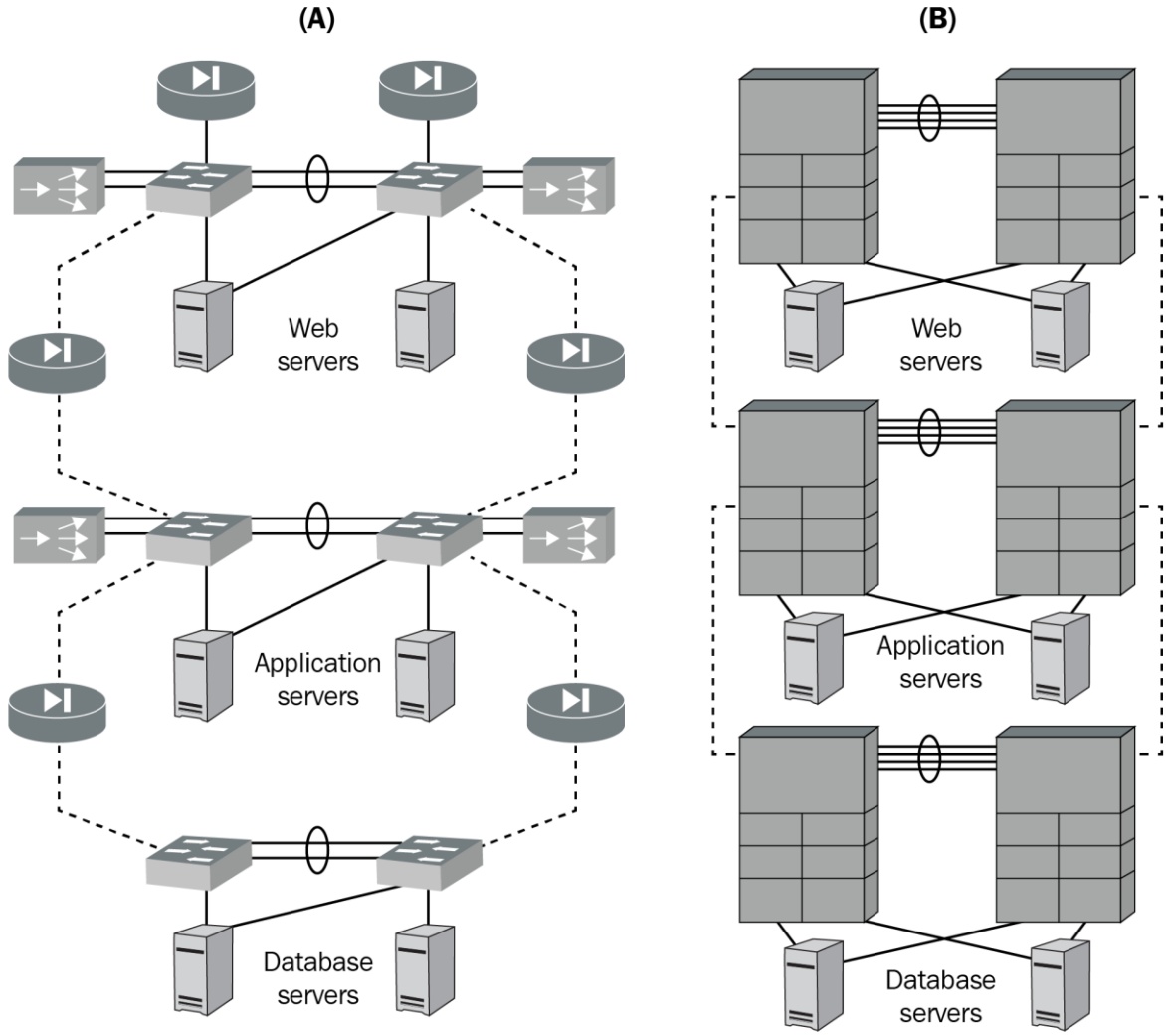
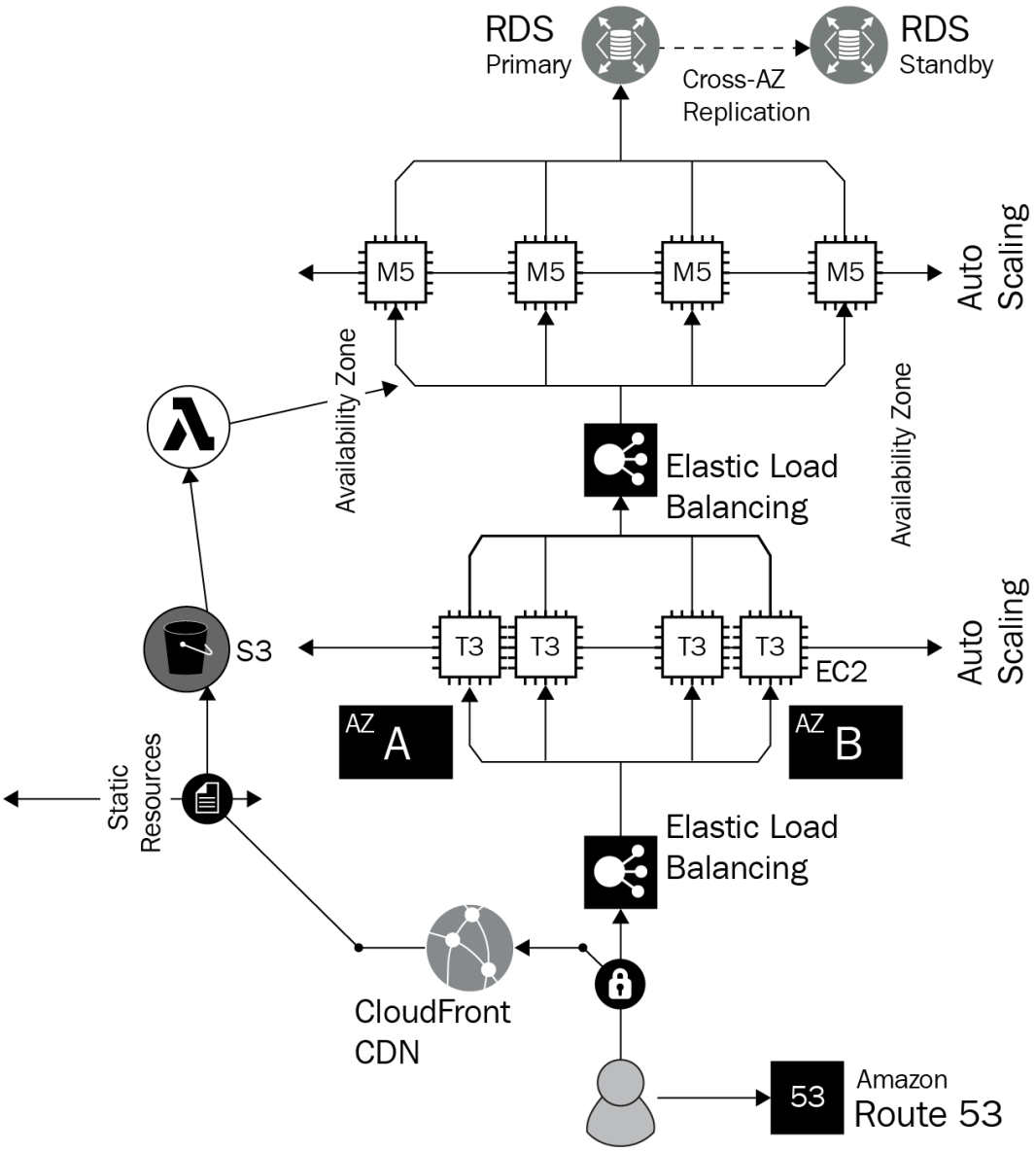
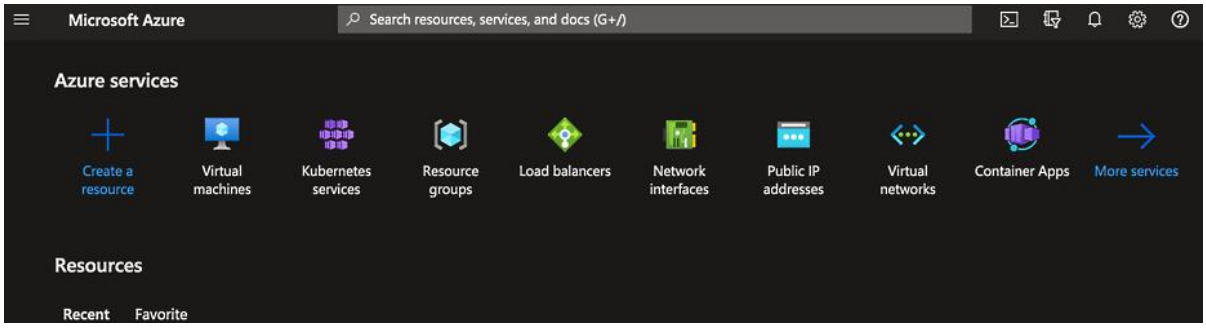
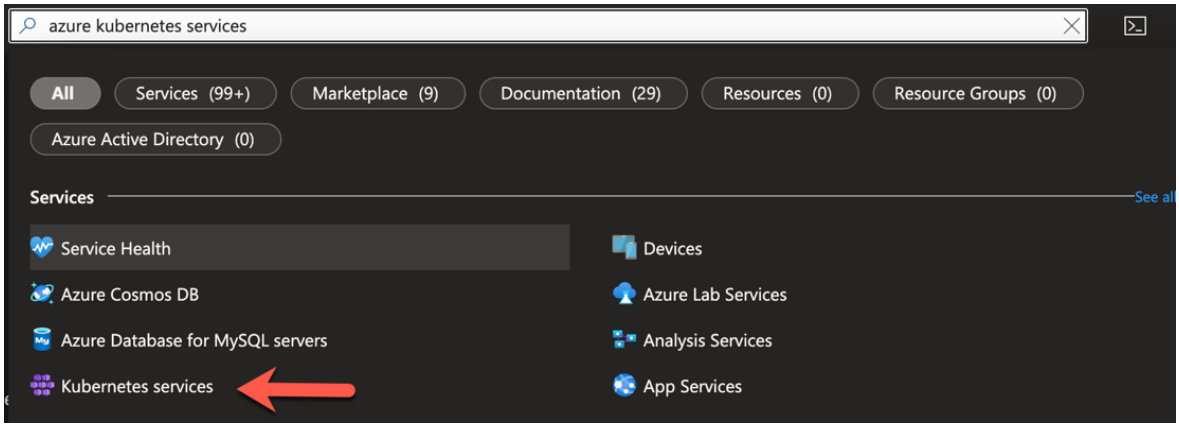
Chapter 1: Kubernetes in Today's World

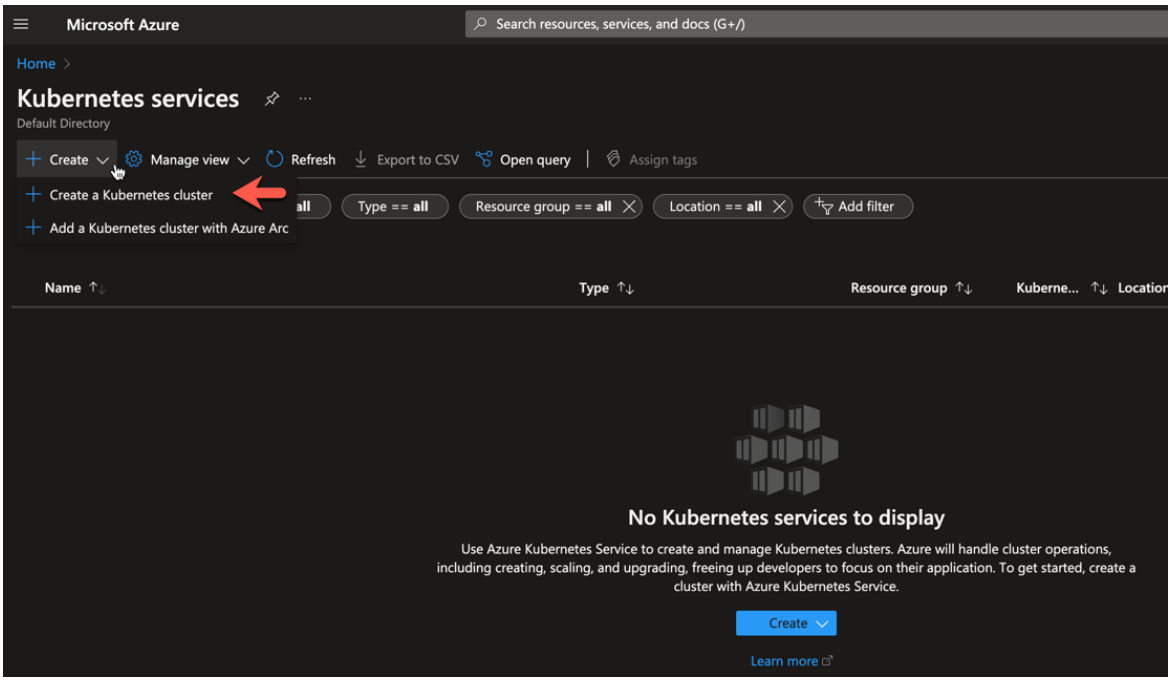


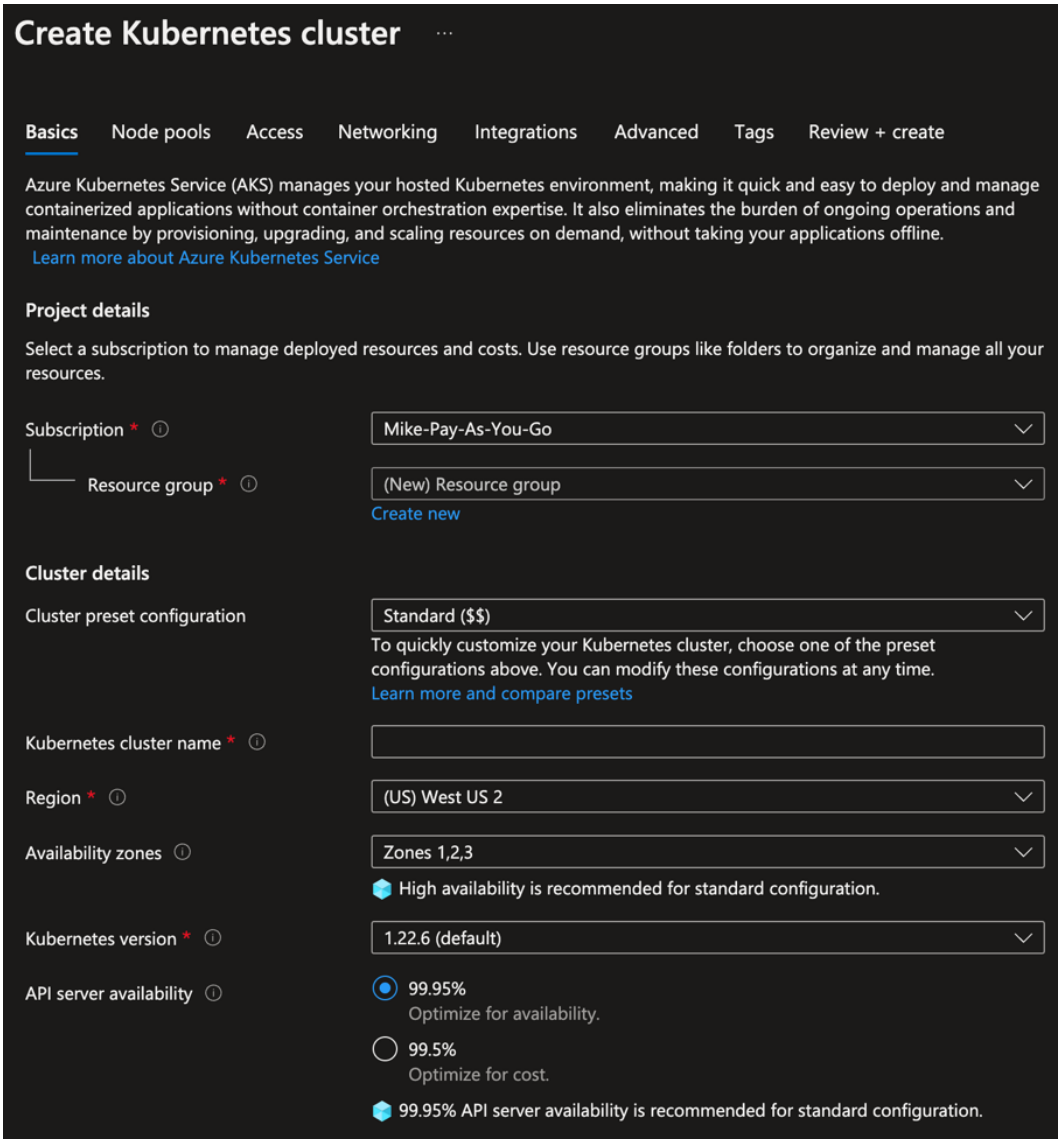

RDS
Primary
Cross-AZ
Replication
RDS
Standby
M5
M5
M5
M5
Auto
Scaling
Availability Zone
Availability Zone
Elastic Load
Balancing
S3
T3
T3
T3
T3
EC2
Auto
Scaling
AZ A
AZ B
Static
Resources
Elastic Load
Balancing
CloudFront
CDN
53
Amazon
Route 53

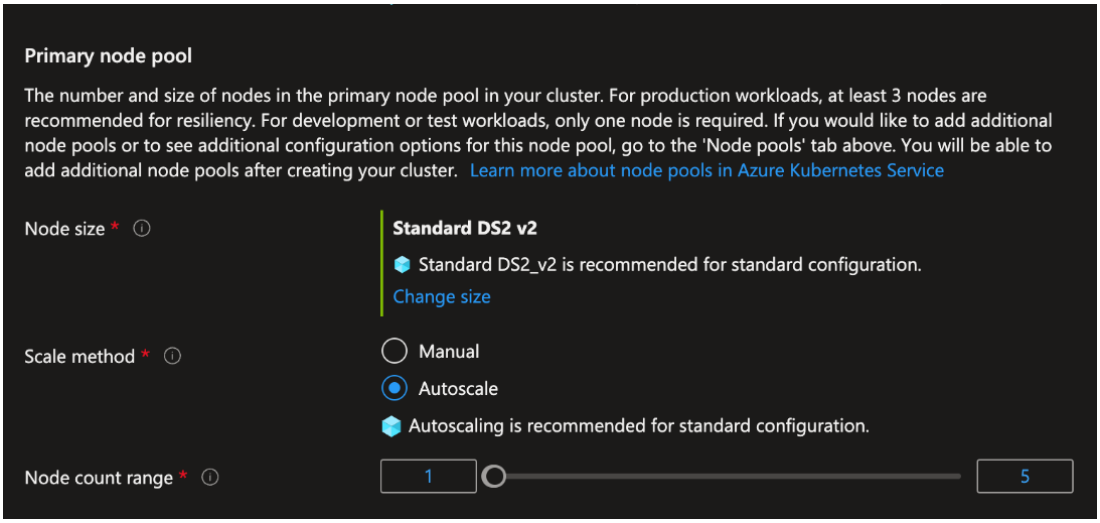
Chapter 2: Getting the Ball Rolling with Kubernetes and the Top Three Cloud Platforms

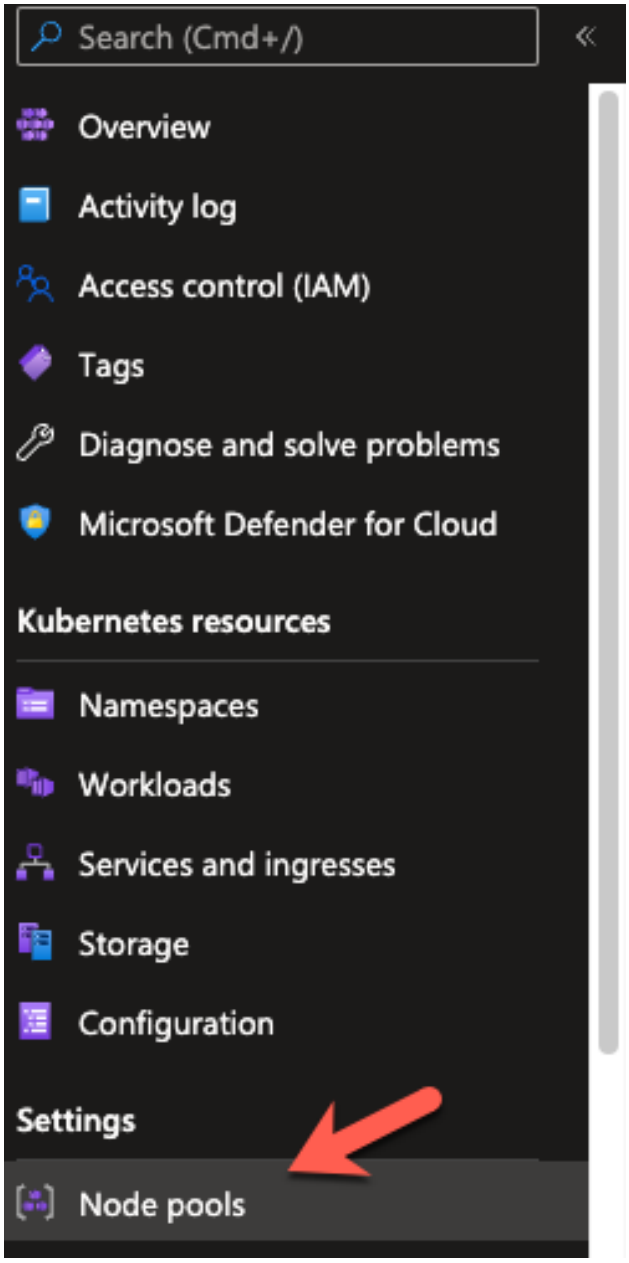


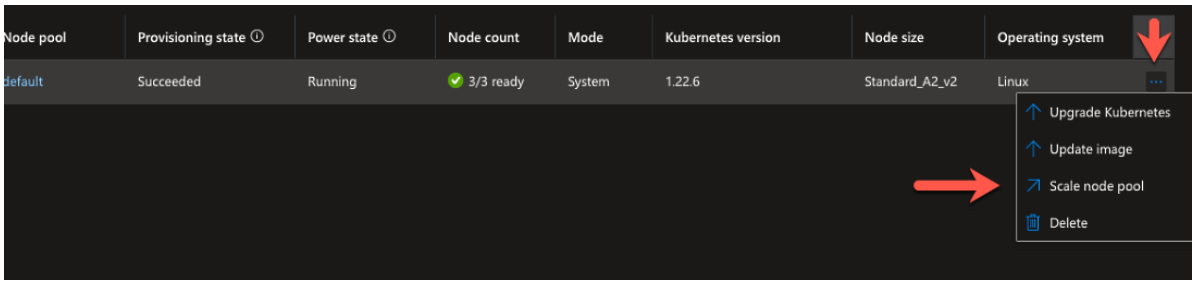


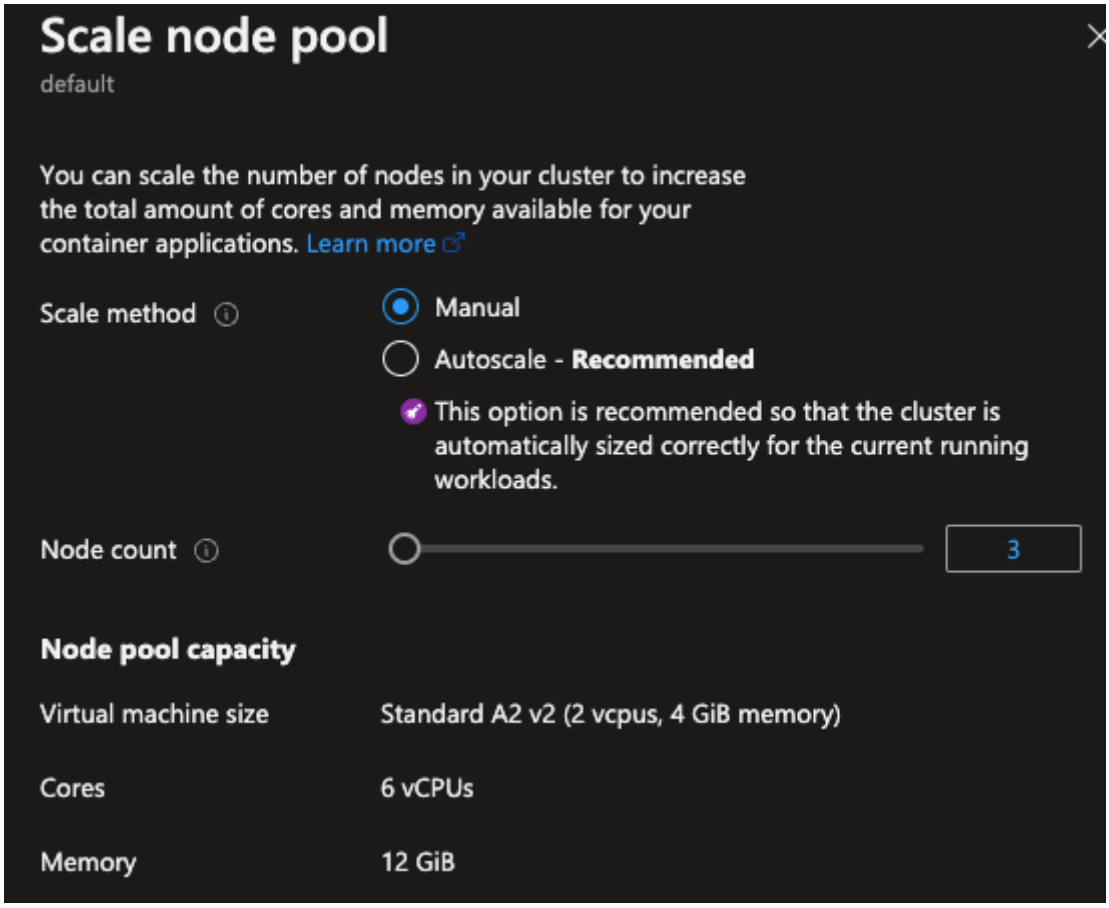


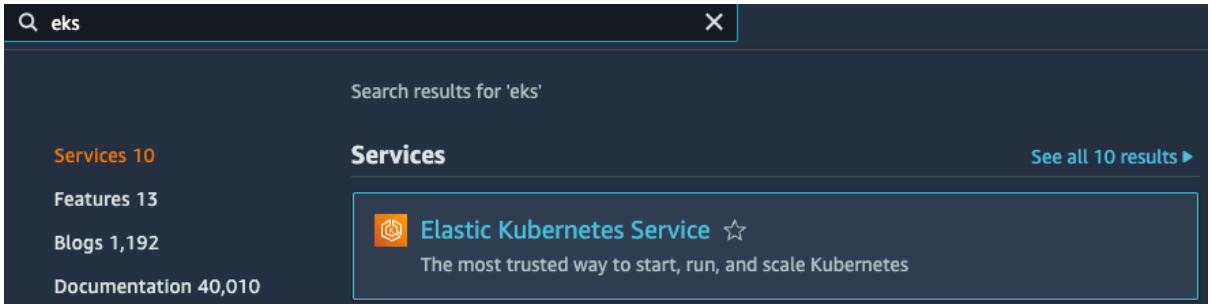

Create Kubernetes cluster
Basics
Node pools
Access
Networking
Integrations
Advanced
Tags
Review + create
Azure Kubernetes Service (AKS) manages your hosted Kubernetes environment, making it quick and easy to deploy and manage containerized applications without container orchestration expertise. It also eliminates the burden of ongoing operations and maintenance by provisioning, upgrading, and scaling resources on demand, without taking your applications offline.
Learn more about Azure Kubernetes Service
Project details
Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.
Subscription *
Mike-Pay-As-You-Go
Resource group *
(New) Resource group
Create new
Cluster details
Cluster preset configuration
Standard ($$)
To quickly customize your Kubernetes cluster, choose one of the preset configurations above. You can modify these configurations at any time.
Learn more and compare presets
Kubernetes cluster name *
Region *
(US) West US 2
Availability zones
Zones 1,2,3
High availability is recommended for standard configuration.
Kubernetes version *
1.22.6 (default)
API server availability
99.95%
Optimize for availability.
99.5%
Optimize for cost.
99.95% API server availability is recommended for standard configuration.

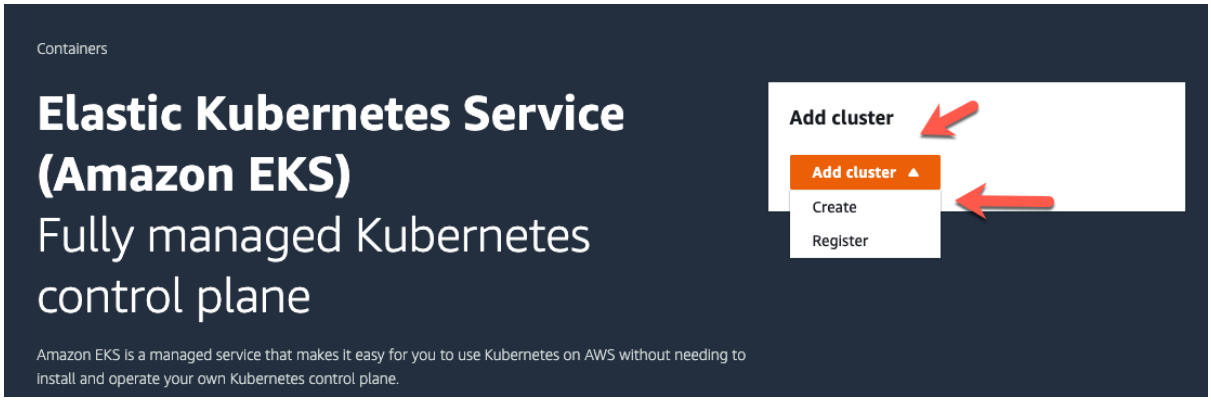

Primary node pool
The number and size of nodes in the primary node pool in your cluster. For production workloads, at least 3 nodes are recommended for resiliency. For development or test workloads, only one node is required. If you would like to add additional node pools or to see additional configuration options for this node pool, go to the 'Node pools' tab above. You will be able to add additional node pools after creating your cluster. Learn more about node pools in Azure Kubernetes Service
Node size *
Standard DS2 v2
Standard DS2_v2 is recommended for standard configuration.
Change size
Scale method *
Manual
Autoscale
Autoscaling is recommended for standard configuration.
Node count range *
1
5


Search (Cmd+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Microsoft Defender for Cloud
Kubernetes resources
Namespaces
Workloads
Services and ingresses
Storage
Configuration
Settings
Node pools


Node pool
Provisioning state
Power state
Node count
Mode
Kubernetes version
Node size
Operating system
default
Succeeded
Running
3/3 ready
System
1.22.6
Standard_A2_v2
Linux
Upgrade Kubernetes
Update image
Scale node pool
Delete


Scale node pool
default
You can scale the number of nodes in your cluster to increase the total amount of cores and memory available for your container applications. Learn more
Scale method
Manual
Autoscale - Recommended
This option is recommended so that the cluster is automatically sized correctly for the current running workloads.
Node count
3
Node pool capacity
Virtual machine size
Standard A2 v2 (2 vcpus, 4 GiB memory)
Cores
6 vCPUs
Memory
12 GiB


eks
Search results for 'eks'
Services 10
Features 13
Blogs 1,192
Documentation 40,010
Services
See all 10 results
Elastic Kubernetes Service
The most trusted way to start, run, and scale Kubernetes


Containers
Elastic Kubernetes Service (Amazon EKS)
Fully managed Kubernetes control plane
Amazon EKS is a managed service that makes it easy for you to use Kubernetes on AWS without needing to install and operate your own Kubernetes control plane.
Add cluster
Add cluster
Create
Register

Configure cluster

Cluster configuration Info

Name - *Not editable after creation.*
Enter a unique name for this cluster.

ekspackt01

Kubernetes version Info
Select the Kubernetes version for this cluster.

1.22

Cluster service role Info - *Not editable after creation.*
Select the IAM role to allow the Kubernetes control plane to manage AWS resources on your behalf. To create a new role, follow the instructions in the Amazon EKS User Guide.

eksmanagement1

Secrets encryption Info

Once enabled, secrets encryption cannot be modified or removed.

Enable envelope encryption of Kubernetes secrets using KMS
Enable envelope encryption to provide an additional layer of encryption for your Kubernetes secrets.

Tags (0) Info

This cluster does not have any tags.

Add tag

Remaining tags available to add: 50

Cancel Next

Specify networking

Networking Info

These properties cannot be changed after the cluster is created.

