# SNMP verwalten (nur für Cluster-Administratoren)

ONTAP 9

NetApp
November 05, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/networking/manage_snmp_on_the_cluster_cluster_administrators_only_overview.html on November 05, 2026. Always check docs.netapp.com for the latest.

# Inhalt


SNMP verwalten (nur für Cluster-Administratoren) . . . 1
Informationen zu SNMP im ONTAP Netzwerk . . . 1
MIB-Übersicht . . . 1
SNMP-Traps . . . 2
Standard SNMP-Traps . . . 2
Integrierte SNMP-Traps . . . 2
SNMP-Communities für das ONTAP Netzwerk erstellen . . . 2
Konfigurieren von SNMPv3 Benutzern in einem ONTAP Cluster . . . 5
SNMPv3 Sicherheitsparameter . . . 5
Beispiele für verschiedene Sicherheitsstufen . . . 6
Traphosts für SNMP im ONTAP Netzwerk konfigurieren . . . 9
SNMP-Abfrage in einem ONTAP Cluster überprüfen . . . 10
ONTAP Befehle zur Verwaltung von SNMP, Traps und Traphosts . . . 11
Befehle zur Konfiguration von SNMP . . . 11
Befehle zur Verwaltung von SNMP v1, v2c und v3 Benutzern . . . 12
Befehle zur Bereitstellung von Kontakt- und Standortinformationen . . . 12
Befehle zur Verwaltung von SNMP-Communities . . . 12
Befehl zum Anzeigen von SNMP Optionswerten . . . 12
Befehle zur Verwaltung von SNMP-Traps und Traphosts . . . 12
Befehle zur Verwaltung von Ereignissen im Zusammenhang mit SNMP-Traps . . . 13

# SNMP verwalten (nur für Cluster-Administratoren)

## Informationen zu SNMP im ONTAP Netzwerk

SNMP kann so konfiguriert werden, dass SVMs in Ihrem Cluster überwacht werden, um Probleme zu vermeiden, bevor sie auftreten, und um auf Probleme zu reagieren, falls sie auftreten. Die Verwaltung von SNMP umfasst die Konfiguration von SNMP-Benutzern und die Konfiguration von SNMP-Traphost-Zielen (Management-Workstations) für alle SNMP-Ereignisse. SNMP ist auf Daten-LIFs standardmäßig deaktiviert.

Sie können im Daten-SVM schreibgeschützte SNMP-Benutzer erstellen und verwalten. Daten-LIFs müssen so konfiguriert sein, dass sie SNMP-Anfragen auf dem SVM empfangen.

SNMP-Netzwerkmanagement-Workstations oder Manager können den SVM-SNMP-Agenten nach Informationen abfragen. Der SNMP-Agent sammelt Informationen und leitet sie an die SNMP-Manager weiter. Der SNMP-Agent generiert außerdem Trap-Benachrichtigungen, sobald bestimmte Ereignisse eintreten. Der SNMP-Agent auf dem SVM verfügt über Leserechte, er kann weder für Set-Operationen noch zur Durchführung einer Korrekturmaßnahme als Reaktion auf einen Trap verwendet werden. ONTAP stellt einen SNMP-Agenten bereit, der mit den SNMP-Versionen v1, v2c und v3 kompatibel ist. SNMPv3 bietet erweiterte Sicherheit durch die Verwendung von Passphrasen und Verschlüsselung.

Weitere Informationen zur SNMP-Unterstützung in ONTAP-Systemen sind unter "TR-4220: SNMP-Unterstützung in Data ONTAP" zu finden.

### MIB-Übersicht

Eine MIB (Management Information Base) ist eine Textdatei, die SNMP-Objekte und Traps beschreibt.

MIBs beschreiben die Struktur der Verwaltungsdaten des Speichersystems und verwenden einen hierarchischen Namensraum mit Objektbezeichnern (OIDs). Jede OID identifiziert eine Variable, die mit SNMP ausgelesen werden kann.

Da MIBs keine Konfigurationsdateien sind und ONTAP diese Dateien nicht liest, wird die SNMP-Funktionalität durch MIBs nicht beeinträchtigt. ONTAP stellt die folgende MIB-Datei bereit:

- Ein NetApp benutzerdefinierter MIB (`netapp.mib`)

ONTAP unterstützt IPv6 (RFC 2465), TCP (RFC 4022), UDP (RFC 4113) und ICMP (RFC 2466) MIBs, die sowohl IPv4- als auch IPv6-Daten anzeigen, werden unterstützt.

