Cisco IOS Router: Local, TACACS+ e autenticação RADIUS do exemplo de configuração da conexão de HTTP

Índice

Introdução

Este documento mostra como configurar o local, o TACACS+, e a autenticação RADIUS da conexão de HTTP. Alguns comandos debugging relevantes são fornecidos igualmente.

Antes de Começar

Convenções

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Pré-requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nas versões de software e hardware abaixo.

- O Cisco IOS ® Software liberam 11.2 ou mais atrasado
- Hardware que suporta essas revisões de software

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se você estiver trabalhando em uma rede ativa, certifique-se de que entende o impacto potencial de qualquer comando antes de utilizá-lo.

Material de Suporte

No Software Release 11.2 de Cisco IOS®, uma característica para controlar o roteador com o HTTP foi adicionada. Do “a seção dos comandos do navegador da Web Cisco IOS” da referência de comandos das configurações fundamentais de IOS Cisco inclui a informação seguinte sobre esta característica.

“O **comando ip http authentication** permite-o de especificar um método de autenticação particular para usuários de servidor de HTTP. O Server do HTTP usa o método de senha da possibilidade para autenticar um usuário a nível de privilégio 15. **O comando ip http authentication** deixa-o agora especificar permite, local, TACACS, ou autenticação de usuário de servidor de HTTP do Authentication, Authorization, and Accounting (AAA).”

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Este documento utiliza as configurações mostradas abaixo.

- Configurando a autenticação local para usuários de servidor de HTTP
- Configurando a autenticação TACACS+ para usuários de servidor de HTTP
- Configurando a autenticação RADIUS para usuários de servidor de HTTP

Nota: Para localizar informações adicionais sobre os comandos usados neste documento, utilize a Ferramenta Command Lookup (somente clientes registrados).

Configurando a autenticação local para usuários de servidor de HTTP

- Configurações do Roteador
- Resultados do usuário

Configurações do Roteador

Autenticação local com Cisco IOS Software Release 11.2
`!--- This is the part of the configuration related to local authentication. ! aaa new-model aaa authentication login default local aaa authorization exec local username one privilege 15 password one username three password three username four privilege 7 password four ip http server ip http authentication aaa ! !--- Example of command moved from level 15 (enable) to level 7 ! privilege exec level 7 clear line`

Autenticação local com Cisco IOS Software Release 11.3.3.T ou Mais Recente

```
!--- This is the part of the configuration !--- related
to local authentication. ! aaa new-model aaa
authentication login default local aaa authorization
exec default local username one privilege 15 password
one username three password three username four
privilege 7 password four ip http server ip http
authentication local ! !--- Example of command moved
from level 15 (enable) to level 7 ! privilege exec level
7 clear line
```

Resultados do usuário

Estes resultados aplicam-se aos usuários nas configurações de roteador precedentes.

- **Usuário um**O usuário passará a autorização web se a URL é incorporada como http://#.#.#.#.Após o telnet ao roteador, o usuário pode executar comandos all após a autenticação de login.O usuário estará no modo habilitar após o login (show privilege será 15).Se o comando authorization é adicionado ao roteador, o usuário ainda sucederá nos comandos all.
- **Usuário três**O usuário falhará a autorização web devido a não ter um nível de privilégio.Após o telnet ao roteador, o usuário pode executar comandos all após a autenticação de login.O usuário estará no modo não habilitado depois do início da sessão (show privilege será 1).Se o comando authorization é adicionado ao roteador, o usuário ainda sucederá nos comandos all.
- **Usuário quatro**O usuário passará a autorização web se a URL é incorporada como http://#.#.#.#/level/7/exec.Os comandos de nível 1 e o comando clear line de nível 7 aparecerão.Após o telnet ao roteador, o usuário pode executar comandos all após a autenticação de login.O usuário estará a nível de privilégio 7 após o início de uma sessão (o **privilégio da mostra** será 7)Se o comando authorization é adicionado ao roteador, o usuário ainda sucederá nos comandos all.

Configurando a autenticação TACACS+ para usuários de servidor de HTTP

Configurações do Roteador

Autenticação com Cisco IOS Software Release 11.2

```
aaa new-model
aaa authentication login default tacacs+
aaa authorization exec tacacs+
ip http server
ip http authentication aaa
tacacs-server host 171.68.118.101
tacacs-server key cisco
```

```
!--- Example of command moved from level 15 (enable) to
level 7 privilege exec level 7 clear line
```

Autenticação com Cisco IOS Software Release 11.3.3.T a 12.0.5.T

```
aaa new-model
aaa authentication login default tacacs+
aaa authorization exec default tacacs
ip http server
ip http authentication aaa|tacacs
tacacs-server host 171.68.118.101
tacacs-server key cisco
!--- Example of command moved from level 15 (enable) to
level 7 privilege exec level 7 clear line
```

Autenticação com Cisco IOS Software Release 12.0.5.T e Mais Recente

```
aaa new-model
aaa authentication login default group tacacs+
aaa authorization exec default group tacacs+
ip http server
ip http authentication aaa
tacacs-server host 171.68.118.101
tacacs-server key cisco
!--- Example of command moved from level 15 (enable) to
level 7 privilege exec level 7 clear line
```

Resultados do usuário

Os seguintes resultados aplicam-se aos usuários nas configurações do servidor abaixo.

