



# **SNMP 구성**

## **System Manager Classic**

NetApp  
January 02, 2024

# 목차

- SNMP 구성 ..... 1
  - SNMP 구성 개요 ..... 1
  - SNMP 구성 워크플로우 ..... 1

# SNMP 구성

## SNMP 구성 개요

ONTAP 9.7 이하와 함께 ONTAP System Manager\_CLASSIC\_INTERFACE를 사용하면 클러스터 관리 수준에서 SNMP를 구성하고 커뮤니티, 보안 사용자 및 트라프호스트를 추가하고 SNMP 통신을 테스트할 수 있습니다.

다음과 같은 방법으로 클러스터에 대한 SNMP 액세스를 구성하려면 다음 절차를 사용해야 합니다.

- ONTAP 9를 실행하는 클러스터로 작업하고 있습니다.
- 사용 가능한 모든 옵션을 탐색하는 것이 아니라 모범 사례를 사용하려고 합니다.



이 절차에는 명령줄 인터페이스를 사용해야 하는 몇 가지 단계가 있습니다.

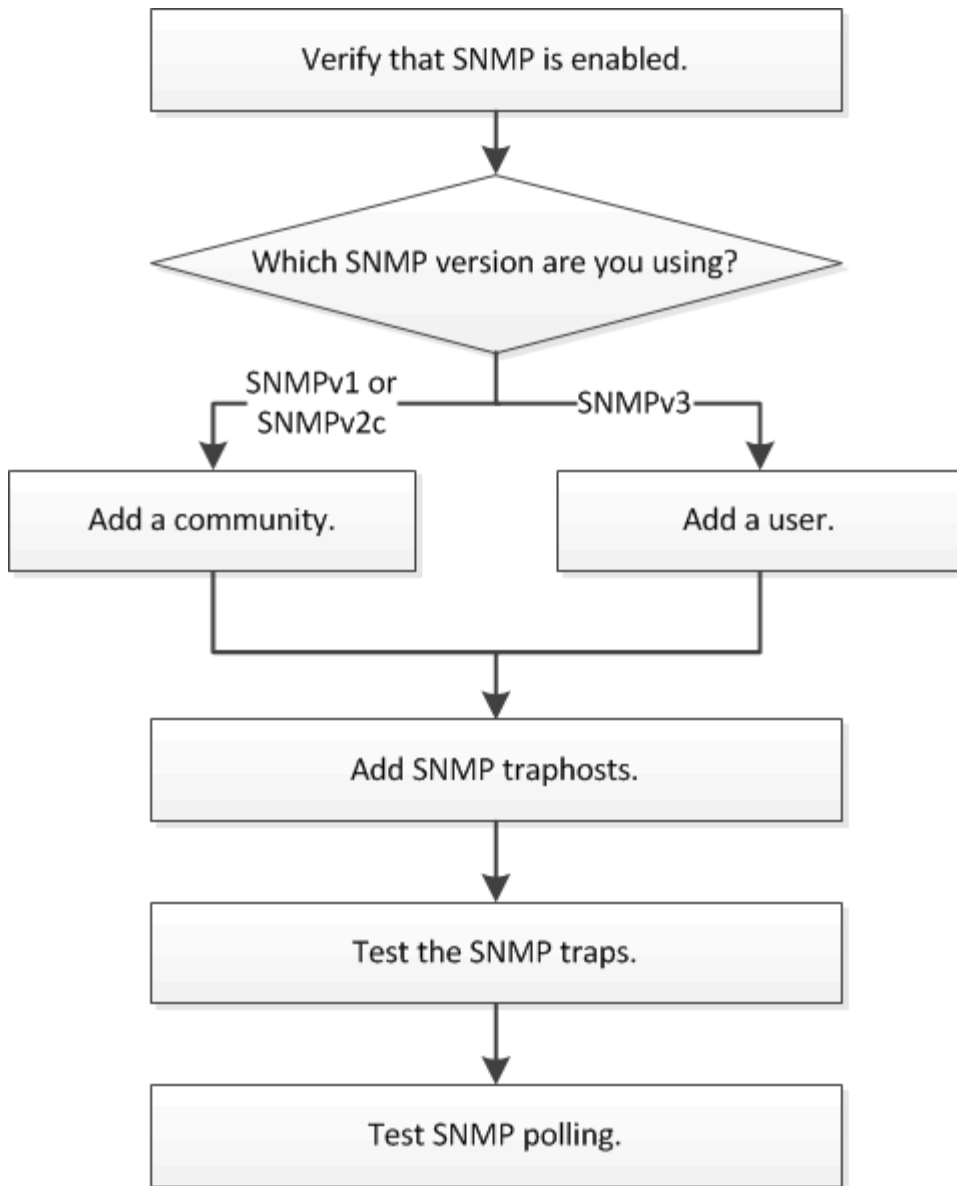
## ONTAP에서 이 작업을 수행하는 다른 방법

모든 ONTAP 9 버전에 대해 를 사용하여 클러스터에 대한 SNMP 액세스를 구성할 수 있습니다. 해당 버전의 ONTAP에 적합한 절차를 사용해야 합니다.

에서 이러한 작업을 수행하려면...	자세한 내용은...
재설계된 System Manager(ONTAP 9.7 이상에서 사용 가능)	"클러스터에서 SNMP 관리(클러스터 관리자만 해당) 및 GT; 개요"