VPC Info

Select a VPC to use for your EKS cluster resources.To create a new VPC, go to the VPC console.

vpc-04954c29dd81de6f6 | MikeVPC

Subnets Info

Choose the subnets in your VPC where the control plane may place elastic network interfaces (ENIs) to facilitate communication with your cluster. To create a new subnet, go to the corresponding page in the VPC console.

Select subnets

subnet-07477bdefd5c5d09a

subnet-06881226c77590b02

subnet-029810ddf7bacd3cc

subnet-0fd98792cf3be9d7d

subnet-0b2a8935a65678b6d

Security groups Info

Choose the security groups to apply to the EKS-managed Elastic Network Interfaces that are created in your worker node subnets. To create a new security group, go to the corresponding page in the VPC console.

Select security groups

Choose cluster IP address family Info

Specify the IP address type for pods and services in your cluster.

- (•) IPv4
- ( ) IPv6

Configure Kubernetes service IP address range Info

Specify the range from which cluster services will receive IP addresses.

Cluster endpoint access Info

Configure access to the Kubernetes API server endpoint.

- (•) **Public**
  The cluster endpoint is accessible from outside of your VPC. Worker node traffic will leave your VPC to connect to the endpoint.
- ( ) **Public and private**
  The cluster endpoint is accessible from outside of your VPC. Worker node traffic to the endpoint will stay within your VPC.
- ( ) **Private**
  The cluster endpoint is only accessible through your VPC. Worker node traffic to the endpoint will stay within your VPC.

▶ **Advanced settings**

Networking add-ons

Configure add-ons that provide advanced networking functionalities on the cluster.

Amazon VPC CNI Info

Enable pod networking within your cluster.

Version

Select the version for this add-on.

v1.10.1-eksbuild.1

This add-on will use the IAM role of the node where it runs. You can change this add-on to use IAM roles for service accounts after cluster creation.

CoreDNS Info

Enable service discovery within your cluster.

Version

Select the version for this add-on.

v1.8.7-eksbuild.1

kube-proxy Info

Enable service networking within your cluster.

Version

Select the version for this add-on.

v1.22.6-eksbuild.1

Cancel Previous Next

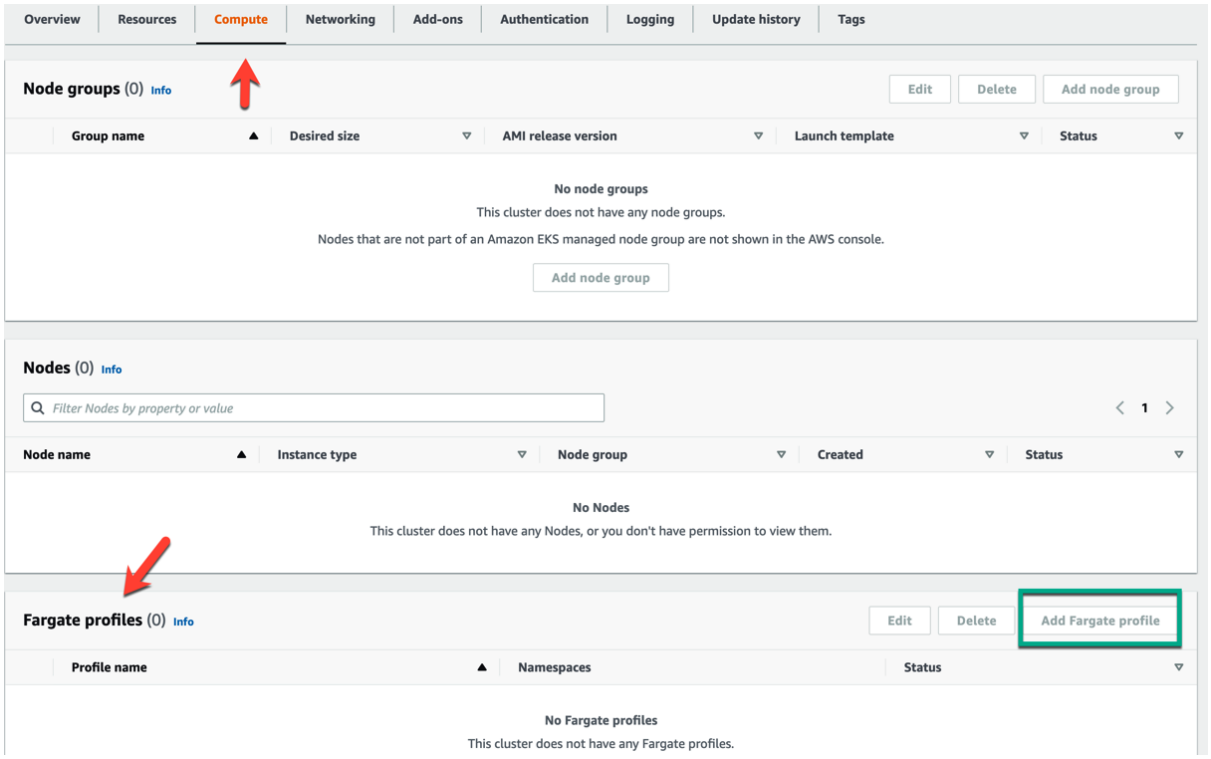
Configure logging

Control plane logging Info

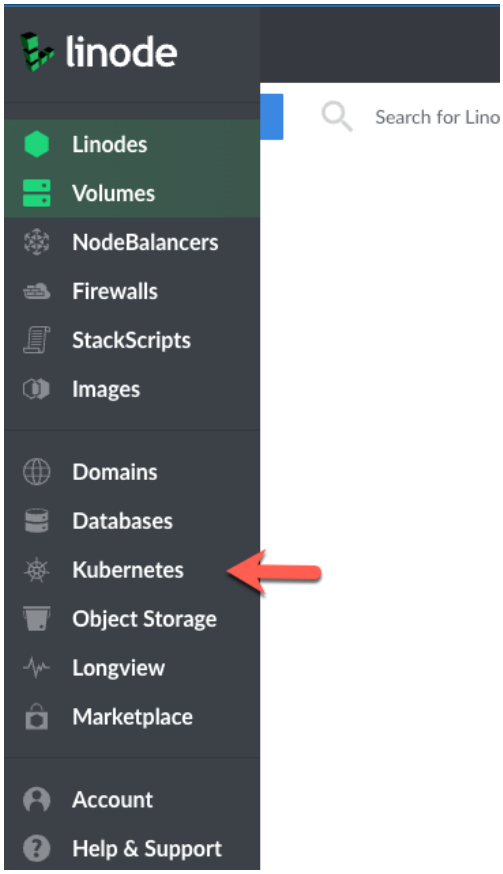
Send audit and diagnostic logs from the Amazon EKS control plane to CloudWatch Logs.

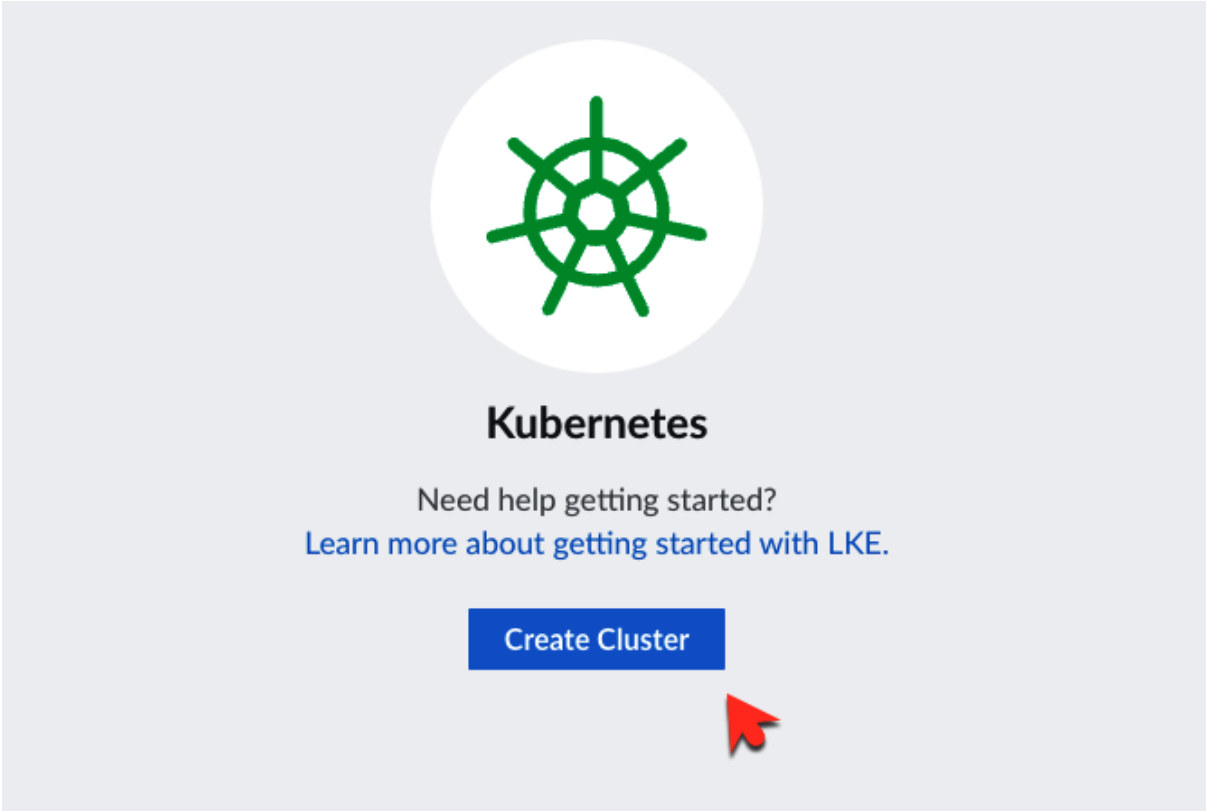
- API server
  Logs pertaining to API requests to the cluster.
- Audit
  Logs pertaining to cluster access via the Kubernetes API.
- Authenticator
  Logs pertaining to authentication requests into the cluster.
- Controller manager
  Logs pertaining to state of cluster controllers.
- Scheduler
  Logs pertaining to scheduling decisions.

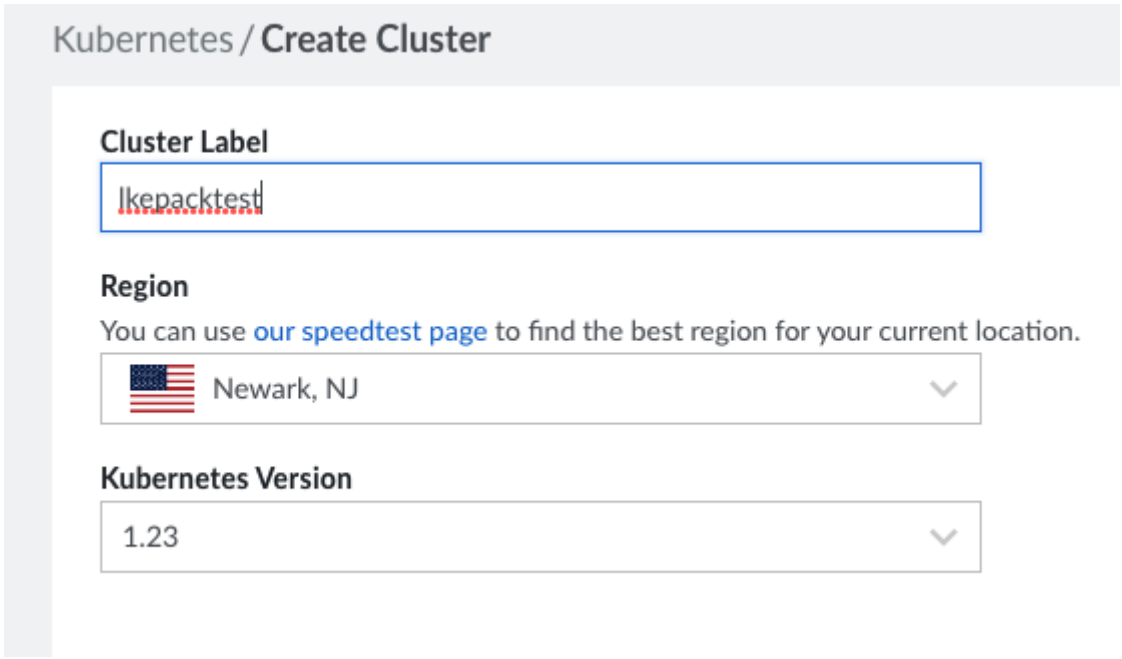
Cancel Previous Next


Overview
Resources
Compute
Networking
Add-ons
Authentication
Logging
Update history
Tags
Node groups (0) Info
Edit
Delete
Add node group
Group name
Desired size
AMI release version
Launch template
Status
No node groups
This cluster does not have any node groups.
Nodes that are not part of an Amazon EKS managed node group are not shown in the AWS console.
Add node group
Nodes (0) Info
Filter Nodes by property or value
1
Node name
Instance type
Node group
Created
Status
No Nodes
This cluster does not have any Nodes, or you don't have permission to view them.
Fargate profiles (0) Info
Edit
Delete
Add Fargate profile
Profile name
Namespaces
Status
No Fargate profiles
This cluster does not have any Fargate profiles.

Chapter 3: Running Kubernetes with Other Cloud Pals







Add Node Pools

Add groups of Linodes to your cluster. You can have a maximum of 100 Linodes per node pool.

Dedicated CPU | Shared CPU | High Memory

Dedicated CPU instances are good for full-duty workloads where consistent performance is important.

Plan	Monthly	Hourly	RAM	CPUs	Storage				
Dedicated 4 GB	$30	$0.045	4 GB	2	80 GB	−	3	+	Add
Dedicated 8 GB	$60	$0.09	8 GB	4	160 GB	−	3	+	Add
Dedicated 16 GB	$120	$0.18	16 GB	8	320 GB	−	3	+	Add
Dedicated 32 GB	$240	$0.36	32 GB	16	640 GB	−	3	+	Add
Dedicated 64 GB	$480	$0.72	64 GB	32	1280 GB	−	3	+	Add
Dedicated 96 GB	$720	$1.08	96 GB	48	1920 GB	−	3	+	Add
Dedicated 128 GB	$960	$1.44	128 GB	50	2500 GB	−	3	+	Add
Dedicated 256 GB	$1920	$2.88	256 GB	56	5000 GB	−	3	+	Add
Dedicated 512 GB	$3840	$5.76	512 GB	64	7200 GB	−	3	+	Add

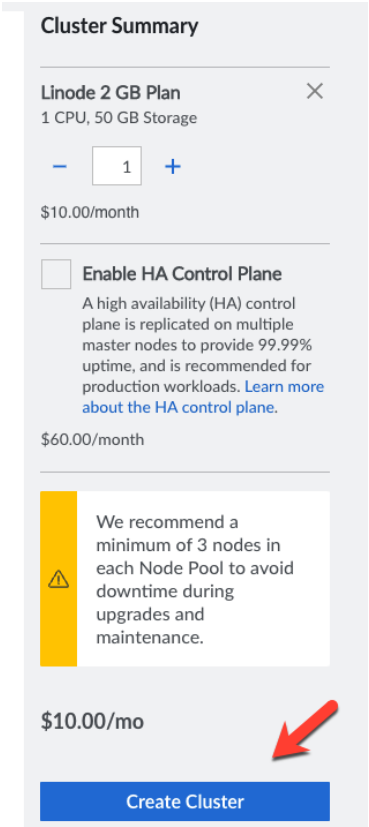
Add Node Pools

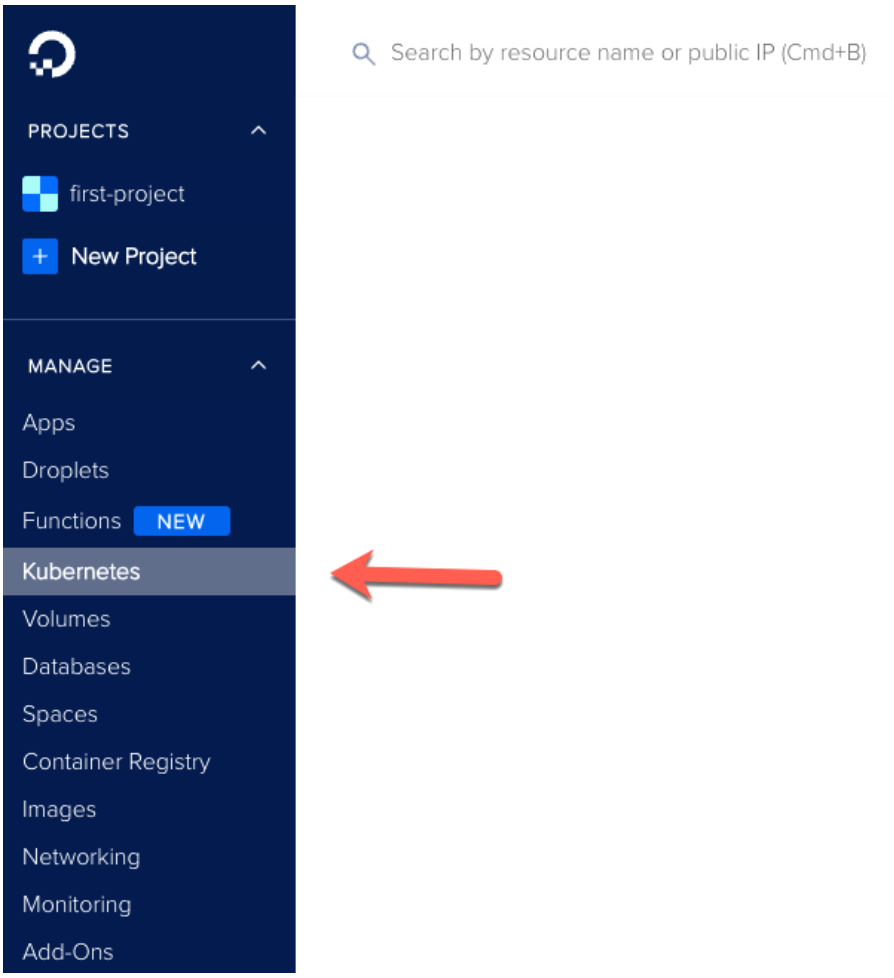
Add groups of Linodes to your cluster. You can have a maximum of 100 Linodes per node pool.

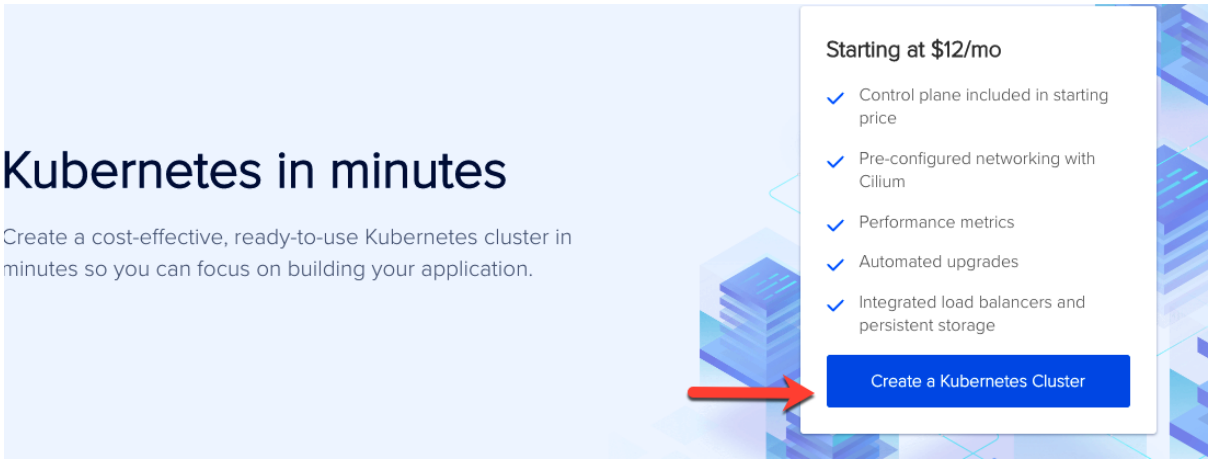
Dedicated CPU | **Shared CPU** | High Memory

Shared CPU instances are good for medium-duty workloads and are a good mix of performance, resources, and price.

Plan	Monthly	Hourly	RAM	CPUs	Storage				
Linode 2 GB	$10	$0.015	2 GB	1	50 GB	−	1	+	Add


Cluster Summary
Linode 2 GB Plan
1 CPU, 50 GB Storage
1
$10.00/month
Enable HA Control Plane
A high availability (HA) control plane is replicated on multiple master nodes to provide 99.99% uptime, and is recommended for production workloads. Learn more about the HA control plane.
$60.00/month
We recommend a minimum of 3 nodes in each Node Pool to avoid downtime during upgrades and maintenance.
$10.00/mo
Create Cluster


Search by resource name or public IP (Cmd+B)
PROJECTS
first-project
New Project
MANAGE
Apps
Droplets
Functions
NEW
Kubernetes
Volumes
Databases
Spaces
Container Registry
Images
Networking
Monitoring
Add-Ons



Create a Kubernetes cluster

Choose a datacenter region

Your Kubernetes cluster will be located in a single datacenter.

New York NYC1

VPC network

default-nyc1 DEFAULT

All resources created in this datacenter will be members of the same VPC network.
They can communicate securely over their Private IP addresses. What does this mean?

Select a version

Select the Kubernetes version. The newest available version is selected by default.

1.22.11-do.0 - Recommended

Tip: We generally recommend the latest version unless your team has a specific need.
See the DigitalOcean Kubernetes release notes

Choose cluster capacity

Select a plan that best suits your workload type. We can help you choose the right sizing approach for overall availability and performance. You can add or remove nodes and node pools at any time.

Important: You have reached the 3 Droplet limit on your account. Request Increase

Node pool name

pool-19kf594uk

Node plan

$24/month per node ($0.036/hour)
2.5 GB RAM usable (4 GB Total) / 2 vCPUs

Machine type (Droplet)

Basic nodes
Variable ratio of memory per shared CPU

Basic nodes
Variable ratio of memory per shared CPU

Basic nodes (Premium Intel)
Variable ratio of memory per shared CPU

Basic nodes (Premium AMD)
Variable ratio of memory per shared CPU

Add Another Node Pool

Add extra reliability to critical workloads

A high availability control plane creates multiple replicas of control plane components which eliminates a single point of failure and helps reduce downtime. You can **not** disable this option after the cluster is created.

☐ **Create cluster on a high availability control plane** **$40/month** ($0.06/hour)

MONTHLY RATE

$72/month ($0.11/hour)

Finalize

You can change the cluster's name, project, and tags at any time.

Name*
Can only contain lowercase alphanumeric characters and dashes.

k8s-1-22-11-do-0-nyc1-1657276272558

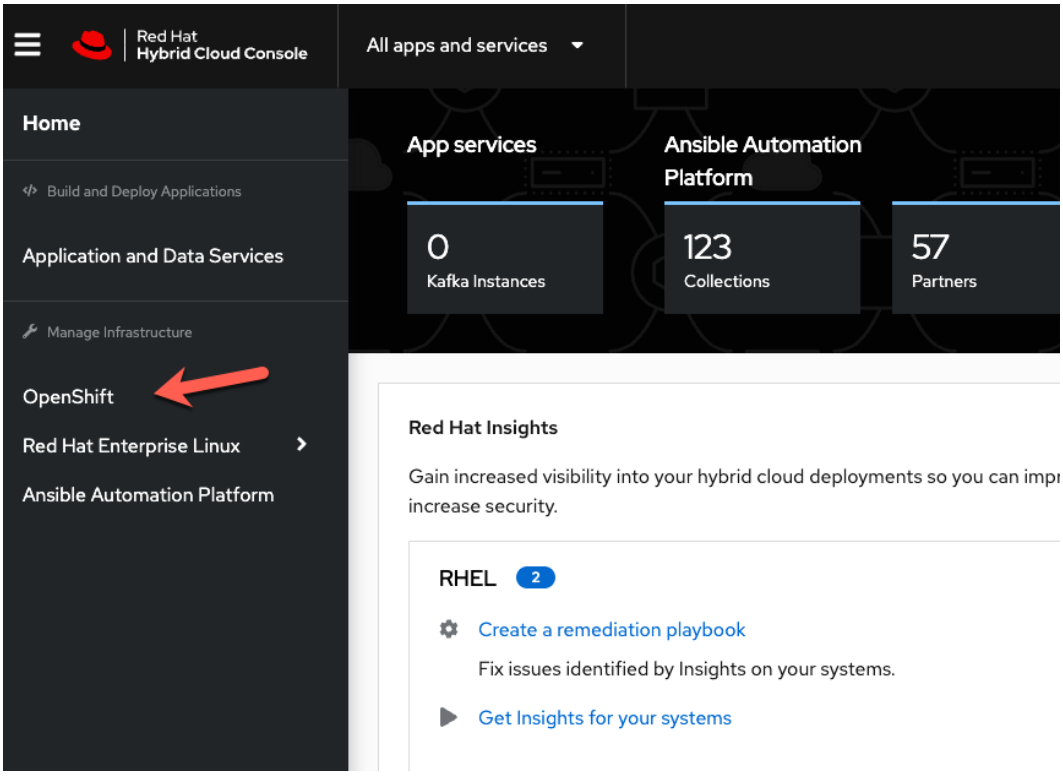
Project

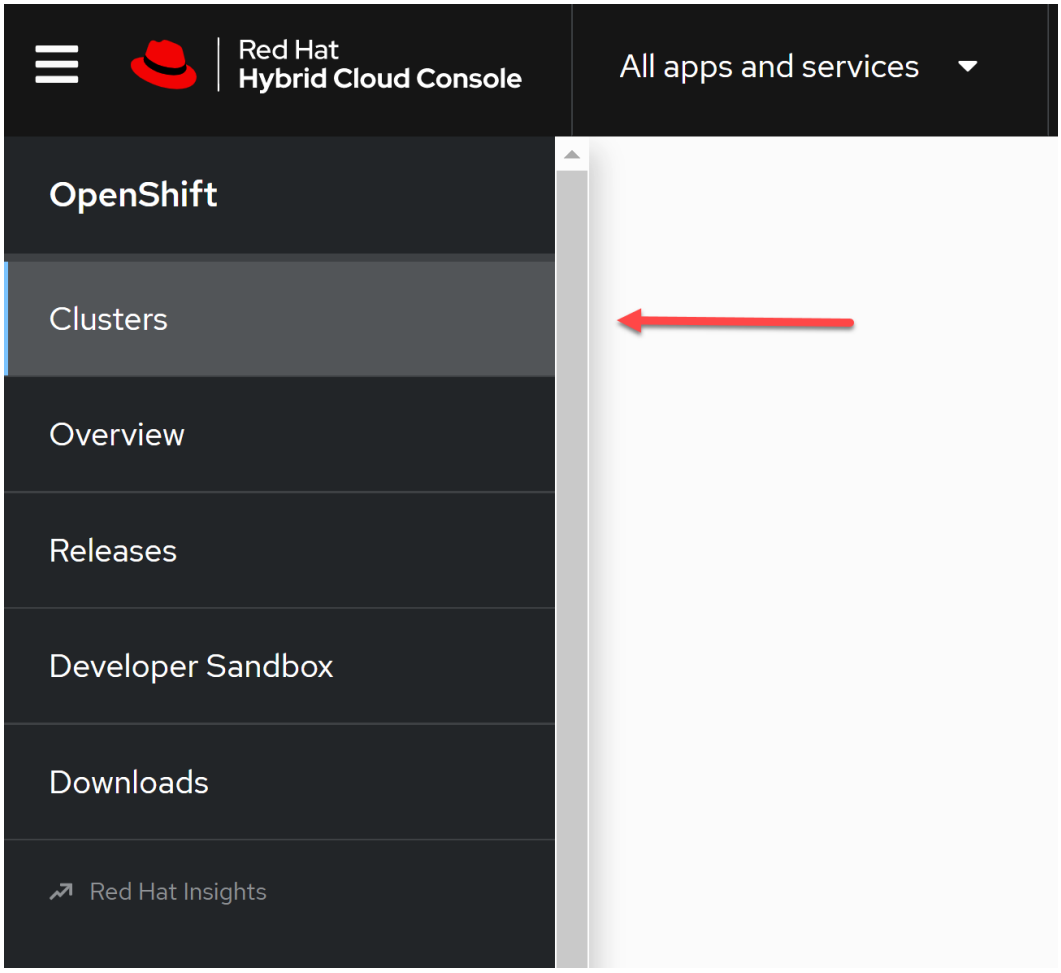
first-project

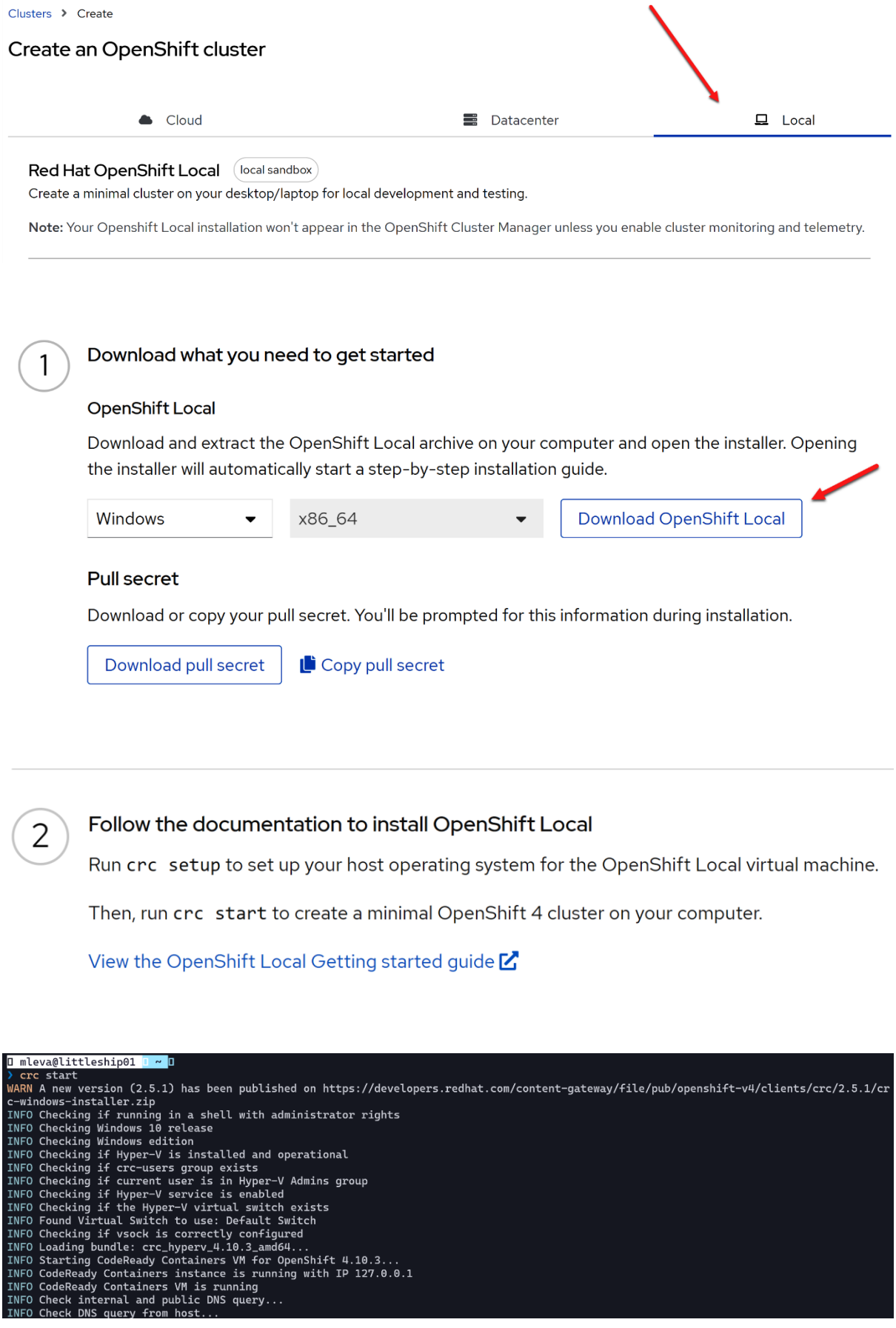
Tags

Use tags to organize and relate resources. They are not added as labels or taints to the cluster. Tags may contain letters, numbers, colons, dashes, and underscores.