- **Usuário um**O usuário passará a autorização web se a URL é incorporada como http://#.#.#.#.Após o telnet ao roteador, o usuário pode executar comandos all após a autenticação de login.O usuário estará no modo habilitar após o login (show privilege será 15).Se o comando authorization é adicionado ao roteador, o usuário ainda sucederá nos comandos all.
- **Usuário dois**O usuário passará a autorização web se a URL é incorporada como http://#.#.#.#.Após o telnet ao roteador, o usuário pode executar comandos all após a autenticação de login.O usuário estará no modo habilitar após o login (show privilege será 15).Se o comando authorization é adicionado ao roteador, o usuário falhará comandos all porque a configuração do servidor não os autoriza.
- **Usuário três**O usuário falhará a autorização web devido a não ter um nível de privilégio.Após o telnet ao roteador, o usuário pode executar comandos all após a autenticação de login.O usuário estará no modo não habilitado depois do início da sessão (show privilege será 1).Se o comando authorization é adicionado ao roteador, o usuário ainda sucederá nos comandos all.
- **Usuário quatro**O usuário passará a autorização web se a URL é incorporada como http://#.#.#.#/level/7/exec.Os comandos de nível 1 e o comando clear line de nível 7 aparecerão.Após o telnet ao roteador, o usuário pode executar comandos all após a autenticação de login.O usuário estará a nível de privilégio 7 após o início de uma sessão (o **privilégio da mostra** será 7)Se o comando authorization é adicionado ao roteador, o usuário ainda sucederá nos comandos all.

Configuração do programa gratuito de servidor de daemon

```
user = one {
default service = permit
login = cleartext "one"
service = exec {
priv-lvl = 15
}
}

user = two {
login = cleartext "two"
service = exec {
priv-lvl = 15
}
}

user = three {
default service = permit
login = cleartext "three"
}

user = four {
default service = permit
login = cleartext "four"
service = exec {
priv-lvl = 7
}
}
```

Cisco Secure ACS para a configuração de servidor Unix

```
# ./ViewProfile -p 9900 -u one
User Profile Information
user = one{
profile_id = 27
profile_cycle = 1
password = clear "********"
default service=permit
service=shell {
set priv-lvl=15
}
}
# ./ViewProfile -p 9900 -u two
User Profile Information
user = two{
profile_id = 28
profile_cycle = 1
password = clear "********"
service=shell {
set priv-lvl=15
}
}
# ./ViewProfile -p 9900 -u three
User Profile Information
user = three{
profile_id = 29
profile_cycle = 1
password = clear "********"
default service=permit
}
# ./ViewProfile -p 9900 -u four
User Profile Information
user = four{
profile_id = 30
```

```
profile_cycle = 1
password = clear "********"
default service=permit
service=shell {
set priv-lvl=7
}
}
```

Configuração do servidor do Cisco Secure ACS for Windows

Usuário um em grupo um

- Configurações de grupoVerificar shell (exec).Verifique o nível de privilégio=15.Verifique serviços padrões (não definidos)**Nota:** Se essa opção não aparecer, vá para Interface Configuration e selecione TACACS+ e, em seguida, Advanced Configuration Options. Escolha Exibir configuração habilitada de serviço padrão (indefinido).
- Configurações de usuárioSenha de qualquer base de dados; incorpore a senha e confirme-a na área superior.

Usuário dois no grupo dois

- Configurações de grupoVerificar shell (exec).Verifique o nível de privilégio=15.Não verifique **serviços (indeterminados) do padrão**.
- Configurações de usuárioSenha de qualquer base de dados; incorpore a senha e confirme-a na área superior.

Usuário três no grupo três

- Configurações de grupoVerificar shell (exec).Deixe o nível de privilégio em branco.Verifique serviços padrões (não definidos)**Nota:** Se essa opção não aparecer, vá para Interface Configuration e selecione TACACS+ e, em seguida, Advanced Configuration Options. Escolha Exibir configuração habilitada de serviço padrão (indefinido).
- Configurações de usuárioSenha de qualquer base de dados; incorpore a senha e confirme-a na área superior.

Usuário quatro no grupo quatro

- Configurações de grupoVerificar shell (exec).Verificar nível de privilégio=7Verifique serviços padrões (não definidos)**Nota:** Se essa opção não aparecer, vá para Interface Configuration e selecione TACACS+ e, em seguida, Advanced Configuration Options. Escolha Exibir configuração habilitada de serviço padrão (indefinido).
- Configurações de usuárioSenha de qualquer base de dados; incorpore a senha e confirme-a na área superior.

