



# Keystone 설정 및 구성

## Keystone

NetApp  
January 15, 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 Collector 설치	8
VMware vSphere 시스템에 Keystone Collector 배포	8
Linux 시스템에 Keystone Collector 설치	10
Keystone 소프트웨어 자동 검증	12
Keystone Collector 구성	12
Keystone Collector에서 HTTP 프록시 구성	14
개인정보 수집 제한	14
사용자 정의 루트 CA 신뢰	15
성능 서비스 수준 생성	16
ITOM Collector 설치	20
Keystone ITOM Collector 설치 요구 사항	21
Linux 시스템에 Keystone ITOM Collector를 설치하세요	22
Windows 시스템에 Keystone ITOM Collector를 설치하세요	23
Keystone 에 대한 AutoSupport 구성	24
모니터링 및 업그레이드	25
Keystone Collector의 상태를 모니터링합니다	25
Keystone Collector를 수동으로 업그레이드하세요	30
Keystone 콜렉터 보안	32
보안 강화	32
Keystone 수집하는 사용자 데이터 유형	33
ONTAP 데이터 수집	33
StorageGRID 데이터 수집	41
원격 측정 데이터 수집	41
개인 모드의 Keystone	43
Keystone (비공개 모드)에 대해 알아보세요	43
Keystone Collector 비공개 모드 설치를 준비하세요	44
Keystone Collector를 개인 모드로 설치하세요	46
개인 모드에서 Keystone Collector 구성	47
개인 모드에서 Keystone Collector 상태 모니터링	51

# Keystone 설정 및 구성

## 요구 사항

### Keystone Collector의 가상 인프라 요구 사항

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

**Keystone Collector** 서버 **VM**의 필수 구성 요소:

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

### 기타 요구 사항

다음의 일반 요구 사항이 충족되는지 확인하세요.

### 네트워킹 요구 사항

Keystone Collector의 네트워킹 요구 사항은 다음 표에 나와 있습니다.



Keystone Collector를 사용하려면 인터넷 연결이 필요합니다. 기본 게이트웨이(NAT를 통해)를 통한 직접 라우팅이나 HTTP 프록시를 통해 인터넷 연결을 제공할 수 있습니다. 두 가지 변형 모두 여기에 설명되어 있습니다.

원천	목적지	서비스	프로토콜 및 포트	범주	목적
Keystone Collector( Keystone ONTAP 용)	Active IQ Unified Manager (통합 관리자)	HTTPS	TCP 443	필수( Keystone ONTAP 사용하는 경우)	ONTAP 에 대한 Keystone Collector 사용 메트릭 수집
Keystone Collector( Keystone StorageGRID 용)	StorageGRID 관리 노드	HTTPS	TCP 443	필수( Keystone StorageGRID 사용하는 경우)	StorageGRID 대한 Keystone Collector 사용 메트릭 수집
Keystone 컬렉터 (일반)	인터넷(나중에 제공되는 URL 요구 사항에 따라)	HTTPS	TCP 443	필수(인터넷 연결)	Keystone Collector 소프트웨어, OS 업데이트 및 메트릭 업로드

Keystone 컬렉터 (일반)	고객 HTTP 프록시	HTTP 프록시	고객 프록시 포트	필수(인터넷 연결)	Keystone Collector 소프트웨어, OS 업데이트 및 메트릭 업로드
Keystone 컬렉터 (일반)	고객 DNS 서버	DNS	TCP/UDP 53	필수적인	DNS 확인
Keystone 컬렉터 (일반)	고객 NTP 서버	엔티피	UDP 123	필수적인	시간 동기화
Keystone Collector( Keystone ONTAP 용)	통합 관리자	MySQL	TCP 3306	선택적 기능	Keystone Collector에 대한 성능 메트릭 수집
Keystone 컬렉터 (일반)	고객 모니터링 시스템	HTTPS	TCP 7777	선택적 기능	Keystone Collector 상태 보고
고객의 운영 워크스테이션	Keystone 컬렉터	SSH	TCP 22	관리	Keystone Collector Management에 대한 액세스
NetApp ONTAP 클러스터 및 노드 관리 주소	Keystone 컬렉터	HTTP_8000, 핑	TCP 8000, ICMP 에코 요청/응답	선택적 기능	ONTAP 펌웨어 업데이트를 위한 웹 서버



Unified Manager를 새로 설치하는 동안 MySQL의 기본 포트인 3306은 localhost로만 제한되므로 Keystone Collector의 성능 지표 수집이 차단됩니다. 자세한 내용은 다음을 참조하세요. "[ONTAP 요구 사항](#)".

#### URL 접근

Keystone Collector는 다음 인터넷 호스트에 액세스해야 합니다.

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

## Keystone Collector의 Linux 요구 사항

필요한 소프트웨어로 Linux 시스템을 준비하면 Keystone Collector가 정확하게 설치되고

데이터를 수집할 수 있습니다.

Linux 및 Keystone Collector 서버 VM에 다음 구성이 있는지 확인하세요.

리눅스 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 환경에만 해당)
- 크로니드 시간 동기화
- 표준 Linux 소프트웨어 저장소에 액세스

동일한 서버에는 다음과 같은 타사 패키지도 있어야 합니다.

- 포드맨(POD 매니저)
- 위급 신호
- 만성
- 파이썬 3(3.9.14~3.11.8)

**Keystone Collector 서버 VM:**

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

기타 요구 사항

다음의 일반 요구 사항이 충족되는지 확인하세요.

네트워킹 요구 사항

Keystone Collector의 네트워킹 요구 사항은 다음 표에 나와 있습니다.



Keystone Collector를 사용하려면 인터넷 연결이 필요합니다. 기본 게이트웨이(NAT를 통해)를 통한 직접 라우팅이나 HTTP 프록시를 통해 인터넷 연결을 제공할 수 있습니다. 두 가지 변형 모두 여기에 설명되어 있습니다.

원천	목적지	서비스	프로토콜 및 포트	범주	목적
Keystone Collector(Keystone ONTAP 용)	Active IQ Unified Manager (통합 관리자)	HTTPS	TCP 443	필수( Keystone ONTAP 사용하는 경우)	ONTAP 에 대한 Keystone Collector 사용 메트릭 수집

Keystone Collector( Keystone StorageGRID 용)	StorageGRID 관리 노드	HTTPS	TCP 443	필수( Keystone StorageGRID 사용하는 경우)	StorageGRID 대한 Keystone Collector 사용 메트릭 수집
Keystone 컬렉터 (일반)	인터넷(나중에 제공되는 URL 요구 사항에 따라)	HTTPS	TCP 443	필수(인터넷 연결)	Keystone Collector 소프트웨어, OS 업데이트 및 메트릭 업로드
Keystone 컬렉터 (일반)	고객 HTTP 프록시	HTTP 프록시	고객 프록시 포트	필수(인터넷 연결)	Keystone Collector 소프트웨어, OS 업데이트 및 메트릭 업로드
Keystone 컬렉터 (일반)	고객 DNS 서버	DNS	TCP/UDP 53	필수적인	DNS 확인
Keystone 컬렉터 (일반)	고객 NTP 서버	엔티피	UDP 123	필수적인	시간 동기화
Keystone Collector( Keystone ONTAP 용)	통합 관리자	MySQL	TCP 3306	선택적 기능	Keystone Collector에 대한 성능 메트릭 수집
Keystone 컬렉터 (일반)	고객 모니터링 시스템	HTTPS	TCP 7777	선택적 기능	Keystone Collector 상태 보고
고객의 운영 워크스테이션	Keystone 컬렉터	SSH	TCP 22	관리	Keystone Collector Management에 대한 액세스
NetApp ONTAP 클러스터 및 노드 관리 주소	Keystone 컬렉터	HTTP_8000, 핑	TCP 8000, ICMP 에코 요청/응답	선택적 기능	ONTAP 펌웨어 업데이트를 위한 웹 서버



Unified Manager를 새로 설치하는 동안 MySQL의 기본 포트인 3306은 localhost로만 제한되므로 Keystone Collector의 성능 지표 수집이 차단됩니다. 자세한 내용은 다음을 참조하세요. ["ONTAP 요구 사항"](#).

#### URL 접근

Keystone Collector는 다음 인터넷 호스트에 액세스해야 합니다.

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

## Keystone 의 ONTAP 및 StorageGRID 요구 사항

Keystone 시작하기 전에 ONTAP 클러스터와 StorageGRID 시스템이 몇 가지 요구 사항을 충족하는지 확인해야 합니다.

## ONTAP

소프트웨어 버전

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

시작하기 전에

ONTAP 통해서만 사용 데이터를 수집하려는 경우 다음 요구 사항을 충족하세요.

1. ONTAP 9.8 이상이 구성되어 있는지 확인하세요. 새 클러스터 구성에 대한 자세한 내용은 다음 링크를 참조하세요.
  - ["System Manager를 사용하여 새 클러스터에 ONTAP 구성"](#)
  - ["CLI로 클러스터 설정"](#)
2. 특정 역할이 있는 ONTAP 로그인 계정을 만듭니다. 자세한 내용은 다음을 참조하세요. ["ONTAP 로그인 계정 생성에 대해 알아보세요"](#).
  - 웹 UI
    - i. 기본 자격 증명을 사용하여 ONTAP 시스템 관리자에 로그인합니다. 자세한 내용은 다음을 참조하세요. ["System Manager를 사용한 클러스터 관리"](#).
    - ii. "읽기 전용" 역할과 "http" 애플리케이션 유형을 가진 ONTAP 사용자를 만들고, \*클러스터 > 설정 > 보안 > 사용자\*로 이동하여 암호 인증을 활성화합니다.
  - CLI
    - i. 기본 자격 증명을 사용하여 ONTAP CLI에 로그인합니다. 자세한 내용은 다음을 참조하세요. ["CLI를 사용한 클러스터 관리"](#).
    - ii. "읽기 전용" 역할과 "http" 애플리케이션 유형을 가진 ONTAP 사용자를 생성하고, 비밀번호 인증을 활성화합니다. 인증에 대해 자세히 알아보려면 다음을 참조하세요. ["ONTAP 계정 비밀번호 액세스 활성화"](#).

Active IQ Unified Manager 통해 사용 데이터를 수집하려면 다음 요구 사항을 충족해야 합니다.

1. Unified Manager 9.10 이상이 구성되어 있는지 확인하세요. Unified Manager 설치에 대한 자세한 내용은 다음 링크를 참조하세요.
  - ["VMware vSphere 시스템에 Unified Manager 설치"](#)
  - ["Linux 시스템에 Unified Manager 설치"](#)
2. ONTAP 클러스터가 Unified Manager에 추가되었는지 확인하세요. 클러스터 추가에 대한 정보는 다음을 참조하세요. ["클러스터 추가"](#).
3. 사용 및 성능 데이터 수집을 위한 특정 역할을 가진 Unified Manager 사용자를 만듭니다. 다음 단계를 수행하세요. 사용자 역할에 대한 정보는 다음을 참조하세요. ["사용자 역할의 정의"](#).
  - a. 설치 중에 생성된 기본 애플리케이션 관리자 사용자 자격 증명을 사용하여 Unified Manager 웹 UI에 로그인합니다. 보다 ["Unified Manager 웹 UI에 액세스하기"](#).
  - b. Keystone Collector에 대한 서비스 계정을 만듭니다. Operator 사용자 역할. Keystone Collector 서비스 API는 이 서비스 계정을 사용하여 Unified Manager와 통신하고 사용 데이터를 수집합니다. 보다 ["사용자 추가"](#).
  - c. 생성하다 Database 사용자 계정과 함께 Report Schema 역할. 이 사용자는 성과 데이터 수집에



필요합니다. 보다 "[데이터베이스 사용자 생성](#)".



Unified Manager를 새로 설치하는 동안 MySQL의 기본 포트인 3306은 localhost로만 제한되므로 Keystone ONTAP 에 대한 성능 데이터 수집이 차단됩니다. 이 구성은 수정될 수 있으며, 연결을 다른 호스트에 사용할 수 있습니다. Control access to MySQL port 3306 Unified Manager 유지 관리 콘솔의 옵션입니다. 자세한 내용은 다음을 참조하세요. "[추가 메뉴 옵션](#)".

