Keystone im privaten Modus

Keystone

NetApp
September 12, 2024

Inhalt

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.

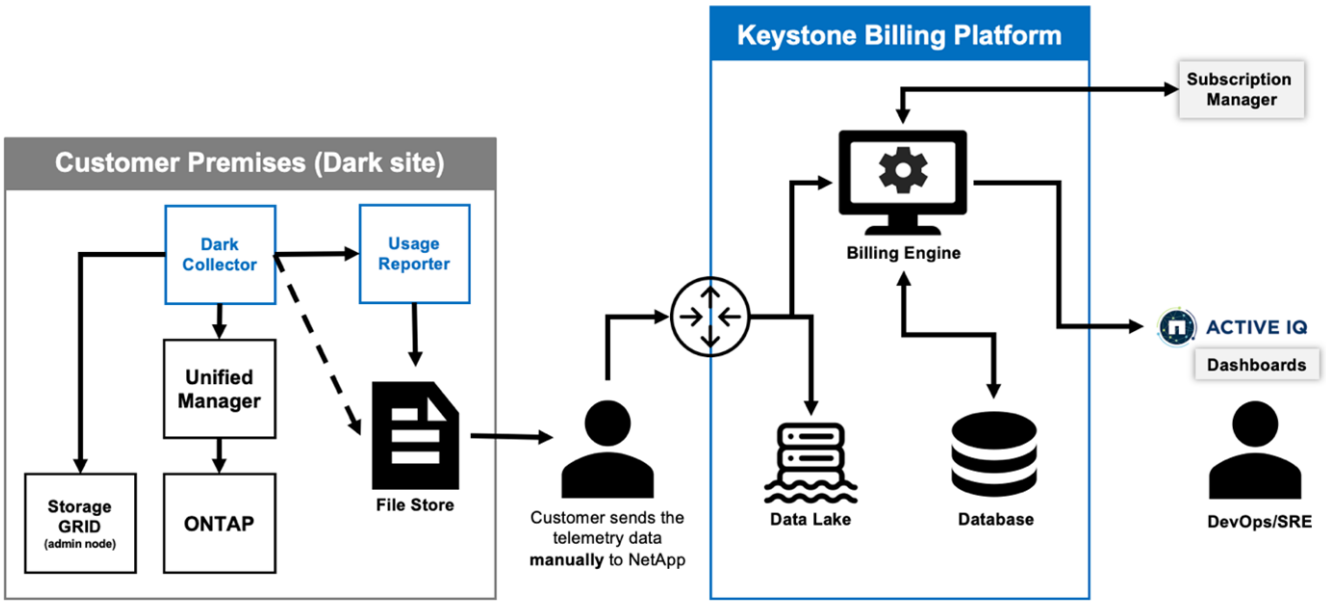
Für NetApp Keystone bedeutet das Angebot von Services für Dark Sites, den flexiblen Keystone Storage Abonnement-Service in einer Weise bereitzustellen, die die Einschränkungen dieser Umgebungen berücksichtigt. Dazu gehören:

- **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.

