Como Atribuir Níveis de Privilégios com TACACS+ e RADIUS

Índice

Introdução

Este documento explica como alterar o nível de privilégio para determinados comandos e fornece um exemplo com partes de configurações de exemplo para um roteador e servidores TACACS+ e RADIUS.

Pré-requisitos

Requisitos

Os leitores deste documento devem ter o conhecimento dos níveis de privilégio em um roteador.

Àrevelia, há três níveis de privilégio no roteador.

- nível de privilégio 1 = NON-privilegiado (a alerta é `Roteador>`), o nível padrão para entrar
- nível de privilégio 15 = privilegiado (o prompt é número de roteador), o nível depois que se entra no modo de ativação
- o nível de privilégio 0 = usado raramente, mas inclui os comandos 5: **o desabilitação**, **permite**, **retira**, **ajuda**, e **saída**

Os níveis 2 a 14 não são usados em uma configuração padrão, mas os comandos que estão normalmente no nível 15 podem ser movidos para baixo para um desses níveis e os comandos que estão normalmente no nível 1 podem ser movidos para cima. Obviamente, este modelo de segurança envolve alguma administração no roteador.

Para determinar o nível de privilégio como um usuário que fez login, datilografe o **comando show privilege**. Para determinar que comandos estão disponíveis a nível de privilégio particular para a versão do software de Cisco IOS® que você está usando, datilografe a**?** na linha de comando

com logon efetuado nesse nível de privilégio.

Nota: Em vez de atribuir níveis de privilégio, você pode fazer o comando authorization se o Authentication Server apoia o TACACS+. O protocolo RADIUS não suporta autorização de comando.

Componentes Utilizados

A informação neste documento é baseada em Cisco IOS Software Release 11.2 e Mais Recente.

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.

Convenções

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

Exemplo

Neste exemplo, os **comandos snmp-server** são abaixados do nível de privilégio 15 (o padrão) para o nível de privilégio 7. **O comando ping** é movido do nível de privilégio 1 para o nível de privilégio 7. Quando o usuário sete é autenticado, esse usuário está atribuído o nível de privilégio 7 pelo server e o nível de privilégio atual dos indicadores de um **comando show privilege** “é 7." que o usuário pode sibilar e fazer a configuração de servidor snmp no modo de configuração. Outros comandos configuration não estão disponíveis.

Configurações - Roteador

Roteador - 11.2

```
aaa new-model
aaa authentication login default tacacs+|radius local
aaa authorization exec tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

Roteador - 11.3.3.T e mais tarde (até 12.0.5.T)

```
aaa new-model
aaa authentication login default tacacs+|radius local
aaa authorization exec default tacacs+|radius local
username backup privilege 7 password 0 backup
```

```
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

Roteador - 12.0.5.T e posterior

```
aaa new-model
aaa authentication login default group tacacs+|radius local
aaa authorization exec default group tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

Configurações - Servidor

Cisco Secure NT TACACS+

Execute as seguintes etapas para configurar o servidor.

1. Preencha o nome do usuário e a senha.
2. Em Configurações de Grupo, certifique-se de marcar shell/exec e de informar 7 na caixa em nível de privilégio.

TACACS+ - Estância no programa gratuito de servidor

```
aaa new-model
aaa authentication login default group tacacs+|radius local
aaa authorization exec default group tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

Cisco UNIX seguro TACACS+

```
aaa new-model
aaa authentication login default group tacacs+|radius local
aaa authorization exec default group tacacs+|radius local
```

```
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

RAIO do Cisco Secure NT

Execute as seguintes etapas para configurar o servidor.

1. Incorpore o nome de usuário e senha.
2. Em Group Settings (Configurações de Grupo) do IETF, o tipo de serviço (atributo 6) = Nas-Prompt
3. Na área CiscoRADIUS, verifique AV-Pair e na caixa retangular inferior, insira o shell:priv-lvl=7.

Cisco Secure UNIX RADIUS

```
aaa new-model
aaa authentication login default group tacacs+|radius local
aaa authorization exec default group tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

Este é o arquivo de usuário para o nome de usuário "seven".

Nota: O servidor deve suportar Cisco av-pairs.

- Senha sete = passwdxyz
- Tipo de serviço = Usuário Shell
- Cisco-avpair =shell:priv-lvl=7

Informações Relacionadas

- Página de suporte RADIUS
- Solicitações de Comentários (RFCs)
- TACACS+ na Documentação do IOS
- Página de suporte de TACACS+
- Página de suporte de UNIX Cisco Secure
- Cisco Secure ACS para página de suporte do Windows

- Suporte Técnico - Cisco Systems