SNMP 모니터링을 사용합니다

StorageGRID

NetApp
September 04, 2024

This PDF was generated from https://docs.netapp.com/ko-kr/storagegrid-116/monitor/configuring-snmp-agent.html on September 04, 2024. Always check docs.netapp.com for the latest.

목차

SNMP 모니터링을 사용합니다 1
제공합니다 1
SNMP 버전 지원 1
제한 사항 2
MIB에 액세스합니다 2
SNMP 에이전트를 구성합니다 2
SNMP 에이전트를 업데이트합니다 11

SNMP 모니터링을 사용합니다

SNMP(Simple Network Management Protocol)를 사용하여 StorageGRID를 모니터링하려면 StorageGRID에 포함된 SNMP 에이전트를 구성해야 합니다.

- SNMP 에이전트를 구성합니다
- SNMP 에이전트를 업데이트합니다

제공합니다

각 StorageGRID 노드는 MIB(Management Information Base)를 제공하는 SNMP 에이전트 또는 데몬을 실행합니다. StorageGRID MIB에는 알림 및 알람에 대한 테이블 및 알림 정의가 포함되어 있습니다. MIB에는 각 노드의 플랫폼 및 모델 번호와 같은 시스템 설명 정보도 포함되어 있습니다. 각 StorageGRID 노드는 MIB-II 객체의 하위 세트도 지원합니다.

처음에는 모든 노드에서 SNMP가 사용되지 않습니다. SNMP 에이전트를 구성할 때 모든 StorageGRID 노드는 동일한 구성을 받습니다.

StorageGRID SNMP 에이전트는 세 가지 버전의 SNMP 프로토콜을 모두 지원합니다. 쿼리에 대한 읽기 전용 MIB 액세스를 제공하며 관리 시스템에 두 가지 유형의 이벤트 기반 알림을 보낼 수 있습니다.

- * 트랩 * 은 관리 시스템에서 확인이 필요하지 않은 SNMP 에이전트가 보낸 알림입니다. 트랩은 알림이 트리거되는 등 StorageGRID 내에 발생한 사항을 관리 시스템에 알리는 역할을 합니다.

  트랩은 SNMP의 세 가지 버전에서 모두 지원됩니다.

- * 알림 * 은 트랩과 유사하지만 관리 시스템에서 확인을 요구합니다. SNMP 에이전트가 일정 시간 내에 승인을 받지 못하면 승인을 받거나 최대 재시도 값에 도달할 때까지 알림을 다시 보냅니다.

  SNMPv2c 및 SNMPv3에서 알림이 지원됩니다.

다음과 같은 경우 트랩 및 알림 알림이 전송됩니다.

- 기본 또는 사용자 지정 알림은 모든 심각도 수준에서 트리거됩니다. 경고에 대한 SNMP 알림을 표시하지 않으려면 경고에 대한 무음을 구성해야 합니다. 경고 알림은 선호하는 송신자가 되도록 구성된 관리 노드에서 보냅니다.

  각 알림은 알림의 심각도 수준, activeMinorAlert, activeMajorAlert 및 activeCriticalAlert 중 하나를 기준으로 세 가지 트랩 유형 중 하나에 매핑됩니다. 이러한 트랩을 트리거할 수 있는 경고에 대한 설명은 을 참조하십시오 경고 참조.

- 특정 알람(기존 시스템)은 지정된 심각도 수준 이상에서 트리거됩니다.

  > 모든 알람 또는 알람 심각도에 대해 SNMP 알림이 전송되지 않습니다.

SNMP 버전 지원

이 표에는 각 SNMP 버전에서 지원되는 항목에 대한 자세한 요약 정보가 나와 있습니다.

	SNMPv1	SNMPv2c입니다	SNMPv3
쿼리	읽기 전용 MIB 쿼리	읽기 전용 MIB 쿼리	읽기 전용 MIB 쿼리
쿼리 인증	커뮤니티 문자열	커뮤니티 문자열	USM(사용자 기반 보안 모델) 사용자
알림	트랩만	함정 및 통보	함정 및 통보
알림 인증	각 트랩 대상에 대한 기본 트랩 커뮤니티 또는 사용자 지정 커뮤니티 문자열입니다	각 트랩 대상에 대한 기본 트랩 커뮤니티 또는 사용자 지정 커뮤니티 문자열입니다	각 트랩 대상에 대한 USM 사용자입니다

제한 사항

- StorageGRID는 읽기 전용 MIB 액세스를 지원합니다. 읽기-쓰기 액세스는 지원되지 않습니다.
- 그리드의 모든 노드는 동일한 구성을 받습니다.
- SNMPv3: StorageGRID는 전송 지원 모드(TSM)를 지원하지 않습니다.
- SNMPv3: 지원되는 유일한 인증 프로토콜은 SHA(HMAC-SHA-96)입니다.
- SNMPv3: 지원되는 유일한 개인 정보 보호 프로토콜은 AES입니다.

MIB에 액세스합니다

StorageGRID 노드의 다음 위치에서 MIB 정의 파일에 액세스할 수 있습니다.

'/usr/share/snmp/mibs/netapp-StorageGrid-mib.txt'

관련 정보

- 경고 참조
- 알람 기준(레거시 시스템)
- SNMP 알림을 생성하는 알람(레거시 시스템)
- 알림 메시지를 해제합니다

SNMP 에이전트를 구성합니다

읽기 전용 MIB 액세스 및 알림에 타사 SNMP 관리 시스템을 사용하려는 경우 StorageGRID SNMP 에이전트를 구성할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 루트 액세스 권한이 있습니다.

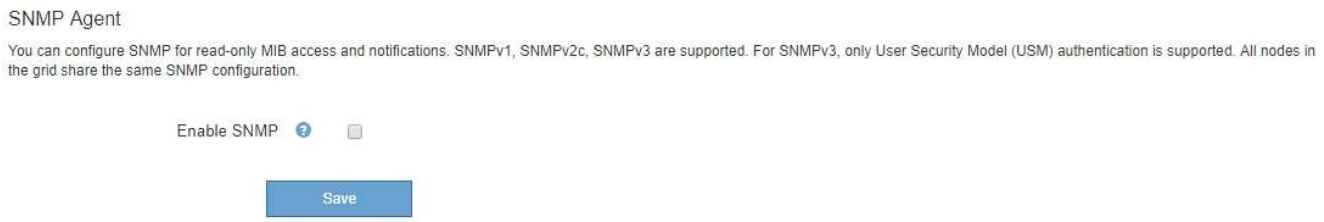
이 작업에 대해

StorageGRID SNMP 에이전트는 세 가지 버전의 SNMP 프로토콜을 모두 지원합니다. 하나 이상의 버전에 대해 에이전트를 구성할 수 있습니다.