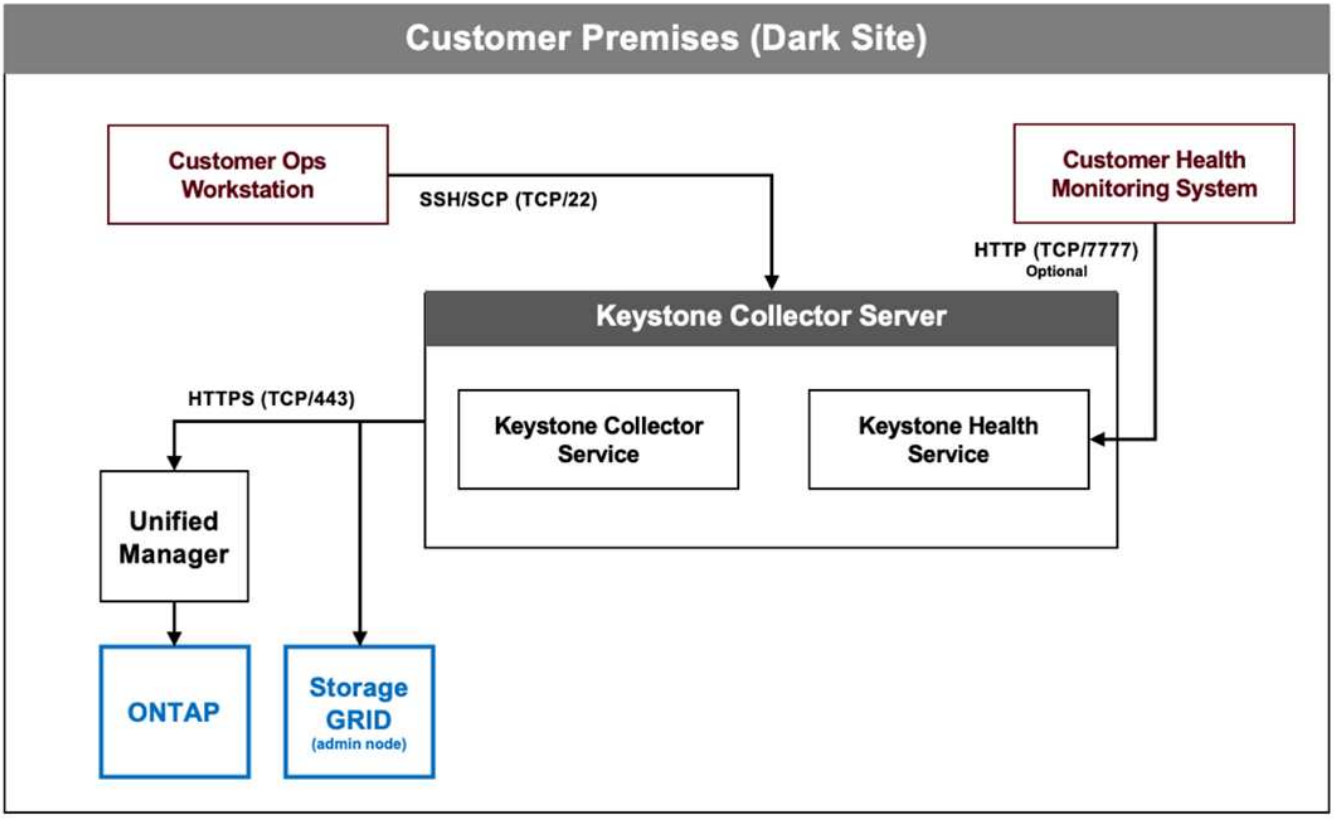
> Keystone Collector kann ohne Konnektivitätsbeschränkungen konfiguriert werden, auch als *Standard*-Modus bekannt. Weitere Informationen finden Sie unter "Weitere Informationen zu Keystone Collector".

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.



Vorbereiten der Installation im privaten Modus

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 6.7 oder höher
- Kern: 1 CPU
- RAM: 2 GB
- Festplattenspeicher: 20 GB vDisk

Anforderungen für Linux

- Betriebssystem: Debian v12 oder Red hat Enterprise Linux 8.6 oder höher
- 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:

- RHEL8
  - python3 >=v3.6.8, 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 Support-Team von NetApp. Weitere Informationen dazu, wie Sie das Support-Team kontaktieren können, finden Sie unter "Keystone hilft Ihnen dabei".