4. Unified Manager에서 API Gateway를 활성화합니다. Keystone Collector는 API Gateway 기능을 사용하여 ONTAP 클러스터와 통신합니다. 웹 UI에서 API Gateway를 활성화하거나 Unified Manager CLI를 통해 몇 가지 명령을 실행하여 API Gateway를 활성화할 수 있습니다.

#### 웹 UI

Unified Manager 웹 UI에서 API Gateway를 활성화하려면 Unified Manager 웹 UI에 로그인하고 API Gateway를 활성화하세요. 자세한 내용은 다음을 참조하세요. "[API 게이트웨이 활성화](#)".

#### CLI

Unified Manager CLI를 통해 API Gateway를 활성화하려면 다음 단계를 따르세요.

- a. Unified Manager 서버에서 SSH 세션을 시작하고 Unified Manager CLI에 로그인합니다.  
`um cli login -u <umadmin>` CLI 명령에 대한 정보는 다음을 참조하세요. "[지원되는 Unified Manager CLI 명령](#)".
- b. API Gateway가 이미 활성화되어 있는지 확인하세요.  
`um option list api.gateway.enabled` 에이 true 값은 API Gateway가 활성화되었음을 나타냅니다.
- c. 반환된 값이 다음과 같은 경우 false , 다음 명령을 실행하세요:  
`um option set api.gateway.enabled=true`
- d. Unified Manager 서버를 다시 시작합니다.
  - 리눅스: "[Unified Manager 다시 시작](#)".
  - VMware vSphere: "[Unified Manager 가상 머신 다시 시작](#)".

#### StorageGRID

StorageGRID 에 Keystone Collector를 설치하려면 다음 구성이 필요합니다.

- StorageGRID 11.6.0 또는 나중에 설치해야 합니다. StorageGRID 업그레이드에 대한 정보는 다음을 참조하세요. "[StorageGRID 소프트웨어 업그레이드: 개요](#)".
- 사용 데이터 수집을 위해 StorageGRID 로컬 관리자 사용자 계정을 만들어야 합니다. 이 서비스 계정은 Keystone Collector 서비스가 관리자 노드 API를 통해 StorageGRID 와 통신하는 데 사용됩니다.

#### 단계

- a. 그리드 관리자에 로그인합니다. 보다 "[그리드 관리자에 Sign in](#)".
- b. 로컬 관리자 그룹을 만듭니다. Access mode: Read-only . 보다 "[관리자 그룹 만들기](#)".
- c. 다음 권한을 추가하세요.
  - 세입자 계정
  - 유지
  - 메트릭 쿼리

d. Keystone 서비스 계정 사용자를 생성하고 이를 관리자 그룹과 연결합니다. 보다 "[사용자 관리](#)".

## Keystone Collector 설치

### VMware vSphere 시스템에 Keystone Collector 배포

VMware vSphere 시스템에 Keystone Collector를 배포하려면 OVA 템플릿을 다운로드하고, **OVF** 템플릿 배포 마법사를 사용하여 템플릿을 배포하고, 인증서의 무결성을 확인하고, VM의 준비 상태를 확인해야 합니다.

#### OVA 템플릿 배포

다음 단계를 따르세요.

##### 단계

1. OVA 파일을 다운로드하세요 "[이 링크](#)" VMware vSphere 시스템에 저장합니다.
2. VMware vSphere 시스템에서 **VM** 및 템플릿 보기로 이동합니다.
3. 가상 머신(VM)(또는 VM 폴더를 사용하지 않는 경우 데이터 센터)에 필요한 폴더를 마우스 오른쪽 버튼으로 클릭하고 \*OVF 템플릿 배포\*를 선택합니다.
4. **OVF** 템플릿 배포 마법사의 \_1단계\_에서 \*OVF 템플릿 선택\*을 클릭하여 다운로드한 템플릿을 선택합니다. KeystoneCollector-latest.ova 파일.
5. 2단계에서는 VM 이름을 지정하고 VM 폴더를 선택합니다.
6. 3단계에서는 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. 다음 단계를 따르세요. Resolution 이 지식 기반(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.

### Deploy OVF Template

- Select an OVF template
- Select a name and folder
- Select a compute resource
- Review details**
- Select storage
- Select networks
- Customize template
- Ready to complete

### Review details

Verify the template details.

Publisher	<a href="#">Sectigo Public Code Signing CA R36</a> (Trusted certificate)
Product	<a href="#">Keystone-Collector</a>
Version	3.12.31910
Vendor	<a href="#">NetApp</a>
Download size	1.7 GB
Size on disk	3.9 GB (thin provisioned) 19.5 GB (thick provisioned)

CANCEL
BACK
NEXT

- OVF** 템플릿 배포 마법사의 5단계에서 VM을 저장할 위치를 지정합니다.
- 6단계에서는 VM이 사용할 대상 네트워크를 선택합니다.
- 7단계 템플릿 사용자 지정\_에서 관리자 사용자 계정의 초기 네트워크 주소와 비밀번호를 지정합니다.



관리자 비밀번호는 vCenter에 가역 형식으로 저장되며 VMware vSphere 시스템에 처음 액세스하기 위한 부트스트랩 자격 증명으로 사용해야 합니다. 초기 소프트웨어 구성 중에 이 관리자 비밀번호를 변경해야 합니다. IPv4 주소에 대한 서브넷 마스크는 CIDR 표기법으로 제공해야 합니다. 예를 들어, 서브넷 마스크가 255.255.255.0인 경우 값 24를 사용합니다.

- OVF** 템플릿 배포 마법사의 8단계 완료 준비\_에서 구성을 검토하고 OVA 배포에 대한 매개변수를 올바르게 설정했는지 확인합니다.

VM이 템플릿에서 배포되고 전원이 켜진 후 VM에 대한 SSH 세션을 열고 임시 관리자 자격 증명으로 로그인하여 VM이 구성할 준비가 되었는지 확인합니다.

#### 초기 시스템 구성

OVA를 통해 배포된 Keystone Collector 서버의 초기 구성을 위해 VMware vSphere 시스템에서 다음 단계를 수행하세요.



배포가 완료되면 Keystone Collector Management Terminal User Interface(TUI) 유틸리티를 사용하여 구성 및 모니터링 활동을 수행할 수 있습니다. Enter 키와 화살표 키 등 다양한 키보드 컨트롤을 사용하여 옵션을 선택하고 이 TUI를 탐색할 수 있습니다.

- Keystone Collector 서버에 SSH 세션을 엽니다. 연결하면 시스템에서 관리자 비밀번호를 업데이트하라는

메시지가 표시됩니다. 필요에 따라 관리자 비밀번호 업데이트를 완료하세요.

2. 새로운 비밀번호로 로그인하여 TUI에 접속하세요. 로그인하면 TUI가 나타납니다.

또는 다음을 실행하여 수동으로 시작할 수 있습니다. `keystone-collector-tui` CLI 명령.

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

## Linux 시스템에 **Keystone Collector** 설치

RPM이나 Debian 패키지를 사용하여 Linux 서버에 Keystone Collector 소프트웨어를 설치할 수 있습니다. Linux 배포판에 따라 설치 단계를 따르세요.

## RPM 사용

1. Keystone Collector 서버에 SSH하고 elevate합니다. root 특권.
2. Keystone 공개 서명을 가져옵니다.  

```
# rpm --import https://keystone.netapp.com/rep01/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/rep01/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 설치하세요.  

```
# yum install keystonerepo.rpm
```
7. Keystone 저장소가 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 사용

1. Keystone Collector 서버에 SSH하고 elevate합니다. root 특권.  

```
sudo su
```
2. 다운로드 keystone-sw-repo.deb 파일:  

```
curl -O https://keystone.netapp.com/downloads/keystone-sw-repo.deb
```
3. Keystone 소프트웨어 저장소 파일을 설치하세요:  

```
# dpkg -i keystone-sw-repo.deb
```
4. 패키지 목록을 업데이트하세요:  

```
# apt-get update
```
5. Keystone repo가 설치되면 keystone-collector 패키지를 설치하세요.  

```
# apt-get install keystone-collector
```



설치가 완료되면 Keystone Collector Management Terminal User Interface(TUI) 유틸리티를 사용하여 구성 및 모니터링 활동을 수행할 수 있습니다. Enter 키와 화살표 키 등 다양한 키보드 컨트롤을 사용하여 옵션을 선택하고 이 TUI를 탐색할 수 있습니다. 보다 "[Keystone Collector 구성](#)" 그리고 "[시스템 상태 모니터링](#)" 정보를 위해.

## Keystone 소프트웨어 자동 검증

Keystone 저장소는 Keystone 소프트웨어의 무결성을 자동으로 검증하도록 구성되어 있어 유효하고 정품 소프트웨어만 귀하의 사이트에 설치됩니다.

Keystone YUM 저장소 클라이언트 구성은 다음과 같습니다. `keystonerepo.rpm` 강제 GPG 검사를 활용합니다 (`gpgcheck=1`) 이 저장소를 통해 다운로드한 모든 소프트웨어에 적용됩니다. Keystone 저장소를 통해 다운로드한 RPM 중 서명 검증에 실패한 경우 설치가 불가능합니다. 이 기능은 Keystone Collector의 예약된 자동 업데이트 기능에서 사용되어 귀하의 사이트에 유효하고 정품 소프트웨어만 설치되도록 보장합니다.

## Keystone Collector 구성

Keystone Collector가 스토리지 환경에서 사용 데이터를 수집할 수 있도록 하려면 몇 가지 구성 작업을 완료해야 합니다. 이는 필요한 구성 요소를 활성화하고 스토리지 환경과 연결하기 위한 일회성 활동입니다.



- Keystone Collector는 구성 및 모니터링 활동을 수행하기 위한 Keystone Collector 관리 터미널 사용자 인터페이스(TUI) 유틸리티를 제공합니다. Enter 키와 화살표 키 등 다양한 키보드 컨트롤을 사용하여 옵션을 선택하고 이 TUI를 탐색할 수 있습니다.
- Keystone Collector는 인터넷 접속이 불가능한 조직, 즉 다크 사이트 또는 \_프라이빗 모드\_에 맞게 구성할 수 있습니다. 자세한 내용은 다음을 참조하세요. "[개인 모드의 Keystone](#)".

단계

1. Keystone Collector 관리 TUI 유틸리티를 시작합니다.  
`$ keystone-collector-tui`
2. 구성 > **KS-Collector**로 이동하여 Keystone Collector 구성 화면을 열고 업데이트에 사용할 수 있는 옵션을 확인하세요.
3. 필요한 옵션을 업데이트합니다.

### <strong> ONTAP 용</strong>

- \* ONTAP 사용량 수집\*: 이 옵션을 사용하면 ONTAP 에 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 ONTAP 에 대한 성능 데이터를 수집할 수 있습니다. 이 기능은 기본적으로 비활성화되어 있습니다. SLA 목적으로 환경에서 성능 모니터링이 필요한 경우 이 옵션을 활성화합니다. Unified Manager Database 사용자 계정 세부 정보를 제공합니다. 데이터베이스 사용자 생성에 대한 정보는 다음을 참조하세요. "[Unified Manager 사용자 만들기](#)".
- 개인 정보 삭제: 이 옵션은 고객의 특정 개인 정보를 삭제하며 기본적으로 활성화되어 있습니다. 이 옵션이 활성화된 경우 메트릭에서 제외되는 데이터에 대한 자세한 내용은 다음을 참조하세요. "[개인정보 수집 제한](#)".

## <strong> StorageGRID 용</strong>

- \* StorageGRID 사용량 수집\*: 이 옵션을 사용하면 노드 사용 세부 정보를 수집할 수 있습니다. StorageGRID 노드 주소와 사용자 세부 정보를 추가합니다.
- 개인 정보 삭제: 이 옵션은 고객의 특정 개인 정보를 삭제하며 기본적으로 활성화되어 있습니다. 이 옵션이 활성화된 경우 메트릭에서 제외되는 데이터에 대한 자세한 내용은 다음을 참조하세요. "[개인정보 수집 제한](#)".

4. 시스템으로 **KS-Collector** 시작 필드를 전환합니다.

5. 저장을 클릭합니다

