



Keystone documentation

Keystone

NetApp
August 08, 2024

Table of Contents

- Keystone documentation 1
- Release notes 2
 - What’s new in Keystone STaaS 2
 - Fixed issues 5
 - Known issues 8
 - Known limitations 8
- Learn about Keystone 10
 - Learn about NetApp Keystone 10
 - Keystone infrastructure 11
 - Learn about Keystone Collector 12
 - Components required for deployment 13
 - Keystone data flow 15
 - Operational models in Keystone 17
- Set up and configure Keystone 19
 - Requirements 19
 - Install Keystone Collector 25
 - Configure Keystone Collector 29
 - Configure AutoSupport for Keystone 33
 - Keystone Collector security 34
 - Types of user data that Keystone collects 35
- Monitor and upgrade 43
 - Monitor the health of Keystone Collector 43
 - Manually upgrade Keystone Collector 48
- Keystone dashboard 51
 - Keystone dashboard overview 51
 - View usage details and generate reports 53
 - View details about your subscriptions 55
 - View the current consumption of your subscriptions 56
 - View consumption trends 58
 - View details about ONTAP volumes and object storage 63
 - View cluster and node details managed by Keystone 67
 - View performance metrics 67
 - Learn about Keystone and BlueXP 71
- Keystone STaaS services 72
 - Metrics and definitions used in Keystone 72
 - Storage QoS in Keystone 73
 - Supported storage in Keystone 76
 - Supported storage capacities in Keystone 78
 - Service levels in Keystone 80
 - Capacity requirements for service levels 82
 - Keystone subscription services | Version 1 85
 - Add-on services 86
- Keystone STaaS SLA 91

Availability SLA	91
Performance SLA	93
Sustainability SLA	95
Ransomware Recovery Guarantee	97
Billing	98
Keystone pricing	98
Billing based on committed capacity	98
Metering based on consumed capacity	99
Billing based on burst consumption	99
Miscellaneous scenarios for Keystone billing	99
Billing schedules	101
Get help with Keystone	102
NetApp Global Services and Support Center	102
Additional Information and Support Contact	102
GSSC monitoring	102
Generating service requests	103
Legal notices	104
Copyright	104
Trademarks	104
Patents	104
Privacy policy	104

Keystone documentation

Release notes

What's new in Keystone STaaS

NetApp offers you new and enhanced features in every release of Keystone STaaS services.

The following enhancements are introduced in the **Keystone Subscriptions** screen of Active IQ Digital Advisor (also known as Digital Advisor):

July 10, 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.

June 27, 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.

May 29, 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.

May 09, 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.

March 28, 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,

all of which show the data based on the selected date of the subscription.

February 29, 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 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.

February 13, 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.

January 11, 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.

December 15, 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

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
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 Capacity Trend option in the Capacity Trends tab.	Usage charts now correctly display data for the specified single-day period.	June 27, 2024

Issue description	After the fix	Fixed in release
Historical accrued burst data is not available for CVO Primary and CVO Secondary service levels within the Capacity Trend 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 Volume Details tab for AutoSupport subscriptions.	The consumed value for object storage now displays correctly.	June 21, 2024
Unable to view cluster-level information within the Assets tab for AutoSupport subscriptions that are configured with a MetroCluster configuration.	Fixed	June, 21, 2024
Misplacement of Keystone data in CSV reports if the Account Name column in CSV reports, generated from the Capacity Trend 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 Capacity Trend tab even if the consumption is below the committed capacity.	Fixed	May 29, 2024
Incorrect tooltip text for the Current Burst index icon in the Capacity Trend 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

Issue description	After the fix	Fixed in release
Occasional mismatch in the number of AQoS non-compliant volumes listed on the Volume Summary and Volume Details 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 Assets 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
For some subscriptions having a single service level or rate plan, the AQoS compliance column was missing in the CSV output of the Volumes 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 Performance 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

Issue description	After the fix	Fixed in release
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

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

There are no known issues at this moment.

Known limitations

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 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](#).

Learn about Keystone

Learn about NetApp Keystone

NetApp Keystone (Keystone) is a pay-as-you-grow, subscription-based service model that delivers seamless hybrid cloud experience for businesses preferring OpEx consumption models to upfront CapEx or leasing.

Keystone enables customers to accelerate time to value by reducing the hurdles in managing unpredictable capacity growth and complex procurement cycles. Keystone allows customers to align economics and operations to their business priorities.



Pay for outcomes

SLA-based service tiers to meet workload requirements



Pay as you grow

Predictable billing that aligns with business growth



Predictable availability

99.999% data availability that comes as standard



Harness the cloud

Leverage cloud services with on-prem services, with one simpler operating model



Managed for you

Assets are owned, operated and supported 24x7 by NetApp

Keystone provides storage capacity at predefined service levels for block, file, and object data types that 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.

A Keystone subscription is associated with rate plans. There can be multiple rate plans attached to a single subscription.

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 the majority of enterprises are still working on their strategy for hybrid cloud, you, as a customer, can opt for an OpEx-based *pay-per-use* consumption model. You might have a mandate to move all your workloads to cloud eventually, and yet not have a clear plan or schedule to migrate specific portions or all of your workloads over to the cloud. Keystone STaaS provides you with the flexibility to start with on-premises services and decide later on the right workloads and point in time to move to the cloud. Keystone STaaS provides commitment protection across deployment models. Instead of paying more for cloud services, you, as an on-premises customer, can reallocate your on-premises spending to add cloud services and essentially pay the same monthly bill that was committed prior to this reallocation.

Related information

- [Keystone pricing](#)
- [Add-on services in Keystone STaaS](#)
- [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 storage controllers.
- Tools to manage and operate the service such as AIOPs solution, Active IQ, and Active IQ Unified Manager.

Storage platforms

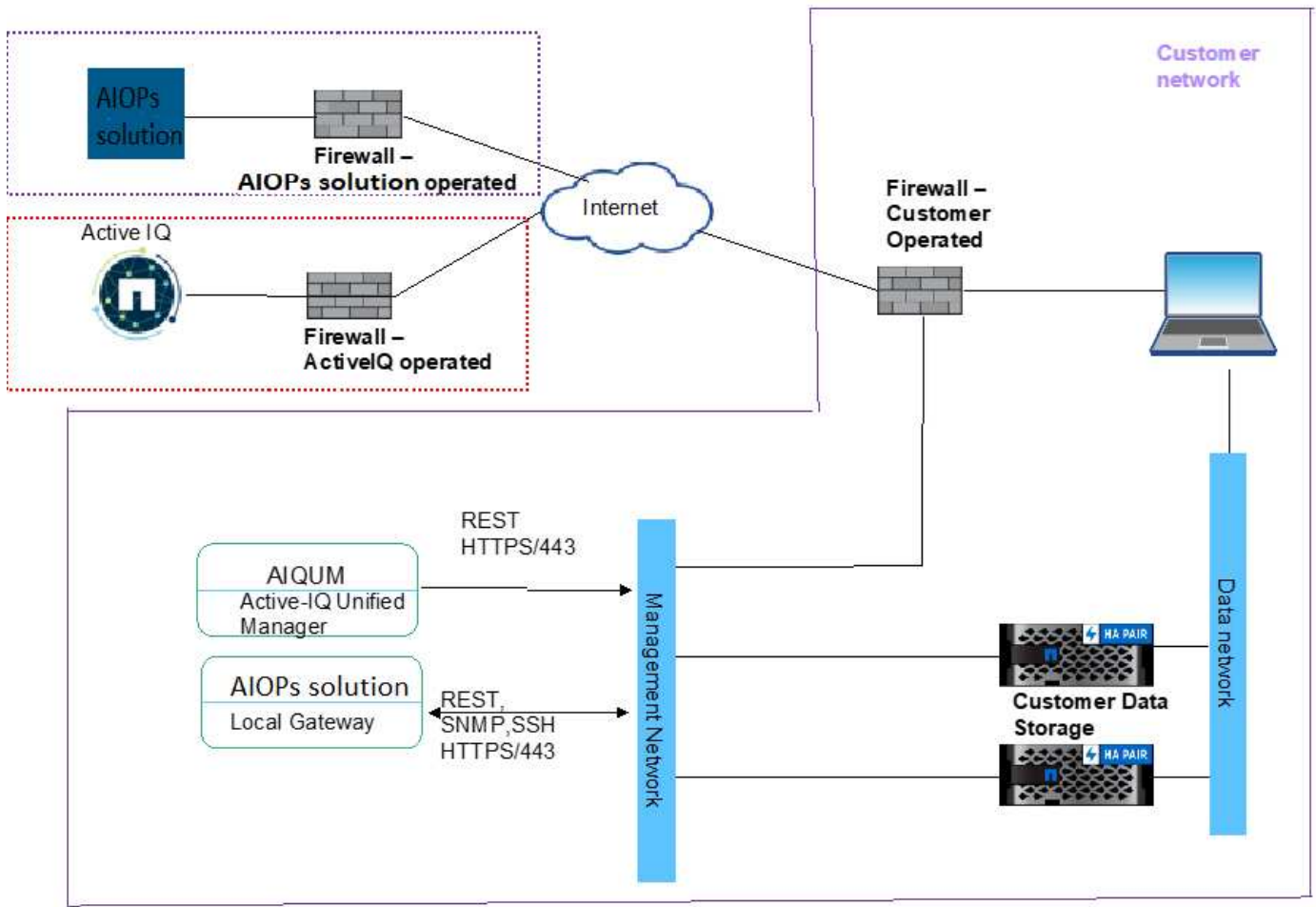
Enterprise applications need storage platforms to support fast provisioning-workflows, maintain continuous availability, sustain high workloads with low latency, deliver higher performance, and support integration with major cloud providers. NetApp has several products and technologies for supporting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

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.

- AIOPs solution local gateway: A cloud-based application used to monitor your network. It has built-in integrations with NetApp storage platforms to collect environmental data and monitor the network. This service is enabled with the help of using a local gateway installed at your site that communicates with the cloud portal.
- Keystone Data Collector: Keystone Collector provides billing services to Keystone customers. 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. Active IQ data lake processes the billing data and sends it to Zuora for billing.



Digital Advisor enables you to log in and view the subscription and consumption details for your Keystone subscriptions. For more information about Keystone reporting on the Digital Advisor dashboard, see [Keystone and Digital Advisor](#).

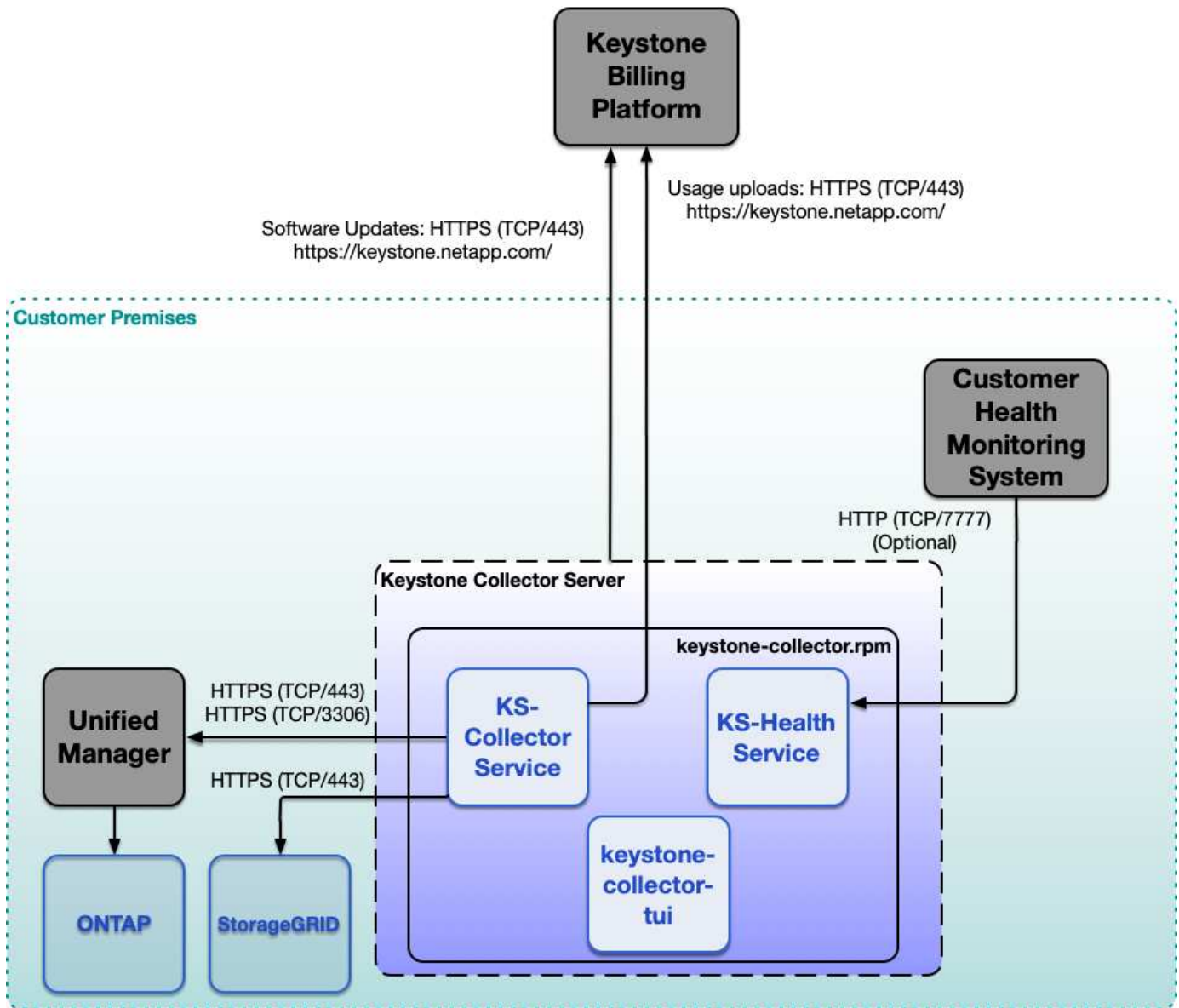
Learn about Keystone Collector

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 SLA 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 represents the standard approach of collecting usage data for Keystone systems. If your environment cannot support Keystone Collector, you can seek authorization from Keystone Product Management 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.