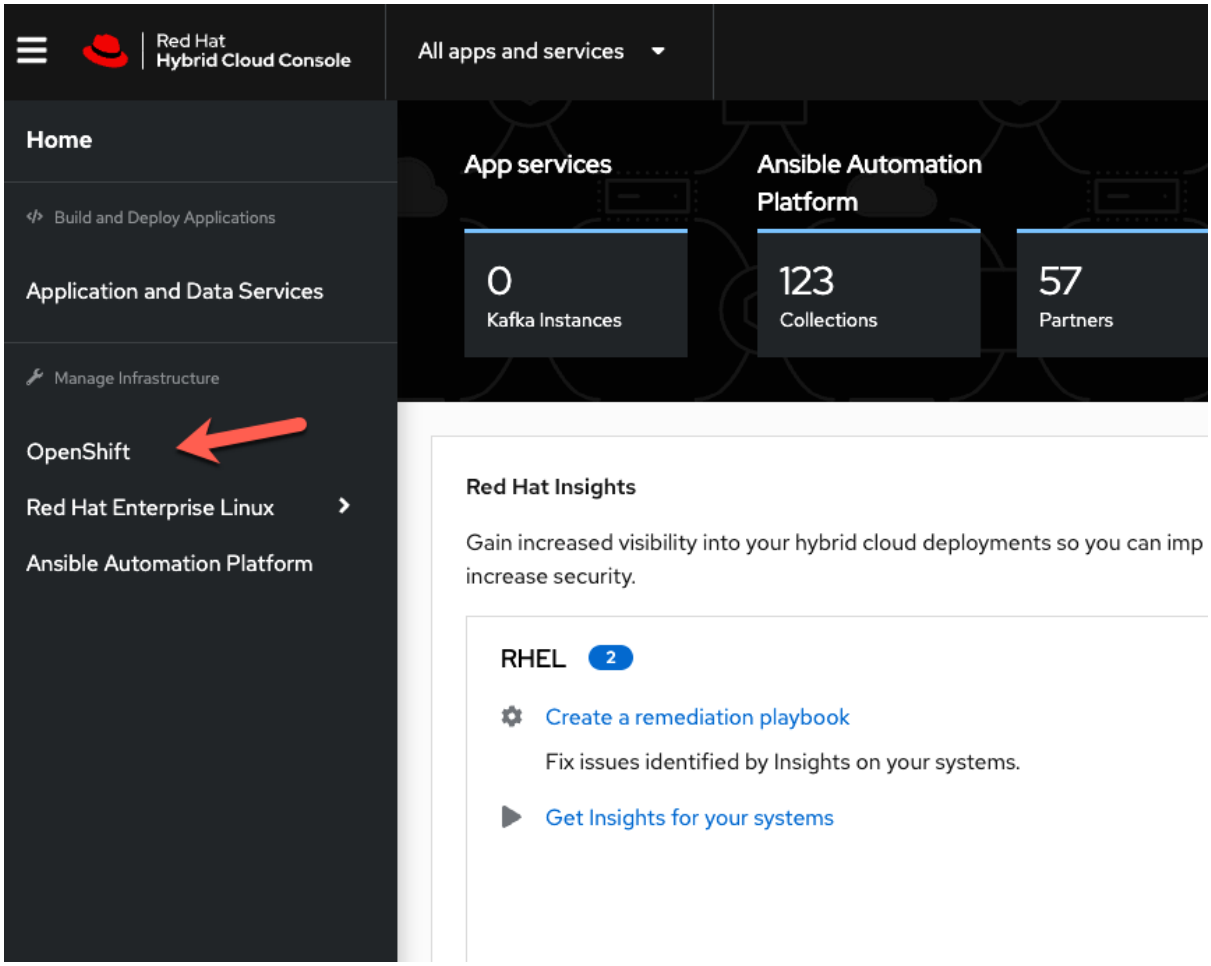
Create Cluster

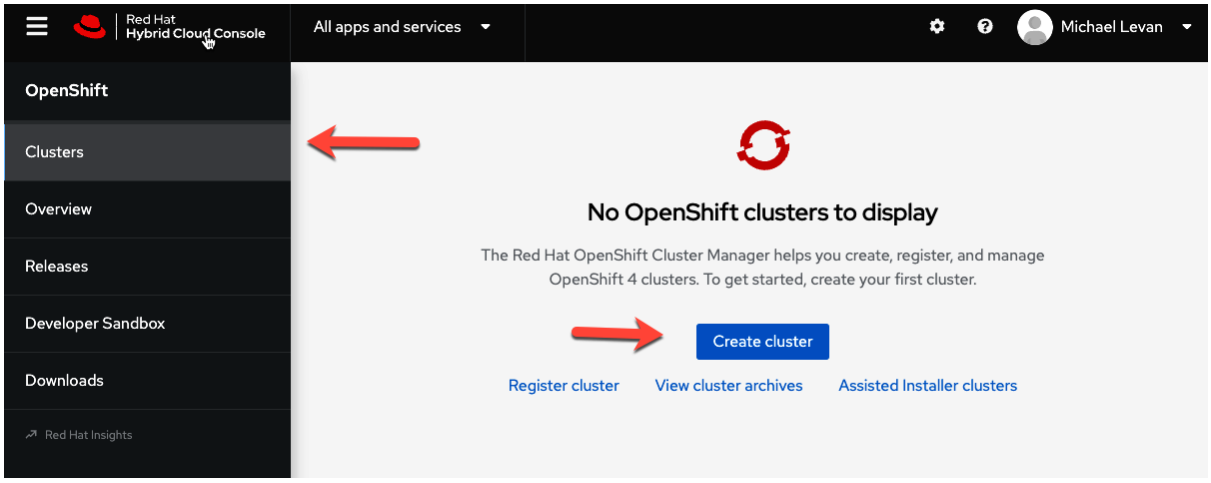

Red Hat
Hybrid Cloud Console
All apps and services
Home
Build and Deploy Applications
Application and Data Services
Manage Infrastructure
OpenShift
Red Hat Enterprise Linux
Ansible Automation Platform
App services
0
Kafka Instances
Ansible Automation Platform
123
Collections
57
Partners
Red Hat Insights
Gain increased visibility into your hybrid cloud deployments so you can impr
increase security.
RHEL
2
Create a remediation playbook
Fix issues identified by Insights on your systems.
Get Insights for your systems

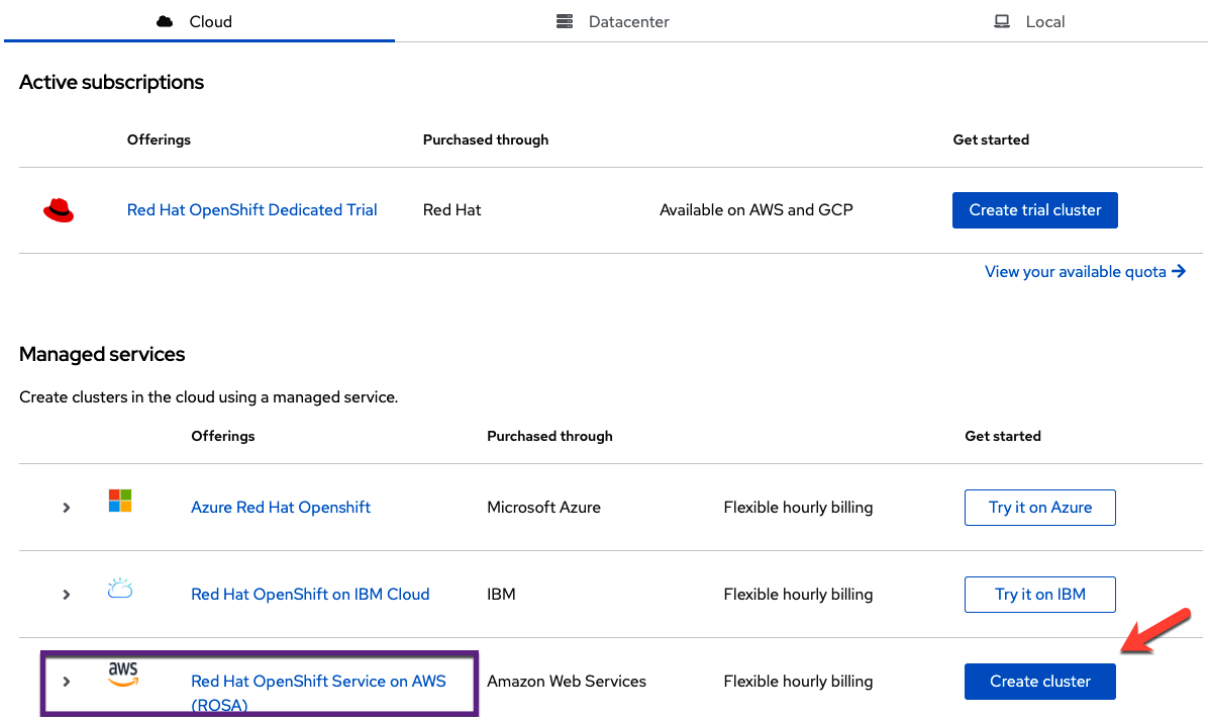

Red Hat
Hybrid Cloud Console
All apps and services
OpenShift
Clusters
Overview
Releases
Developer Sandbox
Downloads
Red Hat Insights

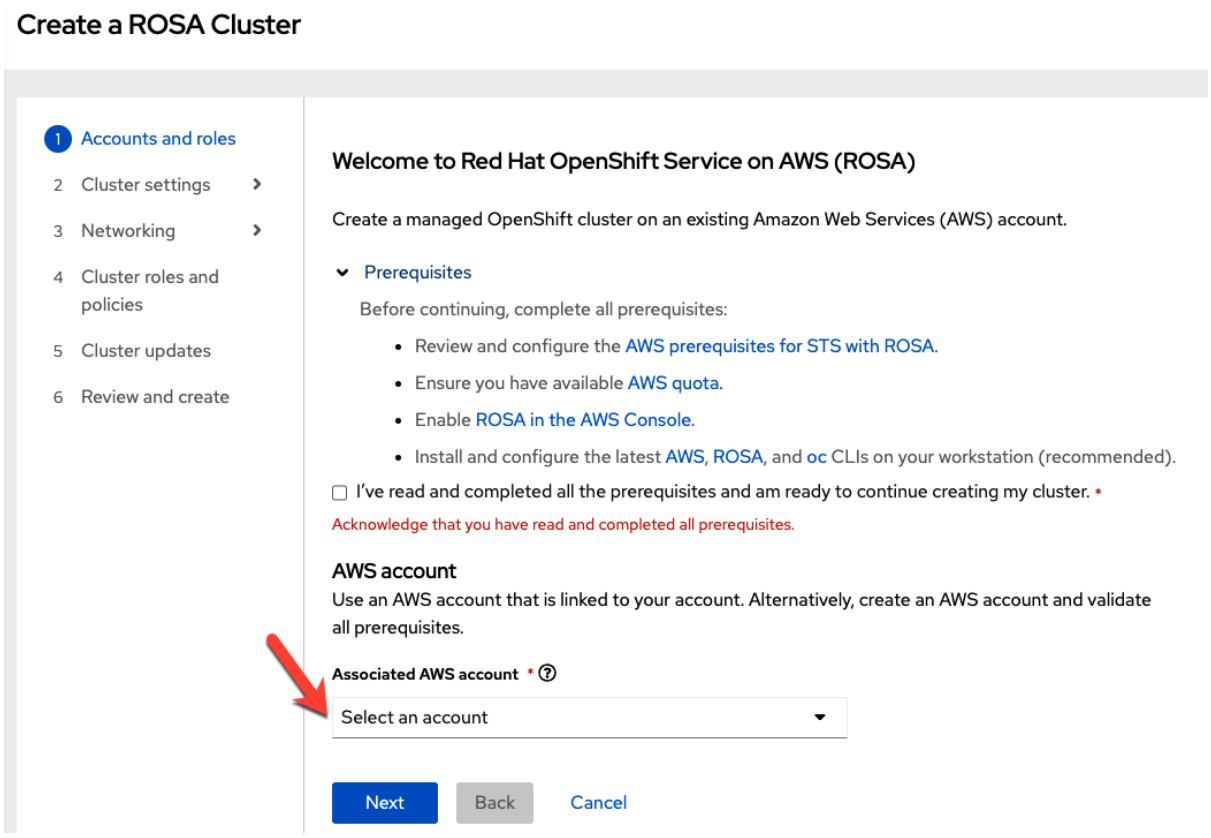


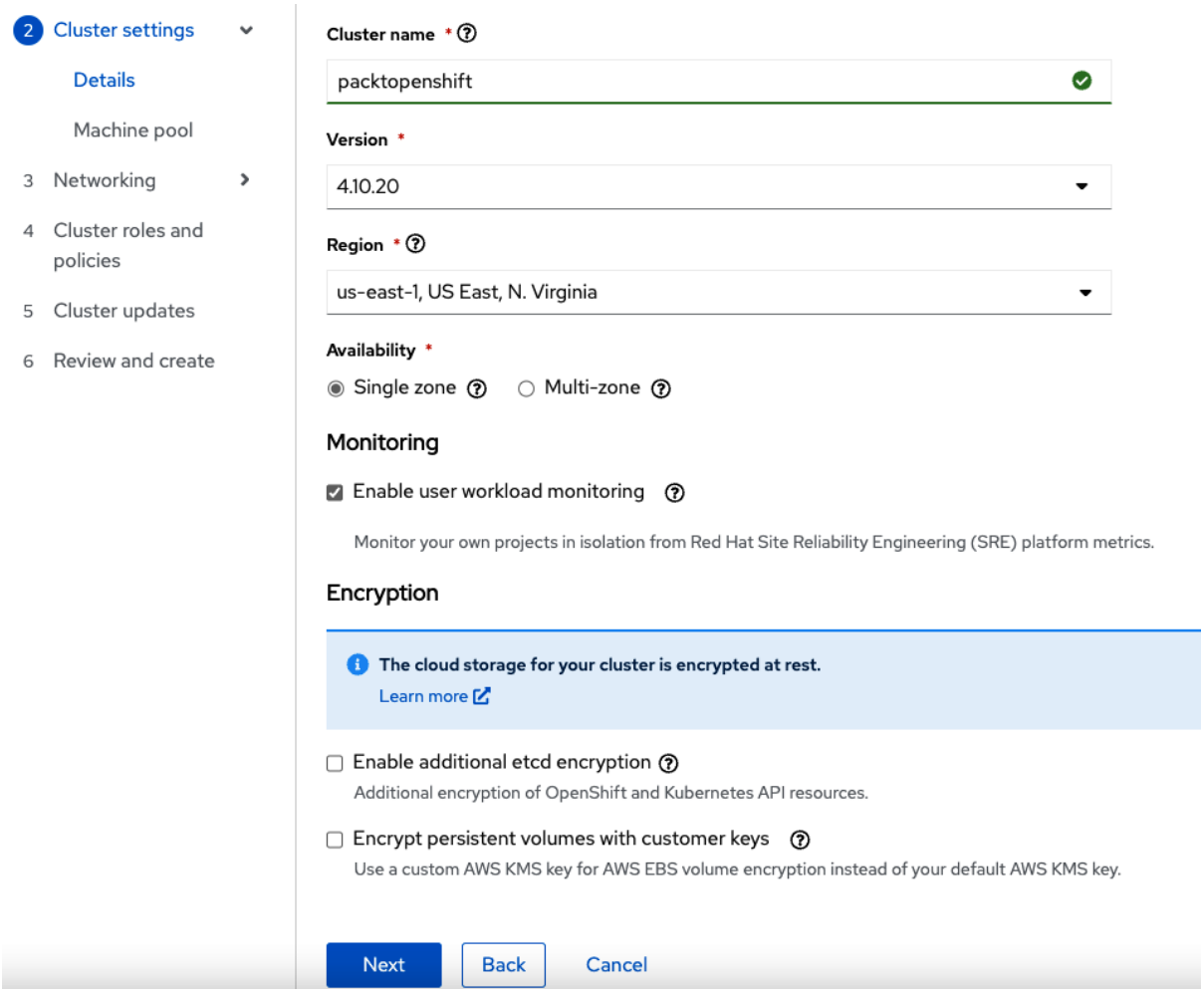

```
mleva@littleship01 ~
> crc start
WARN A new version (2.5.1) has been published on https://developers.redhat.com/content-gateway/file/pub/openshift-v4/clients/crc/2.5.1/crc-windows-installer.zip
INFO Checking if running in a shell with administrator rights
INFO Checking Windows 10 release
INFO Checking Windows edition
INFO Checking if Hyper-V is installed and operational
INFO Checking if crc-users group exists
INFO Checking if current user is in Hyper-V Admins group
INFO Checking if Hyper-V service is enabled
INFO Checking if the Hyper-V virtual switch exists
INFO Found Virtual Switch to use: Default Switch
INFO Checking if vsock is correctly configured
INFO Loading bundle: crc_hyperv_4.10.3_amd64...
INFO Starting CodeReady Containers VM for OpenShift 4.10.3...
INFO CodeReady Containers instance is running with IP 127.0.0.1
INFO CodeReady Containers VM is running
INFO Check internal and public DNS query...
INFO Check DNS query from host...
```

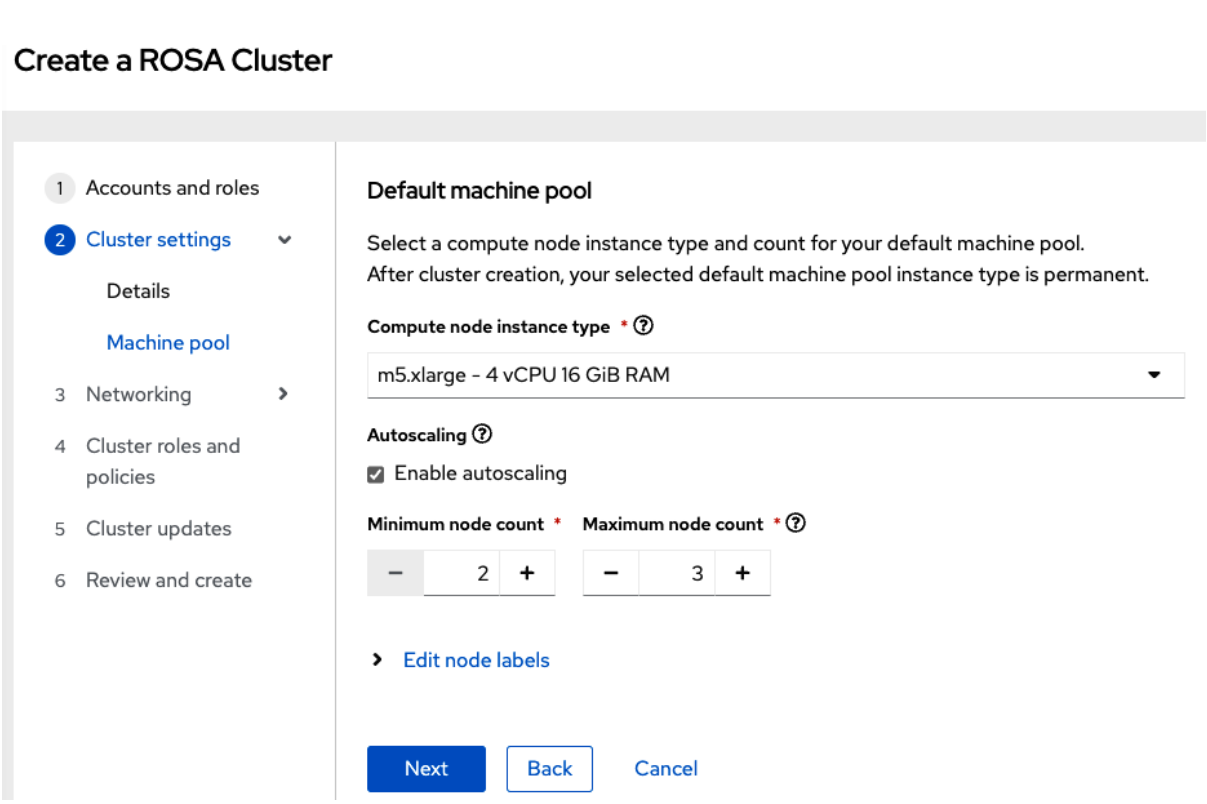

Red Hat
Hybrid Cloud Console
All apps and services
Home
Build and Deploy Applications
Application and Data Services
Manage Infrastructure
OpenShift
Red Hat Enterprise Linux
Ansible Automation Platform
App services
Ansible Automation Platform
0
Kafka Instances
123
Collections
57
Partners
Red Hat Insights
Gain increased visibility into your hybrid cloud deployments so you can imp
increase security.
RHEL
2
Create a remediation playbook
Fix issues identified by Insights on your systems.
Get Insights for your systems

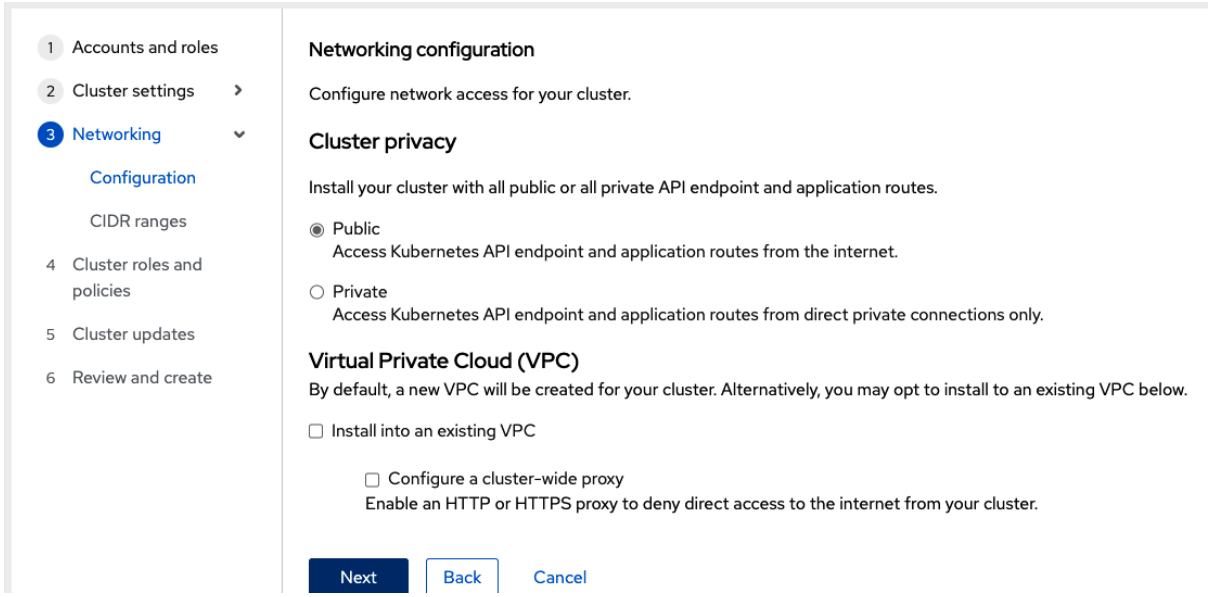

Red Hat
Hybrid Cloud Console
All apps and services
Michael Levan
OpenShift
Clusters
Overview
Releases
Developer Sandbox
Downloads
Red Hat Insights
No OpenShift clusters to display
The Red Hat OpenShift Cluster Manager helps you create, register, and manage
OpenShift 4 clusters. To get started, create your first cluster.
Create cluster
Register cluster
View cluster archives
Assisted Installer clusters

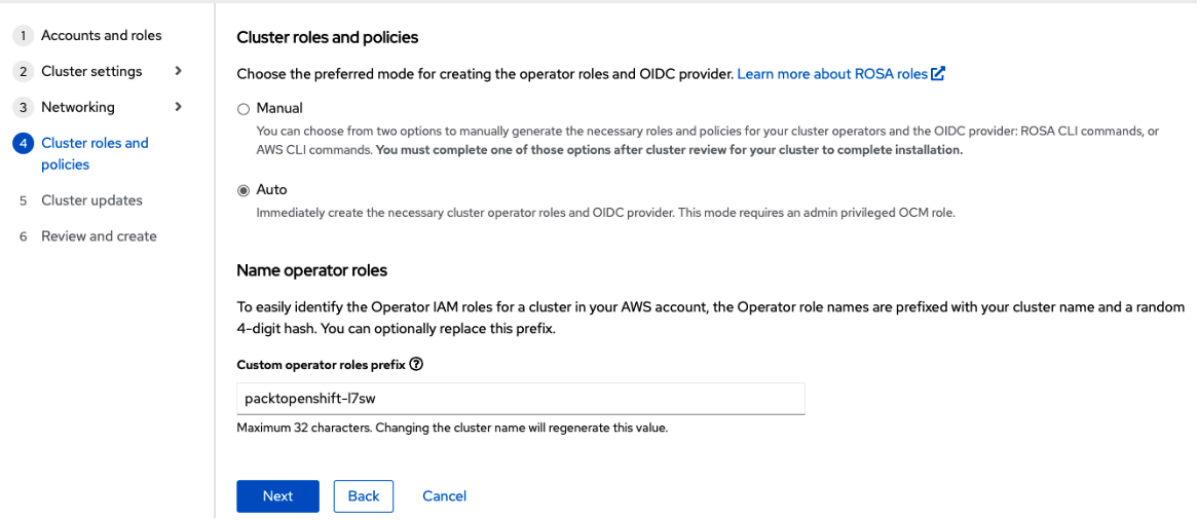

Cloud
Datacenter
Local
Active subscriptions
Offerings
Purchased through
Get started
Red Hat OpenShift Dedicated Trial
Red Hat
Available on AWS and GCP
Create trial cluster
View your available quota
Managed services
Create clusters in the cloud using a managed service.
Offerings
Purchased through
Get started
Azure Red Hat Openshift
Microsoft Azure
Flexible hourly billing
Try it on Azure
Red Hat OpenShift on IBM Cloud
IBM
Flexible hourly billing
Try it on IBM
Red Hat OpenShift Service on AWS (ROSA)
Amazon Web Services
Flexible hourly billing
Create cluster

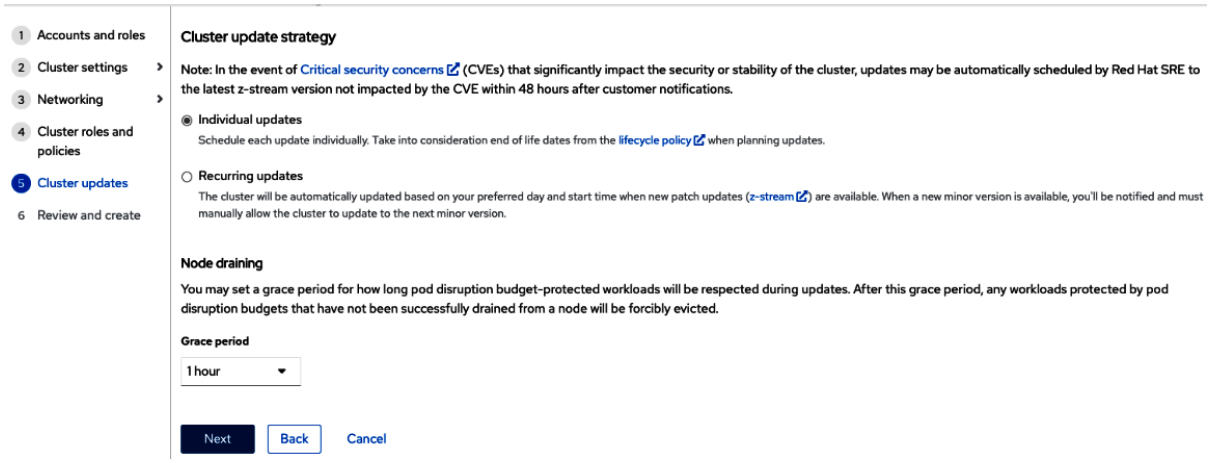

Create a ROSA Cluster
1 Accounts and roles
2 Cluster settings
3 Networking
4 Cluster roles and policies
5 Cluster updates
6 Review and create
Welcome to Red Hat OpenShift Service on AWS (ROSA)
Create a managed OpenShift cluster on an existing Amazon Web Services (AWS) account.
Prerequisites
Before continuing, complete all prerequisites:
Review and configure the AWS prerequisites for STS with ROSA.
Ensure you have available AWS quota.
Enable ROSA in the AWS Console.
Install and configure the latest AWS, ROSA, and oc CLIs on your workstation (recommended).
I've read and completed all the prerequisites and am ready to continue creating my cluster. *
Acknowledge that you have read and completed all prerequisites.
AWS account
Use an AWS account that is linked to your account. Alternatively, create an AWS account and validate all prerequisites.
Associated AWS account *
Select an account
Next
Back
Cancel


2 Cluster settings
Details
Machine pool
3 Networking
4 Cluster roles and policies
5 Cluster updates
6 Review and create
Cluster name *
packtopenshift
Version *
4.10.20
Region *
us-east-1, US East, N. Virginia
Availability *
Single zone
Multi-zone
Monitoring
Enable user workload monitoring
Monitor your own projects in isolation from Red Hat Site Reliability Engineering (SRE) platform metrics.
Encryption
The cloud storage for your cluster is encrypted at rest.
Learn more
Enable additional etcd encryption
Additional encryption of OpenShift and Kubernetes API resources.
Encrypt persistent volumes with customer keys
Use a custom AWS KMS key for AWS EBS volume encryption instead of your default AWS KMS key.
Next
Back
Cancel


Create a ROSA Cluster
1 Accounts and roles
2 Cluster settings
Details
Machine pool
3 Networking
4 Cluster roles and policies
5 Cluster updates
6 Review and create
Default machine pool
Select a compute node instance type and count for your default machine pool.
After cluster creation, your selected default machine pool instance type is permanent.
Compute node instance type *
m5.xlarge - 4 vCPU 16 GiB RAM
Autoscaling
Enable autoscaling
Minimum node count *
2
Maximum node count *
3
Edit node labels
Next
Back
Cancel


1 Accounts and roles
2 Cluster settings
3 Networking
Configuration
CIDR ranges
4 Cluster roles and policies
5 Cluster updates
6 Review and create
Networking configuration
Configure network access for your cluster.
Cluster privacy
Install your cluster with all public or all private API endpoint and application routes.
Public
Access Kubernetes API endpoint and application routes from the internet.
Private
Access Kubernetes API endpoint and application routes from direct private connections only.
Virtual Private Cloud (VPC)
By default, a new VPC will be created for your cluster. Alternatively, you may opt to install to an existing VPC below.
Install into an existing VPC
Configure a cluster-wide proxy
Enable an HTTP or HTTPS proxy to deny direct access to the internet from your cluster.
Next
Back
Cancel


1 Accounts and roles
2 Cluster settings
3 Networking
4 Cluster roles and policies
5 Cluster updates
6 Review and create
Cluster roles and policies
Choose the preferred mode for creating the operator roles and OIDC provider. Learn more about ROSA roles
Manual
You can choose from two options to manually generate the necessary roles and policies for your cluster operators and the OIDC provider: ROSA CLI commands, or AWS CLI commands. You must complete one of those options after cluster review for your cluster to complete installation.
Auto
Immediately create the necessary cluster operator roles and OIDC provider. This mode requires an admin privileged OCM role.
Name operator roles
To easily identify the Operator IAM roles for a cluster in your AWS account, the Operator role names are prefixed with your cluster name and a random 4-digit hash. You can optionally replace this prefix.
Custom operator roles prefix
packtopenshift-l7sw
Maximum 32 characters. Changing the cluster name will regenerate this value.
Next
Back
Cancel

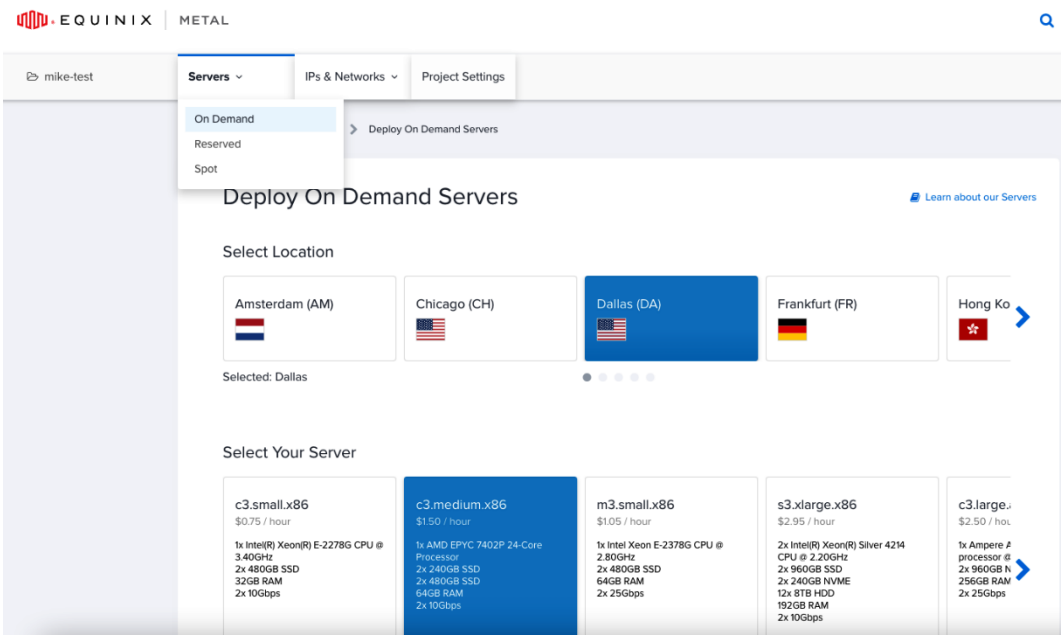

1 Accounts and roles
2 Cluster settings
3 Networking
4 Cluster roles and policies
5 Cluster updates
6 Review and create
Cluster update strategy
Note: In the event of Critical security concerns (CVEs) that significantly impact the security or stability of the cluster, updates may be automatically scheduled by Red Hat SRE to the latest z-stream version not impacted by the CVE within 48 hours after customer notifications.
Individual updates
Schedule each update individually. Take into consideration end of life dates from the lifecycle policy when planning updates.
Recurring updates
The cluster will be automatically updated based on your preferred day and start time when new patch updates (z-stream) are available. When a new minor version is available, you'll be notified and must manually allow the cluster to update to the next minor version.
Node draining
You may set a grace period for how long pod disruption budget-protected workloads will be respected during updates. After this grace period, any workloads protected by pod disruption budgets that have not been successfully drained from a node will be forcibly evicted.
Grace period
1 hour
Next
Back
Cancel

