



Keystoneのセットアップと構成

Keystone

NetApp
January 15, 2026

目次

Keystoneのセットアップと構成	1
要件	1
Keystone Collector の仮想インフラストラクチャ要件	1
Keystone Collector の Linux 要件	3
Keystone向けONTAPおよびStorageGRIDの要件	5
Keystone Collectorをインストールする	8
VMware vSphere システムにKeystone Collector を導入する	8
LinuxシステムにKeystone Collectorをインストールする	10
Keystoneソフトウェアの自動検証	12
Keystone Collector を構成する	12
Keystone Collector で HTTP プロキシを構成する	14
個人データの収集を制限する	15
カスタムルートCAを信頼する	16
パフォーマンスサービスレベルの作成	17
ITOMコレクターをインストールする	21
Keystone ITOM Collector のインストール要件	22
LinuxシステムにKeystone ITOM Collectorをインストールする	23
Windows システムにKeystone ITOM Collector をインストールする	24
KeystoneのAutoSupportを構成する	25
監視とアップグレード	26
Keystone Collector の健全性を監視する	26
Keystone Collectorを手動でアップグレードする	31
Keystone Collectorのセキュリティ	33
セキュリティ強化	33
Keystoneが収集するユーザーデータの種類	34
ONTAPデータ収集	34
StorageGRIDデータ収集	42
テレメトリデータ収集	42
プライベートモードのKeystone	44
Keystoneについて学ぶ（プライベートモード）	44
プライベートモードでのKeystone Collectorのインストールの準備	46
Keystone Collectorをプライベートモードでインストールする	47
Keystone Collectorをプライベートモードで設定する	48
プライベートモードでKeystone Collectorの健全性を監視する	52

Keystoneのセットアップと構成

要件

Keystone Collector の仮想インフラストラクチャ要件

Keystone Collector をインストールする前に、VMware vSphere システムがいくつかの要件を満たしている必要があります。

Keystone Collector サーバー VM の前提条件:

- オペレーティング システム: VMware vCenter Server および ESXi 8.0 以降
- コア: 1 CPU
- RAM: 2 GB RAM
- ディスク容量: 20 GB vDisk

その他の要件

次の一般的な要件が満たされていることを確認してください。

ネットワーク要件

Keystone Collector のネットワーク要件を次の表に示します。



Keystone Collector にはインターネット接続が必要です。デフォルト ゲートウェイ (NAT 経由) または HTTP プロキシ経由で直接ルーティングすることにより、インターネット接続を提供できます。ここでは両方のバリエーションについて説明します。

ソース	デスティネーション	サービス	プロトコルとポート	カテゴリ	目的
Keystone Collector (Keystone ONTAP用)	Active IQ Unified Manager(統合マネージャー)	HTTPS	TCP 443	必須 (Keystone ONTAPを使用している場合)	ONTAP のKeystone Collector 使用状況メトリクス収集
Keystone Collector (Keystone StorageGRID用)	StorageGRID管理ノード	HTTPS	TCP 443	必須 (Keystone StorageGRIDを使用している場合)	StorageGRID のKeystone Collector 使用状況メトリクス収集

Keystoneコレクター（ジェネリック）	インターネット（後述の URL 要件に従う）	HTTPS	TCP 443	必須（インターネット接続）	Keystone Collector ソフトウェア、OS アップデート、メトリックのアップロード
Keystoneコレクター（ジェネリック）	顧客のHTTPプロキシ	HTTP プロキシ	顧客プロキシポート	必須（インターネット接続）	Keystone Collector ソフトウェア、OS アップデート、メトリックのアップロード
Keystoneコレクター（ジェネリック）	顧客DNSサーバー	DNS	TCP/UDP 53	必須	DNS解決
Keystoneコレクター（ジェネリック）	顧客のNTPサーバー	NTP	UDP 123	必須	時間同期
Keystone Collector (Keystone ONTAP用)	Unified Manager	MYSQL	TCP 3306	オプション機能	Keystone Collector のパフォーマンス メトリック収集
Keystoneコレクター（ジェネリック）	顧客監視システム	HTTPS	TCP 7777	オプション機能	Keystone Collector の健全性レポート
顧客の運用ワークステーション	Keystoneコレクター	SSH	TCP 22	管理	Keystone Collector管理へのアクセス
NetApp ONTAP クラスタおよびノード管理アドレス	Keystoneコレクター	HTTP_8000、ピング	TCP 8000、ICMPエコー要求/応答	オプション機能	ONTAPファームウェアアップデート用のWebサーバー



MySQL のデフォルト ポート 3306 は、Unified Manager の新規インストール時に localhost のみに制限されるため、Keystone Collector のパフォーマンス メトリックの収集ができなくなります。詳細については、以下を参照してください。"[ONTAPの要件](#)"。

URLアクセス

Keystone Collector は次のインターネット ホストにアクセスする必要があります。

アドレス	理由
https://keystone.netapp.com	Keystone Collector ソフトウェアの更新と使用状況レポート
https://support.netapp.com	請求情報とAutoSupport配信についてはNetApp HQにお問い合わせください

Keystone Collector の Linux 要件

必要なソフトウェアを使用して Linux システムを準備すると、Keystone Collector による正確なインストールとデータ収集が保証されます。

Linux およびKeystone Collector サーバー VM にこれらの構成があることを確認します。

Linux サーバー:

- オペレーティング システム: 次のいずれか:
 - Debian 12
 - Red Hat Enterprise Linux 8.6 以降の 8.x バージョン
 - Red Hat Enterprise Linux 9.0 以降のバージョン
 - CentOS 7 (既存環境のみ)
- Chronydの時刻同期
- 標準の Linux ソフトウェア リポジトリへのアクセス

同じサーバーには、次のサードパーティ パッケージもインストールされている必要があります。

- podman (POD マネージャー)
- ソス
- クロニー
- Python 3 (3.9.14 から 3.11.8)

Keystone Collector サーバー VM:

- コア: 2 CPU
- RAM: 4GB RAM
- ディスク容量: 50 GB vDisk

その他の要件

次の一般的な要件が満たされていることを確認してください。

ネットワーク要件

Keystone Collector のネットワーク要件を次の表に示します。



Keystone Collector にはインターネット接続が必要です。デフォルト ゲートウェイ (NAT 経由) または HTTP プロキシ経由で直接ルーティングすることにより、インターネット接続を提供できます。ここでは両方のバリエーションについて説明します。

ソース	デスティネーション	サービス	プロトコルとポート	カテゴリ	目的
Keystone Collector (Keystone ONTAP用)	Active IQ Unified Manager(統合マネージャー)	HTTPS	TCP 443	必須 (Keystone ONTAPを使用している場合)	ONTAP のKeystone Collector 使用状況メトリクス収集
Keystone Collector (Keystone StorageGRID用)	StorageGRID管理ノード	HTTPS	TCP 443	必須 (Keystone StorageGRIDを使用している場合)	StorageGRID のKeystone Collector 使用状況メトリクス収集
Keystoneコレクター (ジェネリック)	インターネット (後述の URL 要件に従う)	HTTPS	TCP 443	必須 (インターネット接続)	Keystone Collector ソフトウェア、OS アップデート、メトリックのアップロード
Keystoneコレクター (ジェネリック)	顧客のHTTPプロキシ	HTTP プロキシ	顧客プロキシポート	必須 (インターネット接続)	Keystone Collector ソフトウェア、OS アップデート、メトリックのアップロード
Keystoneコレクター (ジェネリック)	顧客DNSサーバー	DNS	TCP/UDP 53	必須	DNS解決
Keystoneコレクター (ジェネリック)	顧客のNTPサーバー	NTP	UDP 123	必須	時間同期
Keystone Collector (Keystone ONTAP用)	Unified Manager	MYSQL	TCP 3306	オプション機能	Keystone Collector のパフォーマンス メトリック収集
Keystoneコレクター (ジェネリック)	顧客監視システム	HTTPS	TCP 7777	オプション機能	Keystone Collector の健全性レポート

顧客の運用ワークステーション	Keystoneコレクター	SSH	TCP 22	管理	Keystone Collector管理へのアクセス
NetApp ONTAP クラスタおよびノード管理アドレス	Keystoneコレクター	HTTP_8000、ピング	TCP 8000、ICMPエコー要求/応答	オプション機能	ONTAPファームウェアアップデート用のWebサーバー



MySQL のデフォルト ポート 3306 は、Unified Manager の新規インストール時に localhost のみに制限されるため、Keystone Collector のパフォーマンス メトリックの収集ができなくなります。詳細については、以下を参照してください。"[ONTAPの要件](#)"。

URLアクセス

Keystone Collector は次のインターネット ホストにアクセスする必要があります。

アドレス	理由
https://keystone.netapp.com	Keystone Collector ソフトウェアの更新と使用状況レポート
https://support.netapp.com	請求情報とAutoSupport配信についてはNetApp HQにお問い合わせください

Keystone向けONTAPおよびStorageGRIDの要件

Keystoneを使い始める前に、ONTAPクラスタとStorageGRIDシステムがいくつかの要件を満たしていることを確認する必要があります。

ONTAP

ソフトウェアバージョン

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

開始する前に

ONTAPを通じてのみ使用状況データを収集する場合は、次の要件を満たしてください。

1. ONTAP 9.8 以降が設定されていることを確認します。新しいクラスターの構成については、次のリンクを参照してください。
 - ["System Managerを使用した新しいクラスタでのONTAPの設定"](#)
 - ["CLIを使用したクラスタのセットアップ"](#)
2. 特定のロールを持つONTAPログイン アカウントを作成します。詳細については、["ONTAPログインアカウントの作成について学ぶ"](#)。
 - **ウェブUI**
 - i. デフォルトの認証情報を使用してONTAP System Manager にログインします。詳細については、["System Managerを使用したクラスタ管理"](#)。
 - ii. 「読み取り専用」ロールと「http」アプリケーション タイプを持つONTAPユーザーを作成し、「クラスタ」>「設定」>「セキュリティ」>「ユーザー」に移動してパスワード認証を有効にします。
 - **CLI**
 - i. デフォルトの認証情報を使用してONTAP CLI にログインします。詳細については、["CLI によるクラスタ管理"](#)。
 - ii. 「読み取り専用」ロールと「http」アプリケーション タイプを持つONTAPユーザーを作成し、パスワード認証を有効にします。認証の詳細については、以下を参照してください。["ONTAPアカウントのパスワードアクセスを有効にする"](#)。

Active IQ Unified Managerを通じて使用状況データを収集する場合は、次の要件を満たしてください。

1. Unified Manager 9.10 以降が設定されていることを確認します。Unified Manager のインストールについては、次のリンクを参照してください。
 - ["VMware vSphere システムへの Unified Manager のインストール"](#)
 - ["LinuxシステムへのUnified Managerのインストール"](#)
2. ONTAPクラスタが Unified Manager に追加されていることを確認します。クラスターの追加については、以下を参照してください。["クラスタの追加"](#)。
3. 使用状況とパフォーマンス データの収集のための特定のロールを持つ Unified Manager ユーザーを作成します。次の手順を実行します。ユーザーロールの詳細については、["ユーザ ロールの定義"](#)。
 - a. インストール中に生成されるデフォルトのアプリケーション管理者ユーザー資格情報を使用して、Unified Manager Web UI にログインします。見る ["Unified Manager Web UIへのアクセス"](#)。
 - b. Keystone Collectorのサービスアカウントを作成します。`Operator`ユーザー ロール。Keystone Collector サービス API は、このサービス アカウントを使用して Unified Manager と通信し、使用状況データを収集します。見る ["ユーザの追加"](#)。

- c. 作成する `Database` ユーザーアカウント、`Report Schema` 役割。このユーザーはパフォーマンス データの収集に必要です。見る ["データベース ユーザの作成"](#)。



MySQL のデフォルト ポート 3306 は、Unified Manager の新規インストール時に localhost のみに制限されるため、Keystone ONTAPのパフォーマンス データは収集されません。この設定は変更可能で、接続は `Control access to MySQL port 3306` Unified Manager メンテナンス コンソールのオプション。詳細については、"[その他のメニュー オプション](#)"。

4. Unified Manager で API Gateway を有効にします。Keystone Collector は、API Gateway 機能を利用してONTAPクラスターと通信します。API Gateway は、Web UI から、または Unified Manager CLI を通じていくつかのコマンドを実行して有効にすることができます。

