Verwalten von SNMP (nur Cluster-Administratoren)

ONTAP 9

NetApp
April 24, 2024

Inhalt

Verwalten von SNMP (nur Cluster-Administratoren)

SNMP-Überblick

SNMP lässt sich konfigurieren, um SVMs in Ihrem Cluster zu überwachen und Probleme zu vermeiden, bevor sie auftreten, und um auf Probleme zu reagieren, falls diese auftreten. Beim Management von SNMP müssen SNMP-Benutzer konfiguriert und SNMP traphost-Ziele (Management-Workstations) für alle SNMP-Ereignisse konfiguriert werden. SNMP ist standardmäßig auf Daten-LIFs deaktiviert.

Sie können schreibgeschützte SNMP-Benutzer in der Daten-SVM erstellen und managen. Daten-LIFs müssen konfiguriert werden, um SNMP-Anforderungen auf der SVM zu empfangen.

SNMP-Netzwerkmanagement-Workstations oder -Manager können den SVM-SNMP-Agent zur Information abfragen. Der SNMP-Agent sammelt Informationen und leitet sie an die SNMP-Manager weiter. Der SNMP-Agent erzeugt auch Trap-Benachrichtigungen, wenn bestimmte Ereignisse auftreten. Der SNMP-Agent auf der SVM hat schreibgeschützte Berechtigungen. Er kann nicht für bestimmte Vorgänge oder zur Durchführung von Korrekturmaßnahmen als Antwort auf einen Trap verwendet werden. ONTAP stellt einen SNMP-Agent bereit, der mit SNMP-Versionen v1, v2c und v3 kompatibel ist. SNMPv3 bietet erweiterte Sicherheit durch Nutzung von Passphrases und Verschlüsselung.

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

MIB-Übersicht

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

MIBs beschreiben die Struktur der Managementdaten des Storage-Systems und verwenden einen hierarchischen Namespace mit Objekt-IDs (OIDs). Jede OID identifiziert eine Variable, die über SNMP gelesen werden kann.

Da MIBs keine Konfigurationsdateien sind und ONTAP diese Dateien nicht liest, wird die SNMP-Funktionalität von MIBs nicht beeinflusst. ONTAP bietet die folgende MIB-Datei:

- Eine individuelle NetApp 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 enthalten, werden unterstützt.

ONTAP bietet außerdem eine kurze Querverweis zwischen Objekt-IDs (OIDs) und Objektkurznamen in `traps.dat` Datei:

> Die neuesten Versionen der Dateien ONTAP MIBs und `traps.dat `stehen auf der NetApp Support-Website zur Verfügung. Allerdings entsprechen die Versionen dieser Dateien auf der Support-Website nicht unbedingt den SNMP-Fähigkeiten Ihrer ONTAP-Version. Diese Dateien werden bereitgestellt, um Ihnen zu helfen, SNMP-Funktionen in der neuesten ONTAP-Version zu bewerten.

SNMP-Traps

SNMP-Traps erfassen System Monitoring Informationen, die als asynchrone Benachrichtigung vom SNMP-Agent an den SNMP-Manager gesendet werden.

Es gibt drei Arten von SNMP-Traps: Standard, integrierte und benutzerdefinierte definiert. Benutzerdefinierte Traps werden in ONTAP nicht unterstützt.

Ein Trap kann verwendet werden, um regelmäßig auf betriebliche Schwellenwerte oder Fehler zu überprüfen, die in der MIB definiert sind. Wenn ein Schwellenwert erreicht wird oder ein Fehler erkannt wird, sendet der SNMP-Agent eine Meldung (Trap) an die Traphosts, die sie über das Ereignis alarmieren.

> ONTAP unterstützt SNMPv1-Traps und starting in ONTAP 9.1, SNMPv3-Traps. ONTAP unterstützt keine SNMPv2c-Traps und -Informationen.

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 AuthentifizierungFailure.

> Der Trap für die Authentifizierungsausfältung ist standardmäßig deaktiviert. Sie müssen den verwenden `system snmp authtrap` Befehl zum Aktivieren des Trap. Weitere Informationen zu Formatein finden Sie auf den man-Pages: "ONTAP 9-Befehle"

Integrierte SNMP-Traps

Integrierte Traps sind in ONTAP vordefiniert und werden bei Auftreten eines Ereignisses automatisch an die Netzwerk-Management-Stationen in der traphost-Liste gesendet. Diese Traps wie diskFailedShutdown, cpuTooBusy und VolumeNearlyFull sind in der benutzerdefinierten MIB definiert.

