Site Requirements

NetApp Keystone

NetApp
January 15, 2021

Table of Contents

Site Requirements

Space

The customer is responsible for providing the floor space to host KFS equipment. NetApp will provide the weight specifications based on final configuration.

Racks

The customer is responsible for providing four post racks in the customer-operated offering. In the NetApp-operated offering, either NetApp or the customer can provide the racks, depending on requirements. NetApp provides 42 deep racks.

PDUs

The customer is responsible for providing 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

The customer is responsible for providing 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

The customer is responsible for providing the required cooling. NetApp will provide the cooling requirement specifications (Typical BTU, Max BTU), based on the final configuration.

Networking

Depending on customer requirements and the storage controllers used, KFS can provide 10 Gb, 40 Gb, and 100 Gb connectivity to the customer.

NetApp will provide the required transceivers for NetApp-provided Keystone devices only. The customer is responsible for suppling transceivers required for customer devices and cabling to the NetApp-provided Keystone devices.

Network Requirements

The following tables provide the KFS networking requirements.

IP Address Requirements (Customer-Operated)

Interface/Resource	Config. Spec	IPs	DNS Name	Description
Service processor	Each node in the cluster	10.0.0.1 - Node1 Service Processor 10.0.0.2 - Node2 Service Processor	TBD	A remote management device that enables you to access, monitor, and troubleshoot a node remotely.
Cluster management	Cluster level	10.0.0.3 - Cluster Admin Vserver	TBD	Admin storage virtual machine (SVM) to manage the entire cluster from a single console
Node management	Each node in the cluster	10.0.0.4 - Node1 Management 10.0.0.5 - Node2 Management	TBD	A dedicated IP address for managing a particular node
Cluster-interconnect	Two ports of each node in the cluster	Node1 e0a port Node1 e0b port Node2 e0a port Node2 e0b port	TBD	Private network or internal to the cluster; IPs will be auto-assigned when creating the LIF
SVM data	SVM level	10.0.1.5 - Data SVM110.0.1.6 - Data SVM2	TBD	A dedicated IP address for the client access to the data.
Inter cluster	Each node in the cluster	10.0.2.1 - Node1 10.0.2.2 - Node2	TBD	Optional - A network used to replicate data from one cluster to the other (SnapMirror)
Kubernetes Master Node 01-04	Static IP address	10.0.3.10-13	k8m01	Kubernetes Master Node VM
Kubernetes Worker node 01-04	Static IP address	10.0.3.14-17	k8m01	Kubernetes Worker Node VM
AIQ Unified Manager	Static IP address	10.0.3.18	aiqum01	Active IQ unified Manager
OpsRamp Gateway	Static IP address	10.0.3.19	opsgw01	OpsRamp Gateway

Customer Firewall Requirements (Customer- and NetApp-Operated)

The below table lists the customer firewall port and rules requirements.

Source	Destination	Name	Ports	Bi-Directional?	Category	Description
All VMs	Internet (as per URL whitelist table below)	HTTP, HTTPS	80, 443	No	NetApp Service Engine	Software package downloads and operating system updates
All VMs	8.8.8.8,1.1.1.1	DNS	UDP 53	No	NetApp Service Engine	Public or private DNS services
All VMs	au.pool.ntp.org	NTP	UDP 123	No	NetApp Service Engine	Time keeping
Kubernetes Worker Node(s)	NetApp ONTAP Cluster Management IP Address	HTTPS	443	No	NetApp Service Engine	Control/Management plane traffic to drive Ansible automation using ZAPI/REST
Kubernetes Worker Nodes	Active IQ Unified Manager	MySQL	3306	No	NetApp Service Engine	Active IQ Unified Manager MySQL database queries
Kubernetes Worker Nodes	Active Directory	LDAP	389	No	NetApp Service Engine	Active Directory authentication
OpsRamp Gateway	NetApp ONTAP Cluster Management IP Address	HTTPS, SSH, SNMP	443, 22, 161, 162	Yes	OpsRamp	Monitoring of the ONTAP controllers
NetApp ONTAP Controller Nodes	OpsRamp Gateway	HTTP, HTTPS, SNMP	80,443, 161, 162	Yes	OpsRamp	Monitoring of the ONTAP controllers
OpsRamp Gateway	Cluster Switches	SNMP	161,162	Yes	OpsRamp	Monitoring of the ONTAP cluster switches
Jump/Util Servers	NetApp ONTAP Controllers	HTTP, HTTPS, SSH	80, 443, 22	No	Operations	Management of ONTAP clusters

Source	Destination	Name	Ports	Bi-Directional?	Category	Description
Active IQ Unified Manager	NetApp ONTAP Controllers	HTTPS	443	No	NetApp Service Engine Operations	Management of ONTAP clusters

Allow List (Customer- and NetApp-Operated)

The below table lists provide the “Allow List” of URLs and IP addresses for outbound internet access, required for transfer of consumption data and updates.