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:

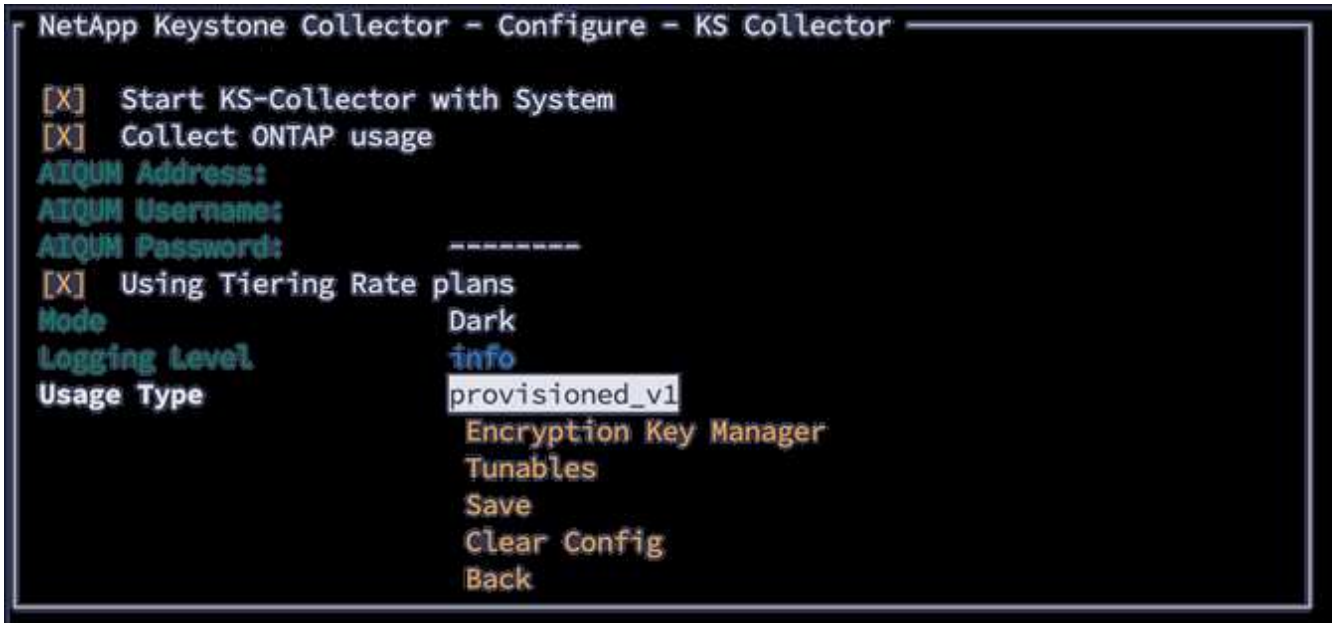
   ```
   keystone-collector-tui
   ```

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

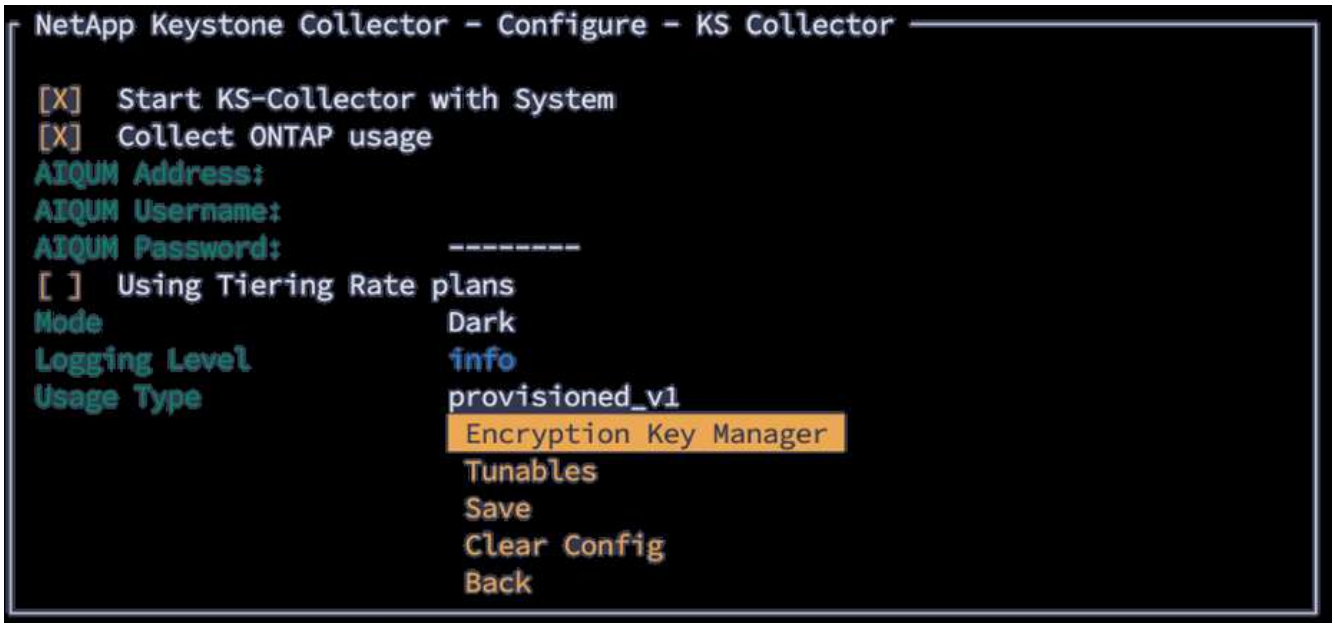
4. Wählen Sie **Speichern**.
5. Gehen Sie zu **Configure > KS-Collector**, um Keystone Collector zu konfigurieren.
6. Schalten Sie das Feld **KS Collector mit System** starten ein.
7. Schalten Sie das Feld **Collect ONTAP Usage** ein. Fügen Sie die Details zum Active IQ Unified Manager-Server (Unified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

