

# OpenShift 4.x Architecture Workshop

CoreOS and OpenShift 4.x

July 2019

# CoreOS



# Container Host Vision

An Ideal Container Host would be	Red Hat CoreOS
Minimal	Only what's needed to run containers
Secure	Read-only & locked down
Immutable	Immutable image-based deployments & updates
Always up-to-date	OS updates are automated and transparent
Updates never break my apps	Isolates all applications as containers
Updates never break my cluster	OS components are compatible with the cluster
Supported on my infra of choice	Inherits majority of the RHEL ecosystem
Simple to configure	Installer generated configuration
Effortless to manage	Managed by Kubernetes Operators

# Red Hat CoreOS

Adapting for the next wave of innovation in distributed systems

Combining the innovations of Container Linux and Atomic with the stability and ecosystem of RHEL

Fully integrated and delivered via OpenShift.

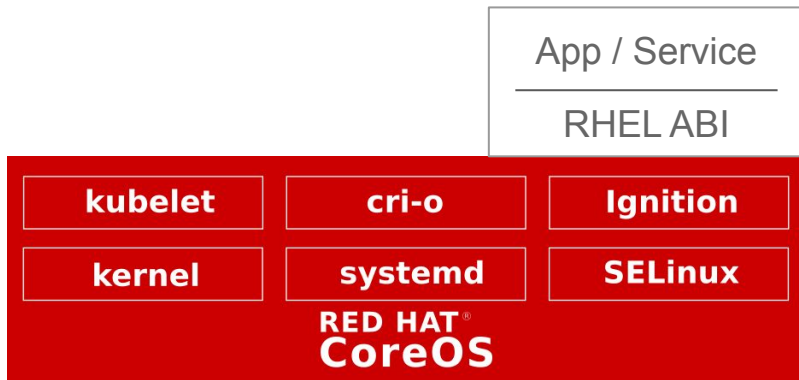
- Small footprint, derived from RHEL
  - ~400 packages
- Fast provisioning: clusters deploy in minutes
- Simplified, cluster-centric updates and upgrades
- Managed and automated via operators



# Red Hat CoreOS

Built for stability, scale, and hands-free operation

- Full support for the RHEL ABI & container ecosystem
- An immutable host, delivered and managed via OpenShift
  - Aligned lifecycle and release cadence
  - Updates & upgrades deployed via operators
- UX inspired by Container Linux
  - Read-only OS binaries in /usr
  - Integrated container & kubernetes stack
  - One-touch provisioning with Ignition



# One Touch provisioning via Ignition

Machine generated; machine validated

Ignition applies a declarative node configuration early in the boot process.

- Generated via openshift-install
- Similar in scope to cloud-init
- Configures storage, systemd units, users, & remote configs
- Executed in the initramfs
- v3.0 spec is in progress

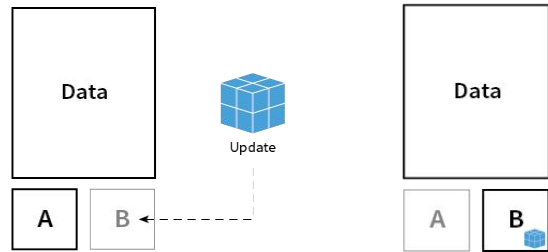
```
{
  "ignition": {
    "config": {},
    "timeouts": {},
    "version": "2.1.0"
  },
  "passwd": {
    "users": [
      {
        "name": "core",
        "passwordHash": "$6$43y3tkl...",
        "sshAuthorizedKeys": [
          "key1"
        ]
      }
    ]
  },
  "storage": {},
  "systemd": {}
}
```

# Transactional Updates via rpm-ostree

## Versioning and Simplifying OS Updates

Transactional updates ensure that the Red Hat CoreOS is never altered during runtime. Rather it is booted directly into an always “known good” version.

