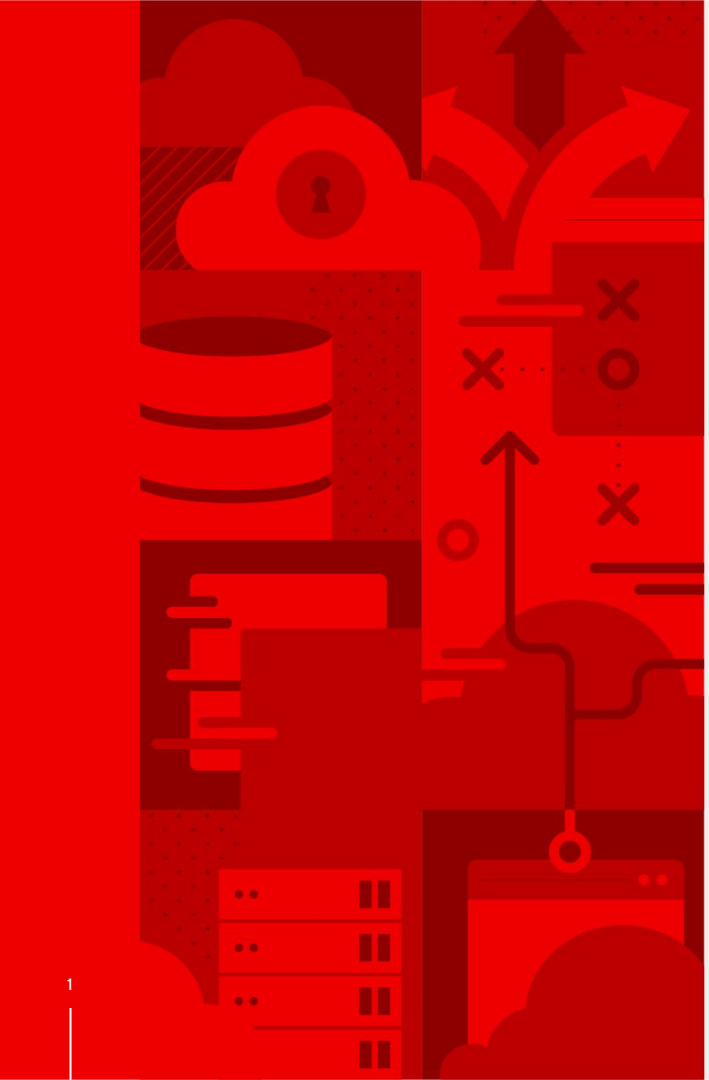


Ceph 4 and OpenShift Container Storage 4

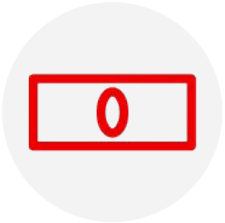
Ceph 4 and OCS 4.3

Joshua Smith
Cloud Solutions Architect
Red Hat

Red Hat

Red Hat Ceph Storage 4

The Benefits of Red Hat Ceph Storage



Scalability: Improved cost to performance ratio

It is a reliable and cost-effective solution—no matter your hardware.

Simplicity: Ability to get started quickly

Our experts can help you get up and running quickly.

Security: Reassurance that it works

You can rest assured that it will work as intended.

Core features

Efficiency

- Containerized deployment to reduce hardware requirements
- Erasure coding for reduced footprint
- Thin provisioning
- In-line compression
- Snapshots, cloning, and copy on write (CoW)

Security

- At-rest and end-to-end encryption
- Pool-level authentication
- Active Directory, LDAP, and Keystone v3
- At-rest encryption—keys held on separate hosts
- Security guide

Performance

- BlueStore back end
- Ability to handle 1 billion objects
- Beast.ASIO front end

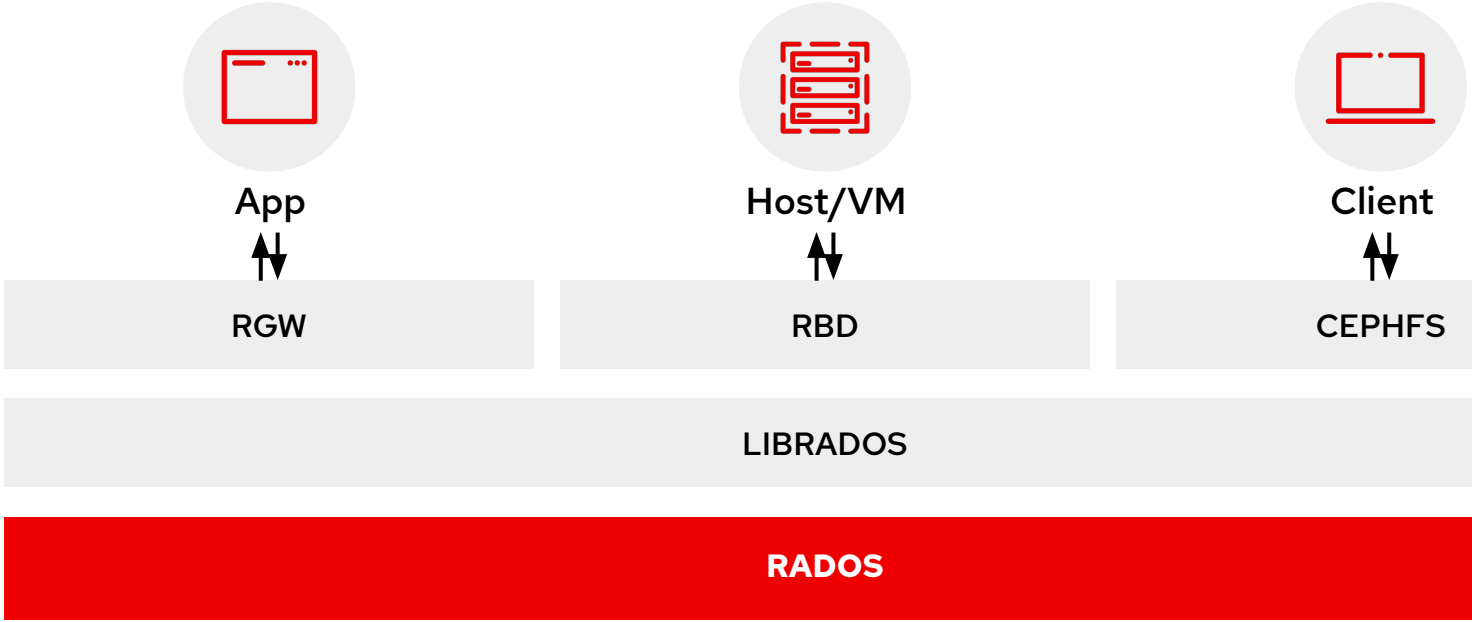
Manageability

- Integrated monitoring and management dashboard
- Simplified user interface (UI) install
- Ansible® automation
- Full command-line interface
- Self-management capabilities

APIs and protocols

- S3, Swift, and Apache Hadoop S3A
- OpenStack® Cinder, Glance, and Manila
- NFS v3 and v4
- iSCSI
- Librados

