Gestione SNMP (solo amministratori cluster)

ONTAP 9

NetApp
April 24, 2024

Sommario

Gestione SNMP (solo amministratori cluster)

Panoramica SNMP

È possibile configurare SNMP per monitorare le SVM nel cluster per evitare i problemi prima che si verifichino e per rispondere ai problemi in caso di verificarsi. La gestione di SNMP implica la configurazione degli utenti SNMP e la configurazione delle destinazioni SNMP traphost (workstation di gestione) per tutti gli eventi SNMP. SNMP è disattivato per impostazione predefinita nei file LIF dei dati.

È possibile creare e gestire utenti SNMP di sola lettura nella SVM dei dati. Le LIF dei dati devono essere configurate per ricevere richieste SNMP su SVM.

Le workstation o i manager di gestione della rete SNMP possono richiedere informazioni all'agente SNMP SVM. L'agente SNMP raccoglie le informazioni e le inoltra ai gestori SNMP. L'agente SNMP genera inoltre notifiche trap ogni volta che si verificano eventi specifici. L'agente SNMP sulla SVM dispone di privilegi di sola lettura; non può essere utilizzato per operazioni impostate o per intraprendere un'azione correttiva in risposta a una trap. ONTAP fornisce un agente SNMP compatibile con le versioni SNMP v1, v2c e v3. SNMPv3 offre sicurezza avanzata utilizzando passphrase e crittografia.

Per ulteriori informazioni sul supporto SNMP nei sistemi ONTAP, vedere "TR-4220: Supporto SNMP in Data ONTAP".

Panoramica MIB

Un MIB (Management Information base) è un file di testo che descrive oggetti e trap SNMP.

I MIB descrivono la struttura dei dati di gestione del sistema di storage e utilizzano uno spazio dei nomi gerarchico contenente OID (Object Identifier). Ogni OID identifica una variabile che può essere letta utilizzando SNMP.

Poiché i MIB non sono file di configurazione e ONTAP non legge questi file, la funzionalità SNMP non viene influenzata dai MIB. ONTAP fornisce il seguente file MIB:

- Una MIB personalizzata di NetApp (`netapp.mib`)

ONTAP supporta i MIB IPv6 (RFC 2465), TCP (RFC 4022), UDP (RFC 4113) e ICMP (RFC 2466), che mostrano sia i dati IPv4 che IPv6.

ONTAP fornisce inoltre un breve riferimento incrociato tra gli OID (Object Identifier) e i nomi brevi degli oggetti in `traps.dat` file.

> Le versioni più recenti dei MIB e dei file `traps.dat `di ONTAP sono disponibili sul sito del supporto NetApp. Tuttavia, le versioni di questi file sul sito di supporto non corrispondono necessariamente alle funzionalità SNMP della versione di ONTAP in uso. Questi file vengono forniti per agevolare la valutazione delle funzionalità SNMP nella versione più recente di ONTAP.

Trap SNMP

I trap SNMP acquisiscono le informazioni di monitoraggio del sistema inviate come notifica asincrona

dall'agente SNMP al gestore SNMP.

Esistono tre tipi di trap SNMP: Standard, incorporato e definito dall'utente. I trap definiti dall'utente non sono supportati in ONTAP.

È possibile utilizzare una trap per controllare periodicamente le soglie operative o gli errori definiti nella MIB. Se viene raggiunta una soglia o viene rilevato un errore, l'agente SNMP invia un messaggio (trap) ai traphost che li avvisano dell'evento.

> ONTAP supporta i trap SNMPv1 e, avviando ONTAP 9.1, i trap SNMPv3. ONTAP non supporta i trap SNMPv2c e informa.

Trap SNMP standard

Questi trap sono definiti in RFC 1215. ONTAP supporta cinque trap SNMP standard: Coldstart, warmStart, linkGiù, linkup e AuthenticationFailure.

> Il trap AuthenticationFailure è disattivato per impostazione predefinita. È necessario utilizzare `system snmp authtrap` per attivare il trap. Per ulteriori informazioni, consulta le pagine man: "Comandi di ONTAP 9"

Trap SNMP integrati

I trap integrati sono predefiniti in ONTAP e vengono inviati automaticamente alle stazioni di gestione di rete presenti nell'elenco degli host trapezoidali in caso di evento. Questi trap, come diskFailedShutdown, cpuTooBusy e volumeNearlyFull, sono definiti nel MIB personalizzato.

