Keystone infrastructure

Keystone

NetApp
January 25, 2023

Table of Contents

Keystone infrastructure

Keystone infrastructure

This section describes the NetApp Keystone STaaS infrastructure, architecture, and management application for the NetApp and customer-operated environments.

Keystone infrastructure, design, choice of technology, and component products reside solely with NetApp. 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 that includes storage controllers.
- Tools to manage and operate the service such as OpsRamp, Active IQ, and Active IQ Unified Manager.

Storage Platforms

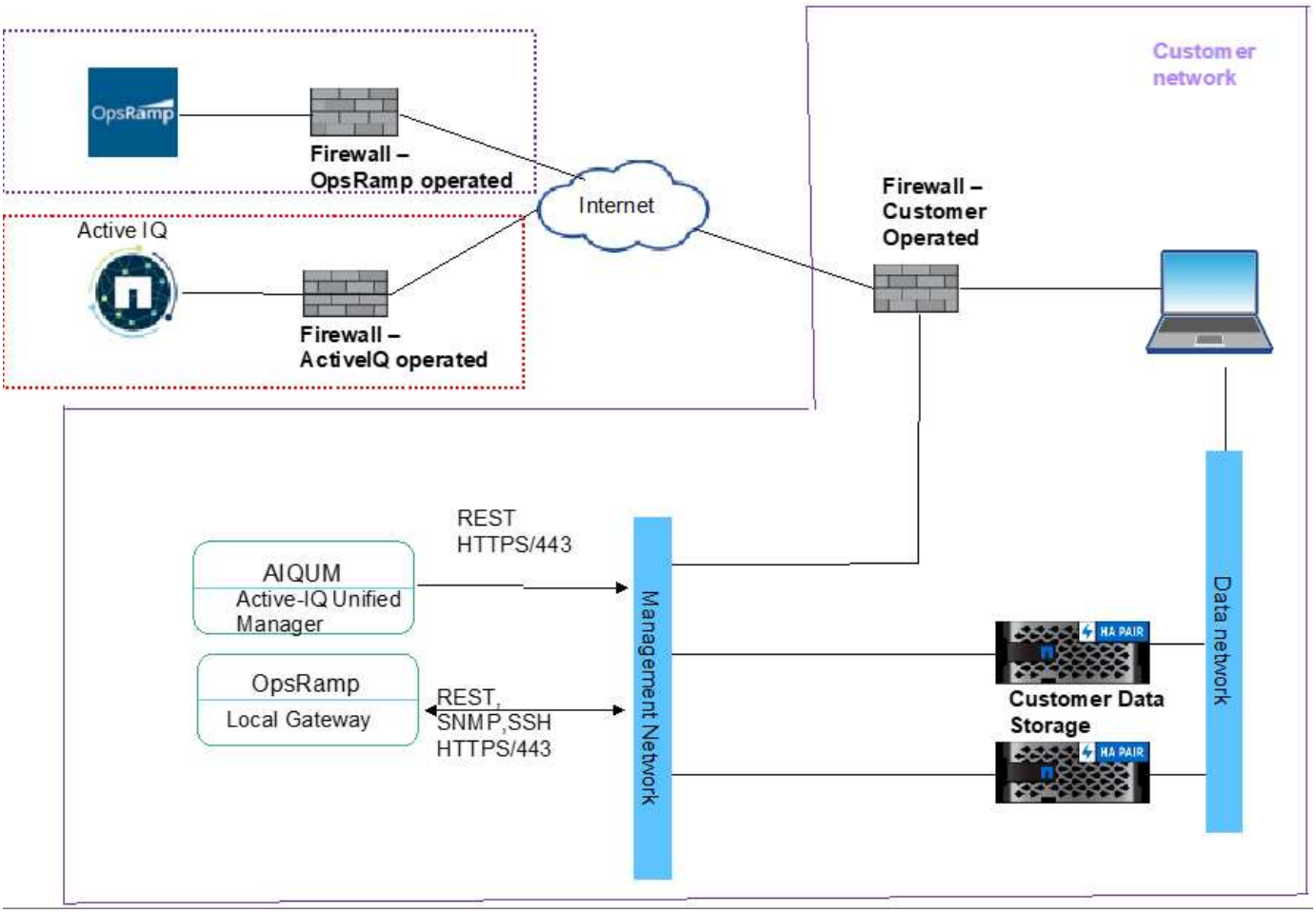
Enterprise applications need storage platforms to support fast provisioning-workflows, maintain continuous availability, sustain high workloads with low latency, deliver higher performance, and support integration with major cloud providers. NetApp has several products and technologies for supporting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

- OpsRamp local gateway: OpsRamp is 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. For information about
- 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 periodically every 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 data for billing and sends it to Zuora for billing. Digital Advisor customer portal allows you to log in and view your subscription and consumption details for your Keystone subscription.



For more information, see Keystone and Digital Advisor.

Components for deployment

This section lists the components required to enable NetApp Keystone STaaS services in your environment.

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.

Storage virtual machines

Storage virtual machines (storage VMs) should be deployed with the following to support the monitoring and metering of Keystone subscriptions. One storage VM is required for theKeystone Collector; another is required for the OpsRamp Gateway

- Keystone Collector- Used to collect usage metrics:
  - vCPU: 4
  - vRAM: 16 GB
  - vDisk: 200 GB
- OpsRamp Gateway – Used to real time monitor + remote support ONTAP by Keystone GSSC:
  - vCPU: 8
  - vRAM: 16 GB
  - vDisk: 100 GB

Deployment Options

The 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, and Keystone software is installed via `.rpm` installation process.

OpsRamp 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 the Keystone Collector and OpsRamp 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

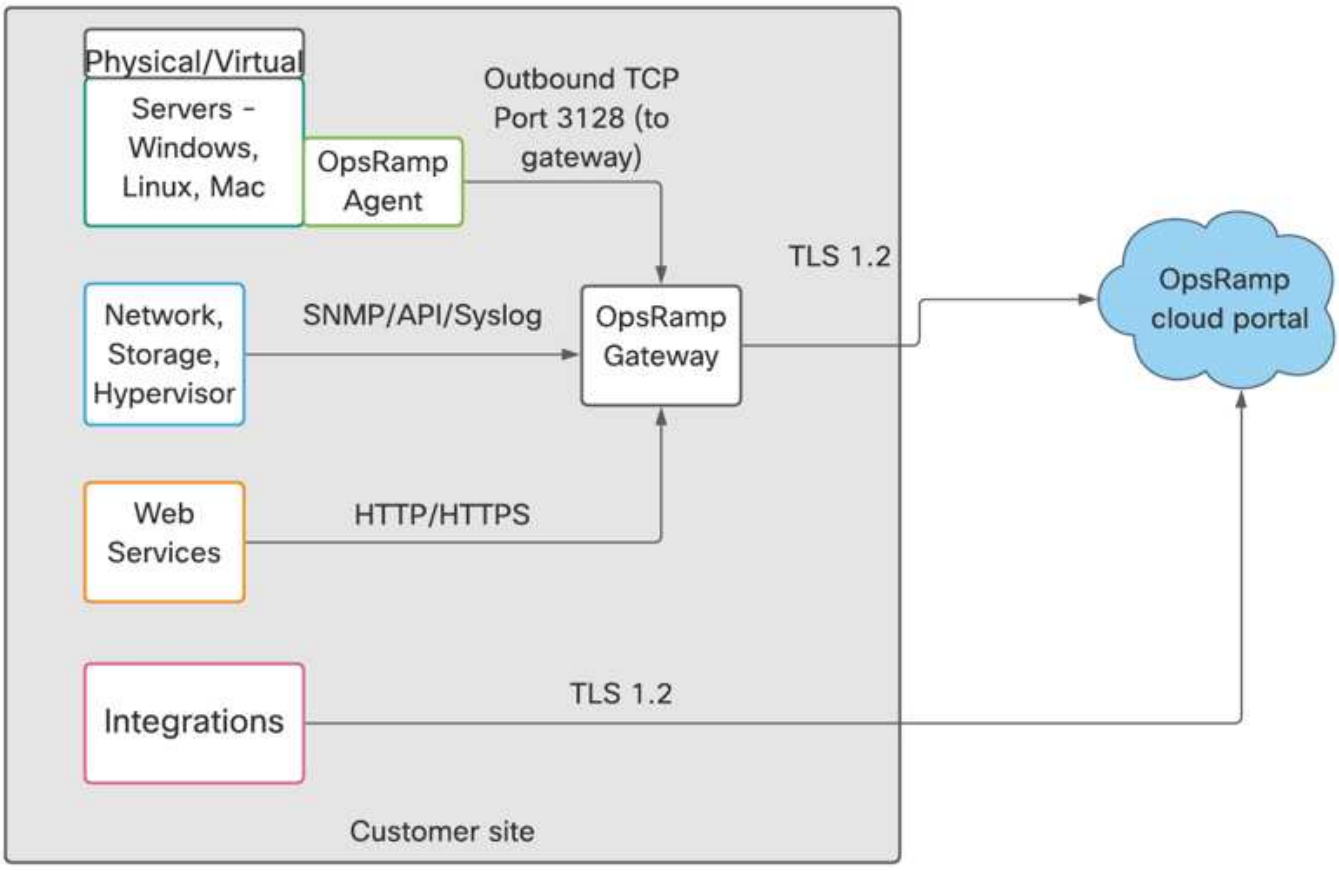
Network connectivity is required between the storage infrastructure installed at the customer data center or customer owned co-located services, and Keystone operations center. The customer is responsible for providing the compute and virtual machines, and the internet services. The network design should 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 OpsRamp and Zuora, use this connection to perform the 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.

OpsRamp as a monitoring application

OpsRamp is a SaaS-based application that Keystone uses to discover, monitor, and continuously manage assets. OpsRamp allows NetApp's monitoring team to remotely provide remote monitoring and management services to the customers deploying Keystone.

This tool has rich and powerful features for discovering assets such as applications, servers, networking devices, containers, and other resources typically used in an IT environment. This remote management service is easy to deploy at different locations, quickly gathers data, and is easily viewed on a centralized dashboard. To obtain more information about the OpsRamp program, please visit https://docs.opsramp.com/.



In the OpsRamp architecture, there are two distinct components of a centralized SaaS application as shown this image. At the monitoring site, there can either be the OpsRamp local gateway that collects the data from assets, or the OpsRamp agent in the resources that are to be monitored, or a combination of both the local gateway and agent.

OpsRamp cloud portal is a SaaS-based application that collects meta data from the agent or local gateway installed at the customer location, processes it, and displays it on its dashboard with observations. The Keystone monitoring team periodically monitors this dashboard for insights.

The OpsRamp centralized tool and OpsRamp local gateway work in tandem to monitor and manage assets. The centralized tool issues the commands and the local gateway acts upon them, collects the data, and sends it back to the centralized portal.

OpsRamp local gateway installed at the customer site provides several benefits, such as:

- Eliminating the need for installing the OpsRamp agent on all assets.
- The assets can point only to the local gateway, which can aggregate and send alerts to the centralized portal.
- Customers can restrict and monitor the incoming and outgoing traffic on the local gateway rather than allowing OpsRamp agent traffic deployed at different devices.

OpsRamp security

OpsRamp is compliant with standards like SOC 2 Type II and is hosted in Tier 1 data center providers that are compliant with ISO 27001 and SOC 1 Type I standards for security, availability, and confidentiality.

In addition, OpsRamp provides Keystone with following security features:

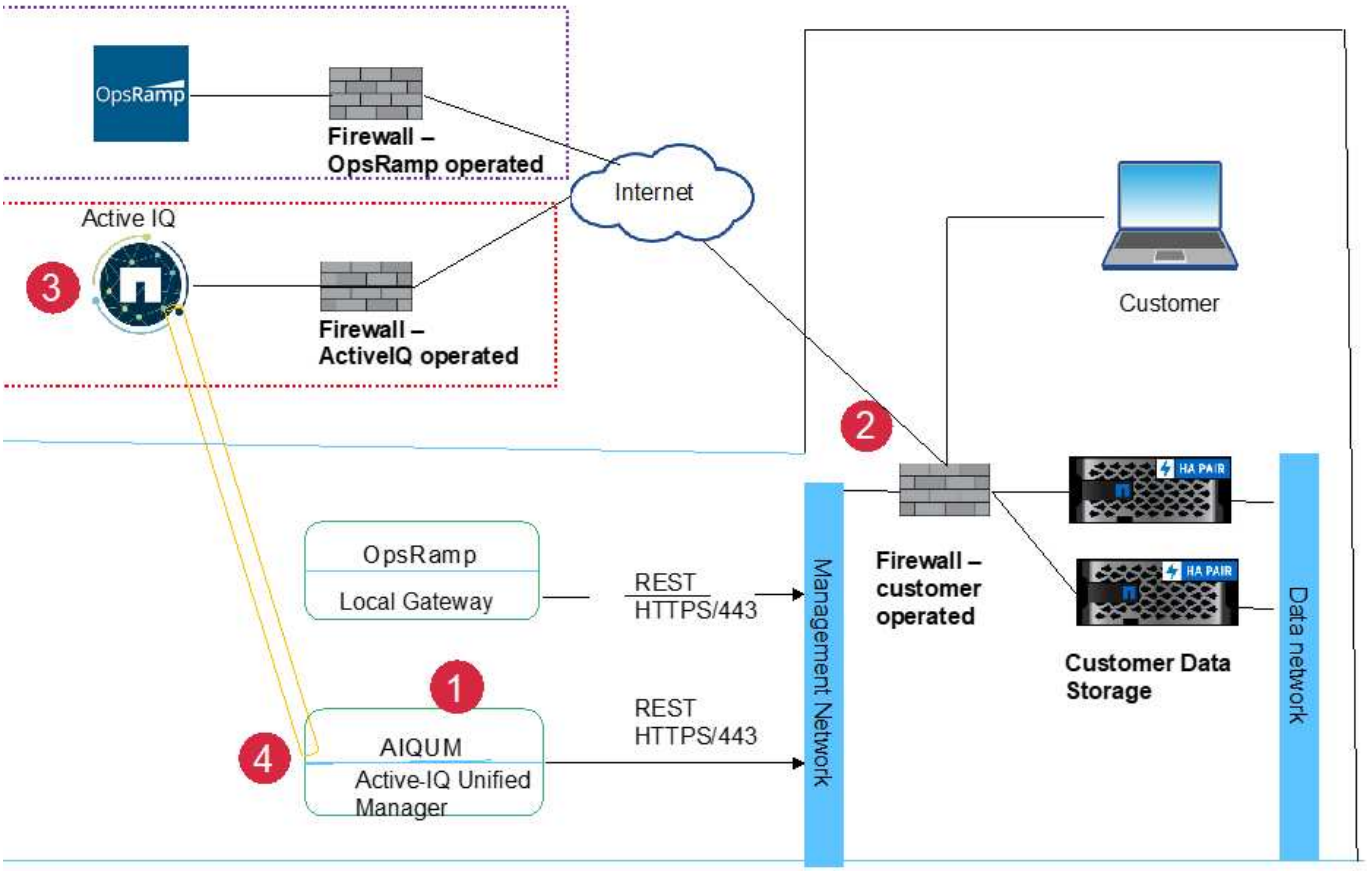
- OpsRamp maintains logs of user activity and Keystone can generate ad-hoc or scheduled reports on user-activity.
- All communication from OpsRamp gateway to OpsRamp cloud portal is TLS encrypted.
- Data-at-rest and Data-in-flight are encrypted using TLS.
- OpsRamp provides two-factor authentication options for Keystone.
- OpsRamp implements role-based access controls, enabling Keystone to create multiple roles and assign appropriate privileges to users.

Keystone data flow

Keystone STaaS systems encounter data flow through Keystone Collector traffic and monitoring data flows.

Keystone Collector data flow

Keystone Collector initiates REST API calls to the storage controllers and obtains usage details of the controllers periodically.



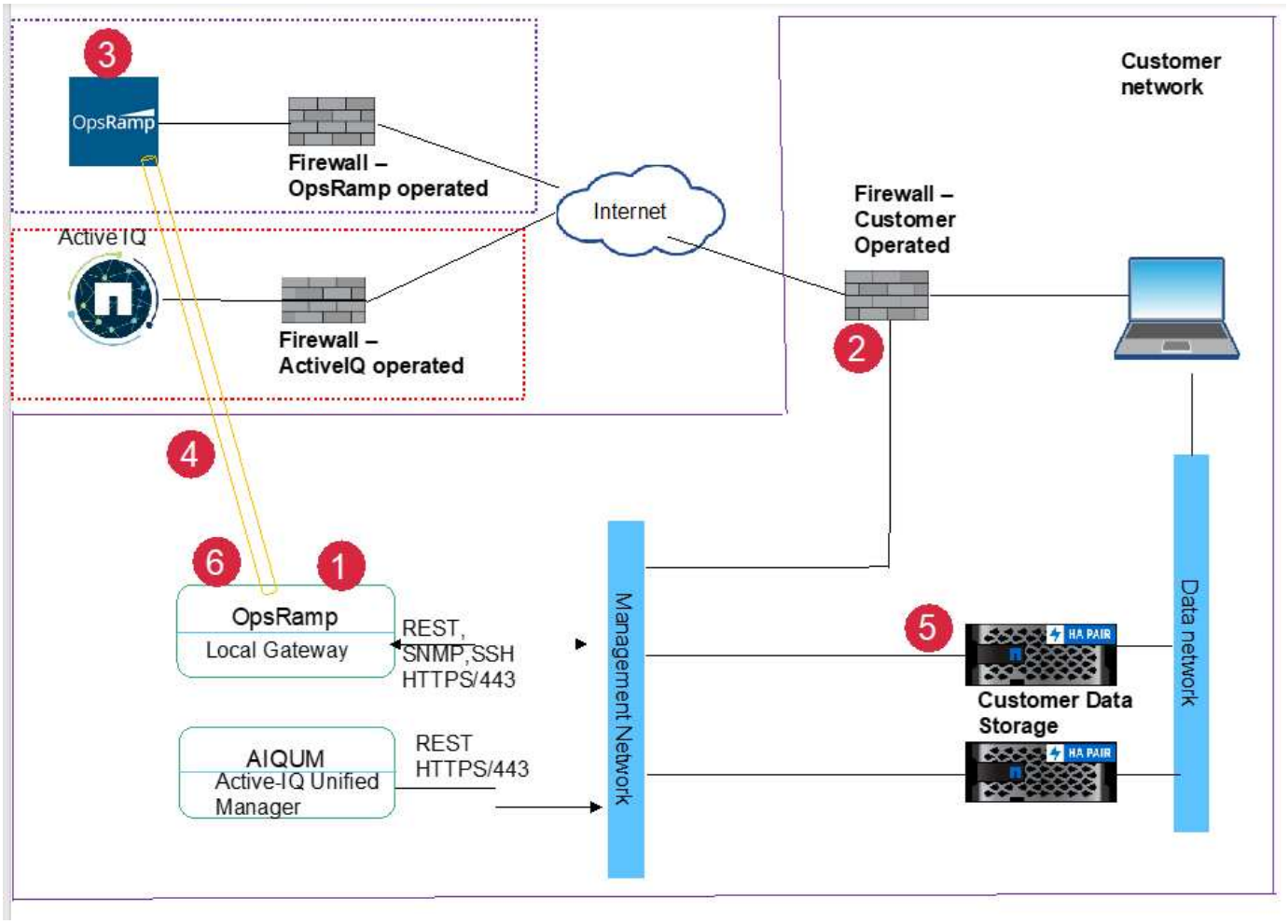
Legend

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



Legend

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

Copyright information

Trademark information