Jeder integrierte Trap wird durch einen eindeutigen Trap-Code identifiziert.

Erstellen Sie eine SNMP Community und Zuweisen zu einem LIF

Sie können bei der Verwendung von SNMPv1 und SNMPv2c eine SNMP-Community erstellen, die als Authentifizierungsmechanismus zwischen der Management Station und der Storage Virtual Machine (SVM) fungiert.

Durch das Erstellen von SNMP Communities in einer Daten-SVM können Sie Befehle wie ausführen `snmpwalk` Und `snmpget` Auf den Daten-LIFs.

Über diese Aufgabe

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

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

- ONTAP unterstützt schreibgeschützte Communitys.
- Standardmäßig ist für die „Daten“ Firewall-Richtlinie, die Daten-LIFs zugewiesen ist, der SNMP-Service festgelegt `deny`.

Sie müssen eine neue Firewallrichtlinie erstellen, bei der der SNMP-Dienst auf festgelegt ist `allow` Beim Erstellen eines SNMP-Benutzers für eine Daten-SVM

> Ab ONTAP 9.10.1 sind Firewall-Richtlinien veraltet und werden vollständig durch LIF-Servicerichtlinien ersetzt. Weitere Informationen finden Sie unter "Konfigurieren Sie Firewallrichtlinien für LIFs".

- 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 bei Anfragen zu Daten-LIFs die NetApp Root OID (1.3.6.1.4.1.789) enthalten – beispielsweise `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`.

Schritte

1. Erstellen Sie eine SNMP Community mit dem `system snmp community add` Befehl. Mit dem folgenden Befehl wird gezeigt, wie eine SNMP-Community in dem Admin-SVM-Cluster-1 erstellt wird:

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

   Mit dem folgenden Befehl wird gezeigt, wie eine SNMP-Community in der Data SVM vs1 erstellt wird:

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

2. Überprüfen Sie, dass die Communities erstellt wurden, indem Sie den System snmp Community show Befehl verwenden.

   Der folgende Befehl zeigt die beiden Gemeinschaften, die für SNMPv1 und SNMPv2c erstellt wurden:

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

3. Überprüfen Sie, ob SNMP als Dienst in der „Daten“ Firewall-Richtlinie über die zulässig ist `system services firewall policy show` Befehl.

   Der folgende Befehl zeigt an, dass der snmp-Dienst in der Standard-Firewall-Richtlinie „Daten“ nicht erlaubt ist (der snmp-Dienst ist nur in der „Management“ Firewall-Richtlinie zulässig):

```
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. Erstellen Sie eine neue Firewallrichtlinie, die den Zugriff über ermöglicht `snmp` Dienst durch Verwendung des `system services firewall policy create` Befehl.

   Die folgenden Befehle erstellen eine neue Daten-Firewall-Richtlinie namens "data1", die das ermöglicht `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. Wenden Sie die Firewallrichtlinie auf eine Daten-LIF an, indem Sie den Befehl `Network Interface modify `mit dem Parameter -Firewall-Policy verwenden.

Mit dem folgenden Befehl wird die neue „data1“ Firewallrichtlinie zu LIF „Daten1“ zugewiesen:

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

Konfigurieren Sie SNMPv3-Benutzer in einem Cluster

SNMPv3 ist ein sicheres Protokoll im Vergleich zu SNMPv1 und SNMPv2c. Um SNMPv3 zu verwenden, müssen Sie einen SNMPv3-Benutzer konfigurieren, um die SNMP-Dienstprogramme vom SNMP-Manager aus auszuführen.

Schritt

Verwenden Sie den Befehl „Security Login create“, um einen SNMPv3-Benutzer zu erstellen.

Sie werden aufgefordert, folgende Informationen einzugeben:

- Engine ID: Standard und Empfohlener Wert ist lokale Engine ID
- Authentifizierungsprotokoll
- Authentifizierungspasswort
- Datenschutzprotokoll
- Passwort für das Datenschutzprotokoll

Ergebnis

Der SNMPv3-Benutzer kann sich über den SNMP-Manager über den Benutzernamen und das Kennwort anmelden und die Befehle des SNMP-Dienstprogramms ausführen.

SNMPv3-Sicherheitsparameter

SNMPv3 umfasst eine Authentifizierungsfunktion, die bei Auswahl von Benutzern erfordert, dass sie beim Aufrufen eines Befehls ihren Namen, ein Authentifizierungsprotokoll, einen Authentifizierungsschlüssel und den gewünschten Sicherheitsgrad eingeben.

In der folgenden Tabelle sind die SNMPv3-Sicherheitsparameter aufgelistet:

Parameter	Befehlszeilenoption	Beschreibung
EngineID	-E EngineID	Engine-ID des SNMP-Agenten. Der Standardwert ist Local EngineID (empfohlen).
Sicherheitsname	-U Name	Der Benutzername darf maximal 32 Zeichen enthalten.
AuthProtocol	-A {None} SHA-256	Authentifizierungstyp kann keine, MD5, SHA oder SHA-256 sein.
AuthKey	-EINE PASSPHRASE	Passphrase mit mindestens acht Zeichen.

Sicherheitsstufe	• L {authNoPriv}	Sicherheitsstufe kann Authentifizierung, Datenschutz, Authentifizierung, Datenschutz oder keine Authentifizierung sein. Kein Datenschutz.
PrivProtocol	-X { none} aes128	Das Datenschutzprotokoll kann keine, des oder aes128 sein
Privatpasswort	-X-Passwort	Passwort mit mindestens acht Zeichen.

Beispiele für unterschiedliche Sicherheitsstufen

Dieses Beispiel zeigt, wie ein SNMPv3-Benutzer, der mit unterschiedlichen Sicherheitsstufen erstellt wurde, die SNMP-Clientbefehle verwenden kann, wie z. B. `snmpwalk`, Um die Clusterobjekte abzufragen.

Für eine bessere Performance sollten Sie alle Objekte in einer Tabelle anstatt in einem einzelnen Objekt oder einigen Objekten aus der Tabelle abrufen.

> Sie müssen verwenden `snmpwalk` 5.3.1 oder höher, wenn das Authentifizierungsprotokoll SHA ist.

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) [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 -username snmpv3user -application snmp -authmethod
usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (sha, sha2-256) [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 snmpwalk-Befehl ausführt:

Für eine bessere Performance sollten Sie alle Objekte in einer Tabelle anstatt in einem einzelnen Objekt oder einigen Objekten aus der Tabelle abrufen.