단계

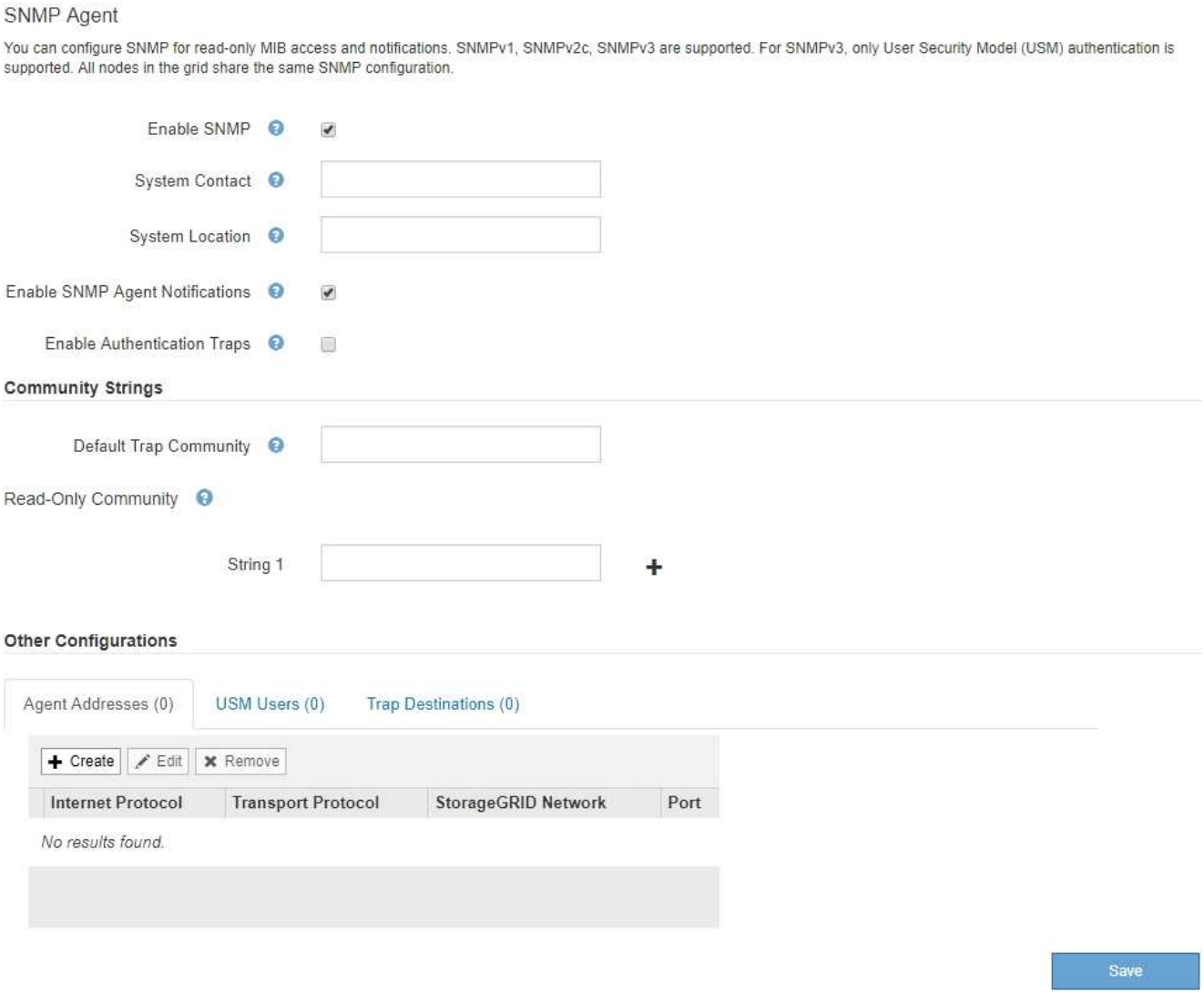
1. 구성 * > * 모니터링 * > * SNMP 에이전트 * 를 선택합니다.

   SNMP Agent 페이지가 나타납니다.



2. 모든 그리드 노드에서 SNMP 에이전트를 활성화하려면 * SNMP * 활성화 확인란을 선택합니다.

   SNMP 에이전트를 구성하는 필드가 나타납니다.



3. 시스템 연락처 * 필드에 sysContact에 대한 SNMP 메시지에 StorageGRID를 제공할 값을 입력합니다.

일반적으로 시스템 담당자는 이메일 주소입니다. 제공하는 값은 StorageGRID 시스템의 모든 노드에 적용됩니다. 시스템 연락처 * 는 최대 255자까지 입력할 수 있습니다.

4. 시스템 위치 * 필드에 sysLocation에 대한 SNMP 메시지에 StorageGRID를 제공할 값을 입력합니다.

   시스템 위치는 StorageGRID 시스템의 위치를 식별하는 데 유용한 모든 정보가 될 수 있습니다. 예를 들어 시설의 주소를 사용할 수 있습니다. 제공하는 값은 StorageGRID 시스템의 모든 노드에 적용됩니다. * 시스템 위치 * 는 최대 255자까지 입력할 수 있습니다.

5. StorageGRID SNMP 에이전트가 트랩을 전송하고 알림을 보내도록 하려면 * SNMP 에이전트 알림 사용 * 확인란을 선택한 상태로 유지합니다.

   이 확인란의 선택을 취소하면 SNMP 에이전트는 읽기 전용 MIB 액세스를 지원하지만 SNMP 알림은 보내지 않습니다.

6. StorageGRID SNMP 에이전트가 잘못 인증된 프로토콜 메시지를 수신할 경우 인증 트랩을 보내도록 하려면 * 인증 트랩 사용 * 확인란을 선택합니다.

7. SNMPv1 또는 SNMPv2c를 사용하는 경우 커뮤니티 문자열 섹션을 완료합니다.

   이 섹션의 필드는 SNMPv1 또는 SNMPv2c에서 커뮤니티 기반 인증에 사용됩니다. 이 필드는 SNMPv3에는 적용되지 않습니다.

   a. 기본 트랩 커뮤니티 * 필드에 트랩 대상에 사용할 기본 커뮤니티 문자열을 입력합니다(선택 사항).