Aktualisieren Sie je nach erworbenem Abonnementtyp den **Nutzungstyp**.

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

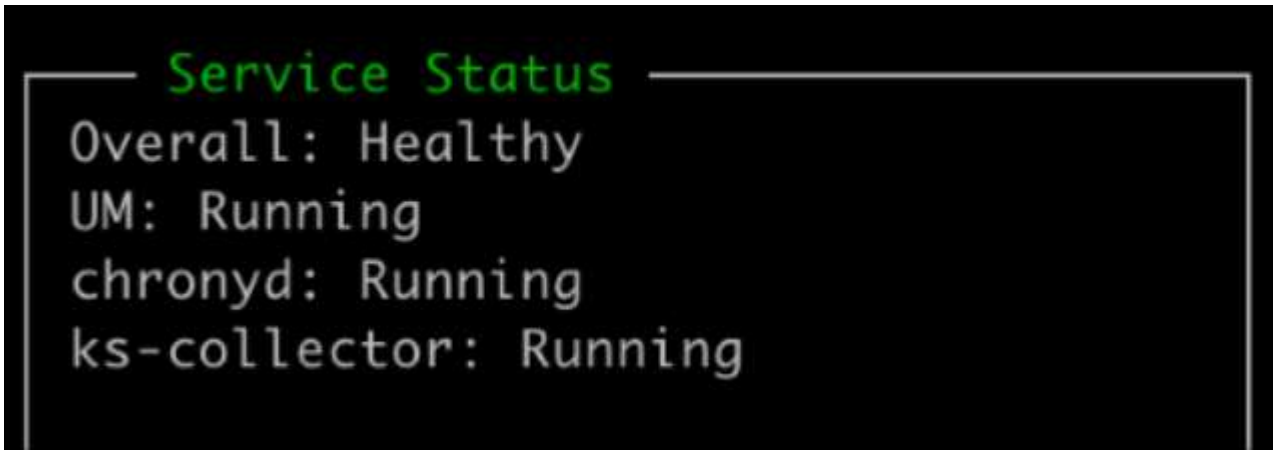


9. Wählen Sie **Speichern**.
10. Gehen Sie zu **Configure > KS-Collector**, um das Keystone Collector-Tastenfeld zu generieren.
11. Gehen Sie zu **Encryption Key Manager** und drücken Sie die Eingabetaste.



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

13. 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.



