Keystone wird eingerichtet und konfiguriert

Keystone

NetApp
February 19, 2026

Inhalt

Keystone wird eingerichtet und konfiguriert

Anforderungen

Anforderungen an die virtuelle Infrastruktur für Keystone Collector

Ihr VMware vSphere System muss mehrere Anforderungen erfüllen, bevor Sie Keystone Collector installieren können.

Voraussetzungen für die Keystone Collector-Server-VM:

- Betriebssystem: VMware vCenter Server und ESXi 8.0 oder höher
- Kern: 1 CPU
- RAM: 2 GB RAM
- Festplattenspeicher: 20 GB vDisk

Andere Anforderungen

Stellen Sie sicher, dass die folgenden allgemeinen Anforderungen erfüllt sind:

Netzwerkanforderungen

Die Netzwerkanforderungen von Keystone Collector sind in der folgenden Tabelle aufgeführt.

Keystone Collector erfordert Internetverbindung. Sie können Internet-Konnektivität durch direktes Routing über Standard-Gateway (über NAT) oder über HTTP Proxy bereitstellen. Beide Varianten werden hier beschrieben.

Quelle	Ziel	Service	Protokoll und Ports	Kategorie	Zweck
Keystone Collector (für Keystone ONTAP)	Active IQ Unified Manager (Unified Manager)	HTTPS	TCP 443	Obligatorisch (bei Verwendung von Keystone ONTAP)	Erfassung der Nutzungsmetriken von Keystone Collector für ONTAP
Keystone Collector (für Keystone StorageGRID)	StorageGRID-Administratorknoten	HTTPS	TCP 443	Obligatorisch (bei Verwendung von Keystone StorageGRID)	Erfassung der Nutzungsmetriken von Keystone Collector für StorageGRID
Keystone Collector (allgemein)	Internet (gemäß URL-Anforderungen, die später angegeben werden)	HTTPS	TCP 443	Obligatorisch (Internetverbindung)	Keystone Collector, OS-Updates und Uploads von Metriken

Keystone Collector (allgemein)	HTTP-Proxy des Kunden	HTTP-Proxy	Proxy-Port Des Kunden	Obligatorisch (Internetverbindung)	Keystone Collector, OS-Updates und Uploads von Metriken
Keystone Collector (allgemein)	DNS-Server des Kunden	DNS	TCP/UDP 53	Obligatorisch	DNS-Auflösung
Keystone Collector (allgemein)	NTP-Server von Kunden	NTP	UDP 123	Obligatorisch	Zeitsynchronisierung
Keystone Collector (für Keystone ONTAP)	Unified Manager	MYSQL	TCP 3306	Optionale Funktionen	Sammlung von Performance-Kennzahlen für Keystone Collector
Keystone Collector (allgemein)	Kundenüberwachungssystem	HTTPS	TCP 7777	Optionale Funktionen	Statusberichte für Keystone Collector
Operations Workstations des Kunden	Keystone Collector	SSH	TCP 22	Vereinfachtes	Zugriff auf die Keystone Collector-Verwaltung
NetApp ONTAP-Cluster- und Node-Management-Adressen	Keystone Collector	HTTP_8000, PING	TCP 8000, ICMP Echo Request/Reply	Optionale Funktionen	Webserver für ONTAP-Firmware-Updates

Der Standardport für MySQL, 3306, ist während einer Neuinstallation von Unified Manager nur auf localhost beschränkt, was die Erfassung von Leistungsmetriken für Keystone Collector verhindert. Weitere Informationen finden Sie unter "ONTAP-Anforderungen".

URL-Zugriff

Keystone Collector benötigt Zugriff auf die folgenden Internet-Hosts:

Adresse	Grund
https://keystone.netapp.com	Keystone Collector Software-Updates und Nutzungsberichte

https://support.netapp.com	NetApp HQ für Rechnungsinformationen und AutoSupport-Lieferungen

Linux-Anforderungen für Keystone Collector

Die Vorbereitung Ihres Linux-Systems mit der erforderlichen Software gewährleistet eine präzise Installation und Datenerfassung durch Keystone Collector.

Stellen Sie sicher, dass Ihre Linux- und Keystone Collector-Server-VM über diese Konfigurationen verfügt.

Linux-Server:

- Betriebssystem: Eines der folgenden Betriebssysteme:
  - Debian 12
  - Red hat Enterprise Linux 8.6 oder höher 8.x-Versionen
  - Red Hat Enterprise Linux 9.0 oder spätere Versionen
  - CentOS 7 (nur für vorhandene Umgebungen)
- Synchronisierungszeit synchronisiert
- Zugriff auf die standardmäßigen Linux-Software-Repositorys

Der gleiche Server sollte auch die folgenden Drittanbieter-Pakete haben:

- Podman (POD Manager)
- sos
- Chrony
- Python 3 (3.9.14 bis 3.11.8)

Keystone Collector-Server-VM:

- Core: 2 CPUs
- RAM: 4 GB RAM
- Festplattenspeicher: 50 GB vDisk

Andere Anforderungen

Stellen Sie sicher, dass die folgenden allgemeinen Anforderungen erfüllt sind:

Netzwerkanforderungen

Die Netzwerkanforderungen von Keystone Collector sind in der folgenden Tabelle aufgeführt.

Keystone Collector erfordert Internetverbindung. Sie können Internet-Konnektivität durch direktes Routing über Standard-Gateway (über NAT) oder über HTTP Proxy bereitstellen. Beide Varianten werden hier beschrieben.

Quelle	Ziel	Service	Protokoll und Ports	Kategorie	Zweck

Keystone Collector (für Keystone ONTAP)	Active IQ Unified Manager (Unified Manager)	HTTPS	TCP 443	Obligatorisch (bei Verwendung von Keystone ONTAP)	Erfassung der Nutzungsmetriken von Keystone Collector für ONTAP
Keystone Collector (für Keystone StorageGRID)	StorageGRID-Administratorknoten	HTTPS	TCP 443	Obligatorisch (bei Verwendung von Keystone StorageGRID)	Erfassung der Nutzungsmetriken von Keystone Collector für StorageGRID
Keystone Collector (allgemein)	Internet (gemäß URL-Anforderungen, die später angegeben werden)	HTTPS	TCP 443	Obligatorisch (Internetverbindung)	Keystone Collector, OS-Updates und Uploads von Metriken
Keystone Collector (allgemein)	HTTP-Proxy des Kunden	HTTP-Proxy	Proxy-Port Des Kunden	Obligatorisch (Internetverbindung)	Keystone Collector, OS-Updates und Uploads von Metriken
Keystone Collector (allgemein)	DNS-Server des Kunden	DNS	TCP/UDP 53	Obligatorisch	DNS-Auflösung
Keystone Collector (allgemein)	NTP-Server von Kunden	NTP	UDP 123	Obligatorisch	Zeitsynchronisierung
Keystone Collector (für Keystone ONTAP)	Unified Manager	MYSQL	TCP 3306	Optionale Funktionen	Sammlung von Performance-Kennzahlen für Keystone Collector
Keystone Collector (allgemein)	Kundenüberwachungssystem	HTTPS	TCP 7777	Optionale Funktionen	Statusberichte für Keystone Collector
Operations Workstations des Kunden	Keystone Collector	SSH	TCP 22	Vereinfachtes	Zugriff auf die Keystone Collector-Verwaltung

NetApp ONTAP-Cluster- und Node-Management-Adressen	Keystone Collector	HTTP_8000, PING	TCP 8000, ICMP Echo Request/Reply	Optionale Funktionen	Webserver für ONTAP-Firmware-Updates

Der Standardport für MySQL, 3306, ist während einer Neuinstallation von Unified Manager nur auf localhost beschränkt, was die Erfassung von Leistungsmetriken für Keystone Collector verhindert. Weitere Informationen finden Sie unter "ONTAP-Anforderungen".

URL-Zugriff

Keystone Collector benötigt Zugriff auf die folgenden Internet-Hosts:

Adresse	Grund
https://keystone.netapp.com	Keystone Collector Software-Updates und Nutzungsberichte
https://support.netapp.com	NetApp HQ für Rechnungsinformationen und AutoSupport-Lieferungen

Anforderungen an ONTAP und StorageGRID für Keystone

Bevor Sie mit Keystone beginnen, müssen Sie sicherstellen, dass ONTAP-Cluster und StorageGRID-Systeme einige Anforderungen erfüllen.

ONTAP

Softwareversionen

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

Bevor Sie beginnen

Erfüllen Sie die folgenden Anforderungen, wenn Sie Nutzungsdaten nur über ONTAP erfassen möchten:

1. Stellen Sie sicher, dass ONTAP 9.8 oder höher konfiguriert ist. Informationen zum Konfigurieren eines neuen Clusters finden Sie unter den folgenden Links:
   - "Konfigurieren Sie ONTAP mit System Manager in einem neuen Cluster"
   - "Richten Sie ein Cluster mit der CLI ein"
2. Erstellen Sie ONTAP Anmeldekonten mit bestimmten Rollen. Weitere Informationen finden Sie unter "Erfahren Sie mehr über das Erstellen von ONTAP-Anmeldekonten".
   - **Web UI**
     i. Melden Sie sich mit Ihren Standardanmeldeinformationen bei ONTAP System Manager an. Weitere Informationen finden Sie unter "Cluster-Management mit System Manager".
     ii. Erstellen Sie einen ONTAP-Benutzer mit der Rolle „Readonly“ und dem Anwendungstyp „http“, und aktivieren Sie die Kennwortauthentifizierung, indem Sie zu **Cluster > Einstellungen > Sicherheit > Benutzer** navigieren.
   - **CLI**
     i. Melden Sie sich bei der ONTAP CLI mit Ihren Standardanmeldeinformationen an. Weitere Informationen finden Sie unter "Cluster-Management mit CLI".
     ii. Erstellen Sie einen ONTAP-Benutzer mit der Rolle „Readonly“ und dem Anwendungstyp „http“, und aktivieren Sie die Kennwortauthentifizierung. Weitere Informationen zur Authentifizierung finden Sie unter "Aktivieren Sie den Zugriff auf das Kennwort des ONTAP-Kontos".

Erfüllen Sie die folgenden Anforderungen, wenn Sie Nutzungsdaten über Active IQ Unified Manager erfassen möchten:

1. Vergewissern Sie sich, dass Unified Manager 9.10 oder höher konfiguriert ist. Informationen zum Installieren von Unified Manager finden Sie unter den folgenden Links:
   - "Installation von Unified Manager auf VMware vSphere Systemen"
   - "Installation von Unified Manager auf Linux Systemen"
2. Stellen Sie sicher, dass das ONTAP-Cluster zu Unified Manager hinzugefügt wurde. Informationen zum Hinzufügen von Clustern finden Sie unter "Hinzufügen von Clustern".
3. Erstellen Sie Unified Manager Benutzer mit spezifischen Rollen für die Erfassung von Nutzungs- und Performance-Daten. Führen Sie diese Schritte aus. Informationen zu Benutzerrollen finden Sie unter "Definitionen von Benutzerrollen".
   a. Melden Sie sich bei der Unified Manager-Web-Benutzeroberfläche mit den Standardanmeldeinformationen des Anwendungsadministrators an, die während der Installation generiert werden. Siehe "Zugriff auf die Web-Benutzeroberfläche von Unified Manager".
   b. Erstellen Sie mit ein Servicekonto für Keystone Collector `Operator` Benutzerrolle. Die Keystone Collector Service-APIs verwenden dieses Servicekonto für die Kommunikation mit Unified

Manager und die Erfassung von Nutzungsdaten. Siehe "Benutzer hinzufügen".

c. Erstellen Sie ein `Database` Benutzerkonto, mit `Report Schema` Rolle: Dieser Benutzer ist für die Erfassung von Leistungsdaten erforderlich. Siehe "Erstellen eines Datenbankbenutzers".

> ⓘ Der Standardport für MySQL, 3306, ist während einer Neuinstallation von Unified Manager nur auf localhost beschränkt, wodurch die Erfassung von Performance-Daten für Keystone ONTAP verhindert wird. Diese Konfiguration kann geändert und die Verbindung kann über die Option in der Wartungskonsole von Unified Manager anderen Hosts zur Verfügung gestellt werden `Control access to MySQL port 3306` . Weitere Informationen finden Sie unter "Zusätzliche Menüoptionen".

4. Aktivieren Sie API Gateway in Unified Manager. Keystone Collector verwendet die API-Gateway-Funktion zur Kommunikation mit ONTAP-Clustern. Sie können das API-Gateway entweder über die Web-UI oder durch Ausführen einiger Befehle über die Unified Manager-CLI aktivieren.

   Web-UI

   Um das API-Gateway über die Web-Benutzeroberfläche von Unified Manager zu aktivieren, melden Sie sich bei der Web-UI von Unified Manager an und aktivieren Sie das API-Gateway. Weitere Informationen finden Sie unter "Aktivieren des API-Gateways".

   CLI

   Um API Gateway über die Unified Manager CLI zu aktivieren, gehen Sie wie folgt vor:

   a. Starten Sie auf dem Unified Manager-Server eine SSH-Session und melden Sie sich bei der Unified Manager CLI an.
   `um cli login -u <*umadmin*>`Informationen zu CLI-Befehlen finden Sie unter "Unterstützte CLI-Befehle von Unified Manager".

   b. Überprüfen Sie, ob das API-Gateway bereits aktiviert ist.
   `um option list api.gateway.enabled`A `true` Wert gibt an, dass das API-Gateway aktiviert ist.

   c. Wenn der zurückgegebene Wert ist `false`, Führen Sie diesen Befehl aus:
   `um option set api.gateway.enabled=true`

   d. Starten Sie den Unified Manager Server neu:

   - Linux "Neustart Von Unified Manager".
   - VMware vSphere: "Starten Sie die Virtual Machine von Unified Manager neu".

StorageGRID

Die folgenden Konfigurationen sind für die Installation von Keystone Collector auf StorageGRID erforderlich.

- StorageGRID `11.6.0` Oder höher sollte installiert werden. Informationen zum Aktualisieren von StorageGRID finden Sie unter "Upgrade der StorageGRID Software: Übersicht".
- Für die Erfassung von Nutzungsdaten sollte ein lokales StorageGRID-Administratorbenutzerkonto erstellt werden. Dieses Servicekonto wird vom Keystone Collector Service für die Kommunikation mit StorageGRID über Administrator-Node-APIs verwendet.

  Schritte

  a. Melden Sie sich beim Grid Manager an. Siehe "Melden Sie sich beim Grid Manager an".

b. Erstellen Sie eine lokale Administratorgruppe mit `Access mode: Read-only`. Siehe "Erstellen einer Admin-Gruppe".

c. Fügen Sie die folgenden Berechtigungen hinzu:

   - Mandantenkonten
   - Wartung
   - Abfrage Von Kennzahlen

d. Erstellen Sie einen Keystone Service-Account-Benutzer und verknüpfen Sie ihn mit der Administratorgruppe. Siehe "Benutzer managen".

Installieren Sie Keystone Collector

Implementieren Sie Keystone Collector auf VMware vSphere Systemen

Die Bereitstellung von Keystone Collector auf VMware vSphere Systemen umfasst das Herunterladen der OVA-Vorlage, die Bereitstellung der Vorlage mithilfe des Assistenten **OVF-Vorlage** bereitstellen, die Integrität der Zertifikate überprüfen und die Bereitschaft der VM überprüfen.

Bereitstellen der OVA-Vorlage

Führen Sie hierzu folgende Schritte aus:

Schritte

1. Laden Sie die OVA-Datei von herunter "Dieser Link" Auf Ihrem VMware vSphere System speichern.
2. Navigieren Sie auf Ihrem VMware vSphere System zur Ansicht **VMs und Vorlagen**.
3. Klicken Sie mit der rechten Maustaste auf den gewünschten Ordner für die virtuelle Maschine (VM) (oder das Rechenzentrum, falls keine VM-Ordner verwendet werden) und wählen Sie **OVF-Vorlage bereitstellen** aus.
4. Klicken Sie auf *Schritt 1* des Assistenten * OVF-Vorlage bereitstellen* auf **Auswählen und OVF-Vorlage**, um das heruntergeladene auszuwählen `KeystoneCollector-latest.ova` Datei:
5. Geben Sie unter *Schritt 2* den VM-Namen an und wählen Sie den VM-Ordner aus.
6. Geben Sie in *Schritt 3* die erforderliche Computing-Ressource an, die zur Ausführung der VM erforderlich ist.
7. Bei Schritt 4: Details überprüfen, vergewissern Sie sich, dass die OVA-Datei korrekt und authentisch ist.

