Keystone in private mode

Keystone

NetApp
September 12, 2024

Table of Contents

Keystone in private mode

Learn about Keystone (private mode)

Keystone offers a *private* deployment mode, also known as a *dark site*, to meet your business and security requirements. This mode is available for organizations with connectivity restrictions.

NetApp offers a specialized deployment of Keystone STaaS tailored for environments with limited or no internet connectivity (also known as dark sites). These are secure or isolated environments where external communication is restricted due to security, compliance, or operational requirements.

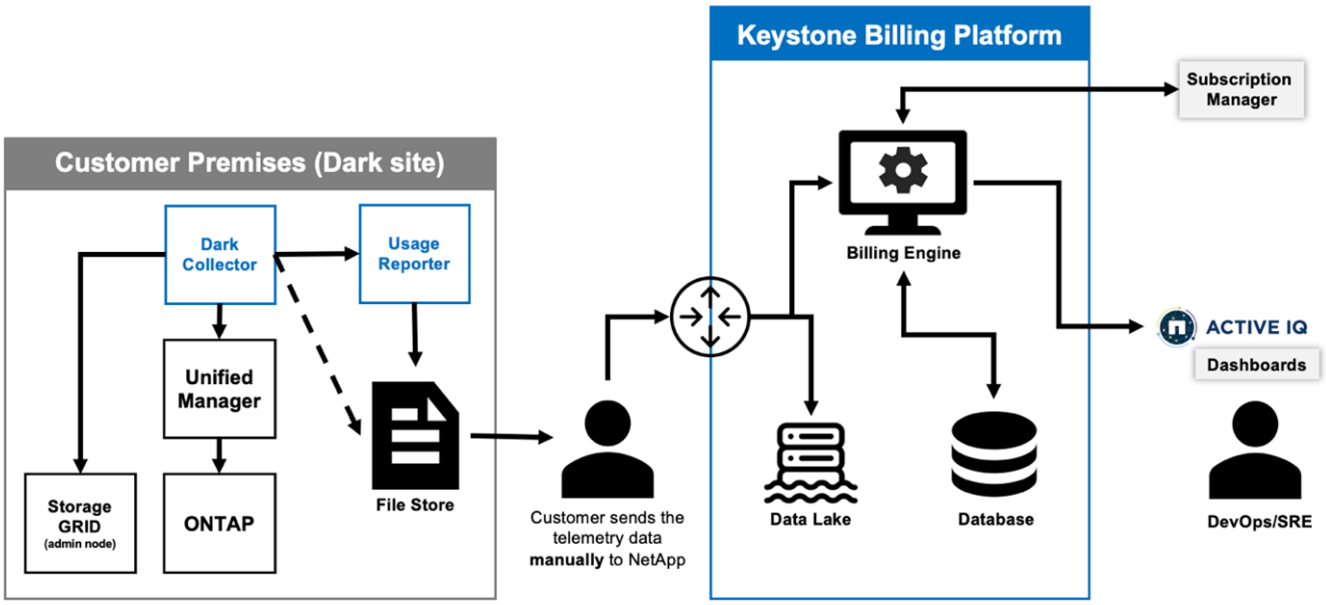
For NetApp Keystone, offering services for dark sites means providing the Keystone flexible storage subscription service in a way that respects the constraints of these environments. This involves:

- **Local deployment**: Keystone can be configured within isolated environments independently, ensuring no need for internet connectivity or external personnel for setup access.
- **Offline operations**: All storage management capabilities with health checks and billing are available offline for operations.
- **Security and compliance**: Keystone ensures that the deployment meets the security and compliance requirements of dark sites, which may include advanced encryption, secure access controls, and detailed auditing capabilities.
- **Help and Support**: NetApp provides 24/7 global support with a dedicated Keystone success manager assigned to each account for assistance and troubleshooting.