PDU's

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.

Storage virtual machines

A storage virtual machine (storage VM) is required for the deployment of Keystone Collector and the AIOPs solution gateway. The prerequisites for installing Keystone Collector are available here: [Installation guide for Keystone 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 Red Hat Enterprise Linux 7 or 8 or CentOS 7 Linux server. The Keystone software is installed via `.rpm` installation process.

AIOPs solution gateway is deployed on the following configuration:

- VMware OVA template (VMware vCenter Server 6.7 or later is required)
- Bootable `.iso` installer for
 - Citrix XenServer
 - Microsoft Hyper-V
 - Kernel-based Virtual Machine (Linux KVM)

Networking

Outbound access is required to the following services for operations and maintenance of Keystone Collector and AIOPs solution gateway:

- `support.netapp.com` (usage data upload)
- `keystone.netapp.com` (software updates)

- Hub.Docker.io (software updates)

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

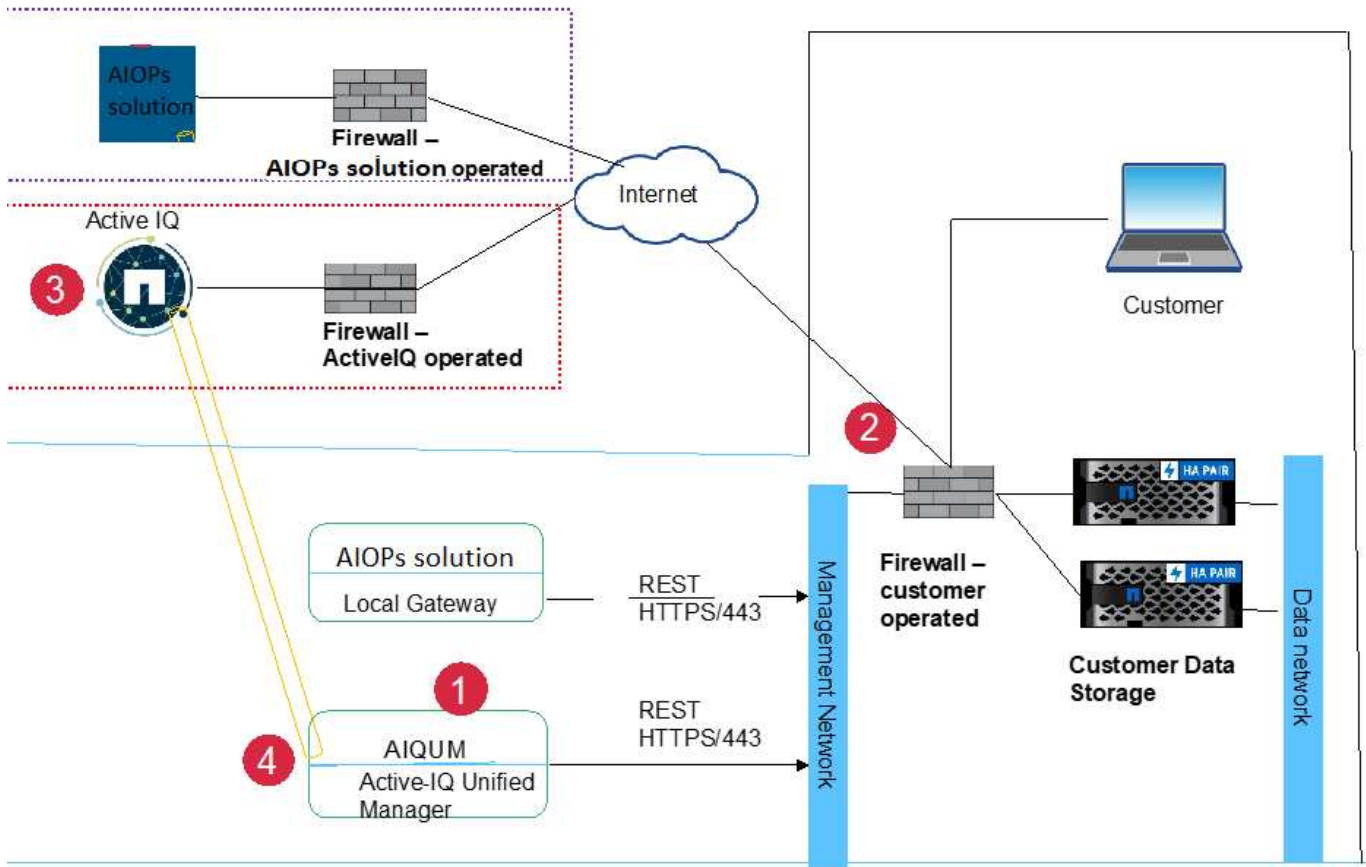
NetApp needs to access the hardware and software components installed for monitoring and management to provide services such as monitoring and billing to Keystone customers. The most common method is to establish a virtual private network (VPN) connection to the customer network and access the required 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 AIOPs 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 AIOPs solution tool, 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:

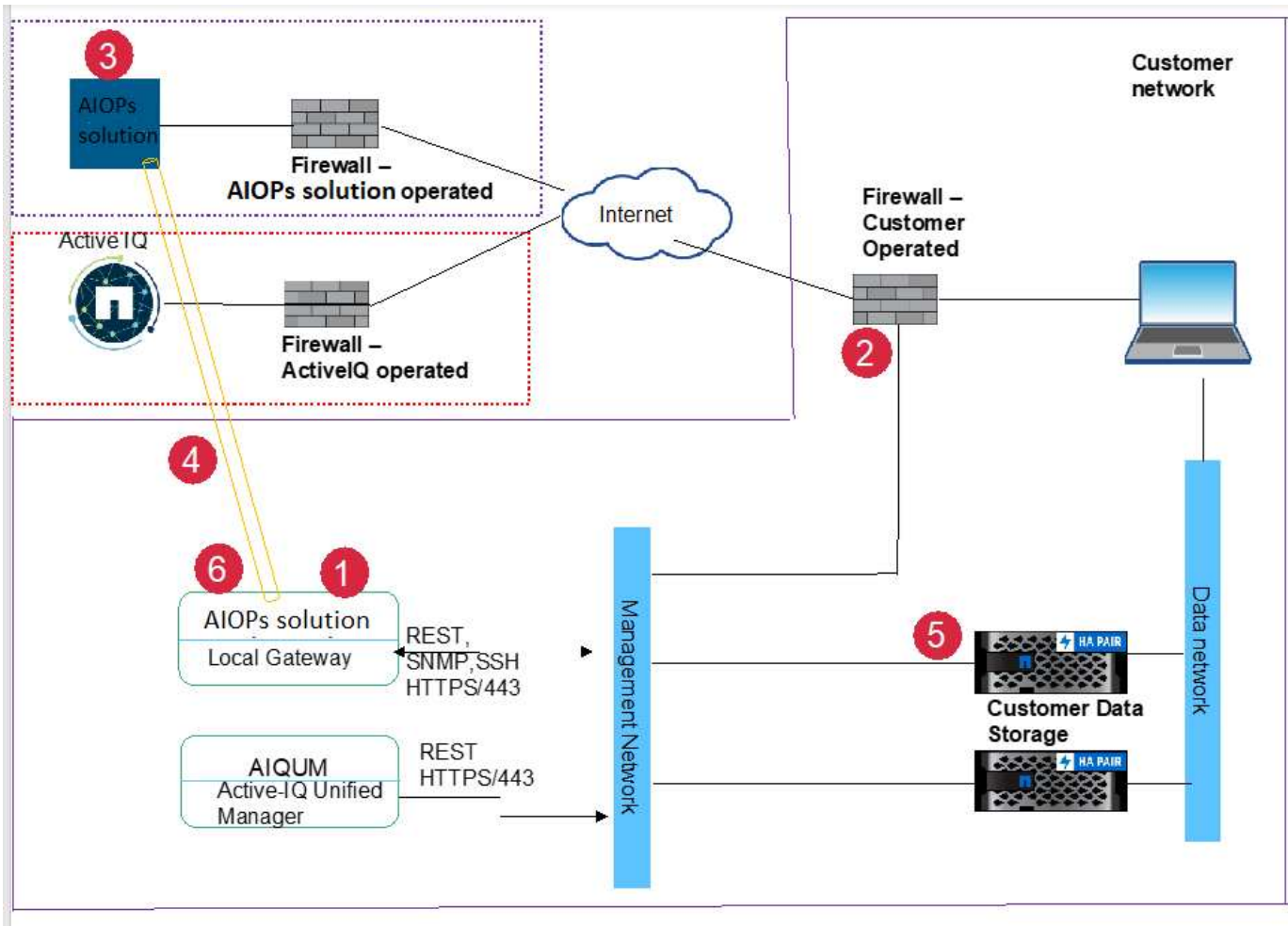


Legend

1. NetApp Collector initiates an HTTPS session to the Active-IQ cloud portal.
2. The firewall operated by the customer allows the connection.
3. The Active IQ cloud portal accepts the connection and establishes a tunnel to the NetApp Collector.
4. The NetApp collector establishes a REST API session to the management connection of the storage controller, obtains environmental data, and sends it to the Active IQ portal.

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 AIOps solution, which needs remote access to customer's network. The following image describes how remote access to the customer location is secured by the AIOps solution tool.



Legend

1. The AIOps solution gateway initiates a TLS session to the cloud portal.
2. The firewall operated by the customer allows the connection.
3. The AIOps solution server in the cloud accepts the connection.
4. A TLS tunnel is established between the cloud portal and the local gateway.
5. The NetApp controllers send alerts using SNMP 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.

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:** A partner or service provider operates the services for their end customers. For NetApp, the partner is the referenced contracted party. Tenants are customers of partners and have no billing relationship with NetApp. A partner-operated model has a multi-tenant environment where tenants and end customers/subtenants have their own subscriptions that are billed by the partner. The partner administrator performs the administrative tasks for all the tenants.

- **Customer-operated model:** As a customer, you can subscribe to Keystone services according to your selected 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. As a customer, you are the tenant or subtenant to NetApp or a partner/service provider. Based on your contract, you can raise service requests to be addressed by NetApp or your service provider. An administrator from your end can perform the administrative tasks at your site (environment). These tasks are tied to the users in your environment.

Roles and responsibilities across the service lifecycle

- **Partner-operated model:** The share of roles and responsibilities depends on the SLA 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"> • Install • Configure • Deploy • Onboard 	✓	None
Administration and monitoring <ul style="list-style-type: none"> • Monitor • Report • Perform administrative tasks • Alert 	None	✓
Operations and optimization <ul style="list-style-type: none"> • Manage capacity • Manage performance • Manage SLA 	None	✓
Support <ul style="list-style-type: none"> • Support customer • Hardware break fix • Software support • Upgrades and patches 	✓	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 6.5 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 80, 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
https://keystone.netapp.com	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: CentOS 7 or Red Hat Enterprise Linux 8.6 or later
- 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 80, 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
https://keystone.netapp.com	Keystone Collector software updates and usage reporting
https://support.netapp.com	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

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 users](#).

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
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- 4 Review details
- 5 Select storage
- 6 Select networks
- 7 Customize template
- 8 Ready to complete

Review details
Verify the template details.

Publisher	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

The Keystone Collector software is distributed by an online YUM software repository. You need to import and install the file on a Linux server.

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

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
```



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.

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.

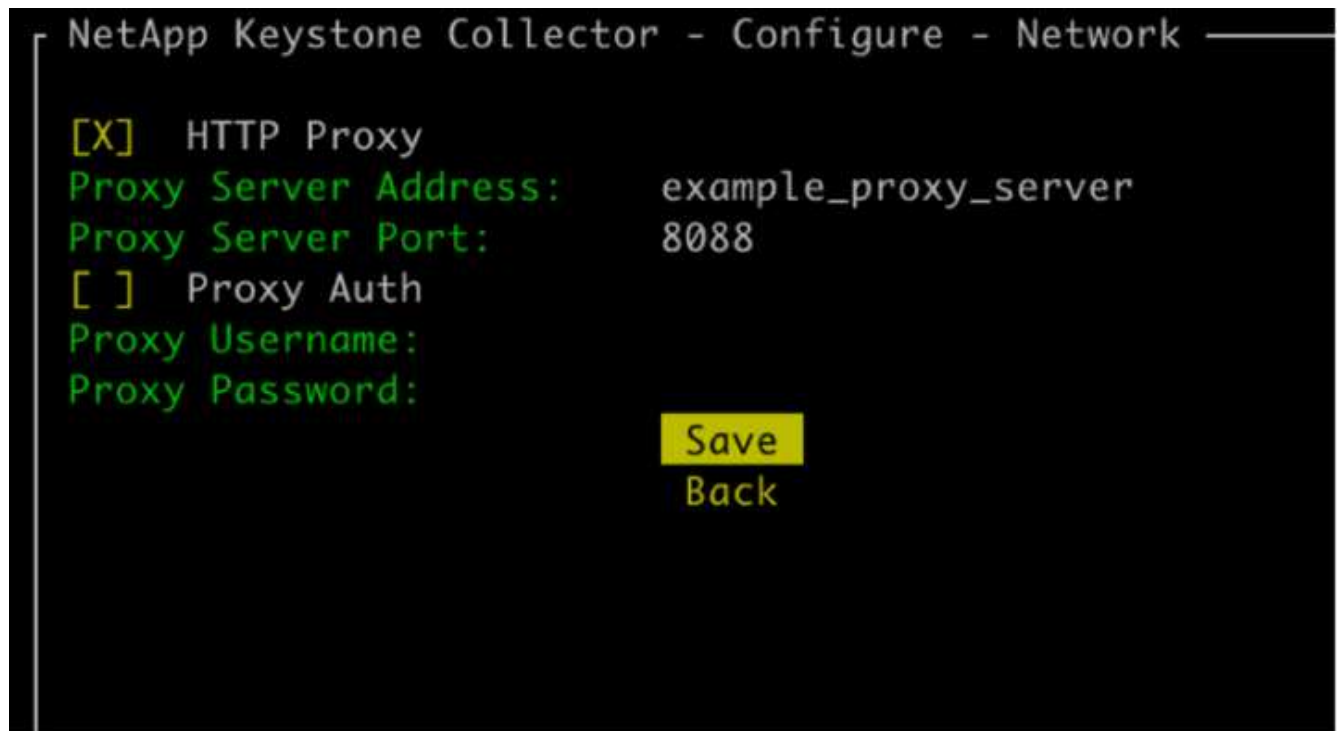
Configure HTTP Proxy on Keystone Collector

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
```

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.

