



# Keystone documentation

## Keystone

NetApp  
August 29, 2025

This PDF was generated from <https://docs.netapp.com/us-en/keystone-staas/index.html> on August 29, 2025. Always check [docs.netapp.com](https://docs.netapp.com) for the latest.

# Table of Contents

Keystone documentation	1
Release notes	2
What's new in Keystone STaaS	2
28 August 2025	2
05 August 2025	2
30 June 2025	2
19 June 2025	2
08 January 2025	3
12 December 2024	3
21 November 2024	3
11 November 2024	4
10 July 2024	4
27 June 2024	4
29 May 2024	4
09 May 2024	5
28 March 2024	5
29 February 2024	6
13 February 2024	6
11 January 2024	7
15 December 2023	7
Fixed issues in Keystone STaaS	7
Known issues in Keystone STaaS	11
Known limitations in Keystone STaaS	12
Keystone Collector limitations	12
Get started	14
Learn about NetApp Keystone	14
Keystone Storage-as-a-service (STaaS)	14
Keystone infrastructure	15
Storage platforms	15
Monitoring tools	15
Learn about Keystone Collector	16
Components required for deployment	17
Site requirements	17
Remote access requirement	18
Keystone data flow	19
Keystone Collector data flow	19
Monitoring data flows	20
Compliance standards	20
Operational models in Keystone	20
Roles and responsibilities across the service lifecycle	21
Set up and configure Keystone	23
Requirements	23
Virtual infrastructure requirements	23

Linux system requirements . . . . .	25
Requirements for ONTAP and StorageGRID . . . . .	27
Install Keystone Collector . . . . .	30
Deploy Keystone Collector on VMware vSphere systems . . . . .	30
Install Keystone Collector on Linux systems . . . . .	32
Automatic validation of Keystone software . . . . .	34
Configure Keystone Collector . . . . .	34
Configure HTTP Proxy on Keystone Collector . . . . .	36
Limit collection of private data . . . . .	36
Trust a custom root CA . . . . .	37
Create Performance Service Levels . . . . .	38
Install ITOM Collector . . . . .	41
Installation requirements for ITOM Collector . . . . .	42
Install ITOM Collector on Linux systems . . . . .	43
Install ITOM Collector on Windows systems . . . . .	44
Configure AutoSupport for Keystone . . . . .	45
Monitor and upgrade . . . . .	46
Monitor the health of Keystone Collector . . . . .	46
Manually upgrade Keystone Collector . . . . .	51
Keystone Collector security . . . . .	53
Security hardening . . . . .	53
Types of user data that Keystone collects . . . . .	54
ONTAP data collection . . . . .	54
StorageGRID data collection . . . . .	60
Telemetry data collection . . . . .	61
Keystone in private mode . . . . .	62
Learn about Keystone (private mode) . . . . .	62
Prepare for installation in private mode . . . . .	64
Install Keystone Collector in private mode . . . . .	65
Configure Keystone Collector in private mode . . . . .	66
Monitor Keystone Collector health in private mode . . . . .	70
Manage and monitor Keystone subscriptions . . . . .	72
Understand the Keystone dashboard . . . . .	72
Learn about the Keystone dashboard . . . . .	72
Get started with the Keystone dashboard . . . . .	73
Keystone dashboard in BlueXP . . . . .	75
Keystone dashboard in Digital Advisor . . . . .	76
Search Keystone data, generate reports, and view alerts . . . . .	78
View subscription insights . . . . .	79
View details about your Keystone subscriptions . . . . .	80
View the current consumption of your Keystone subscriptions . . . . .	84
View consumption trends of your Keystone subscriptions . . . . .	87
View the timeline of your Keystone subscriptions . . . . .	93
View assets . . . . .	94
View assets associated with a Keystone subscription . . . . .	94

View assets across multiple Keystone subscriptions	100
Modify your Keystone subscription from BlueXP	103
View service requests for Keystone subscriptions	105
View details about ONTAP volumes and object storage	106
View ONTAP volumes and object storage details	106
View performance metrics	109
IOPS	109
Throughput	110
Latency (ms)	110
Logical Used (TiB)	111
Concepts	113
Keystone STaaS services	113
Metrics and definitions used in Keystone	113
Supported storage in Keystone	114
Supported storage capacities in Keystone	115
Performance service levels in Keystone	116
Capacity requirements for performance service levels	119
Add-on services	123
Burst capacity options	123
Learn about Data Infrastructure Insights	123
Learn about data tiering	126
Non-returnable, non-volatile components, and SnapLock compliance	127
Learn about USPS	128
Keystone STaaS SLO	128
Availability SLO	128
Performance SLO	131
Sustainability SLO	133
Ransomware Recovery Guarantee	135
Billing	135
Keystone pricing	135
Billing based on committed capacity	136
Metering based on consumed capacity	136
Billing based on burst consumption	136
Miscellaneous scenarios for Keystone billing	137
Billing schedules	138
Access Keystone from Digital Advisor REST API	139
Get started using the Digital Advisor REST API to retrieve Keystone data	139
Generate refresh and access tokens	139
Generate access token using the Digital Advisor REST API	140
Execute the API call	141
Get a list of all customers using the Digital Advisor REST API	141
Get customer subscriptions using the Digital Advisor REST API	142
Get customer consumption details using the Digital Advisor REST API	143
Get the historical consumption details for a customer	145
Keystone subscription services   Version 1	148



Get help with Keystone ..... 149

    NetApp Keystone support ..... 149

    Additional information..... 149

    Keystone support monitoring ..... 149

    Generating service requests ..... 149

Legal notices ..... 151

    Copyright ..... 151

    Trademarks ..... 151

    Patents ..... 151

    Privacy policy ..... 151

# Keystone documentation

# Release notes

## What's new in Keystone STaaS

Learn about the latest features and enhancements in Keystone STaaS services.

### 28 August 2025

#### Enhanced logical usage tracking with a new column

A new column, Total footprint, is added to enhance Keystone consumption tracking for FabricPool volumes:

- **Keystone dashboard in BlueXP:** You can see the **Total footprint** column in the **Volumes in clusters** tab within the **Assets** tab.
- **Digital Advisor:** You can see the **Total Footprint** column in the **Volume Details** tab within the **Volumes & Objects** tab.

This column displays the total logical footprint for volumes using FabricPool tiering, including data from both performance and cold tiers, so you can accurately calculate Keystone consumption.

### 05 August 2025

#### View instance-level consumption data

You can view current consumption and historical data for each performance service level instance through the Keystone dashboard in BlueXP. This feature is available for performance service levels with multiple instances, provided you have a Keystone version 3 (v3) subscription. To learn more, refer to [View the consumption of your Keystone subscriptions](#).

### 30 June 2025

#### Keystone version 3 (v3) release

You can now subscribe to Keystone version 3 (v3), the latest release of the NetApp Keystone STaaS offering. This version introduces several enhancements, including simplified performance service levels, additional burst capacity options, and flexible billing frequencies. These improvements simplify the management, optimization, and scaling of storage solutions. To learn more, refer to [Keystone STaaS services for v3](#).

You can contact the Keystone support team to subscribe to Keystone version 3 (v3). For more details, refer to [Get help with Keystone](#).

### 19 June 2025

#### Keystone dashboard in BlueXP

You can now access the Keystone dashboard directly from BlueXP. This integration gives you a single place to monitor, manage, and keep track of all your Keystone subscriptions along with your other NetApp services.

With the Keystone dashboard in BlueXP, you can:

- View all your subscription details, capacity usage, and assets in one place.

- Easily manage subscriptions and request changes as your needs evolve.
- Stay up to date with the latest information for your storage environment.

To get started, go to **Storage > Keystone** in the BlueXP left navigation menu. To learn more, refer to [Keystone dashboard overview](#).

## 08 January 2025

### Addition of daily accrued data usage viewing options

You can now view daily accrued burst data usage in either graph or table format for a monthly or quarterly billing period by clicking the bar that displays the invoiced data. To learn more, refer to [View daily accrued burst data usage](#).

## 12 December 2024

### Renamed Logical Used column

The **Logical Used** column in the **Volume Details** tab within **Volumes & Objects** is now renamed to **Keystone Logical Used**.

### Enhanced Assets tab

The **Assets** tab in the **Keystone Subscriptions** screen now has two new sub-tabs: **ONTAP** and **StorageGRID**. These sub-tabs offer detailed cluster-level insights for ONTAP and grid-level information for StorageGRID based on your subscriptions. To learn more, refer to [Assets tab](#).

### New Hide/Show Columns option

The **Volume Details** tab within **Volumes & Objects** now includes a **Hide/Show Columns** option. This option enables you to select or deselect columns to customize the tabular listing of volumes according to your preference. To learn more, refer to [Volumes & Objects tab](#).

## 21 November 2024

### Enhanced invoiced accrued burst

You can now view accrued burst usage data on a quarterly basis through the **Invoiced Accrued Burst** option if you have opted for a quarterly billing period. To learn more, refer to [View invoiced accrued burst](#).

### New columns in the Volumes Details tab

To improve clarity in calculating logical usage, two new columns have been added to the **Volume Details** tab within the **Volumes & Objects** tab:

- **Logical AFS:** Displays the logical capacity used by the volume's active file system.
- **Physical Snapshot:** Displays the physical space used by the snapshots.

These columns provide better clarity on the **Logical Used** column, which shows the combined logical capacity used by the volume's active file system and the physical space used by snapshots.

## 11 November 2024

### Enhanced report generation

You can now generate a consolidated report to view the details of your Keystone data using the Report feature in Digital Advisor. To learn more, refer to [Generate consolidated report](#).

## 10 July 2024

### Label modifications

The label **Current Usage** is changed to **Current Consumption**, and **Capacity Trend** is changed to **Consumption Trend**.

### Search bar for subscriptions

The **Subscriptions** dropdown across all tabs within the **Keystone Subscriptions** screen now includes a search bar. You can search for specific subscriptions listed in the **Subscriptions** dropdown.

## 27 June 2024

### Consistent display of subscription

The **Keystone Subscriptions** screen is updated to display the selected subscription number across all tabs.

- When any tab within the **Keystone Subscriptions** screen is refreshed, the screen automatically navigates to the **Subscriptions** tab and reset all tabs to the first subscription listed in the **Subscription** dropdown.
- If the selected subscription is not subscribed to performance metrics, the **Performance** tab will display the first subscription listed in the **Subscription** dropdown upon navigation.

## 29 May 2024

### Enhanced Burst indicator

The **Burst** indicator in the usage graph index is enhanced to display the burst limit percentage value. This value changes depending on the agreed-upon burst limit for a subscription. You can also view the burst limit value in the **Subscriptions** tab by hovering over the **Burst Usage** indicator in the **Usage Status** column.

### Addition of service levels

The service levels **CVO Primary** and **CVO Secondary** are included to support Cloud Volumes ONTAP for subscriptions that has rate plans with zero committed capacity or those configured with a metro cluster.

- You can view the capacity usage graph for these service levels from old dashboard of the **Keystone Subscriptions** widget and the **Capacity Trend** tab, and also detailed usage information from the **Current Usage** tab.
- In the **Subscriptions** tab, these service levels are displayed as CVO (v2) in the **Usage Type** column, allowing for the identification of billing according to these service levels.

### Zoom-in feature for short-term bursts

The **Capacity Trend** tab now includes a zoom-in feature to view the details of short-term bursts in the usage

charts. For more information, see [Capacity Trend tab](#).

### Enhanced display of subscriptions

The default display of subscriptions is enhanced to sort by tracking ID. The subscriptions in the **Subscriptions** tab, including in the **Subscription** dropdown and CSV reports, will now be displayed based on the alphabetical sequence of the tracking IDs, following the order of a, A, b, B, and so on.

### Enhanced accrued burst display

The tooltip that appears when hovering over the capacity usage bar chart in the **Capacity Trend** tab now displays the type of accrued burst based on committed capacity. It differentiates between provisional and invoiced accrued burst, showing **Provisional Accrued Consumption** and **Invoiced Accrued Consumption** for subscriptions with zero committed capacity rate plans, and **Provisional Accrued Burst** and **Invoiced Accrued Burst** for those with non-zero committed capacity.

## 09 May 2024

### New columns in CSV reports

The CSV reports from the **Capacity Trend** tab now include **Subscription Number** and **Account Name** columns for improved detail.

### Enhanced Usage Type column

The **Usage Type** column within the **Subscriptions** tab is enhanced to display logical and physical usages as comma-separated values for subscriptions that cover service levels for both file and object.

### Access object storage details from Volume Details tab

The **Volume Details** tab within the **Volumes & Objects** tab now provides object storage details along with volume information for subscriptions that include service levels for both file and object. You can click the **Object Storage Details** button within the **Volume Details** tab to view the details.

## 28 March 2024

### Improvement to QoS policy compliance display in the Volume Details tab

The **Volume Details** tab within the **Volumes & Objects** tab now provides better visibility into Quality of Service (QoS) policy compliance. The column formerly known as **AQoS** is renamed to **Compliant**, which indicates whether the QoS policy is in compliance. In addition, a new column **QoS Policy Type** is added, which specifies if the policy is fixed or adaptive. If neither applies, the column displays *Not Available*. For more information, see [Volumes & Objects tab](#).

### New column and simplified subscription display in the Volume Summary tab

- The **Volume Summary** tab within the **Volumes & Objects** tab now includes a new column titled **Protected**. This column provides a count of the protected volumes associated with your subscribed service levels. If you click the number of protected volumes, it takes you to the **Volume Details** tab, where you can view a filtered list of protected volumes.
- The **Volume Summary** tab is updated to display only base subscriptions, excluding add-on services. For more information, see [Volumes & Objects tab](#).

## Change to accrued burst detail display in the Capacity Trend tab

The tooltip that appears when hovering over the capacity usage bar chart in the **Capacity Trend** tab will display the details of accrued bursts for the current month. The details will not be available for the previous months.

## Enhanced access to view historical data for Keystone subscriptions

You can now view historical data if a Keystone subscription is modified or renewed. You can set the start date of a subscription to a previous date to view :

- Consumption and accrued burst usage data from the **Capacity Trend** tab.
- Performance metrics of ONTAP volumes from the **Performance** tab.

The data is displayed based on the selected start date of the subscription.

## 29 February 2024

### Addition of the Assets tab

The **Keystone Subscriptions** screen now includes the **Assets** tab. This new tab provides cluster-level information based on your subscriptions. For more information, see [Assets tab](#).

### Improvements to the Volumes & Objects tab

To provide better clarity to your ONTAP system volumes, two new tab buttons, **Volume Summary** and **Volume Details**, have been added to the **Volumes** tab. The **Volume Summary** tab provides an overall count of the volumes associated with your subscribed service levels, including their AQoS compliance status and capacity information. The **Volume Details** tab lists all the volumes and their specifics. For more information, see [Volumes & Objects tab](#).

### Enhanced search experience on Digital Advisor

The search parameters on the **Digital Advisor** screen now include Keystone subscription numbers and watchlists created for Keystone subscriptions. You can enter the first three characters of a subscription number or watchlist name. For more information, see [View the Keystone dashboard on Active IQ Digital Advisor](#).

### View timestamp of the consumption data

You can view the timestamp of the consumption data (in UTC) on the old dashboard of the **Keystone Subscriptions** widget.

## 13 February 2024

### Ability to view subscriptions linked to a primary subscription

Some of your primary subscriptions can have linked, secondary subscriptions. If that is the case, the primary subscription number will continue to be displayed in the **Subscription Number** column, while the linked subscription numbers will be listed in a new column **Linked Subscriptions** on the **Subscriptions** tab. The **Linked Subscriptions** column becomes available to you only if you have linked subscriptions, and you can see information messages notifying you about them.

# 11 January 2024

## Invoiced data returned for accrued burst

The labels for **Accrued Burst** are now modified to **Invoiced Accrued Burst** in the **Capacity Trend** tab. Selecting this option enables you to view the the monthly charts for the billed accrued burst data. For more information, see [View invoiced accrued burst](#).

## Accrued consumption details for specific rate plans

If you have a subscription that has rate plans with **zero** committed capacity, you can view the accrued consumption details in the **Capacity Trend** tab. On selecting the **Invoiced Accrued Consumption** option, you can view the the monthly charts for the billed accrued consumption data.

# 15 December 2023

## Ability to search by watchlists

The support for watchlists in Digital Advisor has been extended to include Keystone systems. You can now view the details of the subscriptions for multiple customers by searching with watchlists. For more information about the use of watchlists in Keystone STaaS, see [Search by Keystone watchlists](#).

## Date converted to UTC timezone

The data returned on the tabs of the **Keystone Subscriptions** screen of Digital Advisor is displayed in UTC time (server timezone). When you enter a date for query, it is automatically considered to be in UTC time. For more information, see [Keystone Subscription dashboard and reporting](#).

# Fixed issues in Keystone STaaS

Issues that were found in previous releases of NetApp Keystone STaaS services have been fixed in later releases.

Issue description	After the fix	Fixed in release
Missing burst threshold line from consumption trend charts for subscriptions configured with a MetroCluster configuration in the Digital Advisor dashboard, showing an incorrect <b>Above Burst Limit</b> status.	Fixed	August 28, 2025
In the <b>Assets</b> tab, assets for StorageGRID are not visible.	Fixed	June 19, 2025
For the Advance Data-Protect service level, in the <b>Consumption Trend</b> tab, the chart shows a split for primary and mirror sites.	The chart no longer shows a split for primary and mirror sites.	June 19, 2025



Issue description	After the fix	Fixed in release
When the existing Keystone Collector installed using a Debian package attempts to configure an HTTP Proxy or enable Unified Manager through the Keystone Collector management TUI, the TUI becomes unresponsive.	Fixed	May 19, 2025
Keystone Collector for StorageGRID fails to configure correctly due to missing common settings.	Fixed	May 12, 2025
Keystone Collector fails to collect usage data for ONTAP clusters running versions lower than 9.11.	Fixed	April 30, 2025
The consumption values for linked subscriptions show incorrect negative numbers, causing the total committed usage to display inaccurately high.	Fixed	April 14, 2025
Unable to view historical data in the <b>Consumption Trend</b> tab for service levels for a few subscriptions.	Fixed	April 14, 2025
Missing <b>Keystone Subscriptions</b> option from <b>Watchlist</b> and the <b>Subscription Number</b> option from <b>Reports</b> on the Digital Advisor dashboard.	Fixed	March 19, 2025
Missing a few Keystone subscriptions from <b>Watchlist</b> after creating or modifying watchlist from the Digital Advisor dashboard.	Fixed	March 19, 2025
Unable to view historical data in the <b>Consumption Trend</b> tab for service levels associated with a subscription that has expired and been renewed with the same tracking ID but different service levels.	Fixed	March 19, 2025

Issue description	After the fix	Fixed in release
Unable to generate reports for subscriptions when selecting more than 10-12 subscriptions from the <b>Subscriptions</b> tab on the <b>Keystone Subscriptions</b> page.	Fixed	January 08, 2025
The <b>Volume Summary</b> sub-tab in the <b>Volumes &amp; Objects</b> tab fails to load for StorageGrid subscriptions.	Fixed	November 21, 2024
The <b>From Date</b> field to select the date range displays a future date by default when navigating to the <b>Consumption Trend</b> tab.	Fixed	September 04, 2024
Keystone Collector management TUI becomes unresponsive when setting up AQoS policies.	Fixed	August 07, 2024
Usage charts display data beyond the specified single-day period when the date corresponding to the current day is selected as both the start and end date for the previous month from the <b>Capacity Trend</b> option in the <b>Capacity Trends</b> tab.	Usage charts now correctly display data for the specified single-day period.	June 27, 2024
Historical accrued burst data is not available for <b>CVO Primary</b> and <b>CVO Secondary</b> service levels within the <b>Capacity Trend</b> tab for subscriptions that are not configured with a MetroCluster configuration.	Fixed	June 21, 2024
Incorrect display of object storage consumed value listed on the <b>Volume Details</b> tab for AutoSupport subscriptions.	The consumed value for object storage now displays correctly.	June 21, 2024
Unable to view cluster-level information within the <b>Assets</b> tab for AutoSupport subscriptions that are configured with a MetroCluster configuration.	Fixed	June, 21, 2024

Issue description	After the fix	Fixed in release
Misplacement of Keystone data in CSV reports if the <b>Account Name</b> column in CSV reports, generated from the <b>Capacity Trend</b> tab, includes an account name with a comma ( , ).	Keystone data is correctly aligned in CSV reports.	May 29, 2024
Display the accrued burst usage from the the <b>Capacity Trend</b> tab even if the consumption is below the committed capacity.	Fixed	May 29, 2024
Incorrect tooltip text for the <b>Current Burst</b> index icon in the <b>Capacity Trend</b> tab.	Displays the correct tooltip text <i>"The amount of burst capacity currently being consumed. Note this is for current billing period, not the selected date range."</i>	March 28, 2024
Information on AQoS non-compliant volumes and MetroCluster partners is unavailable for AutoSupport subscriptions if Keystone data is not present for 24 hours.	Fixed	March 28, 2024
Occasional mismatch in the number of AQoS non-compliant volumes listed on the <b>Volume Summary</b> and <b>Volume Details</b> tabs if there are two service levels assigned to a volume that fulfils AQoS compliance for only one service level.	Fixed	March 28, 2024
No information is available on the <b>Assets</b> tab for AutoSupport subscriptions.	Fixed	March 14, 2024
If both MetroCluster and FabricPool were enabled in an environment where rate plans for both tiering and object storage were applicable, the service levels could be incorrectly derived for the mirror volumes (both constituent and FabricPool volumes).	Correct service levels are applied to mirror volumes.	February 29, 2024

Issue description	After the fix	Fixed in release
For some subscriptions having a single service level or rate plan, the AQoS compliance column was missing in the CSV output of the <b>Volumes</b> tab reports.	The compliance column is visible in the reports.	February 29, 2024
In some MetroCluster environments, occasional anomaly was detected in the IOPS density charts in the <b>Performance</b> tab. This happened due to inaccurate mapping of volumes to service levels.	The charts are correctly displayed.	February 29, 2024
The usage indicator for a burst consumption record was being displayed in amber.	The indicator appears in red.	December 13, 2023
The date range and data in the Capacity Trend, Current Usage, and Performance tabs were not converted to UTC timezone.	The date range for query and data in all the tabs are displayed in UTC time (server timezone). The UTC timezone is also displayed against each date field on the tabs.	December 13, 2023
There was a mismatch in the start date and end date between the tabs and the downloaded CSV reports.	Fixed.	December 13, 2023

## Known issues in Keystone STaaS

Known issues identify problems that might prevent you from using Keystone subscription services effectively.

The following known issues are reported in NetApp Keystone STaaS:

Known issue	Description	Workaround
Incorrect invoice due to data mismatch	A mismatch in consumption data for AutoSupport subscriptions leads to the generation of incorrect invoices, causing billing inaccuracies.	None

Known issue	Description	Workaround
Incorrect QoS policy type display	In the <b>Volume Details</b> tab, the <b>QoS Policy Type</b> column displays QoS when no QoS policy is applied, and the Compliant column shows <i>Not set</i> , causing an inconsistency in the displayed QoS policy status.	None
Volume details unavailable for primary and linked subscriptions	The <b>Volume Summary</b> tab shows zero for the total number of volumes, QoS compliance status, protected volumes count, and total consumed capacity for primary and linked secondary subscriptions.	None

## Known limitations in Keystone STaaS

Known limitations identify platforms, devices, or functions that are not supported by Keystone STaaS services or components, or that do not interoperate correctly. Review these limitations carefully.

### Keystone Collector limitations

#### Keystone Collector authentication failure with StorageGRID SSO enabled

Keystone Collector does not support metering when the StorageGRID system has single sign-on (SSO) enabled. The following error message is displayed in the logs:

```
panic: json: cannot unmarshal object into Go struct field AuthResponse.data of type string
```

See Knowledge Base article [Keystone Collector fails to authenticate with StorageGRID in SSO Mode](#) for information and resolution.

#### Keystone Collector cannot start on vSphere 8.0 Update 1

A Keystone Collector virtual machine (VM) with VMware vSphere version 8.0 Update 1 cannot be switched on, and the following error message is displayed:

```
Property 'Gateway' must be configured for the VM to power on.
```

See Knowledge Base article [Keystone Collector fails to start on vSphere 8.0 U1](#) for information and resolution.

#### Support bundle cannot be generated over Kerberos

If the Keystone Collector home directory is mounted over NFSv4 using Kerberos, the support bundle is not generated, and the following error message is displayed:

```
subprocess.CalledProcessError: Command '['sosreport', '--batch', '-q', '--tmp-
```

`dir', '/home/<user>']'` returned non-zero exit status 1.

See Knowledge Base article [Keystone Collector fails to generate support bundle on Kerberized home directory](#) for information and resolution.

### **Keystone Collector cannot communicate with hosts within specific network range**

Keystone Collector is unable to communicate with devices within the 10.88.0.0/16 network range when the `ks-collector` service is running. See Knowledge Base article [Keystone Collector container conflict with customer network](#) for information and resolution.

### **Keystone Collector cannot verify customer root SSL CA certificate**

If SSL/TLS inspection is enabled at the border firewall in an environment to inspect SSL/TLS traffic, Keystone Collector is unable to establish an HTTPS connection, because the customer's root CA certificate is not trusted.

For more information and resolution, see [Trust a custom root CA](#) or Knowledge Base article [Keystone Collector cannot verify Customer Root SSL CA certificate](#).

# Get started

## Learn about NetApp Keystone

NetApp Keystone is a pay-as-you-go, subscription-based service model that provides a seamless hybrid cloud experience for businesses that prefer operational expense consumption models over upfront capital expenditures or leasing to meet their data storage and protection needs.

With Keystone, you benefit from:

- **Cost efficiency:** Pay only for the storage you need with the flexibility to handle extra capacity.
- **Capital efficiency:** Access enterprise-level storage without upfront investments.
- **Scalability:** Easily scale your storage capacity as your business grows.
- **Customization:** Adjust your storage plans and shift to the cloud as needed, optimizing your overall costs.
- **Cloud integration:** Combine on-premises and cloud services under one subscription.
- **Security:** Protect your data with advanced security measures and guaranteed recovery from threats.



### Predictable billing

Provides cloud-like storage operations in a single, pay-as-you-go subscription – purchase only the storage needed plus 20% burst at same rate



### Preserve capital

Unlocks access to enterprise-level storage capabilities without upfront capital investment



### Scale on demand

Quickly scales out capacity for file, block, and object storage as growing needs dictate



### Flexible rates

Offers flexible 1–5-year terms, adjust capacity or shift to the cloud by up to 25% annually, and save up to 50% of storage TCO with automated data tiering



### Bridge to the cloud

Leverages major public cloud services with on-prem services seamlessly, with a single subscription



### Built-in security

Safeguards data with the most secure storage on the planet and guarantees recovery from ransomware attacks

Keystone provides storage capacity at predefined performance service levels for file, block and object storage types. This storage can be deployed on-premises and operated by NetApp, a partner, or the customer. Keystone can be used in association with NetApp cloud services, such as Cloud Volumes ONTAP that can be deployed on a hyperscaler environment of your choice.

## Keystone Storage-as-a-service (STaaS)

Storage-as-a-service (STaaS) offerings aim to deliver a public cloud-like model for the procurement, deployment, and management of storage infrastructure. While many enterprises are still working on their strategy for hybrid cloud, Keystone STaaS offers the flexibility to start with on-premises services and transition to the cloud when the time is right. This ensures that you can protect your commitments across different deployment models, reallocating your spending as needed without increasing your monthly bill.

### Related information

- [Keystone pricing](#)

- [Add-on services in Keystone STaaS](#)
- [Performance service levels in Keystone](#)
- [Keystone infrastructure](#)
- [Operational models in Keystone](#)

## Keystone infrastructure

NetApp is solely responsible for the infrastructure, design, technology choices, and components of Keystone, which applies to both NetApp and customer-operated environments.

NetApp reserves the rights to take the following actions:

- Select, substitute, or repurpose products.
- Refresh products with new technology when deemed appropriate.
- Increase or decrease capacity of the products to meet service requirements.
- Modify architecture, technology, and/or products to meet service requirements.

The Keystone infrastructure includes multiple components, such as the following, among others:

- The Keystone infrastructure, including NetApp storage systems.
- Tools to manage and operate the service such as the ITOM monitoring solution, BlueXP, Active IQ, and Active IQ Unified Manager.

## Storage platforms

Enterprise applications need storage platforms to support fast provisioning workflows, maintain continuous availability, sustain high workloads with low latency, deliver higher performance, and support integration with major cloud providers. NetApp has several products and technologies for supporting these requirements. For Keystone service, NetApp uses ONTAP systems (AFF, ASA, and FAS) and StorageGRID systems.

## Monitoring tools

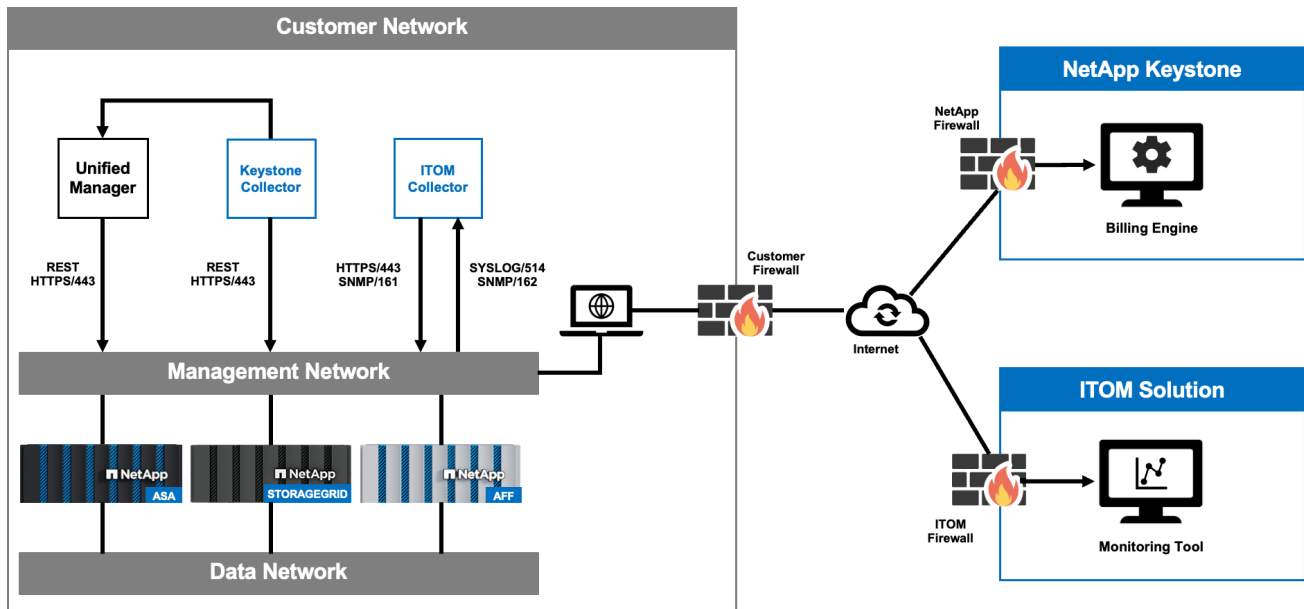
In a Keystone customer-operated service, storage infrastructure and monitoring tools are installed at your site. The storage infrastructure consists of the required storage hardware needed to support your initial order, with the provision to order more storage later.

In addition to the storage equipment, two monitoring tools are provisioned for storage and consumption monitoring.

- **Keystone IT Operations Management (ITOM) monitoring solution:** A cloud-based, SaaS application used to monitor your Keystone environment. It has built-in integrations with NetApp storage platforms to collect environmental data and monitor the compute, network, and storage components of your Keystone infrastructure. This monitoring capability extends to on-premises setups, data centers, cloud environments, or any combination of these. The service is enabled with the help of using a local ITOM Collector installed at your site that communicates with the cloud portal.
- **Keystone Data Collector:** Keystone Data Collector collects data and provides it to the Keystone billing platform for further processing. This application is bundled with Active IQ Unified Manager. It collects data from ONTAP and StorageGRID controllers at an interval of five minutes. The data is processed, and



metadata is sent to the centralized Active IQ data lake through the AutoSupport mechanism, which is used for billing data generation. The Active IQ data lake processes the billing data and sends it to Zuora for billing.



You can view the subscription and consumption details for your Keystone subscriptions through BlueXP or Digital Advisor. To learn more about Keystone reporting, refer to [Keystone dashboard overview](#).

## Learn about Keystone Collector

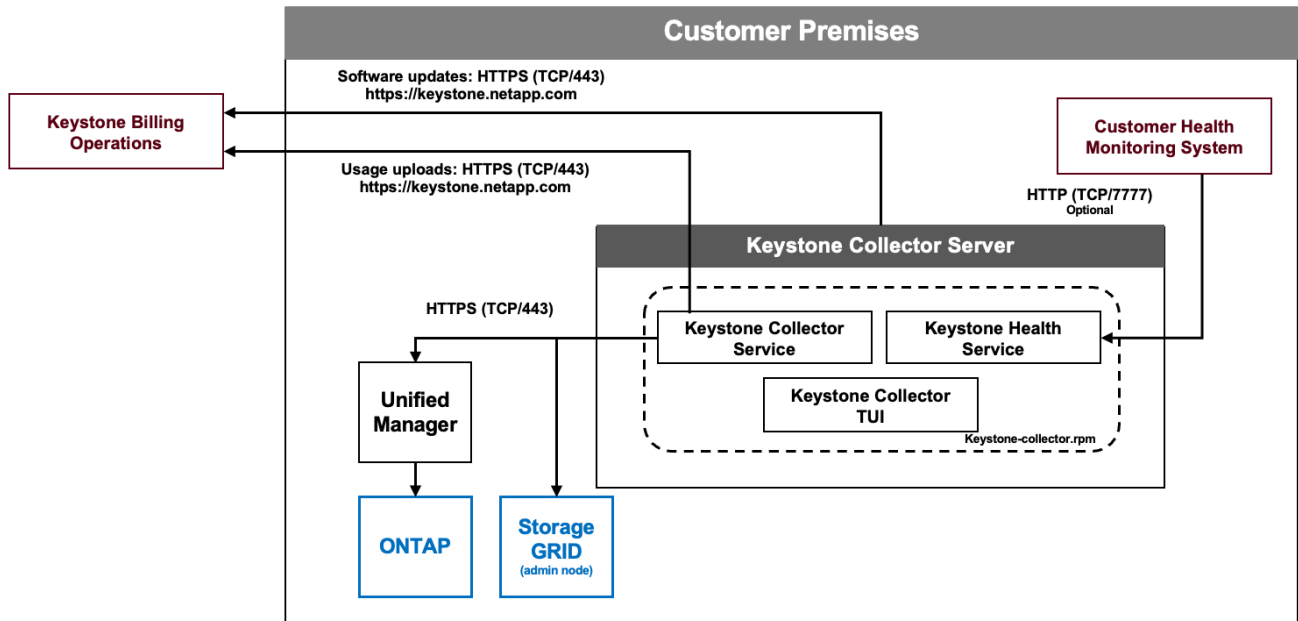
*Keystone Collector* is NetApp software that you install on a VMware vSphere or Linux host at your site to access your Keystone services. It collects usage data for Keystone systems.

Keystone Collector is the usage acquisition component of the Keystone billing platform. It leverages Active IQ Unified Manager and other applications to connect to ONTAP and StorageGRID systems to collect metadata required for usage and performance metering of your Keystone subscriptions. It provides you with the ability to monitor system health, while sending your billing data for reporting.

