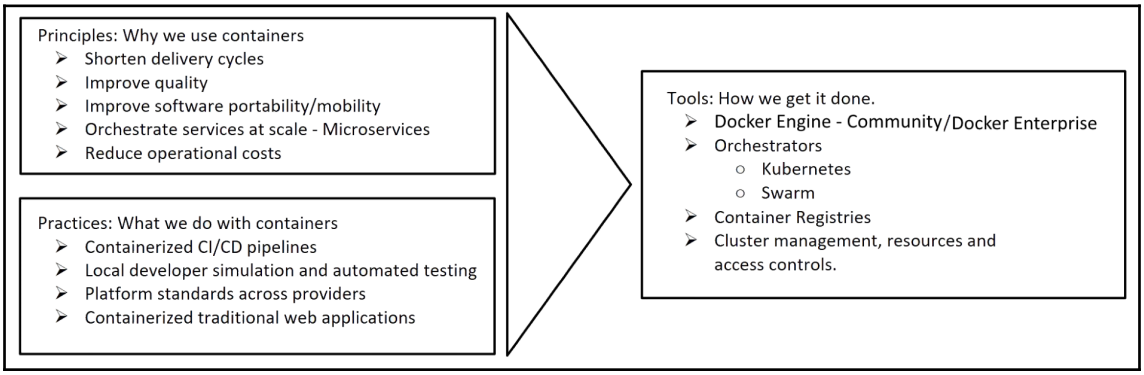
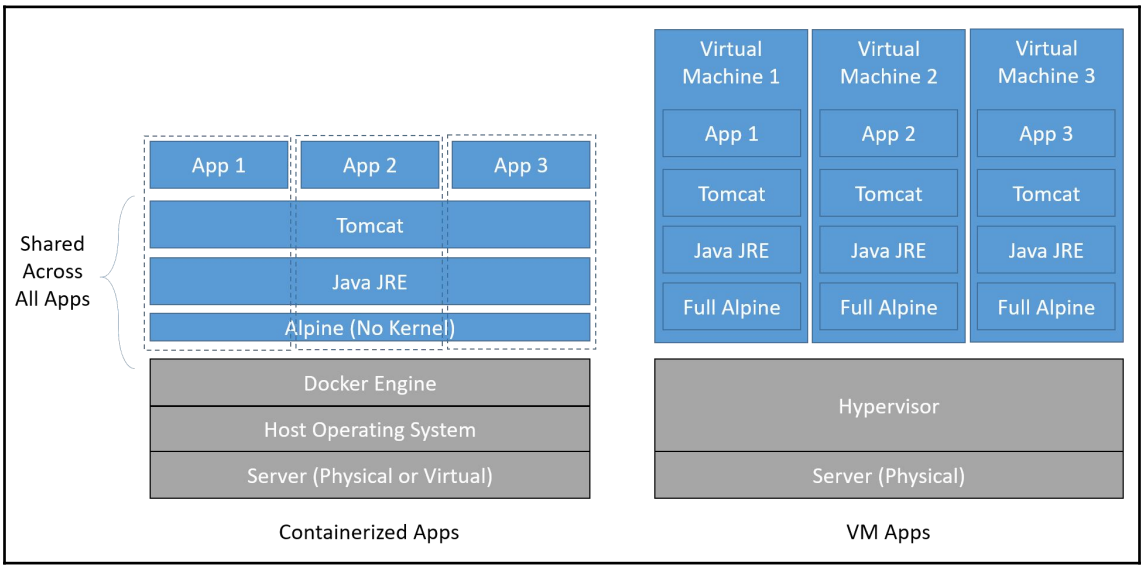
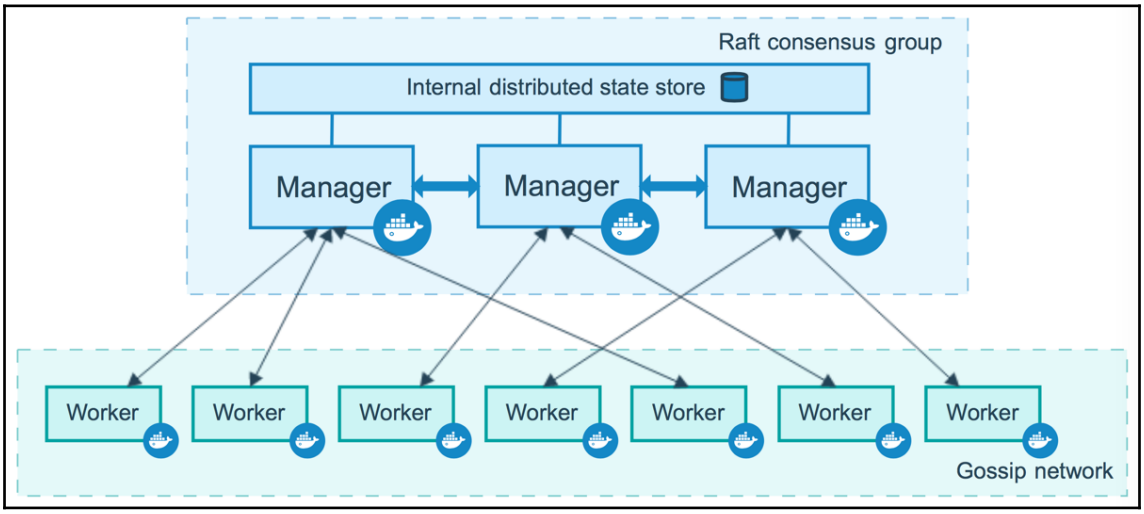
# Chapter 1: Making the Case for Docker Enterprise

