Get started

Keystone

NetApp
January 20, 2026

Table of Contents

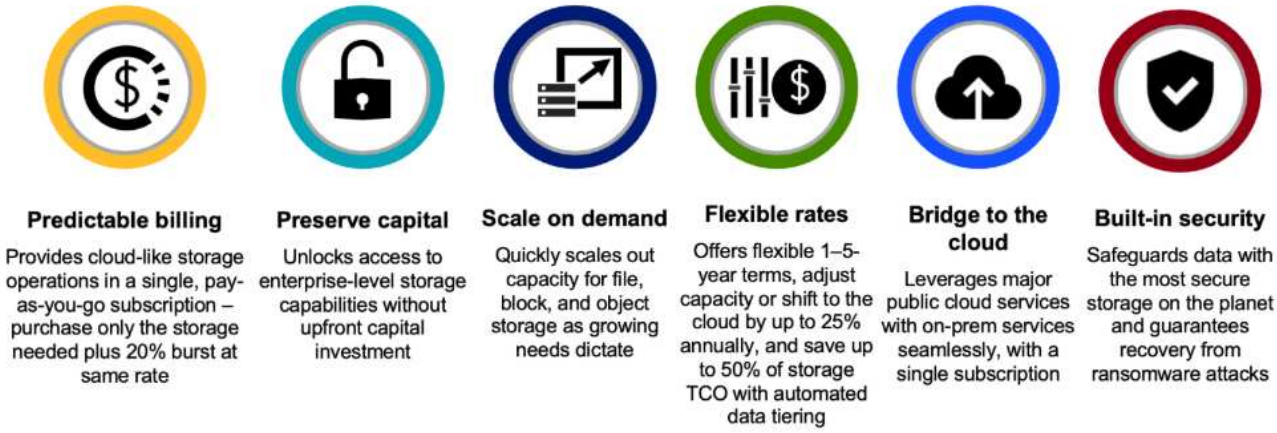
Get started

Learn about NetApp Keystone

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

With Keystone, you benefit from:

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



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

Keystone Storage-as-a-service (STaaS)

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

Related information

- Keystone pricing

- Add-on services in Keystone STaaS
- Performance service levels in Keystone
- Keystone infrastructure
- Operational models in Keystone

Understand Keystone infrastructure

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

NetApp reserves the rights to take the following actions:

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

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

- The Keystone infrastructure, including NetApp storage systems.
- Tools to manage and operate the service such as the ITOM monitoring solution, NetApp Console, 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, ASA, and FAS, and StorageGRID systems.