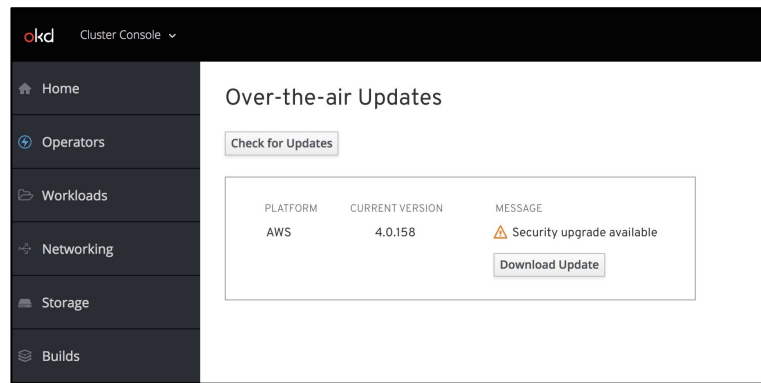
- Each OS update is versioned and tested as an complete image.
- OS binaries (/usr) are read-only
- Updates encapsulated in container images
- file system and package layering available for hotfixes and debugging



# Over-the-air Updates - Delivery Mechanism

For Hosted and on-prem Deployments

- Updates can be driven from either *cloud.openshift.com* and/or the Cluster Console
- Updates are delivered via OCI images
- Auto-update support
- Manual updates will be supported for disconnected environments
  - Tooling to automate updates will be added in later release
  - Single source of content to mirror



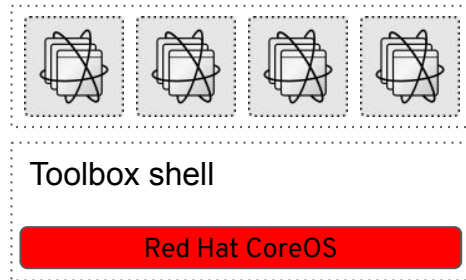


# Low-level Debugging via Toolbox

Bring your tools with you!

Toolbox is a simple script that provides a persistent privileged container for the following use cases:

- Low-level troubleshooting /debugging environment
- Collecting sosreports
- Install additional utilities not available as part of RHCOS



# Container Stack

OCI tooling to create, run, and manage, Linux Containers with a cluster-friendly life cycle



**cri-o**

**Light-weight runtime  
for the Kube CRI**

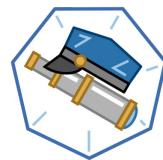
- OCI compliant and docker compatible
- Leverages runC
- CLI via crictl
- Improved performance and scalability



**podman**

**A docker-compatible  
CLI for containers**

- Remote management API via Varlink
- Image/container tagging
- Advanced namespace isolation



**skopeo**

**Inspect, push/pull, &  
signing of OCI images**

- Inspect image manifests
- Can transfer images between multiple registries.

# OpenShift 4.x

# OPENSHIFT 4.x THEMES

## DAY 2 OPERATIONS



Integrate CoreOS technology for a better install, re-config and upgrade experience.

Bring over-the-air upgrades to the platform.

## IMMUTABLE INFRASTRUCTURE



Introduce Red Hat CoreOS as an immutable OS option. Enhance “infrastructure as code” throughout the platform.

## OPERATOR FRAMEWORK

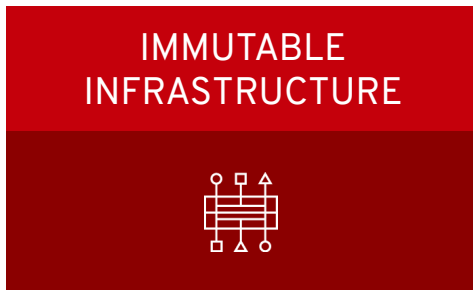


Provide tools, guidance and automation for customers and partners to deliver smart software on top of OpenShift

