SNMP 관리(클러스터 관리자만 해당)

ONTAP 9

NetApp
February 12, 2026

목차

SNMP 관리(클러스터 관리자만 해당)

ONTAP 네트워크의 SNMP에 대해 알아봅니다

문제가 발생하기 전에 이를 방지하고 문제가 발생할 경우 대응하도록 SNMP를 클러스터의 SVM을 모니터링할 수 있습니다. SNMP를 관리하려면 SNMP 사용자를 구성하고 모든 SNMP 이벤트에 대해 SNMP 트라프호스트 대상(관리 워크스테이션)을 구성해야 합니다. 데이터 LIF에서 SNMP는 기본적으로 해제되어 있습니다.

데이터 SVM에서 읽기 전용 SNMP 사용자를 생성하고 관리할 수 있습니다. SVM에서 SNMP 요청을 받도록 데이터 LIF를 구성해야 합니다.

SNMP 네트워크 관리 워크스테이션 또는 관리자는 SVM SNMP 에이전트에 정보를 쿼리할 수 있습니다. SNMP 에이전트는 정보를 수집하여 SNMP 관리자에게 전달합니다. SNMP 에이전트는 또한 특정 이벤트가 발생할 때마다 트랩 알림을 생성합니다. SVM의 SNMP 에이전트는 읽기 전용 권한을 가지고 있으며 설정된 작업에 사용하거나 트랩에 대한 응답으로 수정 조치를 취하는 데 사용할 수 없습니다. ONTAP는 SNMP 버전 v1, v2c 및 v3과 호환되는 SNMP 에이전트를 제공합니다. SNMPv3는 암호 구문 및 암호화를 사용하여 고급 보안을 제공합니다.

ONTAP 시스템의 SNMP 지원에 대한 자세한 내용은 를 참조하십시오 "TR-4220: Data ONTAP에서 SNMP 지원".

MIB 개요

MIB(Management Information Base)는 SNMP 객체 및 트랩을 설명하는 텍스트 파일입니다.

MIB는 스토리지 시스템의 관리 데이터 구조를 설명하며 OID(객체 식별자)가 포함된 계층적 네임스페이스를 사용합니다. 각 OID는 SNMP를 사용하여 읽을 수 있는 변수를 식별합니다.

MIB는 구성 파일이 아니며 ONTAP는 이러한 파일을 읽지 않기 때문에 MIB 기능은 MIB의 영향을 받지 않습니다. ONTAP는 다음과 같은 MIB 파일을 제공합니다.

- NetApp 맞춤형 MIB('NetApp.MIB')

ONTAP는 IPv6(RFC 2465), TCP(RFC 4022), UDP(RFC 4113) 및 IPv4 및 IPv6 데이터를 모두 표시하는 ICMP(RFC 2466) MIB를 지원합니다.

또한 ONTAP는 "trap.dat" 파일에서 OID(개체 식별자)와 개체 약식 이름 간의 짧은 상호 참조를 제공합니다.

> ONTAP MIB 및 traps.dat 파일의 최신 버전은 NetApp Support 사이트에서 확인할 수 있습니다. 그러나 지원 사이트에 있는 이러한 파일의 버전이 ONTAP 버전의 SNMP 기능과 일치하지 않을 수도 있습니다. 이러한 파일은 최신 ONTAP 버전에서 SNMP 기능을 평가하는 데 도움이 됩니다.

SNMP 트랩

SNMP 트랩은 SNMP 에이전트에서 SNMP 관리자로 보내는 비동기 알림으로 전송되는 시스템 모니터링 정보를 캡처합니다.

SNMP 트랩에는 표준, 기본 제공 및 사용자 정의 세 가지 유형이 있습니다. 사용자 정의 트랩은 ONTAP에서 지원되지 않습니다.

트랩을 사용하여 MIB에 정의된 작동 임계값 또는 오류를 정기적으로 확인할 수 있습니다. 임계값에 도달하거나 장애가 감지되면 SNMP 에이전트는 해당 이벤트를 알리는 메시지(트랩)를 Traphosts에 보냅니다.

ONTAP는 SNMPv1 및 SNMPv3 트랩을 지원합니다. ONTAP는 SNMPv2c 트랩 및 정보를 지원하지 않습니다.

