

Configuración de SNMPv2c/v3 en switches Catalyst serie 9000

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Prerrequisitos de SNMP](#)

[Diagrama de la red](#)

[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](#)

[Información Relacionada](#)

Introducción

Este documento describe la configuración básica de SNMPv2c y SNMPv3 en los switches Catalyst 9000.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Protocolo SNMP (protocolo simple de administración de red).
- Familiaridad con los switches Catalyst serie 9000.
- Familiaridad con el identificador de objeto SNMP (OID).

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Prerrequisitos de SNMP

Tanto SNMPv1 como SNMPv2C utilizan una forma de seguridad basada en la comunidad. La comunidad de administradores que pueden acceder a la MIB del agente se define mediante una lista de control de acceso a la dirección IP y una contraseña.

SNMPv2C incluye una función de recuperación masiva y un informe de mensajes de error más detallado para las estaciones de administración. La función de recuperación masiva recupera tablas y grandes cantidades de información, minimizando el número de viajes de ida y vuelta necesarios. El control de errores mejorado de SNMPv2C incluye códigos de error expandidos que distinguen diferentes tipos de condiciones de error; estas condiciones se notifican mediante un único código de error en SNMPv1. Los códigos de retorno de error en SNMPv2C informan del tipo de error.

SNMPv3 proporciona modelos y niveles de seguridad. Un modelo de seguridad es una estrategia de autenticación configurada para un usuario y el grupo en el que reside el usuario. Un nivel de seguridad es el nivel de seguridad permitido dentro de un modelo de seguridad. Una combinación del nivel de seguridad y el modelo de seguridad determinan qué método de seguridad se utiliza al gestionar un paquete SNMP. Los modelos de seguridad disponibles son SNMPv1, SNMPv2C y SNMPv3.

En esta tabla se identifican las características y se comparan diferentes combinaciones de niveles y modelos de seguridad:

Modelo	'Nivel'	Autenticación	Cifrado	Resultado
SNMPv1	noAuthNoPriv	Cadena de comunidad	No	Usa una correspondencia de identificaciones de comunidad para autenticación.
SNMPv2C	noAuthNoPriv	Cadena de comunidad	No	Usa una correspondencia de identificaciones de comunidad para autenticación.
SNMPv3	noAuthNoPriv	Nombre de usuario	No	Utiliza las coincidencias de nombre de usuario

Modelo	'Nivel'	Autenticación	Cifrado	Resultado
				para autenticar.
SNMPv3	authNoPriv	Algoritmo de resumen de mensajes 5 (MD5) o Algoritmo de hash seguro (SHA)	No	Proporciona autenticación sobre la base de algoritmos HMAC-MD5 o HMAC-SHA.
SNMPv3	authPriv	MD5 o SHA	Estándar de cifrado de datos (DES) o Estándar de cifrado avanzado (AES)	Proporciona autenticación sobre la base de algoritmos HMAC-MD5 o HMAC-SHA. Permite especificar el modelo de seguridad basado en el usuario (USM) con estos algoritmos de cifrado: • Cifrado DES de 56 bits además de la autenticación basada en el estándar CBC-DES (DES-56). • Encriptación 3DES de 168 bits • Cifrado AES de 128 bits, 192 bits o 256 bits

Diagrama de la red



SNMPv2c

Config

```
Switch(config)#snmp-server community cisco RW
Switch(config)#snmp-server community cisco RO
```

```
>Read-only access with this community string
>Read-write access with this community string
```

Verificación

```
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
```

Verificación

```
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
```

Verificación

```
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
```

Verificación

```
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
```

Verificación

```
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
```

Verificación

```
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
```

Verificación

```
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 Password12
```

Verificación

```
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
```

Información Relacionada

- [Guía de configuración de administración de redes, Cisco IOS XE 17.15.x \(switches Catalyst 9300\)](#)
- [Navegador de objeto SNMP](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).