ウェブUI

Unified Manager Web UI から API Gateway を有効にするには、Unified Manager Web UI にログインし、API Gateway を有効にします。詳細については、"[APIゲートウェイの有効化](#)"。

CLI

Unified Manager CLI を介して API Gateway を有効にするには、次の手順に従います。

- Unified Manager サーバーで SSH セッションを開始し、Unified Manager CLI にログインします。
`um cli login -u <umadmin>` CLIコマンドの詳細については、"[サポートされるUnified ManagerのCLIコマンド](#)"。
- API Gateway がすでに有効になっているかどうかを確認します。
``um option list api.gateway.enabled`` あ ``true`` 値は、API ゲートウェイが有効になっていることを示します。
- 返される値が `false`` 次のコマンドを実行します。
``um option set api.gateway.enabled=true``
- Unified Manager サーバーを再起動します。
 - リナックス: "[Unified Managerの再起動](#)"。
 - VMware vSphere: "[Unified Manager仮想マシンの再起動](#)"。

StorageGRID

StorageGRIDにKeystone Collector をインストールするには、次の構成が必要です。

- StorageGRID `11.6.0` 以降をインストールする必要があります。StorageGRIDのアップグレードについては、以下を参照してください。"[StorageGRIDソフトウェアのアップグレード: 概要](#)"。
- 使用状況データの収集には、StorageGRIDローカル管理者ユーザー アカウントを作成する必要があります。このサービス アカウントは、管理者ノード API を介してStorageGRIDと通信するためにKeystone Collector サービスによって使用されます。

手順

- グリッド マネージャーにログインします。見る "[グリッドマネージャーにSign in](#)"。
- ローカル管理者グループを作成する Access mode: Read-only。見る "[管理者グループを作成する](#)"。
- 次の権限を追加します。

- テナントアカウント
 - メンテナンス
 - Metrics Query
- d. Keystoneサービス アカウント ユーザーを作成し、それを管理者グループに関連付けます。見る "[ユーザの管理](#)"。

Keystone Collectorをインストールする

VMware vSphere システムにKeystone Collector を導入する

VMware vSphere システムにKeystone Collector をデプロイするには、OVA テンプレートのダウンロード、**OVF** テンプレートのデプロイ ウィザードを使用したテンプレートのデプロイ、証明書の整合性の検証、および VM の準備状況の検証が含まれます。

OVAテンプレートのデプロイ

次の手順を実行します。

手順

1. OVAファイルをダウンロードするには "[このリンク](#)" VMware vSphere システムに保存します。
2. VMware vSphere システムで、**VM** とテンプレート ビューに移動します。
3. 仮想マシン (VM) の必要なフォルダー (VM フォルダーを使用していない場合はデータセンター) を右クリックし、**OVF** テンプレートのデプロイ を選択します。
4. *OVFテンプレートのデプロイ*ウィザードの_ステップ1_で、*OVFテンプレートの選択*をクリックしてダウンロードしたテンプレートを選択します。`KeystoneCollector-latest.ova`ファイル。
5. ステップ 2 で、VM 名を指定し、VM フォルダーを選択します。
6. ステップ 3 で、VM を実行するために必要なコンピューティング リソースを指定します。
7. 「ステップ 4: 詳細の確認」で、OVA ファイルの正確性と信頼性を確認します。

vCenter ルート信頼ストアには VMware 証明書のみが含まれます。NetApp は証明機関として Entrust を使用しており、それらの証明書を vCenter 信頼ストアに追加する必要があります。

- a. Sectigoからコード署名CA証明書をダウンロードする "[ここをクリックしてください](#)"。
- b. 以下の手順に従ってください `Resolution` このナレッジベース (KB) 記事のセクション:
<https://kb.vmware.com/s/article/84240>。



vCenter バージョン 7.x 以前の場合は、vCenter と ESXi をバージョン 8.0 以降に更新する必要があります。以前のバージョンはサポートされなくなりました。

Keystone Collector OVAの完全性と信頼性が検証されると、テキストが表示されます。(Trusted certificate) 出版社と。

Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Select networks

7 Customize template

8 Ready to complete

Review details

×

Verify the template details.

Publisher	Sectigo Public Code Signing CA R36 (Trusted certificate)
Product	Keystone-Collector
Version	3.12.31910
Vendor	NetApp
Download size	1.7 GB
Size on disk	3.9 GB (thin provisioned) 19.5 GB (thick provisioned)

CANCEL

BACK

NEXT

8. *OVF テンプレートのデプロイ*ウィザードの ステップ 5 で、VM を保存する場所を指定します。
9. ステップ 6 で、VM が使用する宛先ネットワークを選択します。
10. ステップ 7 テンプレートのカスタマイズ で、管理者ユーザー アカウントの初期ネットワーク アドレスとパスワードを指定します。



管理者パスワードは、vCentre に可逆形式で保存され、VMware vSphere システムへの初期アクセスを取得するためのブートストラップ資格情報として使用する必要があります。ソフトウェアの初期構成時に、この管理者パスワードを変更する必要があります。IPv4 アドレスのサブネット マスクは CIDR 表記で指定する必要があります。たとえば、サブネット マスク 255.255.255.0 の場合は値 24 を使用します。

11. *OVF テンプレートのデプロイ*ウィザードの_ステップ 8 完了準備_で、構成を確認し、OVA デプロイのパラメータが正しく設定されていることを確認します。

VM がテンプレートからデプロイされ、電源がオンになったら、VM への SSH セッションを開き、一時的な管理者の資格情報を使用してログインし、VM の構成の準備ができていることを確認します。

初期システム構成

OVA を通じて展開されたKeystone Collector サーバーの初期構成を行うには、VMware vSphere システムで次の手順を実行します。



導入が完了したら、Keystone Collector 管理ターミナル ユーザー インターフェイス (TUI) ユーティリティを使用して、構成および監視アクティビティを実行できます。Enter キーや矢印キーなどのさまざまなキーボード コントロールを使用して、オプションを選択し、この TUI 内を移動できます。

1. Keystone Collector サーバーへの SSH セッションを開きます。接続すると、管理者パスワードを更新するように求められます。必要に応じて管理者パスワードの更新を完了します。
2. TUI にアクセスするには、新しいパスワードを使用してログインします。ログインすると、TUI が表示されます。

あるいは、以下のコマンドを実行して手動で起動することもできます。 `keystone-collector-tui` CLI コマンド。

3. 必要に応じて、TUI の `*[構成] > [ネットワーク] セクション*` でプロキシの詳細を設定します。
4. `構成 > システム` セクションで、システムのホスト名、場所、および NTP サーバーを構成します。
5. `メンテナンス > コレクターの更新` オプションを使用して、Keystone コレクターを更新します。更新後、Keystone Collector 管理 TUI ユーティリティを再起動して変更を適用します。

Linux システムに Keystone Collector をインストールする

RPM または Debian パッケージを使用して、Keystone Collector ソフトウェアを Linux サーバーにインストールできます。Linux ディストリビューションに応じてインストール手順に従います。

RPMの使用

1. Keystone CollectorサーバーにSSHで接続し、`root`特権。
2. Keystone公開署名をインポートします。

```
# rpm --import https://keystone.netapp.com/repo1/RPM-GPG-NetApp-Keystone-20251020
```
3. RPM データベースでKeystone Billing Platform のフィンガープリントをチェックして、正しい公開証明書がインポートされていることを確認します。

```
# rpm -qa gpg-pubkey --qf '%{Description}' | gpg --show-keys --fingerprint 正しい指紋は次のようになります。  
9297 0DB6 0867 22E7 7646 E400 4493 5CBB C9E9 FEDC
```
4. ダウンロード keystonerepo.rpm ファイル：

```
curl -O https://keystone.netapp.com/repo1/keystonerepo.rpm
```
5. ファイルの信頼性を確認します。

```
rpm --checksig -v keystonerepo.rpm 本物のファイルの署名は次のようになります。  
Header V4 RSA/SHA512 Signature, key ID c9e9fedc: OK
```
6. YUM ソフトウェア リポジトリ ファイルをインストールします。

```
# yum install keystonerepo.rpm
```
7. Keystoneリポジトリがインストールされたら、YUM パッケージ マネージャーを使用して keystone-collector パッケージをインストールします。

```
# yum install keystone-collector
```

Red Hat Enterprise Linux 9 の場合は、次のコマンドを実行して keystone-collector パッケージをインストールします。

```
# yum install keystone-collector-rhel9
```

Debianの使用

1. Keystone CollectorサーバーにSSHで接続し、`root`特権。

```
`sudo su
```
2. ダウンロード keystone-sw-repo.deb`ファイル：

```
`curl -O https://keystone.netapp.com/downloads/keystone-sw-repo.deb
```
3. Keystoneソフトウェア リポジトリ ファイルをインストールします。

```
# dpkg -i keystone-sw-repo.deb
```
4. パッケージ リストを更新します。

```
# apt-get update
```
5. Keystoneリポジトリがインストールされたら、keystone-collector パッケージをインストールします。

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



インストールが完了すると、Keystone Collector 管理ターミナル ユーザー インターフェイス (TUI) ユーティリティを使用して、構成および監視アクティビティを実行できます。Enter キーや矢印キーなどのさまざまなキーボード コントロールを使用して、オプションを選択し、この TUI 内を移動できます。見る["Keystone Collector を構成する"](#)そして["システムの健全性を監視する"](#)情報については。

Keystoneソフトウェアの自動検証

Keystoneリポジトリは、Keystoneソフトウェアの整合性を自動的に検証するように構成されているため、有効で正規のソフトウェアのみがサイトにインストールされます。

Keystone YUMリポジトリクライアント設定は、`keystonerepo.rpm`強制GPGチェック`を利用する(``gpgcheck=1`)がこのリポジトリを通じてダウンロードされたすべてのソフトウェアに適用されます。Keystoneリポジトリからダウンロードした RPM のうち、署名検証に失敗したものはインストールされません。この機能は、Keystone Collector のスケジュールされた自動更新機能で使用され、有効で正規のソフトウェアのみがサイトにインストールされるようになります。

Keystone Collector を構成する

Keystone Collector がストレージ環境の使用状況データを収集できるようにするには、いくつかの構成タスクを完了する必要があります。これは、必要なコンポーネントをアクティブ化し、ストレージ環境に関連付ける 1 回限りのアクティビティです。



- Keystone Collector には、構成および監視アクティビティを実行するためのKeystone Collector 管理ターミナル ユーザー インターフェイス (TUI) ユーティリティが用意されています。Enter キーや矢印キーなどのさまざまなキーボード コントロールを使用して、オプションを選択し、この TUI 内を移動できます。
- Keystone Collector は、インターネットにアクセスできない組織向けに構成できます。これは、["プライベートモードのKeystone"](#)。これは、["プライベートモードのKeystone"](#)とも呼ばれます。詳細については、以下を参照してください。

手順

1. Keystone Collector 管理 TUI ユーティリティを起動します。
`$ keystone-collector-tui`
2. **[構成] > [KS-Collector]** に移動してKeystone Collector 構成画面を開き、更新に使用できるオプションを表示します。
3. 必要なオプションを更新します。

 ONTAPの場合

- * ONTAP の使用状況の収集*: このオプションにより、ONTAPの使用状況データの収集が有効になります。Active IQ Unified Manager (Unified Manager) サーバーとサービス アカウントの詳細を追加します。
- * ONTAPパフォーマンス データの収集*: このオプションにより、ONTAPのパフォーマンス データの収集が有効になります。これはデフォルトでは無効になっています。SLA の目的で環境でパフォーマンス監視が必要な場合は、このオプションを有効にします。Unified Manager データベース ユーザー アカウントの詳細を入力します。データベースユーザーの作成については、以下を参照してください。["Unified Managerユーザーを作成する"](#)。
- 個人データの削除: このオプションは顧客の特定の個人データを削除し、デフォルトで有効になっています。このオプションが有効になっている場合にメトリックから除外されるデータの詳細については、以下を参照してください。["個人データの収集を制限する"](#)。

 StorageGRIDの場合

- * StorageGRID の使用状況の収集*: このオプションにより、ノードの使用状況の詳細の収集が有効になります。StorageGRIDノード アドレスとユーザーの詳細を追加します。
- 個人データの削除: このオプションは顧客の特定の個人データを削除し、デフォルトで有効になっています。このオプションが有効になっている場合にメトリックから除外されるデータの詳細については、以下を参照してください。["個人データの収集を制限する"](#)。