      필요한 경우 다른 커뮤니티 문자열을 제공할 수 있습니다(""사용자 지정") 특정 트랩 대상을 정의합니다.

      - 기본 트랩 커뮤니티 * 는 최대 32자이고 공백 문자를 포함할 수 없습니다.

   b. 읽기 전용 커뮤니티*의 경우 IPv4 및 IPv6 에이전트 주소에서 읽기 전용 MIB 액세스를 허용하도록 하나 이상의 커뮤니티 문자열을 입력합니다. 더하기 기호를 클릭합니다 ➕ 여러 문자열을 추가합니다.

      관리 시스템이 StorageGRID MIB를 쿼리하면 커뮤니티 문자열을 보냅니다. 커뮤니티 문자열이 여기에 지정된 값 중 하나와 일치하면 SNMP 에이전트는 관리 시스템에 응답을 보냅니다.

      각 커뮤니티 문자열은 최대 32자이고 공백 문자를 포함할 수 없습니다. 최대 5개의 문자열이 허용됩니다.

      > ⓘ StorageGRID 시스템의 보안을 보장하기 위해 커뮤니티 문자열로 ""public""을 사용하지 마십시오. 커뮤니티 문자열을 입력하지 않으면 SNMP 에이전트는 StorageGRID 시스템의 그리드 ID를 커뮤니티 문자열로 사용합니다.

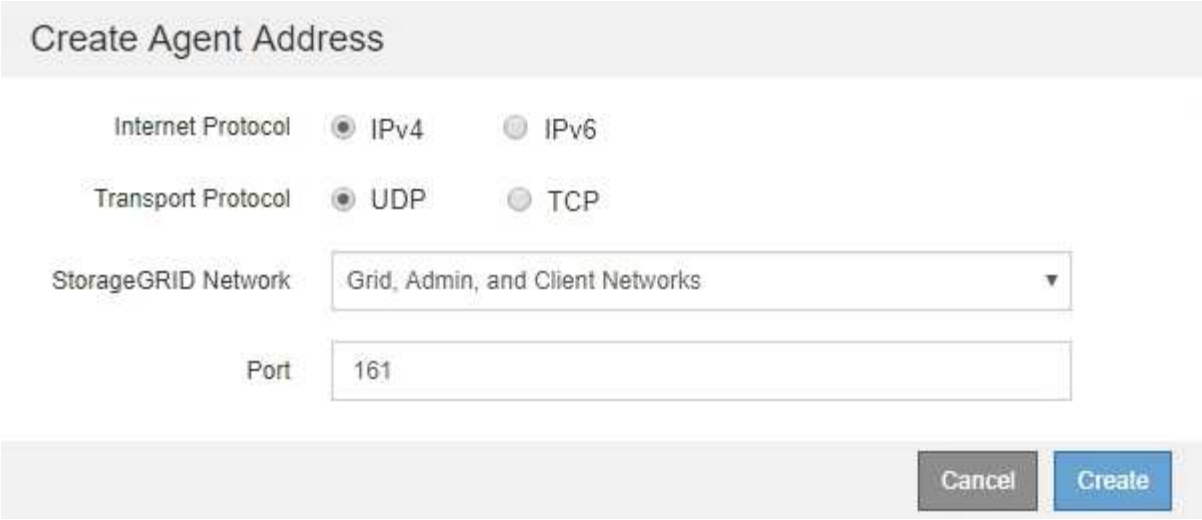
8. 필요에 따라 기타 구성 섹션에서 상담원 주소 탭을 선택합니다.

   이 탭을 사용하여 하나 이상의 ""수신 주소""를 지정하십시오. SNMP 에이전트가 쿼리를 받을 수 있는 StorageGRID 주소입니다. 각 에이전트 주소에는 인터넷 프로토콜, 전송 프로토콜, StorageGRID 네트워크 및 포트(옵션)가 포함됩니다.

   에이전트 주소를 구성하지 않으면 기본 수신 주소는 모든 StorageGRID 네트워크에서 UDP 포트 161입니다.

   a. Create * 를 클릭합니다.

      상담원 주소 작성 대화 상자가 나타납니다.



b. 인터넷 프로토콜 * 의 경우 이 주소가 IPv4와 IPv6을 사용할지 여부를 선택합니다.

   기본적으로 SNMP는 IPv4를 사용합니다.

c. 전송 프로토콜 * 의 경우 이 주소가 UDP 또는 TCP를 사용할지 여부를 선택합니다.

   기본적으로 SNMP는 UDP를 사용합니다.

d. StorageGRID 네트워크 * 필드에서 쿼리를 수신할 StorageGRID 네트워크를 선택합니다.

   - 그리드, 관리자 및 클라이언트 네트워크:StorageGRID는 세 네트워크 모두에서 SNMP 쿼리를 수신해야 합니다.
   - 그리드 네트워크
   - 관리자 네트워크
   - 클라이언트 네트워크

   > StorageGRID와 클라이언트 통신이 안전하게 유지되도록 하려면 클라이언트 네트워크에 대한 에이전트 주소를 만들지 않아야 합니다.

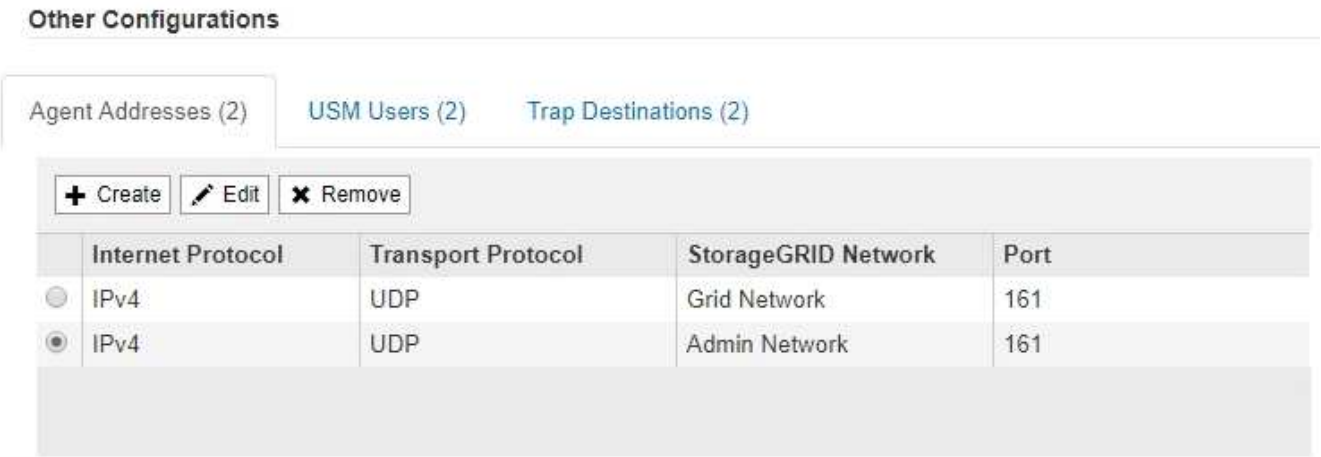
e. Port* 필드에 SNMP 에이전트가 수신 대기해야 하는 포트 번호를 입력합니다(선택 사항).