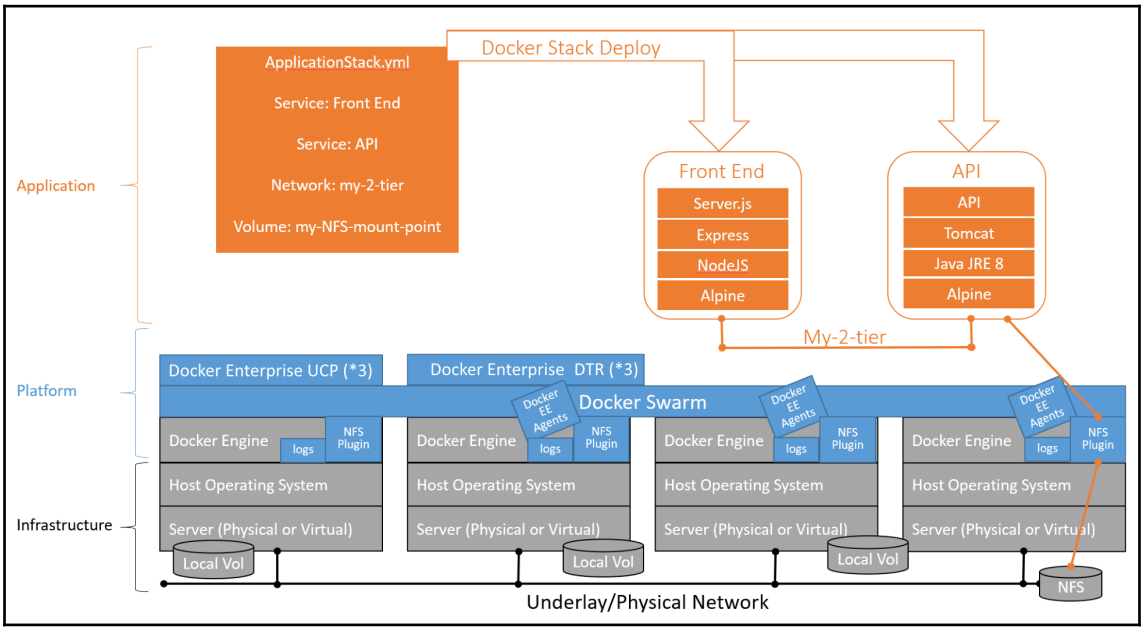


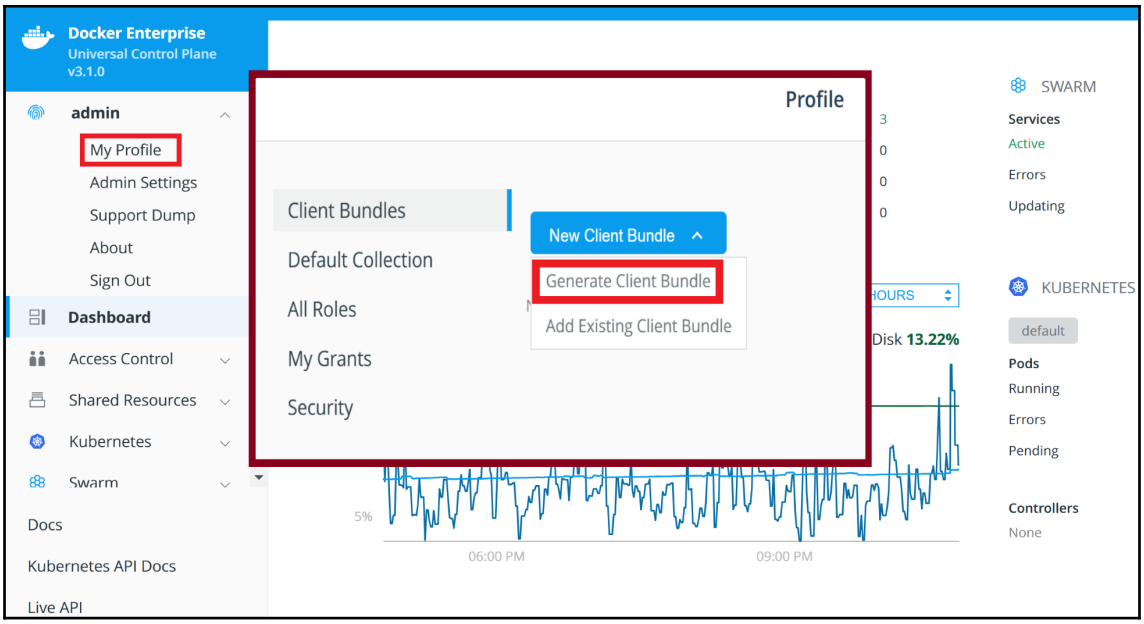



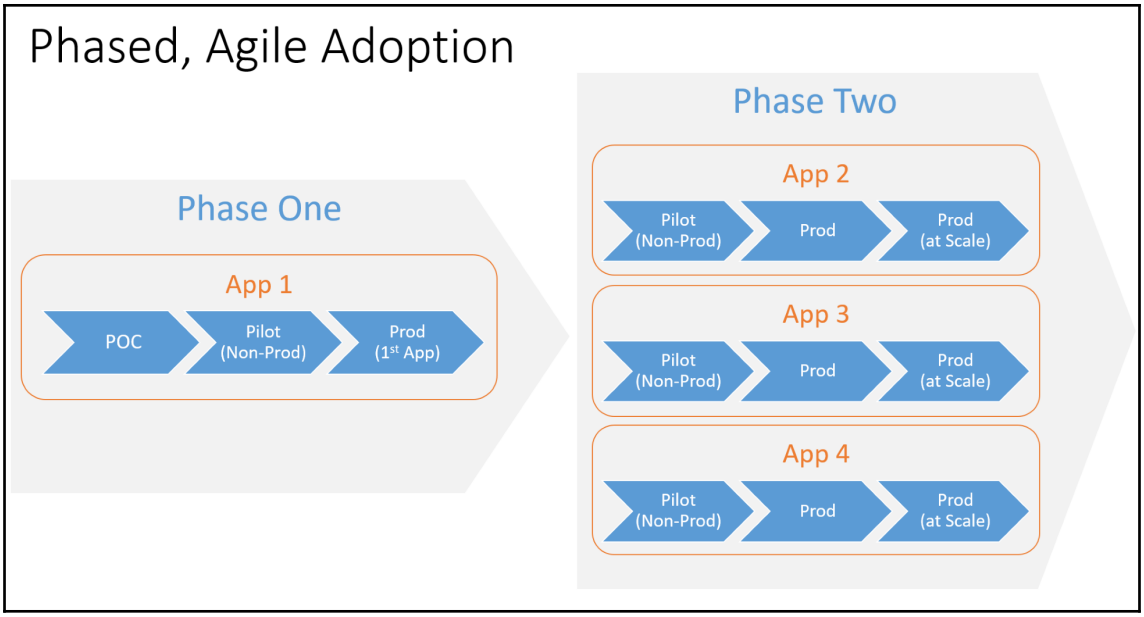
| docker | kubernetes |
| --- | --- |
| • Best where applications are a stack of application dedicated services<br>• Development is application focused<br>• Typical 3 – Tier applications<br>• Lift and shift legacy web applications | • Best where applications are composed from a network of long running services<br>• Development teams are service focused<br>• Large scale microservices applications<br>• Bottom-up, multi layer API services for enterprise or 3rd party consumption |
| **-- Bottom line –**<br>• Swarm is NOT dead – significant enhancements 18.09<br>• Easier to build, manage and secure<br>• Monolithic Service deployment<br>• Production Support for Windows with near Linux Parity | **-- Bottom line --**<br>• Management plane as a Service (AKS/EKS/GKE) with large echo-system modules<br>• Modular Service deployment<br>• Beta, limited Windows capabilities<br>• Vendor lock-in with many supported versions |

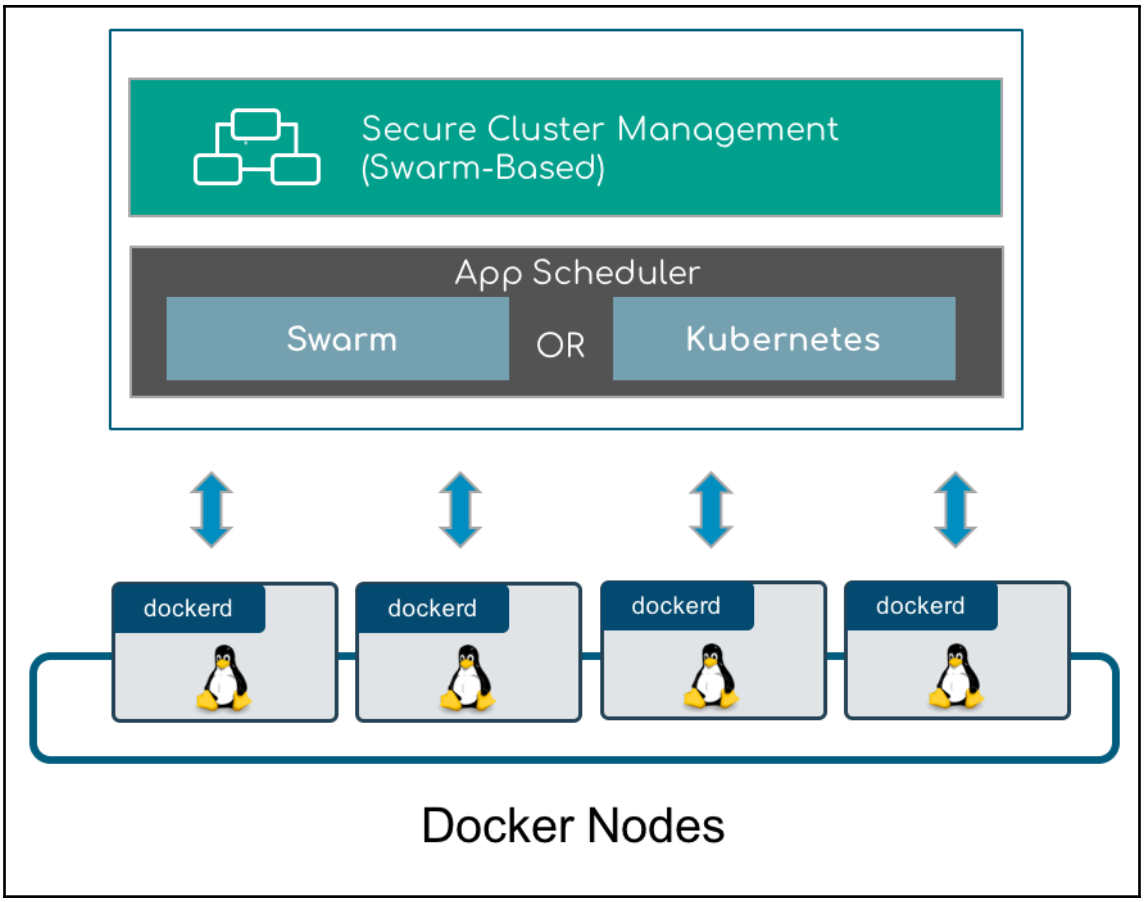
# Chapter 2: Docker Enterprise - an Architectural Overview