ONTAP bietet außerdem eine kurze Querverweisfunktion zwischen Objektbezeichnern (OIDs) und Objektkurznamen in der `traps.dat` Datei.

> Die neuesten Versionen der ONTAP MIBs und der `traps.dat`-Dateien sind auf der NetApp Support Site verfügbar. Die Versionen dieser Dateien auf der Support Site entsprechen jedoch nicht unbedingt den SNMP-Funktionen Ihrer ONTAP Version. Diese Dateien werden bereitgestellt, um die Evaluierung der SNMP-Funktionen in der neuesten ONTAP Version zu unterstützen.

### SNMP-Traps

SNMP-Traps erfassen Systemüberwachungsinformationen, die als asynchrone Benachrichtigung vom SNMP-Agenten an den SNMP-Manager gesendet werden.

Es gibt drei Arten von SNMP-Traps: Standard, integriert und benutzerdefiniert. Benutzerdefinierte Traps werden in ONTAP nicht unterstützt.

Mithilfe eines Traps kann regelmäßig auf im MIB definierte Betriebsschwellenwerte oder Fehler geprüft werden. Wird ein Schwellenwert erreicht oder ein Fehler erkannt, sendet der SNMP-Agent eine Nachricht (Trap) an die Traphosts und benachrichtigt sie über das Ereignis.

ONTAP unterstützt SNMPv1- und SNMPv3-Traps. ONTAP unterstützt keine SNMPv2c-Traps und INFORMs.

### Standard SNMP-Traps

Diese Traps sind in RFC 1215 definiert. Es gibt fünf Standard-SNMP-Traps, die von ONTAP unterstützt werden: coldStart, warmStart, linkDown, linkUp und authenticationFailure.

Die authenticationFailure Trap ist standardmäßig deaktiviert. Der `system snmp authtrap` Befehl muss verwendet werden, um die Trap zu aktivieren. Weitere Informationen zu `system snmp authtrap` finden sich in der "ONTAP-Befehlsreferenz".

### Integrierte SNMP-Traps

Integrierte Traps sind in ONTAP vordefiniert und werden bei einem Ereignis automatisch an die Netzwerkmanagementstationen auf der Traphost-Liste gesendet. Diese Traps, wie diskFailedShutdown, cpuTooBusy und volumeNearlyFull, sind in der benutzerdefinierten MIB definiert.

Jede integrierte Falle wird durch einen eindeutigen Fallencode identifiziert.

# SNMP-Communities für das ONTAP Netzwerk erstellen

Es kann eine SNMP-Community erstellt werden, die als Authentifizierungsmechanismus zwischen der Management-Station und der Storage Virtual Machine (SVM) bei Verwendung von SNMPv1 und SNMPv2c dient.

Durch das Erstellen von SNMP-Communities in einer Daten-SVM lassen sich Befehle wie `snmpwalk` und `snmpget` auf den Daten-LIFs ausführen.

**Über diese Aufgabe**

- Bei Neuinstallationen von ONTAP sind SNMPv1 und SNMPv2c standardmäßig deaktiviert.

  SNMPv1 und SNMPv2c sind aktiviert, nachdem eine SNMP-Community erstellt wurde.

- ONTAP unterstützt schreibgeschützte Communities.
- Standardmäßig ist die Firewall-Richtlinie "data", die Daten-LIFs zugewiesen ist, so eingestellt, dass der SNMP-Dienst auf `deny` gesetzt ist.

  Sie müssen eine neue Firewall-Richtlinie erstellen, bei der der SNMP-Dienst auf `allow` gesetzt ist, wenn

ein SNMP-Benutzer für eine Daten-SVM erstellt wird.

> Ab ONTAP 9.10.1 sind Firewall-Richtlinien veraltet und vollständig durch LIF-Dienstrichtlinien ersetzt. Weitere Informationen finden sich unter "Firewall-Richtlinien für LIFs konfigurieren".