   SNMP 에이전트의 기본 UDP 포트는 161이지만 사용하지 않는 포트 번호를 입력할 수 있습니다.

   > SNMP 에이전트를 저장하면 StorageGRID에서 내부 방화벽에 있는 에이전트 주소 포트를 자동으로 엽니다. 모든 외부 방화벽이 이러한 포트에 대한 액세스를 허용하는지 확인해야 합니다.

f. Create * 를 클릭합니다.

   상담원 주소가 생성되어 테이블에 추가됩니다.



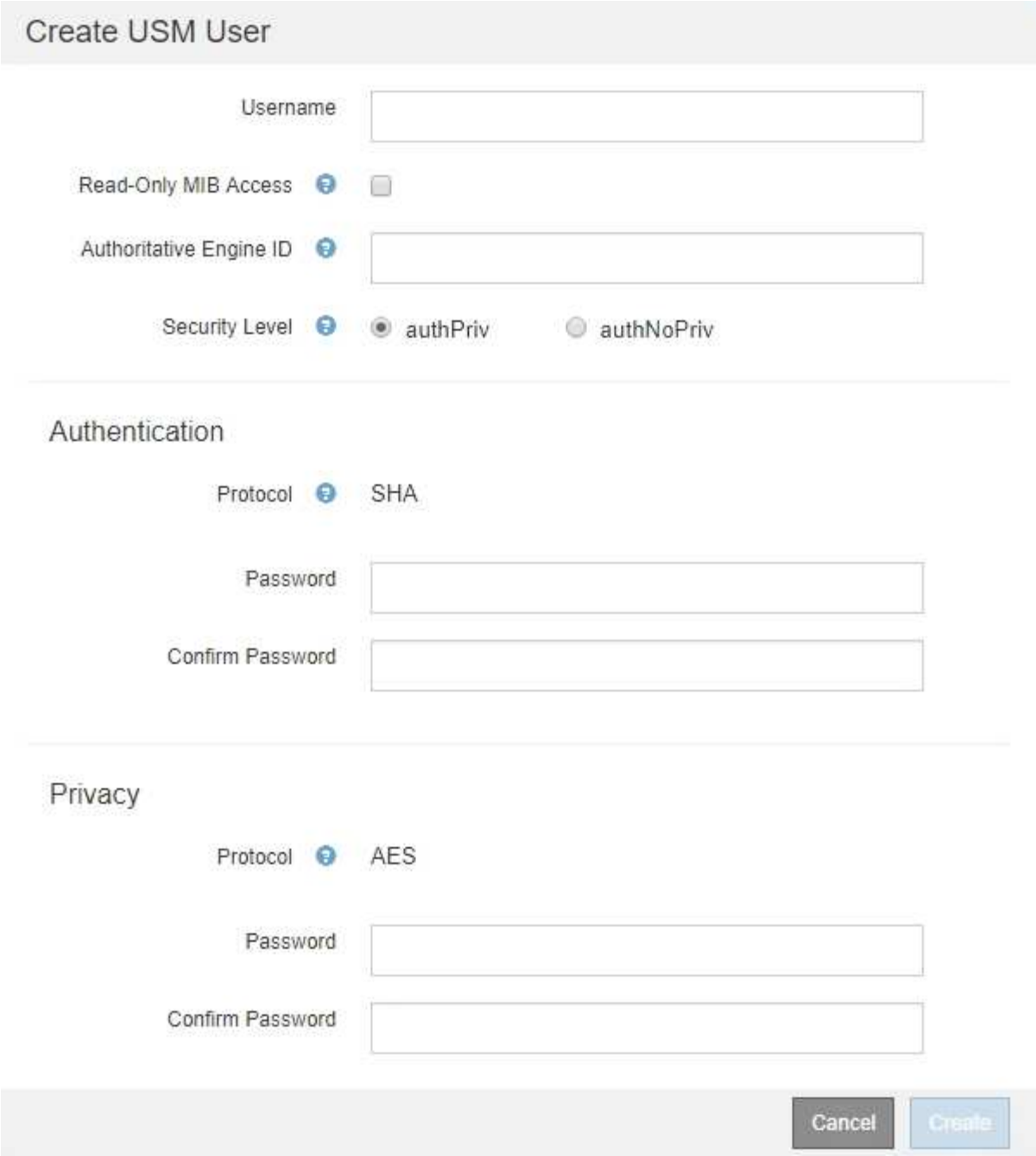
9. SNMPv3을 사용하는 경우 기타 구성 섹션에서 USM 사용자 탭을 선택합니다.

   이 탭을 사용하여 MIB를 쿼리하거나 트랩 및 알림을 받을 권한이 있는 USM 사용자를 정의합니다.

   > SNMPv1 또는 SNMPv2c만 사용하는 경우에는 이 단계가 적용되지 않습니다.

   a. Create * 를 클릭합니다.

      USM 사용자 생성 대화 상자가 나타납니다.



b. 이 USM 사용자에 대한 고유한 * 사용자 이름 * 을 입력합니다.

   사용자 이름은 최대 32자이며 공백 문자를 포함할 수 없습니다. 사용자가 생성된 후에는 사용자 이름을 변경할 수 없습니다.

c. 이 사용자가 MIB에 대한 읽기 전용 액세스를 가지고 있어야 하는 경우 * 읽기 전용 MIB 액세스 * 확인란을 선택합니다.

   읽기 전용 MIB 액세스 * 를 선택하면 * Authoritative Engine ID * 필드가 비활성화됩니다.

   > ⓘ 읽기 전용 MIB 액세스가 있는 USM 사용자는 엔진 ID를 가질 수 없습니다.

d. 이 사용자를 알림 대상에서 사용할 경우 이 사용자에 대한 * Authoritative Engine ID * 를 입력합니다.

