Configurar TACACS+, RADIUS e Kerberos em Switches Catalyst

Contents

Introduction

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 TACACS+ 49, não a porta 49 do Protocolo de Datagrama de Usuário (UDP - User Datagram Protocol), RADIUS ou configuração de usuário do servidor Kerberos para autenticação, autorização e contabilização (AAA - Authentication, Authorization, and Accounting) é a mesma para usuários de roteador. Este documento contém exemplos dos comandos mínimos necessários para habilitar essas funções. Há opções adicionais disponíveis na documentação do switch para a versão em questão.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

Conventions

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

Informações de Apoio

Como versões posteriores do código suportam opções adicionais, você precisa emitir o comando **show version** para determinar a versão do código no switch. Depois de determinar a versão do código que é usada no switch, use esta tabela para determinar quais opções estão disponíveis no seu equipamento e quais opções você deseja configurar.

Sempre permaneça no switch quando você adicionar autenticação e autorização. Teste a configuração em outra janela para evitar que ela seja bloqueada acidentalmente.

Método (mínimo)	**Cat versão 2.2 a 5.1**	**Cat versão 5.1 a 5.4.1**	**Cat versão 5.4.1 a 7.5.1**	**Cat versão 7.5.1 e posterior**
TACACS+ Autenticação OU	Etapa A	Etapa A	Etapa A	Etapa A
Autenticação RADIUS OU	N/A	Etapa B	Etapa B	Etapa B
Autenticação Kerberos OU	N/A	N/A	Etapa K	Etapa K
Autenticação/Autorização de Nome de Usuário Local	N/A	N/A	N/A	Passo C
Mais (opções)				
Autorização do comando TACACS+	N/A	N/A	Etapa D	Etapa D
Autorização de Execução TACACS+	N/A	N/A	Etapa E	Etapa E
Autorização Exec RADIUS	N/A	N/A	Etapa F	Etapa F
Contabilidade - TACACS+ ou RADIUS	N/A	N/A	Etapa G	Etapa G

Autorização de ativação TACACS+	Etapa H	Etapa H	Etapa H	Etapa H
Autorização de ativação RADIUS	N/A	Etapa I	Etapa I	Etapa I
Autorização de ativação TACACS+	N/A	N/A	Etapa J	Etapa J

Configuration Steps

Etapa A - TACACS+ autenticação

Com versões anteriores do código, os comandos não são tão complexos quanto com algumas versões posteriores. Outras opções em versões posteriores podem estar disponíveis no switch.

1. Emita o comando **set authentication login local enable** para garantir que haja uma porta traseira no switch se o servidor estiver inoperante.
2. Execute o comando **set authentication login tacacs enable** para ativar a autenticação TACACS+.
3. Execute o **comando set tacacs server #.#.#.#** para definir o servidor.
4. Emita o comando *your_key* ***set tacacs key*** para definir a chave do servidor, que é opcional com TACACS+, pois faz com que os dados de switch para servidor sejam criptografados. Se usado, ele deve concordar com o servidor.**Observação:** o software Cisco Catalyst OS **não** aceita o ponto de interrogação (**?**) para fazer parte de quaisquer chaves ou senhas. O ponto de interrogação é usado explicitamente para ajuda na sintaxe do comando.

Etapa B – Autenticação de RADIUS

Com versões anteriores do código, os comandos não são tão complexos quanto com algumas versões posteriores. Outras opções em versões posteriores podem estar disponíveis no switch.

1. Emita o comando **set authentication login local enable** para garantir que haja uma porta traseira no switch se o servidor estiver inoperante.
2. Execute o comando **set authentication login radius enable** para ativar a autenticação RADIUS.
3. Defina o servidor. Em todos os outros equipamentos Cisco, as portas RADIUS padrão são 1645/1646 (autenticação/contabilidade).No Catalyst, a porta padrão é 1812/1813. Se você usa o Cisco Secure ou um servidor que se comunica com outro equipamento Cisco, use a porta 1645/1646. Execute o **comando set radius server #.#.#.# auth-port 1645 acct-port 1646 primary** para definir o servidor e o comando equivalente no Cisco IOS como **radius-server source-ports 1645-1646**.
4. Defina a chave do servidor.Isso é obrigatório, pois faz com que a senha de switch para servidor seja criptografada como na RADIUS Authentication/Authorization RFC 2865 e RADIUS Accounting RFC 2866 . Se usado, ele deve concordar com o servidor. Emita o comando **set radius key** ***your_key***.

Etapa C – Autenticação de nome de usuário local/Autorização

A partir da versão 7.5.1 do CatOS, a autenticação de usuário local é possível. Por exemplo, você pode obter autenticação/autorização com o uso de um nome de usuário e senha armazenados no Catalyst, em vez de autenticação com uma senha local.

Há apenas dois níveis de privilégio para autenticação de usuário local, 0 ou 15. O nível 0 é o nível exec não privilegiado. O nível 15 é o nível de habilitação privilegiada.

