Keystone 설정 및 구성

Keystone

NetApp
February 19, 2026

목차

Keystone 설정 및 구성 1
- 요구 사항 1
  - Keystone Collector의 가상 인프라 요구 사항 1
  - Keystone Collector의 Linux 요구 사항 2
  - Keystone 의 ONTAP 및 StorageGRID 요구 사항 5
- Keystone Collector를 설치합니다 8
  - VMware vSphere 시스템에 Keystone Collector 구축 8
  - Linux 시스템에 Keystone Collector를 설치합니다 10
  - Keystone 소프트웨어 자동 검증 12
- Keystone Collector 구성 12
  - Keystone 수집기에서 HTTP 프록시를 구성합니다 14
  - 개인 데이터의 수집 제한 14
  - 사용자 지정 루트 CA를 신뢰합니다 15
  - 성능 서비스 수준 생성 16
- ITOM Collector를 설치합니다 20
  - Keystone ITOM Collector 설치 요구 사항 21
  - Linux 시스템에 Keystone ITOM Collector를 설치하세요 22
  - Windows 시스템에 Keystone ITOM Collector를 설치하세요. 23
- Keystone용 AutoSupport를 구성합니다 24
- 모니터링 및 업그레이드 25
  - Keystone Collector의 상태를 모니터링합니다 25
  - Keystone Collector를 수동으로 업그레이드합니다 30
- Keystone Collector 보안 32
  - 보안 강화 32
- Keystone이 수집하는 사용자 데이터의 유형 33
  - ONTAP 데이터 수집 33
  - StorageGRID 데이터 수집 41
  - 원격 측정 데이터 수집 41
- 비공개 모드의 Keystone 43
  - Keystone에 대해 자세히 알아보기(프라이빗 모드) 43
  - Keystone Collector 비공개 모드 설치를 준비하세요 44
  - Keystone Collector를 비공개 모드로 설치합니다 46
  - Keystone Collector를 비공개 모드로 구성합니다 46
  - 개인 모드에서 Keystone Collector 상태를 모니터링합니다 51

Keystone 설정 및 구성

요구 사항

Keystone Collector의 가상 인프라 요구 사항

Keystone Collector를 설치하려면 VMware vSphere 시스템이 여러 가지 요구 사항을 충족해야 합니다.

Keystone Collector 서버 **VM**의 사전 요구 사항**:**

- 운영 체제: VMware vCentre 서버 및 ESXi 8.0 이상
- 코어: 1 CPU
- RAM: 2GB RAM
- 디스크 공간: 20GB vDisk

기타 요구 사항

다음과 같은 일반 요구 사항이 충족되는지 확인합니다.

네트워킹 요구 사항

Keystone 수집기의 네트워킹 요구사항은 다음 표에 나와 있습니다.

Keystone 수집기는 인터넷 연결이 필요합니다. 기본 게이트웨이(NAT를 통해) 또는 HTTP 프록시를 통해 직접 라우팅하여 인터넷 연결을 제공할 수 있습니다. 두 가지 변형 모델이 모두 여기에 설명되어 있습니다.

출처	목적지	서비스	프로토콜 및 포트	범주	목적
Keystone Collector(Keystone ONTAP용)	Active IQ Unified Manager(유니파이드 매니저)	HTTPS	TCP 443	필수(Keystone ONTAP를 사용하는 경우)	ONTAP에 대한 Keystone Collector 사용 메트릭 수집
Keystone Collector(Keystone StorageGRID용)	StorageGRID 관리 노드	HTTPS	TCP 443	필수(Keystone StorageGRID를 사용하는 경우)	StorageGRID에 대한 Keystone Collector 사용 메트릭 수집
Keystone Collector(일반)	인터넷(나중에 제공된 URL 요구 사항에 따라)	HTTPS	TCP 443	필수(인터넷 연결)	Keystone Collector 소프트웨어, OS 업데이트 및 메트릭 업로드

Keystone Collector(일반)	고객 HTTP 프록시	HTTP 프록시	고객 프록시 포트	필수(인터넷 연결)	Keystone Collector 소프트웨어, OS 업데이트 및 메트릭 업로드
Keystone Collector(일반)	고객 DNS 서버	DNS	TCP/UDP 53	필수입니다	DNS 확인
Keystone Collector(일반)	고객 NTP 서버	NTP	UDP 123입니다	필수입니다	시간 동기화
Keystone Collector(Keystone ONTAP용)	Unified Manager를 참조하십시오	MySQL	TCP 3306	옵션 기능	Keystone 수집기에 대한 성능 메트릭 컬렉션
Keystone Collector(일반)	고객 모니터링 시스템	HTTPS	TCP 7777	옵션 기능	Keystone Collector 상태 보고
고객의 운영 워크스테이션	Keystone 컬렉터	SSH를 클릭합니다	TCP 22	관리	Keystone Collector 관리 액세스
NetApp ONTAP 클러스터 및 노드 관리 주소	Keystone 컬렉터	HTTP_8000, ping	TCP 8000, ICMP Echo Request/Reply	옵션 기능	ONTAP 펌웨어 업데이트를 위한 웹 서버입니다

MySQL의 기본 포트인 3306은 Unified Manager를 새로 설치할 때 로컬 호스트로만 제한되므로 Keystone Collector에 대한 성능 메트릭을 수집하지 못합니다. 자세한 내용은 을 "ONTAP 요구 사항 "참조하십시오.

URL 액세스

Keystone 수집기는 다음 인터넷 호스트에 액세스해야 합니다.

주소	이유
https://keystone.netapp.com	Keystone Collector 소프트웨어 업데이트 및 사용 보고
https://support.netapp.com	청구 정보 및 AutoSupport 제공을 위한 NetApp HQ

Keystone Collector의 Linux 요구 사항

필요한 소프트웨어로 Linux 시스템을 준비하면 Keystone Collector를 통해 정확한 설치 및 데이터 수집이 가능합니다.

Linux 및 Keystone Collector 서버 VM에 이러한 구성이 있는지 확인합니다.

Linux 서버**:**

- 운영 체제: 다음 중 하나:
  - 데비안 12
  - Red Hat Enterprise Linux 8.6 이상 8.x 버전
  - Red Hat Enterprise Linux 9.0 이상 버전
  - CentOS 7(기존 환경 전용)
- 약어 시간 동기화됨
- 표준 Linux 소프트웨어 저장소에 대한 액세스

동일한 서버에 다음과 같은 타사 패키지도 있어야 합니다.

- 포드만(POD 매니저)
- SOS(SOS
- 연대기
- 파이썬 3(3.9.14~3.11.8)

Keystone Collector 서버 **VM:**

- 코어: CPU 2개
- RAM: 4GB RAM
- 디스크 공간: 50GB vDisk

기타 요구 사항

다음과 같은 일반 요구 사항이 충족되는지 확인합니다.

네트워킹 요구 사항

Keystone 수집기의 네트워킹 요구사항은 다음 표에 나와 있습니다.

Keystone 수집기는 인터넷 연결이 필요합니다. 기본 게이트웨이(NAT를 통해) 또는 HTTP 프록시를 통해 직접 라우팅하여 인터넷 연결을 제공할 수 있습니다. 두 가지 변형 모델이 모두 여기에 설명되어 있습니다.

출처	목적지	서비스	프로토콜 및 포트	범주	목적
Keystone Collector(Keystone ONTAP용)	Active IQ Unified Manager(유니파이드 매니저)	HTTPS	TCP 443	필수(Keystone ONTAP를 사용하는 경우)	ONTAP에 대한 Keystone Collector 사용 메트릭 수집

Keystone Collector(Keystone StorageGRID용)	StorageGRID 관리 노드	HTTPS	TCP 443	필수(Keystone StorageGRID를 사용하는 경우)	StorageGRID에 대한 Keystone Collector 사용 메트릭 수집
Keystone Collector(일반)	인터넷(나중에 제공된 URL 요구 사항에 따라)	HTTPS	TCP 443	필수(인터넷 연결)	Keystone Collector 소프트웨어, OS 업데이트 및 메트릭 업로드
Keystone Collector(일반)	고객 HTTP 프록시	HTTP 프록시	고객 프록시 포트	필수(인터넷 연결)	Keystone Collector 소프트웨어, OS 업데이트 및 메트릭 업로드
Keystone Collector(일반)	고객 DNS 서버	DNS	TCP/UDP 53	필수입니다	DNS 확인
Keystone Collector(일반)	고객 NTP 서버	NTP	UDP 123입니다	필수입니다	시간 동기화
Keystone Collector(Keystone ONTAP용)	Unified Manager를 참조하십시오	MySQL	TCP 3306	옵션 기능	Keystone 수집기에 대한 성능 메트릭 컬렉션
Keystone Collector(일반)	고객 모니터링 시스템	HTTPS	TCP 7777	옵션 기능	Keystone Collector 상태 보고
고객의 운영 워크스테이션	Keystone 컬렉터	SSH를 클릭합니다	TCP 22	관리	Keystone Collector 관리 액세스
NetApp ONTAP 클러스터 및 노드 관리 주소	Keystone 컬렉터	HTTP_8000, ping	TCP 8000, ICMP Echo Request/Reply	옵션 기능	ONTAP 펌웨어 업데이트를 위한 웹 서버입니다

MySQL의 기본 포트인 3306은 Unified Manager를 새로 설치할 때 로컬 호스트로만 제한되므로 Keystone Collector에 대한 성능 메트릭을 수집하지 못합니다. 자세한 내용은 을 "ONTAP 요구 사항 "참조하십시오.

URL 액세스

Keystone 수집기는 다음 인터넷 호스트에 액세스해야 합니다.

주소	이유

https://keystone.netapp.com	Keystone Collector 소프트웨어 업데이트 및 사용 보고
https://support.netapp.com	청구 정보 및 AutoSupport 제공을 위한 NetApp HQ

Keystone 의 ONTAP 및 StorageGRID 요구 사항

Keystone을 시작하기 전에 ONTAP 클러스터 및 StorageGRID 시스템이 몇 가지 요구사항을 충족하는지 확인해야 합니다.

ONTAP

소프트웨어 버전

1. ONTAP 9.8 이상
2. Active IQ Unified Manager(Unified Manager) 9.10 이상

시작하기 전에

ONTAP를 통해서만 사용 데이터를 수집하려는 경우 다음 요구 사항을 충족해야 합니다.

1. ONTAP 9.8 이상이 구성되어 있는지 확인합니다. 새 클러스터를 구성하는 방법에 대한 자세한 내용은 다음 링크를 참조하십시오.
   - "System Manager를 사용하여 새 클러스터에서 ONTAP를 구성합니다"
   - "CLI를 사용하여 클러스터 설정"
2. 특정 역할을 사용하여 ONTAP 로그인 계정을 생성합니다. 자세한 내용은 을 "ONTAP 로그인 계정 생성에 대해 자세히 알아봅니다"참조하십시오.
   - 웹 UI *
     i. 기본 자격 증명을 사용하여 ONTAP System Manager에 로그인합니다. 자세한 내용은 을 "System Manager를 이용한 클러스터 관리"참조하십시오.
     ii. "readonly" 역할과 "http" 애플리케이션 유형으로 ONTAP 사용자를 생성하고 * 클러스터 > 설정 > 보안 > 사용자 * 로 이동하여 암호 인증을 사용하도록 설정합니다.
   - * CLI *
     i. 기본 자격 증명을 사용하여 ONTAP CLI에 로그인합니다. 자세한 내용은 을 "CLI를 사용한 클러스터 관리"참조하십시오.
     ii. "readonly" 역할과 "http" 응용 프로그램 유형으로 ONTAP 사용자를 생성하고 암호 인증을 활성화합니다. 인증에 대한 자세한 내용은 을 "ONTAP 계정 암호 액세스를 활성화합니다 "참조하십시오.

Active IQ Unified Manager를 통해 사용 데이터를 수집하려는 경우 다음 요구 사항을 충족해야 합니다.

1. Unified Manager 9.10 이상이 구성되어 있는지 확인합니다. Unified Manager 설치에 대한 자세한 내용은 다음 링크를 참조하십시오.
   - "VMware vSphere 시스템에 Unified Manager 설치"
   - "Linux 시스템에 Unified Manager 설치"
2. ONTAP 클러스터가 Unified Manager에 추가되었는지 확인합니다. 클러스터 추가에 대한 자세한 내용은 을 참조하십시오 "클러스터 추가".
3. 사용량 및 성능 데이터 수집에 대한 특정 역할을 가진 Unified Manager 사용자를 생성합니다. 다음 단계를 수행합니다. 사용자 역할에 대한 자세한 내용은 을 참조하십시오 "사용자 역할의 정의".
   a. 설치 중에 생성되는 기본 애플리케이션 관리자 사용자 자격 증명을 사용하여 Unified Manager 웹 UI에 로그인합니다. 을 참조하십시오 "Unified Manager 웹 UI에 액세스".
   b. 을 사용하여 Keystone 수집기에 대한 서비스 계정을 생성합니다 `Operator` 사용자 역할. Keystone Collector 서비스 API는 이 서비스 계정을 사용하여 Unified Manager와 통신하고 사용 데이터를 수집합니다. 을 참조하십시오 "사용자 추가".
   c. 을 생성합니다 `Database` 사용자 계정, 및 `Report Schema` 역할. 이 사용자는 성능 데이터 수집에

필요합니다. 을 참조하십시오 "데이터베이스 사용자 생성".

> MySQL의 기본 포트인 3306은 Unified Manager를 새로 설치할 때 로컬 호스트로만 제한되므로 Keystone ONTAP에 대한 성능 데이터가 수집되지 않습니다. 이 구성을 수정할 수 있으며 Unified Manager 유지보수 콘솔의 옵션을 사용하여 다른 호스트에서 연결을 사용할 수 있습니다 `Control access to MySQL port 3306`. 자세한 내용은 을 "추가 메뉴 옵션"참조하십시오.

4. Unified Manager에서 API 게이트웨이를 사용하도록 설정합니다. Keystone Collector는 API 게이트웨이 기능을 사용하여 ONTAP 클러스터와 통신합니다. 웹 UI에서 또는 Unified Manager CLI를 통해 몇 가지 명령을 실행하여 API 게이트웨이를 사용하도록 설정할 수 있습니다.

   웹 **UI**

   Unified Manager 웹 UI에서 API 게이트웨이를 사용하도록 설정하려면 Unified Manager 웹 UI에 로그인하여 API 게이트웨이를 사용하도록 설정합니다. 자세한 내용은 을 참조하십시오 "API 게이트웨이 활성화 중".

   CLI를 참조하십시오

   Unified Manager CLI를 통해 API 게이트웨이를 설정하려면 다음 단계를 수행하십시오.

   a. Unified Manager 서버에서 SSH 세션을 시작하고 Unified Manager CLI에 로그인합니다. `um cli login -u <*umadmin*>`CLI 명령에 대한 자세한 내용은 를 참조하십시오 "지원되는 Unified Manager CLI 명령".

   b. API 게이트웨이가 이미 설정되어 있는지 확인합니다. `um option list api.gateway.enabled`A `true` 값은 API 게이트웨이가 활성화되었음을 나타냅니다.

   c. 반환되는 값이 인 경우 `false`에서 다음 명령을 실행합니다. `um option set api.gateway.enabled=true`

   d. Unified Manager 서버를 다시 시작합니다.

      - Linux: "Unified Manager를 다시 시작하는 중입니다".
      - VMware vSphere: "Unified Manager 가상 머신을 재시작합니다".

StorageGRID

StorageGRID에 Keystone Collector를 설치하려면 다음 구성이 필요합니다.

- StorageGRID `11.6.0` 이상 버전이 설치되어 있어야 합니다. StorageGRID 업그레이드에 대한 자세한 내용은 을 참조하십시오 "StorageGRID 소프트웨어 업그레이드: 개요".
- 사용량 데이터 수집을 위해 StorageGRID 로컬 관리자 사용자 계정을 생성해야 합니다. 이 서비스 계정은 Keystone Collector 서비스가 관리자 노드 API를 통해 StorageGRID와 통신하는 데 사용됩니다.

  단계

  a. Grid Manager에 로그인합니다. 을 참조하십시오 "Grid Manager에 로그인합니다".

  b. 를 사용하여 로컬 관리 그룹을 생성합니다 `Access mode: Read-only`. 을 참조하십시오 "관리자 그룹을 생성합니다".

  c. 다음 권한을 추가합니다.

     - 테넌트 계정
     - 유지 관리

- 메트릭 쿼리

d. Keystone 서비스 계정 사용자를 생성하고 이를 관리 그룹에 연결합니다. 을 참조하십시오 "사용자 관리".

Keystone Collector를 설치합니다

VMware vSphere 시스템에 Keystone Collector 구축

VMware vSphere 시스템에 Keystone Collector를 구축하려면 OVA 템플릿 다운로드, * Deploy OVF Template * 마법사를 사용하여 템플릿 구축, 인증서 무결성 확인, VM 준비 상태 확인이 포함됩니다.

OVA 템플릿 배포

다음 단계를 수행하십시오.

단계

1. 에서 OVA 파일을 다운로드합니다 "이 링크" VMware vSphere 시스템에 저장합니다.
2. VMware vSphere 시스템에서 * VMS and Templates * 보기로 이동합니다.
3. 가상 머신(VM) 또는 데이터 센터에 필요한 폴더를 마우스 오른쪽 버튼으로 클릭하고 * Deploy OVF Template * 을 선택합니다.
4. Deploy OVF Template * 마법사의_Step 1_에서 * Select 및 OVF template * 을 클릭하여 다운로드한 파일을 선택합니다 `KeystoneCollector-latest.ova` 파일.
5. 2단계_에서 VM 이름을 지정하고 VM 폴더를 선택합니다.
6. 3단계_에서 VM을 실행하는 데 필요한 컴퓨팅 리소스를 지정합니다.
7. 4단계: 세부 정보 검토_에서 OVA 파일의 정확성과 진위성을 확인하세요.