- Sie können SNMP-Communities für SNMPv1- und SNMPv2c-Benutzer sowohl für die Admin SVM als auch für die Daten SVM erstellen.
- Da eine SVM nicht Teil des SNMP-Standards ist, müssen Abfragen von Daten-LIFs die NetApp Root-OID (1.3.6.1.4.1.789) enthalten, zum Beispiel `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`.

**Schritte**

1. Eine SNMP-Community wird mit dem `system snmp community add` Befehl erstellt. Der folgende Befehl zeigt, wie eine SNMP-Community im Admin-SVM Cluster-1 erstellt wird:

```
system snmp community add -type ro -community-name comty1 -vserver
cluster-1
```

   Der folgende Befehl zeigt, wie eine SNMP-Community in der Daten-SVM vs1 erstellt wird:

```
system snmp community add -type ro -community-name comty2 -vserver vs1
```

2. Es kann mit dem Befehl system snmp community show überprüft werden, ob die Communities erstellt wurden.

   Der folgende Befehl zeigt die beiden für SNMPv1 und SNMPv2c erstellten Communities an:

```
system snmp community show
cluster-1
rocomty1
vs1
rocomty2
```

3. Es kann mit dem `system services firewall policy show` Befehl überprüft werden, ob SNMP als Dienst in der „data“ Firewall-Richtlinie erlaubt ist.

   Der folgende Befehl zeigt, dass der SNMP-Dienst in der Standard-„data“-Firewallrichtlinie nicht zugelassen ist (der SNMP-Dienst ist nur in der „mgmt“-Firewallrichtlinie zugelassen):

```
system services firewall policy show
Vserver Policy       Service    Allowed
------- ------------ ---------- -------------------
cluster-1
        data
```

```
                     dns         0.0.0.0/0
                     ndmp        0.0.0.0/0
                     ndmps       0.0.0.0/0
cluster-1
        intercluster
                     https       0.0.0.0/0
                     ndmp        0.0.0.0/0
                     ndmps       0.0.0.0/0
cluster-1
        mgmt
                     dns         0.0.0.0/0
                     http        0.0.0.0/0
                     https       0.0.0.0/0
                     ndmp        0.0.0.0/0
                     ndmps       0.0.0.0/0
                     ntp         0.0.0.0/0
                     snmp        0.0.0.0/0
                     ssh         0.0.0.0/0
```

4. Eine neue Firewall-Richtlinie wird erstellt, die den Zugriff mit dem `snmp` Service unter Verwendung des `system services firewall policy create` Befehls erlaubt.

   Die folgenden Befehle erstellen eine neue Datenfirewall-Richtlinie mit dem Namen „data1“, die das `snmp`

```
system services firewall policy create -policy data1 -service snmp
-vserver  vs1 -allow-list 0.0.0.0/0

cluster-1::> system services firewall policy show -service snmp
Vserver  Policy       Service    Allowed
-------  ------------ ---------- -------------------
cluster-1
         mgmt
                      snmp       0.0.0.0/0
vs1
         data1
                      snmp       0.0.0.0/0
```

5. Die Firewall-Richtlinie wird auf eine Daten-LIF angewendet, indem der `network interface modify` Befehl mit dem Parameter -firewall-policy verwendet wird.

   Der folgende Befehl weist die neue Firewall-Richtlinie "data1" dem LIF "datalif1" zu:

```
network interface modify -vserver vs1 -lif datalif1 -firewall-policy
data1
```

Weitere Informationen zu `network interface modify` finden sich in der "ONTAP-Befehlsreferenz".

# Konfigurieren von SNMPv3 Benutzern in einem ONTAP Cluster

SNMPv3 ist im Vergleich zu SNMPv1 und SNMPv2c ein sicheres Protokoll. Für die Verwendung von SNMPv3 ist die Konfiguration eines SNMPv3-Benutzers erforderlich, um die SNMP-Dienstprogramme vom SNMP-Manager aus auszuführen.

**Schritt**

Mit dem `security login create` Befehl wird ein SNMPv3-Benutzer erstellt.

Sie werden aufgefordert, folgende Informationen anzugeben:

- Engine ID: Standardwert und empfohlener Wert ist die lokale Engine ID
- Authentifizierungsprotokoll
- Authentifizierungspasswort
- Datenschutzprotokoll
- Passwort für Datenschutzprotokoll

**Ergebnis**

Der SNMPv3-Benutzer kann sich vom SNMP-Manager aus mit Benutzername und Passwort anmelden und die SNMP-Dienstprogrammbefehle ausführen.