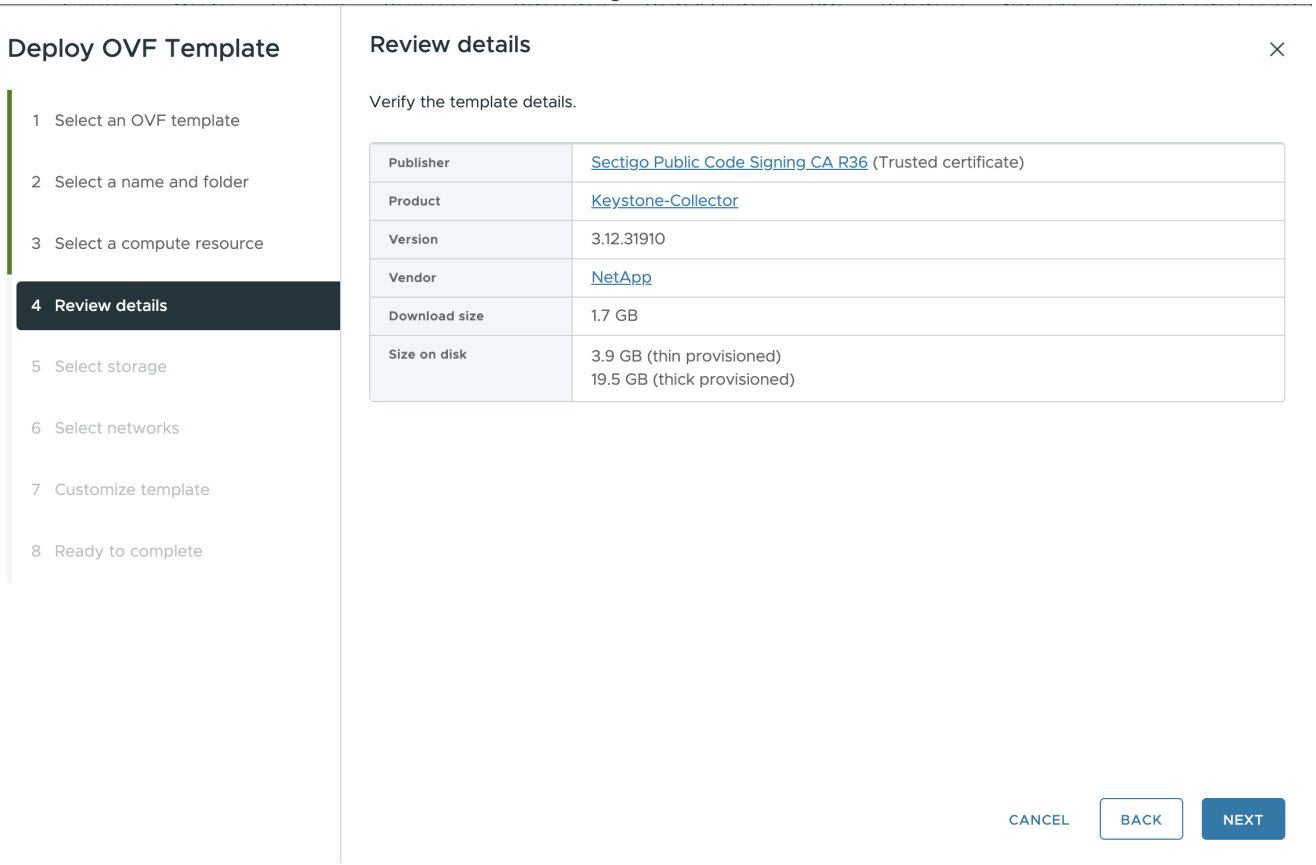
   Der vCenter-Root-Truststore enthält nur VMware-Zertifikate. NetApp verwendet Entrust als Zertifizierungsstelle und diese Zertifikate müssen dem vCenter Trust Store hinzugefügt werden.

   a. Laden Sie das Code-Signatur-CA-Zertifikat von Sectigo herunter. "Hier"Die

   b. Befolgen Sie die Schritte unter `Resolution` Abschnitt dieses Knowledge Base-Artikels (KB): https://kb.vmware.com/s/article/84240.

   > ⓘ Für vCenter Versionen 7.x und älter müssen Sie vCenter und ESXi auf Version 8.0 oder höher aktualisieren. Ältere Versionen werden nicht mehr unterstützt.

Sobald die Integrität und Authentizität der Keystone Collector OVA bestätigt sind, können Sie den Text sehen. `(Trusted certificate)` mit dem Verlag.



8. Geben Sie in *Schritt 5* des Assistenten * OVF-Vorlage bereitstellen* den Speicherort für die VM an.
9. Wählen Sie bei *Schritt 6* das Zielnetzwerk aus, das die VM verwenden soll.
10. Geben Sie in *Schritt 7 Vorlage anpassen* die ursprüngliche Netzwerkadresse und das Kennwort für das Admin-Benutzerkonto an.

> Das Admin-Passwort wird in einem umkehrbaren Format in vCenter gespeichert und sollte als Bootstrap-Anmeldeinformationen verwendet werden, um ersten Zugriff auf das VMware vSphere-System zu erhalten. Dieses Admin-Passwort sollte während der anfänglichen Softwarekonfiguration geändert werden. Die Subnetzmaske für die IPv4-Adresse sollte in CIDR-Notation bereitgestellt werden. Verwenden Sie beispielsweise den Wert 24 für eine Subnetzmaske von 255.255.255.0.

11. Prüfen Sie bei *Schritt 8 Ready to complete* des Assistenten **Deploy OVF Template** die Konfiguration und stellen Sie sicher, dass Sie die Parameter für die OVA-Bereitstellung richtig eingestellt haben.

Nachdem die VM aus der Vorlage implementiert und eingeschaltet wurde, öffnen Sie eine SSH-Sitzung für die VM, und loggen Sie sich mit den temporären Administratorberechtigungen ein, um zu überprüfen, ob die VM bereit für die Konfiguration ist.

Erstkonfiguration des Systems

Führen Sie diese Schritte auf Ihren VMware vSphere-Systemen für die Erstkonfiguration der über OVA bereitgestellten Keystone Collector-Server durch:

Nach Abschluss der Implementierung können Sie die Konfigurations- und Überwachungsaktivitäten über das Dienstprogramm Keystone Collector Management Terminal User Interface (TUI) durchführen. Sie können verschiedene Tastaturbedienungen wie die Eingabetaste und die Pfeiltasten verwenden, um die Optionen auszuwählen und durch diese TUI zu navigieren.

1. Öffnen Sie eine SSH-Sitzung für den Keystone Collector-Server. Wenn Sie eine Verbindung herstellen, werden Sie vom System aufgefordert, das Admin-Passwort zu aktualisieren. Füllen Sie bei Bedarf das Update des Admin-Passworts aus.
2. Melden Sie sich mit dem neuen Passwort an, um auf die TUI zuzugreifen. Beim Anmelden wird die TUI angezeigt.

   Alternativ können Sie es manuell starten, indem Sie den ausführen `keystone-collector-tui` CLI-Befehl.
3. Konfigurieren Sie bei Bedarf die Proxy-Details im Abschnitt **Konfiguration > Netzwerk** auf der TUI.
4. Konfigurieren Sie im Abschnitt **Konfiguration > System** den Hostnamen, den Speicherort und den NTP-Server des Systems.
5. Aktualisieren Sie die Keystone Collectors mit der Option **Wartung > Collectors aktualisieren**. Starten Sie nach der Aktualisierung das TUI-Dienstprogramm für die Verwaltung des Keystone Collectors neu, um die Änderungen anzuwenden.

Installieren Sie Keystone Collector auf Linux Systemen

Sie können die Keystone Collector-Software auf einem Linux-Server mit einem RPM oder einem Debian-Paket installieren. Führen Sie die Installationsschritte je nach Linux-Distribution aus.

RPM wird verwendet

1. SSH auf den Keystone Collector Server und erhöhen auf `root` Berechtigung.
2. Importieren Sie die öffentliche Keystone -Signatur:
   `# rpm --import https://keystone.netapp.com/repo1/RPM-GPG-NetApp-Keystone-20251020`
3. Stellen Sie sicher, dass das richtige öffentliche Zertifikat importiert wurde, indem Sie den Fingerabdruck für die Keystone Billing Platform in der RPM-Datenbank überprüfen:
   `# rpm -qa gpg-pubkey --qf '%{Description}'|gpg --show-keys --fingerprint` Der korrekte Fingerabdruck sieht so aus:
   `9297 0DB6 0867 22E7 7646 E400 4493 5CBB C9E9 FEDC`
4. Laden Sie die `keystonerepo.rpm` Datei:
   `curl -O https://keystone.netapp.com/repo1/keystonerepo.rpm`
5. Überprüfen Sie die Echtheit der Datei:
   `rpm --checksig -v keystonerepo.rpm` Eine Signatur für eine authentische Datei sieht folgendermaßen aus:
   `Header V4 RSA/SHA512 Signature, key ID c9e9fedc: OK`
6. Installieren Sie die YUM-Software-Repository-Datei:
   `# yum install keystonerepo.rpm`
7. Wenn Keystone Repo installiert ist, installieren Sie das Keystone-Collector-Paket über den YUM-Paketmanager:

   `# yum install keystone-collector`

   Führen Sie für Red Hat Enterprise Linux 9 den folgenden Befehl aus, um das Keystone-Collector-Paket zu installieren:
   `# yum install keystone-collector-rhel9`

Debian Verwenden

1. SSH zum Keystone Collector Server und Zugriff auf `root` Berechtigungen.
   `sudo su`
2. Laden Sie die Datei herunter `keystone-sw-repo.deb`:
   `curl -O https://keystone.netapp.com/downloads/keystone-sw-repo.deb`
3. Keystone-Software-Repository-Datei installieren:
   `# dpkg -i keystone-sw-repo.deb`
4. Paketliste aktualisieren:
   `# apt-get update`
5. Installieren Sie beim Installieren des Keystone-Repo das Keystone-Collector-Paket:
   `# apt-get install keystone-collector`

Nach Abschluss der Installation können Sie das Dienstprogramm „Keystone Collector Management Terminal User Interface (TUI)“ verwenden, um die Konfigurations- und Überwachungsaktivitäten durchzuführen. Sie können verschiedene Tastaturbedienungen wie die Eingabetaste und die Pfeiltasten verwenden, um die Optionen auszuwählen und durch diese TUI zu navigieren. Siehe "Konfigurieren Sie Keystone Collector" Und "Systemzustand überwachen" Zur Information.

Automatische Validierung der Keystone Software

Das Keystone Repository ist so konfiguriert, dass die Integrität der Keystone Software automatisch überprüft wird, sodass an Ihrem Standort nur gültige und authentische Software installiert wird.

Die in bereitgestellte Keystone YUM Repository-Client-Konfiguration `keystonerepo.rpm` verwendet die erzwungene GPG-Prüfung (`gpgcheck=1`) für alle Software, die über dieses Repository heruntergeladen wird. Alle RPM, die über das Keystone-Repository heruntergeladen werden, das die Signaturvalidierung fehlschlägt, wird nicht installiert. Diese Funktion wird in der Funktion für die automatische Aktualisierung nach Zeitplan von Keystone Collector verwendet, um sicherzustellen, dass nur gültige und authentische Software an Ihrem Standort installiert wird.

Konfigurieren Sie Keystone Collector

Sie müssen einige Konfigurationsaufgaben ausführen, damit Keystone Collector Nutzungsdaten in Ihrer Speicherumgebung erfasst. Dies ist eine einmalige Aktivität zur Aktivierung und Zuordnung der erforderlichen Komponenten zu Ihrer Storage-Umgebung.

- Keystone Collector stellt Ihnen das Dienstprogramm „Keystone Collector Management Terminal User Interface (TUI)“ zur Verfügung, mit dem Sie Konfigurations- und Überwachungsaktivitäten durchführen können. Sie können verschiedene Tastaturbedienungen wie die Eingabetaste und die Pfeiltasten verwenden, um die Optionen auszuwählen und durch diese TUI zu navigieren.
- Keystone Collector kann für Organisationen konfiguriert werden, die keinen Internetzugang haben, auch als *dark site* oder *private Mode* bezeichnet. Weitere Informationen zu finden Sie unter "Keystone im privaten Modus".

Schritte

1. Starten Sie das Management-TUI-Dienstprogramm Keystone Collector:
   ```
   $ keystone-collector-tui
   ```
2. Gehen Sie zu **Konfigurieren > KS-Collector**, um den Konfigurationsbildschirm von Keystone Collector zu öffnen und die verfügbaren Optionen für das Update anzuzeigen.
3. Aktualisieren Sie die erforderlichen Optionen.

-

- **Collect ONTAP usage**: Diese Option ermöglicht die Erfassung von Nutzungsdaten für ONTAP. Fügen Sie die Details zum Active IQ Unified Manager-Server (Unified Manager) und zum Service-Konto hinzu.
- **Collect ONTAP Leistungsdaten**: Diese Option ermöglicht die Erfassung von Leistungsdaten für ONTAP. Dies ist standardmäßig deaktiviert. Aktivieren Sie diese Option, wenn in Ihrer Umgebung Performance-Monitoring für SLA-Zwecke erforderlich ist. Geben Sie Details zum Benutzerkonto für die Unified Manager Database an. Informationen zum Erstellen von Datenbankbenutzern finden Sie unter "Erstellen von Unified Manager-Benutzern".
- **Private Daten entfernen**: Diese Option entfernt bestimmte private Daten von Kunden und ist standardmäßig aktiviert. Informationen darüber, welche Daten von den Metriken ausgeschlossen werden, wenn diese Option aktiviert ist, finden Sie unter "Begrenzung der Erhebung privater Daten".

** – StorageGRK **

- **Collect StorageGRID Usage**: Diese Option ermöglicht die Erfassung von Node Usage Details. Fügen Sie die StorageGRID-Node-Adresse und Benutzerdetails hinzu.
- **Private Daten entfernen**: Diese Option entfernt bestimmte private Daten von Kunden und ist standardmäßig aktiviert. Informationen darüber, welche Daten von den Metriken ausgeschlossen werden, wenn diese Option aktiviert ist, finden Sie unter "Begrenzung der Erhebung privater Daten".

4. Schalten Sie das Feld **KS-Collector mit System** ein.
5. Klicken Sie Auf **Speichern**
.

6. Stellen Sie sicher, dass sich Keystone Collector in einem gesunden Zustand befindet, indem Sie zum Hauptbildschirm der TUI zurückkehren und die **Service Status**-Informationen überprüfen. Das System sollte zeigen, dass die Dienste in einem **insgesamt: Gesund** Status sind.

7. Beenden Sie die Keystone Collector Management TUI, indem Sie auf dem Home-Bildschirm die Option **Exit to Shell** auswählen.

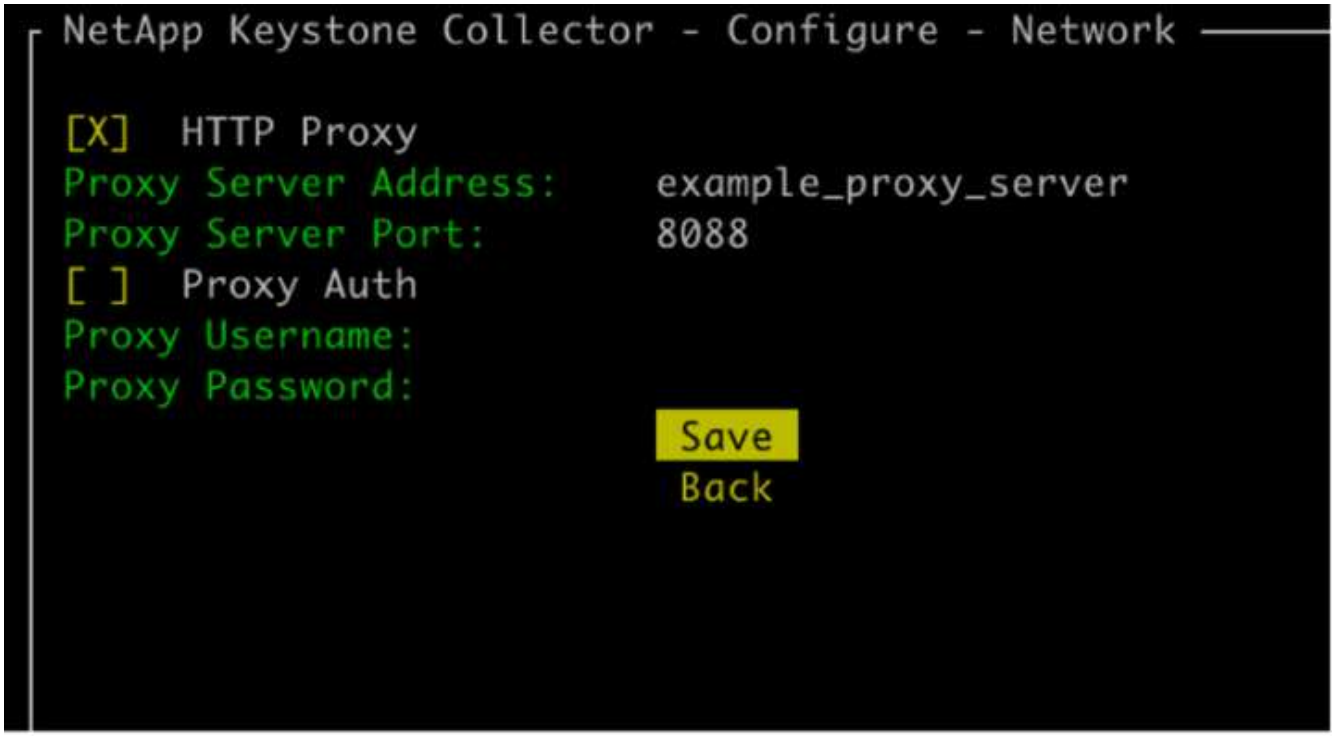
Konfigurieren Sie HTTP-Proxy auf Keystone Collector

Die Collector-Software unterstützt die Verwendung eines HTTP-Proxys für die Kommunikation mit dem Internet. Diese kann in der TUI konfiguriert werden.