표준 SNMP 트랩

이러한 트랩은 RFC 1215에 정의되어 있습니다. ONTAP에서 지원하는 5개의 표준 SNMP 트랩은 coldstart, 웜스타트, Linkdown, Linkup 및 authenticationFailure입니다.

authenticationFailure 트랩은 기본적으로 해제되어 있습니다. 명령을 사용하여 트랩을 활성화해야 `system snmp authtrap` 합니다. 에 대한 자세한 내용은 `system snmp authtrap` "ONTAP 명령 참조입니다"을 참조하십시오.

기본 제공 SNMP 트랩

내장 트랩은 ONTAP에서 미리 정의되며 이벤트가 발생하면 Traphost 목록의 네트워크 관리 스테이션으로 자동으로 전송됩니다. diskFailedShutdown, cpuTooBusy 및 volumeNearlyFull과 같은 이러한 트랩은 사용자 지정 MIB에 정의되어 있습니다.

각 내장 트랩은 고유한 트랩 코드로 식별됩니다.

ONTAP 네트워크용 SNMP 커뮤니티를 생성합니다

SNMPv1 및 SNMPv2c를 사용할 때 관리 스테이션과 SVM(스토리지 가상 머신) 간의 인증 메커니즘 역할을 하는 SNMP 커뮤니티를 생성할 수 있습니다.

데이터 SVM에서 SNMP 커뮤니티를 생성하여 데이터 LIF에서 'snmpwalk', 'snmpget' 등의 명령을 실행할 수 있습니다.

이 작업에 대해

- ONTAP를 새로 설치하면 SNMPv1 및 SNMPv2c가 기본적으로 비활성화됩니다.

  SNMP 커뮤니티를 생성한 후에는 SNMPv1 및 SNMPv2c가 활성화됩니다.

- ONTAP는 읽기 전용 커뮤니티를 지원합니다.
- 기본적으로 데이터 LIF에 할당되는 "데이터" 방화벽 정책은 SNMP 서비스를 "설정"으로 설정합니다.

  데이터 SVM용 SNMP 사용자를 생성할 때 SNMP 서비스 세트가 "허용"인 새 방화벽 정책을 생성해야 합니다.

  ONTAP 9.10.1.1부터 방화벽 정책이 사용되지 않으며 LIF 서비스 정책으로 완전히 대체됩니다. 자세한 내용은 을 참조하십시오 "LIF의 방화벽 정책을 구성합니다".

- 관리 SVM과 데이터 SVM 모두에 대해 SNMPv1 및 SNMPv2c 사용자를 위한 SNMP 커뮤니티를 생성할 수 있습니다.
- SVM은 SNMP 표준의 일부가 아니므로 데이터 LIF에 대한 쿼리에는 'smpwalk-v 2c-c snmpNFS 10.238.19.14 1.3.6.1.4.1.789'와 같은 NetApp 루트 OID(1.3.6.1.4.1.789)가 포함되어야 합니다.

단계

1. '시스템 SNMP community add' 명령어를 사용하여 SNMP community를 생성한다. 다음 명령을 실행하면 관리 SVM 클러스터-1에서 SNMP 커뮤니티를 생성하는 방법이 표시됩니다.

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

   다음 명령을 실행하면 SVM VS1 데이터에 SNMP 커뮤니티를 생성하는 방법이 표시됩니다.

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

2. system snmp community show 명령을 사용하여 커뮤니티가 생성되었는지 확인합니다.

   다음 명령을 실행하면 SNMPv1 및 SNMPv2c에 대해 생성된 두 개의 커뮤니티가 표시됩니다.

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

3. System services firewall policy’show' 명령어를 이용하여 "data" 방화벽 정책에서 SNMP를 서비스로 허용할 수 있는지 확인한다.

   다음 명령을 실행하면 기본 "데이터" 방화벽 정책에서 SNMP 서비스가 허용되지 않습니다(SNMP 서비스는 "관리" 방화벽 정책에서만 허용됨).

```
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. '시스템 서비스 방화벽 정책 생성' 명령을 사용하여 'NMP' 서비스를 사용하여 액세스할 수 있는 새 방화벽 정책을 만듭니다.

   다음 명령을 실행하면 'data1'이라는 새 데이터 방화벽 정책이 생성되어 'snmp'를 사용할 수 있습니다

```
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. 명령을 -firewall-policy 매개 변수와 함께 사용하여 데이터 LIF에 방화벽 정책을 `network interface modify` 적용합니다.

