Configurando o TACACS+, o RAIO, e o Kerberos no Switches do Cisco catalyst

Índice

Introdução

A família Cisco Catalyst de switches (Catalyst 4000, Catalyst 5000 e Catalyst 6000 que executam o CatOS) tem suportado algum formato de autenticação, que começa no código 2.2. As melhorias foram adicionadas em versões posteriores. A porta TCP 49 TACACS+, não a porta 49 do User Datagram Protocol (UDP) XTACACS), RAIO, ou instalação de usuário do servidor Kerberos para o Authentication, Authorization, and Accounting (AAA) é a mesma que para usuários de roteador. Este documento contém exemplos dos comandos mínimos necessários a fim permitir estas funções. As opções adicionais estão disponíveis na documentação do switch para a versão na pergunta.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

Desde que umas versões de código mais atrasadas apoiam opções adicionais, você precisa de emitir o **comando show version** a fim determinar a versão de código no interruptor. Uma vez que você determinou a versão de código que está usada no interruptor, use esta tabela a fim determinar que opções estão disponíveis em seu equipamento, e que opções você deseja configurar.

Permaneça sempre no interruptor quando você adiciona a authentication e autorização. Teste a configuração em um outro indicador a fim evitar acidentalmente ser travado para fora.

Método (mínimo)	**Versão cat 2.2 5.1**	**Versão cat 5.1 5.4.1**	**Versão cat 5.4.1 7.5.1**	**Versão cat 7.5.1 e mais atrasado**
Autenticação TACACS+ OU	Etapa A	Etapa A	Etapa A	Etapa A
Autenticação RADIUS OU	N/A	Etapa B	Etapa B	Etapa B
Autenticação de Kerberos OU	N/A	N/A	Etapa K	Etapa K
Autenticação/autorização do nome de usuário local	N/A	N/A	N/A	Passo C
Positivo (opções)				
Autorização do comando TACACS+	N/A	N/A	Etapa D	Etapa D
Autorização de exec TACACS+	N/A	N/A	Etapa E	Etapa E
Autorização de exec RADIUS	N/A	N/A	Etapa F	Etapa F
Explicar - TACACS+ ou RAIO	N/A	N/A	Etapa G	Etapa G

O TACACS+ permite a autorização	Etapa H	Etapa H	Etapa H	Etapa H
Autorização do habilitado para radius	N/A	Etapa mim	Etapa mim	Etapa mim
O TACACS+ permite a autorização	N/A	N/A	Etapa J	Etapa J

Passos de configuração

Etapa A - TACACS+ autenticação

Com versões anterior do código, os comandos não são tão complexos quanto com algumas versões mais atrasadas. As opções adicionais em umas versões mais atrasadas podem estar disponíveis em seu interruptor.

1. Emita o comando do **set authentication login local enable** a fim certificar-se que há uma porta traseira no interruptor se o server está para baixo.
2. Emita o **comando set authentication login tacacs enable** a fim permitir a autenticação TACACS+.
3. Emita o comando do **set TACASCS server - - - -** a fim definir o server.
4. Emita o comando **chave do** *your_key dos* **tacacs do grupo** a fim definir a chave de servidor, que é opcional com TACACS+, porque faz com que os dados do interruptor-à-server sejam cifrados. Se usada, deve concordar com o server.**Nota:** O OS Software do Cisco catalyst não aceita o ponto de interrogação (**?**) para ser parte de nenhuma chaves ou senhas. O ponto de interrogação é usado explicitamente para a ajuda na sintaxe de comando.

Etapa B – Autenticação de RADIUS

Com versões anterior do código, os comandos não são tão complexos quanto com algumas versões mais atrasadas. As opções adicionais em umas versões mais atrasadas podem estar disponíveis em seu interruptor.

1. Emita o comando do **set authentication login local enable** a fim certificar-se que há uma porta traseira no interruptor se o server está para baixo.
2. Emita o comando do **set authentication login radius enable** a fim permitir a autenticação RADIUS.
3. Defina o server. Em todo equipamento da Cisco restante, as portas do raio padrão são 1645/1646 (autenticação/contabilidade).No catalizador, a porta padrão é 1812/1813. Se você usa Cisco fixe ou um server que se comunique com o outro equipamento da Cisco, usa a porta de 1645/1646. Emita o comando do **set radius server - - - - auth-port 1645 acct-port 1646 primary** a fim definir o server e o comando equivalente no Cisco IOS como **portas de origem do raio-server 1645-1646**.
4. Defina a chave de servidor.Isto é imperativo, porque faz com que a senha do interruptor-à-server seja cifrada como no RFC 2866 da contabilidade da autenticação RADIUS/ do RFC 2865 e RAIO da autorização . Se usado, deve concordar com o server. Emita o comando do

your_key da chave do raio do grupo.