Schritte

1. Starten Sie das Keystone Collector Management TUI Utility neu, falls es bereits geschlossen wurde:
   `$ keystone-collector-tui`
2. Schalten Sie das Feld **HTTP Proxy** ein und fügen Sie die Details für den HTTP Proxy-Server, den Port und die Anmeldeinformationen hinzu, falls eine Authentifizierung erforderlich ist.

3. Klicken Sie Auf **Speichern**
.



Begrenzung der Erhebung privater Daten

Keystone Collector erfasst begrenzte Konfigurations-, Status- und Performance-Informationen, die für die Durchführung der Abonnementmessung erforderlich sind. Es besteht die Möglichkeit, die gesammelten Informationen durch Maskierung sensibler Informationen aus dem hochgeladenen Inhalt weiter einzuschränken. Dies hat keine Auswirkung auf die Berechnung der Abrechnung. Eine Einschränkung der Informationen kann sich jedoch auf die Nutzbarkeit der Berichtsinformationen auswirken, da einige Elemente, die leicht von Benutzern identifiziert werden können, wie z. B. der Volumenname, durch UUIDs ersetzt werden.

Die Begrenzung der Erfassung bestimmter Kundendaten ist eine konfigurierbare Option auf dem Keystone Collector TUI-Bildschirm. Diese Option, **Private Daten entfernen**, ist standardmäßig aktiviert.

Informationen zu den Elementen, die zur Beschränkung des Zugriffs auf private Daten in ONTAP und StorageGRID entfernt wurden, finden Sie unter "Liste der bei der Beschränkung des Zugriffs auf private Daten entfernten Elemente".

Einer benutzerdefinierten Stammzertifizierungsstelle vertrauen

Die Überprüfung von Zertifikaten gegen eine öffentliche Stammzertifizierungsstelle (CA) ist Teil der Sicherheitsfunktionen von Keystone Collector. Falls erforderlich, können Sie Keystone Collector jedoch so konfigurieren, dass eine benutzerdefinierte Stammzertifizierungsstelle vertrauenswürdig ist.

Wenn Sie SSL/TLS-Prüfung in Ihrer System-Firewall verwenden, wird der internetbasierte Datenverkehr mit Ihrem benutzerdefinierten CA-Zertifikat erneut verschlüsselt. Die Einstellungen müssen konfiguriert werden, um die Quelle als vertrauenswürdige CA zu überprüfen, bevor das Stammzertifikat akzeptiert und Verbindungen zugelassen werden. Führen Sie hierzu folgende Schritte aus:

Schritte

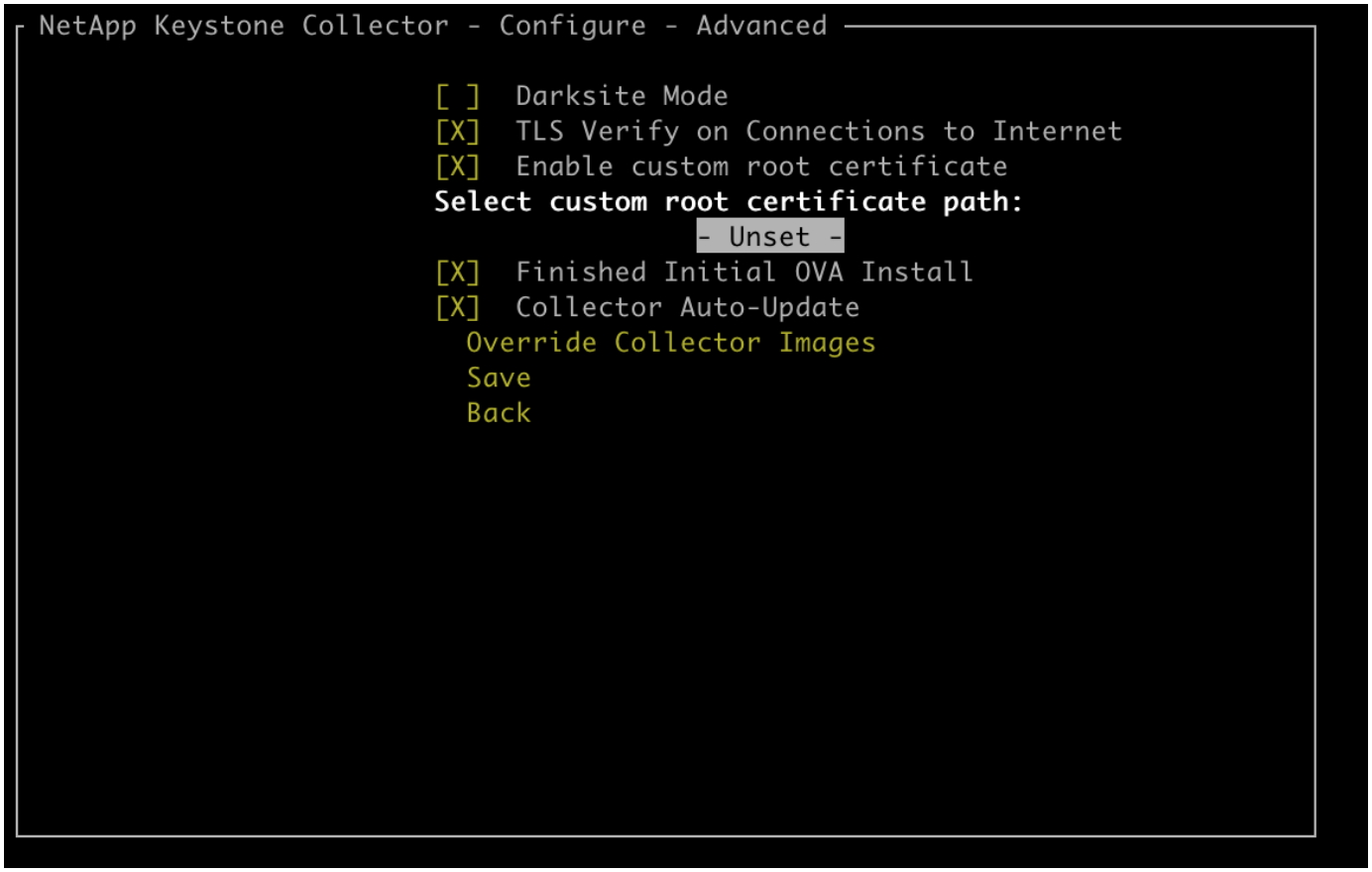
1. Vorbereiten des CA-Zertifikats. Es sollte im *base64-kodierten X.509*-Dateiformat vorliegen.

   Die unterstützten Dateierweiterungen sind `.pem`, `.crt`, `.cert`. Stellen Sie sicher, dass sich das Zertifikat in einem dieser Formate befindet.

2. Kopieren Sie das Zertifikat auf den Keystone Collector-Server. Notieren Sie sich den Speicherort, an den die Datei kopiert wird.
3. Öffnen Sie ein Terminal auf dem Server und führen Sie das Management-TUI-Dienstprogramm aus.
   `$ keystone-collector-tui`
4. Gehen Sie zu **Konfiguration > Erweitert**.

5. Aktivieren Sie die Option **Benutzerdefiniertes Stammzertifikat aktivieren**.
6. Wählen Sie für **Select Custom root Certificate path:** aus `- Unset -`
7. Drücken Sie Die Eingabetaste. Ein Dialogfeld zur Auswahl des Zertifikatspfads wird angezeigt.
8. Wählen Sie das Stammzertifikat im Dateisystem-Browser aus, oder geben Sie den genauen Pfad ein.
9. Drücken Sie Die Eingabetaste. Sie kehren zum **Advanced**-Bildschirm zurück.
10. Wählen Sie **Speichern**. Die Konfiguration wird angewendet.

Das CA-Zertifikat wird kopiert an `/opt/netapp/ks-collector/ca.pem` auf dem Keystone Collector-Server.



Erstellung Von Performance-Service-Leveln

Sie können Performance Service Levels (PSLs) mit dem TUI-Verwaltungsdienstprogramm von Keystone Collector erstellen. Beim Erstellen von PSLs über die TUI werden automatisch die für jedes Leistungsservicelevel festgelegten Standardwerte ausgewählt. Dadurch wird die Wahrscheinlichkeit von Fehlern verringert, die beim manuellen Festlegen dieser Werte beim Erstellen von PSLs über Active IQ Unified Manager auftreten können.

Weitere Informationen zu PSLs finden Sie unter "Performance Service Level".

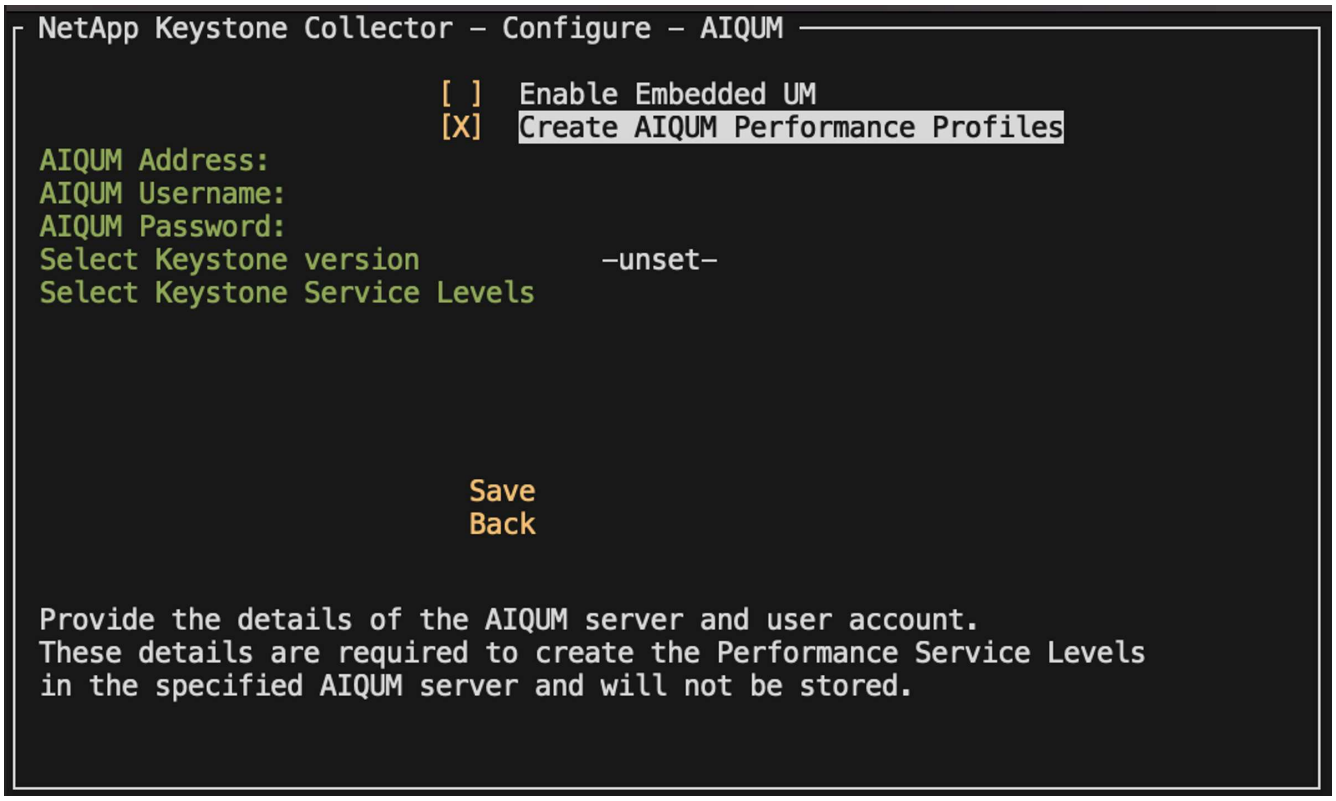
Weitere Informationen zu Service-Levels finden Sie unter "Service-Level bei Keystone".

Schritte

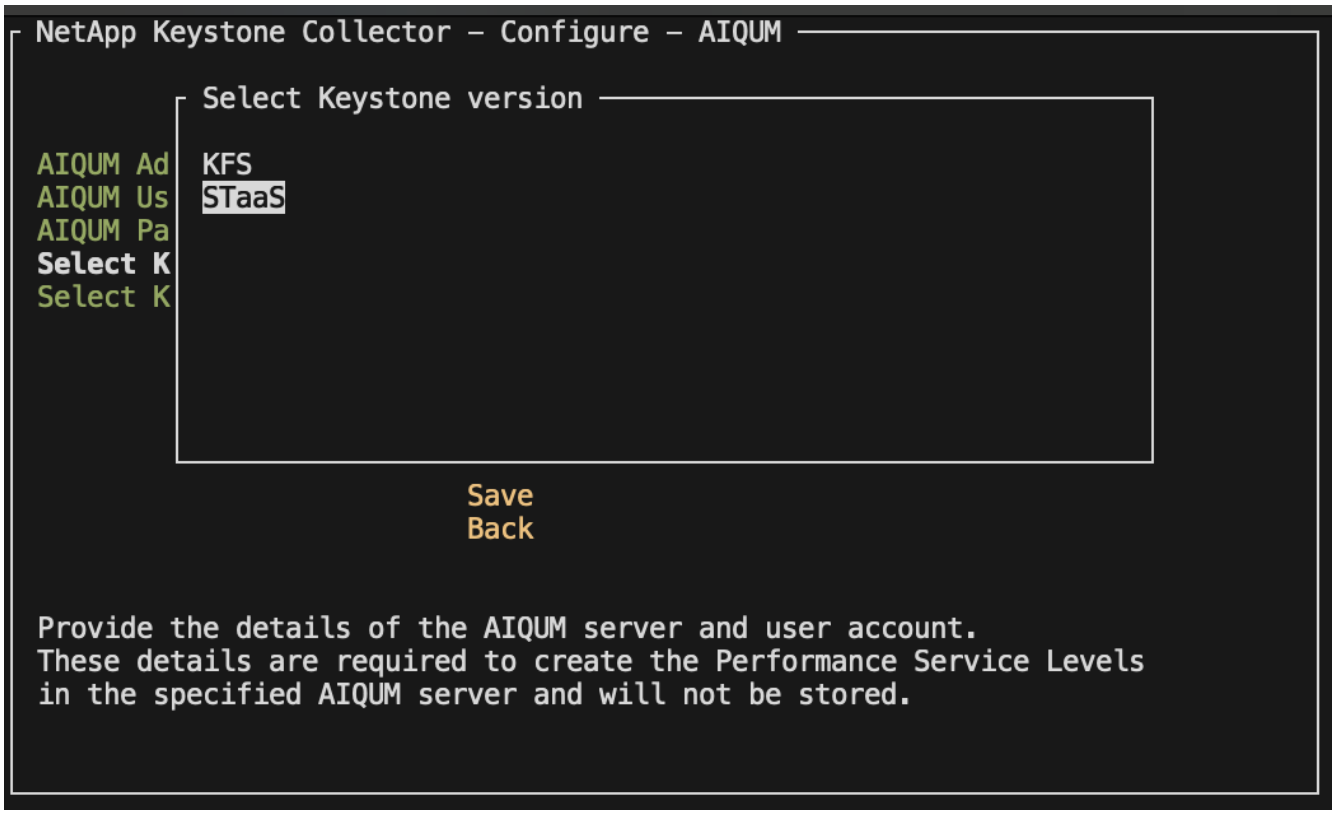
1. Starten Sie das Management-TUI-Dienstprogramm Keystone Collector:

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

2. Gehen Sie zu **Configure>AIQUM**, um den AIQUM-Bildschirm zu öffnen.
3. Aktivieren Sie die Option **AIQUM-Leistungsprofile erstellen**.
4. Geben Sie die Details des Active IQ Unified Manager-Servers und des Benutzerkontos ein. Diese Angaben sind zum Erstellen von PSLs erforderlich und werden nicht gespeichert.