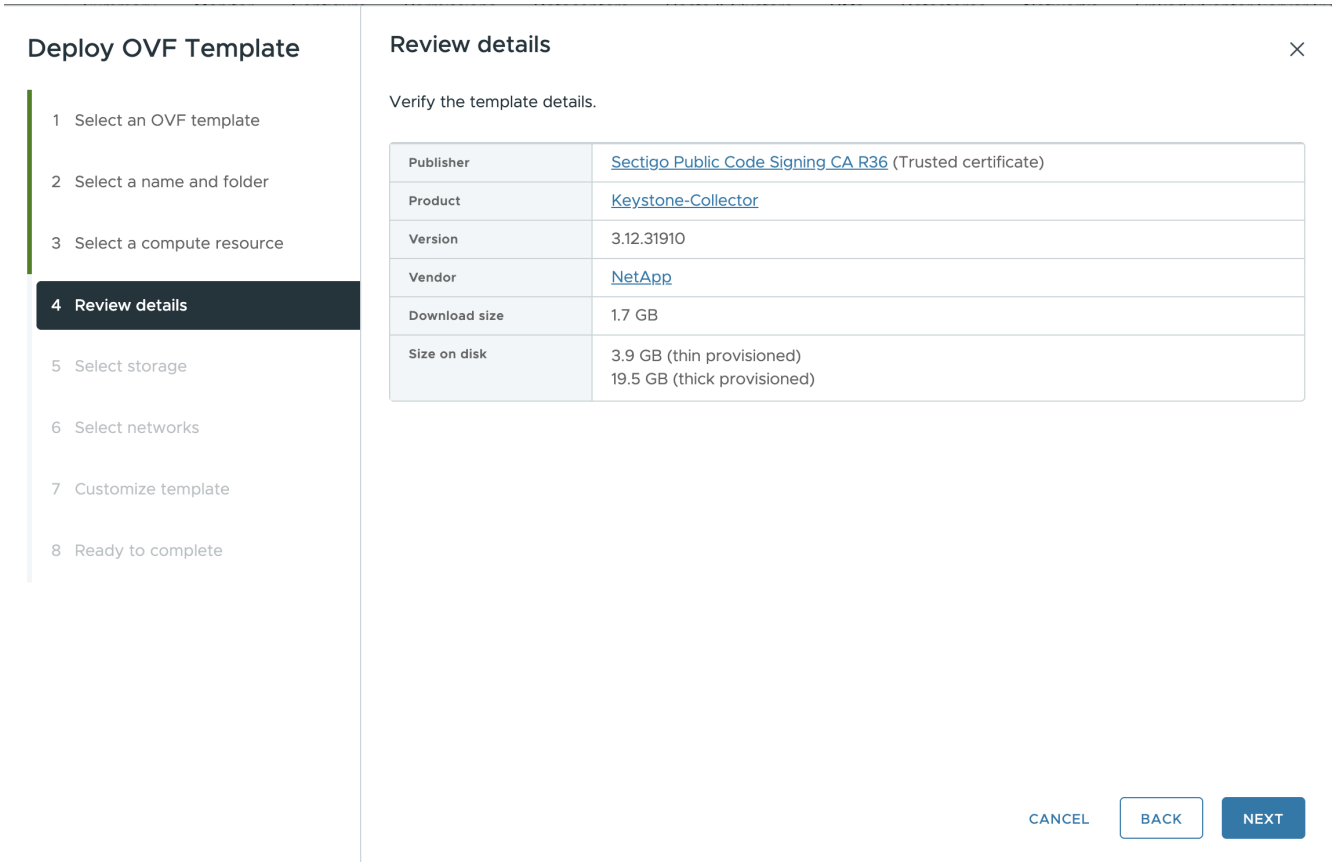
   vCenter 루트 신뢰 저장소에는 VMware 인증서만 포함되어 있습니다. NetApp 인증 기관으로 Entrust를 사용하며, 해당 인증서는 vCenter 신뢰 저장소에 추가되어야 합니다.

   a. Sectigo에서 코드 서명 CA 인증서를 다운로드하세요 "여기".

   b. 의 단계를 따릅니다 `Resolution` 이 기술 자료(KB) 문서의 섹션: https://kb.vmware.com/s/article/84240.

   > vCenter 버전 7.x 및 이전 버전의 경우 vCenter 및 ESXi를 버전 8.0 이상으로 업데이트해야 합니다. 이전 버전은 더 이상 지원되지 않습니다.

   Keystone Collector OVA의 무결성과 진위성이 검증되면 텍스트를 볼 수 있습니다. `(Trusted certificate)` 출판사와 함께.



8. Deploy OVF Template * 마법사의_5단계에서 VM 저장 위치를 지정합니다.
9. 6단계_에서 VM이 사용할 대상 네트워크를 선택합니다.
10. 7단계 사용자 정의 템플릿 _ 에서 admin 사용자 계정의 초기 네트워크 주소와 암호를 지정합니다.

> 관리자 암호는 vCenter에서 가역적인 형식으로 저장되며 VMware vSphere 시스템에 대한 초기 액세스 권한을 얻기 위해 부트스트랩 자격 증명으로 사용해야 합니다. 초기 소프트웨어 구성 중에 이 관리자 암호를 변경해야 합니다. IPv4 주소의 서브넷 마스크는 CIDR 표기법으로 제공되어야 합니다. 예를 들어 서브넷 마스크 255.255.255.0에 대해 24의 값을 사용합니다.

11. 8단계 * Deploy OVF Template * 마법사의 _ 완료 준비 단계에서 구성을 검토하고 OVA 배포에 대한 매개 변수를 올바르게 설정했는지 확인합니다.

VM을 템플릿에서 구축하고 전원을 켠 후 VM에 대한 SSH 세션을 열고 임시 관리자 자격 증명으로 로그인하여 VM이 구성 준비가 되었는지 확인합니다.

초기 시스템 구성

OVA를 통해 구축된 Keystone Collector 서버의 초기 구성을 위해 VMware vSphere 시스템에서 다음 단계를 수행합니다.

> 배포를 완료하면 Keystone Collector 관리 TUI(터미널 사용자 인터페이스) 유틸리티를 사용하여 구성 및 모니터링 작업을 수행할 수 있습니다. Enter 및 화살표 키와 같은 다양한 키보드 컨트롤을 사용하여 옵션을 선택하고 이 TUI를 탐색할 수 있습니다.

1. Keystone Collector 서버에 대한 SSH 세션을 엽니다. 연결할 때 admin 암호를 업데이트하라는 메시지가

표시됩니다. 필요에 따라 관리자 암호 업데이트를 완료합니다.

2. TUI에 액세스하려면 새 암호를 사용하여 로그인하십시오. 로그인 시 TUI가 나타납니다.

   또는 을 실행하여 수동으로 시작할 수도 있습니다 `keystone-collector-tui` CLI 명령:

3. 필요한 경우 TUI의 * 구성 > 네트워크 섹션 * 에서 프록시 세부 정보를 구성합니다.
4. Configuration > System * 섹션에서 시스템 호스트 이름, 위치 및 NTP 서버를 구성합니다.
5. 유지 관리 > Collector 업데이트 * 옵션을 사용하여 Keystone Collector를 업데이트합니다. 업데이트 후 Keystone Collector 관리 TUI 유틸리티를 다시 시작하여 변경 사항을 적용합니다.

Linux 시스템에 Keystone Collector를 설치합니다

RPM 또는 데비안 패키지를 사용하여 Linux 서버에 Keystone Collector 소프트웨어를 설치할 수 있습니다. Linux 배포에 따라 설치 단계를 따릅니다.

RPM 사용

1. Keystone Collector 서버로 SSH를 수행하고 로 승격합니다 `root` 권한.
2. Keystone 공개 서명을 가져옵니다.
   `# rpm --import https://keystone.netapp.com/repo1/RPM-GPG-NetApp-Keystone-20251020`
3. RPM 데이터베이스에서 Keystone Billing Platform의 지문을 확인하여 올바른 공개 인증서가 가져왔는지 확인하세요.
   `# rpm -qa gpg-pubkey --qf '%{Description}'|gpg --show-keys --fingerprint`
   올바른 지문은 다음과 같습니다.
   `9297 0DB6 0867 22E7 7646 E400 4493 5CBB C9E9 FEDC`
4. 다운로드 `keystonerepo.rpm` 파일:
   `curl -O https://keystone.netapp.com/repo1/keystonerepo.rpm`
5. 파일의 진위 여부를 확인하세요.
   `rpm --checksig -v keystonerepo.rpm` 진짜 파일의 서명은 다음과 같습니다.
   `Header V4 RSA/SHA512 Signature, key ID c9e9fedc: OK`
6. YUM 소프트웨어 저장소 파일을 설치합니다.
   `# yum install keystonerepo.rpm`
7. Keystone repo가 설치되면 YUM 패키지 관리자를 통해 Keystone-Collector 패키지를 설치합니다.

   `# yum install keystone-collector`

   Red Hat Enterprise Linux 9의 경우 다음 명령을 실행하여 keystone-collector 패키지를 설치합니다.
   `# yum install keystone-collector-rhel9`

데비안 사용하기

1. Keystone Collector 서버에 SSH로 연결하고 권한을
   `sudo su` 상승합니다. `root`
2. `keystone-sw-repo.deb`다음 파일을 다운로드합니다.
   `curl -O https://keystone.netapp.com/downloads/keystone-sw-repo.deb`
3. Keystone 소프트웨어 저장소 파일을 설치합니다.
   `# dpkg -i keystone-sw-repo.deb`
4. 패키지 목록 업데이트:
   `# apt-get update`
5. Keystone 리포지토리가 설치되면 키스톤-수집기 패키지를 설치합니다.
   `# apt-get install keystone-collector`

설치를 완료하면 Keystone Collector 관리 터미널 사용자 인터페이스(TUI) 유틸리티를 사용하여 구성 및 모니터링 작업을 수행할 수 있습니다. Enter 및 화살표 키와 같은 다양한 키보드 컨트롤을 사용하여 옵션을 선택하고 이 TUI를 탐색할 수 있습니다. 을 참조하십시오 "Keystone Collector 구성" 및 "시스템 상태를 모니터링합니다" 를 참조하십시오.

Keystone 소프트웨어 자동 검증

Keystone 저장소는 Keystone 소프트웨어의 무결성을 자동으로 확인하여 유효하고 인증된 소프트웨어만 사이트에 설치하도록 구성됩니다.

에 제공된 Keystone YUM 리포지토리 클라이언트 구성은 `keystonerepo.rpm` 이 리포지토리를 통해 다운로드된 모든 소프트웨어에서 강제 GPG 검사를 (`gpgcheck=1`사용합니다. Keystone 리포지토리를 통해 다운로드된 RPM이 서명 확인에 실패하면 해당 RPM을 설치할 수 없습니다. 이 기능은 Keystone Collector의 예약된 자동 업데이트 기능에서 사용되어 유효하고 인증된 소프트웨어만 사이트에 설치됩니다.

Keystone Collector 구성

스토리지 환경에서 Keystone 수집기가 사용 데이터를 수집할 수 있도록 몇 가지 구성 작업을 완료해야 합니다. 필수 구성 요소를 활성화하고 스토리지 환경을 연결하는 일회성 활동입니다.

- Keystone Collector는 구성 및 모니터링 작업을 수행할 수 있는 Keystone Collector Management Terminal User Interface(TUI) 유틸리티를 제공합니다. Enter 및 화살표 키와 같은 다양한 키보드 컨트롤을 사용하여 옵션을 선택하고 이 TUI를 탐색할 수 있습니다.
- Keystone Collector는 인터넷에 액세스할 수 없는 조직(_Dark site_또는_private mode_라고도 함)에 대해 구성할 수 있습니다. 에 대한 자세한 내용은 을 "비공개 모드의 Keystone"참조하십시오.

단계

1. Keystone Collector 관리 TUI 유틸리티 시작:
   ```
   $ keystone-collector-tui
   ```
2. [구성] > [KS-Collector]로 이동하여 Keystone Collector 구성 화면을 열고 사용 가능한 업데이트 옵션을 확인합니다.
3. 필요한 옵션을 업데이트합니다.

   **ONTAP 용 **

   - * ONTAP 사용량 수집 *: 이 옵션을 사용하면 ONTAP에 대한 사용 데이터를 수집할 수 있습니다. Active IQ Unified Manager(Unified Manager) 서버 및 서비스 계정의 세부 정보를 추가합니다.
   - * ONTAP 성능 데이터 수집 *: 이 옵션을 사용하면 ONTAP에 대한 성능 데이터를 수집할 수 있습니다. 이 기능은 기본적으로 비활성화되어 있습니다. SLA를 위해 사용자 환경에서 성능 모니터링이 필요한 경우 이 옵션을 활성화하십시오. Unified Manager 데이터베이스 사용자 계정 세부 정보를 제공합니다. 데이터베이스 사용자를 만드는 방법에 대한 자세한 내용은 을 참조하십시오 "Unified Manager 사용자 생성".
   - * 개인 데이터 제거 *: 이 옵션은 고객의 특정 개인 데이터를 제거하며 기본적으로 활성화됩니다. 이 옵션이 활성화된 경우 메트릭에서 제외되는 데이터에 대한 자세한 내용은 을 참조하십시오 "개인 데이터의 수집 제한".

**StorageGRID 용 **

- * Collect StorageGRID usage *: 이 옵션을 사용하면 노드 사용 세부 정보를 수집할 수 있습니다. StorageGRID 노드 주소 및 사용자 세부 정보를 추가합니다.
- * 개인 데이터 제거 *: 이 옵션은 고객의 특정 개인 데이터를 제거하며 기본적으로 활성화됩니다. 이 옵션이 활성화된 경우 메트릭에서 제외되는 데이터에 대한 자세한 내용은 을 참조하십시오 "개인 데이터의 수집 제한".

4. 시작 **KS-Collector with System** 필드를 토글합니다.
5. 저장을 클릭합니다
.

6. TUI의 기본 화면으로 돌아가 서비스 상태 정보를 확인하여 Keystone 수집기가 정상 상태인지 확인합니다. 시스템은 서비스가 전체적: 정상 상태에 있음을 나타내야 합니다

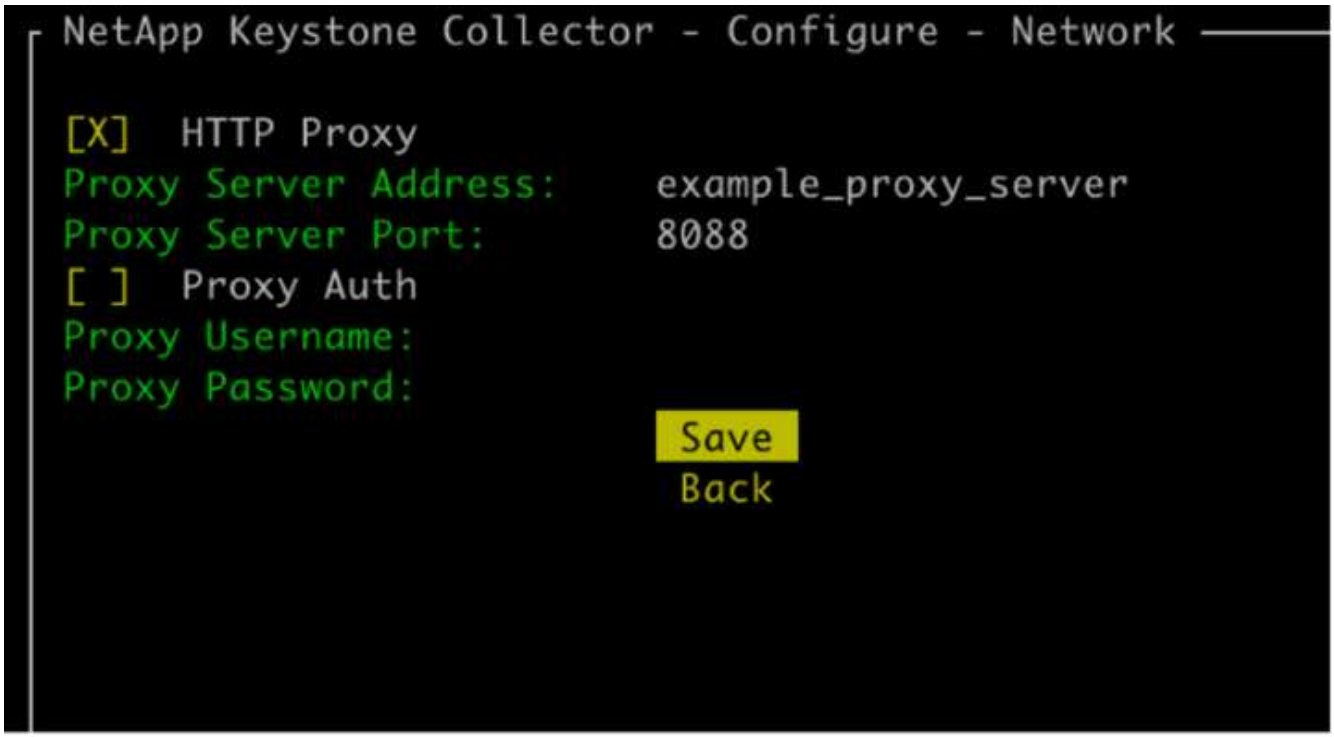
7. 기본 화면에서 **Shell**으로 종료 옵션을 선택하여 Keystone Collector 관리 TUI를 종료합니다.