Keystone Collector can be configured in either *standard* mode, which works without connectivity restrictions, or *private* mode, designed for organizations with connectivity restrictions. To install Keystone Collector in standard mode, refer to [Set up and configure Keystone](#); for private mode, refer to [Keystone in private mode](#).

Keystone Collector represents the standard approach of collecting usage data for Keystone systems. If your environment cannot support Keystone Collector, you can seek authorization from Keystone support to use AutoSupport telemetry mechanism as an alternative. For information about AutoSupport, see [AutoSupport](#). For information about configuring AutoSupport for Keystone, see [Configure AutoSupport for Keystone](#).

This architecture diagram outlines the constituent components and their connectivity in a typical Keystone environment.



## Components required for deployment

Several components are required to enable NetApp Keystone STaaS services in your environment. You should review details about these components before you get started.

### Site requirements

There are some site-specific requirements, such as space, racks, PDUs, power, and cooling, with additional network and security requirements discussed here.

#### Space

Floor space to host the Keystone infrastructure equipment (to be provided by customers). NetApp provides the weight specifications based on the final configuration.

#### Racks

Four post racks in the customer-operated offering (to be provided by customers). In the NetApp-operated offering, either NetApp or the customer can provide the racks, depending on requirements. NetApp provides 42 deep racks.

#### PDUs

You should provide the power distribution units (PDUs), connected to two separate, protected circuits with sufficient C13 outlets. In the customer-operated offering, in some cases, C19 outlets are required. In the NetApp-operated offering, either NetApp or the customer can provide the PDUs, depending on requirements.

## Power

You should provide the required power. NetApp will provide the power requirement specifications based on 200V rating (Typical A, Max A, Typical W, Max W, Power cord type, and quantity), based on the final configuration. All components have redundant power supplies. NetApp will provide the in-cabinet power cords.

## Cooling

NetApp can provide the cooling requirement specifications (Typical BTU, Max BTU), based on the final configuration and requirement.

## Virtual machines

Virtual machines are required for the deployment of Keystone Collector and ITOM Collector. For installation prerequisites, refer to [Installation guide for Keystone Collector](#) and [Installation requirements for ITOM Collector](#). The other requirements are shared during deployment.

## Deployment Options

Keystone Collector can be deployed through the following methods:

- VMware OVA template (VMware vCenter Server 6.7 or later is required)
- Customer provides a Linux server running on one of the following operating systems: Debian 12, Red Hat Enterprise Linux 8.6 or later 8.x versions, or CentOS 7 (for existing environments only). The Keystone software is installed using the `.deb` or `.rpm` package, depending on the Linux distribution.

ITOM Collector can be deployed through the following methods:

- Customer provides a Linux server running on Debian 12, Ubuntu 20.04 LTS, Red Hat Enterprise Linux (RHEL) 8.x, Amazon Linux 2023, or newer versions.
- Customer provides a Windows server running Windows Server 2016 or newer versions.



The recommended operating systems are Debian 12, Windows Server 2016, or newer versions.

## Networking

Outbound access to *keystone.netapp.com* is required for software updates and usage data uploads, which are essential for the operation and maintenance of the Keystone Collector and AIOps solution gateway.

Depending on customer requirements and the storage controllers used, NetApp can provide 10 GB, 40 GB, and 100 GB connectivity at the customer's site.

NetApp provides the required transceivers for NetApp-provided infrastructure devices only. You should supply transceivers required for customer devices and cabling to the NetApp-provided Keystone infrastructure devices.

## Remote access requirement

Network connectivity is required between the storage infrastructure installed at the customer data center or customer owned co-located services, and Keystone operations center. The customer is responsible for providing the compute and virtual machines, and the internet services. The customer is also responsible for OS patching (non-OVA based deployments) and security hardening based on internal security policies. The

network design should be over a secured protocol and firewall policies will be approved by both NetApp and customers.

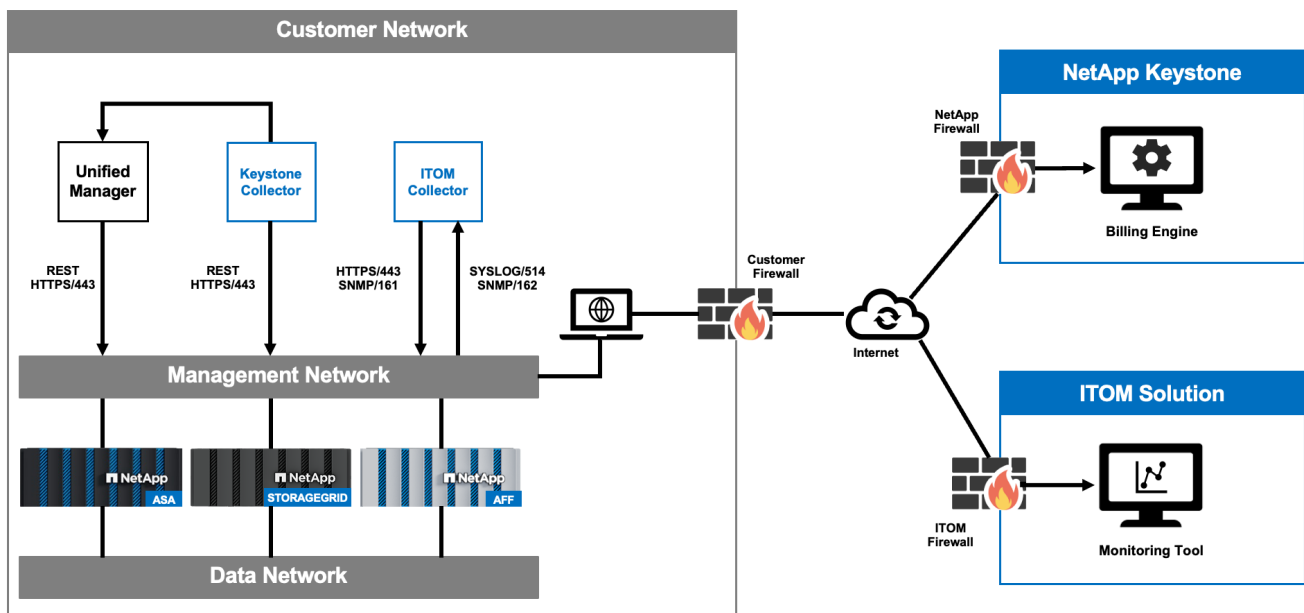
NetApp needs to access the hardware and software components installed for monitoring and management to provide services such as monitoring and billing to Keystone customers. The most common method is to establish a virtual private network (VPN) connection to the customer network and access the required data. To overcome any operational complexity perceived by customers to arise from opening firewall ports to new services, the monitoring tools initiate an external connection. NetApp cloud applications, such as ITOM monitoring solution and Zuora, use this connection to perform their respective services. This method meets the customer requirement of not opening firewall ports though providing access to the monitoring components that are part of this service.

## Keystone data flow

The data in Keystone STaaS systems flows through Keystone Collector and the ITOM monitoring solution, which is the associated monitoring system.

### Keystone Collector data flow

Keystone Collector initiates REST API calls to the storage controllers and obtains usage details of the controllers periodically, as indicated in this flow diagram:

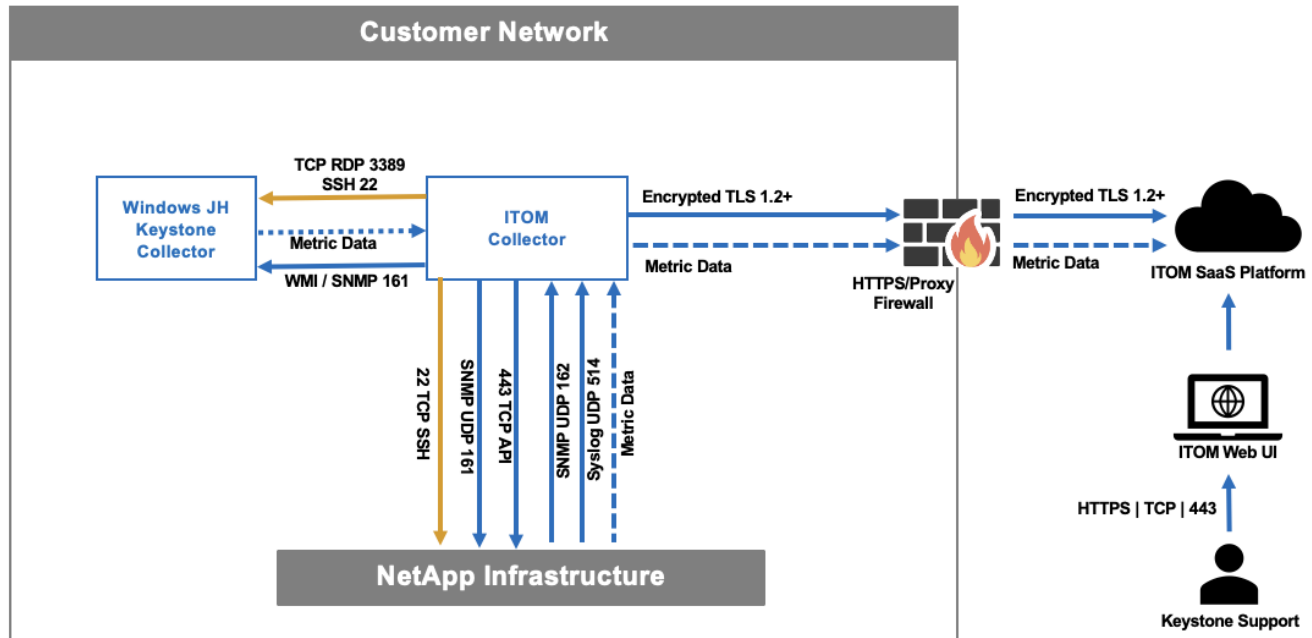


### Legend

1. NetApp Keystone Collector initiates connection to Keystone cloud.
2. The firewall operated by the customer allows the connection.
3. Keystone Collector establishes a REST API connection directly to the management connection of the storage controller or tunnels through Active IQ Unified Manager to gather usage and performance data.
4. This data is sent securely to the Keystone cloud components through HTTPS.

## Monitoring data flows

Monitoring the health of the storage infrastructure continuously is one of the most important features of Keystone service. For monitoring and reporting, Keystone uses ITOM monitoring solution. The following image describes how remote access to the customer location is secured by the ITOM monitoring solution. Customers can opt to enable the remote session feature, which allows the Keystone support team to connect to monitored devices for troubleshooting.



### Legend

1. The ITOM monitoring solution gateway initiates a TLS session to the cloud portal.
2. The firewall operated by the customer allows the connection.
3. The ITOM monitoring solution server in the cloud accepts the connection.
4. A TLS session is established between the cloud portal and the local gateway.
5. The NetApp controllers send alerts using SNMP/Syslog protocol or respond to API requests to the local gateway.
6. The local gateway sends these alerts to its cloud portal using the TLS session, which was established before.

## Compliance standards

Keystone ITOM monitoring solution complies with the European Union General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). It also provides a [Data Protection Addendum \(DPA\)](#) to document these commitments. The ITOM monitoring solution does not collect or store any personal data.

## Operational models in Keystone

NetApp Keystone STaaS offers two operational models for service delivery: partner-operated model and customer-operated model. You should understand these options

before you get started with Keystone.

- **Partner-operated model:** This model offers two options:
  - **Service provider:** A service provider operates the services for their end customers. As the contracted party with NetApp, the service provider manages a multi-tenant environment where each tenant, who is a customer of the service provider, has their own subscription, billed by the service provider. The service provider administrator is responsible for performing all administrative tasks for the tenants.
  - **Reseller:** As a reseller, a partner acts as a bridge between NetApp and the customer. The partner sells Keystone services to the end customer and manages the invoicing. While the partner takes care of billing, NetApp provides direct support to the customer. Keystone support interacts with the customer and handles all administrative tasks for the tenants.
- **Customer-operated model:** As a customer, you can subscribe to Keystone services according to your selected performance service levels and storage. NetApp defines the architecture and products, and deploys Keystone at your premises. You need to manage the infrastructure through your storage and IT resources. Based on your contract, you can raise service requests to be addressed by NetApp or your service provider. An administrator from your organization can perform the administrative tasks at your site (environment). These tasks are associated with the users in your environment.

## Roles and responsibilities across the service lifecycle

- **Partner-operated model:** The share of roles and responsibilities depends on the agreement between you and the service provider or partner. Contact your service provider for information.
- **Customer-operated model:** The following table summarizes the overall service lifecycle model and the roles and responsibilities associated with them in a customer-operated environment.

Task	NetApp	Customer
Installation and related tasks <ul style="list-style-type: none"><li>• Install</li><li>• Configure</li><li>• Deploy</li><li>• Onboard</li></ul>	✓	None
Administration and monitoring <ul style="list-style-type: none"><li>• Monitor</li><li>• Report</li><li>• Perform administrative tasks</li><li>• Alert</li></ul>	None	✓
Operations and optimization <ul style="list-style-type: none"><li>• Manage capacity</li><li>• Manage performance</li><li>• Manage SLA</li></ul>	None	✓

Task	NetApp	Customer
Support <ul style="list-style-type: none"> <li>• Support customer</li> <li>• Hardware break fix</li> <li>• Software support</li> <li>• Upgrades and patches</li> </ul>	✓	None

For more information on deployment, see [Keystone infrastructure](#) and [Components for deployment](#).

# Set up and configure Keystone

## Requirements

### Virtual infrastructure requirements

Your VMware vSphere system must meet several requirements before you can install Keystone Collector.

#### Prerequisites for the Keystone Collector server VM:

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

### Other requirements

Ensure that the following generic requirements are met:

#### Networking Requirements

The networking requirements of Keystone Collector are listed in the following table.



Keystone Collector requires internet connectivity. You can provide internet connectivity by direct routing through default Gateway (via NAT), or through HTTP Proxy. Both variants are described here.

Source	Destination	Service	Protocol and Ports	Category	Purpose
Keystone Collector (for Keystone ONTAP)	Active IQ Unified Manager (Unified Manager)	HTTPS	TCP 443	Mandatory (if using Keystone ONTAP)	Keystone Collector usage metrics collection for ONTAP
Keystone Collector (for Keystone StorageGRID)	StorageGRID Admin Nodes	HTTPS	TCP 443	Mandatory (if using Keystone StorageGRID)	Keystone Collector usage metrics collection for StorageGRID
Keystone Collector (generic)	Internet (as per URL requirements given later)	HTTPS	TCP 443	Mandatory (internet connectivity)	Keystone Collector software, OS updates, and metrics upload



Keystone Collector (generic)	Customer HTTP Proxy	HTTP Proxy	Customer Proxy Port	Mandatory (internet connectivity)	Keystone Collector software, OS updates, and metrics upload
Keystone Collector (generic)	Customer DNS Servers	DNS	TCP/UDP 53	Mandatory	DNS resolution
Keystone Collector (generic)	Customer NTP Servers	NTP	UDP 123	Mandatory	Time synchronization
Keystone Collector (for Keystone ONTAP)	Unified Manager	MYSQL	TCP 3306	Optional Functionality	Performance metrics collection for Keystone Collector
Keystone Collector (generic)	Customer Monitoring System	HTTPS	TCP 7777	Optional Functionality	Keystone Collector health reporting
Customer's Operations Workstations	Keystone Collector	SSH	TCP 22	Management	Access to the Keystone Collector Management
NetApp ONTAP Cluster and Node Management Addresses	Keystone Collector	HTTP_8000, PING	TCP 8000, ICMP Echo Request/Reply	Optional Functionality	Webserver for ONTAP firmware updates



The default port for MySQL, 3306, is restricted only to localhost during a fresh installation of Unified Manager, which prevents the collection of performance metrics for Keystone Collector. For more information, see [ONTAP requirements](#).

#### URL access

Keystone Collector needs access to the following internet hosts:

Address	Reason
<a href="https://keystone.netapp.com">https://keystone.netapp.com</a>	Keystone Collector software updates and usage reporting

## Linux system requirements

Preparing your Linux system with the required software ensures precise installation and data collection by Keystone Collector.

Ensure that your Linux and Keystone Collector server VM have these configurations.

### Linux server:

- Operating system: Any one of the following:
  - Debian 12
  - Red Hat Enterprise Linux 8.6 or later 8.x versions
  - CentOS 7 (for existing environments only)
- Chronyd time synchronized
- Access to the standard Linux software repositories

The same server should also have the following third-party packages:

- podman (POD Manager)
- sos
- chrony
- python 3 (3.6.8 to 3.9.13)

### Keystone Collector server VM:

- Core: 2 CPUs
- RAM: 4 GB RAM
- Disk space: 50 GB vDisk

## Other requirements

Ensure that the following generic requirements are met:

### Networking Requirements

The networking requirements of Keystone Collector are listed in the following table.



Keystone Collector requires internet connectivity. You can provide internet connectivity by direct routing through default Gateway (via NAT), or through HTTP Proxy. Both variants are described here.

Source	Destination	Service	Protocol and Ports	Category	Purpose
--------	-------------	---------	--------------------	----------	---------

Keystone Collector (for Keystone ONTAP)	Active IQ Unified Manager (Unified Manager)	HTTPS	TCP 443	Mandatory (if using Keystone ONTAP)	Keystone Collector usage metrics collection for ONTAP
Keystone Collector (for Keystone StorageGRID)	StorageGRID Admin Nodes	HTTPS	TCP 443	Mandatory (if using Keystone StorageGRID)	Keystone Collector usage metrics collection for StorageGRID
Keystone Collector (generic)	Internet (as per URL requirements given later)	HTTPS	TCP 443	Mandatory (internet connectivity)	Keystone Collector software, OS updates, and metrics upload
Keystone Collector (generic)	Customer HTTP Proxy	HTTP Proxy	Customer Proxy Port	Mandatory (internet connectivity)	Keystone Collector software, OS updates, and metrics upload
Keystone Collector (generic)	Customer DNS Servers	DNS	TCP/UDP 53	Mandatory	DNS resolution
Keystone Collector (generic)	Customer NTP Servers	NTP	UDP 123	Mandatory	Time synchronization
Keystone Collector (for Keystone ONTAP)	Unified Manager	MYSQL	TCP 3306	Optional Functionality	Performance metrics collection for Keystone Collector
Keystone Collector (generic)	Customer Monitoring System	HTTPS	TCP 7777	Optional Functionality	Keystone Collector health reporting
Customer's Operations Workstations	Keystone Collector	SSH	TCP 22	Management	Access to the Keystone Collector Management

NetApp ONTAP Cluster and Node Management Addresses	Keystone Collector	HTTP_8000, PING	TCP 8000, ICMP Echo Request/Reply	Optional Functionality	Webserver for ONTAP firmware updates
--	--------------------	-----------------	-----------------------------------	------------------------	--------------------------------------



The default port for MySQL, 3306, is restricted only to localhost during a fresh installation of Unified Manager, which prevents the collection of performance metrics for Keystone Collector. For more information, see [ONTAP requirements](#).

#### URL access

Keystone Collector needs access to the following internet hosts:

Address	Reason
<a href="https://keystone.netapp.com">https://keystone.netapp.com</a>	Keystone Collector software updates and usage reporting
<a href="https://support.netapp.com">https://support.netapp.com</a>	NetApp HQ for billing information and AutoSupport delivery

## Requirements for ONTAP and StorageGRID

Before you get started with Keystone, you need to ensure that ONTAP clusters and StorageGRID systems meet a few requirements.

## ONTAP

### Software versions

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

### Before you begin

Meet the following requirements if you intend to collect usage data only through ONTAP:

1. Ensure that ONTAP 9.8 or later is configured. For information about configuring a new cluster, see these links:
  - [Configure ONTAP on a new cluster with System Manager](#)
  - [Set up a cluster with the CLI](#)
2. Create ONTAP login accounts with specific roles. To learn more, refer to [Learn about creating ONTAP login accounts](#).
  - **Web UI**
    - a. Log in to ONTAP System Manager using your default credentials. To learn more, refer to [Cluster management with System Manager](#).
    - b. Create an ONTAP user with the "readonly" role and "http" application type, and enable the password authentication by navigating to **Cluster > Settings > Security > Users**.
  - **CLI**
    - a. Log in to ONTAP CLI using your default credentials. To learn more, refer to [Cluster management with CLI](#).
    - b. Create an ONTAP user with the "readonly" role and "http" application type, and enable the password authentication. To learn more about authentication, refer to [Enable ONTAP account password access](#).

Meet the following requirements if you intend to collect usage data through Active IQ Unified Manager:

1. Ensure that Unified Manager 9.10 or later is configured. For information about installing Unified Manager, see these links:
  - [Installing Unified Manager on VMware vSphere systems](#)
  - [Installing Unified Manager on Linux systems](#)
2. Ensure that the ONTAP cluster has been added to Unified Manager. For information about adding clusters, see [Adding clusters](#).
3. Create Unified Manager users with specific roles for usage and performance data collection. Perform these steps. For information about user roles, see [Definitions of user roles](#).
  - a. Log into the Unified Manager web UI with the default application administrator user credentials that are generated during installation. See [Accessing the Unified Manager web UI](#).
  - b. Create a service account for Keystone Collector with `Operator` user role. The Keystone Collector service APIs use this service account to communicate with Unified Manager and collect usage data. See [Adding users](#).
  - c. Create a `Database` user account, with the `Report Schema` role. This user is required for performance data collection. See [Creating a database user](#).



The default port for MySQL, 3306, is restricted only to localhost during a fresh installation of Unified Manager, which prevents the collection of performance data for Keystone ONTAP. This configuration can be modified, and the connection can be made available to other hosts using the `Control access to MySQL port 3306` option on the Unified Manager maintenance console. For information, see [Additional menu options](#).

4. Enable API Gateway in Unified Manager. Keystone Collector makes use of the API Gateway feature to communicate with ONTAP clusters. You can enable API Gateway either from the web UI, or by running a few commands through Unified Manager CLI.

#### Web UI

To enable API Gateway from the Unified Manager web UI, log into the Unified Manager web UI and enable API Gateway. For information, see [Enabling API Gateway](#).

#### CLI

To enable API Gateway through Unified Manager CLI, follow these steps:

- a. On the Unified Manager server, begin an SSH session and log into Unified Manager CLI.  

```
um cli login -u <umadmin>
```

For information about CLI commands, see [Supported Unified Manager CLI commands](#).
- b. Verify whether API Gateway is already enabled.  

```
um option list api.gateway.enabled
```

A `true` value indicates that the API Gateway is enabled.
- c. If the value returned is `false`, run this command:  

```
um option set api.gateway.enabled=true
```
- d. Restart the Unified Manager server:
  - Linux: [Restarting Unified Manager](#).
  - VMware vSphere: [Restarting the Unified Manager virtual machine](#).

#### StorageGRID

The following configurations are required for installing Keystone Collector on StorageGRID.

- StorageGRID 11.6.0 or later should be installed. For information about upgrading StorageGRID, see [Upgrade StorageGRID software: Overview](#).
- A StorageGRID local admin user account should be created for usage data collection. This service account is used by the Keystone Collector service for communicating with StorageGRID through administrator node APIs.

#### Steps

1. Log into the Grid Manager. See [Sign in to the Grid Manager](#).
2. Create a local admin group with `Access mode: Read-only`. See [Create an admin group](#).
3. Add the following permissions:
  - Tenant Accounts
  - Maintenance
  - Metrics Query
4. Create a Keystone service account user and associate it with the admin group. See [Manage](#)

# Install Keystone Collector

## Deploy Keystone Collector on VMware vSphere systems

Deploying Keystone Collector on VMware vSphere systems includes downloading the OVA template, deploying the template by using the **Deploy OVF Template** wizard, verifying the integrity of the certificates, and verifying the readiness of the VM.

### Deploying the OVA template

Follow these steps:

#### Steps

1. Download the OVA file from [this link](#) and store it on your VMware vSphere system.
2. On your VMware vSphere system, navigate to the **VMs and Templates** view.
3. Right click on the required folder for the virtual machine (VM) (or data center, if not using VM folders) and select **Deploy OVF Template**.
4. On *Step 1* of the **Deploy OVF Template** wizard, click **Select and OVF template** to select the downloaded `KeystoneCollector-latest.ova` file.
5. On *Step 2*, specify the VM name and select the VM folder.
6. On *Step 3*, specify the required compute resource that is to run the VM.
7. On *Step 4: Review details*, verify the correctness and authenticity of the OVA file.  
vCentre versions prior to 7.0u2 are unable to automatically verify the authenticity of the code signing certificate. vCentre 7.0u2 and later can perform the verifications, however, for this, the signing certificate authority should be added to vCentre. Follow these instructions for your version of vCentre:

#### vCentre 7.0u1 and earlier: Learn more

vCentre validates the integrity of the OVA file contents and that a valid code-signing digest is provided for the files contained in the OVA file. However, it does not validate the authenticity of the code-signing certificate. For verifying the integrity, you should download the full signing digest certificate, and verify it against the public certificate published by Keystone.

- a. Click the **Publisher** link to download the full signing digest certificate.
- b. Download the *Keystone Billing* public certificate from [this link](#).
- c. Verify the authenticity of the OVA signing certificate against the public certificate by using OpenSSL:  

```
openssl verify -CAfile OVA-SSL-NetApp-Keystone-20221101.pem keystone-collector.cert
```

## vCentre 7.0u2 and later: Learn more

7.0u2 and later versions of vCenter are capable of validating the integrity of the OVA file contents and the authenticity of the code-signing certificate, when a valid code-signing digest is provided. The vCenter root trust store contains only VMware certificates. NetApp uses Entrust as a certifying authority, and those certificates need to be added to the vCenter trust store.

- a. Download the code-signing CA certificate from Entrust [here](#).
- b. Follow the steps in the Resolution section of this knowledge base (KB) article: <https://kb.vmware.com/s/article/84240>.

When the integrity and authenticity of the Keystone Collector OVA are validated, you can see the text (Trusted certificate) with the publisher.

Deploy OVF Template	
✓ 1 Select an OVF template	Review details
✓ 2 Select a name and folder	Verify the template details.
✓ 3 Select a compute resource	
<b>4 Review details</b>	
5 Select storage	
6 Select networks	
7 Customize template	
8 Ready to complete	

Publisher	Entrust Code Signing CA - OVCS2 (Trusted certificate)
Product	NetApp Keystone Collector
Version	20220405
Vendor	NetApp
Download size	8.3 GB
Size on disk	12.1 GB (thin provisioned) 200.0 GB (thick provisioned)

CANCEL BACK NEXT

8. On *Step 5* of the **Deploy OVF Template** wizard, specify the location for storing the VM.
9. On *Step 6*, select the destination network for the VM to use.
10. On *Step 7 Customize template*, specify the initial network address and password for the admin user account.



The admin password is stored in a reversible format in vCentre and should be used as a bootstrap credential to gain initial access to the VMware vSphere system. During the initial software configuration, this admin password should be changed. The subnet mask for the IPv4 address should be supplied in CIDR notation. For example, use the value of 24 for a subnet mask of 255.255.255.0.

11. On *Step 8 Ready to complete* of the **Deploy OVF Template** wizard, review the configuration and verify that you have correctly set the parameters for the OVA deployment.



After the VM has been deployed from the template and powered on, open an SSH session to the VM and log in with the temporary admin credentials to verify that the VM is ready for configuration.

## Initial system configuration

Perform these steps on your VMware vSphere systems for an initial configuration of the Keystone Collector servers deployed through OVA:



On completing the deployment, you can use the Keystone Collector Management Terminal User Interface (TUI) utility to perform the 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.

1. Open an SSH session to the Keystone Collector server. When you connect, the system will prompt you to update the admin password. Complete the admin password update as required.
2. Log in using the new password to access the TUI. On login, the TUI appears.

Alternatively, you can launch it manually by running the `keystone-collector-tui` CLI command.

3. If required, configure the proxy details in the **Configuration > Network section** on the TUI.
4. Configure the system hostname, location, and NTP server in the **Configuration > System** section.
5. Update the Keystone Collectors using the **Maintenance > Update Collectors** option. After the update, restart the Keystone Collector management TUI utility to apply the changes.

## Install Keystone Collector on Linux systems

You can install the Keystone Collector software on a Linux server using an RPM or a Debian package. Follow the installation steps depending on your Linux distribution.

## Using RPM

1. SSH to the Keystone Collector server and elevate to `root` privilege.
2. Import the Keystone public signing signature:  

```
# rpm --import https://keystone.netapp.com/repo/RPM-GPG-NetApp-Keystone-20221101
```
3. Ensure that the correct public certificate has been imported by checking the fingerprint for Keystone Billing Platform in the RPM database:  

```
# rpm -qa gpg-pubkey --qf '%{Description}'|gpg --show-keys --fingerprint
```

The correct fingerprint looks like this:  
90B3 83AF E07B 658A 6058 5B4E 76C2 45E4 33B6 C17D
4. Download the `keystonerepo.rpm` file:  

```
curl -O https://keystone.netapp.com/repo/keystonerepo.rpm
```
5. Verify the authenticity of the file:  

```
rpm --checksig -v keystonerepo.rpm
```

A signature for an authentic file looks like this:  
Header V4 RSA/SHA512 Signature, key ID 33b6c17d: OK
6. Install the YUM software repository file:  

```
# yum install keystonerepo.rpm
```
7. When the Keystone repo is installed, install the `keystone-collector` package through the YUM package manager:  

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

For Red Hat Enterprise Linux 9, run the following command to install the `keystone-collector` package:

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

## Using Debian

1. SSH to the Keystone Collector server and elevate to `root` privilege.  

```
sudo su
```
2. Download the `keystone-sw-repo.deb` file:  

```
curl -O https://keystone.netapp.com/downloads/keystone-sw-repo.deb
```
3. Install the Keystone software repository file:  

```
# dpkg -i keystone-sw-repo.deb
```
4. Update the package list:  

```
# apt-get update
```
5. When the Keystone repo is installed, install the `keystone-collector` package:  

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



On completing the installation, you can use the Keystone Collector Management Terminal User Interface (TUI) utility to perform the 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. See [Configure Keystone Collector](#) and [Monitor system health](#) for information.

## Automatic validation of Keystone software

The Keystone repository is configured to automatically validate the integrity of Keystone software so that only valid and authentic software is installed at your site.

The Keystone YUM repository client configuration provided in `keystonerepo.rpm` makes use of enforced GPG checking (`gpgcheck=1`) on all software downloaded through this repository. Any RPM downloaded through the Keystone repository that fails signature validation is prevented from being installed. This functionality is used in the scheduled auto-update capability of Keystone Collector to ensure only valid and authentic software is installed at your site.

## Configure Keystone Collector

You need to complete a few configuration tasks to enable Keystone Collector to collect usage data in your storage environment. This is a one-time activity to activate and associate the required components with your storage environment.



- 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.
- Keystone Collector can be configured for organizations that do not have internet access, also known as a *dark site* or *private mode*. To learn more about, refer to [Keystone in private mode](#).

### Steps

1. Start the Keystone Collector management TUI utility:  

```
$ keystone-collector-tui
```
2. Go to **Configure > KS-Collector** to open the Keystone Collector configuration screen to view the available options for update.
3. Update the required options.

### For ONTAP

- **Collect ONTAP usage:** This option enables collection of usage data for ONTAP. Add the details of the Active IQ Unified Manager (Unified Manager) server and service account.
- **Collect ONTAP Performance Data:** This option enables collection of performance data for ONTAP. This is disabled by default. Enable this option if performance monitoring is required in your environment for SLA purposes. Provide the Unified Manager Database user account details. For information about creating database users, see [Create Unified Manager users](#).
- **Remove Private Data:** This option removes specific private data of customers and is enabled by default. For information about what data is excluded from the metrics if this option is enabled, see [Limit collection of private data](#).

## For StorageGRID

- **Collect StorageGRID usage:** This option enables collection of node usage details. Add the StorageGRID node address and user details.
- **Remove Private Data:** This option removes specific private data of customers and is enabled by default. For information about what data is excluded from the metrics if this option is enabled, see [Limit collection of private data](#).

4. Toggle the **Start KS-Collector with System** field.

5. Click **Save**.

```
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. Ensure that 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.

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

7. Exit the Keystone Collector management TUI by selecting the **Exit to Shell** option on the home screen.

## Configure HTTP Proxy on Keystone Collector

The Collector software supports using a HTTP proxy to communicate with the internet. This can be configured in the TUI.

### Steps

1. Restart the Keystone Collector management TUI utility if already closed:  
`$ keystone-collector-tui`
2. Toggle on the **HTTP Proxy** field, and add the details for the HTTP proxy server, port, and credentials, if authentication is required.
3. Click **Save**.



## Limit collection of private data

Keystone Collector gathers limited configuration, status, and performance information required to perform subscription metering. There is an option to further limit the information collected by masking sensitive information from the content uploaded. This does not impact billing calculation. However, limiting the information might impact usability of the reporting information, as some elements, which can be easily identified by users, such as volume name, is replaced with UUIDs.

Limiting the collection of specific customer data is a configurable option on the Keystone Collector TUI screen. This option, **Remove Private Data**, is enabled by default.

```
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
```

For information about the items removed on limiting private data access in both ONTAP and StorageGRID, see [List of items removed on limiting private data access](#).

## Trust a custom root CA

Verification of certificates against a public root certificate authority (CA) is a part of the Keystone Collector security features. However, if required, you can configure Keystone Collector to trust a custom root CA.

If you use SSL/TLS inspection in your system firewall, it results in the internet-based traffic to be re-encrypted with your custom CA certificate. It is necessary to configure the settings to verify the source as a trusted CA before accepting the root certificate and allowing connections to occur. Follow these steps:

### Steps

1. Prepare the CA certificate. It should be in *base64-encoded X.509* file format.



The supported file extensions are .pem, .crt, .cert. Ensure that the certificate is in one of these formats.

2. Copy the certificate to the Keystone Collector server. Make a note of the location where the file is copied.
3. Open a terminal on the server and run the management TUI utility.  
\$ keystone-collector-tui
4. Go to **Configuration > Advanced**.
5. Enable the option **Enable custom root certificate**.
6. For **Select custom root certificate path:**, select - Unset -

7. Press Enter. A dialog box for selecting the certificate path is displayed.
8. Select the root certificate from the file system browser or enter the exact path.
9. Press Enter. You return to the **Advanced** screen.
10. Select **Save**. The configuration is applied.

```
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
```

## Create Performance Service Levels

You can create Performance Service Levels (PSLs) using the Keystone Collector management TUI utility. Creating PSLs through the TUI automatically selects the default values set for each service level, reducing the chance of errors that might occur when manually setting these values while creating PSLs through Active IQ Unified Manager.

To learn more about PSLs, refer to [Performance Service Levels](#).

To learn more about service levels, refer to [Service levels in Keystone](#).

### Steps

1. Start the Keystone Collector management TUI utility:  
\$ keystone-collector-tui
2. Go to **Configure>AIQUM** to open the AIQUM screen.
3. Enable the option **Create AIQUM Performance Profiles**.
4. Enter the details of the Active IQ Unified Manager server and user account. These details are required to create PSLs and will not be stored.

NetApp Keystone Collector – Configure – AIQUM

☐ Enable Embedded UM  
☒ 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. For **Select Keystone version**, select -unset-.
6. Press Enter. A dialog box for selecting the Keystone version is displayed.
7. Highlight **STaaS** to specify the Keystone version for Keystone STaaS, and then press Enter.

NetApp Keystone Collector – Configure – AIQUM

Select Keystone version

AIQUM Ad    KFS  
 AIQUM Us    STaaS  
 AIQUM Pa  
 Select K  
 Select K

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.





You can highlight the **KFS** option for Keystone subscription services version 1. Keystone subscription services differ from Keystone STaaS in the constituent service levels, service offerings, and billing principles. To learn more, refer to [Keystone subscription services | Version 1](#).

8. All supported Keystone service levels will be displayed within the **Select Keystone Service Levels** option for the specified Keystone version. Enable the desired service levels from the list.