Ogni trap integrato è identificato da un codice trap univoco.

Creare una community SNMP e assegnarla a una LIF

È possibile creare una community SNMP che funga da meccanismo di autenticazione tra la stazione di gestione e la macchina virtuale di storage (SVM) quando si utilizzano SNMPv1 e SNMPv2c.

Creando community SNMP in una SVM di dati, è possibile eseguire comandi come `snmpwalk` e. `snmpget` Sulle LIF dei dati.

A proposito di questa attività

- Nelle nuove installazioni di ONTAP, SNMPv1 e SNMPv2c sono disattivati per impostazione predefinita.

  SNMPv1 e SNMPv2c vengono attivati dopo la creazione di una community SNMP.

- ONTAP supporta le community di sola lettura.
- Per impostazione predefinita, il servizio SNMP è impostato su per il criterio firewall "dati" assegnato alle LIF dati `deny`.

  È necessario creare un nuovo criterio firewall con il servizio SNMP impostato su `allow` Quando si crea un utente SNMP per un SVM dati.

> A partire da ONTAP 9.10.1, le policy firewall sono obsolete e completamente sostituite con le policy di servizio LIF. Per ulteriori informazioni, vedere "Configurare le policy firewall per le LIF".

- È possibile creare community SNMP per gli utenti SNMPv1 e SNMPv2c sia per SVM admin che per SVM dati.
- Poiché una SVM non fa parte dello standard SNMP, le query sulle LIF dei dati devono includere l'OID root di NetApp (1.3.6.1.4.1.789), ad esempio `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`.

Fasi

1. Creare una community SNMP utilizzando `system snmp community add` comando. Il seguente comando mostra come creare una community SNMP nel cluster SVM di amministrazione-1:

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

   Il seguente comando mostra come creare una community SNMP nei dati SVM vs1:

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

2. Verificare che le community siano state create utilizzando il comando di visualizzazione della community snmp di sistema.

   Il seguente comando mostra le due community create per SNMPv1 e SNMPv2c:

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

3. Verificare se SNMP è consentito come servizio nella policy firewall "dati" utilizzando `system services firewall policy show` comando.

   Il seguente comando indica che il servizio snmp non è consentito nella policy firewall "dati" predefinita (il servizio snmp è consentito solo nella policy firewall "mgmt"):

```
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. Creare un nuovo criterio firewall che consenta l'accesso tramite `snmp` utilizzando `system services firewall policy create` comando.

   I seguenti comandi creano una nuova policy di firewall dati denominata "data1" che consente `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. Applicare il criterio firewall a una LIF dati utilizzando il comando `network interface modify `(modifica interfaccia di rete) con il parametro -firewall-policy.

Il seguente comando assegna il nuovo criterio firewall "data1" a "datalif1" LIF:

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

Configurare gli utenti SNMPv3 in un cluster

SNMPv3 è un protocollo sicuro rispetto a SNMPv1 e SNMPv2c. Per utilizzare SNMPv3, è necessario configurare un utente SNMPv3 per eseguire le utility SNMP dal gestore SNMP.

Fase

Utilizzare il "comando di creazione dell'accesso di sicurezza" per creare un utente SNMPv3.

Viene richiesto di fornire le seguenti informazioni:

- Engine ID (ID motore): Il valore predefinito e raccomandato è l'ID motore locale
- Protocollo di autenticazione
- Password di autenticazione
- Protocollo di privacy
- Password del protocollo di privacy

Risultato

L'utente SNMPv3 può accedere dal gestore SNMP utilizzando il nome utente e la password ed eseguire i comandi dell'utility SNMP.

Parametri di sicurezza SNMPv3

SNMPv3 include una funzionalità di autenticazione che, quando selezionata, richiede agli utenti di inserire i propri nomi, un protocollo di autenticazione, una chiave di autenticazione e il livello di sicurezza desiderato quando si richiama un comando.

Nella tabella seguente sono elencati i parametri di protezione di SNMPv3 :

Parametro	Opzione della riga di comando	Descrizione
ID motore	-E EngineID	ID motore dell'agente SNMP. Il valore predefinito è EngineID locale (consigliato).
SecurityName	-U Nome	Il nome utente non deve superare i 32 caratteri.
AuthProtocol	-A {none	MD5
SHA	SHA-256}	Il tipo di autenticazione può essere None, MD5, SHA o SHA-256.

Chiave authkey	-UNA PASSPHRASE	Passphrase con un minimo di otto caratteri.
Livello di sicurezza	-L {authNoPriv	AuthPriv
noAuthNoPriv}	Il livello di protezione può essere autenticazione, Nessuna privacy, autenticazione, privacy o nessuna autenticazione, Nessuna privacy.	PrivProtocol
-x { none	des	aes128}
Il protocollo di privacy può essere NONE, des o aes128	PrivPassword	-X password

Esempi di diversi livelli di sicurezza

Questo esempio mostra come un utente SNMPv3 creato con diversi livelli di sicurezza può utilizzare i comandi lato client SNMP, ad esempio `snmpwalk`, per eseguire query sugli oggetti del cluster.

Per ottenere prestazioni migliori, è necessario recuperare tutti gli oggetti di una tavola anziché un singolo oggetto o pochi oggetti dalla tavola.

> È necessario utilizzare `snmpwalk` 5.3.1 o versione successiva quando il protocollo di autenticazione è SHA.

Livello di sicurezza: Authprim

Il seguente output mostra la creazione di un utente SNMPv3 con il livello di sicurezza authprim.