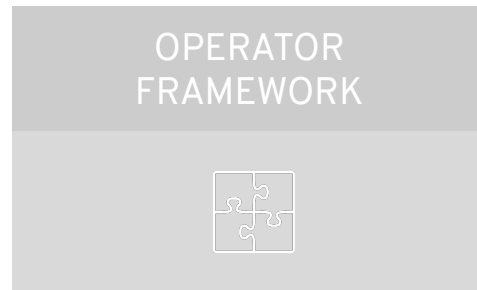
# OPENSIFT 4.x WORKSTREAMS



**AWS Installer + bootstrapping**  
**Autoscale out of the box**  
**MachineSet node pools**

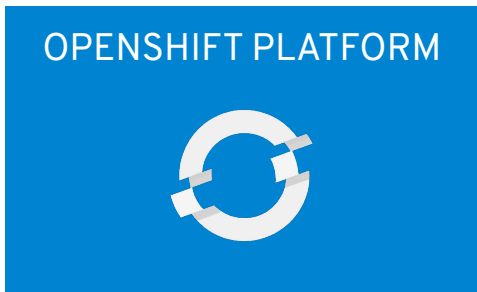


**Red Hat CoreOS**  
**Discourage SSH/node mutation**  
**Ignition for Machine config**



# IMMUTABLE INFRASTRUCTURE

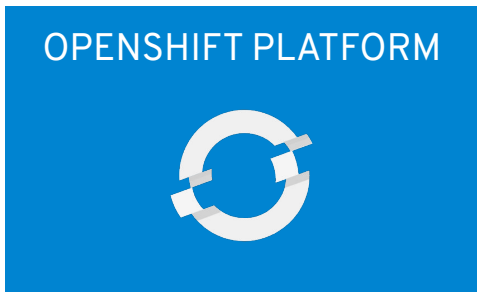
## OPENSIFT 3



- Manually provision RHEL, bring to cluster
- Rely on admin to correctly configure OS
- Configuration drift over time
- Upgrades control the platform and limited parts of the node

# IMMUTABLE INFRASTRUCTURE

## OPENSIFT 3



## OPENSIFT 4



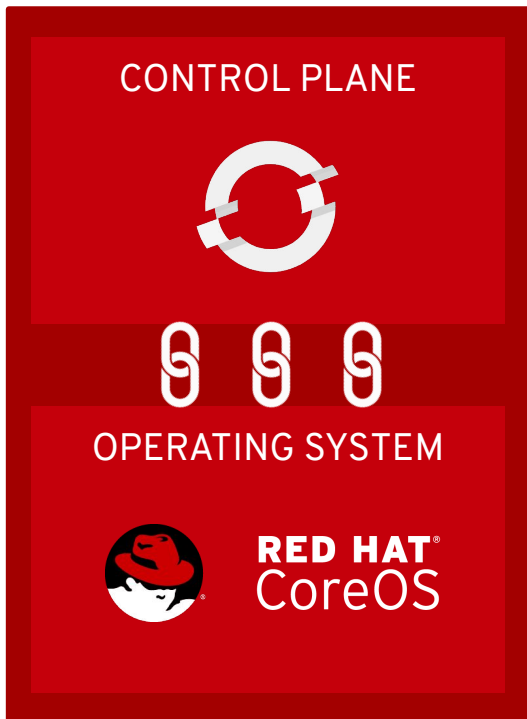
# IMMUTABLE INFRASTRUCTURE



For Day 2 management, the cluster needs full control over the nodes.



# IMMUTABLE INFRASTRUCTURE

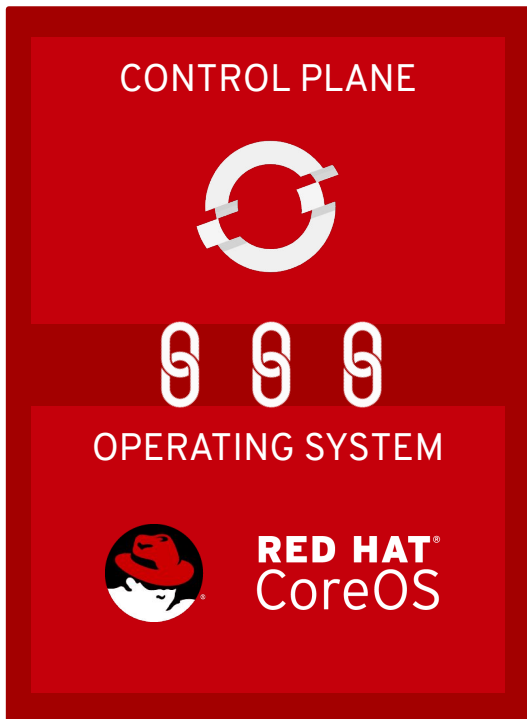


For Day 2 management, the cluster needs full control over the nodes.