```
$ 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"
```

Sicherheitsstufe: AuthNoPriv

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

```
security login create -username snmpv3user1 -application snmp -authmethod
usm -role admin
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 Ihnen nicht, **none** für das Datenschutzprotokoll zu wählen. 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 snmpwalk-Befehl ausführt:

Für eine bessere Performance sollten Sie alle Objekte in einer Tabelle anstatt in einem einzelnen Objekt oder

einigen Objekten aus der Tabelle abrufen.

```
$ 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 Sicherheitsstufe noAuthNoPriv.

```
security login create -username snmpv3user2 -application snmp -authmethod
usm -role admin
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 Ihnen nicht, **none** für das Datenschutzprotokoll zu wählen.

Snmpwalk-Test

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

Für eine bessere Performance sollten Sie alle Objekte in einer Tabelle anstatt in einem einzelnen Objekt oder einigen Objekten aus der Tabelle abrufen.

```
$ 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"
```

Konfigurieren Sie traphosts für den Empfang von SNMP-Benachrichtigungen

Sie können traphost (SNMP Manager) so konfigurieren, dass Benachrichtigungen (SNMP Trap PDUs) empfangen werden, wenn SNMP Traps im Cluster generiert werden. Sie können entweder den Hostnamen oder die IP-Adresse (IPv4 oder IPv6) des SNMP

traphost angeben.

Bevor Sie beginnen

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

> SNMP- und SNMP-Traps sind standardmäßig aktiviert.

- Für das Auflösen der traphost-Namen muss auf dem Cluster DNS konfiguriert sein.
- IPv6 muss auf dem Cluster aktiviert sein, um SNMP-Traphosts mithilfe von IPv6-Adressen zu konfigurieren.
- Für ONTAP 9.1 und neuere Versionen müssen Sie beim Erstellen von Traphosts die Authentifizierung eines vordefinierten Benutzer-basierten Sicherheitsmodells (USM) und der Privatsphäre-Anmeldeinformationen angegeben haben.

Schritt

Hinzufügen eines SNMP traphost:

```
system snmp traphost add
```

> Traps können nur gesendet werden, wenn mindestens eine SNMP Management Station als traphost angegeben ist.