```
NetApp Keystone Collector - Configure - AIQUM

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

AIQUM Address:
AIQUM Username:
AIQUM Password:
Select Keystone version: STaaS
Select Keystone Service Levels:
[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.
```



You can select multiple service levels simultaneously to create PSLs.

9. Select **Save** and press Enter. Performance Service Levels will be created.

You can view the created PSLs, such as Premium-KS-STaaS for STaaS or Extreme KFS for KFS, on the **Performance Service Levels** page in Active IQ Unified Manager. If the created PSLs do not meet your requirements, then you can modify PSLs to meet your needs. To learn more, refer to [Creating and editing Performance Service Levels](#).




## Performance Service Levels

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

 Filter

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



<input type="checkbox"/>	Name ^	Type	Expected IOPS/TB	Peak IOPS/TB	Absolute Minim...	Expected Latency	Capacity	Workloads
	<input type="checkbox"/> Extreme - KFS	User-defined	6144	12288	1000	1	<div><div></div></div> Used: 0 bytes Available: 283.85 TiB	0
	<input type="checkbox"/> 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						
	<input type="checkbox"/> Premium ...S-STaaS	User-defined	2048	4096	500	2	<div><div></div></div> Used: 0 bytes Available: 283.85 TiB	0

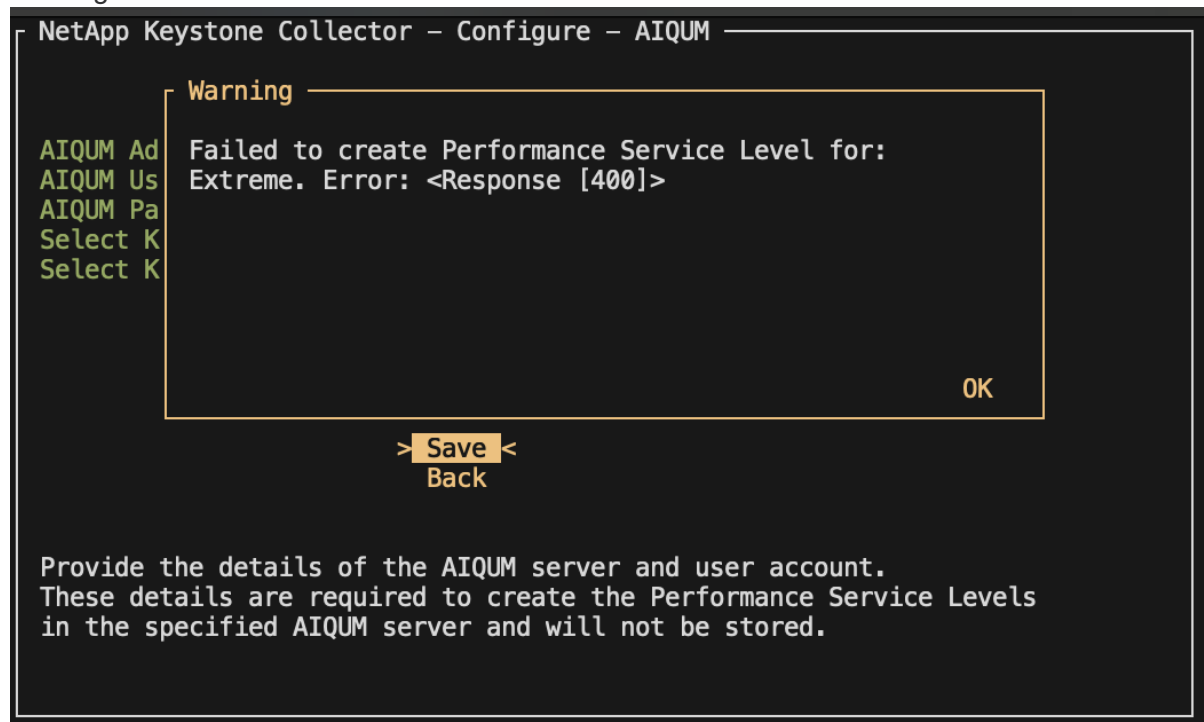
Overview

Description Premium - KS-STaaS

Added Date 1 Aug 2024, 18:08

Last Modified Date 1 Aug 2024, 18:08

If a PSL for the selected service level already exist on the specified Active IQ Unified Manager server, then you cannot create it again. If you attempt to do so, you will receive an error message.



## Install ITOM Collector

## Installation requirements for ITOM Collector

Before installing ITOM Collector, ensure that your systems are prepared with the necessary software and meet all required prerequisites.

### Prerequisites for the ITOM Collector server VM:

- Supported operating system: Debian 12, Windows Server 2016, Ubuntu 20.04 LTS, Red Hat Enterprise Linux (RHEL) 8.x, Amazon Linux 2023, or newer versions of these operating systems.



The recommended operating systems are Debian 12, Windows Server 2016, or newer versions.

- Resource requirement: The VM resource requirements based on the number of NetApp nodes monitored are as follows:
  - 2-10 nodes: 4 CPUs, 8 GB RAM, 40 GB Disk
  - 12-20 nodes: 8 CPUs, 16 GB RAM, 40 GB Disk
- Configuration requirement: Ensure that a read-only account and SNMP are configured on the monitored devices. The ITOM Collector server VM also needs to be configured as an SNMP trap host and Syslog server on the NetApp cluster and cluster switches, if applicable.

### Networking requirements

The networking requirements of ITOM Collector are listed in the following table.

Source	Destination	Protocol	Ports	Description
ITOM Collector	NetApp ONTAP cluster management IPs	HTTPS, SNMP	TCP 443, UDP 161	Monitoring of the ONTAP controllers
NetApp ONTAP cluster and node management IPs	ITOM Collector	SNMP, Syslog	UDP 162, UDP 514	SNMP traps and Syslogs from controllers
ITOM Collector	Cluster switches	SNMP	UDP 161	Monitoring of switches
Cluster switches	ITOM Collector	SNMP, Syslog	UDP 162, UDP 514	SNMP traps and Syslogs from switches
ITOM Collector	StorageGRID nodes IPs	HTTPS, SNMP	TCP 443, UDP 161	SNMP monitoring of StorageGRID
StorageGRID nodes IPs	ITOM Collector	SNMP, Syslog	UDP 162, UDP 514	SNMP traps from StorageGRID
ITOM Collector	Keystone Collector	SSH, HTTPS, SNMP	TCP 22, TCP 443, UDP 161	Keystone Collector monitoring and remote management
ITOM Collector	Local DNS	DNS	UDP 53	Public or private DNS services

ITOM Collector	NTP server(s) of choice	NTP	UDP 123	Time keeping
----------------	-------------------------	-----	---------	--------------

## Install ITOM Collector on Linux systems

Complete a few steps to install ITOM Collector, which collects metrics data in your storage environment. You can install it on either Windows or Linux systems, depending on your requirements.



Keystone support team provides a dynamic link to download the ITOM Collector setup file, which expires in two hours.

To install ITOM Collector on Windows systems, refer to [Install ITOM Collector on Windows systems](#).

Follow these steps to install software on your Linux server:

### Before you begin

- Verify that the Bourne shell is available for the Linux installation script.
- Install the `vim-common` package to get the `xxd` binary required for the ITOM Collector setup file.
- Ensure the `sudo` package is installed if planning to run ITOM Collector as a non-root user.

### Steps

1. Download the ITOM collector setup file to your Linux server.
2. Open a terminal on the server and run the following command to change the permissions and make the binaries executable:  

```
# chmod +x <installer_file_name>.bin
```
3. Run the command to start the ITOM collector setup file:  

```
# ./<installer_file_name>.bin
```
4. Running the setup file prompts you to:
  - a. Accept the end-user license agreement (EULA).
  - b. Enter the user details for the installation.
  - c. Specify the installation parent directory.
  - d. Select the collector size.
  - e. Provide proxy details, if applicable.

For each prompt, a default option is displayed. It is recommended to select the default option unless you have specific requirements. Press the **Enter** key to choose the default option. When the installation completes, a message confirms that the ITOM Collector is installed successfully.



- The ITOM Collector setup file makes additions to `/etc/sudoers` to handle service restarts and memory dumps.
- Installing ITOM Collector on the Linux server creates a default user called **ITOM** to run ITOM Collector without root privileges. You can choose a different user or run it as root, but it is recommended to use the ITOM user created by the Linux installation script.

## What's next?

On successful installation, contact the Keystone support team to validate the successful installation of ITOM Collector through the ITOM support portal. After verification, the Keystone support team will configure the ITOM Collector remotely, including further device discovery and monitoring setup, and will send a confirmation once the configuration is complete. For any queries or additional information, contact [keystone.services@netapp.com](mailto:keystone.services@netapp.com).

## Install ITOM Collector on Windows systems

Install ITOM Collector on a Windows system by downloading the ITOM Collector setup file, running the InstallShield wizard, and entering the required monitoring credentials.



Keystone support team provides a dynamic link to download the ITOM Collector setup file, which expires in two hours.

You can install it on Linux systems based on your requirements. To install ITOM Collector on Linux systems, refer to [Install ITOM Collector on Linux systems](#).

Follow these steps to install ITOM collector software on your Windows server:

### Before you begin

Ensure ITOM Collector service is granted **Log on as a service** under Local Policy/User Rights Assignment in the Windows server's local security policy settings.

### Steps

1. Download the ITOM collector setup file to your Windows server.
2. Open the setup file to start the InstallShield wizard.
3. Accept the end-user license agreement (EULA). The InstallShield wizard extracts the necessary binaries and prompts you to enter credentials.
4. Enter the credentials for the account that ITOM Collector will run under:
  - If ITOM Collector is not monitoring other Windows servers, use local system.
  - If ITOM Collector is monitoring other Windows servers in the same domain, use a domain account with local administrator permissions.
  - If ITOM Collector is monitoring other Windows servers that are not part of the same domain, use a local administrator account and connect to each resource with local administrator credentials. You may choose to set the password so that it does not expire, to reduce authentication issues between ITOM Collector and its monitored resources.
5. Select the collector size. The default is the recommended size based on the setup file. Proceed with the suggested size unless you have specific requirements.
6. Select *Next* to begin the installation. You can use the populated folder or choose a different one. A status box displays the installation progress, followed by the InstallShield Wizard Completed dialog box.

## What's next?

On successful installation, contact the Keystone support team to validate the successful installation of ITOM Collector through the ITOM support portal. After verification, the Keystone support team will configure the ITOM Collector remotely, including further device discovery and monitoring setup, and will send a confirmation once the configuration is complete. For any queries or additional information, contact [keystone.services@netapp.com](mailto:keystone.services@netapp.com).

# Configure AutoSupport for Keystone

When using the AutoSupport telemetry mechanism, Keystone calculates the usage based on the AutoSupport telemetry data. To achieve the necessary level of granularity, you should configure AutoSupport to incorporate Keystone data in the daily support bundles sent by the ONTAP clusters.

## About this task

You should note the following before configuring AutoSupport to include Keystone data.

- You edit the AutoSupport telemetry options by using ONTAP CLI. For information about managing AutoSupport services and system (cluster) administrator role, see [Manage AutoSupport overview](#) and [Cluster and SVM administrators](#).
- You include the subsystems in the daily and weekly AutoSupport bundles to ensure precise data collection for Keystone. For information about AutoSupport subsystems, see [What AutoSupport subsystems are](#).

## Steps

1. As a system administrator user, log in to the Keystone ONTAP cluster by using SSH. For information, see [Access the cluster by using SSH](#).
2. Modify the log content.
  - For ONTAP 9.16.1 and above, run this command to modify the daily log content:

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

- For earlier ONTAP versions, run this command to modify the daily log content:

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

- Run this command to modify the weekly log content:

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

For more information about this command, see [system node autosupport trigger modify](#).

# Monitor and upgrade

## Monitor the health of Keystone Collector

You can monitor the health of Keystone Collector by using any monitoring system that supports HTTP requests. Monitoring the health can help to ensure that data is available on the Keystone dashboard.

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 this error, add your monitoring system to the *allow* list from **Keystone Collector management TUI > Configure > Health Monitoring**.



### Linux users, note this known issue:

**Issue description:** Keystone Collector runs a number of containers as part of the usage metering system. When the Red Hat Enterprise Linux 8.x server is hardened with USA Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG) policies, a known issue with `fapolicyd` (File Access Policy Daemon) has been seen intermittently. This issue is identified as [bug 1907870](#).

**Workaround:** Until resolved by Red Hat Enterprise, NetApp recommends that you work around this issue by putting `fapolicyd` into permissive mode. In `/etc/fapolicyd/fapolicyd.conf`, set the value of `permissive = 1`.

## View system logs

You can view Keystone Collector system logs to review system information and perform troubleshooting by using those logs. Keystone Collector uses the host's *journald* logging system, and the system logs can be reviewed through the standard *journalctl* system utility. You can avail the following key services to examine the logs:

- `ks-collector`

- ks-health
- ks-autoupdate

The main data collection service *ks-collector* produces logs in JSON format with a `run-id` attribute associated with each scheduled data collection job. The following is an example of a successful job for standard usage data collection:



```

{"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-a826be4fdb7_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"}

```

The following is an example of a successful job for optional performance data collection:

```
{"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"}
```

## Generate and collect support bundles

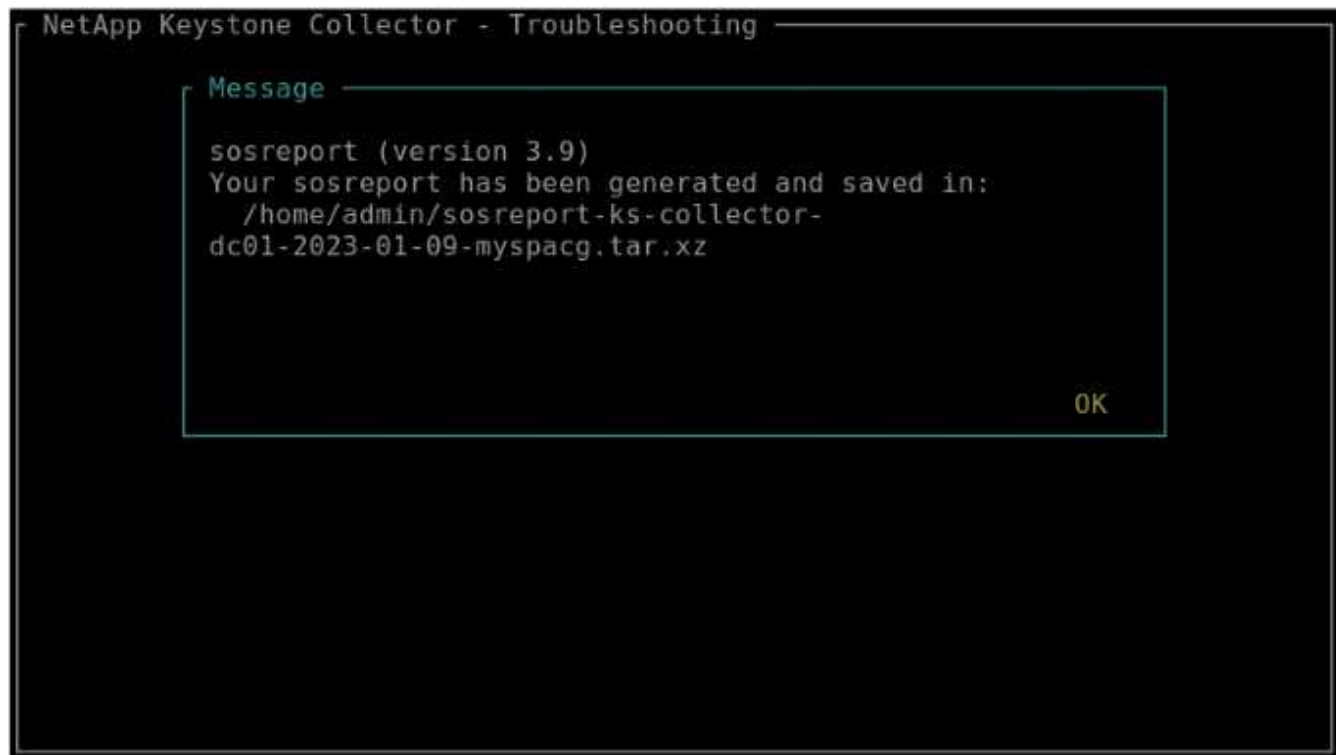
The Keystone Collector TUI enables you to generate support bundles and add them to service requests for resolving support issues. Follow this procedure:

### Steps

1. Start the Keystone Collector management TUI utility:  
`$ keystone-collector-tui`
2. Go to **Troubleshooting > Generate Support Bundle**.



3. When generated, the location where the bundle is saved is displayed. Use FTP, SFTP, or SCP to connect to the location and download the log file to a local system.



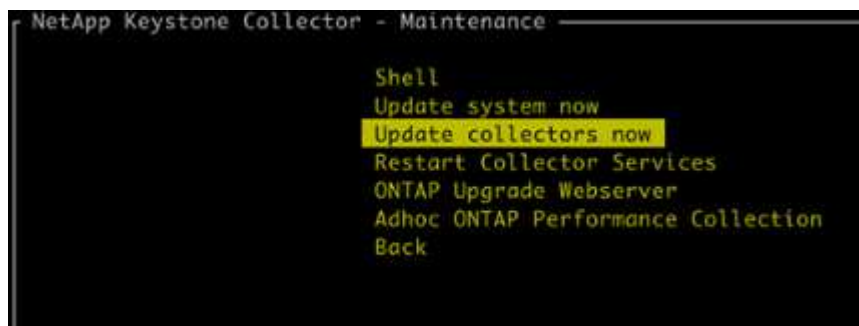
4. When the file is downloaded, you can attach it to the Keystone ServiceNow support ticket. For information about raising tickets, see [Generating service requests](#).

## Manually upgrade Keystone Collector

The auto-update feature in Keystone Collector is enabled by default, which automatically upgrades the Keystone Collector software with every new release. You can, however, disable this feature and manually upgrade the software.

### Steps

1. Start the Keystone Collector management TUI utility:  
`$ keystone-collector-tui`
2. On the maintenance screen, selecting the **Update collectors now** option.



Alternately, run these commands to upgrade the version:

For CentOS:

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

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

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

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

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

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

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

Upgraded:
keystone-collector-1.3.2-1.noarch

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

For Debian:

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

- Restart Keystone Collector management TUI, you can see the latest version on the upper left portion of the home screen.

Alternately, run these commands to view the latest version:

For CentOS:

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

For Debian:

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

## Keystone Collector security

Keystone Collector includes security features that monitor the performance and usage metrics of Keystone systems, without risking the security of customer data.

The functioning of Keystone Collector is based on the following security principles:

- **Privacy by design**-Keystone Collector collects minimum data to perform usage metering and performance monitoring. For more information, see [Data collected for billing](#). The [Remove Private Data](#) option is enabled by default, which masks and protects sensitive information.
- **Least privilege access**-Keystone Collector requires minimum permissions to monitor the storage systems, which minimizes security risks and prevents any unintended modifications to the data. This approach aligns with the principle of least privilege, enhancing the overall security posture of the monitored environments.
- **Secure software development framework**- Keystone uses a secure software development framework throughout the development cycle, which mitigates risks, reduces vulnerabilities, and protects the system against potential threats.

## Security hardening

By default, Keystone Collector is configured to use security-hardened configurations. The following are the recommended security configurations:

- The operating system of the Keystone Collector virtual machine:
  - Complies with the CIS Debian Linux 12 Benchmark standard. Making any changes to the OS configuration outside the Keystone Collector management software may reduce the system security. For more information, see [CIS Benchmark guide](#).
  - Automatically receives and installs security patches that are verified by Keystone Collector through the auto-update feature. Disabling this functionality may lead to unpatched vulnerable software.
  - Authenticates updates received from Keystone Collector. Disabling APT repository verification can lead to the automatic installation of unauthorized patches, potentially introducing vulnerabilities.
- Keystone Collector automatically validates HTTPS certificates to ensure connection security. Disabling this feature could lead to impersonation of external endpoints and usage data leakage.
- Keystone Collector supports [Custom Trusted CA](#) certification. By default, it trusts certificates that are signed by public root CAs recognized by the [Mozilla CA Certificate program](#). By enabling additional Trusted CAs, Keystone Collector enables HTTPS certificate validation for connections to endpoints that present these certificates.
- Keystone collector enables the **Remove Private Data** option by default, which masks and protects sensitive information. For more information, see [Limit collection of private data](#). Disabling this option results in additional data being communicated to the Keystone system. For example, it can include user-entered information such as volume names which may be considered sensitive information.

## Related information

- [Keystone Collector overview](#)

- [Virtual infrastructure requirements](#)
- [Configure Keystone Collector](#)

## Types of user data that Keystone collects

Keystone collects configuration, status, and usage information from Keystone ONTAP and Keystone StorageGRID subscriptions, as well as telemetry data from the virtual machine (VM) hosting Keystone Collector. It can collect performance data for ONTAP only, if this option is enabled in Keystone Collector.

### ONTAP data collection

## Usage data collected for ONTAP: [Learn more](#)

The following list is a representative sample of the capacity consumption data collected for ONTAP:

- Clusters
  - ClusterUUID
  - ClusterName
  - SerialNumber
  - Location (based on value input in ONTAP cluster)
  - Contact
  - Version
- Nodes
  - SerialNumber
  - Node name
- Volumes
  - Aggregate name
  - Volume Name
  - VolumeInstanceUUID
  - IsCloneVolume flag
  - IsFlexGroupConstituent flag
  - IsSpaceEnforcementLogical flag
  - IsSpaceReportingLogical flag
  - LogicalSpaceUsedByAfs
  - PercentSnapshotSpace
  - PerformanceTierInactiveUserData
  - PerformanceTierInactiveUserDataPercent
  - QoSAdaptivePolicyGroup Name
  - QoSPolicyGroup Name
  - Size
  - Used
  - PhysicalUsed
  - SizeUsedBySnapshots
  - Type
  - VolumeStyleExtended
  - Vserver name
  - IsVsRoot flag
- VServers
  - VserverName



- VserverUUID
- Subtype
- Storage aggregates
  - StorageType
  - Aggregate Name
  - Aggregate UUID
- Aggregate object stores
  - ObjectStoreName
  - ObjectStoreUUID
  - ProviderType
  - Aggregate Name
- Clone volumes
  - FlexClone
  - Size
  - Used
  - Vserver
  - Type
  - ParentVolume
  - ParentVserver
  - IsConstituent
  - SplitEstimate
  - State
  - FlexCloneUsedPercent
- Storage LUNs
  - LUN UUID
  - LUN Name
  - Size
  - Used
  - IsReserved flag
  - IsRequested flag
  - LogicalUnit Name
  - QoSPolicyUUID
  - QoSPolicyName
  - VolumeUUID
  - VolumeName
  - SVMUUID
  - SVM Name

- Storage volumes
  - VolumeInstanceUUID
  - VolumeName
  - SVMName
  - SVMUUID
  - QoSPolicyUUID
  - QoSPolicyName
  - CapacityTierFootprint
  - PerformanceTierFootprint
  - TotalFootprint
  - TieringPolicy
  - IsProtected flag
  - IsDestination flag
  - Used
  - PhysicalUsed
  - CloneParentUUID
  - LogicalSpaceUsedByAfs
- QoS policy groups
  - PolicyGroup
  - QoSPolicyUUID
  - MaxThroughput
  - MinThroughput
  - MaxThroughputIOPS
  - MaxThroughputMBps
  - MinThroughputIOPS
  - MinThroughputMBps
  - IsShared flag
- ONTAP adaptive QoS policy groups
  - QoSPolicyName
  - QoSPolicyUUID
  - PeakIOPS
  - PeakIOPSAllocation
  - AbsoluteMinIOPS
  - ExpectedIOPS
  - ExpectedIOPSAllocation
  - BlockSize
- Footprints

- Vserver
- Volume
- TotalFootprint
- VolumeBlocksFootprintBin0
- VolumeBlocksFootprintBin1
- MetroCluster clusters
  - ClusterUUID
  - ClusterName
  - RemoteClusterUUID
  - RemoteClusterName
  - LocalConfigurationState
  - RemoteConfigurationState
  - Mode
- Collector Observability Metrics
  - Collection Time
  - Active IQ Unified Manager API endpoint queried
  - Response time
  - Number of records
  - AIQUMInstance IP
  - CollectorInstance ID

## Performance data collected for ONTAP: [Learn more](#)

The following list is a representative sample of the performance data collected for ONTAP:

- Cluster Name
- Cluster UUID
- ObjectID
- VolumeName
- Volume Instance UUID
- Vserver
- VserverUUID
- Node Serial
- ONTAPVersion
- AIQUM version
- Aggregate
- AggregateUUID
- ResourceKey
- TimeStamp
- IOPSPerTb
- Latency
- ReadLatency
- WriteMBps
- QoSMinThroughputLatency
- QoSNBladeLatency
- UsedHeadRoom
- CacheMissRatio
- OtherLatency
- QoSAggregateLatency
- IOPS
- QoSNetworkLatency
- AvailableOps
- WriteLatency
- QoSCloudLatency
- QoSClusterInterconnectLatency
- OtherMBps
- QoSCopLatency
- QoSDBladeLatency
- Utilization

- ReadIOPS
- MBps
- OtherIOPS
- QoSPolicyGroupLatency
- ReadMBps
- QoSSyncSnapmirrorLatency
- WriteIOPS

#### List of items removed on limiting private data access: [Learn more](#)

When the **Remove Private Data** option is enabled on Keystone Collector, the following usage information is eliminated for ONTAP. This option is enabled by default.

- Cluster Name
- Cluster Location
- Cluster Contact
- Node Name
- Aggregate name
- Volume Name
- QoSAdaptivePolicyGroup Name
- QoSPolicyGroup Name
- Vserver name
- Storage LUN name
- Aggregate Name
- LogicalUnit Name
- SVM Name
- AIQUMInstance IP
- FlexClone
- RemoteClusterName

## StorageGRID data collection

## Usage data collected for StorageGRID: [Learn more](#)

The following list is a representative sample of the `Logical Data` collected for StorageGRID:

- StorageGRID ID
- Account ID
- Account Name
- Account Quota Bytes
- Bucket Name
- Bucket Object Count
- Bucket Data Bytes

The following list is a representative sample of the `Physical Data` collected for StorageGRID:

- StorageGRID ID
- Node ID
- Site ID
- Site Name
- Instance
- StorageGRID storage utilization Bytes
- StorageGRID storage utilization metadata Bytes

## List of items removed on limiting private data access: [Learn more](#)

When the **Remove Private Data** option is enabled on Keystone Collector, the following usage information is eliminated for StorageGRID. This option is enabled by default.

- AccountName
- BucketName
- SiteName
- Instance/NodeName

## Telemetry data collection

## Telemetry data collected from Keystone Collector VM: Learn more

The following list is a representative sample of the telemetry data collected for Keystone systems:

- System information
  - Operating system name
  - Operating system version
  - Operating system ID
  - System hostname
  - System default IP address
- System resource usage
  - System uptime
  - CPU core count
  - System load (1 min, 5 min, 15 min)
  - Total memory
  - Free memory
  - Available memory
  - Shared memory
  - Buffer memory
  - Cached memory
  - Total swap
  - Free swap
  - Cached swap
  - Disk filesystem name
  - Disk size
  - Disk used
  - Disk available
  - Disk usage percentage
  - Disk mount point
- Installed packages
- Collector configuration
- Service logs
  - Service logs from Keystone services

## 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:

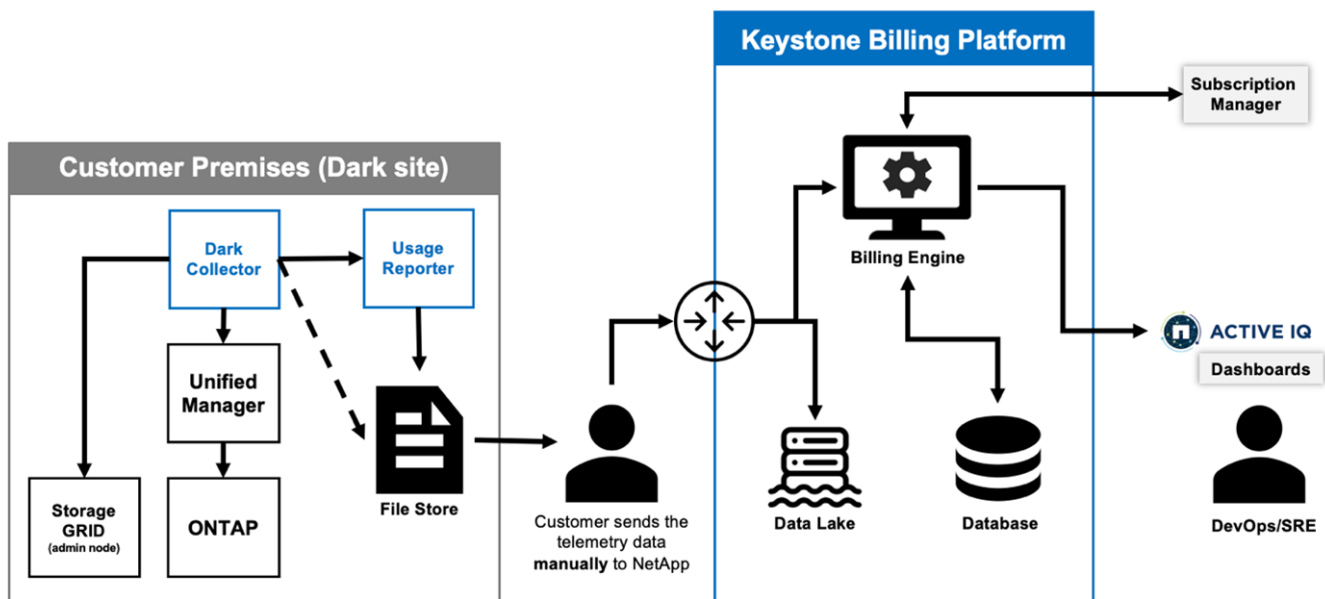
- **Local deployment:** Keystone can be configured within isolated environments independently, ensuring no need for internet connectivity or external personnel for setup access.
- **Offline operations:** All storage management capabilities with health checks and billing are available offline for operations.
- **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

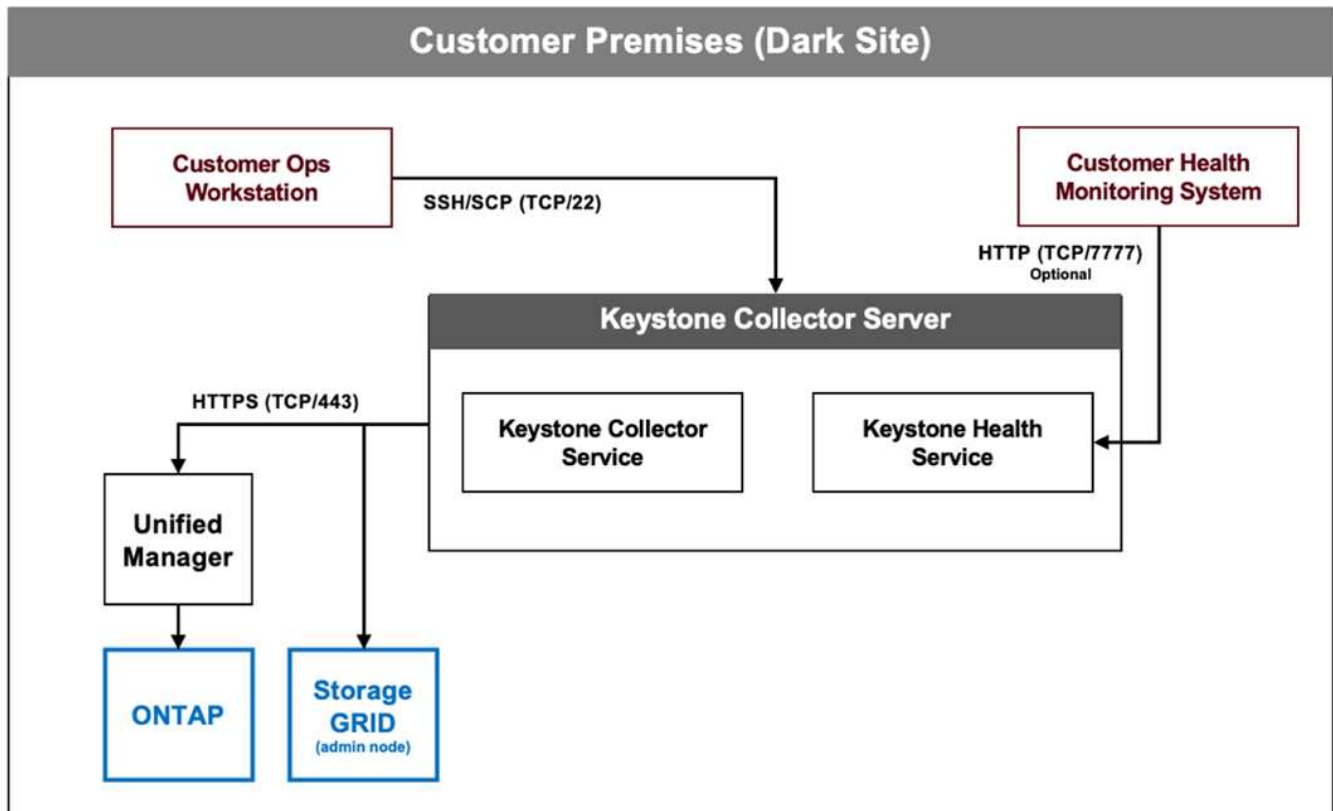
Keystone Collector is responsible for periodically collecting usage data from storage systems and exporting the metrics to an offline usage reporter and a local file store. The generated files, which are created in both encrypted and plain text formats, are then manually forwarded to NetApp by the user 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 12, or Red Hat Enterprise Linux (RHEL) 8.6, or later versions within the RHEL 8.x series
- 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 *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.



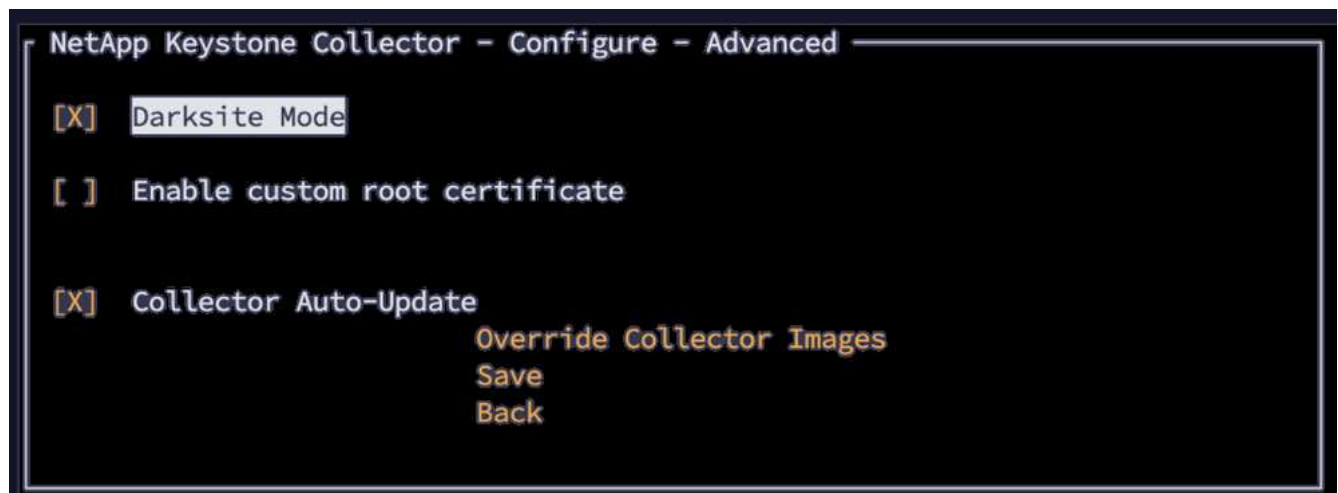
Keystone Collector provides you with the Keystone Collector Management Terminal User Interface (TUI) utility to perform configuration and monitoring activities. You can use various keyboard controls, such as the Enter and arrow keys, to select the options and navigate across this TUI.

### Steps

1. Start the Keystone Collector management TUI utility:

```
keystone-collector-tui
```

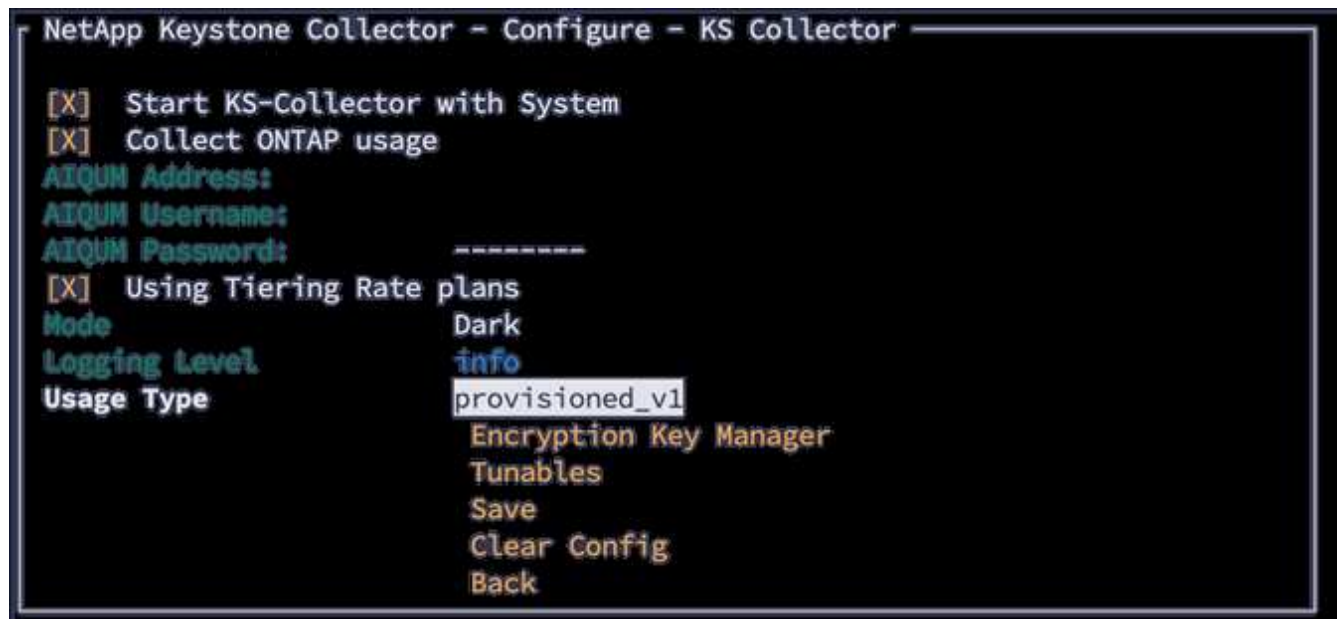
2. Go to **Configure > Advanced**.
3. Toggle the **Darksite Mode** option.



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



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



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

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

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

Generate Collector Keypair
Back
```

14. 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.

```
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. Exit the Keystone Collector management TUI by selecting **Exit to Shell** option on the home screen.

16. Retrieve the generated public key:

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

17. Send an email with this file to [ng-keystone-secure-site-upload@netapp.com](mailto:ng-keystone-secure-site-upload@netapp.com) for secure non-USPS sites, or to [ng-keystone-secure-site-usps-upload@netapp.com](mailto:ng-keystone-secure-site-usps-upload@netapp.com) for secure USPS sites.

## 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 **Export Usage** on the Keystone Collector TUI home screen.
2. Collect the files and send them to [ng-keystone-secure-site-upload@netapp.com](mailto:ng-keystone-secure-site-upload@netapp.com) for secure non-USPS sites, or to [ng-keystone-secure-site-usps-upload@netapp.com](mailto:ng-keystone-secure-site-usps-upload@netapp.com) for secure USPS sites.

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"}}
```

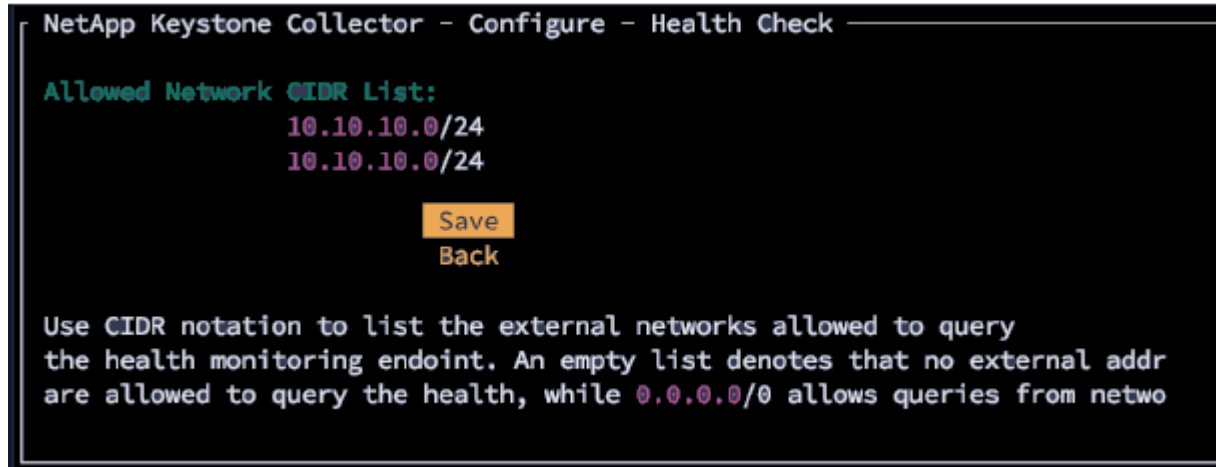
These status codes are returned:

- **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**.

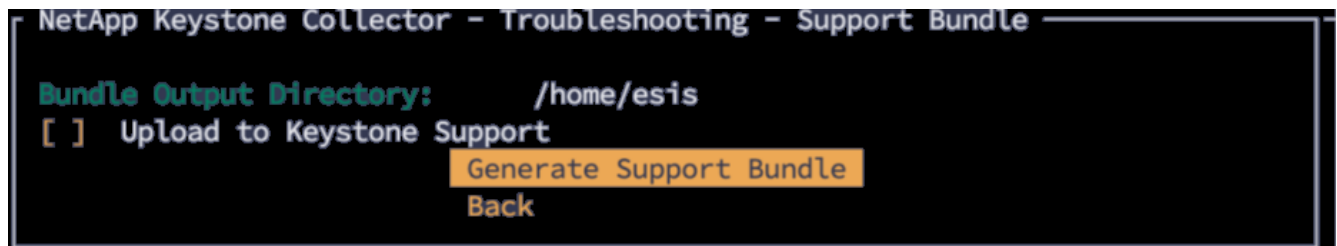


### Generate and collect support bundles

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](#).



# Manage and monitor Keystone subscriptions

## Understand the Keystone dashboard

### Learn about the Keystone dashboard

The Keystone dashboard is your go-to solution for efficiently monitoring, analyzing, and managing your Keystone subscriptions. Through the Keystone dashboard, you can achieve the following goals:

- **Monitor subscription details:** View detailed information about your Keystone subscriptions, including performance service levels, capacity usage, assets, and alerts.
- **Track capacity usage and generate reports:** Keep track of current and historical capacity usage, and generate reports to analyze subscription data and make informed decisions.
- **View subscription timeline:** Stay informed about key dates and events by monitoring the timeline of your subscriptions.
- **Manage subscriptions:** Submit requests to modify performance service levels or other subscription parameters as your needs change.
- **Analyze volumes and objects:** Gain detailed insights into the volumes and objects of your subscriptions, including their capacity at both the volume and object levels.

### Access the Keystone dashboard

You can access the Keystone dashboard through:

- **BlueXP:** Access the dashboard from **Storage > Keystone > Overview** in BlueXP. To learn more, refer to [Keystone dashboard in BlueXP](#).
- **Active IQ Digital Advisor** (also known as Digital Advisor): Access the dashboard from **General > Keystone Subscriptions** in Digital Advisor. To learn more, refer to [Keystone dashboard in Digital Advisor](#).

Note the following:

- While BlueXP and Digital Advisor offer some exclusive features, BlueXP provides administrative functionality for Keystone, allowing you to manage subscriptions and make necessary adjustments.
- You must be assigned to the **Keystone admin** role to modify subscriptions. To learn more, refer to [Learn about BlueXP access roles](#).
- Digital Advisor is integrated with BlueXP, allowing you to access all Digital Advisor features, including the Keystone dashboard, directly from BlueXP. To learn more, refer to [Digital Advisor integration with BlueXP](#).

### Keystone features in BlueXP and Digital Advisor

The following table shows the availability of features in BlueXP and Digital Advisor, helping you quickly identify the right platform for your needs:

Feature	BlueXP	Digital Advisor
<a href="#">View your subscription details</a>	Yes	Yes

Monitor current and historical capacity usage	Yes	Yes
Track subscription timeline	Yes	No
View assets associated with a Keystone subscription	Yes	Yes
View assets across multiple Keystone subscriptions	Yes	No
Modify your subscriptions (only for Keystone administrators)	Yes	No
Generate reports	Yes	Yes
View volumes and objects details	Yes	Yes
View performance metrics	No	Yes

#### Related information

- [Get started with the Keystone dashboard](#)
- [Keystone dashboard in BlueXP](#)
- [Keystone dashboard in Digital Advisor](#)

#### Get started with the Keystone dashboard

You can access the Keystone dashboard through NetApp BlueXP or Digital Advisor after subscribing to NetApp Keystone services.

## BlueXP

To log in to BlueXP, you can use your NetApp Support Site credentials or you can sign up for BlueXP using your email and a password. Learn more about [logging in to BlueXP](#).

### Steps

1. Log in to BlueXP.
2. From the BlueXP left navigation menu, select **Storage > Keystone**.

The Keystone dashboard appears.

## Digital Advisor

The Digital Advisor dashboard enables you to view the details of your Keystone subscriptions. To log in to Digital Advisor, you can use your NetApp Support Site credentials.

### Steps

1. Open a web browser, and go to the [Digital Advisor](#) login page.
2. Provide your username and password and click **Sign In**.

You can view the details of your subscription and usage, and see a summary of capacity usage against your purchased Keystone services, on the **Keystone Subscriptions** widget in the Digital Advisor dashboard. To learn more about the **Keystone Subscriptions** widget, refer to [Keystone dashboard in Digital Advisor](#).

## Related information

- [Keystone dashboard in BlueXP](#)
- [Keystone dashboard in Digital Advisor](#)
- [View your subscription details](#)

## Keystone dashboard in BlueXP

You can use the **Overview** tab to quickly determine the workloads at risk, view the capacity and expiry status of subscriptions, identify the unresolved alerts, and view the subscriptions with the highest capacity utilization. You can also view the status of your subscriptions across different versions of Keystone, highlighting any issues that need your attention.

To view the **Overview** tab, from the BlueXP left navigation menu, go to **Storage > Keystone > Overview**.

**NetApp BlueXP** Overview

Last updated: Aug 4, 2025, 2:30 PM PST

**Summary**

7 Subscriptions	5 Clusters	2 Grids	15 Nodes
-----------------	------------	---------	----------

**Expiring soon**

1 Subscription
----------------

**Open requests**

2 Requests
------------

**Capacity usage**

1 Above burst	2 Using burst	1 Underutilized
---------------	---------------	-----------------

**Top 5 subscriptions with highest capacity utilization**

Subscription	Service level	Capacity utilization
9876543210	Standard	98%
9876543210	Extreme	98%
9876543210	Data protect standard	98%
9876543210	Extreme	98%
9876543210	Extreme	98%

The **Overview** tab offers the following insights:

- **Summary:** Displays the total number of subscriptions, ONTAP clusters, StorageGRID nodes, and ONTAP nodes. Each category has a **View** button to easily navigate to detailed sections on the **Subscriptions** or **Assets** tab.
- **Expiring soon:** The number of subscriptions expiring within 6 months. Click **View** to see these subscriptions in the **Subscriptions** tab.
- **Open requests:** The total number of open service requests.
- **Capacity usage:** The capacity consumption status for subscriptions that are above burst, using burst, and underutilized. Each category includes a **View** button to navigate to the **Subscriptions** tab with relevant

filters applied.

- **Top 5 subscriptions with highest capacity utilization:** Displays a table of the top five Keystone subscriptions with the highest percentage of capacity utilization. You can click the subscription number from the **Subscription** column to get detailed insights.

## Related information

- [Learn about the Keystone dashboard](#)
- [Get started with the Keystone dashboard](#)
- [Keystone dashboard in Digital Advisor](#)
- [View your subscription details](#)
- [View your current consumption details](#)
- [View consumption trends](#)

## Keystone dashboard in Digital Advisor

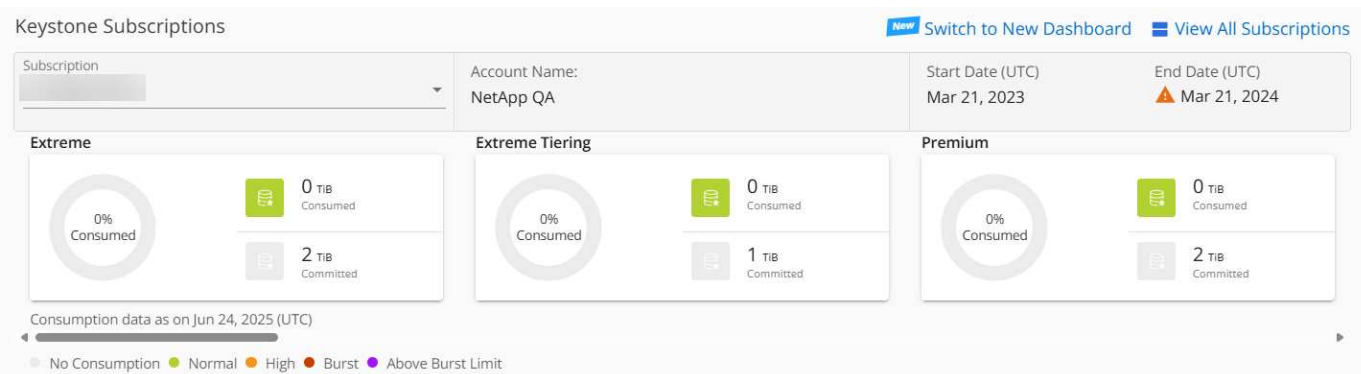
As a NetApp Keystone STaaS subscriber, you can get an overview of your subscriptions on the **Keystone Subscriptions** widget of the Digital Advisor dashboard.

You can search for a specific Keystone subscription by entering the first three characters of a customer or watchlist name, or the Keystone subscription number. For information about how to search Keystone STaaS subscriptions by watchlists, see [Search by using Keystone watchlists](#).

Digital Advisor offers a unified dashboard that gives insights into various levels of your subscription data and usage information through the **Switch to old/new dashboard** button.

### Default (old) dashboard

You can see your customer name and subscription number, account name, start and end dates of the subscription, and the capacity usage graphs as per your subscribed performance service levels. You can see the collection timestamp of the consumption data in UTC time.



### Alternative (new) dashboard

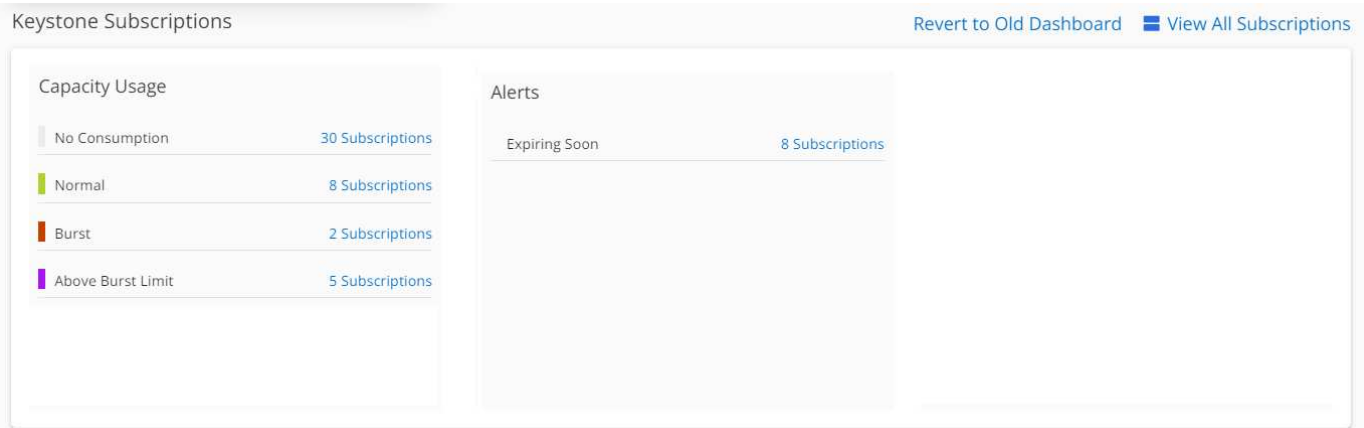
You can see the breakup of the capacity usage as per your subscriptions, and warnings and alerts that require immediate attention or action. The information appears selectively, depending on your subscriptions and the status of your usage. You can view this information:

- **Capacity usage:** Consumption data such as no usage, consumption exceeding 80% of the committed capacity, burst usage, and consumption above the burst capacity.

- **Alerts:** You see alerts for various scenarios if they are applicable to you.



Click the **Subscriptions** link to view the list of filtered subscriptions in the **Subscriptions** tab.



You can click **View All Subscriptions** to view the usage details and alerts on your volumes on the **Keystone Subscriptions** page.

The details of the subscriptions, usage charts for each performance service level, and volume details are displayed in the different tabs on the **Keystone Subscriptions** screen.



Capacity consumption in Keystone subscriptions is displayed in TiBs on the dashboards and reports, and is rounded off to two decimal places. If the usage is less than 0.01 TiB, then the value is shown as 0 or No Usage. The data on these screens is displayed in UTC time (server timezone). When you enter a date for query, it is automatically considered to be in UTC time. To learn more about usage metrics, refer to [Metrics measurement](#). For information about different capacities used in Keystone, see [Supported storage capacities](#).

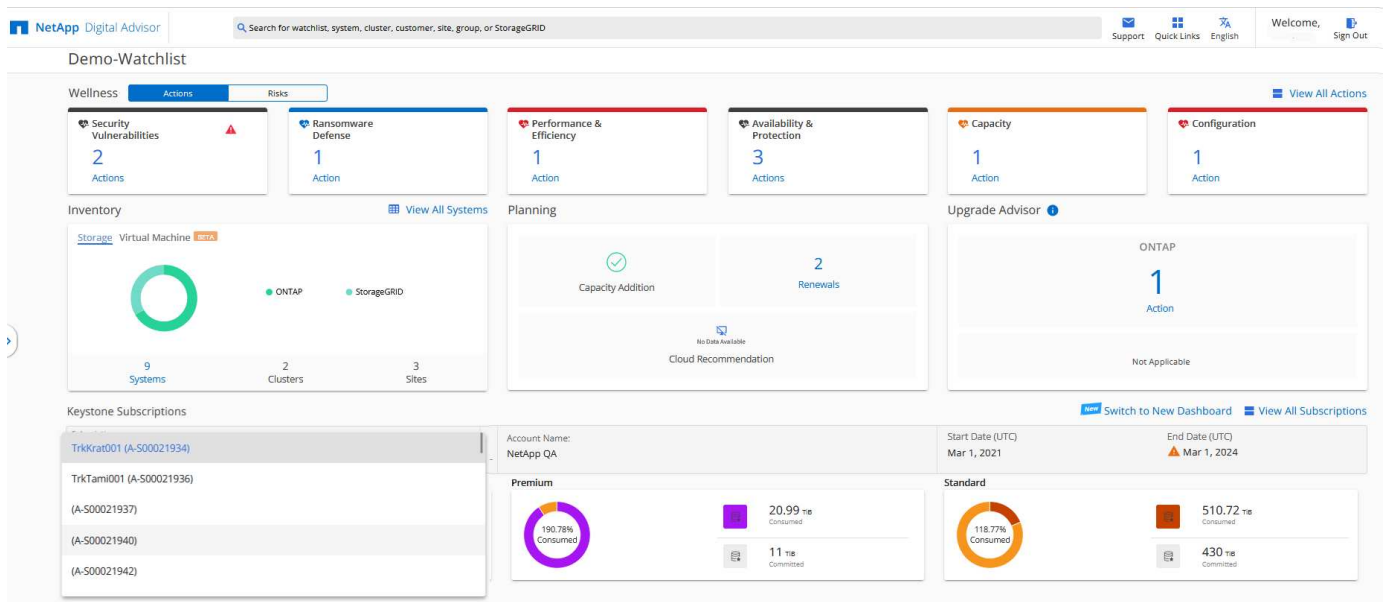
### Search by Keystone watchlists

Watchlist is a feature available in Digital Advisor. For information, see [Understand watchlist](#). For information about creating watchlists, see [Create a watchlist](#).

You can create watchlists for customers or subscription numbers and search for a Keystone subscription using the first three characters of a subscription number or watchlist name on the Digital Advisor screen. When you search by a watchlist name, you can view the customers and their subscriptions in the **Subscription** drop-down list on the **Keystone Subscriptions** widget.



A search by watchlists retrieves the list of subscriptions on the old dashboard. If a watchlist consists of subscription numbers, only the **Keystone Subscriptions** widget is displayed on the Digital Advisor dashboard.



## Related information

- [Get started with Keystone dashboard](#)
- [Keystone dashboard in BlueXP](#)
- [View your subscription details](#)
- [View your current consumption details](#)
- [View consumption trends](#)

## Search Keystone data, generate reports, and view alerts

You can search and filter your data, generate reports for subscriptions and usage, and view alerts to stay informed about your storage environment.

### Search and filter data from BlueXP

In BlueXP, you can search and filter Keystone data based on the column parameters available in the table within a tab. For example, in the **Subscriptions** sub-tab under the **Subscriptions** tab, you can filter data by entering the Keystone version in the search box. Similarly, in the **Volumes in clusters** tab under the **Assets** tab, you can filter volumes by entering volume name in the search box.

You can refine your searches by using the advanced filter option where available. For example, in the **Subscriptions** sub-tab, you can filter data by Keystone version, billing period, highest capacity, and days to subscription expiry, and in the **Volumes in clusters** tab, you can filter by volume name, cluster name, volume type, and more. Multiple filters can be applied simultaneously to narrow down your results with precision.

## Generate reports from BlueXP or Digital Advisor

The details are generated in CSV format that you can save for future use and comparison.

In Digital Advisor, you can generate and view a consolidated report for your subscriptions, historical usage, burst usage, performance, assets, and volumes and objects. To do this, select **Keystone Subscriptions** as the report type from the Report feature in Digital Advisor. You can generate these reports at the customer, cluster, watchlist, or subscription level.

The report is generated in Excel format, with each type of information, such as subscription details or usage history, displayed on separate sheets. These sheets are named according to the tabs on the **Keystone Subscriptions** page for easy viewing. You can save the report for future use.

To learn more about generating reports, refer to [Generate custom reports](#).

## View subscription insights



## View details about your Keystone subscriptions

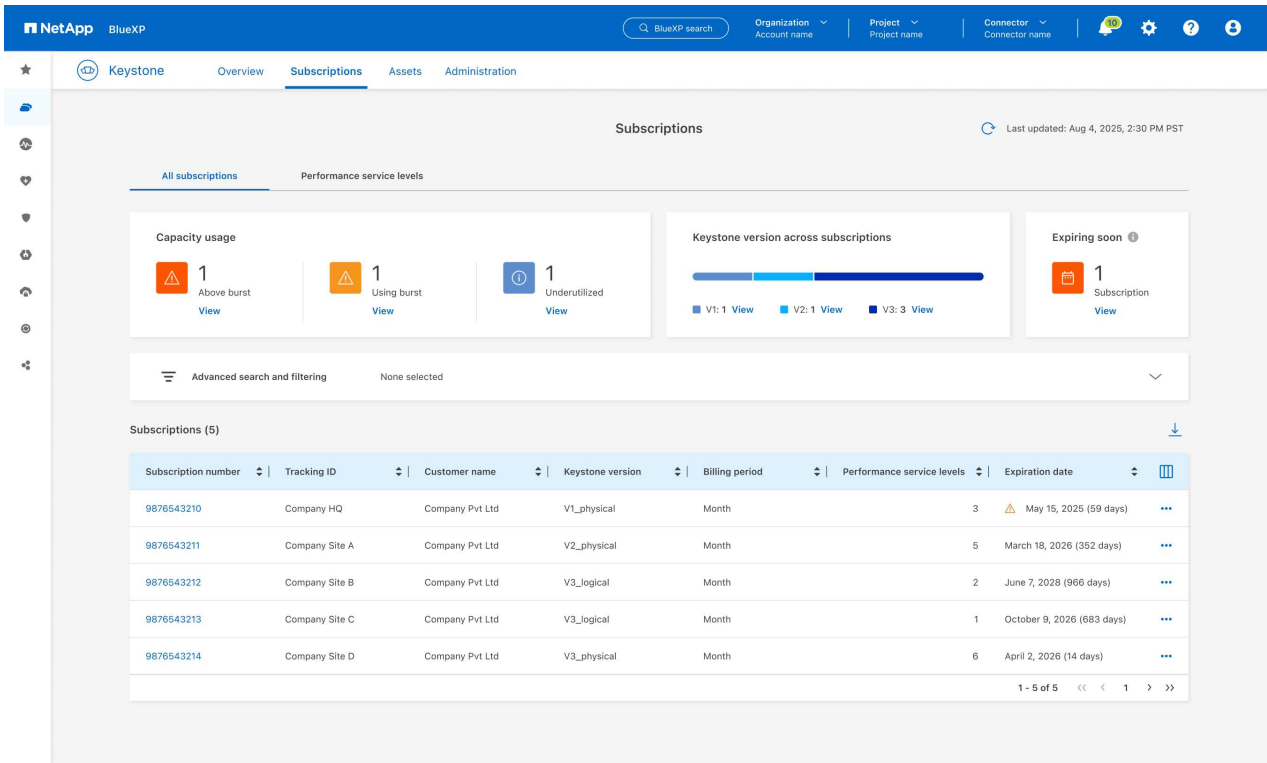
You can view a list of all your subscriptions from the **Subscriptions** tab in both BlueXP and Digital Advisor. This tab provides easy-to-understand insights based on your subscription status and usage, helping you stay informed and take action when needed.

## BlueXP

The **Subscriptions** tab in BlueXP is divided into two sections: **Subscriptions** and **Performance service levels**. Each section offers specific insights to help you manage and monitor your Keystone subscriptions. To view detailed information for your subscriptions, follow these steps:

### Steps

1. From the BlueXP left navigation menu, go to **Storage > Keystone > Subscriptions**.




You see the key metrics such as capacity usage, subscription expiry status, and Keystone version across subscriptions. To learn more, refer to [Keystone dashboard in BlueXP](#).

You can see the following details from the table:

- **Subscription number:** The subscription number of the Keystone subscription assigned by NetApp.
- **Tracking ID:** The tracking ID assigned at the time of subscription activation. This is a unique ID for each subscription and site, used for tracking the subscription.
- **Customer name:** The name of the customer associated with the Keystone subscription.
- **Linked subscriptions:** If you have any secondary subscriptions linked to your primary subscription, this column lists the linked subscription numbers for the primary subscription. This subscription number can be of your primary or secondary (linked) subscription.
- **Keystone version:** The version of the Keystone service that is being used for the subscription. The rate plan rules for performance service levels may differ between subscription versions. To learn more about version v1, refer to [Keystone subscription services | Version 1 documentation](#).
- **Billing period:** The invoicing period of the subscription.
- **Performance service levels:** The number of rate plans associated with the subscription, with each rate plan corresponding to a specific performance service level and committed capacity.

- **Highest capacity:** The maximum capacity consumed within the subscription.
- **Days to subscription expiry:** The number of days remaining until the subscription expires.



You can customize the columns displayed in the table using the column selector  icon. For certain fields and columns, you might see information or warning icons and tooltips that provide you with additional information about the data.

2. You can select the **Performance service levels** sub-tab to view the performance service levels across all subscriptions.

The screenshot shows the NetApp BlueXP interface. The top navigation bar includes the NetApp logo, BlueXP, a search bar, and dropdown menus for Organization, Project, and Connector. The main navigation pane on the left has tabs for Overview, Subscriptions, Assets, and Administration. The Subscriptions tab is active, showing a 'Performance service levels' sub-tab. The main content area displays two summary cards: 'Performance service levels across subscriptions' and 'Provisioning consistency across subscriptions'. Below these is an 'Advanced search & filtering' section. The main table, titled 'Performance service levels (10)', lists various subscriptions with columns for Customer, Subscription number, Performance service level, Volumes, Protected, Provisioned capacity, Committed capacity, and Consumed capacity.

Customer	Subscription number	Performance service level	Volumes	Protected	Provisioned capacity	Committed capacity	Consumed capacity
Company Pvt Ltd	9876543210	Value	27	0 View	248.32 TiB	250 TiB	181.55 TiB
Company Pvt Ltd	9876543210	Premium	28	0 View	38.27 TiB	40 TiB	38.27 TiB
Company Pvt Ltd	9876543210	Data-Protect Premium	0	0 View	0 TiB	20 TiB	19.14 TiB
Company Pvt Ltd	9876543210	Advanced Data-Protect Premium	0	0 View	0 TiB	20 TiB	19.14 TiB
Company Pvt Ltd	9876543212	Premium	28	0 View	38.27 TiB	40 TiB	38.27 TiB
Company Pvt Ltd	9876543212	Data-Protect Premium	0	0 View	0 TiB	20 TiB	19.14 TiB

- **Performance service levels across subscriptions:** Displays the number of performance service levels across the subscriptions.
- **Provisioning consistency across subscriptions:** Shows the counts for over-provisioned and under-provisioned performance service levels.

You can see the listing of performance service levels, including key details such as the name of the customer, subscription number, type of performance service level, and total number of volumes. The table also displays the count of protected volumes, the total committed, consumed, provisioned, available capacity (with and without burst), and accrued burst capacity.

## Digital Advisor

To view your subscriptions in Digital Advisor, follow these steps:

### Steps

1. From the Digital Advisor left navigation pane, go to **General > Keystone Subscriptions > Subscriptions**.

You can view all your subscriptions here, with detailed insights for each one.

Subscriptions

Current Consumption

Consumption Trend

Volumes & Objects

Assets

Performance

Clear Filters

View Usage Indicators






Download CSV

<input type="checkbox"/>	Subscription Number	<input type="checkbox"/>	Linked Subscriptions	<input type="checkbox"/>	Tracking ID	<input type="checkbox"/>	Usage Type	<input type="checkbox"/>	Billing Period	<input type="checkbox"/>	Start Date (UTC)	<input type="checkbox"/>	End Date (UTC)
<input type="checkbox"/>	A-500022706	--			QaAutoMonthly		Provisioned (v1)		Month		January 24, 2023	▲	January 24, 2023
<input type="checkbox"/>	A-500018891	--			test		Logical (v1)		Month		December 1, 2021		December 1, 2021
<input type="checkbox"/>	A-500027074	1921550700-PROD			Test-Sub-CI-01		CVO (v2)		Month		August 19, 2024	▲	August 19, 2024
<input type="checkbox"/>	A-500027051	--			Test-Subs-004		Logical (v2)		Annual	📊	August 4, 2024	▲	August 4, 2024
<input type="checkbox"/>	A-500026418	--			TrackSG002				Annual	📊	March 19, 2024	▲	March 19, 2024
<input type="checkbox"/>	A-500027587	--			v3_02		Logical (v3)		Month		April 29, 2025		April 29, 2026
<input type="checkbox"/>	A-500027643	--			v3_All		Logical (v3),Physical (v3)		Month		May 27, 2025		May 27, 2026
<input type="checkbox"/>	A-500027641	--			V3_mcc_SiteA		Logical (v3)		Month		May 27, 2025		May 27, 2026

For certain fields and columns, you might see information or warning icons and tooltips that provide you with additional information about the data.

- **Subscription Number:** The subscription number of the Keystone subscription assigned by NetApp.
- **Linked Subscriptions:** This column is optionally available to you. If you have any secondary subscriptions linked to your primary subscription, this column lists the linked subscription numbers for the primary subscription. This subscription number can be of your primary or secondary (linked) subscription.
- **Tracking ID:** The tracking ID assigned at the time of subscription activation. This is a unique ID for each subscription and site.
- **Usage Type:** You might have subscribed to multiple Keystone versions. The rate plan rules for performance service levels may differ between subscription versions. By looking at the value in this column, you know whether the usage type is billed as per the provisioned, physical, or logical usage. To learn more about version 1, refer to [Keystone subscription services | Version 1 documentation](#).
- **Billing Period:** The invoicing period of the subscription.
- **Start Date:** The start date of the subscription.
- **End Date:** The end date of the subscription. If you have a monthly-billable subscription that renews automatically every month, you see `Month-on-month` instead of the end date. Based on this date, you might see notifications for subscriptions that are about to end or have auto-renewal policies attached.
- **Usage Status:** Displays the usage indicator to indicate whether the consumption is within or exceeding the subscription limit. You can sort the list by this column if you want to view the highest consumption records.
- : Clicking this icon for a subscription opens the **Current Consumption** tab with the usage details of that subscription.
- : Clicking this icon opens the **Consumption Trend** tab where you can see the historical usage data for each performance service level included in this subscription.

You can refer to the usage indicators to check the usage status of each subscription:

-  **No consumption:** No capacity usage recorded against the committed capacity of the performance service level.
-  **Normal:** The consumption is normal.
-  **High:** Maximum consumption, that is the usage is about to reach 100% or more of the committed capacity.
-  **Burst:** The consumption is within the burst limit. The burst consumption is the consumption that tops the 100% committed capacity of a performance service level, and is within the agreed-upon burst usage limit.
-  **Above burst limit:** Indicates consumption above the agreed-upon burst limit.

## Related information

- [Understand the Keystone dashboard](#)
- [View your current consumption details](#)
- [View consumption trends](#)
- [View your subscription timeline](#)
- [View your Keystone subscription assets](#)
- [View assets across your Keystone subscriptions](#)
- [View volumes & objects details](#)

## View the current consumption of your Keystone subscriptions

You can gain insights into your subscription usage by viewing detailed information such as committed capacity, consumed capacity, and available capacity, with the current consumption status displayed and segregated by performance service levels.