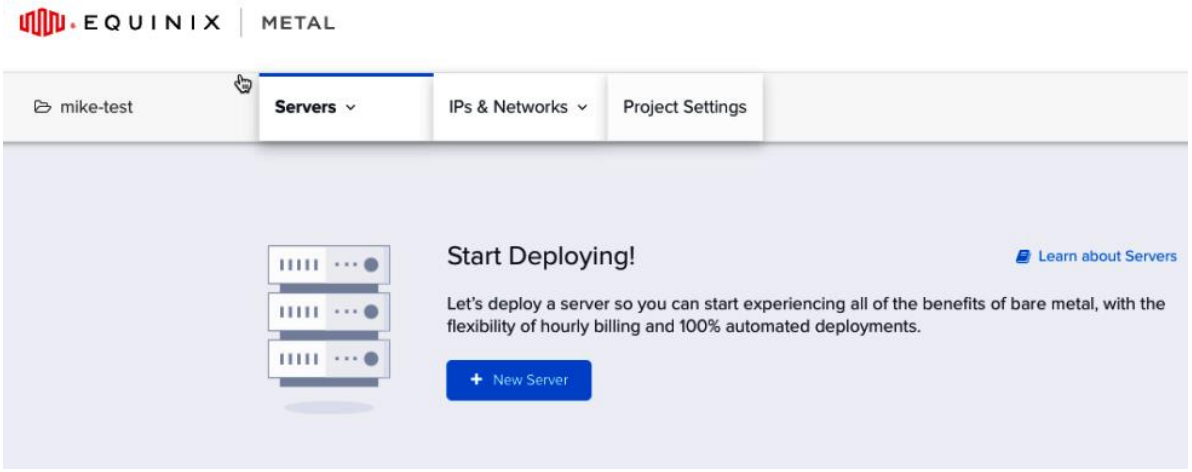
Chapter 4: The On-Prem Kubernetes Reality Check

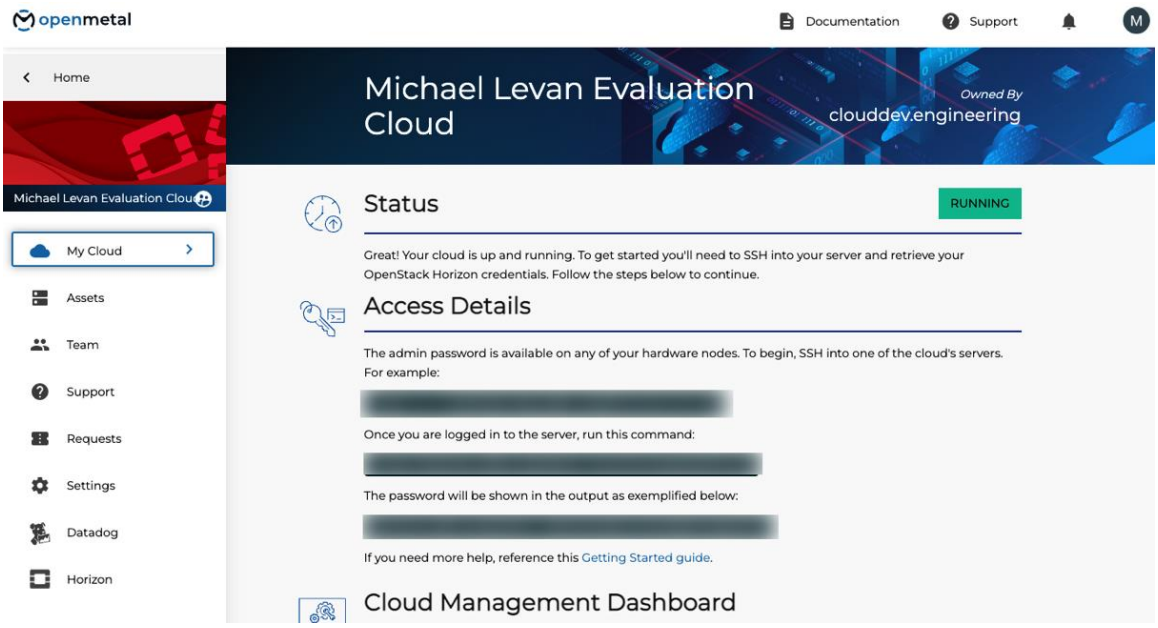
```
~ kubectl describe deployment nginx-deployment
Name:                   nginx-deployment
Namespace:              default
CreationTimestamp:      Fri, 22 Jul 2022 06:31:07 -0400
Labels:                 <none>
Annotations:            deployment.kubernetes.io/revision: 1
Selector:               app=nginxdeployment
Replicas:               2 desired | 2 updated | 2 total | 2 available | 0 unavailable
StrategyType:           RollingUpdate
MinReadySeconds:        0
RollingUpdateStrategy:  25% max unavailable, 25% max surge
Pod Template:
  Labels:  app=nginxdeployment
  Containers:
   nginxdeployment:
    Image:        nginx:latest
    Port:         80/TCP
    Host Port:    0/TCP
    Environment:  <none>
    Mounts:       <none>
  Volumes:        <none>
Conditions:
  Type           Status  Reason
  ----           ------  ------
  Available      True    MinimumReplicasAvailable
  Progressing    True    NewReplicaSetAvailable
OldReplicaSets:  <none>
NewReplicaSet:   nginx-deployment-588c8d7b4b (2/2 replicas created)
Events:
  Type    Reason             Age    From                   Message
  ----    ------             ----   ----                   -------
  Normal  ScalingReplicaSet  3m10s  deployment-controller  Scaled up replica set nginx-deployment-588c8d7b4b to 2
```

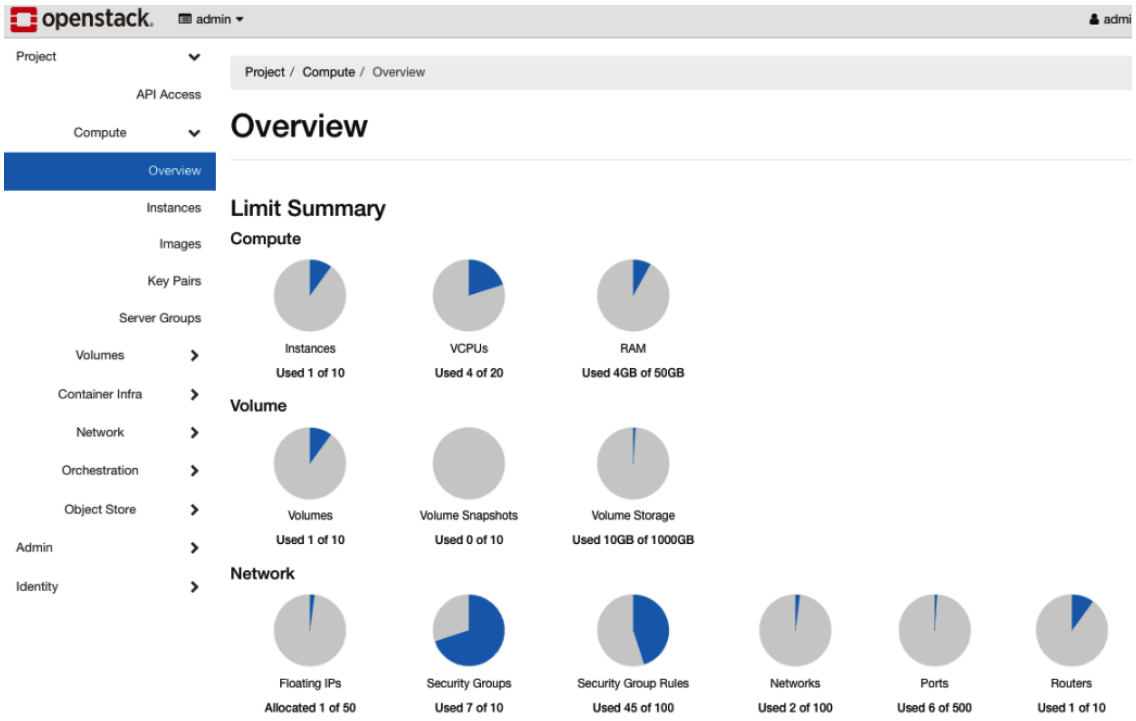
```
I0608 12:42:34.194982       1 controller.go:884] Started provisioner controller k8s.io/minikube-hostpath_minikube_f128d371-5449-
!
==== END logs for container storage-provisioner of pod kube-system/storage-provisioner ====
{
    "kind": "EventList",
    "apiVersion": "v1",
    "metadata": {
        "resourceVersion": "1851361"
    },
    "items": [
        {
            "metadata": {
                "name": "nginx-deployment-588c8d7b4b-wmg9z.1704201c144e865e",
                "namespace": "default",
                "uid": "6130e548-9297-410a-b69b-692254752795",
                "resourceVersion": "1851039",
                "creationTimestamp": "2022-07-22T10:31:07Z"
            },
            "involvedObject": {
                "kind": "Pod",
                "namespace": "default",
                "name": "nginx-deployment-588c8d7b4b-wmg9z",
                "uid": "06fb02a9-64ca-47ac-aeca-bfb3e9bbb552",
                "apiVersion": "v1",
                "resourceVersion": "1851033"
            },
            "reason": "Scheduled",
            "message": "Successfully assigned default/nginx-deployment-588c8d7b4b-wmg9z to minikube",
            "source": {
                "component": "default-scheduler"
            },
            "firstTimestamp": "2022-07-22T10:31:07Z",
            "lastTimestamp": "2022-07-22T10:31:07Z",
            "count": 1,
            "type": "Normal",
            "eventTime": null,
            "reportingComponent": "",
            "reportingInstance": ""
```

```
☁  ~  kubectl logs nginx-deployment-588c8d7b4b-wmg9z
/docker-entrypoint.sh: /docker-entrypoint.d/ is not empty, will attempt to perform configuration
/docker-entrypoint.sh: Looking for shell scripts in /docker-entrypoint.d/
/docker-entrypoint.sh: Launching /docker-entrypoint.d/10-listen-on-ipv6-by-default.sh
10-listen-on-ipv6-by-default.sh: info: Getting the checksum of /etc/nginx/conf.d/default.conf
10-listen-on-ipv6-by-default.sh: info: Enabled listen on IPv6 in /etc/nginx/conf.d/default.conf
/docker-entrypoint.sh: Launching /docker-entrypoint.d/20-envsubst-on-templates.sh
/docker-entrypoint.sh: Launching /docker-entrypoint.d/30-tune-worker-processes.sh
/docker-entrypoint.sh: Configuration complete; ready for start up
2022/07/22 10:31:12 [notice] 1#1: using the "epoll" event method
2022/07/22 10:31:12 [notice] 1#1: nginx/1.23.1
2022/07/22 10:31:12 [notice] 1#1: built by gcc 10.2.1 20210110 (Debian 10.2.1-6)
2022/07/22 10:31:12 [notice] 1#1: OS: Linux 5.10.104-linuxkit
2022/07/22 10:31:12 [notice] 1#1: getrlimit(RLIMIT_NOFILE): 1048576:1048576
2022/07/22 10:31:12 [notice] 1#1: start worker processes
2022/07/22 10:31:12 [notice] 1#1: start worker process 32
2022/07/22 10:31:12 [notice] 1#1: start worker process 33
2022/07/22 10:31:12 [notice] 1#1: start worker process 34
2022/07/22 10:31:12 [notice] 1#1: start worker process 35
```

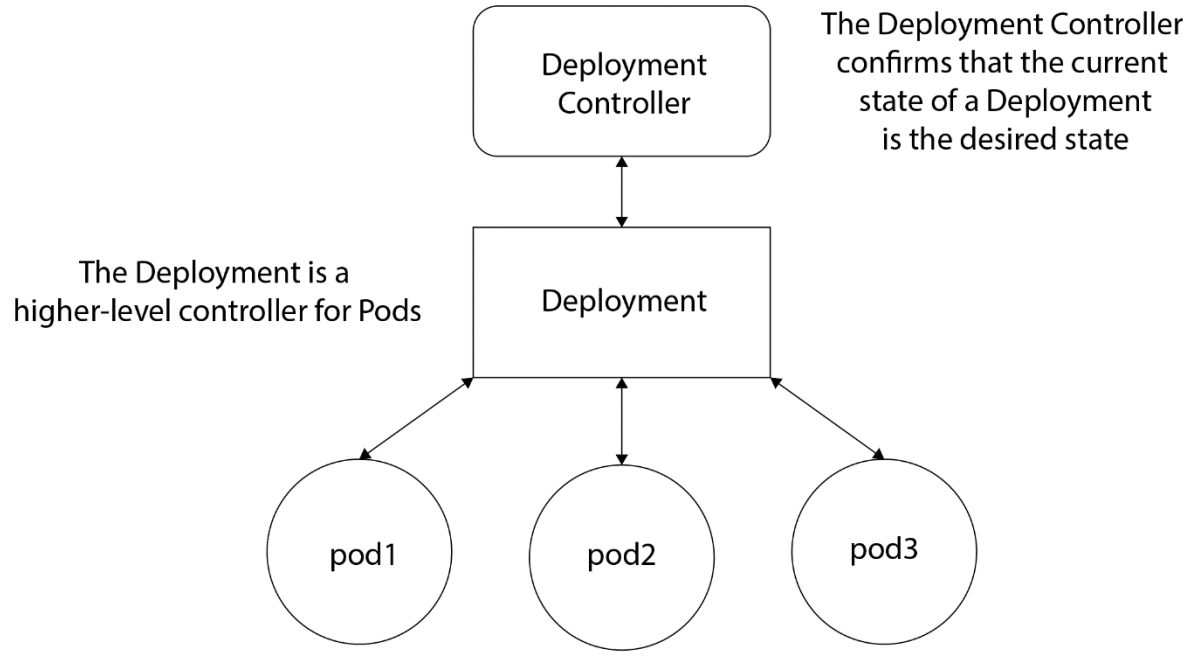




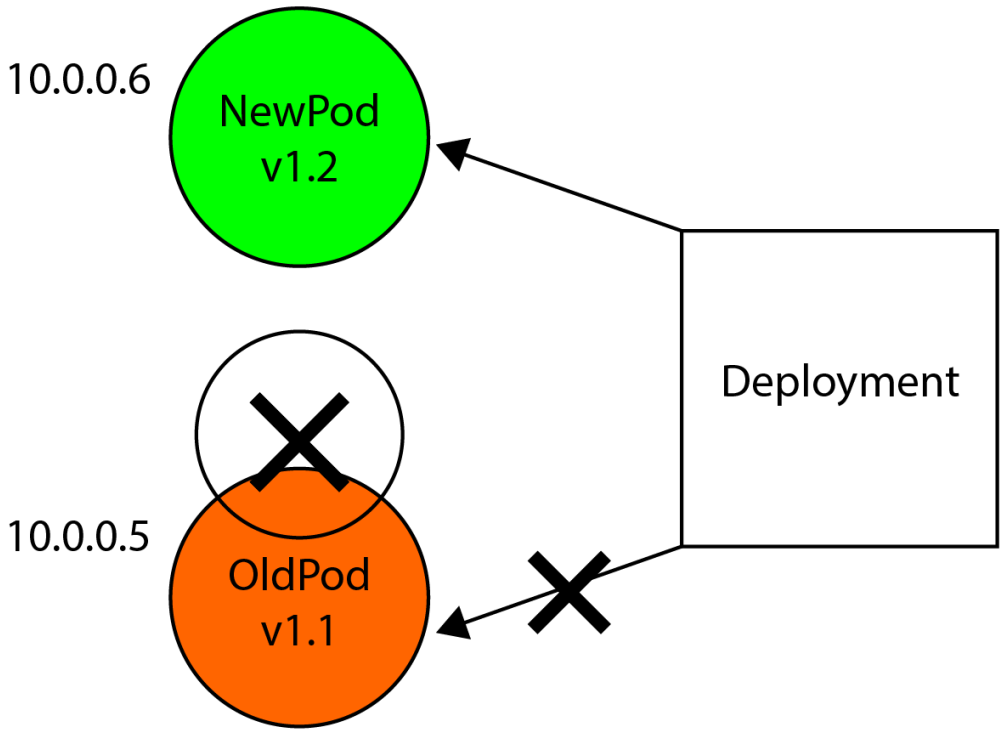

openmetal
Documentation
Support
M
Home
Michael Levan Evaluation Clou
My Cloud
Assets
Team
Support
Requests
Settings
Datadog
Horizon
Michael Levan Evaluation Cloud
Owned By
clouddev.engineering
Status
RUNNING
Great! Your cloud is up and running. To get started you'll need to SSH into your server and retrieve your OpenStack Horizon credentials. Follow the steps below to continue.
Access Details
The admin password is available on any of your hardware nodes. To begin, SSH into one of the cloud's servers. For example:
Once you are logged in to the server, run this command:
The password will be shown in the output as exemplified below:
If you need more help, reference this Getting Started guide.
Cloud Management Dashboard


openstack.
admin
admi
Project
API Access
Compute
Overview
Instances
Images
Key Pairs
Server Groups
Volumes
Container Infra
Network
Orchestration
Object Store
Admin
Identity
Project / Compute / Overview
Overview
Limit Summary
Compute
Instances
Used 1 of 10
VCPUs
Used 4 of 20
RAM
Used 4GB of 50GB
Volume
Volumes
Used 1 of 10
Volume Snapshots
Used 0 of 10
Volume Storage
Used 10GB of 1000GB
Network
Floating IPs
Allocated 1 of 50
Security Groups
Used 7 of 10
Security Group Rules
Used 45 of 100
Networks
Used 2 of 100
Ports
Used 6 of 500
Routers
Used 1 of 10

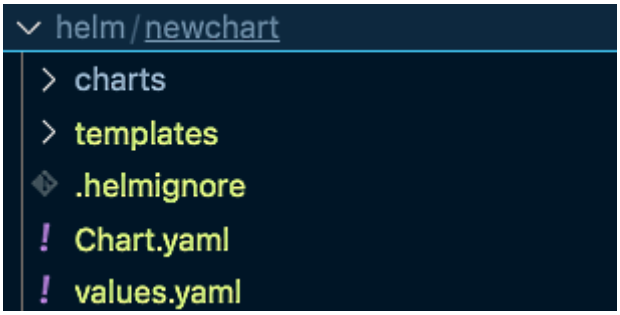
Chapter 5: Deploying Kubernetes Apps Like a True Cloud Native

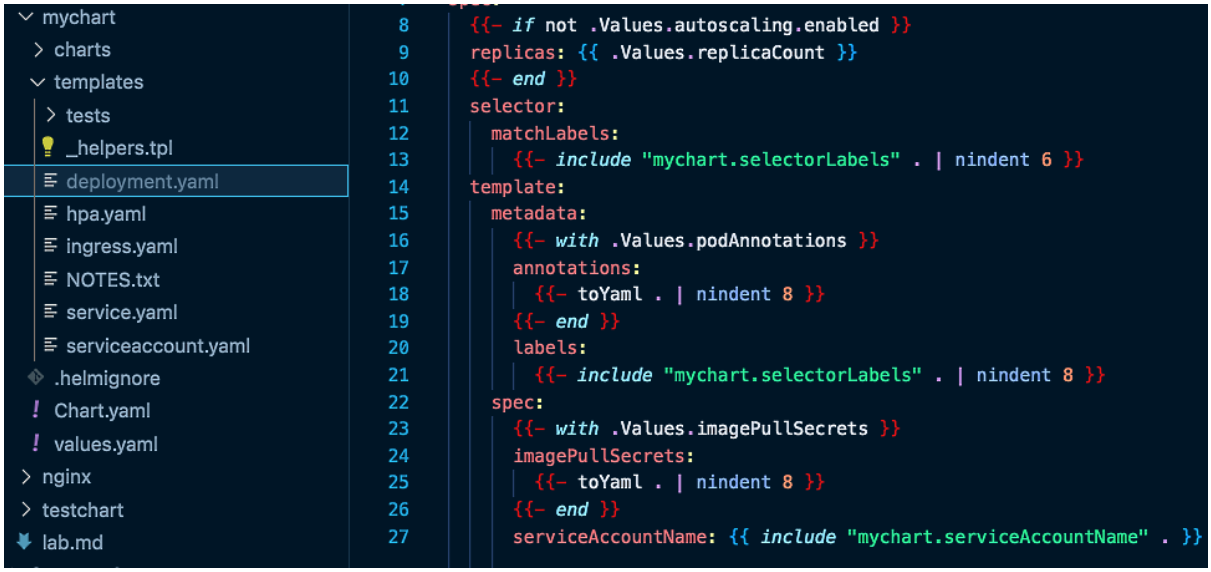


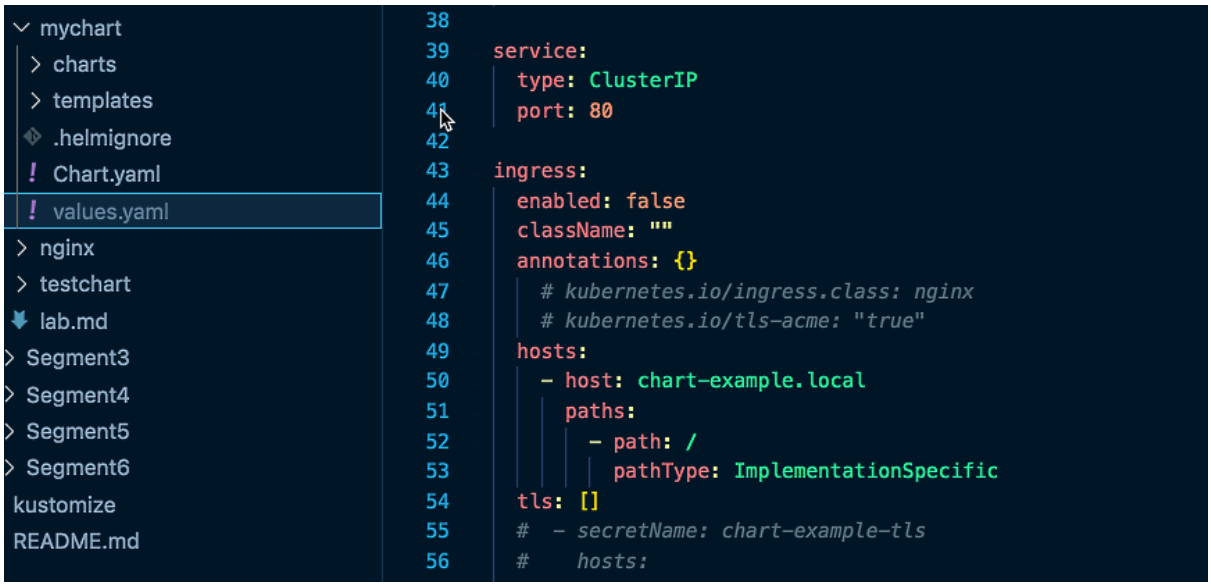

```
michael@michaels-MBP:~
argocd        argocd-application-controller-0                  1/1     Running   2 (40h ago)   4d19h
argocd        argocd-applicationset-controller-5b6b596788-9bpnm  1/1     Running   0             4d19h
argocd        argocd-dex-server-7f5957b5df-2xhvb                1/1     Running   0             4d19h
argocd        argocd-notifications-controller-76b9c588c-hwkq6   1/1     Running   0             4d19h
argocd        argocd-redis-ha-haproxy-6dc6757955-65tsn          0/1     Pending   0             4d19h
argocd        argocd-redis-ha-haproxy-6dc6757955-t4str          1/1     Running   2 (40h ago)   4d19h
argocd        argocd-redis-ha-haproxy-6dc6757955-vzrrs          0/1     Pending   0             4d19h
argocd        argocd-redis-ha-server-0                          2/2     Running   2 (39h ago)   4d19h
argocd        argocd-redis-ha-server-1                          0/2     Pending   0             4d19h
argocd        argocd-repo-server-6c75584b95-pg48m               0/1     Pending   0             4d19h
argocd        argocd-repo-server-6c75584b95-sxj2r               1/1     Running   11 (14h ago)  4d19h
argocd        argocd-server-8484cf8cbd-5kbxc                    0/1     Pending   0             4d19h
argocd        argocd-server-8484cf8cbd-hs8k7                    1/1     Running   11 (39h ago)  4d19h
default       nginx-deployment-0                                1/1     Running   0             54m
default       nginx-deployment-1                                1/1     Running   0             54m
default       nginx-deployment-cfmnw                            1/1     Running   0             62m
kube-system   coredns-64897985d-fgcts                           1/1     Running   0             4d19h
kube-system   etcd-minikube                                     1/1     Running   0             4d19h
kube-system   kube-apiserver-minikube                           1/1     Running   0             4d19h
kube-system   kube-controller-manager-minikube                  1/1     Running   0             4d19h
kube-system   kube-proxy-5ttt5                                  1/1     Running   0             4d19h
kube-system   kube-scheduler-minikube                           1/1     Running   0             4d19h
kube-system   storage-provisioner                               1/1     Running   3 (14h ago)   4d19h
monitoring    alertmanager-main-0                               2/2     Running   0             4d19h
monitoring    alertmanager-main-1                               2/2     Running   0             4d19h
monitoring    alertmanager-main-2                               2/2     Running   0             4d19h
monitoring    blackbox-exporter-67bbdf4897-cj4c4                3/3     Running   0             4d19h
monitoring    grafana-86dfcbf9cc-cgs7k                          1/1     Running   0             4d19h
monitoring    kube-state-metrics-7b88fc766c-tzzjv               3/3     Running   0             4d19h
monitoring    node-exporter-b7m2z                               2/2     Running   0             4d19h
monitoring    prometheus-adapter-6455646bdc-6n8zn               1/1     Running   0             4d19h
monitoring    prometheus-adapter-6455646bdc-9s2rr               1/1     Running   0             4d19h
monitoring    prometheus-k8s-0                                  2/2     Running   0             4d19h
monitoring    prometheus-k8s-1                                  2/2     Running   0             4d19h
monitoring    prometheus-operator-5c56ccbbcd-s7v9v              2/2     Running   0             4d19h
~
```

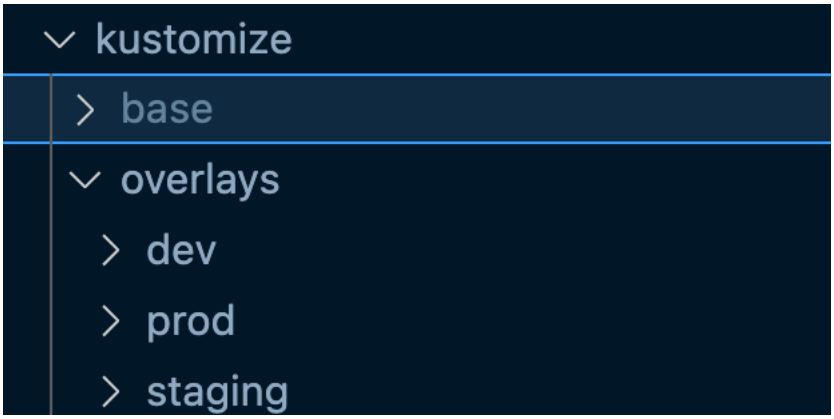

10.0.0.6
NewPod
v1.2
Deployment
10.0.0.5
OldPod
v1.1

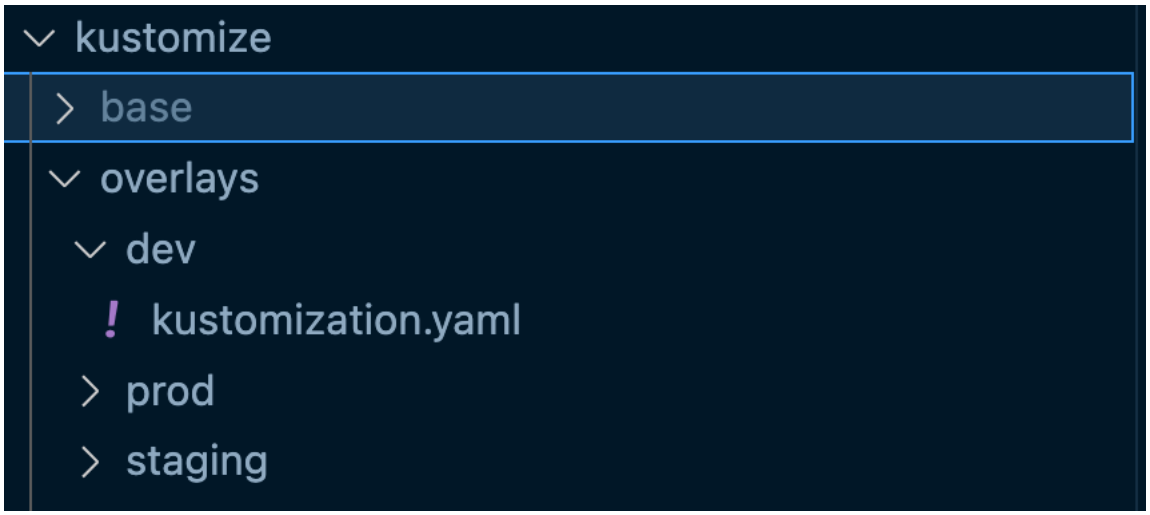
Chapter 6: Kubernetes Deployment – Same Game, Next Level







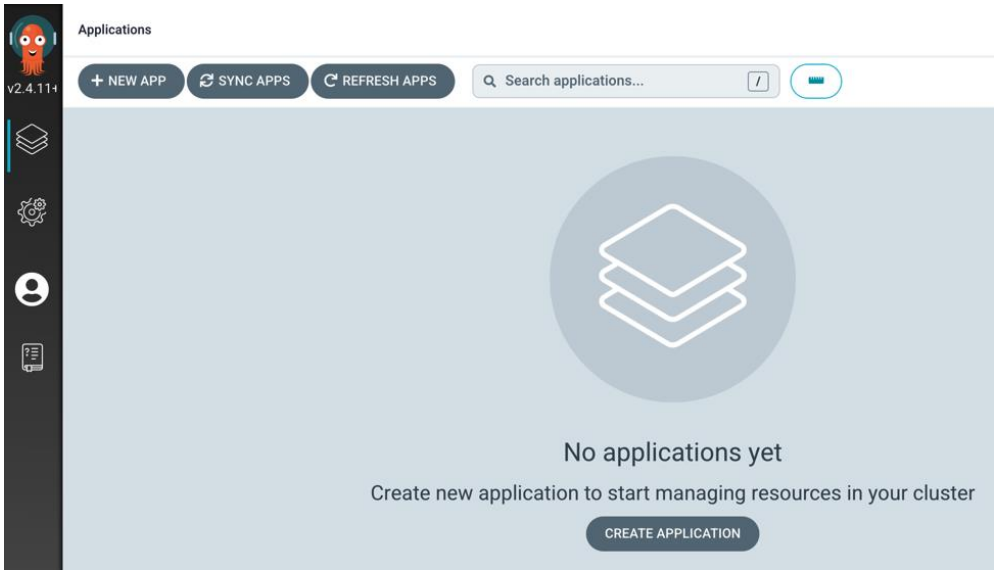





```yaml
apiVersion: kustomize.config.k8s.io/v1beta1
kind: Kustomization
resources:
- ../../base/

replicas:
- name: nginx-deployment
  count: 1      You, 4 months ago • kustomize
```