Architectural components



Technical detailed architecture

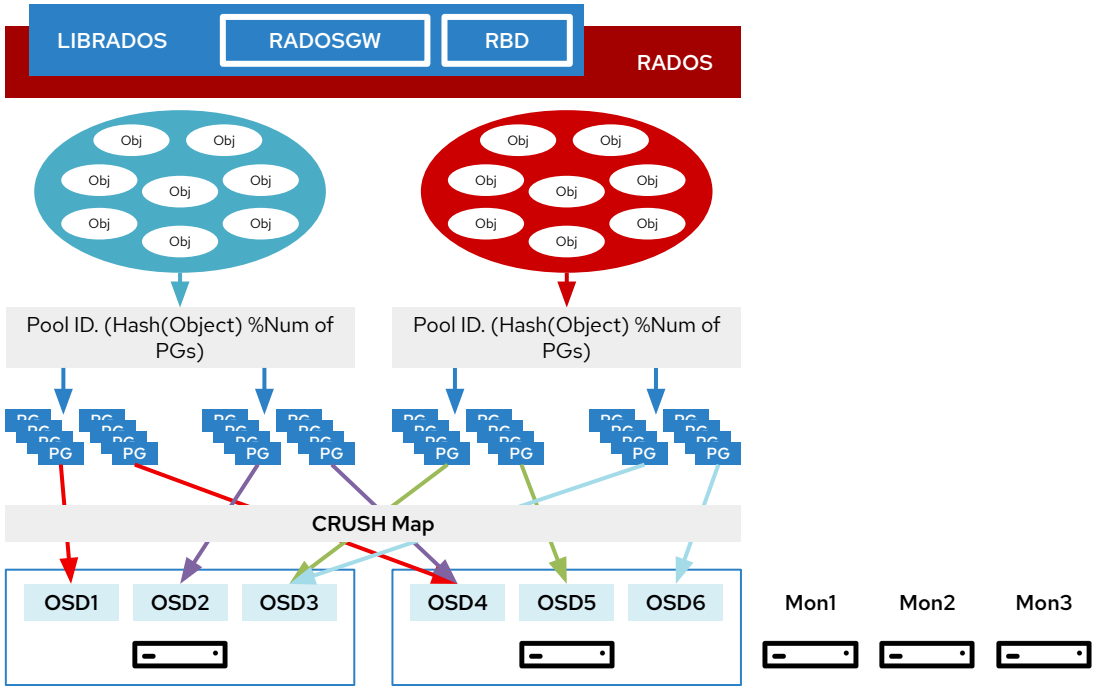
Client interface layer

Objects in pools

CRUSH ruleset

Placement groups

Ceph nodes:
OSD hosts
monitors (mons)



Red Hat

What's new in Red Hat Ceph Storage 4?

The latest update offers improvements to scalability, performance, and security.

Red Hat

Easier to Get Started

It's easier than ever to get started

Red Hat Ceph Storage 4 has a **new installation wizard** that makes it so easy to get started even your cat could do it.

No prior Ceph knowledge required

Backed by the same Ansible logic operators are already familiar with, Red Hat Ceph Storage 4 requires **minimal Ceph knowledge to deploy clusters for the first time.**

New management tools

Red Hat Ceph Storage 4 doesn't require mastering the internal details of the RADOS storage system, significantly **lowering the curve to SDS adoption**.

Easier to Use

Improved monitoring tools for better insights

One of the most requested features, “RBD Top”, is now available. Gain **immediate insights** on what clients are generating the most IO.

New dashboard gives you greater control

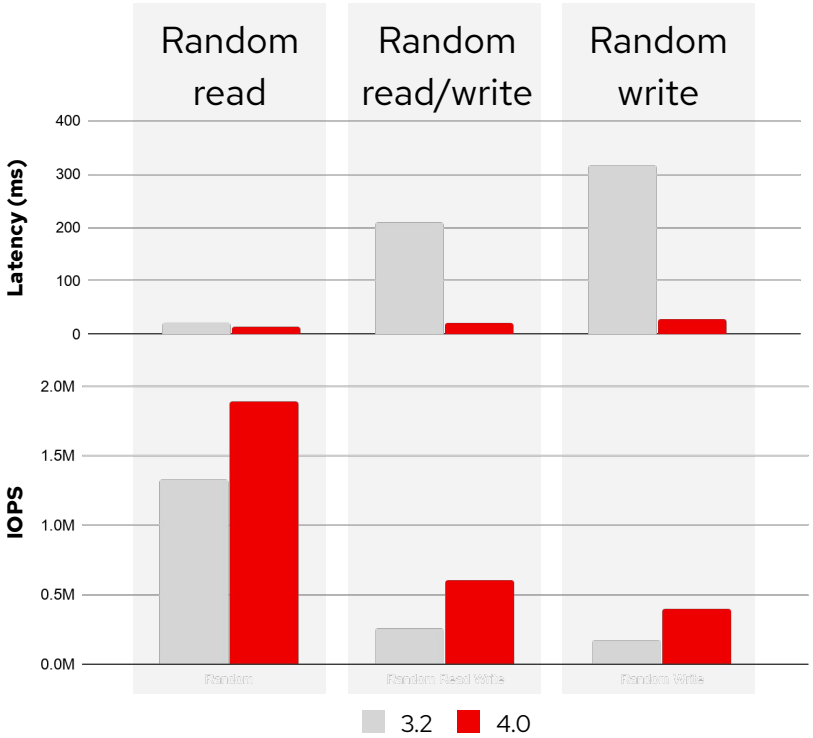
Do even more from the **new dashboard**, including manage storage volumes, create users, monitor performance and even initiate cluster upgrades.

Do more with less

The **total cost of ownership is lowered** as Red Hat Ceph Storage 4 introduces minimum configurations for customers looking at smaller Object store deployments.

Increased performance

Lower latency and more IOPS

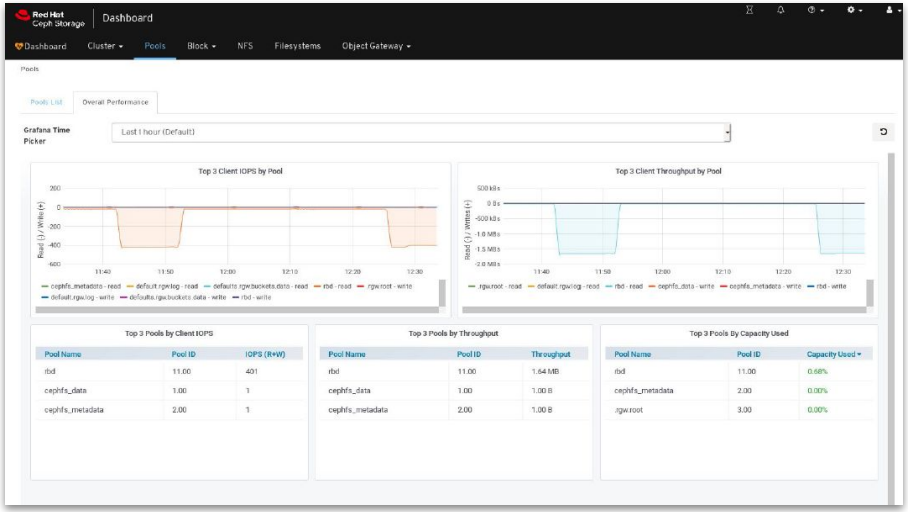


- Twice the object store performance we were delivering just a year ago:
  - New object store front end
  - Bluestore back end
- Improved RADOS block device (RBD):
  - RBD top
  - RBD namespace
  - RBD live pool migration
- Reduced latency variance benefits RDBMs workloads
- Lower base configurations:
  - 3 nodes minimum
  - 4 nodes recommended

Red Hat

New dashboard

For better monitoring and management



- New monitoring functionality
- Improved usability
- Operators can delegate junior administrators with replacement of failed drives, users, and quota management through a role-based access control (RBAC) system

Red Hat

Red Hat Ceph Storage 4

Scalability

You need to store more and improve performance while getting value for money.

Simplicity

You want 1 solution that can manage all your storage and minimize the admin burden.

Security

You need to not just secure your data from cyberattacks, but also manage data protection and resiliency.

Red Hat Ceph Storage 4 delivers:

- Scalability to thousands of petabytes and billions of objects.
- Increased performance.
- Easier installation—minimal Ceph experience is required.
- Better monitoring and management.
- Improved automation.
- More granular permissions and delegation.
- Protection against hardware failures.
- Improved encryption.