Immutability  $\equiv$  repeatability

Immutability  $\equiv$  auditability

# IMMUTABLE INFRASTRUCTURE



For Day 2 management, the cluster needs full control over the nodes.

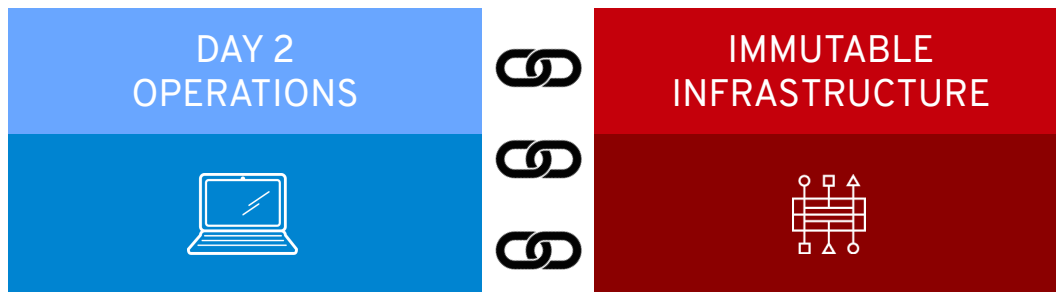
Immutability  $\equiv$  repeatability

Immutability  $\equiv$  auditability

Immutability  $\neq$  static clusters

Immutability  $\neq$  no config changes

# OPENS SHIFT 4.x THEMES

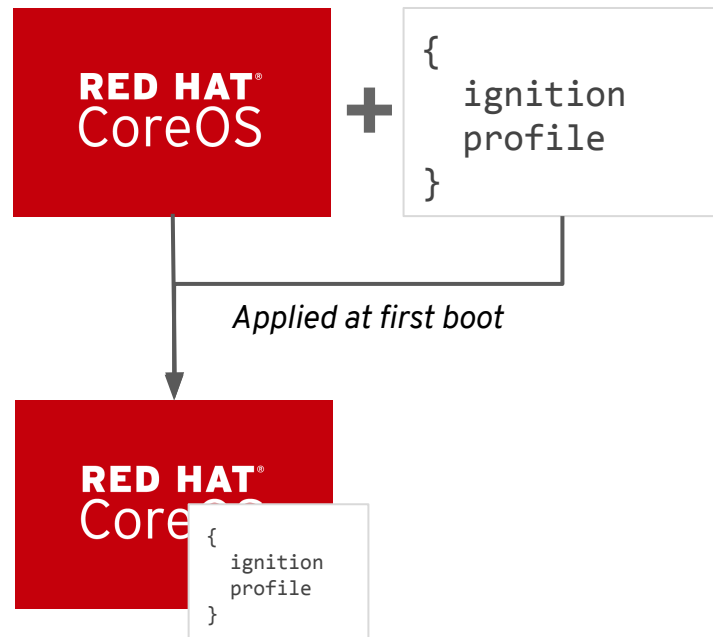


# INFRASTRUCTURE PROVISIONING

	OpenShift 3	OpenShift 4
User Provisioned Infrastructure	<b>Default</b>	Optional
Installer Provisioned Infrastructure	not possible	<b>Default</b>