- Run this command to modify the daily log content:

```
autosupport trigger modify -node * -autosupport-message
management.log -basic-additional
waf1,performance,snapshot,platform,object_store_server,san,raid,snapp
irror -troubleshooting-additional waf1
```

- Run this command to modify the weekly log content:

```
autosupport trigger modify -autosupport-message weekly
-troubleshooting-additional waf1 -node *
```

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

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 for your Keystone ONTAP and Keystone StorageGRID subscriptions. It can also collect performance data for only ONTAP, if the 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
- QoSNetworkLatency
- 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

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-a826be4fdb7_1667193651.tar.gz"}

{"level":"info","time":"2022-10-31T05:21:31.385Z","caller":"reception/reception.go:75","msg":"Sending file 65a71542-cb4d-bdb2-e9a7-a826be4fdb7_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

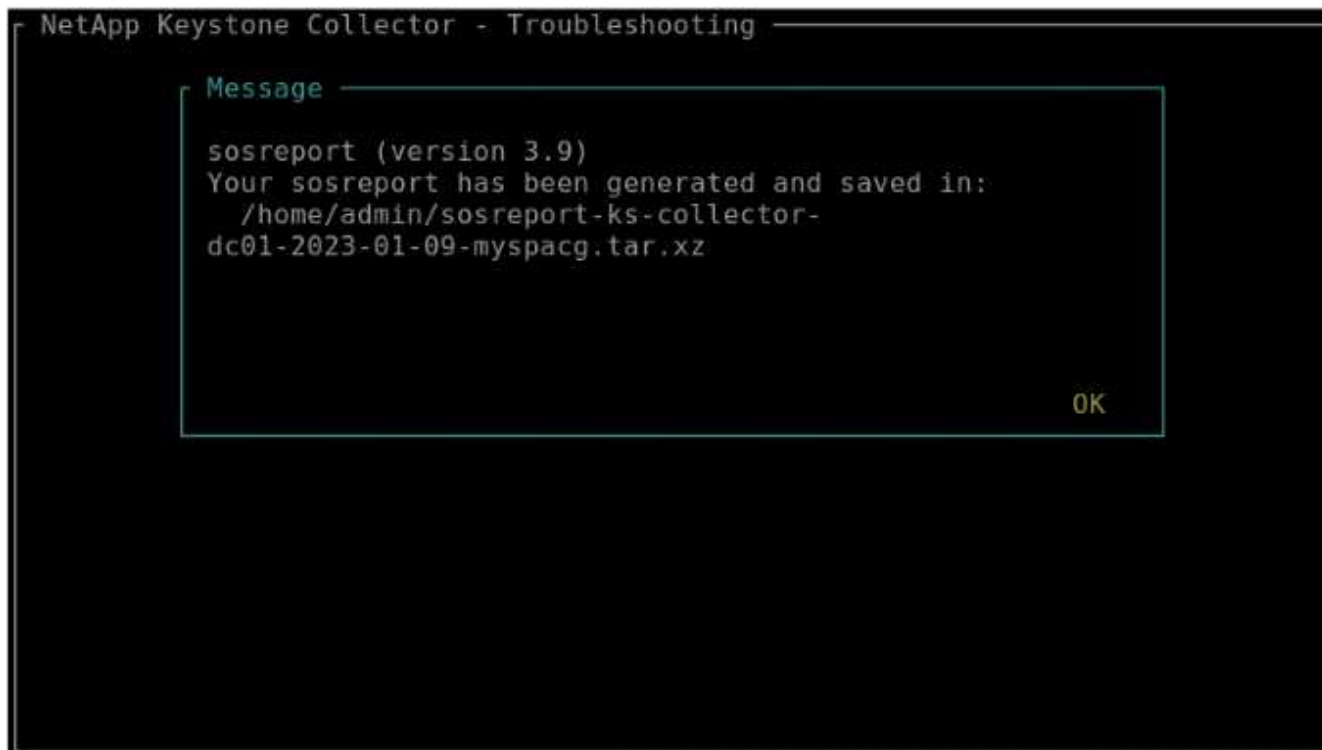
1. Start the Keystone Collector management TUI utility:

```
$ 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.



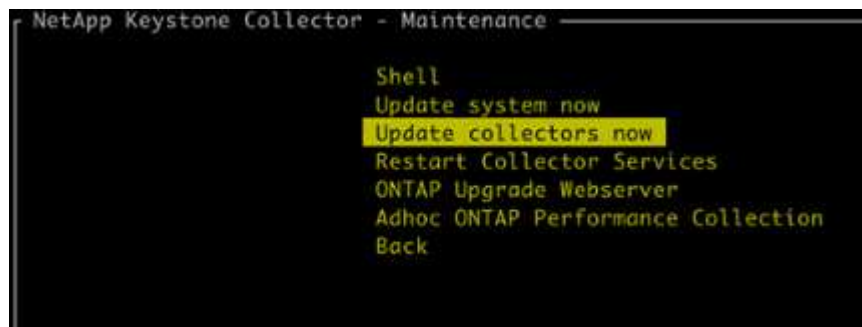
4. When the file is downloaded, you can attach it to the Keystone ServiceNow support ticket. For information about raising tickets, see [Generating service requests](#).

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 dashboard

Keystone dashboard overview

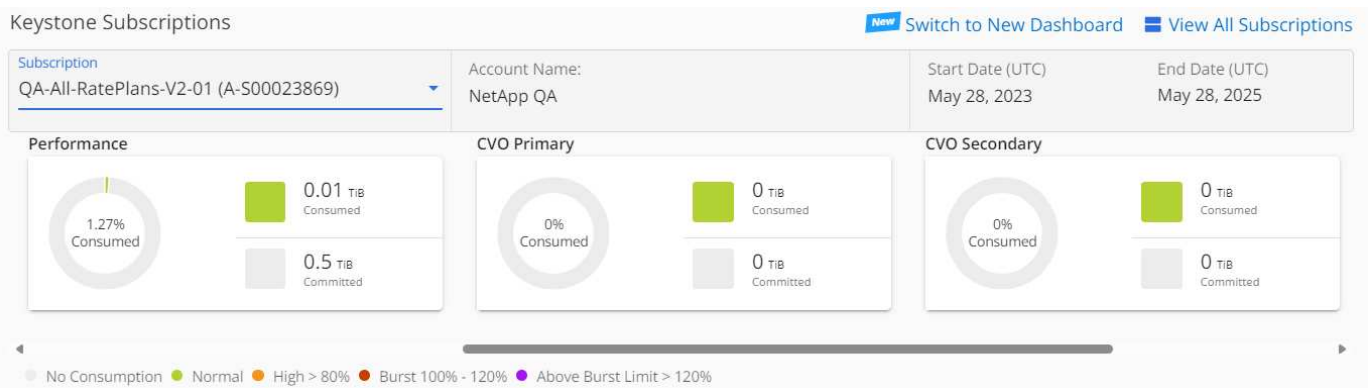
As a NetApp Keystone STaaS subscriber, you can get an overview of your subscriptions on the **Keystone Subscriptions** widget of the Active IQ Digital Advisor (also known as Digital Advisor) dashboard.

You can search for 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 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.
 - Consumptions above the burst capacity.
- **Alerts:** You see alerts for various scenarios if they are applicable to you.
 - **Expiring soon:** In case your subscriptions expire within 90 days.
 - **QoS Warnings:** You have volumes without AQoS policies assigned.



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

Keystone Subscriptions [Revert to Old Dashboard](#) [View All Subscriptions](#)

Capacity Usage	
No Consumption	30 Subscriptions
Normal	8 Subscriptions
Burst	2 Subscriptions
Above Burst Limit	5 Subscriptions
Draft	4 Subscriptions

Alerts	
Expiring Soon	8 Subscriptions
QoS Warnings	13 Subscriptions

For more information about Digital Advisor dashboard widget for Keystone, see [Digital Advisor documentation](#).

For more information about Keystone dashboard and reporting, see [Keystone Subscription dashboard and reporting](#).

Search by Keystone watchlists

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

For Keystone STaaS, you can create watchlists for customers or subscription numbers. You can search by the watchlist name on the Digital Advisor screen. On searching by a watchlist, 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.

NetApp Digital Advisor Support Quick Links English Welcome Sign Out

Search for watchlist, system, cluster, customer, site, group, or StorageGRID

Demo-Watchlist

Wellness Actions Risks View All Actions

Security Vulnerabilities 2 Actions	Ransomware Defense 1 Action	Performance & Efficiency 1 Action	Availability & Protection 3 Actions	Capacity 1 Action	Configuration 1 Action
---------------------------------------	--------------------------------	--------------------------------------	----------------------------------------	----------------------	---------------------------

Inventory View All Systems

Storage Virtual Machine ONTAP StorageGRID

9 Systems 2 Clusters 3 Sites

Planning

Capacity Addition 2 Renewals

No Data Available Cloud Recommendation

Upgrade Advisor

ONTAP 1 Action

Not Applicable

Keystone Subscriptions

Switch to New Dashboard View All Subscriptions

<ul style="list-style-type: none"> TrkKrat001 (A-500021934) TrkTami001 (A-500021936) (A-500021937) (A-500021940) (A-500021942) 	<p>Account Name: NetApp QA</p> <p>Start Date (UTC): Mar 1, 2021</p> <p>End Date (UTC): Mar 1, 2024</p>
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------

<p>Premium</p> <p>190.78% Consumed</p> <p>20.99 M€ Consumed</p> <p>11 M€ Committed</p>	<p>Standard</p> <p>118.77% Consumed</p> <p>510.72 M€ Consumed</p> <p>430 M€ Committed</p>
-----------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------

View usage details and generate reports

The Digital Advisor dashboard enables you to view the details of your Keystone subscriptions, monitor capacity usage, and generate reports.

On subscribing to Keystone services, you can view the details of your subscription and usage on the **Keystone Subscriptions** widget on the Digital Advisor dashboard.



The information here applies to both ONTAP and StorageGRID. Exceptions have been pointed out in the relevant sections.

To learn more about the Keystone Digital Advisor widget, refer to [View capacity utilization with NetApp Keystone Subscription](#).

To view your Keystone subscription and usage details, perform the following steps:

Steps

1. Log in to Digital Advisor. You can see the **Keystone Subscriptions** widget that summarizes the capacity usage against your purchased Keystone services.
2. On the **Keystone Subscriptions** widget, click **View All Subscriptions** to view the usage details and alerts on your volumes on the **Keystone Subscriptions** page. Alternately, from the left navigation pane, go to **GENERAL > Keystone Subscriptions**.
The details of the subscriptions, usage charts for each 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](#).

The following links provide more information about each of these tabs:

- [Subscriptions](#)
- [Current Consumption](#)
- [Consumption Trend](#)
- [Volumes & Objects](#)
- [Assets](#)
- [Performance](#)

Generate reports

You can generate and view reports for your Keystone data. Each tab on the **Keystone Subscriptions** page enables you to generate reports for your subscriptions, historical usage and burst usage, performance, assets,

and volumes and objects by clicking the download button:



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

A sample report for the **Consumption Trend** tab, where the graphical data is converted:

	A	B	C	D	E	F	G	H	I
1	Subscription Number	Account Name	Service Level	Timestamp (UTC)	Committed (TiB)	Consumed (TiB)	Burst (TiB)	Accrued Burst (TiB)	
2	xxxxxxxxx	xxxxx	Premium	01-04-2024 00:00	200	189.3899	0	0	
3	xxxxxxxxx	xxxxx	Premium	01-04-2024 23:00	200	189.3899	0	0	
4	xxxxxxxxx	xxxxx	Premium	02-04-2024 22:00	200	189.3899	0	0	
5	xxxxxxxxx	xxxxx	Premium	03-04-2024 21:00	200	189.3899	0	0	
6	xxxxxxxxx	xxxxx	Premium	04-04-2024 20:00	200	189.3899	0	0	
7	xxxxxxxxx	xxxxx	Premium	05-04-2024 19:00	200	189.3899	0	0	
8	xxxxxxxxx	xxxxx	Premium	06-04-2024 18:00	200	172.3899	0	0	
9	xxxxxxxxx	xxxxx	Premium	07-04-2024 17:00	200	172.3899	0	0	
10	xxxxxxxxx	xxxxx	Premium	08-04-2024 16:00	200	172.3899	0	0	
11	xxxxxxxxx	xxxxx	Premium	09-04-2024 15:00	200	172.3899	0	0	
12	xxxxxxxxx	xxxxx	Premium	10-04-2024 14:00	200	172.3899	0	0	
13	xxxxxxxxx	xxxxx	Premium	11-04-2024 13:00	200	172.3899	0	0	
14	xxxxxxxxx	xxxxx	Premium	12-04-2024 12:00	200	172.3899	0	0	
15	xxxxxxxxx	xxxxx	Premium	13-04-2024 11:00	200	172.3899	0	0	
16	xxxxxxxxx	xxxxx	Premium	14-04-2024 10:00	200	172.3899	0	0	
17	xxxxxxxxx	xxxxx	Premium	15-04-2024 09:00	200	172.3899	0	0	

View alerts

The dashboard provides alert notifications that enable you to understand the issues occurring in your storage environment. These notifications may appear as informational alerts or warnings. For example, if there are volumes within your managed clusters that do not have adaptive QoS (AQoS) policies attached, you can see a warning message. You can click the link on the warning message to see the list of the non-compliant volumes in the **Volumes & Objects** tab.



If you have subscribed to a single service level or rate plan, you won't be able to see the alert for non-compliant volumes.

Keystone Subscriptions [Help](#)

Subscriptions **Current Consumption** Consumption Trend Volumes & Objects Assets Performance SLA Details

Subscription: QA-All-RatePlans-V2-01 (A-S00023869) Start Date (UTC): May 28, 2023 End Date (UTC): May 28, 2025 Billing Period: Month

Warning: [39 volumes do not comply with this subscription's QoS policies.](#)