다음 명령을 실행하면 새 "data1" 방화벽 정책이 LIF "datalif1"에 할당됩니다.

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

에 대한 자세한 내용은 `network interface modify` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 클러스터에서 SNMPv3 사용자를 구성합니다

SNMPv3는 SNMPv1 및 SNMPv2c와 비교할 때 보안 프로토콜입니다. SNMPv3을 사용하려면 SNMP 관리자에서 SNMP 유틸리티를 실행하도록 SNMPv3 사용자를 구성해야 합니다.

단계

사용하세요 `security login create` SNMPv3 사용자를 생성하는 명령입니다.

다음 정보를 제공하라는 메시지가 표시됩니다.

- 엔진 ID: 기본값과 권장 값은 로컬 엔진 ID입니다
- 인증 프로토콜
- 인증 암호입니다
- 개인 정보 보호 프로토콜
- 개인 정보 프로토콜 암호

결과

SNMPv3 사용자는 사용자 이름 및 암호를 사용하여 SNMP 관리자에서 로그인하고 SNMP 유틸리티 명령을 실행할 수 있습니다.

SNMPv3 보안 매개 변수

SNMPv3에는 사용자가 명령을 호출할 때 이름, 인증 프로토콜, 인증 키 및 원하는 보안 수준을 입력해야 하는 인증 기능이 포함되어 있습니다.

다음 표에는 SNMPv3 보안 매개 변수가 나열되어 있습니다.

매개 변수	명령줄 옵션입니다	설명
엔진 ID	-e 엔지니어링 ID	SNMP 에이전트의 엔진 ID입니다. 기본값은 Local EngineID(권장)입니다.
보안 이름	-u 이름	사용자 이름은 32자를 초과할 수 없습니다.
authProtocol의 약어입니다	-a {none	MD5

SHA	SHA-256}	인증 유형은 없음, MD5, SHA 또는 SHA-256일 수 있습니다.
인증 키	• 암호문	최소 8자의 암호 구문
보안 수준	-l {authNo암호화	Auth암호화
noAuthNo암호화}	보안 수준은 인증, 개인 정보 보호 없음, 인증, 개인 정보 보호 또는 인증 없음일 수 있습니다. 개인 정보 보호.	개인 프로토콜
-x{none	des	aes128}
개인 정보 보호 프로토콜은 없음, des 또는 aes128일 수 있습니다	privPassword(비밀 번호)	-X 암호

다양한 보안 수준에 대한 예

이 예에서는 서로 다른 보안 수준으로 생성된 SNMPv3 사용자가 'snmpwalk'와 같은 SNMP 클라이언트 측 명령을 사용하여 클러스터 객체를 쿼리하는 방법을 보여 줍니다.

성능을 향상시키려면 테이블에서 단일 개체나 몇 개의 개체를 검색하는 대신 테이블의 모든 개체를 검색해야 합니다.

인증 프로토콜이 SHA 인 경우 'snmpwalk' 5.3.1 이상을 사용해야 합니다.

보안 수준**: auth**암호화

다음 출력에서는 auth암호화 보안 수준으로 SNMPv3 사용자를 생성하는 방법을 보여 줍니다.

```
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 모드

```
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) [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 테스트

다음 출력에서는 snmpwalk 명령을 실행하는 SNMPv3 사용자를 보여 줍니다.

성능을 향상시키려면 테이블에서 단일 개체나 몇 개의 개체를 검색하는 대신 테이블의 모든 개체를 검색해야 합니다.

```
$ 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"
```

보안 수준**: authNo**암호화

다음 출력에서는 authNo암호화 보안 수준으로 SNMPv3 사용자를 생성하는 방법을 보여 줍니다.

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

FIPS 모드

FIPS에서는 개인 정보 프로토콜에 대해 * 없음 * 을 선택할 수 없습니다. 따라서 FIPS 모드에서 authNoSNMPv3 사용자를 구성할 수 없습니다.

snmpwalk 테스트

다음 출력에서는 snmpwalk 명령을 실행하는 SNMPv3 사용자를 보여 줍니다.