Ab ONTAP 9.20.1 können Sie SNMPv3-Benutzer erstellen, die SHA-512-Authentifizierung verwenden. Sie können nur Benutzer erstellen und löschen, die SHA-512-Authentifizierung verwenden. Das Authentifizierungsprotokoll eines vorhandenen Benutzers kann nicht geändert werden. Zum Ändern des Authentifizierungsprotokolls ist es erforderlich, den Benutzer zu löschen und erneut zu erstellen.

## SNMPv3 Sicherheitsparameter

SNMPv3 beinhaltet eine Authentifizierungsfunktion, die, wenn sie ausgewählt ist, von den Benutzern verlangt, ihren Namen, ein Authentifizierungsprotokoll, einen Authentifizierungsschlüssel und das gewünschte Sicherheitsniveau beim Aufruf eines Befehls einzugeben.

Die folgende Tabelle listet die SNMPv3 Sicherheitsparameter auf:

| Parameter | Befehlszeilenoption | Beschreibung |
|---|---|---|
| engineID | -e EngineID | Engine ID des SNMP-Agenten. Standardwert ist die lokale Engine ID (empfohlen). |
| securityName | -u Name | Der Benutzername darf maximal 32 Zeichen lang sein. |
| authProtocol | -a {none | MD5 |
| SHA | SHA-256 | SHA-512} |

| | | |
|---|---|---|
| Der Authentifizierungstyp kann none, MD5, SHA, SHA-256 oder SHA-512 sein. Ab ONTAP 9.20.1 wird SHA-512 unterstützt. | authKey | -EINE PASSPHRASE |
| Passphrase mit mindestens acht Zeichen. | securityLevel | -l {authNoPriv |
| AuthPriv | noAuthNoPriv} | Die Sicherheitsstufe kann Authentifizierung, keine Privatsphäre; Authentifizierung, Privatsphäre; oder keine Authentifizierung, keine Privatsphäre sein. |
| privProtocol | -x { none | des |
| aes128} | Das Datenschutzprotokoll kann none, des oder aes128 sein. | privPassword |

## Beispiele für verschiedene Sicherheitsstufen

Dieses Beispiel zeigt, wie ein SNMPv3-Benutzer, der mit unterschiedlichen Sicherheitsstufen erstellt wurde, die SNMP Client-seitig Befehle wie `snmpwalk` verwenden kann, um die Clusterobjekte abzufragen.

Für eine bessere Performance empfiehlt es sich, alle Objekte in einer Tabelle abzurufen, statt nur ein einzelnes Objekt oder einige wenige Objekte aus der Tabelle.

Sie müssen `snmpwalk` 5.3.1 oder höher verwenden, wenn das Authentifizierungsprotokoll SHA ist. Für die Verwendung der SHA-512-Authentifizierung muss der SNMP-Client SNMPv3 und das SHA-512-Authentifizierungsprotokoll unterstützen.

#### Sicherheitsstufe: authPriv

Die folgende Ausgabe zeigt die Erstellung eines SNMPv3-Benutzers mit der authPriv Sicherheitsstufe.

```
security login create -user-or-group-name snmpv3user -application snmp
-authentication-method usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha, sha2-
256, sha512) [none]: md5

Enter the authentication protocol password (minimum 8 characters long):
Enter the authentication protocol password again:
Which privacy protocol do you want to choose (none, des, aes128) [none]:
des
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

#### FIPS-Modus

```
security login create -user-or-group-name snmpv3user -application snmp
-authmethod usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (sha, sha2-256,
sha512) [sha]

Enter authentication protocol password (minimum 8 characters long):
Enter authentication protocol password again:
Which privacy protocol do you want to choose (aes128) [aes128]:
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

#### snmpwalk-Test

Die folgende Ausgabe zeigt den SNMPv3 Benutzer, der den Befehl snmpwalk ausführt:

Für eine bessere Performance empfiehlt es sich, alle Objekte in einer Tabelle abzurufen, statt nur ein einzelnes Objekt oder einige wenige Objekte aus der Tabelle.

```
$ snmpwalk -v 3 -u snmpv3user -a SHA -A password1! -x DES -X password1! -l
authPriv 192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

Die folgende Ausgabe zeigt einen SNMPv3-Benutzer, der den Befehl snmpwalk mit SHA-512-Authentifizierung ausführt:

```
$ snmpwalk -v 3 -u snmpv3user -a SHA-512 -A password1! -x AES -X
password1! -l authPriv 192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

### Sicherheitsstufe: authNoPriv

Die folgende Ausgabe zeigt die Erstellung eines SNMPv3-Benutzers mit der authNoPriv Sicherheitsstufe.

```
security login create -user-or-group-name snmpv3user -application snmp
-authmethod usm -role readonly
```

```
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: md5
```

#### FIPS Modus

FIPS erlaubt die Auswahl von **kein** Datenschutzprotokoll für das Privacy-Protokoll nicht. Daher ist es nicht möglich, einen authNoPriv SNMPv3-Benutzer im FIPS-Modus zu konfigurieren.

#### snmpwalk-Test

Die folgende Ausgabe zeigt den SNMPv3 Benutzer, der den Befehl snmpwalk ausführt:

Für eine bessere Performance empfiehlt es sich, alle Objekte in einer Tabelle abzurufen, statt nur ein einzelnes Objekt oder einige wenige Objekte aus der Tabelle.

```
$ snmpwalk -v 3 -u snmpv3user1 -a MD5 -A password1!  -l authNoPriv
192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

### Sicherheitsstufe: noAuthNoPriv

Die folgende Ausgabe zeigt die Erstellung eines SNMPv3 Benutzers mit der noAuthNoPriv Sicherheitsstufe.

```
security login create -user-or-group-name snmpv3user -application snmp
-authmethod usm -role readonly
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: none
```

#### FIPS Modus

FIPS erlaubt die Auswahl von **kein** Datenschutzprotokoll für das Privacy-Protokoll nicht.

#### snmpwalk-Test

Die folgende Ausgabe zeigt den SNMPv3 Benutzer, der den Befehl snmpwalk ausführt:

Für eine bessere Performance empfiehlt es sich, alle Objekte in einer Tabelle abzurufen, statt nur ein einzelnes Objekt oder einige wenige Objekte aus der Tabelle.

```
$ snmpwalk -v 3 -u snmpv3user2 -l noAuthNoPriv 192.0.2.62
.1.3.6.1.4.1.789.1.5.8.1.2
```

```
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

Weitere Informationen zu `security login create` finden sich in der "ONTAP-Befehlsreferenz".

Weitere Informationen zu SNMPv3 für den Ethernet Switch Systemstatus Monitor (CSHM), einschließlich Informationen zur Konfiguration der Ethernet Switches, enthält "SNMPv3 für die Zustandsüberwachung von Ethernet-Switches konfigurieren".

# Traphosts für SNMP im ONTAP Netzwerk konfigurieren

Sie können den Traphost (SNMP-Manager) so konfigurieren, dass er Benachrichtigungen (SNMP-Trap-PDUs) empfängt, wenn SNMP-Traps im Cluster generiert werden. Es kann entweder der Hostname oder die IP-Adresse (IPv4 oder IPv6) des SNMP-Traphost angegeben werden.

**Bevor Sie beginnen**

- SNMP und SNMP Traps müssen auf dem Cluster aktiviert sein.

  SNMP und SNMP Traps sind standardmäßig aktiviert.

- DNS muss auf dem Cluster konfiguriert sein, damit die Traphost-Namen aufgelöst werden können.
- IPv6 muss auf dem Cluster aktiviert sein, um SNMP-Traphosts mit IPv6-Adressen zu konfigurieren.
- Sie müssen die Authentifizierung eines vordefinierten benutzerbasierten Sicherheitsmodells (USM) und die Datenschutzanmeldeinformationen bei der Erstellung von Traphosts angegeben haben.

**Schritt**

Einen SNMP Traphost hinzufügen:

```
system snmp traphost add
```

Traps können nur gesendet werden, wenn mindestens eine SNMP-Managementstation als Traphost angegeben ist.