Se você adicionar esses comandos neste exemplo, o usuário `poweruser` chega ao modo enable em um Telnet ou console para o switch e o usuário `nonenable` chega ao modo exec em um Telnet ou console para o switch.

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

Observação: se o usuário `nonenable` souber a senha **enable**, ele poderá continuar a ativar o modo.

Após a configuração, as senhas são armazenadas criptografadas.

A autenticação de nome de usuário local pode ser usada em conjunto com a execução remota TACACS+, a contabilidade de comandos ou a contabilidade de execução remota RADIUS. Ele também pode ser usado em conjunto com autorização de execução ou comando remoto TACACS+, mas não faz sentido usá-lo dessa maneira porque o nome de usuário precisa ser armazenado tanto no servidor TACACS+ como localmente no switch.

Etapa D – Autorização de comando TACACS+

Neste exemplo, o switch deve exigir autorização somente para comandos de configuração com TACACS+. Caso o servidor TACACS+ esteja inoperante, a autenticação não é nenhuma. Isso se aplica à porta de console e à sessão Telnet. Emita este comando:

set authorization commands enable config tacacs none

Neste exemplo, você pode configurar o servidor TACACS+ para permitir ao definir estes parâmetros:

```
command=set
arguments (permit)=port 2/12
```

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

Observação: com autorização de comando habilitada, ao contrário do roteador em que enable não é considerado um comando, o switch envia o comando **enable** ao servidor quando uma ativação é tentada. Verifique se o servidor também está configurado para permitir o comando **enable**.

Etapa E - TACACS+ autorização de exec

Neste exemplo, o switch é instruído a exigir autorização para uma sessão exec com TACACS+. Caso o servidor TACACS+ esteja inoperante, a autorização não é nenhuma. Isso se aplica à porta de console e à sessão Telnet. Emita o comando **set authorization exec enable tacacs+ none**

Além da solicitação de autenticação, isso envia uma solicitação de autorização separada para o servidor TACACS+ do switch. Se o perfil de usuário estiver configurado para shell/exec no servidor TACACS+, esse usuário poderá acessar o switch.

Isso evita que os usuários sem serviço shell/exec configurado no servidor, como os usuários PPP, acessem o switch. Você recebe uma mensagem de `falha na autorização do modo Exec`. Além de permitir/negar o modo exec para os usuários, você pode ser forçado ao modo enable quando digitar com o nível de privilégio 15 atribuído no servidor. Ele deve executar um código no qual a ID de bug da Cisco CSCdr51314 (somente clientes registrados) é corrigida.

Etapa F - Autorização para exec RADIUS

Não há nenhum comando para habilitar a autorização exec RADIUS. A alternativa é definir o Tipo de serviço (atributo RADIUS 6) como Administrativo (um valor de 6) no servidor RADIUS para iniciar o usuário no modo de ativação no servidor RADIUS. Se o tipo de serviço for definido para qualquer coisa diferente de 6-administrativas, por exemplo, 1-login, 7-shell ou 2-framed, o usuário chega ao prompt exec do switch, mas não ao prompt de ativação.

Adicione estes comandos no switch para autenticação e autorização:

```
aaa authorization exec TEST group radius
 line vty 0 4
 authorization exec TEST
 login authentication TEST
```

Etapa G – Relatório - TACACS+ ou RADIUS

Para habilitar a contabilidade TACACS+ para:

1. Se você receber o prompt do switch, execute o comando **set accounting exec enable start-stop tacacs+**.
2. Os usuários que fazem Telnet fora do switch executam o **comando set accounting connect enable start-stop tacacs+**.
3. Se você reinicializar o switch, execute o comando **set accounting system enable start-stop tacacs+**.
4. Usuários que executam comandos, emita os **comandos set accounting enable all start-stop tacacs+** command.
5. Lembre ao servidor, por exemplo, de atualizar registros uma vez por minuto para mostrar que o usuário ainda está conectado, emita o comando **set accounting update periódico 1**.

Para habilitar a contabilização de RADIUS para:

1. Usuários que recebem o prompt do switch, emita o comando **set accounting exec enable start-stop radius**.
2. Usuários que fazem telnet para fora do switch, emita o comando **set accounting connect enable start-stop radius**.
3. Quando você reinicializa o switch, execute o comando **set accounting system enable start-stop radius**.
4. Lembre ao servidor, por exemplo, de atualizar registros uma vez por minuto para mostrar que o usuário ainda está conectado, execute o comando **set accounting update periódico 1**.