4. システムで **KS-Collector** を起動 フィールドを切り替えます。
5. **[保存]**をクリックします。


```
NetApp Keystone Collector - Configure - KS Collector

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

6. TUI のメイン画面に戻り、サービス ステータス 情報を確認して、Keystone Collector が正常な状態であることを確認します。システムでは、サービスが 全体: 正常 状態にあることが示されるはずで

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

す。

7. ホーム画面で **[Exit to Shell]** オプションを選択して、Keystone Collector 管理 TUI を終了します。

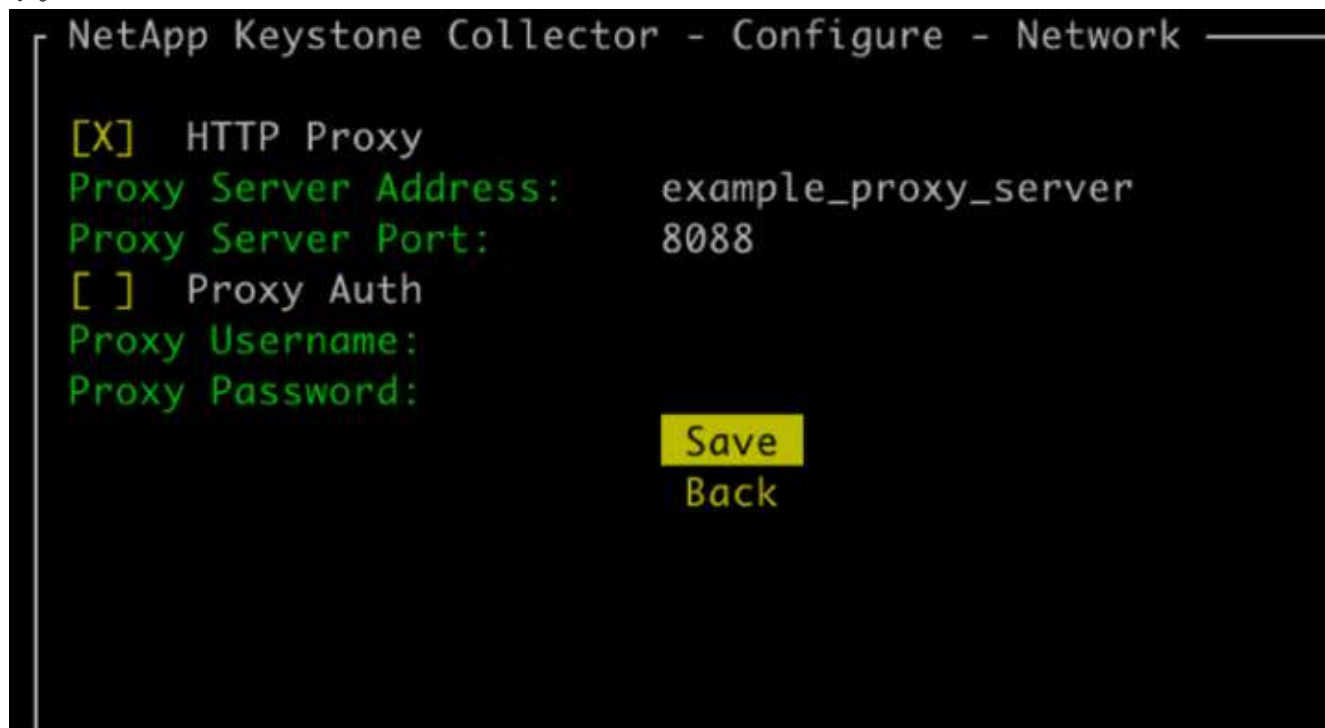
Keystone Collector で HTTP プロキシを構成する

コレクター ソフトウェアは、インターネットとの通信に HTTP プロキシの使用をサポートしています。これは TUI で設定できます。

手順

1. すでに閉じられている場合は、Keystone Collector 管理 TUI ユーティリティを再起動します。
\$ keystone-collector-tui
2. **HTTP** プロキシ フィールドをオンにして、認証が必要な場合は、HTTP プロキシ サーバー、ポート、および資格情報の詳細を追加します。
3. **[保存]**をクリックしま

す。



個人データの収集を制限する

Keystone Collector は、サブスクリプション計測を実行するために必要な限定された構成、ステータス、およびパフォーマンス情報を収集します。アップロードされたコンテンツから機密情報をマスクすることで、収集される情報をさらに制限するオプションがあります。これは請求額の計算には影響しません。ただし、情報を制限すると、ボリューム名などユーザーが簡単に識別できる一部の要素が UUID に置き換えられるため、レポート情報の使いやすさに影響する可能性があります。

特定の顧客データの収集を制限することは、Keystone Collector TUI 画面で構成可能なオプションです。このオプション「プライベート データの削除」は、デフォルトで有効になっています。

```
NetApp Keystone Collector - Configure - KS Collector

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

[ ] Collect ONTAP Performance Data

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

ONTAPとStorageGRIDの両方でプライベートデータアクセスを制限する際に削除された項目については、以下を参照してください。["個人データへのアクセス制限により削除された項目のリスト"](#)。

カスタムルートCAを信頼する

公開ルート証明機関 (CA) に対する証明書の検証は、Keystone Collector のセキュリティ機能の一部です。ただし、必要に応じて、カスタム ルート CA を信頼するようにKeystone Collector を構成することもできます。

システム ファイアウォールで SSL/TLS 検査を使用すると、インターネット ベースのトラフィックがカスタム CA 証明書で再暗号化されます。ルート証明書を受け入れて接続を許可する前に、ソースを信頼できる CA として検証するための設定を構成する必要があります。次の手順を実行します。

手順

1. CA 証明書を準備します。base64 エンコード X.509 ファイル形式である必要があります。



サポートされているファイル拡張子は .pem、.crt、.cert。証明書がこれらの形式のいずれかであることを確認してください。

2. 証明書をKeystone Collector サーバーにコピーします。ファイルがコピーされる場所をメモしておきます。
3. サーバー上でターミナルを開き、管理 TUI ユーティリティを実行します。
`$ keystone-collector-tui`
4. *[構成] > [詳細設定]*に移動します。
5. カスタム ルート証明書を有効にする オプションを有効にします。

6. *カスタムルート証明書のパスを選択*で、 - Unset -
7. Enterキーを押します。証明書パスを選択するためのダイアログ ボックスが表示されます。
8. ファイル システム ブラウザからルート証明書を選択するか、正確なパスを入力します。
9. Enterキーを押します。*詳細*画面に戻ります。
10. *保存*を選択します。設定が適用されます。



CA証明書は以下にコピーされます /opt/netapp/ks-collector/ca.pem Keystone Collector サーバー上。

```
NetApp Keystone Collector - Configure - Advanced

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

パフォーマンスサービスレベルの作成

Keystone Collector 管理 TUI ユーティリティを使用して、パフォーマンス サービス レベル (PSL) を作成できます。TUI を使用して PSL を作成すると、各パフォーマンス サービス レベルに設定されているデフォルト値が自動的に選択されるため、Active IQ Unified Managerを使用して PSL を作成する際にこれらの値を手動で設定した場合に発生する可能性のあるエラーの可能性が軽減されます。

PSLの詳細については、以下を参照してください。["パフォーマンスサービスレベル"](#)。

サービスレベルの詳細については、以下を参照してください。["Keystoneのサービスレベル"](#)。

手順

1. Keystone Collector 管理 TUI ユーティリティを起動します。
\$ keystone-collector-tui

2. AIQUM 画面を開くには、「**Configure>AIQUM**」に移動します。
3. **AIQUM** パフォーマンス プロファイルの作成 オプションを有効にします。
4. Active IQ Unified Managerサーバーとユーザー アカウントの詳細を入力します。これらの詳細は PSL の作成に必要であり、保存されません。

```
NetApp Keystone Collector - Configure - AIQUM

[ ] Enable Embedded UM
[X] Create AIQUM Performance Profiles

AIQUM Address:
AIQUM Username:
AIQUM Password:
Select Keystone version      -unset-
Select Keystone Service Levels

Save
Back

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

5. * Keystoneバージョンを選択*の場合は、 -unset- 。
6. Enterキーを押します。Keystone のバージョンを選択するためのダイアログ ボックスが表示されます。
7. **STaaS** を強調表示してKeystone STaaS のKeystoneバージョンを指定し、Enter キーを押します。

NetApp Keystone Collector – Configure – AIQUM

AIQUM Ad
AIQUM Us
AIQUM Pa
Select K
Select K

Select Keystone version

KFS
STaaS

Save
Back

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



Keystoneサブスクリプション サービス バージョン 1 の **KFS** オプションを強調表示できます。Keystoneサブスクリプション サービスは、構成パフォーマンス サービス レベル、サービス提供、課金原則においてKeystone STaaS とは異なります。詳細については、"[Keystoneサブスクリプション サービス | バージョン 1](#)"。

- 指定されたKeystoneバージョンの * Keystoneサービス レベルの選択* オプション内に、サポートされているすべてのKeystoneパフォーマンス サービス レベルが表示されます。リストから必要なパフォーマンス サービス レベルを有効にします。

```

NetApp Keystone Collector - Configure - AIQUM

[ ] Enable Embedded UM
[X] Create AIQUM Performance Profiles

AIQUM Address:
AIQUM Username:
AIQUM Password:
Select Keystone version
Select Keystone Service Levels

-----
STaaS
[X] Extreme
[X] Premium
[ ] Performance
[ ] Standard
[ ] Value

Save
Back

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

```



複数のパフォーマンス サービス レベルを同時に選択して PSL を作成できます。

9. *保存*を選択し、Enterを押します。パフォーマンス サービス レベルが作成されます。

STaaS の場合は Premium-KS-STaaS、KFS の場合は Extreme KFS など、作成された PSL は、Active IQ Unified Managerの パフォーマンス サービス レベル ページで確認できます。作成された PSL が要件を満たしていない場合は、ニーズを満たすように PSL を変更できます。詳細については、"[パフォーマンス サービス レベルの作成と編集](#)"。




Performance Service Levels

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

 Filter

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



<input type="checkbox"/>	Name ^	Type	Expected IOPS/TB	Peak IOPS/TB	Absolute Minim...	Expected Latency	Capacity	Workloads
	Extreme - KFS	User-defined	6144	12288	1000	1	<div><div></div></div> Used: 0 bytes Available: 283.85 TiB	0
	Extreme - KS-STaaS	User-defined	6144	12288	1000	1	<div><div></div></div> Used: 0 bytes Available: 283.85 TiB	0
Overview								
Description		Extreme - KS-STaaS						
Added Date		1 Aug 2024, 18:08						
Last Modified Date		1 Aug 2024, 18:08						
	Premium ...S-STaaS	User-defined	2048	4096	500	2	<div><div></div></div> Used: 0 bytes Available: 283.85 TiB	0