Der folgende Befehl fügt einen neuen SNMPv3 Traphost namens yyy.example.com mit einem bekannten USM-Benutzer hinzu:

```
system snmp traphost add -peer-address yyy.example.com -usm-username
MyUsmUser
```

Der folgende Befehl fügt einen Traphost unter Verwendung der IPv6-Adresse des Hosts hinzu:

```
system snmp traphost add -peer-address 2001:0db8:1:1:209:6bff:feae:6d67
```

# SNMP-Abfrage in einem ONTAP Cluster überprüfen

Nach der Konfiguration von SNMP sollte überprüft werden, ob der Cluster abgefragt werden kann.

**Über diese Aufgabe**

Um einen Cluster abzufragen, müssen Sie einen Drittanbieterbefehl wie `snmpwalk` verwenden.

**Schritte**

1. Ein SNMP-Befehl kann gesendet werden, um den Cluster von einem anderen Cluster aus abzufragen.

   Für Systeme mit SNMPv1 kann der CLI-Befehl `snmpwalk -v version -c community_stringip_address_or_host_name system` verwendet werden, um den Inhalt der MIB (Management Information Base) zu ermitteln.

   In diesem Beispiel lautet die IP-Adresse des Cluster-Management-LIF, das Sie abfragen, 10.11.12.123. Der Befehl zeigt die angeforderten Informationen aus der MIB an:

   ```
   C:\Windows\System32>snmpwalk -v 1 -c public 10.11.12.123 system

   SNMPv1-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
              Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
   SNMPv1-MIB::sysObjectID.0 = OID: SNMPv1-SMI::enterprises.789.2.5
   DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162644448) 18 days,
   19:47:24.48
   SNMPv1-MIB::sysContact.0 = STRING:
   SNMPv1-MIB::sysName.0 = STRING: systemname.testlabs.com
   SNMPv1-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
   SNMPv1-MIB::sysServices.0 = INTEGER: 72
   ```

   Für Systeme mit SNMPv2c kann der CLI-Befehl `snmpwalk -v version -c community_stringip_address_or_host_name system` verwendet werden, um den Inhalt der MIB (Management Information Base) zu ermitteln.

   In diesem Beispiel lautet die IP-Adresse des Cluster-Management-LIF, das Sie abfragen, 10.11.12.123. Der Befehl zeigt die angeforderten Informationen aus der MIB an:

   ```
   C:\Windows\System32>snmpwalk -v 2c -c public 10.11.12.123 system

   SNMPv2-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
              Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
   SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.789.2.5
   DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162635772) 18 days,
   ```

```
19:45:57.72
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv2-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv2-MIB::sysServices.0 = INTEGER: 72
```

Für Systeme mit SNMPv3 kann der CLI-Befehl `snmpwalk -v 3 -a MD5 or SHA -l authnopriv -u username -A passwordip_address_or_host_name system` verwendet werden, um den Inhalt der MIB (Management Information Base) zu ermitteln.

In diesem Beispiel lautet die IP-Adresse des Cluster-Management-LIF, das Sie abfragen, 10.11.12.123. Der Befehl zeigt die angeforderten Informationen aus der MIB an:

```
C:\Windows\System32>snmpwalk -v 3 -a MD5 -l authnopriv -u snmpv3
       -A password123 10.11.12.123 system

SNMPv3-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
       Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv3-MIB::sysObjectID.0 = OID: SNMPv3-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162666569) 18 days,
19:51:05.69
SNMPv3-MIB::sysContact.0 = STRING:
SNMPv3-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv3-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv3-MIB::sysServices.0 = INTEGER: 72
```

# ONTAP Befehle zur Verwaltung von SNMP, Traps und Traphosts

Die `system snmp` Befehle können zur Verwaltung von SNMP, Traps und Traphosts verwendet werden. Die `security` Befehle können zur Verwaltung von SNMP Benutzern pro SVM verwendet werden. Die `event` Befehle können zur Verwaltung von Ereignissen im Zusammenhang mit SNMP Traps verwendet werden.