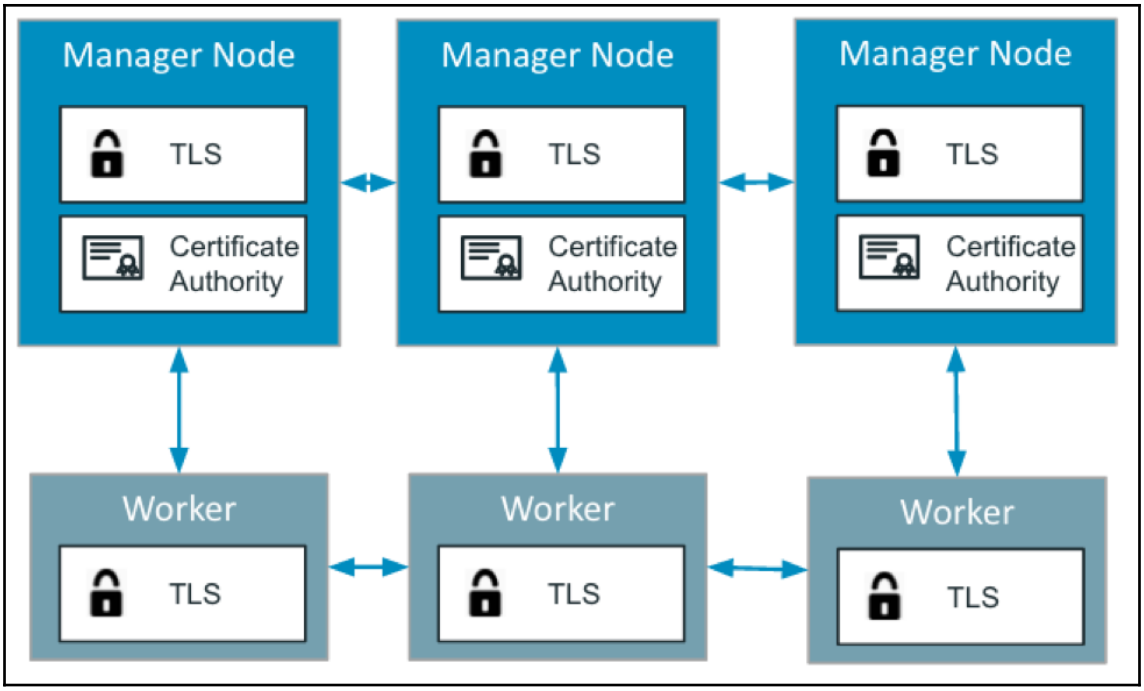


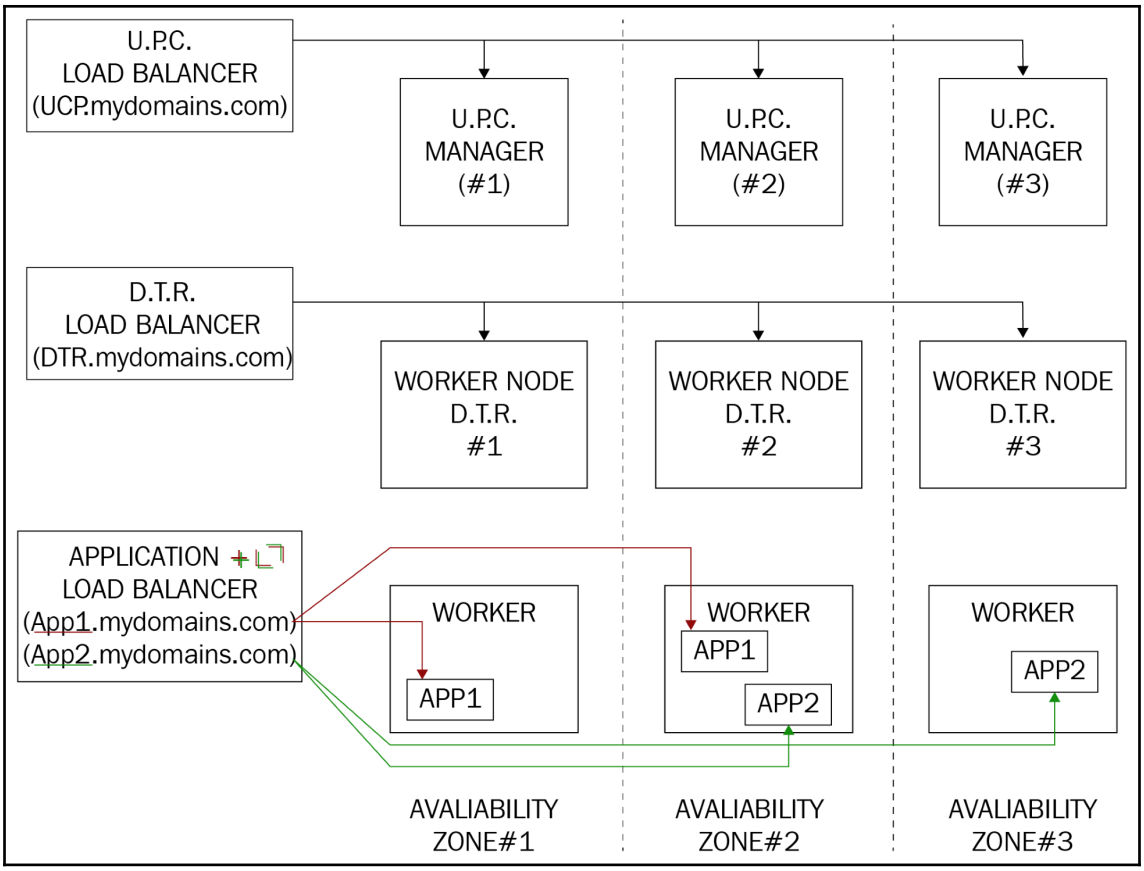



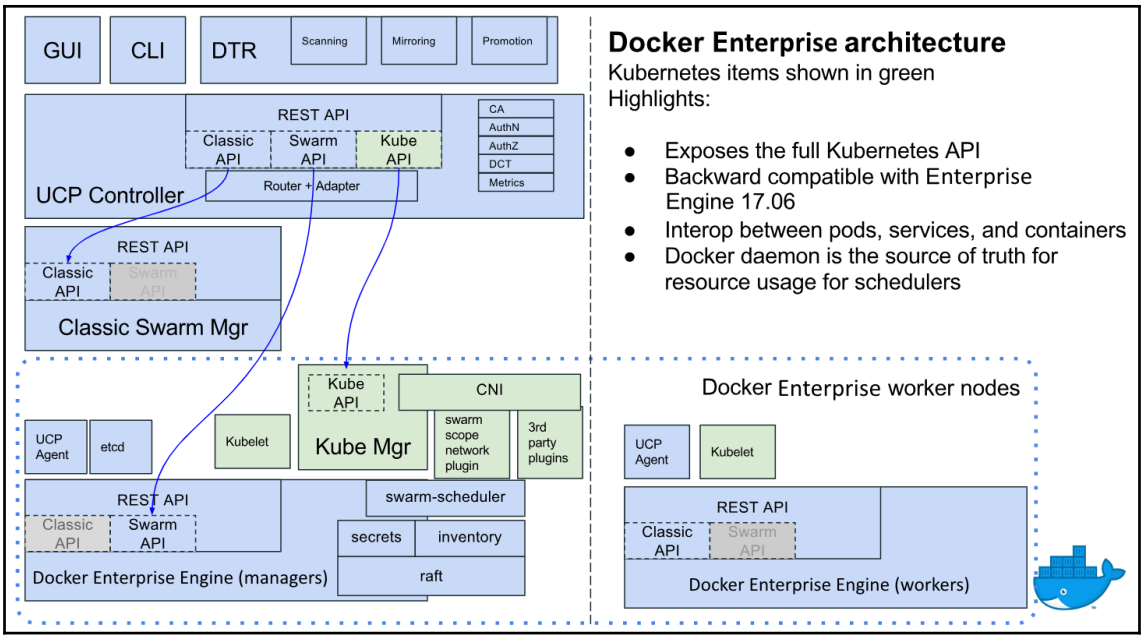

Docker Enterprise
Universal Control Plane
v3.1.0
admin
My Profile
Admin Settings
Support Dump
About
Sign Out
Dashboard
Access Control
Shared Resources
Kubernetes
Swarm
Docs
Kubernetes API Docs
Live API
Profile
Client Bundles
Default Collection
All Roles
My Grants
Security
New Client Bundle
Generate Client Bundle
Add Existing Client Bundle
SWARM
Services
Active
Errors
Updating
KUBERNETES
default
Pods
Running
Errors
Pending
Controllers
None
Disk 13.22%
5%
06:00 PM
09:00 PM


Phased, Agile Adoption
Phase One
App 1
POC
Pilot (Non-Prod)
Prod (1st App)
Phase Two
App 2
Pilot (Non-Prod)
Prod
Prod (at Scale)
App 3
Pilot (Non-Prod)
Prod
Prod (at Scale)
App 4
Pilot (Non-Prod)
Prod
Prod (at Scale)

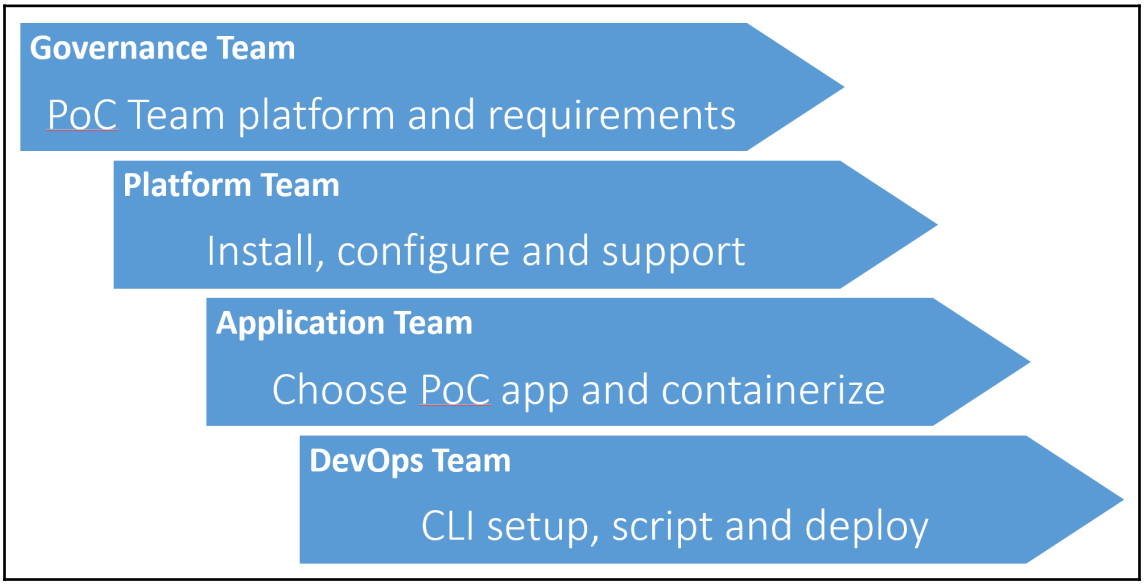

Secure Cluster Management
(Swarm-Based)
App Scheduler
Swarm
OR
Kubernetes
dockerd
dockerd
dockerd
dockerd
Docker Nodes

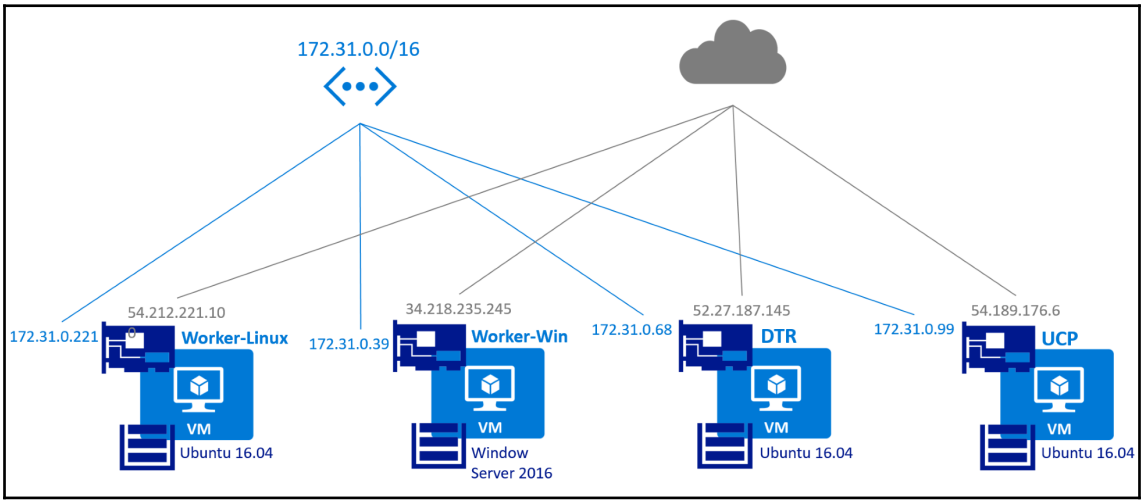

Manager Node
TLS
Certificate Authority
Manager Node
TLS
Certificate Authority
Manager Node
TLS
Certificate Authority
Worker
TLS
Worker
TLS
Worker
TLS

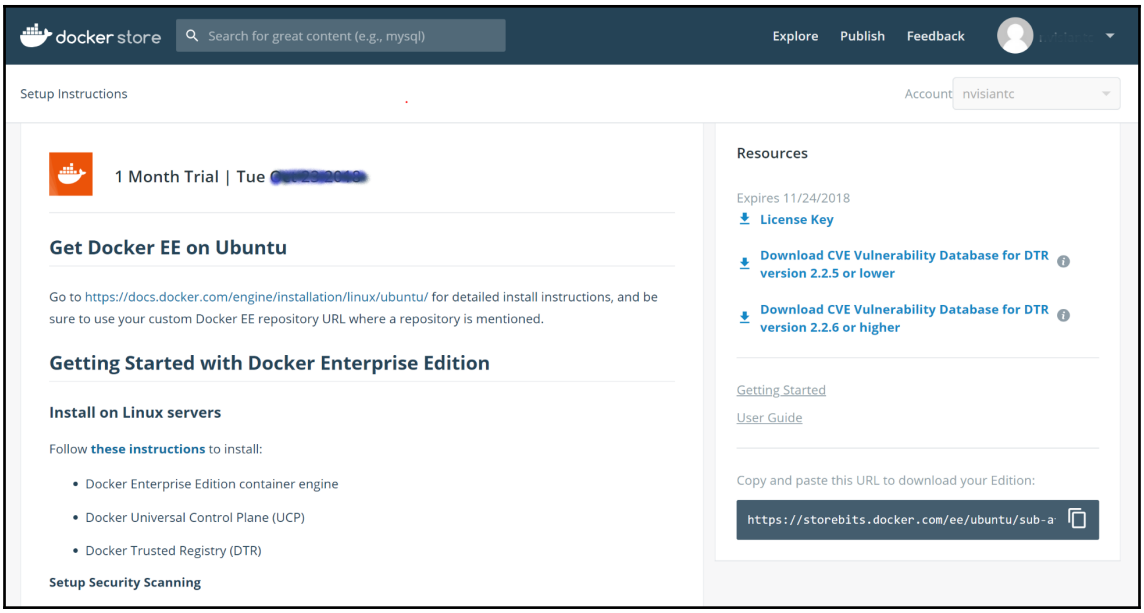

U.P.C.
LOAD BALANCER
(UCP.mydomains.com)
U.P.C.
MANAGER
(#1)
U.P.C.
MANAGER
(#2)
U.P.C.
MANAGER
(#3)
D.T.R.
LOAD BALANCER
(DTR.mydomains.com)
WORKER NODE
D.T.R.
#1
WORKER NODE
D.T.R.
#2
WORKER NODE
D.T.R.
#3
APPLICATION
LOAD BALANCER
(App1.mydomains.com)
(App2.mydomains.com)
WORKER
APP1
WORKER
APP1
APP2
WORKER
APP2
AVALIABILITY
ZONE#1
AVALIABILITY
ZONE#2
AVALIABILITY
ZONE#3


