

Configurar o SNMPv2c/v3 nos switches Catalyst 9000 Series

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Pré-requisitos para SNMP](#)

[Diagrama de Rede](#)

[SNMPv2c](#)

[SNMPv3](#)

[noAuthNoPriv](#)

[authNoPriv](#)

[auth-SHA](#)

[auth-MD5](#)

[authPriv](#)

[auth-SHA + priv-DES](#)

[auth-SHA + priv-AES](#)

[auth-MD5 + priv-DES](#)

[auth-MD5 + priv-AES](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve a configuração básica de SNMPv2c e SNMPv3 nos Switches Catalyst 9000.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Protocolo SNMP (Simple Network Management Protocol).
- Familiaridade com os switches Catalyst 9000 Series.
- Familiaridade com o Identificador de Objeto (OID - Object Identifier) SNMP.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- C9200
- C9300
- C9400
- C9500
- C9600
- Software Cisco IOS® XE & 17.X

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 a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Pré-requisitos para SNMP

O SNMPv1 e o SNMPv2C usam uma forma de segurança baseada em comunidade. A comunidade de gerentes capazes de acessar a MIB do agente é definida por uma lista de controle de acesso e senha de endereço IP.

O SNMPv2C inclui uma função de recuperação em massa e um relatório de mensagem de erro mais detalhado para as estações de gerenciamento. A função de recuperação em massa recupera tabelas e grandes quantidades de informações, minimizando o número de percursos circulares necessários. O tratamento de erros melhorado do SNMPv2C inclui códigos de erro expandidos que distinguem diferentes tipos de condições de erro; essas condições são reportadas por meio de um único código de erro no SNMPv1. Os códigos de retorno de erro no SNMPv2C reportam o tipo de erro.

O SNMPv3 fornece modelos de segurança e níveis de segurança. Um modelo de segurança é uma estratégia de autenticação configurada para um usuário e o grupo no qual o usuário reside. Um nível de segurança é o nível permitido de segurança em um modelo de segurança. Uma combinação do nível de segurança e do modelo de segurança determina qual método de segurança é usado ao manipular um pacote SNMP. Os modelos de segurança disponíveis são SNMPv1, SNMPv2C e SNMPv3.

Esta tabela identifica características e compara diferentes combinações de modelos e níveis de segurança:

Modelo	Nível	Autenticação	Criptografia	Resultado
SNMPv1	noAuthNoPriv	Sequência de caracteres de comunidade	No	Usa uma comparação de série de comunidade para autenticação.
SNMPv2C	noAuthNoPriv	Sequência de caracteres de comunidade	No	Usa uma comparação de série de comunidade para autenticação.
SNMPv3	noAuthNoPriv	Nome de usuário	No	Usa uma correspondência de nome de usuário para autenticação.
SNMPv3	authNoPriv	Message Digest 5	No	Fornece autenticação com

Modelo	Nível	Autenticação	Criptografia	Resultado
		(MD5) ou Secure Hash Algorithm (SHA)		base nos algoritmos HMAC-MD5 ou HMAC-SHA.
SNMPv3	authPriv	MD5 ou SHA	Padrão de Criptografia de Dados (DES) ou Padrão de Criptografia Avançada (AES)	Fornece autenticação com base nos algoritmos HMAC-MD5 ou HMAC-SHA. Permite especificar o Modelo de Segurança Baseado no Usuário (USM - User-based Security Model) com estes algoritmos de criptografia: • Criptografia DES de 56 bits, além da autenticação baseada no padrão CBC-DES (DES-56). • Criptografia 3DES de 168 bits • Criptografia AES de 128, 192 ou 256 bits

Diagrama de Rede



SNMPv2c

Config

```
Switch(config)#snmp-server community cisco RW      >Read-only access with this community string
Switch(config)#snmp-server community cisco RO      >Read-write access with this community string
```

Verificar

```
Switch#show snmp community
Community name: cisco
Community Index: cisco
Community SecurityName: cisco
storage-type: nonvolatile active
```

```
~ % snmpwalk -v2c -c cisco 192.168.1.1 1.3.6.1.2.1.1.3
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (111410969) 12 days, 21:28:29.69
```

SNMPv3

noAuthNoPriv

Config

```
Switch(config)#snmp-server group noAuthNoPrivGroup v3 noauth
Switch(config)#snmp-server user testuser1 noAuthNoPrivGroup v3
```