Keystone 수집기에서 HTTP 프록시를 구성합니다

Collector 소프트웨어는 HTTP 프록시를 사용하여 인터넷과 통신할 수 있도록 지원합니다. TUI에서 구성할 수 있습니다.

단계

1. 이미 종료된 경우 Keystone Collector 관리 TUI 유틸리티를 다시 시작합니다.
   ```
   $ keystone-collector-tui
   ```
2. 인증이 필요한 경우 **HTTP** 프록시 필드를 토글하고 HTTP 프록시 서버, 포트 및 자격 증명의 세부 정보를 추가합니다.
3. 저장을 클릭합니다
   .



개인 데이터의 수집 제한

Keystone Collector는 구독 측정을 수행하는 데 필요한 제한된 구성, 상태 및 성능 정보를 수집합니다. 업로드한 콘텐츠에서 중요한 정보를 마스킹하여 수집된 정보를 추가로 제한할 수 있는 옵션이 있습니다. 이는 청구 계산에 영향을 미치지 않습니다. 그러나 볼륨 이름과 같은 사용자가 쉽게 식별할 수 있는 일부 요소가 UUID로 교체되므로 정보를 제한하면 보고 정보의 유용성에 영향을 줄 수 있습니다.

Keystone Collector TUI 화면에서 특정 고객 데이터의 수집을 제한할 수 있습니다. 이 옵션 * 개인 데이터 제거 * 는 기본적으로 사용됩니다.

ONTAP 및 StorageGRID에서 개인 데이터 액세스를 제한하는 데 제거된 항목에 대한 자세한 내용은 을 참조하십시오 "개인 데이터 액세스를 제한할 때 제거된 항목의 목록입니다".

사용자 지정 루트 CA를 신뢰합니다

공용 루트 CA(인증 기관)에 대한 인증서 확인은 Keystone Collector 보안 기능의 일부입니다. 그러나 필요한 경우 사용자 지정 루트 CA를 신뢰하도록 Keystone Collector를 구성할 수 있습니다.

시스템 방화벽에서 SSL/TLS 검사를 사용하면 사용자 지정 CA 인증서로 인터넷 기반 트래픽이 다시 암호화됩니다. 루트 인증서를 수락하고 연결을 허용하기 전에 원본을 신뢰할 수 있는 CA로 확인하도록 설정을 구성해야 합니다. 다음 단계를 수행하십시오.

단계

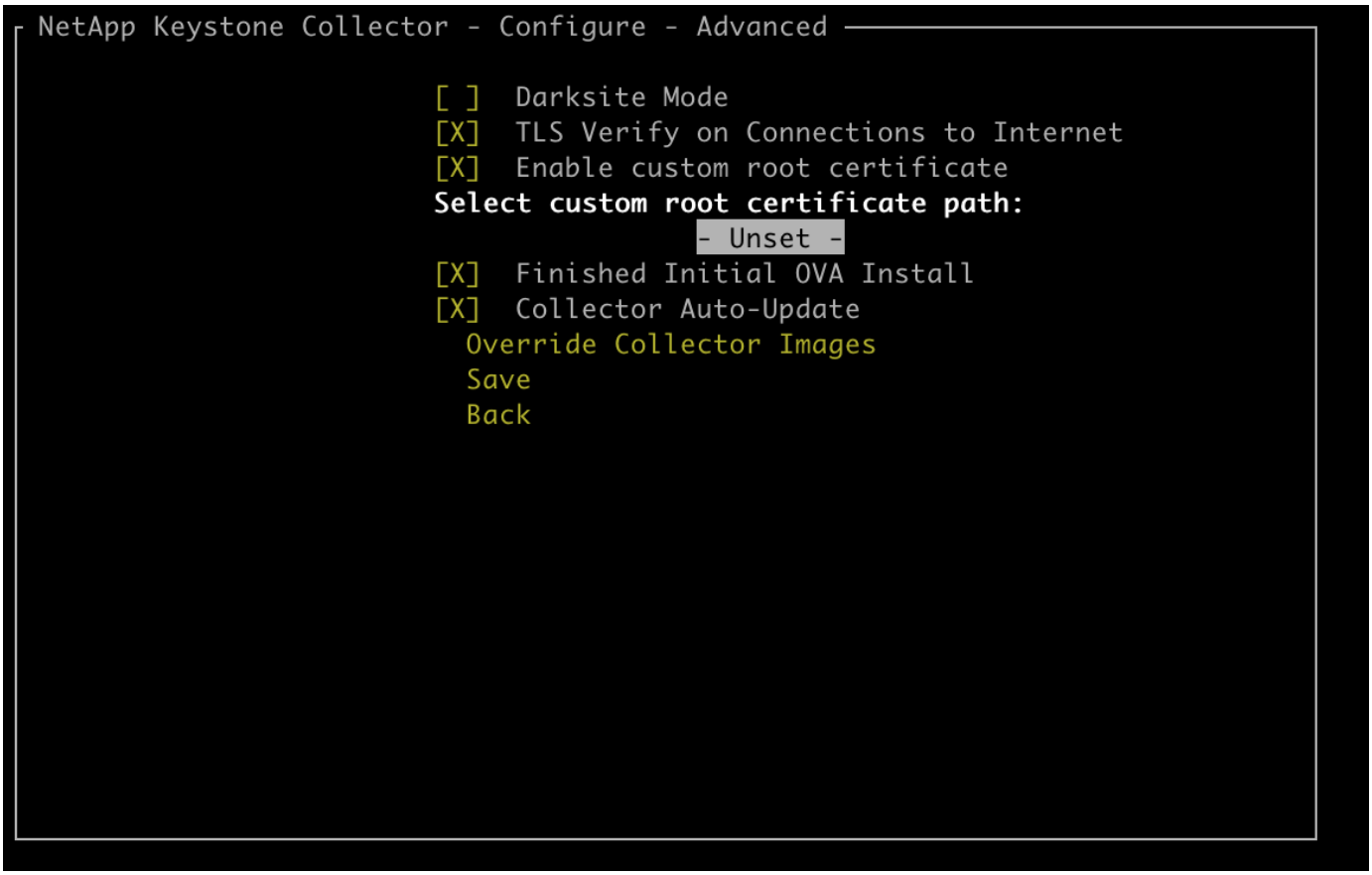
1. CA 인증서를 준비합니다. base64로 인코딩된 X.509_file 형식이어야 합니다.

   지원되는 파일 확장명은 입니다 `.pem`, `.crt`, `.cert`. 인증서가 이러한 형식 중 하나인지 확인합니다.

2. 인증서를 Keystone Collector 서버에 복사합니다. 파일이 복사되는 위치를 기록해 둡니다.
3. 서버에서 터미널을 열고 관리 TUI 유틸리티를 실행합니다.
   ```
   $ keystone-collector-tui
   ```
4. 구성 > 고급 * 으로 이동합니다.
5. 사용자 지정 루트 인증서 활성화 * 옵션을 활성화합니다.
6. 사용자 지정 루트 인증서 경로 선택: * 에 대해 을 선택합니다 `- Unset -`

7. Enter 키를 누릅니다. 인증서 경로를 선택하기 위한 대화 상자가 표시됩니다.
8. 파일 시스템 브라우저에서 루트 인증서를 선택하거나 정확한 경로를 입력합니다.
9. Enter 키를 누릅니다. 고급 * 화면으로 돌아갑니다.
10. 저장 * 을 선택합니다. 설정이 적용됩니다.

CA 인증서가 복사됩니다. `/opt/netapp/ks-collector/ca.pem` Keystone Collector 서버에서.



성능 서비스 수준 생성

Keystone Collector 관리 TUI 유틸리티를 사용하여 성능 서비스 수준(PSL)을 생성할 수 있습니다. TUI를 통해 PSL을 생성하면 각 성능 서비스 수준에 설정된 기본값이 자동으로 선택되므로 Active IQ Unified Manager 통해 PSL을 생성하는 동안 이러한 값을 수동으로 설정할 때 발생할 수 있는 오류 가능성이 줄어듭니다.

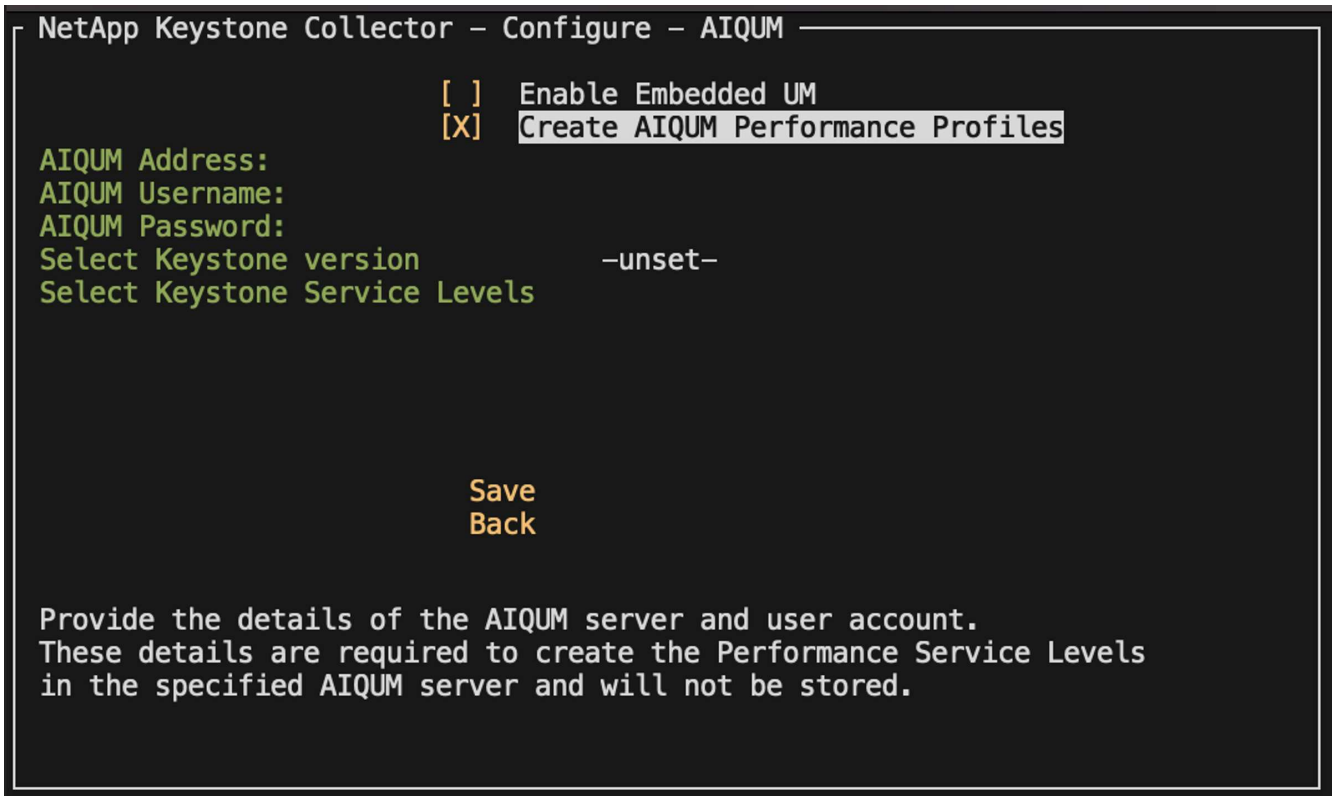
PSL에 대한 자세한 내용은 을 "성능 서비스 레벨"참조하십시오.

서비스 수준에 대한 자세한 내용은 을 "Keystone의 서비스 수준"참조하십시오.

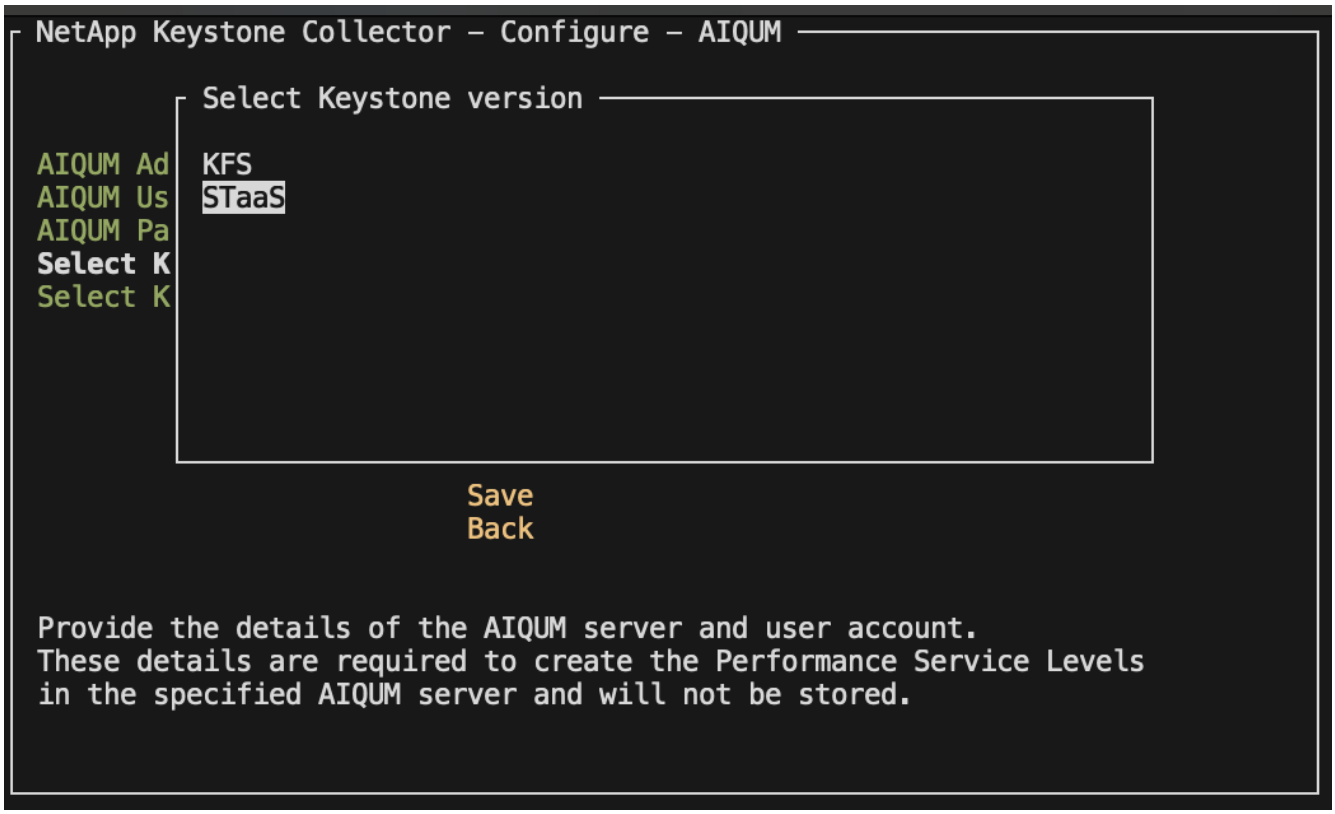
단계

1. Keystone Collector 관리 TUI 유틸리티 시작:
   ```
   $ keystone-collector-tui
   ```
2. Configure > AIQUM * 으로 이동하여 AIQUM 화면을 엽니다.
3. AIQUM 성능 프로파일 만들기 * 옵션을 활성화합니다.