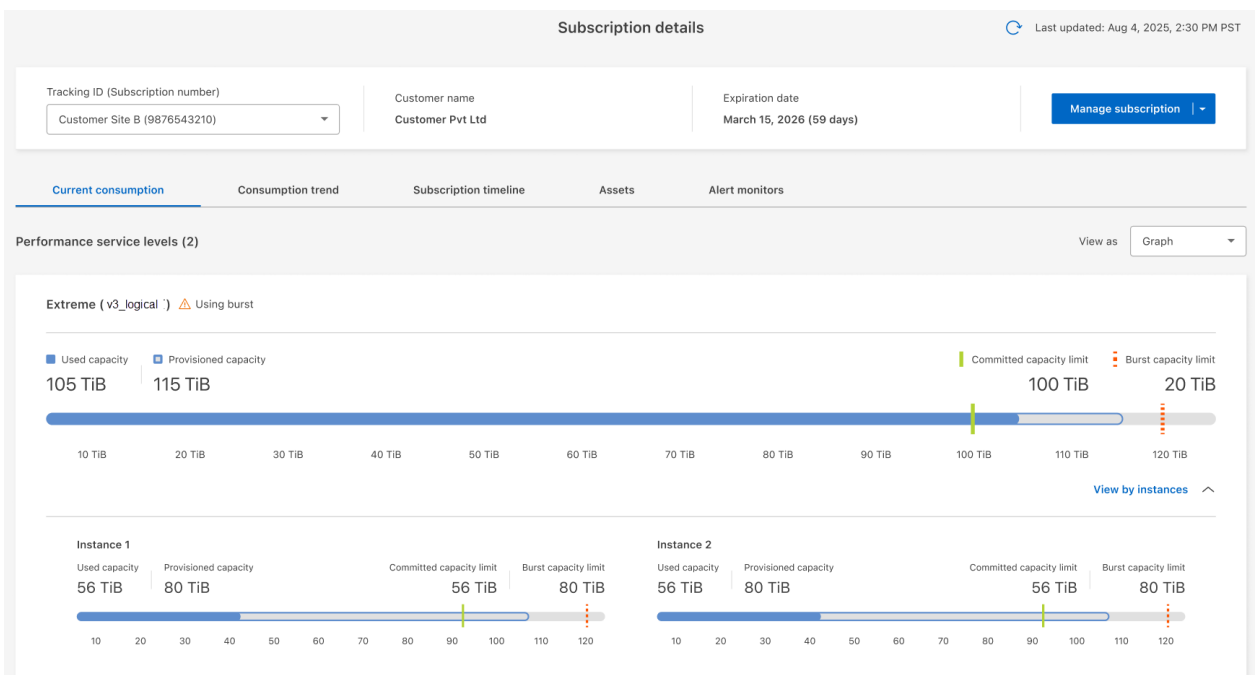
To view the current consumption status of your subscriptions through BlueXP or Digital Advisor, follow these steps:

## BlueXP

### Steps

1. From the BlueXP left navigation menu, select **Storage > Keystone > Subscriptions**.
2. Select the subscription number in the **Subscription number** column of the table to view the current consumption.

You are redirected to the **Current consumption** tab.



For the selected subscription, you can view consumption details in either table or graphical format using the **Table** or **Graph** option from the **View as** dropdown. In the graphical view, you can see the current consumption per performance service level, including used capacity, provisioned capacity, committed capacity limit, and burst capacity limit.



If a performance service level has multiple instances, you can expand **View by instances** in either view to see current consumption details for each instance separately. For example, if you have two instances of the Extreme performance service level within a subscription, each instance will display its own committed, consumed, and available capacities separately.

In the table view, you can see details like maximum capacity consumed and days remaining until expiration. As part of monitoring your subscription usage, you can view the performance service level name, consumption status, committed and used capacities, provisioned and burst capacities, available capacity, and volumes. You can customize the table using the column selector icon.

Subscription detailsLast updated: Aug 4, 2025, 2:30 PM PST

Tracking ID (Subscription number)  
Customer Site B (9876543210)

Customer name  
Customer Pvt Ltd

Expiration date  
March 15, 2026 (59 days)

Manage subscription

Current consumption

Consumption trend

Subscription timeline

Assets

Alert monitors

Performance service levels (2)

View asTable

Service level	Consumption status	Committed capacity	Total used capacity	Provisioned capacity	Burst capacity	Available capacity	Keystone version	Available capacity with burst
Extreme	Above burst	100 TiB	125 TiB	130 TiB	20 TiB	0 TiB	V3_logical	0 TiB
Standard	Using burst	100 TiB	105 TiB	105 TiB	20 TiB	0 TiB	V3_logical	15 TiB

Instance	Capacity usage	Committed capacity	Total used capacity	Provisioned capacity	Burst capacity	Available capacity	Available capacity with burst
Instance 1	38%	50 TiB	50 TiB	50 TiB	20 TiB	0 TiB	0 TiB
Instance 2	70%	50 TiB	55 TiB	55 TiB	20 TiB	0 TiB	0 TiB

1 - 2 of 2

Digital Advisor

Steps

1. From the Digital Advisor left navigation pane, go to **General > Keystone Subscriptions > Current Consumption**.

2. Select or search the required subscription number from the **Subscription** dropdown list.

Subscription

Start Date (UTC)  
January 3, 2024

End Date (UTC)  
January 3, 2026

Billing Period  
Annual

Current Consumption per Service Level

No Consumption
Normal
High
Burst
Above Burst Limit

Service Level	Committed	Consumed	Current Burst	Available	Available With Bur
Extreme	1.02 TiB	0 TiB	0 TiB	1.02 TiB	1.22 TiB
Premium	0 TiB	0 TiB	0 TiB	0 TiB	0 TiB
Standard	0 TiB	0 TiB	0 TiB	0 TiB	0 TiB
Value	0 TiB	0 TiB	0 TiB	0 TiB	0 TiB
Data-Protect Extreme	0 TiB	0 TiB	0 TiB	0 TiB	0 TiB
Data-Protect Premium	0 TiB	0 TiB	0 TiB	0 TiB	0 TiB
Data-Protect Standard	0 TiB	0 TiB	0 TiB	0 TiB	0 TiB

For the selected subscription, you can view details, such as the start and end dates of the subscription, and the billing period, such as monthly or annual. As a part of the subscription usage, you can view the performance service level name, committed, consumed, available capacities, and current and accrued burst usage (in TiB). Specific performance service levels that record higher consumption are highlighted. You can also view warnings and alerts generated for your volumes.



If a performance service level has multiple instances, you can select the **Instances** tab to see current consumption details for each instance. For example, if you have two instances of the Extreme performance service level within a subscription, each instance will display its own committed, consumed, and available capacities separately. To learn more about the performance service levels, see [Performance service levels in Keystone](#).

Coupled with the current consumption, you might want to view the historical usage data for comparison. Click the **View Historical Data** button to navigate to the **Consumption Trend** tab to view the historical data for the same subscription.

For information about your Keystone storage services and the relevant performance service levels, see [Performance service levels in Keystone](#).

### Related information

- [Understand the Keystone dashboard](#)
- [View your subscription details](#)
- [View consumption trends](#)
- [View your subscription timeline](#)
- [View your Keystone subscription assets](#)
- [View assets across your Keystone subscriptions](#)
- [View volumes & objects details](#)

## View consumption trends of your Keystone subscriptions

You can monitor your subscription usage by viewing historical data of your Keystone subscriptions for a specific period of time. This allows you to gain valuable insights into your usage patterns.

You can view historical data of your Keystone subscriptions through BlueXP or Digital Advisor:



## BlueXP

### Steps

1. From the BlueXP left navigation menu, select **Storage > Keystone > Subscriptions**.
2. Select the subscription number in the **Subscription number** column.

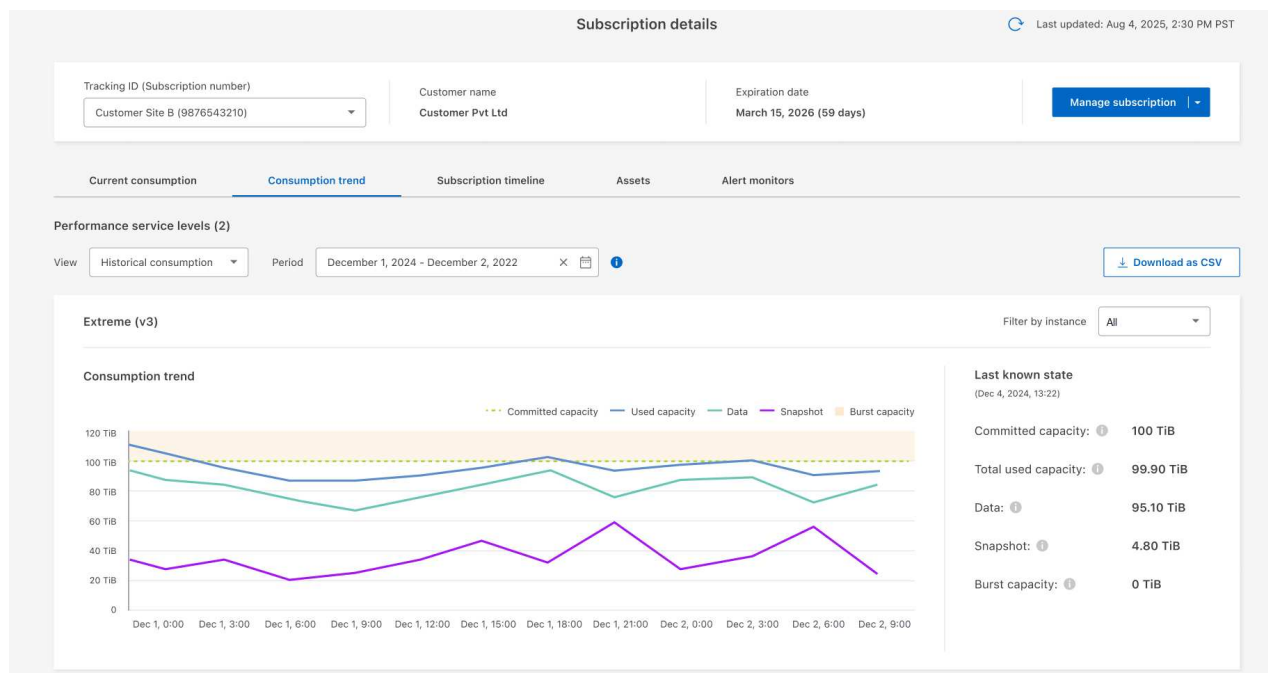
You are redirected to the **Current consumption** tab.

3. Select the **Consumption trend** tab.
4. Select **Historical consumption** from the **View** dropdown and choose the time range using the calendar icon in the **Period** field to analyze capacity usage trends.

The historical consumption data for each performance service level is displayed in a line graph based on the selected time range.



You can select **Accrued burst** from the **View** dropdown if you want to view the historical burst usage data for which invoices have been generated. You can use this data to analyze the billed usage reflected in your invoice. To learn more, refer to [View accrued burst](#).



The line graph displays historical consumption data and allows users to analyze trends over a selected date range. The graph shows metrics such as used capacity (total storage capacity, including both data and snapshot data), data (storage capacity used by user data), and snapshot (storage capacity used by snapshot data), along with committed and burst capacity. The date and time of each data point are displayed at the bottom of the graph. Based on the date range of your query, the usage charts show up to 30 data collection points. You can hover your mouse cursor over the graph to view the usage breakdown at each data collection point.



If a performance service level has multiple instances, you can filter by instance to view historical data for each one separately.

You can also view a summary of current consumption alongside historical consumption to get a clear

understanding of your usage.

## Digital Advisor

### Steps

1. Click **General > Keystone Subscriptions > Consumption Trend**.
2. Select the required subscription for which you want to view the details. The first subscription in your account name is selected by default.
3. Select **Consumption Trend** if you want to view the historical data and analyze the capacity usage trend.



You can select **Invoiced Accrued Burst** if you want to view the historical burst usage data for which invoices have been generated. You can use this data to analyze the billed usage reflected in your invoice. To learn more, refer to [View accrued burst](#).

4. Select the time range from the calendar icons in the **From Date** and **To Date** fields. Select the date range for the query. The date range can be the beginning of the month or the subscription start date to the current date or the subscription end date. You cannot select a future date.

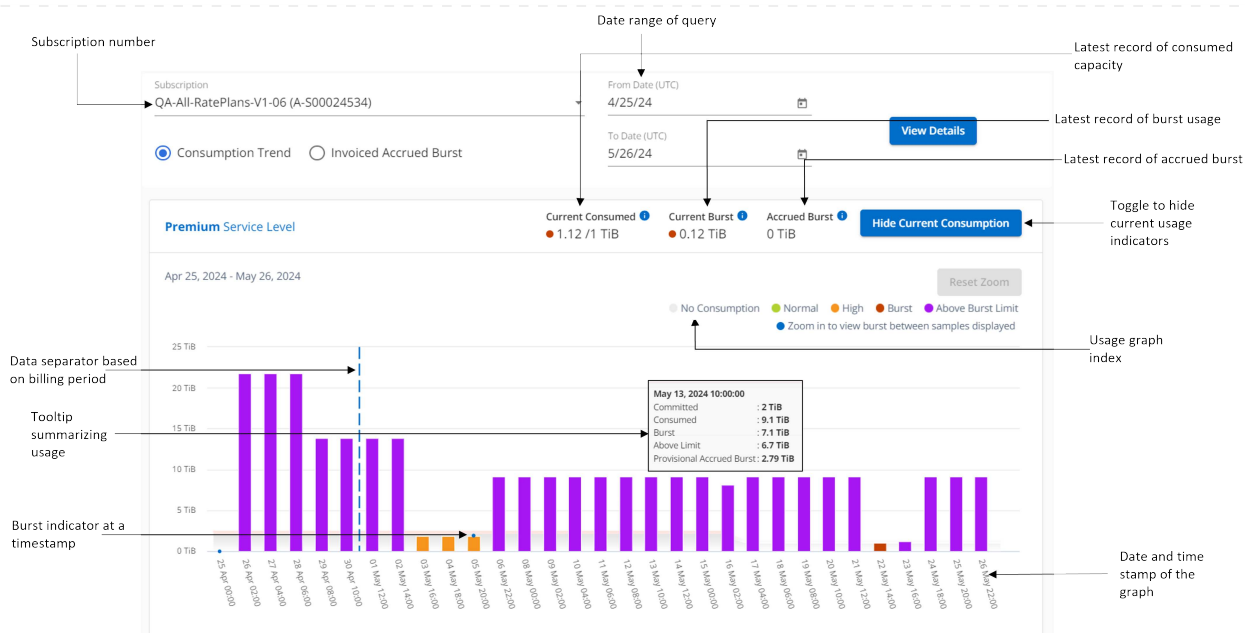


For optimal performance and user experience, limit the date range of your query to three months.

5. Click **View Details**. The historical consumption data of the subscription for each performance service level is displayed based on the selected time range.

The bar charts display the performance service level name and the capacity consumed against that performance service level for the date range. The date and time of the collection are displayed at the bottom of the chart. Based on the date range of your query, the usage charts are displayed in a range of 30 data collection points. You can hover your mouse cursor over the charts to view the usage breakdown in terms of committed, consumed, burst, and above the burst limit data at that data collection point.

The bar charts display short-term bursts, and you can view these bursts by using the zoom-in feature. When a short-term burst is present, it is indicated by a blue dot on the corresponding bar or directly on the x-axis if no data is consumed. To view the details, click and hold on the bar or the x-axis where the blue dot appears, then drag the cursor across the chart to select the desired time interval, and release to confirm your selection. This action zooms into the data, providing a more granular view of the capacity used at that performance service level for the selected interval. You can click the **Reset Zoom** button to return to the original chart view.



Monthly data across the charts is separated by a vertical line.



A blank chart indicates that there was no data available in your environment at that data collection point.

You can click the toggle button **Show Current Usage** to view the consumption, burst usage, and accrued burst data for the current billing period. These details are not based on the date range of the query.

- **Current Consumed:** Indicator for the consumed capacity (in TiB) defined for the performance service level. This field uses specific colors:
  - No color: Burst or above burst usage.
  - Grey: No usage.
  - Green: Within 80% of the committed capacity.
  - Amber: 80% of the committed to the burst capacity.
- **Current Burst:** Indicator for the consumed capacity within or above the defined burst limit. Any usage within the burst limit for your subscription, for example, 20% above the committed capacity is within the burst limit. Further usage is considered as usage above the burst limit. This field displays specific colors:
  - No color: No burst usage.
  - Red: Burst usage.
  - Purple: Above the burst limit.
- **Accrued Burst:** Indicator of the total burst capacity (in TiB) accumulated during each 2-minute interval within a month for the current billing cycle.

## Accrued burst computation

The accrued burst usage for an entire month is calculated as this:

$$[\text{sum of bursts in month} / ((\text{days in month}) \times 24 \times 60)] \times \text{interval duration}$$

You can calculate the accrued burst for short periods, such as every two minutes, using this:

$$[\text{burst} / ((\text{days in month}) \times 24 \times 60)] \times \text{interval duration}$$

The burst is the difference between the consumed capacity and the committed capacity. For example, with a 30-day in month, if the consumed capacity reaches 120 TiB and the committed capacity is 100 TiB for a 2-minute interval, this results in a burst capacity of 20 TiB, equating to an accrued burst usage of 0.000925926 TiB for that interval.

**View accrued burst**

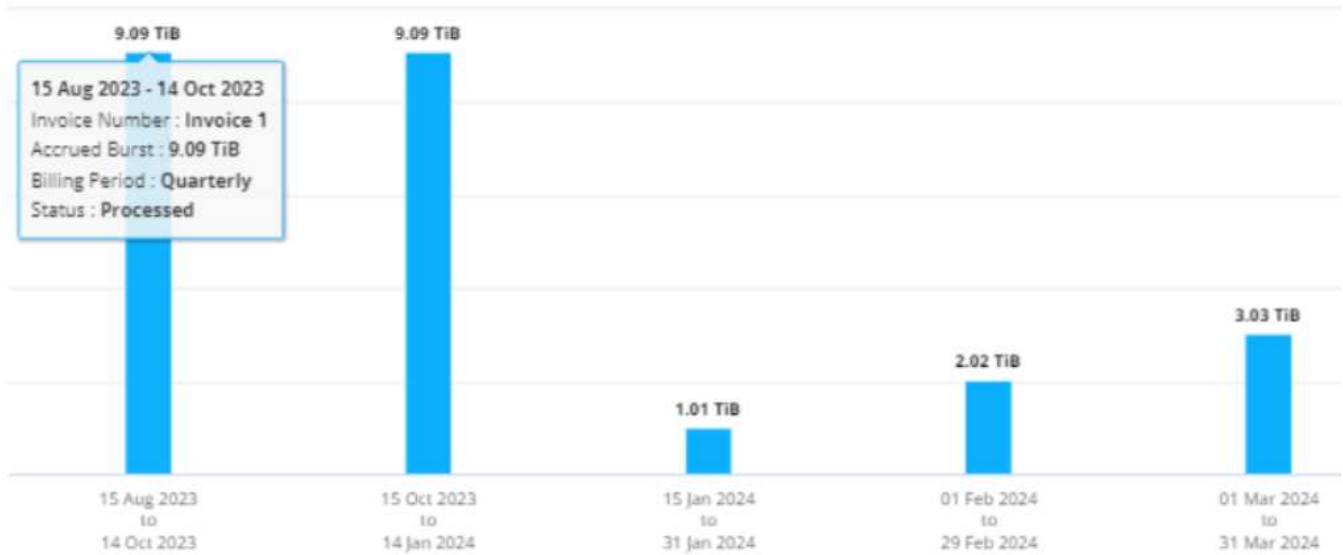
You can view the accrued burst data usage through BlueXP or Digital Advisor. If you have selected **Accrued burst** from the **View** dropdown in the **Consumption trend** tab in BlueXP, or the **Invoiced Accrued Burst** option from the **Consumption Trend** tab in Digital Advisor, you can see accrued burst data usage on a monthly or quarterly basis, depending on your selected billing period. This data is available for the last 12 months that have been billed, and you can query by the date range for up to past 30 months. Bar charts display the invoiced data, and if the usage has not yet been billed, it will be marked as *Pending* for that period.



The invoiced accrued burst usage is calculated per billing period, based on the committed and consumed capacity for a performance service level.

For a quarterly billing period, if the subscription starts on a date other than the 1<sup>st</sup> of the month, the quarterly invoice will cover the subsequent 90-day period. For example, if your subscription starts on August 15, the invoice will be generated for the period from August 15 to October 14.

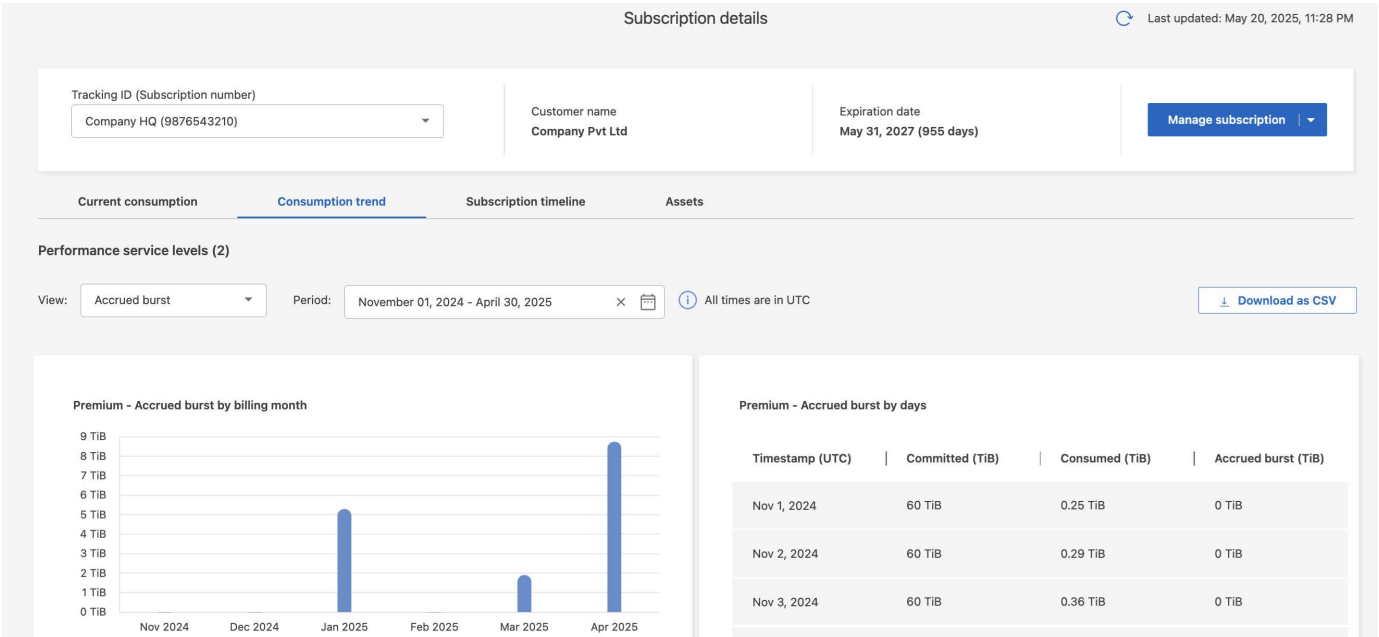
If you switch from quarterly to monthly billing, the quarterly invoice will still cover the 90-day period, with two invoices generated in the last month of the quarter: one for the quarterly billing period and another for the remaining days of that month. This transition allows the monthly billing period to start on the 1<sup>st</sup> of the following month. For example, if your subscription starts on October 15, you will receive two invoices in January—one for October 15 to January 14 and another for January 15 to 31—before the monthly billing period begins on February 1.

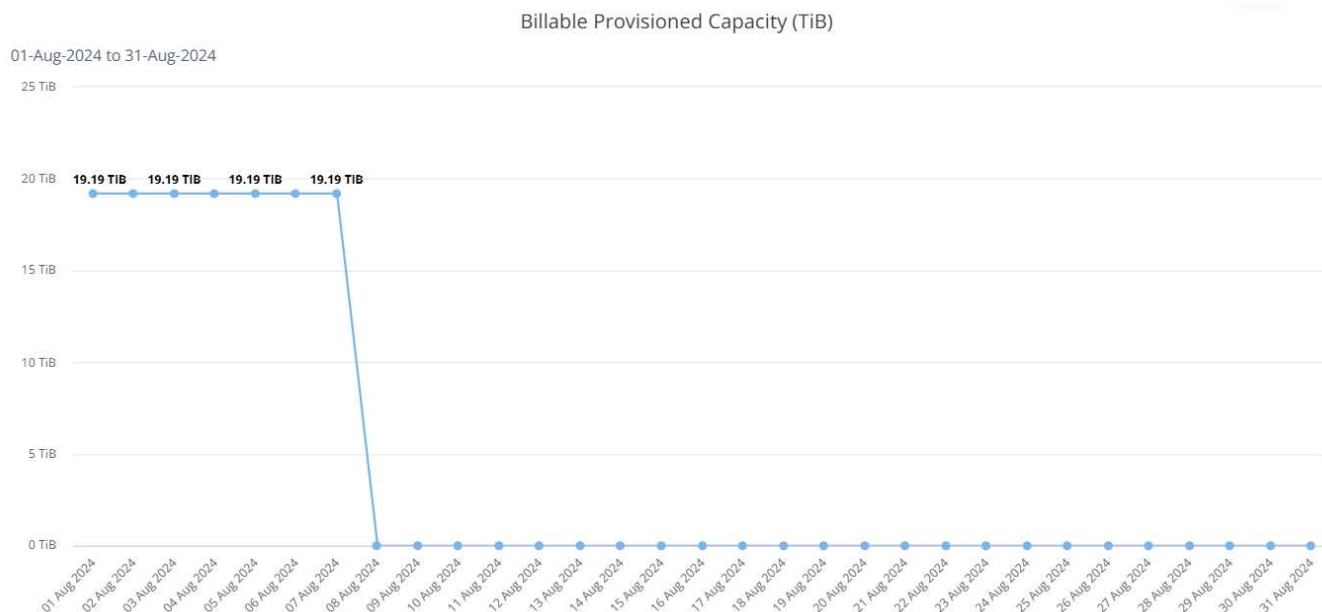


This functionality is available in a preview-only mode. Contact your KSM to learn more about this feature.

View daily accrued burst data usage

You can view daily accrued burst data usage for a monthly or quarterly billing period through BlueXP or Digital Advisor. In BlueXP, the **Accrued burst by days** table provides detailed data including the timestamp, committed, consumed, and accrued burst capacity if you select **Accrued burst** from the **View** dropdown in the **Consumption trend** tab.





You can switch to a table view by clicking the **Table** option at the top right corner of the graph. The table view provides detailed daily usage metrics, including performance service level, timestamp, committed capacity, consumed capacity, and billable provisioned capacity. You can also generate a report of these details in CSV format for future use and comparison.

## View the timeline of your Keystone subscriptions

The Keystone dashboard in BlueXP provides a timeline view of your Keystone subscriptions, displaying events such as activation, modification, and renewal dates. This timeline view is not available in Digital Advisor.

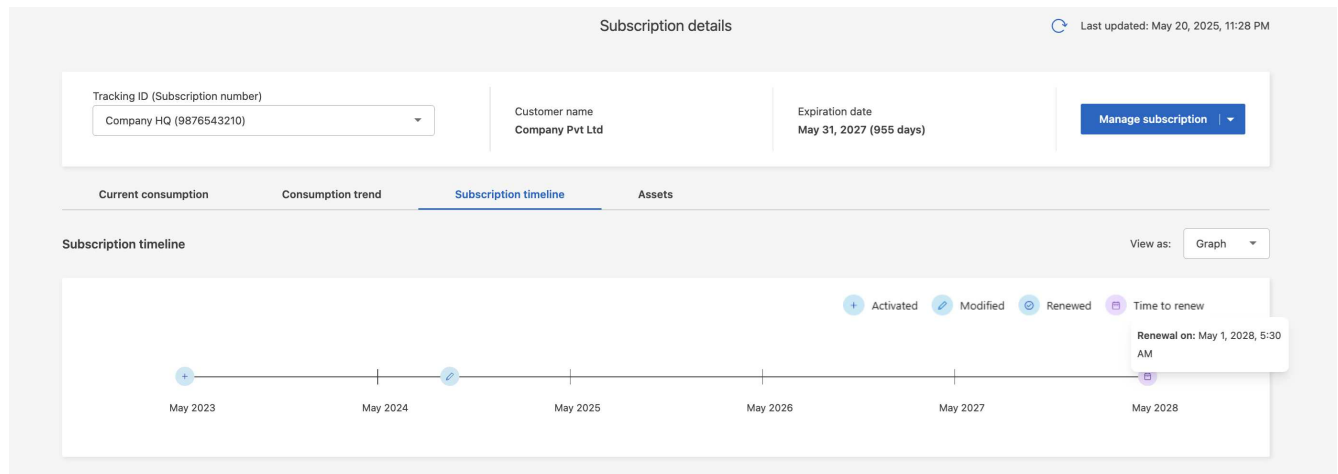
To view the subscription timeline, follow these steps:

### Steps

1. From the BlueXP left navigation menu, select **Storage > Keystone > Subscriptions**.
2. Select the subscription number in the **Subscription number** column to view the subscription timeline.

You are redirected to the **Current consumption** tab.

3. Select the **Subscription timeline** tab.



The subscription timeline is displayed as a line graph by default, with icons marking important events. Hover over an event to see detailed information, such as the date and changes made to committed capacity during a modification. To view these events in a table, select the **Table** option from the **View as** dropdown. You can also see the timeline of other subscriptions by selecting or searching from the **Tracking ID** dropdown list.

Subscription details

Last updated: May 20, 2025, 11:28 PM

Tracking ID (Subscription number): Company HQ (9876543210)

Customer name: Company Pvt Ltd

Expiration date: May 31, 2027 (955 days)

Manage subscription

Current consumption | Consumption trend | **Subscription timeline** | Assets

Subscription timeline (3)

View as: Table

Date	Event	Performance service level	Details
May 1, 2023	Activated	Object	Committed: 500 TiB
Sep 15, 2024	Modified	Premium	Committed: 60 TiB
May 1, 2028	Time to renew	N/A	N/A

## Related information

- [Understand the Keystone dashboard](#)
- [View your subscription details](#)
- [View consumption trends](#)
- [View your Keystone subscription assets](#)
- [View assets across your Keystone subscriptions](#)
- [View volumes & objects details](#)

# View assets

## View assets associated with a Keystone subscription

You can view detailed information about ONTAP clusters and nodes, as well as the StorageGRID grids, sites, and nodes, managed by a single Keystone subscription. This

view of your subscription assets is available in the Keystone dashboard views from both BlueXP and Digital Advisor.

### View Keystone subscription assets from BlueXP

The **Assets** tab within the **Subscriptions** tab in BlueXP provides detailed information about volumes in clusters, StorageGRID nodes, and ONTAP nodes associated with the subscription, including various details and capacity status.



This view is limited to one Keystone subscription at a time. You can also see the assets of other subscriptions by selecting from the **Tracking ID** dropdown list. The Keystone dashboard in BlueXP allows you to view assets across multiple Keystone subscriptions. To learn more, refer to [View assets across your Keystone subscriptions](#).

You can view this information by following these steps:



## Volumes in clusters

### Steps

1. From the BlueXP left navigation menu, select **Storage > Keystone > Subscriptions**.
2. Select the subscription number in the **Subscription number** column of the table.

You are redirected to the **Current consumption** tab.

3. Select the **Assets** tab.
4. Select **Volumes in cluster** from the **View** dropdown.

Subscription details

Last updated: Aug 4, 2025, 2:30 PM PST

Tracking ID (Subscription number)  
Customer Site B (9876543210)

Customer name  
Customer Pvt Ltd

Expiration date  
March 15, 2026 (59 days)

Manage subscription

Current consumption

Consumption trend

Subscription timeline

Assets

Alert monitors

View

Volumes in clusters

Advanced search and filtering

None selected


Volumes (5)

Volume name	Node serial	Cluster name	Host name	Aggregate name	SVM	Volume type
hq_vol1	987654321012	Cluster1	host_1	aggr1	svm02-nfs	Read/write
hq_vol2	987654321012	Cluster1	host_1	aggr2	svm02-nfs	Read/write
hq_vol3	987654321012	Cluster2	host_1	aggr2	svm02-nfs	Read/write
hq_vol4	987654321012	Cluster2	host_1	aggr2	svm02-nfs	Read/write
hq_vol5	987654321012	Cluster3	host_1	aggr3	svm02-nfs	Read/write

1 - 5 of 5

You see the detailed information about volumes in clusters including volume name, node serial number, cluster name, host name, and performance service levels. You can also monitor the provisioned capacity, logical and physical utilization, and cold data.



You can customize the table using the column selector  icon and use the search bar at the top to search and filter table data based on the column parameters.

## Nodes in clusters

### Steps

1. From the BlueXP left navigation menu, select **Storage > Keystone > Subscriptions**.

By default, the **Subscriptions** tab displays the **Subscriptions** sub-tab.

2. Select the subscription number in the **Subscription number** column of the table.

You are redirected to the **Current consumption** tab.

3. Select the **Assets** tab.
4. Select **Nodes in clusters** from the **View** dropdown.

Subscription details

Last updated: May 20, 2025, 11:28 PM

Tracking ID (Subscription number)

Company HQ (9876543210)

Customer name

Company Pvt Ltd

Expiration date

May 31, 2027 (955 days)

Manage subscription

Current consumption

Consumption trend

Subscription timeline

Assets

View:

Nodes in clusters

Advanced search & filtering

None selected

Nodes in clusters (2)

Node serial

Node status

Cluster name

ONTAP version

SE ratio

Platform


Raw capacity

987654321012	ACTIVE	company02	9.12.1P7	1.45	AFF-A800	563 TiB
987654321013	ACTIVE	company02	9.12.1P7	1.45	AFF-A800	358 TiB

1 - 2 of 2

You see ONTAP cluster details, broken down by storage efficiency settings, platform type, and capacity details.



You can customize the table using the column selector  icon and use the search bar at the top to search and filter table data based on the column parameters.

## Nodes in grids

### Steps

1. From the BlueXP left navigation menu, select **Storage > Keystone > Subscriptions**.

By default, the **Subscriptions** tab displays the **Subscriptions** sub-tab.

2. Select the subscription number in the **Subscription number** column of the table.

You are redirected to the **Current consumption** tab.

3. Select the **Assets** tab.
4. Select **Nodes in grids** from the **View** dropdown.

Subscription details

Last updated: May 20, 2025, 11:28 PM

Tracking ID (Subscription number)

Company HQ (9876543210)

Customer name

Company Pvt Ltd

Expiration date

May 31, 2027 (955 days)

Manage subscription

Current consumption

Consumption trend

Subscription timeline

Assets

View:

Nodes in grids

Advanced search & filtering

None selected

Nodes in grids (4)

Node name

Node ID

Grid name

Node type

Consumed data capacity

Consumed metadata capacity


CPU usage

company-sg01	2.11.111.111111.1.1.11111.1.1.1.1.1.3	HQ-STORGRID	Storage Node	124 TiB	4 TiB	21%	
company-sg02	2.11.111.111111.1.1.11111.1.1.1.1.1.2	HQ-STORGRID	Storage Node	213 TiB	15 TiB	34%	
company-sg03	2.11.111.111111.1.1.11111.1.1.1.1.1.4	HQ-STORGRID	Storage Node	45 TiB	5 TiB	11%	
company-sg04	2.11.111.111111.1.1.11111.1.1.1.1.1.6	HQ-STORGRID	Storage Node	145 TiB	2 TiB	31%	

1 - 4 of 4 << < 1 > >>

You can view detailed information about nodes in grids, including node name, node status, grid name, node type, and customer. You can also monitor consumed and available data capacity, CPU usage, and usable data capacity.



You can customize the table using the column selector  icon and use the search bar at the top to search and filter table data based on the column parameters.

### View Keystone subscription assets from Digital Advisor

The **Assets** tab of the Keystone dashboard in Digital Advisor includes two sub-tabs: **ONTAP** and **StorageGRID**. This tab accumulates cluster-level information for ONTAP and grid-level information for StorageGRID based on your subscriptions, segregating and presenting the data with accurate details. You can view this information by clicking the respective sub-tabs.