Etapa C – Autenticação de nome de usuário local/Autorização

Começando na versão cactos 7.5.1, a autenticação de usuário local é possível. Por exemplo, você pode conseguir a autenticação/autorização com o uso de um nome de usuário e senha armazenado no catalizador, em vez da autenticação com uma senha local.

Há somente dois níveis de privilégio para a autenticação de usuário local, o 0 ou os 15. O nível 0 é o nível NON-privilegiado do executivo. O nível 15 é o privilegiado permite o nível.

Se você adiciona estes comandos neste exemplo, o `poweruser do` usuário chega no modo enable em um telnet ou o console ao interruptor e ao usuário `nonenable` chega no modo exec em um telnet ou em um console ao interruptor.

```
set localuser user poweruser password powerpass privilege 15
set localuser user nonenable password nonenable
```

Nota: Se o usuário `nonenable` conhece o grupo permita a senha, esse usuário pode continuar ao modo enable.

Após a configuração, as senhas são armazenadas cifraram.

A autenticação do nome de usuário local pode ser usada conjuntamente com o executivo remoto TACACS+, a contabilidade do comando, ou relatórios exec remotos do RAIO. Pode igualmente ser usada conjuntamente com o executivo remoto ou o comando authorization TACACS+, mas não faz o sentido usá-lo esta maneira porque o username precisa de ser armazenado no server TACACS+ assim como localmente no interruptor.

Etapa D – Autorização de comando TACACS+

Neste exemplo, o interruptor é dito para exigir a autorização para somente comandos configuration com TACACS+. Caso o server TACACS+ estiver para baixo, a autenticação não é nenhuma. Isto aplica-se à porta de Console e à sessão de Telnet. Emita este comando:

set authorization commands enable config tacacs none both

Neste exemplo, você pode configurar o server TACACS+ para permitir quando você ajusta estes parâmetros:

```
set localuser user poweruser password powerpass privilege 15
set localuser user nonenable password nonenable
```

O comando set port enable 2/12 é enviado ao servidor para verificação TACACS+.

Nota: Com o comando authorization permitido, ao contrário no roteador onde permita não está considerado um comando, o interruptor envia o **comando enable ao** server quando uma possibilidade é tentada. Certifique-se de que o server está configurado igualmente para permitir o **comando enable**.

Etapa E - TACACS+ autorização de exec

Neste exemplo, o interruptor é dito para exigir a autorização para uma sessão de exec com TACACS+. Caso o server TACACS+ estiver para baixo, a autorização não é nenhuma. Isto aplica-se à porta de Console e à sessão de Telnet. Emita o comando do **set authorization exec enable tacacs+ none both**

Além do que o pedido de autenticação, isto envia um pedido de autorização separado ao server TACACS+ do interruptor. Se o perfil de usuário é configurado para o shell/executivo no server TACACS+, esse usuário pode alcançar o interruptor.

Isto impede usuários sem serviço do shell/executivo configurado no server, tal como usuários PPP, do registro no interruptor. Você recebe uma mensagem que leia a `autorização do modo exec falhada`. Além do que a permissão/que nega o modo exec para usuários, você pode ser forçado no modo enable quando você entra com o nível de privilégio 15 atribuído no server. Deve o runcode em que a identificação de bug Cisco CSCdr51314 (clientes registrados somente) é fixa.

Etapa F - Autorização para exec RADIUS

Não há nenhum comando permitir a autorização de exec RADIUS. A alternativa é ajustar o tipo de serviço (atributo RADIUS 6) a administrativo (um valor de 6) no servidor Radius para lançar o usuário no modo enable no servidor Radius. Se o tipo de serviço é ajustado para qualquer coisa a não ser 6-administrative, por exemplo, 1-login, 7-shell, ou 2-framed, o usuário chega no prompt de exec do interruptor, mas não na alerta da possibilidade.

Adicionar estes comandos no interruptor para a authentication e autorização:

```
set localuser user poweruser password powerpass privilege 15
set localuser user nonenable password nonenable
```

Etapa G – Relatório - TACACS+ ou RADIUS

A fim permitir o TACACS+ que esclarece:

1. Se você obtém a alerta do interruptor, emita o comando do **set accounting exec enable start-stop tacacs+**.
2. Usuários esse telnet fora da questão de switch o comando do **set accounting connect enable start-stop tacacs+**.
3. Se você recarrega o interruptor, emita o comando do **set accounting system enable start-stop tacacs+**.
4. Os usuários que executam comandos, emitem o **set accounting commands enable todo o comando tacacs+ start-stop**.
5. Lembretes ao server, por exemplo, para atualizar registros uma vez que um minúsculo a fim mostrar que o usuário está entrado ainda, emite o comando do **set accounting update periodic 1**.