ONTAP CLI(명령줄 인터페이스)	"SNMP 관리를 위한 명령입니다"

## SNMP 구성 워크플로우

SNMP를 구성하려면 SNMP를 활성화하고, 선택적으로 SNMPv1 또는 SNMPv2c 커뮤니티를 구성하고, 선택적으로 SNMPv3 사용자를 추가하고, SNMP 트라프호스트를 추가하고, SNMP 폴링 및 트랩을 테스트해야 합니다.



## SNMP가 활성화되어 있는지 확인합니다

ONTAP 9.7 이하와 ONTAP System Manager\_CLASSIC\_INTERFACE를 사용하여 클러스터에서 SNMP가 활성화되었는지 확인할 수 있습니다.

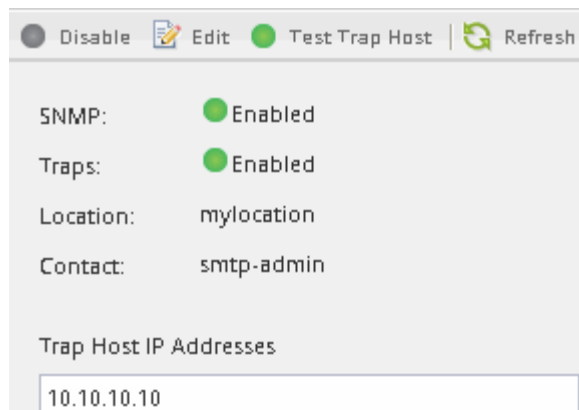
이 작업에 대해

모든 버전의 ONTAP에서 SNMPv3는 기본적으로 클러스터 수준에서 활성화되어 있으며 SNMPv1 및 SNMPv2c는 기본적으로 비활성화되어 있습니다. SNMP 커뮤니티를 생성하면 SNMPv1 및 SNMPv2c가 활성화됩니다.

데이터 LIF에서 SNMP는 기본적으로 해제되어 있습니다. 데이터 LIF에서 SNMP를 사용하는 방법에 대한 자세한 내용은 를 참조하십시오 ["네트워크 관리"](#).

단계

1. 홈 아이콘을 클릭합니다.
2. Setup\* 창에서 \* SNMP \* 창으로 이동합니다.



클러스터의 현재 SNMP 상태를 볼 수 있습니다.

SNMP가 활성화되지 않은 경우 \* Enable \* 을 클릭합니다.