## ONTAP

### Steps

1. Click **General > Keystone Subscriptions > Assets > ONTAP**.
2. Select the subscription number for which you want to view the clusters.

You see the cluster details, broken down by storage efficiency settings, platform type, and capacity details. Clicking on one of the clusters takes you to the **Clusters** widget on the Digital Advisor screen, where you get additional information for that cluster. Digital Advisor provides a comprehensive inventory-level information of your deployments.

Keystone Subscriptions [Help](#)

Subscriptions Current Consumption Consumption Trend Volumes & Objects **Assets** Subscription Timeline SLA Details

ONTAP StorageGRID

[Download CSV](#)

Subscription: XXX1234567 Start Date (UTC): May 1, 2022 Billing Period: Month

Cluster Name	SE Ratio	ONTAP Version	Platform	Node Serial	HW Support End Date	To
AXXXXX00001	1.02:1	9.10.1P12	AFF-A700s	123456789	December 31, 2026	16
AXXXXX00002	1.02:1	9.10.1P19	AFF-A700s	123456789	December 31, 2026	16

## StorageGRID

### Steps

1. Click **General > Keystone Subscriptions > Assets > StorageGRID**.
2. Select the subscription number.

You see the grid details, categorized by grid and node identifiers, site information, hardware specifications, and capacity details, which help in monitoring and managing nodes in your StorageGRID infrastructure.

ONTAP

StorageGRID

[Download CSV](#)Subscription  
XXX1234567Start Date (UTC)  
March 1, 2022Billing Period  
Month

Grid Name	Node Name	Site Name	Grid OID	Node ID	Node Serial	Dis
StorageGRID	StorageGRID007	NYC	2.16.124.1125002.1.60...	2.16.124.1125002.1.60...	752052500071	NL
StorageGRID	StorageGRID008	NYC	2.16.124.1125002.1.60...	2.16.124.1125002.1.60...	752052500180	NL
StorageGRID	StorageGRID009	NYC	2.16.124.1125002.1.60...	2.16.124.1125002.1.60...	950019500090	NL
StorageGRID	StorageGRID010	NYC	2.16.124.1125002.1.60...	2.16.124.1125002.1.60...	950019500091	NL
StorageGRID	StorageGRID011	NYC	2.16.124.1125002.1.60...	2.16.124.1125002.1.60...	950019500092	NL

## Related information

- [Understand the Keystone dashboard](#)
- [View your subscription details](#)
- [View your current consumption details](#)
- [View consumption trends](#)
- [View your subscription timeline](#)
- [View assets across your Keystone subscriptions](#)
- [View volumes & objects details](#)

## View assets across multiple Keystone subscriptions

The Keystone dashboard in BlueXP allows you to view detailed information about nodes in clusters, provisioned volumes, and StorageGRID nodes across multiple Keystone subscriptions, according to your access permissions. This view is not available in Digital Advisor.

## Nodes in clusters

### Steps

1. From the BlueXP left navigation menu, select **Storage > Keystone > Assets**.

The **Assets** tab displays the **Nodes in cluster** sub-tab.


The screenshot shows the NetApp BlueXP interface. The top navigation bar includes the NetApp logo, BlueXP text, a search bar, and dropdown menus for Organization, Project, and Connector. The left sidebar shows the navigation menu with 'Keystone' selected. The main content area is titled 'Assets' and shows a sub-tab 'Nodes in clusters' selected. The page displays three summary cards: 'Summary' (2 Subscriptions, 2 Nodes), 'Node consumption status' (1 > 90% consumed, 1 < 50% consumed), and 'Nodes summary based on ONTAP versions' (1 Within latest 3 versions, 1 Older than latest 3 versions). Below these cards is a table titled 'Nodes in clusters (2)' with columns: Node serial, Node status, Subscription number, Customer, Cluster name, ONTAP version, and SE ratio. The table contains two rows of data.

Node serial	Node status	Subscription number	Customer	Cluster name	ONTAP version	SE ratio
987654321012	ACTIVE	9876543210	Company Pvt Ltd	company02	9.12.1P7	1.45
987654321013	ACTIVE	9876543210	Company Pvt Ltd	company02	9.15.1P3	1.45

You can view detailed information about all nodes in clusters across Keystone subscriptions, including node serial numbers, status, storage efficiency settings, platform type, and capacity details. You also get an overview of:

- Total number of subscriptions and ONTAP nodes.
- Node capacity consumption, with a clickable **View** button to filter the table and display assets that meet specific criteria (> 90% consumed or < 50% consumed).
- Nodes based on ONTAP versions, with the **View** button to filter for nodes within the latest three versions or older.



You can customize the table using the column selector  icon and use the search bar at the top to search and filter Keystone data based on the column parameters.

## Volumes in clusters

### Steps

1. From the BlueXP left navigation menu, select **Storage > Keystone > Assets**.
2. Select the **Volumes in clusters** tab.

NetApp BlueXP

Organization Account name | Project Project name | Connector Connector name

Keystone Overview Subscriptions **Assets** Administration

Assets Last updated: Aug 4, 2025, 2:30 PM PST

Nodes in clusters Volumes in clusters Nodes in grids

Summary

5 Subscriptions [View](#)

5 Clusters [View](#)

201 Volumes

Volume compliance and protection status

198 Compliant [View](#)

3 Not compliant [View](#)

7 Not protected [View](#)

Advanced search and filtering None selected

Volumes (201)


Volume name	Subscription number	Node serial	Customer name	Cluster name	Host name	Aggregate name	SVM
hq_vol1	9876543210	987654321012	Customer Pvt Ltd	Cluster 1	company02-03	aggr1	svm02-nfs
hq_vol2	9876543210	987654321012	Customer Pvt Ltd	Cluster 1	company02-03	aggr1	svm02-nfs
hq_vol3	9876543210	987654321012	Customer Pvt Ltd	Cluster 1	company02-03	aggr2	svm02-nfs
hq_vol4	9876543210	987654321012	Customer Pvt Ltd	Cluster 2	company02-04	aggr3	svm02-nfs
hq_vol5	9876543210	987654321012	Customer Pvt Ltd	Cluster 3	company02-04	aggr4	svm02-nfs
site_vol1	9876543210	987654321012	Customer Pvt Ltd	Cluster 3	company02-05	aggr4	svm02-nfs
site_vol2	9876543210	987654321012	Customer Pvt Ltd	Cluster 3	company02-06	aggr4	svm02-nfs
site_vol3	9876543210	987654321012	Customer Pvt Ltd	Cluster 3	company02-07	aggr5	svm02-nfs

1 - 8 of 201

You see the detailed information about all volumes in clusters across Keystone subscriptions including volume name, subscription number, node serial number, compliance with QoS policies, cluster name, host name, and performance service levels. You can monitor the provisioned capacity, logical and physical utilization, and cold data. You also get an overview of:

- The total number of subscriptions, clusters, and volumes.
- Volume compliance and protection status, with a **View** button to filter the table and display assets based on criteria such as compliant, not compliant, or not protected.



You can customize the table using the column selector  icon and use the search bar at the top to search and filter Keystone data based on the column parameters.

You can click a subscription number in the **Subscription number** column to go to the **Subscriptions** tab, where you can view subscription consumption details, timelines, and associated asset information. To learn more, refer to [View your current consumption details](#).

## Nodes in grids

### Steps

1. From the BlueXP left navigation menu, select **Storage > Keystone > Assets**.
2. Select the **Nodes in grids** tab.


The screenshot shows the NetApp BlueXP interface. The top navigation bar includes the NetApp logo, 'BlueXP', a search bar, and dropdown menus for Organization, Project, and Connector. The main navigation tabs are Keystone, Overview, Subscriptions, Assets (selected), and Administration. The 'Assets' section is titled 'Assets' with a 'Last updated: May 21, 2025, 12:08 AM' timestamp. Below the title are three tabs: 'Nodes in clusters', 'Volumes in clusters', and 'Nodes in grids' (selected). A search bar labeled 'Advanced search & filtering' is present. The table 'Nodes in grids (6)' displays the following data:

Node name	Node ID	Subscription number	Customer	Grid name	Node type	Consumed data ca
company-sg01	2.22.222.222222.2.1.222222.1.1.1.1	<a href="#">9876543210</a>	Company Pvt Ltd	HQ-STORGRID	Storage Node	127 TiB
company-sg02	2.22.222.222222.2.1.222222.1.1.1.1	<a href="#">9876543210</a>	Company Pvt Ltd	HQ-STORGRID	Storage Node	34 TiB
company-sg03	2.22.222.222222.2.1.222222.1.1.1.1	<a href="#">9876543210</a>	Company Pvt Ltd	HQ-STORGRID	Storage Node	196 TiB
company-sg04	2.22.222.222222.2.1.222222.1.1.1.1	<a href="#">9876543210</a>	Company Pvt Ltd	HQ-STORGRID	Storage Node	435 TiB
site-sg-01	2.22.333.222222.2.1.222222.1.1.1.1	<a href="#">1234567890</a>	Company Pvt Ltd	SITE-SG	Storage Node	254 TiB
site-sg-02	2.22.222.444555.2.1.222222.1.1.1.1	<a href="#">1234567890</a>	Company Pvt Ltd	SITE-SG	Storage Node	31 TiB

At the bottom right of the table, it says '1 - 6 of 6' with navigation arrows.

You can view detailed information about all nodes in grids across Keystone subscriptions including node name, node ID, subscription number, grid name, node type, and customer. You can monitor the consumed and available data capacity, CPU usage, and usable data capacity.



You can customize the table using the column selector  icon and use the search bar at the top to search and filter Keystone data based on the column parameters.

You can click a subscription number in the **Subscription number** column to go to the **Subscriptions** tab, where you can view subscription consumption details, timelines, and associated asset information. To learn more, refer to [View your current consumption details](#).

## Related information

- [Understand the Keystone dashboard](#)
- [View your subscription details](#)
- [View your current consumption details](#)
- [View consumption trends](#)
- [View your subscription timeline](#)
- [View your Keystone subscription assets](#)
- [View volumes & objects details](#)

## Modify your Keystone subscription from BlueXP

You can modify the committed capacity of your Keystone subscription for the associated performance service levels through BlueXP.





- You can modify the committed capacity if the subscription has more than 90 days remaining before it expires.
- You must be assigned to the **Keystone admin** role to modify the committed capacity. To learn more, refer to [Learn about BlueXP access roles](#).

To change the committed capacity, follow these steps:

### Steps

1. From the BlueXP menu, select **Storage > Keystone > Subscriptions**.
2. Click the ellipsis icon from the table for the subscription you wish to modify, and then select **Modify**.

The **Modify subscription** page displays the details for the subscribed performance service levels associated with the selected subscription number.



Optionally, you can access the **Modify subscription** page by clicking **Manage subscription** in the subscription details section, and then selecting **Modify**.

The screenshot displays the NetApp BlueXP interface for the 'Subscriptions' section. At the top, there's a navigation bar with 'Keystone', 'Overview', 'Subscriptions', 'Assets', and 'Administration'. Below this, a 'Subscriptions' header indicates the last update on Aug 4, 2025. The main content area features a 'Capacity usage' section with three cards: 'Above burst' (1), 'Using burst' (1), and 'Underutilized' (1). To the right, a 'Keystone version across subscriptions' bar chart shows V1: 1, V2: 1, and V3: 3. Further right, an 'Expiring soon' card shows 1 subscription expiring on May 15, 2025. Below these is an 'Advanced search and filtering' section. The main part of the page is a table titled 'Subscriptions (5)' with the following data:

Subscription number	Tracking ID	Customer name	Keystone version	Billing period	Performance service levels	Expiration date	
9876543210	Company HQ	Company Pvt Ltd	V1_physical	Month	3	May 15, 2025 (59 days)	⋮
9876543211	Company Site A	Company Pvt Ltd	V2_physical	Month	5	March 18, 20	⋮
9876543212	Company Site B	Company Pvt Ltd	V3_logical	Month	2	June 7, 2028 (966 days)	⋮
9876543213	Company Site C	Company Pvt Ltd	V3_logical	Month	1	October 9, 2026 (683 days)	⋮
9876543214	Company Site D	Company Pvt Ltd	V3_physical	Month	6	April 2, 2026 (14 days)	⋮

The table footer indicates '1 - 5 of 5' items.

3. Click **Edit capacity** to modify committed capacity for the performance service levels, provide the necessary details, and click **Submit**.

You see the request in the **Modifications** section on the same page.

4. Review the request details, click the **Review** button, provide the necessary confirmation, and then submit the request.

You can track and monitor the progress of your request under the **Administration** tab. To learn more about the **Administration** tab, refer to [View service requests for Keystone subscriptions](#).

# View service requests for Keystone subscriptions


You can view and track service requests for modifying Keystone subscriptions through BlueXP, providing a quick summary and monitoring progress.

To view the progress or cancel a request, follow these steps:

## Steps

1. From the BlueXP left navigation menu, select **Storage > Keystone > Administration**.

You see a list of all service requests, including the request number, type of request, and current status.

2. You can click the  icon next to the **Submission date** column to expand the request number and view details. You see the performance service levels for which the requests are raised.

NetApp BlueXP

BlueXP search

Organization Account name

Project Project name

Connector Connector name

10

Settings

Help

User

Keystone Overview Subscriptions Assets Administration

Administration

Last updated: Jan 30, 2024, 2:30 PM

Requests Collector management Service level

Requests status summary

2 In Progress View

2 Completed View

2 Canceled View

Requests (6)

Request number	Customer	Subscription number	Status	Type	Submission date	
19623	Company Pvt Ltd	9876543210	In progress	Modification	January 1, 2025	...
19384	Company Pvt Ltd	9876543210	In progress	Modification	January 1, 2025	...
17932	Company Pvt Ltd	9876543210	Completed	Modification	August 30, 2024	^

Request summary

Service levels	Committed capacity	Type
Extreme (V1_physical)	100 TiB → 250 TiB	Unified
Extreme (V2_logical)	200 TiB	Object

1 - 6 of 6

3. Select the request number to view detailed information, including modification details for the requested subscription and the current progress status.

Request detail

Last updated: May 5, 2025, 2:30 PM

Subscription: 9876543210 | Tracking ID: Company-HQ | Customer name: Company Pvt Ltd

Status

In progress

Request type

Modification

Submission date

May 1, 2025

Cancel request

Requested subscription

There are 2 modifications in this request

Service level	Committed capacity	Storage type
Extreme (V1_physical) Edited	100 TiB → 250 TiB	Unified
Value (V2_logical)	100 TiB	Unified
Extreme (V2_logical) Added	200 TiB	Object

Submitted

January 10, 2024

2

Technical solutions review

Current step

3 Sales order creation

4 Customer sign-off

5 Fulfillment

6 Complete

Technical solutions review

Hardware analysis and BOM creation

Step status

In progress

Last updated

May 5, 2025, 2:30 PM

Notes

- May 04, 2025, 7:01 AM  
New hardware is required
- May 03, 2025, 6:51 PM  
Current hardware is on latest ONTAP version

## View details about ONTAP volumes and object storage

If you want to view capacity details at the volume or object storage level, you can navigate to the **Volumes & Objects** tab in Digital Advisor. For StorageGRID, you can use this tab to read the usage by the individual nodes in your object storage environment.

You can refer to the **Assets** tab in BlueXP to view these details. To view the details for a specific Keystone STaaS subscription, refer to [View assets associated with a Keystone subscription](#). If you want to view details across multiple Keystone subscriptions, refer to [View assets across your Keystone subscriptions](#).



The title of this tab varies with the nature of deployment at your site. If you have both ONTAP and object storage, the title of the tab appears as **Volumes & Objects**. For only ONTAP, the name appears **Volumes**. For StorageGRID object storage, you can see the **Objects** tab.

## View ONTAP volumes and object storage details

The **Volumes & Objects** tab offers insights into ONTAP system volumes and object storage at different levels of detail. For ONTAP volumes, there are two sub-tabs: **Volume Summary**, which provides an overall count of the volumes mapped to the subscribed performance service levels, and **Volume Details**, which lists these volumes again with their specific particulars. The **Objects** sub-tab provides details on object storage for subscriptions that include performance service levels for both file and object storage.

## Volume Summary

1. From the Digital Advisor left navigation pane, go to **General > Keystone Subscriptions > Volumes & Objects > Volume Summary**.
2. Select the subscription number.

For the selected Keystone STaaS subscription, you can see the total number of volumes, count of protected volumes, anti ransomware protection status, and the total committed, consumed, and available capacity in all those volumes. If you click the number of protected volumes, it takes you to the **Volume Details** tab, where you can view a filtered list showing the protected volumes, based on your selection.

Keystone Subscriptions <span>Help</span>						
Subscriptions   Current Consumption   Consumption Trend   Volumes & Objects   Assets   Performance						
Volume Summary   Volume Details   Objects <span>Download CSV</span>						
Subscription v3_All (A-S00027643)		Start Date (UTC) May 27, 2025		End Date (UTC) May 27, 2026		Billing Period Month
Service Level	Volumes	Protected	ARP	Committed	Consumed	Available
Block-Extreme	2203	48	0	1 TiB	1.12 TiB	0 TiB
Block-Premium	1758	336	1	1 TiB	0.33 TiB	0.67 TiB

## Volume Details

1. From the Digital Advisor left navigation pane, go to **General > Keystone Subscriptions > Volumes > Volume Details**.
2. Select the subscription number.

You can see the tabular listing of the volumes, such as capacity usage, volume type, cluster, aggregate, and the assigned Keystone performance service levels. You can scroll across the columns and learn more about them by hovering your mouse on the information icons beside the column headings. You can sort by the columns and filter the lists to view specific information.

You can use **Hide/Show Columns** to add or remove columns displayed in the table. By default, the table shows your previously saved column preferences. Newly added columns, such as the **Department** or **Total Footprint** columns, are hidden by default and should be manually selected to appear in the table. You can select or deselect any columns, and your preferences will be saved for later use. When downloading the CSV report, all available columns are included in the export regardless of your display preferences.

[Volume Summary](#)[Volume Details](#)[Objects](#)[Download CSV](#)Subscription  
v3\_All (A-S00027643) ▼[Copy Node Serials](#)[Hide/Show Columns](#)  
Volume Name, Clus... ▼[Clear Filters](#)

Volume Name	Volume Type	Volume Style	Is Clone	Is Destination	Is Protected	ARP
DSTG_vol_1	Read-Write	flexvol	false	false	false	false
DSTG_vol_2	Read-Write	flexvol	false	false	false	false
DSTG_vol_3	Read-Write	flexvol	false	false	false	false
DSTG_vol_4	Read-Write	flexvol	false	false	false	false
DSTG_vol_5	Read-Write	flexvol	false	false	false	false

## Objects

1. From the Digital Advisor left navigation pane, go to **General > Keystone Subscriptions > Objects**.
2. Select the subscription number. By default, the first available subscription number is selected if the previously selected subscription does not include performance service levels for both file and object storage.



For StorageGRID, this tab displays the physical usage for the nodes for object storage.

[Volume Summary](#)[Volume Details](#)[Objects](#)[Download CSV](#)Subscription  
TrackSG002 (A-S00021959) ▼

Start Date (UTC)

November 15, 2022

End Date (UTC)

November 15, 2024

Billing Period

Month

Node Name	Physical Used
sgsn02	1.74 TiB
sgsn01	1.8 TiB
sgsn03	1.51 TiB

## Related information

- [Understand the Keystone dashboard](#)
- [View your subscription details](#)
- [View your current consumption details](#)
- [View consumption trends](#)
- [View your subscription timeline](#)

- [View your Keystone subscription assets](#)
- [View assets across your Keystone subscriptions](#)
- [View performance metrics](#)

## View performance metrics

To monitor the performance of your systems, you can view performance metrics of the ONTAP volumes managed by your Keystone subscriptions.



This tab is optionally available to you in Digital Advisor. Contact support for viewing this tab. It is not available in BlueXP.

To view this tab in Digital Advisor, follow these steps:

### Steps

1. Click **General > Keystone Subscriptions > Performance**.
2. Select the subscription number. By default, the first subscription number is selected.
3. Select the required volume name from the list.



Alternately, you can click the icon against an ONTAP volume in the **Volumes** tab to navigate to this tab.

4. Select the date range for the query. The date range can be the beginning of the month or the subscription start date to the current date or the subscription end date. You cannot select a future date.

The retrieved details are based on the performance service level objective for each performance service level. For example, the peak IOPS, maximum throughput, target latency, and other metrics are determined by the individual settings for the performance service level. For more information about the settings, see [Performance service levels in Keystone](#).



If you select the **SLO Reference Line** check box, the IOPS, throughput, and latency graphs are rendered based on the performance service level objective for the performance service level. Else, they are displayed in actual numbers.

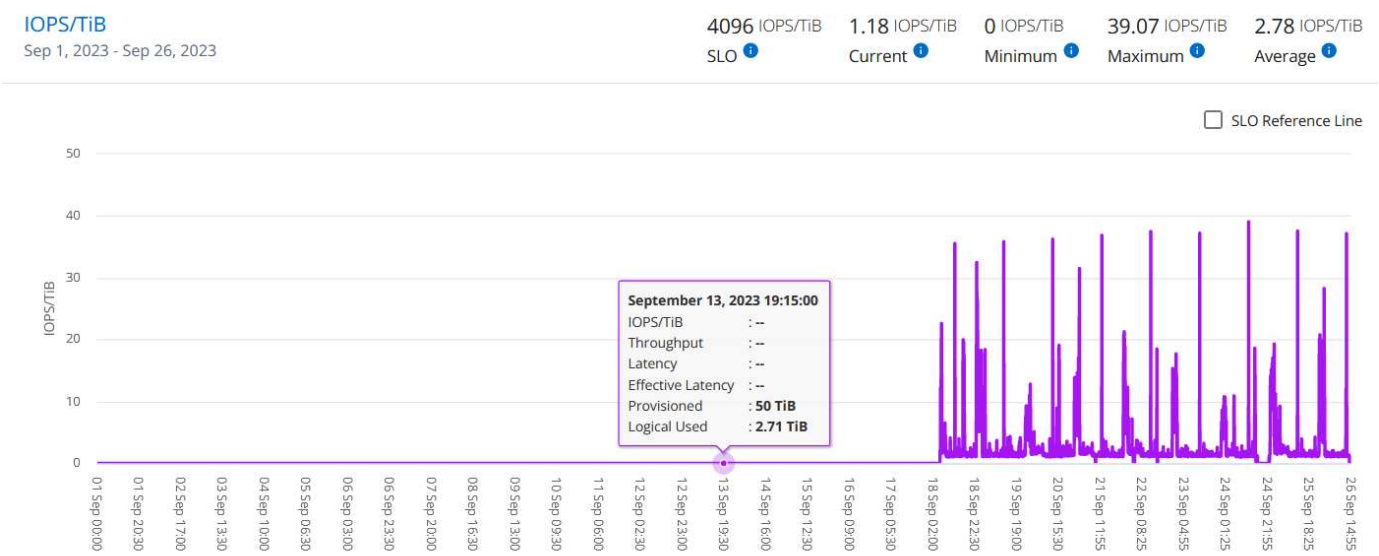
The performance data displayed on the horizontal graph is an average at every five-minute interval, and arranged as per the date range of the query. You can scroll across the graphs and hover your mouse over specific data points to drill further down into the collected data.

You can view and compare the performance metrics in the following sections based on the combination of the subscription number, volume name, and the date range selected. The details are displayed as per performance service level assigned to the volume. You can see the cluster name and volume type, that is, the read and write permissions assigned to the volume. Any warning message associated with the volume is also displayed.

## IOPS

This section displays the input-output graphs for the workloads in the volume based on the date range of the query. The peak IOPS for the performance service level and the current IOPS (in the last five minutes, not based on the date range of the query) are displayed, along with the minimum, maximum, and average IOPS

for the time range, in IOPS/Tib.

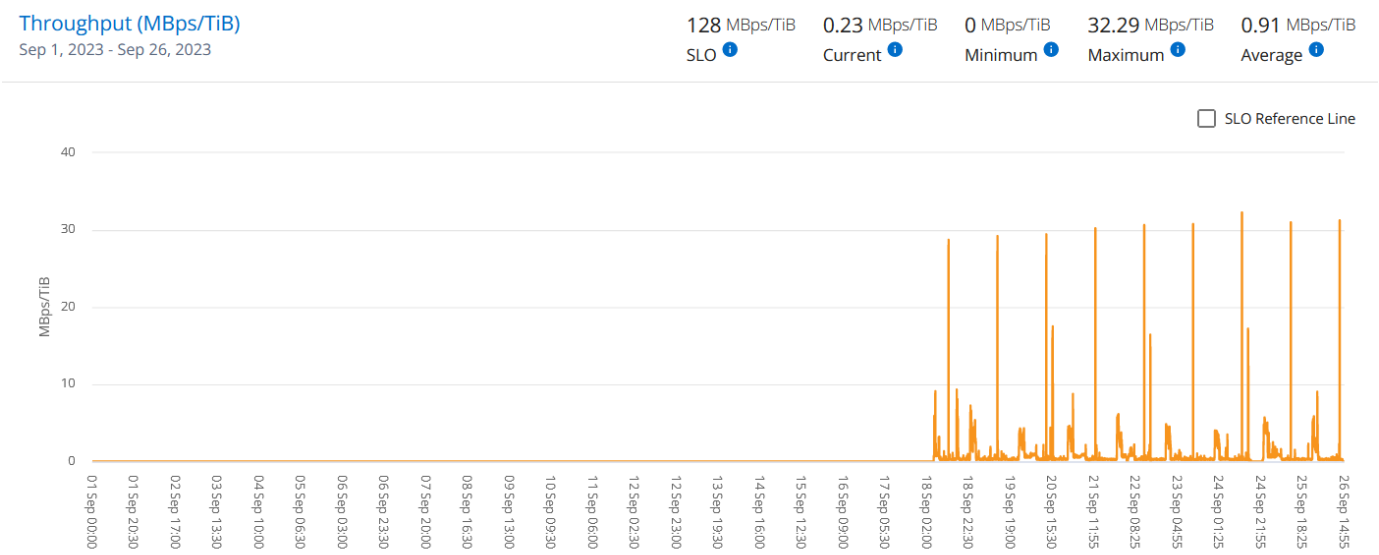


SLO Reference Line

September 13, 2023 19:15:00  
IOPS/TiB : --  
Throughput : --  
Latency : --  
Effective Latency : --  
Provisioned : 50 TiB  
Logical Used : 2.71 TiB

## Throughput

This section displays the throughput graphs for the workloads in the volume based on the date range of the query. The maximum throughput for the performance service level (SLO Max), and current throughput (in the last five minutes, not based on the date range of the query) are displayed, along with the minimum, maximum, and average throughput for the time range, in MBps/TiB.



SLO Reference Line

September 13, 2023 19:15:00  
IOPS/TiB : --  
Throughput : --  
Latency : --  
Effective Latency : --  
Provisioned : 50 TiB  
Logical Used : 2.71 TiB

## Latency (ms)

This section displays the latency graphs for the workloads in the volume based on the date range of the query. The maximum latency for performance service level (SLO Target), and current latency (in the last five minutes, not based on the date range of the query) are displayed, along with the minimum, maximum, and average latency for the time range, in milliseconds.

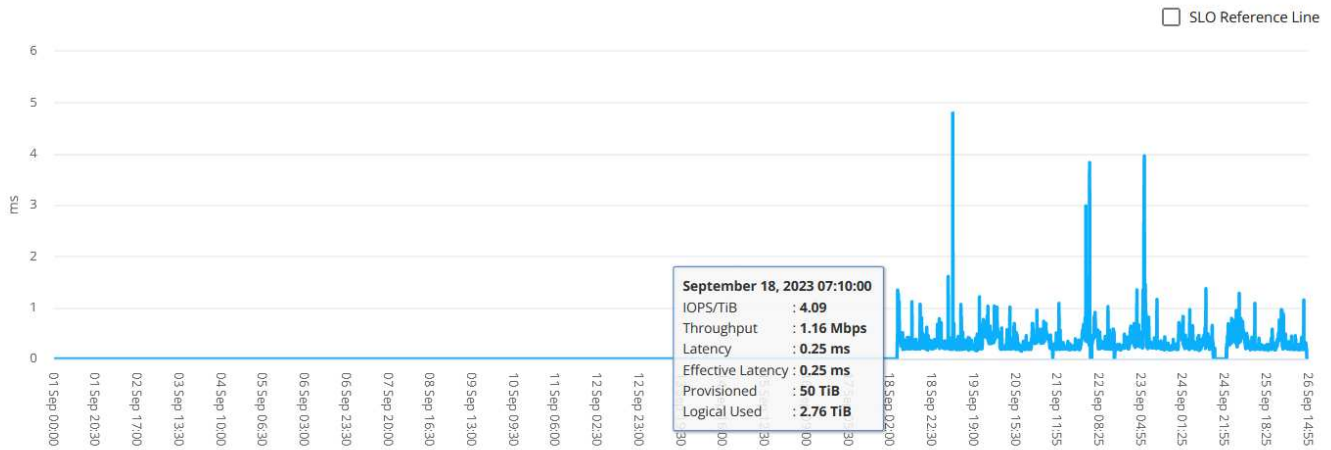
This graph has the following colors:

- Light blue: *Latency*. This is the actual latency that includes any latency other than your Keystone service. This might include additional latency, such as the latency occurring between your network and client.
- Dark blue: *Effective latency*. Effective latency is the latency applicable only to your Keystone service with respect to your SLA.

#### Latency (ms)

Sep 1, 2023 - Sep 26, 2023

2 ms   0.19 ms   0 ms   4.8 ms   0.32 ms  
SLO   Current   Minimum   Maximum   Average



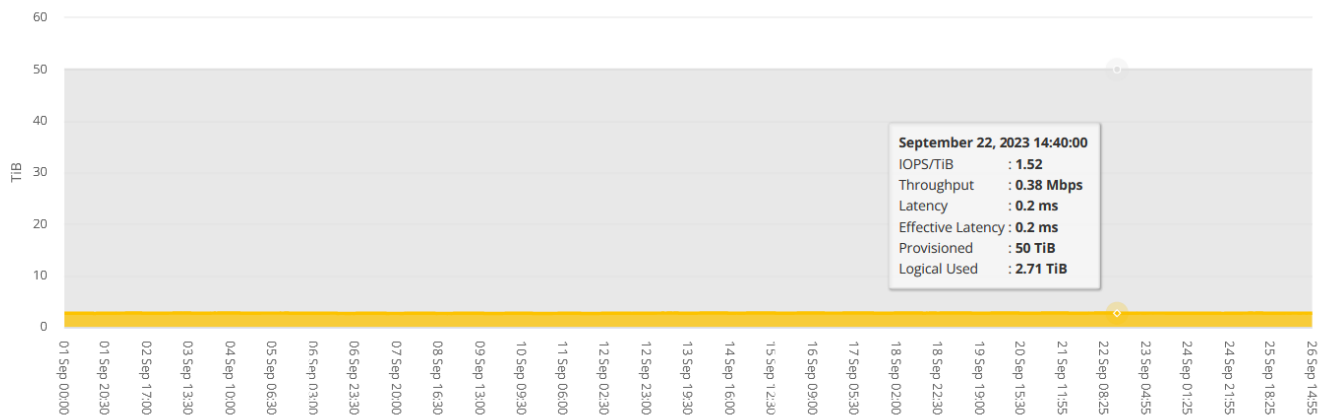
## Logical Used (TiB)

This section displays the provisioned and the logical used capacities of the volume. The current logical used capacity (in the last five minutes, not based on the date range of the query), along with the minimum, maximum, and average usage for the time range are displayed in TiBs. On this graph, the grey area represents the committed capacity, and the yellow graph indicates the logical use.

#### Logical Used (TiB)

Sep 1, 2023 - Sep 26, 2023

2.7/50 TiB   2.65 TiB   2.77 TiB   2.72 TiB  
Current   Minimum   Maximum   Average



## Related information

- [Understand the Keystone dashboard](#)
- [View your subscription details](#)
- [View your current consumption details](#)



- [View consumption trends](#)
- [View your subscription timeline](#)
- [View your Keystone subscription assets](#)
- [View assets across your Keystone subscriptions](#)
- [View volumes & objects details](#)

# Concepts

## Keystone STaaS services

### Metrics and definitions used in Keystone

The NetApp Keystone STaaS service uses several terms to measure metrics. You might want to learn more about these terms as you use Keystone.

The following terms and definitions are used within the Keystone STaaS service to measure metrics:

- **Capacity:** Measured in GiB, TiB, and PiB.
- **IOPS:** Number of input/output operations processed per second.
- **Service availability**
- **Durability** in accurate data access
- **Latency and speed**

### Metrics measurement

- **Capacity measurement in GiB, TiB, and PiB:** Measurements of data storage capacity using base of 1024 (1 GiB =  $1024^3$  bytes, 1 TiB =  $1024^4$  bytes, and 1 PiB =  $1024^5$  bytes).
- **Operations counter chart in IOPS:** The protocol operations per second, requested by the application.
- **Availability:** Measured as a percentage of the number of I/O requests successfully responded to by the service, divided by total number of I/O requests made to the service. This is measured at the service demarcation in a month and does not include the scheduled service downtime or unavailability of the facilities, network, or other services provided by the customer.
- **Durability:** Percentage of data accessed without loss of fidelity, excluding customer-caused deletion or corruption.
- **Latency:** Time to service an I/O request received from a client, measured at the service demarcation (storage controller I/O port).

### Performance metrics

The following performance metrics are applicable to unified and block-optimized services:

#### Unified services:

- **IOPS:** For ONTAP 9.16.1 with NFS, each performance level instance supports random access with a 70% read and 30% write ratio, an 8 KB block size, and a latency of 1 ms (4 ms for Standard).
- **Throughput:** For ONTAP 9.16.1 with NFS, each performance level instance supports sequential access with 100% read and a 32 KB block size.

#### Block optimized services:

- **IOPS:** For ONTAP 9.16.1 with FCP, each performance level instance supports random access with a 70% read and 30% write ratio, an 8 KB block size, and a latency of 1 ms.
- **Throughput:** For ONTAP 9.16.1 with FCP, each performance level instance supports sequential access with 100% read and a 64 KB block size.

## Supported storage in Keystone

Keystone STaaS service supports unified, block-optimized, and object storage of NetApp, and Cloud Volumes ONTAP.

The supported storage options are:

- **Unified storage:** Includes both file, block, and S3 object storage, available on NetApp ONTAP AFF as well as FAS systems.
- **Block-optimized storage:** Includes block storage available on NetApp ONTAP ASA systems.
- **Object storage:** Includes object storage available on NetApp StorageGRID systems.

Keystone STaaS provides standard and optional services for your storage.

**Keystone STaaS standard services:** Standard services are included within the base subscription and are not charged separately.

**Keystone STaaS add-on services:** These are optional, chargeable services that provide additional utilities and benefits on top of standard Keystone STaaS subscription services.

Keystone STaaS services can be used at the same time. For example, a cloud storage subscription can have the same term as unified, block-optimized, and object storage subscriptions. A cloud service can be included at any point during the service term of an existing storage subscription. However, if you do not plan to renew an existing unified, block-optimized, or object storage subscription, a cloud storage subscription cannot be added during the last 90 days of the subscription.

### Services for unified, block-optimized, and object storage

Keystone STaaS services for unified, block-optimized, and object storage, support multiple features and protocols, and described in the following table:

Storage	Platform	Protocols	Supported features
Unified storage	ONTAP	NFS and CIFS	Supports all ONTAP One features
Block optimized storage	ONTAP	FC and iSCSI	Supports all ONTAP One features
Object storage	StorageGRID	S3	Supports all ONTAP One features

To learn more about ONTAP One, refer to [ONTAP licensing overview](#) and [ONTAP One: The full power of ONTAP, now all in one](#).