```
NetApp Keystone Collector - Configure - KS Collector

[X] Start KS-Collector with System
[X] Collect ONTAP usage
AIQUM Address: 123.123.123.123
AIQUM Username: collector-user
AIQUM Password: -----
[X] Collect StorageGRID usage
StorageGRID Address: sgadminnode.address
StorageGRID Username: collector-user
StorageGRID Password: -----
[X] Collect ONTAP Performance Data
AIQUM Database Username: sla-reporter
AIQUM Database Password: -----
[X] Remove Private Data
Mode Standard
Logging Level info
Tunables
Save
Clear Config
Back
```

6. TUI의 메인 화면으로 돌아가서 서비스 상태 정보를 확인하여 Keystone Collector가 정상 상태인지 확인하세요. 시스템은 서비스가 전반적으로: 양호 상태를 표시해야 합니다

```
Service Status
Overall: Healthy
UM: Running
chronyd: Running
ks-collector: Running
```

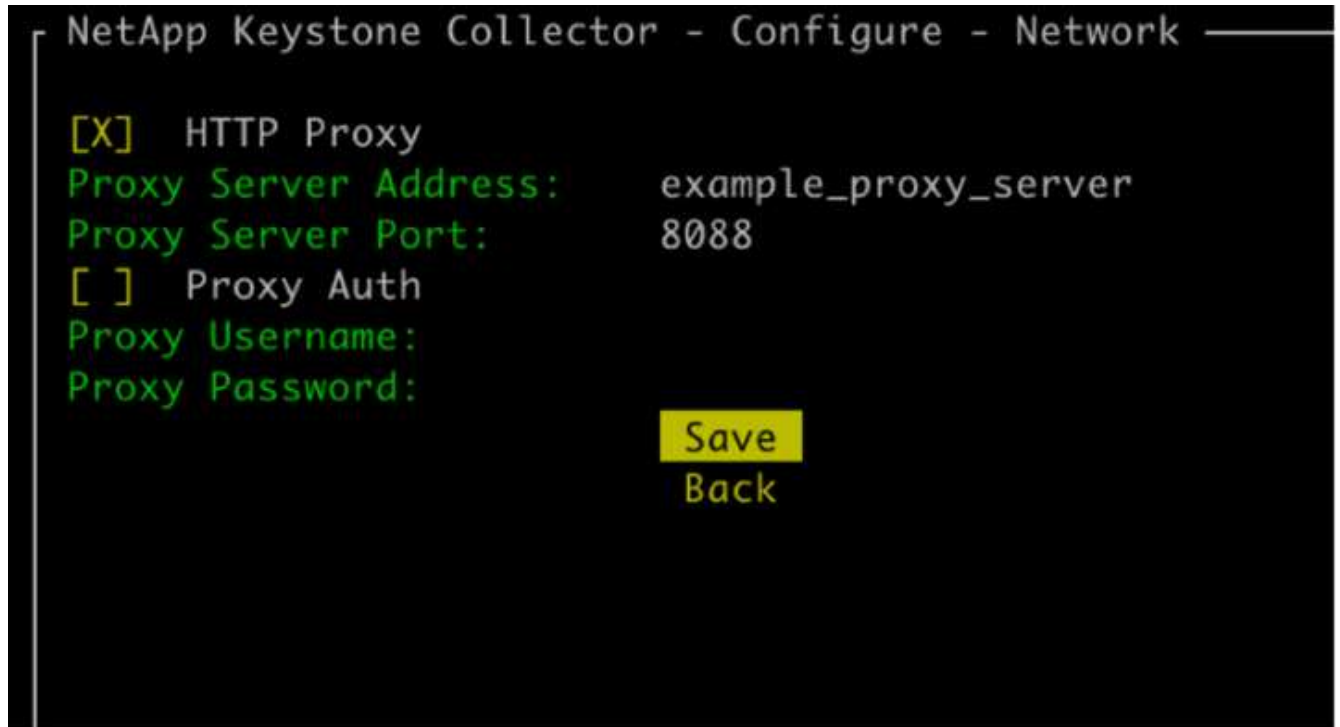
7. 홈 화면에서 셸로 종료 옵션을 선택하여 Keystone Collector 관리 TUI를 종료합니다.

## Keystone Collector에서 HTTP 프록시 구성

Collector 소프트웨어는 HTTP 프록시를 사용하여 인터넷과 통신하는 것을 지원합니다. 이는 TUI에서 구성할 수 있습니다.

단계

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



## 개인정보 수집 제한

Keystone Collector는 구독 측정을 수행하는 데 필요한 제한된 구성, 상태 및 성능 정보를 수집합니다. 업로드된 콘텐츠에서 민감한 정보를 마스킹하여 수집되는 정보를 더욱 제한하는 옵션이 있습니다. 이는 청구 계산에 영향을 미치지 않습니다. 그러나 정보를 제한하면 사용자가 쉽게 식별할 수 있는 볼륨 이름 등의 일부 요소가 UUID로 대체되므로 보고 정보의 유용성에 영향을 줄 수 있습니다.

특정 고객 데이터 수집을 제한하는 것은 Keystone Collector TUI 화면에서 구성 가능한 옵션입니다. 이 옵션인 \*개인 데이터 제거\*는 기본적으로 활성화되어 있습니다.



```
NetApp Keystone Collector - Configure - KS Collector

[X] Start KS-Collector with System
[X] Collect ONTAP usage
AIQUM Address:      123.123.123.123
AIQUM Username:     collector
AIQUM Password:     -----
[ ] Collect StorageGRID usage

[ ] Collect ONTAP Performance Data

[X] Remove Private Data
Mode               Standard
Logging Level      info
                   Tunables
                   Save
                   Clear Config
                   Back
```

ONTAP 및 StorageGRID 에서 개인 데이터 액세스 제한에 대해 제거된 항목에 대한 정보는 다음을 참조하세요."개인 데이터 접근 제한에서 제거된 항목 목록".

### 사용자 정의 루트 CA 신뢰

공개 루트 인증 기관(CA)에 대한 인증서 검증은 Keystone Collector 보안 기능의 일부입니다. 하지만 필요한 경우 Keystone Collector를 구성하여 사용자 정의 루트 CA를 신뢰하도록 할 수 있습니다.

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

단계

1. CA 인증서를 준비합니다. *base64*로 인코딩된 *X.509* 파일 형식이어야 합니다.



지원되는 파일 확장자는 다음과 같습니다. *.pem* , *.crt* , *.cert* . 인증서가 다음 형식 중 하나인지 확인하세요.

2. 인증서를 Keystone Collector 서버로 복사합니다. 파일이 복사된 위치를 기록해 두세요.
3. 서버에서 터미널을 열고 관리 TUI 유틸리티를 실행합니다.  
\$ keystone-collector-tui
4. \*구성 > 고급\*으로 이동합니다.
5. 사용자 정의 루트 인증서 사용 옵션을 활성화합니다.
6. \*사용자 지정 루트 인증서 경로 선택:\*에서 다음을 선택하세요. - Unset -

7. Enter 키를 누르세요. 인증서 경로를 선택하기 위한 대화 상자가 표시됩니다.
8. 파일 시스템 브라우저에서 루트 인증서를 선택하거나 정확한 경로를 입력하세요.
9. Enter 키를 누르세요. 고급 화면으로 돌아갑니다.
10. \*저장\*을 선택하세요. 구성이 적용됩니다.



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