## Befehle zur Konfiguration von SNMP

| Wenn Sie möchten… | Verwenden Sie diesen Befehl… |
|---|---|
| SNMP auf dem Cluster aktivieren | `options -option-name snmp.enable -option-value on`<br><br>Der SNMP-Dienst muss in der Management-Firewall-Richtlinie (mgmt) zugelassen sein. Ob SNMP zugelassen ist, lässt sich mit dem Befehl `system services firewall policy show` überprüfen. |

| | |
|---|---|
| SNMP auf dem Cluster deaktivieren | `options -option-name snmp.enable -option-value off` |

## Befehle zur Verwaltung von SNMP v1, v2c und v3 Benutzern

| Wenn Sie möchten… | Verwenden Sie diesen Befehl… |
|---|---|
| SNMP-Benutzer konfigurieren | `security login create` |
| SNMP-Benutzer anzeigen | `security snmpusers` und `security login show -application snmp` |
| SNMP-Benutzer löschen | `security login delete` |
| Den Namen der Zugriffskontrollrolle einer Anmeldemethode für SNMP-Benutzer ändern | `security login modify` |

## Befehle zur Bereitstellung von Kontakt- und Standortinformationen

| Wenn Sie möchten… | Verwenden Sie diesen Befehl… |
|---|---|
| Kontaktdaten des Clusters anzeigen oder ändern | `system snmp contact` |
| Standortdetails des Clusters anzeigen oder ändern | `system snmp location` |

## Befehle zur Verwaltung von SNMP-Communities

| Wenn Sie möchten… | Verwenden Sie diesen Befehl… |
|---|---|
| Eine schreibgeschützte (ro) Community für eine SVM oder für alle SVMs im Cluster hinzufügen | `system snmp community add` |
| Eine Community oder alle Communities löschen | `system snmp community delete` |
| Anzeige der Liste aller Communities | `system snmp community show` |

Da SVMs nicht Teil des SNMP-Standards sind, müssen Abfragen von Daten-LIFs die NetApp Root-OID (1.3.6.1.4.1.789) enthalten, zum Beispiel `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`.

## Befehl zum Anzeigen von SNMP Optionswerten

| Wenn Sie möchten… | Verwenden Sie diesen Befehl… |
|---|---|
| Zeigt die aktuellen Werte aller SNMP-Optionen an, einschließlich Cluster-Kontakt, Kontaktstandort, ob der Cluster für das Senden von Traps konfiguriert ist, die Liste der Traphosts sowie die Liste der Communities und des Zugriffskontrolltyps. | `system snmp show` |

## Befehle zur Verwaltung von SNMP-Traps und Traphosts

| Wenn Sie möchten… | Verwenden Sie diesen Befehl… |
|---|---|

| | |
|---|---|
| SNMP-Traps, die vom Cluster gesendet werden, aktivieren | `system snmp init -init 1` |
| SNMP-Traps, die vom Cluster gesendet werden, deaktivieren | `system snmp init -init 0` |
| Einen Traphost hinzufügen, der SNMP-Benachrichtigungen für bestimmte Ereignisse im Cluster empfängt | `system snmp traphost add` |
| Einen Traphost löschen | `system snmp traphost delete` |
| Anzeige der Liste der Traphosts | `system snmp traphost show` |

## Befehle zur Verwaltung von Ereignissen im Zusammenhang mit SNMP-Traps

| Wenn Sie möchten… | Verwenden Sie diesen Befehl… |
|---|---|
| Zeigt die Ereignisse an, für die SNMP Traps (integriert) generiert werden | `event route show`<br><br>Der `-snmp-support true`Parameter zeigt nur SNMP-bezogene Ereignisse an.<br><br>Mit dem `instance -messagename <message>` Parameter wird eine detaillierte Beschreibung angezeigt, warum ein Ereignis aufgetreten sein könnte, sowie eine mögliche Korrekturmaßnahme.<br><br>Das Routing einzelner SNMP-Trap-Ereignisse zu bestimmten Traphost-Zielen wird nicht unterstützt. Alle SNMP-Trap-Ereignisse werden an alle Traphost-Ziele gesendet. |
| Eine Liste der SNMP-Trap-Verlaufsdatensätze wird angezeigt, also Ereignisbenachrichtigungen, die an SNMP-Traps gesendet wurden. | `event snmphistory show` |
| Löschen eines SNMP Trap Verlaufseintrags | `event snmphistory delete` |

**Verwandte Informationen**

- "system snmp"
- "security snmpusers"
- "Sicherheit"
- "Ereignis"
- "Security Login"

**Copyright-Informationen**

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

**Markeninformationen**

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.