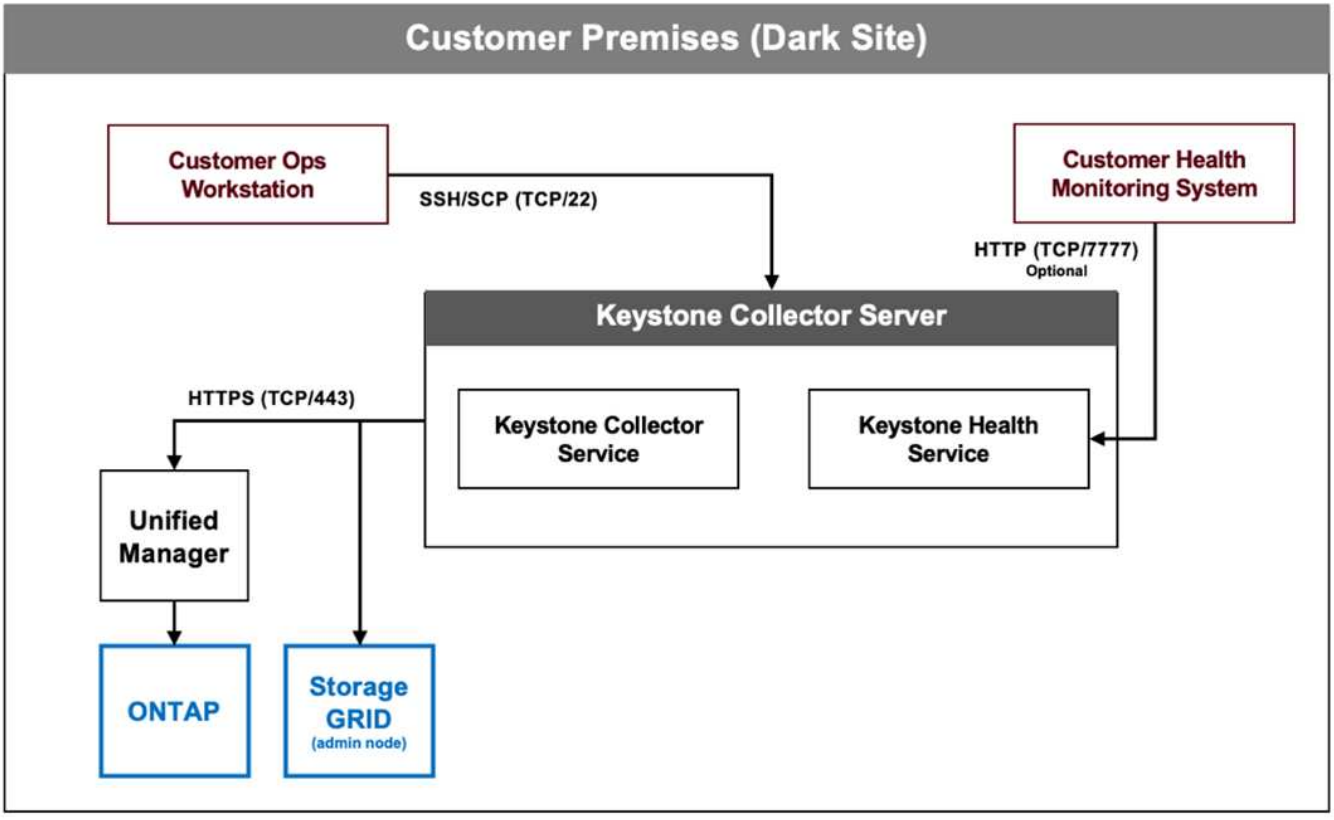
Keystone Collector can be configured without connectivity restrictions, also known as *standard* mode. To learn more, refer to Learn about Keystone Collector.

Keystone Collector in private mode

Keystone Collector is responsible for periodically collecting usage data from storage systems and exporting the metrics to an offline usage reporter and a local file store. The generated files, which are created in both encrypted and plain text formats, are then manually forwarded to NetApp by the user after the validation checks. Upon receipt, NetApp's Keystone billing platform authenticates and processes these files, integrating them into the billing and subscription management systems to calculate the monthly charges.



The Keystone Collector service on the server is tasked with periodically gathering usage data, processing this information, and generating a usage file locally on the server. The health service conducts system health checks and is designed to interface with health monitoring systems used by the customer. These reports are available for offline access by users, allowing for validation and aiding in troubleshooting issues.



Prepare for installation in private mode

Before installing Keystone Collector in an environment without internet access, also

known as a *dark site* or *private mode*, ensure your systems are prepared with the necessary software and meet all required prerequisites.