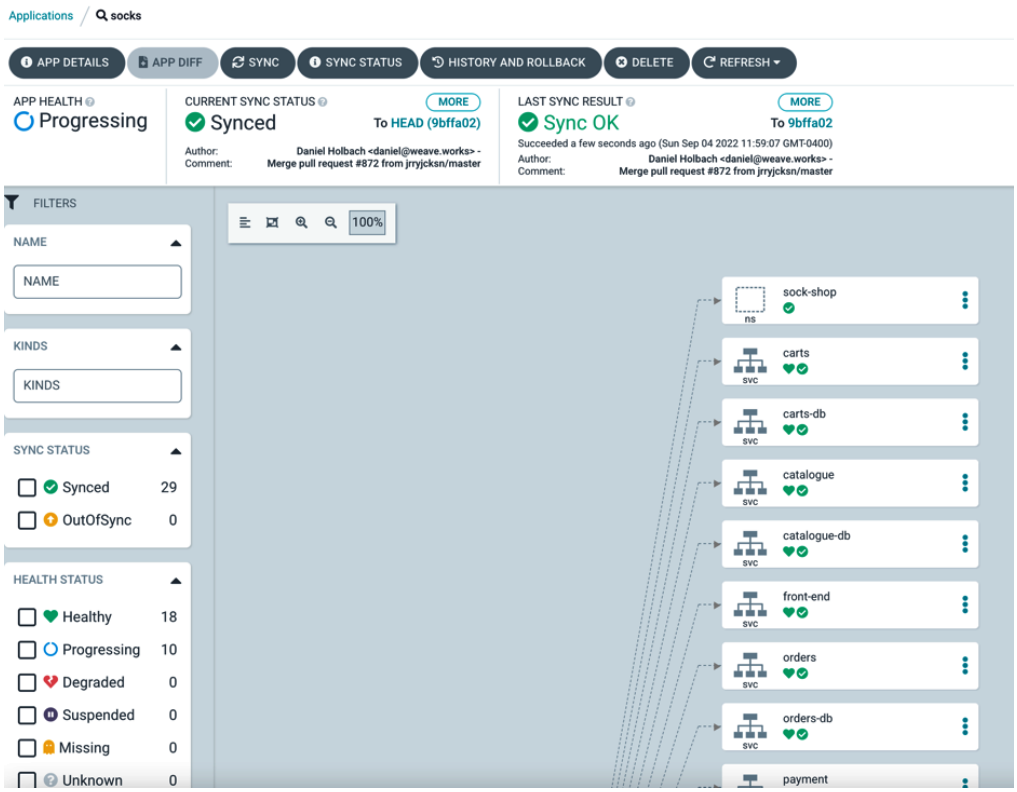
```
dev [main] ⚡   kubectl kustomize
apiVersion: apps/v1
kind: Deployment
metadata:
  name: nginx-deployment
spec:
  replicas: 1
  selector:
    matchLabels:
      app: nginxdeployment
  template:
    metadata:
      labels:
        app: nginxdeployment
    spec:
      containers:
      - image: nginx:latest
        name: nginxdeployment
        ports:
        - containerPort: 80
```

```
kubectl port-forward -n argocd service/argocd-server :80
kubectl (kubectl) ⌘1 | ~ (-zsh) ⌘2
namespace/argocd created
~ kubectl apply -n argocd -f https://raw.githubusercontent.com/argoproj/argo-cd/stable/manifests/ha/install.yaml
customresourcedefinition.apiextensions.k8s.io/applications.argoproj.io created
customresourcedefinition.apiextensions.k8s.io/applicationsets.argoproj.io created
customresourcedefinition.apiextensions.k8s.io/appprojects.argoproj.io created
serviceaccount/argocd-application-controller created
serviceaccount/argocd-applicationset-controller created
serviceaccount/argocd-dex-server created
serviceaccount/argocd-notifications-controller created
serviceaccount/argocd-redis-ha created
serviceaccount/argocd-redis-ha-haproxy created
serviceaccount/argocd-repo-server created
serviceaccount/argocd-server created
role.rbac.authorization.k8s.io/argocd-application-controller created
role.rbac.authorization.k8s.io/argocd-applicationset-controller created
role.rbac.authorization.k8s.io/argocd-dex-server created
role.rbac.authorization.k8s.io/argocd-notifications-controller created
role.rbac.authorization.k8s.io/argocd-redis-ha created
role.rbac.authorization.k8s.io/argocd-redis-ha-haproxy created
role.rbac.authorization.k8s.io/argocd-server created
clusterrole.rbac.authorization.k8s.io/argocd-application-controller created
clusterrole.rbac.authorization.k8s.io/argocd-server created
rolebinding.rbac.authorization.k8s.io/argocd-application-controller created
rolebinding.rbac.authorization.k8s.io/argocd-applicationset-controller created
rolebinding.rbac.authorization.k8s.io/argocd-dex-server created
rolebinding.rbac.authorization.k8s.io/argocd-notifications-controller created
rolebinding.rbac.authorization.k8s.io/argocd-redis-ha created
rolebinding.rbac.authorization.k8s.io/argocd-redis-ha-haproxy created
rolebinding.rbac.authorization.k8s.io/argocd-server created
clusterrolebinding.rbac.authorization.k8s.io/argocd-application-controller created
clusterrolebinding.rbac.authorization.k8s.io/argocd-server created
configmap/argocd-cm created
configmap/argocd-cmd-params-cm created
configmap/argocd-gpg-keys-cm created
configmap/argocd-notifications-cm created
configmap/argocd-rbac-cm created
configmap/argocd-redis-ha-configmap created
configmap/argocd-redis-ha-health-configmap created
configmap/argocd-ssh-known-hosts-cm created
```




```
WARNING: server certificate had error: x509: “Argo CD” certificate is not trusted. Proceed insecurely (y/n)? y
Username: admin
Password:
'admin:login' logged in successfully
Context '127.0.0.1:59341' updated
```

```
GROUP  KIND        NAMESPACE  NAME          STATUS   HEALTH       HOOK  MESSAGE
       Namespace   sock-shop  sock-shop     Running  Synced            namespace/sock-shop configured. Warning: resource name
aces/sock-shop is missing the kubectl.kubernetes.io/last-applied-configuration annotation which is required by  apply.  apply s
ould only be used on resources created declaratively by either  create --save-config or  apply. The missing annotation will be
atched automatically.
       Service     sock-shop  carts-db      Synced   Healthy           service/carts-db created
       Service     sock-shop  carts         Synced   Healthy           service/carts created
       Service     sock-shop  user-db       Synced   Healthy           service/user-db created
       Service     sock-shop  rabbitmq      Synced   Healthy           service/rabbitmq created
       Service     sock-shop  shipping      Synced   Healthy           service/shipping created
       Service     sock-shop  payment       Synced   Healthy           service/payment created
       Service     sock-shop  queue-master  Synced   Healthy           service/queue-master created
       Service     sock-shop  catalogue     Synced   Healthy           service/catalogue created
       Service     sock-shop  session-db    Synced   Healthy           service/session-db created
       Service     sock-shop  orders        Synced   Healthy           service/orders created
       Service     sock-shop  catalogue-db  Synced   Healthy           service/catalogue-db created
       Service     sock-shop  orders-db     Synced   Healthy           service/orders-db created
       Service     sock-shop  front-end     Synced   Healthy           service/front-end created
       Service     sock-shop  user          Synced   Healthy           service/user created
apps   Deployment  sock-shop  carts-db      Synced   Progressing       deployment.apps/carts-db created
apps   Deployment  sock-shop  carts         Synced   Progressing       deployment.apps/carts created
apps   Deployment  sock-shop  user          Synced   Progressing       deployment.apps/user created
apps   Deployment  sock-shop  user-db       Synced   Progressing       deployment.apps/user-db created
apps   Deployment  sock-shop  catalogue-db  Synced   Progressing       deployment.apps/catalogue-db created
apps   Deployment  sock-shop  rabbitmq      Synced   Progressing       deployment.apps/rabbitmq created
apps   Deployment  sock-shop  orders        Synced   Progressing       deployment.apps/orders created
apps   Deployment  sock-shop  front-end     Synced   Progressing       deployment.apps/front-end created
apps   Deployment  sock-shop  payment       Synced   Progressing       deployment.apps/payment created
apps   Deployment  sock-shop  session-db    Synced   Progressing       deployment.apps/session-db created
apps   Deployment  sock-shop  queue-master  Synced   Progressing       deployment.apps/queue-master created
apps   Deployment  sock-shop  shipping      Synced   Progressing       deployment.apps/shipping created
apps   Deployment  sock-shop  orders-db     Synced   Progressing       deployment.apps/orders-db created
apps   Deployment  sock-shop  catalogue     Synced   Progressing       deployment.apps/catalogue created
       Namespace             sock-shop     Synced
```




```
NAME                                READY   STATUS         RESTARTS   AGE
nginx-deployment-78bb975ccb-ll6nt   0/1     ErrImagePull   0          12s
nginx-deployment-78bb975ccb-wl898   0/1     ErrImagePull   0          12s
```

```
Conditions:
  Type              Status
  Initialized       True
  Ready             False
  ContainersReady   False
  PodScheduled      True
Volumes:
  kube-api-access-9f4gz:
    Type:                    Projected (a volume that contains injected data from multiple sources)
    TokenExpirationSeconds:  3607
    ConfigMapName:           kube-root-ca.crt
    ConfigMapOptional:       <nil>
    DownwardAPI:             true
QoS Class:                   BestEffort
Node-Selectors:              <none>
Tolerations:                 node.kubernetes.io/not-ready:NoExecute op=Exists for 300s
                             node.kubernetes.io/unreachable:NoExecute op=Exists for 300s

Events:
  Type     Reason     Age                  From               Message
  ----     ------     ----                 ----               -------
  Normal   Scheduled  3m1s                 default-scheduler  Successfully assigned default/nginx-deployment-78bb975ccb-ll6nt to minikube
  Normal   Pulling    83s (x4 over 3m)     kubelet            Pulling image "nginx:lates"
  Warning  Failed     83s (x4 over 3m)     kubelet            Failed to pull image "nginx:lates": rpc error: code = Unknown desc = Error
response from daemon: manifest for nginx:lates not found: manifest unknown: manifest unknown
  Warning  Failed     83s (x4 over 3m)     kubelet            Error: ErrImagePull
  Warning  Failed     71s (x6 over 2m59s)  kubelet            Error: ImagePullBackOff
  Normal   BackOff    59s (x7 over 2m59s)  kubelet            Back-off pulling image "nginx:lates"
```

```
Error from server (BadRequest): container "nginxdeployment" in pod "nginx-deploymen
t-78bb975ccb-ll6nt" is waiting to start: trying and failing to pull image
```

```
kubernetes-examples [main] ⚡  kubectl get service
NAME           TYPE           CLUSTER-IP       EXTERNAL-IP   PORT(S)        AGE
kubernetes     ClusterIP      10.96.0.1        <none>        443/TCP        87m
nginxservice   LoadBalancer   10.110.183.138   <pending>     80:30702/TCP   74m
kubernetes-examples [main] ⚡
```

```
/ # nslookup nginxservice
Server:    10.96.0.10
Address 1: 10.96.0.10 kube-dns.kube-system.svc.cluster.local

Name:      nginxservice
Address 1: 10.110.183.138 nginxservice.default.svc.cluster.local
```

```
/ # nslookup nginxservice.default.svc.cluster.local
Server:    10.96.0.10
Address 1: 10.96.0.10 kube-dns.kube-system.svc.cluster.local

Name:      nginxservice.default.svc.cluster.local
Address 1: 10.110.183.138 nginxservice.default.svc.cluster.local
/ #
```

```
☁  kubernetes-examples [main] ⚡  kubectl get service nginxservice -o json
{
    "apiVersion": "v1",
    "kind": "Service",
    "metadata": {
        "annotations": {
            "kubectl.kubernetes.io/last-applied-configuration": "{\"apiVersion\":\"v1\",\"kind\":\"Service\",\"metadata\":{\"annotations\":{
},\"name\":\"nginxservice\",\"namespace\":\"default\"},\"spec\":{\"ports\":[{\"port\":80,\"protocol\":\"TCP\"}],\"selector\":{\"app\":\"ngi
xdeployment\"},\"type\":\"LoadBalancer\"}}\n"
        },
        "creationTimestamp": "2022-09-09T12:43:26Z",
        "name": "nginxservice",
        "namespace": "default",
        "resourceVersion": "1068",
        "uid": "096e2852-d486-4d2d-a34a-8952f38acbc5"
    },
    "spec": {
        "allocateLoadBalancerNodePorts": true,
        "clusterIP": "10.110.183.138",
        "clusterIPs": [
            "10.110.183.138"
        ],
        "externalTrafficPolicy": "Cluster",
        "internalTrafficPolicy": "Cluster",
        "ipFamilies": [
            "IPv4"
        ],
        "ipFamilyPolicy": "SingleStack",
        "ports": [
            {
                "nodePort": 30702,
                "port": 80,
```

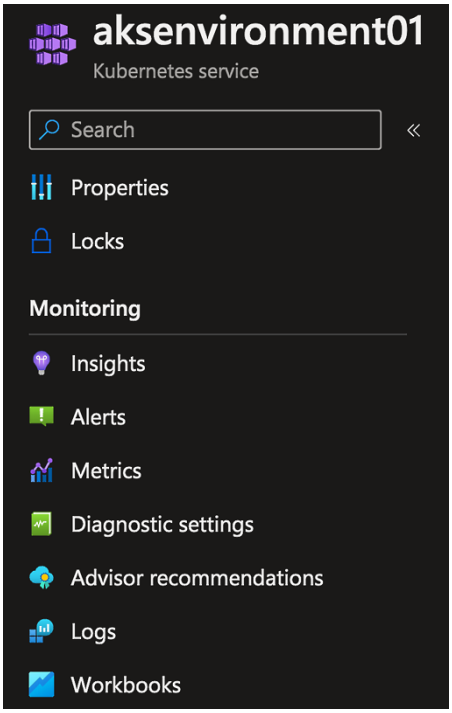
```
☁  kubernetes-examples [main] ⚡  kubectl get pods -l app=nginxdeployment
NAME                                READY   STATUS    RESTARTS   AGE
nginx-deployment-588c8d7b4b-6zxth   1/1     Running   0          83m
nginx-deployment-588c8d7b4b-9wtd8   1/1     Running   0          83m
☁  kubernetes-examples [main] ⚡
```

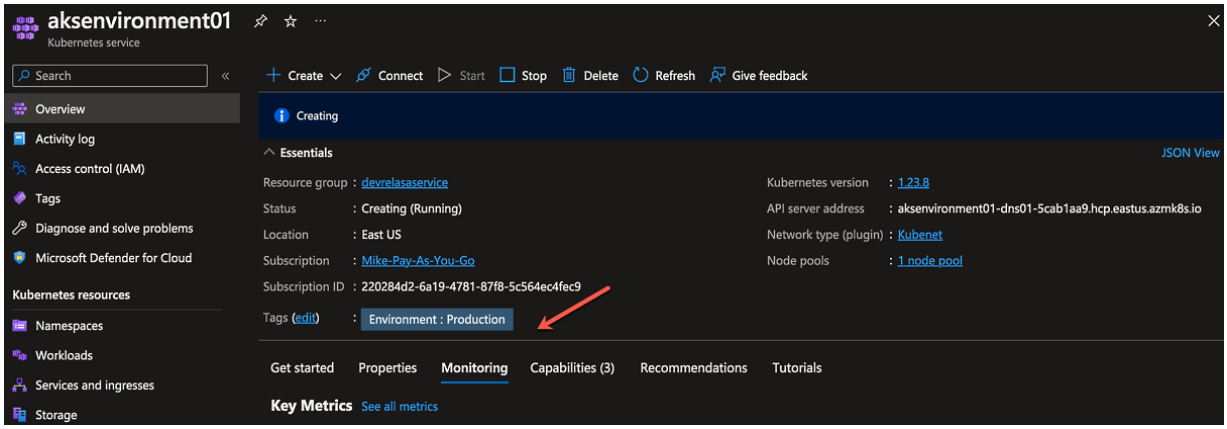
```
☁  kubernetes-examples [main] ⚡  kubectl describe deployment nginx-deployment
Name:                   nginx-deployment
Namespace:              default
CreationTimestamp:      Fri, 09 Sep 2022 08:43:26 -0400
Labels:                 <none>
Annotations:            deployment.kubernetes.io/revision: 1
Selector:               app=nginxdeployment
Replicas:               2 desired | 2 updated | 2 total | 2 available | 0 unavailable
StrategyType:           RollingUpdate
MinReadySeconds:        0
RollingUpdateStrategy:  25% max unavailable, 25% max surge
Pod Template:
  Labels:  app=nginxdeployment
  Containers:
   nginxdeployment:
    Image:        nginx:latest
    Port:         80/TCP
    Host Port:    0/TCP
    Environment:  <none>
    Mounts:       <none>
  Volumes:        <none>
Conditions:
  Type           Status  Reason
  ----           ------  ------
  Available      True    MinimumReplicasAvailable
  Progressing    True    NewReplicaSetAvailable
OldReplicaSets:  <none>
NewReplicaSet:   nginx-deployment-588c8d7b4b (2/2 replicas created)
Events:          <none>
```

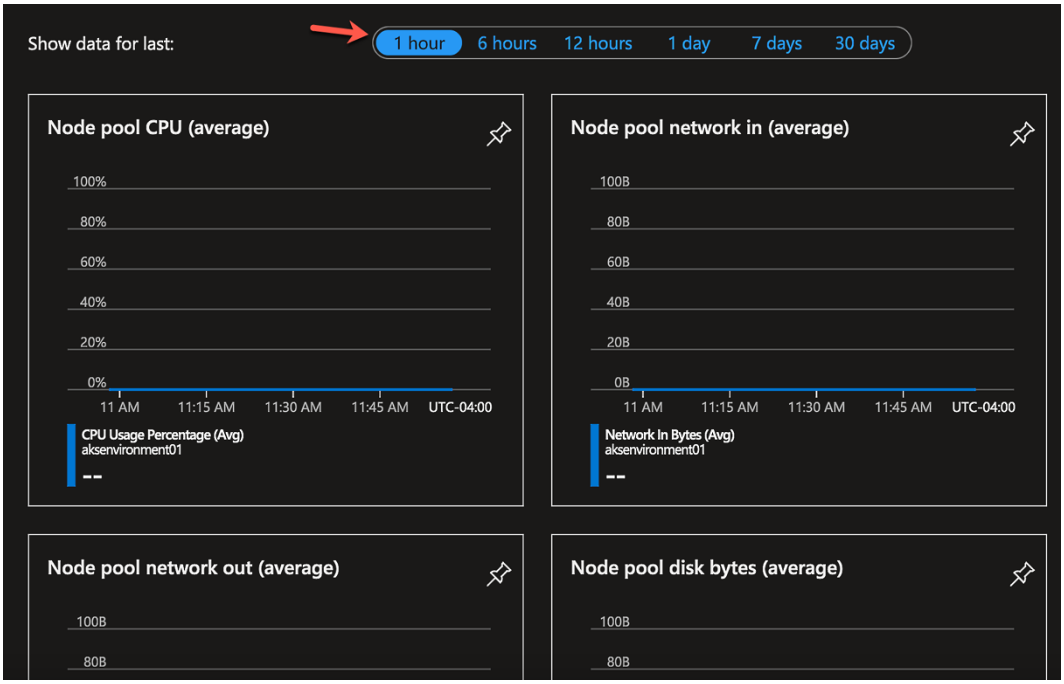
```
☁  aks [main] ⚡  kubectl port-forward service/aks-helloworld-one :80
Forwarding from 127.0.0.1:55319 -> 80
Forwarding from [::1]:55319 -> 80
```

Welcome to Azure Kubernetes Service (AKS)

Chapter 7: Kubernetes Monitoring and Observability







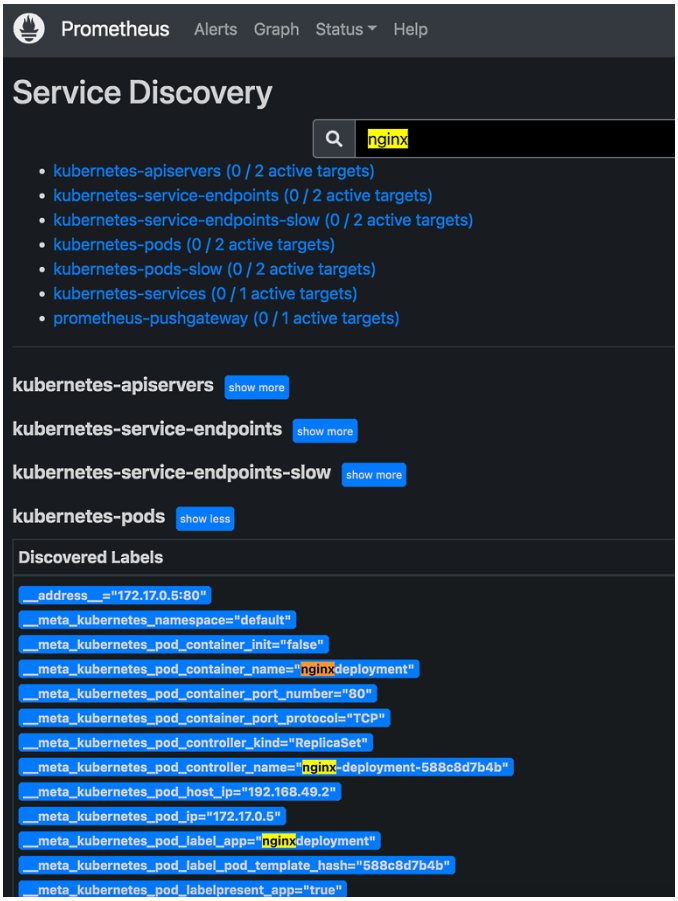

```
stress_testing [main] ⚡  kubectl top pod nginx-deployment-588c8d7b4b-5fllw --namespace=default

NAME                                CPU(cores)   MEMORY(bytes)
nginx-deployment-588c8d7b4b-5fllw   0m           1Mi
stress_testing [main] ⚡
```

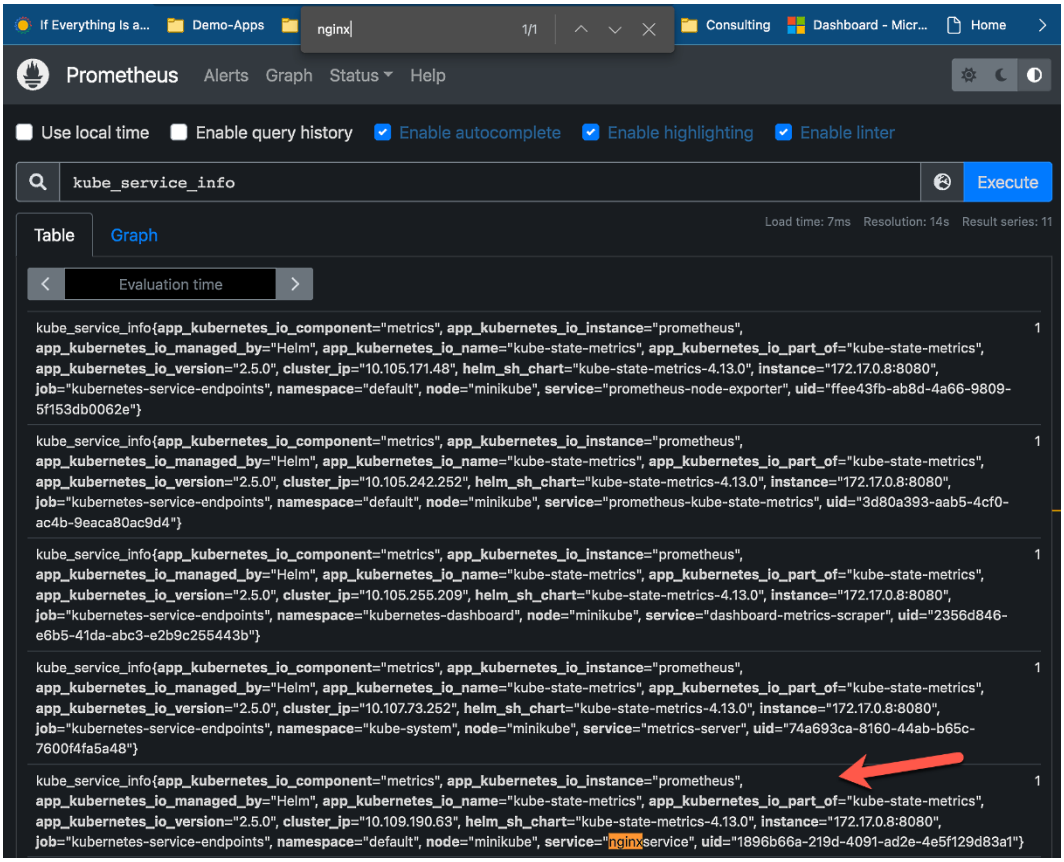
```
running (0m31.0s), 000/100 VUs, 2930 complete and 0 interrupted iterations
default ✓ [======================================] 100 VUs  30s

     data_received..................: 34 MB  1.1 MB/s
     data_sent......................: 321 kB 10 kB/s
     http_req_blocked...............: avg=17.05ms  min=0s      med=3µs     max=764.24ms p(90)=7µs     p(95)=12µs
     http_req_connecting............: avg=967.12µs min=0s      med=0s      max=55.97ms  p(90)=0s      p(95)=0s
     http_req_duration..............: avg=20.98ms  min=13.24ms med=18.38ms max=133.13ms p(90)=27.21ms p(95)=32.01ms
       { expected_response:true }...: avg=20.98ms  min=13.24ms med=18.38ms max=133.13ms p(90)=27.21ms p(95)=32.01ms
     http_req_failed................: 0.00%  ✓ 0        ✗ 2930
     http_req_receiving.............: avg=948.27µs min=8µs     med=49µs    max=23.43ms  p(90)=123.2µs p(95)=11.01ms
     http_req_sending...............: avg=16.26µs  min=2µs     med=13µs    max=1.71ms   p(90)=24µs    p(95)=30µs
     http_req_tls_handshaking.......: avg=10.03ms  min=0s      med=0s      max=530.15ms p(90)=0s      p(95)=0s
     http_req_waiting...............: avg=20.01ms  min=12.79ms med=18.02ms max=133.1ms  p(90)=24.84ms p(95)=26.69ms
     http_reqs......................: 2930   94.55905/s
     iteration_duration.............: avg=1.03s    min=1.01s   med=1.01s   max=1.79s    p(90)=1.02s   p(95)=1.03s
     iterations.....................: 2930   94.55905/s
     vus............................: 100    min=100     max=100
     vus_max........................: 100    min=100     max=100
```

```
kubernetes-examples [main] ⚡  kubectl top pod nginx-deployment-588c8d7b4b-5fllw --namespace=default

NAME                                CPU(cores)   MEMORY(bytes)
nginx-deployment-588c8d7b4b-5fllw   0m           3Mi
```

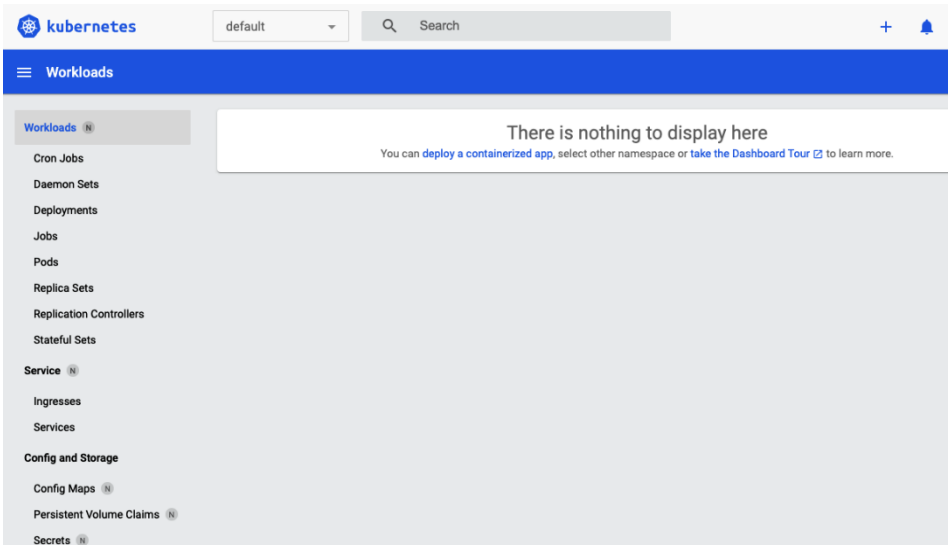
Pods

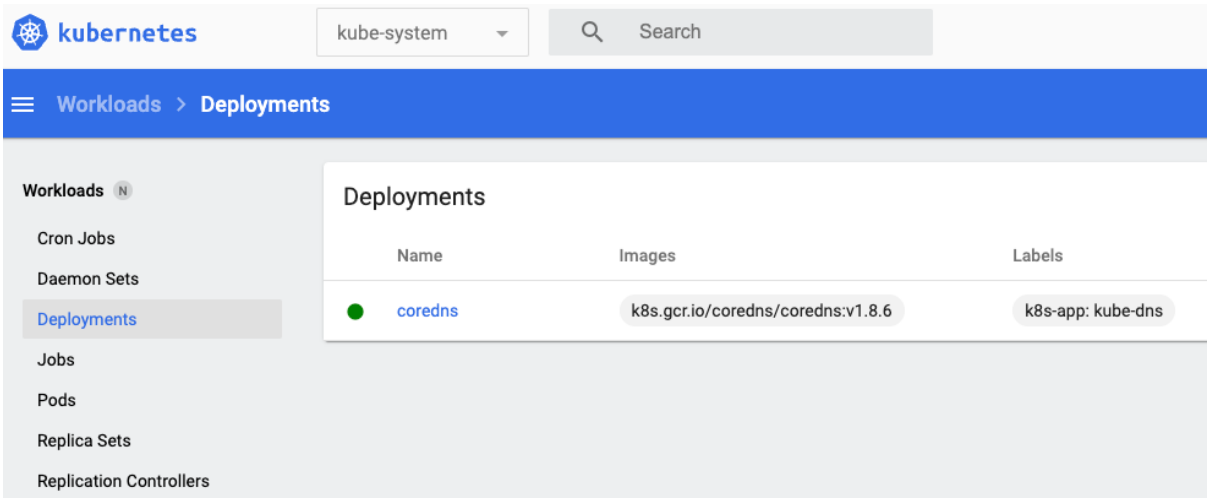
	Name	Namespace	Images	Labels	Node	Status	Restarts	CPU Usage (cores)	Memory Usage (bytes)
●	nginx-deployment-588c8d7b4b-5fllw	default	nginx:latest	app: nginxdeployment pod-template-hash: 588c8d7b4b	minikube	Running	0	0.00m	3.80Mi
●	nginx-deployment-588c8d7b4b-6dm7m	default	nginx:latest	app: nginxdeployment pod-template-hash: 588c8d7b4b	minikube	Running	0	0.00m	3.82Mi

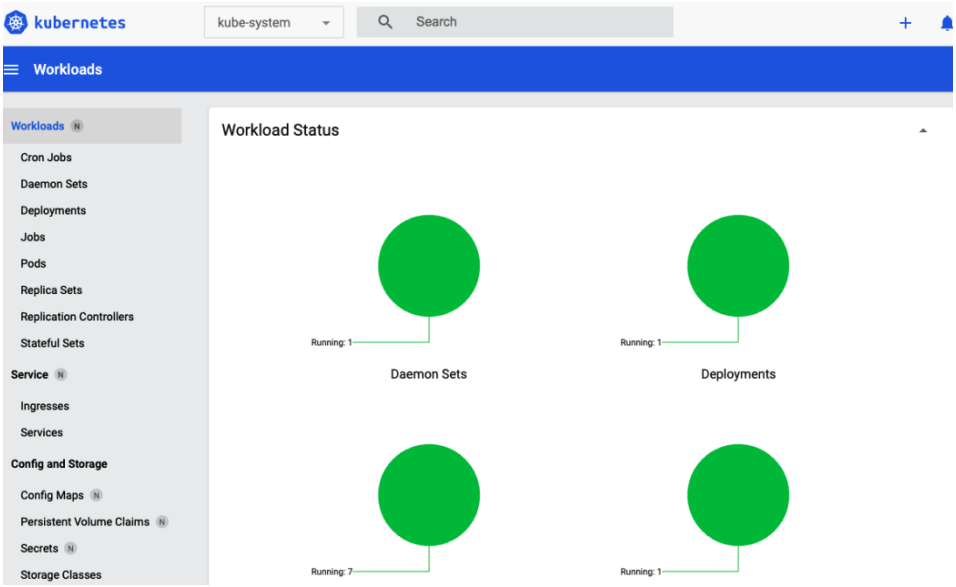

Prometheus
Alerts
Graph
Status
Help
Service Discovery
nginx
kubernetes-apiservers (0 / 2 active targets)
kubernetes-service-endpoints (0 / 2 active targets)
kubernetes-service-endpoints-slow (0 / 2 active targets)
kubernetes-pods (0 / 2 active targets)
kubernetes-pods-slow (0 / 2 active targets)
kubernetes-services (0 / 1 active targets)
prometheus-pushgateway (0 / 1 active targets)
kubernetes-apiservers show more
kubernetes-service-endpoints show more
kubernetes-service-endpoints-slow show more
kubernetes-pods show less
Discovered Labels
__address__="172.17.0.5:80"
__meta_kubernetes_namespace="default"
__meta_kubernetes_pod_container_init="false"
__meta_kubernetes_pod_container_name="nginxdeployment"
__meta_kubernetes_pod_container_port_number="80"
__meta_kubernetes_pod_container_port_protocol="TCP"
__meta_kubernetes_pod_controller_kind="ReplicaSet"
__meta_kubernetes_pod_controller_name="nginx-deployment-588c8d7b4b"
__meta_kubernetes_pod_host_ip="192.168.49.2"
__meta_kubernetes_pod_ip="172.17.0.5"
__meta_kubernetes_pod_label_app="nginxdeployment"
__meta_kubernetes_pod_label_pod_template_hash="588c8d7b4b"
__meta_kubernetes_pod_labelpresent_app="true"