Source	Destination URL/IP Addresses	Connectivity	Protocol	Port	Description
Kubernetes nodes	github.com	Outbound	HTTP, HTTPS	80,443	NetApp Service Engine platform configuration management
Kubernetes nodes	rest.zuora.com	Outbound	HTTP, HTTPS	80,443	NetApp cloud billing
Kubernetes nodes	auth.docker.io	Outbound	HTTP, HTTPS	80,443	Docker registry auth
Kubernetes nodes	registry-1.docker.io	Outbound	HTTP, HTTPS	80,443	Docker Hub images; general Docker images including NetApp Service Engine pods
Kubernetes nodes	production.cloudflare.docker.com	Outbound	HTTP, HTTPS	80,443	Docker Hub images; general Docker images including NetApp Service Engine pods
Kubernetes nodes	quay.io	Outbound	HTTP, HTTPS	80,443	Quay images - Prometheus Pods
Kubernetes nodes	cdn.quay.io	Outbound	HTTP, HTTPS	80,443	Quay images - Prometheus Pods
Kubernetes nodes	k8s.gcr.io	Outbound	HTTP, HTTPS	80,443	Google images - Kubernetes Cluster Pods
Kubernetes nodes	storage.googleapis.com	Outbound	HTTP, HTTPS	80,443	Google images - Kubernetes Cluster Pods

Source	Destination URL/IP Addresses	Connectivity	Protocol	Port	Description
Kubernetes nodes	kubernetes-charts.storage.googleapis.com	Outbound	HTTP, HTTPS	80,443	Helm repository
All CentOS VMs	rackspace.com	Outbound	HTTP, HTTPS	80,443	CentOS yum package mirror
OpsRamp Gateway	netapp.api.opsramp.com	Outbound	HTTPS	443	Cloud monitoring and NetApp Support tunnel connectivity
OpsRamp Gateway	140.239.76.0/24 206.80.7.128/26 63.251.89.0/24 199.250.248.0/24 74.217.75.0/24	Outbound	HTTPS	443	Cloud monitoring and NetApp Support tunnel connectivity

Service Account (Customer-Operated)

After the initial Active IQ Unified Manager discovery is complete (~15 minutes), a read-only service account must be created for Active IQ Unified Manager, OpsRamp, and NetApp Service Engine at Admin SVM on the NetApp Clusters, named “keystone,” with the applications enabled.

Application	Permission	Authentication	Category	Description
HTTP	Read-only	Password	OpsRamp	API monitoring from OpsRamp
ONTAP	Read-only	Password	OpsRamp	API monitoring from OpsRamp
SNMP	Read-only	Password	OpsRamp	SNMP monitoring from OpsRamp

VMs (Customer-Operated)