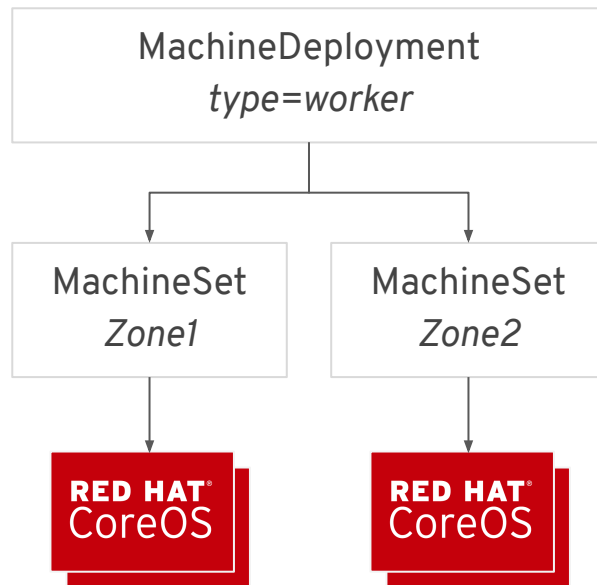
# MACHINE CONFIGURATION

- Red Hat CoreOS uses Ignition for configuration
- Ignition only runs once, on the first boot
- Ignition runs before systemd starts
  - Configure networking
  - Provision disks/RAID



# CLUSTER API OBJECTS

- New API objects to declaratively manage the cluster
  - MachineDeployment
  - MachineSet
  - Machine



RED HAT  
OPENSHIFT

Workloads

Networking

Storage

Builds

Monitoring

Administration

Cluster Settings

Namespaces

Nodes

Machine Deployments

Machine Sets

Machines

Service Accounts

Roles

Role Bindings

Resource Quotas

Limit Ranges

CRDs

console-openshift-console.apps.robszumski-0100.cloud.robszumski.com

kube:admin

You are logged in as a temporary administrative user.

Project: openshift-cluster-api

Add

Machines

Filter Machines by name...

NAME ↑	NAMESPACE	REGION	AVAILABILITY ZONE
M robszumski-0100-master-0	NS openshift-cluster-api	us-east-2	us-east-2a
M robszumski-0100-master-1	NS openshift-cluster-api	us-east-2	us-east-2b
M robszumski-0100-master-2	NS openshift-cluster-api	us-east-2	us-east-2c
M robszumski-0100-worker-us-east-2a-86wfh	NS openshift-cluster-api	us-east-2	us-east-2a
M robszumski-0100-worker-us-east-2b-sp8wx	NS openshift-cluster-api	us-east-2	us-east-2b
M robszumski-0100-worker-us-east-2c-vjfwf	NS openshift-cluster-api	us-east-2	us-east-2c

RED HAT  
OPENSIFT

Workloads

Networking

Storage

Builds

Monitoring

Administration

Cluster Settings

Namespaces

Nodes

Machine Deployments

Machine Sets

Machines

Service Accounts

Roles

Role Bindings

Resource Quotas

Limit Ranges

CRDs

console-openshift-console.apps.robszumski-0100.cloud.robszumski.com

kube:admin

You are logged in as a temporary administrative user.

Project: openshift-cluster-api

Add

Machine Sets

Create Machine Set

Filter Machine Sets by name...

NAME ↑	NAMESPACE	MACHINES
MS robszumski-0100-worker-us-east-2a	NS openshift-cluster-api	1 of 1 machines
MS robszumski-0100-worker-us-east-2b	NS openshift-cluster-api	1 of 1 machines
MS robszumski-0100-worker-us-east-2c	NS openshift-cluster-api	1 of 1 machines



console-openshift-console.apps.robszumski-0100.cloud.robszumski.com

kube:admin

Workloads

Networking

Storage

Builds

Monitoring

Administration

Cluster Settings

Namespaces

Nodes

Machine Deployments

Machine Sets

Machines

Service Accounts

Roles

Role Bindings

Resource Quotas

Limit Ranges

CRDs

You are logged in as a temporary administrative user.