### Services for cloud storage

Keystone STaaS provides cloud storage services. Keystone STaaS supports Cloud Volumes ONTAP data management capabilities on Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform.



Hyperscalar-based compute, storage, and network services required by Cloud Volumes ONTAP are not provided by NetApp as a part of Keystone STaaS subscriptions; these subscriptions need to be procured directly from hyperscalar cloud service providers.

## Supported storage capacities in Keystone

The NetApp Keystone STaaS service supports several types of storage capacities. Understanding these different capacity terms can help as you use Keystone.

### Logical capacity

This is the amount of storage capacity required to store user data before any data efficiencies provided by the storage array are applied.

### Committed capacity

The minimum logical capacity billed each month during the subscription:

- Capacity is committed to each service level.
- Committed capacity and additional performance service levels can be added during the term.

### Changes to committed capacity

During the tenure of a subscription, you can change the committed capacities. However, there are certain preconditions:

- The committed capacity can be decreased based on certain conditions. For information, see [Capacity reduction](#).
- The committed capacity cannot be increased 90 days prior to the expiry of your subscription, unless the subscription is to be renewed for an additional 12-month term.
- You can request changes to committed capacity through the BlueXP interface or from your Keystone Success Manager (KSM).  
For information about requesting changes, see [NetApp Keystone support](#).

### Consumed capacity

Consumed capacity refers to the capacity (in TiB of storage) currently being consumed on the service. It is calculated differently based on the storage type:

- **Unified or block-optimized storage:** Consumed capacity is calculated based on the type of capacity (either logical or physical) selected during the ordering process. The calculation is performed per performance service level instance.
  - a. **Logical capacity:** It is the sum of:
    - Metered logical capacity, before storage array data efficiencies, to store all instances and types of customer data, such as copies, mirrored copies, versions, and clones.
    - Physical capacity used to store metadata and differential data of snapshots and certain clones.
    - Any thick-provisioned physical capacity.
  - b. **Physical capacity:** It is the sum of:
    - Metered physical capacity, after storage array data efficiencies, to store all instances and types of

customer data, such as copies, mirrored copies, versions, clones.

- Physical capacity used to store metadata and differential data of snapshots.
- Any thick-provisioned physical capacity.
- **Object storage:** Consumed capacity is calculated as the amount of metered physical capacity used to store all instances and types of customer data across all nodes. This calculation is based on the information lifecycle management (ILM) policies configured.
- **Cloud Volumes ONTAP:** Consumed capacity is calculated as the amount of metered provisioned capacity of all Cloud Volumes ONTAP volumes.

## Burst capacity

The NetApp Keystone STaaS service enables you to use additional capacity on top of the committed capacity for a performance service level. This is referred to as the burst capacity usage.

Note these points:

- Burst capacity is agreed upon in the Keystone agreement. It is usually set up to 20% above the committed capacity, per performance service level instance, with additional options available to select burst capacity limits of 40% or 60% of committed capacity.
- Burst capacity consumption is invoiced at the same rate as the committed capacity corresponding to the selected performance service level.
- Keystone STaaS services provide a burst waiver period of 60 days from the start date.

## Billed capacity

Monthly bill = (committed capacity [TiB] \* committed rate [\$ / TiB]) + (daily average provisioned burst capacity [TiB] \* burst rate [\$ / TiB]). The monthly bill contains a minimum charge based on the committed capacity.

The monthly bill varies beyond the minimum charge based on daily average burst capacity consumption.

## Performance service levels in Keystone

Keystone STaaS offers data storage capacity at pre-defined performance service levels. Each volume managed by Keystone services is associated with a performance service level.

A subscription can have multiple rate plans and each rate plan corresponds to a performance service level. Each rate plan has a committed capacity per performance service level.

A performance service level can have multiple instances, with each instance representing a separate storage array assigned to that performance service level in the customer's environment. Each performance service level is defined by input/output operations per second (IOPS), throughput (GBps), and latency (ms), with these metrics measured and applied per performance service level instance.

You select performance service levels based on your storage environment, and storage and consumption needs. The base performance service levels are available for you by default. Specific performance service levels are additionally available, if you have opted for add-on services.



A detailed service description for NetApp Keystone STaaS performance service levels is available [here](#).

The base performance service levels for the supported storage types, unified, block-optimized, object, and cloud services are described in the following sections:

### Performance service levels for unified storage

**Supported protocols:** FC, iSCSI, NFS, NFSv4/RDMA, NVMe/FC, NVMe/TCP, SMB, S3

<b>Performance service level</b> (all specifications per performance service level instance)	<b>Extreme</b>	<b>Premium</b>	<b>Standard</b>	<b>Value</b>
<b>Sample workload types</b>	AI/ML, HPC, InMem DB	Analytics, EDA, OLTP	OLAP, IoT, Containers	Backup, Archive
<b>Maximum IOPS<sup>1</sup></b>	1M	550K	500K	NA
<b>Maximum GBps</b>	40	20	20	NA
<b>Target 90<sup>th</sup> percentile latency</b>	<=1 ms	<=1 ms	<=4 ms	>4 ms
<b>Minimum committed capacity</b>	50 TiB	50 TiB	100 TiB	100 TiB
<b>Incremental committed capacity increase</b>	25TiB			
<b>Committed and metered capacity type</b>	Logical or physical			

### Performance service levels for block-optimized storage

**Supported protocols:** NVMe/TCP, NVMe/FC, FC, iSCSI

<b>Performance service level</b> (all specifications per performance service level instance)	<b>Extreme</b>	<b>Premium</b>
<b>Sample workload types</b>	SAP HANA, Oracle, MS SQL Server, EPIC	
<b>Maximum IOPS<sup>1</sup></b>	850K	450K
<b>Maximum GBps</b>	65	25
<b>Target 90<sup>th</sup> percentile latency</b>	<=1 ms	<=1 ms
<b>Minimum committed capacity</b>	50 TiB	50 TiB
<b>Incremental committed capacity increase</b>	25TiB	
<b>Committed and metered capacity type</b>	Logical or physical	



<sup>1</sup>Mutually exclusive targets. Actual performance may differ based on various factors, including the operating system version, hardware, workload type, and number of concurrent operations.

### More on performance service levels for unified and block-optimized storage

The base performance service level metrics depend on the following conditions:

- The performance service levels support ONTAP 9.8 and later.
- For unified storage,
  - **IOPS:** For ONTAP 9.16.1 with NFS, each performance level instance supports random access with a 70% read and 30% write ratio, an 8 KB block size, and a latency of 1 ms (4 ms for Standard).
  - **Throughput:** For ONTAP 9.16.1 with NFS, each performance level instance supports sequential access with 100% read and a 32 KB block size.
- For block-optimized storage,
  - **IOPS:** For ONTAP 9.16.1 with FCP, each performance level instance supports random access with a 70% read and 30% write ratio, an 8 KB block size, and a latency of 1 ms.
  - **Throughput:** For ONTAP 9.16.1 with FCP, each performance level instance supports sequential access with 100% read and a 64 KB block size.
- Latency does not include the following:
  - application or host latency
  - customer network latency to or from the controller ports
  - overheads associated with the data transfer to the object store in case of FabricPool
- Latency values are not applicable to MetroCluster write operations. These write operations are dependent on the distance of remote systems.
- *Expected IOPS* is targeted for FabricPool only if the tiering policy is set to "none" and no blocks are in the cloud. *Expected IOPS* is targeted for volumes that are not in a SnapMirror synchronous relationship.

### Performance service levels for object storage

Supported protocol: S3

Performance service level	Standard	Value
Minimum committed capacity per order	200 TiB	500 TiB
Incremental committed capacity increase	25 TiB	100 TiB
Committed and metered capacity type	Physical	

### Cloud storage

Supported protocols: NFS, CIFS, iSCSI, and S3 (AWS and Azure only)

Performance service level	Cloud Volumes ONTAP
Minimum committed capacity per order	4 TiB

<b>Incremental committed capacity increase</b>	1 TiB
<b>Committed and metered capacity type</b>	Logical



- Cloud native services, such as compute, storage, networking, are invoiced by cloud providers.
- These services are dependent on cloud storage and compute characteristics.

## Related information

- [Supported storage capacities](#)
- [Metrics and definitions used in Keystone Services](#)
- [Keystone pricing](#)

## Capacity requirements for performance service levels

The capacity requirements for Keystone STaaS performance service levels differ between the unified, block-optimized, object, or cloud storage offerings supported by the Keystone STaaS subscription.

### Minimum capacity requirements for unified and block-optimized storage

You can see the minimum capacity and incremental capacity allowed per subscription for unified and block-optimized storage in the following tables:

#### Unified storage

Capacity	Extreme	Premium	Standard	Value
Minimum capacity [in TiB]	50		100	
Incremental capacity (and in multiples) allowed at start of subscription [in TiB]	25			
Incremental capacity (and in multiples) allowed as add-on during subscription [in TiB]	25			

#### Block optimized storage

Capacity	Extreme	Premium
Minimum capacity [in TiB]	50	



Incremental capacity (and in multiples) allowed at start of subscription [in TiB]	25
Incremental capacity (and in multiples) allowed as add-on during subscription [in TiB]	25

The minimum capacity for each performance service level is the same across all Keystone sales.

### Minimum capacity requirements for object storage

You can see the minimum capacity requirements for object storage in the following table:

Capacity	Standard	Value
Minimum capacity [in TiB] per order	200	500
Incremental capacity (and in multiples) allowed at start of subscription [in TiB]	25	100
Incremental capacity (and in multiples) allowed as add-on during subscription [in TiB]	25	100

### Minimum capacity requirements for cloud services

You can see the minimum capacity requirements for cloud services in the following table:

Capacity	Cloud Volumes ONTAP
Minimum capacity [in TiB] per order	4
Incremental capacity (and in multiples) allowed at start of subscription [in TiB]	1
Incremental capacity (and in multiples) allowed as add-on during subscription [in TiB]	1

### Capacity adjustments

Learn more about capacity adjustments:

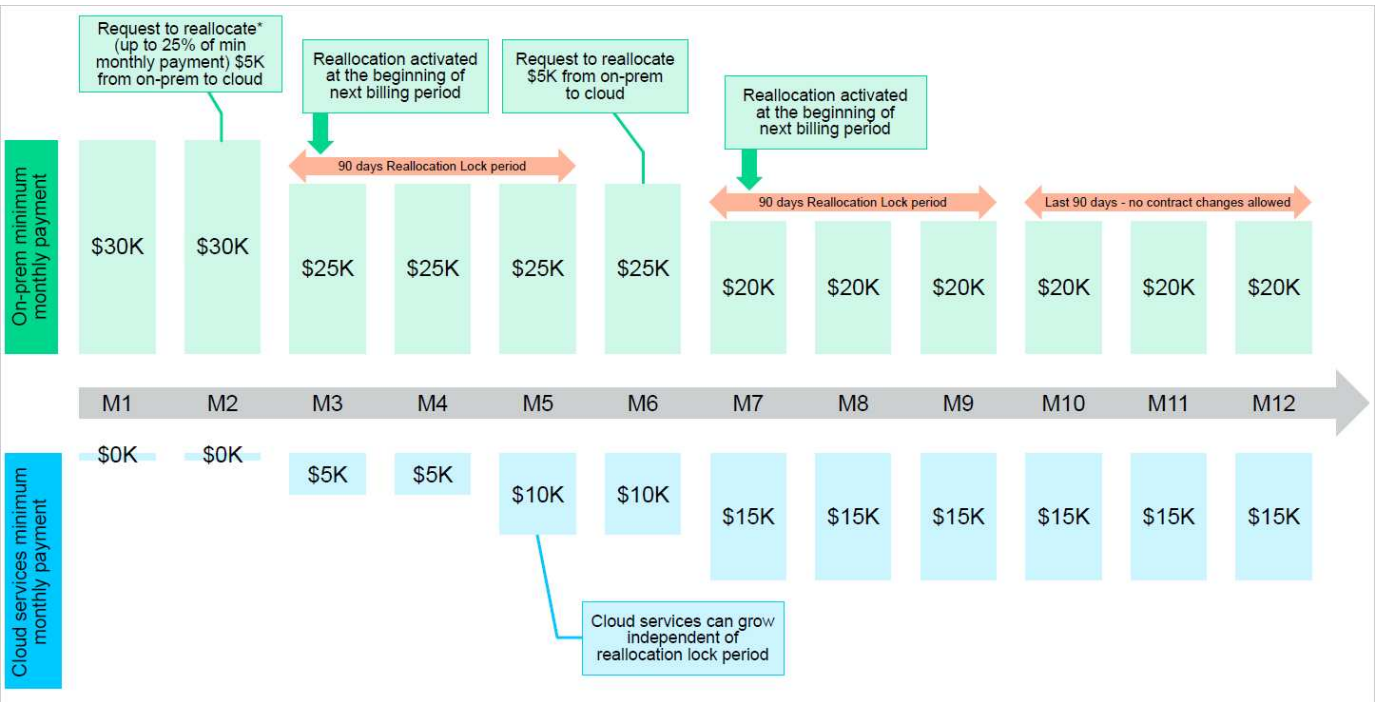
- Capacity can be added anytime during the term, except for the last 90 days of the contract term, in the increments per performance service level as described in the tables in the previous section. Addition of capacity or services is allowed within the last 90 days of the contract term as long as there is a consent of service renewal. Any addition in capacity, new service on-prem or cloud can co-term with the existing term. The invoice sent to you following the activation of the new services reflects the revised billing. Committed

capacity of cloud services cannot be reduced at any point during the subscription term. Meanwhile, committed capacity and committed spend on the on-premises services during the term of the contract can be reduced based on certain criteria as defined in the following section *Capacity reduction*.

- A burst capacity is available at each site, based on the Keystone agreement. Usually, it is set up to 20% above the committed capacity for a performance service level. Any burst usage is billed only for that billing period. If you have additional burst requirement greater than the capacity you agreed upon, contact support.
- Committed capacity can be altered during a contract term, only under certain conditions, as described in the following section *Capacity reduction*.
- Increasing capacity or changing to higher performance service level during a subscription term is allowed. However, moving from a higher performance service level to a lower performance service level is not permitted.
- Any change request in the last 90 days of the service term requires a renewal of the service for a minimum of one year.

### Capacity reduction

Capacity reduction (annual) is applicable to the *Annual in Advance* payment model and on-premises only deployments. It is not available for cloud services or hybrid cloud services. It provides provision for on-premises capacity, which can be reduced by up to 25% per service level per subscription. This reduction is allowed once every year to be made effective at the beginning of the next annual billing period. On-premises service-based annual payments should be  $\geq \$200K$  anytime during the term in order to take advantage of capacity reduction. Because it is supported only for on-premises deployments, this billing model does not provide reallocation in spending from on-premises to cloud services. An example of annual capacity reduction is illustrated in the following image.



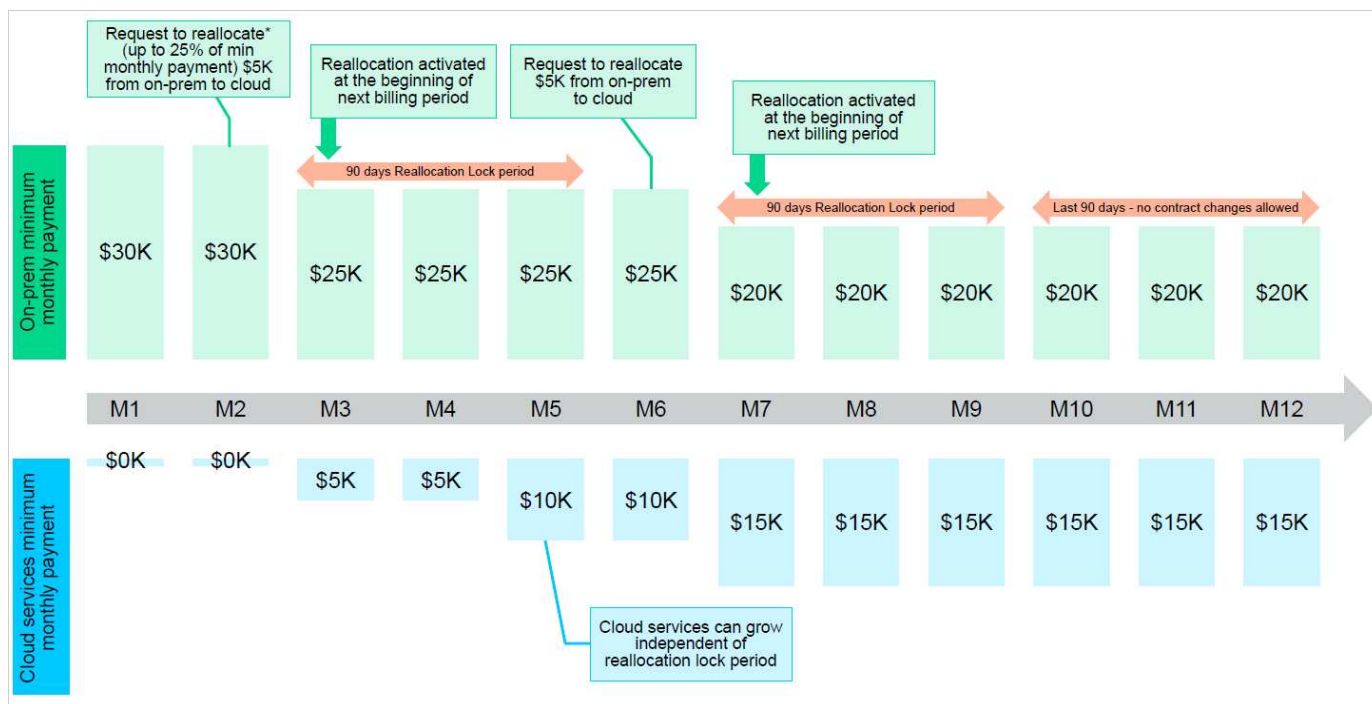
### Quarterly spend reallocation

Keystone STaaS offers you the option to reallocate on-premises service spend to Cloud Volumes ONTAP spend.

## Requirements and conditions at a subscription level:

- Applies only to monthly billing in arrear model.
- Applies only to subscriptions with 1, 2, or 3-year term commitments.
- Capacity for Cloud Volumes ONTAP and Cloud Backup service should be purchased through Keystone.
- Up to 25% of the existing on-premises, service-based monthly payments can be used for reallocation to cloud services.
- Reallocation requests are made effective only after 90 days from the previous activation date of the reallocation.
- Reallocation cannot be done from cloud services back to on-premises services.
- A request to reallocate should be formally submitted by the customer or partner to Keystone Success Manager (KSM) at least one week before the next billing cycle.
- New requests go into effect only from the consecutive billing cycle.

You can allocate a portion of your expenses towards your subscribed file, block, or object storage performance service levels to hybrid cloud storage services. Up to 25% of the Annual Contract Value (ACV) can be reallocated on a quarterly basis to Cloud Volumes ONTAP Primary and Cloud Volumes ONTAP Secondary services:



This table provides a set of sample values to demonstrate how the reallocation of expenses works. In this example, \$5000 from the monthly spend is reallocated to hybrid cloud storage service.

Before allocation	Capacity (TiB)	Monthly designated expense
Extreme	125	37,376
After reallocation	Capacity (TiB)	Monthly designated expense
Extreme	108	37,376
Cloud Volumes ONTAP	47	5,000

		37,376
--	--	--------

The reduction is of  $(125-108) = 17$  TiB of the capacity allocated for the Extreme performance service level. On spend reallocation, the allotted hybrid cloud storage is not of 17 TiB but an equivalent capacity that \$5000 can purchase. In this example, for \$5000, you can get 17 TiB on-prem storage capacity for the Extreme performance service level and 47 TiB hybrid cloud capacity of Cloud Volumes ONTAP performance service level. Therefore, the reallocation is with respect to the spend, not capacity.

Contact your Keystone Success Manager (KSM) if you want to reallocate expenses from your on-premises services to cloud services.

## Add-on services

### Burst capacity options

You can opt for the burst capacity add-on service as part of your NetApp Keystone subscription. This service allows you to increase your burst capacity limits to 40% or 60% above your committed capacity, providing the flexibility to handle unexpected surges in workload demand.

Burst capacity refers to the additional storage capacity that can be utilized beyond the committed capacity of your subscription. It is measured and billed per performance service level. By default, your burst limit is set at 20% above the committed capacity. However, with this add-on service, you can increase the limit to 40% or 60%.

To change your burst limit to 40% or 60%, contact the NetApp Keystone support team.

To learn more about how burst capacity is billed, refer to [Billing based on burst consumption](#).

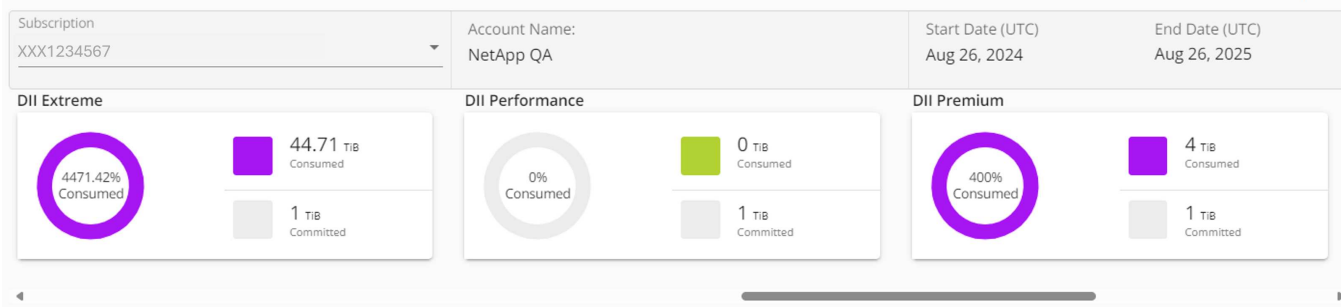
### Learn about Data Infrastructure Insights

NetApp Data Infrastructure Insights (DII, formerly known as Cloud Insights) is an add-on offering for Keystone STaaS. The integration of this service with Keystone STaaS enhances the monitoring, troubleshooting, and optimization capabilities of Keystone-provided storage resources across public clouds and private data centers.

To learn more about Data Infrastructure Insights, refer to [Data Infrastructure Insights documentation](#).

DII is available for both new and existing subscriptions. It can be integrated into a Keystone subscription as an add-on for the committed capacity. When DII is integrated into a Keystone subscription, it will have a corresponding performance service level for each base performance service level in the subscription. For example, Extreme maps to DII Extreme, Premium maps to DII Premium, and Performance maps to DII Performance. These mappings ensure that the DII performance service level aligns with the base performance service level of your Keystone subscription.

A view of DII performance service levels within a **Keystone Subscriptions** widget on the Digital Advisor dashboard:



## Deployment of DII for Keystone

Customers can integrate DII for Keystone in two ways: either as part of an existing instance that monitors other non-Keystone environments, or as part of a new instance. It is the customer's responsibility to set up DII. If help is needed for setting up DII in a complex environment, the account team can engage [NetApp Professional Services](#).

To set up DII, refer to [Data Infrastructure Insights onboarding](#).

Note the following:

- If the customer is starting a new DII instance, it is recommended to begin with a [DII free trial](#). To learn about this feature and the required startup checklist, refer to [Feature Tutorials](#).
- For each site, an Acquisition Unit is required. To install an Acquisition Unit, refer to [Install an Acquisition Unit](#). If the customer already has a DII instance and Acquisition Unit set up, they can proceed with configuring the data collector.
- For each storage hardware deployed, the customer must configure a data collector on the Acquisition Unit. To configure data collectors, refer to [Configure Data Collectors](#). The required data collectors for Keystone storage, based on the underlying hardware, are as follows:

Storage hardware	Data collector
ONTAP Systems	NetApp ONTAP Data Management Software
StorageGRID	NetApp StorageGRID
Cloud Volumes ONTAP	NetApp Cloud Volumes ONTAP

Once configured, the DII instance will begin monitoring the NetApp storage resources deployed as part of Keystone.



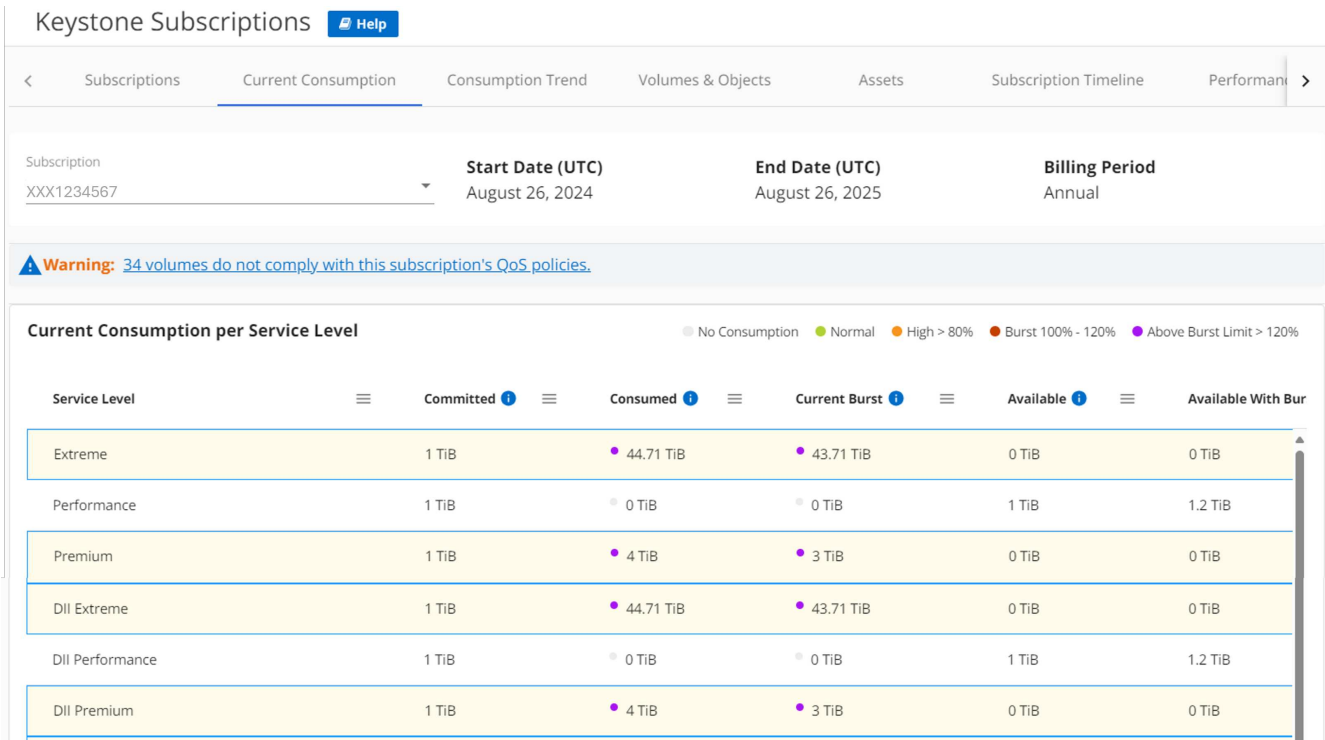
While DII offers extensive monitoring capabilities for the deployed hardware, it does not provide insights into your Keystone subscription, such as subscription usage or details on performance service levels. For subscription insights, see [Keystone dashboard and reporting](#).

## Billing and metering

The following outlines the billing and metering details of the DII add-on service:

- This service is measured in the same way as your main subscription. For example, if your main subscription includes 100 TiB of Extreme service and 100 TiB of Premium service, both measured on a logical usage basis, the add-on services, DII Extreme 100 TiB and DII Premium 100 TiB, are also

measured on a logical usage basis. If your main subscription is measured on a provisioned basis, the add-on service is measured the same way for the same capacity. The add-on service will follow the same measurement method as your main subscription.



- This service is metered and invoiced along with your Keystone subscription on the same invoice. If you configure DII for Keystone before activating your Keystone subscription, billing still begins from the Keystone subscription activation date, or the modification date for existing subscriptions.
- This service is metered and invoiced based on both committed capacity and burst usage for DII performance service levels, in addition to the standard Keystone invoice. The metering of this add-on service follows the same methodology as the underlying Keystone subscription performance service level, which could be logical, provisioned, or physical.
- This service ends with the Keystone subscription to which it is linked. At renewal, you can choose whether to renew the add-on service. If you don't renew the Keystone subscription, the monitored hardware is decommissioned, and the add-on service automatically terminates.

Support and user access

Approved NetApp Support team members can access the customer's DII instance if the customer enables the **Allow NetApp Access to your Data Infrastructure Insights Environment** option. To do so, go to **Help > Support**, and enable the option.

**NetApp Data Infrastructure Insights** Tutorial 0% Complete Getting Started

Tenant Name: NetApp PCS Sandbox

**Support**

When opening a support ticket please include the URL of the client tenant.

**Technical Support:**  
[Live Chat](#) | [Open a Support Ticket](#) | [Phone\(P1\)](#)

**Sales:**  
 Have questions regarding your subscription? [Contact Sales](#).

**Support Entitlement**

**Data Infrastructure Insights Serial Number:**  
 [Redacted]

**Data Infrastructure Insights Subscription Name:**  
 [Redacted]

**Support Level:**  
 Not registered - [Register Now](#)

☒ Allow NetApp access to your Data Infrastructure Insights Environment. ?

**Feedback**

We value your input. [Your feedback](#) helps us improve Data Infrastructure Insights.

**Documentation**

**Documentation Center**  
 Visit the [Data Infrastructure Insights](#) documentation to find any step by step instructions to get started with Data Infrastructure Insights.

**Knowledge Base:**  
 Search through the articles.

**What's New:**  
 See [What's New with Data Infrastructure Insights](#) to find recent product updates and changes.

**API Access:**  
 To Integrate Data Infrastructure Insights with other applications see the Data Infrastructure Insights [API List](#) and [documentation](#).

**Proxy Settings**

Need to setup proxy exceptions? Click [here](#) to learn more.

**Learning Center**

**Data Infrastructure Insights Course List:**

- Hybrid Cloud Resource Management
- Data Infrastructure Insights Fundamentals
- Cloud Resource Management
- Storage Workload Security

Customers can provide access to internal or external users from the **User Management** screen using the **+ User** option.

**NetApp Data Infrastructure Insights** Tutorial 0% Complete Getting Started

Tenant Name: NetApp PCS Sandbox

**Admin / User Management**

SSO Auto Provisioning: **Enabled**

**Users (55)** ☐ Show SSO Auto Provisioning Users

[Restrict Domains](#) **+ User**

Name ↓	Email	Observability Role	Workload Security Role	Reporting Role	Last Login
[Redacted]	[Redacted]	Administrator	Administrator	Administrator	8 days ago
[Redacted]	[Redacted]	Administrator	Administrator	No Access	3 hours ago
[Redacted]	[Redacted]	Administrator	Administrator	Administrator	21 hours ago
[Redacted]	[Redacted]	Administrator	Administrator	Administrator	21 hours ago
[Redacted]	[Redacted]	Administrator	Administrator	Administrator	a day ago
[Redacted]	[Redacted]	Administrator	Administrator	Administrator	4 days ago
[Redacted]	[Redacted]	Administrator	Administrator	Administrator	4 minutes ago
[Redacted]	[Redacted]	Administrator	Administrator	Guest	10 days ago
[Redacted]	[Redacted]	Administrator	Administrator	Guest	3 days ago
[Redacted]	[Redacted]	Administrator	No Access	User	2 minutes ago
[Redacted]	[Redacted]	Administrator	Administrator	Administrator	2 days ago
[Redacted]	[Redacted]	Administrator	Administrator	Administrator	an hour ago
[Redacted]	[Redacted]	Administrator	Administrator	No Access	15 days ago

## Learn about data tiering

Keystone STaaS standard services for file and block storage include tiering capabilities that identify less-frequently used data, and tiers it to Keystone STaaS-supported NetApp cold storage. You can use data tiering as an add-on service if you want to tier your cold



data to any Keystone STaaS-supported, non-NetApp storage.

For information about standard and add-on services, see [Keystone STaaS services](#).

For information about performance service Levels, see [Performance service levels in Keystone](#).



The tiering add-on service is required only when data is tiered to any non-NetApp storage such as Amazon Web Services (AWS) S3, Azure Blob, Google Cloud Platform (GCP), and other Keystone STaaS-supported, S3-compatible, third party object storage.

The tiering capability leverages the NetApp FabricPool technology that enables automated tiering of infrequently accessed data to object storage tiers on and off premises.

The add-on data tiering service enables tiering from Extreme, Premium, Performance, Standard, and Value tier to an object storage target. The ratio of hot to cold data to be tiered is not fixed, and each tier is metered and invoiced separately.

For example, if the target for cold storage tier is:

- Keystone STaaS Value tier, Keystone STaaS StorageGRID Object Tier, or existing StorageGRID Webscale (SGWS) grid (customer owned) - There is no additional charge; it is part of the standard service.
- Public cloud (AWS, Azure, Google) or Keystone STaaS-supported, third party object storage - There is an additional charge for data capacity that is tiered to cold storage target.

The charges for add-on tiering services apply through the entire subscription term.



Hyperscaler-based compute, storage, and network services required by Cloud Volumes ONTAP are not provided by NetApp as a part of Keystone STaaS subscriptions; these services need to be procured directly from hyperscaler cloud service providers.

## Related information

[How to approximate Keystone consumption with data tiering \(FabricPool\) using the ONTAP CLI](#)

## Non-returnable, non-volatile components, and SnapLock compliance

As a part of your NetApp Keystone subscription, NetApp extends the non-returnable, non-volatile components (NRNVC) offering for your file, block, and object services.

NetApp does not recover the physical storage media used during the entire service tenure or at service termination when NetApp otherwise recovers all of its physical assets used in the delivery of the service.

You can subscribe to this add-on service as a part of your Keystone subscription. If you have purchased this service, note the following:

- You do not need to return any drives and nonvolatile memory at end of the service term or if they failed or were found defective during the service term.
- However, you need to produce a certificate of destruction for the drives and/or nonvolatile memory and cannot be used for any other purpose.
- The additional cost associated with the NRNVC is charged as a percentage of the total subscription services (includes standard service, Advanced Data Protection, and data tiering) monthly bill.
- This service is applicable only to file, block, and object services.



For information about the standard and cloud services, see [Keystone STaaS services](#).

For information about performance service Levels, see [Performance service Levels in Keystone](#).

## SnapLock compliance

The SnapLock technology enables the NRNVC feature by making the drive unusable after the expiry date set in the volume. For using the SnapLock technology on your volumes, you need to subscribe to NRNVC. This is applicable only to file and block services.

For information about SnapLock technology, see [What SnapLock is](#).

## Learn about USPS

United States Protected Support (USPS) is an add-on offering for NetApp Keystone Subscriptions. It entitles you to receive delivery and support of ongoing Keystone services from U.S. citizens on U.S. soil.

Read the following sections to understand which elements of your subscriptions are bound by this add-on service and are provided under the terms of NetApp Keystone Agreement. <sup>[1]</sup>

### NetApp USPS monitoring

NetApp USPS Keystone support team monitors the health of your products and subscribed services, provides remote support, and collaborates with your Keystone Success Manager. All personnel monitoring the products associated with the relevant Keystone subscription orders are U.S. citizens operating on U.S. soil.

### Keystone Success Manager

The Keystone Success Manager (KSM) is a U.S. citizen operating on U.S. soil. Their responsibilities are specified in your NetApp Keystone Agreement.

