivo para ignorar um comando de porta de devolução RADIUS Change of Authorization (CoA), use o comando authentication bounce-port ignore no modo de configuração global.

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

- authentication command disable-port ignore - Para configurar o dispositivo para ignorar um comando disable-port RADIUS CoA, use esse comando no modo de configuração global.

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

- delimitador de domínio <caractere> - Para configurar o delimitador de domínio de nome de usuário para solicitações de PoD e CoA recebidas, use o comando delimitador de domínio no modo de configuração de servidor local de autorização dinâmica.

```
domain delimiter $
```

Neste exemplo, o caractere $ é configurado como um delimitador.

- remoção de domínio [da direita para a esquerda] - Para habilitar e definir o comportamento da remoção de domínio de nome de usuário para Solicitações PoD e CoA recebidas, use o comando de remoção de domínio no modo de configuração de servidor local de autorização dinâmica.

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

- ignore server-key - Esse comando é usado no modo de configuração de servidor local de autorização dinâmica para configurar o dispositivo para ignorar a chave de servidor de CoA.

```
ignore server-key
```

Comandos CLI no modo exec privilegiado

No modo exec privilegiado, você pode executar comandos show nos clientes autenticados, limpar os contadores do cliente e mostrar a configuração do Servidor de Autorização Dinâmica.

- Use o comando show aaa clients para mostrar as estatísticas do cliente AAA (CoA).

```
show aaa clients
```

- Use o comando show aaa server radius dynamic-author para exibir a configuração de CoA.

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

- clear aaa counters pode ser usado para limpar os contadores de clientes aaa

```
clear aaa clients counters
```

Conclusão

Agora você concluiu uma alteração básica da configuração de autorização (CoA) no switch Catalyst 1300 usando CLI.

Para obter mais informações sobre os comandos CLI para os switches Catalyst 1300, consulte o Guia da CLI da série Cisco Catalyst 1300 Switches.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.