Project: openshift-cluster-api

Machine Set Details

MS robszumski-0100-worker-us-east-2a

Actions

OverviewYAMLMachines

```
30 spec:
31   metadata:
32     creationTimestamp: null
33   providerSpec:
34     value:
35       userDataSecret:
36         name: worker-user-data
37       placement:
38         availabilityZone: us-east-2a
39         region: us-east-2
40       keyName: null
41       credentialsSecret: null
42       instanceType: m4.large
43     metadata:
44       creationTimestamp: null
45     publicIp: null
46     securityGroups:
47       - arn: null
48         filters:
49           - name: 'tag:Name'
50             values:
51               - robszumski-0100_worker_sg
52       id: null
53     kind: AWSMachineProviderConfig
54     loadBalancers: null
55     tags:
56       - name: openshiftClusterID
```

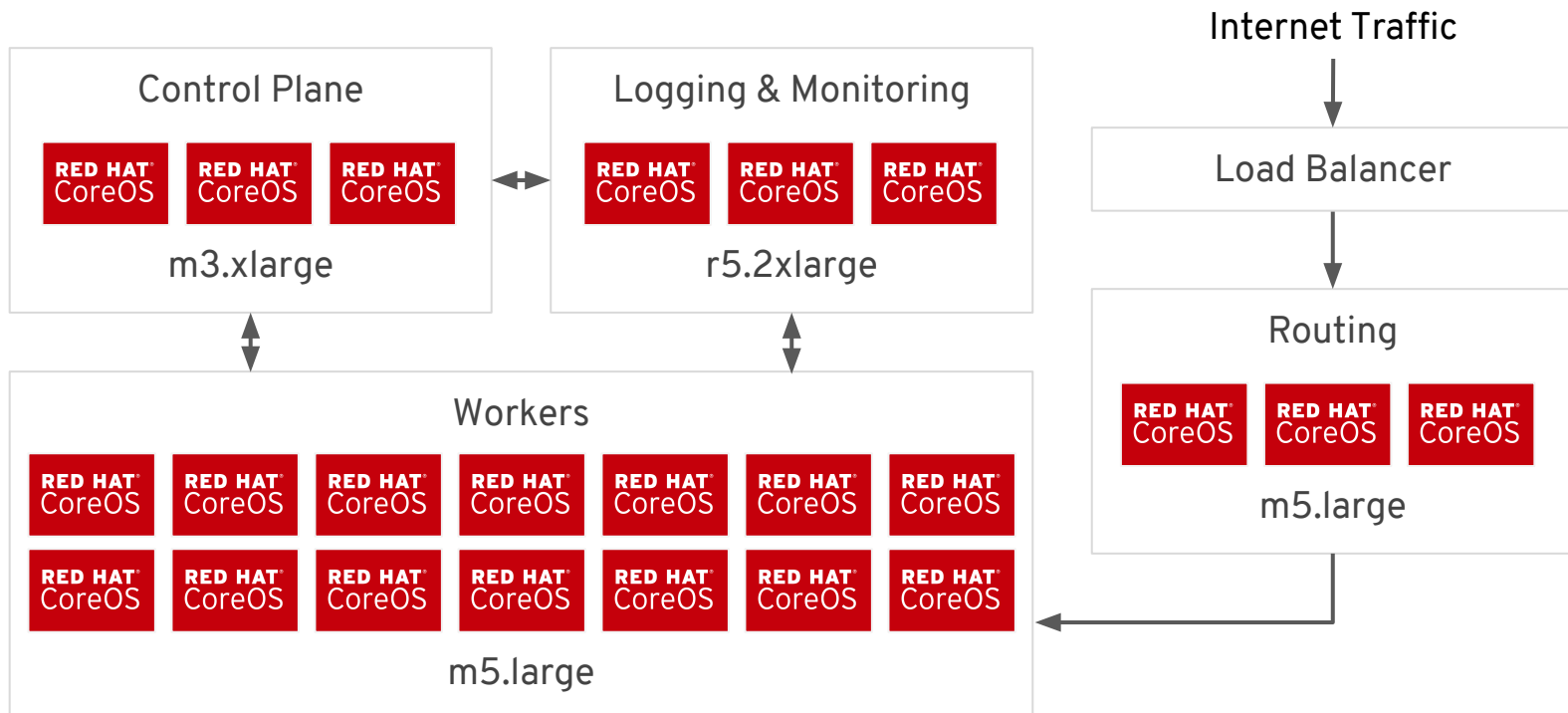
Save

Reload

Cancel

Download

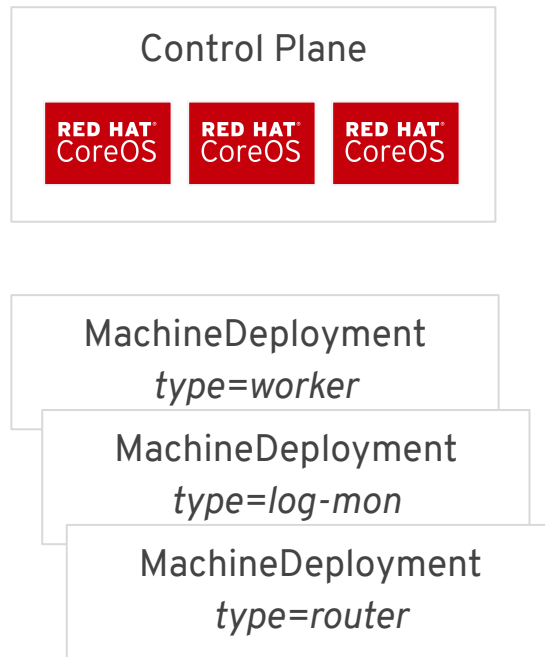
# POSSIBLE CLUSTER ARCHITECTURE



# CLUSTER ARCHITECTURE

- Scale Deployments independently
- Desired state managed by cluster
- Autoscale is no effort at all
- Rolling Machine config updates

Special GPU           = MachineDeployment  
Special security       = MachineDeployment  
Special \$anything   = MachineDeployment



# DAY 2 OPERATIONS




Machine Operators



Cluster Operators



Update Operators



Home Projects Status Search Events Catalog Workloads Networking Storage Builds Monitoring Administration Cluster Settings Namespaces Nodes Machine Deployments Machine Sets

console-openshift-console.apps.robszumski-0100.cloud.robszumski.com kube:admin