### Deployment activities

Where available, onsite and remote deployment and installation activities are conducted by U.S. citizens on U.S. soil. <sup>[2]</sup>

### Support

Where available, the necessary onsite troubleshooting and support activities are conducted by U.S. citizens on U.S. soil. <sup>[2]</sup>

## Keystone STaaS SLO

### Availability SLO

Availability SLO targets an uptime of 99.999% during a billing period for all NetApp ONTAP flash storage arrays deployed to deliver the Keystone order.

### Metrics

- **Monthly uptime percentage** = [(number of eligible seconds in a month - average of number of seconds of

downtimes for all AFF storage arrays deployed to deliver the Keystone order in that month) / number of eligible seconds in a month] x 100%

- **Downtime:** The period of time when both controllers in a pair within a storage array are not available, as determined by NetApp.
- **Eligible number of seconds:** These are seconds in a month that count towards the uptime calculation. It does not include the time period when the STaaS services are not available because of planned maintenance, upgrades, support activities agreed upon with NetApp, or due to circumstances that are beyond control or responsibility of NetApp or Keystone services.

## Performance service levels

All performance service levels that ONTAP flash storage arrays support are eligible for Availability SLO. To learn more, refer to [Performance service levels in Keystone](#).

## Service credits



SLAs and guarantees are available on a nomination basis.

If the availability of ONTAP flash storage arrays for eligible subscriptions falls below the 99.999% monthly uptime target within a billing period, then NetApp issues service credits as follows:

Monthly uptime (less than)	Service credit
99.999%	5%
99.99%	10%
99.9%	25%
99.0%	50%

## Service credit calculation

Service credits are determined using the following formula:

Service credits = (impacted capacity / total committed capacity) X capacity fees X credit percentage

Where:

- **impacted capacity:** The amount of stored capacity affected.
- **total committed capacity:** The committed capacity for the performance service level for the Keystone order.
- **capacity fees:** The fees for the affected performance service level for the month.
- **credit percentage:** The predetermined percentage for service credit.

## Example

The following example shows the method of calculation for service credits:

1. Calculate monthly uptime to determine the service credit percentage :

- Eligible seconds in a 30-day month: 30 (days) X 24 (hours/day) X 60 (minutes/hour) X 60 (seconds/minute) = 2,592,000 seconds
- Downtime in seconds: 95 seconds

Using the formula:

$$\text{Monthly uptime percentage} = [(2,592,000 - 95)/(2,592,000)] \times 100$$

Based on calculation, the monthly uptime will be 99.996%, and the service credit percentage will be 5%.

## 2. Calculate service credits:

Service level	Impacted capacity	Total committed capacity	Capacity fees	Credit percentage
Extreme	10 Tib for 95 seconds	100 Tib	\$1000	5%

Using the formula:

$$\text{Service credits} = (10 / 100) \times 1000 \times 0.05$$

Based on calculation, the service credits will be \$5.

## Service credit request

If a breach of the SLA is detected, open a priority 3 (P3) support ticket with NetApp Keystone support.

- The following details are required:
  - a. Keystone subscription number
  - b. Volumes and storage controller details
  - c. Site, time, date, and description of the issue
  - d. Calculated time duration of latency detection
  - e. Measurement tools and methods
  - f. Any other applicable document
- Provide the details in the excel sheet as shown below for a P3 ticket opened with NetApp Keystone support.

	A	B	C	D	E
1	Subscription_No	Service_level	Volume_uuid	Date	Is_SLB_Breached
2	192037XXX	premium	fxxxxb1-fxxb-xxed-axxx-dxxxexxxxxx5	2024-01-01	Yes
3	192037XXX	premium	fxxxxb1-fxxb-xxed-axxx-dxxxexxxxxx6	2024-01-02	Yes
4	192037XXX	premium	fxxxxb1-fxxb-xxed-axxx-dxxxexxxxxx7	2024-01-03	Yes
5	192037XXX	premium	fxxxxb1-fxxb-xxed-axxx-dxxxexxxxxx8	2024-01-06	Yes
6	192037XXX	premium	fxxxxb1-fxxb-xxed-axxx-dxxxexxxxxx9	2024-01-17	Yes



- A service credit request should be initiated within six weeks after NetApp Keystone support has validated a breach. All service credits should be acknowledged and approved by NetApp.
- Service credits may be applied to a future invoice. Service credits do not apply to expired Keystone subscriptions. To learn more, refer to [NetApp Keystone support](#).

## Performance SLO

NetApp Keystone offers latency-based SLO per performance service level, as described in the Keystone order for consumed capacity up to the burst limit, according to the following listed terms and conditions.

### Metrics

- **Degraded performance:** The amount of time, in minutes, per incident, during which the 90<sup>th</sup> percentile latency target is not met.
- The **90<sup>th</sup> percentile latency** is measured per volume, per performance level, for all volumes within a Keystone Order. Latency is sampled every five minutes, and the 90<sup>th</sup> percentile value calculated over a 24-hour period is used as the daily measure, considering the following points:
  - The volumes that record at least five IOPS at the time of metrics collection are considered for a sample.
  - Volumes with greater than 30% write operations at the time of metrics collection are excluded from the sample.
  - Latency added by AQoS for requested IOPS/TiB that is greater than target IOPS/TiB are excluded from the sample.
  - Latency added by AQoS to maintain minimum IOPS per volume are excluded from the sample.
  - For volumes that have FabricPool enabled, the latency incurred due to the transfer of data to and from the target (cold) storage is not counted.
  - Latency caused by the application, host, or customer network outside of the ONTAP cluster is not counted.
  - During a 24-hour period, at least ten valid metrics should be available. If not, the metrics will be discarded.
  - If one or more volumes on a storage array do not have a valid AQoS policy applied, then number of IOPS available to other volumes may be affected, and NetApp will not be responsible for targeting or meeting performance levels on that storage array.
  - In FabricPool configurations, performance levels are applicable when all requested data blocks are on FabricPool source (hot) storage and the source storage is not in a SnapMirror Synchronous relationship.

### Performance service levels

All performance service levels that ONTAP flash storage arrays support are eligible for Performance SLO and guarantee meeting the following target latency:

Service level	Extreme	Premium	Performance	Standard
---------------	---------	---------	-------------	----------

<b>Target 90<sup>th</sup> percentile latency</b>	<1ms	<2ms	<4ms	<4ms
--	------	------	------	------

To learn more about the latency requirements of the performance service levels, refer to [Performance service Levels in Keystone](#).

## Service credits



SLAs and guarantees are available on a nomination basis.

NetApp issues service credits for the degraded performance:

Performance threshold	Service credit
90 <sup>th</sup> percentile latency > target latency	3% for each calendar day of occurrence

## Service credit calculation

Service credits are determined using the following formula:

Service credits = (impacted capacity / total committed capacity) X capacity fees X affected days X credit percentage

Where:

- **impacted capacity:** The amount of stored capacity affected.
- **total committed capacity:** The committed capacity for the performance service level for the Keystone order.
- **capacity fees:** The fees for the affected performance level as per the Keystone order.
- **affected days:** The number of calendar days impacted.
- **credit percentage:** The predetermined percentage for service credit.

## Example

The following example shows the method of calculation for service credits:

Service level	Impacted capacity	Total committed capacity	Capacity fees	Affected calendar days	Credit percentage
Extreme	10 Tib	50 Tib	\$1000	2	3%

Using the formula:

Service credits = ( 10 / 50 ) X 1000 x 2 x 0.03

Based on calculation, the service credits will be \$12.

## Service credit request

If a breach of the SLA is detected, open a priority 3 (P3) support ticket with NetApp Keystone support.

- The following details are required:
  - a. Keystone subscription number
  - b. Volumes and storage controller details
  - c. Site, time, date, and description of the issue
  - d. Calculated time duration of latency detection
  - e. Measurement tools and methods
  - f. Any other applicable document
- Provide the details in the excel sheet as shown below for a P3 ticket opened with NetApp Keystone support.

	A	B	C	D	E
1	Subscription_No	Service_level	Volume_uuid	Date	Is_SLB_Breached
2	192037XXX	premium	fxxxxb1-fxb-xxed-axxx-dxxxexxxxxx5	2024-01-01	Yes
3	192037XXX	premium	fxxxxb1-fxb-xxed-axxx-dxxxexxxxxx6	2024-01-02	Yes
4	192037XXX	premium	fxxxxb1-fxb-xxed-axxx-dxxxexxxxxx7	2024-01-03	Yes
5	192037XXX	premium	fxxxxb1-fxb-xxed-axxx-dxxxexxxxxx8	2024-01-06	Yes
6	192037XXX	premium	fxxxxb1-fxb-xxed-axxx-dxxxexxxxxx9	2024-01-17	Yes



- A service credit request should be initiated within six weeks after NetApp Keystone support has validated a breach. All service credits should be acknowledged and approved by NetApp.
- Service credits may be applied to a future invoice. Service credits do not apply to expired Keystone subscriptions. To learn more, refer to [NetApp Keystone support](#).

## Sustainability SLO

NetApp Keystone delivers a guaranteed measurement of maximum number of actual watts per terabyte (W/TiB) for storage services based on ONTAP flash storage arrays with Sustainability SLO. Sustainability SLO defines the maximum consumption of W/TiB for each eligible performance service level, helping organizations meet their sustainability goals.

### Metrics

- **Watts:** The power consumption reported from daily AutoSupport, including the usage by the controller and attached disk shelves.
- **Tebibyte:** The maximum of:
  - the committed capacity + allocated burst capacity for the performance service level, or
  - the effective deployed capacity, assuming a storage efficiency factor of 2 : 1.

To learn more about storage efficiency ratio, refer to [Analyze capacity and storage efficiency savings](#).

Performance service levels

Sustainability SLO is based on the following consumption criteria:

Service level	SLO criteria	Minimum committed capacity	Platform
Extreme	<= 8 W/TiB	200 TiB	AFF A800 and AFF A900
Premium	<= 4 W/TiB	300 TiB	AFF A800 and AFF A900
Performance	<= 4 W/TiB	300 TiB	AFF A800 and AFF A900

To learn more, refer to [Performance service levels in Keystone](#).

Service credits



SLAs and guarantees are available on a nomination basis.

If W/TiB consumption during a billing period fails to meet the SLA criteria, then NetApp issues service credits as follows:

Days SLA missed in billing period	Service credit
1 to 2	3%
3 to 7	15%
14	50%

Service credit request

If a breach of the SLA is detected, open a priority 3 (P3) support ticket with NetApp Keystone support, and provide the details as requested in the excel sheet as shown below:

	A	B	C	D	E
1	Subscription_No	Service_level	Volume_uuid	Date	Is_SLB_Breached
2	192037XXX	premium	fxxxxb1-fxb-xxed-axxx-dxxxexxxxxx5	2024-01-01	Yes
3	192037XXX	premium	fxxxxb1-fxb-xxed-axxx-dxxxexxxxxx6	2024-01-02	Yes
4	192037XXX	premium	fxxxxb1-fxb-xxed-axxx-dxxxexxxxxx7	2024-01-03	Yes
5	192037XXX	premium	fxxxxb1-fxb-xxed-axxx-dxxxexxxxxx8	2024-01-06	Yes
6	192037XXX	premium	fxxxxb1-fxb-xxed-axxx-dxxxexxxxxx9	2024-01-17	Yes



- A service credit request should be initiated within six weeks after NetApp Keystone support has validated a breach. All service credits should be acknowledged and approved by NetApp.
- Service credits may be applied to a future invoice. Service credits do not apply to expired Keystone subscriptions. To learn more, refer to [NetApp Keystone support](#).

## Ransomware Recovery Guarantee

NetApp guarantees the recovery of Snapshot data from SnapLock Compliance volumes in the event of a ransomware attack with the Ransomware Recovery Guarantee program. NetApp Ransomware Recovery Assurance Service is required to support the Ransomware Recovery Guarantee program and should be purchased separately from the associated Keystone order.

### Service levels

Ransomware Recovery Assurance Service is required for all hardware supporting the Keystone subscription for the duration of the applicable subscription term.

### Service credits



SLAs and guarantees are available on a nomination basis.

If SnapLock Compliance is deployed as per best practices, and NetApp professional services either configure it or validate it upon the purchase of Ransomware Recovery Assurance Service, then NetApp issues the service credits if the data protected by SnapLock is not recoverable. The criteria for these credits are as follows:

- Service credits can be applied to future invoices. The credits are capped at 10% of the Committed Contract Value (CCV) and are paid out on a per-subscription basis.
- Credits are provided during the active subscription term of the relevant Keystone order.
- For subscriptions with monthly billing, the credits will be divided over the next 12 months and can be used for any future Keystone invoices until the end of the subscription term. If the subscription ends in less than 12 months, it can be renewed to continue using the credits, or the credits can be applied to other NetApp invoices.
- For annual subscriptions, the credits will be applied to the next Keystone invoice, if available. If there are no future Keystone invoices, the credits can be applied to other NetApp invoices.

## Billing

### Keystone pricing

The NetApp Keystone STaaS pay-as-you-go subscription service offers flexible and scalable consumption with predictable and upfront pricing for your storage requirements.

Keystone provides you with the following billing facilities:

- You can pay based on IOPS and latency committed capacity to meet various workload needs. The different performance service tiers - Extreme, Premium, Standard, Value, Object, and Cloud Volumes ONTAP enable you to manage your storage based on your purchased service level.



- It presents predictable billing for the committed capacity and pay-per-use for variable (burst) capacity usage.
- You can select a bundle price for hardware, core OS, and support for one \$/TiB price. You have a single invoice for each storage type, unified, block, optimized, object, or cloud storage services.
- You can select a flexible term for the services and payment options, such as monthly, quarterly, semi-annual, or annual.

Keystone billing is based on committed capacity and variable burst consumption.

For information about different capacities supported in Keystone, see [Supported storage capacities in Keystone](#).

## Related information

- [Billing based on committed capacity](#)
- [Metering based on consumed capacity](#)
- [Billing based on burst consumption](#)
- [Billing based on miscellaneous volume types](#)
- [Billing schedules](#)

## Billing based on committed capacity

Committed capacity is the capacity committed for a particular performance service level while purchasing the subscription.

Committed capacity can be the total capacity for various performance service levels in a single subscription, as accepted by you and NetApp/partner. This capacity is stated on each Keystone order and is billed, regardless of the actual capacity consumption.

For information about different capacities supported in Keystone, see [Supported storage capacities in Keystone](#).

## Metering based on consumed capacity

Keystone STaaS has metering based on the capacity consumed by you during your service usage. Consumed capacity is the capacity that your workloads actually use.

As a part of the Keystone service deployment, NetApp continuously monitors and measures the consumption of the service. At least once in every five minutes, a consumption record is generated by the system, detailing the current consumed capacity for your subscription. These records are aggregated over the billing period to generate invoices and usage reports.

For information about different capacities supported in Keystone, see [Supported storage capacities in Keystone](#).

## Billing based on burst consumption

Keystone STaaS billing is based on *burst capacity*, which is the capacity consumed by you, on top of the committed capacity of your subscription.

Your burst limit is determined and specified in your Keystone agreement. By default, it is set at 20% above the committed capacity. You also have the option to choose burst capacity limits of 40% or 60% of the committed capacity. To learn more, refer to [Burst capacity increase options](#).

Committed capacity is the capacity committed to you while purchasing the subscription. The committed capacity and burst capacity are measured per performance service level. Consumed capacity is the capacity that your workloads actually use.

When the consumed capacity is greater than the committed capacity for a performance service level, burst consumption is recorded and charged accordingly. The usage above the burst capacity is indicated as "Above Burst Limit".

This process occurs for each consumption record generated. Burst consumption, therefore, is a reflection of both the amount and tenure of your over-consumed capacities on top of your committed capacities. To learn more, refer to [View consumption trends of your Keystone subscriptions](#).

For information about different capacities supported in Keystone, see [Supported storage capacities in Keystone](#).

## **Miscellaneous scenarios for Keystone billing**

Understanding Keystone billing for specific configurations can help you optimize service usage and manage costs. The configurations include cloned volumes, temporary volumes, SnapMirror destinations, LUNs, and system/root volumes.

### **Billing for cloned volumes**

If volumes are cloned in ONTAP and you use them for backing up and restoring your data, you can continue using the clones without any additional payments. However, cloned volumes used for any other purpose in your business for an extensive duration are charged.

Note the following:

- Clone volumes are free from charging as long as their size is less than 10% of the parent volume (the physical capacity used in the clone volume compared to the physical capacity used in the parent volume).
- There is no 24-hour grace period for cloned volumes. Only the size of the clone is considered.
- Once the clone volume exceeds 10% of the physical size of the parent, the clone is billed as a standard volume (logical used capacity).

### **Billing for temporary volumes**

Occasionally, temporary (TMP) volumes are created by ONTAP when moving volumes. These temporary volumes are short-lived, and the consumption on these volumes is not measured for billing.

### **Billing for SnapMirror destinations**

The pricing for SnapMirror destination volumes, whether used for disaster recovery or long-term retention, is based on the performance service level assigned to the destination. There is no extra fee for data protection.

### **Billing for LUNs**

For LUNs, the billing is based on the performance service levels of the volume.

## System and root volumes

System and root volumes are monitored as a part of the overall monitoring of the Keystone service but are not counted or billed. The consumption on these volumes is exempted for billing.

## Billing schedules

Keystone STaaS subscriptions are billed on a monthly, quarterly, semi-annually, or annually basis.

### Monthly billing

Invoices are sent monthly. For the month in which the services are availed, an invoice is sent in the next month. For example, the invoice for the services you have used in January is delivered at the beginning of February. This invoice includes the charges for the committed capacity and if applicable, any burst usage.

### Quarterly, semi-annually, and annually billing

For quarterly, semi-annually, and annually billing, the process is similar with slight variations in timing:

- **Quarterly billing:** An invoice is generated at the beginning of each subscription quarter for the minimum payment of the committed capacity. Another invoice is sent at the end of the quarter for any burst usage accrued.
- **Semi-annually billing:** An invoice is generated at the beginning of every six months for the minimum payment of the committed capacity. Another invoice is sent at the end of each quarter for any burst usage accrued.
- **Annually billing:** An invoice is generated at the beginning of each subscription year for the minimum payment of the committed capacity. Another invoice is sent at the end of each quarter for any burst usage accrued.

For quarterly, semi-annually, and annually billing, if the committed capacity is changed during a subscription, an invoice is sent on the same day for the prorated minimum payments for the rest of that subscription year. Billing is calculated from the day the change in committed capacity becomes effective.

[1] The services and offerings described here are subject to, and limited and governed by a fully-executed Keystone Agreement.

[2] Availability of appropriate personnel for onsite activities is dependent on the geographical location at which the Keystone systems are deployed.

# Access Keystone from Digital Advisor REST API

## Get started using the Digital Advisor REST API to retrieve Keystone data

Digital Advisor REST API provides a programmatic interface for retrieving Keystone subscription and consumption details.

At a high level, the workflow to interact with Digital Advisor REST API involves the following steps:

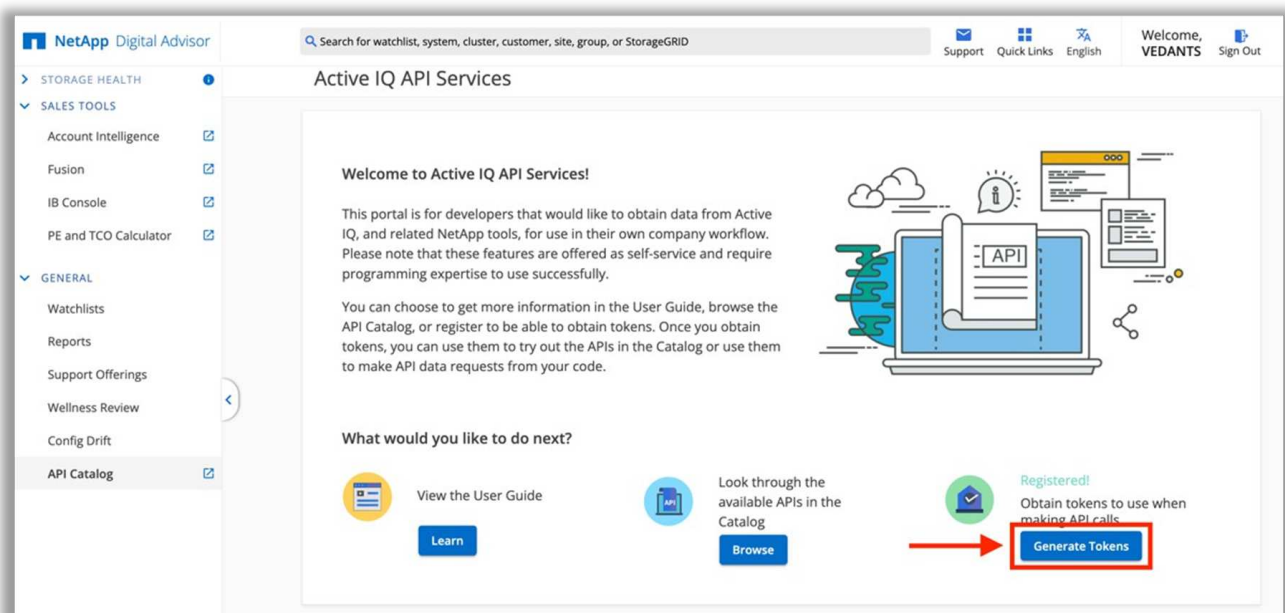
1. Set up your Digital Advisor account. You must have valid NetApp Support site credentials to log in to Digital Advisor. To learn more, refer to [Log in to Digital Advisor](#).
2. Understand the two-step authentication process.
  - a. **Generate a refresh token:** A refresh token is obtained through Digital Advisor console using NetApp credentials. This token is used to ensure continuous access without the need for repeated logins.
  - b. **Generate an access token:** The refresh token is used to generate access tokens. An access token is required to authorize API calls to the Keystone service and is valid for one hour.
3. Execute an API call to retrieve the desired data. You can programmatically retrieve lists of customers, customer subscription data, and customer consumption details.

## Generate refresh and access tokens

A refresh token is used to programmatically obtain a new set of access tokens and is good for one week or until it has been used to obtain a new set of tokens.

Steps to generate a refresh token using the Digital Advisor portal are as follows:

1. Log in to the [Digital Advisor portal](#) using NetApp credentials and select **Generate Tokens**.



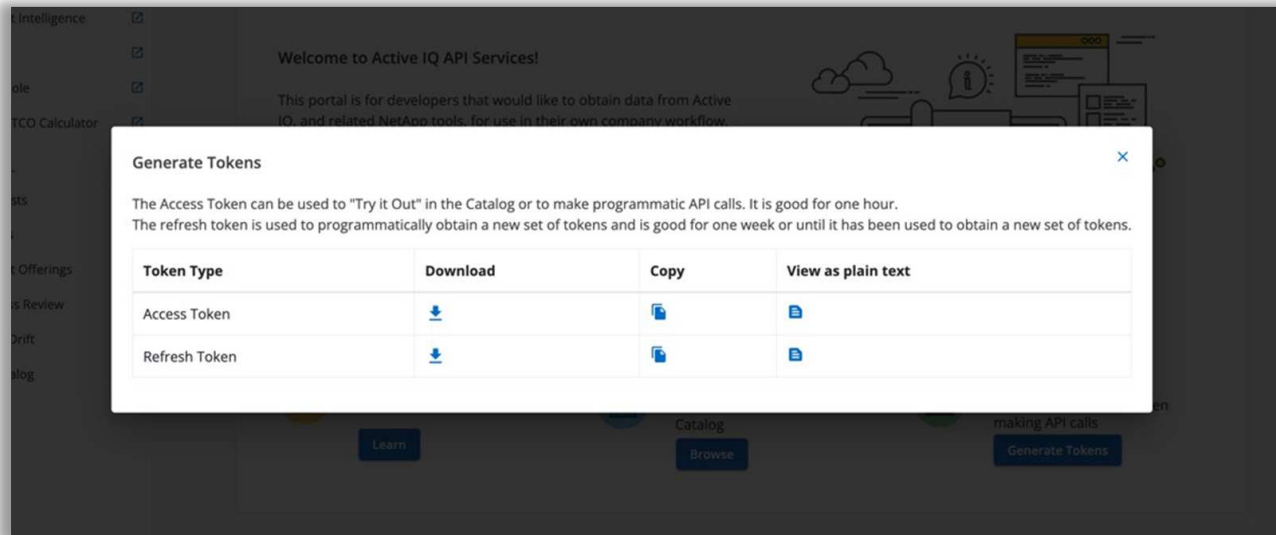


For first-time users, if **Generate Tokens** option is not available, select **Register** to submit an authorization request. Fill out the registration form to enable the functionality.

2. The system generates an access token and a refresh token. Save the refresh token on a trusted platform.



The portal gives you multiple ways to save one or both tokens in the set. You can copy them to clipboard, download them as a text file, or view them as plain text.



## Generate access token using the Digital Advisor REST API

The access token is used to authenticate Digital Advisor API requests. It can be generated directly through the console along with the refresh token or using the following API call:

### Request:

<b>Method</b>	POST
<b>Endpoint</b>	<a href="https://api.activeiq.netapp.com/v1/tokens/accessToken">https://api.activeiq.netapp.com/v1/tokens/accessToken</a>
<b>Headers</b>	<ul style="list-style-type: none"> <li>• accept: application/json</li> <li>• Content-Type: application/json</li> </ul>
<b>Request Body</b>	<pre>{   "refresh_token": "&lt;refresh-token&gt;" }</pre>



You should have administrative privileges for Digital Advisor to access this endpoint.

### Response:

API returns an access token and a refresh token in a JSON format as response.

```
{
  "refresh_token": "string",
  "access_token": "string"
}
```

**Status code:** 200 – Successful request

**Curl example:**

```
curl -X 'POST' \ 'https://api.activeiq.netapp.com/v1/tokens/accessToken' \
-H 'accept: application/json' \ -H 'Content-Type: application/json' \ -d '
{ "refresh_token": "<refresh-token>" }'
```

## Execute the API call

Upon successful generation of an access token, authorized Digital Advisor API calls can be executed for the required information.

## Get a list of all customers using the Digital Advisor REST API

This API retrieves a list of all the customerIDs associated with the user.

**Request:**

<b>Method</b>	GET
<b>Endpoint</b>	<a href="https://api.activeiq.netapp.com/v1/keystone/customers">https://api.activeiq.netapp.com/v1/keystone/customers</a>
<b>Headers</b>	<ul style="list-style-type: none"><li>• accept: application/json</li><li>• authorizationToken: &lt;access_key&gt;</li></ul>

**Response:**

The API will respond with a JSON object containing a list of customer names and respective IDs. Here's an example response:

```
{
  "results": {
    "returned_records": 0,
    "records": [
      {
        "Customers": [
          {
            "customer_id": "string",
            "customer_name": "string"
          }
        ]
      }
    ],
    "request_id": "string",
    "response_time": "string"
  }
}
```

**Status code:** 200 – Successful request

**Curl example:**

```
curl -X 'GET' \ 'https://api.activeiq.netapp.com/v1/keystone/customers' \
-H 'accept: application/json' -H 'authorizationToken: <access-key>'
```

## Get customer subscriptions using the Digital Advisor REST API

This API retrieves a list of all the subscriptions and service levels associated with the given customerID.

**Request:**

<b>Method</b>	GET
<b>Endpoint</b>	<a href="https://api.activeiq.netapp.com/v1/keystone/customer/subscriptions-info">https://api.activeiq.netapp.com/v1/keystone/customer/subscriptions-info</a>
<b>Parameters</b>	<ul style="list-style-type: none"> <li>• type: "customer"</li> <li>• id: &lt;customer-id&gt;</li> </ul>
<b>Headers</b>	<ul style="list-style-type: none"> <li>• accept: application/json</li> <li>• authorizationToken: &lt;access_key&gt;</li> </ul>

**Response:**

The API will respond with a JSON object containing a list of all the subscriptions and associated service level details for the given customer. Here's an example response:

```
[
{
  "results": {
    "returned_records": 0,
    "records": [
      {
        "subscription": {
          "account_name": "string",
          "number": "string",
          "start_date": "2024-05-28T15:47:49.254Z",
          "end_date": "2024-05-28T15:47:49.255Z"
        },
        "service_levels": [
          {
            "name": "string",
            "committed_tib": 0
          }
        ]
      },
      {
        "request_id": "string",
        "response_time": "string"
      }
    ]
  }
}
```

**Status code:** 200 – Successful request

**Curl example:**

```
curl -X 'GET' \
'https://api.activeiq.netapp.com/v1/keystone/customer/subscriptions-
info?type=customer&id=<customerID>' \ -H 'accept: application/json' \ -H
'authorizationToken: <access-key>'
```

## Get customer consumption details using the Digital Advisor REST API

This API retrieves the current consumption details for all the subscriptions associated with the given customerID.



**Request:**

<b>Method</b>	GET
<b>EndPoint</b>	<a href="https://api.activeiq.netapp.com/v1/keystone/customer/consumption-details">https://api.activeiq.netapp.com/v1/keystone/customer/consumption-details</a>
<b>Parameters</b>	<ul style="list-style-type: none"><li>• type: "customer"</li><li>• id: &lt;customer-id&gt;</li></ul>
<b>Headers</b>	<ul style="list-style-type: none"><li>• accept: application/json</li><li>• authorizationToken: &lt;access_key&gt;</li></ul>

**Response:**

The API will respond with a JSON object containing a list of all the subscriptions with the current service usage metrics for the given customer. Here's an example response:

```
{
  "result": {
    "returned_records": "string",
    "records": [
      {
        "subscription": {
          "account_name": "string",
          "number": "string",
          "start_date": "string",
          "end_date": "string"
        },
        "service_levels": [
          {
            "name": "string",
            "committed_tib": "string",
            "consumed_tib": "string",
            "consumed_timestamp_utc": "string",
            "burst_tib": "string",
            "accrued_burst_tib": "string"
          }
        ]
      }
    ],
    "request_id": "string",
    "response_time": "string"
  }
}
```

**Status code:** 200 – Successful request

### Curl example:

```
curl -X 'GET' \
'https://api.activeiq.netapp.com/v1/keystone/customer/consumption-
details?type=customer&id=<customerID>' \ -H 'accept: application/json' \
-H 'authorizationToken: <access-key>'
```

## Get the historical consumption details for a customer

This API retrieves the historical consumption details for all the subscriptions associated with the given customerID as per the time range specified.

### Request:

<b>Method</b>	GET
<b>EndPoint</b>	<a href="https://api.activeiq.netapp.com/v1/keystone/customer/historical-consumption-details">https://api.activeiq.netapp.com/v1/keystone/customer/historical-consumption-details</a>
<b>Parameters</b>	<ul style="list-style-type: none"><li>• type: "customer"</li><li>• id: &lt;customer-id&gt;</li><li>• from_date_utc: &lt;start date(in RFC3339 format)&gt;</li><li>• to_date_utc: &lt;end date(in RFC3339 format)&gt;</li></ul>
<b>Headers</b>	<ul style="list-style-type: none"><li>• accept: application/json</li><li>• authorizationToken: &lt;access_key&gt;</li></ul>

### Response:

The API will respond with a JSON object containing a list of all the subscriptions with the historical service usage metrics for the given customer in the selected time range. Here's an example response:

```

{
  "results": {
    "returned_records": 0,
    "records": [
      {
        "subscription": {
          "account_name": "string",
          "number": "string",
          "start_date": "2023-08-24T14:15:22Z",
          "end_date": "2023-08-24T14:15:22Z"
        },
        "service_levels": [
          {
            "name": "string",
            "historical_consumption": [
              {
                "committed_tib": 0,
                "consumed_tib": 0,
                "timestamp_utc": "2023-08-24T14:15:22Z",
                "burst_tib": 0,
                "accrued_burst_tib": 0,
                "is_invoiced": true
              }
            ]
          }
        ]
      },
      {
        "request_parameters": {
          "from_date_utc": "2023-08-24",
          "to_date_utc": "2023-08-24",
          "customer_id": "string"
        },
        "request_id": "string",
        "response_time": "string",
        "customer": {
          "name": "string",
          "id": "string"
        }
      }
    ]
  }
}

```

**Status code:** 200 – Successful request

**Curl example:**

```
curl -X 'GET' \ 'https://api.activeiq-  
stg.netapp.com/v1/keystone/customer/historical-consumption-details?  
type=customer&id=<customerID>&from_date_utc=2023-08-24T14%3A15%3A22Z&t  
_date_utc=2023-08-24T14%3A15%3A22Z' \ -H 'accept: application/json' \ -H  
'authorizationToken: <access-key>'
```

# Keystone subscription services | Version 1

Keystone STaaS was preceded by Keystone subscription services (previously known as Keystone Flex Subscription services).

While the navigation of the two offerings is similar in the [Keystone dashboard](#), Keystone subscription services differ from Keystone STaaS in the constituent performance service levels, service offering, and billing principles. As of April 2024, NetApp maintains and publishes documentation for only Keystone STaaS. If you are still using Keystone subscription services, contact your KSM for support in migrating to Keystone STaaS. If required, you can access a PDF version of the Keystone subscription services documentation [here](#):

- [English](#)
- [Japanese](#)
- [Korean](#)
- [Chinese \(Simplified\)](#)
- [Chinese \(Traditional\)](#)
- [German](#)
- [Spanish](#)
- [French](#)
- [Italian](#)

# Get help with Keystone

NetApp Keystone support team and Keystone Success Manager (KSM) are responsible for providing you service for your Keystone subscriptions. If you need help, you can contact the Keystone support team.

## NetApp Keystone support

NetApp provides operational services remotely to NetApp Keystone customers. These services encompass a range of operational disciplines across storage management activities. These services include asset and configuration management, capacity and performance management, change management, event, incident and problem management, service request fulfillment, and reporting. NetApp demonstrates a state of control and supporting evidence as required.

## Additional information

NetApp uses ITOM monitoring solution to proactively monitor and connect to the NetApp Keystone environment for troubleshooting.



In a partner-operated model, the tenant and subtenant's service requests are assigned to the partner's service desk. The partner's support tool might have integration with ITOM solution.

For more information about Keystone services, see:

- NetApp Keystone  
<https://www.netapp.com/us/solutions/keystone/index.aspx>
- NetApp Product Documentation  
<https://docs.netapp.com>

## Keystone support monitoring

NetApp Keystone support monitors the health of your products and subscribed services, provides remote support, and collaborates with your Keystone Success Manager.

### Keystone Success Manager

The Keystone Success Manager (KSM) works closely with you on your Keystone services and updates you on weekly or monthly billing and operational reports. The responsibilities are specified in your NetApp Keystone agreement.

## Generating service requests

During onboarding, if you were provided credentials for accessing and using Netapp Keystone ServiceNow, you can use the portal to generate service requests for issues related to your Keystone subscriptions:

<https://netappgssc.service-now.com/csm>

Ensure that you have the system details, logs, and related information ready before raising the service request. When you raise a service request, the Keystone support team receives the support ticket and accesses the information for troubleshooting. You can follow your ServiceNow ticket to know the status and resolution.

For information about adding support bundles, see [Generate and collect support bundle](#).

If you have an open case/ticket that needs to be escalated, send an email to one of the following addresses:

[keystone.services@netapp.com](mailto:keystone.services@netapp.com)

[keystone.escalations@netapp.com](mailto:keystone.escalations@netapp.com)

# Legal notices

Legal notices provide access to copyright statements, trademarks, patents, and more.

## Copyright

<https://www.netapp.com/company/legal/copyright/>

## Trademarks

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

<https://www.netapp.com/company/legal/trademarks/>

## Patents

A current list of NetApp owned patents can be found at:

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

## Privacy policy

<https://www.netapp.com/company/legal/privacy-policy/>



## Copyright information

Copyright © 2025 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.