Mit dem folgenden Befehl wird ein neuer SNMPv3 traphost mit dem Namen yyy.example.com mit einem bekannten USM-Benutzer hinzugefügt:

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

Mit dem folgenden Befehl wird ein traphost unter Verwendung der IPv6-Adresse des Hosts hinzugefügt:

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

Befehle zum Verwalten von SNMP

Sie können das verwenden `system snmp` Befehle zum Verwalten von SNMP, Traps und traphosts. Sie können das verwenden `security` Befehle zum Managen von SNMP-Benutzern pro SVM. Sie können das verwenden `event` Befehle zum Verwalten von Ereignissen im Zusammenhang mit SNMP-Traps.

Befehle zum Konfigurieren von SNMP

Ihr Ziel ist	Befehl

Aktivieren Sie SNMP auf dem Cluster	`options -option-name snmp.enable -option-value on` Der SNMP-Service muss unter der Management (Mgmt) Firewall-Richtlinie zugelassen werden. Sie können überprüfen, ob SNMP zulässig ist, indem Sie den Befehl System Services Firewall Policy show verwenden.
Deaktivieren Sie SNMP auf dem Cluster	`options -option-name snmp.enable -option-value off`

Befehle zum Verwalten von SNMP v1-, v2c- und v3-Benutzern

Ihr Ziel ist	Befehl
Konfigurieren Sie SNMP-Benutzer	`security login create`
Anzeigen von SNMP-Benutzern	`security snmpusers and security login show -application snmp`
Löschen Sie SNMP-Benutzer	`security login delete`
Ändern Sie den Namen der Zugriffskontrollrolle einer Anmeldemethode für SNMP-Benutzer	`security login modify`

Befehle zur Bereitstellung von Kontakt- und Standortinformationen

Ihr Ziel ist	Befehl
Zeigt die Kontaktinformationen des Clusters an oder ändern sie	`system snmp contact`
Zeigt die Standortdetails des Clusters an oder ändern sie	`system snmp location`

Befehle zum Verwalten von SNMP-Communitys

Ihr Ziel ist	Befehl
Fügen Sie eine schreibgeschützte Community (ro) für eine SVM oder alle SVMs im Cluster hinzu	`system snmp community add`
Löschen Sie eine Community oder alle Communities	`system snmp community delete`

Zeigen Sie die Liste aller Communitys an	`system snmp community show`

Da SVMs nicht Teil des SNMP-Standards sind, müssen bei Anfragen zu Daten-LIFs die NetApp Root OID (1.3.6.1.4.1.789) enthalten sein. `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`.

Befehl zum Anzeigen von SNMP-Optionswerten

Ihr Ziel ist	Befehl
Zeigen Sie die aktuellen Werte aller SNMP-Optionen an, einschließlich Clusterkontakt, Kontaktstelle, ob das Cluster zum Senden von Traps konfiguriert ist, die Liste der Traphosts, Liste der Communities und Zugriffsteuerungsarten	`system snmp show`

Befehle zum Verwalten von SNMP-Traps und traphosts

Ihr Ziel ist	Befehl
Aktivieren Sie SNMP-Traps die vom Cluster gesendet werden	`system snmp init -init 1`
Deaktivieren Sie SNMP-Traps die vom Cluster gesendet werden	`system snmp init -init 0`
Fügen Sie einen traphost hinzu, der SNMP-Benachrichtigungen für bestimmte Ereignisse im Cluster erhält	`system snmp traphost add`
Löschen Sie einen traphost	`system snmp traphost delete`
Zeigt die Liste der Traphosts an	`system snmp traphost show`

Befehle zum Verwalten von Ereignissen im Zusammenhang mit SNMP-Traps

Ihr Ziel ist	Befehl

Zeigen Sie die Ereignisse an, für die SNMP-Traps (integriert) generiert werden	`event route show` Verwenden Sie die `-snmp-support true` Parameter zum Anzeigen von nur SNMP-bezogenen Ereignissen. Verwenden Sie die `instance -messagename <message>` Parameter zum Anzeigen einer detaillierten Beschreibung, warum ein Ereignis aufgetreten ist, sowie aller Korrekturmaßnahmen. Das Routing einzelner SNMP-Trap-Ereignisse zu bestimmten traphost-Zielen wird nicht unterstützt. Alle SNMP-Trap-Ereignisse werden an alle traphost-Ziele gesendet.
Zeigt eine Liste der SNMP-Trap-Verlaufsdatensätze an, bei denen es sich um Ereignisbenachrichtigungen handelt, die an SNMP-Traps gesendet wurden	`event snmphistory show`
Löschen Sie einen SNMP-Trap-Verlaufsdatensatz	`event snmphistory delete`

Weitere Informationen zum `system snmp`, `security`, und `event` Befehle, siehe die man-Pages: "ONTAP 9-Befehle"