Current Consumption per Service Level

Legend: No Consumption (grey), Normal (green), High > 80% (orange), Burst 100% - 120% (red), Above Burst Limit > 120% (purple)

Service Level	Committed	Consumed	Current Burst	Available	Available
Data Tiering	2 TiB	0 TiB	0 TiB	2 TiB	2.4 TiB
Extreme	1 TiB	0 TiB	0 TiB	1 TiB	1.2 TiB
Performance	0.5 TiB	0.01 TiB	0 TiB	0.49 TiB	0.59 TiB
CVO Primary	0 TiB	0 TiB	0 TiB	0 TiB	0 TiB
CVO Secondary	0 TiB	0 TiB	0 TiB	0 TiB	0 TiB
Advanced Data-Protect	1 TiB	0 TiB	0 TiB	1 TiB	1.2 TiB

For information about AQoS policies, see [Adaptive QoS](#).


Contact NetApp support for more information on these messages. For information about raising service requests, see [Generating service requests](#).

View details about your subscriptions

To learn more about your Keystone subscriptions, you can view a list of all your subscriptions from the **Subscriptions** tab.

To view this tab, from the left navigation pane, go to **GENERAL > Keystone Subscriptions > Subscriptions**. All your subscriptions are listed.

Subscription Number	Linked Subscriptions	Tracking ID	Usage Type	Billing Period	Start Date (UTC)	End Date (UTC)	Consumption Status
A-500026419	--	QA-All-RatePlans-V1-05	Physical (v1)	Annual	March 19, 2024	March 19, 2025	Normal
A-500024534	--	QA-All-RatePlans-V1-06	Physical (v1)	Annual	August 1, 2023	▲ August 1, 2024	Above Burst Limit
A-500023869	--	QA-All-RatePlans-V2-01	Physical (v2)	Month	May 28, 2023	May 28, 2025	Normal
A-500024530	--	QA-All-RatePlans-V2-03	Physical (v2)	Annual	August 1, 2023	▲ August 1, 2024	Above Burst Limit
A-500024535	--	QA-All-RatePlans-V2-05	Logical (v2)	Annual	August 1, 2023	▲ August 1, 2024	Above Burst Limit
A-500024537	--	QA-All-RatePlans-V2-06	Logical (v2)	Annual	August 1, 2023	▲ August 1, 2024	No Consumption
A-500026932	--	QA-CVO-v1-combo1		Month	May 21, 2024	May 21, 2025	No Consumption
A-500026933	--	QA-CVO-v1-combo2		Month	May 21, 2024	May 21, 2025	No Consumption
A-500026927	--	qa-cvo-v2-combo1	CVO (v2) Logical (v2)	Month	May 1, 2024	May 1, 2025	Above Burst Limit



You can filter the selection by clicking the hamburger icon  for a column, or view all the subscriptions by clicking the **Clear Filters** button. 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.
- **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.



If you have subscribed to advanced data protection add-on service, then you can click the tooltip against your subscription number to view the tracking ID of the partner subscription in a MetroCluster setup. To know how to view detailed consumption by partner subscriptions in a MetroCluster configuration, see [Reference charts for advanced data protection](#).

- **Usage Type:** You might have subscribed to multiple Keystone (version 1) or Keystone STaaS (version 2) subscriptions. The rate plan rules for the service levels might vary for the two subscription types. By looking at the value in this column, you know whether the usage type is billed as per the provisioned, physical, or logical usage for either v1 or v2. To learn more about Keystone Subscriptions version 1, refer to [Documentation for NetApp Keystone](#).
- **Billing Period:** The billing period of the subscription, such as monthly, quarterly, or yearly.
- **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 service level included in this subscription.

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

- No Consumption 0%
- Normal 0% - 80%
- High > 80%
- Burst
- Above Burst Limit

Index

- : No capacity usage recorded against the committed capacity of the service level
- : The consumption is normal, within 80% of the committed capacity
- : Maximum consumption, that is the usage is about to reach 100% or more of the committed capacity. The **Consumed** column displays this indicator for any consumption above 80% of the committed capacity
- : The consumption is within the burst limit. The burst consumption is the consumption that tops the 100% committed capacity of a service level, and is within the agreed-upon burst usage limit, such as 120%
- : Indicates consumption above the stipulated burst limit

Related information

- [Use Keystone dashboard and reporting](#)
- [Current Consumption](#)
- [Consumption Trend](#)
- [Volumes & Objects](#)
- [Assets](#)
- [Performance](#)

View the current consumption of your subscriptions

To understand your subscription usage, you can view the usage details like committed capacity, consumed capacity, available capacity, and more.

To view this tab, from the left navigation pane, go to **GENERAL > Keystone Subscriptions > Current Consumption**, and select the required subscription number.

Keystone Subscriptions [Help](#)

Subscriptions Current Consumption Consumption Trend Volumes & Objects Assets Performance

Subscription: QA-All-RatePlans-V2-01 (A-S00023869) Start Date (UTC): May 28, 2023 End Date (UTC): May 28, 2025 Billing Period: Month

Warning: 39 volumes do not comply with this subscription's QoS policies.

Current Consumption per Service Level

Legend: No Consumption (grey), Normal (green), High > 80% (orange), Burst 100% - 120% (red), Above Burst Limit > 120% (purple)

Service Level	Committed	Consumed	Current Burst	Available	Available
Data Tiering	2 TiB	0 TiB	0 TiB	2 TiB	2.4 TiB
Extreme	1 TiB	0 TiB	0 TiB	1 TiB	1.2 TiB
Performance	0.5 TiB	0.01 TiB	0 TiB	0.49 TiB	0.59 TiB
CVO Primary	0 TiB	0 TiB	0 TiB	0 TiB	0 TiB
CVO Secondary	0 TiB	0 TiB	0 TiB	0 TiB	0 TiB
Advanced Data-Protect	1 TiB	0 TiB	0 TiB	1 TiB	1.2 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 service level name, committed, consumed, available capacities, and current and accrued burst usage (in TiB).



The **i** icon next to each column provides comprehensive information about that column. Specific service levels that record higher consumption are highlighted. You can also view warnings and alerts generated for your volumes.

For information about your Keystone storage services and the relevant service levels, see [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.

Related information

- [Use Keystone dashboard and reporting](#)
- [Subscriptions](#)
- [Consumption Trend](#)
- [Volumes & Objects](#)
- [Assets tab](#)
- [Performance](#)

View consumption trends

To help you monitor your subscription usage, you can view historical data of your Keystone subscriptions for a specific period of time.

The vertical graphs display the usage details for the selected time range with appropriate indicators for you to compare and generate reports.

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. 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 as per your invoice.

View consumption trend

If you have selected the **Consumption Trend** option, follow these steps:

Steps

1. 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.

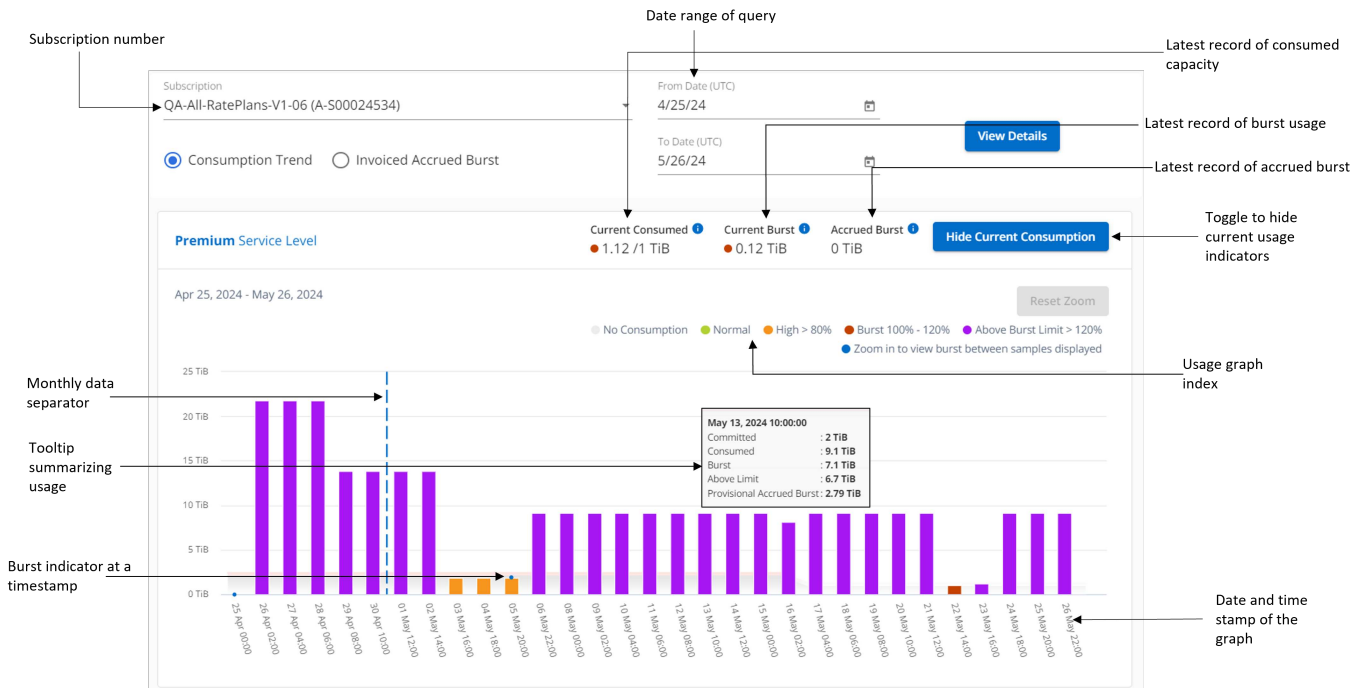


For optimal performance and user experience, limit the date range of your query to three months.

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

The bar charts display the service level name and the capacity consumed against that 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 service level for the selected interval. You can click the **Reset Zoom** button to return to the original chart view.



The following colors in the bar charts indicate the consumed capacity as defined within the service level. Monthly data across the charts is separated by a vertical line.

- Green: Within 80%.
- Amber: 80% - 100%.
- Red: Burst usage (100% of the committed capacity to the agreed burst limit)
- Purple: Above the burst limit or Above Limit.



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 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. 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:

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

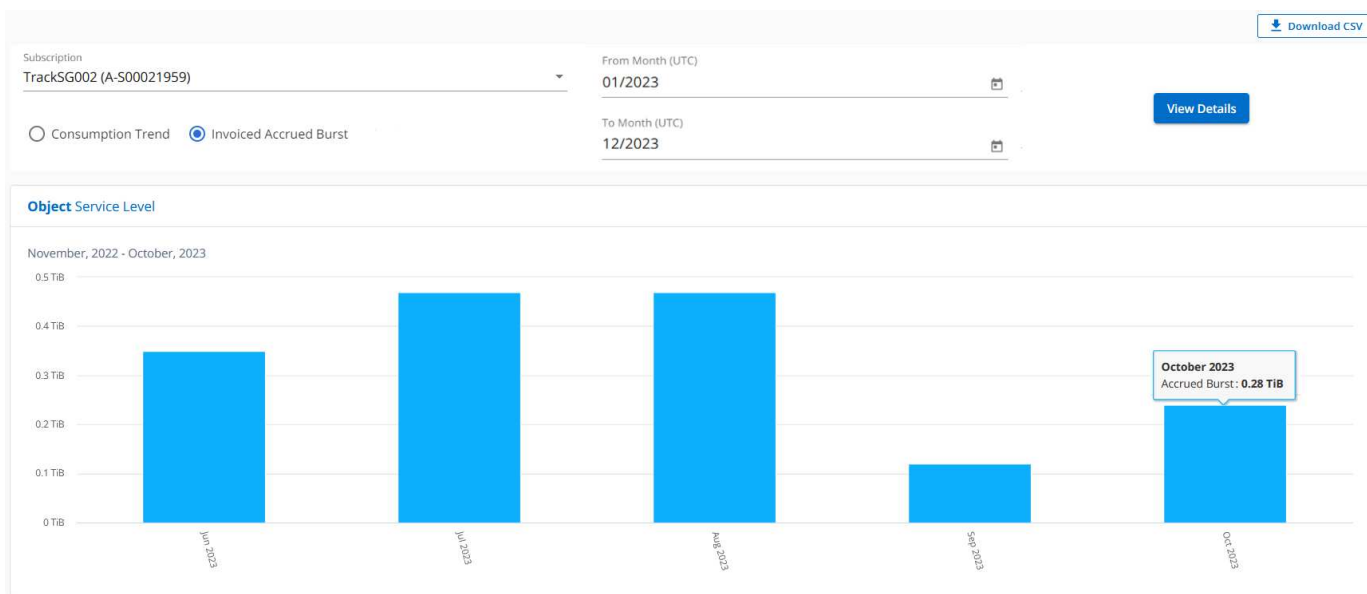
The burst is the difference between the consumed capacity and the committed capacity. For example, with a 30-day in month, if the consumed capacity reaches 120 TiB and the committed capacity is 100 TiB for a 2-minute interval, this results in a burst capacity of 20 TiB, equating to an accrued burst usage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

View invoiced accrued burst

If you have selected the **Invoiced Accrued Burst** option, by default, you can see the monthly accrued burst usage data for the last 12 months that has been billed. You can query by the date range of up to past 30 months. Bar charts are displayed for invoiced data, and if the usage has not yet been billed, you see *Pending* for that month.