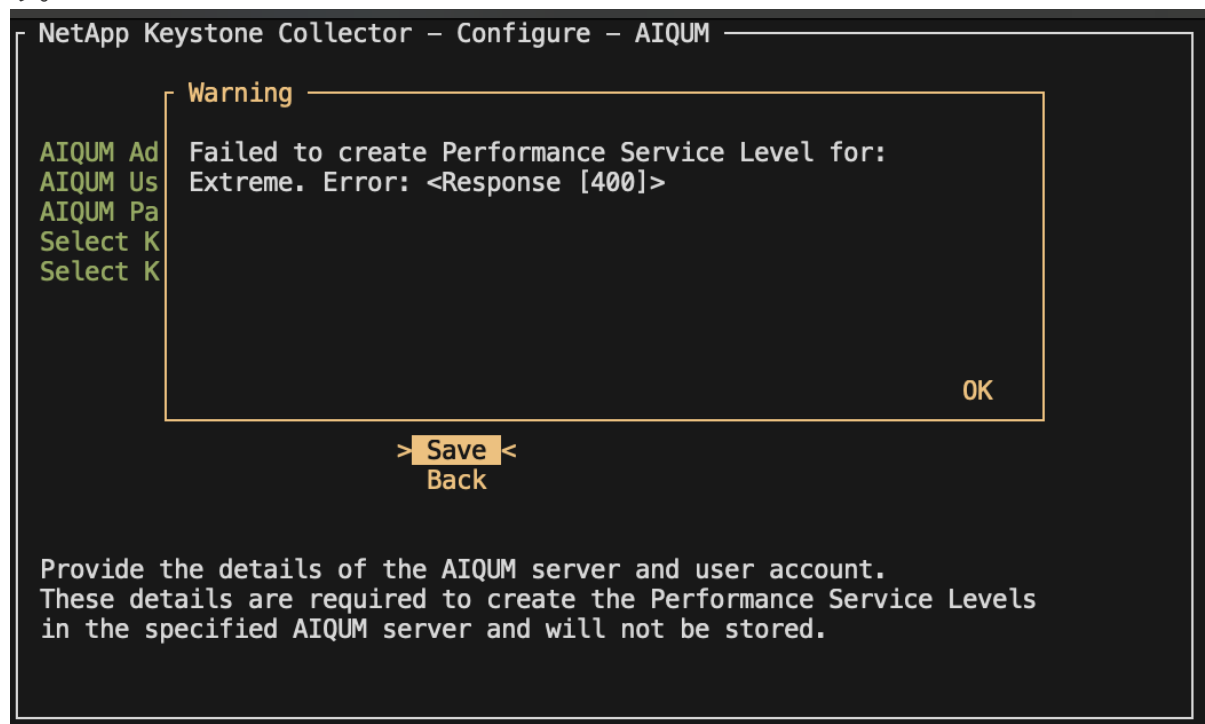
Overview

Description Premium - KS-STaaS

Added Date 1 Aug 2024, 18:08

Last Modified Date 1 Aug 2024, 18:08

選択したパフォーマンス サービス レベルの PSL が、指定されたActive IQ Unified Manager サーバーにすでに存在する場合は、再度作成することはできません。そうしようとすると、エラーメッセージが表示されます。



ITOMコレクターをインストールする

Keystone ITOM Collector のインストール要件

ITOM Collector をインストールする前に、システムに必要なソフトウェアが準備されており、必要な前提条件をすべて満たしていることを確認してください。

ITOM コレクター サーバー VM の前提条件:

- サポートされているオペレーティング システム:
 - Debian 12以降
 - Windows Server 2016以降
 - Ubuntu 20.04 LTS以降
 - Red Hat Enterprise Linux (RHEL) 8.x
 - Red Hat Enterprise Linux 9.0 以降
 - Amazon Linux 2023以降



推奨されるオペレーティング システムは、Debian 12、Windows Server 2016、またはそれ以降のバージョンです。

- リソース要件: 監視対象のNetAppノードの数に基づく VM リソース要件は次のとおりです。
 - 2 ～ 10 ノード: 4 CPU、8 GB RAM、40 GB ディスク
 - 12 ～ 20 ノード: 8 CPU、16 GB RAM、40 GB ディスク
- 構成要件: 監視対象デバイスに読み取り専用アカウントと SNMP が設定されていることを確認します。ITOM コレクター サーバー VM は、NetAppクラスターおよびクラスター スイッチ (該当する場合) 上の SNMP トラップ ホストおよび Syslog サーバーとして構成する必要があります。

ネットワーク要件

ITOM Collector のネットワーク要件を次の表に示します。

ソース	デスティネーション	プロトコル	ポート	説明
ITOMコレクター	NetApp ONTAPクラスタ管理 IP	HTTPS、SNMP	TCP 443、UDP 161	ONTAPコントローラの監視
NetApp ONTAPクラスタおよびノード管理 IP	ITOMコレクター	SNMP、Syslog	UDP 162、UDP 514	コントローラからのSNMPトラップとSyslog
ITOMコレクター	クラスタースイッチ	SNMP	UDP 161	スイッチの監視
クラスタースイッチ	ITOMコレクター	SNMP、Syslog	UDP 162、UDP 514	スイッチからのSNMPトラップとSyslog
ITOMコレクター	StorageGRIDノードのIP	HTTPS、SNMP	TCP 443、UDP 161	StorageGRIDのSNMP監視
StorageGRIDノードのIP	ITOMコレクター	SNMP、Syslog	UDP 162、UDP 514	StorageGRIDからのSNMPトラップ

ITOMコレクター	Keystoneコレクター	SSH、HTTPS、SNMP	TCP 22、TCP 443、UDP 161	Keystone Collectorの監視とリモート管理
ITOMコレクター	ローカルDNS	DNS	UDP 53	パブリックまたはプライベートDNSサービス
ITOMコレクター	選択したNTPサーバー	NTP	UDP 123	時間管理

LinuxシステムにKeystone ITOM Collectorをインストールする

ストレージ環境内のメトリック データを収集する ITOM Collector をインストールするには、いくつかの手順を実行します。要件に応じて、Windows システムまたは Linux システムにインストールできます。



Keystoneサポート チームは、ITOM Collector セットアップ ファイルをダウンロードするための動的リンクを提供しますが、このリンクは 2 時間で有効期限が切れます。

WindowsシステムにITOM Collectorをインストールするには、"[WindowsシステムにITOM Collectorをインストールする](#)"。

Linux サーバーにソフトウェアをインストールするには、次の手順に従います。

開始する前に

- Linux インストール スクリプトで Bourne シェルが使用できることを確認します。
- インストール `vim-common` ITOM Collector セットアップ ファイルに必要な **xxd** バイナリを取得するパッケージ。
- 確実に `sudo package` ITOM Collector を非ルート ユーザーとして実行する予定の場合はインストールされます。

手順

1. ITOM コレクターのセットアップ ファイルを Linux サーバーにダウンロードします。
2. サーバー上でターミナルを開き、次のコマンドを実行して権限を変更し、バイナリを実行可能にします。
`chmod +x <installer_file_name>.bin`
3. 次のコマンドを実行して、ITOM コレクターのセットアップ ファイルを起動します。
`./<installer_file_name>.bin`
4. セットアップ ファイルを実行すると、次のプロンプトが表示されます。
 - a. エンドユーザー使用許諾契約 (EULA) に同意します。
 - b. インストールのユーザー詳細を入力します。
 - c. インストール親ディレクトリを指定します。
 - d. コレクターのサイズを選択します。
 - e. 該当する場合は、プロキシの詳細を入力します。

各プロンプトに対して、デフォルトのオプションが表示されます。特別な要件がない限り、デフォルト

ト オプションを選択することをお勧めします。デフォルトのオプションを選択するには、**Enter** キーを押してください。インストールが完了すると、ITOM Collector が正常にインストールされたことを確認するメッセージが表示されます。



- ITOMコレクターのセットアップファイルは、`/etc/sudoers`サービスの再起動とメモリ ダンプを処理します。
- Linux サーバーに ITOM Collector をインストールすると、ルート権限なしで ITOM Collector を実行するための **ITOM** というデフォルトのユーザーが作成されます。別のユーザーを選択したり、root として実行したりすることもできますが、Linux インストール スクリプトによって作成された ITOM ユーザーを使用することをお勧めします。

次の手順

インストールが成功したら、Keystoneサポート チームに連絡して、ITOM サポート ポータルを通じて ITOM Collector のインストールが成功したことを確認してください。検証後、Keystoneサポート チームは、デバイスの検出や監視の設定など、ITOM Collector をリモートで構成し、構成が完了したら確認を送信します。ご質問や追加情報については、keystone.services@netapp.com までお問い合わせください。

Windows システムにKeystone ITOM Collector をインストールする

ITOM Collector セットアップ ファイルをダウンロードし、InstallShield ウィザードを実行して、必要な監視資格情報を入力して、Windows システムに ITOM Collector をインストールします。



Keystoneサポート チームは、ITOM Collector セットアップ ファイルをダウンロードするための動的リンクを提供しますが、このリンクは 2 時間で有効期限が切れます。

要件に応じて Linux システムにインストールできます。LinuxシステムにITOM Collectorをインストールするには、"[LinuxシステムにITOM Collectorをインストールする](#)"。

Windows サーバーに ITOM コレクター ソフトウェアをインストールするには、次の手順に従います。

開始する前に

Windows サーバーのローカル セキュリティ ポリシー設定のローカル ポリシー/ユーザー権利の割り当てで、ITOM Collector サービスに サービスとしてログオン が許可されていることを確認します。

手順

1. ITOM コレクターのセットアップ ファイルを Windows サーバーにダウンロードします。
2. セットアップ ファイルを開いて、InstallShield ウィザードを起動します。
3. エンドユーザー使用許諾契約 (EULA) に同意します。InstallShield ウィザードは必要なバイナリを抽出し、資格情報の入力を求めます。
4. ITOM Collector を実行するアカウントの資格情報を入力します。
 - ITOM Collector が他の Windows サーバーを監視していない場合は、ローカル システムを使用します。
 - ITOM Collector が同じドメイン内の他の Windows サーバーを監視している場合は、ローカル管理者権限を持つドメイン アカウントを使用します。
 - ITOM Collector が同じドメインに属さない他の Windows サーバーを監視している場合は、ローカル管

理者アカウントを使用し、ローカル管理者の資格情報で各リソースに接続します。ITOM Collector と監視対象リソース間の認証の問題を軽減するために、パスワードが期限切れにならないように設定することもできます。

- コレクターのサイズを選択します。デフォルトはセットアップ ファイルに基づく推奨サイズです。特別な要件がない限り、推奨サイズで進めてください。
- インストールを開始するには、[次へ] を選択します。既存のフォルダーを使用することも、別のフォルダーを選択することもできます。ステータス ボックスにインストールの進行状況が表示され、その後に [InstallShield ウィザードが完了しました] ダイアログ ボックスが表示されます。

次の手順

インストールが成功したら、Keystoneサポート チームに連絡して、ITOM サポート ポータルを通じて ITOM Collector のインストールが成功したことを確認してください。検証後、Keystoneサポート チームは、デバイスの検出や監視の設定など、ITOM Collector をリモートで構成し、構成が完了したら確認を送信します。ご質問や追加情報については、keystone.services@netapp.com までお問い合わせください。

KeystoneのAutoSupportを構成する

AutoSupportテレメトリ メカニズムを使用する場合、Keystone はAutoSupportテレメトリ データに基づいて使用状況を計算します。必要な粒度レベルを実現するには、ONTAPクラスタから送信される毎日のサポート バンドルにKeystoneデータを組み込むようにAutoSupportを設定する必要があります。

タスク概要

Keystoneデータを含めるようにAutoSupportを設定する前に、次の点に注意してください。

- AutoSupportテレメトリ オプションは、ONTAP CLI を使用して編集します。AutoSupportサービスとシステム（クラスタ）管理者ロールの管理については、以下を参照してください。"[AutoSupportの管理 - 概要](#)"そして"[クラスタ管理者とSVM管理者](#)"。
- Keystoneの正確なデータ収集を確実に行うには、サブシステムを毎日および毎週のAutoSupportバンドルに含めます。AutoSupportサブシステムの詳細については、以下を参照してください。"[AutoSupportサブシステムとは](#)"。

手順

- システム管理者ユーザーとして、SSH を使用してKeystone ONTAPクラスタにログインします。詳細については、"[SSHを使用したクラスタへのアクセス](#)"。
- ログの内容を変更します。
 - ONTAP 9.16.1 以降では、次のコマンドを実行して日次ログの内容を変更します。

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

クラスタがMetroCluster構成の場合、次のコマンドを実行します。

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

- 以前のONTAPバージョンの場合は、次のコマンドを実行して日次ログの内容を変更します。

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

クラスタがMetroCluster構成の場合、次のコマンドを実行します。

```
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
```

- 週次ログの内容を変更するには、次のコマンドを実行します。

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

このコマンドの詳細については、["system node autosupport trigger modify"](#)。

監視とアップグレード

Keystone Collector の健全性を監視する

HTTP リクエストをサポートする任意の監視システムを使用して、Keystone Collector の健全性を監視できます。ヘルスを監視することで、Keystoneダッシュボードでデータを利用できるようになります。

デフォルトでは、Keystoneヘルス サービスは、localhost 以外の IP からの接続を受け入れません。Keystoneヘルスエンドポイントは /uber/health、Keystone Collectorサーバーのすべてのインターフェースのポートでリッスンします 7777。クエリを実行すると、エンドポイントから応答として、Keystone Collector システムのステータスを示す JSON 出力を含む HTTP 要求ステータス コードが返されます。JSON本体は、`is_healthy`属性はブール値であり、コンポーネントごとの詳細なステータスリストは `component_details`属性。次に例を示します。