> SNMPv3 알림 대상에는 엔진 ID가 있는 사용자가 있어야 합니다. SNMPv3 트랩 대상에는 엔진 ID를 가진 사용자가 있을 수 없습니다.

신뢰할 수 있는 엔진 ID는 5바이트에서 32바이트까지 16진수로 지정할 수 있습니다.

e. USM 사용자의 보안 수준을 선택합니다.

- * auth암호화 *: 이 사용자는 인증 및 개인 정보 보호(암호화)와 통신합니다. 인증 프로토콜 및 암호와 개인 정보 보호 프로토콜 및 암호를 지정해야 합니다.
- * authNo암호화 *: 이 사용자는 개인 정보 보호 없이 인증과 통신합니다(암호화 없음). 인증 프로토콜과 암호를 지정해야 합니다.

f. 이 사용자가 인증에 사용할 암호를 입력하고 확인합니다.

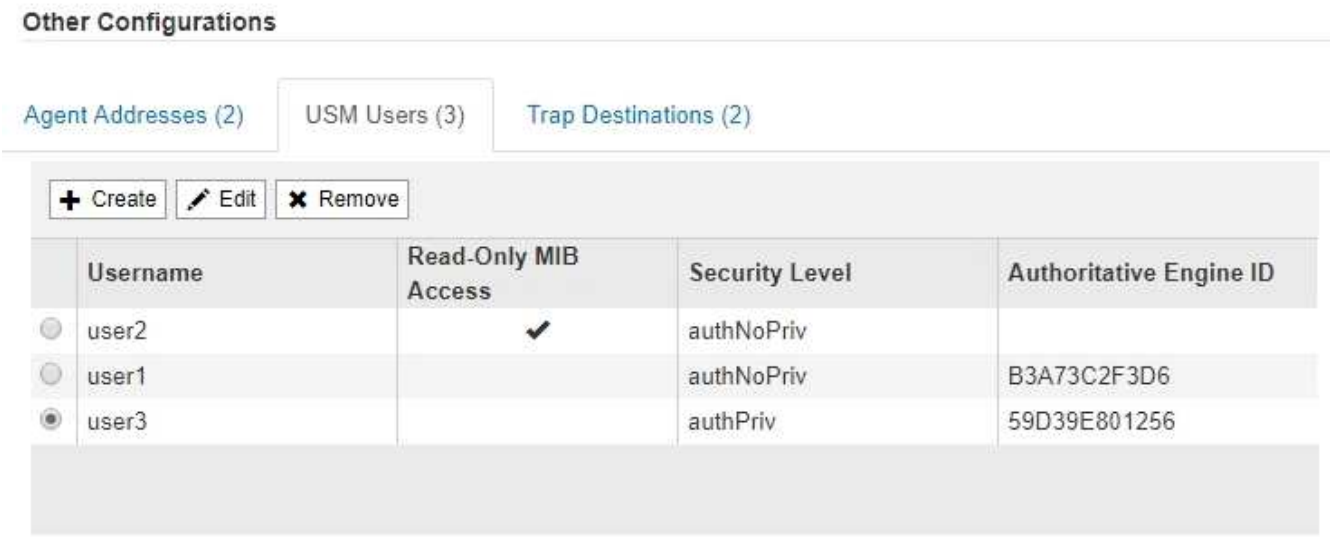
> 지원되는 유일한 인증 프로토콜은 SHA(HMAC-SHA-96)입니다.

g. auth암호화 * 를 선택한 경우 이 사용자가 개인 정보 보호에 사용할 암호를 입력하고 확인합니다.

> 지원되는 개인 정보 보호 프로토콜은 AES 뿐입니다.

h. Create * 를 클릭합니다.

USM 사용자가 생성되어 테이블에 추가됩니다.

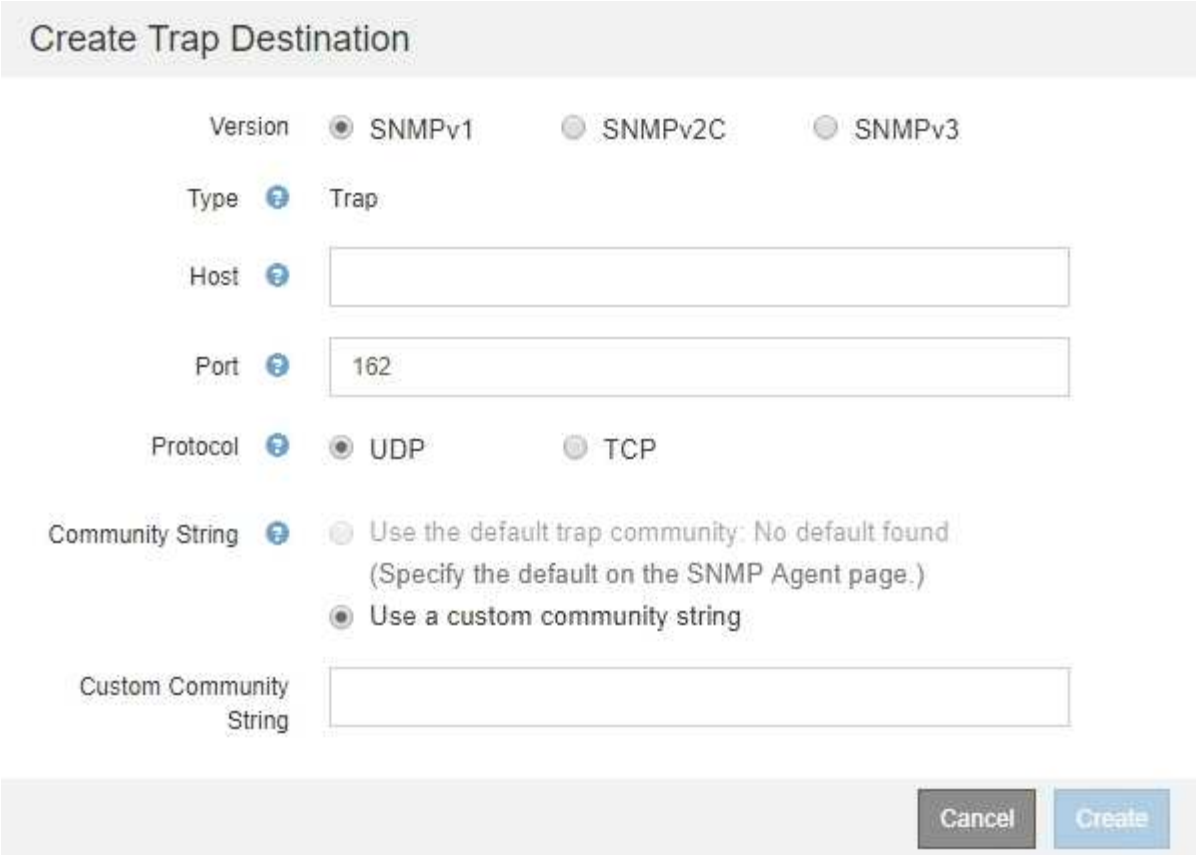


10. 기타 구성 섹션에서 트랩 대상 탭을 선택합니다.