Red Hat Ceph Storage 4 and Security

Red Hat

Improved security features

Supports FIPS compliant encryption

Encryption on the wire for back-end protocol

Front-end quality of service for block users

RGW MFA delete

Red Hat Ceph Storage 4

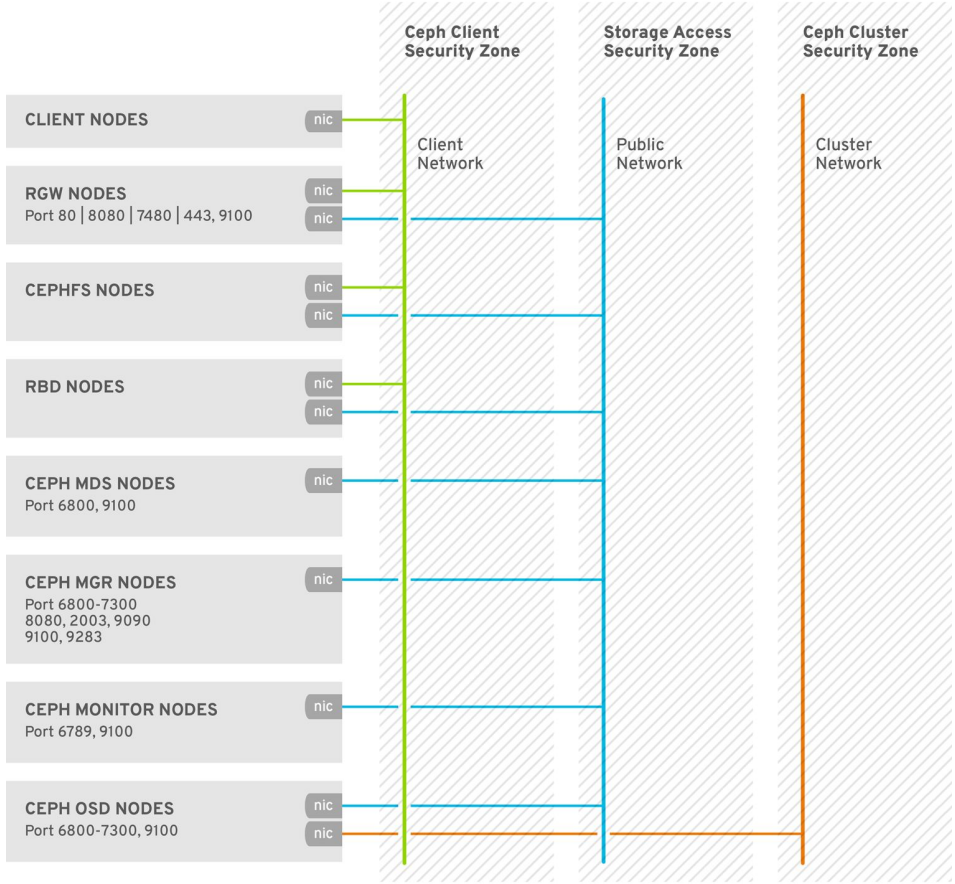
Lifecycle—up to five years

- Standard support for three years:
  - New point releases
  - Repository updates
  - Bug fixes
  - Security errata
  - Feature enhancements.
- An additional two years ELS lifecycle is available

Version compatibility

- All previous releases still under support can import an external cluster through director automation
- Red Hat OpenShift versions 3+
- GA support in Red Hat OpenStack Platform for external and hyperconverged clusters alike
- *Red Hat OpenShift Container Storage 4.2 recommended for use in OpenShift*

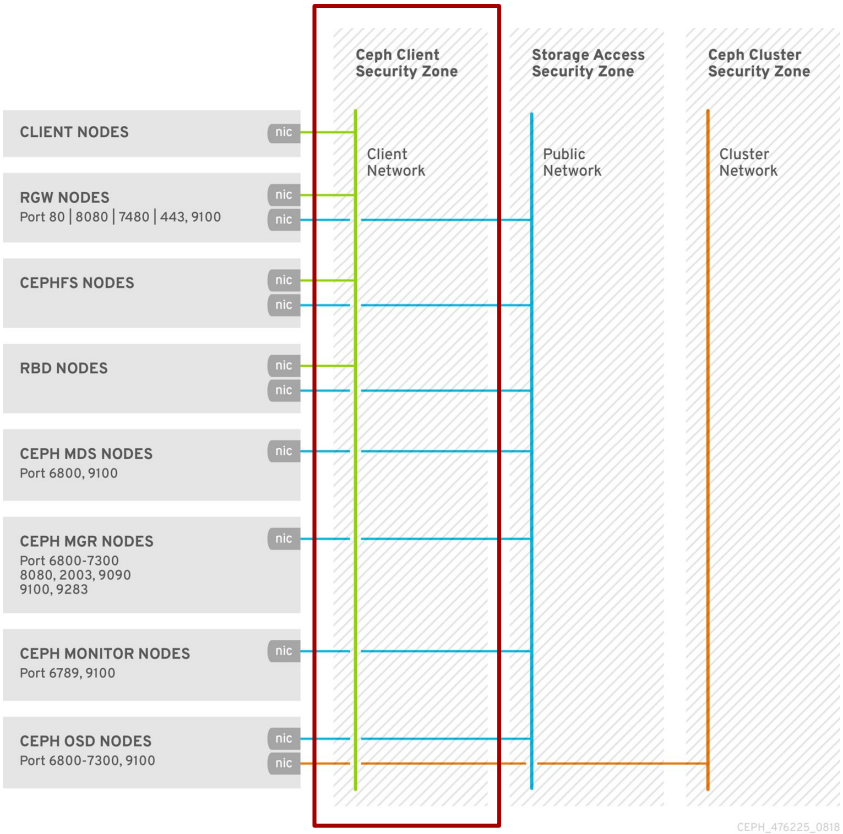
Security Zones – Best Practices



CEPH_476225_0818

Red Hat

Security Zones - Best Practices



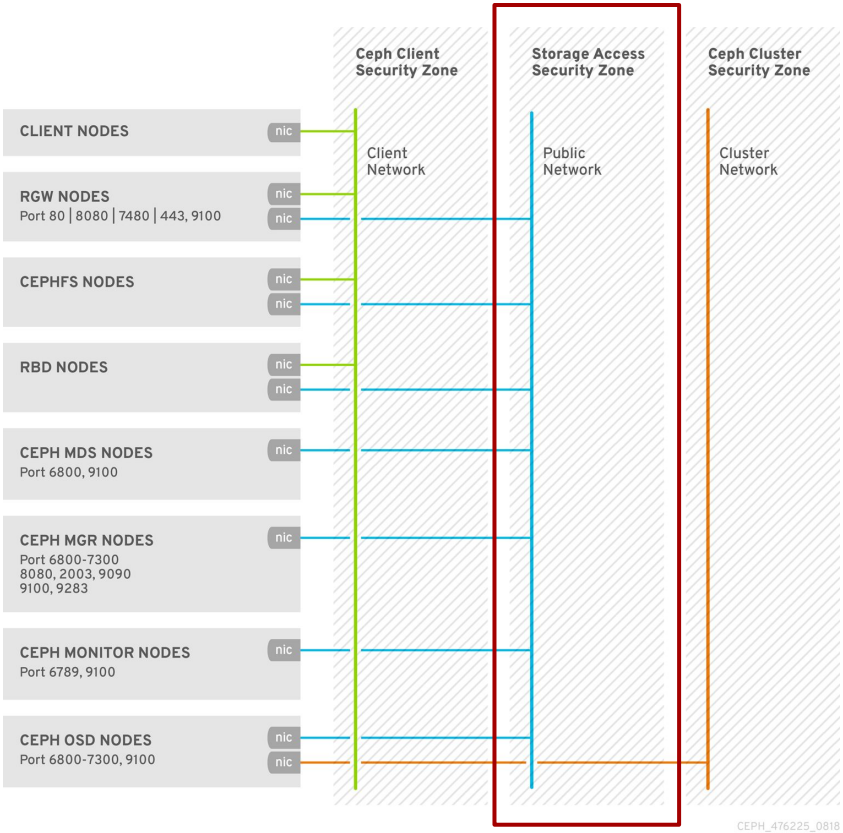
Ceph Client Security Zone

Networks accessing Ceph clients such as Ceph Object Gateway, Ceph Block Device, Ceph Filesystem, or librados.