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

次のステータス コードが返されます。

- **200:** 監視対象のすべてのコンポーネントが正常であることを示します
- **503:** 1つ以上のコンポーネントが正常でないことを示します
- **403:** ヘルス ステータスを照会している HTTP クライアントが、許可されたネットワーク CIDR のリストである *allow* リストに含まれていないことを示します。このステータスの場合、健康情報は返されません。*allow* リストは、ネットワーク CIDR 方式を使用して、どのネットワーク デバイスがKeystoneヘルスシステムを照会できるかを制御します。このエラーが発生した場合は、* Keystone Collector 管理 TUI > 構成 > ヘルス モニタリング* から監視システムを 許可 リストに追加してください。

Linux ユーザーの方は、次の既知の問題に注意してください。



問題の説明: Keystone Collector は、使用量計測システムの一部として多数のコンテナを実行します。Red Hat Enterprise Linux 8.x サーバーが米国国防情報システム局 (DISA) のセキュリティ技術実装ガイド (STIG) ポリシーで強化されている場合、*fapolicyd* (ファイル アクセス ポリシー デーモン) に関する既知の問題が断続的に発生します。この問題は次のように認識されています"[バグ 1907870](#)"。回避策: Red Hat Enterpriseで解決されるまで、NetAppこの問題を回避するために、*fapolicyd* 許容モードに移行します。

で`etc/fapolicyd/fapolicyd.conf`の値を設定する `permissive = 1。

システムログを表示する

Keystone Collector システム ログを表示してシステム情報を確認したり、それらのログを使用してトラブルシューティングを実行したりできます。Keystone Collector はホストの *journald* ログ システムを使用し、システム ログは標準の *journalctl* システム ユーティリティを通じて確認できます。ログを調べるには、次の主要なサービスを利用できます。

- ksコレクター
- ks-ヘルス
- ks-自動更新

メインのデータ収集サービス *_ks-collector_* は、JSON形式でログを生成します。`run-id` スケジュールされた各データ収集ジョブに関連付けられた属性。以下は、標準的な使用状況データ収集の成功したジョブの例です。

```

{"level":"info","time":"2022-10-31T05:20:01.831Z","caller":"light-
collector/main.go:31","msg":"initialising light collector with run-id
cdf1m0f74cgphgfon8cg","run-id":"cdf1m0f74cgphgfon8cg"}
{"level":"info","time":"2022-10-
31T05:20:04.624Z","caller":"ontap/service.go:215","msg":"223 volumes
collected for cluster a2049dd4-bfcf-11ec-8500-00505695ce60","run-
id":"cdf1m0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-
31T05:20:18.821Z","caller":"ontap/service.go:215","msg":"697 volumes
collected for cluster 909cbacc-bfcf-11ec-8500-00505695ce60","run-
id":"cdf1m0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-
31T05:20:41.598Z","caller":"ontap/service.go:215","msg":"7 volumes
collected for cluster f7b9a30c-55dc-11ed-9c88-005056b3d66f","run-
id":"cdf1m0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-
31T05:20:48.247Z","caller":"ontap/service.go:215","msg":"24 volumes
collected for cluster a9e2dcff-ab21-11ec-8428-00a098ad3ba2","run-
id":"cdf1m0f74cgphgfon8cg"}

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

{"level":"info","time":"2022-10-
31T05:20:48.839Z","caller":"reception/reception.go:75","msg":"Sending file
65a71542-cb4d-bdb2-e9a7-a826be4fdcb7_1667193648.tar.gz type=ontap to
reception","run-id":"cdf1m0f74cgphgfon8cg"}

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

{"level":"info","time":"2022-10-
31T05:20:51.324Z","caller":"reception/reception.go:99","msg":"uploaded
usage file to reception with status 201 Created","run-
id":"cdf1m0f74cgphgfon8cg"}

```

以下は、オプションのパフォーマンス データ収集の成功したジョブの例です。

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

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

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

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

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

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

{"level":"info","time":"2022-10-31T05:21:31.385Z","caller":"worker/collector.go:244","msg":"New file generated: 65a71542-cb4d-bdb2-e9a7-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":"cdf1m0f74cgphgfon8cg"}

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

{"level":"info","time":"2022-10-31T05:21:33.025Z","caller":"reception/reception.go:99","msg":"uploaded usage file to reception with status 201 Created","run-id":"cdf1m0f74cgphgfon8cg"}

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

サポートバンドルを生成して収集する

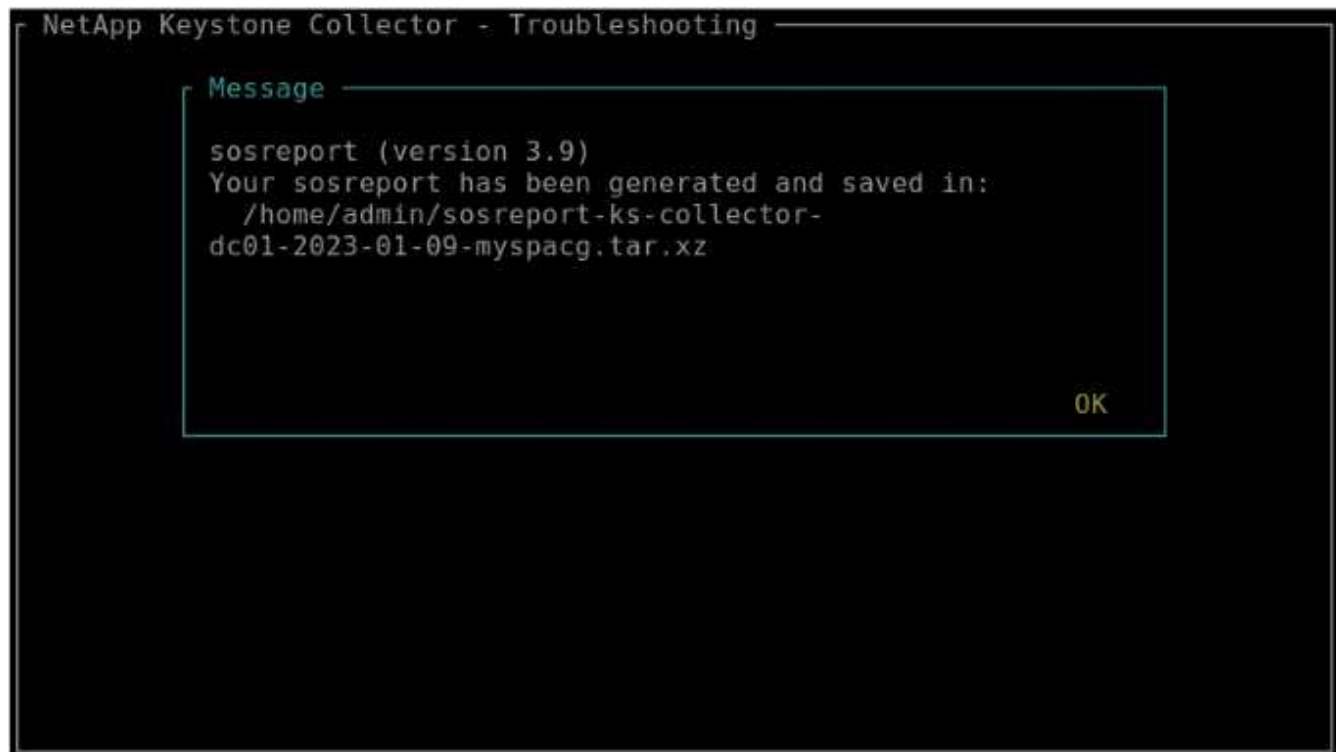
Keystone Collector TUI を使用すると、サポート バンドルを生成し、サポートの問題を解決するためにサービス リクエストに追加できます。次の手順に従ってください。

手順

1. Keystone Collector 管理 TUI ユーティリティを起動します。
\$ keystone-collector-tui
2. トラブルシューティング > サポート バンドルの生成 に移動します。



3. 生成されると、バンドルが保存される場所が表示されます。FTP、SFTP、または SCP を使用してその場所に接続し、ログ ファイルをローカル システムにダウンロードします。



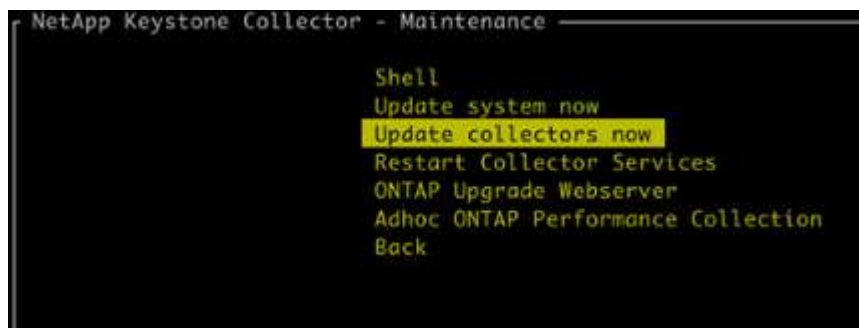
4. ファイルをダウンロードしたら、Keystone ServiceNow サポート チケットに添付できます。チケットの発行については、以下を参照してください。"[サービスリクエストの生成](#)"。

Keystone Collectorを手動でアップグレードする

Keystone Collector の自動更新機能はデフォルトで有効になっており、新しいリリースごとにKeystone Collector ソフトウェアが自動的にアップグレードされます。ただし、この機能を無効にして、ソフトウェアを手動でアップグレードすることもできます。

手順

1. Keystone Collector 管理 TUI ユーティリティを起動します。
`$ keystone-collector-tui`
2. メンテナンス画面で、[コレクターを今すぐ更新] オプションを選択します。



または、次のコマンドを実行してバージョンをアップグレードします。

CentOS の場合:

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

Debian の場合:

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

3. Keystone Collector 管理 TUI を再起動すると、ホーム画面の左上に最新バージョンが表示されます。

または、次のコマンドを実行して最新バージョンを表示します。

CentOS の場合:

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

Debian の場合:

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

Keystone Collectorのセキュリティ

Keystone Collector には、顧客データのセキュリティを危険にさらすことなく、Keystoneシステムのパフォーマンスと使用状況メトリックを監視するセキュリティ機能が含まれています。

Keystone Collector の機能は、次のセキュリティ原則に基づいています。

- プライバシー設計 - Keystone Collector は、使用状況の計測とパフォーマンスの監視を実行するために最小限のデータのみを収集します。詳細については、以下を参照してください。"[請求のために収集されたデータ](#)"。その"[個人データの削除](#)"オプションはデフォルトで有効になっており、機密情報をマスクして保護します。
- 最小権限アクセス - Keystone Collector では、ストレージ システムを監視するために最小限の権限しか必要としません。これにより、セキュリティ リスクが最小限に抑えられ、データへの意図しない変更が防止されます。このアプローチは最小権限の原則に沿っており、監視対象環境の全体的なセキュリティ体制を強化します。
- 安全なソフトウェア開発フレームワーク - Keystone は開発サイクル全体にわたって安全なソフトウェア開発フレームワークを使用しており、リスクを軽減し、脆弱性を減らし、システムを潜在的な脅威から保護します。

セキュリティ強化

デフォルトでは、Keystone Collector はセキュリティが強化された構成を使用するように設定されています。推奨されるセキュリティ構成は次のとおりです。

- Keystone Collector 仮想マシンのオペレーティング システム:
 - CIS Debian Linux 12 ベンチマーク標準に準拠しています。Keystone Collector 管理ソフトウェアの外部で OS 構成に変更を加えると、システムのセキュリティが低下する可能性があります。詳細については、以下を参照してください。"[CISベンチマークガイド](#)"。
 - 自動更新機能を通じて、Keystone Collector によって検証されたセキュリティ パッチを自動的に受信してインストールします。この機能を無効にすると、パッチが適用されていない脆弱なソフトウェアが発生する可能性があります。
 - Keystone Collector から受信した更新を認証します。APT リポジトリ検証を無効にすると、不正なパッチが自動的にインストールされ、脆弱性が生じる可能性があります。
- Keystone Collector は、接続のセキュリティを確保するために HTTPS 証明書を自動的に検証します。この機能を無効にすると、外部エンドポイントのなりすましや使用状況データの漏洩につながる可能性があります。
- Keystone Collectorはサポートしています"[カスタム信頼CA](#)"認証。デフォルトでは、"[Mozilla CA 証明書プログラム](#)"。追加の信頼できる CA を有効にすることで、Keystone Collector はこれらの証明書を提示するエンドポイントへの接続に対して HTTPS 証明書の検証を有効にします。
- Keystoneコレクターは、機密情報をマスクして保護する プライベート データの削除 オプションをデフォルトで有効にします。詳細については、以下を参照してください。"[個人データの収集を制限する](#)"。このオプションを無効にすると、追加のデータがKeystoneシステムに通信されることになります。たとえば、