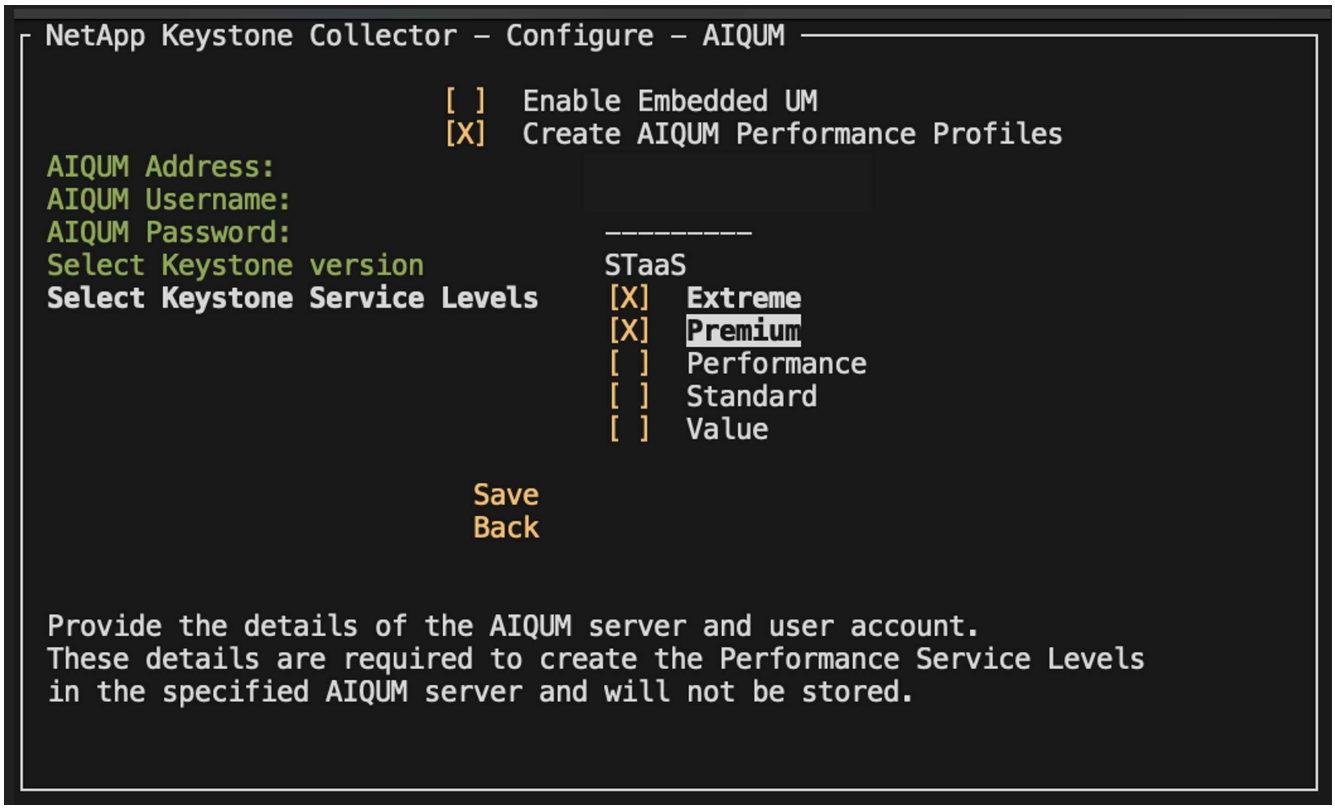


5. Wählen Sie für **Keystone-Version auswählen** `-unset-` .
6. Drücken Sie Die Eingabetaste. Ein Dialogfeld zur Auswahl der Keystone-Version wird angezeigt.
7. Markieren Sie **STaaS**, um die Keystone Version für Keystone STaaS anzugeben, und drücken Sie dann die Eingabetaste.



Sie können die Option **KFS** für Keystone -Abonnementdienste Version 1 hervorheben. Die Abonnementdienste von Keystone unterscheiden sich von Keystone STaaS in den Leistungsstufen, Serviceangeboten und Abrechnungsgrundsätzen. Weitere Informationen finden Sie unter"Keystone Abonnementservices von Version 1" .

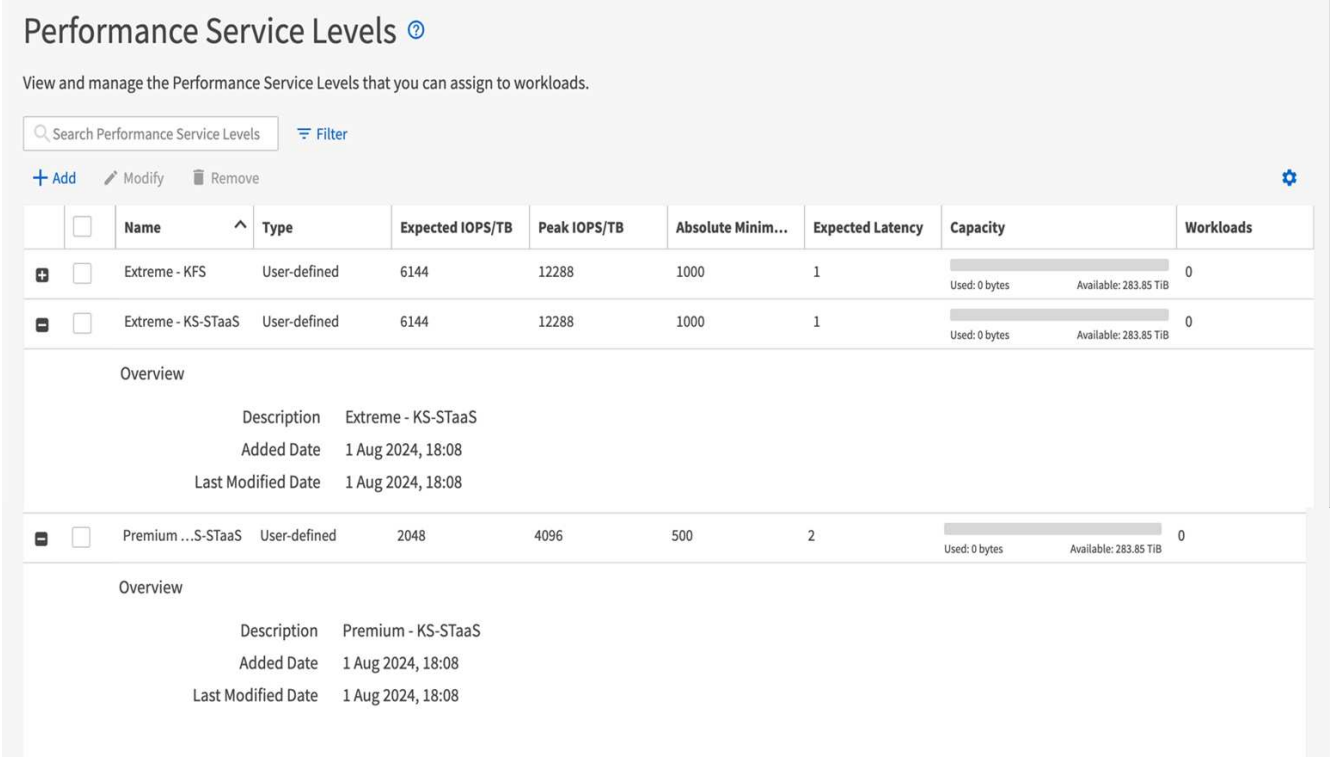
8. Alle unterstützten Keystone Leistungsservicelevel werden in der Option * Keystone -Servicelevel auswählen* für die angegebene Keystone Version angezeigt. Aktivieren Sie die gewünschten Leistungsservicelevel aus der Liste.



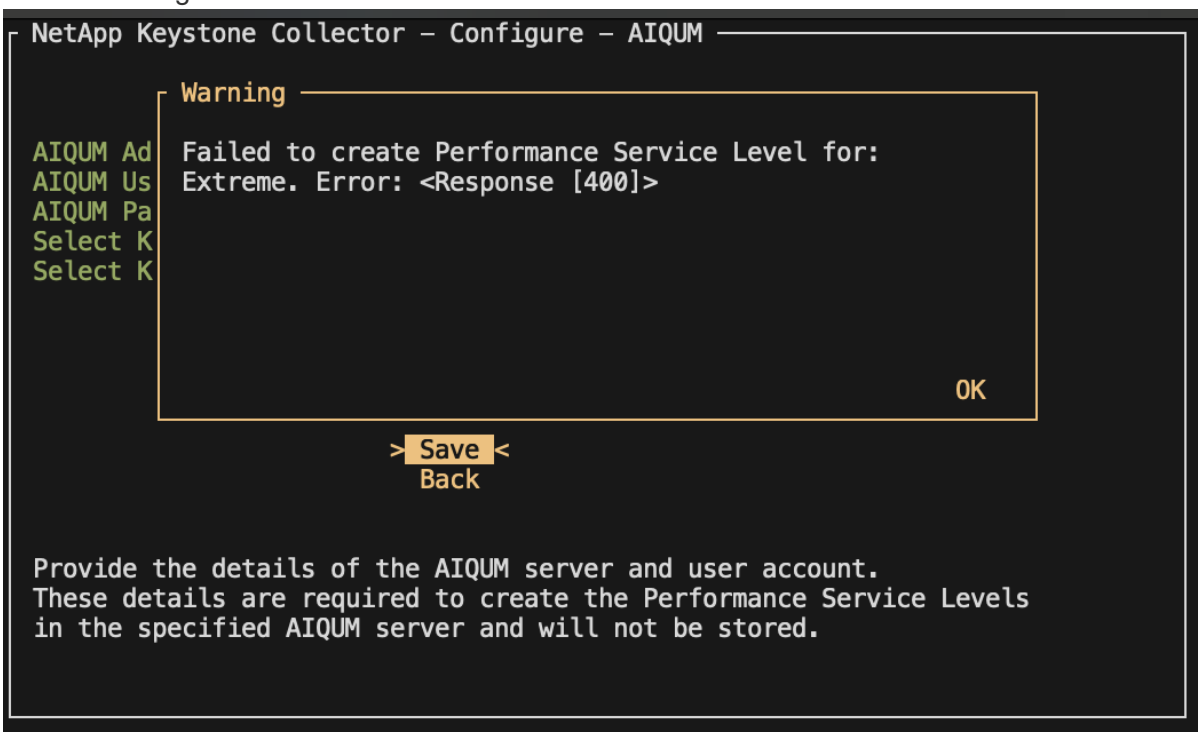
Sie können mehrere Leistungsservicelevel gleichzeitig auswählen, um PSLs zu erstellen.

9. Wählen Sie **Speichern** und drücken Sie die Eingabetaste. Performance Service Levels werden erstellt.

   Sie können die erstellten PSLs, wie Premium-KS-STaaS für STaaS oder Extreme KFS für KFS, auf der Seite **Leistungsstufen** in Active IQ Unified Manager anzeigen. Wenn die erstellten PSLs nicht Ihren Anforderungen entsprechen, können Sie PSLs an Ihre Anforderungen anpassen. Weitere Informationen finden Sie unter "Erstellen und Bearbeiten von Performance Service Levels".



Wenn auf dem angegebenen Active IQ Unified Manager-Server bereits ein PSL für das ausgewählte Performance-Service-Level vorhanden ist, können Sie es nicht erneut erstellen. Wenn Sie dies versuchen, erhalten Sie eine Fehlermeldung.



Installieren Sie ITOM Collector

Installationsvoraussetzungen für Keystone ITOM Collector

Stellen Sie vor der Installation von ITOM Collector sicher, dass Ihre Systeme mit der erforderlichen Software vorbereitet sind und alle erforderlichen Voraussetzungen erfüllen.

Voraussetzungen für die ITOM Collector-Server-VM:

- Unterstützte Betriebssysteme:
  - Debian 12 oder höher
  - Windows Server 2016 oder höher
  - Ubuntu 20.04 LTS oder höher
  - Red Hat Enterprise Linux (RHEL) 8.x
  - Red Hat Enterprise Linux 9.0 oder höher
  - Amazon Linux 2023 oder höher

  Die empfohlenen Betriebssysteme sind Debian 12, Windows Server 2016 oder neuere Versionen.

- Ressourcenanforderungen: Die VM-Ressourcenanforderungen basierend auf der Anzahl der überwachten NetApp-Knoten sind wie folgt:
  - 2-10 Knoten: 4 CPUs, 8 GB RAM, 40 GB Festplatte
  - 12-20 Knoten: 8 CPUs, 16 GB RAM, 40 GB Festplatte
- Konfigurationsanforderung: Stellen Sie sicher, dass ein schreibgeschütztes Konto und SNMP auf den überwachten Geräten konfiguriert sind. Die ITOM Collector-Server-VM muss auch als SNMP-Trap-Host und Syslog-Server auf dem NetApp-Cluster und Cluster-Switches konfiguriert werden, falls zutreffend.

Netzwerkanforderungen

Die Netzwerkanforderungen von ITOM Collector sind in der folgenden Tabelle aufgeführt.

Quelle	Ziel	Protokoll	Ports	Beschreibung
ITOM Collector	NetApp ONTAP Cluster-Management-IPs	HTTPS, SNMP	TCP 443, UDP 161	Überwachung der ONTAP Controller
NetApp ONTAP Cluster- und Node-Management-IPs	ITOM Collector	SNMP, Syslog	UDP 162, UDP 514	SNMP-Traps und Syslog von Controllern
ITOM Collector	Cluster-Switches	SNMP	UDP 161	Überwachung von Switches
Cluster-Switches	ITOM Collector	SNMP, Syslog	UDP 162, UDP 514	SNMP-Traps und Syslogs von Switches
ITOM Collector	StorageGRID-Node-IPs	HTTPS, SNMP	TCP 443, UDP 161	SNMP-Überwachung von StorageGRID

StorageGRID-Node-IPs	ITOM Collector	SNMP, Syslog	UDP 162, UDP 514	SNMP-Traps von StorageGRID
ITOM Collector	Keystone Collector	SSH, HTTPS, SNMP	TCP 22, TCP 443, UDP 161	Überwachung und Remote-Management mit Keystone Collector
ITOM Collector	Lokaler DNS	DNS	UDP 53	Öffentliche oder private DNS-Services
ITOM Collector	NTP-Server Ihrer Wahl	NTP	UDP 123	Zeitmessung

Keystone ITOM Collector auf Linux-Systemen installieren

Führen Sie einige Schritte aus, um ITOM Collector zu installieren, der Messdaten in Ihrer Speicherumgebung sammelt. Sie können es auf Windows- oder Linux-Systemen installieren, je nach Ihren Anforderungen.

Das Keystone Support-Team stellt einen dynamischen Link zum Herunterladen der Setup-Datei für ITOM Collector bereit, die innerhalb von zwei Stunden abläuft.

Informationen zur Installation von ITOM Collector auf Windows-Systemen finden Sie unter "Installieren Sie ITOM Collector auf Windows-Systemen".

Führen Sie die folgenden Schritte aus, um Software auf Ihrem Linux-Server zu installieren:

Bevor Sie beginnen

- Stellen Sie sicher, dass die Bourne Shell für das Linux-Installationsskript verfügbar ist.
- Installieren Sie das `vim-common` Paket, um die für die ITOM Collector-Setup-Datei erforderliche Binärdatei **xxd** zu erhalten.
- Stellen Sie sicher, dass der `sudo package` installiert ist, wenn Sie ITOM Collector als Benutzer ohne Root ausführen möchten.

Schritte

1. Laden Sie die ITOM-Collector-Setup-Datei auf Ihren Linux-Server herunter.
2. Öffnen Sie ein Terminal auf dem Server, und führen Sie den folgenden Befehl aus, um die Berechtigungen zu ändern und die Binärdateien ausführbar zu machen:
   `# chmod +x <installer_file_name>.bin`
3. Führen Sie den Befehl aus, um die Setup-Datei für den ITOM-Collector zu starten:
   `#./<installer_file_name>.bin`
4. Wenn Sie die Setup-Datei ausführen, werden Sie aufgefordert, Folgendes zu tun:
   a. Akzeptieren Sie die Endbenutzer-Lizenzvereinbarung (EULA).
   b. Geben Sie die Benutzerdetails für die Installation ein.
   c. Geben Sie das übergeordnete Installationsverzeichnis an.
   d. Wählen Sie die Kollektorgröße aus.

e. Geben Sie ggf. Proxy-Details an.

   Für jede Eingabeaufforderung wird eine Standardoption angezeigt. Es wird empfohlen, die Standardoption auszuwählen, es sei denn, Sie haben spezielle Anforderungen. Drücken Sie die Taste **Enter**, um die Standardoption auszuwählen. Nach Abschluss der Installation bestätigt eine Meldung, dass der ITOM Collector erfolgreich installiert wurde.