The Ceph client security zone is typically behind a firewall separating itself from the public security zone.

Red Hat

Security Zones - Best Practices



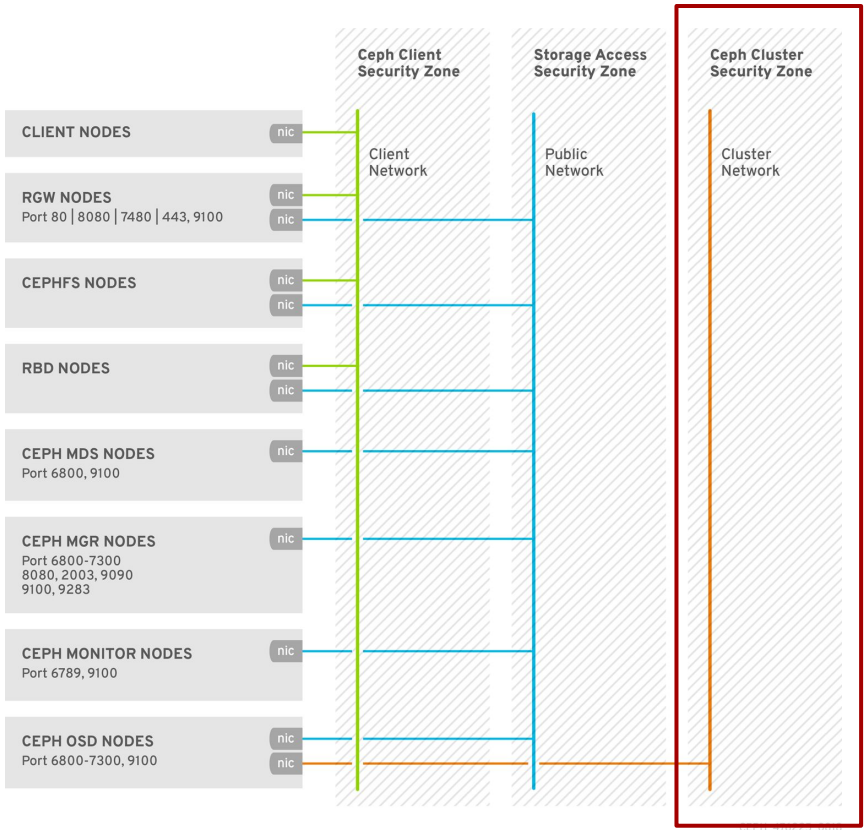
Storage Access Security Zone

Networks providing Ceph clients with access to the Ceph Storage Cluster.

The storage access security zone includes the Ceph Storage Cluster's front- or client-side network, which is referred to as the public_network in RHCS.

Red Hat

Security Zones - Best Practices



Ceph Cluster Security Zone

Internal networks providing the Ceph Storage Cluster's OSD daemons with network communications for replication, heartbeating, backfilling, and recovery.

The Ceph cluster security zone includes the Ceph Storage Cluster's backside network, which is referred to as the cluster_network in RHCS.

Red Hat

Key Management

- All nodes in the RHCS cluster use SSH as part of deploying the cluster.
- Also, the Ceph Object Gateway supports encryption with customer-provided keys using its S3 API.

Encryption In-Flight

- Starting with Red Hat Ceph Storage 4 and later, you can enable encryption for all Ceph traffic over the network with the introduction of the messenger version 2 protocol.
- The secure mode setting for messenger v2 encrypts communication between Ceph daemons and Ceph clients, giving you **end-to-end encryption**.

Encryption at Rest

Red Hat Ceph Storage supports encryption at rest in a few scenarios:

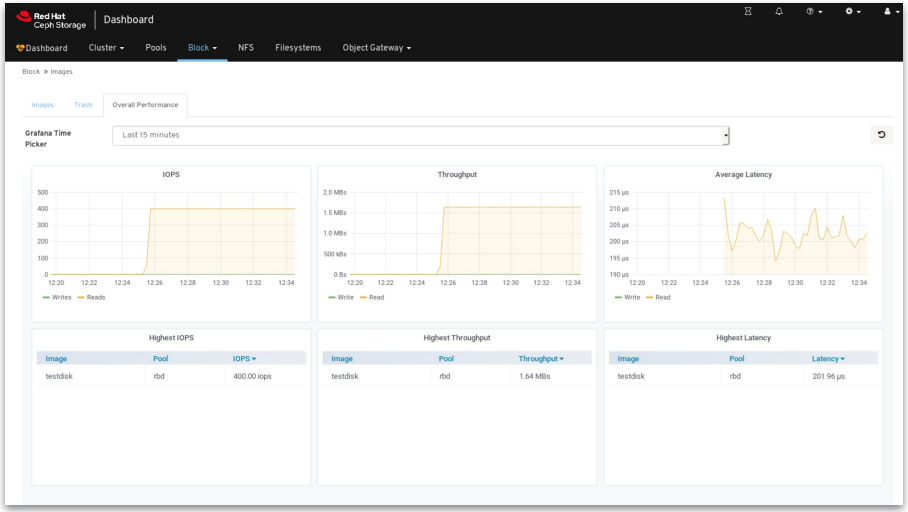
- Ceph Storage Cluster: supports Linux Unified Key Setup or LUKS encryption of OSDs and their corresponding journals, write-ahead logs, and metadata databases. In this scenario, **Ceph will encrypt all data at rest** irrespective of whether the client is a Ceph Block Device, Ceph Filesystem, Ceph Object Storage cluster or a custom application built on librados.
- Ceph Object Gateway: supports encryption of client objects. When the Ceph Object Gateway encrypts objects, they are **encrypted independently** of the Red Hat Ceph Storage cluster. Additionally, the data transmitted is between the Ceph Object Gateway and the Ceph Storage Cluster is in encrypted form.

Identity and Access Management

- Red Hat Ceph Storage provides identity and access management for:
  - Ceph Storage Cluster User Access
  - Ceph Object Gateway User Access
  - Ceph Object Gateway LDAP/AD Authentication
  - Ceph Object Gateway OpenStack Keystone Authentication

More granular permissions

For greater efficiency while maintaining control



- Power users can delegate tasks to junior administrators or developers.
- Junior admins and developers get the confidence to do what they need to do, and power users get reassurance that those admins and developers won't do things they shouldn't be doing.
- Monitoring interface pinpoints IOPS, throughput, and latency outliers to pre-emptively identify issues.

Red Hat

Auditing

An important aspect of system security is to periodically audit administrator actions on the cluster. Red Hat Ceph Storage stores a history of administrator actions in the /var/log/ceph/ceph.audit.log file.

Each entry will contain:

- Timestamp: Indicates when the command was executed.
- Monitor Address: Identifies the monitor modified.
- Client Node: Identifies the client node initiating the change.
- Entity: Identifies the user making the change.
- Command: Identifies the command executed.

Federal Information Processing Standard (FIPS)

Red Hat Ceph Storage is supported on Red Hat Enterprise Linux configured in Federal Information Processing Standard (FIPS) mode. FIPS mode ensures that cryptographic tools implement their algorithms properly. You do not need to change any Ceph configuration for Ceph to work with FIPS mode, FIPS just needs to enabled in the operating system.

Prerequisites:

- Red Hat Enterprise Linux 7.6 or higher is used with FIPS mode enabled.
- Red Hat Ceph Storage 3.2.z2 or higher is used.