A fim permitir o RAIO que esclarece:

1. Os usuários que obtêm a alerta do interruptor, emitem o comando do **set accounting exec enable start-stop radius**.
2. Usuários que o telnet fora do interruptor, emite o comando do **set accounting connect enable start-stop radius**.
3. Quando você recarrega o interruptor, emita o comando do **set accounting system enable**

start-stop radius.

4. Lembretes ao server, por exemplo, para atualizar registros uma vez que um minúsculo a fim mostrar que o usuário está entrado ainda, emite o comando do **set accounting update periodic** 1.

Registros do freeware TACACS+

Esta saída é um exemplo de como os registros podem aparecer no server:

```
set localuser user poweruser password powerpass privilege 15
set localuser user nonenable password nonenable
```

RAIO na saída do registro de UNIX

Esta saída é um exemplo de como os registros podem aparecer no server:

```
set localuser user poweruser password powerpass privilege 15
set localuser user nonenable password nonenable
```

Passo H – Ativação da autenticação TACACS+

Conclua estes passos:

1. Emita o comando do **set authentication enable local enable** a fim certificar-se de que há uma porta traseira dentro se o server está para baixo.
2. Emita o **comando set authentication enable tacacs enable** a fim dizer o interruptor para enviar requisições de habilitação ao server.

Etapa I – Ativação de autenticação de RADIUS

Adicionar estes comandos a fim conseguir o interruptor enviar o username `$enab15$ ao` servidor Radius. Não todos os servidores Radius apoiam este tipo de um username. Veja a etapa E para uma outra alternativa, por exemplo, se você ajusta um [RADIUS attribute 6 - to Administrative] do tipo de serviço, que lança usuários individuais no modo enable.

1. Emita o comando do **set authentication enable local enable** a fim certificar-se que há uma porta traseira dentro se o server está para baixo.
2. Emita o comando do **set authentication enable radius enable** a fim dizer o interruptor para enviar requisições de habilitação ao server se seu servidor Radius apoia o username $enab15$.

Etapa J - Autorização para ativação de TACACS+

A adição deste comando conduz à emissão do interruptor permite ao server quando o usuário tenta permitir. O server precisa de ter o **comando enable** permitido. Neste exemplo, há um Failover a nenhuns no evento que o server está para baixo:

set author enable enable tacacs+ none both

Etapa K – Autenticação do Kerberos

Refira o controlando e monitorando o acesso ao comutador usando a autenticação, a autorização, e esclarecer mais informação em como estabelecer o Kerberos ao interruptor.

Recuperação de senha:

Refira procedimentos de recuperação de senha para obter mais informações sobre dos procedimentos de recuperação de senha.

Esta página é o deslocamento predeterminado dos procedimentos de recuperação de senha para o Produtos da Cisco.

Comandos ip permit para segurança adicional

Para a segurança adicional, o catalizador pode ser configurado para controlar o acesso do telnet através dos **comandos ip permit**:

set ip permit enable telnet

ajuste a *máscara da escala da* **licença IP|***host*

Isto permite somente a escala ou os anfitriões especificada ao telnet no interruptor.

Depuração no Catalyst

Antes de permitir a eliminação de erros no catalizador, verifique os log de servidor para ver se há razões para a falha. Isto é mais fácil e menos disruptivo ao interruptor. Em umas versões de switch mais adiantadas, **debugar** foi executado no modo de engenharia. Não é necessário alcançar o modo de engenharia a fim executar **comandos debug em umas** versões de código mais atrasadas:

ajuste tacacs do traço|radius|Kerberos 4

Nota: Os tacacs do traço do grupo|radius|o comando 0 do Kerberos retorna o catalizador ao modo deseguimento.

Refira a página de suporte do produto do Switches para obter mais informações sobre dos switch LAN multicamada.

Informações Relacionadas

- Comparação TACACS+ e RADIUS
- RAIO, TACACS+, e Kerberos na documentação IOS Cisco
- Página de suporte RADIUS
- Página de Suporte do TACACS/TACACS+
- Página de suporte do Kerberos
- Solicitações de Comentários (RFCs)

- Suporte Técnico e Documentação - Cisco Systems