- Die ITOM Collector Setup-Datei macht Ergänzungen zu Dienst neu gestartet und Speicher-Dumps zu `/etc/sudoers` behandeln.
- Durch die Installation von ITOM Collector auf dem Linux-Server wird ein Standardbenutzer namens **ITOM** erstellt, um ITOM Collector ohne Root-Privileges auszuführen. Sie können einen anderen Benutzer auswählen oder als root ausführen, es wird jedoch empfohlen, den vom Linux-Installationsskript erstellten ITOM-Benutzer zu verwenden.

Was kommt als Nächstes?

Bei erfolgreicher Installation wenden Sie sich an das Keystone Support-Team, um die erfolgreiche Installation von ITOM Collector über das ITOM Support-Portal zu validieren. Nach der Überprüfung konfiguriert das Keystone Support-Team den ITOM Collector Remote, einschließlich weiterer Geräteerkennung und Überwachungseinrichtung, und sendet eine Bestätigung, sobald die Konfiguration abgeschlossen ist. Für Fragen oder weitere Informationen wenden Sie sich bitte an keystone.services@NetApp.com.

Keystone ITOM Collector auf Windows-Systemen installieren

Installieren Sie ITOM Collector auf einem Windows-System, indem Sie die Setup-Datei von ITOM Collector herunterladen, den InstallShield-Assistenten ausführen und die erforderlichen Monitoring-Anmeldeinformationen eingeben.

Das Keystone Support-Team stellt einen dynamischen Link zum Herunterladen der Setup-Datei für ITOM Collector bereit, die innerhalb von zwei Stunden abläuft.

Sie können es je nach Ihren Anforderungen auf Linux-Systemen installieren. Informationen zur Installation von ITOM Collector auf Linux-Systemen finden Sie unter "Installieren Sie ITOM Collector auf Linux-Systemen".

Führen Sie die folgenden Schritte aus, um die ITOM-Collector-Software auf Ihrem Windows-Server zu installieren:

Bevor Sie beginnen

Stellen Sie sicher, dass der ITOM Collector-Dienst in den Einstellungen der lokalen Sicherheitsrichtlinien des Windows-Servers unter Lokale Richtlinie/Zuweisung von Benutzerrechten als Dienst * aktiviert ist.

Schritte

1. Laden Sie die Setup-Datei für den ITOM-Collector auf Ihren Windows-Server herunter.
2. Öffnen Sie die Setup-Datei, um den InstallShield-Assistenten zu starten.
3. Akzeptieren Sie die Endbenutzer-Lizenzvereinbarung (EULA). Der InstallShield-Assistent extrahiert die erforderlichen Binärdateien und fordert Sie auf, Anmeldeinformationen einzugeben.
4. Geben Sie die Anmeldeinformationen für das Konto ein, unter dem ITOM Collector ausgeführt werden soll:
   - Wenn ITOM Collector andere Windows-Server nicht überwacht, verwenden Sie das lokale System.
   - Wenn ITOM Collector andere Windows-Server in derselben Domäne überwacht, verwenden Sie ein Domänenkonto mit lokalen Administratorberechtigungen.

- Wenn ITOM Collector andere Windows-Server überwacht, die nicht Teil derselben Domäne sind, verwenden Sie ein lokales Administratorkonto, und stellen Sie eine Verbindung zu jeder Ressource mit lokalen Administratoranmeldeinformationen her. Sie können das Kennwort so festlegen, dass es nicht abläuft, um Authentifizierungsprobleme zwischen ITOM Collector und seinen überwachten Ressourcen zu reduzieren.

5. Wählen Sie die Kollektorgröße aus. Die Standardeinstellung ist die empfohlene Größe basierend auf der Setup-Datei. Fahren Sie mit der vorgeschlagenen Größe fort, es sei denn, Sie haben bestimmte Anforderungen.
6. Wählen Sie *Next*, um mit der Installation zu beginnen. Sie können den gefüllten Ordner verwenden oder einen anderen auswählen. In einem Statusfeld wird der Installationsfortschritt angezeigt, gefolgt vom Dialogfeld InstallShield-Assistent abgeschlossen.

Was kommt als Nächstes?

Bei erfolgreicher Installation wenden Sie sich an das Keystone Support-Team, um die erfolgreiche Installation von ITOM Collector über das ITOM Support-Portal zu validieren. Nach der Überprüfung konfiguriert das Keystone Support-Team den ITOM Collector Remote, einschließlich weiterer Geräteerkennung und Überwachungseinrichtung, und sendet eine Bestätigung, sobald die Konfiguration abgeschlossen ist. Für Fragen oder weitere Informationen wenden Sie sich bitte an keystone.services@NetApp.com.

AutoSupport für Keystone konfigurieren

Bei Verwendung des AutoSupport Telemetrie-Mechanismus berechnet Keystone die Nutzung auf Basis der AutoSupport Telemetriedaten. Um die erforderliche Granularität zu erreichen, sollten Sie AutoSupport so konfigurieren, dass Keystone Daten in die täglich von den ONTAP Clustern gesendeten Support-Bundles integriert werden.

Über diese Aufgabe

Beachten Sie Folgendes, bevor Sie AutoSupport für die Einbeziehung von Keystone Daten konfigurieren.

- Sie bearbeiten die AutoSupport Telemetrieoptionen mithilfe der ONTAP CLI. Informationen zum Verwalten von AutoSupport-Services und der Administratorrolle des Systems (Clusters) finden Sie unter "AutoSupport managen – Übersicht" Und "Cluster- und SVM-Administratoren".
- Sie integrieren die Subsysteme in die täglichen und wöchentlichen AutoSupport Bundles, um eine präzise Datenerfassung für Keystone zu gewährleisten. Informationen zu AutoSupport-Subsystemen finden Sie unter "Was sind AutoSupport-Subsysteme".

Schritte

1. Melden Sie sich als Systemadministrator über SSH beim Keystone ONTAP-Cluster an. Weitere Informationen finden Sie unter "Greifen Sie über SSH auf das Cluster zu".
2. Ändern Sie den Protokollinhalt.

   - Führen Sie für ONTAP 9.16.1 und höher diesen Befehl aus, um den täglichen Protokollinhalt zu ändern:

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

Wenn der Cluster in einer MetroCluster -Konfiguration vorliegt, führen Sie diesen Befehl aus:

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

- Führen Sie für frühere ONTAP Versionen diesen Befehl aus, um den Inhalt des täglichen Protokolls zu ändern:

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

Wenn der Cluster in einer MetroCluster -Konfiguration vorliegt, führen Sie diesen Befehl aus:

```
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
```

- Führen Sie diesen Befehl aus, um den wöchentlichen Protokollinhalt zu ändern:

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

Weitere Informationen zu diesem Befehl finden Sie unter "System-Node AutoSupport löst Modify aus".

Monitoring und Upgrade

Überwachen Sie den Systemzustand von Keystone Collector

Sie können den Systemzustand von Keystone Collector mit einem beliebigen Überwachungssystem überwachen, das HTTP-Anfragen unterstützt. Durch das Monitoring des Systemzustands kann sichergestellt werden, dass Daten im Keystone Dashboard verfügbar sind.

Standardmäßig akzeptieren die Keystone Systemzustandsservices keine Verbindungen von anderen IP-Adressen als localhost. Der Keystone Zustandsendpunkt ist `/uber/health`, Und es wartet auf alle Schnittstellen des Keystone Collector Servers am Port `7777`. Bei der Abfrage wird ein HTTP-Anforderungsstatuscode mit einer JSON-Ausgabe vom Endpunkt als Antwort zurückgegeben, der den Status des Keystone Collector-Systems beschreibt.

Der JSON-Körper bietet einen allgemeinen Integritätsstatus für das `is_healthy` Attribut, das ein boolescher Wert ist; und eine detaillierte Liste der Status pro Komponente für das `component_details` Attribut. Hier ein Beispiel:

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

Diese Statuscodes werden zurückgegeben:

- **200**: Zeigt an, dass alle überwachten Komponenten gesund sind
- **503**: Zeigt an, dass eine oder mehrere Komponenten ungesund sind
- **403**: Zeigt an, dass der HTTP-Client, der den Integritätsstatus abfragt, nicht auf der *allow*-Liste steht, was eine Liste der zugelassenen Netzwerk-CIDRs ist. Für diesen Status werden keine Systemzustandsinformationen zurückgegeben. Die Liste *allow* verwendet die Netzwerk-CIDR-Methode, um zu steuern, welche Netzwerkgeräte das Keystone-Integritätssystem abfragen dürfen. Wenn Sie diesen Fehler erhalten, fügen Sie Ihr Überwachungssystem in die Liste *allow* von **Keystone Collector Management TUI > Configure > Health Monitoring** ein.

> **Linux-Benutzer, beachten Sie dieses bekannte Problem:**
>
> **Beschreibung der Ausgabe**: Keystone Collector führt eine Reihe von Containern als Teil des Verbrauchsmesssystems aus. Wenn der Red hat Enterprise Linux 8.x-Server mit den USA Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG) gehärtet wird, wurde zeitweise ein bekanntes Problem mit dem fapolicyd (File Access Policy Daemon) festgestellt. Dieses Problem wird als identifiziert "Bug 1907870". **Problemumgehung**: Bis zur Lösung durch Red hat Enterprise empfiehlt NetApp, dieses Problem durch den Einsatz zu umgehen `fapolicyd` In den permissiven Modus. In `/etc/fapolicyd/fapolicyd.conf`, Legt den Wert von fest `permissive = 1`.

Systemprotokolle anzeigen

Sie können Keystone Collector-Systemprotokolle anzeigen, um Systeminformationen zu überprüfen und mithilfe dieser Protokolle eine Fehlerbehebung durchzuführen. Keystone Collector verwendet das Logging-System *journald* des Hosts, und die Systemprotokolle können über das Standard-Dienstprogramm *journalctl* geprüft werden. Sie können die folgenden wichtigen Dienste nutzen, um die Protokolle zu prüfen:

- ks-Kollektor
- ks-Health
- ks-autoupdate

Der Hauptdatenerfassungsdienst *ks-Collector* erzeugt Protokolle im JSON-Format mit A `run-id` Jedem geplanten Datenerfassungsauftrag zugeordnete Attribut. Nachfolgend ein Beispiel für einen erfolgreichen Auftrag zur Erfassung von Standard-Nutzungsdaten:

```
{"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"}
```


Nachfolgend ein Beispiel für einen erfolgreichen Auftrag zur optionalen Erfassung von Leistungsdaten:

```
{"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"}
```

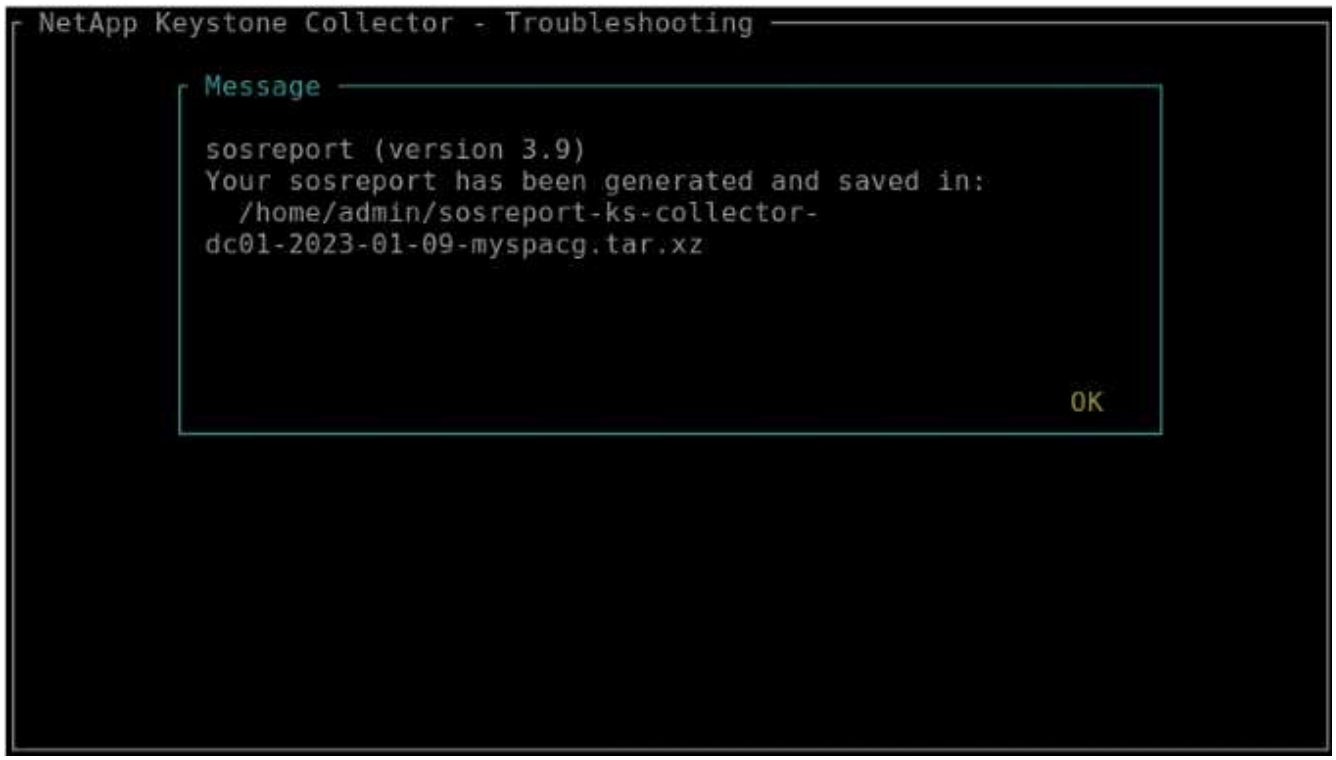
Supportpakete generieren und sammeln

Über die Keystone Collector TUI lassen sich Supportpakete generieren und Serviceanforderungen zur Behebung von Supportproblemen hinzufügen. Gehen Sie folgendermaßen vor:

Schritte

1. Starten Sie das Management-TUI-Dienstprogramm Keystone Collector:
   ```
   $ keystone-collector-tui
   ```
2. Gehen Sie zu **Fehlerbehebung > Supportpaket generieren**
   .

3. Bei der Erzeugung wird der Speicherort des Pakets angezeigt. Verwenden Sie FTP, SFTP oder SCP, um eine Verbindung zum Speicherort herzustellen und die Protokolldatei auf ein lokales System herunterzuladen.



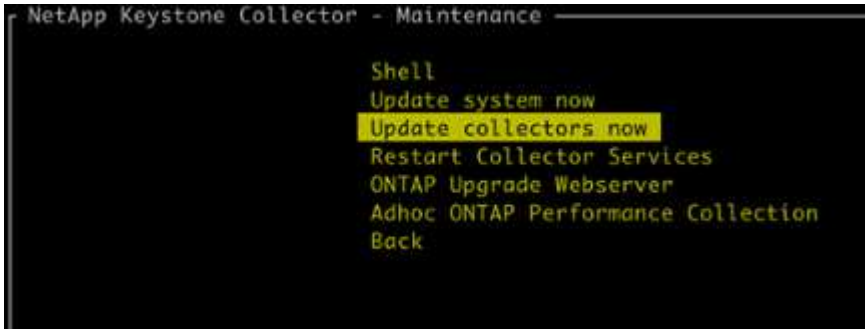
4. Wenn die Datei heruntergeladen ist, können Sie sie an das Keystone ServiceNow-Supportticket anhängen. Informationen zum Sammeln von Tickets finden Sie unter "Serviceanforderungen werden erstellt"Die

Aktualisieren Sie Keystone Collector manuell

Die automatische Aktualisierungsfunktion in Keystone Collector ist standardmäßig aktiviert, wodurch die Keystone Collector-Software bei jeder neuen Version automatisch aktualisiert wird. Sie können diese Funktion jedoch deaktivieren und die Software manuell aktualisieren.