GUI
CLI
DTR
Scanning
Mirroring
Promotion
REST API
Classic API
Swarm API
Kube API
Router + Adapter
UCP Controller
CA
AuthN
AuthZ
DCT
Metrics
REST API
Classic API
Swarm API
Classic Swarm Mgr
Kube API
CNI
UCP Agent
etcd
Kubelet
Kube Mgr
swarm scope network plugin
3rd party plugins
REST API
Classic API
Swarm API
swarm-scheduler
secrets
inventory
raft
Docker Enterprise Engine (managers)
Docker Enterprise architecture
Kubernetes items shown in green
Highlights:
Exposes the full Kubernetes API
Backward compatible with Enterprise Engine 17.06
Interop between pods, services, and containers
Docker daemon is the source of truth for resource usage for schedulers
Docker Enterprise worker nodes
UCP Agent
Kubelet
REST API
Classic API
Swarm API
Docker Enterprise Engine (workers)

# Chapter 3: Getting Started - Docker Enterprise Proof of Concept




docker store
Search for great content (e.g., mysql)
Explore
Publish
Feedback
Setup Instructions
Account nvisiantc
1 Month Trial | Tue
Get Docker EE on Ubuntu
Go to https://docs.docker.com/engine/installation/linux/ubuntu/ for detailed install instructions, and be sure to use your custom Docker EE repository URL where a repository is mentioned.
Getting Started with Docker Enterprise Edition
Install on Linux servers
Follow these instructions to install:
Docker Enterprise Edition container engine
Docker Universal Control Plane (UCP)
Docker Trusted Registry (DTR)
Setup Security Scanning
Resources
Expires 11/24/2018
License Key
Download CVE Vulnerability Database for DTR version 2.2.5 or lower
Download CVE Vulnerability Database for DTR version 2.2.6 or higher
Getting Started
User Guide
Copy and paste this URL to download your Edition:
https://storebits.docker.com/ee/ubuntu/sub-a

Install-EE-Engine-notes.md - MasteringDockerEE - Visual Studio Code

File Edit Selection View Go Debug Terminal Help

Install-EE-Engine-notes.md | nodes.txt

```
4
5   Docker Engine Install Docs - https://docs.docker.com/ee/supported-platforms/
6
7   ## Ubuntu Docker Engine Install
8   This page walks through the process described here
9   https://docs.docker.com/install/linux/docker-ee/ubuntu/
10
11  On each linux node, update the package manager.
12  ```
13  sudo apt-get update
14  ```
15
16  Now oEnable apt over HTTPS...
17  ```
18  sudo apt-get install -y \
19      apt-transport-https \
20      ca-certificates \
21      curl \
22      software-properties-common
23  ```
24  Set up temp environmental variables
25  ```
```

PROBLEMS 11 OUTPUT DEBUG CONSOLE TERMINAL 1: bash

```
ubuntu@ip-172-31-0-99:~$
```

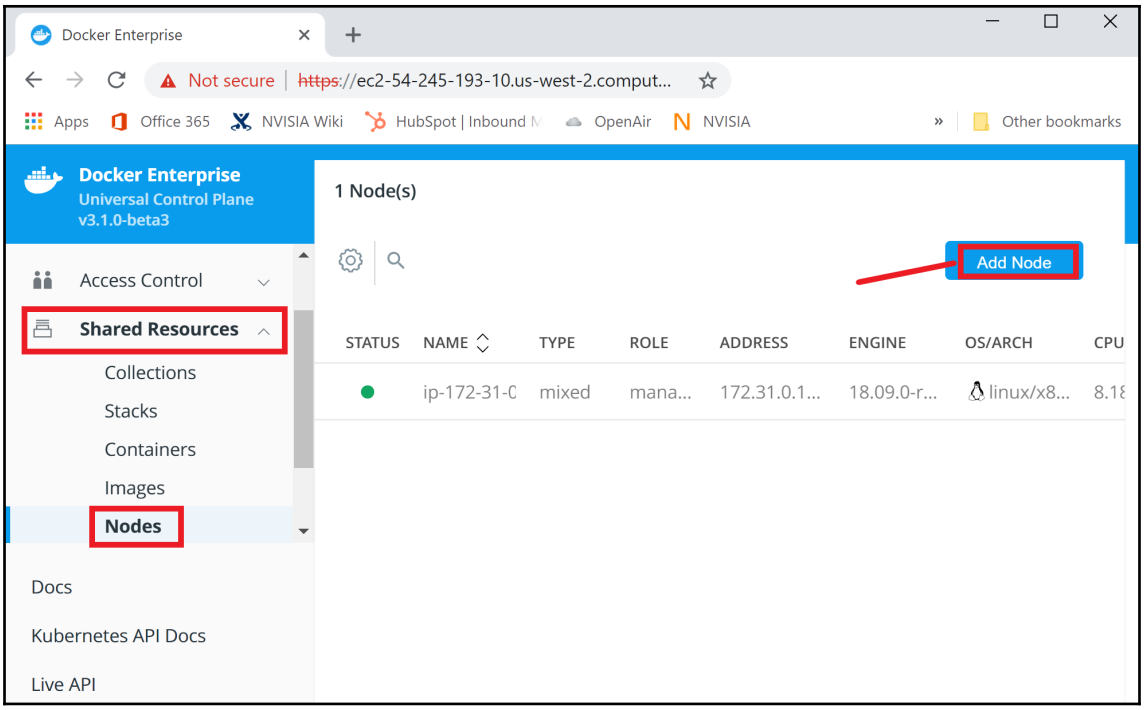
master* 0 0 11 Server not selected markdown | Install-EE-Engine-notes.md Ln 3, Col 114 Spaces: 2 UTF-8 LF Markdown

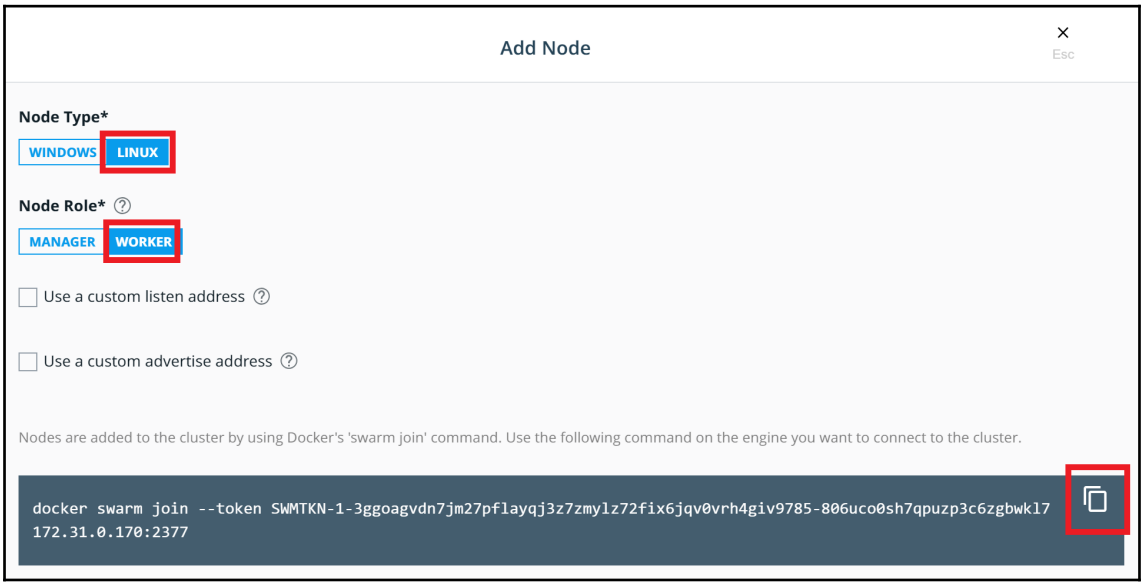
```
ubuntu@ip-172-31-0-170:~$ sudo docker info
Containers: 0
 Running: 0
 Paused: 0
 Stopped: 0
Images: 0
Server Version: 18.09.0-rc1
Storage Driver: overlay2
 Backing Filesystem: extfs
 Supports d_type: true
 Native Overlay Diff: true
Logging Driver: json-file
Cgroup Driver: cgroupfs
Plugins:
 Volume: local
 Network: bridge host macvlan null overlay
 Log: awslogs fluentd gcplogs gelf journald json-file local logentries splunk syslog
Swarm: inactive
Runtimes: runc
Default Runtime: runc
Init Binary: docker-init
containerd version: 99fc40fd6088baebe3c18b8f8093cd50d58815d6 (expected: 468a545b9edcd5932818eb9de8e72413e616e86e)
runc version: 4fc53a81fb7c994640722ac585fa9ca548971871 (expected: 69663f0bd4b60df09991c08812a60108003fa340)
init version: fec3683
Security Options:
 apparmor
 seccomp
  Profile: default
Kernel Version: 4.4.0-1067-aws
Operating System: Ubuntu 16.04.5 LTS
OSType: linux
Architecture: x86_64
CPUs: 2
Total Memory: 7.795GiB
```

Administrator: Windows PowerShell

```
PS C:\Users\Administrator> docker info
Containers: 0
 Running: 0
 Paused: 0
 Stopped: 0
Images: 0
Server Version: 18.09.0-beta3
Storage Driver: windowsfilter
 Windows:
Logging Driver: json-file
Plugins:
 Volume: local
 Network: ics l2bridge l2tunnel nat null overlay transparent
 Log: awslogs etwlogs fluentd gelf json-file local logentries splunk syslog
Swarm: inactive
Default Isolation: process
Kernel Version: 10.0 14393 (14393.2551.amd64fre.rs1_release.181004-1309)
Operating System: Windows Server 2016 Datacenter Version 1607 (OS Build 14393.2551)
OSType: windows
Architecture: x86_64
CPUs: 2
Total Memory: 8GiB
Name: EC2AMAZ-SNCEIC7
ID: VZIV:QABT:63VB:KUOW:4FOR:BTTB:QULZ:U7KS:CIZK:QWTU:63SI:65EG
Docker Root Dir: C:\ProgramData\docker
Debug Mode (client): false
Debug Mode (server): false
Registry: https://index.docker.io/v1/
Labels:
 com.docker.security.fips=enabled
Experimental: false
Insecure Registries:
 127.0.0.0/8
Live Restore Enabled: false

PS C:\Users\Administrator>
```


Docker Enterprise
Not secure
https://ec2-54-245-193-10.us-west-2.comput...
Apps
Office 365
NVISIA Wiki
HubSpot | Inbound
OpenAir
NVISIA
Other bookmarks
Docker Enterprise
Universal Control Plane
v3.1.0-beta3
1 Node(s)
Add Node
Access Control
Shared Resources
Collections
Stacks
Containers
Images
Nodes
Docs
Kubernetes API Docs
Live API
STATUS
NAME
TYPE
ROLE
ADDRESS
ENGINE
OS/ARCH
CPU
ip-172-31-0
mixed
mana...
172.31.0.1...
18.09.0-r...
linux/x8...