## SNMP 커뮤니티를 추가합니다

ONTAP 9.7 이하와 함께 ONTAP System Manager\_CLASSIC\_INTERFACE를 사용하여 SNMPv1 또는 SNMPv2c를 실행하는 클러스터의 관리 스토리지 가상 시스템(SVM)에 커뮤니티를 추가할 수 있습니다. System Manager는 SNMP 프로토콜 SNMPv1 및 SNMPv2c 및 SNMP 커뮤니티를 사용하여 스토리지 시스템을 검색합니다.

이 작업에 대해

이 절차는 클러스터의 관리 SVM에 SNMP 커뮤니티를 추가하기 위한 것입니다. 데이터 SVM에 SNMP 커뮤니티를 추가하는 절차는 에서 설명합니다 ["네트워크 관리"](#).

ONTAP를 새로 설치하면 SNMPv1 및 SNMPv2c가 기본적으로 비활성화됩니다. SNMP 커뮤니티를 생성하면 SNMPv1 및 SNMPv2c가 활성화됩니다.

단계

1. SNMP 창에서 \* Edit \* 를 클릭하여 \* Edit SNMP Settings \* 대화 상자를 엽니다.
2. 일반 \* 탭에서 ONTAP 시스템의 담당자 및 위치를 지정합니다.
3. 추가 \* 를 클릭하고 커뮤니티 이름을 입력한 다음 \* 커뮤니티 이름 \* 창에서 \* 확인 \* 을 클릭합니다.

여러 커뮤니티 이름을 추가할 수 있습니다. 커뮤니티 이름은 최대 32자까지 가능하며 특수 문자(", /:", |")는 포함할 수 없습니다

4. 커뮤니티 이름 추가를 마치면 \* SNMP 설정 편집 \* 대화 상자에서 \* 확인 \* 을 클릭합니다.

## SNMPv3 보안 사용자를 추가합니다

ONTAP 9.7 이하와 함께 ONTAP System Manager\_CLASSIC\_INTERFACE를 사용하여 클러스터 레벨에 SNMPv3 사용자를 추가할 수 있습니다.

SNMPv3 사용자는 지정한 인증 및 개인 정보 보호 설정을 사용하여 traphost(SNMP 관리자)에서 SNMP 유틸리티를 실행할 수 있습니다. SNMPv3는 암호 구문 및 암호화를 사용하여 고급 보안을 제공합니다.

이 작업에 대해

클러스터 수준에서 SNMPv3 사용자를 추가하면 해당 사용자는 ""GMT" 방화벽 정책이 적용된 모든 LIF를 통해 클러스터에 액세스할 수 있습니다.

단계

1. SNMP 창에서 \* Edit \* 를 클릭하여 \* Edit SNMP Settings \* 대화 상자를 엽니다.
2. SNMPv3 \* 탭에서 \* 추가 \* 를 클릭하여 \* SNMPv3 사용자 추가 \* 대화 상자를 엽니다.
3. 다음 값을 입력합니다.

- a. SNMPv3 사용자 이름을 입력합니다.

보안 사용자 이름은 31자를 초과할 수 없으며 다음 특수 문자를 포함할 수 없습니다.

','/:'"|'

- b. 엔진 ID에서 기본값인 Local Engine ID를 선택합니다.

엔진 ID는 SNMPv3 메시지에 대한 인증 및 암호화 키를 생성하는 데 사용됩니다.

- c. 인증 프로토콜을 선택하고 인증 암호를 입력합니다.

암호는 8자 이상이어야 합니다.

- d. 선택 사항: 개인 정보 보호 프로토콜을 선택하고 암호를 입력합니다.

4. SNMPv3 사용자 추가 \* 대화 상자에서 \* 확인 \* 을 클릭합니다.

보안 사용자 이름을 여러 개 추가할 때마다 \* OK \* 를 클릭하여 추가할 수 있습니다. 예를 들어, SNMP를 사용하여 다른 권한이 필요한 여러 애플리케이션을 모니터링하는 경우 각 모니터링 또는 관리 기능에 대해 SNMPv3 사용자를 추가해야 할 수 있습니다.