```
NetApp Keystone Collector - Configure - Advanced
[ ] Darksite Mode
[X] TLS Verify on Connections to Internet
[X] Enable custom root certificate
Select custom root certificate path:
    - Unset -
[X] Finished Initial OVA Install
[X] Collector Auto-Update
    Override Collector Images
    Save
    Back
```

## 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 대해 자세히 알아보려면 다음을 참조하세요. "[성능 서비스 수준](#)".

서비스 수준에 대해 자세히 알아보려면 다음을 참조하세요. "[Keystone 의 서비스 수준](#)".

### 단계

1. Keystone Collector 관리 TUI 유틸리티를 시작합니다.  
\$ keystone-collector-tui
2. \*구성>AIQUM\*으로 가서 AIQUM 화면을 엽니다.
3. **AIQUM** 성능 프로필 만들기 옵션을 활성화합니다.

4. Active IQ Unified Manager 서버와 사용자 계정의 세부 정보를 입력하세요. 이러한 세부정보는 PSL을 생성하는 데 필요하며 저장되지 않습니다.

NetApp Keystone Collector – Configure – AIQUM

[ ]

Enable Embedded UM

[X]

Create AIQUM Performance Profiles

AIQUM Address:

AIQUM Username:

AIQUM Password:

Select Keystone version

Select Keystone Service Levels

-unset-

Save

Back

Provide the details of the AIQUM server and user account.

These details are required to create the Performance Service Levels

in the specified AIQUM server and will not be stored.

5. \* Keystone 버전 선택\*을 선택하려면 -unset- .
6. Enter 키를 누르세요. Keystone 버전을 선택하는 대화 상자가 표시됩니다.
7. Keystone STaaS에 대한 Keystone 버전을 지정하려면 \*STaaS\*를 강조 표시한 다음 Enter를 누릅니다.

NetApp Keystone Collector – Configure – AIQUM

AIQUM Ad

AIQUM Us

AIQUM Pa

Select K

Select K

Select Keystone version

KFS

STaaS

Save

Back

Provide the details of the AIQUM server and user account.  
 These details are required to create the Performance Service Levels  
 in the specified AIQUM server and will not be stored.



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](#)".

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



## Performance Service Levels ?

View and manage the Performance Service Levels that you can assign to workloads.

[Filter](#)
[+ Add](#) [✎ Modify](#) [🗑 Remove](#)


<input type="checkbox"/>	Name	Type	Expected IOPS/TB	Peak IOPS/TB	Absolute Minim...	Expected Latency	Capacity	Workloads
<input checked="" type="checkbox"/>	Extreme - KFS	User-defined	6144	12288	1000	1	Used: 0 bytes Available: 283.85 TiB	0
<input checked="" type="checkbox"/>	Extreme - KS-STaaS	User-defined	6144	12288	1000	1	Used: 0 bytes Available: 283.85 TiB	0

### Overview

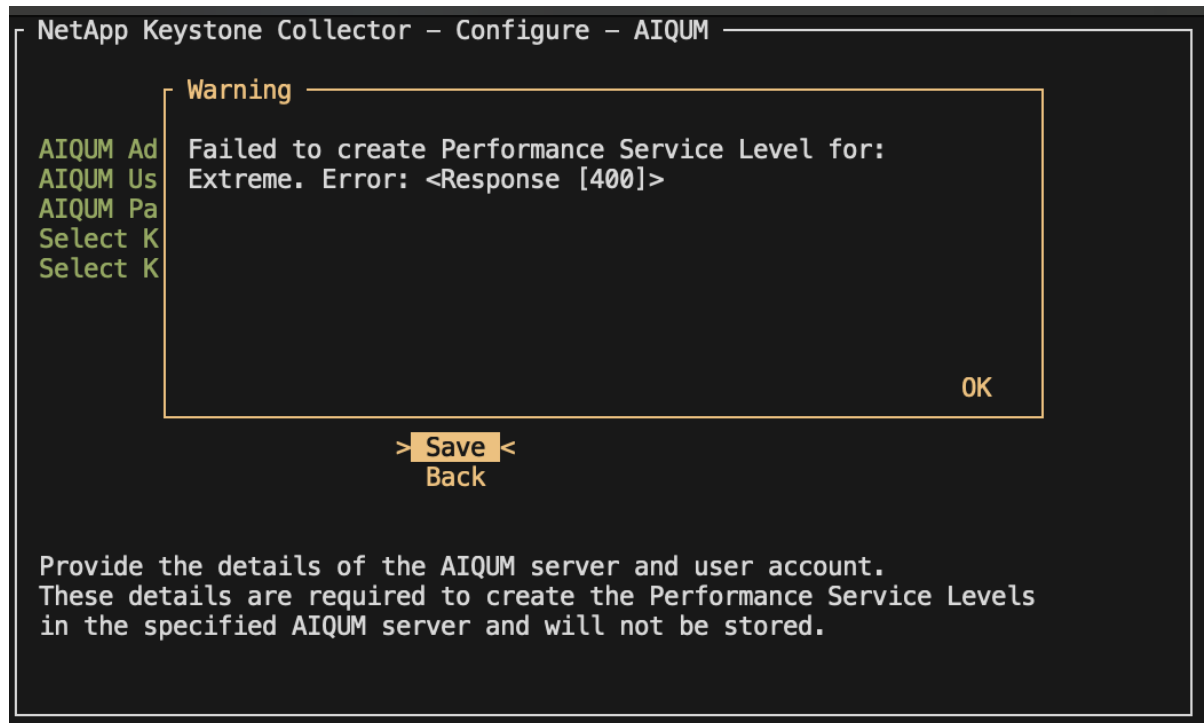
Description Extreme - KS-STaaS  
 Added Date 1 Aug 2024, 18:08  
 Last Modified Date 1 Aug 2024, 18:08

<input checked="" type="checkbox"/>	Premium ...S-STaaS	User-defined	2048	4096	500	2	Used: 0 bytes Available: 283.85 TiB	0
-------------------------------------	--------------------	--------------	------	------	-----	---	-------------------------------------	---

### Overview

Description Premium - KS-STaaS  
 Added Date 1 Aug 2024, 18:08  
 Last Modified Date 1 Aug 2024, 18:08

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



## ITOM Collector 설치

## Keystone ITOM Collector 설치 요구 사항

ITOM Collector를 설치하기 전에 시스템에 필요한 소프트웨어가 준비되어 있고 모든 필수 전제 조건을 충족하는지 확인하세요.

ITOM Collector 서버 VM의 필수 구성 요소:

- 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 최신 버전입니다.

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

### 네트워킹 요구 사항

ITOM Collector의 네트워킹 요구 사항은 다음 표에 나와 있습니다.

원천	목적지	규약	포트	설명
ITOM 수집가	NetApp ONTAP 클러스터 관리 IP	HTTPS, SNMP	TCP 443, UDP 161	ONTAP 컨트롤러 모니터링
NetApp ONTAP 클러스터 및 노드 관리 IP	ITOM 수집가	SNMP, 시스템로그	UDP 162, UDP 514	컨트롤러의 SNMP 트랩 및 Syslog
ITOM 수집가	클러스터 스위치	SNMP	UDP 161	스위치 모니터링
클러스터 스위치	ITOM 수집가	SNMP, 시스템로그	UDP 162, UDP 514	스위치의 SNMP 트랩 및 Syslog
ITOM 수집가	StorageGRID 노드 IP	HTTPS, SNMP	TCP 443, UDP 161	StorageGRID의 SNMP 모니터링
StorageGRID 노드 IP	ITOM 수집가	SNMP, 시스템로그	UDP 162, UDP 514	StorageGRID의 SNMP 트랩
ITOM 수집가	Keystone 컬렉터	SSH, HTTPS, SNMP	TCP 22, TCP 443, UDP 161	Keystone Collector 모니터링 및 원격 관리

ITOM 수집가	로컬 DNS	DNS	UDP 53	공개 또는 비공개 DNS 서비스
ITOM 수집가	선택한 NTP 서버	엔티피	UDP 123	시간 유지

## Linux 시스템에 **Keystone ITOM Collector**를 설치하세요

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



Keystone 지원팀은 ITOM Collector 설치 파일을 다운로드할 수 있는 동적 링크를 제공하는데, 이 링크는 2시간 후에 만료됩니다.

Windows 시스템에 ITOM Collector를 설치하려면 다음을 참조하세요. "[Windows 시스템에 ITOM Collector 설치](#)".

Linux 서버에 소프트웨어를 설치하려면 다음 단계를 따르세요.

### 시작하기 전에

- Linux 설치 스크립트에 Bourne shell을 사용할 수 있는지 확인하세요.
- 설치하다 vim-common ITOM Collector 설치 파일에 필요한 **xxd** 바이너리를 얻기 위한 패키지입니다.
- 확인하십시오 `sudo package` 루트가 아닌 사용자로 ITOM Collector를 실행하려는 경우 설치됩니다.

### 단계

1. ITOM 수집기 설치 파일을 Linux 서버에 다운로드합니다.
2. 서버에서 터미널을 열고 다음 명령을 실행하여 권한을 변경하고 바이너리를 실행 가능하게 만듭니다.  
# `chmod +x <installer_file_name>.bin`
3. ITOM 수집기 설치 파일을 시작하려면 다음 명령을 실행하세요.  
# `./<installer_file_name>.bin`
4. 설치 파일을 실행하면 다음 메시지가 표시됩니다.
  - a. 최종 사용자 라이선스 계약(EULA)에 동의합니다.
  - b. 설치를 위해 사용자 세부 정보를 입력하세요.
  - c. 설치 상위 디렉토리를 지정합니다.
  - d. 수집기 크기를 선택하세요.
  - e. 해당되는 경우, 대리인 세부 정보를 제공하세요.

각 프롬프트에 대해 기본 옵션이 표시됩니다. 특별한 요구 사항이 없다면 기본 옵션을 선택하는 것이 좋습니다. 기본 옵션을 선택하려면 **Enter** 키를 누르세요. 설치가 완료되면 ITOM Collector가 성공적으로 설치되었다는 메시지가 나타납니다.





- ITOM Collector 설치 파일은 다음을 추가합니다. `/etc/sudoers` 서비스 재시작 및 메모리 덤프를 처리합니다.
- Linux 서버에 ITOM Collector를 설치하면 \*ITOM\*이라는 기본 사용자가 생성되어 루트 권한 없이 ITOM Collector를 실행합니다. 다른 사용자를 선택하거나 루트로 실행할 수 있지만 Linux 설치 스크립트에서 생성된 ITOM 사용자를 사용하는 것이 좋습니다.

다음은 무엇인가요?

성공적으로 설치되면 Keystone 지원팀에 연락하여 ITOM 지원 포털을 통해 ITOM Collector가 성공적으로 설치되었는지 확인하세요. 검증 후, Keystone 지원팀은 ITOM 수집기를 원격으로 구성하고, 추가적인 장치 검색 및 모니터링 설정을 진행하며, 구성이 완료되면 확인 메시지를 보냅니다. 문의사항이나 추가 정보가 있으시면 [keystone.services@netapp.com](mailto:keystone.services@netapp.com)으로 연락해 주시기 바랍니다.

## Windows 시스템에 Keystone ITOM Collector를 설치하세요.

ITOM Collector 설치 파일을 다운로드하고, InstallShield 마법사를 실행하고, 필요한 모니터링 자격 증명을 입력하여 Windows 시스템에 ITOM Collector를 설치합니다.



Keystone 지원팀은 ITOM Collector 설치 파일을 다운로드할 수 있는 동적 링크를 제공하는데, 이 링크는 2시간 후에 만료됩니다.

귀하의 요구 사항에 따라 Linux 시스템에 설치할 수 있습니다. Linux 시스템에 ITOM Collector를 설치하려면 다음을 참조하세요. "[Linux 시스템에 ITOM Collector 설치](#)".

Windows 서버에 ITOM 수집기 소프트웨어를 설치하려면 다음 단계를 따르세요.

시작하기 전에

Windows 서버의 로컬 보안 정책 설정에서 로컬 정책/사용자 권한 할당에 따라 ITOM Collector 서비스에 서비스로 로그인 권한이 부여되었는지 확인하세요.

단계

1. ITOM 수집기 설치 파일을 Windows 서버에 다운로드합니다.
2. 설치 파일을 열어 InstallShield 마법사를 시작합니다.
3. 최종 사용자 라이선스 계약(EULA)에 동의합니다. InstallShield 마법사는 필요한 바이너리를 추출하고 자격 증명을 입력하라는 메시지를 표시합니다.
4. ITOM Collector가 실행될 계정의 자격 증명을 입력하세요.
  - 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 사용하세요.
  - ITOM Collector가 동일한 도메인에 속하지 않은 다른 Windows 서버를 모니터링하는 경우 로컬 관리자 계정을 사용하고 로컬 관리자 자격 증명으로 각 리소스에 연결합니다. ITOM Collector와 모니터링되는 리소스 간의 인증 문제를 줄이기 위해 비밀번호가 만료되지 않도록 설정할 수 있습니다.
5. 수집기 크기를 선택하세요. 기본값은 설치 파일에 따라 권장되는 크기입니다. 특별한 요구 사항이 없다면 제안된 크기로 진행하세요.
6. 다음 을 선택하여 설치를 시작하세요. 이미 채워진 폴더를 사용하거나 다른 폴더를 선택할 수 있습니다. 상태 상자에 설치 진행률이 표시되고, 그 다음에 InstallShield 마법사 완료 대화 상자가 표시됩니다.

다음은 무엇인가요?

성공적으로 설치되면 Keystone 지원팀에 연락하여 ITOM 지원 포털을 통해 ITOM Collector가 성공적으로 설치되었는지 확인하세요. 검증 후, Keystone 지원팀은 ITOM 수집기를 원격으로 구성하고, 추가적인 장치 검색 및 모니터링 설정을 진행하며, 구성이 완료되면 확인 메시지를 보냅니다. 문의사항이나 추가 정보가 있으시면 [keystone.services@netapp.com](mailto:keystone.services@netapp.com)으로 연락해 주시기 바랍니다.

## Keystone 에 대한 AutoSupport 구성

AutoSupport 원격 측정 메커니즘을 사용하는 경우 Keystone AutoSupport 원격 측정 데이터를 기반으로 사용량을 계산합니다. 필요한 수준의 세분성을 달성하려면 ONTAP 클러스터에서 보낸 일일 지원 번들에 Keystone 데이터를 통합하도록 AutoSupport 구성해야 합니다.

이 작업에 관하여

Keystone 데이터를 포함하도록 AutoSupport 구성하기 전에 다음 사항에 유의하세요.

- ONTAP CLI를 사용하여 AutoSupport 원격 측정 옵션을 편집합니다. AutoSupport 서비스 및 시스템(클러스터) 관리자 역할 관리에 대한 자세한 내용은 다음을 참조하세요. "[AutoSupport 관리 개요](#)" 그리고 "[클러스터 및 SVM 관리자](#)".
- Keystone의 정확한 데이터 수집을 보장하기 위해 일일 및 주간 AutoSupport 번들에 하위 시스템을 포함합니다. AutoSupport 하위 시스템에 대한 정보는 다음을 참조하세요. "[AutoSupport 하위 시스템은 무엇입니까?](#)".

단계

1. 시스템 관리자 사용자로 SSH를 사용하여 Keystone ONTAP 클러스터에 로그인합니다. 자세한 내용은 다음을 참조하세요. "[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
```

◦ 주간 로그 내용을 수정하려면 다음 명령을 실행하세요.

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

이 명령에 대한 자세한 내용은 다음을 참조하세요. ["시스템 노드 자동 지원 트리거 수정"](#).

## 모니터링 및 업그레이드

**Keystone Collector**의 상태를 모니터링합니다.

HTTP 요청을 지원하는 모니터링 시스템을 사용하여 Keystone Collector의 상태를 모니터링할 수 있습니다. 상태를 모니터링하면 Keystone 대시보드에서 데이터를 사용할 수 있는지 확인하는데 도움이 됩니다.

기본적으로 Keystone Health 서비스는 localhost 이외의 다른 IP에서의 연결을 허용하지 않습니다. Keystone 상태 종료점은 다음과 같습니다. /uber/health 그리고 Keystone Collector 서버의 모든 인터페이스에서 포트를 수신합니다. 7777. 쿼리 시 JSON 출력이 포함된 HTTP 요청 상태 코드가 엔드포인트에서 응답으로 반환되며, Keystone Collector 시스템의 상태를 설명합니다. JSON 본문은 전반적인 상태를 제공합니다. is\_healthy 속성은 부울이고 구성 요소별 상태의 자세한 목록입니다. component\_details 기인하다. 다음은 그 예입니다.

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

반환되는 상태 코드는 다음과 같습니다.

- **200:** 모니터링되는 모든 구성 요소가 정상임을 나타냅니다.
- **503:** 하나 이상의 구성 요소가 정상적이지 않음을 나타냅니다.

- **403:** 상태를 쿼리하는 HTTP 클라이언트가 허용된 네트워크 CIDR 목록인 허용 목록에 없음을 나타냅니다. 이 상태에서는 건강 정보가 반환되지 않습니다. *allow* 목록은 네트워크 CIDR 방식을 사용하여 어떤 네트워크 장치가 Keystone 상태 시스템을 쿼리할 수 있는지 제어합니다. 이 오류가 발생하면 \* Keystone Collector 관리 TUI > 구성 > 상태 모니터링\*에서 모니터링 시스템을 허용 목록에 추가하세요.