4. Active IQ Unified Manager 서버 및 사용자 계정의 세부 정보를 입력합니다. 이러한 세부 정보는 PSL을 만드는 데 필요하며 저장되지 않습니다.

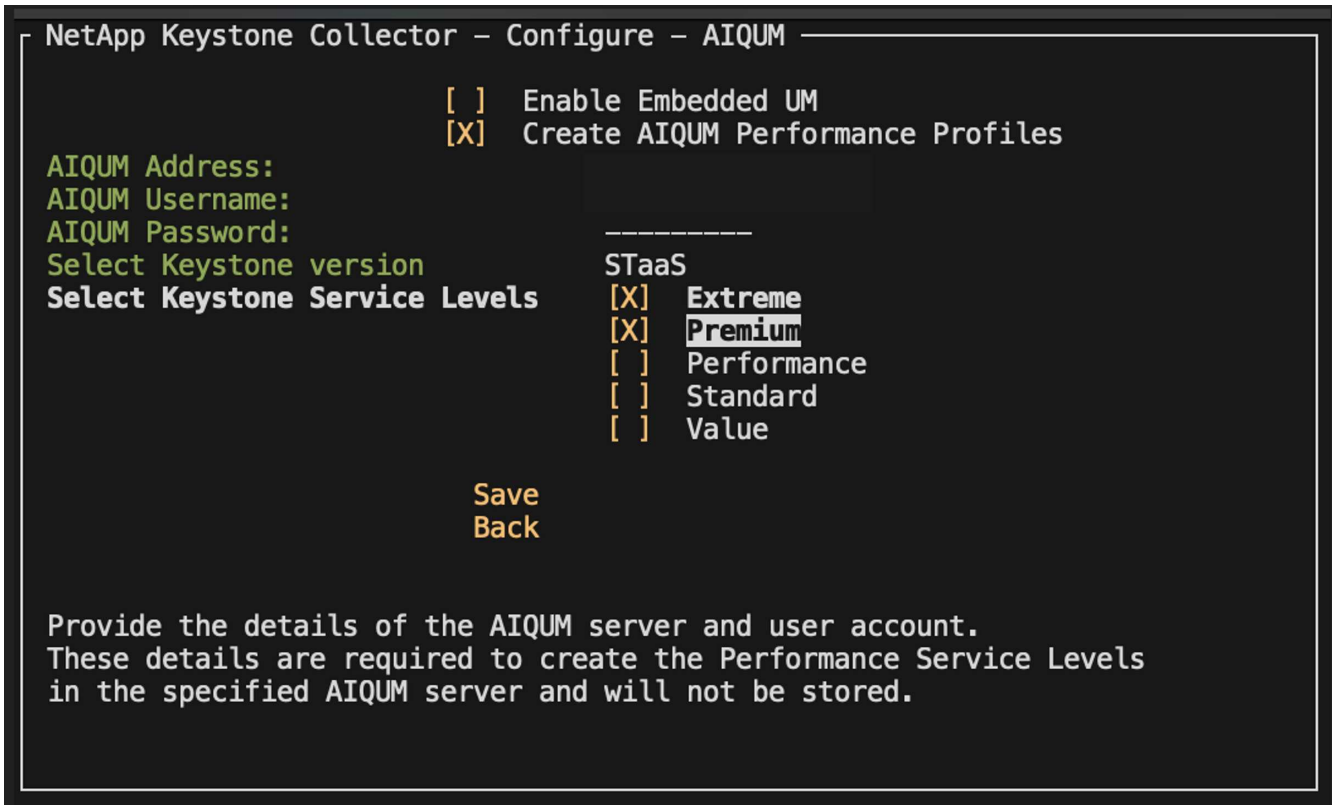


5. Select Keystone 버전 * 의 경우 를 `-unset-`선택합니다.
6. Enter 키를 누릅니다. Keystone 버전을 선택하기 위한 대화 상자가 표시됩니다.
7. STaaS * 를 강조 표시하여 Keystone STaaS의 Keystone 버전을 지정한 다음 Enter 키를 누릅니다.



Keystone 구독 서비스 버전 1의 **KFS** 옵션을 강조 표시할 수 있습니다. Keystone 구독 서비스는 구성 성능 서비스 수준, 서비스 제공, 청구 원칙 측면에서 Keystone STaaS와 다릅니다. 자세한 내용은 다음을 참조하세요."Keystone 구독 서비스 | 버전 1" .

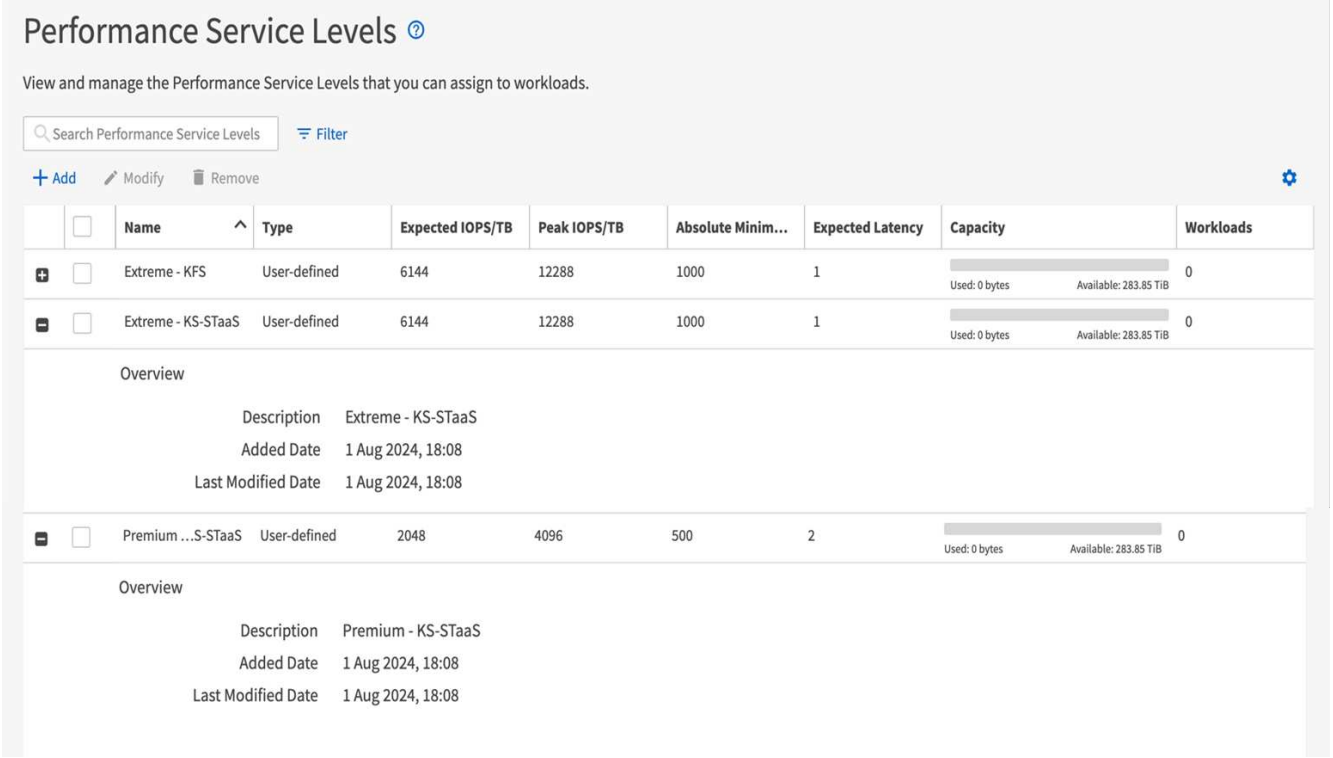
8. 지원되는 모든 Keystone 성능 서비스 수준은 지정된 Keystone 버전의 * Keystone 서비스 수준 선택* 옵션에 표시됩니다. 목록에서 원하는 성능 서비스 수준을 활성화합니다.



여러 성과 서비스 수준을 동시에 선택하여 PSL을 생성할 수 있습니다.

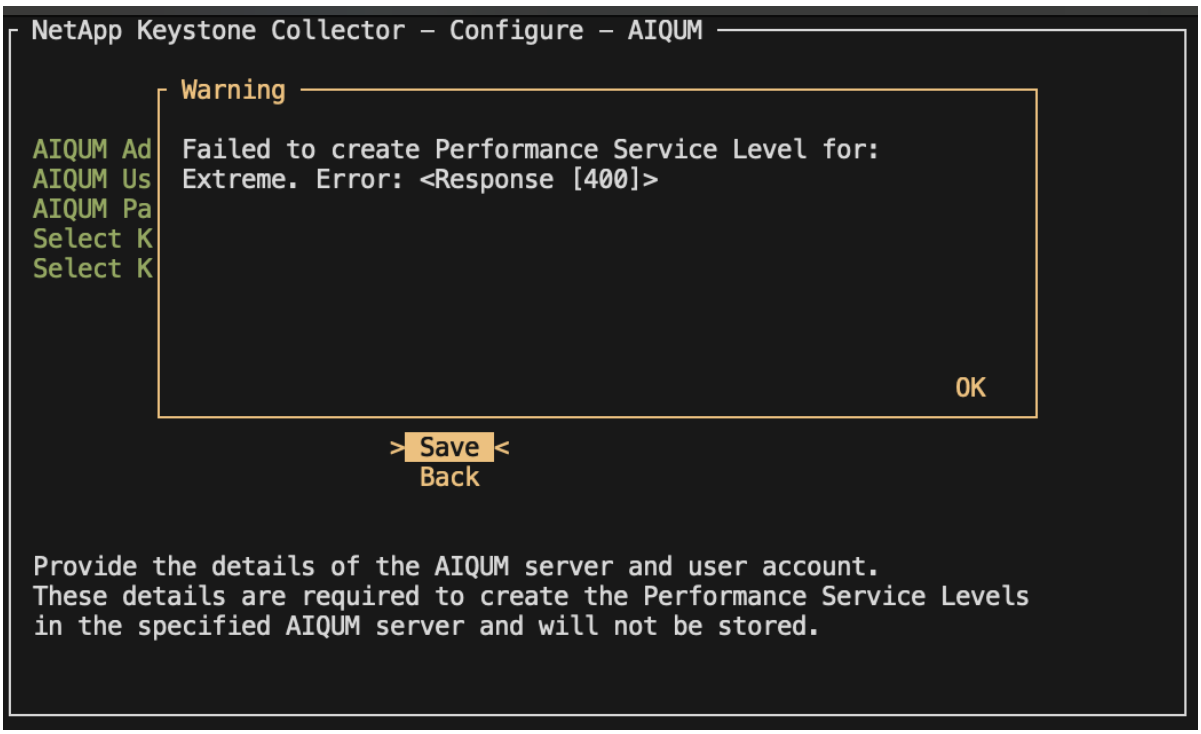
9. Save * 를 선택하고 Enter 키를 누릅니다. 성능 서비스 수준이 생성됩니다.

   STaaS용 프리미엄-KS-STaaS 또는 KFS용 익스트림 KFS와 같이 생성된 PSL은 Active IQ Unified Manager의 * 성능 서비스 수준 * 페이지에서 볼 수 있습니다. 생성된 PSL이 요구 사항을 충족하지 않는 경우 필요에 맞게 PSL을 수정할 수 있습니다. 자세한 내용은 을 "성능 서비스 수준 생성 및 편집"참조하십시오.



선택한 성능 서비스 수준에 대한 PSL이 지정된 Active IQ Unified Manger 서버에 이미 있는 경우 다시 생성할 수 없습니다. 이를 시도하면 오류 메시지가 표시됩니다

.



ITOM Collector를 설치합니다

Keystone ITOM Collector 설치 요구 사항

ITOM Collector를 설치하기 전에 시스템에 필요한 소프트웨어가 준비되어 있고 필요한 모든 필수 구성 요소를 충족하는지 확인하십시오.

ITOM Collector 서버 **VM**의 사전 요구 사항**:**

- 지원되는 운영 체제:
  - 데비안 12 이상
  - Windows Server 2016 이상
  - Ubuntu 20.04 LTS 이상
  - 레드햇 엔터프라이즈 리눅스(RHEL) 8.x
  - Red Hat Enterprise Linux 9.0 이상
  - Amazon Linux 2023 이상

  권장되는 운영 체제는 Debian 12, Windows Server 2016 또는 이후 버전입니다.

- 리소스 요구 사항: 모니터링되는 NetApp 노드 수에 따른 VM 리소스 요구 사항은 다음과 같습니다.
  - 2-10개 노드: CPU 4개, 8GB RAM, 40GB 디스크
  - 12-20개 노드: CPU 8개, 16GB RAM, 40GB 디스크
- 구성 요구 사항: 모니터링되는 장치에 읽기 전용 계정과 SNMP가 구성되어 있는지 확인합니다. ITOM Collector 서버 VM도 NetApp 클러스터 및 클러스터 스위치에서 SNMP 트랩 호스트 및 Syslog 서버로 구성해야 합니다 (해당하는 경우).

네트워킹 요구 사항

다음 표에는 ITOM Collector의 네트워킹 요구 사항이 나와 있습니다.

출처	목적지	프로토콜	포트	설명
ITOM 수집기	NetApp ONTAP 클러스터 관리 IP	HTTPS, SNMP	TCP 443, UDP 161	ONTAP 컨트롤러 모니터링
NetApp ONTAP 클러스터 및 노드 관리 IP	ITOM 수집기	SNMP, Syslog	UDP 162, UDP 514	컨트롤러의 SNMP 트랩 및 Syslog
ITOM 수집기	클러스터 스위치	SNMP를 선택합니다	UDP 161 를 참조하십시오	스위치 모니터링
클러스터 스위치	ITOM 수집기	SNMP, Syslog	UDP 162, UDP 514	스위치의 SNMP 트랩 및 Syslog
ITOM 수집기	StorageGRID 노드 IP	HTTPS, SNMP	TCP 443, UDP 161	StorageGRID의 SNMP 모니터링
StorageGRID 노드 IP	ITOM 수집기	SNMP, Syslog	UDP 162, UDP 514	StorageGRID의 SNMP 트랩
ITOM 수집기	Keystone 컬렉터	SSH, HTTPS, SNMP를 선택합니다	TCP 22, TCP 443, UDP 161	Keystone Collector 모니터링 및 원격 관리

ITOM 수집기	로컬 DNS	DNS	UDP 53 를 참조하십시오	공용 또는 사설 DNS 서비스
ITOM 수집기	선택한 NTP 서버입니다	NTP	UDP 123입니다	시간 유지

Linux 시스템에 Keystone ITOM Collector를 설치하세요

스토리지 환경에서 메트릭 데이터를 수집하는 ITOM Collector를 설치하려면 몇 가지 단계를 완료하세요. 요구 사항에 따라 Windows 또는 Linux 시스템에 설치할 수 있습니다.

Keystone 지원 팀은 ITOM Collector 설정 파일을 다운로드할 수 있는 동적 링크를 제공합니다. 이 파일은 2시간 후에 만료됩니다.

Windows 시스템에 ITOM Collector를 설치하려면 을 "Windows 시스템에 ITOM Collector를 설치합니다 "참조하십시오.

Linux 서버에 소프트웨어를 설치하려면 다음 단계를 수행하십시오.

시작하기 전에

- Linux 설치 스크립트에 Bourne 셸을 사용할 수 있는지 확인합니다.
- `vim-common`패키지를 설치하여 ITOM Collector 설치 파일에 필요한 * xxd * 바이너리를 가져옵니다.
- ITOM Collector를 루트가 아닌 사용자로 실행하려면 가 `sudo package` 설치되어 있어야 합니다.

단계

1. Linux 서버에 ITOM Collector 설정 파일을 다운로드합니다.
2. 서버에서 터미널을 열고 다음 명령을 실행하여 권한을 변경하고 바이너리를 실행 파일로 만듭니다.
   `# chmod +x <installer_file_name>.bin`
3. 다음 명령을 실행하여 ITOM Collector 설정 파일을 시작합니다.
   `#./<installer_file_name>.bin`
4. 설치 파일을 실행하면 다음 메시지가 표시됩니다.
   a. 최종 사용자 사용권 계약(EULA)에 동의합니다.
   b. 설치에 대한 사용자 세부 정보를 입력합니다.
   c. 설치 상위 디렉토리를 지정합니다.
   d. 수집기 크기를 선택합니다.
   e. 해당하는 경우 프록시 세부 정보를 제공합니다.

      각 프롬프트마다 기본 옵션이 표시됩니다. 특정 요구 사항이 없는 경우 기본 옵션을 선택하는 것이 좋습니다. Enter * 키를 눌러 기본 옵션을 선택합니다. 설치가 완료되면 ITOM Collector가 성공적으로 설치되었음을 확인하는 메시지가 표시됩니다.

- ITOM Collector 설치 파일은 서비스 재시작 및 메모리 덤프를 처리하기 위해 에 `/etc/sudoers` 추가합니다.
- Linux 서버에 ITOM Collector를 설치하면 * ITOM * 이라는 기본 사용자가 만들어져 루트 Privileges 없이 ITOM Collector를 실행할 수 있습니다. 다른 사용자를 선택하거나 루트로 실행할 수 있지만 Linux 설치 스크립트로 만든 ITOM 사용자를 사용하는 것이 좋습니다.

다음 단계

설치가 완료되면 Keystone 지원 팀에 문의하여 ITOM 지원 포털을 통해 ITOM Collector가 성공적으로 설치되었는지 확인합니다. 확인 후 Keystone 지원 팀은 추가 장치 검색 및 모니터링 설정을 포함하여 ITOM Collector를 원격으로 구성하고 구성이 완료되면 확인 메시지를 보냅니다. 문의 사항이나 추가 정보는 keystone.services@ NetApp.com에 문의하십시오.

Windows 시스템에 Keystone ITOM Collector를 설치하세요.

ITOM Collector 설정 파일을 다운로드하고 InstallShield 마법사를 실행한 다음 필요한 모니터링 자격 증명을 입력하여 Windows 시스템에 ITOM Collector를 설치합니다.

Keystone 지원 팀은 ITOM Collector 설정 파일을 다운로드할 수 있는 동적 링크를 제공합니다. 이 파일은 2시간 후에 만료됩니다.

요구 사항에 따라 Linux 시스템에 설치할 수 있습니다. Linux 시스템에 ITOM Collector를 설치하려면 을 "Linux 시스템에 ITOM Collector를 설치합니다"참조하십시오.

Windows 서버에 ITOM Collector 소프트웨어를 설치하려면 다음 단계를 수행하십시오.

시작하기 전에

ITOM Collector 서비스가 부여되었는지 확인 * Windows 서버의 로컬 보안 정책 설정에 있는 로컬 정책/사용자 권한 할당 아래의 서비스로 로그온 *.