Further resources

Visit our product page to find out more about Red Hat Ceph Storage and the benefits it could bring to your business.

redhat.com/ceph

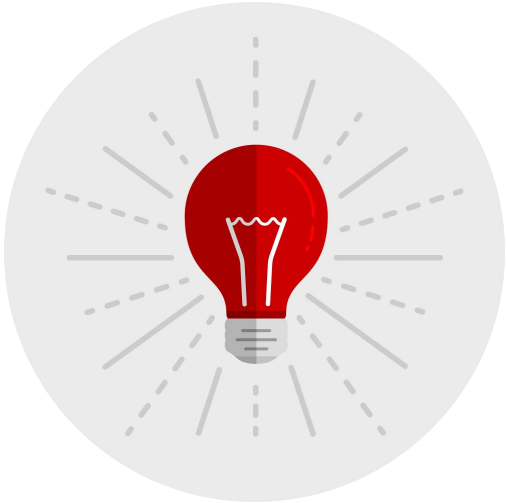
Data Security and Hardening Guide, Red Hat Ceph Storage 4: https://access.redhat.com/documentation/en-us/red_hat_ceph_storage/4/html/data_security_and_hardening_guide/index

Red Hat

OpenShift Container Storage 4.3

Red Hat

OpenShift Container Storage 4



1 **WHY**

OpenShift stateful applications need a complete data and storage management platform.

2 **WHAT**

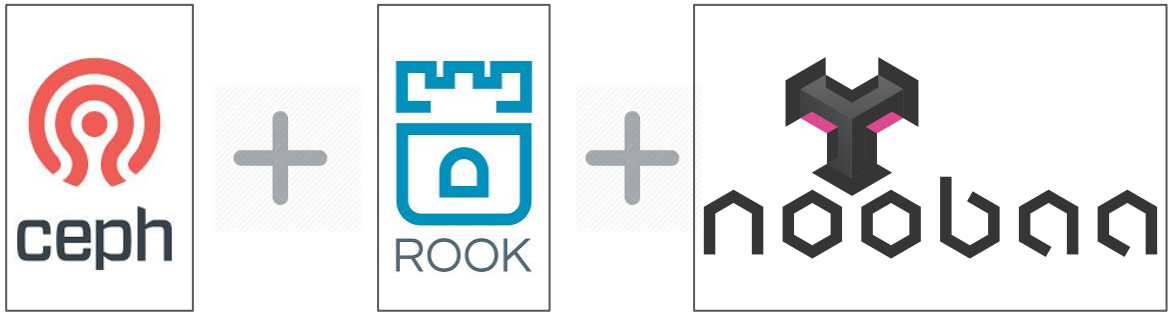
A seamless and an intuitive developer and storage experience for OpenShift users across the open hybrid cloud

3 **HOW**

By using Red Hat Ceph storage, combined with the Kubernetes-centric Rook open project and Noobaa

Red Hat

The OCS 4 Technology Stack



About ROOK

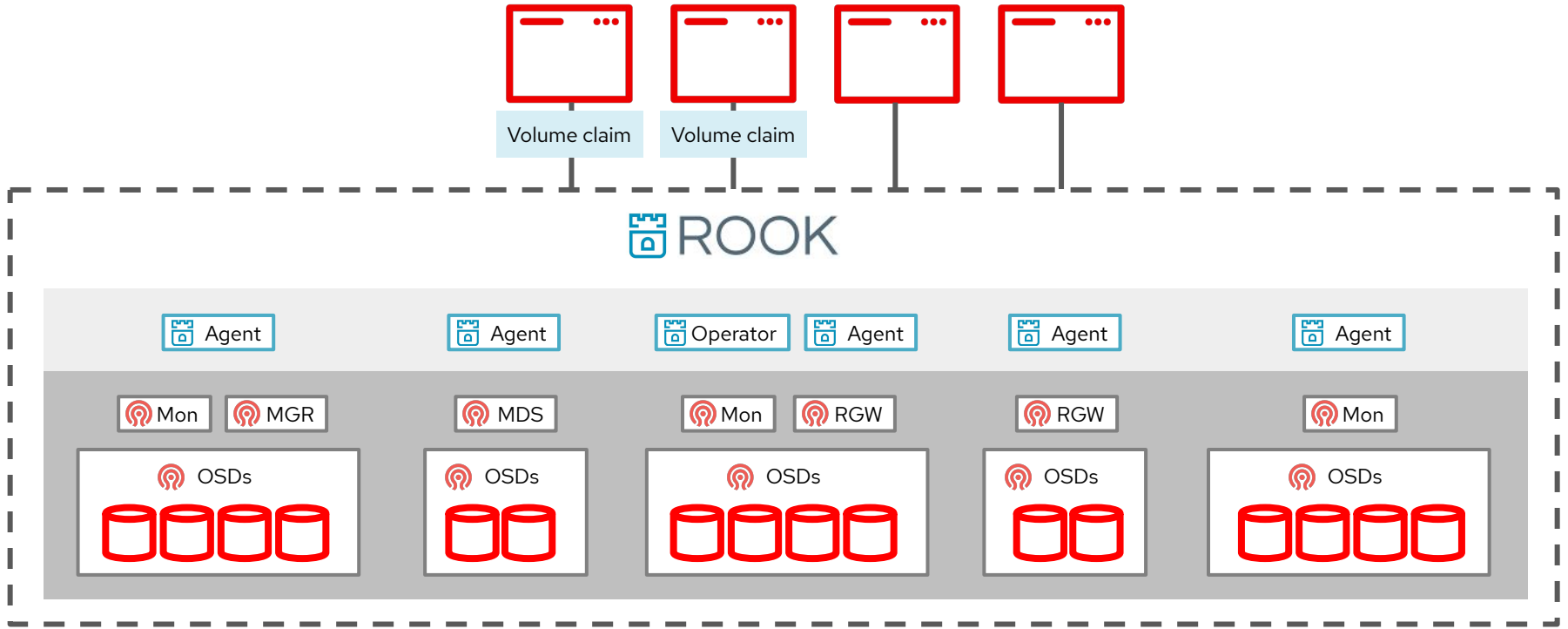
- ROOK Project: cloud-native storage orchestrator, automated deployment and life-cycle management
- Ceph Storage bootstrapping
- Configuration, provisioning, scaling, upgrading, migration, disaster recovery, monitoring, and resource management

