

Konfigurieren von SNMPv2c/v3 auf Catalyst Switches der Serie 9000

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Voraussetzungen für SNMP](#)

[Netzwerkdiagramm](#)

[SNMPv2c](#)

[SNMPv3](#)

[neinAuthNeinPriv](#)

[AuthNrPriv](#)

[auth-SHA](#)

[auth-MD5](#)

[AuthPriv](#)

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

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

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

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

[Zugehörige Informationen](#)

Einleitung

Dieses Dokument beschreibt die grundlegende Konfiguration von SNMPv2c und SNMPv3 auf Catalyst 9000-Switches.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- SNMP-Protokoll (Simple Network Management Protocol).
- Vertrautheit mit Catalyst Switches der Serie 9000
- Kompatibilität mit SNMP Object Identifier (OID)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Voraussetzungen für SNMP

Sowohl SNMPv1 als auch SNMPv2C verwenden eine Community-basierte Form der Sicherheit. Die Community der Manager, die auf die MIB des Agenten zugreifen können, wird durch eine Zugriffskontrollliste mit IP-Adressen und ein Passwort definiert.

SNMPv2C umfasst eine Massenabruffunktion und detailliertere Fehlermeldungen, die an Verwaltungsstationen gemeldet werden. Die Bulk-Retrieval-Funktion ruft Tabellen und große Informationsmengen ab und minimiert so die Anzahl der erforderlichen Round-Trips. Die verbesserte Fehlerbehandlung von SNMPv2C umfasst erweiterte Fehlercodes, die verschiedene Arten von Fehlerzuständen unterscheiden. Diese Bedingungen werden über einen einzelnen Fehlercode in SNMPv1 gemeldet. Fehlerrückgabecodes in SNMPv2C geben den Fehlertyp an.

SNMPv3 bietet sowohl Sicherheitsmodelle als auch Sicherheitsstufen. Ein Sicherheitsmodell ist eine Authentifizierungsstrategie, die für einen Benutzer und die Gruppe, in der sich der Benutzer befindet, eingerichtet wurde. Eine Sicherheitsstufe ist die zulässige Sicherheitsstufe innerhalb eines Sicherheitsmodells. Durch eine Kombination aus Sicherheitsstufe und Sicherheitsmodell wird festgelegt, welche Sicherheitsmethode bei der Verarbeitung eines SNMP-Pakets verwendet wird. Verfügbare Sicherheitsmodelle sind SNMPv1, SNMPv2C und SNMPv3.

In dieser Tabelle werden die Merkmale beschrieben und verschiedene Kombinationen von Sicherheitsmodellen und Sicherheitsstufen verglichen:

Modell	Stufe	Authentifizierung	Verschlüsselung	Ergebnis
SNMPv1	neinAuthNeinPriv	Community-String	Nein	Verwendet einen Community-String-Abgleich für die Authentifizierung.
SNMPv2C	neinAuthNeinPriv	Community-String	Nein	Verwendet einen Community-String-Abgleich für die Authentifizierung.
SNMPv3	neinAuthNeinPriv	Benutzername	Nein	Verwendet einen Benutzernamen-Abgleich für die Authentifizierung.
SNMPv3	AuthNrPriv	Message Digest 5 (MD5) oder	Nein	Bietet Authentifizierung auf Basis der HMAC-MD5- oder

Modell	Stufe	Authentifizierung	Verschlüsselung	Ergebnis
		Secure Hash Algorithm (SHA)		HMAC-SHA-Algorithmen.
SNMPv3	AuthPriv	MD5 oder SHA	DES (Data Encryption Standard) oder AES (Advanced Encryption Standard)	Bietet Authentifizierung auf Basis der HMAC-MD5- oder HMAC-SHA-Algorithmen. Ermöglicht die Angabe des benutzerbasierten Sicherheitsmodells (USM) mit folgenden Verschlüsselungsalgorithmen: • DES 56-Bit-Verschlüsselung zusätzlich zur Authentifizierung nach dem CBC-DES (DES-56)-Standard. • 3DES 168-Bit-Verschlüsselung • AES-Verschlüsselung mit 128, 192 oder 256 Bit

Netzwerkdiagramm



SNMPv2c

Konfig.

```
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
```

Überprüfung

```
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

neinAuthNeinPriv

Konfig.

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

Überprüfung

```
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
```

AuthNrPriv

auth-SHA

Konfig.

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

Überprüfung

```
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

Konfig.

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

Überprüfung

```
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

Konfig.

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

Überprüfung

```
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

Konfig.

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

Überprüfung

```
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

Konfig.

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

Überprüfung

```
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

Konfig.

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

Überprüfung

```
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

Zugehörige Informationen

- [Konfigurationsanleitung für die Netzwerkverwaltung, Cisco IOS XE 17.15.x \(Catalyst 9300 Switches\)](#)
- [SNMP Object Navigator](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.