Os níveis de privilégio de IOS não conseguem ver a configuração em execução completa

Contents

Introduction

Este documento explica como os níveis de privilégio afetam a capacidade de um usuário para executar determinados comandos em um roteador.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Exibir a configuração do roteador

Quando o acesso ao roteador é configurado por níveis de privilégio, um problema comum é que os comandos **show running ou write terminal são configurados no nível de privilégio do usuário ou abaixo dele.** Quando o usuário executa o comando, a configuração parece estar em branco. Isso é realmente proposital pelos motivos a seguir:

- O **comando write terminal/show running-config mostra uma configuração em branco.** Esse

comando exibe todos os comandos que o usuário atual é capaz de modificar (em outras palavras, todos os comandos no nível de privilégio atual do usuário ou abaixo dele). O comando não deverá exibir comandos acima do nível de privilégio atual do usuário devido a considerações de segurança. Em caso afirmativo, comandos como **snmp-server community podem ser usados para modificar a configuração atual do roteador e obter acesso completo a ele.**
- O comando **show config/show start-up config exibe uma configuração completa, mas não mostra a configuração real.** Em vez disso, o comando simplesmente imprime o conteúdo da NVRAM, que é a configuração do roteador no momento em que o usuário faz uma **gravação de memória**.

Níveis de privilégio

Para permitir que um usuário privilegiado visualize toda a configuração na memória, o usuário precisa modificar privilégios para todos os comandos que são configurados no roteador. Por exemplo:

```
aaa new-model
aaa authentication login default local
aaa authorization exec default local

username john privilege 9 password 0 doe
username six privilege 6 password 0 six
username poweruser privilege 15 password poweruser
username inout password inout
username inout privilege 15 autocommand show running

privilege configure level 8 snmp-server community
privilege exec level 6 show running
privilege exec level 8 configure terminal
```

Para entender este exemplo, é necessário entender os níveis de privilégio. Por padrão, há três níveis de comando no roteador:

- nível de privilégio 0 — inclui os comandos desable**, enable, exit, help e logout.**
- nível de privilégio 1 — nível Normal na Telnet; inclui todos os comandos de nível de usuário no prompt `router>`.
- nível de privilégio 15 — inclui todos os comandos de nível de permissão no prompt router#.

Os comandos disponíveis em um nível específico de um determinado roteador podem ser encontrados digitando **?** no prompt do roteador. Os comandos podem ser movidos entre os níveis de privilégio usando o **comando privilege, conforme mostrado no exemplo.** Embora este exemplo mostre a autenticação e a autorização local, os comandos funcionam de forma semelhante para a autenticação TACACS+ ou RADIUS e a autorização de execução (maior granularidade no controle do roteador pode ser obtida com a implementação da autorização de comando TACACS+ com um servidor).

Os detalhes adicionais sobre os usuários e os níveis de privilégio são apresentados no exemplo:

- O usuário *seis é capaz de executar o* **comando show run da Telnet, mas a configuração resultante é praticamente em branco, pois esse usuário não pode configurar algo (configure terminal fica no nível 8, não no nível 6).** O usuário não tem permissão de ver os nomes de

usuário e senhas de outros usuários ou ver as informações do SNMP (Simple Network Management Protocol).

- O usuário *john é capaz de executar a Telnet e o* **comando show run, mas vê apenas os comandos que ele pode configurar (o snmp-server community faz parte da configuração do roteador, já que este usuário é o nosso administrador de gerenciamento de rede).** Ele pode configurar **snmp-server community porque configure terminal está no nível 8 (no igual ou abaixo de 9), e snmp-server community é um comando de nível 8.** O usuário não tem permissão para ver os nomes de usuário e senhas de outros usuários, mas ele é confiável com a configuração do SNMP.
- O usuário inout é capaz entrar na Telnet e, como está sendo configurado para **show autocommand running**, vê a configuração exibida, mas é desconectado depois disso.
- O usuário *poweruser é capaz de entrar na Telnet e executar o* **comando show run.** Este usuário está no nível 15 e pode ver todos os comandos. Todos os comandos estão no nível 15; ou abaixo os usuários neste nível também podem exibir e controlar nomes de usuário e senhas.

Informações Relacionadas

- Ferramenta Command Lookup (somente clientes registrados)
- Documentação do IOS para TACACS+ e RADIUS
- Página de Suporte do TACACS/TACACS+
- Página de suporte RADIUS
- Solicitações de Comentários (RFCs)
- Suporte Técnico - Cisco Systems