단계

1. ITOM Collector 설정 파일을 Windows 서버에 다운로드합니다.
2. 설치 파일을 열어 InstallShield 마법사를 시작합니다.
3. 최종 사용자 사용권 계약(EULA)에 동의합니다. InstallShield 마법사가 필요한 바이너리를 추출하고 자격 증명을 입력하라는 메시지를 표시합니다.
4. ITOM Collector가 실행할 계정의 자격 증명을 입력합니다.
   - ITOM Collector가 다른 Windows 서버를 모니터링하지 않는 경우 로컬 시스템을 사용합니다.
   - ITOM Collector가 동일한 도메인의 다른 Windows 서버를 모니터링하는 경우 로컬 관리자 권한이 있는 도메인 계정을 사용합니다.
   - ITOM Collector가 동일한 도메인에 속하지 않는 다른 Windows 서버를 모니터링하는 경우 로컬 관리자 계정을 사용하고 로컬 관리자 자격 증명을 사용하여 각 리소스에 연결합니다. ITOM Collector와 모니터링되는 리소스 간의 인증 문제를 줄이기 위해 만료되지 않도록 암호를 설정할 수 있습니다.
5. 수집기 크기를 선택합니다. 기본값은 설치 파일을 기준으로 권장되는 크기입니다. 구체적인 요구 사항이 없는 경우 제안된 크기를 계속 진행합니다.
6. 설치를 시작하려면 _Next_를 선택하십시오. 채워진 폴더를 사용하거나 다른 폴더를 선택할 수 있습니다. 상태 상자에 설치 진행률이 표시된 후 InstallShield 마법사 완료 대화 상자가 나타납니다.

다음 단계

설치가 완료되면 Keystone 지원 팀에 문의하여 ITOM 지원 포털을 통해 ITOM Collector가 성공적으로 설치되었는지 확인합니다. 확인 후 Keystone 지원 팀은 추가 장치 검색 및 모니터링 설정을 포함하여 ITOM Collector를 원격으로 구성하고 구성이 완료되면 확인 메시지를 보냅니다. 문의 사항이나 추가 정보는 keystone.services@ NetApp.com에 문의하십시오.

Keystone용 AutoSupport를 구성합니다

AutoSupport 원격 측정 메커니즘을 사용할 때 Keystone은 AutoSupport 원격 측정 데이터를 기준으로 사용량을 계산합니다. 필요한 세분화 수준을 달성하려면 ONTAP 클러스터에서 보내는 일별 지원 번들에 Keystone 데이터를 통합하도록 AutoSupport을 구성해야 합니다.

이 작업에 대해

Keystone 데이터를 포함하도록 AutoSupport을 구성하기 전에 다음 사항에 유의하십시오.

- ONTAP CLI를 사용하여 AutoSupport 원격 측정 옵션을 편집합니다. AutoSupport 서비스 및 시스템(클러스터) 관리자 역할 관리에 대한 자세한 내용은 을 참조하십시오 "AutoSupport 개요 관리" 및 "클러스터 및 SVM 관리자".
- 일별 및 주별 AutoSupport 번들에 서브시스템을 포함하여 Keystone의 데이터를 정확하게 수집할 수 있습니다. AutoSupport 하위 시스템에 대한 자세한 내용은 을 참조하십시오 "AutoSupport 하위 시스템이란 무엇입니까".

단계

1. 시스템 관리자 사용자는 SSH를 사용하여 Keystone ONTAP 클러스터에 로그인합니다. 자세한 내용은 을 참조하십시오 "SSH를 사용하여 클러스터에 액세스합니다".
2. 로그 내용을 수정합니다.
   - ONTAP 9.16.1 이상의 경우 다음 명령을 실행하여 일일 로그 내용을 수정하세요.

     ```
     autosupport trigger modify -node * -autosupport-message
     management.log -basic-additional
     wafl,performance,snapshot,object_store_server,san,raid,snapmirror
     -troubleshooting-additional wafl
     ```

     클러스터가 MetroCluster 구성에 있는 경우 다음 명령을 실행합니다.

     ```
     autosupport trigger modify -node * -autosupport-message
     management.log -basic-additional
     wafl,performance,snapshot,object_store_server,san,raid,snapmirror,met
     rocluster -troubleshooting-additional wafl
     ```

   - 이전 ONTAP 버전의 경우 다음 명령을 실행하여 일일 로그 내용을 수정하세요.

```
autosupport trigger modify -node * -autosupport-message
management.log -basic-additional
wafl,performance,snapshot,platform,object_store_server,san,raid,snapm
irror -troubleshooting-additional wafl
```

클러스터가 MetroCluster 구성에 있는 경우 다음 명령을 실행합니다.

```
autosupport trigger modify -node * -autosupport-message management.log
-basic-additional
wafl,performance,snapshot,platform,object_store_server,san,raid,snapmirr
or,metrocluster -troubleshooting-additional wafl
```

- 다음 명령을 실행하여 주간 로그 내용을 수정합니다.

```
autosupport trigger modify -autosupport-message weekly
-troubleshooting-additional wafl -node *
```

이 명령에 대한 자세한 내용은 을 참조하십시오 "시스템 노드 AutoSupport 트리거 수정".

모니터링 및 업그레이드

Keystone Collector의 상태를 모니터링합니다

HTTP 요청을 지원하는 모니터링 시스템을 사용하여 Keystone Collector의 상태를 모니터링할 수 있습니다. 상태 모니터링은 Keystone 대시보드에서 데이터를 사용할 수 있도록 하는 데 도움이 될 수 있습니다.

기본적으로 Keystone 상태 서비스는 localhost 이외의 IP로부터의 연결을 허용하지 않습니다. Keystone 상태 엔드포인트는 입니다 `/uber/health`또한 포트에서 `Keystone Collector` 서버의 모든 인터페이스를 수신합니다 `7777`. 쿼리 시 JSON 출력이 있는 HTTP 요청 상태 코드가 끝점에서 응답으로 반환되어 Keystone Collector 시스템의 상태를 설명합니다.
JSON 본체는 에 대한 전반적인 상태를 제공합니다 `is_healthy` 속성, 부울, 에 대한 구성 요소별 상태의 세부 목록 `component_details` 속성.
예를 들면 다음과 같습니다.

```
$ curl http://127.0.0.1:7777/uber/health
{"is_healthy": true, "component_details": {"vicmet": "Running", "ks-
collector": "Running", "ks-billing": "Running", "chronyd": "Running"}}
```

다음 상태 코드가 반환됩니다.

- * 200 *: 모니터링되는 모든 구성 요소가 정상 상태임을 나타냅니다

- * 503 *: 하나 이상의 구성 요소가 정상 상태가 아님을 나타냅니다
- * 403 * : 상태를 쿼리하는 HTTP 클라이언트가 허용되는 네트워크 CIDR 목록인 _allow_list에 없음을 나타냅니다. 이 상태에서는 상태 정보가 반환되지 않습니다. allow_list는 네트워크 CIDR 방법을 사용하여 Keystone 상태 시스템을 쿼리할 수 있는 네트워크 디바이스를 제어합니다. 이 오류가 발생하면 * Keystone Collector 관리 TUI > 구성 > 상태 모니터링 * 에서 _allow_list에 모니터링 시스템을 추가하십시오.

> **Linux** 사용자의 경우 이 알려진 문제를 확인하십시오.
>
> * 문제 설명 *: Keystone 수집기는 사용량 측정 시스템의 일부로 다수의 컨테이너를 실행합니다. Red Hat Enterprise Linux 8.x 서버가 ISA(USA Defense Information Systems Agency) STIG(Security Technical Implementation Guides) 정책으로 강화되면, flapolicyd(File Access Policy Daemon)와 관련된 알려진 문제가 간헐적으로 나타납니다. 이 문제는 로 식별됩니다 "버그 1907870". * 해결 방법 *: Red Hat Enterprise가 해결될 때까지 NetApp은 이 문제를 해결해 드립니다 `fapolicyd` 허용 모드로 전환합니다. 인치 `/etc/fapolicyd/fapolicyd.conf`에서 값을 설정합니다 `permissive = 1`.

시스템 로그를 봅니다

Keystone Collector 시스템 로그를 보고 시스템 정보를 검토하고 해당 로그를 사용하여 문제 해결을 수행할 수 있습니다. Keystone Collector는 호스트의 _저널_로깅 시스템을 사용하며, STANDARD_저널_시스템 유틸리티를 통해 시스템 로그를 검토할 수 있습니다. 다음 주요 서비스를 사용하여 로그를 검토할 수 있습니다.

- KS - 콜렉터
- KS - 상태
- KS - 자동 업데이트

메인 데이터 수집 service_ks-collector_는 를 사용하여 JSON 형식의 로그를 생성합니다 `run-id` 예약된 각 데이터 수집 작업과 연결된 속성입니다. 다음은 표준 사용 데이터 수집에 성공한 작업의 예입니다.

```
{"level":"info","time":"2022-10-31T05:20:01.831Z","caller":"light-
collector/main.go:31","msg":"initialising light collector with run-id
cdflm0f74cgphgfon8cg","run-id":"cdflm0f74cgphgfon8cg"}
{"level":"info","time":"2022-10-
31T05:20:04.624Z","caller":"ontap/service.go:215","msg":"223 volumes
collected for cluster a2049dd4-bfcf-11ec-8500-00505695ce60","run-
id":"cdflm0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-
31T05:20:18.821Z","caller":"ontap/service.go:215","msg":"697 volumes
collected for cluster 909cbacc-bfcf-11ec-8500-00505695ce60","run-
id":"cdflm0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-
31T05:20:41.598Z","caller":"ontap/service.go:215","msg":"7 volumes
collected for cluster f7b9a30c-55dc-11ed-9c88-005056b3d66f","run-
id":"cdflm0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-
31T05:20:48.247Z","caller":"ontap/service.go:215","msg":"24 volumes
collected for cluster a9e2dcff-ab21-11ec-8428-00a098ad3ba2","run-
id":"cdflm0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-
31T05:20:48.786Z","caller":"worker/collector.go:75","msg":"4 clusters
collected","run-id":"cdflm0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-
31T05:20:48.839Z","caller":"reception/reception.go:75","msg":"Sending file
65a71542-cb4d-bdb2-e9a7-a826be4fdcb7_1667193648.tar.gz type=ontap to
reception","run-id":"cdflm0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-
31T05:20:48.840Z","caller":"reception/reception.go:76","msg":"File bytes
123425","run-id":"cdflm0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-
31T05:20:51.324Z","caller":"reception/reception.go:99","msg":"uploaded
usage file to reception with status 201 Created","run-
id":"cdflm0f74cgphgfon8cg"}
```

다음은 선택적 성능 데이터 수집을 위한 성공적인 작업의 예입니다.

```
{"level":"info","time":"2022-10-
31T05:20:51.324Z","caller":"sql/service.go:28","msg":"initialising MySql
service at 10.128.114.214"}

{"level":"info","time":"2022-10-
31T05:20:51.324Z","caller":"sql/service.go:55","msg":"Opening MySql db
connection at server 10.128.114.214"}

{"level":"info","time":"2022-10-
31T05:20:51.324Z","caller":"sql/service.go:39","msg":"Creating MySql db
config object"}

{"level":"info","time":"2022-10-
31T05:20:51.324Z","caller":"sla_reporting/service.go:69","msg":"initialisi
ng SLA service"}

{"level":"info","time":"2022-10-
31T05:20:51.324Z","caller":"sla_reporting/service.go:71","msg":"SLA
service successfully initialised"}

{"level":"info","time":"2022-10-
31T05:20:51.324Z","caller":"worker/collector.go:217","msg":"Performance
data would be collected for timerange: 2022-10-31T10:24:52~2022-10-
31T10:29:52"}

{"level":"info","time":"2022-10-
31T05:21:31.385Z","caller":"worker/collector.go:244","msg":"New file
generated: 65a71542-cb4d-bdb2-e9a7-a826be4fdcb7_1667193651.tar.gz"}

{"level":"info","time":"2022-10-
31T05:21:31.385Z","caller":"reception/reception.go:75","msg":"Sending file
65a71542-cb4d-bdb2-e9a7-a826be4fdcb7_1667193651.tar.gz type=ontap-perf to
reception","run-id":"cdflm0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-
31T05:21:31.386Z","caller":"reception/reception.go:76","msg":"File bytes
17767","run-id":"cdflm0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-
31T05:21:33.025Z","caller":"reception/reception.go:99","msg":"uploaded
usage file to reception with status 201 Created","run-
id":"cdflm0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-31T05:21:33.025Z","caller":"light-
collector/main.go:88","msg":"exiting","run-id":"cdflm0f74cgphgfon8cg"}
```

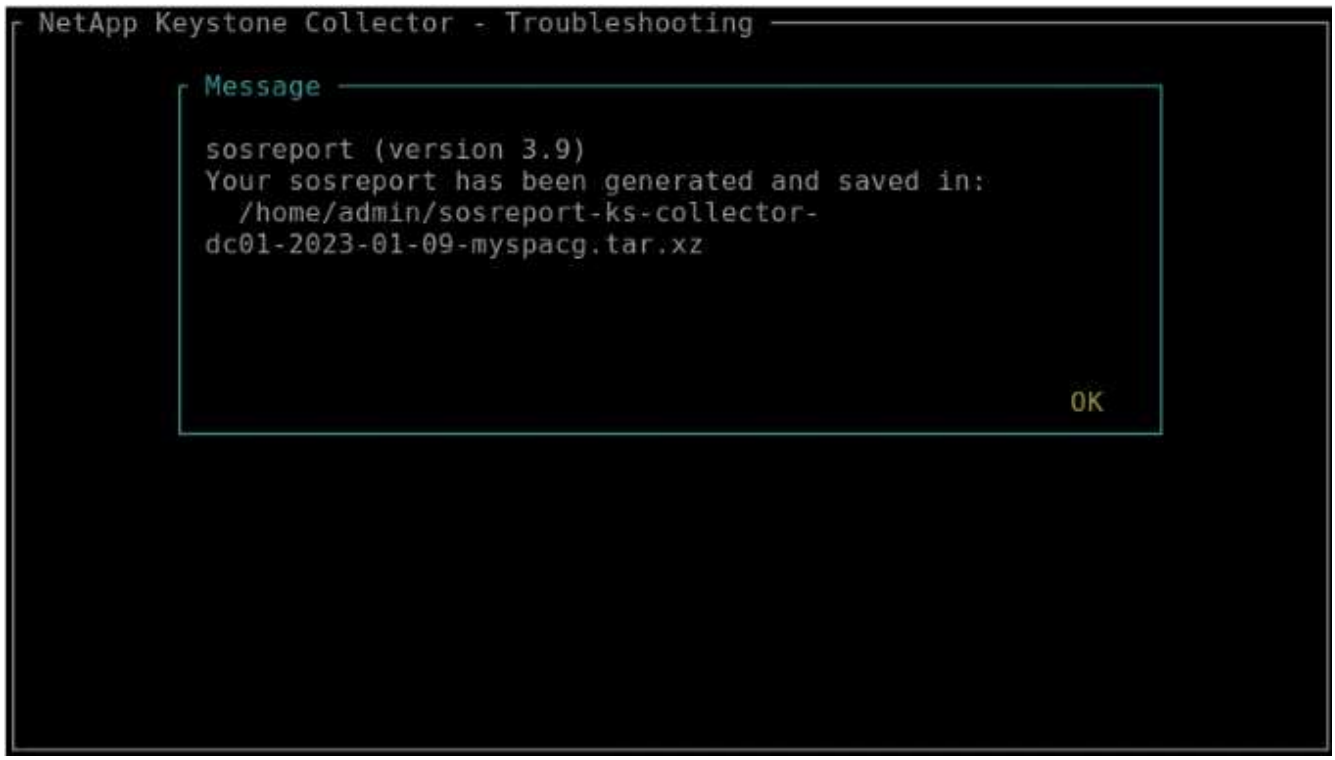
지원 번들을 생성하고 수집합니다

Keystone Collector TUI를 사용하면 지원 번들을 생성한 다음 지원 문제 해결을 위한 서비스 요청에 추가할 수 있습니다. 다음 절차를 따르십시오.

단계

1. Keystone Collector 관리 TUI 유틸리티 시작:
   ```
   $ keystone-collector-tui
   ```
2. 문제 해결 > 지원 번들 생성 * 으로 이동합니다
   .

3. 생성된 경우, Bundle이 저장된 위치가 표시됩니다. FTP, SFTP 또는 SCP를 사용하여 위치에 연결하고 로그 파일을 로컬 시스템에 다운로드합니다
   .



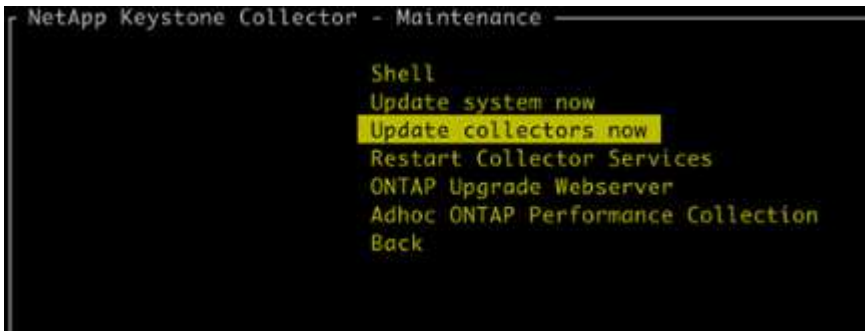
4. 파일을 다운로드한 후 Keystone ServiceNow 지원 티켓에 첨부할 수 있습니다. 티켓 발행에 대한 정보는 다음을 참조하세요. "서비스 요청을 생성하는 중입니다".

Keystone Collector를 수동으로 업그레이드합니다

Keystone 수집기의 자동 업데이트 기능은 기본적으로 활성화되어 있으며, 새 릴리즈마다 Keystone Collector 소프트웨어를 자동으로 업그레이드합니다. 그러나 이 기능을 비활성화하고 소프트웨어를 수동으로 업그레이드할 수 있습니다.