If Everything Is a...
Demo-Apps
nginx
1/1
Consulting
Dashboard - Micr...
Home
Prometheus
Alerts
Graph
Status
Help
Use local time
Enable query history
Enable autocomplete
Enable highlighting
Enable linter
kube_service_info
Execute
Table
Graph
Load time: 7ms
Resolution: 14s
Result series: 11
Evaluation time
kube_service_info{app_kubernetes_io_component="metrics", app_kubernetes_io_instance="prometheus", app_kubernetes_io_managed_by="Helm", app_kubernetes_io_name="kube-state-metrics", app_kubernetes_io_part_of="kube-state-metrics", app_kubernetes_io_version="2.5.0", cluster_ip="10.105.171.48", helm_sh_chart="kube-state-metrics-4.13.0", instance="172.17.0.8:8080", job="kubernetes-service-endpoints", namespace="default", node="minikube", service="prometheus-node-exporter", uid="ffee43fb-ab8d-4a66-9809-5f153db0062e"} 1
kube_service_info{app_kubernetes_io_component="metrics", app_kubernetes_io_instance="prometheus", app_kubernetes_io_managed_by="Helm", app_kubernetes_io_name="kube-state-metrics", app_kubernetes_io_part_of="kube-state-metrics", app_kubernetes_io_version="2.5.0", cluster_ip="10.105.242.252", helm_sh_chart="kube-state-metrics-4.13.0", instance="172.17.0.8:8080", job="kubernetes-service-endpoints", namespace="default", node="minikube", service="prometheus-kube-state-metrics", uid="3d80a393-aab5-4cf0-ac4b-9eaca80ac9d4"} 1
kube_service_info{app_kubernetes_io_component="metrics", app_kubernetes_io_instance="prometheus", app_kubernetes_io_managed_by="Helm", app_kubernetes_io_name="kube-state-metrics", app_kubernetes_io_part_of="kube-state-metrics", app_kubernetes_io_version="2.5.0", cluster_ip="10.105.255.209", helm_sh_chart="kube-state-metrics-4.13.0", instance="172.17.0.8:8080", job="kubernetes-service-endpoints", namespace="kubernetes-dashboard", node="minikube", service="dashboard-metrics-scraper", uid="2356d846-e6b5-41da-abc3-e2b9c255443b"} 1
kube_service_info{app_kubernetes_io_component="metrics", app_kubernetes_io_instance="prometheus", app_kubernetes_io_managed_by="Helm", app_kubernetes_io_name="kube-state-metrics", app_kubernetes_io_part_of="kube-state-metrics", app_kubernetes_io_version="2.5.0", cluster_ip="10.107.73.252", helm_sh_chart="kube-state-metrics-4.13.0", instance="172.17.0.8:8080", job="kubernetes-service-endpoints", namespace="kube-system", node="minikube", service="metrics-server", uid="74a693ca-8160-44ab-b65c-7600f4fa5a48"} 1
kube_service_info{app_kubernetes_io_component="metrics", app_kubernetes_io_instance="prometheus", app_kubernetes_io_managed_by="Helm", app_kubernetes_io_name="kube-state-metrics", app_kubernetes_io_part_of="kube-state-metrics", app_kubernetes_io_version="2.5.0", cluster_ip="10.109.190.63", helm_sh_chart="kube-state-metrics-4.13.0", instance="172.17.0.8:8080", job="kubernetes-service-endpoints", namespace="default", node="minikube", service="nginxservice", uid="1896b66a-219d-4091-ad2e-4e5f129d83a1"} 1

```
✨  Automatically selected the docker driver
👍  Starting control plane node minikube in cluster minikube
🚜  Pulling base image ...
🔥  Creating docker container (CPUs=2, Memory=4000MB) ...
🐳  Preparing Kubernetes v1.23.1 on Docker 20.10.12 ...
    ▪ kubelet.housekeeping-interval=5m
    ▪ Generating certificates and keys ...
    ▪ Booting up control plane ...
    ▪ Configuring RBAC rules ...
🔎  Verifying Kubernetes components...
    ▪ Using image gcr.io/k8s-minikube/storage-provisioner:v5
🌟  Enabled addons: default-storageclass, storage-provisioner
🏄  Done! kubectl is now configured to use "minikube" cluster and "default" namespace by default
```







aemon Sets

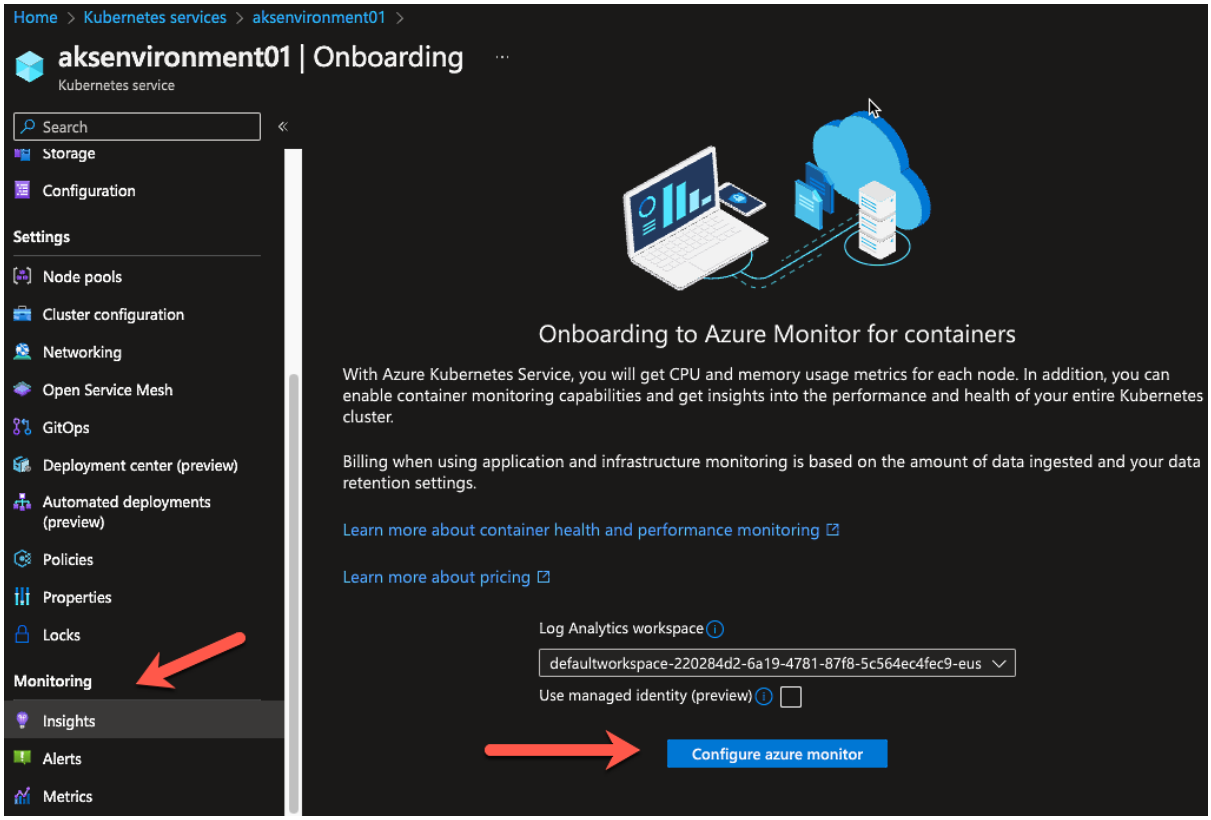
	Name	Images	Labels	Pods
●	kube-proxy	k8s.gcr.io/kube-proxy:v1.23.1	k8s-app: kube-proxy	1 / 1

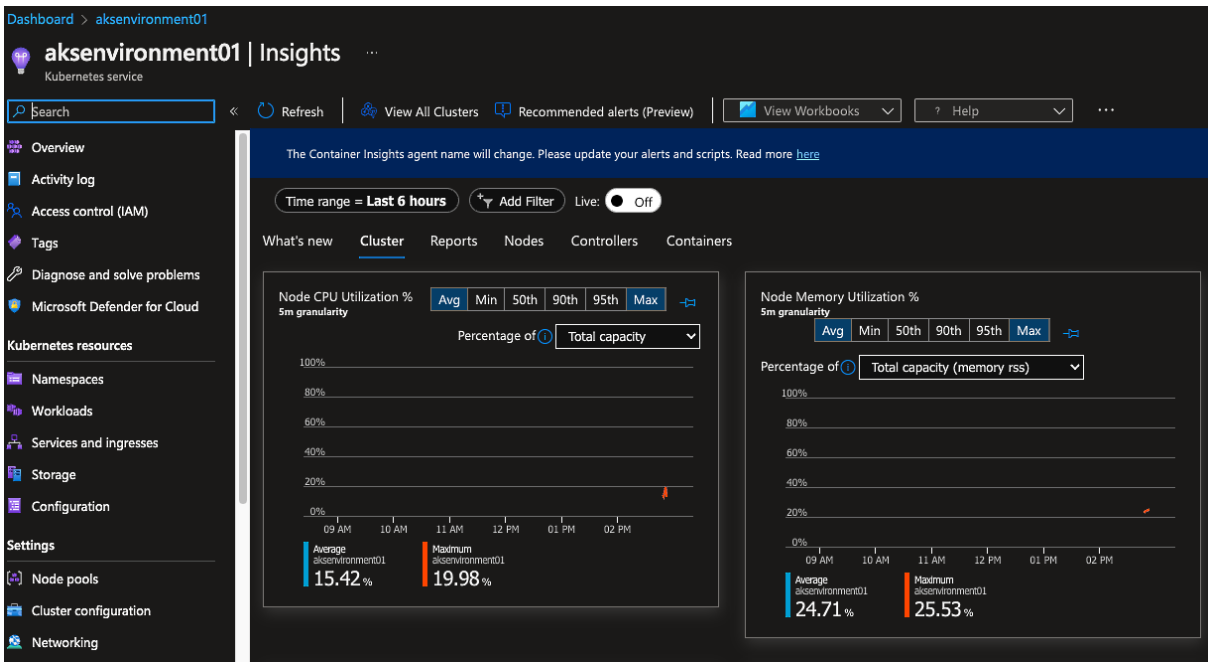
eployments

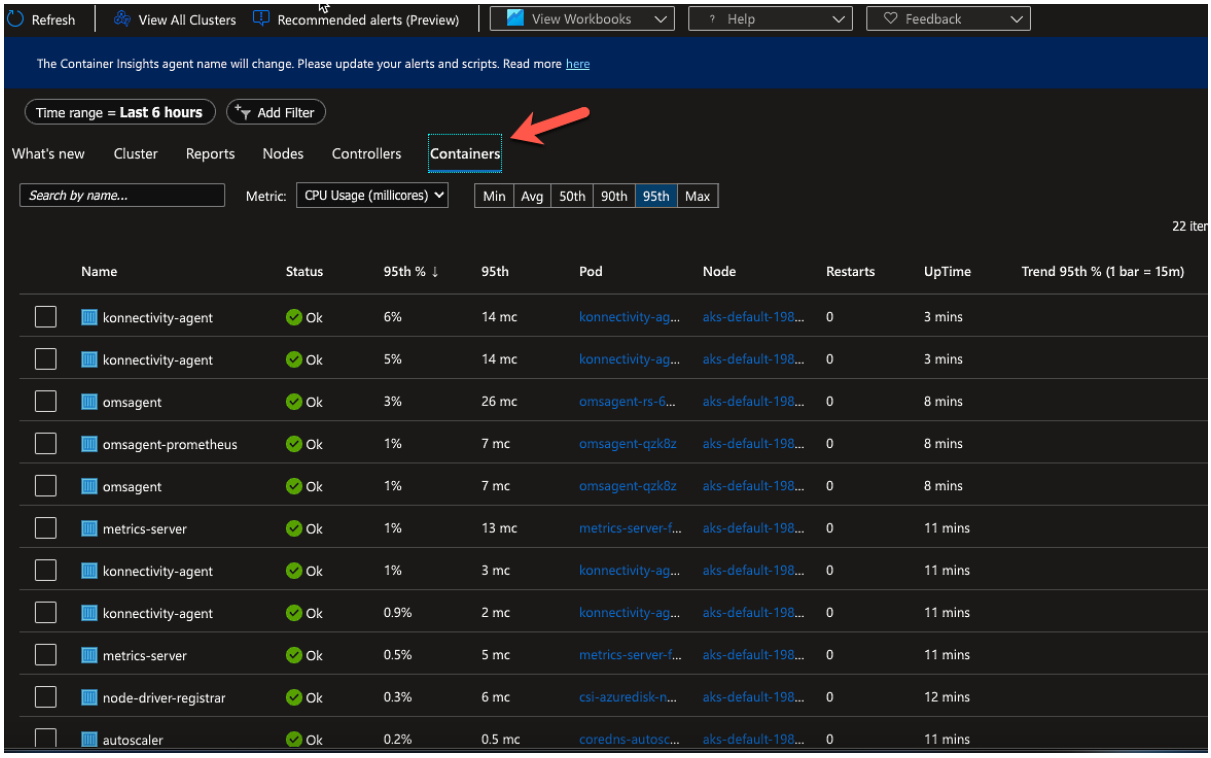
	Name	Images	Labels	Pods
●	coredns	k8s.gcr.io/coredns/coredns:v1.8.6	k8s-app: kube-dns	1 / 1

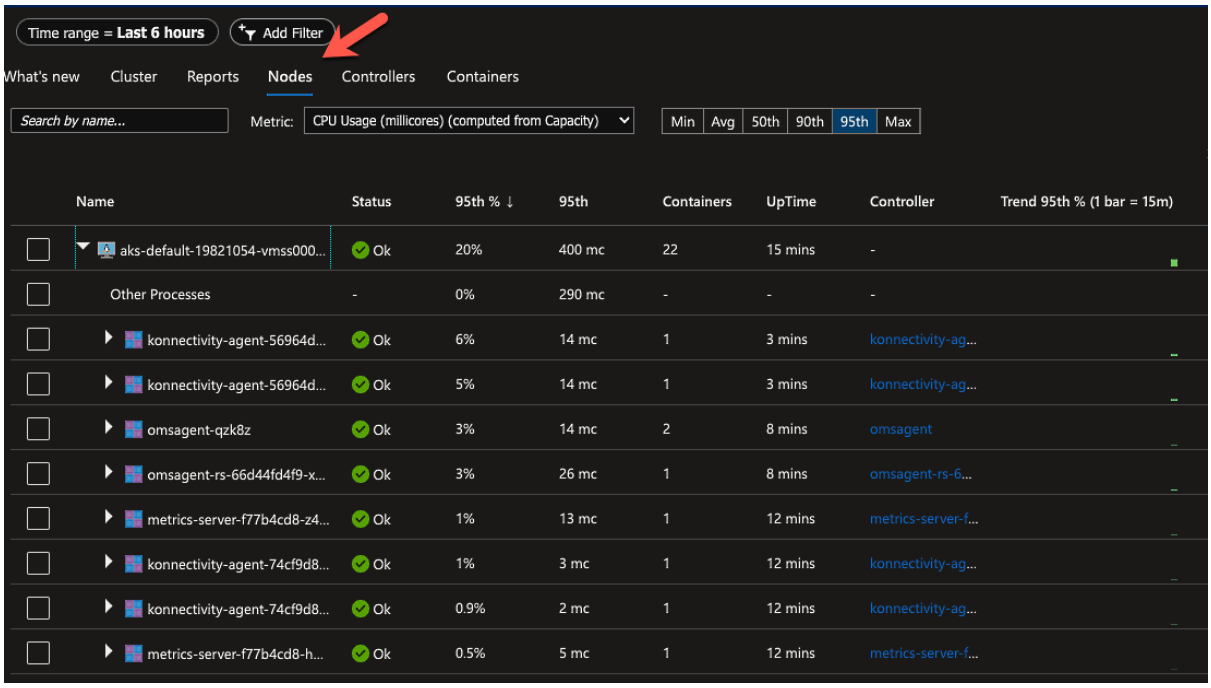
ods

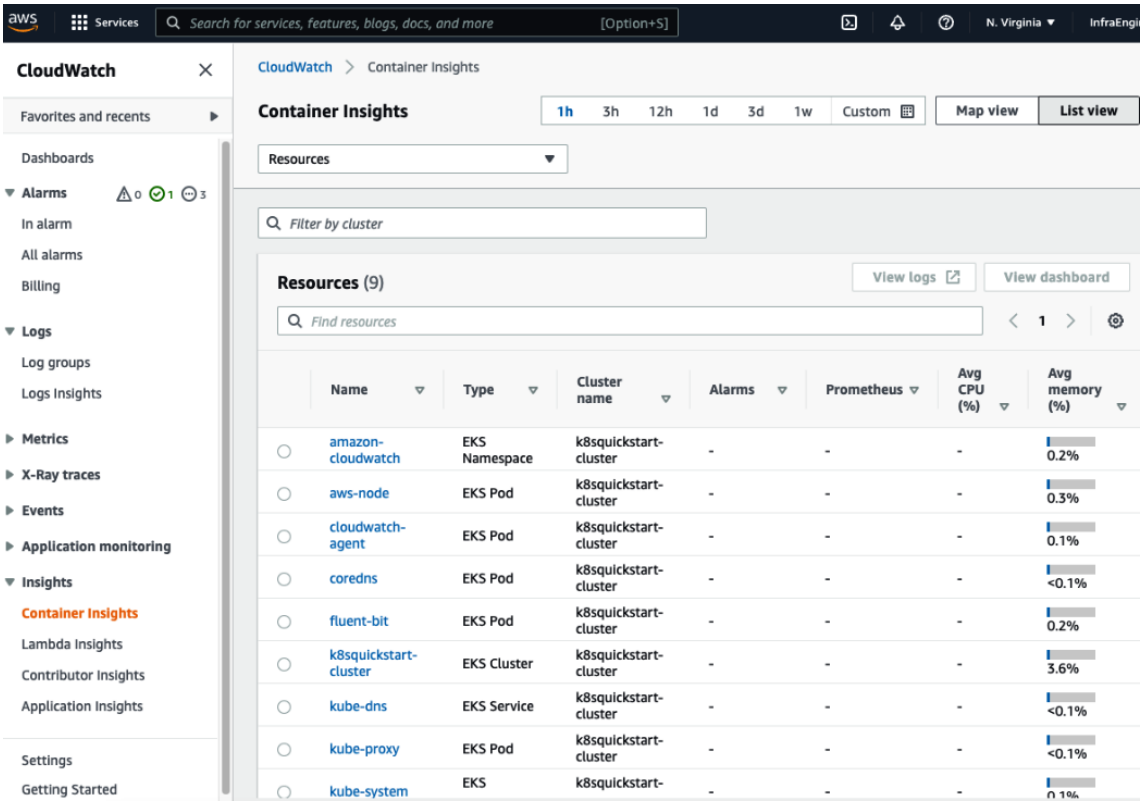
	Name	Images	Labels	Node	Status	Restarts	CPU Usage (cores)
●	coredns-64897985d-v9j6b	k8s.gcr.io/coredns/coredns:v1.8.6	k8s-app: kube-dns pod-template-hash: 64897985d	minikube	Running	0	-
●	kube-proxy-lsk69	k8s.gcr.io/kube-proxy:v1.23.1	controller-revision-hash: 8485885f8b k8s-app: kube-proxy pod-template-generation: 1	minikube	Running	0	-
●	storage-provisioner	gcr.io/k8s-minikube/storage-provisioner:v5	addonmanager.kubernetes.io/mode: Reconcile integration-test: storage-provisioner	minikube	Running	1	-


Home > Kubernetes services > aksenvironment01 >
aksenvironment01 | Onboarding
Kubernetes service
Search
Storage
Configuration
Settings
Node pools
Cluster configuration
Networking
Open Service Mesh
GitOps
Deployment center (preview)
Automated deployments (preview)
Policies
Properties
Locks
Monitoring
Insights
Alerts
Metrics
Onboarding to Azure Monitor for containers
With Azure Kubernetes Service, you will get CPU and memory usage metrics for each node. In addition, you can enable container monitoring capabilities and get insights into the performance and health of your entire Kubernetes cluster.
Billing when using application and infrastructure monitoring is based on the amount of data ingested and your data retention settings.
Learn more about container health and performance monitoring
Learn more about pricing
Log Analytics workspace
defaultworkspace-220284d2-6a19-4781-87f8-5c564ec4fec9-eus
Use managed identity (preview)
Configure azure monitor

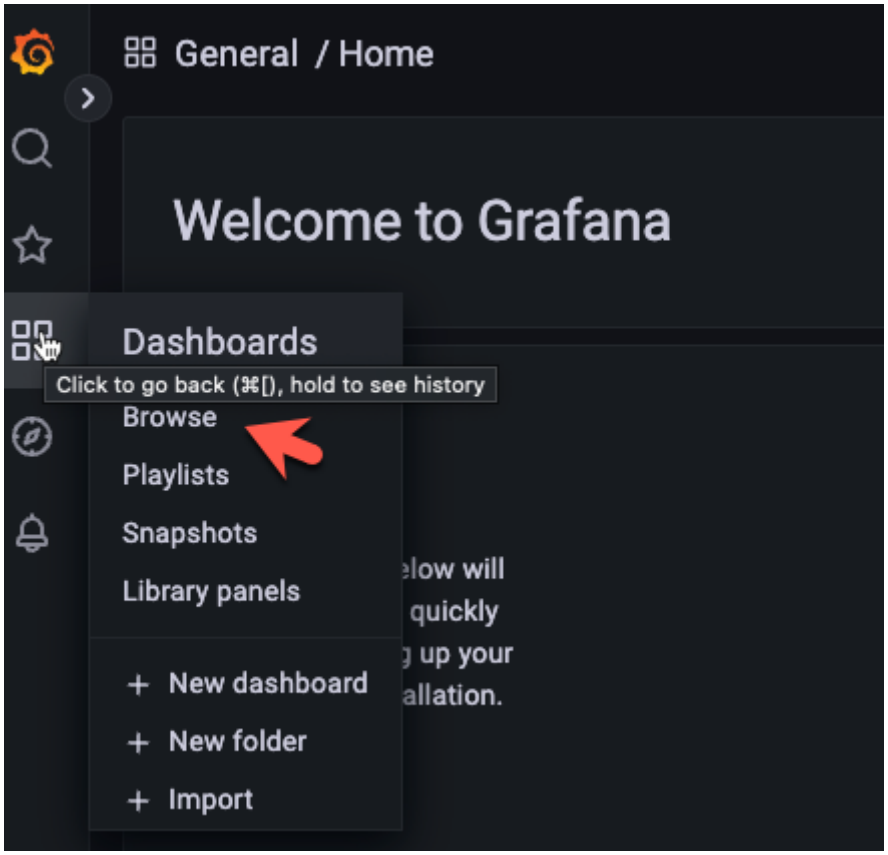

Dashboard > aksenvironment01
aksenvironment01 | Insights
Kubernetes service
Search
Refresh
View All Clusters
Recommended alerts (Preview)
View Workbooks
Help
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Microsoft Defender for Cloud
Kubernetes resources
Namespaces
Workloads
Services and ingresses
Storage
Configuration
Settings
Node pools
Cluster configuration
Networking
The Container Insights agent name will change. Please update your alerts and scripts. Read more here
Time range = Last 6 hours
Add Filter
Live: Off
What's new
Cluster
Reports
Nodes
Controllers
Containers
Node CPU Utilization %
5m granularity
Avg Min 50th 90th 95th Max
Percentage of
Total capacity
100%
80%
60%
40%
20%
0%
09 AM 10 AM 11 AM 12 PM 01 PM 02 PM
Average aksenvironment01 15.42 %
Maximum aksenvironment01 19.98 %
Node Memory Utilization %
5m granularity
Avg Min 50th 90th 95th Max
Percentage of
Total capacity (memory rss)
100%
80%
60%
40%
20%
0%
09 AM 10 AM 11 AM 12 PM 01 PM 02 PM
Average aksenvironment01 24.71 %
Maximum aksenvironment01 25.53 %

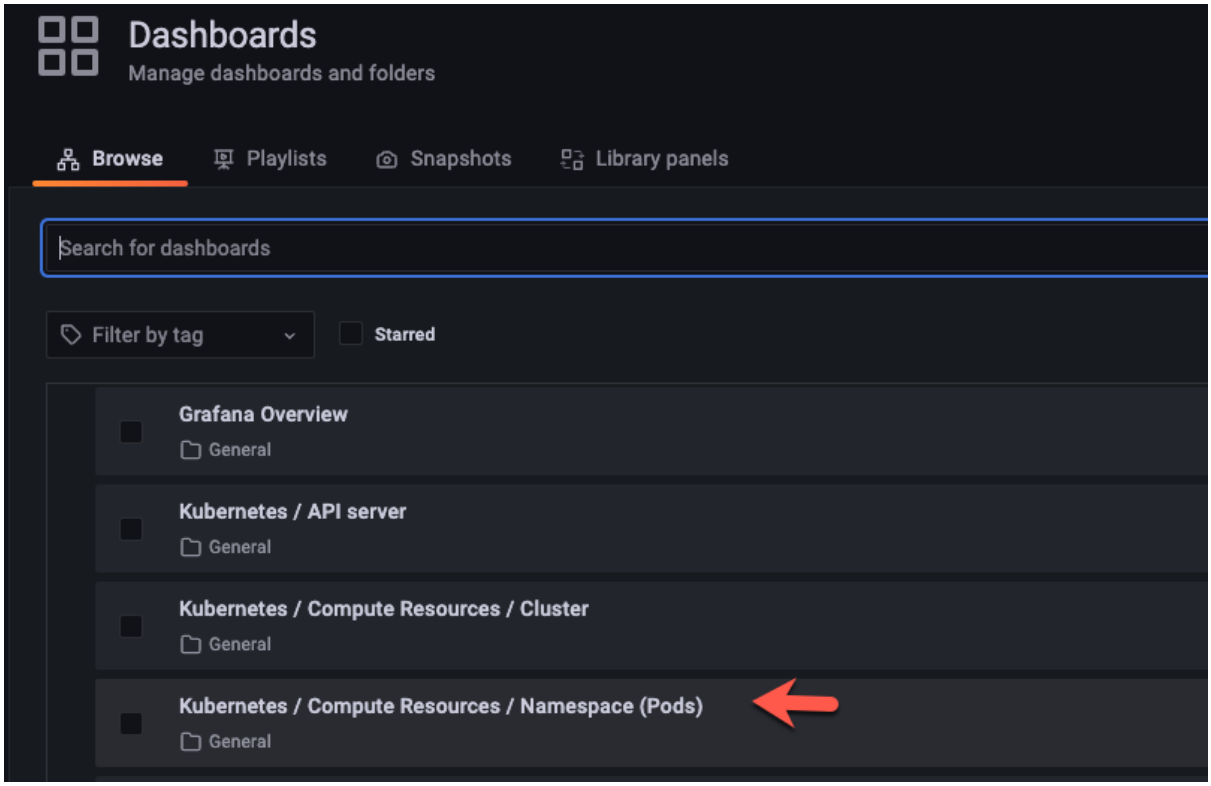

Refresh
View All Clusters
Recommended alerts (Preview)
View Workbooks
Help
Feedback
The Container Insights agent name will change. Please update your alerts and scripts. Read more here
Time range = Last 6 hours
Add Filter
What's new
Cluster
Reports
Nodes
Controllers
Containers
Search by name...
Metric:
CPU Usage (millicores)
Min
Avg
50th
90th
95th
Max
22 iter
Name
Status
95th % ↓
95th
Pod
Node
Restarts
UpTime
Trend 95th % (1 bar = 15m)
konnectivity-agent Ok 6% 14 mc konnectivity-ag... aks-default-198... 0 3 mins
konnectivity-agent Ok 5% 14 mc konnectivity-ag... aks-default-198... 0 3 mins
omsagent Ok 3% 26 mc omsagent-rs-6... aks-default-198... 0 8 mins
omsagent-prometheus Ok 1% 7 mc omsagent-qzk8z aks-default-198... 0 8 mins
omsagent Ok 1% 7 mc omsagent-qzk8z aks-default-198... 0 8 mins
metrics-server Ok 1% 13 mc metrics-server-f... aks-default-198... 0 11 mins
konnectivity-agent Ok 1% 3 mc konnectivity-ag... aks-default-198... 0 11 mins
konnectivity-agent Ok 0.9% 2 mc konnectivity-ag... aks-default-198... 0 11 mins
metrics-server Ok 0.5% 5 mc metrics-server-f... aks-default-198... 0 11 mins
node-driver-registrar Ok 0.3% 6 mc csi-azuredisk-n... aks-default-198... 0 12 mins
autoscaler Ok 0.2% 0.5 mc coredns-autosc... aks-default-198... 0 11 mins

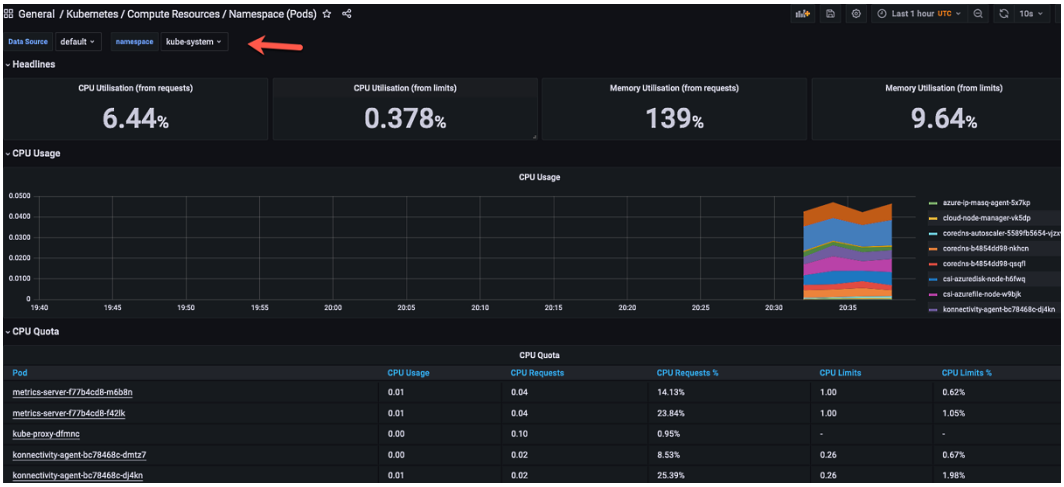

Time range = Last 6 hours
Add Filter
What's new
Cluster
Reports
Nodes
Controllers
Containers
Search by name...
Metric:
CPU Usage (millicores) (computed from Capacity)
Min
Avg
50th
90th
95th
Max
Name
Status
95th % ↓
95th
Containers
UpTime
Controller
Trend 95th % (1 bar = 15m)
aks-default-19821054-vmss000... Ok 20% 400 mc 22 15 mins -
Other Processes - 0% 290 mc - - -
konnectivity-agent-56964d... Ok 6% 14 mc 1 3 mins konnectivity-ag...
konnectivity-agent-56964d... Ok 5% 14 mc 1 3 mins konnectivity-ag...
omsagent-qzk8z Ok 3% 14 mc 2 8 mins omsagent
omsagent-rs-66d44fd4f9-x... Ok 3% 26 mc 1 8 mins omsagent-rs-6...
metrics-server-f77b4cd8-z4... Ok 1% 13 mc 1 12 mins metrics-server-f...
konnectivity-agent-74cf9d8... Ok 1% 3 mc 1 12 mins konnectivity-ag...
konnectivity-agent-74cf9d8... Ok 0.9% 2 mc 1 12 mins konnectivity-ag...
metrics-server-f77b4cd8-h... Ok 0.5% 5 mc 1 12 mins metrics-server-f...