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

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

16. Senden Sie eine E-Mail mit dieser Datei an keystone.services@NetApp.com.

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 an keystone.services@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.

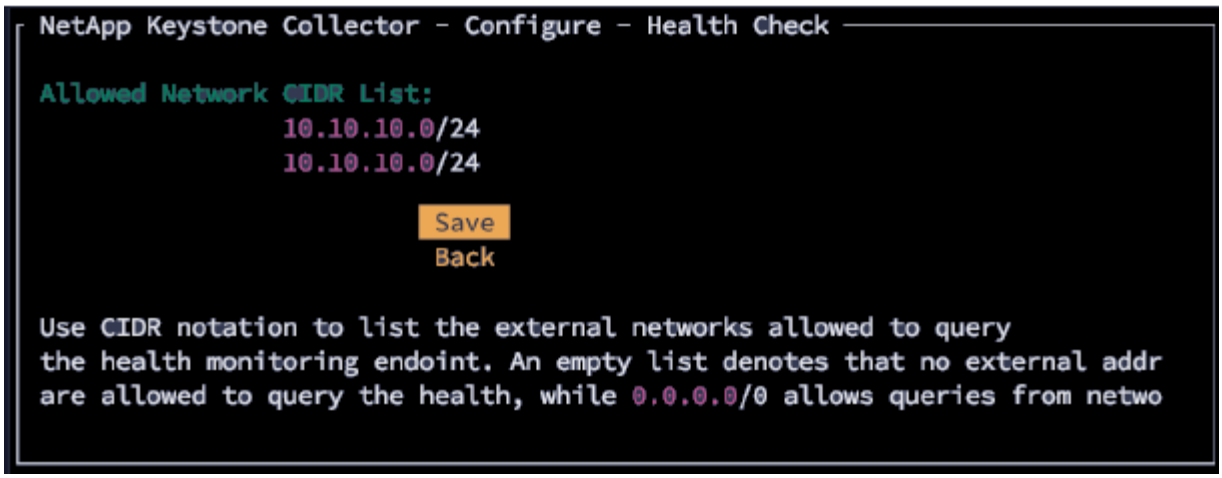
Standardmäßig akzeptieren die Keystone Systemzustandsservices keine Verbindungen von anderen IP-Adressen als localhost. Der Keystone Zustandsendpunkt ist `/uber/health`, Und es wartet auf alle Schnittstellen des Keystone Collector Servers am Port `7777`. Bei der Abfrage wird ein HTTP-Anforderungsstatuscode 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.

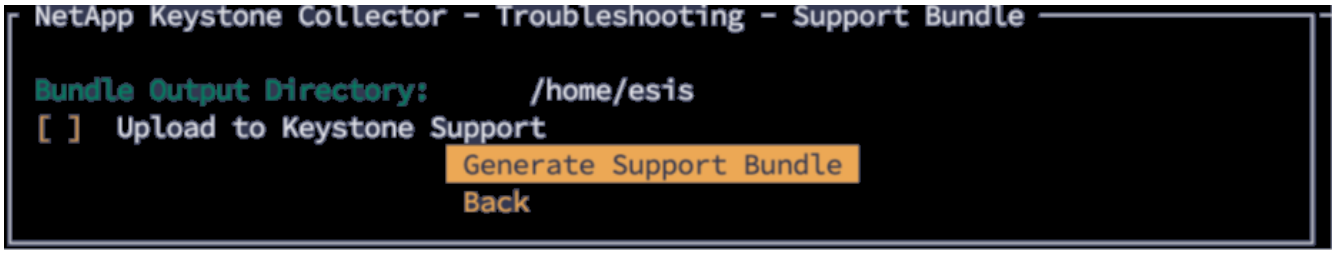


Supportpakete generieren und sammeln

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 wird, können Sie sie an das Keystone ServiceNow Support Ticket anhängen. Weitere Informationen zum Anheben von Tickets finden Sie unter "Serviceanforderungen werden erstellt".