단계

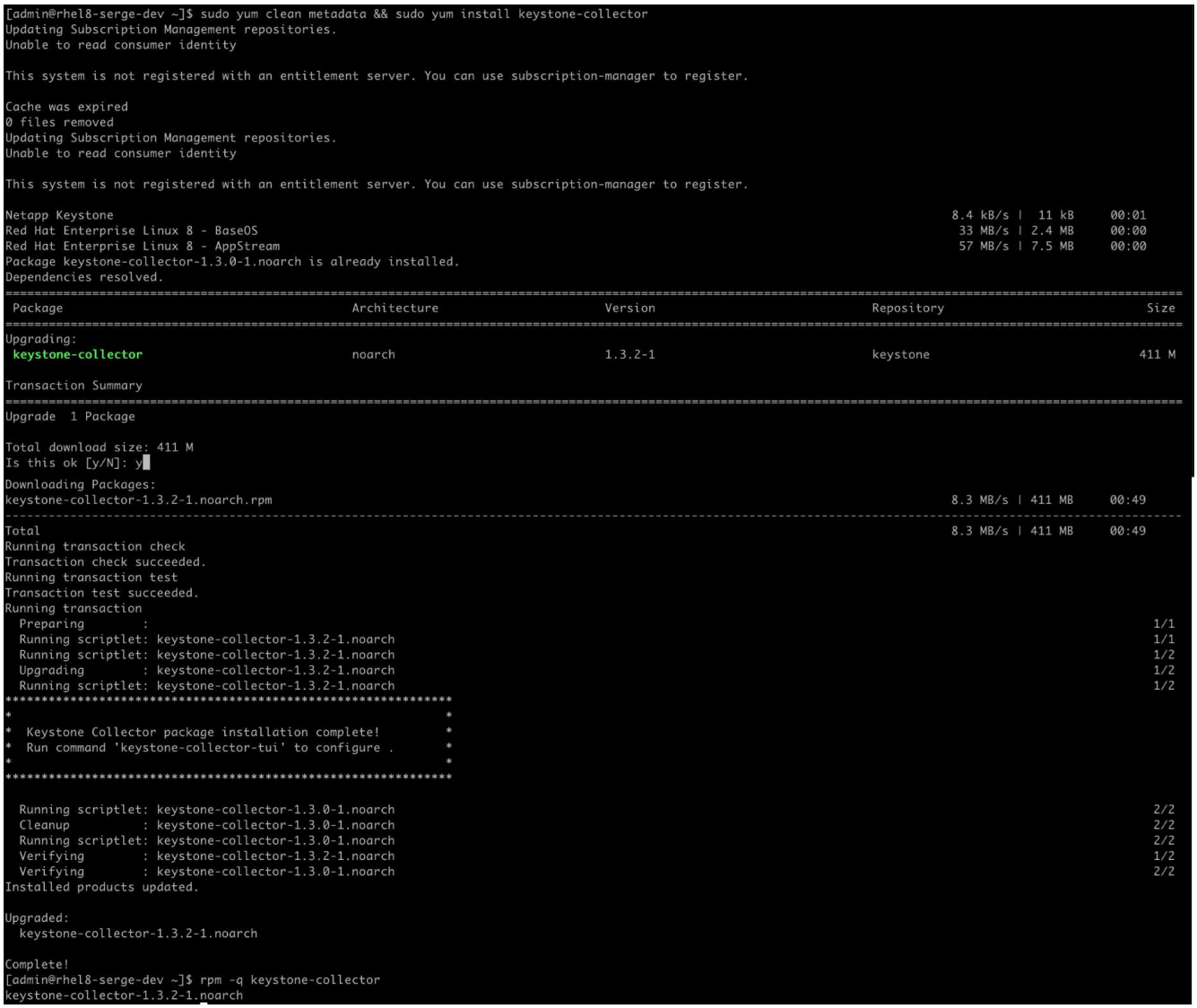
1. Keystone Collector 관리 TUI 유틸리티 시작:
   `$ keystone-collector-tui`
2. 유지 관리 화면에서 * 지금 수집기 업데이트 * 옵션을 선택합니다.



또는 다음 명령을 실행하여 버전을 업그레이드합니다.

CentOS의 경우:

```
sudo yum clean metadata && sudo yum install keystone-collector
```



데비안의 경우:

```
sudo apt-get update && sudo apt-get upgrade keystone-collector
```

3. Keystone Collector 관리 TUI를 다시 시작하면 홈 화면의 왼쪽 상단에 최신 버전이 표시됩니다.

   또는 다음 명령을 실행하여 최신 버전을 볼 수도 있습니다.

   CentOS의 경우:

```
rpm -q keystone-collector
```

   데비안의 경우:

```
dpkg -l | grep keystone-collector
```

Keystone Collector 보안

Keystone Collector에는 고객 데이터의 보안을 침해하지 않고 Keystone 시스템의 성능 및 사용 메트릭을 모니터링하는 보안 기능이 포함되어 있습니다.

Keystone Collector의 기능은 다음과 같은 보안 원칙을 기반으로 합니다.

- * 프라이버시 설계 * - Keystone Collector는 사용량 측정 및 성능 모니터링을 수행하기 위해 최소 데이터를 수집합니다. 자세한 내용은 을 참조하십시오 "대금 청구를 위해 수집된 데이터". 를 클릭합니다 "개인 데이터를 제거합니다" 옵션은 기본적으로 활성화되어 있으며 중요한 정보를 마스크하고 보호합니다.
- * 최소 권한 액세스 * - Keystone Collector는 스토리지 시스템을 모니터링할 수 있는 최소 권한을 요구하므로 보안 위험을 최소화하고 의도하지 않은 데이터 수정을 방지할 수 있습니다. 이 접근 방식은 최소 권한 원칙에 따라 모니터링되는 환경의 전반적인 보안 상태를 개선합니다.
- * 보안 소프트웨어 개발 프레임워크 * - Keystone은 개발 주기 전반에 걸쳐 보안 소프트웨어 개발 프레임워크를 사용하여 위험을 완화하고 취약점을 줄이며 잠재적인 위협으로부터 시스템을 보호합니다.

보안 강화

기본적으로 Keystone Collector는 보안이 강화된 구성을 사용하도록 구성됩니다. 권장되는 보안 구성은 다음과 같습니다.

- Keystone Collector 가상 머신의 운영 체제:
  - CIS Debian Linux 12 벤치마크 표준을 준수합니다. Keystone Collector 관리 소프트웨어 외부에서 OS 구성을 변경하면 시스템 보안이 저하될 수 있습니다. 자세한 내용은 을 참조하십시오 "CIS 벤치마크 가이드".
  - 자동 업데이트 기능을 통해 Keystone Collector에서 확인된 보안 패치를 자동으로 수신하고 설치합니다. 이 기능을 비활성화하면 패치가 적용되지 않은 소프트웨어가 발생할 수 있습니다.
  - Keystone Collector에서 받은 업데이트를 인증합니다. APT 리포지토리 확인을 사용하지 않도록 설정하면 승인되지 않은 패치가 자동으로 설치되어 취약점이 발생할 수 있습니다.
- Keystone Collector는 자동으로 HTTPS 인증서를 검증하여 연결 보안을 보장합니다. 이 기능을 사용하지 않으면 외부 끝점을 가장하고 사용 데이터가 유출될 수 있습니다.
- Keystone Collector가 지원합니다 "사용자 지정 신뢰할 수 있는 CA" 인증. 기본적으로 이 인증서는 에서 인식하는 공용 루트 CA에 의해 서명된 인증서를 신뢰합니다 "Mozilla CA 인증서 프로그램". Keystone Collector는 신뢰할 수 있는 CA를 추가로 활성화하여 이러한 인증서를 제공하는 엔드포인트에 대한 연결에 대해 HTTPS 인증서 유효성 검사를 활성화합니다.
- Keystone Collector는 기본적으로 * Remove Private Data * 옵션을 사용하도록 설정하며, 이 옵션은 중요한 정보를 마스킹하고 보호합니다. 자세한 내용은 을 참조하십시오 "개인 데이터의 수집 제한". 이 옵션을 비활성화하면 Keystone 시스템에 추가로 데이터가 전달됩니다. 예를 들어, 중요한 정보로 간주될 수 있는 볼륨 이름과 같은 사용자 입력 정보를 포함할 수 있습니다.
- 관련 정보 *
- "Keystone Collector 개요"
- "가상 인프라 요구 사항"

- "Keystone Collector 구성"

Keystone이 수집하는 사용자 데이터의 유형

Keystone Keystone ONTAP 및 Keystone StorageGRID 구독의 구성, 상태 및 사용 정보와 Keystone Collector를 호스팅하는 가상 머신(VM)의 원격 측정 데이터를 수집합니다. Keystone Collector에서 이 옵션이 활성화된 경우 ONTAP 에 대한 성능 데이터만 수집할 수 있습니다.

ONTAP 데이터 수집

ONTAP에 대해 수집된 **** 사용 데이터**:** 자세히 알아보기 ****

다음 목록은 ONTAP에 대해 수집된 용량 소비 데이터의 대표적인 예입니다.

- 클러스터
  - 클러스터 UUID입니다
  - 클러스터 이름
  - 일련 번호
  - 위치(ONTAP 클러스터의 값 입력 기준)
  - 연락처
  - 버전
- 노드
  - 일련 번호
  - 노드 이름
- 볼륨
  - 애그리게이트 이름입니다
  - 볼륨 이름
  - VolumeInstanceUUID
  - IsCloneVolume 플래그
  - IsFlexGroupConstituent 플래그입니다
  - IsSpaceEnforcementLogical 플래그
  - IsSpaceReportingLogical 플래그
  - LogicalSpaceUsedByAfs
  - PercentSnapshotSpace를 참조하십시오
  - PerformanceTierInactiveUserData 를 참조하십시오
  - PerformanceTierInactiveUserDataPercent 를 참조하십시오
  - QoSAdapitivePolicyGroup 이름입니다
  - QoSPolicyGroup 이름입니다
  - 크기
  - 사용됨
  - PhysicalUsed(PhysicalUsed)
  - SizeUsedBySnapshots입니다
  - 유형
  - VolumeStyleExtended 를 참조하십시오
  - SVM 이름
  - IsVsRoot 플래그입니다

- 가상 서버
  - VserverName입니다
  - VserverUUID입니다
  - 하위 유형
- 스토리지 애그리게이트
  - 스토리지 유형
  - 애그리게이트 이름
  - 총 UUID
  - 물리적 사용
  - 사용 가능한 크기
  - 크기
  - 사용된 사이즈
- 오브젝트 저장소를 통합합니다
  - ObjectStoreName입니다
  - ObjectStoreUUID입니다
  - providerType을 참조하십시오
  - 애그리게이트 이름
- 클론 볼륨
  - 플랙스클론
  - 크기
  - 사용됨
  - SVM
  - 유형
  - ParentVolume
  - ParentVserver
  - IsConstituent(제원)
  - Splitimate
  - 상태
  - FlexCloneUsedPercent
- 스토리지 LUN
  - LUN UUID입니다
  - LUN 이름입니다
  - 크기
  - 사용됨
  - IsReserved 플래그입니다

- IsRequested 플래그입니다
- LogicalUnit 이름입니다
- QoSPolicyUUID입니다
- QoSPolicyName입니다
- UUID입니다
- 볼륨 이름
- SVM의 UUID입니다
- SVM 이름

- 스토리지 볼륨
  - VolumeInstanceUUID
  - 볼륨 이름
  - SVM 이름
  - SVM의 UUID입니다
  - QoSPolicyUUID입니다
  - QoSPolicyName입니다
  - 용량설치 공간
  - 성능설치 공간
  - TotalFootprint
  - TieringPolicy를 참조하십시오
  - IsProtected 플래그
  - IsDestination 플래그입니다
  - 사용됨
  - PhysicalUsed(PhysicalUsed)
  - CloneParentUUID입니다
  - LogicalSpaceUsedByAfs
- QoS 정책 그룹
  - PolicyGroup을 참조하십시오
  - QoSPolicyUUID입니다
  - 최대 처리량
  - MinThroughput
  - 최대 처리량 IOPS
  - 최대 처리량
  - 최소 처리량 IOPS
  - 최소 처리량
  - IsShared 플래그

- ONTAP 적응형 QoS 정책 그룹
  - QoSPolicyName입니다
  - QoSPolicyUUID입니다
  - PeakIOPS를 참조하십시오
  - PeakIOPSALLOCATION을 참조하십시오
  - 절대 최소 IOPS
  - ExpectedIOPS입니다
  - ExpectedIOPSALLOCATION을 참조하십시오
  - 블록 크기
- 풋프린트
  - SVM
  - 볼륨
  - TotalFootprint
  - VolumeBlocksFootprintBin0
  - VolumeBlocksFootprintBin1
- MetroCluster
  - 마디
  - 집계
  - LIFs
  - 구성 복제
  - 사이
  - 클러스터
  - 볼륨
- MetroCluster 클러스터
  - 클러스터 UUID입니다
  - 클러스터 이름
  - RemoteClusterUUID입니다
  - RemoteCluserName입니다
  - LocalConfigurationState 를 선택합니다
  - RemoteConfigurationState 를 선택합니다
- MetroCluster 노드
  - DR 미러링 상태
  - 클러스터 간 LIF
  - 노드 도달성
  - DR 파트너 노드

    - DR Aux 파트너 노드
    - DR, DR Aux 및 HA 노드 대칭 관계
    - 자동 계획되지 않은 전환
- MetroCluster 구성 복제
    - 원격 하트비트
    - 마지막 하트비트 전송됨
    - 마지막 하트비트 수신
    - Vserver 스트림
    - 클러스터 스트림
    - 스토리지
    - 사용 중인 저장 용량
- MetroCluster 중재자
    - 중재자 주소
    - 중재자 포트
    - 중재자 구성됨
    - 중재자 접근 가능
    - 모드를 선택합니다
- Collector Observablility Metrics(수집기 불임 메트릭)
    - 수집 시간
    - Active IQ Unified Manager API 종점이 쿼리되었습니다
    - 응답 시간입니다
    - 레코드 수입니다
    - AIQUMInstance IP(AIQUMInstance IP)
    - 수집기 인스턴스 ID입니다

ONTAP를 위해 수집된 **** 성능 데이터**:** 자세히 알아보기 ****

다음 목록은 ONTAP에 대해 수집된 성능 데이터의 대표적인 예입니다.

- 클러스터 이름
- 클러스터 UUID
- ObjectID입니다
- 볼륨 이름
- 볼륨 인스턴스 UUID입니다
- SVM
- VserverUUID입니다
- 노드 일련 번호
- ONTAP 버전
- AIQUM 버전
- 집계
- 애그리게이트 UUID입니다
- 리소스 키
- 타임 스탬프입니다
- IOPSPerTb입니다
- 지연 시간
- 읽기 지연 시간
- WriteMBps 를 클릭합니다
- QoSMinThroughut지연 시간
- QoSNBladeLatency
- 중고 헤드룸
- CacheMisssRatio(캐시비율
- 기타 지연 시간
- QoSAgregateLatency를 참조하십시오
- IOPS
- QoSNetworkLetency를 참조하십시오
- 가용성 작업
- 쓰기 대기 시간
- QoSCloud지연 시간
- QoSClusterInterconnectLatency를 참조하십시오
- OtherMBps(OtherMBps)
- QoSCop지연 시간

- QoSDBladeLatency
- 활용률
- 읽기 IOPS
- Mbps
- 기타 IOPS
- QoSPolicyGroupLatency를 참조하십시오
- ReadMBps
- QoSSyncSnap미러지연 시간
- 시스템 수준 데이터
  - 쓰기/읽기/기타/총 IOPS
  - 쓰기/읽기/기타/총 처리량
  - 쓰기/읽기/기타/전체 대기 시간
- 쓰기 IOPS입니다

**** 개인 데이터 액세스를 제한할 때 제거된 항목 목록**:** 자세한 내용 ****

Keystone 수집기에서 * 개인 데이터 제거 * 옵션을 활성화하면 ONTAP에 대해 다음 사용 정보가 제거됩니다. 이 옵션은 기본적으로 활성화되어 있습니다.

- 클러스터 이름
- 클러스터 위치
- 클러스터 담당자
- 노드 이름
- 애그리게이트 이름입니다
- 볼륨 이름
- QoSAdapitivePolicyGroup 이름입니다
- QoSPolicyGroup 이름입니다
- SVM 이름
- 스토리지 LUN 이름입니다
- 애그리게이트 이름
- LogicalUnit 이름입니다
- SVM 이름
- AIQUMInstance IP(AIQUMInstance IP)
- 플랙스클론
- RemoteClusterName(원격 클러스터 이름)

StorageGRID 데이터 수집

StorageGRID에 대해 수집된 **** 사용 데이터**:** 자세히 알아보기 ****

다음 목록은 의 대표적인 예입니다 `Logical Data` StorageGRID를 위해 수집:

- StorageGRID ID입니다
- 계정 ID입니다
- 계정 이름
- 계정 할당량 바이트
- 버킷 이름
- 버킷 객체 수
- 버킷 데이터 바이트

다음 목록은 의 대표적인 예입니다 `Physical Data` StorageGRID를 위해 수집:

- StorageGRID ID입니다
- 노드 ID입니다
- 사이트 ID입니다
- 사이트 이름
- 인스턴스
- StorageGRID 스토리지 사용률 바이트
- StorageGRID 스토리지 활용률 메타데이터 바이트

다음 목록은 대표적인 샘플입니다. `Availability/Uptime Data` StorageGRID 에 대해 수집됨:

- SLA 가동 시간 비율

**** 개인 데이터 액세스를 제한할 때 제거된 항목 목록**:** 자세한 내용 ****

Keystone 수집기에서 * 개인 데이터 제거 * 옵션을 활성화하면 StorageGRID에 대해 다음 사용 정보가 제거됩니다. 이 옵션은 기본적으로 활성화되어 있습니다.