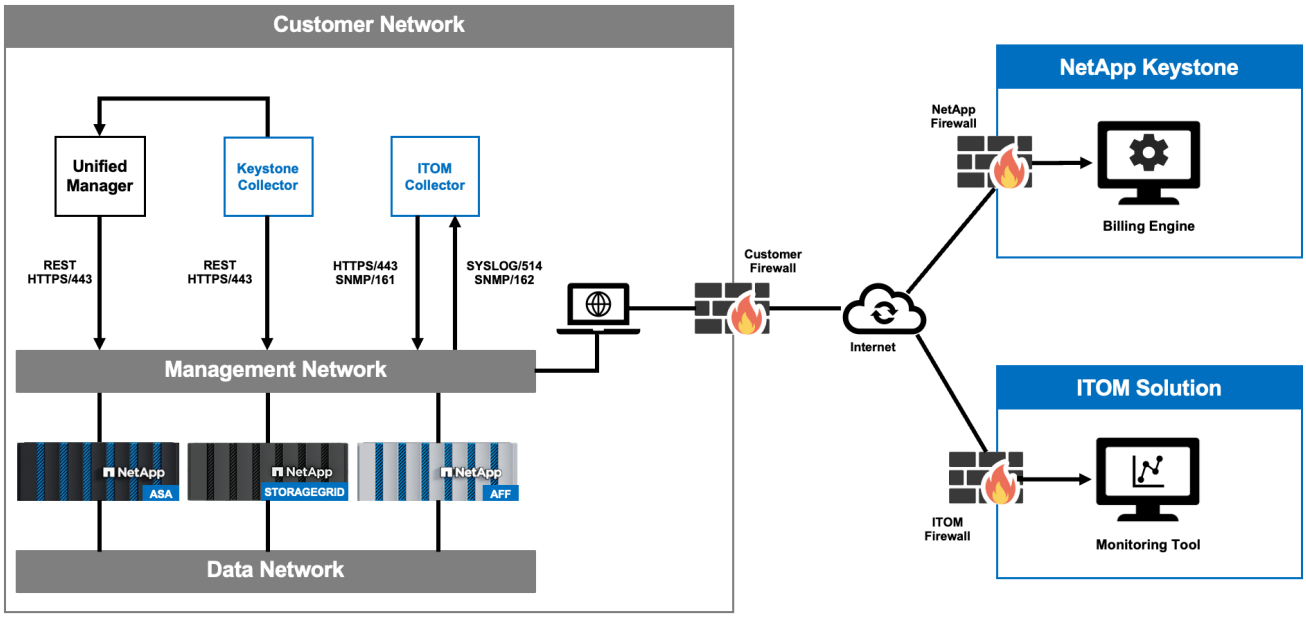
Monitoring tools

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

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

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

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



You can view the subscription and consumption details for your Keystone subscriptions through the NetApp Console or Digital Advisor. To learn more about Keystone reporting, refer to Keystone dashboard overview.

Learn about Keystone Collector

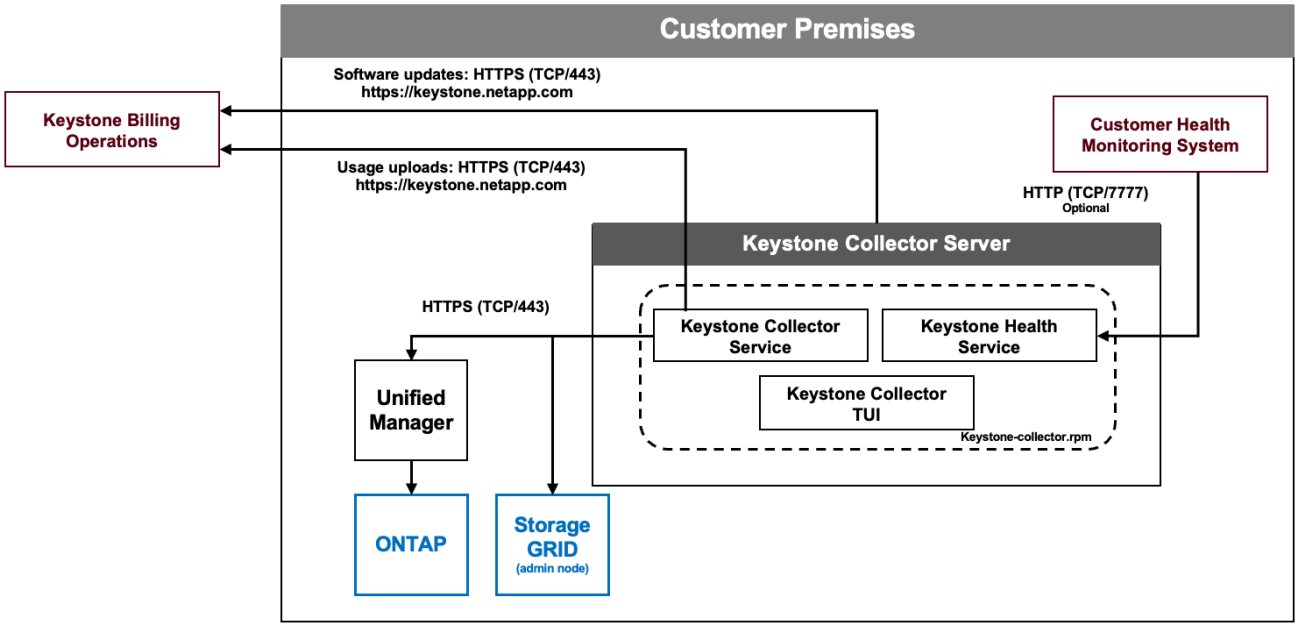
Keystone Collector is NetApp software that you install on a VMware vSphere or Linux host at your site to access your Keystone services. It collects usage data for Keystone systems.

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

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

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

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



Components required for Keystone services

You need several components to enable NetApp Keystone STaaS services. Review these components before you begin.

Site requirements

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

Space

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

Racks

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

PDUs

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

Power

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

Cooling

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

Virtual machines

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

Deployment Options

Keystone Collector can be deployed through the following methods:

- VMware OVA template (VMware vCenter Server 6.7 or later is required)
- Customer provides a Linux server running on one of the following operating systems: Debian 12, Red Hat Enterprise Linux 8.6 or later 8.x versions, Red Hat Enterprise Linux 9.0 or later versions, or CentOS 7 (for existing environments only). The Keystone software is installed using the `.deb` or `.rpm` package, depending on the Linux distribution.

ITOM Collector can be deployed through the following methods:

- Customer provides a Linux server running on Debian 12, Ubuntu 20.04 LTS, Red Hat Enterprise Linux (RHEL) 8.x, Red Hat Enterprise Linux 9.0, Amazon Linux 2023, or newer versions.
- Customer provides a Windows server running Windows Server 2016 or newer versions.

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

Networking

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

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

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

Remote access requirement

Network connectivity is required between the storage infrastructure installed at the customer data center or customer owned co-located services, and Keystone operations center. The customer is responsible for providing the compute and virtual machines, and the internet services. The customer is also responsible for OS

patching (non-OVA based deployments) and security hardening based on internal security policies. The network design should be over a secured protocol and firewall policies will be approved by both NetApp and customers.

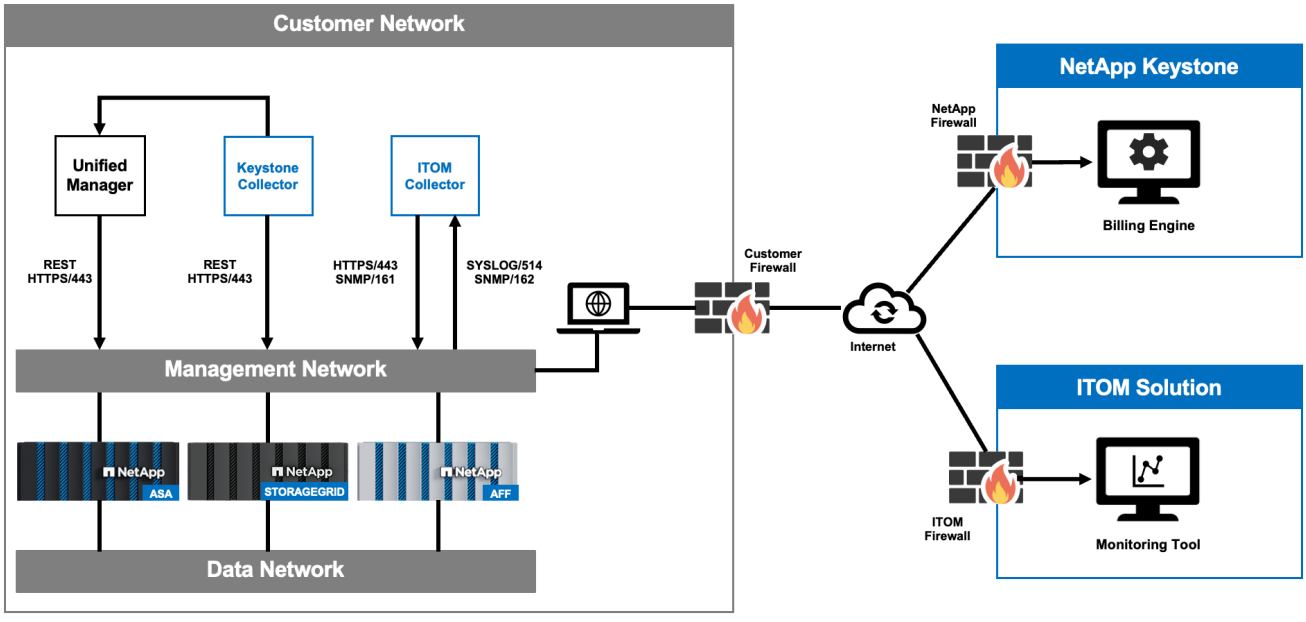
NetApp needs to access the hardware and software components installed for monitoring and management to provide services such as monitoring and billing to Keystone customers. The most common method is to establish a virtual private network (VPN) connection to the customer network and access the required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

Keystone data flow

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

Keystone Collector data flow

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

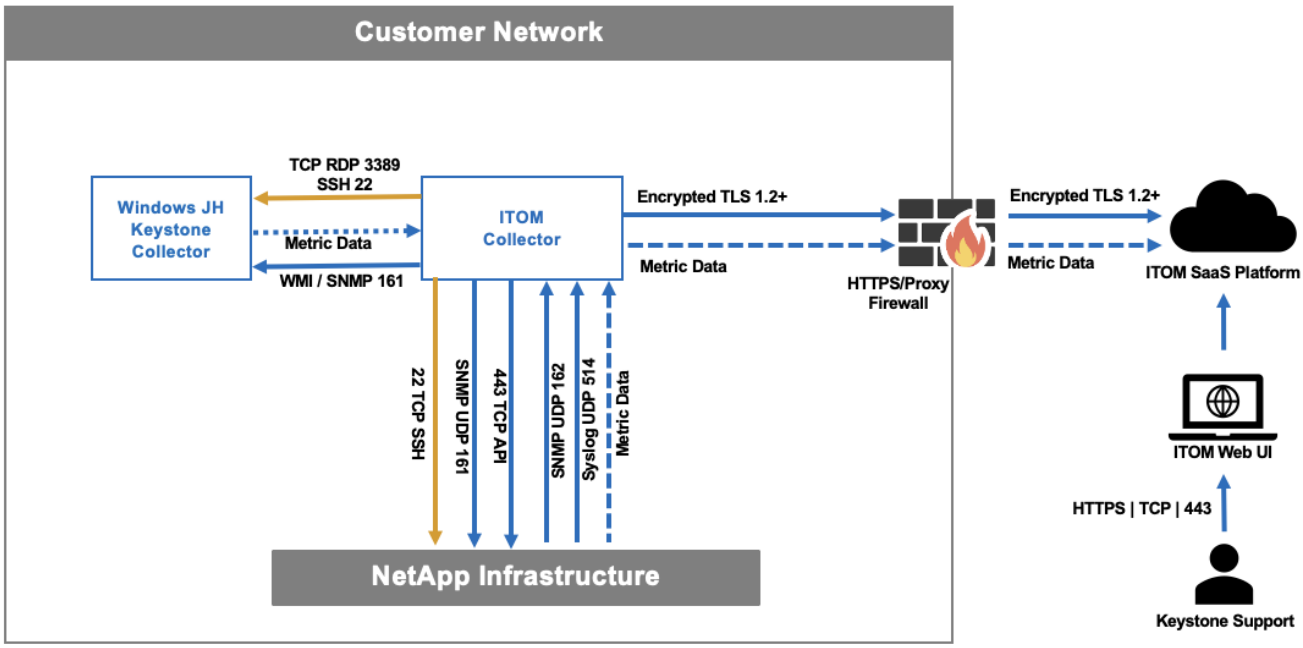


Legend

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

Monitoring data flows

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



Legend

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

Compliance standards

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

Operational models in Keystone

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

before you get started with Keystone.

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

Roles and responsibilities across the service lifecycle

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

Task	NetApp	Customer
Installation and related tasks • Install • Configure • Deploy • Onboard	✓	None
Administration and monitoring • Monitor • Report • Perform administrative tasks • Alert	None	✓
Operations and optimization • Manage capacity • Manage performance • Manage SLA	None	✓

Task	NetApp	Customer
Support • Support customer • Hardware break fix • Software support • Upgrades and patches	✓	None

For more information on deployment, see Keystone infrastructure and Components for deployment.

Copyright information

Trademark information