성능을 향상시키려면 테이블에서 단일 개체나 몇 개의 개체를 검색하는 대신 테이블의 모든 개체를 검색해야 합니다.

```
$ 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"
```

보안 수준: **noAuthNo**암호화

다음 출력에서는 NOAuthNo암호화 보안 수준으로 SNMPv3 사용자를 생성하는 방법을 보여 줍니다.

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

FIPS 모드

FIPS에서는 개인 정보 프로토콜에 대해 * 없음 * 을 선택할 수 없습니다.

snmpwalk 테스트

다음 출력에서는 snmpwalk 명령을 실행하는 SNMPv3 사용자를 보여 줍니다.

성능을 향상시키려면 테이블에서 단일 개체나 몇 개의 개체를 검색하는 대신 테이블의 모든 개체를 검색해야 합니다.

```
$ 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"
```

에 대한 자세한 내용은 `security login create` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 네트워크에서 SNMP용 traphosts를 구성합니다

클러스터에서 SNMP 트랩이 생성될 때 알림(SNMP 트랩 PDU)을 받도록 Traphost(SNMP 관리자)를 구성할 수 있습니다. SNMP traphost의 호스트 이름 또는 IP 주소(IPv4 또는 IPv6)를

지정할 수 있습니다.

시작하기 전에

- 클러스터에서 SNMP 및 SNMP 트랩을 활성화해야 합니다.

  SNMP 및 SNMP 트랩은 기본적으로 사용하도록 설정됩니다.

- traphost 이름을 확인하기 위해 클러스터에서 DNS를 구성해야 합니다.
- IPv6 주소를 사용하여 SNMP traaphosts를 구성하려면 클러스터에서 IPv6을 활성화해야 합니다.
- traphost를 생성할 때 미리 정의된 USM(사용자 기반 보안 모델) 인증 및 개인 정보 보호 자격 증명을 지정해야 합니다.

단계

SNMP traaphost 추가:

```
system snmp traphost add
```

트랩은 하나 이상의 SNMP 관리 스테이션이 트랩 호스트로 지정된 경우에만 보낼 수 있습니다.

다음 명령을 실행하면 알려진 USM 사용자와 함께 yyy.example.com 이라는 새로운 SNMPv3 traphost가 추가됩니다.

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

다음 명령을 실행하면 호스트의 IPv6 주소를 사용하는 traphost가 추가됩니다.

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

ONTAP 클러스터에서 SNMP 폴링을 확인합니다

SNMP를 구성한 후에는 클러스터를 폴링할 수 있는지 확인해야 합니다.

이 작업에 대해

클러스터를 폴링하려면 과 같은 타사 명령을 사용해야 합니다 `snmpwalk`.

단계

1. SNMP 명령을 전송하여 다른 클러스터에서 클러스터를 폴링합니다.

   SNMPv1을 실행하는 시스템의 경우 CLI 명령을 사용합니다 `snmpwalk -v version -c community_stringip_address_or_host_name system` MIB(Management Information Base)의 내용을 검색합니다.

   이 예제에서 폴링할 클러스터 관리 LIF의 IP 주소는 10.11.12.123입니다. 명령은 MIB에서 요청된 정보를

표시합니다.

```
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
```

SNMPv2c를 실행하는 시스템의 경우 CLI 명령을 사용합니다 `snmpwalk -v version -c community_stringip_address_or_host_name system` MIB(Management Information Base)의 내용을 검색합니다.

이 예제에서 폴링할 클러스터 관리 LIF의 IP 주소는 10.11.12.123입니다. 명령은 MIB에서 요청된 정보를 표시합니다.

```
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
```

SNMPv3를 실행하는 시스템의 경우 CLI 명령을 사용합니다 `snmpwalk -v 3 -a MD5 or SHA -l authnopriv -u username -A passwordip_address_or_host_name system` MIB(Management Information Base)의 내용을 검색합니다.

이 예제에서 폴링할 클러스터 관리 LIF의 IP 주소는 10.11.12.123입니다. 명령은 MIB에서 요청된 정보를 표시합니다.

```
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
```

SNMP, 트랩 및 traphost를 관리하는 ONTAP 명령입니다

'시스템 SNMP' 명령어를 이용하여 SNMP, 트랩, Traphosts를 관리할 수 있다. SVM별로 SNMP 사용자를 관리하기 위해 '보안' 명령을 사용할 수 있다. 이벤트 명령을 사용하여 SNMP 트랩과 관련된 이벤트를 관리할 수 있습니다.