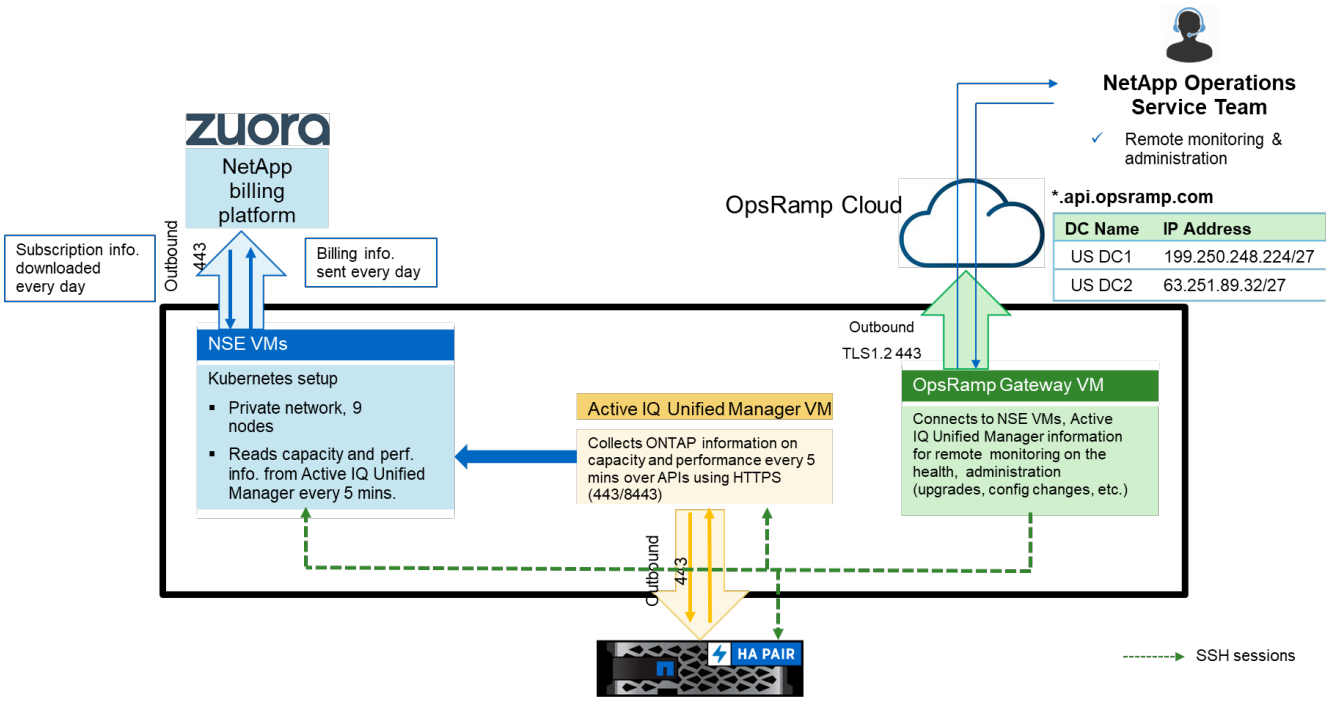
In the customer-operated version, the customer is responsible for providing the VMs required for the consumption and health monitoring software.

Name	Function	OS/Version	vCPU	Memory (GB)	Storage
Kubernetes Master Node 01	Kubernetes Master Node (Stacked ETCD) VM	VMWare OVA	4	16	40GB

Name	Function	OS/Version	vCPU	Memory (GB)	Storage
Kubernetes Worker Node 01	Kubernetes Worker Node VM	VMware OVA	4	16	40 GB
Active IQ Unified Manager	Active IQ Unified Manager	9.7 (VMware OVA)	4	12	60 GB
OpsRamp Gateway	OpsRamp Gateway	OVA	4	16	40 GB

Remote Access

Keystone connects to external cloud services for billing and remote operations. As discussed in the earlier sections, all the connections are established outbound (from inside the data center to the cloud services) and over a secured connection. The below figure is an overview of the connectivity and the traffic flow between the various deployed components.



NetApp Global Services and Support Center (GSSC) will have the capability to remotely log in and perform any maintenance process or collect any logs for triaging. This is achieved by using OpsRamp Cloud services.

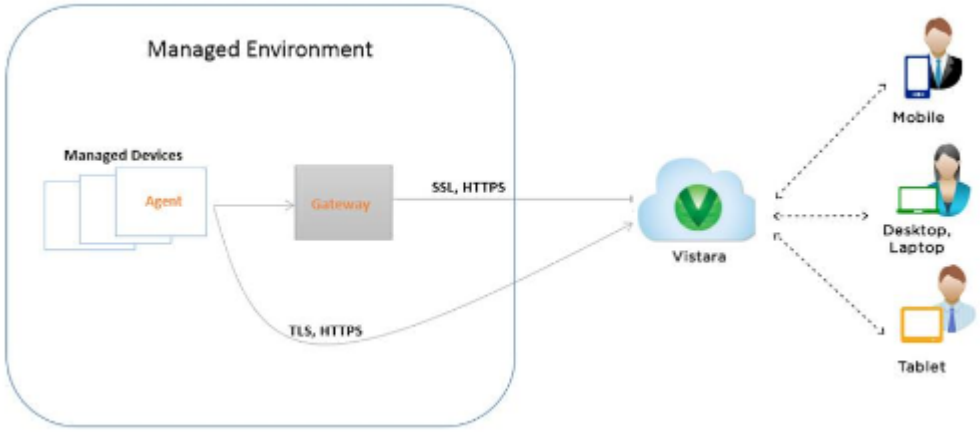
OpsRamp Architecture

OpsRamp is a cloud-based service, which also has a gateway software deployed at the customer site. All the Keystone devices are registered to OpsRamp gateway and the gateway connects to the OpsRamp Cloud services through an outbound internet connectivity over a secured connection.