https://rook.io

Red Hat

ROOK

Rook architecture



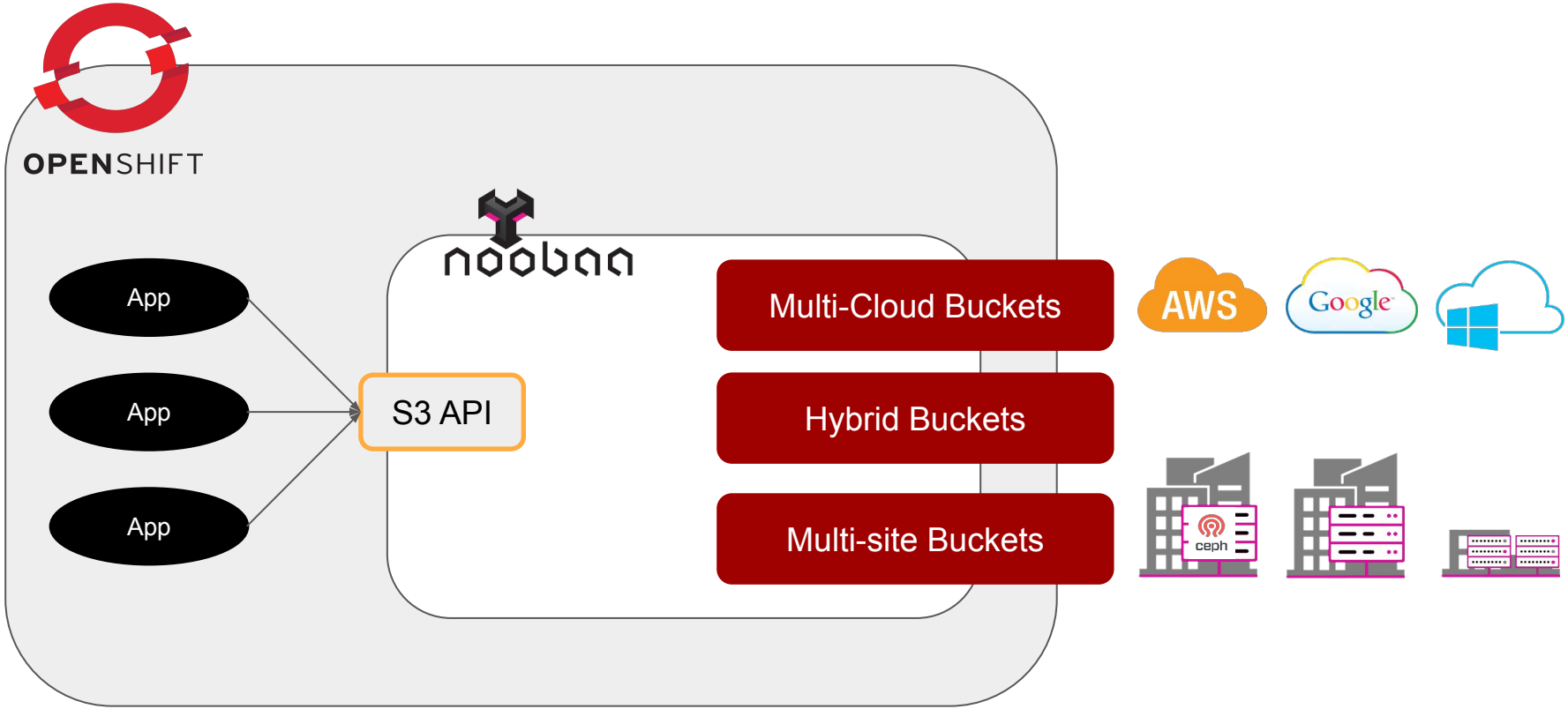
Red Hat

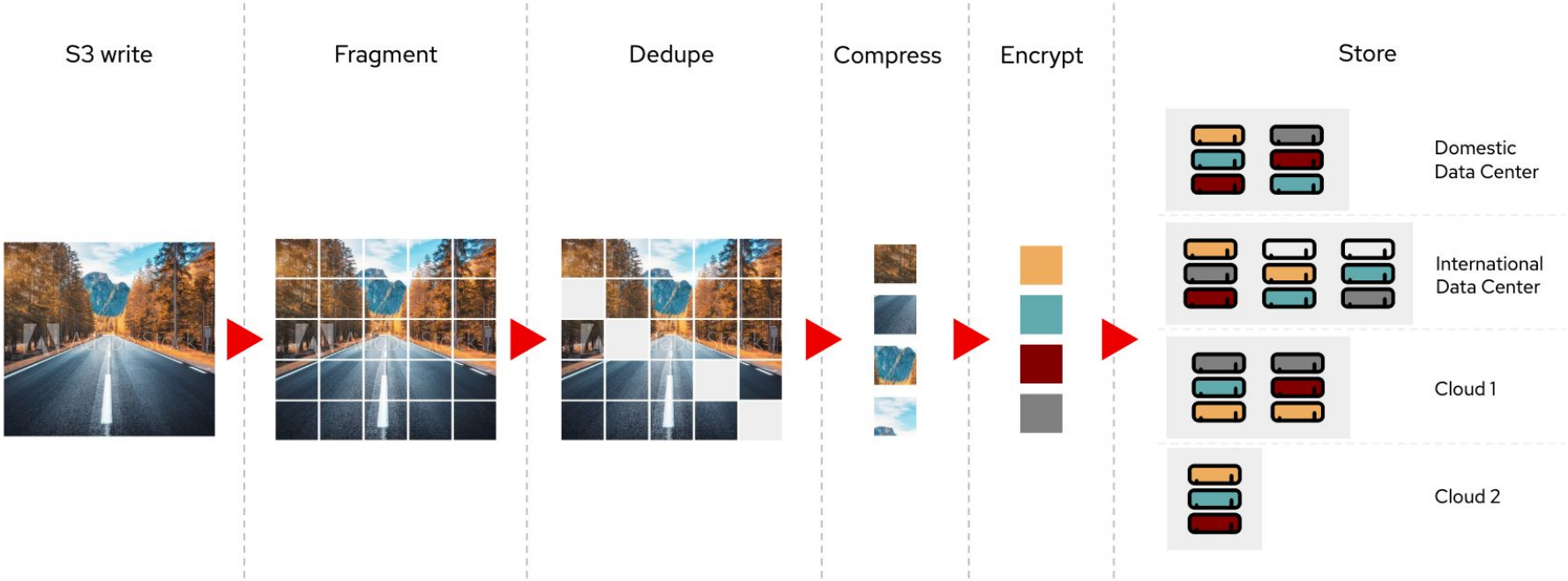
About Noobaa

- Multi-cloud object gateway
- Data federation across multiple clouds, private *or* public