ボリューム名など、機密情報と見なされる可能性のあるユーザーが入力した情報が含まれる場合があります。

関連情報

- ["Keystone Collector の概要"](#)
- ["仮想インフラストラクチャの要件"](#)
- ["Keystone Collector を構成する"](#)

Keystoneが収集するユーザーデータの種類

Keystone は、Keystone ONTAPおよびKeystone StorageGRIDサブスクリプションから構成、ステータス、使用状況情報、およびKeystone Collector をホストする仮想マシン (VM) からのテレメトリ データを収集します。 Keystone Collector でこのオプションが有効になっている場合、ONTAPのパフォーマンス データのみを収集できます。

ONTAPデータ収集

** ONTAPで収集される使用状況データ: 詳細はこちら**

次のリストは、ONTAPで収集された容量消費データの代表的なサンプルです。

- クラスタ
 - ClusterUUID
 - クラスタ名
 - シリアルナンバー
 - 場所（ONTAPクラスタに入力された値に基づく）
 - 担当者
 - version
- ノード
 - シリアルナンバー
 - ノード名
- ボリューム
 - アグリゲート名
 - ボリューム名
 - ボリュームインスタンスUUID
 - IsCloneVolumeフラグ
 - IsFlexGroupConstituentフラグ
 - IsSpaceEnforcementLogicalフラグ
 - IsSpaceReportingLogicalフラグ
 - 論理スペース使用率
 - スナップショットスペースの割合
 - パフォーマンス層非アクティブユーザーデータ
 - パフォーマンス層非アクティブユーザーデータ率
 - QoSAdaptivePolicyGroup名
 - QoSポリシーグループ名
 - サイズ
 - 使用済み
 - 物理的使用
 - スナップショットで使用されるサイズ
 - タイプ
 - ボリュームスタイル拡張
 - SVM名
 - IsVsRootフラグ

- Vサーバー
 - Vサーバー名
 - VserverUUID
 - サブタイプ
- ストレージアグリゲート
 - ストレージタイプ
 - アグリゲート名
 - 集約UUID
 - 物理使用
 - 使用可能なサイズ
 - サイズ
 - 使用済みサイズ
- 集約オブジェクトストア
 - オブジェクトストア名
 - オブジェクトストアUUID
 - プロバイダータイプ
 - アグリゲート名
- クローン ボリューム
 - FlexClone
 - サイズ
 - 使用済み
 - Vサーバー
 - タイプ
 - 親ボリューム
 - 親Vサーバー
 - 構成要素
 - 分割見積
 - 州
 - FlexClone使用率
- ストレージLUN
 - LUN UUID
 - LUN名
 - サイズ
 - 使用済み

- IsReservedフラグ
- IsRequestedフラグ
- 論理ユニット名
- QoSポリシーUUID
- QoSポリシー名
- ボリュームUUID
- ボリューム名
- SVMUUID
- SVM 名
- ストレージボリューム
 - ボリュームインスタンスUUID
 - ボリューム名
 - SVM名
 - SVMUUID
 - QoSポリシーUUID
 - QoSポリシー名
 - 容量層フットプリント
 - パフォーマンス層フットプリント
 - トータルフットプリント
 - 階層化ポリシー
 - IsProtectedフラグ
 - IsDestinationフラグ
 - 使用済み
 - 物理的使用
 - クローン親UUID
 - 論理スペース使用率
- QoSポリシー グループ
 - ポリシーグループ
 - QoSポリシーUUID
 - 最大スループット
 - 最小スループット
 - 最大スループットIOPS
 - 最大スループットMBps
 - 最小スループットIOPS

- 最小スループットMBps
- IsSharedフラグ
- ONTAPアダプティブQoSポリシーグループ
 - QoSポリシー名
 - QoSポリシーUUID
 - ピークIOPS
 - ピークIOPS割り当て
 - 絶対最小IOPS
 - 期待IOPS
 - 予想されるIOPS割り当て
 - ブロックサイズ
- 足跡
 - Vサーバー
 - Volume
 - トータルフットプリント
 - ボリュームブロックフットプリントビン0
 - ボリュームブロックフットプリントビン1
- MetroCluster
 - ノード
 - Aggregate
 - LIF
 - 設定のレプリケーション
 - 接続
 - クラスタ
 - ボリューム
- MetroClusterクラスタ
 - ClusterUUID
 - クラスタ名
 - リモートクラスタUUID
 - リモートクラスタ名
 - ローカル構成状態
 - リモート構成状態
- MetroClusterノード
 - DRミラーリング状態
 - クラスタ間LIF

- ノードの到達可能性
- DRパートナーノード
- DR補助パートナーノード
- DR、DR Aux、HAノードの対称関係
- 計画外の自動切り替え
- MetroCluster構成レプリケーション
 - リモートハートビート
 - 最後に送信されたハートビート
 - 最後に受信したハートビート
 - Vserver ストリーム
 - クラスターストリーム
 - ストレージ
 - 使用中のストレージ容量
- MetroClusterメディエーター
 - 調停人の住所
 - メディエーターポート
 - メディエーターが構成されました
 - 仲介者に到達可能
 - モード
- コレクターの可観測性メトリクス
 - 収集時間
 - Active IQ Unified Manager APIエンドポイントのクエリ
 - 応答時間
 - レコード数
 - AIQUMインスタンスIP
 - コレクタインスタンスID

** ONTAPで収集されたパフォーマンス データ: 詳細はこちら**

次のリストは、ONTAPで収集されたパフォーマンス データの代表的なサンプルです。

- クラスター名
- クラスタUUID
- オブジェクトID
- ボリューム名
- ボリュームインスタンスUUID
- Vサーバー
- VserverUUID
- ノードシリアル
- ONTAPVersion
- AIQUMバージョン
- Aggregate
- 集約UUID
- リソースキー
- タイムスタンプ
- IOPS/テラバイト
- レイテンシー
- 読み取り遅延
- 書き込みMBps
- QoS最小スループットレイテンシー
- QoSNBladeLatency
- 中古ヘッドルーム
- キャッシュミス率
- その他の遅延
- QoS 総計レイテンシ
- IOPS
- QoSネットワーク遅延
- 利用可能なオペレーション
- 書き込み遅延
- QoSクラウドレイテンシー
- QoSクラスタ相互接続レイテンシ
- その他のMBps
- QoSコプレーナレイテンシー

- QoSDBladeLatency
- 利用率
- 読み取りIOPS
- MBps
- その他のIOPS
- QoSポリシーグループレイテンシー
- 読み取りMBps
- QoS同期スナップミラーレイテンシー
- システムレベルのデータ
 - 書き込み/読み取り/その他/合計IOPS
 - 書き込み/読み取り/その他/合計スループット
 - 書き込み/読み取り/その他/合計レイテンシ
- 書き込みIOPS

****プライベートデータへのアクセス制限で削除された項目のリスト: 詳細はこちら****

Keystone Collector で プライベート データの削除 オプションが有効になっている場合、ONTAPの次の使用情報も削除されます。このオプションはデフォルトで有効になっています。

- クラスター名
- クラスターの場所
- クラスターコンタクト
- Node Name
- アグリゲート名
- ボリューム名
- QoSAdaptivePolicyGroup名
- QoSポリシーグループ名
- SVM名
- Storage LUN名
- アグリゲート名
- 論理ユニット名
- SVM 名
- AIQUMインスタンスIP
- FlexClone
- リモートクラスタ名

StorageGRIDデータ収集

** StorageGRIDで収集される使用状況データ: 詳細はこちら**

以下のリストは代表的な例です。 Logical Data StorageGRID用に収集されたもの：

- StorageGRID ID
- アカウント ID
- アカウント名
- アカウントクォータバイト
- バケット名
- バケットオブジェクト数
- バケットデータバイト

以下のリストは代表的な例です。 Physical Data StorageGRID用に収集されたもの：

- StorageGRID ID
- ノードID
- サイト ID
- サイト名
- 実例
- StorageGRIDストレージ使用率 バイト
- StorageGRIDストレージ使用率メタデータ バイト

以下のリストは代表的な例です。 Availability/Uptime Data StorageGRID用に収集されたもの：

- SLA 稼働率

プライベートデータへのアクセス制限で削除された項目のリスト: 詳細はこちら

Keystone Collector で プライベート データの削除 オプションが有効になっている場合、StorageGRIDの次の使用状況情報が削除されます。このオプションはデフォルトで有効になっています。

- アカウント名
- バケット名
- サイト名
- インスタンス/ノード名

テレメトリデータ収集

** Keystone Collector VM から収集されたテレメトリ データ: 詳細はこちら**

次のリストは、Keystoneシステムで収集されたテレメトリ データの代表的なサンプルです。

- システム情報
 - オペレーティングシステム名
 - オペレーティング システムのバージョン
 - オペレーティング システム ID
 - システムホスト名
 - システムのデフォルトIPアドレス
- システムリソースの使用状況
 - システム稼働時間
 - CPUコア数
 - システム負荷（1分、5分、15分）
 - 合計メモリ
 - 空きメモリ
 - 使用可能なメモリ
 - 共有メモリ
 - バッファメモリ
 - キャッシュメモリ
 - 合計スワップ
 - 無料交換
 - キャッシュされたスワップ
 - ディスクファイルシステム名
 - ディスク サイズ
 - 使用済みディスク
 - ディスク利用可能
 - ディスク使用率
 - ディスクマウントポイント
- インストールされたパッケージ
- コレクター構成
- サービスログ
 - Keystoneサービスからのサービスログ

プライベートモードのKeystone

Keystoneについて学ぶ（プライベートモード）

Keystone は、ビジネス要件とセキュリティ要件を満たすために、ダーク サイト とも呼ばれる プライベート デプロイメント モードを提供します。このモードは、接続制限のある組織で利用できます。

NetApp は、インターネット接続が制限されているか、インターネット接続がない環境 (ダーク サイトとも呼ばれます) 向けにカスタマイズされたKeystone STaaS の特殊な導入を提供します。これらは、セキュリティ、コンプライアンス、または運用上の要件により外部との通信が制限されている、安全な環境または分離された環境です。

NetApp Keystoneにとって、ダーク サイト向けのサービスを提供するということは、これらの環境の制約を尊重する方法でKeystone の柔軟なストレージ サブスクリプション サービスを提供することを意味します。これには以下が含まれます。

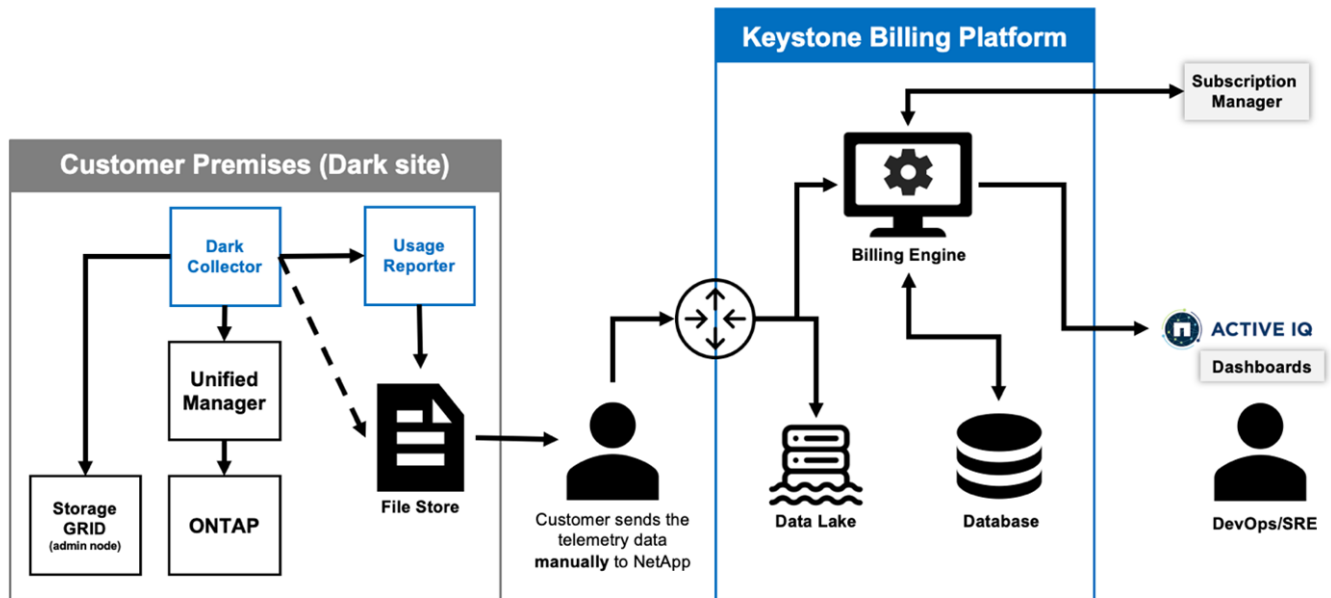
- ローカル展開: Keystone は分離された環境内で独立して構成できるため、セットアップ アクセスにインターネット接続や外部担当者が必要としません。
- オフライン操作: ヘルスチェックと課金機能を備えたすべてのストレージ管理機能は、オフラインで操作できます。
- セキュリティとコンプライアンス: Keystone は、高度な暗号化、安全なアクセス制御、詳細な監査機能など、ダーク サイトのセキュリティとコンプライアンスの要件が導入によって満たされることを保証します。
- ヘルプとサポート: NetApp は、各アカウントに割り当てられた専任のKeystoneサクセス マネージャーが支援とトラブルシューティングを担当し、24 時間 365 日のグローバル サポートを提供します。