트랩 대상 탭에서는 StorageGRID 트랩 또는 알림 알림에 대한 하나 이상의 대상을 정의할 수 있습니다. SNMP 에이전트를 활성화하고 * 저장 * 을 클릭하면 StorageGRID가 정의된 각 대상으로 알림을 보내기 시작합니다. 알림 및 알람이 트리거되면 알림이 전송됩니다. 지원되는 MIB-II 엔티티에 대해서도 표준 알림이 전송됩니다(예: ifdown 및 coldstart).

a. Create * 를 클릭합니다.

Create Trap Destination 대화상자가 나타납니다.



b. 버전 * 필드에서 이 알림에 사용할 SNMP 버전을 선택합니다.

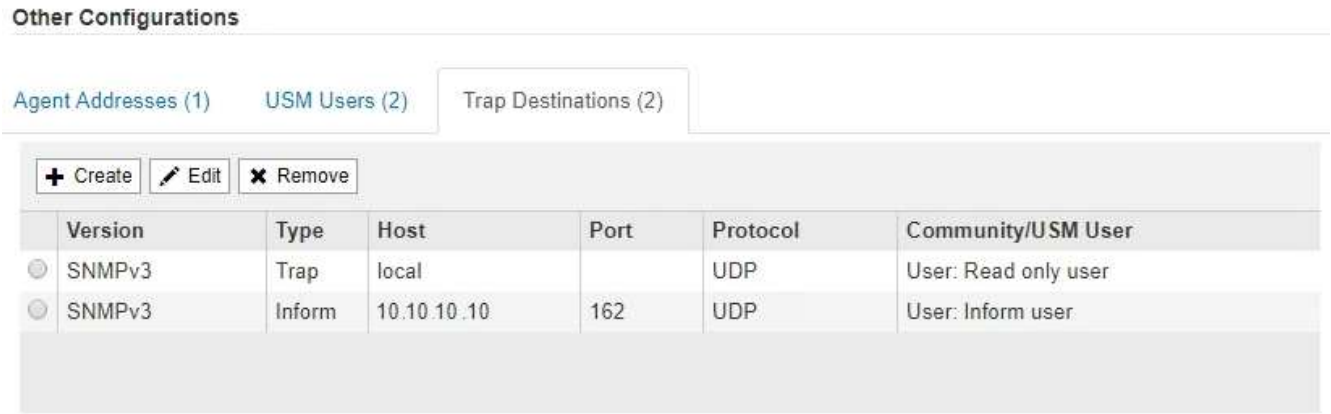
c. 선택한 버전에 따라 양식을 작성합니다

버전	이 정보를 지정하십시오
SNMPv1	• 참고: * SNMPv1의 경우 SNMP 에이전트는 트랩만 보낼 수 있습니다. 알림이 지원되지 않습니다. i. Host * 필드에 트랩을 수신할 IPv4 또는 IPv6 주소(또는 FQDN)를 입력합니다. ii. 포트*의 경우 다른 값을 사용해야 하는 경우가 아니면 기본값(162)을 사용합니다. (162는 SNMP 트랩의 표준 포트입니다.) iii. 프로토콜 * 의 경우 기본값(UDP)을 사용합니다. TCP도 지원됩니다. (UDP는 표준 SNMP 트랩 프로토콜입니다.) iv. SNMP 에이전트 페이지에 지정된 경우 기본 트랩 커뮤니티를 사용하거나 이 트랩 대상에 대한 사용자 지정 커뮤니티 문자열을 입력합니다. 사용자 지정 커뮤니티 문자열은 최대 32자이며 공백을 포함할 수 없습니다.

버전	이 정보를 지정하십시오
SNMPv2c입니다	i. 대상이 트랩에 사용되는지 아니면 정보를 제공할 것인지 선택합니다. ii. Host * 필드에 트랩을 수신할 IPv4 또는 IPv6 주소(또는 FQDN)를 입력합니다. iii. 포트*의 경우 다른 값을 사용해야 하는 경우가 아니면 기본값(162)을 사용합니다. (162는 SNMP 트랩의 표준 포트입니다.) iv. 프로토콜 * 의 경우 기본값(UDP)을 사용합니다. TCP도 지원됩니다. (UDP는 표준 SNMP 트랩 프로토콜입니다.) v. SNMP 에이전트 페이지에 지정된 경우 기본 트랩 커뮤니티를 사용하거나 이 트랩 대상에 대한 사용자 지정 커뮤니티 문자열을 입력합니다. 사용자 지정 커뮤니티 문자열은 최대 32자이며 공백을 포함할 수 없습니다.
SNMPv3	i. 대상이 트랩에 사용되는지 아니면 정보를 제공할 것인지 선택합니다. ii. Host * 필드에 트랩을 수신할 IPv4 또는 IPv6 주소(또는 FQDN)를 입력합니다. iii. 포트*의 경우 다른 값을 사용해야 하는 경우가 아니면 기본값(162)을 사용합니다. (162는 SNMP 트랩의 표준 포트입니다.) iv. 프로토콜 * 의 경우 기본값(UDP)을 사용합니다. TCP도 지원됩니다. (UDP는 표준 SNMP 트랩 프로토콜입니다.) v. 인증에 사용할 USM 사용자를 선택합니다. ◦ Trap * 을 선택하면 권한 있는 엔진 ID가 없는 USM 사용자만 표시됩니다. ◦ 알림 * 을 선택하면 권한 있는 엔진 ID가 있는 USM 사용자만 표시됩니다.

d. Create * 를 클릭합니다.

   트랩 대상이 생성되어 테이블에 추가됩니다.



11. SNMP 에이전트 구성을 완료하면 * Save * 를 클릭합니다

    새 SNMP 에이전트 구성이 활성화됩니다.

관련 정보

알림 메시지를 해제합니다

SNMP 에이전트를 업데이트합니다

SNMP 알림을 비활성화하거나 커뮤니티 문자열을 업데이트하거나 에이전트 주소, USM 사용자 및 트랩 대상을 추가 또는 제거할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 루트 액세스 권한이 있어야 합니다.