**Linux** 사용자는 다음과 같은 알려진 문제에 유의하세요.

문제 설명: Keystone Collector는 사용량 측정 시스템의 일부로 여러 컨테이너를 실행합니다. Red Hat Enterprise Linux 8.x 서버가 미국 국방 정보 시스템 기관(DISA) 보안 기술 구현 가이드(STIG) 정책으로 강화되었을 때 *fapolicyd*(파일 액세스 정책 데몬)와 관련된 알려진 문제가 간헐적으로 나타났습니다. 이 문제는 다음과 같이 식별됩니다. "[버그 1907870](#)". 해결 방법: Red Hat Enterprise에서 해결할 때까지 NetApp 다음을 수행하여 이 문제를 해결할 것을 권장합니다. *fapolicyd* 허용 모드로 전환. ~ 안에/etc/fapolicyd/fapolicyd.conf, 값을 설정하다 `permissive = 1.`

## 시스템 로그 보기

Keystone Collector 시스템 로그를 보고 시스템 정보를 검토하고 해당 로그를 사용하여 문제 해결을 수행할 수 있습니다. Keystone Collector는 호스트의 *journald* 로깅 시스템을 사용하고, 시스템 로그는 표준 *journalctl* 시스템 유틸리티를 통해 검토할 수 있습니다. 로그를 조사하려면 다음과 같은 주요 서비스를 이용할 수 있습니다.

- ks-컬렉터
- ks-헬스
- ks-자동 업데이트

주요 데이터 수집 서비스 `_ks-collector_`는 JSON 형식으로 로그를 생성합니다. `run-id` 각 예약된 데이터 수집 작업과 연관된 속성입니다. 다음은 표준 사용 데이터 수집을 위한 성공적인 작업의 예입니다.

```

{"level":"info","time":"2022-10-31T05:20:01.831Z","caller":"light-
collector/main.go:31","msg":"initialising light collector with run-id
cdf1m0f74cgphgfon8cg","run-id":"cdf1m0f74cgphgfon8cg"}
{"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":"cdf1m0f74cgphgfon8cg"}

{"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":"cdf1m0f74cgphgfon8cg"}

{"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":"cdf1m0f74cgphgfon8cg"}

{"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":"cdf1m0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-
31T05:20:48.786Z","caller":"worker/collector.go:75","msg":"4 clusters
collected","run-id":"cdf1m0f74cgphgfon8cg"}

{"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":"cdf1m0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-
31T05:20:48.840Z","caller":"reception/reception.go:76","msg":"File bytes
123425","run-id":"cdf1m0f74cgphgfon8cg"}

{"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":"cdf1m0f74cgphgfon8cg"}

```

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":"initialising 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-a826be4fdb7_1667193651.tar.gz"}

{"level":"info","time":"2022-10-31T05:21:31.385Z","caller":"reception/reception.go:75","msg":"Sending file 65a71542-cb4d-bdb2-e9a7-a826be4fdb7_1667193651.tar.gz type=ontap-perf to reception","run-id":"cdf1m0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-31T05:21:31.386Z","caller":"reception/reception.go:76","msg":"File bytes 17767","run-id":"cdf1m0f74cgphgfon8cg"}

{"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":"cdf1m0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-31T05:21:33.025Z","caller":"light-collector/main.go:88","msg":"exiting","run-id":"cdf1m0f74cgphgfon8cg"}
```

지원 번들을 생성하고 수집합니다.

Keystone Collector TUI를 사용하면 지원 번들을 생성하고 이를 서비스 요청에 추가하여 지원 문제를 해결할 수 있습니다. 다음 절차를 따르세요.

단계

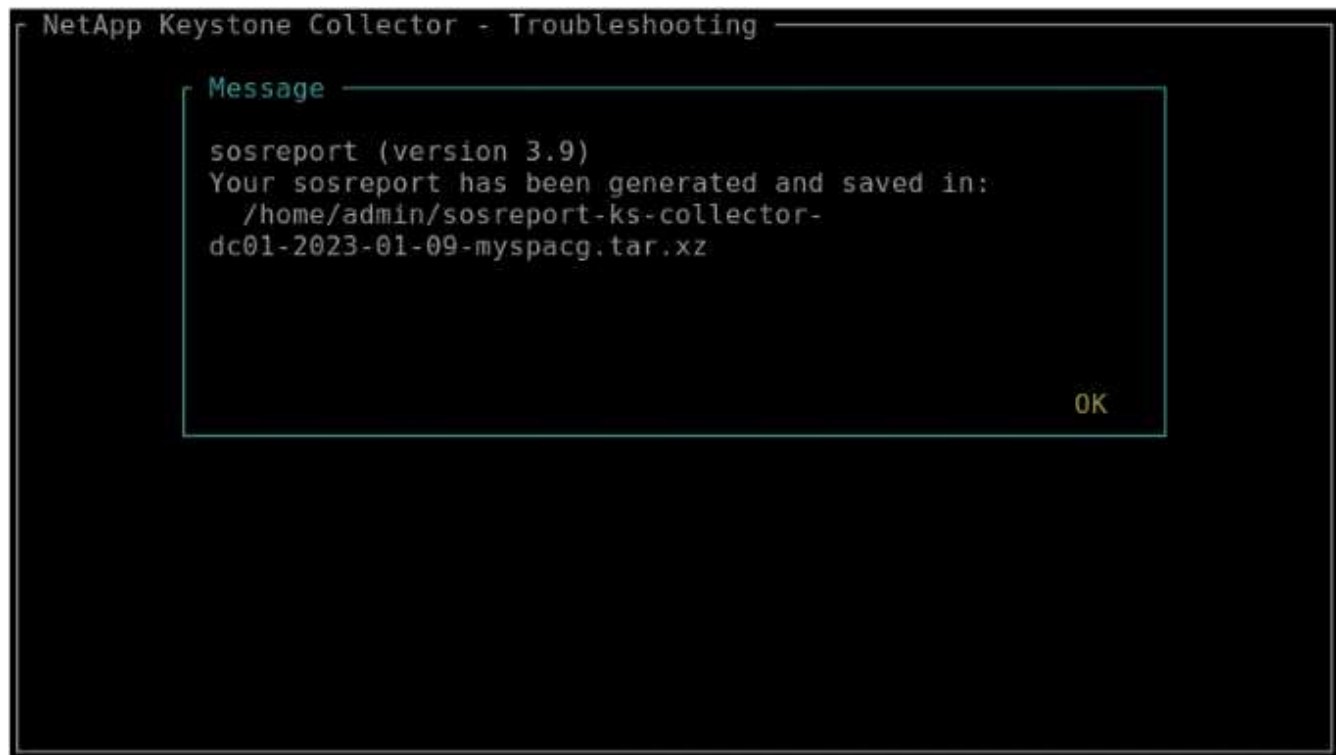
1. Keystone Collector 관리 TUI 유틸리티를 시작합니다.

```
$ keystone-collector-tui
```

2. \*문제 해결 > 지원 번들 생성\*으로 이동합니다



3. 생성되면 번들이 저장된 위치가 표시됩니다. FTP, SFTP 또는 SCP를 사용하여 해당 위치에 연결하고 로그 파일을 로컬 시스템에 다운로드합니다



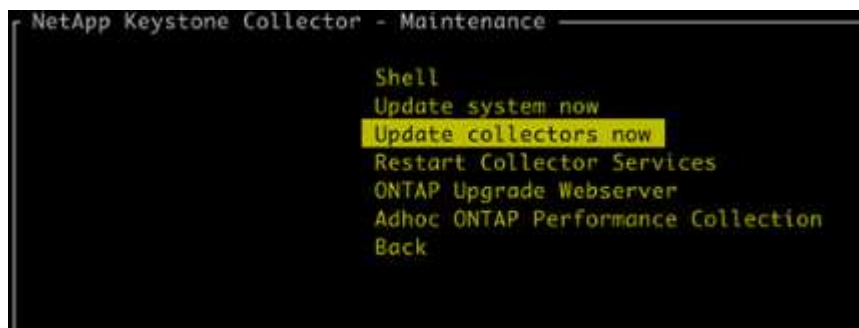
4. 파일을 다운로드한 후 Keystone ServiceNow 지원 티켓에 첨부할 수 있습니다. 티켓 발행에 대한 정보는 다음을 참조하세요. "[서비스 요청 생성](#)".

## Keystone Collector를 수동으로 업그레이드하세요

Keystone Collector의 자동 업데이트 기능은 기본적으로 활성화되어 있어, 새로운 릴리스가 나올 때마다 Keystone Collector 소프트웨어가 자동으로 업그레이드됩니다. 하지만 이 기능을 비활성화하고 소프트웨어를 수동으로 업그레이드할 수 있습니다.

단계

1. Keystone Collector 관리 TUI 유틸리티를 시작합니다.  
`$ keystone-collector-tui`
2. 유지 관리 화면에서 지금 수집기 업데이트 옵션을 선택합니다.



또는 다음 명령을 실행하여 버전을 업그레이드하세요.

CentOS의 경우:



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

```
[admin@rhel8-serge-dev ~]$ sudo yum clean metadata && sudo yum install keystone-collector
Updating Subscription Management repositories.
Unable to read consumer identity

This system is not registered with an entitlement server. You can use subscription-manager to register.

Cache was expired
0 files removed
Updating Subscription Management repositories.
Unable to read consumer identity

This system is not registered with an entitlement server. You can use subscription-manager to register.

Netapp Keystone                               8.4 kB/s | 11 kB    00:01
Red Hat Enterprise Linux 8 - BaseOS           33 MB/s | 2.4 MB   00:00
Red Hat Enterprise Linux 8 - AppStream        57 MB/s | 7.5 MB   00:00
Package keystone-collector-1.3.0-1.noarch is already installed.
Dependencies resolved.
=====
Package                                Architecture      Version           Size              Repository
=====
Upgrading:
keystone-collector                     noarch            1.3.2-1           411 M             keystone
Transaction Summary
=====
Upgrade 1 Package

Total download size: 411 M
Is this ok [y/N]: y
Downloading Packages:
keystone-collector-1.3.2-1.noarch.rpm      8.3 MB/s | 411 MB   00:49
-----
Total                                     8.3 MB/s | 411 MB   00:49
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing      :                                1/1
  Running scriptlet: keystone-collector-1.3.2-1.noarch 1/1
  Running scriptlet: keystone-collector-1.3.2-1.noarch 1/2
  Upgrading      : keystone-collector-1.3.2-1.noarch 1/2
  Running scriptlet: keystone-collector-1.3.2-1.noarch 1/2
*****
*
* Keystone Collector package installation complete!
* Run command 'keystone-collector-tui' to configure .
*
*****
Running scriptlet: keystone-collector-1.3.0-1.noarch 2/2
Cleanup      : keystone-collector-1.3.0-1.noarch 2/2
Running scriptlet: keystone-collector-1.3.0-1.noarch 2/2
Verifying    : keystone-collector-1.3.2-1.noarch 1/2
Verifying    : keystone-collector-1.3.0-1.noarch 2/2
Installed products updated.