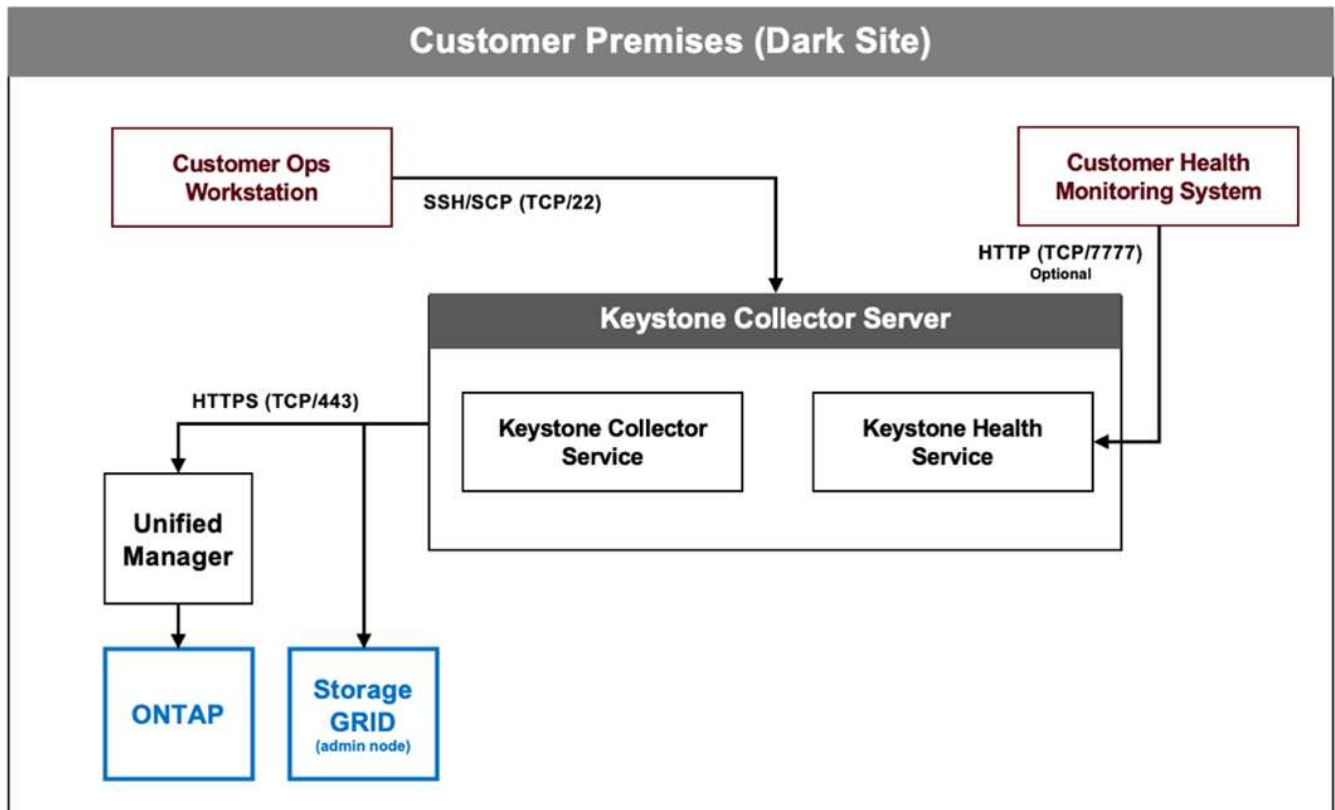
Keystone Collector は、接続制限なしで構成できます。これは、標準 モードとも呼ばれます。詳細については、"[Keystone Collectorについて学ぶ](#)"。

プライベートモードのKeystone Collector

Keystone Collector は、ストレージ システムから使用状況データを定期的に収集し、そのメトリックをオフライン使用状況レポーターとローカル ファイル ストアにエクスポートする役割を担います。生成されたファイルは、暗号化形式とプレーン テキスト形式の両方で作成され、検証チェック後にユーザーが手動でNetAppに転送します。受信すると、NetApp のKeystone課金プラットフォームがこれらのファイルを認証して処理し、課金およびサブスクリプション管理システムに統合して月額料金を計算します。



サーバー上のKeystone Collector サービスは、使用状況データを定期的に収集し、この情報を処理し、サーバー上でローカルに使用状況ファイルを生成する役割を担っています。ヘルス サービスはシステムのヘルス チェックを実行し、顧客が使用するヘルス モニタリング システムとインターフェイスするように設計されています。これらのレポートはユーザーがオフラインでアクセスできるため、検証が可能になり、問題のトラブルシューティングに役立ちます。



プライベートモードでの**Keystone Collector**のインストールの準備

インターネットにアクセスできない環境 (ダーク サイト または プライベート モード と呼ばれます) にKeystone Collector をインストールする前に、システムに必要なソフトウェアが用意されており、必要な前提条件をすべて満たしていることを確認してください。

VMware vSphere の要件

- オペレーティング システム: VMware vCenter Server および ESXi 8.0 以降
- コア: 1 CPU
- メモリ: 2 GB
- ディスク容量: 20 GB vDisk

Linuxの要件

- オペレーティング システム (いずれかを選択):
 - Red Hat Enterprise Linux (RHEL) 8.6 またはそれ以降の 8.x シリーズ
 - Red Hat Enterprise Linux 9.0 以降のバージョン
 - Debian 12
- コア: 2 CPU
- メモリ: 4 GB
- ディスク容量: 50 GB vDisk
 - 少なくとも2GBの空き容量 `/var/lib/`
 - 少なくとも48GBの空き容量 `/opt/netapp`

同じサーバーに次のサードパーティ パッケージもインストールされている必要があります。リポジトリから利用可能な場合、これらのパッケージは前提条件として自動的にインストールされます。

- RHEL 8.6+ (8.x)
 - Python3 \geq v3.6.8、Python3 \leq v3.9.13
 - ポッドマン
 - ソス
 - yum-utils
 - python3-dnf-プラグインのバージョンロック
- RHEL 9.0以降
 - python3 \geq v3.9.0、python3 \leq v3.9.13
 - ポッドマン
 - ソス
 - yum-utils

- python3-dnf-プラグインのバージョンロック
- Debian v12
 - python3 >= v3.9.0、python3 <= v3.12.0
 - ポッドマン
 - SOSレポート

ネットワーク要件

Keystone Collector のネットワーク要件は次のとおりです。

- API ゲートウェイ機能が有効になっているサーバー上に構成された、Active IQ Unified Manager (Unified Manager) 9.10 以降。
- Unified Manager サーバーは、ポート 443 (HTTPS) 上のKeystone Collector サーバーからアクセスできる必要があります。
- Unified Manager サーバー上のKeystone Collector に対して、アプリケーション ユーザー権限を持つサービス アカウントを設定する必要があります。
- 外部インターネット接続は必要ありません。
- 毎月、Keystone Collector からファイルをエクスポートし、NetAppサポート チームに電子メールで送信します。サポートチームへの連絡方法の詳細については、以下を参照してください。"[Keystoneのサポートを受ける](#)"。

Keystone Collectorをプライベートモードでインストールする

インターネットにアクセスできない環境 (ダーク サイト または プライベート モード と呼ばれる) にKeystone Collector をインストールするには、いくつかの手順を実行します。このタイプのインストールは、安全なサイトに最適です。

要件に応じて、Keystone Collector を VMware vSphere システムにデプロイするか、Linux システムにインストールすることができます。選択したオプションに対応するインストール手順に従います。

VMware vSphere にデプロイ

次の手順を実行します。

1. OVAテンプレートファイルを以下からダウンロードしてください "[NetApp Keystoneウェブポータル](#)"。
2. OVAファイルを使用してKeystoneコレクターを展開する手順については、セクションを参照してください。"[OVAテンプレートのデプロイ](#)"。

Linuxにインストールする

Keystone Collector ソフトウェアは、Linux ディストリビューションに基づいて提供された .deb または .rpm ファイルを使用して Linux サーバーにインストールされます。

Linux サーバーにソフトウェアをインストールするには、次の手順に従います。

1. Keystone Collector インストール ファイルを Linux サーバーにダウンロードまたは転送します。

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

2. サーバー上でターミナルを開き、次のコマンドを実行してインストールを開始します。

- **Debian**パッケージを使用

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

- **RPM**ファイルの使用

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

または

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

3. 入力 `y` パッケージのインストールを要求されたとき。

Keystone Collectorをプライベートモードで設定する

いくつかの構成タスクを完了して、Keystone Collector がインターネットにアクセスできない環境 (ダーク サイト または プライベート モード と呼ばれる) で使用状況データを収集できるようにします。これは、必要なコンポーネントをアクティブ化し、ストレージ環境に関連付ける 1 回限りのアクティビティです。設定が完了すると、Keystone Collector はActive IQ Unified Managerによって管理されるすべてのONTAPクラスターを監視します。



Keystone Collector には、構成および監視アクティビティを実行するためのKeystone Collector 管理ターミナル ユーザー インターフェイス (TUI) ユーティリティが用意されています。Enter キーや矢印キーなどのさまざまなキーボード コントロールを使用して、オプションを選択し、この TUI 内を移動できます。