- 계정 이름
- BucketName
- 사이트 이름
- 인스턴스/노드 이름

원격 측정 데이터 수집

** Keystone Collector VM**에서 수집된 원격 측정 데이터**:** 자세히 알아보기****

다음 목록은 Keystone 시스템에서 수집된 원격 측정 데이터의 대표적인 샘플입니다.

- 시스템 정보
  - 운영 체제 이름입니다
  - 운영 체제 버전입니다
  - 운영 체제 ID
  - 시스템 호스트 이름
  - 시스템 기본 IP 주소
- 시스템 리소스 사용량
  - 시스템 가동 시간
  - CPU 코어 수
  - 시스템 부하(1분, 5분, 15분)
  - 총 메모리
  - 여유 메모리
  - 사용 가능한 메모리
  - 공유 메모리
  - 버퍼 메모리
  - 캐시된 메모리
  - 총 스왑
  - 무료 교환
  - 캐시된 스왑
  - 디스크 파일 시스템 이름
  - 디스크 크기입니다
  - 사용된 디스크
  - 디스크 사용 가능
  - 디스크 사용률
  - 디스크 마운트 지점
- 설치된 패키지
- 수집기 구성
- 서비스 로그
  - Keystone 서비스의 서비스 로그

비공개 모드의 **Keystone**

Keystone에 대해 자세히 알아보기(프라이빗 모드)

Keystone은 _private_dark site_라고도 하는 _private_deployment 모드를 제공하여 비즈니스 및 보안 요구사항을 충족합니다. 이 모드는 연결이 제한된 조직에서 사용할 수 있습니다.

NetApp은 인터넷 연결이 제한되거나 없는 환경(다크 사이트라고도 함)에 맞게 조정된 Keystone STaaS를 전문적으로 구현합니다. 보안, 규정 준수 또는 운영 요구 사항으로 인해 외부 통신이 제한된 보안 또는 격리된 환경입니다.

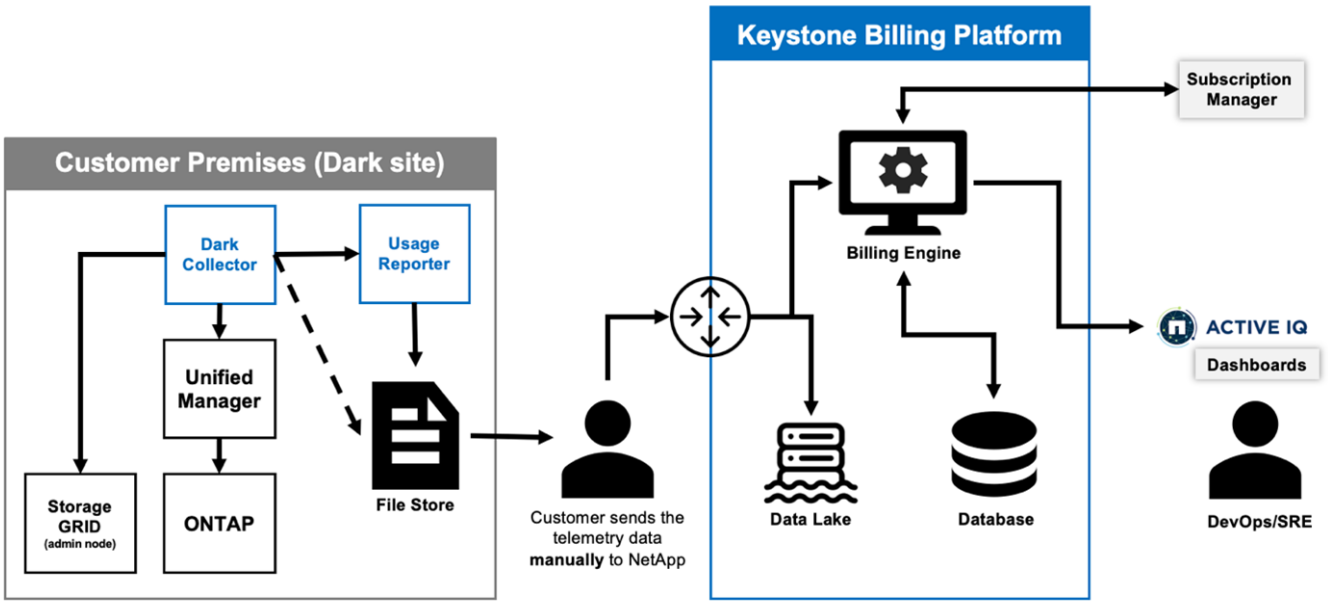
NetApp Keystone의 경우, 다크 사이트에 대한 서비스를 제공하면 이러한 환경의 제약을 존중하는 방식으로 Keystone의 유연한 스토리지 구독 서비스를 제공할 수 있습니다. 여기에는 다음이 포함됩니다.

- * 로컬 배포 *: Keystone은 분리된 환경 내에서 독립적으로 구성될 수 있으므로 인터넷 연결이나 외부 인력이 설치 액세스에 필요하지 않습니다.
- * 오프라인 운영 *: 상태 점검 및 청구 기능이 있는 모든 스토리지 관리 기능을 오프라인으로 사용할 수 있습니다.
- * 보안 및 규정 준수 *: Keystone은 고급 암호화, 보안 액세스 제어 및 세부 감사 기능을 비롯한 다크 사이트의 보안 및 규정 준수 요구 사항을 충족하도록 배포를 보장합니다.
- * 도움말 및 지원 * : NetApp는 지원 및 문제 해결을 위해 각 계정에 할당된 Keystone 성공 전담 관리자를 통해 연중무휴 24시간 글로벌 지원을 제공합니다.

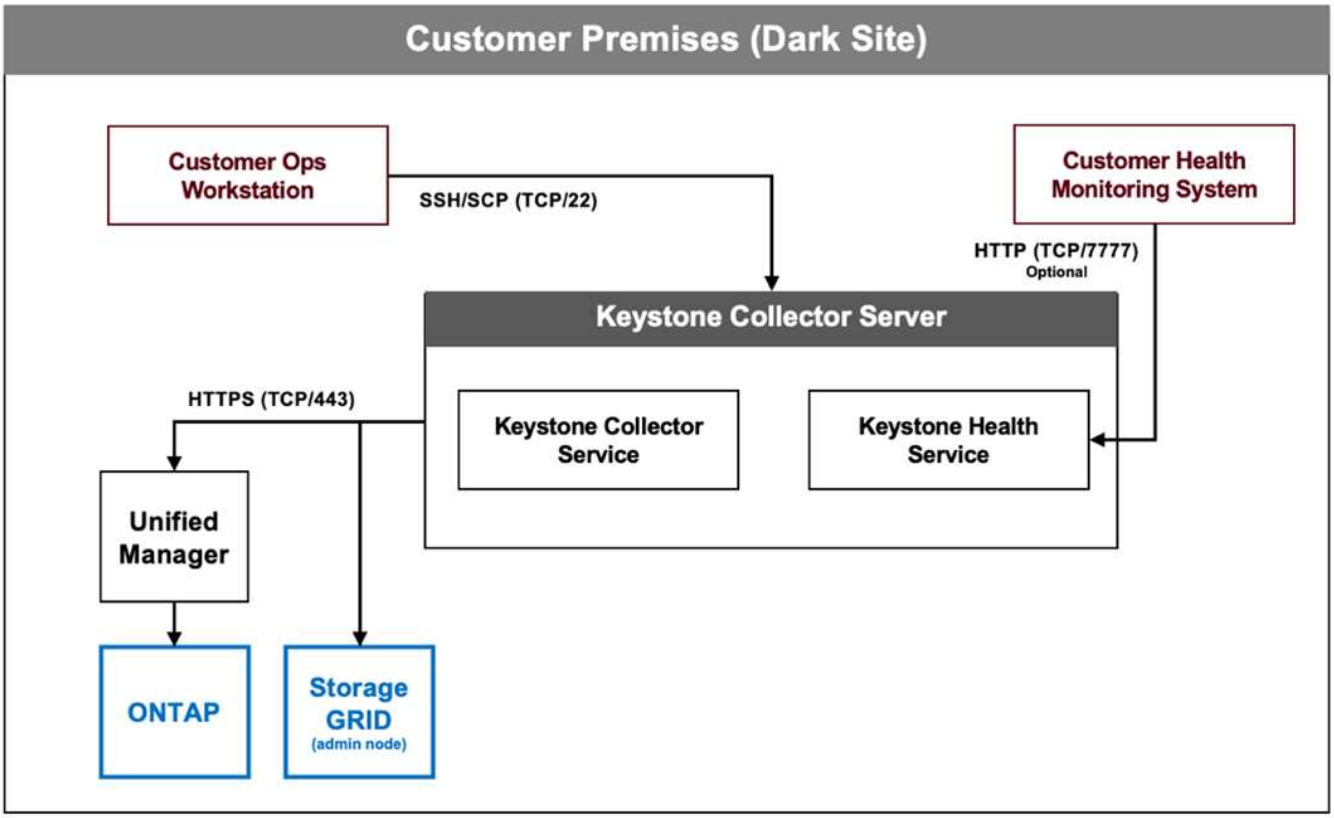
Keystone Collector는 연결 제한 없이 구성할 수 있으며, _STANDARD_MODE라고도 합니다. 자세한 내용은 을 "Keystone Collector에 대해 자세히 알아보십시오"참조하십시오.

개인 모드의 **Keystone Collector**

Keystone Collector는 스토리지 시스템에서 사용량 데이터를 주기적으로 수집하고 메트릭을 오프라인 사용량 리포터 및 로컬 파일 저장소로 내보내는 작업을 담당합니다. 생성된 파일은 암호화된 형식 및 일반 텍스트 형식으로 작성되며 유효성 검사 후 사용자가 수동으로 NetApp에 전달합니다. NetApp의 Keystone 결제 플랫폼은 이러한 파일을 인증 및 처리하여 청구 및 구독 관리 시스템에 통합하여 월별 요금을 계산합니다.



서버의 Keystone Collector 서비스는 주기적으로 사용 데이터를 수집하고, 이 정보를 처리하고, 서버에서 로컬로 사용 파일을 생성하는 업무를 담당합니다. 상태 서비스는 시스템 상태 점검을 수행하며 고객이 사용하는 상태 모니터링 시스템과 연동하도록 설계되었습니다. 이러한 보고서는 사용자가 오프라인에서 액세스할 수 있으므로 유효성 검사를 수행하고 문제를 해결하는 데 도움이 됩니다.



Keystone Collector 비공개 모드 설치를 준비하세요

인터넷에 액세스할 수 없는 환경(예: _ Dark site_ 또는 *private mode*)에 Keystone Collector를 설치하기 전에 시스템이 필요한 소프트웨어를 준비하고 필요한 모든 필수 구성 요소를 충족하는지 확인하십시오.

요구 사항을 충족합니다

- 운영 체제: VMware vCenter Server 및 ESXi 8.0 이상
- 코어: 1 CPU
- RAM: 2GB
- 디스크 공간: 20GB vDisk

Linux에 대한 요구 사항

- 운영 체제(하나 선택):
  - Red Hat Enterprise Linux(RHEL) 8.6 또는 이후 8.x 시리즈
  - Red Hat Enterprise Linux 9.0 이상 버전

    - 데비안 12
- 코어: 2 CPU
- RAM: 4GB
- 디스크 공간: 50GB vDisk
    - 에서 최소 2GB의 여유 공간이 있습니다 `/var/lib/`
    - 최소 48GB의 여유 공간 `/opt/netapp`

또한 동일한 서버에 다음과 같은 타사 패키지가 설치되어 있어야 합니다. 리포지토리를 통해 사용할 수 있는 경우 이러한 패키지는 사전 요구 사항으로 자동으로 설치됩니다.

- RHEL 8.6 이상(8.x)
    - python3>= v3.6.8, python3<= v3.9.13
    - 포더맨
    - SOS(SOS
    - yum-utils입니다
    - python3-dnf-plugin-versionlock 을 참조하십시오
- RHEL 9.0 이상
    - python3 >= v3.9.0, python3 <= v3.9.13
    - 포더맨
    - SOS(SOS
    - yum-utils입니다
    - python3-dnf-plugin-versionlock 을 참조하십시오
- 데비안 v12
    - python3>= v3.9.0, python3<= v3.12.0
    - 포더맨
    - Sosreport(Sosreport

네트워킹 요구 사항

Keystone Collector의 네트워킹 요구 사항은 다음과 같습니다.

- Active IQ Unified Manager(Unified Manager) 9.10 이상, API 게이트웨이 기능이 활성화된 서버에서 구성됩니다.
- Unified Manager 서버는 포트 443(HTTPS)에서 Keystone Collector 서버를 통해 액세스할 수 있어야 합니다.
- Unified Manager 서버에서 Keystone Collector에 대해 애플리케이션 사용자 권한이 있는 서비스 계정을 설정해야 합니다.
- 외부 인터넷 연결이 필요하지 않습니다.
- 매달 Keystone Collector에서 파일을 내보내어 NetApp 지원팀에 이메일로 보내세요. 지원팀에 연락하는 방법에 대한 자세한 내용은 다음을 참조하세요. "Keystone에 대한 도움을 받으십시오".

Keystone Collector를 비공개 모드로 설치합니다

인터넷에 액세스할 수 없는 환경(_Dark site_또는_private mode_라고도 함)에 Keystone Collector를 설치하는 몇 가지 단계를 완료합니다. 이러한 유형의 설치는 보안 사이트에 적합합니다.

요구 사항에 따라 Keystone Collector를 VMware vSphere 시스템에 구축하거나 Linux 시스템에 설치할 수 있습니다. 선택한 옵션에 해당하는 설치 단계를 따릅니다.

VMware vSphere에 구축

다음 단계를 수행하십시오.

1. 에서 OVA 템플릿 파일을 "NetApp Keystone 웹 포털" 다운로드합니다.
2. OVA 파일을 사용하여 Keystone Collector를 구축하는 단계는 섹션을 참조하십시오"OVA 템플릿 배포".

Linux에 설치합니다

Keystone Collector 소프트웨어는 Linux 배포판을 기반으로 제공된 .deb 또는 .rpm 파일을 사용하여 Linux 서버에 설치됩니다.

Linux 서버에 소프트웨어를 설치하려면 다음 단계를 수행하십시오.

1. Keystone Collector 설치 파일을 Linux 서버로 다운로드하거나 전송합니다.

   ```
   keystone-collector-<version>.noarch.rpm
   ```

2. 서버에서 터미널을 열고 다음 명령을 실행하여 설치를 시작합니다.

   - * 데비안 패키지 사용 *

     ```
     dpkg -i keystone-collector_<version>_all.deb
     ```

   - * RPM 파일 사용 *

     ```
     yum install keystone-collector-<version>.noarch.rpm
     ```

     또는

   ```
   rpm -i keystone-collector-<version>.noarch.rpm
   ```

3. `y`패키지를 설치하라는 메시지가 표시되면 를 입력합니다.

Keystone Collector를 비공개 모드로 구성합니다

Keystone Collector가 인터넷에 액세스할 수 없는 환경(예: A_Dark site_ 또는 _private mode_라고도 함)에서 사용 데이터를 수집할 수 있도록 몇 가지 구성 작업을 완료합니다. 필수 구성 요소를 활성화하고 스토리지 환경을 연결하는 일회성 활동입니다. 구성되면 Keystone Collector는 Active IQ Unified Manager에서 관리하는 모든 ONTAP 클러스터를 모니터링합니다.

Keystone Collector는 구성 및 모니터링 작업을 수행할 수 있는 Keystone Collector Management Terminal User Interface(TUI) 유틸리티를 제공합니다. Enter 및 화살표 키와 같은 다양한 키보드 컨트롤을 사용하여 옵션을 선택하고 이 TUI를 탐색할 수 있습니다.