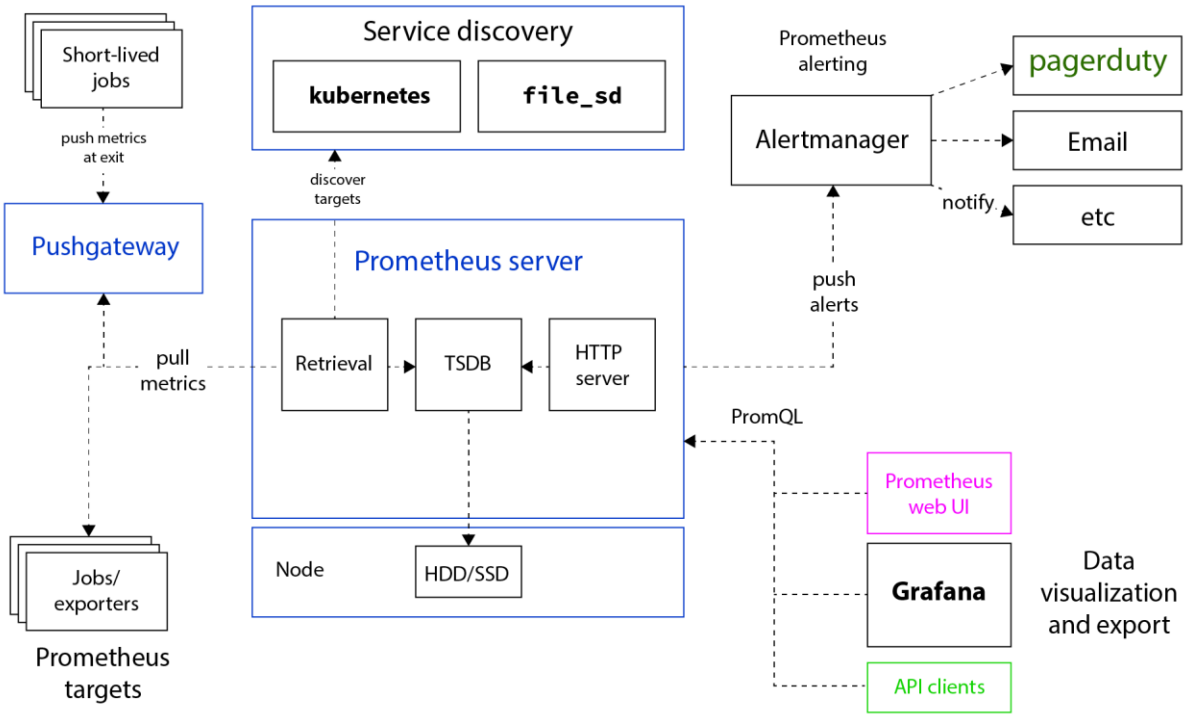



```
NAME                                    READY   STATUS    RESTARTS   AGE
pod/azure-ip-masq-agent-5x7kp           1/1     Running   0          20m
pod/cloud-node-manager-vk5dp            1/1     Running   0          20m
pod/coredns-autoscaler-5589fb5654-vjzxw 1/1     Running   0          21m
pod/coredns-b4854dd98-nkhcn             1/1     Running   0          21m
pod/coredns-b4854dd98-qsqfl             1/1     Running   0          19m
pod/csi-azuredisk-node-h6fwq            3/3     Running   0          20m
pod/csi-azurefile-node-w9bjk            3/3     Running   0          20m
pod/konnectivity-agent-5bc84fc8b7-p4mbz 1/1     Running   0          21m
pod/konnectivity-agent-5bc84fc8b7-zn54t 1/1     Running   0          21m
pod/kube-proxy-dfmnc                    1/1     Running   0          20m
pod/metrics-server-f77b4cd8-f42lk       1/1     Running   0          21m
pod/metrics-server-f77b4cd8-m6b8n       1/1     Running   0          21m
```


General / Home
Welcome to Grafana
Dashboards
Click to go back (⌘[), hold to see history
Browse
Playlists
Snapshots
Library panels
New dashboard
New folder
Import


Dashboards
Manage dashboards and folders
Browse
Playlists
Snapshots
Library panels
Search for dashboards
Filter by tag
Starred
Grafana Overview
General
Kubernetes / API server
General
Kubernetes / Compute Resources / Cluster
General
Kubernetes / Compute Resources / Namespace (Pods)
General



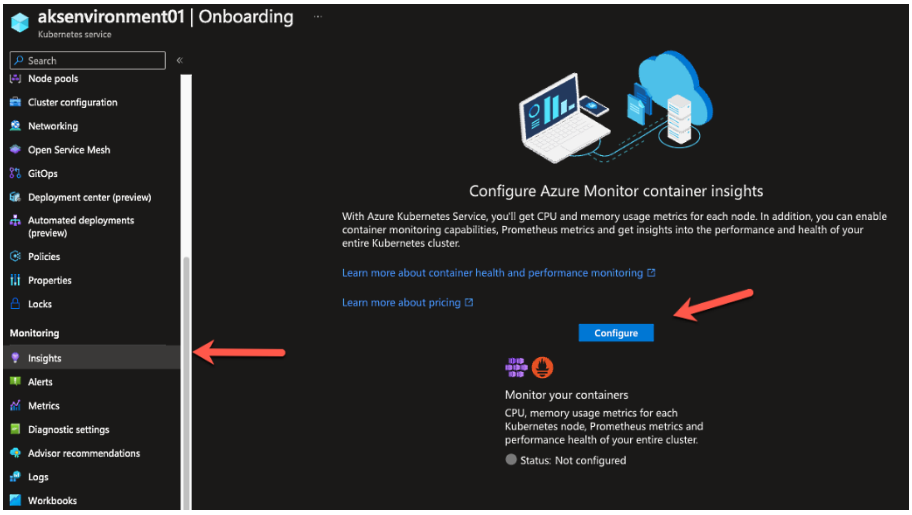


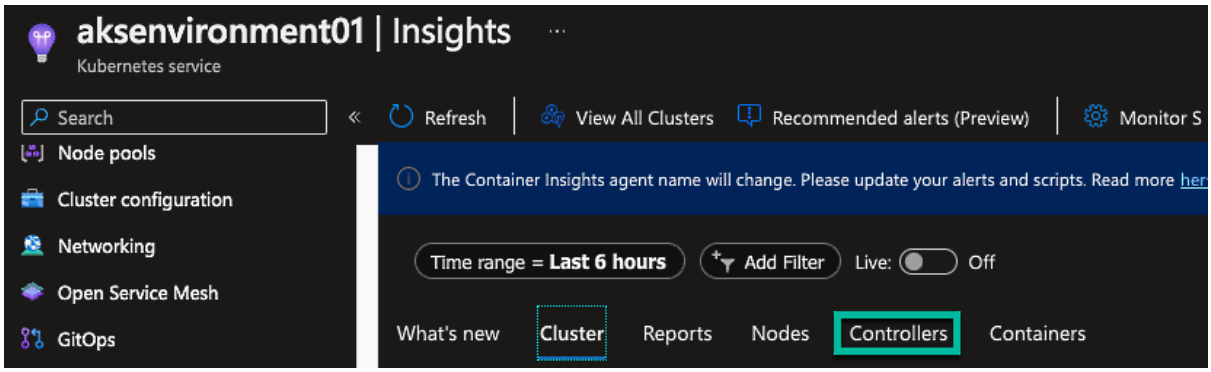

```
NAME                                      READY   STATUS    RESTARTS   AGE
azure-ip-masq-agent-wmrg5                 1/1     Running   0          24m
cloud-node-manager-zwc64                  1/1     Running   0          24m
coredns-autoscaler-5589fb5654-lx62m       1/1     Running   0          25m
coredns-b4854dd98-bxfxv                   1/1     Running   0          25m
coredns-b4854dd98-npvb6                   1/1     Running   0          23m
csi-azuredisk-node-mjxp4                  3/3     Running   0          24m
csi-azurefile-node-4twwr                  3/3     Running   0          24m
konnectivity-agent-5488874d6f-945qs       1/1     Running   0          7m3s
konnectivity-agent-5488874d6f-frx8c       1/1     Running   0          7m5s
kube-proxy-cv9xq                          1/1     Running   0          24m
metrics-server-f77b4cd8-r9f6d             1/1     Running   0          25m
metrics-server-f77b4cd8-x84bs             1/1     Running   0          25m
```

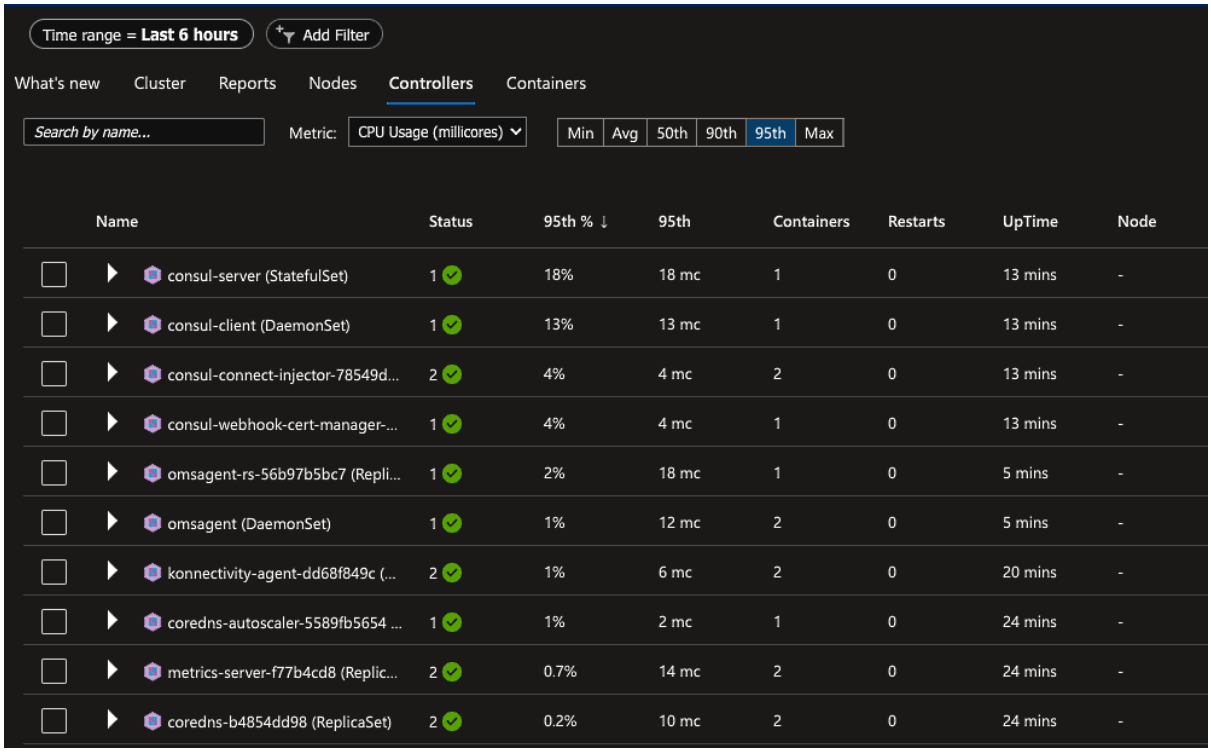
```
apiVersion: v1
data:
  ClusterConfiguration: |
    apiServer:
      extraArgs:
        authorization-mode: Node,RBAC
      timeoutForControlPlane: 4m0s
    apiVersion: kubeadm.k8s.io/v1beta3
    certificatesDir: /etc/kubernetes/pki
    serverTLSBootstrap: true
    clusterName: kubernetes
    controlPlaneEndpoint: 192.168.1.61:6443
    controllerManager: {}
    dns: {}
    etcd:
      local:
        dataDir: /var/lib/etcd
    imageRepository: registry.k8s.io
    kind: ClusterConfiguration
    kubernetesVersion: v1.25.2
    networking:
      dnsDomain: cluster.local
      podSubnet: 172.17.0.0/16
      serviceSubnet: 10.96.0.0/12
    scheduler: {}
kind: ConfigMap
metadata:
  creationTimestamp: "2022-10-12T21:13:48Z"
  name: kubeadm-config
  namespace: kube-system
  resourceVersion: "396121"
  uid: d359b06d-a128-499e-b2ee-ef29bd5c1e28
~
"/tmp/kubectl-edit-3472111723.yaml" 36L, 1052B
```

```
apiVersion: kubelet.config.k8s.io/v1beta1
serverTLSBootstrap: true
authentication:
  anonymous:
    enabled: false
  webhook:
    cacheTTL: 0s
    enabled: true
  x509:
    clientCAFile: /etc/kubernetes/pki/ca.crt
authorization:
  mode: Webhook
  webhook:
    cacheAuthorizedTTL: 0s
    cacheUnauthorizedTTL: 0s
cgroupDriver: systemd
clusterDNS:
```

```
☁  aks [main] ⚡  curl -sL https://run.linkerd.io/emojivoto.yml \
  | sed 's|    metadata:|    metadata:\n      annotations:\n        consul.hashicorp.com/connect-inject: "true"|' \
  | sed 's|targetPort: 8080|targetPort: 20000|' \
  | kubectl apply -f -
namespace/emojivoto created
serviceaccount/emoji created
serviceaccount/voting created
serviceaccount/web created
service/emoji-svc created
service/voting-svc created
service/web-svc created
deployment.apps/emoji created
deployment.apps/vote-bot created
deployment.apps/voting created
deployment.apps/web created
```



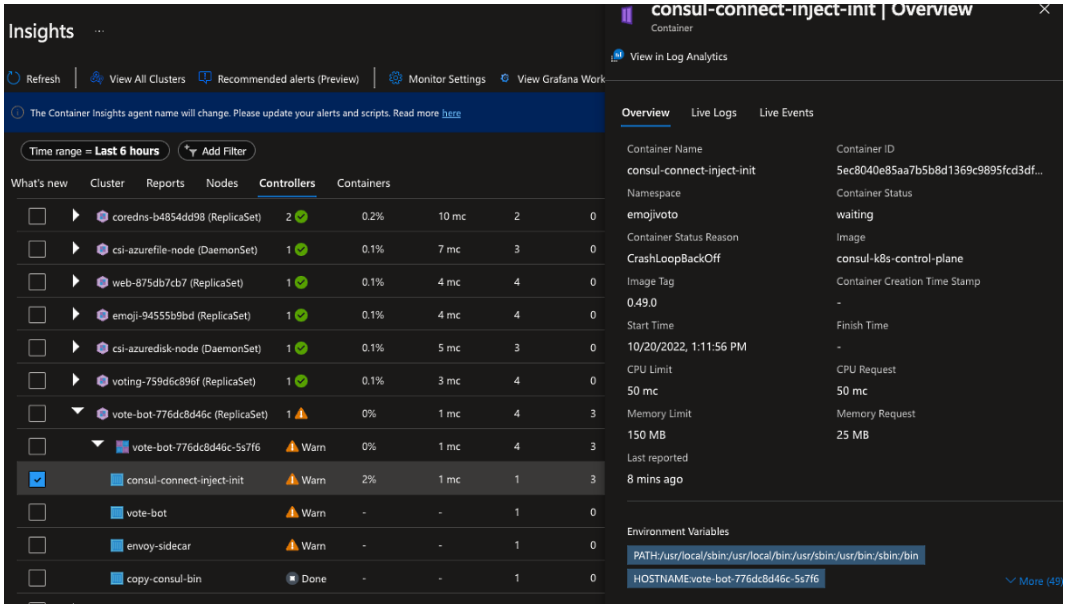




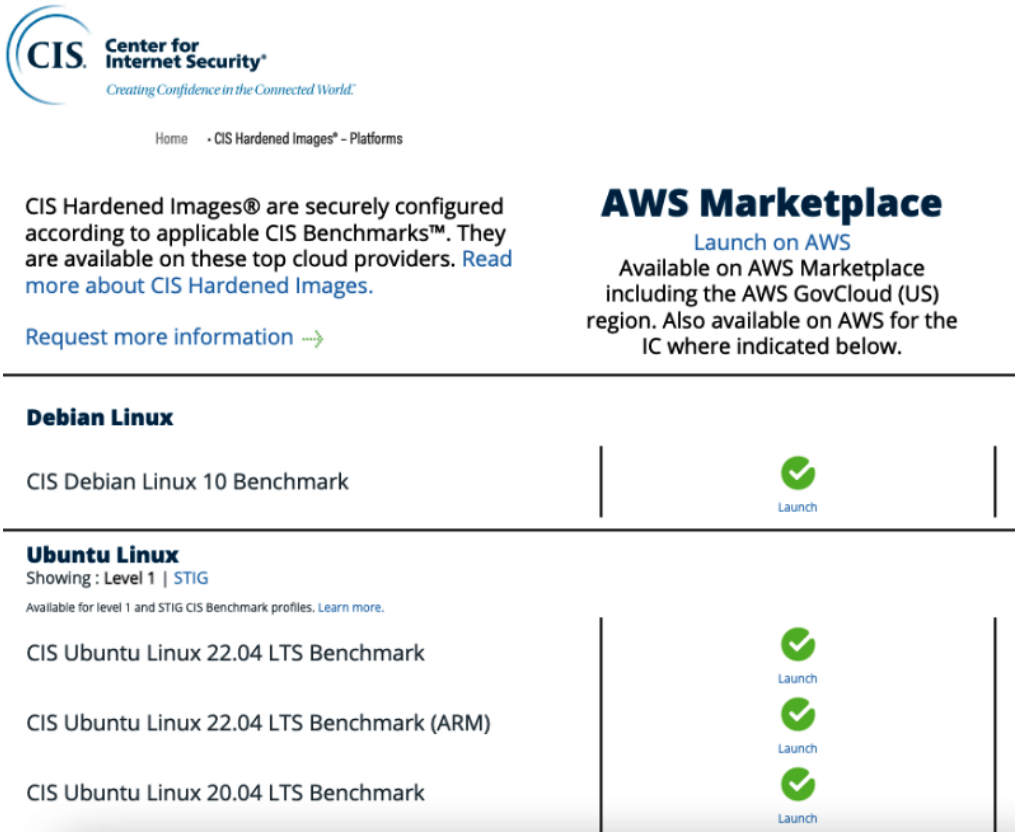
Name	Status	95th % ↓	95th	Containers	Restarts	UpTime	Node
consul-server (StatefulSet)	1	18%	18 mc	1	0	13 mins	-
consul-client (DaemonSet)	1	13%	13 mc	1	0	13 mins	-
consul-connect-injector-78549d...	2	4%	4 mc	2	0	13 mins	-
consul-webhook-cert-manager-...	1	4%	4 mc	1	0	13 mins	-
omsagent-rs-56b97b5bc7 (Repli...	1	2%	18 mc	1	0	5 mins	-
omsagent (DaemonSet)	1	1%	12 mc	2	0	5 mins	-
konnectivity-agent-dd68f849c (...	2	1%	6 mc	2	0	20 mins	-
coredns-autoscaler-5589fb5654 ...	1	1%	2 mc	1	0	24 mins	-
metrics-server-f77b4cd8 (Replic...	2	0.7%	14 mc	2	0	24 mins	-
coredns-b4854dd98 (ReplicaSet)	2	0.2%	10 mc	2	0	24 mins	-

emoji-94555b9bd-whh6k	Ok	0.2%	4 mc	4	7 mins	emoji-94555b9bd
envoy-sidecar	Ok	0.2%	3 mc	1	7 mins	emoji-94555b9bd
emoji-svc	Ok	0%	0.8 mc	1	8 mins	emoji-94555b9bd
copy-consul-bin	Done	-	-	1	-	emoji-94555b9bd
consul-connect-inject-init	Done	-	-	1	-	emoji-94555b9bd
voting-759d6c896f-9njg9	Ok	0.2%	3 mc	4	7 mins	voting-759d6c896f
envoy-sidecar	Ok	0.1%	2 mc	1	7 mins	voting-759d6c896f
voting-svc	Ok	0%	0.9 mc	1	8 mins	voting-759d6c896f
copy-consul-bin	Done	-	-	1	-	voting-759d6c896f
consul-connect-inject-init	Done	-	-	1	-	voting-759d6c896f

vote-bot-776dc8d46c (ReplicaSet)	1	0%	1 mc	4	3	3 mins	-
vote-bot-776dc8d46c-5s7f6	Warn	0%	1 mc	4	3	N/A	aks-default-115...
consul-connect-inject-init	Warn	2%	1 mc	1	3	0 msec	aks-default-115...
vote-bot	Warn	-	-	1	0	0 msec	aks-default-115...
envoy-sidecar	Warn	-	-	1	0	0 msec	aks-default-115...
copy-consul-bin	Done	-	-	1	0	0 msec	aks-default-115...



Chapter 8: Security Reality Check



CIS Center for Internet Security®
Creating Confidence in the Connected World.

CIS Hardened

Home > CIS Benchmarks > CIS Kubernetes Benchmarks

Securing Kubernetes

An objective, consensus-driven security guideline for the Kubernetes Server Software.

A step-by-step checklist to secure Kubernetes:

DOWNLOAD LATEST CIS BENCHMARK →
FREE TO EVERYONE

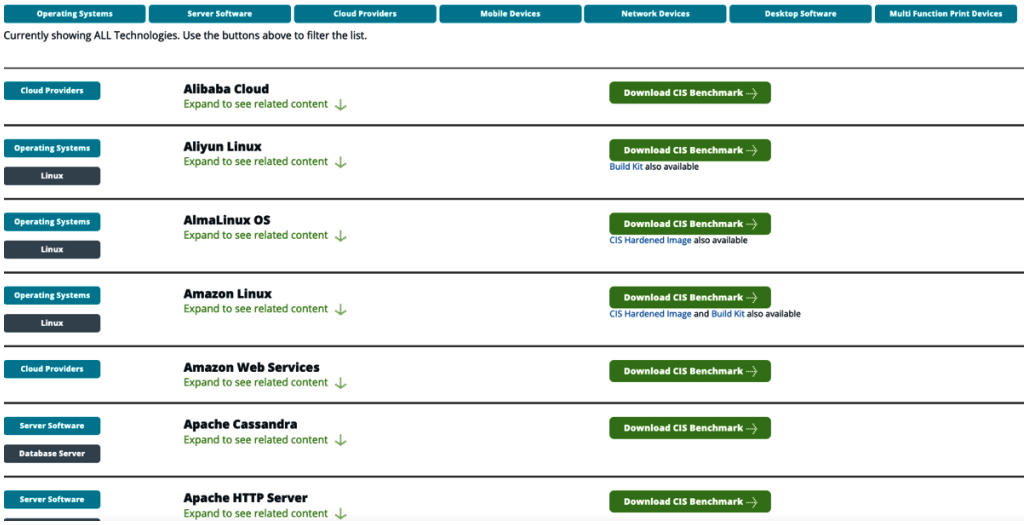
For Kubernetes 1.2.0 (CIS Azure Kubernetes Service (AKS) Benchmark version 1.2.0)

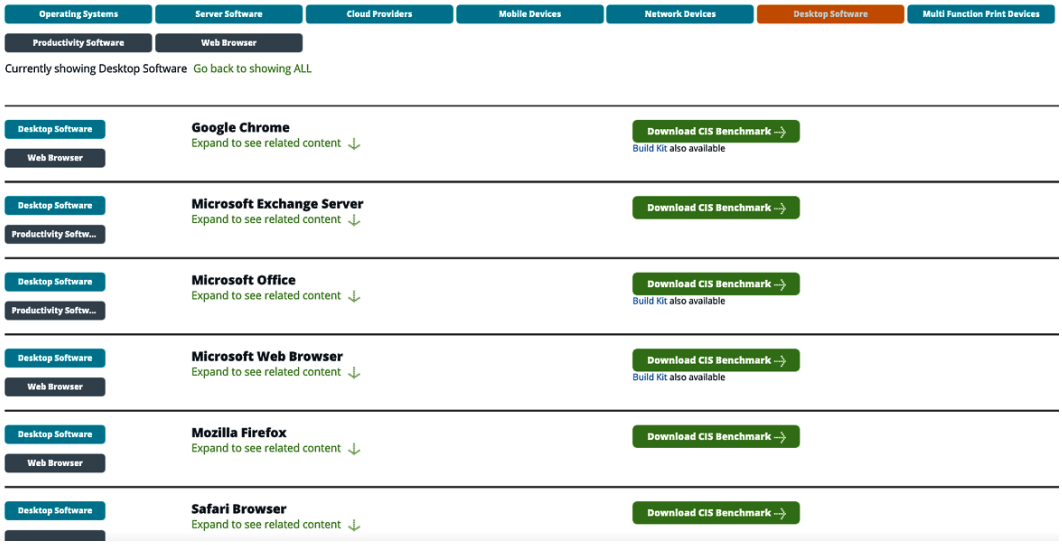
CIS has worked with the community since 2017 to publish a benchmark for Kubernetes.

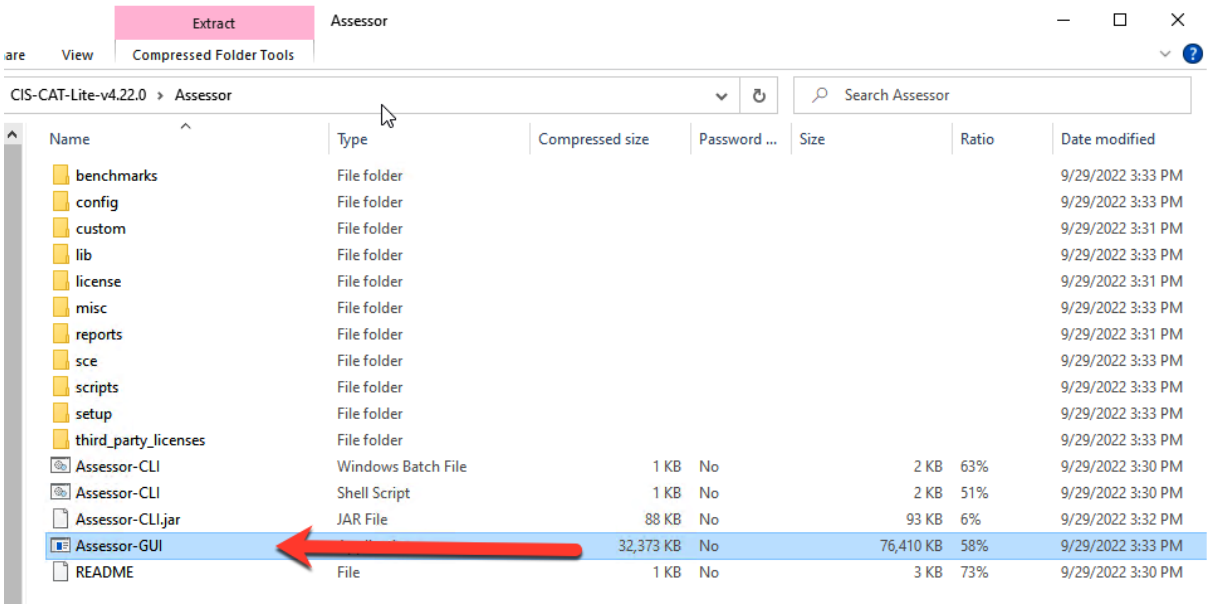
JOIN THE KUBERNETES COMMUNITY →

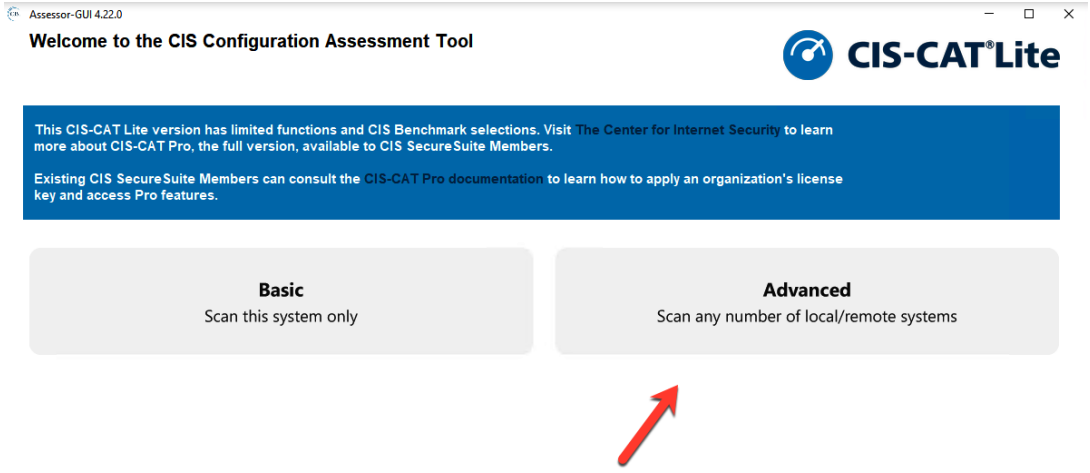
Kubernetes Virtualization

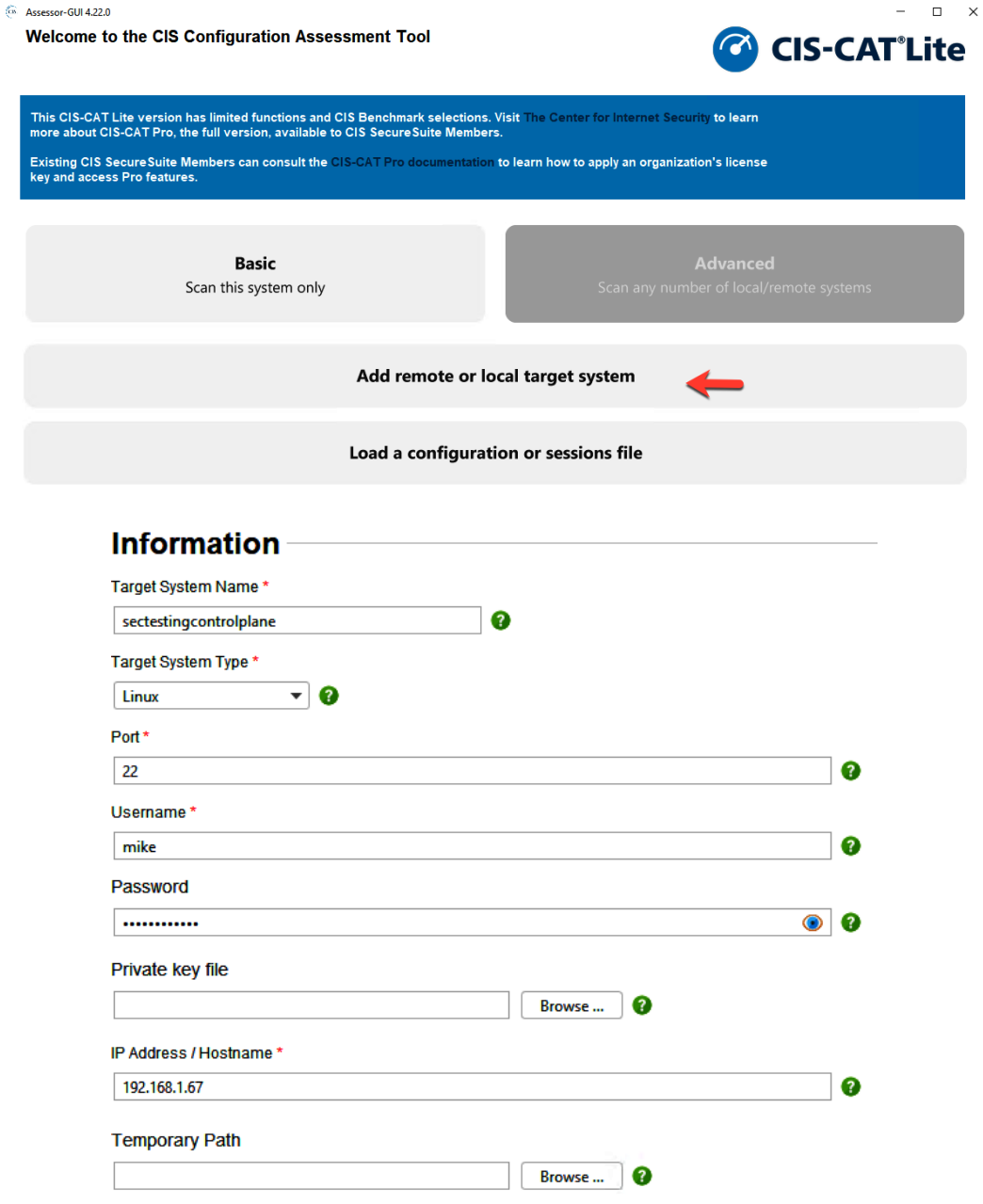
CIS Kubernetes V1.23 Benchmark v1.0.0	Download PDF
CIS Kubernetes V1.24 Benchmark v1.0.0	Download PDF
CIS RedHat OpenShift Container Platform Benchmark v1.2.0	Download PDF
CIS Oracle Cloud Infrastructure Container Engine for Kubernetes(OKE) Benchmark v1.1.0	Download PDF
CIS Kubernetes V1.23 Benchmark v1.0.1	Download PDF
CIS Amazon Elastic Kubernetes Service (EKS) Benchmark v1.1.0	Download PDF
CIS Azure Kubernetes Service (AKS) Benchmark v1.1.0	Download PDF
CIS Google Kubernetes Engine (GKE) Benchmark v1.2.0	Download PDF
CIS Alibaba Cloud Container Service For Kubernetes (ACK) Benchmark v1.0.0	Download PDF
CIS Kubernetes Benchmark v1.6.0	Download PDF
CIS Kubernetes Benchmark v1.5.1	Download PDF