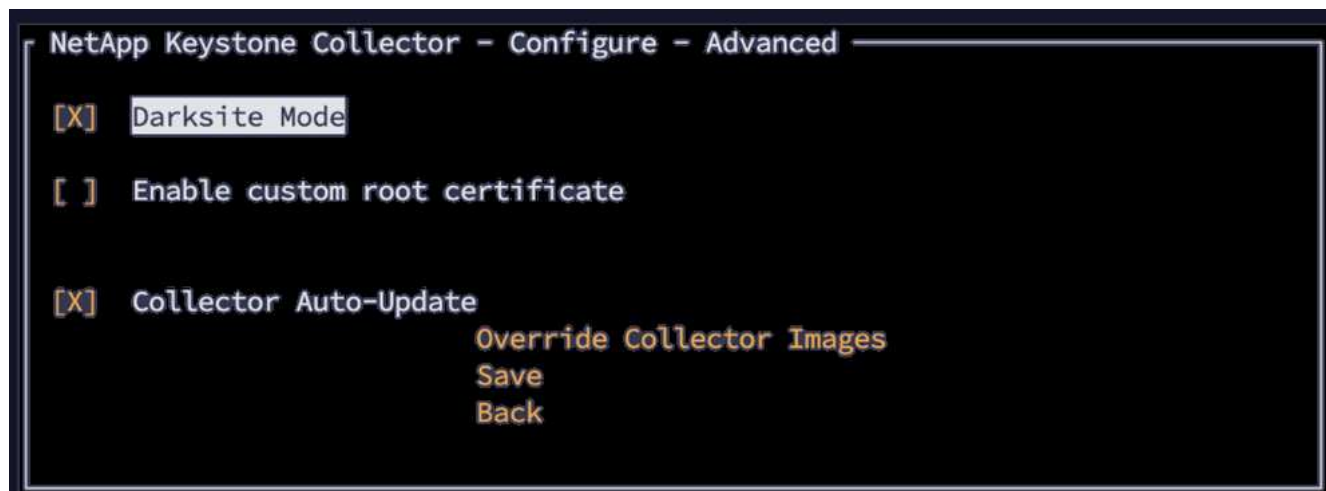
手順

1. Keystone Collector 管理 TUI ユーティリティを起動します。

```
keystone-collector-tui
```

2. ***[構成] > [詳細設定]***に移動します。

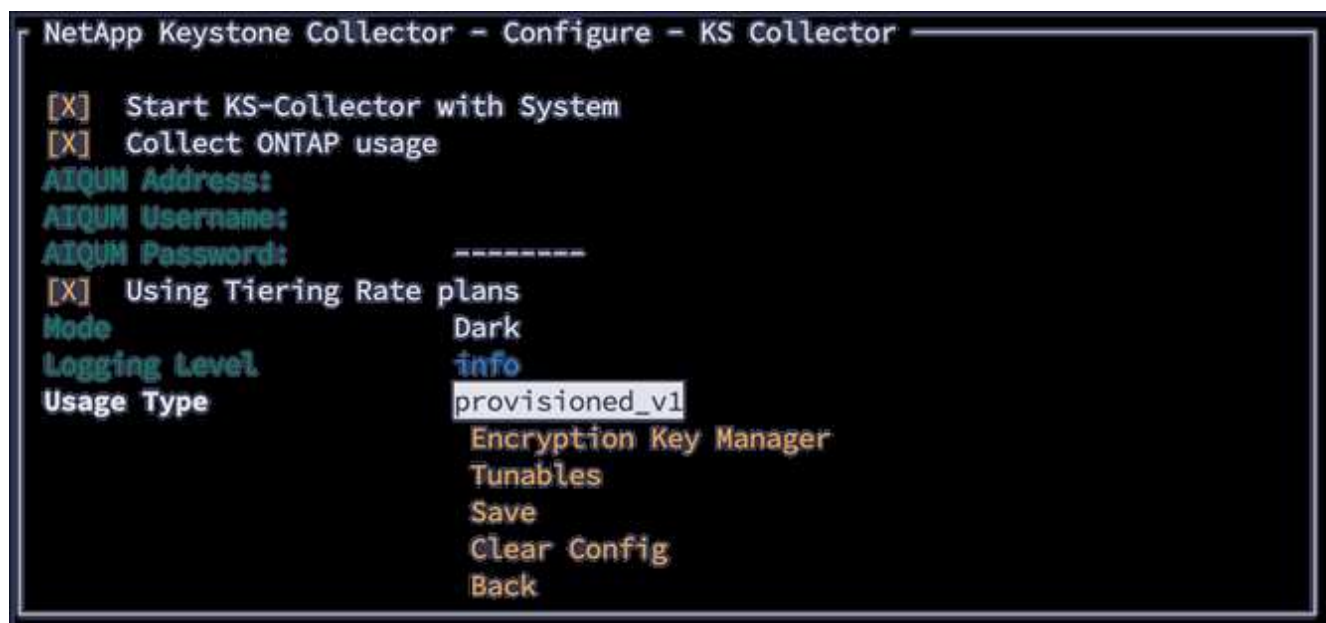
3. ***ダークサイトモード***オプションを切り替えます。



4. *保存*を選択します。
5. Keystone Collector を構成するには、構成 > **KS-Collector** に移動します。
6. システムで **KS** コレクターを起動 フィールドを切り替えます。
7. * ONTAP使用状況の収集* フィールドを切り替えます。 Active IQ Unified Manager (Unified Manager) サーバーとユーザー アカウントの詳細を追加します。
8. オプション: サブスクリプションにデータ階層化が必要な場合は、階層化料金プランの使用 フィールドを切り替えます。
9. 購入したサブスクリプションの種類に基づいて、「使用タイプ」を更新します。



設定する前に、NetAppからのサブスクリプションに関連付けられている使用タイプを確認してください。



10. *保存*を選択します。
11. Keystone Collector キーペアを生成するには、「構成 > KS-Collector」に移動します。
12. *暗号化キーマネージャー*に移動して、Enter キーを押します。

```
NetApp Keystone Collector - Configure - KS Collector

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

13. *コレクターキーペアの生成*を選択し、Enterを押します。

```
NetApp Keystone Collector - Configure - KS Collector - Key Manager

Generate Collector Keypair
Back
```

14. TUI のメイン画面に戻り、サービス ステータス 情報を確認して、Keystone Collector が正常な状態であることを確認します。システムでは、サービスが 全体: 正常 状態にあることが示されるはずです。最大 10 分間待機し、この期間が経過しても全体的なステータスが正常でない場合は、以前の構成手順を確認し、NetAppサポート チームに連絡してください。

```
Service Status
Overall: Healthy
UM-Dark: Running
ks-billing: Running
ks-collector-dark: Running
Recent collector data: Healthy
ONTAP REST response time: Healthy
DB Disk space: Healthy
DB Disk space 30d: Healthy
DB API responses: Healthy
DB Concurrent flushes: Healthy
DB Slow insert rate: Healthy
```

15. ホーム画面で **Exit to Shell** オプションを選択して、Keystone Collector 管理 TUI を終了します。

16. 生成された公開鍵を取得します。

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

17. このファイルを添付した電子メールを、安全な非 USPS サイトの場合は ng-keystone-secure-site-upload@netapp.com に、安全な USPS サイトの場合は ng-keystone-secure-site-usps-upload@netapp.com に送信してください。

使用状況レポートをエクスポートする

毎月末に月次使用状況概要レポートをNetAppに送信する必要があります。このレポートは手動で生成できます。

使用状況レポートを生成するには、次の手順に従います。

1. Keystone Collector TUI ホーム画面で 使用状況のエクスポート に移動します。
2. ファイルを収集し、安全な非 USPS サイトの場合は ng-keystone-secure-site-upload@netapp.com に、安全な USPS サイトの場合は ng-keystone-secure-site-usps-upload@netapp.com に送信します。

Keystone Collector はクリア ファイルと暗号化されたファイルの両方を生成するため、これらのファイルは手動でNetAppに送信する必要があります。クリアファイルレポートには、顧客が検証できる次の詳細が含まれます。

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

<Signature>
31b3d8eb338ee319ef1

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

ONTAPのアップグレード

Keystone Collector は、TUI を介してONTAP のアップグレードをサポートします。

ONTAPをアップグレードするには、次の手順に従います。

1. メンテナンス > **ONTAPアップグレード Web** サーバー に移動します。
2. ONTAPアップグレード イメージ ファイルを `/opt/netapp/ontap-upgrade/` にコピーし、**Start Webserver** を選択して Web サーバを起動します。



3. へ移動 `http://<collector-ip>:8000` アップグレードのサポートには Web ブラウザを使用します。

Keystone Collector を再起動する

TUI を通じて Keystone Collector サービスを再起動できます。TUI で メンテナンス > コレクター サービスの再起動に移動します。これにより、すべてのコレクター サービスが再起動され、TUI ホーム画面からそのステータスを監視できるようになります。



プライベートモードで Keystone Collector の健全性を監視する

HTTP リクエストをサポートする任意の監視システムを使用して、Keystone Collector の健全性を監視できます。

デフォルトでは、Keystoneヘルス サービスは、localhost 以外の IP からの接続を受け入れません。Keystoneヘルスエンドポイントは /uber/health、Keystone Collectorサーバーのすべてのインターフェースのポートでリッスンします 7777。クエリを実行すると、エンドポイントから応答として、Keystone Collector システムのステータスを示す JSON 出力を含む HTTP 要求ステータス コードが返されます。JSON本体は、`is_healthy` 属性はブール値であり、コンポーネントごとの詳細なステータスリストは `component_details` 属性。次に例を示します。

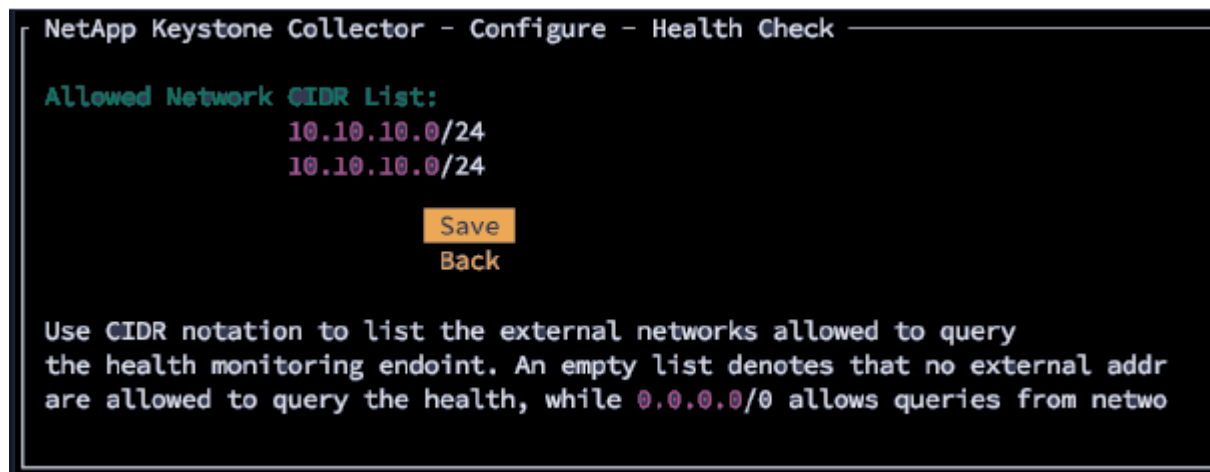
```
$ curl http://127.0.0.1:7777/uber/health
{"is_healthy": true, "component_details": {"vicmet": "Running", "ks-collector": "Running", "ks-billing": "Running", "chronyd": "Running"}}
```

次のステータス コードが返されます。

- **200:** 監視対象のすべてのコンポーネントが正常であることを示します

- **503:** 1つ以上のコンポーネントが正常でないことを示します
- **403:** ヘルス ステータスを照会している HTTP クライアントが、許可されたネットワーク CIDR のリストである *allow* リストに含まれていないことを示します。このステータスの場合、健康情報は返されません。

allow リストは、ネットワーク CIDR 方式を使用して、どのネットワーク デバイスがKeystoneヘルス システムを照会できるかを制御します。403 エラーが発生した場合は、* Keystone Collector 管理 TUI > 構成 > ヘルス モニタリング* から監視システムを *allow* リストに追加します。

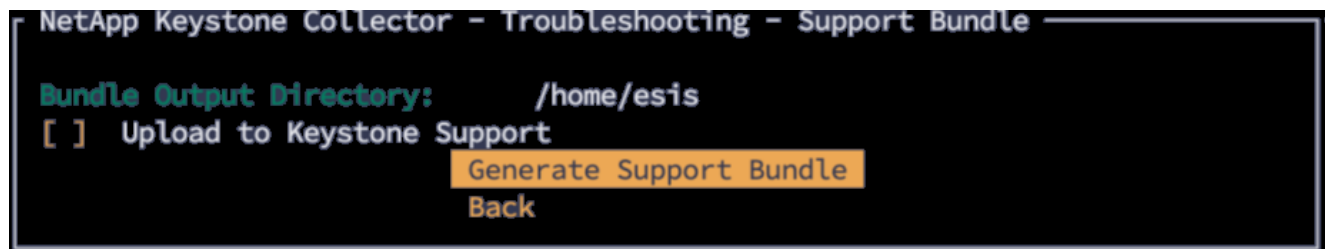


サポートバンドルを生成して収集する

Keystone Collector に関する問題をトラブルシューティングするには、NetAppサポートに問い合わせ、*.tar* ファイルの提供を依頼することができます。このファイルは、Keystone Collector 管理 TUI ユーティリティを通じて生成できます。

.tar ファイルを生成するには、次の手順に従います。

1. トラブルシューティング > サポート バンドルの生成 に移動します。
2. バンドルを保存する場所を選択し、「サポート バンドルの生成」をクリックします。



このプロセスにより、`tar` 上記の場所にあるパッケージは、問題のトラブルシューティングのためにNetAppと共有できます。

3. ファイルをダウンロードしたら、Keystone ServiceNow サポート チケットに添付できます。チケットの発行については、以下を参照してください。"[サービスリクエストの生成](#)"。

著作権に関する情報

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。