Schritte

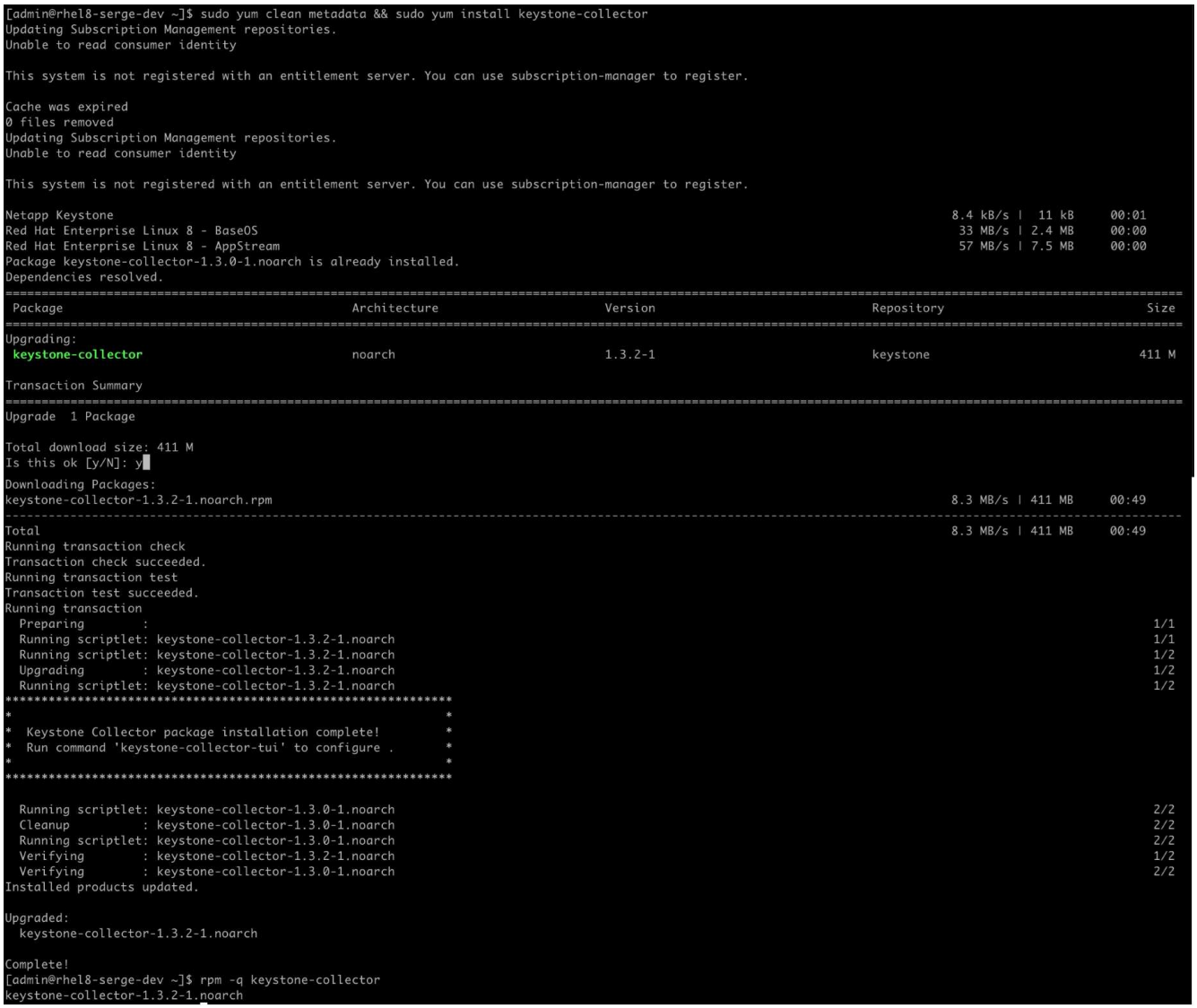
1. Starten Sie das Management-TUI-Dienstprogramm Keystone Collector:
   ```
   $ keystone-collector-tui
   ```
2. Wählen Sie auf dem Wartungsbildschirm die Option **Collectors jetzt aktualisieren** aus.



Führen Sie alternativ die folgenden Befehle aus, um die Version zu aktualisieren:

Für CentOS:

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



Für Debian:

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

3. Keystone Collector Management neu starten TUI, Sie können die neueste Version im oberen linken Bereich des Home-Bildschirms sehen.

   Führen Sie alternativ die folgenden Befehle aus, um die neueste Version anzuzeigen:

   Für CentOS:

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

   Für Debian:

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

Sicherheit mit Keystone Collector

Keystone Collector umfasst Sicherheitsfunktionen, mit denen die Performance- und Nutzungsmetriken von Keystone Systemen überwacht werden, ohne die Sicherheit von Kundendaten zu gefährden.

Die Funktionsweise von Keystone Collector basiert auf folgenden Sicherheitsprinzipien:

- **Privacy by Design**-Keystone Collector sammelt minimale Daten, um Nutzungsmessung und Leistungsüberwachung durchzuführen. Weitere Informationen finden Sie unter "Daten, die zur Abrechnung erfasst werden". Der "Private Daten Entfernen" Die Option ist standardmäßig aktiviert, wodurch vertrauliche Informationen maskiert und geschützt werden.
- **Least Privilege Access**-Keystone Collector erfordert Mindestberechtigungen zur Überwachung der Speichersysteme, wodurch Sicherheitsrisiken minimiert und unbeabsichtigte Änderungen an den Daten verhindert werden. Dieser Ansatz steht im Einklang mit dem Prinzip des geringsten Privilegs und verbessert den allgemeinen Sicherheitsstatus der überwachten Umgebungen.
- **Secure Software Development Framework**- Keystone nutzt während des gesamten Entwicklungszyklus ein sicheres Software Development Framework, das Risiken reduziert, Schwachstellen reduziert und das System vor potenziellen Bedrohungen schützt.

Verstärkte Sicherheit

Standardmäßig ist Keystone Collector für die Verwendung sicherheitsgesicherter Konfigurationen konfiguriert. Im Folgenden werden die empfohlenen Sicherheitskonfigurationen aufgeführt:

- Das Betriebssystem der virtuellen Maschine Keystone Collector:
  - Entspricht dem CIS Debian Linux 12 Benchmark Standard. Änderungen an der Betriebssystemkonfiguration außerhalb der Keystone Collector-Verwaltungssoftware können die Systemsicherheit verringern. Weitere Informationen finden Sie unter "CIS Benchmark-Handbuch".
  - Empfängt und installiert automatisch Sicherheitspatches, die von Keystone Collector über die automatische Aktualisierungsfunktion überprüft werden. Wenn Sie diese Funktion deaktivieren, kann es zu ungepatchter anfälliger Software kommen.
  - Authentifiziert die von Keystone Collector empfangenen Updates. Die Deaktivierung der APT-Repository-Verifizierung kann zur automatischen Installation nicht autorisierter Patches führen, was zu potenziellen Schwachstellen führen kann.
- Keystone Collector validiert automatisch HTTPS-Zertifikate, um die Verbindungssicherheit zu gewährleisten. Wenn Sie diese Funktion deaktivieren, kann dies zu Identitätswechsel von externen Endpunkten und zu Datenlecks bei der Nutzung führen.
- Keystone Collector unterstützt "Benutzerdefinierte vertrauenswürdige CA" Zertifizierung: Standardmäßig vertraut es Zertifikaten, die von der vom erkannten öffentlichen Stammzertifizierungsstelle signiert wurden "Mozilla CA-Zertifikatsprogramm". Durch die Aktivierung zusätzlicher vertrauenswürdiger CAS ermöglicht Keystone Collector die HTTPS-Zertifikatvalidierung für Verbindungen zu Endpunkten, die diese Zertifikate aufweisen.
- Keystone Collector aktiviert standardmäßig die Option **Private Daten entfernen**, die sensible Informationen maskiert und schützt. Weitere Informationen finden Sie unter "Begrenzung der Erhebung

privater Daten". Wenn Sie diese Option deaktivieren, werden zusätzliche Daten an das Keystone System übermittelt. Sie kann z. B. vom Benutzer eingegebene Informationen wie Volumennamen enthalten, die als vertrauliche Informationen betrachtet werden können.

Verwandte Informationen

- "Übersicht über Keystone Collector"
- "Anforderungen an die virtuelle Infrastruktur"
- "Konfigurieren Sie Keystone Collector"

Arten von Benutzerdaten, die Keystone erfasst

Keystone erfasst Konfigurations-, Status- und Nutzungsinformationen von Keystone ONTAP und Keystone StorageGRID -Abonnements sowie Telemetriedaten der virtuellen Maschine (VM), auf der Keystone Collector läuft. Leistungsdaten für ONTAP können nur erfasst werden, wenn diese Option in Keystone Collector aktiviert ist.

ONTAP Datenerfassung

-DatenausDatenausDatenerhebung für ONTAP: Lern-

Die folgende Liste enthält ein repräsentatives Beispiel für die Daten zur Kapazitätsnutzung, die für ONTAP erfasst wurden:

- Cluster
  - ClusterUUID
  - ClusterName
  - Seriennummer
  - Standort (basierend auf Werteingabe im ONTAP Cluster)
  - Kontakt
  - Version
- Knoten
  - Seriennummer
  - Node-Name
- Volumes
  - Aggregatname
  - Volume-Name
  - VolumeInstanceUUID
  - IsCloneVolume-Flagge
  - IsFlexGroupKonstituierende Flagge
  - IsSpaceEnforceLogische Flagge
  - IsSpaceReportingLogische Flagge
  - LogicalSpaceUsedByAfs
  - PercentSnapshotSpace
  - PerformanceTierInvactiveUserData
  - PerformanceTierInvactiveUserDataPercent
  - QoSAdaptivePolicyGruppenname
  - QoSPolicyGroup-Name
  - Größe
  - Verwendet
  - PhysischeVerwendet
  - SizeUsedBySnapshots
  - Typ
  - VolumeStyleErweitert
  - Name des Vserver
  - IsVsRoot-Flagge
- VServer
  - VserverName

    - VserverUUID
    - Untertyp
- Storage-Aggregate
    - Storage-Typ
    - Aggregatname
    - Aggregat-UUID
    - Physisch verwendet
    - Verfügbare Größe
    - Größe
    - Verwendete Größe
- Aggregieren von Objektspeichern
    - Objektspeichername
    - ObjectStoreUUID
    - Providertyp
    - Aggregatname
- Volumes klonen
    - FlexClone
    - Größe
    - Verwendet
    - Vserver
    - Typ
    - ParentVolume
    - ParentVserver
    - Konstituent
    - SplitSchätzung
    - Status
    - FlexCloneUsedPercent
- Storage-LUNs
    - LUN-UUID
    - Der LUN-Name
    - Größe
    - Verwendet
    - IsReservierte Flagge
    - IsAnfordertes Flag
    - LogicalUnit-Name
    - QoSPolicyUUID
    - QoSPolicyName

    - VolumeUUID
    - VolumeName
    - SVMUUID
    - SVM-Name
- Storage Volumes
    - VolumeInstanceUUID
    - VolumeName
    - SVMName
    - SVMUUID
    - QoSPolicyUUID
    - QoSPolicyName
    - KapazitätTierFußprint
    - PerformanceTierFußprint
    - Gesamtfußabdruck
    - TieringPolicy
    - IsProtected-Flag
    - IsDestination-Flag
    - Verwendet
    - PhysischeVerwendet
    - CloneParentUUID
    - LogicalSpaceUsedByAfs
- QoS-Richtliniengruppen
    - Richtliniengruppe
    - QoSPolicyUUID
    - MaxThroughput
    - MinThroughput
    - MaxThroughputIOPS
    - MaxThroughputMBps
    - MinenthrughIOPS
    - MinThroughput MBit/s
    - IsShared-Flag
- Anpassungsfähige QoS-Richtliniengruppen von ONTAP
    - QoSPolicyName
    - QoSPolicyUUID
    - PeakIOPS
    - PeakIOPSAllocation
    - AbsoluteMinIOPS

    - ExpectedIOPS
    - ExpectedIOPSAllocation
    - Blockgröße
- Fußspuren
    - Vserver
    - Datenmenge
    - Gesamtfußabdruck
    - VolumeBlocksFootprintBin0
    - VolumeBlocksFootprintBin1
- MetroCluster
    - Node
    - Aggregat
    - LIFs
    - Konfigurationsreplikation
    - Anschlüsse
    - Cluster
    - Volumes
- MetroCluster Cluster
    - ClusterUUID
    - ClusterName
    - RemoteClusterUUID
    - RemoteCluserName
    - LocalConfigurationState
    - RemoteConfigurationState
- MetroCluster -Knoten
    - DR-Spiegelungsstatus
    - Intercluster LIF
    - Knotenerreichbarkeit
    - DR-Partnerknoten
    - DR Aux Partner-Knoten
    - Symmetrische Beziehung zwischen DR, DR Aux und HA-Knoten
    - Automatische ungeplante Umschaltung
- MetroCluster -Konfigurationsreplikation
    - Remote-Heartbeat
    - Letzter gesendeter Heartbeat
    - Letzter empfangener Heartbeat
    - Vserver Stream

    - Cluster-Stream
    - Storage
    - Speichervolumen im Einsatz
- MetroCluster Mediatoren
    - Adresse des Mediators
    - Mediator-Port
    - Mediator konfiguriert
    - Mediator erreichbar
    - Modus
- Messgrößen Für Die Kollektorbeobachtbarkeit
    - Erfassungszeit
    - Active IQ Unified Manager-API-Endpunkt abgefragt
    - Reaktionszeit
    - Anzahl an Datensätzen
    - AIQUMInstance IP
    - CollectorEing.-ID

-DatenausDatenausDatenerhebung für ONTAP: Lern-

Die folgende Liste ist ein repräsentatives Beispiel für die Performance-Daten, die für ONTAP erfasst wurden:

- Cluster-Name
- Cluster-UUID
- Objekt-ID
- VolumeName
- UUID der Volume-Instanz
- Vserver
- VserverUUID
- Serieller Knoten
- ONTAPVersion
- AIQUM-Version
- Aggregat
- AggregateUUID
- Ressourcenschlüssel
- Zeitstempel
- IOPSPerTb
- Latenz
- Leselatenz
- WriteMBps
- QoSMinDurchgangLatenz
- QoSNBladeLatency
- UsedHeadRoom
- CacheMissRatio
- AndereLatenz
- QoSAggregateLatency
- IOPS
- QoSNetworkLetenz
- AvailableOps
- WriteLatency
- QoSCloudLatency
- QoSClusterLatenz für InterconnectLatenz
- SonstigesMBit/s
- QoSCopLatency
- QoSDBladeLatency
- Auslastung

- Lese-IOPS
- MB/Sek.
- OtherIOPS
- QoSPolicyGroupLatenzzeit
- ReadMBps
- QoSSyncSnapmirrorLatency
- Daten auf Systemebene
  - Schreiben/Lesen/Sonstige/Gesamt-IOPS
  - Schreiben/Lesen/Sonstiges/Gesamtdurchsatz
  - Schreiben/Lesen/Sonstiges/Gesamtlatenz
- WriteIOPS

** Ausbegehen von Objekten entfernt auf Beschränkung des privaten Datenzugangs: Lernen Sie Ausbegehen **

Wenn die Option **Private Daten entfernen** auf Keystone Collector aktiviert ist, werden die folgenden Nutzungsinformationen für ONTAP gelöscht. Diese Option ist standardmäßig aktiviert.

- Cluster-Name
- Clusterstandort
- Cluster-Kontakt
- Node-Name
- Aggregatname
- Volume-Name
- QoSAdaptivePolicyGruppenname
- QoSPolicyGroup-Name
- Name des Vserver
- Name der Storage-LUN
- Aggregatname
- LogicalUnit-Name
- SVM-Name
- AIQUMInstance IP
- FlexClone
- RemoteClusterName

StorageGRID Datenerfassung

-DatenausDatenausDatenerhebung für StorageGRID: Lern-

Die folgende Liste enthält ein repräsentatives Beispiel für die `Logical Data` Für StorageGRID gesammelt:

- StorageGRID-ID
- Konto-ID
- Kontoname
- Kontogotingbytes
- Bucket-Name
- Anzahl Bucket-Objekte
- Bucket-Daten-Bytes

Die folgende Liste enthält ein repräsentatives Beispiel für die `Physical Data` Für StorageGRID gesammelt:

- StorageGRID-ID
- Node-ID
- Standort-ID
- Standortname
- Instanz
- StorageGRID-Speicherauslastung Byte
- StorageGRID-Metadaten für Storage-Auslastung

Die folgende Liste ist eine repräsentative Auswahl der `Availability/Uptime Data` für StorageGRID gesammelt:

- SLA-Betriebszeit in Prozent

** Ausbegehen von Objekten entfernt auf Beschränkung des privaten Datenzugangs: Lernen Sie Ausbegehen **

Wenn die Option **Private Daten entfernen** auf Keystone Collector aktiviert ist, werden die folgenden Nutzungsinformationen für StorageGRID gelöscht. Diese Option ist standardmäßig aktiviert.