Keystone infrastructure is configured through the OpsRamp web portal for remote access to the controller's service processor or switch service port through SSH. OpsRamp gateway also collects the following information from the registered devices (the stats can be viewed on the web portal by NetApp GSSC):

- Performance statistics, CPU, memory utilization, operating system events, and hardware events
- Events and SNMP traps
- System level information: make/model, DNS names, operating system configuration, and so on

OpsRamp gateway is a virtual appliance that runs on VMWare vSphere with a hardened configuration of CentOS operating system.



OpsRamp Security

OpsRamp security includes the following measures:

- OpsRamp instance runs on Keystone service management network.
- Single-sign-on (SSO) logins to OpsRamp platform are tightly secured with multifactor authentication and NetApp corporate login practices.
- All logins and actions on OpsRamp platform are tracked to individual employees using SSO for auditing purposes and compliance.
- Remote console sessions are automatically recorded and stored for a period of up to 180 days.
- Role-based accounts for NetApp employees ensure that only authorized employees can access customer-managed environments and only in the capacity that is needed to perform the assigned functions.
- All sensitive data is encrypted in OpsRamp. Data such as inventory, alerts, and tickets are logically partitioned and only available to authorized NetApp users based on their role in the project.
- Communications between the customer environment, OpsRamp and NetApp are encrypted with 256-bit encryption.
- All sensitive data in stored in encrypted format in non-web facing database, providing further levels of security and isolation.
- OpsRamp development organization is ISO 27001 certified and is periodically being audited for security compliance.
- All metadata collected from the customers IT infrastructure is stored in secured data centers in the continental Unites States.
- OpsRamp creates an outbound tunnel through HTTPS/443 – no inbound access required. NetApp accesses environment through this tunnel.
- Communications between the customer environment, OpsRamp, and NetApp are encrypted with 256-bit encryption.

- All sensitive data in stored in encrypted format in non-web facing database, providing further levels of security and isolation.
- A dedicated Keystone Operations team exists to remotely monitor, and optionally manage Keystone deployments
- OpsRamp development organization is ISO 27001 certified and is periodically being audited for security compliance.
- All metadata collected from the customers IT infrastructure is stored in secured datacenters in the continental Unites States.
- OpsRamp creates an outbound tunnel via HTTPS/443 – no inbound access required.
- OpsRamp is SOC-2 Type 2 validated by NetApp
- NetApp internal security team scans for vulnerabilities every six months

Security

Protecting a customer's environment from unauthorized access and actions is of paramount importance. Since Keystone is an on-premises solution that is remotely monitored, and optionally managed, Keystone security architecture provides the following elements to ensure the Keystone storage environment and the customer's environment are protected:

- Device hardening:
  - All devices (switches, firewalls, servers, K8, CentOS, ONTAP) are hardened per NetApp best practices, including per NetApp Technical Report TR-4569.
  - All unused switch ports are disabled.
  - All device management ports are user/password protected.
- Password management:
  - NetApp stores and manages passwords used by Keystone Operations personnel in a secure and encrypted password management system.
  - Only select operations personnel have read/write access to password management system.
  - All activities on password management system are logged and monitored.
  - Passwords used to remotely monitor and manage systems cannot be viewed by operations personnel.
  - Unique passwords are used for each physical or logical entity/device (including cluster admin).
- Management network:
  - Consists of firewalls, management switches, management compute servers, management storage, and console switches.
  - All management network traffic is through HTTPS.
  - All internet connections are established outbound from the management network only.
  - This network is separate from the data network.
  - No Keystone service device within the Keystone management network can get beyond the firewall to the customer management network.
  - Only SSH and HTTPS (no HTTP) can be used on the management network.
- Keystone firewalls:

    - Keystone firewalls reside on the Keystone management network.
    - Provide northbound connection to the internet proxy server and the customer management network.
    - Provide southbound management switches.
    - Allow segregation/isolation of KS management network from customer's management network.
    - Disallow customer access and activities to/on the Keystone management network.
    - Establish outbound tunnel through the customer's HTTPS proxy to internet (no inbound connections).
    - The only inbound connection to the management network is through HTTPS port 443 for the Keystone GUI and API access to the GUI/API interface host.
- Data network:
    - Consists of data switches and storage controllers
    - Northbound to customer data switches
    - Southbound to storage controllers
    - Separate from the control plane
    - Only VLANs associated with SVMs can access the customer's data network
    - Storage controller ports only respond to iSCSI, CIFS, or NFS protocols only
    - IP address associated with SVMs on storage controllers use IPSpaces:
        - SVMs are associated with the VLANs
    - SVMs have secure virtual routing table
        - SVMs do not route any customer traffic from customers data network
        - No inter- SVM traffic or routing path possible
        - No connectivity between management network or ports to SVMs or their associated VLANs.
        - No SSH sessions to storage controller data ports possible
- APIs:
    - NetApp ONTAP 9 has two types of API access:
        - ZAPI, legacy SOAP/XML based API interface is used by Active IQ Unified Manager and by OpsRamp.
        - The newer REST API is used by NetApp Service Engine components for accessing controller metrics and configuration.
    - Neither API can access stored data, but both can manipulate the systems if given the permissions required to do so.
    - Certain hosts in NetApp management network have API access (REST/ZAPI) to e0M ports on storage controllers over HTTPS/443.
    - After the initial Active IQ Unified Manager discovery is complete (~15 minutes), NetApp requests that Active IQ Unified Manager, OpsRamp, and NetApp Service Engine are provided with services accounts with read-only permissions.
- Role-based access control (RBAC):
    - RBAC can be used to provide fine-grained (per-API call) and coarse (for example, to make particular users completely read-only) access control.
    - Service accounts on controllers have RBAC restrictions to enforce read-only access through API.
- Active IQ Unified Manager:

- Active IQ Unified Manager requires full administrator credentials for the initial discovery (~15 min) of the ONTAP controllers through NetApp Manageability SDK.
- After initial Active IQ Unified Manager discovery is complete (~15 minutes), NetApp requests that Active IQ Unified Manager, OpsRamp and NetApp Service Engine are provided with services accounts with read-only permissions.

Security Requirements

The security requirements include:

- Provide an allow list for firewalls.
- The access control list (ACL) for API's RBAC and Active IQ Unified Manager.

Source	Destination URL/IP Addresses	Connectivity	Protocol	Port	Description
Kubernetes nodes	github.com	Outbound	HTTP, HTTPS	80,443	NetApp Service Engine platform configuration management
Kubernetes nodes	rest.zuora.com	Outbound	HTTP, HTTPS	80,443	NetApp cloud billing
Kubernetes nodes	auth.docker.io	Outbound	HTTP, HTTPS	80,443	Docker registry auth
Kubernetes nodes	registry-1.docker.io	Outbound	HTTP, HTTPS	80,443	Docker Hub images; general Docker images including NetApp Service Engine pods
Kubernetes nodes	production.cloudflare.docker.com	Outbound	HTTP, HTTPS	80,443	Docker Hub images; general Docker images including NetApp Service Engine pods
Kubernetes nodes	quay.io	Outbound	HTTP, HTTPS	80,443	Quay images - Prometheus Pods
Kubernetes nodes	cdn.quay.io	Outbound	HTTP, HTTPS	80,443	Quay images - Prometheus Pods
Kubernetes nodes	k8s.gcr.io	Outbound	HTTP, HTTPS	80,443	Google images - Kubernetes Cluster Pods

Source	Destination URL/IP Addresses	Connectivity	Protocol	Port	Description
Kubernetes nodes	storage.googleapis.com	Outbound	HTTP, HTTPS	80,443	Google images - Kubernetes Cluster Pods
Kubernetes nodes	kubernetes-charts.storage.googleapis.com	Outbound	HTTP, HTTPS	80,443	Helm repository
All CentOS VMs	rackspace.com	Outbound	HTTP, HTTPS	80,443	CentOS yum package mirror
OpsRamp Gateway	netapp.api.opsramp.com	Outbound	HTTPS	443	Cloud monitoring and NetApp Support tunnel connectivity
OpsRamp Gateway	140.239.76.0/24 206.80.7.128/26 63.251.89.0/24 199.250.248.0/24 74.217.75.0/24	Outbound	HTTPS	443	Cloud monitoring and NetApp Support tunnel connectivity