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



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

Reference charts for advanced data protection

If you have subscribed to the advanced data protection add-on service, you can view the breakup of the consumption data for the MetroCluster partner sites on the **Consumption Trend** tab.

For information about advanced data protection add-on service, see [Advanced data protection](#).

If the clusters in your ONTAP storage environment are configured in a MetroCluster setup, the consumption data of your Keystone subscription is split in the same historical data chart to display the consumption at the

primary and mirror sites for the base service levels.



The consumption bar charts are split for only the base service levels. For advanced data protection add-on service, that is the *Advanced Data-Protect* service level, this demarcation does not appear.

Advanced data protection service level

For the *Advanced Data-Protect* service level, the total consumption is split between the partner sites, and the usage at each partner site is reflected and billed in a separate subscription; one subscription for the primary site, and another for the mirror site. That is the reason why, when you select the subscription number for the primary site on the **Consumption Trend** tab, the consumption charts for the advanced data protection add-on service display the discrete consumption details of only the primary site. Because each partner site in a MetroCluster configuration acts both as a source and mirror, the total consumption at each site includes the source and the mirror volumes created at that site.



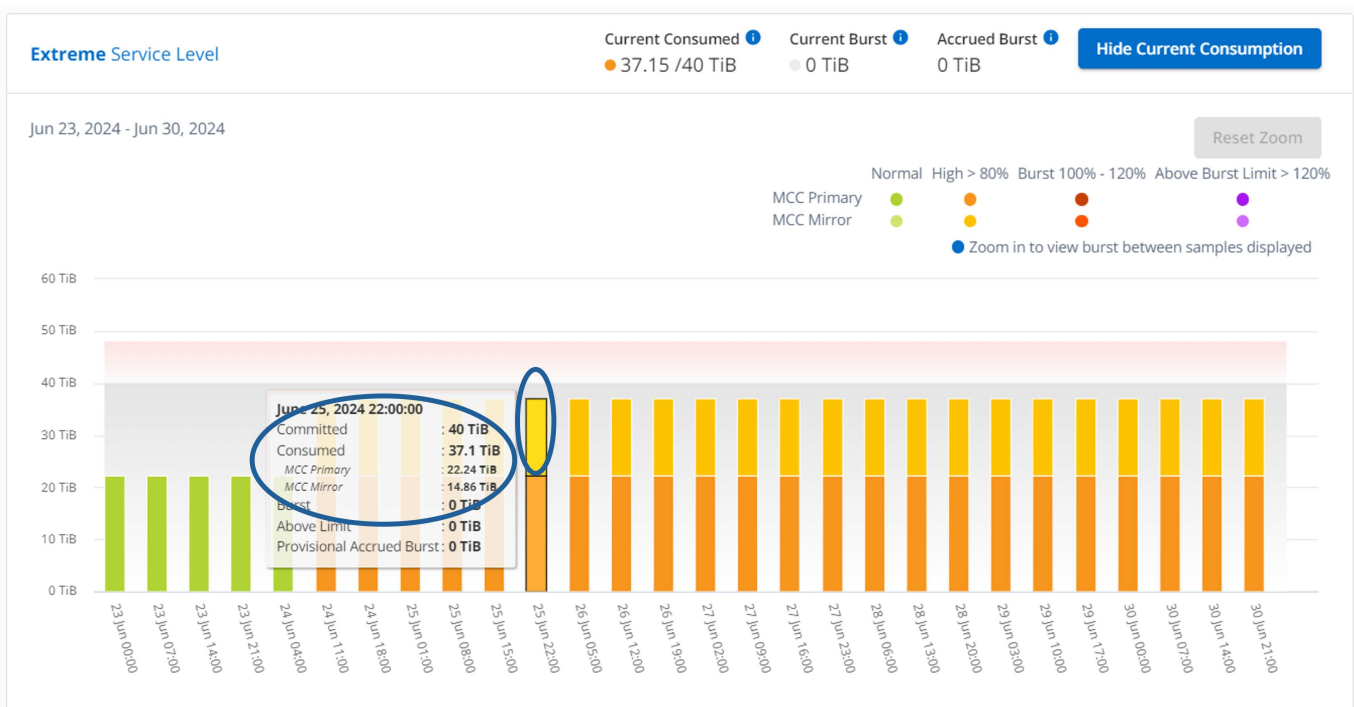
The tooltip next to the tracking ID of your subscription in the **Current Consumption** tab helps you identify the partner subscription in the MetroCluster setup.

Base service levels

For the base service levels, each volume is charged as provisioned at the primary and mirror sites, and hence the same bar chart is split according to the consumption at the primary and mirror sites.

What you can see for the primary subscription

The following image displays the charts for the *Extreme* service level (base service level) and a primary subscription number. The same historical data chart also indicates the mirror site consumption in a lighter shade of the same color code used for the primary site. The tooltip on mouse hover displays the consumption breakup (in TiB) for the primary and mirror sites, 22.24 TiB and 14.86 TiB respectively.

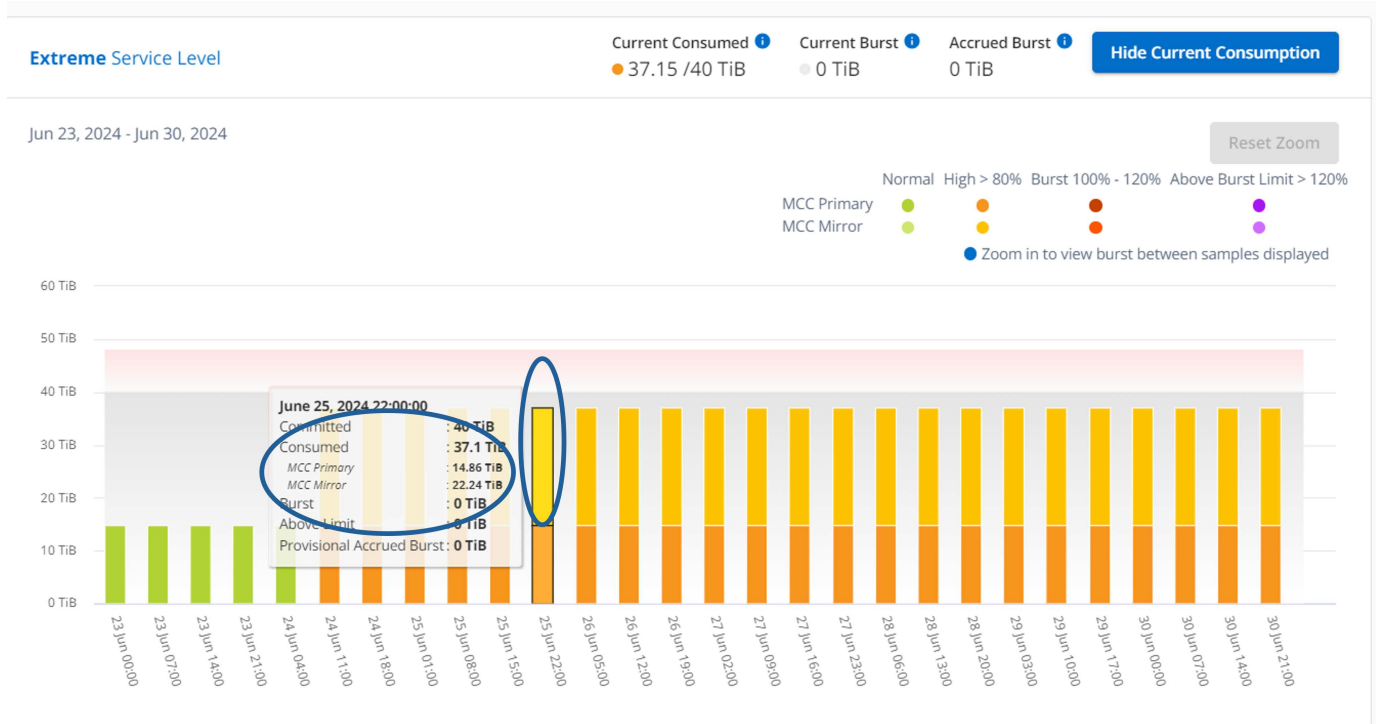


For the *Advanced Data-Protect* service level, the charts appear like this:

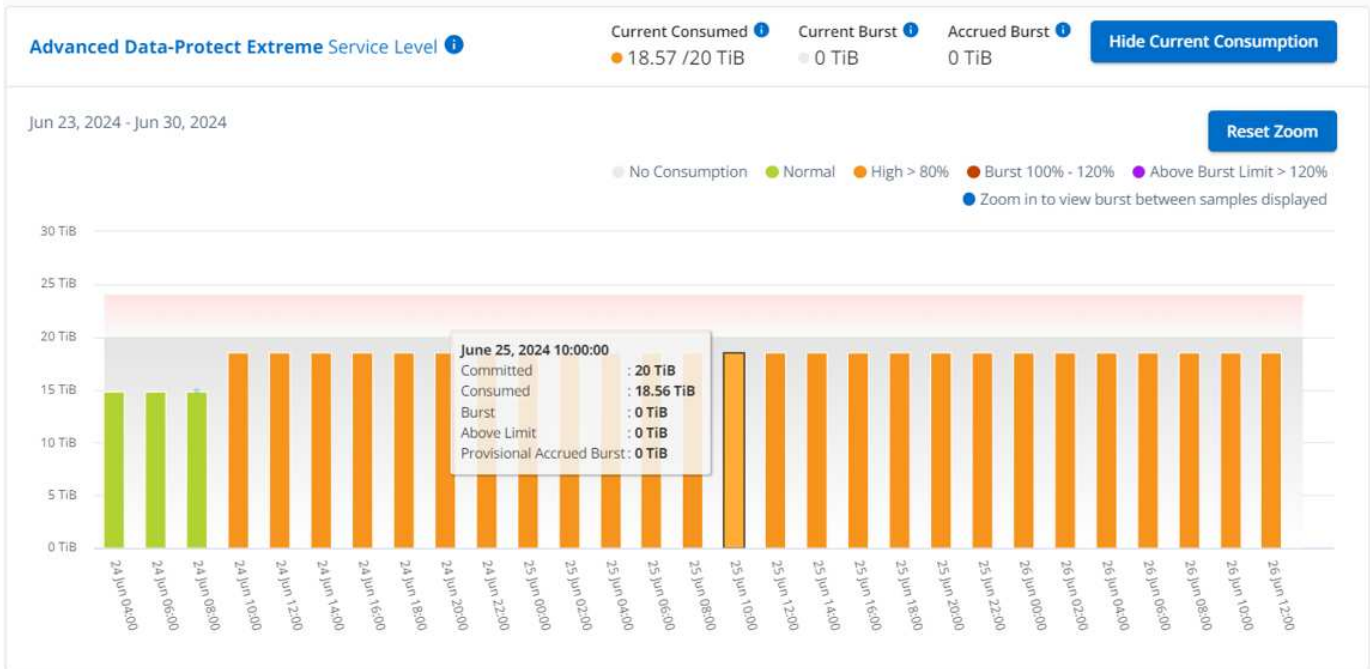


What you can see for the secondary (mirror site) subscription

When you check the secondary subscription, you can see that the bar chart for the *Extreme* service level (base service level) at the same data collection point as the partner site is reversed, and the consumption breakup at the primary and mirror sites is 14.86 TiB and 22.24 TiB respectively.



For the *Advanced Data-Protect* service level, the chart appears like this for the same collection point as at the partner site:



For information about how MetroCluster protects your data, see [Understanding MetroCluster data protection and disaster recovery](#).

Related information

- [Use Keystone dashboard and reporting](#)
- [Subscriptions](#)
- [Current Consumption](#)
- [Volumes & Objects](#)
- [Assets](#)
- [Performance](#)

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**. For StorageGRID, you can use this tab to read the usage by the individual nodes in your object storage environment.



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 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 service levels for both file and object storage.



The **Objects** sub-tab is unavailable under the **Volumes** tab, and within the **Objects** tab, the **Volume Summary** and **Volume Details** sub-tabs contain no data.

Volume Summary

1. Click **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, their QoS compliance status, count of protected volumes, and the total committed, consumed, and available capacity in all those volumes. If you click the number of non-compliant or protected volumes, it takes you to the **Volume Details** tab, where you can view a filtered list showing either the non-compliant volumes or the protected volumes, based on your selection.

Keystone Subscriptions [Help](#)

Subscriptions Current Consumption Consumption Trend **Volumes & Objects** Assets Performance

Volume Summary Volume Details Objects [Download CSV](#)

Subscription: QA-All-RatePlans-V2-03 (A-500024530) Start Date (UTC): August 1, 2023 End Date (UTC): August 1, 2024 Billing Period: Annual

Service Level	Volumes	QoS Compliant	QoS Non-Compliant	Protected
Extreme	766	147	619	129
Performance	346	148	198	37
Premium	0	0	0	0
Standard	0	0	0	0
Value	0	0	0	0

Volume Details

1. Click **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 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.



For advanced data protection add-on service, an additional column appears to indicate whether the volume is a primary or mirror volume in the MetroCluster configuration. You can copy individual node serial numbers by clicking the **Copy Node Serials** button.

Volume Summary Volume Details Objects

[Download CSV](#)

Subscription

QA-All-RatePlans-V2-03 (A-S00024530) Copy Node Serials⚠ QoS non-compliance can impact performance.

Clear Filters

Volume Name	Compliant	QoS Policy Type	Cluster Name	Host Name	Aggregate Name
aksept14_vol	Compliant	AQoS	ks-qa-ots-02222	ks-qa-ots-02222-01	SSD01
aksrcvs_vol	Compliant	AQoS	ks-qa-ots-02222	ks-qa-ots-02222-01	SSD01
akvol1	⚠ Not set	Not Available	ks-qa-ots-01222	ks-qa-ots-01222-01	SSD02
akvol1	⚠ Not set	Not Available	ks-qa-ots-03222	ks-qa-ots-03222-01	ks_qa_ots_03_01_VM_D...

Objects

1. Click **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 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

- [Use Keystone dashboard and reporting](#)
- [Subscriptions](#)
- [Current Consumption](#)
- [Consumption Trend](#)

- [Assets](#)
- [Performance](#)

View cluster and node details managed by Keystone

Use the **Assets** tab to view details about the clusters and nodes managed by your Keystone subscriptions.

Digital Advisor provides a comprehensive inventory-level information of your deployments. The **Assets** tab of the Keystone dashboard, on the other hand, accumulates the cluster-level information on the basis of your subscriptions, and segregates and presents it with the accurate level of details.

Steps

1. Click **GENERAL > Keystone Subscriptions > Assets**.
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.

Keystone Subscriptions [Help](#)

Subscriptions Current Consumption Consumption Trend Volumes & Objects **Assets** Performance SLA Details

[Download CSV](#)

Subscription	Start Date (UTC)	End Date (UTC)	Billing Period
QA-Sust-AFF (A-S00024086)	June 21, 2023	June 21, 2025	Annual

Cluster Name	SE Ratio	ONTAP Version	Platform	Node Serial	HW Support End Date
KSDEVAFF	2.49:1	9.13.1P4	AFF-A300	451704000173	November 30, 2026
KSDEVAFF	2.49:1	9.13.1P4	AFF-A300	451704000174	November 30, 2026

Related information

- [Use Keystone dashboard and reporting](#)
- [Subscriptions](#)
- [Current Consumption](#)
- [Volumes & Objects](#)
- [Consumption Trend](#)
- [Performance](#)

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. Contact support for viewing this tab.

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



If you select the **SLO Reference Line** check box, the IOPS, throughput, and latency graphs are rendered based on the service level objective for the 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 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.

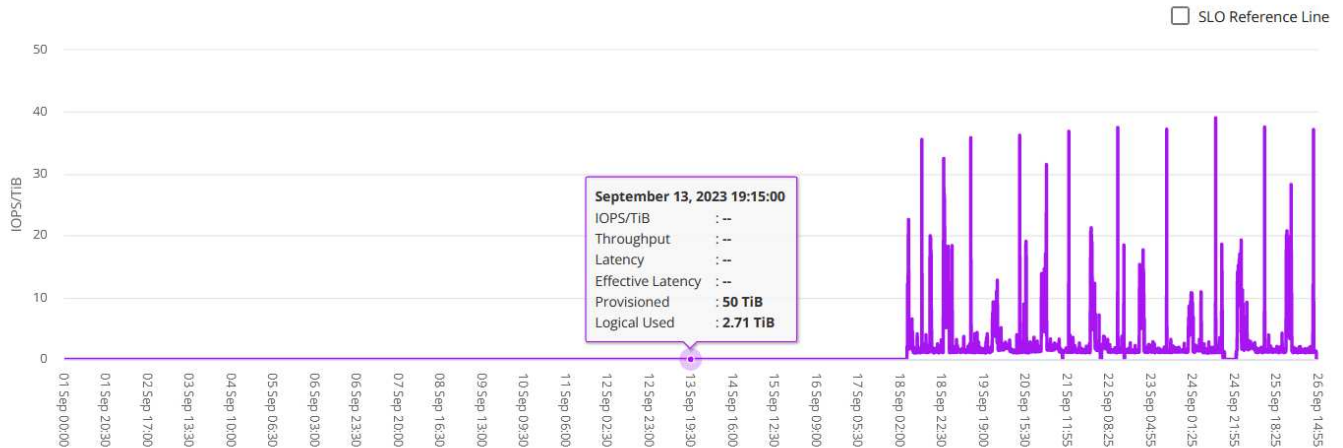
IOPS/TiB

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 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.

IOPS/TiB

Sep 1, 2023 - Sep 26, 2023

4096 IOPS/TiB SLO ⓘ 1.18 IOPS/TiB Current ⓘ 0 IOPS/TiB Minimum ⓘ 39.07 IOPS/TiB Maximum ⓘ 2.78 IOPS/TiB Average ⓘ



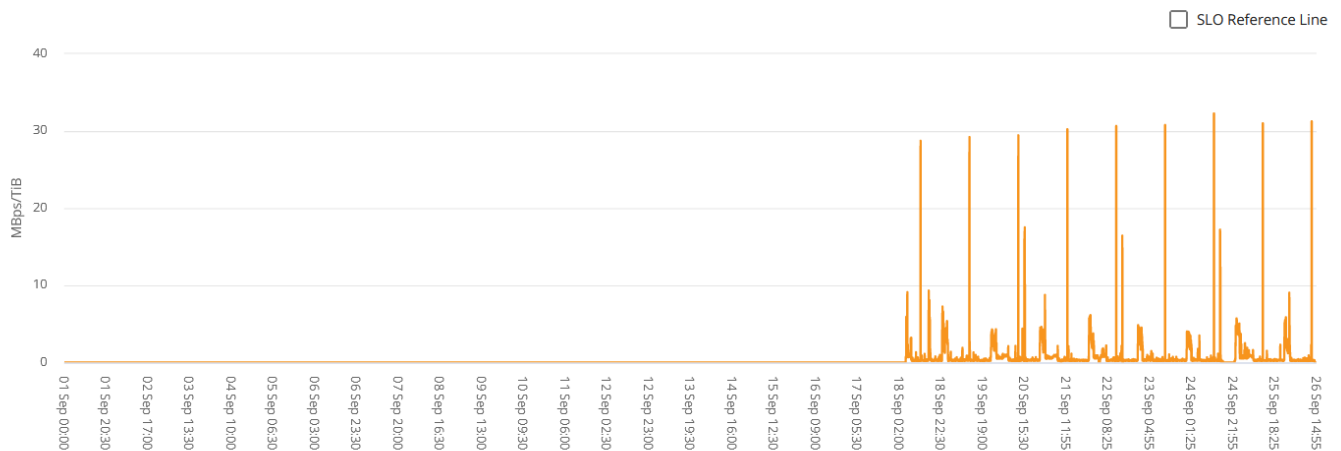
Throughput (MBps/TiB)