Add Node
Esc
Node Type*
WINDOWS
LINUX
Node Role*
MANAGER
WORKER
Use a custom listen address
Use a custom advertise address
Nodes are added to the cluster by using Docker's 'swarm join' command. Use the following command on the engine you want to connect to the cluster.
docker swarm join --token SWMTKN-1-3ggoagvdn7jm27pflayqj3z7zmylz72fix6jqv0vrh4giv9785-806uco0sh7qpuzp3c6zgbwkl7
172.31.0.170:2377

Add Node

Esc

Default Orchestrator Type

The default orchestrator type for new nodes created is swarm. To change the orchestrator type, as an admin, go to Settings -> Scheduler page

**Node Type***

WINDOWS LINUX

*Windows nodes can only be added as worker nodes

Step 1

## Adding Windows nodes to UCP

If you're deploying windows nodes, please follow the steps in the Documentation

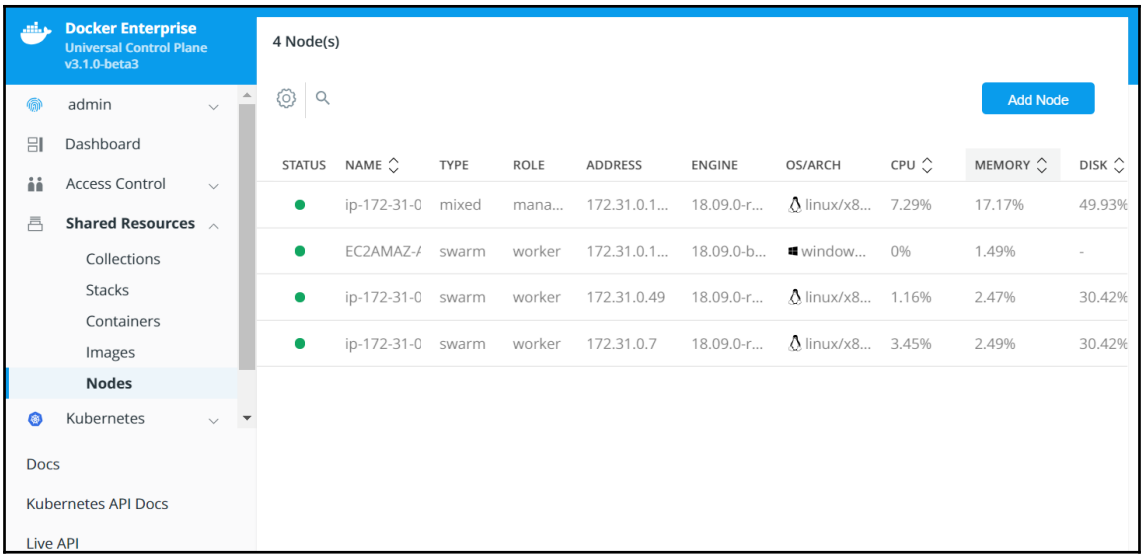
View The Docs

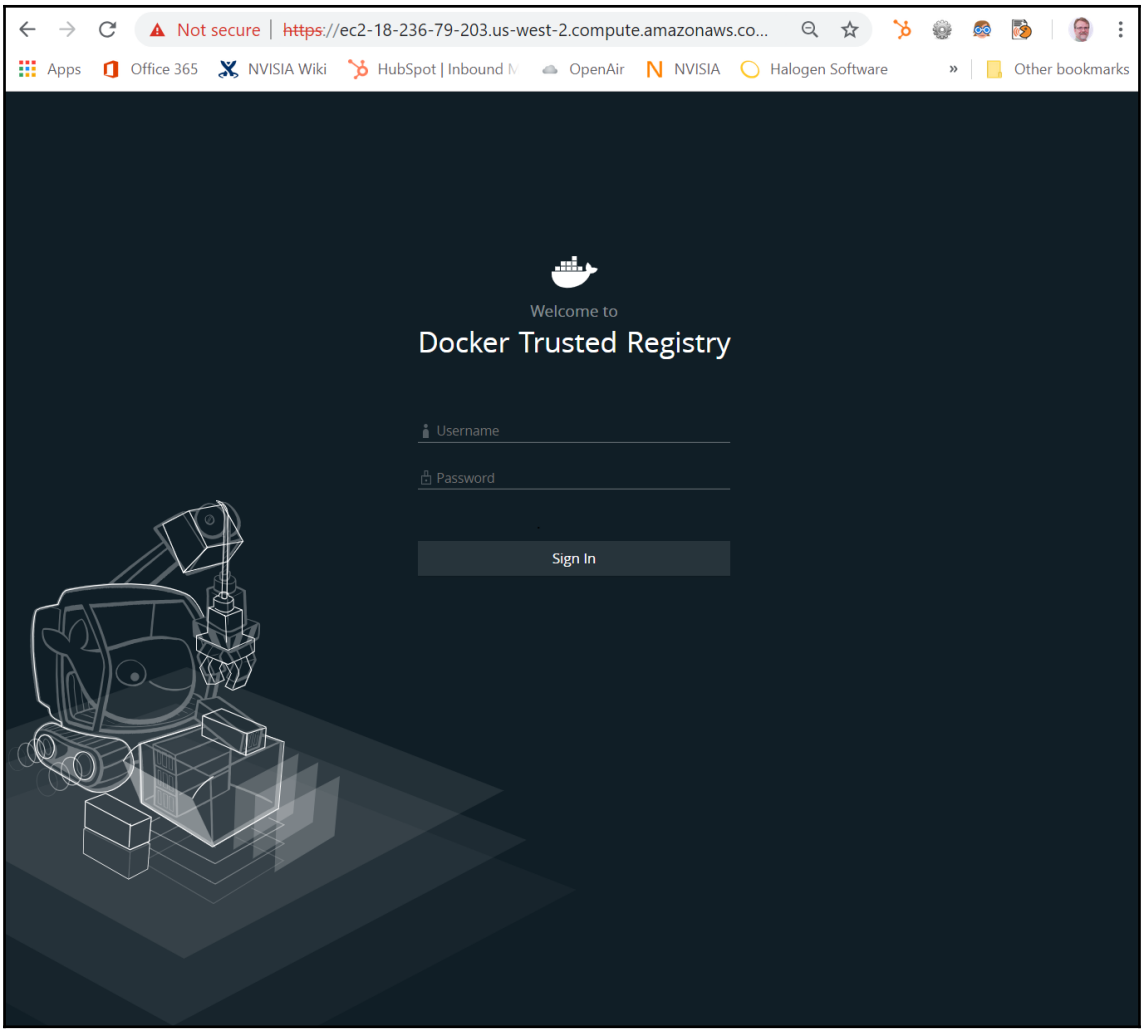
Step 2

- [x] I have followed the instructions and I'm ready to join my windows node.
- [ ] Use a custom listen address
- [ ] Use a custom advertise address

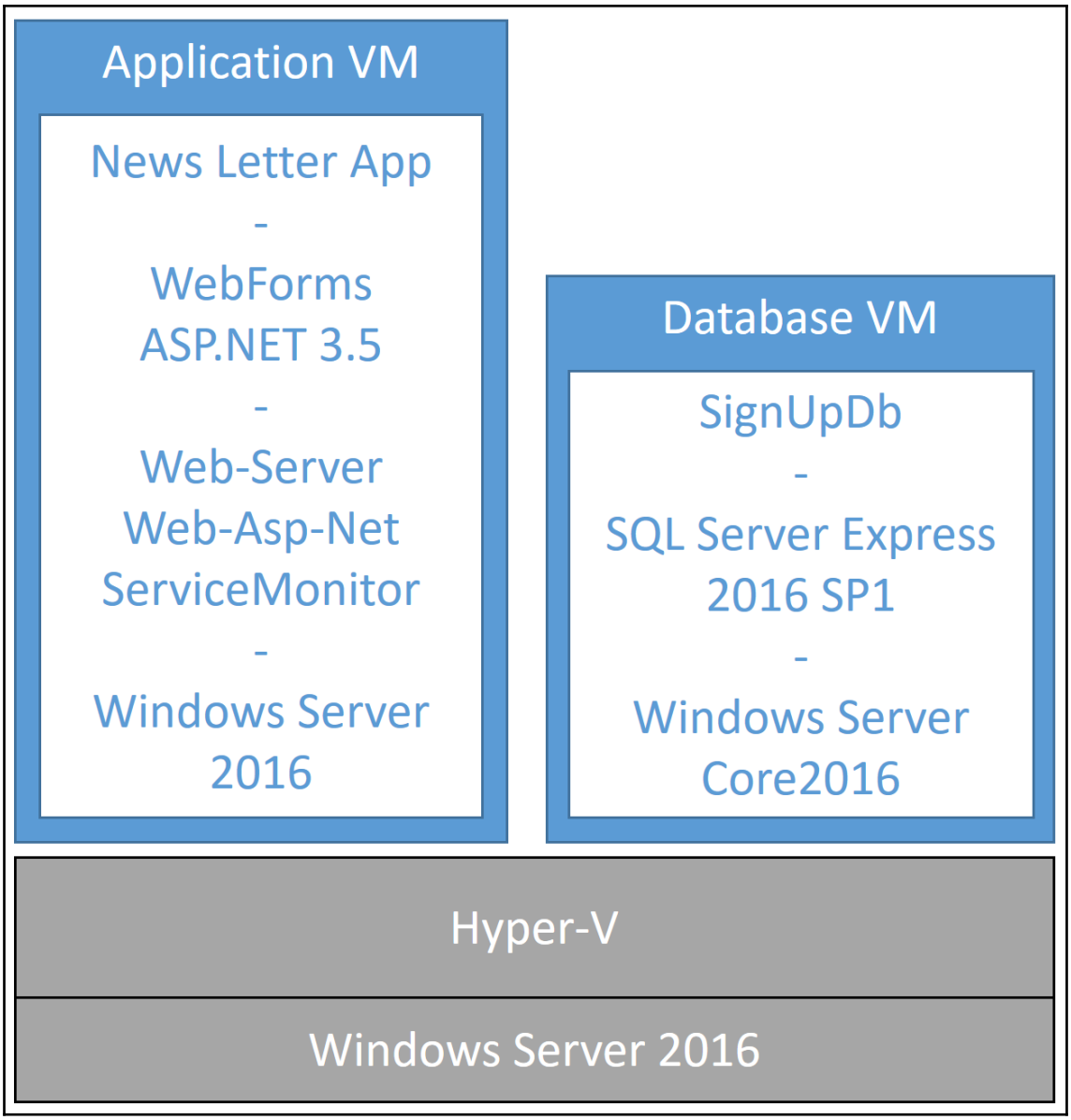
Nodes are added to the cluster by using Docker's 'swarm join' command. Use the following command on the engine you want to connect to the cluster.