Upgraded:
keystone-collector-1.3.2-1.noarch

Complete!
[admin@rhel8-serge-dev ~]$ rpm -q keystone-collector
keystone-collector-1.3.2-1.noarch
```

데비안의 경우:

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

3. Keystone Collector 관리 TUI를 다시 시작하면 홈 화면의 왼쪽 상단에서 최신 버전을 확인할 수 있습니다.

또는 다음 명령을 실행하여 최신 버전을 확인하세요.

CentOS의 경우:

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

데비안의 경우:

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

## Keystone 콜렉터 보안

Keystone Collector에는 고객 데이터 보안을 위협하지 않으면 Keystone 시스템의 성능과 사용 측정 항목을 모니터링하는 보안 기능이 포함되어 있습니다.

Keystone Collector의 기능은 다음과 같은 보안 원칙에 따라 작동합니다.

- 개인정보 보호를 위한 설계- Keystone Collector는 사용량 측정 및 성능 모니터링을 수행하기 위해 최소한의 데이터를 수집합니다. 자세한 내용은 다음을 참조하세요. "[청구를 위해 수집된 데이터](#)". 그만큼 "[개인 데이터 제거](#)" 민감한 정보를 마스크하고 보호하는 옵션이 기본적으로 활성화되어 있습니다.
- 최소 권한 액세스- Keystone Collector는 스토리지 시스템을 모니터링하기 위해 최소한의 권한만 요구하며, 이를 통해 보안 위험을 최소화하고 데이터에 대한 의도치 않은 수정을 방지합니다. 이러한 접근 방식은 최소 권한의 원칙에 부합하며, 모니터링되는 환경의 전반적인 보안 태세를 강화합니다.
- 안전한 소프트웨어 개발 프레임워크- Keystone 개발 주기 전반에 걸쳐 안전한 소프트웨어 개발 프레임워크를 사용하여 위험을 완화하고, 취약성을 줄이며, 잠재적 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 약화될 수 있습니다. 자세한 내용은 다음을 참조하세요. "[CIS 벤치마크 가이드](#)".
  - Keystone Collector의 자동 업데이트 기능을 통해 검증된 보안 패치를 자동으로 수신하여 설치합니다. 이 기능을 비활성화하면 패치되지 않은 취약한 소프트웨어가 설치될 수 있습니다.
  - Keystone Collector에서 받은 업데이트를 인증합니다. APT 저장소 검증을 비활성화하면 승인되지 않은 패치가 자동으로 설치되어 잠재적으로 취약점이 발생할 수 있습니다.
- Keystone Collector는 HTTPS 인증서를 자동으로 검증하여 연결 보안을 보장합니다. 이 기능을 비활성화하면 외부 엔드포인트 사칭 및 사용 데이터 유출이 발생할 수 있습니다.
- Keystone Collector 지원 "[맞춤형 신뢰할 수 있는 CA](#)" 인증. 기본적으로는 공개 루트 CA에서 인식한 서명된 인증서를 신뢰합니다. "[모질라 CA 인증 프로그램](#)". Keystone Collector는 신뢰할 수 있는 CA를 추가로 활성화하여 이러한 인증서를 제시하는 엔드포인트에 대한 연결에 대해 HTTPS 인증서 유효성 검사를 활성화합니다.
- Keystone 수집기는 기본적으로 개인 데이터 제거 옵션을 활성화하여 민감한 정보를 마스크하고 보호합니다. 자세한 내용은 다음을 참조하세요. "[개인정보 수집 제한](#)". 이 옵션을 비활성화하면 추가 데이터가 Keystone 시스템으로 전송됩니다. 예를 들어, 볼륨 이름과 같이 민감한 정보로 간주될 수 있는 사용자가 입력한 정보가 포함될 수 있습니다.

## 관련 정보

- "[Keystone 컬렉터 개요](#)"

- ["가상 인프라 요구 사항"](#)
- ["Keystone Collector 구성"](#)

## Keystone 수집하는 사용자 데이터 유형

Keystone Keystone ONTAP 및 Keystone StorageGRID 구독에서 구성, 상태 및 사용 정보를 수집하고 Keystone Collector를 호스팅하는 가상 머신(VM)에서 원격 측정 데이터를 수집합니다. Keystone Collector에서 이 옵션을 활성화하면 ONTAP 에 대한 성능 데이터만 수집할 수 있습니다.

### ONTAP 데이터 수집

## <strong> ONTAP 에 대해 수집된 사용 데이터: 자세히 알아보기</strong>

다음 목록은 ONTAP 에 대해 수집된 용량 소비 데이터의 대표적인 샘플입니다.

- 클러스터
  - 클러스터UUID
  - 클러스터 이름
  - 일련번호
  - 위치( ONTAP 클러스터에 입력된 값 기반)
  - 연락처
  - 버전
- 노드
  - 일련번호
  - 노드 이름
- 볼륨
  - 집계 이름
  - 볼륨 이름
  - 볼륨인스턴스UUID
  - IsCloneVolume 플래그
  - IsFlexGroupConstituent 플래그
  - IsSpaceEnforcementLogical 플래그
  - IsSpaceReportingLogical 플래그
  - Afs에 의해 사용된 논리적 공간
  - 퍼센트스냅샷스페이스
  - 성능 계층 비활성 사용자 데이터
  - 성능 계층 비활성 사용자 데이터 백분율
  - QoSAdaptivePolicyGroup 이름
  - QoSPolicyGroup 이름
  - 크기
  - 사용된
  - 물리적 사용됨
  - 스냅샷에 사용된 크기
  - 유형
  - 볼륨 스타일 확장
  - Vserver 이름

- IsVsRoot 플래그
- V서버
  - 가상 서버 이름
  - VserverUUID
  - 하위 유형
- 저장 집계
  - 스토리지 유형
  - 집계 이름
  - 집계 UUID
  - 물리적 사용
  - 사용 가능한 크기
  - 크기
  - 사용된 사이즈
- 집계 객체 저장소
  - ObjectStoreName
  - 객체 저장소 UUID
  - 공급자 유형
  - 집계 이름
- 볼륨 복제
  - FlexClone
  - 크기
  - 사용된
  - V서버
  - 유형
  - 부모 볼륨
  - 부모V서버
  - IsConstituent
  - 분할 추정
  - 상태
  - FlexCloneUsedPercent
- 스토리지 LUN
  - LUN UUID
  - LUN 이름
  - 크기
  - 사용된

- IsReserved 플래그
- IsRequested 플래그
- LogicalUnit 이름
- QoSPolicyUUID
- QoSPolicyName
- 볼륨UUID
- 볼륨 이름
- SVMUUID
- SVM 이름
- 저장 볼륨
  - 볼륨인스턴스UUID
  - 볼륨 이름
  - SVM 이름
  - SVMUUID
  - QoSPolicyUUID
  - QoSPolicyName
  - 용량 계층 발자국
  - 성능 계층 발자국
  - 총 발자국
  - 계층화 정책
  - IsProtected 플래그
  - IsDestination 플래그
  - 사용된
  - 물리적 사용됨
  - 복제 부모 UUID
  - Afs에 의해 사용된 논리적 공간
- QoS 정책 그룹
  - 정책그룹
  - QoSPolicyUUID
  - 최대 처리량
  - 최소 처리량
  - 최대 처리량 IOPS
  - 최대 처리량(MBps)
  - 최소 처리량 IOPS
  - 최소 처리량(MBps)

- IsShared 플래그
- ONTAP 적응형 QoS 정책 그룹
  - QoSPolicyName
  - QoSPolicyUUID
  - 피크 IOPS
  - 피크 IOPS 할당
  - 절대 최소 IOPS
  - 예상 IOPS
  - 예상 IOPS 할당
  - 블록 크기
- 발자취
  - V서버
  - 용량
  - 총 발자국
  - VolumeBlocksFootprintBin0
  - VolumeBlocksFootprintBin1
- MetroCluster
  - 마디
  - 골재
  - LIFs
  - 구성 복제
  - 사이
  - 클러스터
  - 볼륨
- MetroCluster 클러스터
  - 클러스터UUID
  - 클러스터 이름
  - 원격 클러스터 UUID
  - 원격클러저이름
  - 로컬 구성 상태
  - 원격 구성 상태
- 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
  - 방법
- 수집기 관측 가능성 지표
  - 수집 시간
  - Active IQ Unified Manager API 엔드포인트가 쿼리되었습니다.
  - 응답 시간
  - 레코드 수
  - AIQUM인스턴스 IP
  - CollectorInstance ID



## <strong> ONTAP 에 대해 수집된 성능 데이터: 자세히 알아보기</strong>

다음 목록은 ONTAP 에 대해 수집된 성능 데이터의 대표적인 샘플입니다.

- 클러스터 이름
- 클러스터 UUID
- 개체ID
- 볼륨 이름
- 볼륨 인스턴스 UUID
- V서버
- VserverUUID
- 노드 시리얼
- ONTAP 버전
- AIQUM 버전
- 골재
- 집계UUID
- 리소스키
- 타임스탬프
- IOPSPerTb
- 숨어 있음
- 읽기 지연 시간
- 쓰기MBps
- QoSMinThroughput 대기 시간
- QoSNBladeLatency
- 사용된 헤드룸
- 캐시 미스 비율
- 기타 대기 시간
- QoSAggregateLatency
- 아이오프스
- QoSNetworkLatency
- 사용 가능한 작업
- 쓰기 지연 시간
- QoS클라우드 지연 시간
- QoSClusterInterconnect 지연 시간
- 기타MBps
- QoSCop 대기 시간

- QoSDBladeLatency
- 이용
- 읽기IOPS
- MBps
- 기타 IOPS
- QoSPolicyGroupLatency
- 읽기 MBps
- QoSSyncSnapmirrorLatency
- 시스템 수준 데이터
  - 쓰기/읽기/기타/총 IOPS
  - 쓰기/읽기/기타/총 처리량
  - 쓰기/읽기/기타/전체 대기 시간
- 쓰기IOPS

**<strong>개인 데이터 접근 제한에서 제거된 항목 목록: 자세히 알아보기</strong>**

Keystone Collector에서 개인 데이터 제거 옵션을 활성화하면 ONTAP 에 대한 다음 사용 정보가 제거됩니다. 이 옵션은 기본적으로 활성화되어 있습니다.