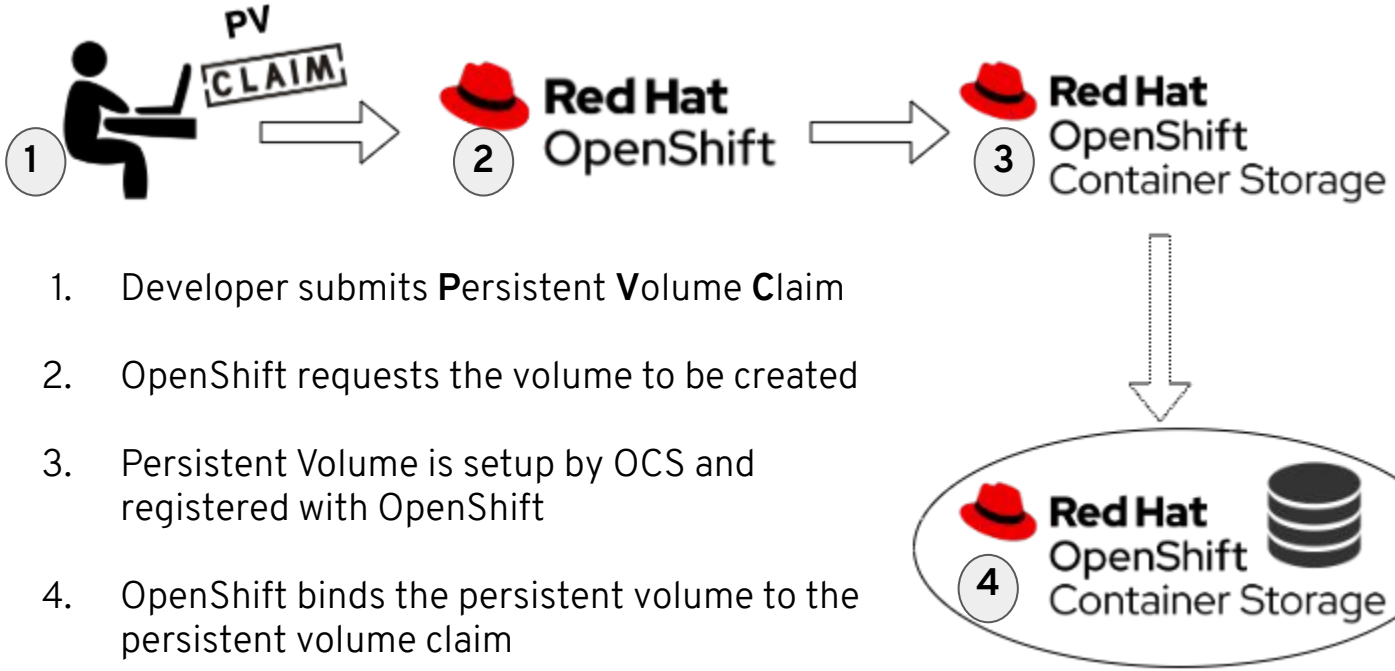
https://www.noobaa.io/

Deploy and Manage *Object* Data Services



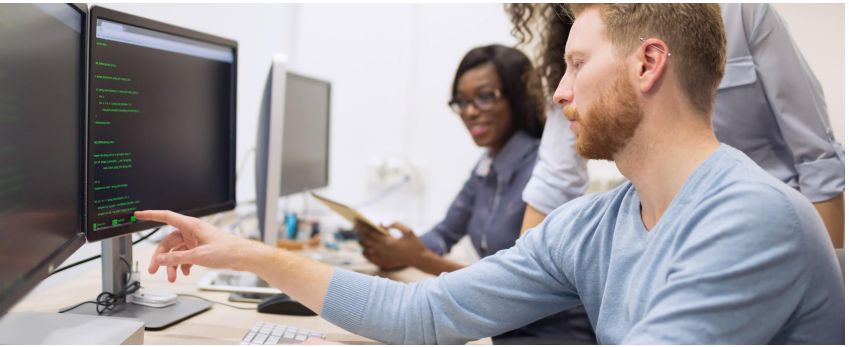

S3 write
Fragment
Dedupe
Compress
Encrypt
Store
Domestic
Data Center
International
Data Center
Cloud 1
Cloud 2

OpenShift Container Storage Workflow



1. Developer submits **P**ersistent **V**olume **C**laim
2. OpenShift requests the volume to be created
3. Persistent Volume is setup by OCS and registered with OpenShift
4. OpenShift binds the persistent volume to the persistent volume claim

OCS 4.3
new features



Red Hat

RED HAT® OPENSHIFT Container Storage

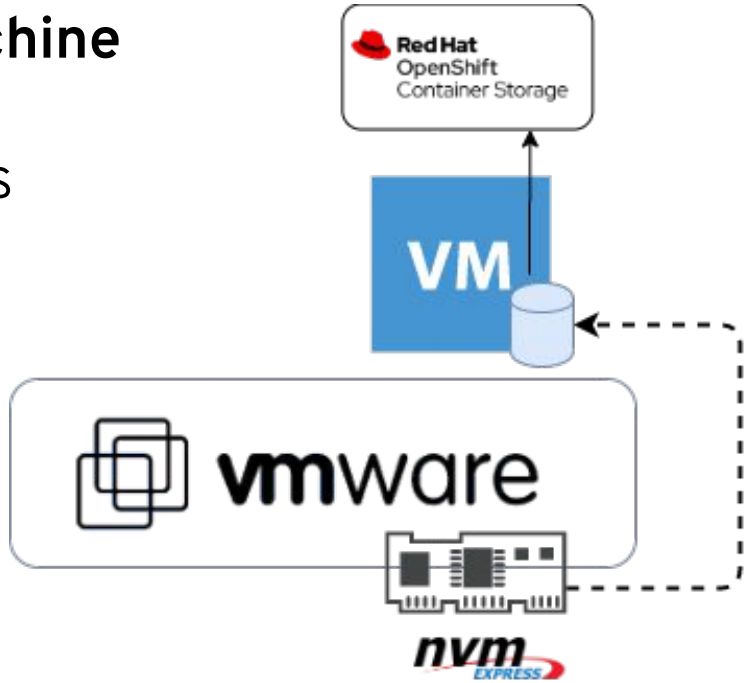
OCS 4.3 - Release highlights

- **Flexibility**: AWS i3 instance **Tech Preview**
  - Ability to work in smaller instances
  - Recommended for cloud bursting, or other ephemeral storage

OCS 4.3 - Release highlights

RED HAT OPENSHIFT Container Storage

- **Local Storage in Virtual Machine**
  - Better performance with VMware-attached devices

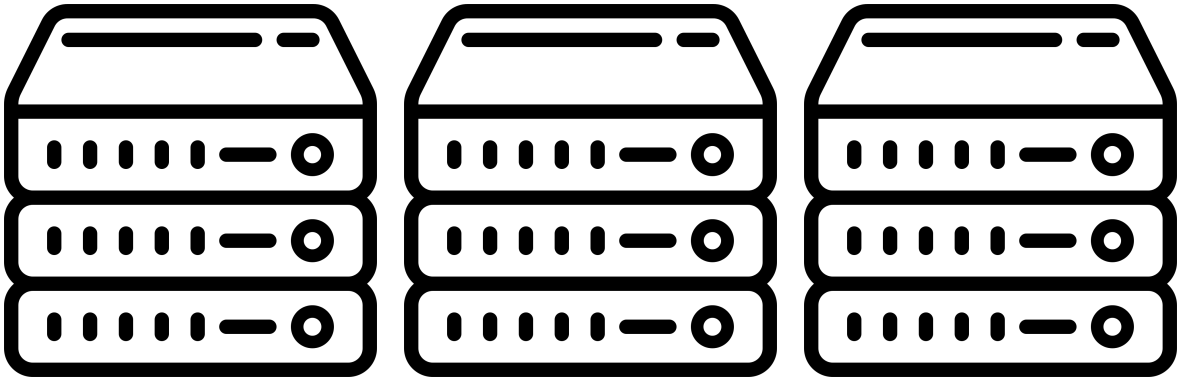


Tech Preview

OCS 4.3 - Release highlights

RED HAT® OPENSHIFT Container Storage

- **Run on bare metal** Tech Preview



OCS 4.3 - Release highlights

RED HAT® OPENSHIFT Container Storage

- **OSD Sizing**
  - Optional smaller cluster size for PoC purposes (0.5TB)
  - Option to start with larger cluster size (4TB)



OCS 4.3 - Release highlights

RED HAT® OPENSHIFT Container Storage

- **Multicloud Object Gateway**

  Added support for IBM COS backing store 

  in addition to 

  , 

  , 

  , 

  and any other  S3 compatible solution

RED HAT® OPENSHIFT Container Storage

OCS 4.3 - Release strategy

- **OCS Release Strategy**
  - Red Hat releases small updates, frequently, to enable responsive changes
  - OCS version alignment with OCP versions as soon as possible.

picture source: pexels.com

Red Hat

OpenShift Container Storage roadmap

Released OCS 4.3
April 14th 2020

- Flexibility in Deployment
  - AWS i3 instance - TP
  - VMware Local drive - TP
  - Flexible OSD Size - GA
- Bare Metal - Tech preview
- Multicloud gateway
  - Performance
  - IBM COS Support
  - Bucket policy
  - Data Portability/Hybrid Cloud

Near term (4.4)
June 4th 2020

- GA support for VMware local drive
- GA support for Bare Metal

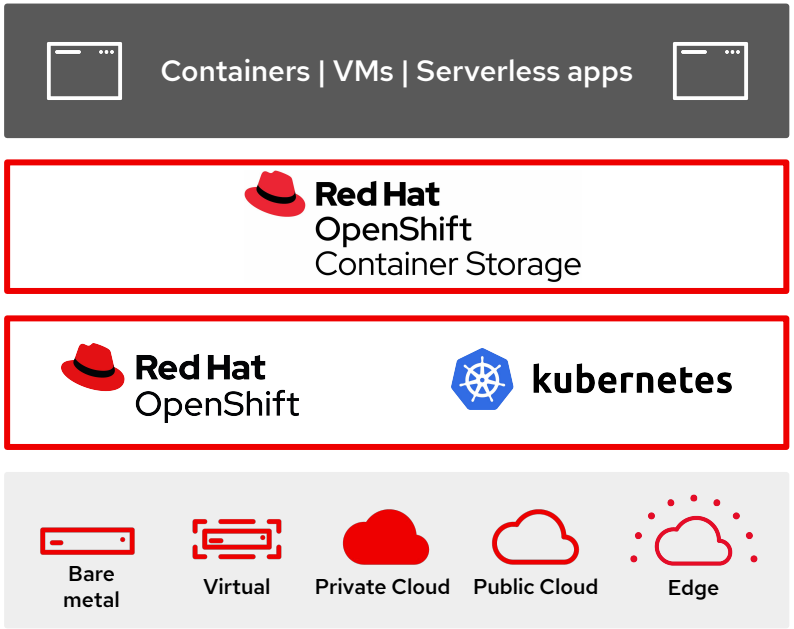
Medium Term (4.5)
August-ish 2020

- Independent Mode - OCS -> RHCS GA
- FIPS validated cryptography
- PV Expansion - TP
- Disconnected Environment
- Proxy environments

* This is an uncommitted roadmap and Red Hat reserves the right to change it.