Requirements for VMware vSphere

- Operating system: VMware vCenter server and ESXi 6.7 or later
- Core: 1 CPU
- RAM: 2 GB
- Disk space: 20 GB vDisk

Requirements for Linux

- Operating system: Debian v12 or Red Hat Enterprise Linux 8.6 or later
- Core: 2 CPU
- RAM: 4 GB
- Disk space: 50 GB vDisk
  - At least 2 GB free in `/var/lib/`
  - At least 48 GB free in `/opt/netapp`

The same server should also have the following third-party packages installed. If available through the repository, these packages will be automatically installed as prerequisites:

- RHEL8
  - python3 >=v3.6.8, python3 <=v3.9.13
  - podman
  - sos
  - yum-utils
  - python3-dnf-plugin-versionlock
- Debian v12
  - python3 >= v3.9.0, python3 <= v3.12.0
  - podman
  - sosreport

Networking requirements

The networking requirements for Keystone Collector include the following:

- Active IQ Unified Manager (Unified Manager) 9.10 or later, configured on a sever with the API Gateway functionality enabled.
- The Unified Manager server should be accessible by the Keystone Collector server on port 443 (HTTPS).
- A service account with Application User permissions should be set up for the Keystone Collector on the Unified Manager server.
- External internet connectivity is not required.

- Each month, export a file from Keystone Collector and email it to the NetApp support team. For more information on how to contact the support team, refer to Get help with Keystone.

Install Keystone Collector in private mode

Complete a few steps to install Keystone Collector in an environment that does not have internet access, also known as a *dark site* or *private mode*. This type of installation is perfect for your secure sites.

You can either deploy Keystone Collector on VMware vSphere systems or install it on Linux systems, depending on your requirements. Follow the installation steps that correspond to your selected option.

Deploy on VMware vSphere

Follow these steps:

1. Download the OVA template file from NetApp Keystone web portal.
2. For steps to deploy Keystone collector with OVA file, refer to the section Deploying the OVA template.

Install on Linux

Keystone Collector software is installed on the Linux server using the provided .deb or .rpm files, based on the Linux distribution.

Follow these steps to install the software on your Linux server:

1. Download or transfer the Keystone Collector installation file to the Linux server:

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

2. Open a terminal on the server and run the following commands to begin the installation.
   - **Using Debian package**

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

   - **Using RPM file**

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

     or

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

3. Enter `y` when prompted to install the package.

Configure Keystone Collector in private mode

Complete a few configuration tasks to enable Keystone Collector to collect usage data in an environment that does not have internet access, also known as a as a *dark site* or *private mode*. This is a one-time activity to activate and associate the required

components with your storage environment. Once configured, Keystone Collector will monitor all ONTAP clusters managed by Active IQ Unified Manager.

Keystone Collector provides you with the Keystone Collector Management Terminal User Interface (TUI) utility to perform configuration and monitoring activities. You can use various keyboard controls, such as the Enter and arrow keys, to select the options and navigate across this TUI.