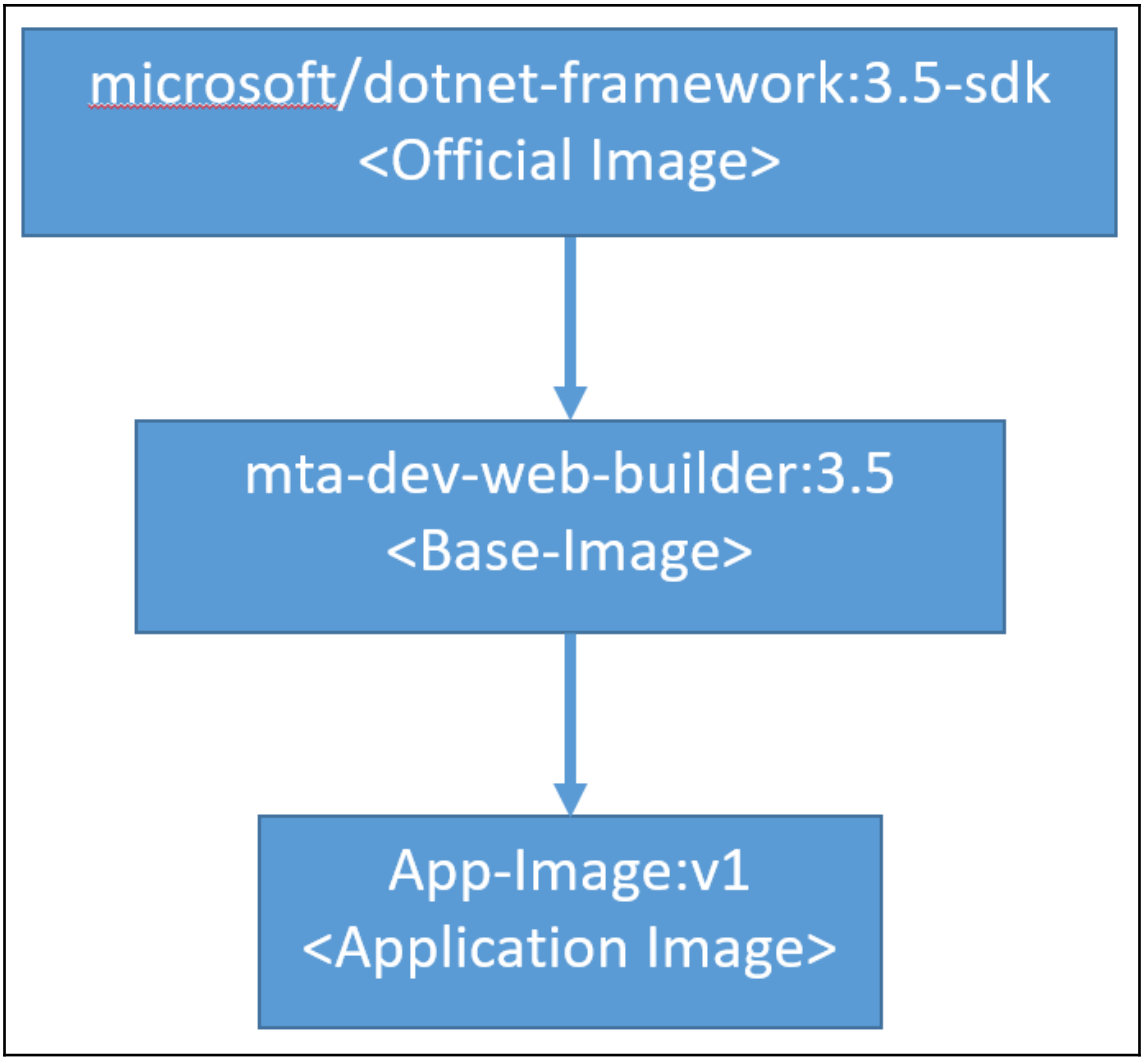
```
docker swarm join --token SWMTKN-1-52gmoem4bupp74ozji2983jtuo2col9oyt4a01sxcj0nigw4wn-23gl3ty0hnvwisfwnwjmvyx8w
10.10.1.40:2377
```

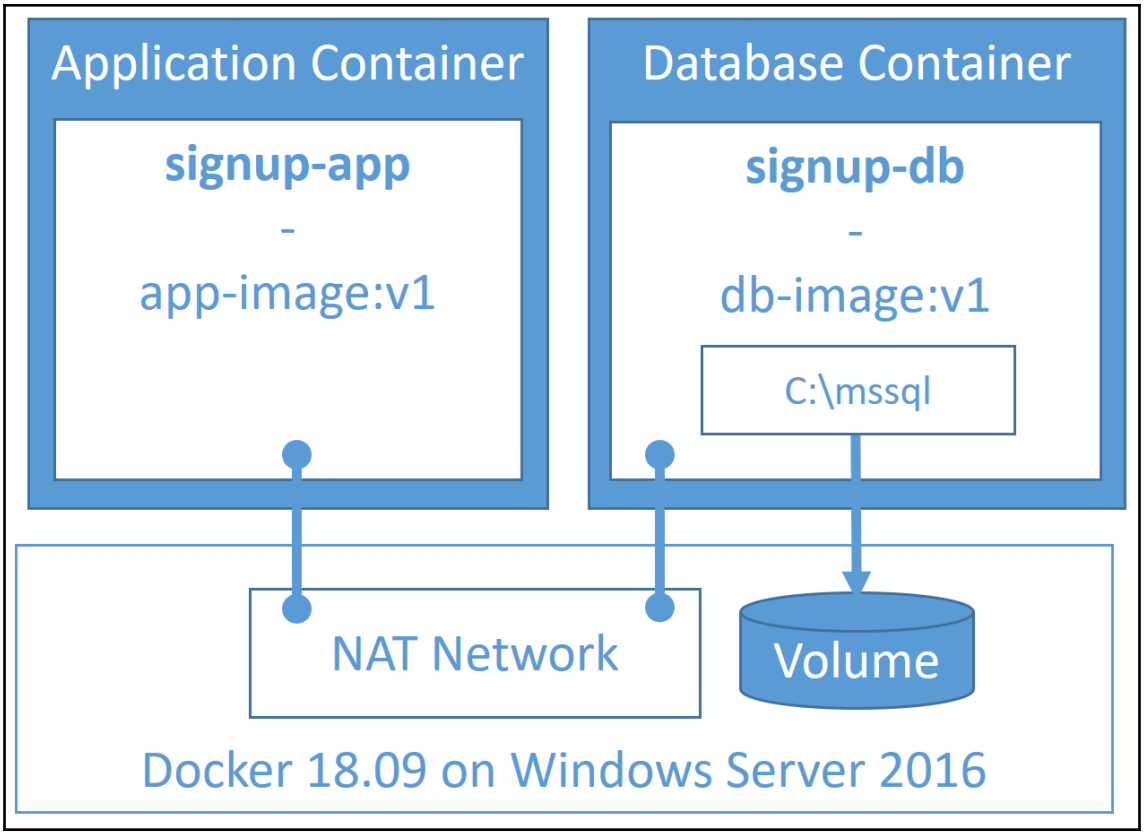

Docker Enterprise
Universal Control Plane
v3.1.0-beta3
admin
Dashboard
Access Control
Shared Resources
Collections
Stacks
Containers
Images
Nodes
Kubernetes
Docs
Kubernetes API Docs
Live API
4 Node(s)
Add Node
STATUS NAME TYPE ROLE ADDRESS ENGINE OS/ARCH CPU MEMORY DISK
ip-172-31-0 mixed mana... 172.31.0.1... 18.09.0-r... linux/x8... 7.29% 17.17% 49.93%
EC2AMAZ-/ swarm worker 172.31.0.1... 18.09.0-b... window... 0% 1.49% -
ip-172-31-0 swarm worker 172.31.0.49 18.09.0-r... linux/x8... 1.16% 2.47% 30.42%
ip-172-31-0 swarm worker 172.31.0.7 18.09.0-r... linux/x8... 3.45% 2.49% 30.42%

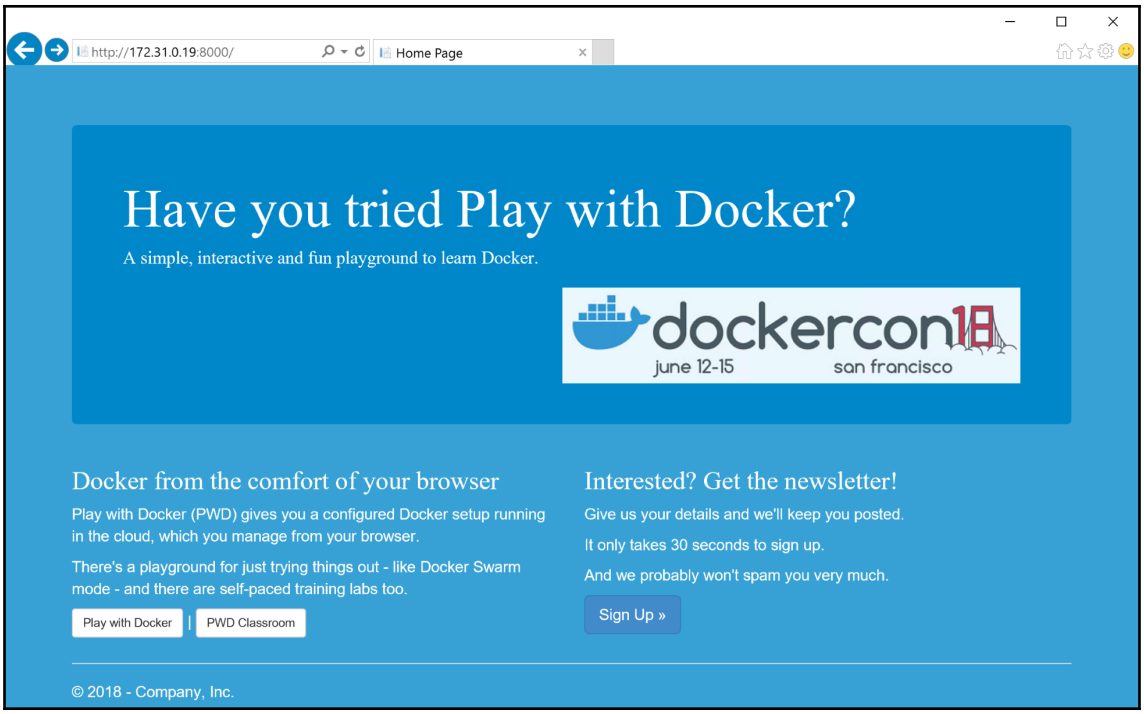

Not secure
https://ec2-18-236-79-203.us-west-2.compute.amazonaws.co...
Apps
Office 365
NVISIA Wiki
HubSpot | Inbound
OpenAir
NVISIA
Halogen Software
Other bookmarks
Welcome to
Docker Trusted Registry
Username
Password
Sign In