- 클러스터 이름
- 클러스터 위치
- 클러스터 연락처
- 노드 이름
- 집계 이름
- 볼륨 이름
- QoSAdaptivePolicyGroup 이름
- QoSPolicyGroup 이름
- Vserver 이름
- 스토리지 LUN 이름
- 집계 이름
- LogicalUnit 이름
- SVM 이름
- AIQUM인스턴스 IP
- FlexClone
- 원격 클러스터 이름

## StorageGRID 데이터 수집

### <strong> StorageGRID 에 대해 수집된 사용 데이터: 자세히 알아보기</strong>

다음 목록은 대표적인 샘플입니다. Logical Data StorageGRID 에 대해 수집됨:

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

다음 목록은 대표적인 샘플입니다. Physical Data StorageGRID 에 대해 수집됨:

- StorageGRID ID
- 노드 ID
- 사이트 ID
- 사이트 이름
- 사례
- StorageGRID 스토리지 사용량 바이트
- StorageGRID 스토리지 활용도 메타데이터 바이트

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

- SLA 가동 시간 비율

### <strong>개인 데이터 접근 제한에서 제거된 항목 목록: 자세히 알아보기</strong>

Keystone Collector에서 개인 데이터 제거 옵션을 활성화하면 StorageGRID 에 대한 다음 사용 정보가 제거됩니다. 이 옵션은 기본적으로 활성화되어 있습니다.

- 계정 이름
- 버킷 이름
- 사이트 이름
- 인스턴스/노드 이름

## 원격 측정 데이터 수집

## <strong> Keystone Collector VM에서 수집된 원격 측정 데이터: 자세히 알아보기</strong>

다음 목록은 Keystone 시스템에서 수집된 원격 측정 데이터의 대표적인 샘플입니다.

- 시스템 정보
  - 운영체제 이름
  - 운영 체제 버전
  - 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 크기
  - 사용된 디스크
  - 디스크 사용 가능
  - 디스크 사용률
  - 디스크 마운트 지점
- 설치된 패키지
- 수집기 구성
- 서비스 로그
  - Keystone 서비스의 서비스 로그

# 개인 모드의 **Keystone**

## Keystone (비공개 모드)에 대해 알아보세요

Keystone 귀사의 비즈니스 및 보안 요구 사항을 충족하기 위해 개인 배포 모드(\_다크 사이트\_라고도 함)를 제공합니다. 이 모드는 연결 제한이 있는 조직에서 사용할 수 있습니다.

NetApp 인터넷 연결이 제한적이거나 전혀 없는 환경(다크 사이트라고도 함)에 맞춰 Keystone STaaS를 특별히 배포합니다. 이러한 환경은 보안, 규정 준수 또는 운영 요구 사항으로 인해 외부 통신이 제한되는 안전하거나 격리된 환경입니다.

NetApp Keystone 의 경우 다크 사이트에 대한 서비스를 제공한다는 것은 이러한 환경의 제약을 존중하는 방식으로 Keystone 유연 스토리지 구독 서비스를 제공한다는 것을 의미합니다. 여기에는 다음이 포함됩니다.

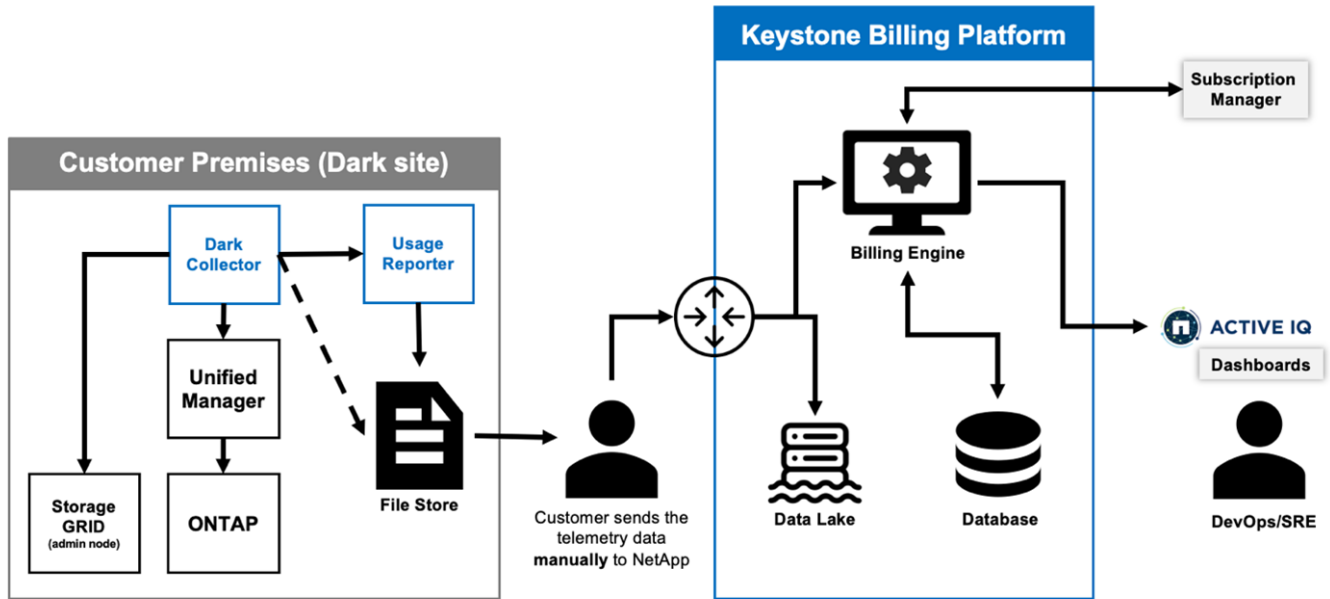
- 로컬 배포: Keystone 격리된 환경 내에서 독립적으로 구성할 수 있으므로 설정 액세스를 위한 인터넷 연결이나 외부 인력이 필요 없습니다.
- 오프라인 작업: 상태 점검 및 청구 기능을 포함한 모든 스토리지 관리 기능은 오프라인에서 작업을 수행할 수 있습니다.
- 보안 및 규정 준수: Keystone 배포가 고급 암호화, 안전한 액세스 제어, 세부적인 감사 기능 등을 포함할 수 있는 다크 사이트의 보안 및 규정 준수 요구 사항을 충족하는지 확인합니다.
- 도움말 및 지원: NetApp 각 계정에 전담 Keystone 성공 관리자를 지정하여 지원 및 문제 해결을 담당하고, 연중무휴 글로벌 지원을 제공합니다.



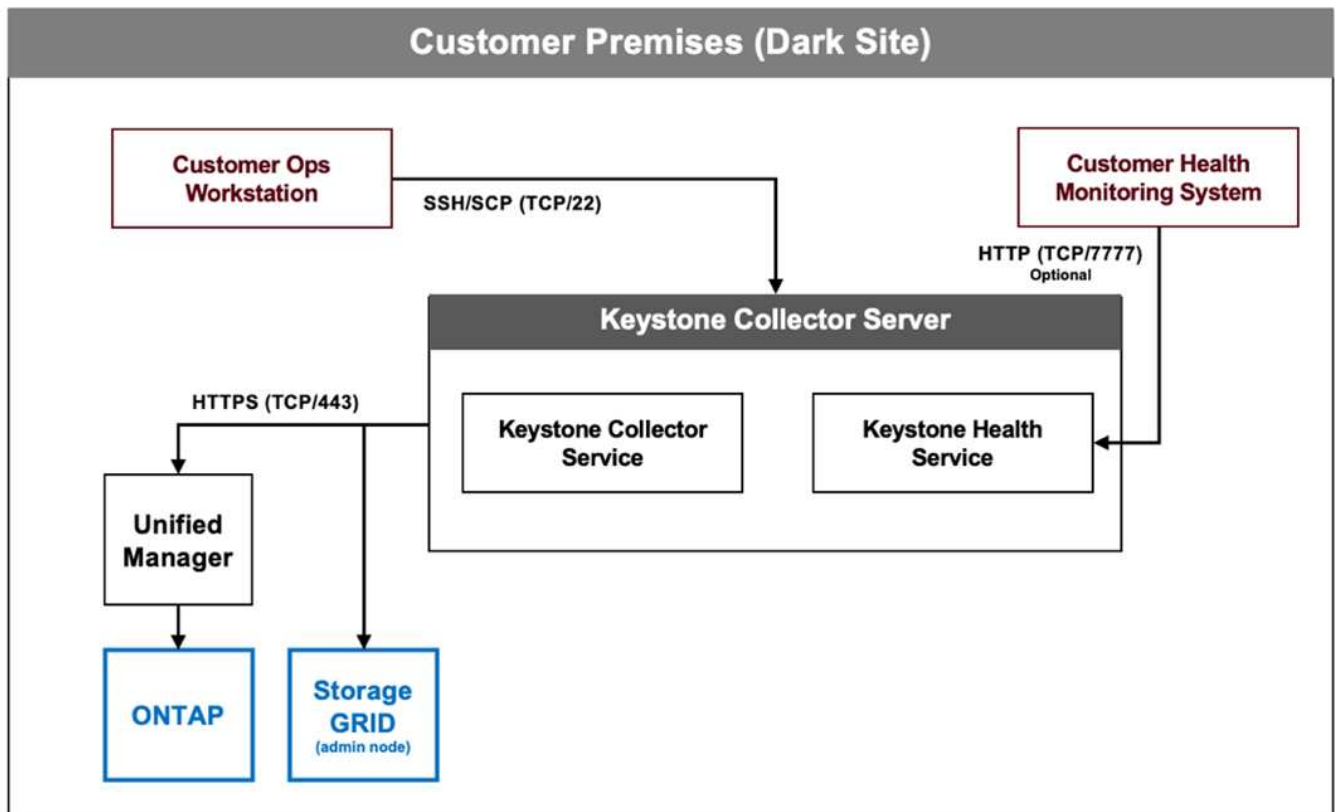
Keystone Collector는 연결 제한 없이 구성할 수 있으며, 이를 표준 모드라고도 합니다. 자세한 내용은 다음을 참조하세요. "[Keystone Collector에 대해 알아보세요](#)".

## 개인 모드의 **Keystone** 수집기

Keystone Collector는 스토리지 시스템에서 사용 데이터를 주기적으로 수집하고 해당 지표를 오프라인 사용 보고자와 로컬 파일 저장소로 내보내는 역할을 합니다. 암호화된 형식과 일반 텍스트 형식으로 생성된 파일은 유효성 검사를 거친 후 사용자가 수동으로 NetApp 에 전달합니다. NetApp의 Keystone 청구 플랫폼은 이러한 파일을 수신하면 이를 인증하고 처리하여 청구 및 구독 관리 시스템에 통합하여 월별 요금을 계산합니다.



서버의 Keystone Collector 서비스는 주기적으로 사용 데이터를 수집하고, 이 정보를 처리하고, 서버에 로컬로 사용 파일을 생성하는 역할을 합니다. 건강 서비스는 시스템 상태 점검을 실시하며 고객이 사용하는 건강 모니터링 시스템과 인터페이스하도록 설계되었습니다. 이러한 보고서는 사용자가 오프라인으로 접근하여 검증하고 문제 해결에 도움이 됩니다.



## Keystone Collector 비공개 모드 설치를 준비하세요

인터넷 접속이 불가능한 환경(다크 사이트 또는 프라이빗 모드라고도 함)에 Keystone

Collector를 설치하기 전에 시스템에 필요한 소프트웨어가 설치되어 있고 모든 필수 전제 조건이 충족되는지 확인하세요.

#### VMware vSphere에 대한 요구 사항

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

#### Linux 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
- 램: 4GB
- 디스크 공간: 50GB vDisk
  - 최소 2GB 여유 공간 `/var/lib/`
  - 최소 48GB 여유 공간 `/opt/netapp`

동일한 서버에는 다음과 같은 타사 패키지도 설치되어 있어야 합니다. 저장소를 통해 사용 가능한 경우 다음 패키지는 필수 구성 요소로 자동 설치됩니다.

- RHEL 8.6 이상(8.x)
  - 파이썬3  $\geq v3.6.8$ , 파이썬3  $\leq v3.9.13$
  - 포드맨
  - 위급 신호
  - yum-utils
  - python3-dnf-플러그인 버전 잠금
- RHEL 9.0 이상
  - python3  $\geq v3.9.0$ , python3  $\leq v3.9.13$
  - 포드맨
  - 위급 신호
  - yum-utils
  - python3-dnf-플러그인 버전 잠금
- 데비안 v12
  - python3  $\geq v3.9.0$ , python3  $\leq v3.12.0$

- 포트맨
- 소스리포트

## 네트워킹 요구 사항

Keystone Collector의 네트워킹 요구 사항은 다음과 같습니다.

- API Gateway 기능이 활성화된 서버에 Active IQ Unified Manager (Unified Manager) 9.10 이상이 구성되어 있습니다.
- Unified Manager 서버는 포트 443(HTTPS)에서 Keystone Collector 서버에서 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 보내내어 NetApp 지원팀에 이메일로 보내세요. 지원팀에 연락하는 방법에 대한 자세한 내용은 다음을 참조하세요. "[Keystone 에 대한 도움말 받기](#)".

## Keystone Collector를 개인 모드로 설치하세요

인터넷 접속이 불가능한 환경, 즉 다크 사이트 또는 \_프라이빗 모드\_에 Keystone Collector를 설치하려면 몇 가지 단계를 완료하세요. 이러한 유형의 설치 는 보안 사이트에 적합합니다.

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

### VMware vSphere에 배포

다음 단계를 따르세요.

1. OVA 템플릿 파일을 다운로드하세요 "[NetApp Keystone 웹 포털](#)".
2. OVA 파일로 Keystone 수집기를 배포하는 단계는 섹션을 참조하세요."[OVA 템플릿 배포](#)".

### 리눅스에 설치

Keystone Collector 소프트웨어는 Linux 배포판에 따라 제공된 .deb 또는 .rpm 파일을 사용하여 Linux 서버에 설치됩니다.

Linux 서버에 소프트웨어를 설치하려면 다음 단계를 따르세요.

1. Keystone Collector 설치 파일을 Linux 서버로 다운로드하거나 전송하세요.

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

2. 서버에서 터미널을 열고 다음 명령을 실행하여 설치를 시작하세요.

- 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. 입력하다 *y* 패키지를 설치하라는 메시지가 표시되면.

## 개인 모드에서 **Keystone Collector** 구성

인터넷 접속이 불가능한 환경(다크 사이트 또는 프라이빗 모드라고도 함)에서 Keystone Collector가 사용 데이터를 수집할 수 있도록 몇 가지 구성 작업을 완료하세요. 이는 필요한 구성 요소를 활성화하고 스토리지 환경과 연결하기 위한 일회성 활동입니다. Keystone Collector를 구성하면 Active IQ Unified Manager 에서 관리하는 모든 ONTAP 클러스터를 모니터링합니다.



Keystone Collector는 구성 및 모니터링 활동을 수행하기 위한 Keystone Collector 관리 터미널 사용자 인터페이스(TUI) 유틸리티를 제공합니다. Enter 키와 화살표 키 등 다양한 키보드 컨트롤을 사용하여 옵션을 선택하고 이 TUI를 탐색할 수 있습니다.

단계

1. Keystone Collector 관리 TUI 유틸리티를 시작합니다.