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 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.

Throughput (MBps/TiB)

Sep 1, 2023 - Sep 26, 2023

128 MBps/TiB SLO ⓘ 0.23 MBps/TiB Current ⓘ 0 MBps/TiB Minimum ⓘ 32.29 MBps/TiB Maximum ⓘ 0.91 MBps/TiB Average ⓘ



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 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:

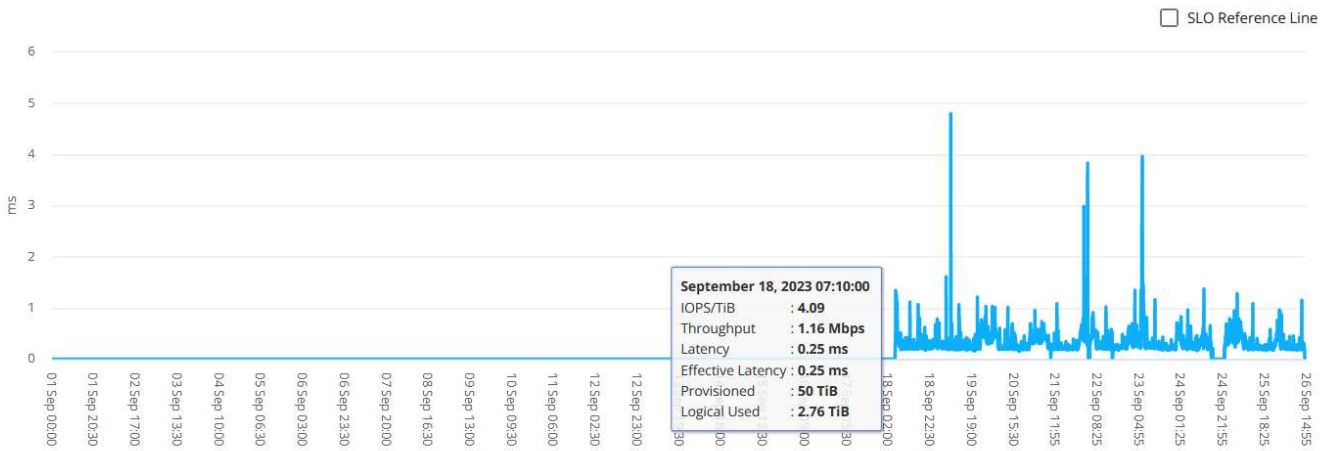
- Light blue: *Latency*. This is the actual latency that includes any latency other than your Keystone service. This might include additional latency, such as the latency occurring between your network and client.

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



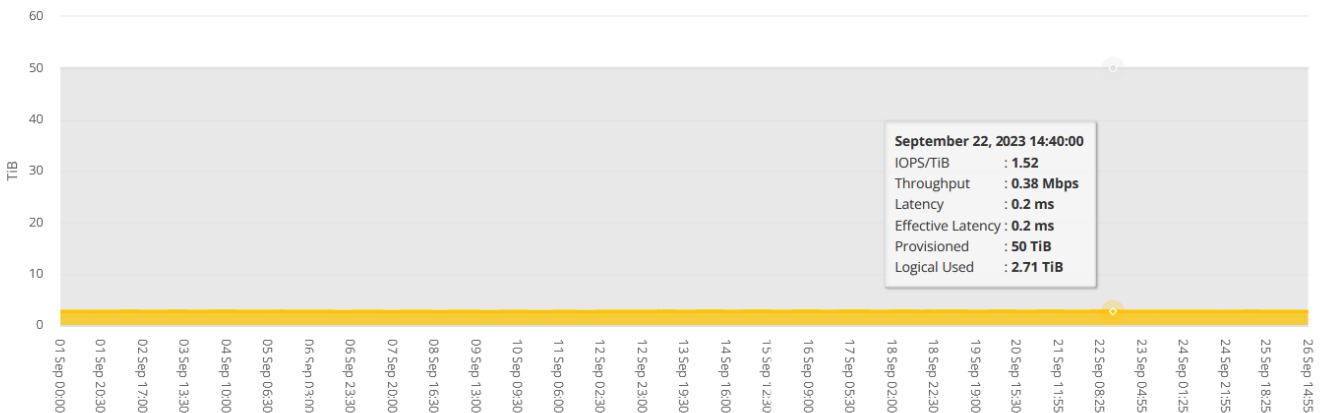
Logical Used (TiB)

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 Current
2.65 TiB Minimum
2.77 TiB Maximum
2.72 TiB Average



Related information

- [Use Keystone dashboard and reporting](#)
- [Subscriptions](#)
- [Current Consumption](#)
- [Consumption Trend](#)
- [Volumes & Objects](#)

- [Assets](#)

Learn about Keystone and BlueXP

NetApp BlueXP is a single control plane to build, protect, and govern data across your on-premises and cloud environments. If you purchase a cloud service on your NetApp Keystone subscription, you can access and manage those services through BlueXP.

The BlueXP Digital Advisor dashboard provides you with a graphical view and drill-down capabilities to monitor your Keystone subscription usage and generate reports. For more information about Digital Advisor dashboard and Keystone, see [Keystone Subscription dashboard and reporting](#).

As a Keystone customer, if you have Cloud Volumes ONTAP subscription, you can use Keystone services to charge your Cloud Volumes ONTAP usage and view your billing and consumption details through BlueXP.

For this, you should create one or more BlueXP accounts and link them with your Keystone account. While you purchase a cloud service through Keystone, you need to provide the details of your BlueXP accounts to your Keystone Success Manager (KSM). This enables proper metering and charging of your cloud service usage through your Keystone subscription.

For more information about Keystone and BlueXP, see the following links in the BlueXP documents:

- [Keystone Subscription](#)
- [Manage Keystone Subscriptions](#)

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 measurement units: GiB, TiB, and PiB
- IO density: IOPS/TiB: Number of input/output operations processed per second based on the total space that is being consumed by the workload, in tebibytes.
- Service availability
- Durability in accurate data access
- Latency and speed

Metrics measurement

- **Capacity measurement in gibibyte (GiB), tebibyte (TiB), and pebibyte (PiB):** Measurements of data storage capacity using base of 1024 (1 GiB = 1024³ bytes, 1 TiB = 1024⁴ bytes, and 1 PiB = 1024⁵ bytes).
- **Operations counter chart in IOPS/TiB:** The protocol operations per second, requested by the application, divided by the size of the volume used by workloads.
- **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).

Throughput performance metrics

Throughput performance metrics are applicable only for file and block services based on:

- 32 KB block sizes
- 70% read/30% write I/O mix

Variations in IO density

IO density calculated in IOPS/TiB and/or MBps/TiB varies based on the following factors:

- Workload characteristics
- Latency, excluding the following:
 - Application latency
 - Host latency

- Latency in the customer network while transferring data to and from the controller ports
- Overhead latency associated with data transfer to the object store in the case of FabricPool
- The latency automatically applied by the QoS to keep IO within service level maximums
- The user and Snapshot copy data that is counted as part of the used capacity
- The allocated absolute minimum IOPS on each ONTAP volume, regardless of the amount of data in the volume:
 - Extreme: 1,000 IOPS
 - Premium: 500 IOPS
 - Performance, Standard, and Value: 75 IOPS
- While using the Advanced Data Protection add-on services, the target latency applies only to servicing IO requests from the local storage.

Volume AQoS

Each ONTAP volume should have the applicable adaptive quality of service (AQoS) policy applied. Otherwise, the capacity within each volume that does not have an AQoS policy applied is billed at the rate of the highest Service Level.

Storage QoS in Keystone

Keystone uses storage quality of service (QoS) to ensure that applications obtain consistent and predictable performance. Without QoS, certain workloads, such as those for booting of multiple systems, might consume most or all of the resources for a period of time and affect other workloads.

For information about QoS, see [Guarantee throughput with QoS overview](#).

Adaptive QoS

Adaptive QoS (AQoS) is used by Keystone services to dynamically maintain the IOPS/TiB ratio based on the volume size. For information about AQoS policies, see [About adaptive QoS](#).

Keystone provides you with AQoS policies that you can set up once your cluster is in production. You should ensure that all your volumes are associated with the correct AQoS policies that are already created and available in your system.

An ONTAP volume is non-compliant if it does not have an AQoS policy applied. A volume without a QoS policy is the last on the list of priority for the system to provide any available input-output operations. However, if any input-output operations are available, then the volume could consume all available IOs.



If you have not applied AQoS policies to your volumes, those volumes will be measured and charged at the highest service level as per your subscription. This may result in unintended burst charges.

Adaptive QoS settings

The Adaptive QoS (AQoS) settings vary with service levels.

Policy name	Extreme	Premium	Performance	Standard	Value
Expected IOPS	6,144	2,048	1,024	256	64
Expected IOPS Allocation	Allocated space				
Peak IOPS	12,288	4,096	2,048	512	128
Peak IOPS Allocation	Used space				
Block Size	32K				

Configuration of adaptive QoS policy group

You can configure adaptive QoS (AQoS) policies to automatically scale a throughput ceiling or floor to volume size. Not all Keystone service levels are aligned with the default ONTAP QoS policies. You can create custom QoS policies for them. For configuring a policy, you should be aware of the following:

- **Policy group name:** The name of the AQoS policy group. For example, `Keystone_extreme`.
- **VServer:** The name of the VServer or storage VM (storage virtual machine).
- **Expected IOPS:** The minimum number of IOPS, per allocated TiB per volume, that the system attempts to provide when enough system IOPS are available.
- **Peak IOPS:** The maximum number of IOPS, per used TiB per volume, that the system allows the volume to reach before it throttles the IOPS through injection of latency.
- **Expected IOPS allocation:** This parameter controls whether the expected IOPS available to the volume is based on the allocated or used size of the volume. In Keystone, this is based on the allocated space.
- **Peak IOPS allocation:** This parameter controls whether the peak IOPS available to the volume is based on the allocated or used size of the volume. In Keystone, this is based on the used space.
- **Absolute minimum IOPS:** The lowest number of expected IOPS that will be applied to a volume if the volume size is very small and would otherwise result in an unacceptable number of IOPS. This value defaults to 1,000 for `Extreme`, 500 for `Premium`, and 250 for `Performance`, and 75 for `Standard` and `Value` service levels.



This is not IOPS density (for example, 75 IOPS/TiB), but an absolute minimum number of IOPS.

For information about IO density, see [Metrics and definitions used in Keystone Services](#). For more information about AQoS policy groups, see [Use adaptive QoS policy groups](#).

Settings of adaptive QoS policies

The settings for adaptive QoS (AQoS) policies for each service level are described in the following sections. The minimum and maximum volume sizes for each service level provided here allow for optimal IOPs and latency values for a volume. Creating too many volumes outside of these guidelines may negatively impact performance in those volumes.

Settings for Extreme service level

Settings and commands for the Extreme service level:

- Sample command:

```
qos adaptive-policy-group create -policy-group <Keystone_extreme> -vserver <SVM_name> -expected-iops 6144 -peak-iops 12288 -expected-iops-allocation allocated-space -peak-iops-allocation used-space -block-size 32K -absolute -min-iops 1000
```

- Minimum volume size: 100GiB, 0.1TiB
- Maximum volume size: 10TiB

Settings for Premium service level

Settings and commands for the Premium service level:

- Sample command:

```
qos adaptive-policy-group create -policy-group <Keystone_premium> -vserver <SVM_name> -expected-iops 2048 -peak-iops 4096 -expected-iops-allocation allocated-space -peak-iops-allocation used-space -block-size 32K -absolute -min-iops 500
```

- Minimum volume size: 500GiB, 0.5TiB
- Maximum volume size: 50TiB

Settings for Performance service level

Settings and commands for the Performance service level:

- Sample command:

```
qos adaptive-policy-group create -policy-group <Keystone_performance> -vserver <SVM_name> -expected-iops 1024 -peak-iops 2048 -expected-iops-allocation allocated-space -peak-iops-allocation used-space -block-size 32K -absolute-min-iops 250
```

- Minimum volume size: 500GiB, 0.5TiB
- Maximum volume size: 80TiB

Settings for Standard service level

Settings and commands for the Standard service level:

- Sample command:

```
gos adaptive-policy-group create -policy-group <Keystone_standard>
-vserver <SVM_name> -expected-iops 256 -peak-iops 512 -expected-iops
-allocation allocated-space -peak-iops-allocation used-space -block-size
32K -absolute-min-iops 75
```

- Minimum volume size: 1TiB
- Maximum volume size: 100TiB

Settings for Value service level

Settings and commands for the Value service level:

- Sample command:

```
gos adaptive-policy-group create -policy-group <Keystone_value> -vserver
<SVM_name> -expected-iops 64 -peak-iops 128 -expected-iops-allocation
allocated-space -peak-iops-allocation used-space -block-size 32K -absolute
-min-iops 75
```

- Minimum volume size: 1TiB
- Maximum volume size: 100TiB

Block size calculation

Note these points before you calculate the block size by using these settings:

- IOPS/TiB = MBps/TiB divided by (block size * 1024)
- Block size is in KB/IO
- TiB = 1024GiB; GiB = 1024MiB; MiB = 1024KiB; KiB = 1024Bytes; as per base 2
- TB = 1000GB; GB = 1000MB; MB = 1000KB; KB = 1000Bytes; as per base 10

Sample block size calculation

To calculate the throughput for a service level, for example `Extreme` service level:

- Maximum IOPS: 12,288
- Block size per I/O: 32KB
- Maximum throughput = $(12288 * 32 * 1024) / (1024 * 1024) = 384\text{MBps/TiB}$

If a volume has 700GiB of logical used data, the available throughput will be:

Maximum throughput = $384 * 0.7 = 268.8\text{MBps}$

Supported storage in Keystone

Keystone STaaS services support file and block storage of ONTAP, object storage of

StorageGRID platform, and data management capabilities of Cloud Volumes ONTAP.

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 coexist with each other. For example, a cloud storage subscription can co-term with file, block, 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 file, block, and object subscription, a cloud storage subscription cannot be added during the last 90 days of the subscription.

Services for file, block, and object storage

Keystone STaaS services for ONTAP file and block storage, and StorageGRID object storage, support multiple features and protocols, and described in the following table:

Storage	Platform	Protocols	Supported features
File storage	ONTAP	NFS and CIFS	Supported ONTAP features: <ul style="list-style-type: none">• FlexVol• FlexGroup• Snapshot copies• SnapMirror (Asynchronous)• SnapVault• SnapLock Enterprise• FabricPool/Cloud tiering• SnapRestore• FlexClone• SnapCenter (license is included but is not a part of Keystone services, and management is not guaranteed)• Autonomous ransomware protection¹

Storage	Platform	Protocols	Supported features
Block storage	ONTAP	FC and iSCSI	Supported ONTAP features: <ul style="list-style-type: none"> • FlexVol • FlexGroup • Snapshot copies • SnapMirror (Asynchronous) • SnapVault • SnapLock Enterprise • FabricPool/Cloud tiering • SnapRestore • FlexClone • SnapCenter (license is included but is not a part of Keystone services, and management is not guaranteed)
Object storage	StorageGRID	S3	Supports multiple information lifecycle management (ILM) policies across multiple sites ²



¹ For information about ransomware protection in ONTAP, see [Autonomous Ransomware Protection](#).

² Each site requires a separate subscription.

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.



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 subscriptions need to be procured directly from hyperscaler 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 data placed on the Keystone infrastructure by a customer. All Keystone capacities refer to a logical capacity.

For example, if a 1 TiB file is stored on the Keystone infrastructure then a minimum of 1 TiB of capacity should be purchased.

Committed capacity

The minimum logical capacity billed each month during the subscription:

- Capacity is committed to each service level.
- Committed capacity and additional 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 through Keystone Success Manager (KSM).
For information about requesting changes, see [NetApp Global Services Support Center](#).

Consumed capacity

Consumed capacity refers to the capacity (in TiB of storage) currently being consumed on the service. Keystone service considers the sum of the logical used sizes (not the physical capacity used) of all volumes on a particular service level to calculate the consumed capacity for that service level.

Burst capacity

Keystone service enables you to use additional capacity on top of the committed capacity for a service level. This is 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, and is charged at the same rate as the committed capacity.
- Burst capacity can be consumed on an elastic basis and is charged on a daily basis for the consumed average.

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.

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 service level.

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

Each service level is defined by its I/O density, that is IOPS/TiB/volume. This is the ratio of performance (input/output operations per second [IOPS]) and used storage capacity (TiB) which is IOPS/TiB at average latency per volume.

You select service levels based on your storage environment, and storage and consumption needs. The base service levels are available for you by default. Specific service levels are additionally available, if you have opted for add-on services. For example, for the advanced data protection add-on service, the *Advanced Data-Protect* service level is assigned to your subscription.



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

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

Service levels for file and block storage

Supported protocols: NFS, CIFS, iSCSI, and FC

Service level	Extreme	Premium	Performance	Standard	Value
Sample workload types	Analytics, databases, mission-critical apps	VDI, VSI, software development	OLTP, OLAP, containers, software development	File shares, web servers	Backup
Maximum IOPS/logical TiBs stored per volume	12,288	4,096	2,048	512	128
Maximum IOPS/logical TiBs allocated per volume	6,144	2,048	1,024	256	64
Maximum MBps/logical TiBs stored per volume @ 32K B/S	384	128	64	16	4
Target 90th percentile latency	<1 ms	<2 ms	<4 ms	<4 ms	<17 ms
Block size	32K				

More on service levels for file and block storage

The base service level metrics depend on the following conditions:

- The service levels for file and block storage support ONTAP 9.7 and later.
- IOPS/TiB/volume, MBps/TiB/volume, and latency values for service levels are based on the amount of data stored in the volume, 32KB block size, and a random combination of 70% read and 30% write IO operations.
- Actual IOPS/TiB/volume and MBps/TiB/volume may vary based on the actual or assumed block size, system workload concurrency, or input-output operations.
- 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 automatically applied by QoS to keep IO within service level maximums
- Latency values are not applicable to MetroCluster write operations. These write operations are dependent on the distance of remote systems.
- If one or more volumes on a storage system do not have an AQoS policy assigned, then these volumes are considered as non-compliant volumes, and no target service levels are applicable for those 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.
- Workload IO operations need to be balanced across all deployed controllers, as determined by the Keystone order.

Object storage

Supported protocol: S3

Service level	Object
Workload type	Media repository, archiving
Maximum IOPS/logical TiB stored per volume	N/A
Maximum MBps/logical TiB stored per volume	N/A
Average Latency	N/A



Latency does not include overheads associated with data transfer to the object store in case of FabricPool storage.

Cloud storage

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

Service level	Cloud Volumes ONTAP
Workload type	Disaster Recovery, software development/testing, business apps

Maximum IOPS/logical TiB stored per volume	N/A
Maximum MBps/logical TiB stored per volume	N/A
Average Latency	N/A



- 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](#)
- [Quality of Service \(QoS\) in Keystone](#)
- [Keystone pricing](#)

Capacity requirements for service levels

The capacity requirements for Keystone STaaS service levels differ with the file, block, object, or cloud storage supported by the Keystone STaaS subscription.

Minimum capacity requirements for file and block services

The minimum capacity and incremental capacity allowed per subscription is described in the following table. The minimum capacity per service level is defined to be the same across Keystone sales motions. The capacity above the minimum capacity either at the beginning of the subscription, or as an add-on service to the subscription, or after reallocation during the subscription is also structured in the table.

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

Minimum capacity requirements for object storage

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

Capacity	Data tiering	Object	Cloud Volumes ONTAP	Cloud Backup service
Minimum capacity [in TiB]	Not applicable	500	4	4
Incremental capacity (and in multiples) allowed at start of subscription [in TiB]	Not applicable	100	1	1
Incremental capacity (and in multiples) allowed as add-on during subscription [in TiB]	Not applicable	100	1	1

Capacity adjustments

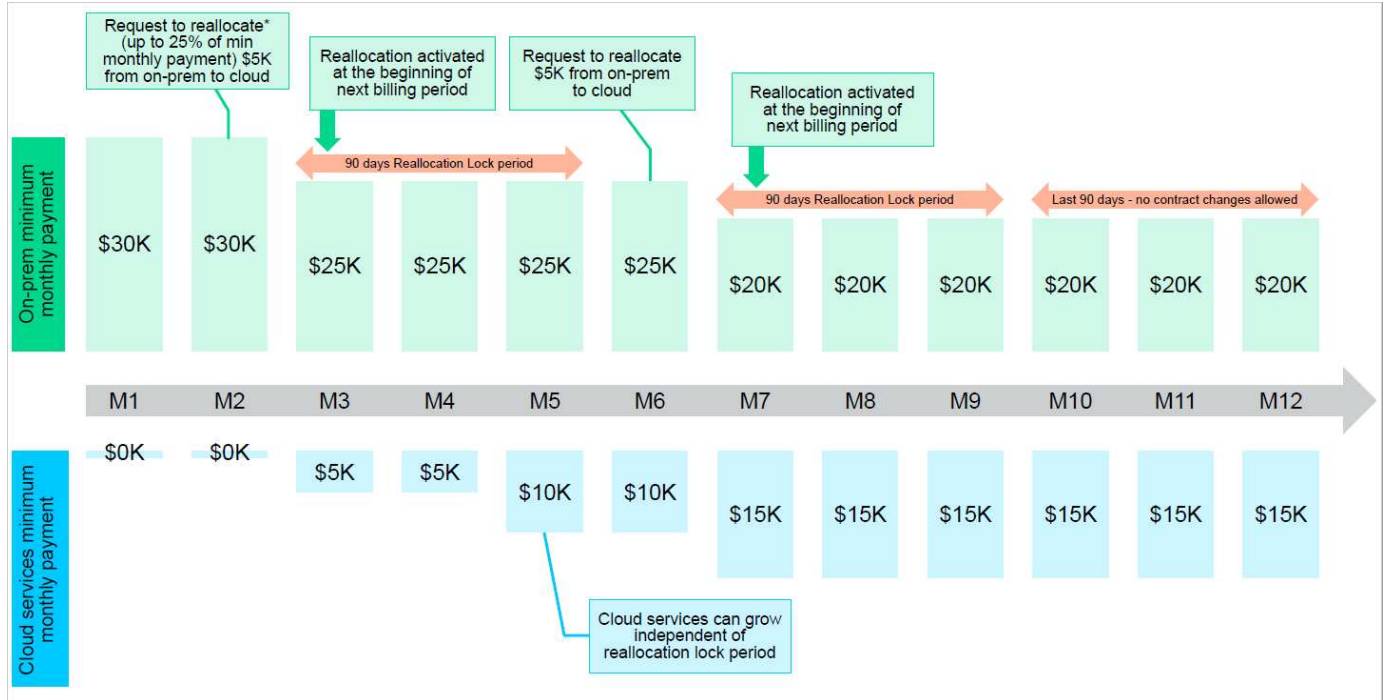
Note the following clauses for capacity adjustments:

- Capacity can be added anytime during the term, except for the last 90 days of the contract term, in the increments per service level as described in the tables in the previous section. Addition of capacity and/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 20% above the committed capacity for a 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 service level during a subscription term is allowed. However, moving from a higher service level to a lower 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.



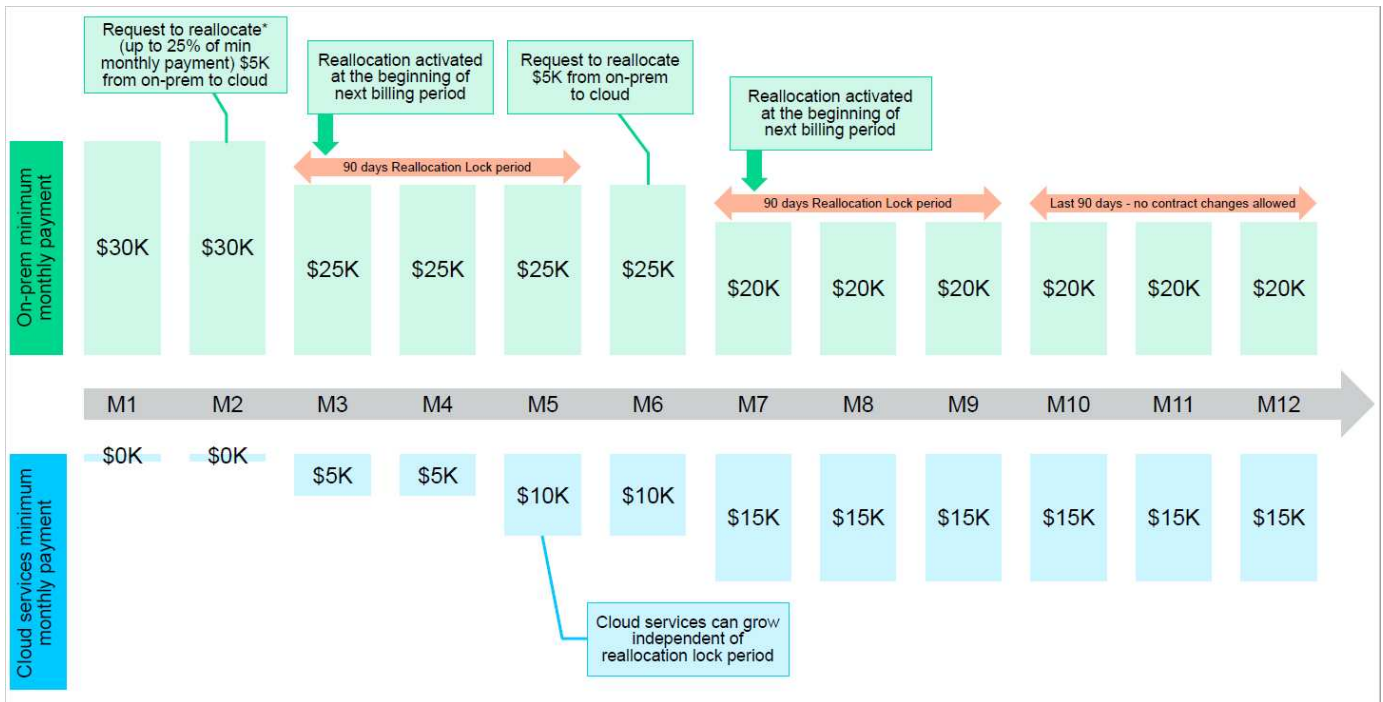
Quarterly spend reallocation

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 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 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 service level and 47 TiB hybrid cloud capacity of Cloud Volumes ONTAP 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.

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 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](#)

Add-on services

Learn about advanced data protection

You can subscribe to the advanced data protection add-on service as a part of your Keystone STaaS subscription. This add-on service leverages NetApp MetroCluster technology to ensure efficient data protection of your mission-critical workloads at a recovery point objective (RPO) of 0.



Keystone STaaS standard services for file and block storage offer default data protection services by leveraging NetApp technologies, such as SnapMirror, SnapVault, and Snapshot.

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

Keystone advanced data protection service can synchronously mirror data to a secondary site. In case of a disaster at the primary site, the secondary site can take over, without any loss of data. This feature leverages the MetroCluster configuration between two sites to enable data protection. You can avail the advanced data protection add-on services for only your file and block storage services. As a part of this add-on service, the `Advanced Data-Protect` service level is assigned to your subscription.

For information about ONTAP MetroCluster, see [MetroCluster Documentation](#).

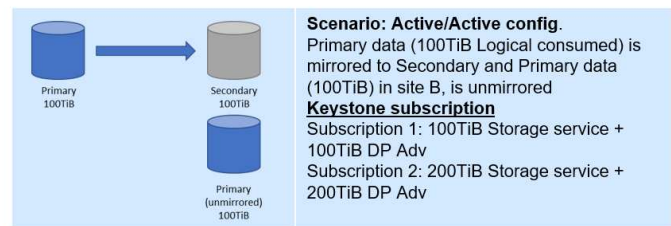
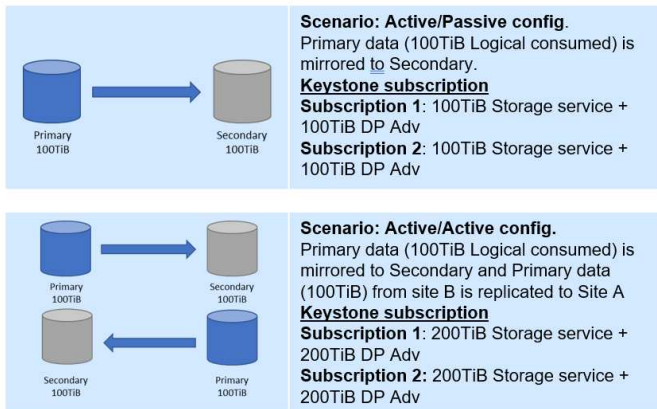
For information about how to view the consumption in a MetroCluster configuration, see [Reference charts for advanced data protection](#).

The add-on charges are applicable to all the capacities in the subscription: the source, mirrored copy, and unmirrored data.

Note the following:

- For this service, 100% of the committed capacity on an associated storage is configured as committed capacity.
- Storage is charged for both the source and the destination clusters. This add-on service is also charged for both the primary and secondary (mirrored) volumes.
- The charges are applicable only to your file and block storage.

The following MetroCluster scenarios are supported:



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 Service Levels, see [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 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.

Learn about co-location services powered by Equinix

To provide a full-stack solution as a service, NetApp has partnered with Equinix for hosting NetApp Keystone STaaS services in an Equinix data center.

Keystone co-location (Co-Lo) services powered by Equinix remain unchanged from the standard Keystone service offering.

In this service:

- Equinix provides space, power, cooling, networking, invoice, and storage, on a monthly basis.
- Support is provided for certain Keystone sales motions.
- The services are supported in the data centers across 11 countries.

Equinix has data centers at these locations:

Data center	Country
Amsterdam	Netherlands
Atlanta	U.S.
Chicago	U.S.
Dallas	U.S.
Denver	U.S.
Frankfurt	Germany
London	U.K.
Los Angeles	U.S.
Madrid	Spain
Melbourne	Australia
Miami	U.S.
Milan	Italy
Osaka	Japan
Paris	France
Seattle	U.S.
Silicon Valley	U.S.
Sydney	Australia

Data center	Country
Tokyo	Japan
Toronto	Canada
Washington DC	U.S.
Zurich	Switzerland

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 Service Levels, see [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 USCS

United States Citizen Support (USCS) 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. ^[1]

NetApp Global Services Support Center monitoring

NetApp Global Services and Support Center (GSSC) 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. ^[2]

Support

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

[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.

Keystone STaaS SLA

Availability SLA

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



SLAs and guarantees are available on a nomination basis.

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.

Service levels

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

Service credits

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 service level for the Keystone order.
- **capacity fees:** The fees for the affected 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 Keystone Global Services and Support Center (GSSC).

- 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 Keystone GSSC.

	A	B	C	D	E
1	Subscription_No	Service_level	Volume_uuid	Date	Is_SLA_Breached
2	192037XXX	premium	fxxxxb1-fxb-xxed-axxx-dxxxxxxx5	2024-01-01	Yes
3	192037XXX	premium	fxxxxb1-fxb-xxed-axxx-dxxxxxxx6	2024-01-02	Yes
4	192037XXX	premium	fxxxxb1-fxb-xxed-axxx-dxxxxxxx7	2024-01-03	Yes
5	192037XXX	premium	fxxxxb1-fxb-xxed-axxx-dxxxxxxx8	2024-01-06	Yes
6	192037XXX	premium	fxxxxb1-fxb-xxed-axxx-dxxxxxxx9	2024-01-17	Yes



- A service credit request should be initiated within six weeks after GSSC 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 Global Services Support Center](#).

Performance SLA

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



SLAs and guarantees are available on a nomination basis.

Metrics

- **Degraded performance:** The amount of time, in minutes, per incident, during which the 90th percentile latency target is not met.
- The **90th percentile latency** is measured per volume, per performance level, for all volumes within a Keystone Order. Latency is sampled every five minutes, and the 90th 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.
 - When using the advanced data protection add-on service, the target latency includes only IO operations to and from the local storage array.
 - 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 AQuS 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.

Service levels

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

Service level	Extreme	Premium	Performance	Standard
Target 90 th percentile latency	<1ms	<2ms	<4ms	<4ms

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

Service credits

NetApp issues service credits for the degraded performance:

Performance threshold	Service credit
90 th 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 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:

$$\text{Service credits} = (10 / 50) \times 1000 \times 2 \times 0.03$$

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 Keystone Global Services and Support Center (GSSC).

- 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 Keystone GSSC.

	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 GSSC 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 Global Services Support Center](#).

Sustainability SLA

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 SLA. Sustainability SLA defines the maximum consumption of W/TiB for each eligible service level, helping organizations meet their sustainability goals.



SLAs and guarantees are available on a nomination basis.

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 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](#).

Service levels

Sustainability SLA is based on the following consumption criteria:

Service level	SLA 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 [Service levels in Keystone](#).

Service credits

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 Keystone Global Services and Support Center (GSSC), 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_SLA_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 GSSC 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 Global Services Support Center](#).

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.



SLAs and guarantees are available on a nomination basis.

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

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

If you prefer operational expenditures (OpEx) consumption model over capital expenditure (CapEx) or leasing, you can opt for the NetApp Keystone STaaS pay-as-you-grow model, which offers flexible and scalable consumption with predictable and upfront pricing for your storage subscription.

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, Performance, Standard, Value, and Object 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, file, block, object, or cloud storage services.
- Select a flexible term for the services and payment: You can opt for 12 months, 25TiB, or more per site. Thereafter, you can auto renew for 12 months.

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 service level while purchasing the subscription.

Committed capacity can be the total capacity for various 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. Usually, it is 20% above the committed capacity.

Committed capacity is the capacity committed to you while purchasing the subscription. The committed capacity and burst capacity are measured per service level. Consumed capacity is the capacity that your workloads actually use.

When the consumed capacity is greater than the committed capacity for a service level, burst consumption is recorded and charged accordingly. Usually, it is 20% above the committed capacity. 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 [Consumption Trend tab](#).

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 optimize service usage and manage costs. The scenarios include cloned volumes, advanced data protection, temporary volumes, QoS policies, 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 advanced data protection

Advanced data protection uses NetApp MetroCluster to mirror data between two physically separated clusters. For MetroCluster mirrored aggregates, data is written twice, once on each cluster. The Keystone service charges for consumption on each side independently, resulting in two identical consumption records. The add-on charges are applied on all the capacities in the subscription, irrespective of whether the data is at the source, or it is mirrored or unmirrored data.

If you monitor your clusters through ONTAP System Manager (System Manager) or Active IQ Unified Manager (Unified Manager), you might see a discrepancy between the consumption reported on these tools and Keystone. System Manager and Unified Manager do not report volumes on the mirrored (remote) cluster, and in doing so, reports half the consumption metrics that the Keystone service reports.

Example:

Site A and Site B are set up in a MetroCluster configuration. When a user creates a volume of 10TB in site A, an identical volume of 10TB is created in site B. Keystone identifies 10TB of consumption in each site, for a total increase of 20TB. System Manager and Unified Manager report a 10TB volume created in site A, but do not report a 10TB volume in Site B.

Additionally, all volumes created on a Keystone system with advanced data protection will be counted towards the consumption of advanced data protection, regardless of whether those volumes are mirrored or not.

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 and adaptive QoS policies

Keystone measures consumption based on Service Levels. Each Service Level is associated with a specific adaptive quality of service (QoS) policy. During deployment, you will be informed of the details of each QoS policy for your subscribed Keystone services. During storage management operations, ensure that your volumes have the appropriate QoS policies assigned as per your subscribed Service Levels, to avoid unexpected billing.

For more information about QoS policies in ONTAP, see [Guarantee throughput with QoS overview](#).

Billing for SnapMirror destinations

The pricing for the SnapMirror destination volume is governed by the QoS policy for the service level assigned on the source. However, if the source does not have an associated QoS policy, the destination is billed based on the lowest available service level.

Billing for LUNs

For LUNs, the same billing pattern is followed as for the volumes that are governed by QoS policies. If separate QoS policies are set on LUNs, then:

- The size of the LUN is counted for consumption according to the associated service level of that LUN.
- The remainder of the space in the volume, if any, is charged according to the QoS policy of the service level set on 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 monthly and yearly.

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.

Annual billing

An invoice is generated at the beginning of each subscription year for the minimum payment of the committed capacity. It is generated on the start date of the subscription.

Another invoice is sent at the end of a subscription quarter, summing up the applicable charges of any burst usage accrued in that quarter.

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. The billing is calculated from the day when the change in the committed capacity is effective.

Get help with Keystone

NetApp Global Services and Support Center (GSSC) and NetApp Keystone Success Manager (KSM) are responsible for providing you service for your Keystone subscriptions. If you need help, you can contact the support team.

NetApp Global Services and Support Center

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 and Support Contact

The NetApp Global Services and Support Center team primarily support the services to NetApp Keystone customers. You can use the following information to reach out to the support team.

- Global service contacts :
<https://www.netapp.com/company/contact-us/support/>
- 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
keystone.escalations@netapp.com
- NetApp uses AIOPs 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 AIOPs solution and GSSC applications. Only L3 issues are escalated to NetApp through GSSC.

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>

GSSC monitoring

NetApp Global Services and Support Center 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) 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 GSSC 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](#).

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 © 2024 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.