Steps

1. Start the Keystone Collector management TUI utility:

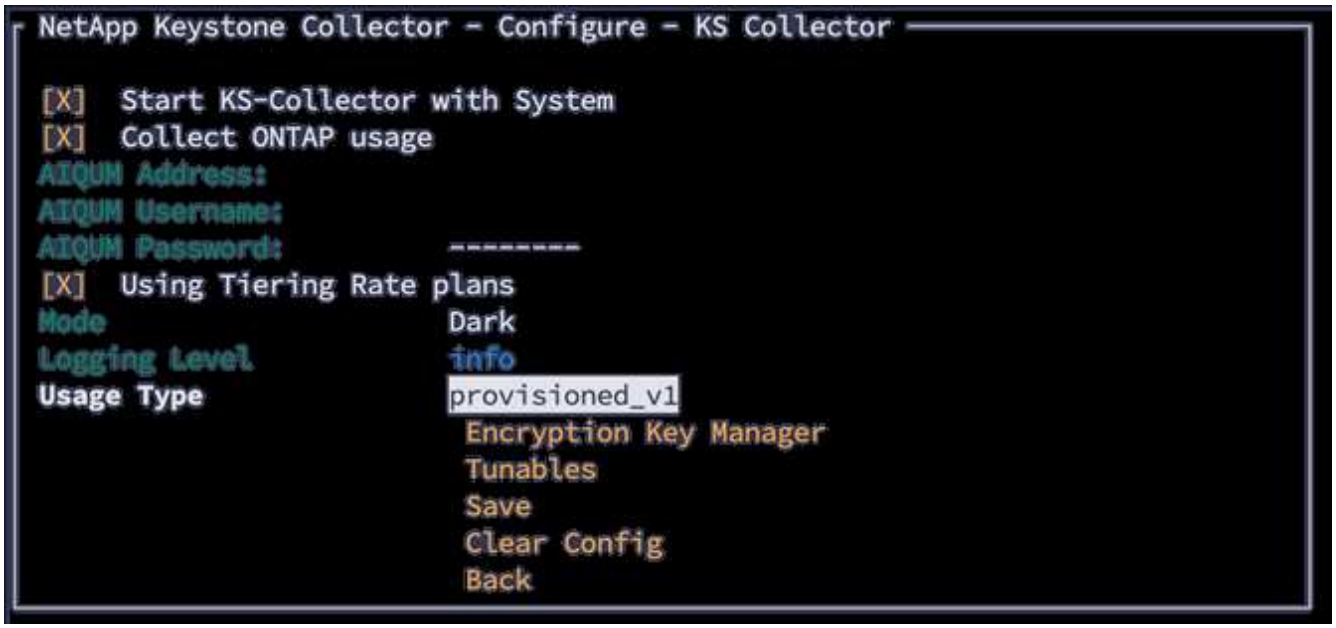
   ```
   keystone-collector-tui
   ```

2. Go to **Configure > Advanced**.
3. Toggle the **Darksite Mode** option.

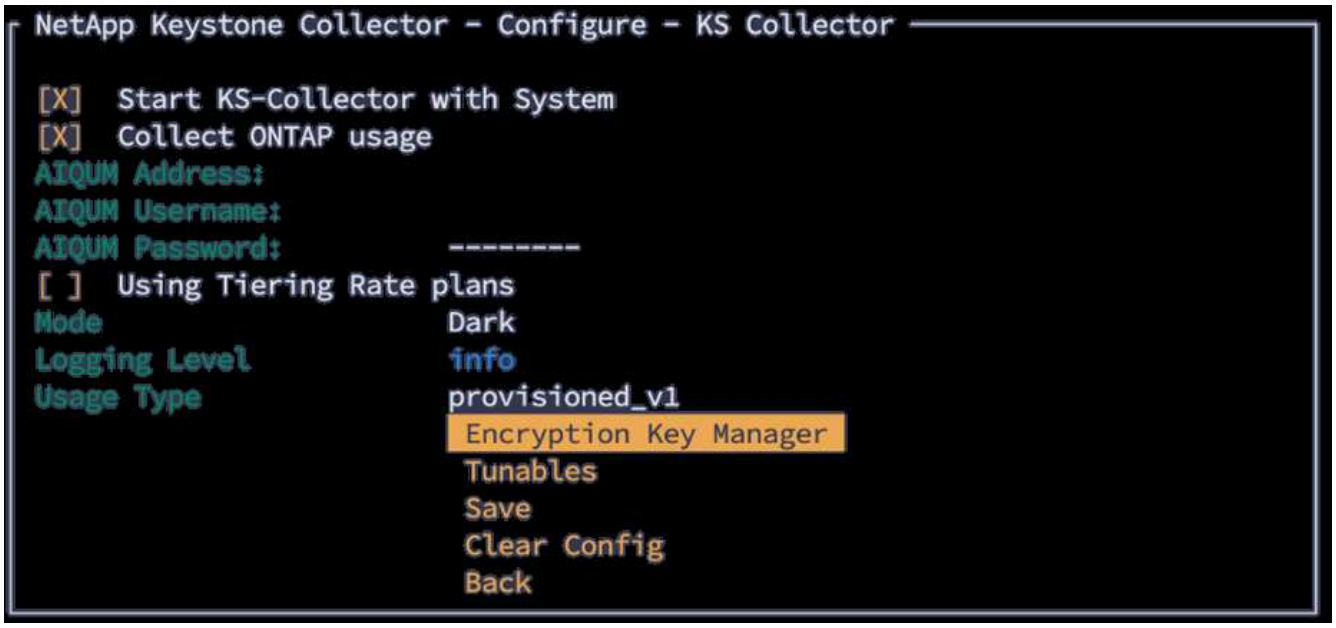
4. Select **Save**.
5. Go to **Configure > KS-Collector** to configure Keystone Collector.
6. Toggle the **Start KS Collector with System** field.
7. Toggle the **Collect ONTAP Usage** field. Add the details of the Active IQ Unified Manager (Unified Manager) server and user account.
8. **Optional**: Toggle the **Using Tiering Rate plans** field if data tiering is required for the subscription.