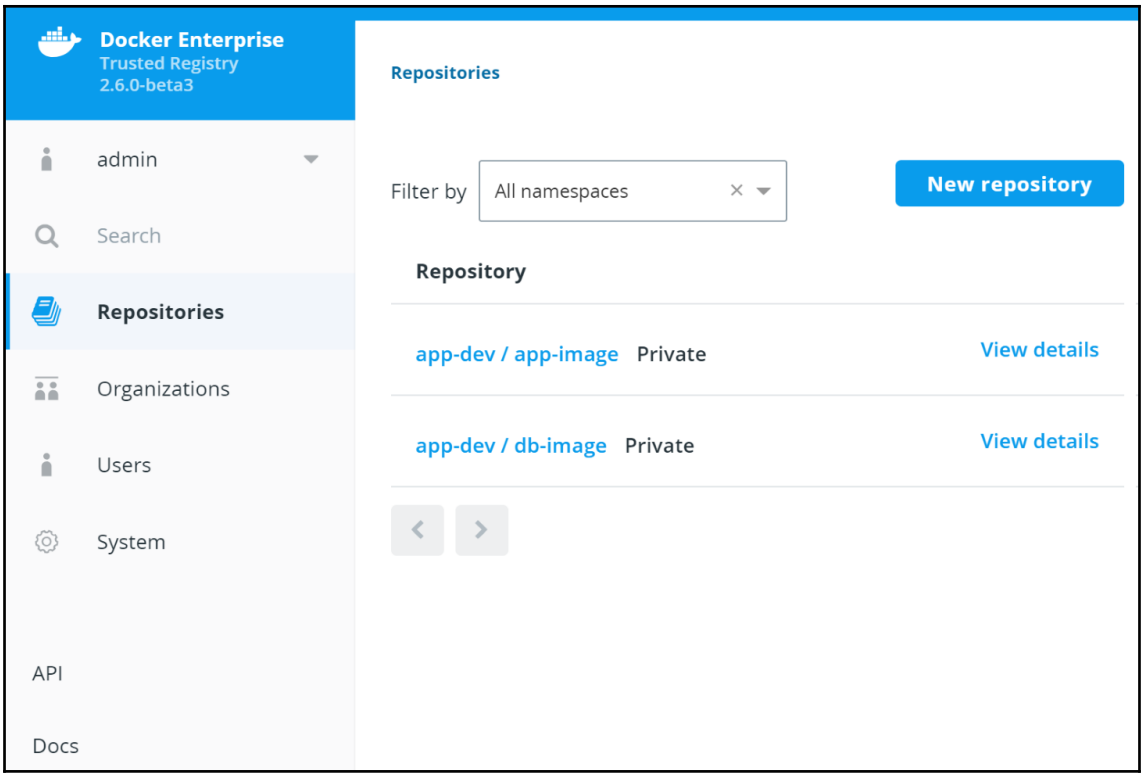

About Docker
Discover Docker Enterprise Edition
Settings
Check for Updates
Diagnose and Feedback...
Switch to Windows containers...
Docker Store
Documentation
Kitematic
nvisiantc
Repositories
Kubernetes
Restart...
Quit Docker

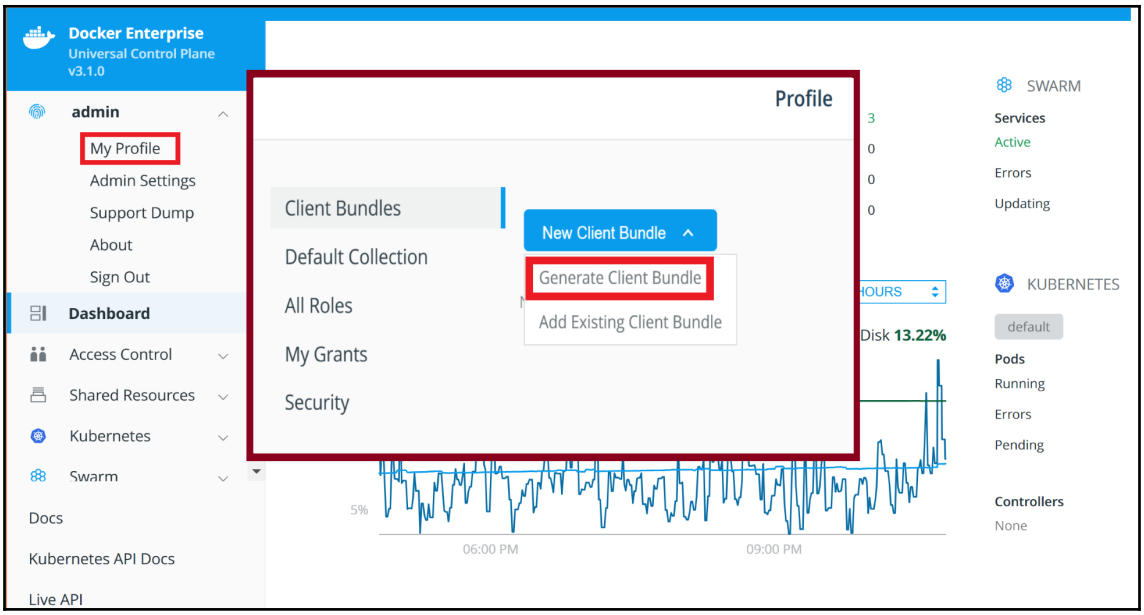

Application VM
News Letter App
-
WebForms
ASP.NET 3.5
-
Web-Server
Web-Asp-Net
ServiceMonitor
-
Windows Server
2016
Database VM
SignUpDb
-
SQL Server Express
2016 SP1
-
Windows Server
Core2016
Hyper-V
Windows Server 2016

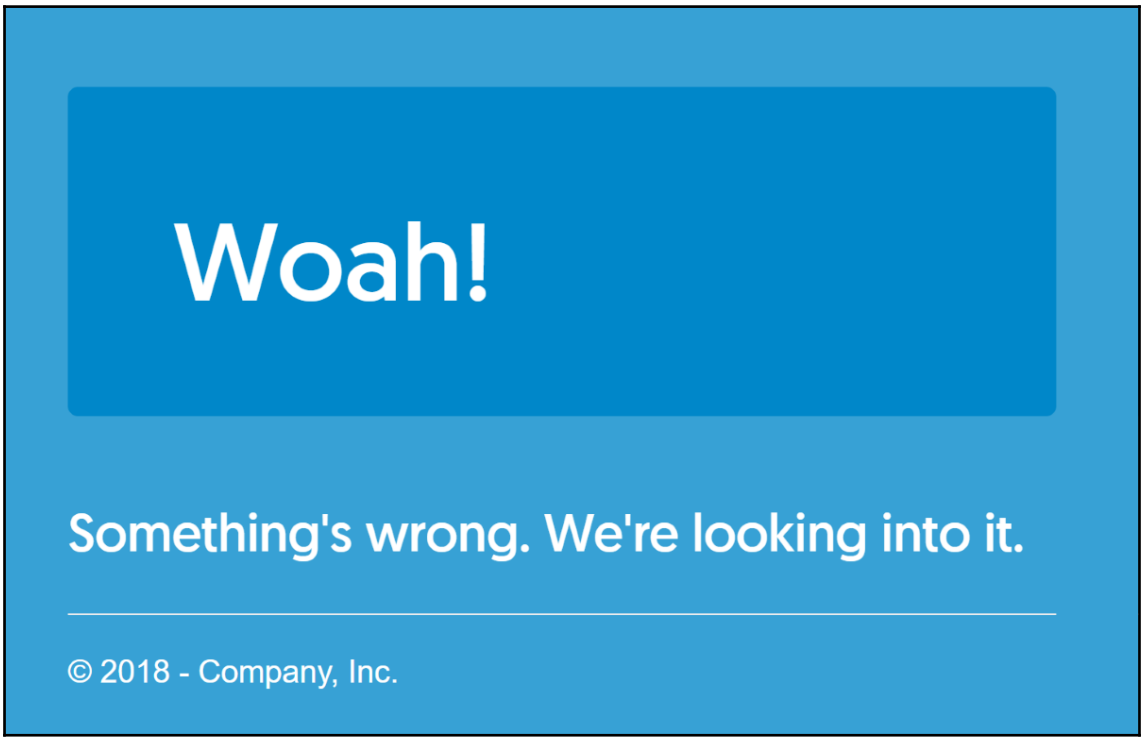

microsoft/dotnet-framework:3.5-sdk
<Official Image>
mta-dev-web-builder:3.5
<Base-Image>
App-Image:v1
<Application Image>


Application Container
signup-app
-
app-image:v1
Database Container
signup-db
-
db-image:v1
C:\mssql
NAT Network
Volume
Docker 18.09 on Windows Server 2016