이 작업에 대해

를 업데이트할 때마다 SNMP 에이전트 구성각 탭에서 변경한 내용을 적용하려면 SNMP 에이전트 페이지 하단의 * Save * 를 클릭해야 합니다.

단계

1. 구성 * > * 모니터링 * > * SNMP 에이전트 * 를 선택합니다.

   SNMP Agent 페이지가 나타납니다.

2. 모든 그리드 노드에서 SNMP 에이전트를 비활성화하려면 * SNMP * 활성화 확인란의 선택을 취소하고 * 저장 * 을 클릭합니다.

   SNMP 에이전트는 모든 그리드 노드에 대해 비활성화됩니다. 나중에 에이전트를 다시 활성화하면 이전의 모든 SNMP 구성 설정이 유지됩니다.

3. 선택적으로 * 시스템 연락처 * 및 * 시스템 위치 * 에 대해 입력한 값을 업데이트합니다.
4. StorageGRID SNMP 에이전트가 트랩을 전송하고 알림을 보내지 않도록 하려면 선택적으로 * SNMP 에이전트 알림 사용 * 확인란을 선택 취소합니다.

   이 확인란의 선택을 취소하면 SNMP 에이전트는 읽기 전용 MIB 액세스를 지원하지만 SNMP 알림은 보내지

않습니다.

5. StorageGRID SNMP 에이전트가 부적절하게 인증된 프로토콜 메시지를 받을 때 더 이상 인증 트랩을 보내지 않도록 하려면 [인증 트랩 사용] * 확인란을 선택 취소합니다.
6. SNMPv1 또는 SNMPv2c를 사용하는 경우 선택적으로 커뮤니티 문자열 섹션을 업데이트합니다.

   이 섹션의 필드는 SNMPv1 또는 SNMPv2c에서 커뮤니티 기반 인증에 사용됩니다. 이 필드는 SNMPv3에는 적용되지 않습니다.

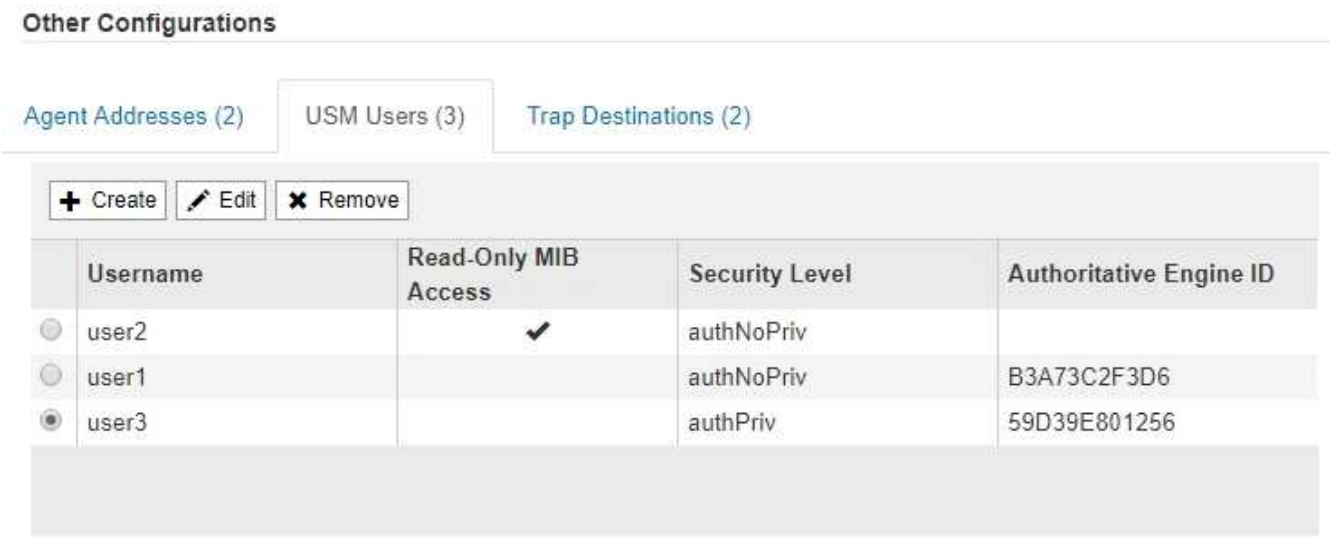
   > 기본 커뮤니티 문자열을 제거하려면 먼저 모든 트랩 대상에 사용자 지정 커뮤니티 문자열을 사용해야 합니다.

7. 상담원 주소를 업데이트하려면 기타 구성 섹션에서 상담원 주소 탭을 선택합니다.

   이 탭을 사용하여 하나 이상의 ""수신 주소""를 지정하십시오. SNMP 에이전트가 쿼리를 받을 수 있는 StorageGRID 주소입니다. 각 에이전트 주소에는 인터넷 프로토콜, 전송 프로토콜, StorageGRID 네트워크 및 포트가 포함됩니다.

   a. 상담원 주소를 추가하려면 * 생성 * 을 클릭합니다. 그런 다음 SNMP 에이전트 구성 지침에 있는 에이전트 주소 단계를 참조하십시오.
   b. 상담원 주소를 편집하려면 주소의 라디오 버튼을 선택하고 * 편집 * 을 클릭합니다. 그런 다음 SNMP 에이전트 구성 지침에 있는 에이전트 주소 단계를 참조하십시오.
   c. 상담원 주소를 제거하려면 주소의 라디오 버튼을 선택하고 * 제거 * 를 클릭합니다. 그런 다음 * 확인 * 을 클릭하여 이 주소를 제거할 것인지 확인합니다.
   d. 변경 사항을 커밋하려면 SNMP 에이전트 페이지 맨 아래에 있는 * Save * 를 클릭합니다.

8. USM 사용자를 업데이트하려면 기타 구성 섹션에서 USM 사용자 탭을 선택합니다.



이 탭을 사용하여 MIB를 쿼리하거나 트랩 및 알림을 받을 권한이 있는 USM 사용자를 정의합니다.

a. USM 사용자를 추가하려면 * Create * 를 클릭합니다. 그런 다음 SNMP 에이전트를 구성하는 지침은 USM 사용자에 대한 단계를 참조하십시오.