Operating Systems
Server Software
Cloud Providers
Mobile Devices
Network Devices
Desktop Software
Multi Function Print Devices
Currently showing ALL Technologies. Use the buttons above to filter the list.
Cloud Providers
Alibaba Cloud
Expand to see related content
Download CIS Benchmark
Operating Systems
Linux
Aliyun Linux
Expand to see related content
Download CIS Benchmark
Build Kit also available
Operating Systems
Linux
AlmaLinux OS
Expand to see related content
Download CIS Benchmark
CIS Hardened Image also available
Operating Systems
Linux
Amazon Linux
Expand to see related content
Download CIS Benchmark
CIS Hardened Image and Build Kit also available
Cloud Providers
Amazon Web Services
Expand to see related content
Download CIS Benchmark
Server Software
Database Server
Apache Cassandra
Expand to see related content
Download CIS Benchmark
Server Software
Apache HTTP Server
Expand to see related content
Download CIS Benchmark


Operating Systems
Server Software
Cloud Providers
Mobile Devices
Network Devices
Desktop Software
Multi Function Print Devices
Productivity Software
Web Browser
Currently showing Desktop Software Go back to showing ALL
Desktop Software
Web Browser
Google Chrome
Expand to see related content
Download CIS Benchmark
Build Kit also available
Desktop Software
Productivity Softw...
Microsoft Exchange Server
Expand to see related content
Download CIS Benchmark
Desktop Software
Productivity Softw...
Microsoft Office
Expand to see related content
Download CIS Benchmark
Build Kit also available
Desktop Software
Web Browser
Microsoft Web Browser
Expand to see related content
Download CIS Benchmark
Build Kit also available
Desktop Software
Web Browser
Mozilla Firefox
Expand to see related content
Download CIS Benchmark
Desktop Software
Safari Browser
Expand to see related content
Download CIS Benchmark

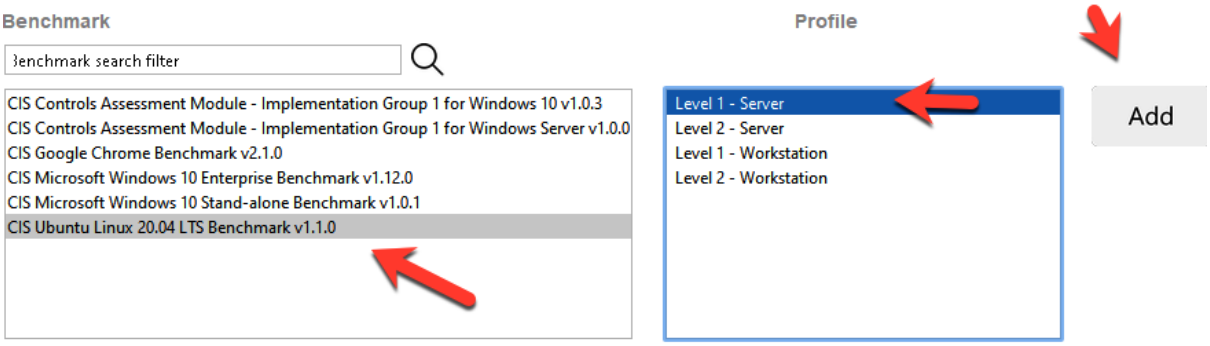

Extract
Assessor
are
View
Compressed Folder Tools
CIS-CAT-Lite-v4.22.0 › Assessor
Search Assessor
Name
Type
Compressed size
Password ...
Size
Ratio
Date modified
benchmarks
File folder
9/29/2022 3:33 PM
config
File folder
9/29/2022 3:33 PM
custom
File folder
9/29/2022 3:31 PM
lib
File folder
9/29/2022 3:33 PM
license
File folder
9/29/2022 3:31 PM
misc
File folder
9/29/2022 3:33 PM
reports
File folder
9/29/2022 3:31 PM
sce
File folder
9/29/2022 3:33 PM
scripts
File folder
9/29/2022 3:33 PM
setup
File folder
9/29/2022 3:33 PM
third_party_licenses
File folder
9/29/2022 3:33 PM
Assessor-CLI
Windows Batch File
1 KB
No
2 KB
63%
9/29/2022 3:30 PM
Assessor-CLI
Shell Script
1 KB
No
2 KB
51%
9/29/2022 3:30 PM
Assessor-CLI.jar
JAR File
88 KB
No
93 KB
6%
9/29/2022 3:32 PM
Assessor-GUI
32,373 KB
No
76,410 KB
58%
9/29/2022 3:33 PM
README
File
1 KB
No
3 KB
73%
9/29/2022 3:30 PM


Assessor-GUI 4.22.0
Welcome to the CIS Configuration Assessment Tool
CIS-CAT Lite
This CIS-CAT Lite version has limited functions and CIS Benchmark selections. Visit The Center for Internet Security to learn more about CIS-CAT Pro, the full version, available to CIS SecureSuite Members.
Existing CIS SecureSuite Members can consult the CIS-CAT Pro documentation to learn how to apply an organization's license key and access Pro features.
Basic
Scan this system only
Advanced
Scan any number of local/remote systems

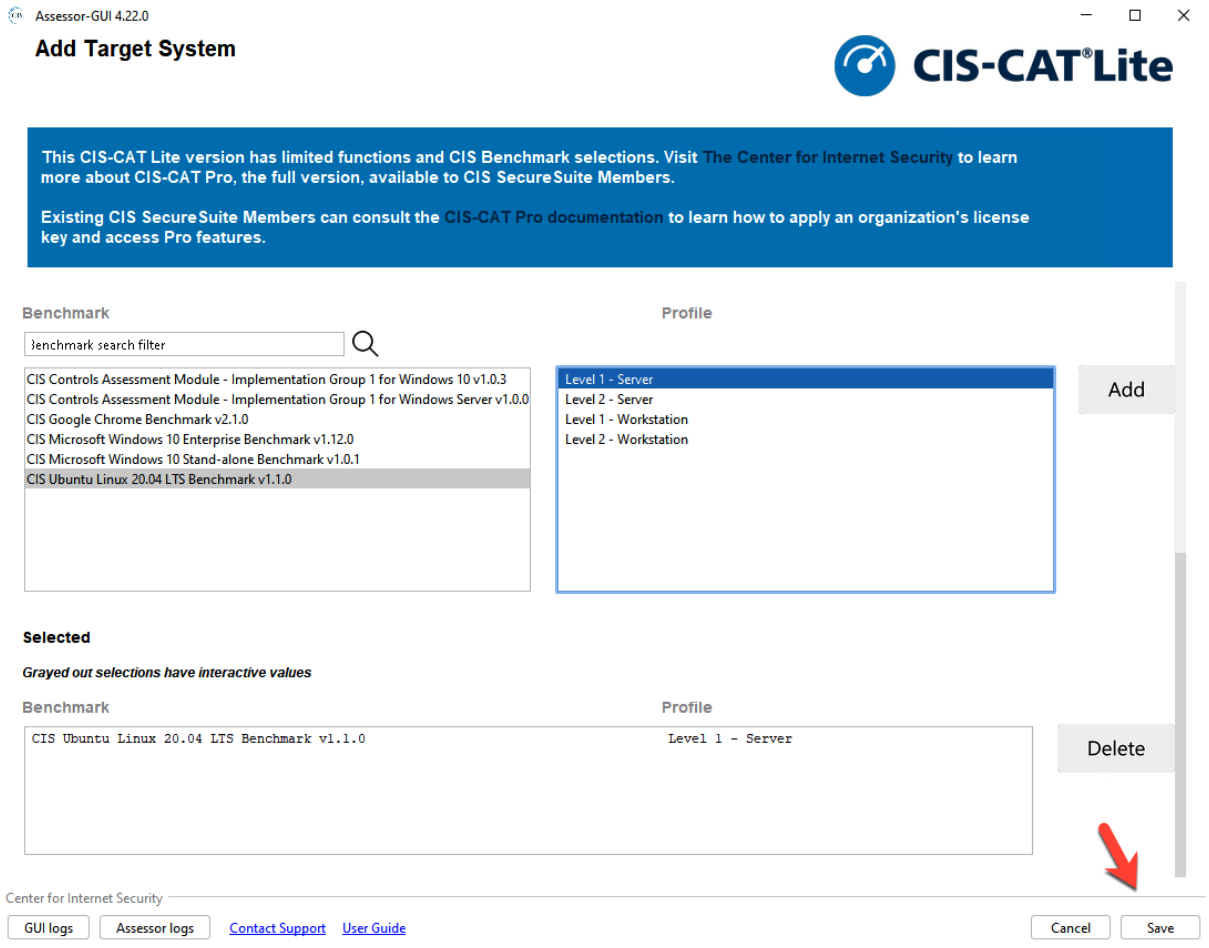

Assessor-GUI 4.22.0
Welcome to the CIS Configuration Assessment Tool
CIS-CAT Lite
This CIS-CAT Lite version has limited functions and CIS Benchmark selections. Visit The Center for Internet Security to learn more about CIS-CAT Pro, the full version, available to CIS SecureSuite Members.
Existing CIS SecureSuite Members can consult the CIS-CAT Pro documentation to learn how to apply an organization's license key and access Pro features.
Basic
Scan this system only
Advanced
Scan any number of local/remote systems
Add remote or local target system
Load a configuration or sessions file
Information
Target System Name *
sectestingcontrolplane
Target System Type *
Linux
Port *
22
Username *
mike
Password
Private key file
Browse ...
IP Address / Hostname *
192.168.1.67
Temporary Path
Browse ...

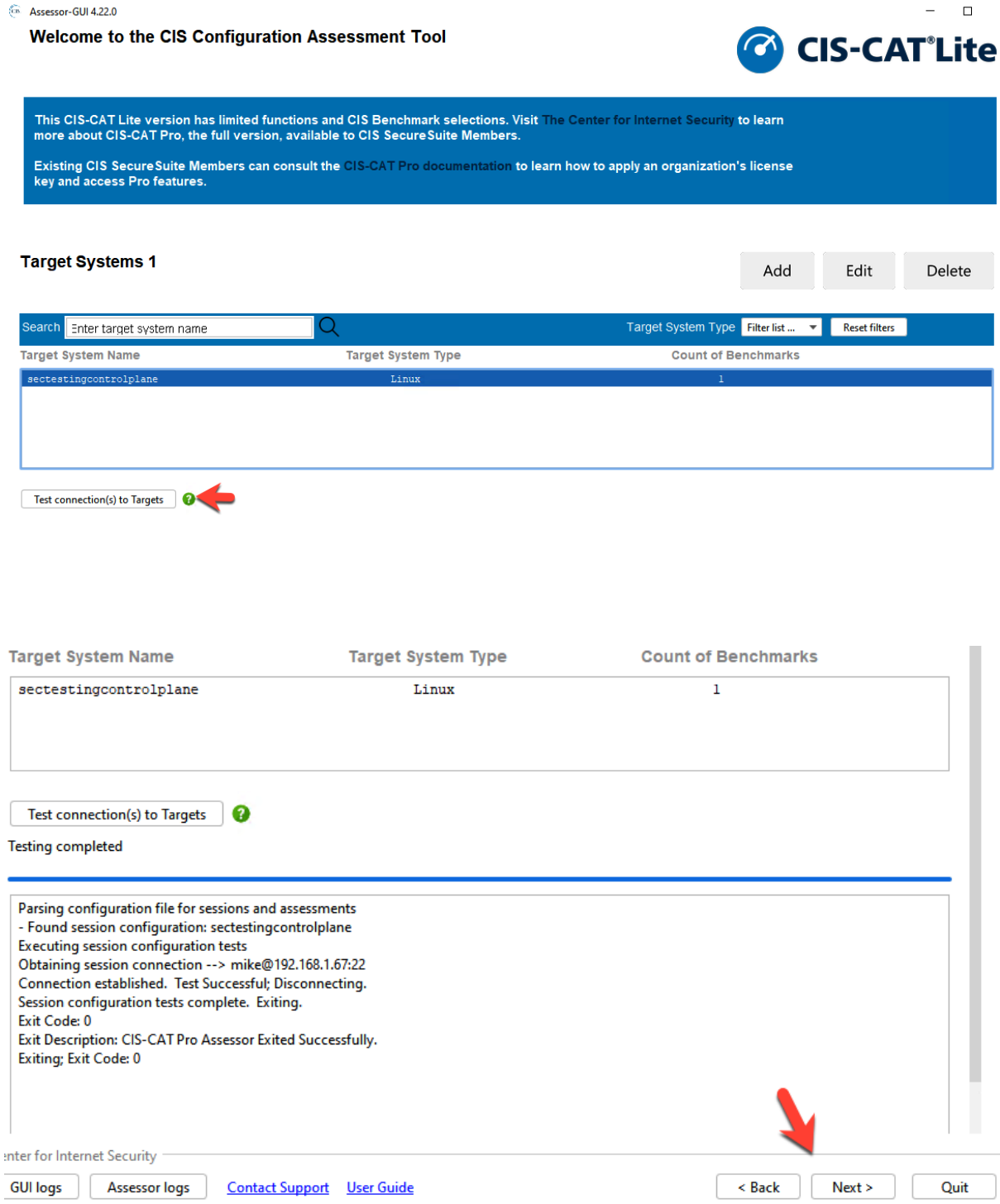
Benchmarks

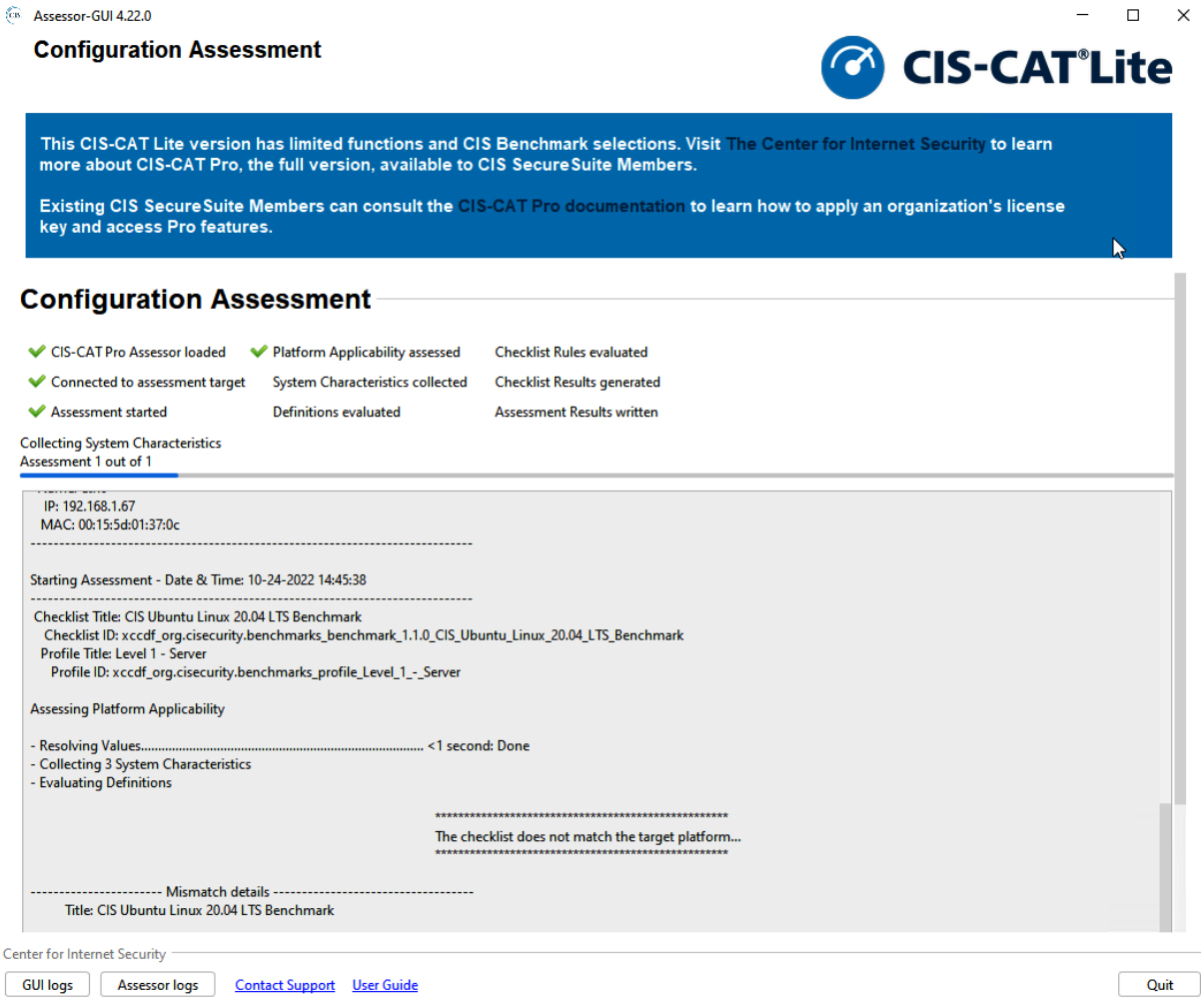
Available

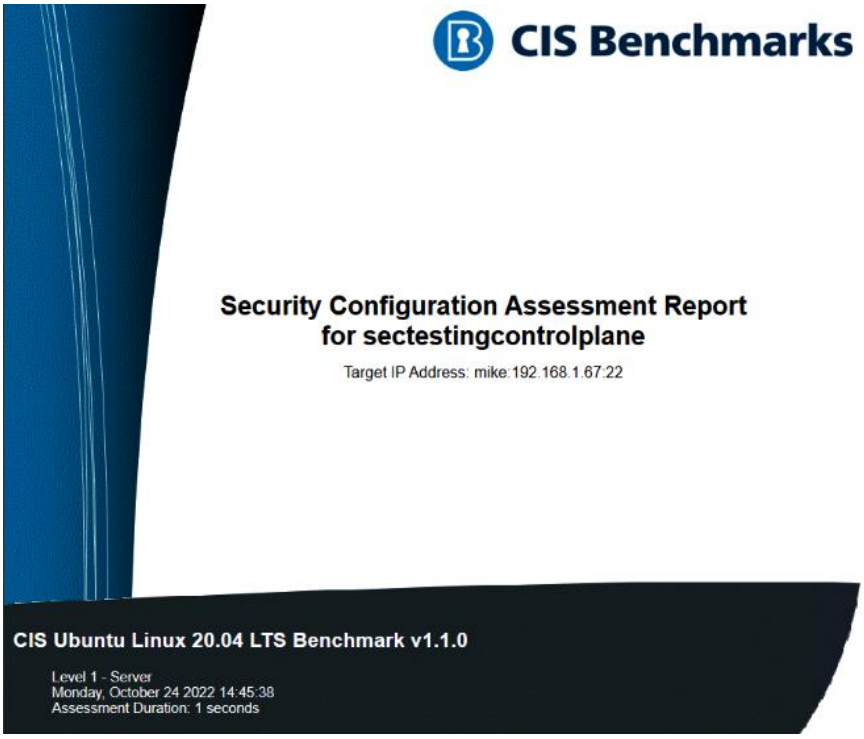


Selected




Assessor-GUI 4.22.0
Welcome to the CIS Configuration Assessment Tool
CIS-CAT®Lite
This CIS-CAT Lite version has limited functions and CIS Benchmark selections. Visit The Center for Internet Security to learn more about CIS-CAT Pro, the full version, available to CIS SecureSuite Members.
Existing CIS SecureSuite Members can consult the CIS-CAT Pro documentation to learn how to apply an organization's license key and access Pro features.
Target Systems 1
Add
Edit
Delete
Search
Enter target system name
Target System Type
Filter list ...
Reset filters
Target System Name
Target System Type
Count of Benchmarks
sectestingcontrolplane
Linux
1
Test connection(s) to Targets
Target System Name
Target System Type
Count of Benchmarks
sectestingcontrolplane
Linux
1
Test connection(s) to Targets
Testing completed
Parsing configuration file for sessions and assessments
- Found session configuration: sectestingcontrolplane
Executing session configuration tests
Obtaining session connection --> mike@192.168.1.67:22
Connection established. Test Successful; Disconnecting.
Session configuration tests complete. Exiting.
Exit Code: 0
Exit Description: CIS-CAT Pro Assessor Exited Successfully.
Exiting; Exit Code: 0
nter for Internet Security
GUI logs
Assessor logs
Contact Support
User Guide
< Back
Next >
Quit


Assessor-GUI 4.22.0
Configuration Assessment
CIS-CAT Lite
This CIS-CAT Lite version has limited functions and CIS Benchmark selections. Visit The Center for Internet Security to learn more about CIS-CAT Pro, the full version, available to CIS SecureSuite Members.
Existing CIS SecureSuite Members can consult the CIS-CAT Pro documentation to learn how to apply an organization's license key and access Pro features.
Configuration Assessment
CIS-CAT Pro Assessor loaded
Platform Applicability assessed
Checklist Rules evaluated
Connected to assessment target
System Characteristics collected
Checklist Results generated
Assessment started
Definitions evaluated
Assessment Results written
Collecting System Characteristics
Assessment 1 out of 1
IP: 192.168.1.67
MAC: 00:15:5d:01:37:0c
Starting Assessment - Date & Time: 10-24-2022 14:45:38
Checklist Title: CIS Ubuntu Linux 20.04 LTS Benchmark
Checklist ID: xccdf_org.cisecurity.benchmarks_benchmark_1.1.0_CIS_Ubuntu_Linux_20.04_LTS_Benchmark
Profile Title: Level 1 - Server
Profile ID: xccdf_org.cisecurity.benchmarks_profile_Level_1_-_Server
Assessing Platform Applicability
- Resolving Values..... <1 second: Done
- Collecting 3 System Characteristics
- Evaluating Definitions
The checklist does not match the target platform...
---------- Mismatch details ----------
Title: CIS Ubuntu Linux 20.04 LTS Benchmark
Center for Internet Security
GUI logs
Assessor logs
Contact Support
User Guide
Quit


CIS Benchmarks
Security Configuration Assessment Report
for sectestingcontrolplane
Target IP Address: mike:192.168.1.67:22
CIS Ubuntu Linux 20.04 LTS Benchmark v1.1.0
Level 1 - Server
Monday, October 24 2022 14:45:38
Assessment Duration: 1 seconds

```
                :~$ kubectl get pods -n kube-system
NAME                                  READY   STATUS
cilium-8w29b                          1/1     Running
cilium-operator-67fdc9d687-8bqz6      1/1     Running
cilium-operator-67fdc9d687-s29sd      1/1     Running
cilium-r4w4g                          1/1     Running
coredns-565d847f94-cknk7              1/1     Running
coredns-565d847f94-hx8fh              1/1     Running
etcd-cpcinium                         1/1     Running
kube-apiserver-cpcinium               1/1     Running
kube-controller-manager-cpcinium      1/1     Running
kube-scheduler-cpcinium               1/1     Running
```

```
mike@cpcinium:~$ sudo kubeadm upgrade plan
[sudo] password for mike:
[upgrade/config] Making sure the configuration is correct:
[upgrade/config] Reading configuration from the cluster...
[upgrade/config] FYI: You can look at this config file with 'kubectl -n kube-system get cm kubeadm-config -o yaml'
W1104 20:59:42.418765  110033 cluster.go:94] error unmarshaling configuration schema.GroupVersionKind{Group:"kubeadm.k8s
.io", Version:"v1beta3", Kind:"ClusterConfiguration"}: strict decoding error: unknown field "serverTLSBootstrap"
[preflight] Running pre-flight checks.
[upgrade] Running cluster health checks
[upgrade] Fetching available versions to upgrade to
[upgrade/versions] Cluster version: v1.25.2
[upgrade/versions] kubeadm version: v1.25.2
[upgrade/versions] Target version: v1.25.3
[upgrade/versions] Latest version in the v1.25 series: v1.25.3
```

```
Upgrade to the latest version in the v1.25 series:

COMPONENT                 CURRENT   TARGET
kube-apiserver            v1.25.2   v1.25.3
kube-controller-manager   v1.25.2   v1.25.3
kube-scheduler            v1.25.2   v1.25.3
kube-proxy                v1.25.2   v1.25.3
CoreDNS                   v1.9.3    v1.9.3
etcd                      3.5.4-0   3.5.4-0

You can now apply the upgrade by executing the following command:

        kubeadm upgrade apply v1.25.3

Note: Before you can perform this upgrade, you have to update kubeadm to v1.25.3.
```

```
mike@cpcinium:~$ sudo kubeadm upgrade apply v1.25.3
[upgrade/config] Making sure the configuration is correct:
[upgrade/config] Reading configuration from the cluster...
[upgrade/config] FYI: You can look at this config file with 'kubectl -n kube-system get cm kubeadm-config -o yaml'
W1104 21:22:36.564001    2575 cluster.go:94] error unmarshaling configuration schema.GroupVersionKind{Group:"kubeadm.k8
s.io", Version:"v1beta3", Kind:"ClusterConfiguration"}: strict decoding error: unknown field "serverTLSBootstrap"
W1104 21:22:36.905302    2575 configset.go:78] Warning: No kubeproxy.config.k8s.io/v1alpha1 config is loaded. Continuin
g without it: configmaps "kube-proxy" not found
[preflight] Running pre-flight checks.
[upgrade] Running cluster health checks
[upgrade/version] You have chosen to change the cluster version to "v1.25.3"
[upgrade/versions] Cluster version: v1.25.2
[upgrade/versions] kubeadm version: v1.25.3
[upgrade] Are you sure you want to proceed? [y/N]: y
[upgrade/prepull] Pulling images required for setting up a Kubernetes cluster
[upgrade/prepull] This might take a minute or two, depending on the speed of your internet connection
[upgrade/prepull] You can also perform this action in beforehand using 'kubeadm config images pull'
[upgrade/apply] Upgrading your Static Pod-hosted control plane to version "v1.25.3" (timeout: 5m0s)...
[upgrade/etcd] Upgrading to TLS for etcd
[upgrade/staticpods] Preparing for "etcd" upgrade
[upgrade/staticpods] Current and new manifests of etcd are equal, skipping upgrade
[upgrade/etcd] Waiting for etcd to become available
[upgrade/staticpods] Writing new Static Pod manifests to "/etc/kubernetes/tmp/kubeadm-upgraded-manifests3827787850"
[upgrade/staticpods] Preparing for "kube-apiserver" upgrade
[upgrade/staticpods] Renewing apiserver certificate
[upgrade/staticpods] Renewing apiserver-kubelet-client certificate
[upgrade/staticpods] Renewing front-proxy-client certificate
[upgrade/staticpods] Renewing apiserver-etcd-client certificate
[upgrade/staticpods] Moved new manifest to "/etc/kubernetes/manifests/kube-apiserver.yaml" and backed up old manifest t
o "/etc/kubernetes/tmp/kubeadm-backup-manifests-2022-11-04-21-22-55/kube-apiserver.yaml"
[upgrade/staticpods] Waiting for the kubelet to restart the component
[upgrade/staticpods] This might take a minute or longer depending on the component/version gap (timeout 5m0s)
```

```
kubelet-start] Writing kubelet configuration to file "/var/lib/kubelet/config.yaml"
bootstrap-token] Configured RBAC rules to allow Node Bootstrap tokens to get nodes
bootstrap-token] Configured RBAC rules to allow Node Bootstrap tokens to post CSRs in order for nodes to get long term
certificate credentials
bootstrap-token] Configured RBAC rules to allow the csrapprover controller automatically approve CSRs from a Node Boot
trap Token
bootstrap-token] Configured RBAC rules to allow certificate rotation for all node client certificates in the cluster
addons] Applied essential addon: CoreDNS
1104 21:24:13.239836    2575 postupgrade.go:146] the ConfigMap "kube-proxy" in the namespace "kube-system" was not fou
d. Assuming that kube-proxy was not deployed for this cluster. Note that once 'kubeadm upgrade apply' supports phases
ou will have to skip the kube-proxy upgrade manually

upgrade/successful] SUCCESS! Your cluster was upgraded to "v1.25.3". Enjoy!

upgrade/kubelet] Now that your control plane is upgraded, please proceed with upgrading your kubelets if you haven't a
ready done so.
```

```
mike@wpcilium:~$ sudo kubeadm upgrade node
[sudo] password for mike:
[upgrade] Reading configuration from the cluster...
[upgrade] FYI: You can look at this config file with 'kubectl -n kube-system get cm kubeadm-config -o yaml'
W1104 21:25:49.049984  110330 configset.go:78] Warning: No kubeproxy.config.k8s.io/v1alpha1 config is loaded. Continuin
g without it: configmaps "kube-proxy" is forbidden: User "system:node:wpcilium" cannot get resource "configmaps" in API
 group "" in the namespace "kube-system": no relationship found between node 'wpcilium' and this object
[preflight] Running pre-flight checks
[preflight] Skipping prepull. Not a control plane node.
[upgrade] Skipping phase. Not a control plane node.
[kubelet-start] Writing kubelet configuration to file "/var/lib/kubelet/config.yaml"
[upgrade] The configuration for this node was successfully updated!
[upgrade] Now you should go ahead and upgrade the kubelet package using your package manager.
```

The following logging sources should be enabled and configured appropriately:

Kubernetes Audit Logs: Audit logging is a Kubernetes feature that records actions taken by the API for later analysis. Audit logs help answer questions pertaining to events occurring on the API server itself.

Ensure logs are monitoring for anomalous or unwanted API calls, especially any authorization failures (these log entries will have a status message "Forbidden"). Authorization failures could mean that an attacker is trying to abuse stolen credentials.

Managed Kubernetes providers, including AWS, Azure, and GCP provide optional access to this data in their cloud console and may allow you to set up alerts on authorization failures.

Kubernetes Events: Kubernetes events can indicate any Kubernetes resource state changes and errors, such as exceeded resource quota or pending pods, as well as any informational messages.

Application & Container Logs: Applications running inside of Kubernetes generate useful logs from a security perspective. The easiest method for capturing these logs is to ensure the output is written to standard output `stdout` and standard error `stderr` streams. Persisting these logs can be carried out in a number of ways. It is common for operators to configure applications to write logs to a log file which is then consumed by a sidecar container to be shipped and processed centrally.

Operating System Logs: Depending on the OS running the Kubernetes nodes, additional logs may be available for processing. Logs from programs such as `systemd` are available using the `journalctl -u` command.

Cloud Provider Logs: If you are operating Kubernetes in a managed environment such as AWS EKS, Azure AKS, or GCP GKE you can find a number of additional logging streams available for consumption. One example, is within Amazon EKS there exists a log stream specifically for the Authenticator component. These logs represent the control plane component that EKS uses for RBAC authentication using AWS IAM credentials and can be a rich source of data for security operations teams.

Network Logs: Network logs can be captured within Kubernetes at a number of layers. If you are working with traditional proxy or ingress components such as nginx or apache, you should use the standard out `stdout` and standard error `stderr` pattern to capture and ship these logs for further investigation. Other projects such as eBPF aim to provide consumable network and kernel logs to greater enhance security observability within the cluster.

As outlined above, there is no shortage of logging mechanisms available within the Kubernetes ecosystem. A robust security logging architecture should not only capture relevant security events, but also be centralized in a way that is queryable, long term, and maintains integrity.


```yaml
volumeMounts:
- mountPath: /etc/kubernetes/simple-policy.yaml
  name: audit
  readOnly: true
- mountPath: /var/log/audit.log
  name: audit-log
```

```yaml
volumes:
- hostPath:
    path: /etc/kubernetes/simple-policy.yaml
    type: File
  name: audit
- hostPath:
    path: /var/log/audit.log
    type: FileOrCreate
  name: audit-log
```

```
☁  ~  kubectl get pods -o wide
NAME       READY   STATUS    RESTARTS   AGE   IP
ES
busybox1   1/1     Running   0          13s   172.17.0.3
busybox2   1/1     Running   0          6s    172.17.0.4
```

```
☁  ~  kubectl exec -ti busybox2 -- ping -c3 172.17.0.3
PING 172.17.0.3 (172.17.0.3): 56 data bytes
64 bytes from 172.17.0.3: seq=0 ttl=64 time=0.234 ms
64 bytes from 172.17.0.3: seq=1 ttl=64 time=0.076 ms
64 bytes from 172.17.0.3: seq=2 ttl=64 time=0.052 ms
```