   Based on the subscription type purchased, update the **Usage Type**.

   Before configuring, confirm the usage type associated with the subscription from NetApp.



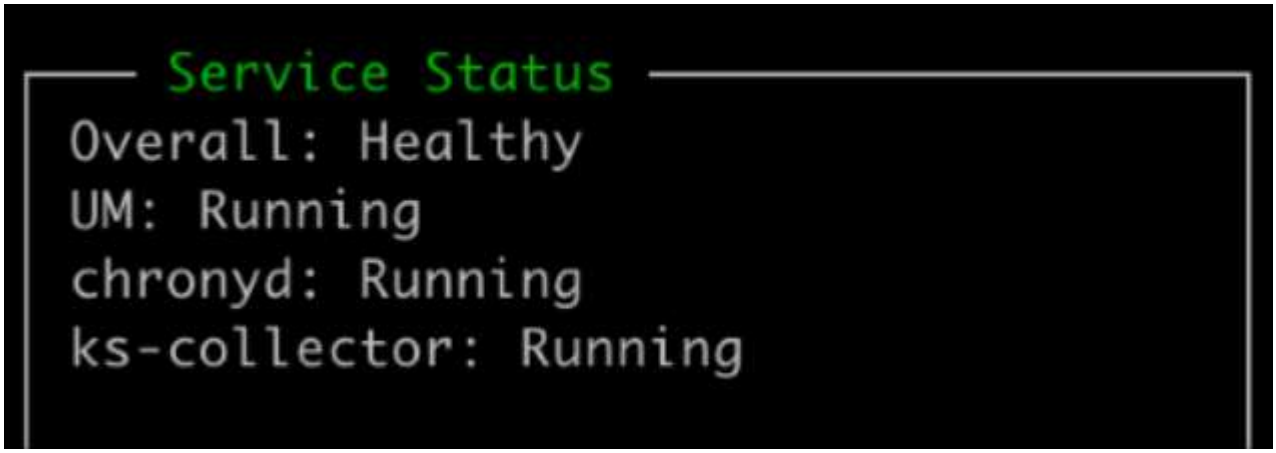
9. Select **Save**.
10. Go to **Configure > KS-Collector** to generate the Keystone Collector keypair.
11. Go to **Encryption Key Manager** and press Enter.



12. Select **Generate Collector Keypair** and press Enter.

13. Ensure that the Keystone Collector is in a healthy state by returning to the main screen of the TUI and verifying the **Service Status** information. The system should show that the services are in an **Overall: Healthy** status. Wait up to 10 minutes, if the overall status remains unhealthy after this period, review the

previous configuration steps and contact the NetApp support team.



14. Exit the Keystone Collector management TUI by selecting **Exit to Shell** option on the home screen.
15. Retrieve the generated public key:

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

16. Send an email with this file to keystone.services@netapp.com.

Export usage report

You should send the monthly usage summary report to NetApp at the end of every month. You can generate this report manually.

Follow these steps to generate the usage report:

1. Go to to **Export Usage** on the Keystone Collector TUI home screen.
2. Collect the files and send them to keystone.services@netapp.com.