You are logged in as a temporary administrative user.

Cluster Settings

Overview Global Configuration Cluster Operators

Edit the following resources to manage the configuration of your cluster.

CONFIGURATION RESOURCE	
Authentication	Edit YAML
DNS	Edit YAML
Image	Edit YAML
Infrastructure	Edit YAML
Ingress	Edit YAML
OAuth	Edit YAML

console-openshift-console.apps.robszumski-0100.cloud.robszumski.com

RED HAT  
OPENSIFT

☰

Home

Projects

Status

Search

Events

Catalog

Workloads

Networking

Storage

Builds

Monitoring

Administration

Cluster Settings

Namespaces

Nodes

Machine Deployments

Machine Sets

kube:admin

You are logged in as a temporary administrative user.

Cluster Settings

















OverviewGlobal ConfigurationCluster Operators


Filter Cluster Operators by name...

12 Available0 Updating0 Failing0 Unknown

Select All Filters

12 Items

NAME ↑	STATUS	MESSAGE	VERSION
 cluster-autoscaler-operator	 Available	-	v4.0.0-0.139.0.0-dirty
 cluster-image-registry-operator	 Available	deployment has minimum availability	v4.0.0-0.136.0-dirty
 kube-controller-manager	 Available	3 of 3 nodes are at revision 2	Unknown
 machine-api-operator	 Available	cluster-api ready	v4.0.0-0.139.0.0-dirty
 machine-config-operator	 Available	-	4.0.0-0.139.0.0-dirty
 openshift-apiserer	 Available	-	Unknown
 openshift-cluster-kube-scheduler-operator	 Available	3 of 3 nodes are at revision 1	Unknown
 openshift-cluster-samples-operator	 Available	Samples installation successful at v4.0.0-0.139.0.0-17aa1e7fd	v4.0.0-0.139.0.0-17aa1e7fd



# Thank you !