- Kontoname
- BucketName
- Standortname
- Instanz/Knotenname

Telemetriedatenerfassung

Von der Keystone Collector VM erfasste Telemetriedaten: Weitere Informationen

Die folgende Liste ist eine repräsentative Auswahl der für Keystone -Systeme gesammelten Telemetriedaten:

- Systeminformationen
  - Der Name des Betriebssystems
  - Betriebssystemversion
  - Betriebssystem-ID
  - Systemhostname
  - Standard-IP-Adresse des Systems
- Nutzung der Systemressourcen
  - Systemverfügbarkeit
  - Anzahl der CPU-Kerne
  - Systemlast (1 Min., 5 Min., 15 Min.)
  - Gesamtspeicher
  - Freier Speicher
  - Verfügbarer Speicher
  - Gemeinsam genutzter Speicher
  - Pufferspeicher
  - Zwischengespeicherter Speicher
  - Gesamttausch
  - Kostenloser Tausch
  - Zwischengespeicherter Swap
  - Name des Datenträgerdateisystems
  - Festplattengröße
  - Verwendete Festplatte
  - Datenträger verfügbar
  - Prozentsatz der Festplattennutzung
  - Datenträger-Einhängepunkt
- Installierte Pakete
- Collector-Konfiguration
- Dienstprotokolle
  - Serviceprotokolle von Keystone -Diensten

Keystone im privaten Modus

Weitere Informationen zu Keystone (privater Modus)

Keystone bietet einen *privaten* Implementierungsmodus, auch bekannt als *Dark Site*, um Ihre geschäftlichen und Sicherheitsanforderungen zu erfüllen. Dieser Modus ist für Unternehmen mit Konnektivitätsbeschränkungen verfügbar.

NetApp bietet eine spezielle Implementierung von Keystone STaaS an, die auf Umgebungen mit eingeschränkter oder keiner Internetverbindung (auch als Dark Sites bezeichnet) zugeschnitten ist. Hierbei handelt es sich um sichere oder isolierte Umgebungen, in denen die externe Kommunikation aufgrund von Sicherheits-, Compliance- oder betrieblichen Anforderungen eingeschränkt ist.

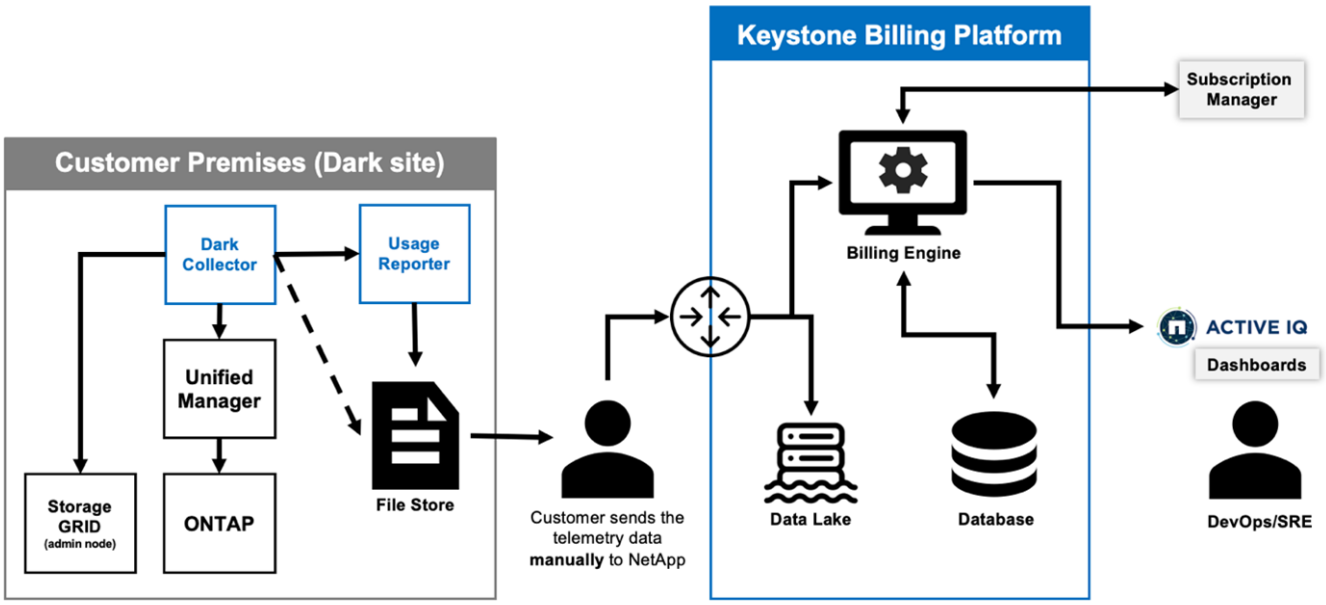
Für NetApp Keystone bedeutet das Angebot von Services für Dark Sites, den flexiblen Keystone Storage Abonnement-Service in einer Weise bereitzustellen, die die Einschränkungen dieser Umgebungen berücksichtigt. Dazu gehören:

- **Local Deployment**: Keystone kann in isolierten Umgebungen unabhängig konfiguriert werden, sodass keine Internetverbindung oder externe Mitarbeiter für den Setup-Zugang erforderlich sind.
- **Offline-Betrieb**: Alle Storage-Management-Funktionen mit Health Checks und Abrechnung sind offline für den Betrieb verfügbar.
- **Sicherheit und Compliance**: Keystone stellt sicher, dass die Bereitstellung die Sicherheits- und Compliance-Anforderungen von Dark Sites erfüllt. Dazu gehören u. a. erweiterte Verschlüsselung, sichere Zugriffskontrollen und detaillierte Auditing-Funktionen.
- **Hilfe und Support**: NetApp bietet 24/7 globalen Support mit einem speziellen Keystone Success Manager, der jedem Account für Unterstützung und Fehlerbehebung zugewiesen ist.

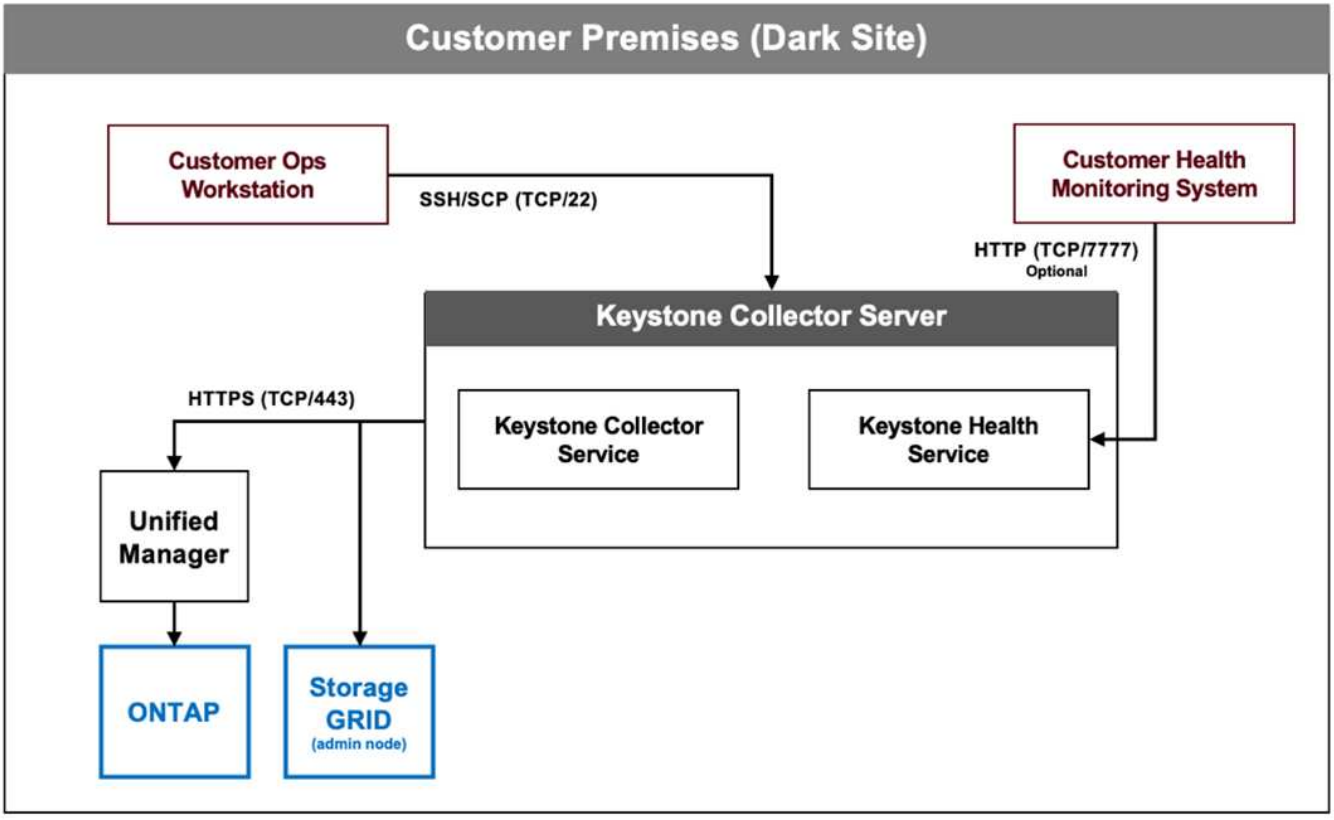
> Keystone Collector kann ohne Konnektivitätsbeschränkungen konfiguriert werden, auch als *Standard*-Modus bekannt. Weitere Informationen finden Sie unter "Weitere Informationen zu Keystone Collector".

Keystone Collector im privaten Modus

Keystone Collector ist für das regelmäßige Erfassen von Nutzungsdaten aus Storage-Systemen und den Export der Kennzahlen in einen Offline- bzw. Nutzungs-Reporter und lokalen Datenspeicher verantwortlich. Die generierten Dateien, die sowohl im verschlüsselten als auch im Klartext-Format erstellt werden, werden nach den Validierungsprüfungen vom Benutzer manuell an NetApp weitergeleitet. Nach Erhalt werden diese Dateien von der NetApp Keystone Abrechnungsplattform authentifiziert und verarbeitet und in die Abrechnungs- und Abonnement-Managementsysteme integriert, um die monatlichen Gebühren zu berechnen.



Der Keystone Collector-Dienst auf dem Server ist damit beauftragt, regelmäßig Nutzungsdaten zu sammeln, diese Informationen zu verarbeiten und lokal auf dem Server eine Nutzungsdatei zu erstellen. Der Systemzustandsservice führt Systemzustandsprüfungen durch und hat eine Schnittstelle zu den vom Kunden verwendeten Systemen zur Statusüberwachung. Diese Berichte stehen Benutzern für den Offline-Zugriff zur Verfügung, sodass sie validiert und bei der Fehlerbehebung unterstützt werden können.



Bereiten Sie die Installation des Keystone Collectors im privaten Modus vor.

Bevor Sie Keystone Collector in einer Umgebung ohne Internetzugang installieren, die

auch als *dark site* oder *private Mode* bezeichnet wird, stellen Sie sicher, dass Ihre Systeme mit der erforderlichen Software vorbereitet sind und alle erforderlichen Voraussetzungen erfüllen.

Anforderungen für VMware vSphere

- Betriebssystem: VMware vCenter Server und ESXi 8.0 oder höher
- Kern: 1 CPU
- RAM: 2 GB
- Festplattenspeicher: 20 GB vDisk

Anforderungen für Linux

- Betriebssystem (bitte eines auswählen):
  - Red Hat Enterprise Linux (RHEL) 8.6 oder eine spätere Version der 8.x-Serie
  - Red Hat Enterprise Linux 9.0 oder spätere Versionen
  - Debian 12
- Kern: 2 CPU
- RAM: 4 GB
- Festplattenspeicher: 50 GB vDisk
  - Mindestens 2 GB frei in `/var/lib/`
  - Mindestens 48 GB frei in `/opt/netapp`

Auf demselben Server sollten auch die folgenden Drittanbieterpakete installiert sein. Wenn diese Pakete über das Repository verfügbar sind, werden sie automatisch als Voraussetzungen installiert:

- RHEL 8.6+ (8.x)
  - python3 >=v3.6.8, python3 <=v3.9.13
  - Podman
  - sos
  - Toll-utils
  - python3-dnf-Plugin-Versionlock
- RHEL 9,0+
  - python3 >= v3.9.0, python3 <= v3.9.13
  - Podman
  - sos
  - Toll-utils
  - python3-dnf-Plugin-Versionlock
- Debian v12
  - python3 >= v3.9.0, python3 <= v3.12.0
  - Podman

- Sosreport

Netzwerkanforderungen

Die Netzwerkanforderungen für Keystone Collector umfassen:

- Active IQ Unified Manager (Unified Manager) 9.10 oder höher, konfiguriert auf einem Server mit aktivierter API-Gateway-Funktion.
- Auf den Unified Manager-Server sollte der Keystone Collector-Server auf Port 443 (HTTPS) zugreifen können.
- Für Keystone Collector auf dem Unified Manager-Server sollte ein Servicekonto mit Anwendungsbenutzerberechtigungen eingerichtet werden.
- Eine externe Internetverbindung ist nicht erforderlich.
- Exportieren Sie jeden Monat eine Datei aus Keystone Collector und senden Sie sie per E-Mail an das NetApp Supportteam. Weitere Informationen zur Kontaktaufnahme mit dem Support-Team finden Sie unter "Keystone hilft Ihnen dabei"Die

Installieren Sie Keystone Collector im privaten Modus

Führen Sie einige Schritte durch, um Keystone Collector in einer Umgebung zu installieren, die keinen Internetzugang hat, auch als *dark site* oder *private Mode* bekannt. Diese Art der Installation ist perfekt für Ihre sicheren Standorte.

Sie können Keystone Collector je nach Ihren Anforderungen entweder auf VMware vSphere-Systemen bereitstellen oder auf Linux-Systemen installieren. Befolgen Sie die Installationsschritte, die Ihrer ausgewählten Option entsprechen.

Implementieren auf VMware vSphere

Führen Sie hierzu folgende Schritte aus:

1. Laden Sie die OVA-Vorlagendatei von herunter "NetApp Keystone-Webportal".
2. Schritte zum Bereitstellen von Keystone Collector mit OVA-Datei finden Sie im Abschnitt "Bereitstellen der OVA-Vorlage".

Installation unter Linux

Die Keystone Collector-Software wird auf dem Linux-Server mit den bereitgestellten .deb- oder .rpm-Dateien auf Basis der Linux-Distribution installiert.

Führen Sie die folgenden Schritte aus, um die Software auf Ihrem Linux-Server zu installieren:

1. Laden Sie die Installationsdatei für den Keystone Collector herunter oder übertragen Sie sie auf den Linux-Server:

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

2. Öffnen Sie ein Terminal auf dem Server, und führen Sie die folgenden Befehle aus, um die Installation zu starten.

   - **Debian-Paket verwenden**

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

- **Mit RPM-Datei**

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

Oder

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

3. Geben Sie ein `y`, wenn Sie zur Installation des Pakets aufgefordert werden.

Konfigurieren Sie Keystone Collector im privaten Modus

Führen Sie einige Konfigurationsaufgaben aus, um Keystone Collector zu aktivieren, um Nutzungsdaten in einer Umgebung zu erfassen, die keinen Internetzugang hat, auch als *dark site* oder *private Mode* bezeichnet. Dies ist eine einmalige Aktivität zur Aktivierung und Zuordnung der erforderlichen Komponenten zu Ihrer Storage-Umgebung. Nach der Konfiguration überwacht Keystone Collector alle von Active IQ Unified Manager gemanagten ONTAP-Cluster.

Keystone Collector stellt Ihnen das Dienstprogramm „Keystone Collector Management Terminal User Interface (TUI)“ zur Verfügung, mit dem Sie Konfigurations- und Überwachungsaktivitäten durchführen können. Sie können verschiedene Tastaturbedienungen wie die Eingabetaste und die Pfeiltasten verwenden, um die Optionen auszuwählen und durch diese TUI zu navigieren.