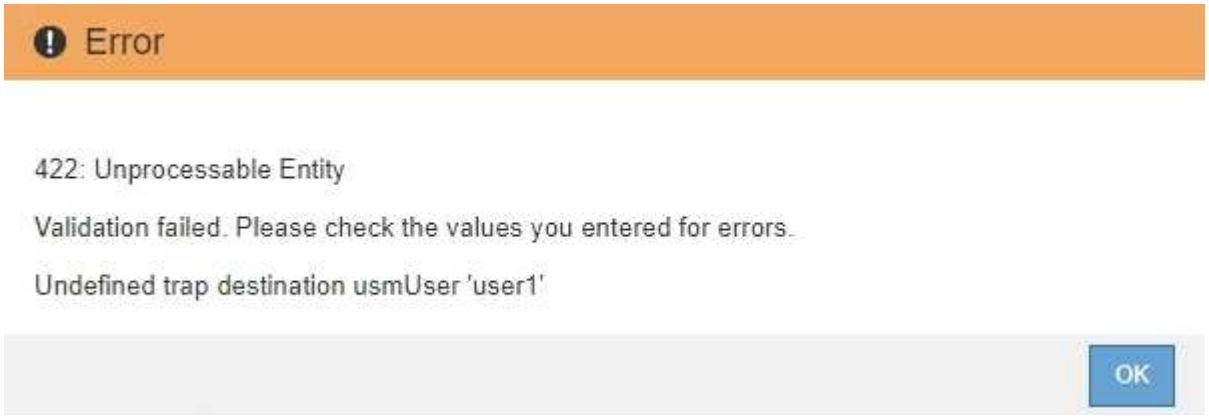
b. USM 사용자를 편집하려면 해당 사용자의 라디오 버튼을 선택하고 * Edit * 를 클릭합니다. 그런 다음 SNMP 에이전트를 구성하는 지침은 USM 사용자에 대한 단계를 참조하십시오.

   기존 USM 사용자의 사용자 이름은 변경할 수 없습니다. 사용자 이름을 변경해야 하는 경우 사용자를 제거하고 새 사용자 이름을 만들어야 합니다.

   > 사용자의 신뢰할 수 있는 엔진 ID를 추가 또는 제거하고 해당 사용자가 현재 대상에 대해 선택된 경우 단계에 설명된 대로 대상을 편집하거나 제거해야 합니다 SNMP 트랩 대상입니다. 그렇지 않으면 SNMP 에이전트 구성을 저장할 때 유효성 검사 오류가 발생합니다.

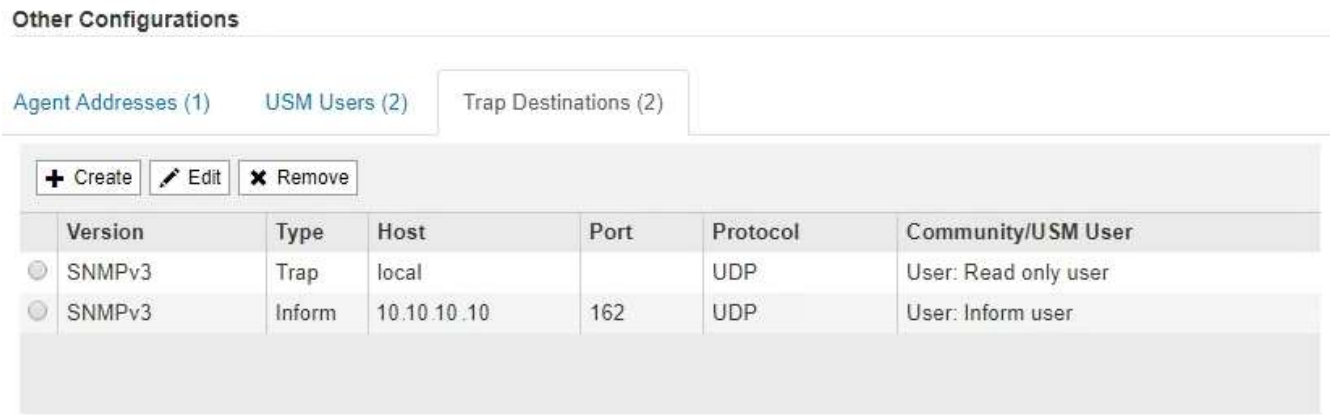
c. USM 사용자를 제거하려면 해당 사용자의 라디오 버튼을 선택하고 * Remove * 를 클릭합니다. 그런 다음 * 확인 * 을 클릭하여 이 사용자를 제거할 것인지 확인합니다.

   > 제거한 사용자가 현재 트랩 대상에 대해 선택된 경우 단계에 설명된 대로 대상을 편집하거나 제거해야 합니다 SNMP 트랩 대상입니다. 그렇지 않으면 SNMP 에이전트 구성을 저장할 때 유효성 검사 오류가 발생합니다.



a. 변경 사항을 커밋하려면 SNMP 에이전트 페이지 맨 아래에 있는 * Save * 를 클릭합니다.

9. 트랩 대상을 업데이트하려면 기타 구성 섹션에서 트랩 대상 탭을 선택합니다.



트랩 대상 탭에서는 StorageGRID 트랩 또는 알림 알림에 대한 하나 이상의 대상을 정의할 수 있습니다. SNMP 에이전트를 활성화하고 * 저장 * 을 클릭하면 StorageGRID가 정의된 각 대상으로 알림을 보내기 시작합니다. 알림 및 알람이 트리거되면 알림이 전송됩니다. 지원되는 MIB-II 엔티티에 대해서도 표준 알림이 전송됩니다(예: ifdown 및 coldstart).

a. 트랩 대상을 추가하려면 * Create * 를 클릭합니다. 그런 다음 SNMP 에이전트 구성 지침에 있는 트랩 대상 단계를 참조하십시오.

b. 트랩 대상을 편집하려면 사용자의 라디오 버튼을 선택하고 * Edit * 를 클릭합니다. 그런 다음 SNMP 에이전트 구성 지침에 있는 트랩 대상 단계를 참조하십시오.

c. 트랩 대상을 제거하려면 대상의 라디오 단추를 선택하고 * 제거 * 를 클릭합니다. 그런 다음 * 확인 * 을 클릭하여 이 대상을 제거할 것인지 확인합니다.

d. 변경 사항을 커밋하려면 SNMP 에이전트 페이지 맨 아래에 있는 * Save * 를 클릭합니다.

10. SNMP 에이전트 구성을 업데이트했으면 * Save * 를 클릭합니다.

저작권 정보

Copyright © 2024 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 라이센스와 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 라이센스도 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 라이센스를 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 라이센스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

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