   Keystone Collector generates both a clear file and an encrypted file, which should be manually sent to NetApp. The clear file report contains the following details that can be validated by the customer.

```
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 supports ONTAP upgrades through TUI.

Follow these steps to upgrade ONTAP:

1. Go to **Maintenance > ONTAP Upgrade Webserver**.
2. Copy the ONTAP upgrade image file to **/opt/netapp/ontap-upgrade/**, then select **Start Webserver** to start the web server.

3. Go to http://<collector-ip>:8000 using a web browser for upgrade assistance.

Restart Keystone Collector

You can restart the Keystone Collector service through the TUI. Go to **Maintenance > Restart Collector** Services in the TUI. This will reboot all collector services, and their status can be monitored from the TUI home screen.

Monitor Keystone Collector health in private mode

You can monitor the health of Keystone Collector by using any monitoring system that supports HTTP requests.

By default, Keystone health services do not accept connections from any IP other than localhost. The Keystone health endpoint is `/uber/health`, and it listens on all interfaces of the Keystone Collector server on port `7777`. On query, an HTTP request status code with a JSON output is returned from the endpoint as a response, describing the status of the Keystone Collector system.
The JSON body provides an overall health status for the `is_healthy` attribute, which is a boolean; and a detailed list of statuses per-component for the `component_details` attribute.

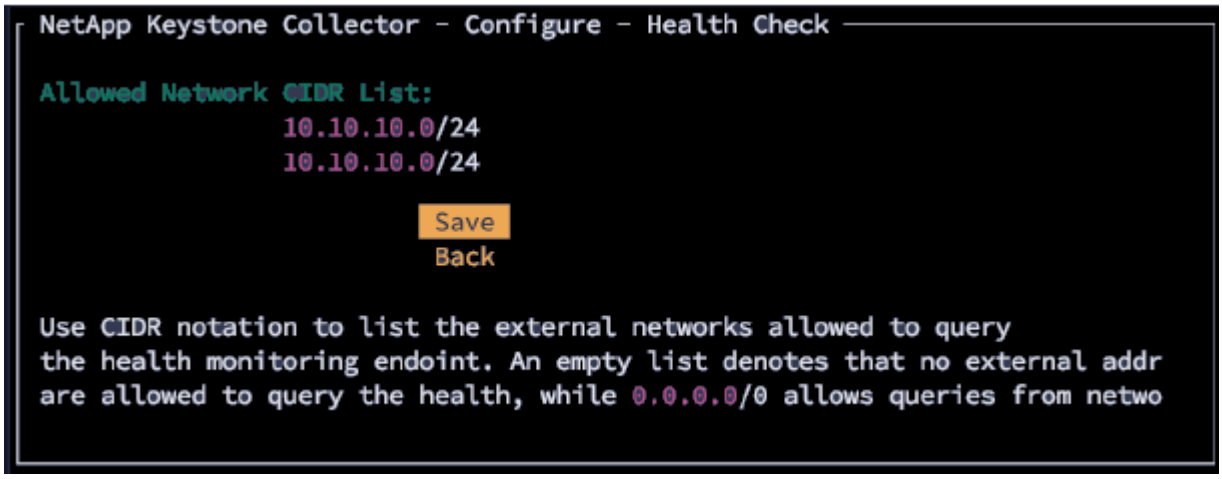
Here is an example:

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

These status codes are returned:

- **200**: indicates that all monitored components are healthy
- **503**: indicates that one or more components are unhealthy
- **403**: indicates that the HTTP client querying the health status is not on the *allow* list, which is a list of allowed network CIDRs. For this status, no health information is returned.

  The *allow* list uses the network CIDR method to control which network devices are allowed to query the Keystone health system. If you receive the 403 error, add your monitoring system to the *allow* list from **Keystone Collector management TUI > Configure > Health Monitoring**.

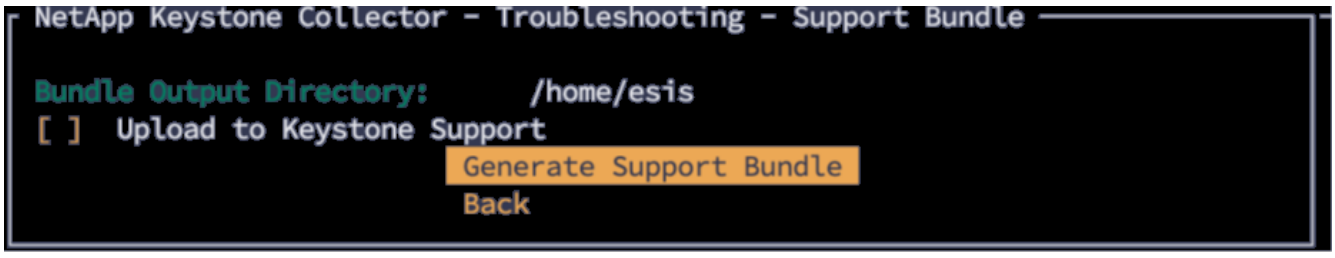


Generate and collect support bundles

To troubleshoot issues with Keystone Collector, you can work with NetApp Support who might ask for a *.tar* file. You can generate this file through the Keystone Collector management TUI utility.

Follow these steps to generate a *.tar* file:

1. Go to **Troubleshooting > Generate Support Bundle**.
2. Select the location to save the bundle, then click **Generate Support Bundle**.



This process creates a `tar` package at the mentioned location which can be shared with NetApp for troubleshooting issues.

3. When the file is downloaded, you can attach it to the Keystone ServiceNow support ticket. For information about raising tickets, see Generating service requests.

Copyright information

Trademark information