단계

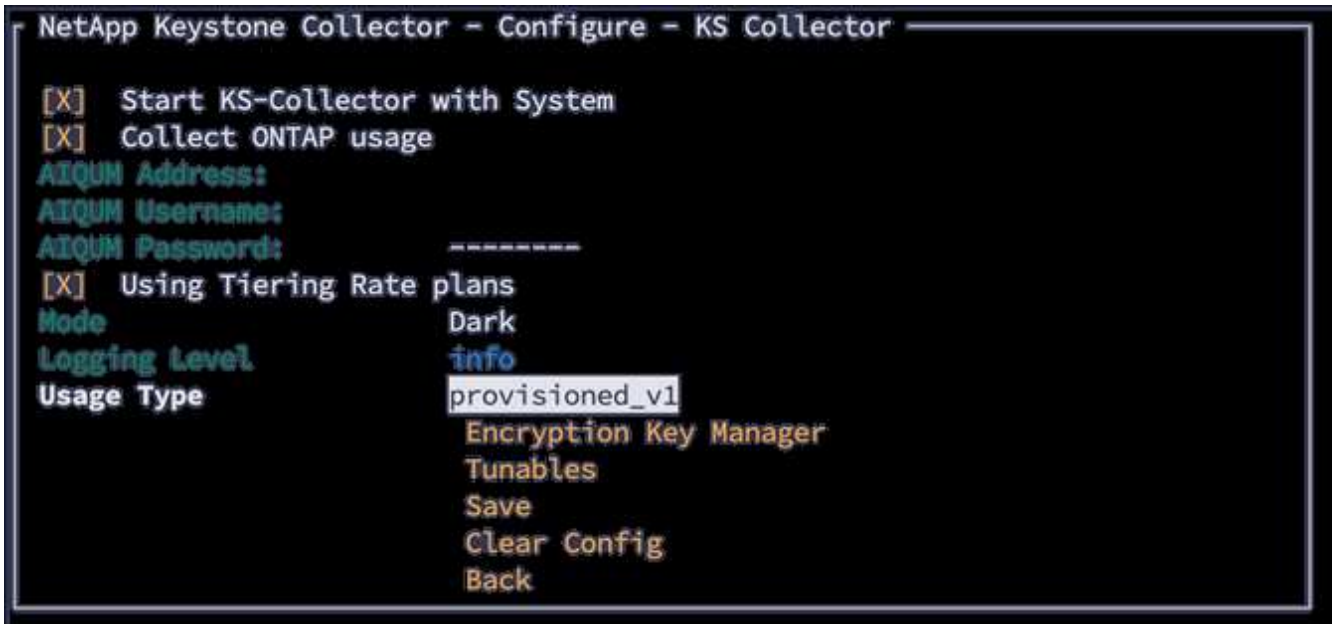
1. Keystone Collector 관리 TUI 유틸리티 시작:

   ```
   keystone-collector-tui
   ```

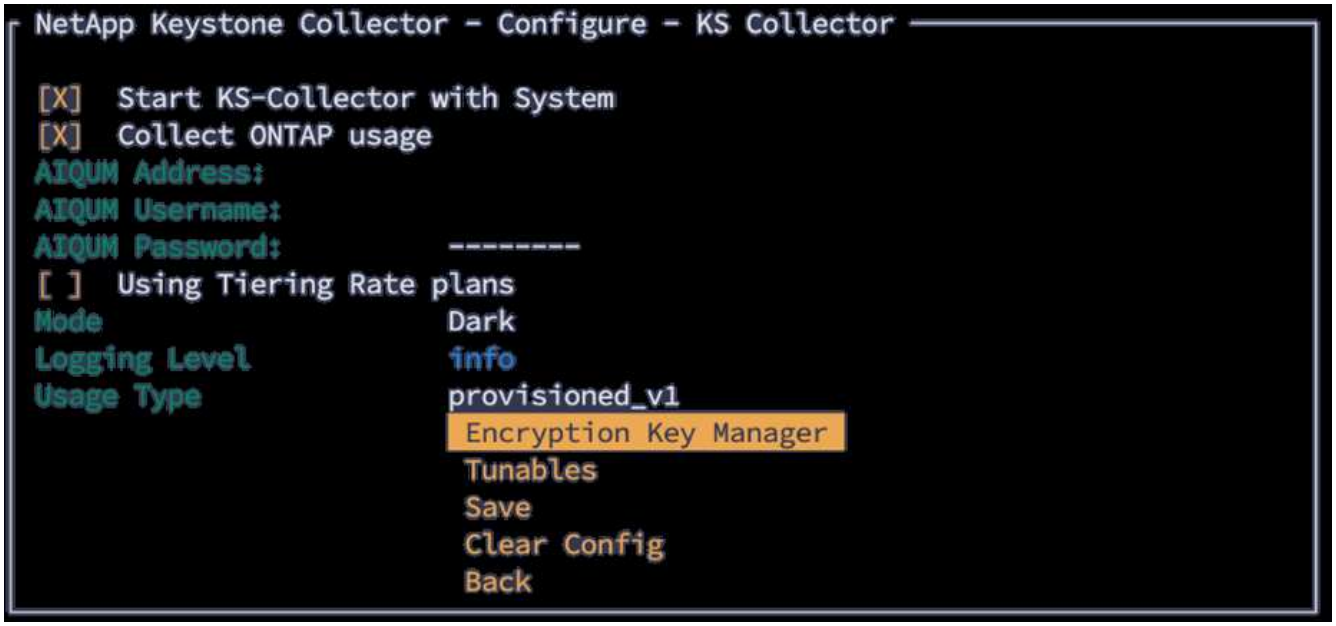
2. 구성 > 고급 * 으로 이동합니다.
3. Darksite Mode * 옵션을 전환합니다.

4. 저장 * 을 선택합니다.
5. Configure > KS-Collector * 로 이동하여 Keystone Collector를 구성합니다.
6. Start KS Collector with System * 필드를 토글합니다.
7. ONTAP 사용량 수집 * 필드를 토글합니다. Active IQ Unified Manager(Unified Manager) 서버 및 사용자 계정의 세부 정보를 추가합니다.
8. * 선택 사항 *: 가입에 데이터 계층화가 필요한 경우 * 계층화 비율 계획 사용 * 필드를 전환합니다.
9. 구매한 구독 유형에 따라 * 사용 유형 * 을 업데이트합니다.

   구성하기 전에 NetApp에서 구독과 연결된 사용 유형을 확인하십시오.



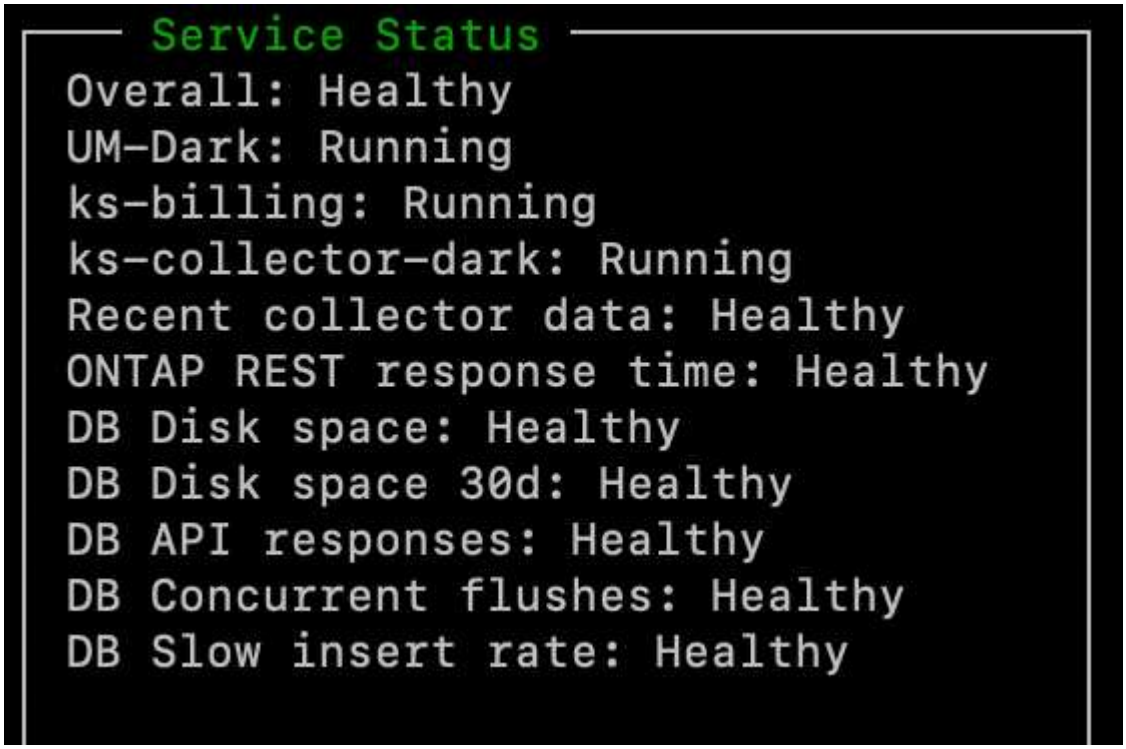
10. 저장 * 을 선택합니다.
11. Configure > KS-Collector * 로 이동하여 Keystone Collector 키페이어를 생성합니다.
12. Encryption Key Manager * 로 이동한 후 Enter 키를 누릅니다.



13. Generate Collector keypair * 를 선택하고 Enter 키를 누릅니다.

14. TUI의 기본 화면으로 돌아가 * 서비스 상태 * 정보를 확인하여 Keystone Collector가 정상 상태인지 확인합니다. 시스템에서 서비스가 * 전체: 정상 * 상태임을 표시해야 합니다. 최대 10분 동안 기다립니다. 이 기간 후에도 전체

상태가 정상 상태가 지속되면 이전 구성 단계를 검토하고 NetApp 지원 팀에 문의하십시오.



15. 기본 화면에서 * Exit to Shell * 옵션을 선택하여 Keystone Collector 관리 TUI를 종료합니다.
16. 생성된 공개 키 검색:

    ```
    ~/collector-public.pem
    ```

17. 보안된 비 USPS 사이트의 경우 이 파일이 포함된 이메일을 ng-keystone-secure-site-upload@netapp.com으로 보내고, 보안된 USPS 사이트의 경우 ng-keystone-secure-site-usps-upload@netapp.com으로 보내세요.

사용 보고서를 내보냅니다

매월 말에 NetApp에 월별 사용량 요약 보고서를 보내야 합니다. 이 보고서를 수동으로 생성할 수 있습니다.

사용 현황 보고서를 생성하려면 다음 단계를 수행하십시오.

1. Keystone Collector TUI 홈 화면의 * Export Usage * 로 이동합니다.
2. 파일을 모아서 보안이 강화된 비 USPS 사이트의 경우 ng-keystone-secure-site-upload@netapp.com으로, 보안이 강화된 USPS 사이트의 경우 ng-keystone-secure-site-usps-upload@netapp.com으로 보내주세요.

   Keystone Collector는 일반 파일과 암호화된 파일을 모두 생성하며, 이 파일은 수동으로 NetApp로 전송되어야 합니다. 지우기 파일 보고서에는 고객이 확인할 수 있는 다음과 같은 세부 정보가 포함됩니다.

```
node_serial,derived_service_level,usage_tib,start,duration_seconds
123456781,extreme,25.0,2024-05-27T00:00:00,86400
123456782,premium,10.0,2024-05-27T00:00:00,86400
123456783,standard,15.0,2024-05-27T00:00:00,86400

<Signature>
31b3d8eb338ee319ef1

-----BEGIN PUBLIC KEY-----
31b3d8eb338ee319ef1
-----END PUBLIC KEY-----
```

ONTAP를 업그레이드합니다

Keystone Collector는 TUI를 통한 ONTAP 업그레이드를 지원합니다.

ONTAP를 업그레이드하려면 다음 단계를 수행하십시오.

1. 유지 관리 > ONTAP 업그레이드 웹 서버 * 로 이동합니다.
2. ONTAP 업그레이드 이미지 파일을 */opt/NetApp/ONTAP-upgrade/ * 로 복사한 다음 * 웹 서버 시작 * 을 선택하여 웹 서버를 시작합니다.

3. `http://<collector-ip>:8000`업그레이드 지원을 받으려면 웹 브라우저 사용 으로 이동하십시오.

Keystone Collector를 다시 시작합니다

TUI를 통해 Keystone Collector 서비스를 다시 시작할 수 있습니다. TUI에서 * 유지 관리 > 수집기 * 서비스 다시 시작으로 이동합니다. 그러면 모든 Collector 서비스가 재부팅되고 해당 상태는 TUI 홈 화면에서 모니터링될 수 있습니다.

개인 모드에서 **Keystone Collector** 상태를 모니터링합니다

HTTP 요청을 지원하는 모니터링 시스템을 사용하여 Keystone Collector의 상태를 모니터링할 수 있습니다.

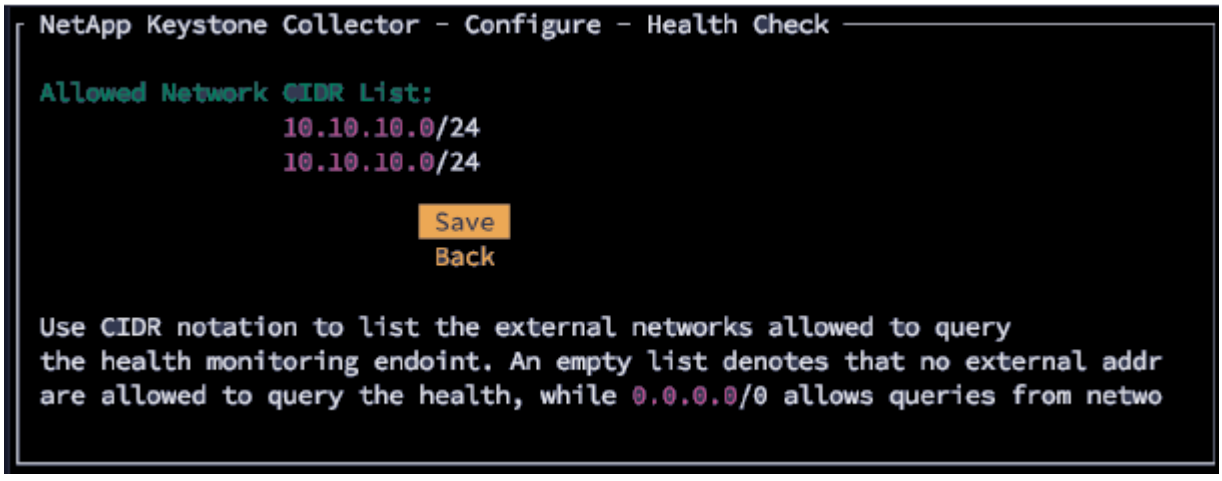
기본적으로 Keystone 상태 서비스는 localhost 이외의 IP로부터의 연결을 허용하지 않습니다. Keystone 상태 엔드포인트는 입니다 `/uber/health`또한 포트에서 `Keystone Collector` 서버의 모든 인터페이스를 수신합니다 `7777`. 쿼리 시 JSON 출력이 있는 HTTP 요청 상태 코드가 끝점에서 응답으로 반환되어 Keystone Collector 시스템의 상태를 설명합니다.
JSON 본체는 에 대한 전반적인 상태를 제공합니다 `is_healthy` 속성, 부울, 에 대한 구성 요소별 상태의 세부 목록 `component_details` 속성.
예를 들면 다음과 같습니다.

```
$ curl http://127.0.0.1:7777/uber/health
{"is_healthy": true, "component_details": {"vicmet": "Running", "ks-
collector": "Running", "ks-billing": "Running", "chronyd": "Running"}}
```

다음 상태 코드가 반환됩니다.

- * 200 *: 모니터링되는 모든 구성 요소가 정상 상태임을 나타냅니다
- * 503 *: 하나 이상의 구성 요소가 정상 상태가 아님을 나타냅니다
- * 403 * : 상태를 쿼리하는 HTTP 클라이언트가 허용되는 네트워크 CIDR 목록인 _allow_list에 없음을 나타냅니다. 이 상태에서는 상태 정보가 반환되지 않습니다.

  allow_list는 네트워크 CIDR 방법을 사용하여 Keystone 상태 시스템을 쿼리할 수 있는 네트워크 디바이스를 제어합니다. 403 오류가 표시되면 * Keystone Collector 관리 TUI > 구성 > 상태 모니터링 * 에서 모니터링 시스템을 _allow_list에 추가합니다.

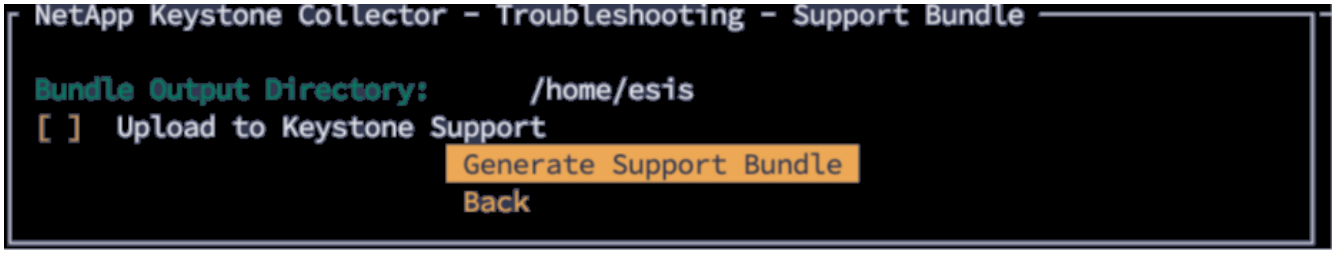


지원 번들을 생성하고 수집합니다

Keystone Collector 관련 문제를 해결하려면 _.tar_file을 요청할 수 있는 NetApp 지원 팀과 상의하십시오. Keystone Collector 관리 TUI 유틸리티를 통해 이 파일을 생성할 수 있습니다.

다음 단계에 따라 _.tar_file을 생성합니다.

1. 문제 해결 > 지원 번들 생성 * 으로 이동합니다.
2. 번들을 저장할 위치를 선택한 다음 * 지원 번들 생성 * 을 클릭합니다.



이 프로세스는 `tar` 문제 해결을 위해 NetApp와 공유할 수 있는 패키지를 언급된 위치에 생성합니다.

3. 파일을 다운로드한 후 Keystone ServiceNow 지원 티켓에 첨부할 수 있습니다. 티켓 발행에 대한 정보는 다음을 참조하세요. "서비스 요청을 생성하는 중입니다".