Registros de freeware TACACS+

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

```
Fri Mar 24 13:22:41 2000 10.31.1.151 pinecone telnet85
171.68.118.100 stop task_id=5 start_time=953936729 timezone=UTC
service=shell disc-cause=2 elapsed_time=236
Fri Mar 24 13:22:50 2000 10.31.1.151 pinecone telnet85
171.68.118.100 stop task_id=15 start_time=953936975 timezone=UTC
service=shell priv-lvl=0 cmd=enable
Fri Mar 24 13:22:54 2000 10.31.1.151 pinecone telnet85
171.68.118.100 stop task_id=16 start_time=953936979 timezone=UTC
service=shell priv-lvl=15 cmd=write terminal
Fri Mar 24 13:22:59 2000 10.31.1.151 pinecone telnet85
171.68.118.100 stop task_id=17 start_time=953936984 timezone=UTC
service=shell priv-lvl=15 cmd=show version
Fri Mar 24 13:23:19 2000 10.31.1.151 pinecone telnet85
171.68.118.100 update task_id=14 start_time=953936974 timezone=UTC
service=shell
```

RADIUS na saída do registro UNIX

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

```
Client-Id = 10.31.1.151
NAS-Port-Type = 0
User-Name = "login"
Acct-Status-Type = Start
Acct-Authentic = RADIUS
User-Service-Type = 7
Acct-Session-Id = "0000002b"
Acct-Delay-Time = 0

Client-Id = 10.31.1.151
NAS-Port-Type = 0
User-Name = "login"
Calling-Station-Id = "171.68.118.100"
Acct-Status-Type = Start
User-Service-Type = Login-User
Acct-Session-Id = "0000002c"
Login-Service = Telnet
Login-Host = 171.68.118.100
Acct-Delay-Time = 0

Client-Id = 10.31.1.151
NAS-Port-Type = 0
User-Name = "login"
Calling-Station-Id = "171.68.118.100"
Acct-Status-Type = Stop
User-Service-Type = Login-User
Acct-Session-Id = "0000002c"
Login-Service = Telnet
Login-Host = 171.68.118.100
Acct-Session-Time = 9
Acct-Delay-Time = 0

Client-Id = 10.31.1.151
NAS-Port-Type = 0
User-Name = "login"
Acct-Status-Type = Stop
```

```
Acct-Authentic = RADIUS
User-Service-Type = 7
Acct-Session-Id = "0000002b"
Received unknown attribute 49
Acct-Session-Time = 30
Acct-Delay-Time = 0
```

Passo H – Ativação da autenticação TACACS+

Conclua estes passos:

1. Emita o comando **set authentication enable local enable** para verificar se há uma porta traseira no caso do servidor estar inoperante.
2. Emita o comando **set authentication enable tacacs enable** para instruir o switch a enviar solicitações de ativação ao servidor.

Etapa I – Ativação de autenticação de RADIUS

Adicione esses comandos para fazer com que o switch envie o nome de usuário `$suas15$` ao servidor RADIUS. Nem todos os servidores RADIUS suportam esse tipo de nome de usuário. Consulte a Etapa E para obter outra alternativa, por exemplo, se você definir um tipo de serviço [atributo RADIUS 6 - para Administrativo], que iniciará usuários individuais no modo de ativação.

1. Execute o comando **set authentication enable local enable** para garantir que haja uma porta traseira no caso do servidor estar inoperante.
2. Emita o comando **set authentication enable radius enable** para instruir o switch a enviar solicitações de ativação ao servidor se o servidor RADIUS suportar o nome de usuário $Ch15$.

Etapa J - Autorização para ativação de TACACS+

A adição desse comando faz com que o switch envie enable ao servidor quando o usuário tenta ativar. O servidor precisa ter o comando **enable** permitido. Neste exemplo, há um failover para nenhum caso o servidor esteja inoperante:

set autor enable tacacs+ none ambos

Etapa K – Autenticação do Kerberos

Consulte Controlando e Monitorando o Acesso ao Switch Usando Autenticação, Autorização e Contabilidade para obter mais informações sobre como configurar Kerberos no switch.

Recuperação de senha:

Consulte Procedimentos de Recuperação de Senha para obter mais informações sobre procedimentos de Recuperação de Senha.

Esta página é o índice de procedimentos de recuperação de senha para produtos Cisco.

Comandos ip permit para segurança adicional

Para segurança adicional, o Catalyst pode ser configurado para controlar o acesso Telnet através dos comandos **ip permit**:

set ip permit enable telnet

set ip permit *range mask*|*host*

Isso permite somente o intervalo ou hosts especificados para executar telnet no switch.

Depuração no Catalyst

Antes de habilitar a depuração no Catalyst, verifique os registros do servidor para saber os motivos da falha. Isso é mais fácil e menos prejudicial para o switch. Nas versões anteriores do switch, a **depuração** foi executada no modo de engenharia. Não é necessário acessar o modo de engenharia para executar comandos **debug** em versões posteriores do código:

set trace tacacs|radius|kerberos 4

Observação: o comando **set trace tacacs|radius|kerberos 0** retorna o Catalyst ao modo sem rastreamento.

Consulte a página de suporte a produtos de switches para obter mais informações sobre switches LAN multicamada.

Informações Relacionadas

- Comparação TACACS+ e RADIUS
- RADIUS, TACACS+ e Kerberos na documentação do Cisco IOS
- 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