Schritte

1. Starten Sie das Management-TUI-Dienstprogramm Keystone Collector:

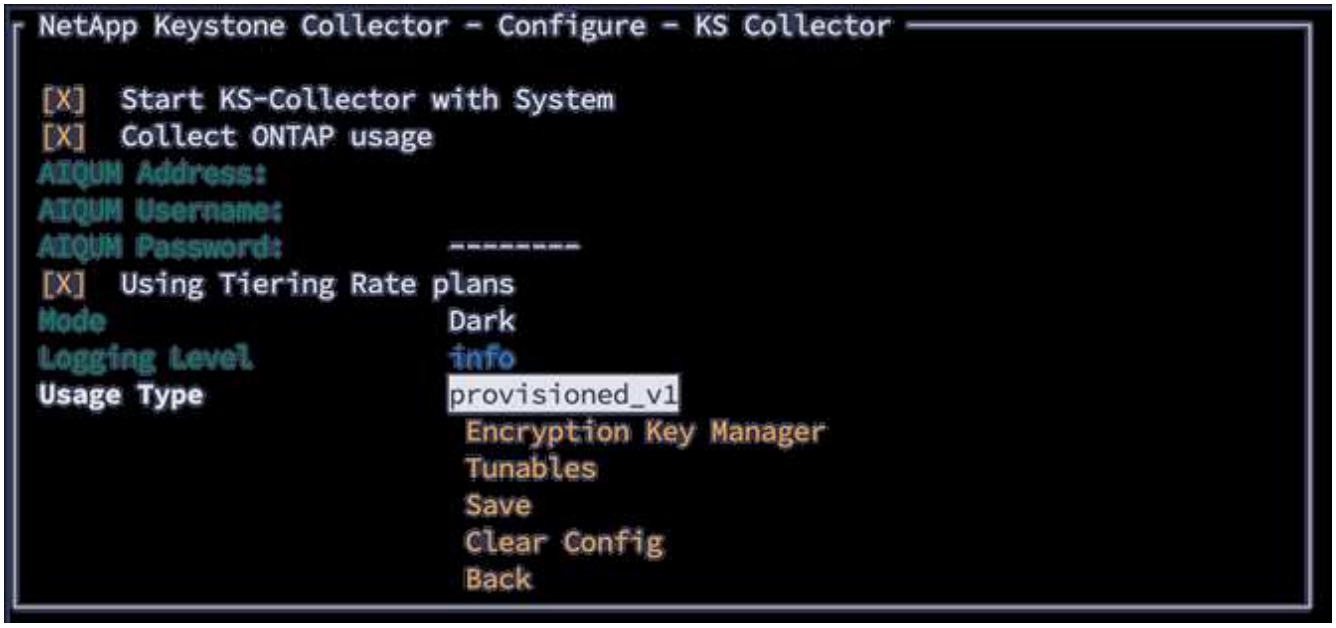
```
keystone-collector-tui
```

2. Gehen Sie zu **Konfigurieren > Erweitert**.
3. Schalten Sie die Option **Darksite-Modus** ein.

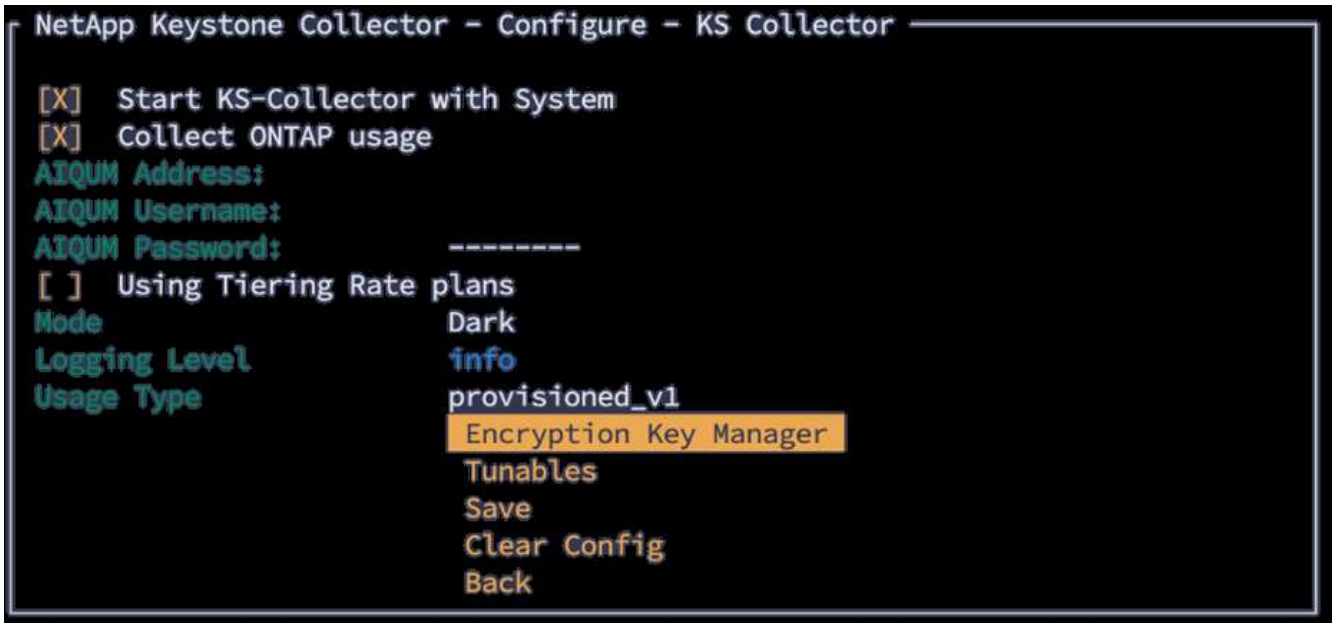
4. Wählen Sie **Speichern**.

5. Gehen Sie zu **Configure > KS-Collector**, um Keystone Collector zu konfigurieren.
6. Schalten Sie das Feld **KS Collector mit System** starten ein.
7. Schalten Sie das Feld **Collect ONTAP Usage** ein. Fügen Sie die Details zum Active IQ Unified Manager-Server (Unified Manager) und zum Benutzerkonto hinzu.
8. **Optional**: Aktivieren Sie das Feld **mit Tiering Rate Plans**, wenn Daten-Tiering für das Abonnement erforderlich ist.
9. Aktualisieren Sie je nach erworbenem Abonnementtyp den **Nutzungstyp**.

> Bestätigen Sie vor der Konfiguration den mit dem Abonnement verbundenen Nutzungstyp von NetApp.

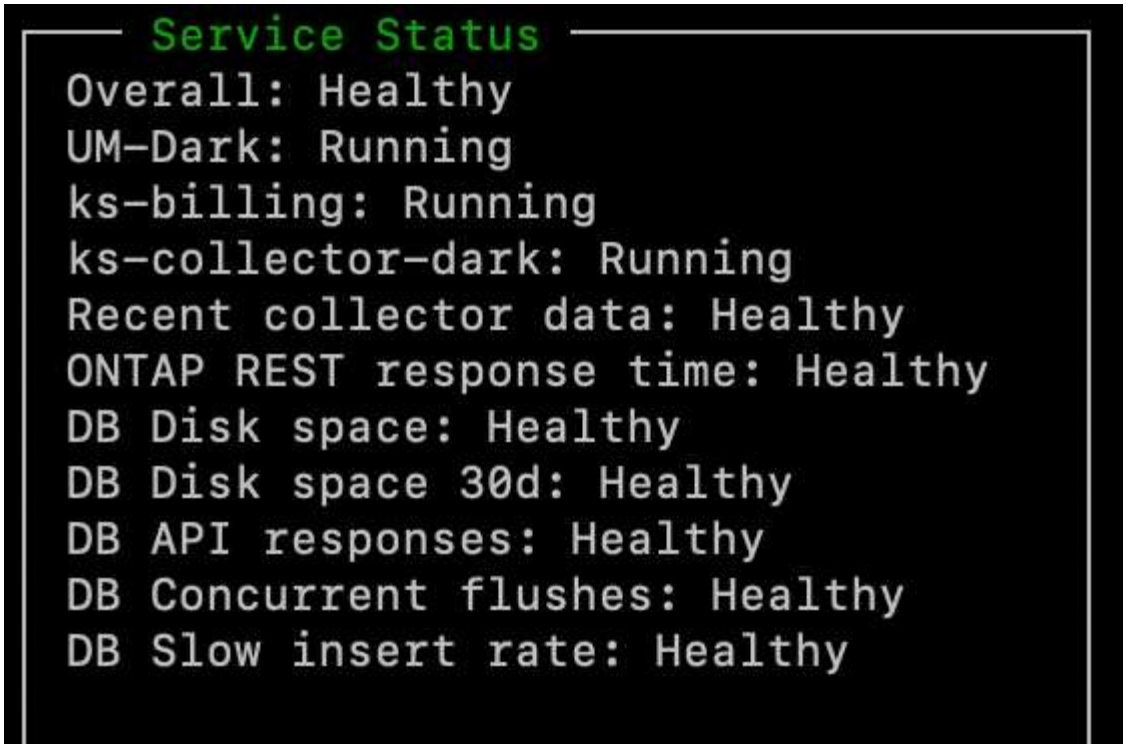


10. Wählen Sie **Speichern**.
11. Gehen Sie zu **Configure > KS-Collector**, um das Keystone Collector-Tastenfeld zu generieren.
12. Gehen Sie zu **Encryption Key Manager** und drücken Sie die Eingabetaste.



13. Wählen Sie **Collector-Tastenfeld generieren**, und drücken Sie die Eingabetaste.

14. Stellen Sie sicher, dass sich der Keystone Collector in einem gesunden Zustand befindet, indem Sie zum Hauptbildschirm der TUI zurückkehren und die Informationen **Service Status** überprüfen. Das System sollte zeigen, dass sich die Dienste im Status **Overall: Healthy** befinden. Warten Sie bis zu 10 Minuten. Wenn der Gesamtstatus nach diesem Zeitraum weiterhin fehlerhaft ist, lesen Sie die vorherigen Konfigurationsschritte durch, und wenden Sie sich an das NetApp Support-Team.



15. Beenden Sie die Management-TUI von Keystone Collector, indem Sie auf dem Startbildschirm die Option **Exit to Shell** auswählen.
16. Generierten öffentlichen Schlüssel abrufen:

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

17. Senden Sie eine E-Mail mit dieser Datei an ng-keystone-secure-site-upload@netapp.com für sichere Nicht-USPS-Sites oder an ng-keystone-secure-site-usps-upload@netapp.com für sichere USPS-Sites.

Nutzungsbericht exportieren

Sie sollten die monatliche Nutzungsübersicht am Ende jedes Monats an NetApp senden. Sie können diesen Bericht manuell erstellen.

Führen Sie die folgenden Schritte aus, um den Nutzungsbericht zu erstellen:

1. Gehen Sie auf dem Keystone Collector TUI-Startbildschirm zu **Nutzung exportieren**.
2. Sammeln Sie die Dateien und senden Sie sie für sichere Nicht-USPS-Sites an ng-keystone-secure-site-upload@netapp.com oder für sichere USPS-Sites an ng-keystone-secure-site-usps-upload@netapp.com.

   Keystone Collector erzeugt sowohl eine klare als auch eine verschlüsselte Datei, die manuell an NetApp gesendet werden sollte. Der Clear File Report enthält die folgenden Details, die vom Kunden validiert werden können.

```
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-----
```

Upgrade ONTAP

Keystone Collector unterstützt ONTAP Upgrades über TUI.

Führen Sie zum Upgrade von ONTAP die folgenden Schritte aus:

1. Gehen Sie zu **Wartung > ONTAP-Upgrade-Webserver**.
2. Kopieren Sie die ONTAP-Upgrade-Image-Datei nach **/opt/NetApp/ONTAP-Upgrade/**, und wählen Sie dann **Webserver starten** aus, um den Webserver zu starten.

3. Rufen Sie `http://<collector-ip>:8000` einen Webbrowser auf, um Unterstützung bei der Aktualisierung zu erhalten.

Starten Sie Keystone Collector Neu

Sie können den Keystone Collector-Dienst über die TUI neu starten. Gehen Sie in der TUI zu **Wartung > Collector neu starten** Dienste. Dadurch werden alle Collector-Dienste neu gestartet, und ihr Status kann über den TUI-Startbildschirm überwacht werden.

Überwachen Sie den Zustand von Keystone Collector im privaten Modus

Sie können den Systemzustand von Keystone Collector mit einem beliebigen Überwachungssystem überwachen, das HTTP-Anfragen unterstützt.

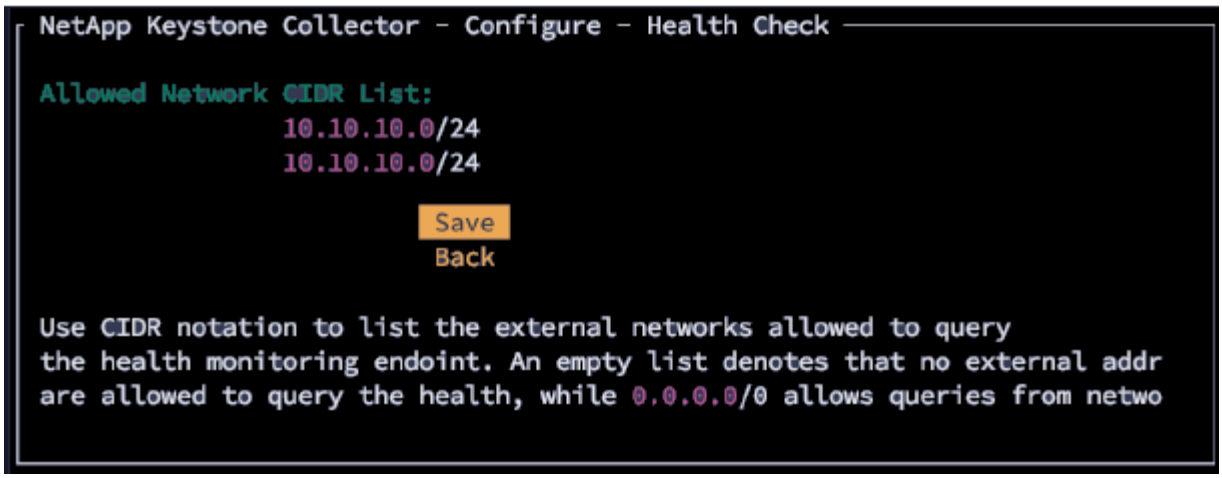
Standardmäßig akzeptieren die Keystone Systemzustandsservices keine Verbindungen von anderen IP-Adressen als localhost. Der Keystone Zustandsendpunkt ist `/uber/health`, Und es wartet auf alle Schnittstellen des Keystone Collector Servers am Port `7777`. Bei der Abfrage wird ein HTTP-Anforderungsstatuscode mit einer JSON-Ausgabe vom Endpunkt als Antwort zurückgegeben, der den Status des Keystone Collector-Systems beschreibt.
Der JSON-Körper bietet einen allgemeinen Integritätsstatus für das `is_healthy` Attribut, das ein boolescher Wert ist; und eine detaillierte Liste der Status pro Komponente für das `component_details` Attribut.
Hier ein Beispiel:

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

Diese Statuscodes werden zurückgegeben:

- **200**: Zeigt an, dass alle überwachten Komponenten gesund sind
- **503**: Zeigt an, dass eine oder mehrere Komponenten ungesund sind
- **403**: Zeigt an, dass der HTTP-Client, der den Integritätsstatus abfragt, nicht auf der *allow*-Liste steht, was eine Liste der zugelassenen Netzwerk-CIDRs ist. Für diesen Status werden keine Systemzustandsinformationen zurückgegeben.

  Die Liste *allow* verwendet die Netzwerk-CIDR-Methode, um zu steuern, welche Netzwerkgeräte das Keystone-Integritätssystem abfragen dürfen. Wenn Sie den Fehler 403 erhalten, fügen Sie Ihr Überwachungssystem der Liste *allow* von **Keystone Collector Management TUI > Configure > Health Monitoring** hinzu.

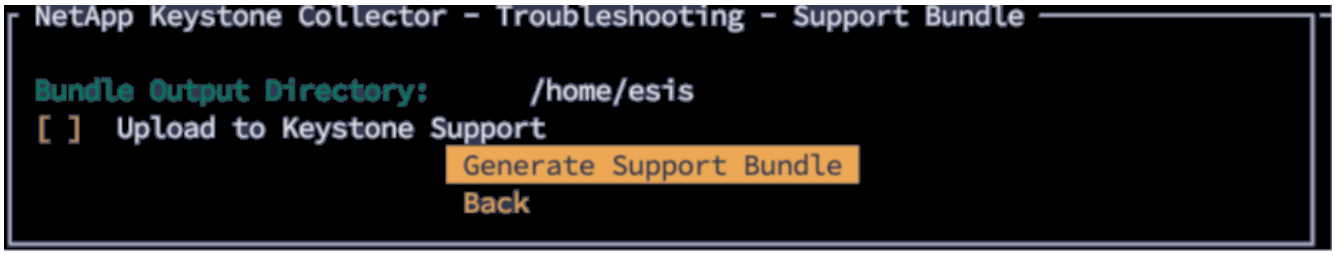


Supportpakete generieren und sammeln

Um Probleme mit dem Keystone Collector zu beheben, können Sie mit dem NetApp-Support zusammenarbeiten, der möglicherweise nach einer *.tar*-Datei fragt. Sie können diese Datei über das Management-TUI-Dienstprogramm Keystone Collector generieren.

Führen Sie die folgenden Schritte aus, um eine *.tar*-Datei zu generieren:

1. Gehen Sie zu **Fehlerbehebung > Supportpaket generieren**.
2. Wählen Sie den Speicherort für das Paket aus, und klicken Sie dann auf **Supportpaket generieren**.



   Durch diesen Prozess wird ein `tar` Paket an dem genannten Speicherort erstellt, das zur Fehlerbehebung mit NetApp geteilt werden kann.

3. Wenn die Datei heruntergeladen ist, können Sie sie an das Keystone ServiceNow-Supportticket anhängen. Informationen zum Sammeln von Tickets finden Sie unter "Serviceanforderungen werden erstellt"Die