Configurando a autenticação RADIUS para usuários de servidor de HTTP

Configurações do Roteador

Autenticação com Cisco IOS Software Release 11.2

```
aaa new-model
aaa authentication login default radius
aaa authorization exec radius
ip http server
ip http authentication aaa
!
!--- Example of command moved from level 15 (enable) to
level 7 ! privilege exec level 7 clear line radius-
server host 171.68.118.101 radius-server key cisco
```

Autenticação com Cisco IOS Software Release 11.3.3.T a 12.0.5.T

```
aaa new-model
aaa authentication login default radius
aaa authorization exec default radius
ip http server
ip http authentication aaa
radius-server host 171.68.118.101 auth-port 1645 acct-
port 1646
radius-server key cisco
privilege exec level 7 clear line
```

Autenticação com Cisco IOS Software Release 12.0.5.T e Mais Recente

```
aaa new-model
aaa authentication login default group radius
aaa authorization exec default group radius
ip http server
ip http authentication aaa
radius-server host 171.68.118.101 auth-port 1645 acct-
port 1646
radius-server key cisco
privilege exec level 7 clear line
```

Resultados do usuário

Os seguintes resultados aplicam-se aos usuários nas configurações do servidor abaixo.

- **Usuário um**O usuário passará a autorização web se a URL é incorporada como http://#.#.#.#.Após o telnet ao roteador, o usuário pode executar comandos all após a autenticação de login.O usuário estará no modo habilitar após o login (show privilege será 15).
- **Usuário três**O usuário falhará a autorização web devido a não ter um nível de privilégio.Após o telnet ao roteador, o usuário pode executar comandos all após a autenticação de login.O usuário estará no modo não habilitado depois do início da sessão (show privilege será 1).
- **Usuário quatro**O usuário passará a autorização web se a URL é incorporada como http://#.#.#.#/level/7/exec.Os comandos de nível 1 e o comando clear line de nível 7 aparecerão.Após o telnet ao roteador, o usuário pode executar comandos all após a autenticação de login.O usuário estará a nível de privilégio 7 após o início de uma sessão (o **privilégio da mostra** será 7)

Configuração RADIUS no server que apoia pares Cisco AV

```
one Password= "one"
Service-Type = Shell-User
cisco-avpair = "shell:priv-lvl=15"
```

```
three Password = "three"
Service-Type = Login-User

four Password= "four"
Service-Type = Login-User
cisco-avpair = "shell:priv-lvl=7"
```

Cisco Secure ACS para a configuração de servidor Unix

```
# ./ViewProfile -p 9900 -u one
User Profile Information
user = one{
profile_id = 31
set server current-failed-logins = 0
profile_cycle = 3
radius=Cisco {
check_items= {
2="one"
}
reply_attributes= {
6=6
}
}
}
# ./ViewProfile -p 9900 -u three
User Profile Information
user = three{
profile_id = 32
set server current-failed-logins = 0
profile_cycle = 3
radius=Cisco {
check_items= {
2="three"
}
reply_attributes= {
6=1
}
}
}
# ./ViewProfile -p 9900 -u four
User Profile Information
user = four{
profile_id = 33
profile_cycle = 1
radius=Cisco {
check_items= {
2="four"
}
reply_attributes= {
6=1
9,1="shell:priv-lvl=7"
}
}
}
```

Configuração do servidor do Cisco Secure ACS for Windows

- User = um, tipo de serviço (atributo 6) = administrativo
- Usuário = três, tipo de serviço (atributo 6) = logon
- Usuário = quatro, tipo de serviço (atributo 6) = login, verifique o Cisco AV-pairs box e insira shell:priv-lvl=7

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Comandos para Troubleshooting

Os comandos seguintes são para debugar autenticação de HTTP útil. São emitidos no roteador.

Nota: Antes de emitir **comandos debug**, consulte Informações importantes sobre comandos debug.

- **monitor terminal** - Indicadores **comando debug** e mensagens de erro de sistema para o terminal atual e a sessão.
- **debugar a autenticação aaa** - Indica a informação na autenticação AAA/TACACS+.
- **debug aaa authorization** - Indica a informação na autorização AAA/TACACS+.
- **debugar o raio** - Indica o informação detalhada sobre debug associado com o RAIO.
- **debugar tacacs** - Indica a informação associada com o TACACS.
- **debug ip http authentication** - Use este comando pesquisar defeitos problemas da autenticação de HTTP. Indica o método de autenticação mensagens de status tentados e autenticação-específicos do roteador.

Informações Relacionadas

- Página de suporte do Cisco TACACS + software de acesso
- Página de suporte RADIUS
- Cisco Secure ACS para página de suporte do Windows
- Cisco Secure ACS para página de suporte do UNIX
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems