Dell ObjectScale Appliance Overview and Architecture

October 2023

H19789

White Paper

Abstract

This document provides a technical overview of the Dell ObjectScale appliance.

DELL Technologies

Copyright

Contents

Executive summary

Introduction

Organizations require options for consuming public cloud services with the reliability and control of a private-cloud infrastructure. Dell ObjectScale appliance is a software-defined, Kubernetes-native, object storage platform that delivers S3 services. The ObjectScale appliance, which is an All Flash, high-performance turnkey system built on the latest generation of Dell PowerEdge.

ObjectScale appliance is uniquely positioned to enable generative AI models to tap into vast amounts of real and near-time data, supporting use cases including customer operations, content creation, management, and software development.

Audience

This document is intended for anyone interested in understanding the value and architecture of ObjectScale appliance. It aims to provide context with links to additional information.

Scope

This document focuses primarily on ObjectScale appliance architecture. It does not cover installation, administration, and upgrade procedures for ObjectScale software or hardware. It also does not cover specifics on using and creating applications with ObjectScale APIs.

Updates to this document typically coincide with major releases or new features.

Revisions

Date	Part number/ revision	Description
October 2023	H19789	Initial release

We value your feedback

Dell Technologies and the authors of this document welcome your feedback on this document. Contact the Dell Technologies team by email.

Author: Jarvis Zhu

Note: For more information about ObjectScale, see ObjectScale and ECS.

Value of ObjectScale appliance

ObjectScale provides significant value for enterprises and service providers seeking a platform built to support rapid data growth. The main advantages and features of ObjectScale appliance that enable enterprises to globally manage and store distributed content at scale include:

Power modern apps:

- Go cloud-native faster with the best of microservices and Kubernetes orchestration backed with S3 compatibility
- Accelerate development cycles with powerful 16G server performance and full-stack NVMe connectivity

Run demanding workloads at scale:

- Simplify with a modern turnkey hardware and software platform – integrated, deployed and supported as one by Dell Technologies
- Scale for growth
- Choose from flexible deployment options available with Capex and Opex: ObjectScale appliance, ObjectScale software bundle, or as an ObjectScale application

Consolidated data lake

- Serve as a centralized data lake storing sensor telemetry, machine-generated logs, and application data. Federate multiple sites to eliminate data silos and provide anywhere access to data from edge to core. Objects are tagged to enhance analysis and make data more discoverable.

Analytics and machine learning

- Run rapid queries on a performant ObjectScale data lake to generate operational insights at the speed the business demands. With the ability to deploy analytics on NVMe-based, all-flash drives, storage performance is no longer a bottleneck. S3a enables Hadoop workloads to directly read and write data to ObjectScale, replacing the need for complex HDFS cluster management.

Architecture

Introduction

Dell ObjectScale XF960 is high-performance, all-flash storage powered by ObjectScale software and the first of the ObjectScale appliance family.

Architecture overview

ObjectScale appliance is deployed on a set of qualified industry standard hardware or as a turnkey storage appliance. The main components of ObjectScale appliance are the:

- **Object stores** - Object stores are discrete storage systems with an individualized life cycle. They are Kubernetes applications deployed by ObjectScale. Object stores provide data services as unique and independent storage systems that are deployed and managed by ObjectScale. They are created, updated, and deleted independently from all other object stores managed by ObjectScale.

  Buckets are object containers that are used to control access to objects. A bucket is associated with ObjectScale instances, the object store and account, or tenant. In ObjectScale, buckets are limited to S3 only.

- **ObjectScale instance** - ObjectScale is a software bundle that provides management of shared services for deploying and consuming Dell object storage within a Kubernetes cluster. Administrators can deploy a single ObjectScale, which is referred to as an ObjectScale instance (OSI), per Kubernetes cluster.

  In ObjectScale, Kubernetes provides the connective glue between physical infrastructure, such as disk and network, and the application services running in containers. ObjectScale uses Kubernetes' efficient resource-management capabilities and relies on Kubernetes to manage operating-system and hardware interaction.

  - **Bare metal CSI** - ObjectScale uses Kubernetes custom resources including the Dell bare-metal container storage interface (CSI) to access the physical components.
  - **Dell supported Kubernetes platform** - Dell created a common RKE2 Kubernetes and management platform also known as Common Management Operations or Atlantic.

- **Infrastructure** – A customized Operation System based on the SUSE Linux Enterprise Server 15 SP4 in the turnkey appliance for industry standard hardware configuration.
- **Hardware** - A turnkey appliance or qualified industry standard hardware.

Note: The current ObjectScale appliance uses the ObjectScale 1.3 software package which supports only one object store in ObjectScale instance.

The following figure shows a graphical view of these layers which are described in detail in the sections that follow.

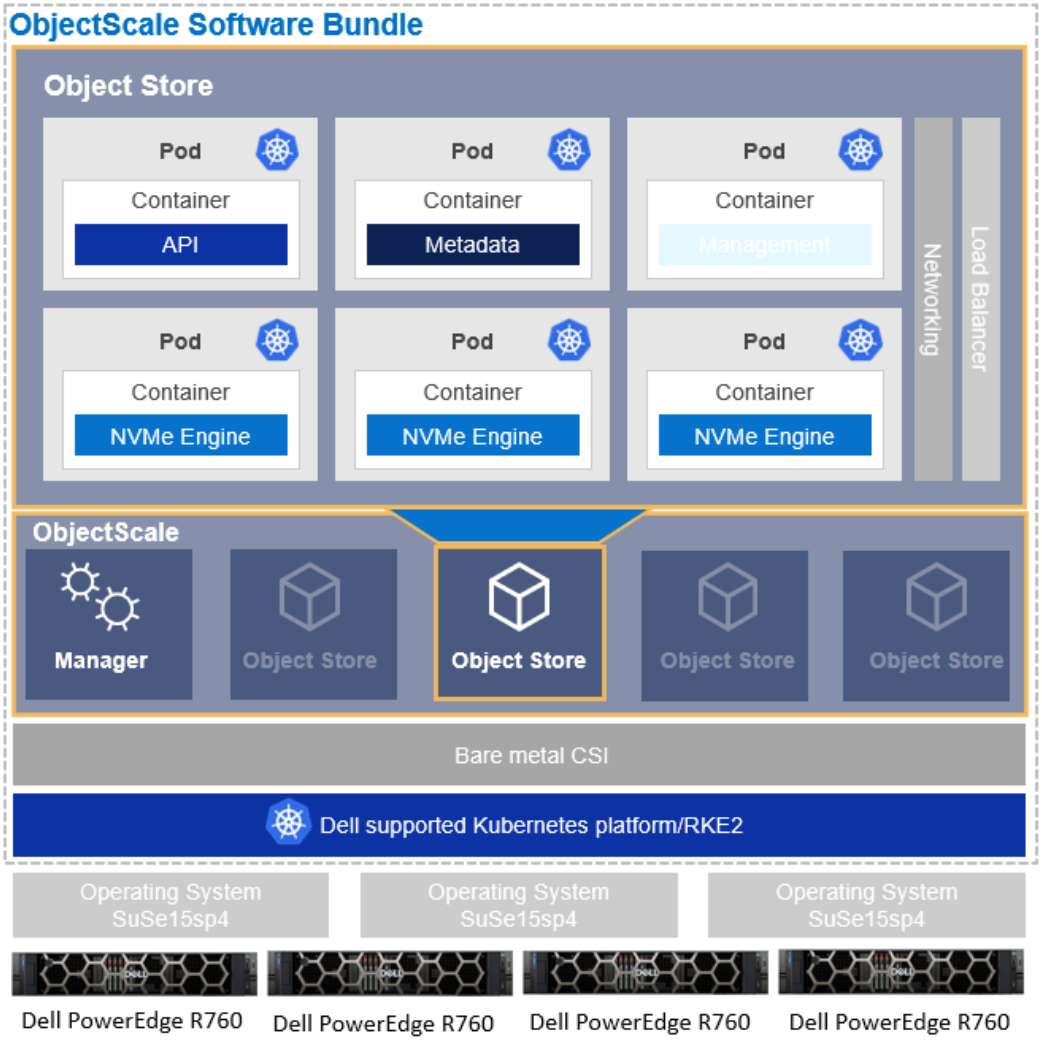


Figure 1. ObjectScale appliance architecture layers

Note: See *Dell ObjectScale overview and architecture* for more information about ObjectScale architecture.

ObjectScale portal and provisioning services

Storage administrators manage ObjectScale appliances using the ObjectScale portal and provisioning services. ObjectScale provides a web-based GUI (WebUI) to manage, license, and provision.

The ObjectScale dashboard provides overall system-level health and performance information. This unified view enhances overall system visibility. Alerts and logs in the dashboard notify users about different events, such as capacity limits, quota limits, disk and/or node failures, and software failures.

Note: Hardware alerts are enabled by default in the appliance model. Users can enable or disable hardware alerts in the UI.

The following figure shows the ObjectScale dashboard:

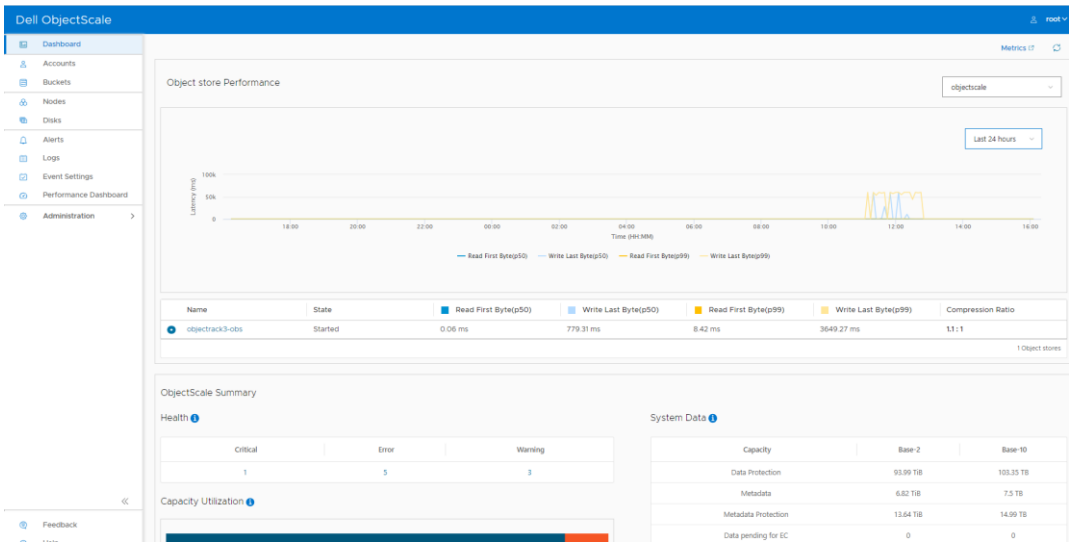


Figure 2. ObjectScale Web UI dashboard

Detailed performance reporting is displayed in a Grafana dashboard. You can access ObjectScale overview reports by clicking **Metrics** on the dashboard. ObjectScale also provides metrics details for each individual object store by clicking the **Metrics** link for each object store. The following figure shows an example of an object store performance report:

Figure 3. Advanced monitoring visualization using Grafana

See the *Dell ObjectScale 1.3.x Administration Guide* for more information of viewing metrics using Grafana.

ObjectScale can also be managed using RESTful APIs. The management API allows users to administer ObjectScale with their own tools, scripts, and new or existing applications. For more information, see the *Dell ObjectScale 1.3.x Rest API Reference*.

Storage topology

Administrators can install only one ObjectScale instance per Kubernetes cluster. The Kubernetes cluster consists of nodes. An ObjectScale instance can have only one object store at **a time.** The object stores reside on physical nodes within the Kubernetes cluster.

ObjectScale appliance **is** deployed with the ObjectScale software bundle package by default.

In a Kubernetes cluster, a node is a physical worker node. In ObjectScale, a node is referred to as a Storage Server (SS). An SS provides disk access in an object store. At most, one SS instance from each object store is scheduled on a Kubernetes node.

SS instances are used to store user object data, which includes any associated user object metadata, and system object metadata, such as where an object is stored on disk.

The following figure depicts the Kubernetes and object store topology trees from the preceding example. Each object store is aware of its own topology only.

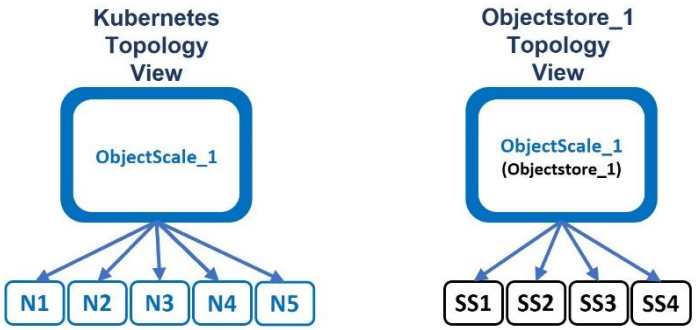


Figure 4. Topology trees for Kubernetes and Objectstore

The following figure shows the relationship between disks and SS instances for this example. The Objectstore_1 instance independently accesses dedicated volumes and disks for data storage on Kubernetes nodes.

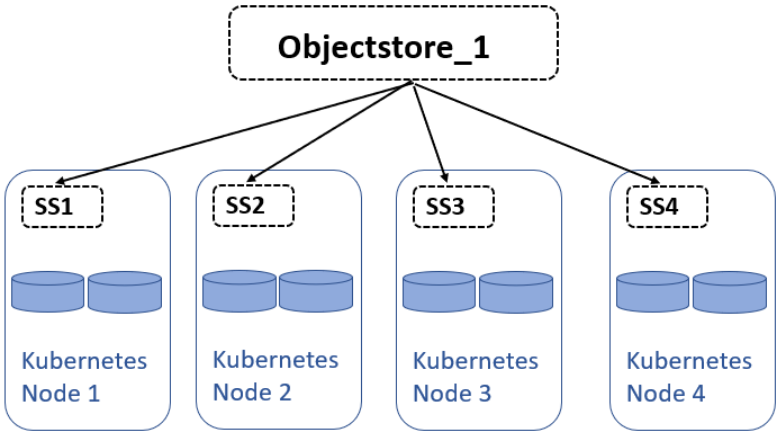


Figure 5. SS instances independently access dedicated volumes and disks

The figure shows each SS instance connected to a single disk for simplicity. The key point to understand is that each SS instance in an object store is tied to a single Kubernetes node. SS instances are assigned to be scheduled on a Kubernetes node. During node failure, the SS instance and underlying persistent storage are lost. The data segments in the persistent volumes that are lost are re-created across other nodes. This functionality contrasts with a common Kubernetes behavior where instances that are lost during node

failure are created elsewhere. The ephemeral SS instances are associated with the persistent storage to which they attach in ObjectScale.

S3 Data services

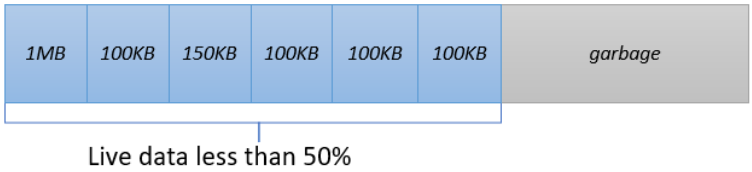
Data services, which are also referred to as head services, are responsible for taking client requests, extracting the required information, and passing it to the storage engine for further processing. ObjectScale supports the S3 protocol only, and uses port 80 and 443 for S3 communication, and port 4443 and 12002 for internal service communication.

Client applications including S3 Browser and Cyberduck provide a way to quickly test, or access data stored in ObjectScale.

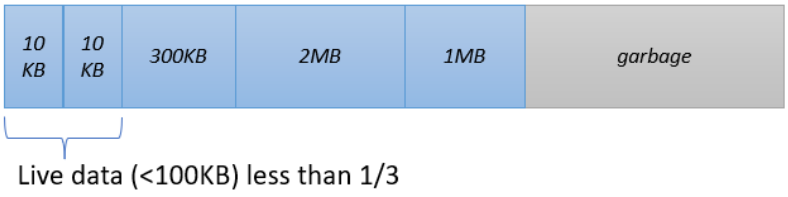
Space reclamation

Writing chunks in an append-only manner means that data is added or updated by keeping the original written data in place, and creating net new chunk segments. These segments may or may not be included in the chunk container of the original object. The benefit of append-only data modification is an active/active data access model which is not hindered by file-locking issues of traditional filesystems. As objects are updated or deleted, data in chunks is no longer referenced or needed. Two Garbage Collection (GC) methods are used by ObjectScale to reclaim space from discarded full chunks, or chunks containing a mixture of deleted and non-deleted object fragments which are no longer referenced:

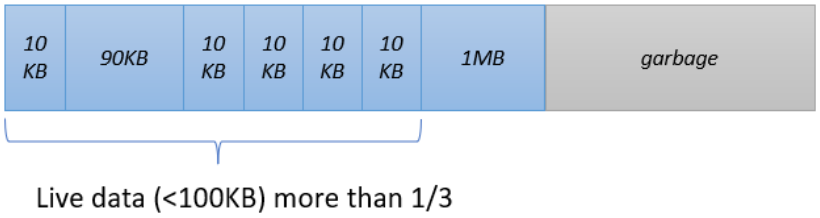
- **Normal Garbage Collection** - When an entire chunk is considered garbage, reclaim the space.
- **Partial Garbage Collection by Merge** – When a chunk meets the garbage threshold, reclaim space by merging valid chunk segments with other partial chunks to create a new chunk.
  - When objects within a chuck are >=100KB, the threshold of partial GC is 50% of the chunk.



  - When the total space of live (<100KB) objects is less than one third of the chunk, the threshold of partial GC is 50% of the chunk.



  - When the total space of live (<100KB) object is more than one third of the chunk, the threshold of partial GC is two thirds of the chunk.



ObjectScale appliance hardware models

Introduction

Flexible entry points enable ObjectScale appliance to rapidly scale to petabytes and exabytes of data. With minimal business impact, an ObjectScale appliance solution can scale linearly in both capacity and performance by adding nodes and disks.

XF960 is an all-flash object storage solution of hyper-converged nodes for low latency and high IOPs ObjectScale appliance deployments. It has options for 32 cores dual CPUs, 256GB memory, 24 drives, 30TB NVMe drive per node, and up to 5GB/sec reads and 4GB/sec writes per node for large objects (>200MB). This platform starts at 2.9PB RAW minimum configuration and scales to 11.7PB RAW per rack.

Note: ObjectScale appliance supports a minimum deployment of 4 nodes and a maximum of 16 nodes in a single rack cluster. Only a single rack cluster is supported in the ObjectScale 1.3 release.

The XF960 is a hardware stack which includes the server, switch, rack mount equipment and appropriate power cables, and is optimized to run the ObjectScale software.

ObjectScale appliance offers self-encrypting drives (SEDs), hard drives that transparently encrypt all on-disk data using an internal key and a drive access password. Protection is achieved by requiring a key to unlock the drives before any data can be retrieved. This encryption protects the system from data theft when a drive is removed. If a SED drive's internal key or drive access password is lost, the drive data becomes permanently inaccessible, and the drive must be reset and reformatted to be repurposed. SEDs include boot drives and data drives.

The ObjectScale appliance starting capacity options allow users to begin an ObjectScale deployment with only the capacity needed, and to easily grow as needs change in the future. See the *Dell ObjectScale XF960 Hardware Guide* for more information.

ObjectScale appliance networking

ObjectScale appliances use the Dell S5448F for the pair of back-end switches. Customers must supply the two front-end switches for the client accessible.

Back-end switches

Dell provides two 100 GbE S5448F back-end switches with two 400GbE VLT cables. These switches are referred to as the Fox (BE1) and Hound (BE2) switches. All iDRAC cables from nodes and all front-end switch management cable connections route to the

Fox switch. The following figure provides a visual representation of how ports are intended to be used to enable ObjectScale appliance management traffic and diagnostic ports. These port allocations are standard across all implementations.

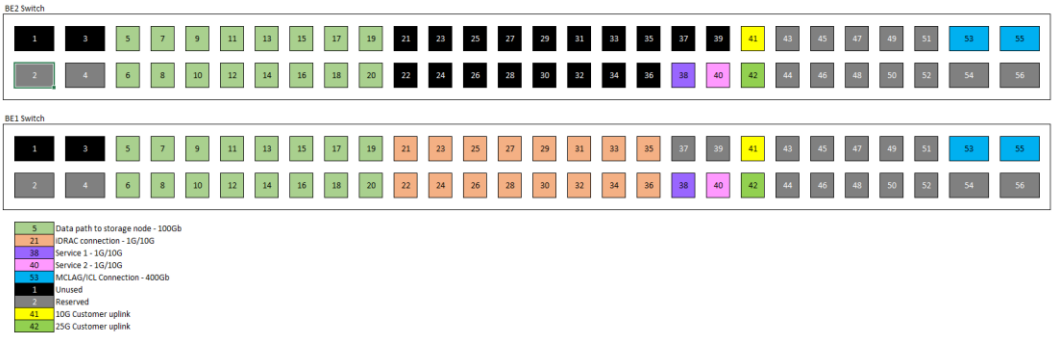


Figure 6. Back-end network switch port designation and usage

As a best practice, the two back-end switches should be configured in an aggregation by VLT and the network cards in the nodes should be configured as a bonded interface.

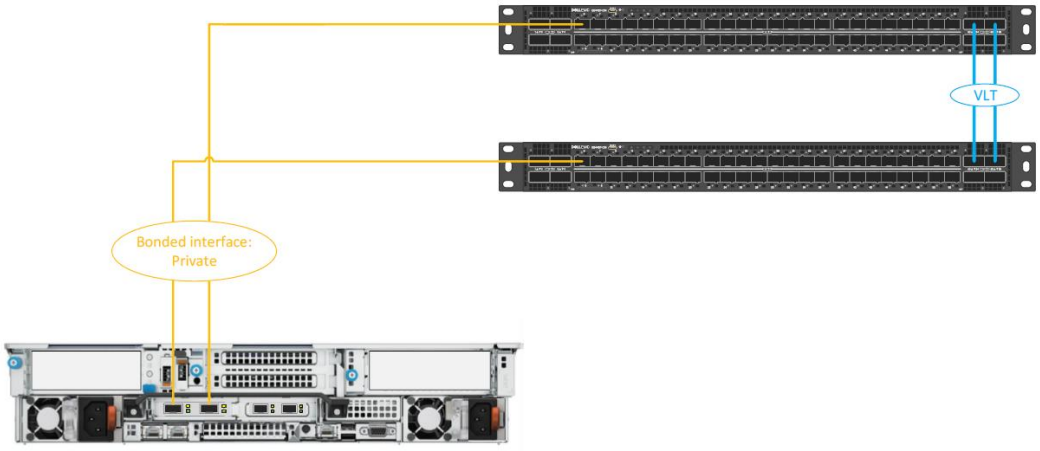


Figure 7. Back-end switch network architecture

Front-end switches

Customers must use their own front-end switches to connect to the ObjectScale appliance. Below are the recommendations:

- Use 25 GbE switches for optimal performance.
- For redundancy and to maintain a certain level of performance, have:
  - Two physical switches configured in a multi-chassis aggregation (VLT, vPC, MLAG)
  - Two uplinks per switch to customer switch, or four uplinks per rack minimum.
- Use dedicated switches for ObjectScale appliance. Do not use shared ports on the customer core network.
- LACP bond between storage nodes and the front-end switches.

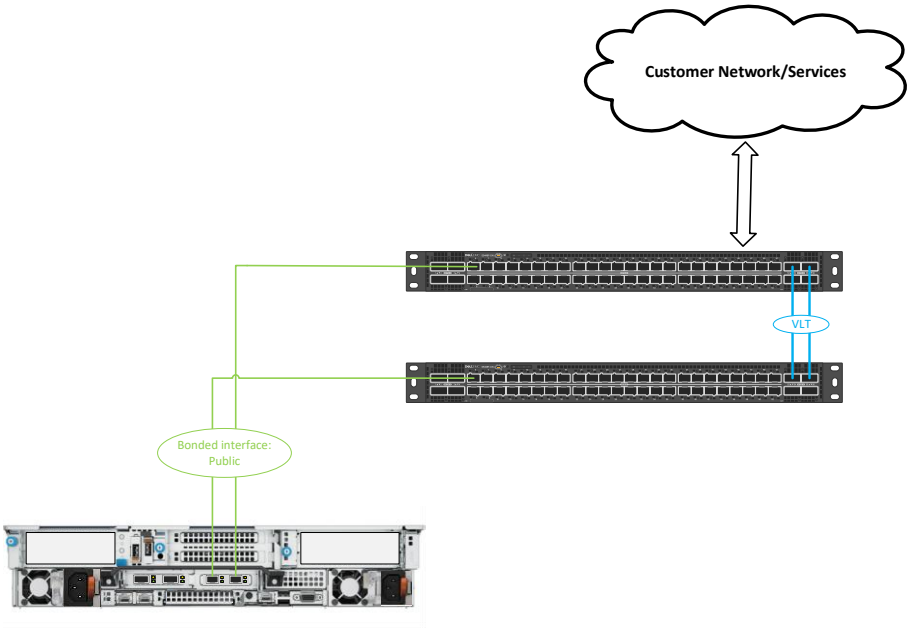


Figure 8. Front-end switch network architecture

Load balancer

A load balancer is a device that acts as a reverse proxy and distributes network or application traffic across a number of nodes. Load balancers are used to increase capacity (concurrent users) and reliability of applications. They improve the overall performance of applications by decreasing the burden on servers associated with managing and maintaining application and network sessions, as well as by performing application-specific tasks.

MetalLB, the load-balancer implementation for a bare-metal Kubernetes cluster, offers a network load-balancer solution that integrates with standard network equipment in ObjectScale. ObjectScale appliance leverages layer 3 (BGP) mode by default for networking. All machines in the cluster establish BGP peering sessions with nearby routers that customers control, and instruct routers on how to forward traffic to the service IPs. Using BGP allows for true load balancing across multiple nodes and fine-grained traffic control, using BGP policy mechanisms. After packets arrive at the node, kube-proxy is responsible for the final traffic routing hop to move the packets to one specific pod in the service.

The exact behavior of the load balancing depends on the specific router model and configuration, but the common behavior is to balance per connection, based on TCP/UDP 5-tuple (source IP address, source port, destination IP address, destination port, transport protocol). Per-connection balancing means that all the packets for a single TCP or UDP session are directed to a single machine in the cluster. Traffic spreads only between different connections, and not for packets within one connection.

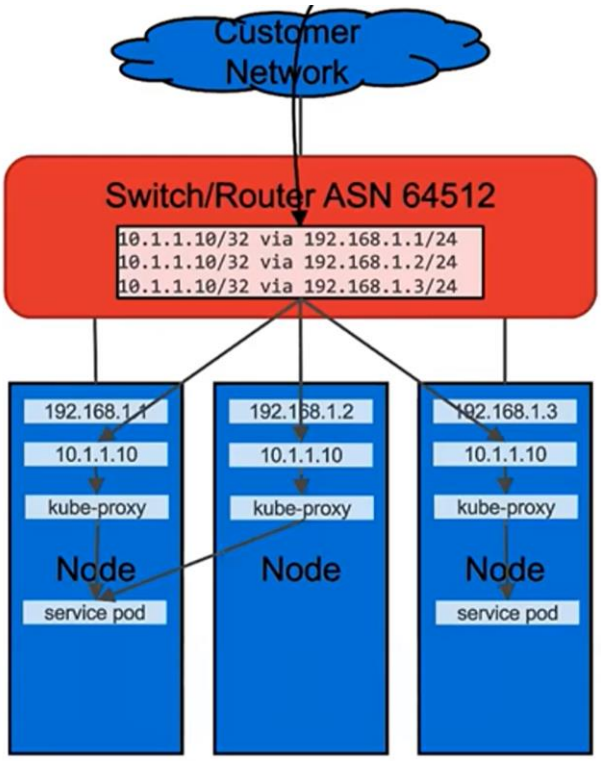


Figure 9. MetalLB Layer 3 (BGP) mode

Here is an example of the BGP configuration in front-end switches:

```
router bgp 64512
maximum-paths ibgp 128
router-id 192.168.10.250
!
Address-family ipv4 unicast
redistribute connected
redistribute static
!
neighbor 192.168.10.104
remote-as 64520
no shutdown
!
neighbor 192.168.10.105
remote-as 64520
no shutdown
!
```

For more information about the networking and cabling, see the *Dell ObjectScale XF960 Hardware Guide*.

Security

Introduction

ObjectScale appliance inherits all the security strengths offered in a Kubernetes environment. In addition, it implements the following security options, as recommended by Kubernetes.

- Hardening the Kubernetes deployment by allowing access only through published endpoints
- Enumerating and securing every resource, whether it is a system or custom resource, and with role-based access control (RBAC)
- Logging from each system component, including event generation and their collection through daemon sets
- Using Linux capabilities as permission sets for code to run in the containers so there is no undetected or uncontrolled access to the host
- Securing all external and internal connectivity using proxies and TLS for external-facing connections
- Using service accounts specific to applications so there is a containment and isolation of privilege with which applications run
- Securing permissions on individual operations and access of resources to prevent unauthorized access

Authentication

ObjectScale appliance supports Active Directory and LDAP authentication methods to provide access to manage and configure ObjectScale. However, limitations exist as shown in the following table. See the *Dell ObjectScale 1.3.x Security Configuration Guide* for more information on security.

Table 1. Supported authentication methods

Authentication method	Supported
Active Directory	• AD group support for management users • Multi-domain is supported
LDAP	• Management users may individually authenticate using LDAP • LDAP Groups are supported for management users, with group mapping. • Multi-domain is supported.

Data-at-rest encryption (D@RE)

Compliance requirements often mandate the use of encryption to protect data written on disks. In ObjectScale encryption can be enabled at the bucket levels. Key features of ObjectScale D@RE include:

- ObjectScale supports FIPS 140-2 mode by default only for the DARE module. It is Level 1 compliant using an AES 256-bit encryption algorithm.

- ObjectScale uses RSA BSAFE Crypto-J JSAFE and JCE software module version 6.2.5 for data encryption that is based on the AES256 algorithm.
- Enabled through the ObjectScale Portal or ObjectScale REST Management APIs
- Can be enabled when an account is added to an object store. Users can enable at the account level and at the bucket level with transitivity.
- Not all buckets or objects must be encrypted within a specific object store
- Supports Amazon S3 Server-Side Encryption (SSE) constructs that enable object encryption and user-supplied keys
- Each object store with an added IAM account, bucket, and object have an associated key that is auto generated at creation
- Keys are separated between object stores with an IAM account
- All user data are encrypted inline before being stored on ObjectScale commodity drives
- There is no limit on the number of accounts and buckets that can be encrypted

See the *Dell ObjectScale 1.3.x Security Configuration Guide* for further information about D@RE.

IAM

Identify and Access Management (IAM) enables users to control and secure access to the ObjectScale resources. This functionality ensures that each access request to an ObjectScale resource is identified, authenticated, and authorized. ObjectScale IAM allows admin to add users, roles, and groups. Admins can also restrict the access by adding policies to the IAM entities.

IAM consists of the following components

- **Account Management** - an ObjectScale account is a logical construct that corresponds to a customer business unit, tenant, which is relevant to the account admin role and end users that belong to an account. ObjectScale users with the Admin role can create accounts in an ObjectScale instance
- **Access Management** - access is managed by creating policies and attaching them to IAM identities or resources
- **Identity Federation** - identity is be established and authenticated by SAML (Security Assertion Markup Language). After an identity is established, use the Secure Token Service to obtain temporary credentials that are used to access the resource
- **Secure Token Service** - enables users to request temporary credentials for same and cross account access to resources, and for users who are authenticated using SAML authentication from an enterprise identity provider or directory service

By using IAM, users can control authentication and authorization to use ObjectScale resources by creating and managing:

- **Users** - IAM user represents a person or application in the account that can interact with ObjectScale resources

- **Groups** - IAM group is a collection of IAM users. Use groups to specify permissions for a collection of IAM users
- **Roles** - IAM Role is an identity that could be assumed by anyone who requires the role. A role is similar to a user, an identity with permission policies that determine what the identity can and cannot do.
- **Policies** - IAM policy is a document in JSON format, which defines the permissions for a role. Assign and attach policies to IAM Users, IAM Groups, and IAM Roles.
- **SAML provider**- SAML is an open standard for exchanging authentication and authorization data between an identity provider and a service provider. SAML provider in ObjectScale is used to establish trust between a SAML-compatible Identity Provider (IdP) and ObjectScale

See the *Dell ObjectScale 1.3.x Administration Guide* for more information about IAM.

Privileged Actions Approval System (PAAS)

The Privileged Actions Approval System (PAAS) prevents a management user from obtaining root-like privileges and circumventing security controls. To prevent this scenario, the PAAS workflow requires an approval from a second user before certain management or account actions can occur. The actions that require approval are high risk if they were performed by bad actors. The picture below shows the workflow f the privileged action approval system.

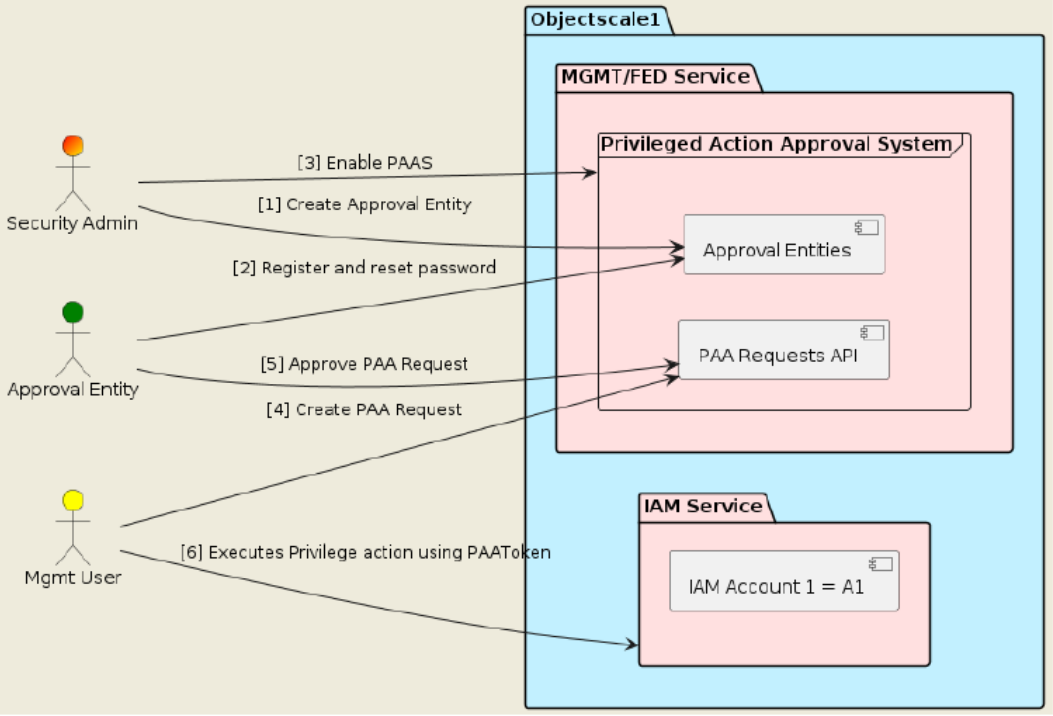


Figure 10. Privileged action approval system (PAAS)

PAAS supports the following ObjectScale protection modes. These protection modes require PAAS to be enabled.

- Account protection mode—Protects S3 data from bad actor risks by requiring approval through PAAS for certain predefined data access and account

configuration actions. Account protection mode is enabled separately on each IAM account.

  - When a resource (bucket or object) owner's account is under protection, then certain S3 actions must use PAAS approval.
  - When an account is protected, default governance lock override privilege no-longer works. All APIs that support Bypass Governance require PAAS approval.

- Platform protection mode—Protects the ObjectScale platform from bad actor risks by requiring approval through PAAS for a set of predefined configuration actions and operating system access.

.

See the *Dell ObjectScale 1.3.x Security Configuration Guide* for more information about privileged actions approval system.

Object lock

Object lock protects object versions from accidental or malicious deletion such as a ransomware attack. It does this by allowing object versions to enter a Write Once Read Many (WORM) state in a standard S3 protocol, where access is restricted based on attributes set on the object version.

In standard S3 protocol, Object lock is only for versioning enabled buckets. ObjectScale extends the standard S3 protocol to permit Object lock at the bucket level, with versioning turned off. The extensions support the standard S3 object locking on versioned buckets and adds support for Object lock on non-versioned buckets.

When Object lock is enabled with versioning, it uses the standard S3 protocol behavior. When Object lock is enabled without versioning, the object lock functionality operates on the bucket, rather than versions of the bucket, similar to ECS retention and traditional file locking.

There are two lock types for object lock:

- **Retention period** -- Specifies a fixed period during which an object version remains locked. During this period, the object version is WORM-protected and cannot be overwritten or deleted.
- **Legal hold** -- Provides the same protection as a retention period, but it has no expiration date. Instead, a legal hold remains in place until it is removed. Legal holds are independent from retention periods.

There are two modes for the retention period:

- **Governance mode** -- users cannot overwrite or delete an object version, or alter its lock settings, unless they have special permissions. With Governance mode, objects are protected against being deleted by most users, but users with relevant permission can alter the retention settings or delete the object if necessary. Governance mode can be used to test retention-period settings before creating a Compliance-mode retention period.
- **Compliance mode** -- a protected object version cannot be overwritten or deleted by any user, including the root user on the account. When an object is locked in

Compliance mode, its retention mode cannot be changed, and its retention period cannot be shortened. Compliance mode helps ensure that an object version cannot be overwritten or deleted during the retention period.

See the *Dell ObjectScale 1.3.x Administration Guide* for more information on ObjectScale object lock.

Bucket logging

S3 bucket access logging is a recommended security best practice that helps companies maintain compliance standards and identify unauthorized access to the data. It records the details for all requests going from a source bucket to a designated target S3 bucket. These include resources specified in the request, request type, and the date and time for when the request was processed. S3 access logs are one of the first sources required in any data breach investigation as they track data access patterns to the buckets. Organizations can configure bucket logging from the ObjectScale Portal user interface. The feature supports prefixes within the target bucket.

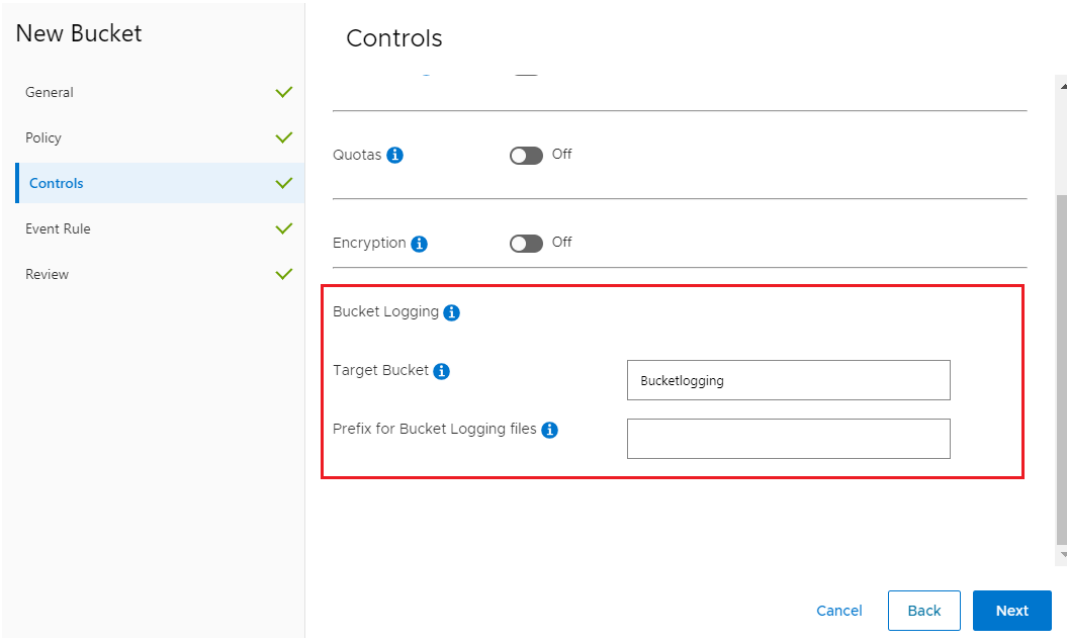


Figure 11. Configure bucket logging

See the *Dell ObjectScale 1.3.x Administration Guide* for more information about ObjectScale bucket logging.

Data integrity and protection

ObjectScale protects data using Dell object storage Erasure Coding (EC) mechanics. EC is a method of data protection in which data is broken into segments, expanded, encoded with redundant data segments, and stored at various locations across the storage platform. ObjectScale implements a Reed Solomon error correction scheme for production environments:

12+4—A chunk is broken into 12 data segments, and four coding (parity) segments are created. A minimum of five disks are required per node for a four-node cluster with 12+4 EC scheme. This allows for one disk failure from a single node or a single node failure.

For the EC scheme, the resulting data and coding segments of each chunk are equally distributed across the nodes in the Kubernetes cluster.

Upon a Kubernetes node permanent failure, copies of lost data segments are re-created using remaining data and coding segments. During temporary Kubernetes node failure, data services continue with data and coding segments that are being used to re-create data when needed.

ObjectScale minimum disk requirements vary based on object store EC requirements. When an object store is created, the total raw capacity and EC scheme are specified. Administrators choose the topology based on input to provide optimal protection and SS size. The number and size of SS instances in an object store represent the persistent storage capacity allocated for raw user data. SS instances attach to Kubernetes persistent volumes (PVs) on disks using Kubernetes persistent volume claims (PVCs). ObjectScale writes data for best protection considering number of volumes on disk, disks per SS, and SS instances across the cluster.

During the object store creation process, the number of Kubernetes nodes in the cluster determine the available EC schemes that are presented within the New Object Store wizard. ObjectScale uses the Kubernetes anti-affinity rules to ensure that the SS replicas are properly placed across the nodes in the cluster. The New Object Store wizard ensures that the number of SS replicas for the new object store is not below the minimum for the selected EC scheme.

The EC scheme of an object store cannot be changed after deployment. Capacity may be added to an object store, but the EC scheme does not change, only the amount of available storage changes.

Note: It is recommended not to wait until the storage platform is completely full before adding drives or nodes. A reasonable storage utilization threshold is 70% taking into consideration the daily ingest rate and expected order, delivery, and integration time of added drives or nodes.

Deployment and provisioning

ObjectScale appliance is a total solution which includes the hardware and software platform. Once the ObjectScale service has been deployed and the external services are configured and available, the next step is to provision accounts, users, object store, and buckets, to provide data access to the ObjectScale storage platform.

Naming conventions

Defining appropriate names for components is sometimes overlooked during provisioning. This oversight might be problematic in some cases or, at most, inconvenient to change once set. Use DNS-appropriate naming conventions for all ObjectScale constructs. Some constructs might allow additional characters, such as an underscore. However, limiting characters to those that are acceptable to DNS eliminates potential application-related conflicts that might arise. Use only the following characters:

- Lowercase letters (a-z). Do not use uppercase letters.

- Numbers (0-9)
- Hyphens

Object stores

An object store provides a way to organize or group items, separating the space for different uses or purposes. The current ObjectScale 1.3 software package supports one object store only.

Buckets

Buckets are containers for object data. Buckets are created in an object store to give applications access to data stored within ObjectScale. Recommendations related to buckets include:

- Use buckets for a specific environment, workflow, or purpose, for example, dev, test, finance, operations
- Bucket names must be unique within an object store. Use DNS-appropriate naming conventions, as previously described in Naming conventions.

User accounts

ObjectScale manages users through IAM, which enables secure, access control to S3 resources. This functionality ensures that each access request to the resource is identified, authenticated, and authorized. With IAM, customers can add users, roles, and groups, and grant and restrict access by adding policies to the IAM entities.

We recommend the following guidelines for user accounts:

- Lock root access keys and do not use the root user for tasks. Instead, use the root user credentials only to create an IAM admin user. Lock the root user credentials and use them to perform only certain account-management and service-management tasks.
- Do not share the IAM credentials between users. Preferably, applications should use temporary credentials, using an IAM role for accessing.
- Change access keys regularly to avoid misuse of compromised credentials.
- Delete IAM user credentials that are no longer required.
- When creating IAM policies, follow the standard security advice of granting least privilege, or grant only the permissions that are required to perform a task.
- Do not define permissions for individual IAM users who perform similar job functions. Create groups, define the permissions for each group, and assign IAM users to groups.

ObjectScale replication

ObjectScale replication (OSR), also referred to as cross-region replication (CRR), is an eventual consistency model that provides more pause and throttle replication flexibility.

OSR allows users to manage and monitor replication policies and replicate bucket data. Replication between object stores complies with the AWS S3 protocol.

Each source bucket can be configured to replicate some or all its data to one or more destination buckets. The data that is replicated from the source bucket can be replicated based on a key prefix or a tag, or both, for more granular replication. An IAM role must be selected for the source bucket account to replicate the data. On the destination bucket

account, the rule can target specific destination buckets that are based on the key prefix and tag.

Object store capacity expansion

The number of replicas and volumes per SS may be increased in an object store using horizontal or vertical expansion:

- **Horizontal expansion:** In this method, increasing the number of replicas increases the number of SS pods used by an object store. Increasing the number of SS pods also increases the number of Kubernetes nodes used by the object store within the cluster. During the horizontal expansion, ObjectScale confirms if there are enough nodes and resources in the Kubernetes environment to schedule the newly added pods.
- **Vertical expansion:** With this method, increasing the number of volumes increases the number of PVCs per node. Increasing the number of PVCs per node increases the amount of capacity used on Kubernetes nodes running the SS pods. During the vertical expansion, ObjectScale confirms that there is enough storage available to allocate to the newly added persistent volumes.

Cluster management

ObjectScale version 1.3, contains a new feature called Cluster management, which provides a unified experience on node/disk operation for the ObjectScale appliance. It can be activated from the ObjectScale Portal as in the following image.

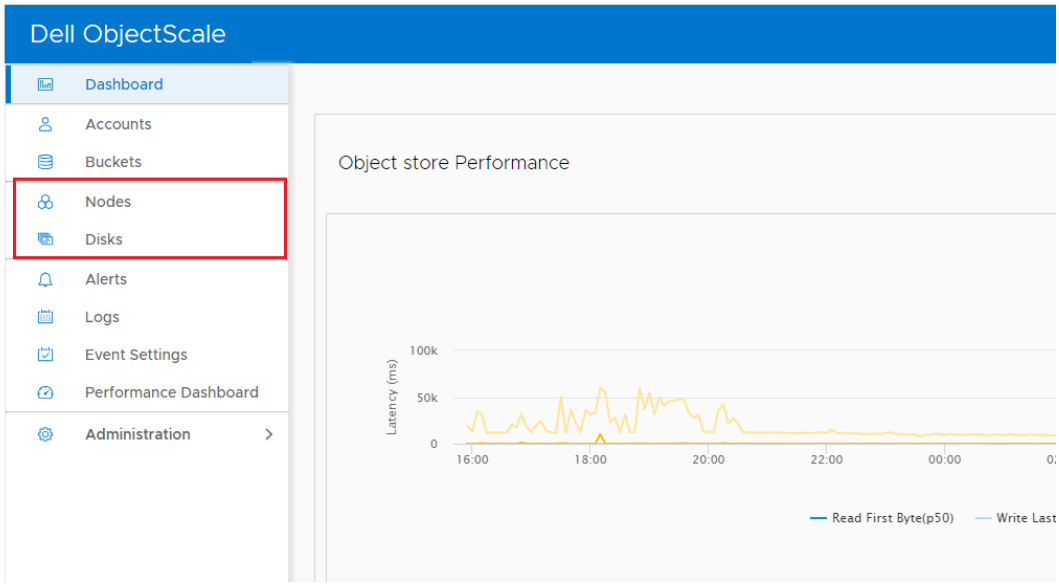


Figure 12. Cluster management for nodes and disks

Cluster management supports below functions:

- **Enter maintenance mode** - When a user wants to complete maintenance work on the node, such as system upgrades to or resolving hardware or software issues
- **Exit maintenance mode** - When a user completes maintenance work on the node and wants to add it back into the cluster
- **Node addition** - The user wants to add new node or add a repaired node back into the cluster.

- **Node removal** - When a user wants to remove a node (healthy node or failed node) from the cluster for repair or retirement
- **Disk removal** - When a user wants to proactively remove a disk from the cluster
- **Disk ejection** - When disk removal is completed and waiting for physical removal

SupportAssist

SupportAssist is a secure support technology that collects system state information and telemetry, automates issue detection, and enables remote troubleshooting and resolutions. Dell recommends that SupportAssist be enabled and configured to accelerate problem diagnosis, expedite troubleshooting, and facilitate time to resolution. The SupportAssist feature employs multiple security layers throughout each step in the remote connectivity process to ensure that customers and Dell can use the solution with confidence:

- All notifications to Dell originate from the customer site, and never from an outside source. They are secured using Advanced Encryption Standard (AES) 256-bit encryption.
- The IP-based architecture integrates with existing infrastructure and maintains the security of the environment.
- Communications between the customer site and Dell are bilaterally authenticated using RSA digital certificates.
- Only authorized Dell Customer Service professionals verified through two-factor authentication can download the digital certificates needed to view a notification from the customer site.
- The optional SupportAssist v3 Policy Manager application allows customers to grant or restrict Dell Support access based on the customer's specific guidelines and requirements. The application includes a detailed audit log.

Conclusion

Summary

Dell ObjectScale appliance provides organizations flexibility in deploying and managing enterprise-grade object storage. ObjectScale is a distributed system that has a layered architecture. Every function is built as an independent layer, which provides horizontal scalability across all nodes and enables high availability. ObjectScale software provides optimum protection, geo-replication, greater availability, and secure data access. Running inside Kubernetes, object stores can be co-located and managed with the applications they support.

References

Dell Technologies documentation

The following Dell Technologies documentation provides additional information related to this white paper. Access to these documents depends on an individual's login credentials. For access to a document, contact a Dell Technologies representative.

ObjectScale and ECS white papers:

- ObjectScale and ECS Info Hub
- Dell ObjectScale 1.3.x Release Notes
- Dell ObjectScale 1.3.x Administration Guide
- Dell ObjectScale 1.3.x Security Configuration Guide
- Dell ObjectScale 1.3.x Rest API Reference
- Dell ObjectScale XF960 Hardware Guide