5. 사용자 이름 추가를 마치면 \* SNMP 설정 편집 \* 대화 상자에서 \* 확인 \* 을 클릭합니다.

## SNMP traaphost를 추가합니다

ONTAP 9.7 이하와 함께 ONTAP System Manager\_CLASSIC\_INTERFACE를 사용하여 트랩이 클러스터에서 생성될 때 SNMP 알림(SNMP 트랩 프로토콜 데이터 단위)을 수신할 트랩 호스트(SNMP 매니저)를 추가할 수 있습니다.

시작하기 전에

IPv6 주소가 있는 SNMP 트라프호스트를 구성하는 경우 클러스터에서 IPv6를 활성화해야 합니다.

이 작업에 대해

SNMP 및 SNMP 트랩은 기본적으로 사용하도록 설정됩니다. SNMP 지원의 NetApp 기술 보고서 TR-4220 에는 SNMP 트랩이 지원하는 모든 기본 이벤트 목록이 포함되어 있습니다.

["NetApp 기술 보고서 4220: Data ONTAP의 SNMP 지원"](#)

단계

1. SNMP 창에서 \* EDIT \* 를 클릭하여 \* SNMP 설정 편집 \* 대화 상자를 엽니다.
2. [[step2-verify-enable-trap] \* Trap Hosts \* 탭에서 \* 트랩 사용 \* 확인란이 선택되어 있는지 확인하고 \* 추가 \* 를 클릭합니다.
3. traphost IP 주소를 입력한 다음 \* Trap Hosts \* 창에서 \* OK \* 를 클릭합니다.

SNMP traphost의 IP 주소는 IPv4 또는 IPv6일 수 있습니다.

4. 다른 traaphost를 추가하려면 를 반복합니다 [2단계](#) 및 [3단계](#).
5. traphosts 추가를 마치면 \* SNMP 설정 편집 \* 대화 상자에서 \* 확인 \* 을 클릭합니다.

## SNMP 트랩을 테스트합니다

ONTAP 9.7 이하와 함께 ONTAP System Manager\_CLASSIC\_INTERFACE를 사용하여 SNMP 트랩을 테스트할 수 있습니다. traphost와의 통신은 추가 시 자동으로 검증되지 않으므로 SNMP traphost가 트랩을 올바르게 수신할 수 있는지 확인해야 합니다.

단계

1. SNMP \* 화면으로 이동합니다.
2. Traphost를 추가한 클러스터에서 트랩을 생성하려면 \* Test Trap Host \* 를 클릭합니다.
3. 트랩 호스트 위치에서 트랩이 수신되었는지 확인합니다.

SNMP traaphost를 관리하는 데 일반적으로 사용하는 소프트웨어가 무엇이든 사용합니다.

## SNMP 폴링을 테스트합니다

SNMP를 구성한 후에는 클러스터를 폴링할 수 있는지 확인해야 합니다.

이 작업에 대해

클러스터를 폴링하려면 'snmpwalk'와 같은 타사 명령을 사용해야 합니다.

단계

1. SNMP 명령을 전송하여 다른 클러스터에서 클러스터를 폴링합니다.

SNMPv1을 실행하는 시스템의 경우 CLI 명령 'snmpwalk -v version -c community\_stringip\_address\_or\_host\_name system'을 사용하여 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 명령 'snmpwalk -v version -c community\_stringip\_address\_or\_host\_name system'을 사용하여 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
```

SNMPv3을 실행하는 시스템의 경우 CLI 명령 'snmpwalk -v 3 -a MD5 or SHA-1 AuthNo암호화 -u username -a passwordip\_address\_or\_host\_name system'을 사용하여 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
```

## 저작권 정보

Copyright © 2023 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

## 상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.