```
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:
```

Modalità FIPS

```
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:
```

Test snmpwalk

Il seguente output mostra l'utente SNMPv3 che esegue il comando snmpwalk:

Per ottenere prestazioni migliori, è necessario recuperare tutti gli oggetti di una tavola anziché un singolo oggetto o pochi oggetti dalla tavola.

```
$ 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"
```

Livello di sicurezza: AuthNoPriv

Il seguente output mostra la creazione di un utente SNMPv3 con il livello di sicurezza autNoPriv.

```
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
```

Modalità FIPS

FIPS non consente di scegliere **nessuno** per il protocollo di privacy. Di conseguenza, non è possibile configurare un utente authNoPrivat SNMPv3 in modalità FIPS.

Test snmpwalk

Il seguente output mostra l'utente SNMPv3 che esegue il comando snmpwalk:

Per ottenere prestazioni migliori, è necessario recuperare tutti gli oggetti di una tavola anziché un singolo oggetto o pochi oggetti dalla tavola.

```
$ 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"
```

Livello di sicurezza: NoAuthNoPriv

Il seguente output mostra la creazione di un utente SNMPv3 con il livello di sicurezza noAuthNoPrimv.

```
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
```

Modalità FIPS

FIPS non consente di scegliere **nessuno** per il protocollo di privacy.

Test snmpwalk

Il seguente output mostra l'utente SNMPv3 che esegue il comando snmpwalk:

Per ottenere prestazioni migliori, è necessario recuperare tutti gli oggetti di una tavola anziché un singolo oggetto o pochi oggetti dalla tavola.

```
$ 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"
```

Configurare i traphost per ricevere notifiche SNMP

È possibile configurare il traphost (gestore SNMP) in modo che riceva notifiche (PDU trap SNMP) quando vengono generati trap SNMP nel cluster. È possibile specificare il nome host o l'indirizzo IP (IPv4 o IPv6) del traphost SNMP.

Prima di iniziare

- I trap SNMP e SNMP devono essere attivati sul cluster.

> I trap SNMP e SNMP sono attivati per impostazione predefinita.

- Il DNS deve essere configurato sul cluster per risolvere i nomi degli host trapezoidali.
- IPv6 deve essere attivato sul cluster per configurare i traphost SNMP utilizzando gli indirizzi IPv6.
- Per ONTAP 9.1 e versioni successive, è necessario specificare l'autenticazione di un modello di sicurezza basato sull'utente (USM) e le credenziali di privacy predefiniti durante la creazione di traphost.

Fase

Aggiunta di un host SNMP traphost:

```
system snmp traphost add
```

> I trap possono essere inviati solo quando almeno una stazione di gestione SNMP è specificata come host trapotato.

Il seguente comando aggiunge un nuovo host trapezoidale SNMPv3 denominato yyy.example.com con un utente USM noto:

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

Il seguente comando aggiunge un host trapezoidale utilizzando l'indirizzo IPv6 dell'host:

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

Comandi per la gestione di SNMP

È possibile utilizzare `system snmp` Comandi per gestire SNMP, trap e traphost. È possibile utilizzare `security` Comandi per gestire gli utenti SNMP per SVM. È possibile utilizzare `event` Comandi per gestire gli eventi relativi ai trap SNMP.

Comandi per la configurazione di SNMP

Se si desidera…	Utilizzare questo comando…

Abilitare SNMP sul cluster	`options -option-name snmp.enable -option-value on` Il servizio SNMP deve essere consentito in base alla policy firewall di gestione (mgmt). È possibile verificare se SNMP è consentito utilizzando il comando show del criterio firewall dei servizi di sistema.
Disattivare SNMP sul cluster	`options -option-name snmp.enable -option-value off`

Comandi per la gestione degli utenti SNMP v1, v2c e v3

Se si desidera…	Utilizzare questo comando…
Configurare gli utenti SNMP	`security login create`
Visualizzare gli utenti SNMP	`security snmpusers and security login show -application snmp`
Eliminare gli utenti SNMP	`security login delete`
Modificare il nome del ruolo di controllo dell'accesso di un metodo di accesso per gli utenti SNMP	`security login modify`

Comandi per fornire informazioni di contatto e posizione

Se si desidera…	Utilizzare questo comando…
Visualizzare o modificare i dettagli di contatto del cluster	`system snmp contact`
Visualizzare o modificare i dettagli della posizione del cluster	`system snmp location`

Comandi per la gestione delle community SNMP

Se si desidera…	Utilizzare questo comando…
Aggiungere una community di sola lettura (ro) per una SVM o per tutte le SVM nel cluster	`system snmp community add`
Eliminare una community o tutte le community	`system snmp community delete`

Visualizza l'elenco di tutte le community	`system snmp community show`

Poiché le SVM non fanno parte dello standard SNMP, le query sulle LIF dei dati devono includere l'OID root di NetApp (1.3.6.1.4.1.789), ad esempio `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`.

Comando per la visualizzazione dei valori delle opzioni SNMP

Se si desidera…	Utilizzare questo comando…
Visualizza i valori correnti di tutte le opzioni SNMP, inclusi il contatto del cluster, la posizione del contatto, se il cluster è configurato per l'invio di trap, l'elenco dei traphost, l'elenco delle community e il tipo di controllo degli accessi	`system snmp show`

Comandi per la gestione di trap SNMP e traphosts

Se si desidera…	Utilizzare questo comando…
Abilitare i trap SNMP inviati dal cluster	`system snmp init -init 1`
Disattiva i trap SNMP inviati dal cluster	`system snmp init -init 0`
Aggiungere un host trapotato che riceve notifiche SNMP per eventi specifici nel cluster	`system snmp traphost add`
Eliminare un host trapezoidale	`system snmp traphost delete`
Visualizza l'elenco di traphosts	`system snmp traphost show`

Comandi per la gestione degli eventi relativi ai trap SNMP

Se si desidera…	Utilizzare questo comando…

Visualizza gli eventi per i quali vengono generati i trap SNMP (integrati)	`event route show` Utilizzare `-snmp-support true` Parametro per visualizzare solo gli eventi relativi a SNMP. Utilizzare `instance -messagename <message>` parametro per visualizzare una descrizione dettagliata del motivo per cui si è verificato un evento e di eventuali azioni correttive. Il routing di singoli eventi trap SNMP a destinazioni host trapotate specifiche non è supportato. Tutti gli eventi trap SNMP vengono inviati a tutte le destinazioni dell'host trapotato.
Visualizza un elenco di record della cronologia delle trap SNMP, che sono notifiche di eventi inviate alle trap SNMP	`event snmphistory show`
Eliminare un record di cronologia trap SNMP	`event snmphistory delete`

Per ulteriori informazioni su `system snmp`, `security`, e. `event` comandi, vedere le pagine man: "Comandi di ONTAP 9"