```
keystone-collector-tui
```

2. \*구성 > 고급\*으로 이동합니다.

3. 다크사이트 모드 옵션을 전환합니다.



4. \*저장\*을 선택하세요.

5. \*구성 > KS-Collector\*로 이동하여 Keystone Collector를 구성합니다.

6. 시스템으로 **KS Collector** 시작 필드를 전환합니다.

7. \* ONTAP 사용량 수집\* 필드를 전환합니다. Active IQ Unified Manager (Unified Manager) 서버 및 사용자 계정의

세부 정보를 추가합니다.

8. 선택 사항: 구독에 데이터 계층화가 필요한 경우 계층화 요금제 사용 필드를 전환합니다.
9. 구매한 구독 유형에 따라 \*사용 유형\*을 업데이트하세요.



구성하기 전에 NetApp의 구독과 연관된 사용 유형을 확인하세요.

```
NetApp Keystone Collector - Configure - KS Collector

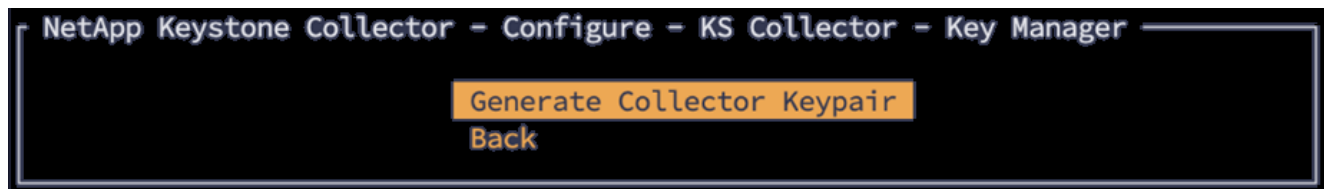
[X] Start KS-Collector with System
[X] Collect ONTAP usage
AIQUM Address:
AIQUM Username:
AIQUM Password: -----
[X] Using Tiering Rate plans
Mode Dark
Logging Level info
Usage Type provisioned_v1
Encryption Key Manager
Tunables
Save
Clear Config
Back
```

10. \*저장\*을 선택하세요.
11. \*구성 > KS-Collector\*로 이동하여 Keystone Collector 키 쌍을 생성합니다.
12. \*암호화 키 관리자\*로 가서 Enter를 누릅니다.

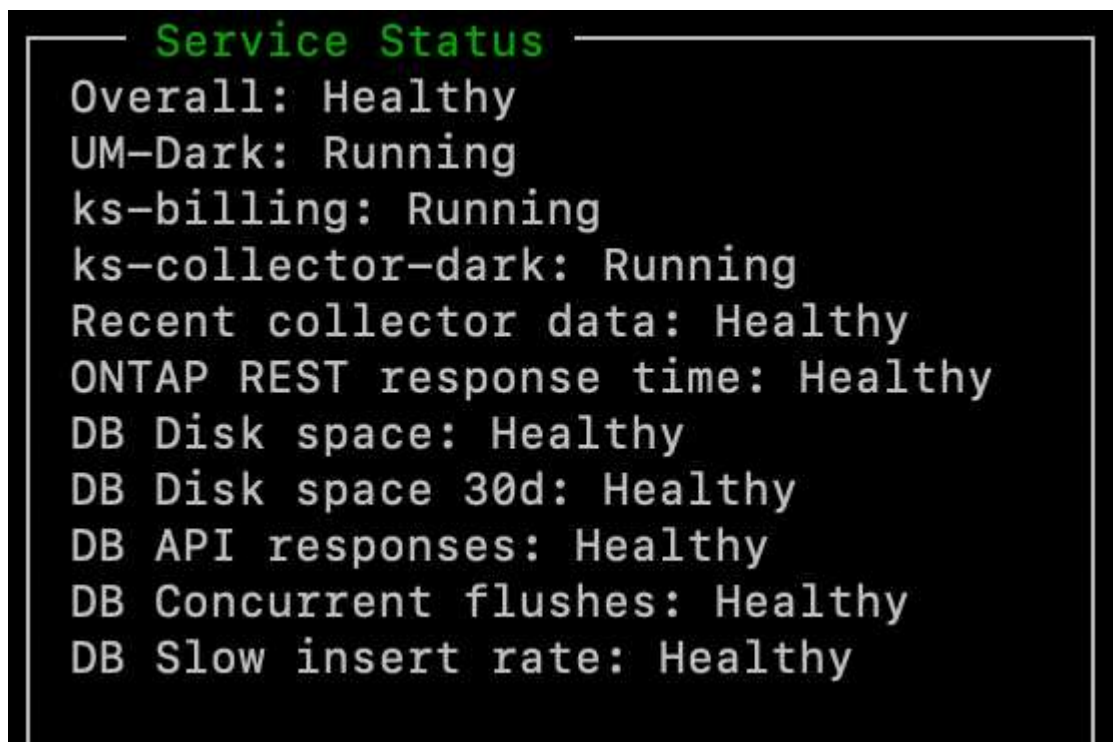
```
NetApp Keystone Collector - Configure - KS Collector

[X] Start KS-Collector with System
[X] Collect ONTAP usage
AIQUM Address:
AIQUM Username:
AIQUM Password: -----
[ ] Using Tiering Rate plans
Mode Dark
Logging Level info
Usage Type provisioned_v1
Encryption Key Manager
Tunables
Save
Clear Config
Back
```

13. \*수집기 키 쌍 생성\*을 선택하고 Enter를 누릅니다.



14. TUI의 메인 화면으로 돌아가서 서비스 상태 정보를 확인하여 Keystone Collector가 정상 상태인지 확인하세요. 시스템은 서비스가 전반적으로: 양호 상태임을 표시해야 합니다. 최대 10분 정도 기다려 보세요. 이 기간이 지난 후에도 전반적인 상태가 여전히 좋지 않으면 이전 구성 단계를 검토하고 NetApp 지원팀에 문의하세요.



15. 홈 화면에서 셸로 종료 옵션을 선택하여 Keystone Collector 관리 TUI를 종료합니다.
16. 생성된 공개 키를 검색합니다.

```
~/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 보고서 내보내기

매월 말에 NetApp 에 월별 사용 요약 보고서를 보내야 합니다. 이 보고서는 수동으로 생성할 수 있습니다.

사용 보고서를 생성하려면 다음 단계를 따르세요.

1. Keystone Collector TUI 홈 화면에서 \*사용량 내보내기\*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 생성하는데, 이는 NetApp 에 수동으로 전송해야 합니다.

클리어 파일 보고서에는 고객이 검증할 수 있는 다음과 같은 세부 정보가 포함되어 있습니다.

```
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-----
```

## ONTAP 업그레이드

Keystone Collector는 TUI를 통해 ONTAP 업그레이드를 지원합니다.

ONTAP 업그레이드하려면 다음 단계를 따르세요.

1. \*유지관리 > ONTAP 웹서버 업그레이드\*로 이동합니다.
2. ONTAP 업그레이드 이미지 파일을 \*/opt/netapp/ontap-upgrade/\*에 복사한 다음 \*웹 서버 시작\*을 선택하여 웹 서버를 시작합니다.



3. 로 가다 <http://<collector-ip>:8000> 업그레이드 지원을 위해 웹 브라우저를 사용합니다.

## Keystone Collector를 다시 시작하세요

TUI를 통해 Keystone Collector 서비스를 다시 시작할 수 있습니다. TUI에서 유지 관리 > 수집기 다시 시작 서비스로 이동합니다. 이렇게 하면 모든 수집기 서비스가 재부팅되고, TUI 홈 화면에서 해당 상태를 모니터링할 수 있습니다.



## 개인 모드에서 **Keystone Collector** 상태 모니터링

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

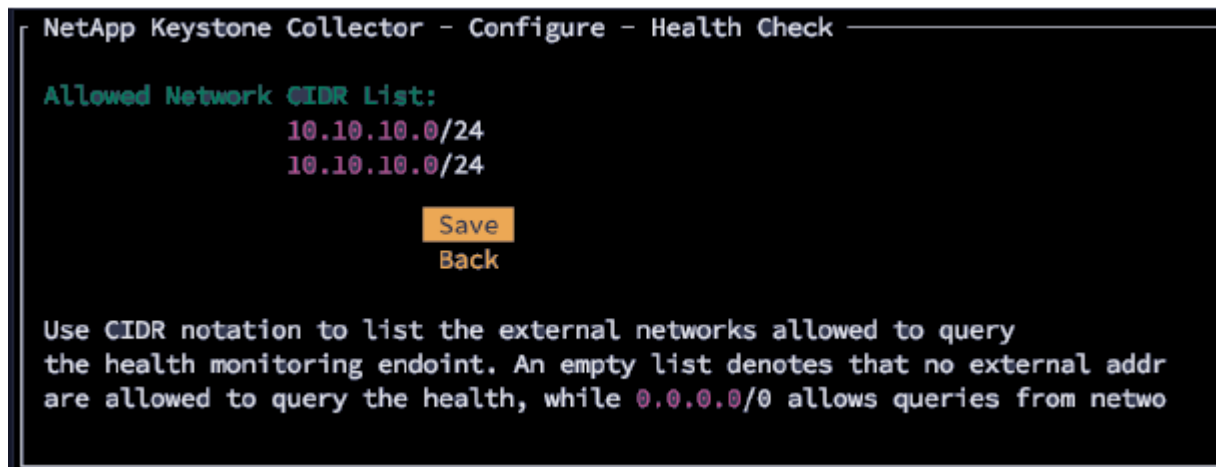
기본적으로 Keystone Health 서비스는 localhost 이외의 다른 IP에서의 연결을 허용하지 않습니다. Keystone 상태 종료점은 다음과 같습니다. /uber/health 그리고 Keystone Collector 서버의 모든 인터페이스에서 포트를 수신합니다. 7777. 쿼리 시 JSON 출력이 포함된 HTTP 요청 상태 코드가 엔드포인트에서 응답으로 반환되며, Keystone Collector 시스템의 상태를 설명합니다. JSON 본문은 전반적인 상태를 제공합니다. is\_healthy 속성은 부울이고 구성 요소별 상태의 자세한 목록입니다. component\_details 기인하다. 다음은 그 예입니다.

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

반환되는 상태 코드는 다음과 같습니다.

- **200:** 모니터링되는 모든 구성 요소가 정상임을 나타냅니다.
- **503:** 하나 이상의 구성 요소가 정상적이지 않음을 나타냅니다.
- **403:** 상태를 쿼리하는 HTTP 클라이언트가 허용된 네트워크 CIDR 목록인 허용 목록에 없음을 나타냅니다. 이 상태에서는 건강 정보가 반환되지 않습니다.

allow 목록은 네트워크 CIDR 방식을 사용하여 어떤 네트워크 장치가 Keystone 상태 시스템을 쿼리할 수 있는지 제어합니다. 403 오류가 발생하면 \* Keystone Collector 관리 TUI > 구성 > 상태 모니터링\*에서 모니터링 시스템을 허용 목록에 추가하세요.

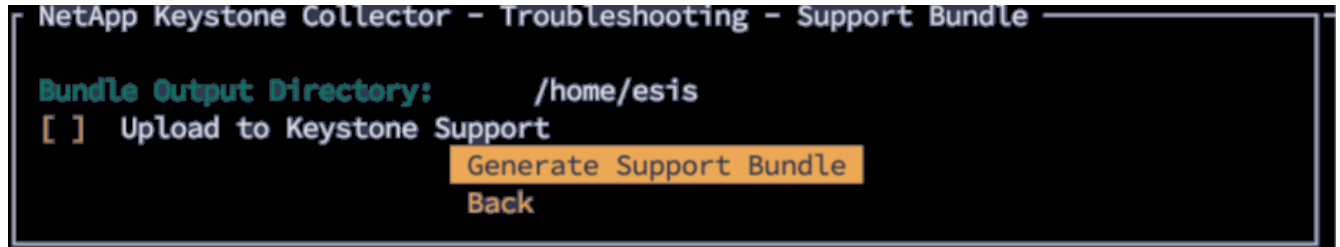


지원 번들을 생성하고 수집합니다.

Keystone Collector 관련 문제를 해결하려면 NetApp 지원팀에 문의하세요. 지원팀에서는 *.tar* 파일을 요청할 수 있습니다. Keystone Collector 관리 TUI 유틸리티를 통해 이 파일을 생성할 수 있습니다.

*.tar* 파일을 생성하려면 다음 단계를 따르세요.

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



이 프로세스는 다음을 생성합니다. *tar* 문제 해결을 위해 NetApp 과 공유할 수 있는 언급된 위치에 패키지가 있습니다.

3. 파일을 다운로드한 후 Keystone ServiceNow 지원 티켓에 첨부할 수 있습니다. 티켓 발행에 대한 정보는 다음을 참조하세요. "[서비스 요청 생성](#)".

## 저작권 정보

Copyright © 2026 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.