SNMP를 구성하는 명령입니다

원하는 작업	이 명령 사용…
클러스터에서 SNMP를 설정합니다	'options-option-name snmp.enable-option-value on'입니다 관리(관리) 방화벽 정책에서 SNMP 서비스를 허용해야 합니다. 시스템 서비스 방화벽 policy show 명령을 사용하여 SNMP가 허용되는지 여부를 확인할 수 있습니다.
클러스터에서 SNMP를 해제합니다	'options-option-name snmp.enable-option-value off'

SNMP v1, v2c 및 v3 사용자를 관리하는 명령입니다

원하는 작업	이 명령 사용…
SNMP 사용자를 구성합니다	'보안 로그인 생성'
SNMP 사용자를 표시합니다	`security snmpusers`그리고 `security login show -application snmp`
SNMP 사용자를 삭제합니다	'보안 로그인 삭제

SNMP 사용자에 대한 로그인 방법의 액세스 제어 역할 이름을 수정합니다	보안 로그인 수정

연락처 및 위치 정보를 제공하는 명령입니다

원하는 작업	이 명령 사용…
클러스터의 연락처 정보를 표시하거나 수정합니다	'시스템 SNMP 연락처'
클러스터의 위치 세부 정보를 표시하거나 수정합니다	'시스템 SNMP 위치'

SNMP 커뮤니티 관리를 위한 명령입니다

원하는 작업	이 명령 사용…
SVM이나 클러스터의 모든 SVM에 대해 읽기 전용(ro) 커뮤니티를 추가할 수 있습니다	'시스템 SNMP 커뮤니티 추가'
커뮤니티 또는 모든 커뮤니티를 삭제합니다	시스템 SNMP community delete
모든 커뮤니티 목록을 표시합니다	'시스템 SNMP 커뮤니티 쇼'

SVM은 SNMP 표준의 일부가 아니므로 데이터 LIF에 대한 쿼리에는 'snmpwalk-v 2c-c snmpNFS 10.238.19.14 1.3.6.1.4.1.789'와 같은 NetApp 루트 OID(1.3.6.1.4.1.789)가 포함되어야 합니다.

SNMP 옵션 값을 표시하는 명령입니다

원하는 작업	이 명령 사용…
클러스터 연락처, 연락처 위치, 클러스터가 트랩을 전송하도록 구성되었는지 여부, 트랩 목록, 커뮤니티 및 액세스 제어 유형 목록을 포함한 모든 SNMP 옵션의 현재 값을 표시합니다	'시스템 SNMP 쇼'

SNMP 트랩 및 트랩 호스트를 관리하는 명령입니다

원하는 작업	이 명령 사용…
클러스터에서 보낸 SNMP 트랩을 설정합니다	'시스템 SNMP init-init 1'
클러스터에서 보낸 SNMP 트랩을 해제합니다	'시스템 SNMP init-init 0'
클러스터의 특정 이벤트에 대해 SNMP 알림을 수신하는 Traphost를 추가합니다	'시스템 SNMP traaphost add'

traphost를 삭제합니다	'system SNMP traaphost delete
Traphosts 목록을 표시합니다	'system SNMP traaphost show'

SNMP 트랩과 관련된 이벤트를 관리하는 명령입니다

원하는 작업	이 명령 사용…
SNMP 트랩(기본 제공)이 생성되는 이벤트를 표시합니다	이벤트 루트쇼 SNMP 관련 이벤트만 보려면 '-snmp-support true' 매개변수를 사용하십시오. 'instance-messagename<message>' 매개 변수를 사용하여 이벤트가 발생한 이유와 수정 조치에 대해 자세히 설명합니다. 개별 SNMP 트랩 이벤트를 특정 트랩 호스트 대상으로 라우팅하는 것은 지원되지 않습니다. 모든 SNMP 트랩 이벤트가 모든 트랩 호스트 대상으로 전송됩니다.
SNMP 트랩으로 전송된 이벤트 알림인 SNMP 트랩 기록 레코드 목록을 표시합니다	이벤트 스내피스토리 쇼
SNMP 트랩 기록 레코드를 삭제합니다	이벤트 스내피스토리 삭제

관련 정보

- "시스템 SNMP"
- "보안 snmpusers"
- "보안"
- "이벤트"
- "보안 로그인"