Verificar

```
Switch#show snmp user
User name: testuser1
Engine ID: 800000090300EC1D8B0A7B80
storage-type: nonvolatile active
Authentication Protocol: None
Privacy Protocol: None
Group-name: noAuthNoPrivGroup
```

```
~ % snmpwalk -v3 -u testuser1 -l noAuthNoPriv 192.168.1.1 1.3.6.1.2.1.1.3
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (111425887) 12 days, 21:30:58.87
```

authNoPriv

auth-SHA

Config

```
Switch(config)#snmp-server group AuthNoPrivGroup v3 auth
Switch(config)#snmp-server user testuser2 AuthNoPrivGroup v3 auth sha Password123
```

Verificar

```
Switch#show snmp user
User name: testuser2
Engine ID: 800000090300EC1D8B0A7B80
storage-type: nonvolatile active
Authentication Protocol: SHA
Privacy Protocol: None
Group-name: AuthNoPrivGroup
```

```
~ % snmpwalk -v3 -u testuser3 -l authNoPriv -a MD5 -A Password123 192.168.1.1 1.3.6.1.2.1.1.3
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (111447478) 12 days, 21:34:34.78
```

auth-MD5

Config

```
Switch(config)#snmp-server group AuthNoPrivGroup v3 auth
Switch(config)#snmp-server user testuser3 AuthNoPrivGroup v3 auth md5 Password123
```

Verificar

```
Switch#show snmp user
User name: testuser3
Engine ID: 800000090300EC1D8B0A7B80
storage-type: nonvolatile active
Authentication Protocol: MD5
Privacy Protocol: None
Group-name: AuthNoPrivGroup
```

```
~ % snmpwalk -v3 -u testuser3 -l authNoPriv -a MD5 -A Password123 192.168.1.1 1.3.6.1.2.1.1.3
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (111455526) 12 days, 21:35:55.26
```

authPriv

auth-SHA + priv-DES

Config

```
Switch(config)#snmp-server group AuthPrivGroup v3 priv
Switch(config)#snmp-server user testuser4 AuthPrivGroup v3 auth sha Password123 priv des Password123
```

Verificar

```
Switch#show snmp user
User name: testuser4
Engine ID: 800000090300EC1D8B0A7B80
storage-type: nonvolatile active
Authentication Protocol: SHA
Privacy Protocol: DES
Group-name: AuthPrivGroup
```

```
~ % snmpwalk -v3 -u testuser4 -l authPriv -a SHA -A Password123 -x DES -X Password123 192.168.1.1 1.3.6
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (111472744) 12 days, 21:38:47.44
```

auth-SHA + priv-AES

Config

```
Switch(config)#snmp-server group AuthPrivGroup v3 priv
Switch(config)#snmp-server user testuser5 AuthPrivGroup v3 auth sha Password123 priv aes 128 Password123
```

Verificar

```
Switch#show snmp user
User name: testuser5
Engine ID: 800000090300EC1D8B0A7B80
storage-type: nonvolatile active
Authentication Protocol: SHA
Privacy Protocol: AES128
Group-name: AuthPrivGroup
```

```
~ % snmpwalk -v3 -u testuser5 -l authPriv -a SHA -A Password123 -x AES -X Password123 192.168.1.1 1.3.6
```

DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (111476608) 12 days, 21:39:26.08

auth-MD5 + priv-DES

Config

```
Switch(config)#snmp-server group AuthPrivGroup v3 priv
Switch(config)#snmp-server user testuser6 AuthPrivGroup v3 auth md5 Password123 priv des Password123
```

Verificar

```
Switch#show snmp user
User name: testuser6
Engine ID: 800000090300EC1D8B0A7B80
storage-type: nonvolatile active
Authentication Protocol: MD5
Privacy Protocol: DES
Group-name: AuthPrivGroup
```

```
~ % snmpwalk -v3 -u testuser6 -l authPriv -a MD5 -A Password123 -x DES -X Password123 192.168.1.1 1.3.6
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (76726018) 8 days, 21:07:40.18
```

auth-MD5 + priv-AES

Config

```
Switch(config)#snmp-server group AuthPrivGroup v3 priv
Switch(config)#snmp-server user testuser7 AuthPrivGroup v3 auth md5 Password123 priv aes 128 Password123
```

Verificar

```
Switch#show snmp user
User name: testuser7
Engine ID: 800000090300EC1D8B0A7B80
storage-type: nonvolatile active
Authentication Protocol: MD5
Privacy Protocol: AES128
Group-name: AuthPrivGroup
```

```
~ % snmpwalk -v3 -u testuser7 -l authPriv -a MD5 -A Password123 -x AES -X Password123 192.168.1.1 1.3.6
```

DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (76738170) 8 days, 21:09:41.70

Informações Relacionadas

- [Guia de configuração de gerenciamento de rede, Cisco IOS XE 17.15.x \(switches Catalyst 9300\)](#)
- [Navegador de objeto SNMP Navigator](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.