Os níveis de privilégio IO não podem considerar a configuração running completa

Índice

Introdução

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

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

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

Veja a configuração de roteador

Quando o acesso ao roteador é configurado por níveis de privilégio, um problema comum é que os **comandos show running or write terminal** estão configurados a ou abaixo do nível de privilégio do usuário. Quando o usuário executa o comando, a configuração parece estar vazia. Isto é realmente pelo projeto por estas razões:

- **O terminal/comando show running-config da escrita** mostra uma configuração vazia. Este comando indica todos os comandos que o usuário atual pode alterar (ou seja todos os comandos a ou abaixo do nível de privilégio atual do usuário). O comando não deve comandos display acima do nível de privilégio atual do usuário devido às considerações de segurança. Em caso afirmativo, os comandos tais como a **comunidade do servidor snmp** podiam ser usados para alterar a configuração atual do roteador e para ganhar o acesso completo ao roteador.
- **O comando show config/show start-up config** indica uma configuração direta, mas não mostra verdadeiramente a configuração real. Em lugar de, o comando imprime simplesmente - para fora os índices do NVRAM, que acontece ser a configuração do roteador naquele tempo o usuário fazem uma **memória da escrita**.

Níveis de privilégio

Para permitir um usuário privilegiado de ver a configuração completa na memória, o usuário precisa de alterar privilégios para os comandos all 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 compreender este exemplo, é necessário compreender níveis de privilégio. À revelia, há três níveis de comando no roteador:

- nível de privilégio 0 — Inclui o **desabilitação**, **permitem-no**, **comandos exit, help, e logout**.
- nível de privilégio 1 — Normal em nível no telnet; inclui todos os comandos do nível de usuário na alerta do `Roteador>`.
- nível de privilégio 15 — Inclui todos os comandos do permitir-nível na alerta do `router-`.

Os comandos disponíveis a nível particular em um roteador particular podem ser encontrados pela de datilografia**?** na alerta de roteador. Os comandos podem ser movidos entre níveis de privilégio usando o **comando privilege**, como ilustrado no exemplo. Quando este exemplo mostrar a autenticação local e a autorização, os comandos trabalham similarmente para o TACACS+ ou a autenticação RADIUS e a autorização de exec (mais granularidade no controle do roteador pode ser conseguida com aplicação da autorização do comando tacacs+ com um server.)

Detalhes adicionais nos usuários e nos níveis de privilégio apresentados no exemplo:

- O usuário *seis* pode ao telnet dentro e executa o **comando show run**, mas a configuração resultante está virtualmente vazia porque este usuário não pode configurar qualquer coisa (**configurar o terminal** está a nível 8, não a nível 6). O usuário não é permitido para ver nomes de usuário e senha dos outros usuários, ou para ver a informação do Simple Network

Management Protocol (SNMP).

- O usuário *john* pode ao telnet dentro e executa o **comando show run**, mas vê somente os comandos que pode configurar (a **comunidade do servidor snmp** parte da configuração de roteador, desde que este usuário é nosso administrador do Gerenciamento de redes). Pode configurar a **comunidade do servidor snmp** porque **configurar o terminal** está a nível 8 (a ou abaixo do nível 9), e a **comunidade do servidor snmp** é um comando do nível 8. O usuário não é permitido para ver nomes de usuário e senha dos outros usuários, mas é confiado com a configuração de SNMP.
- O inout de usuário pode ao telnet dentro, e, em virtude de ser configurado para o **corredor da mostra do comando automático**, vê a configuração indicada mas é desligado depois disso.
- *O poweruser do* usuário pode ao telnet dentro e executa o **comando show run**. Este usuário pode a nível 15, e é ver comandos all. Os comandos all são a ou abaixo do nível 15; os usuários neste nível podem igualmente ver e controlar nomes de usuário e senha.

Informações Relacionadas

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