Deployment Modes: Converted and Independent

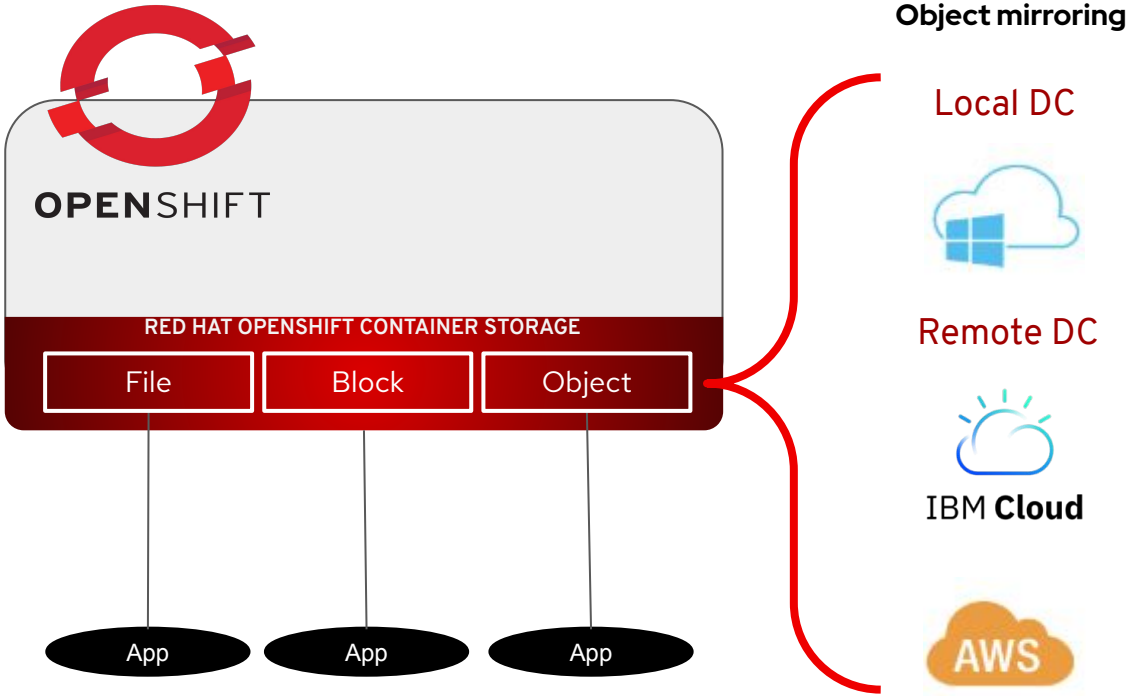
Converged Mode



- Autonomous solution
- Agnostic to the underlying storage
- Agnostic to the hosting platform

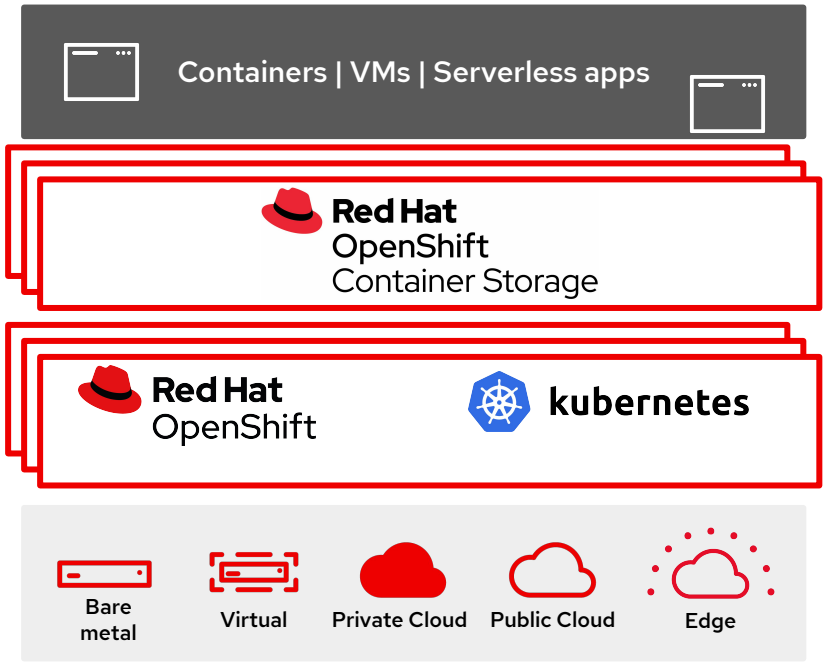
Red Hat

Converged Mode



Red Hat

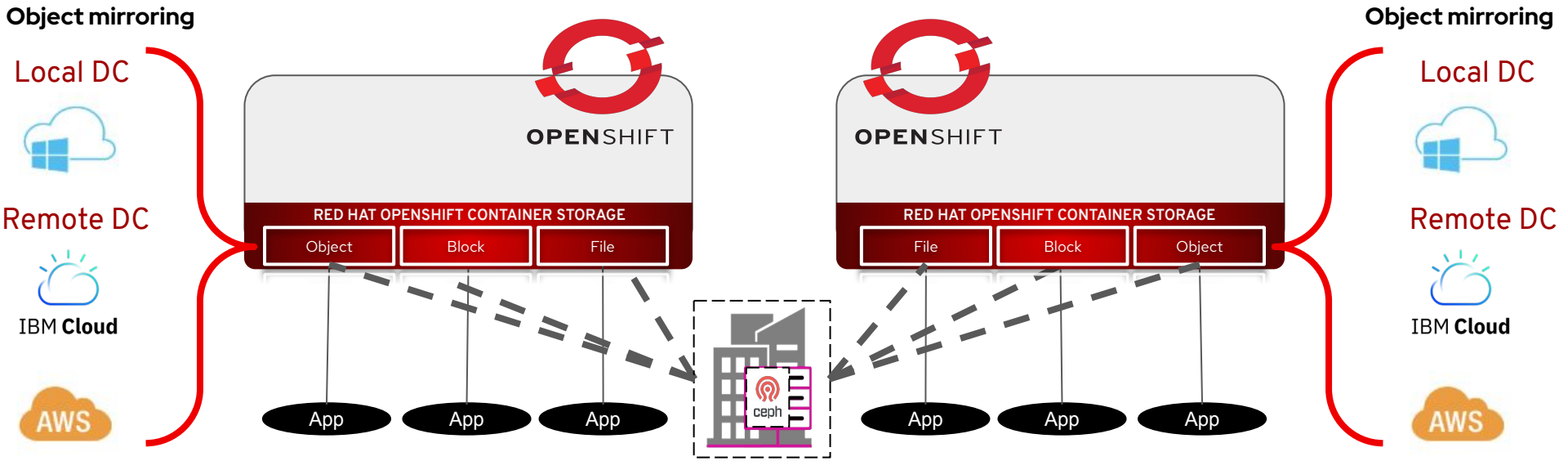
Independent Mode



- Centralized storage serving multiple OpenShift Container Platforms
- Slim OpenShift Container Storage deployment on each OpenShift Container Platform
- Scale to PB with elastic resources

Red Hat

Independent Mode



Red Hat

Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.


linkedin.com/company/red-hat


youtube.com/user/RedHatVideos


facebook.com/redhatinc


twitter.com/RedHat

Red Hat