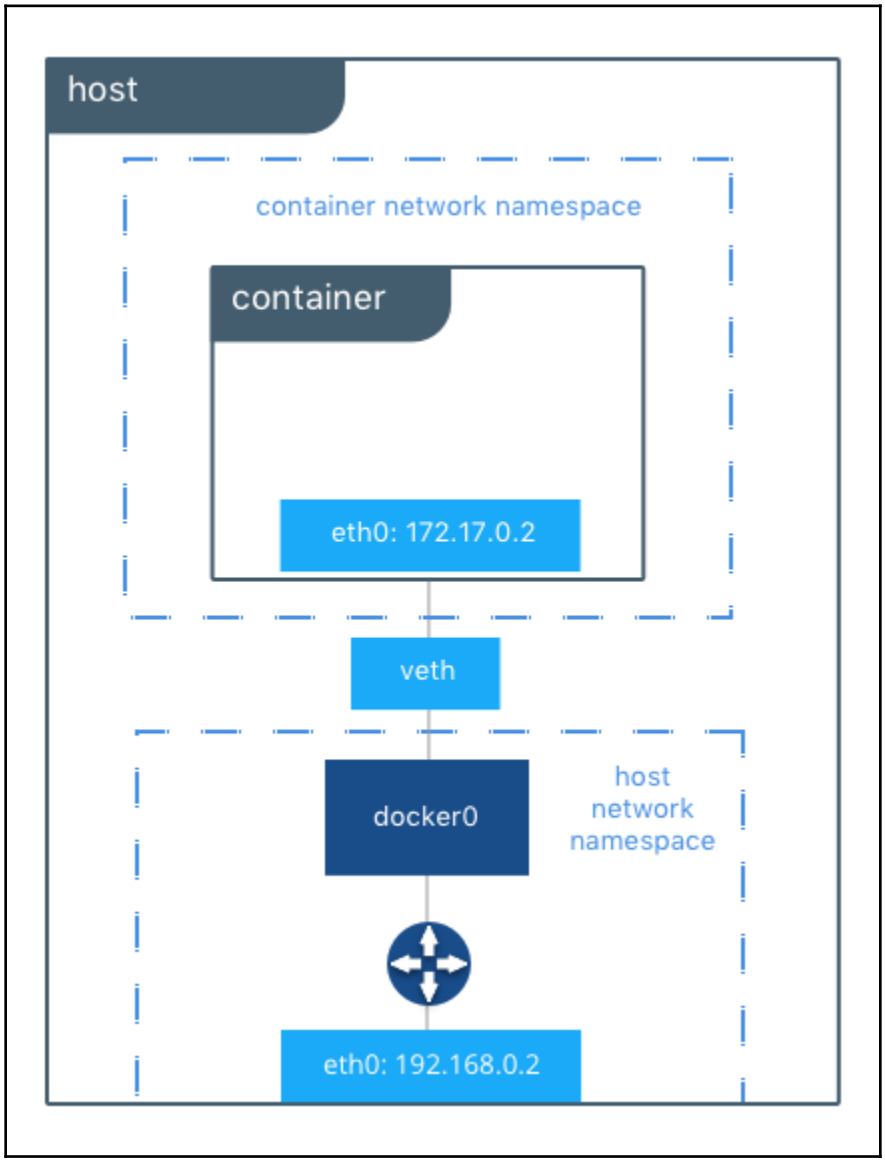

http://172.31.0.19:8000/
Home Page
Have you tried Play with Docker?
A simple, interactive and fun playground to learn Docker.
dockercon18
june 12-15
san francisco
Docker from the comfort of your browser
Play with Docker (PWD) gives you a configured Docker setup running in the cloud, which you manage from your browser.
There's a playground for just trying things out - like Docker Swarm mode - and there are self-paced training labs too.
Play with Docker
PWD Classroom
Interested? Get the newsletter!
Give us your details and we'll keep you posted.
It only takes 30 seconds to sign up.
And we probably won't spam you very much.
Sign Up »
© 2018 - Company, Inc.

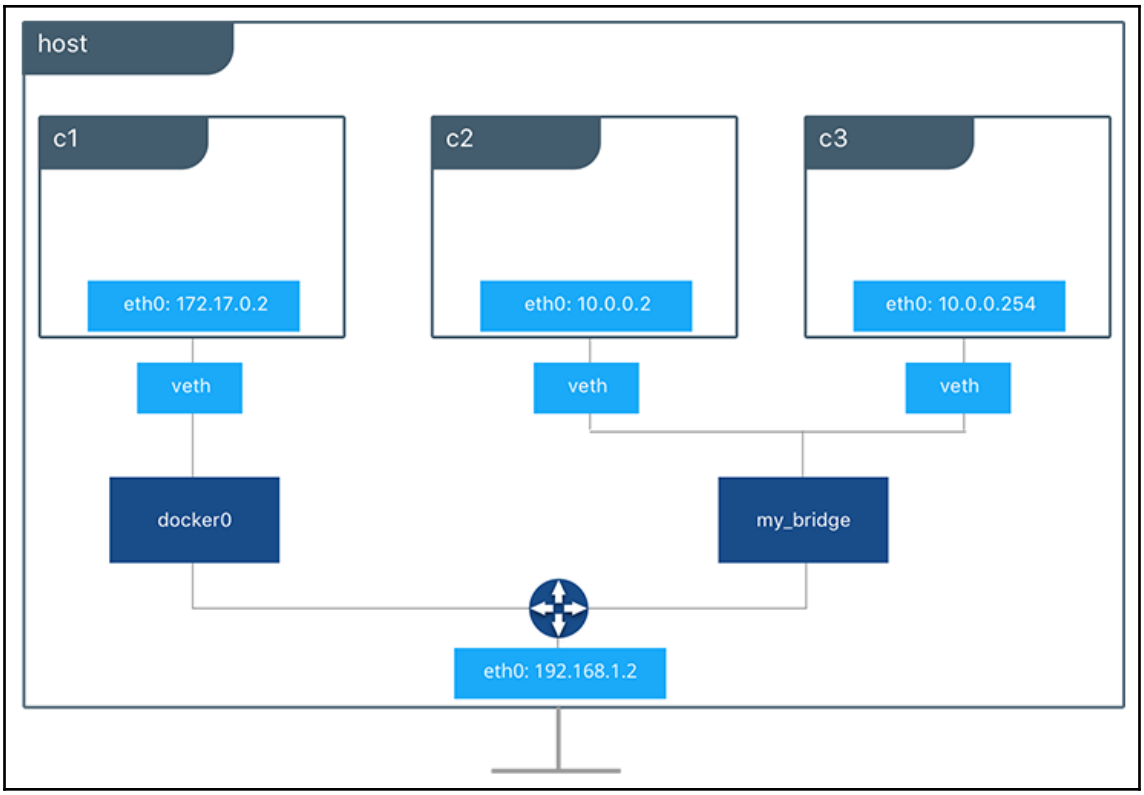

Docker Enterprise
Trusted Registry
2.6.0-beta3
admin
Search
Repositories
Organizations
Users
System
API
Docs
Repositories
Filter by
All namespaces
New repository
Repository
app-dev / app-image
Private
View details
app-dev / db-image
Private
View details

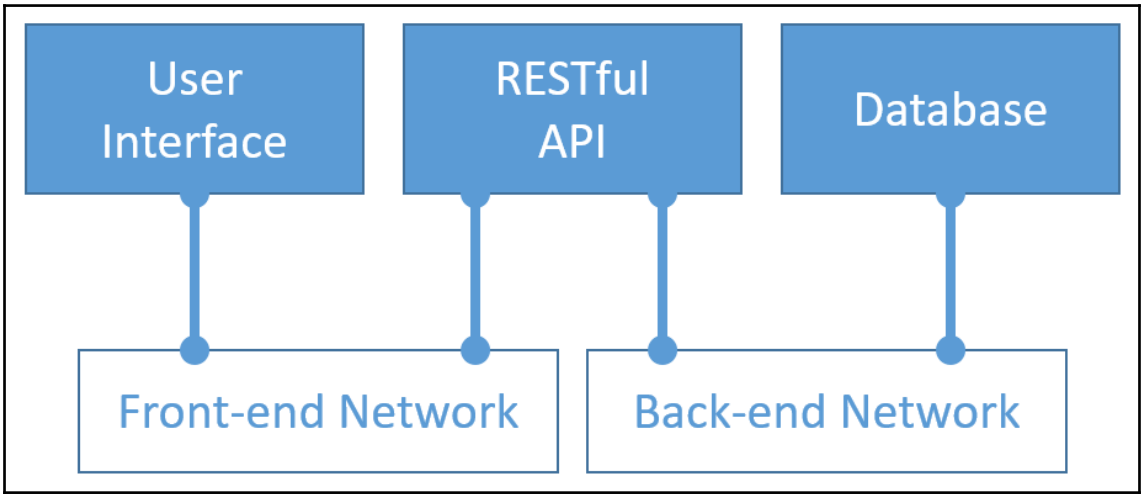

Docker Enterprise
Universal Control Plane
v3.1.0
admin
My Profile
Admin Settings
Support Dump
About
Sign Out
Dashboard
Access Control
Shared Resources
Kubernetes
Swarm
Docs
Kubernetes API Docs
Live API
Profile
Client Bundles
Default Collection
All Roles
My Grants
Security
New Client Bundle
Generate Client Bundle
Add Existing Client Bundle
SWARM
Services
Active
Errors
Updating
KUBERNETES
default
Pods
Running
Errors
Pending
Controllers
None
Disk 13.22%
5%
06:00 PM
09:00 PM

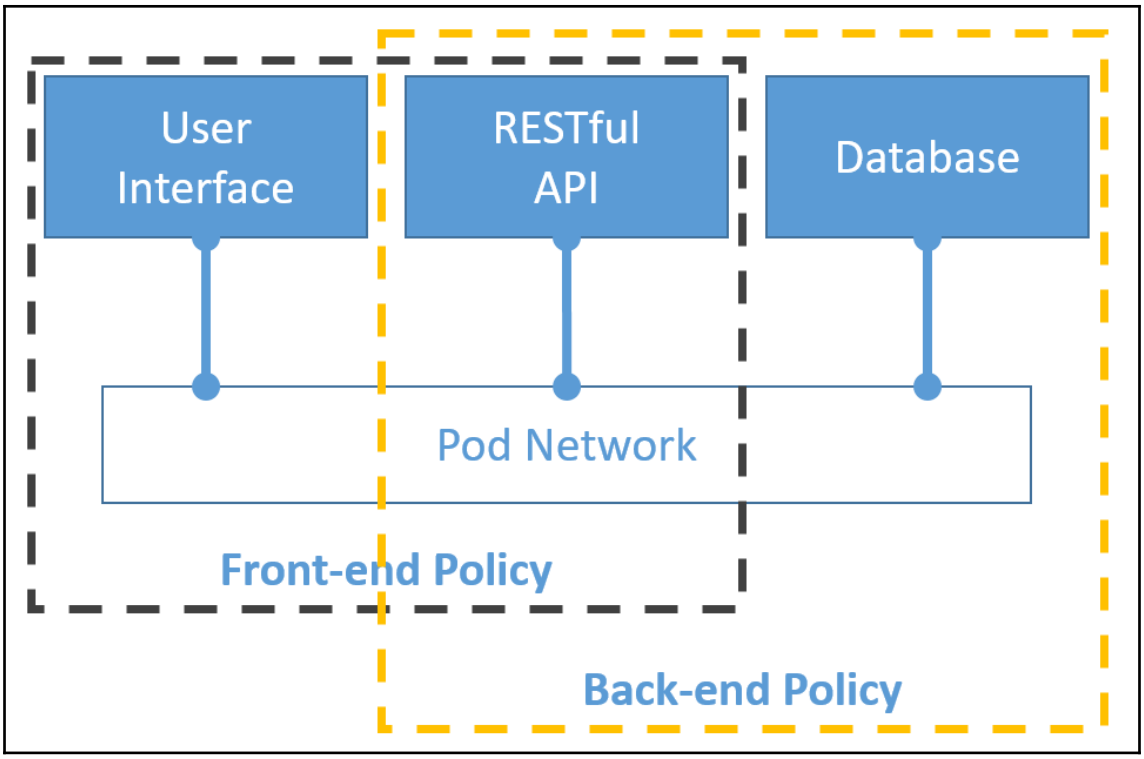

Woah!
Something's wrong. We're looking into it.
© 2018 - Company, Inc.

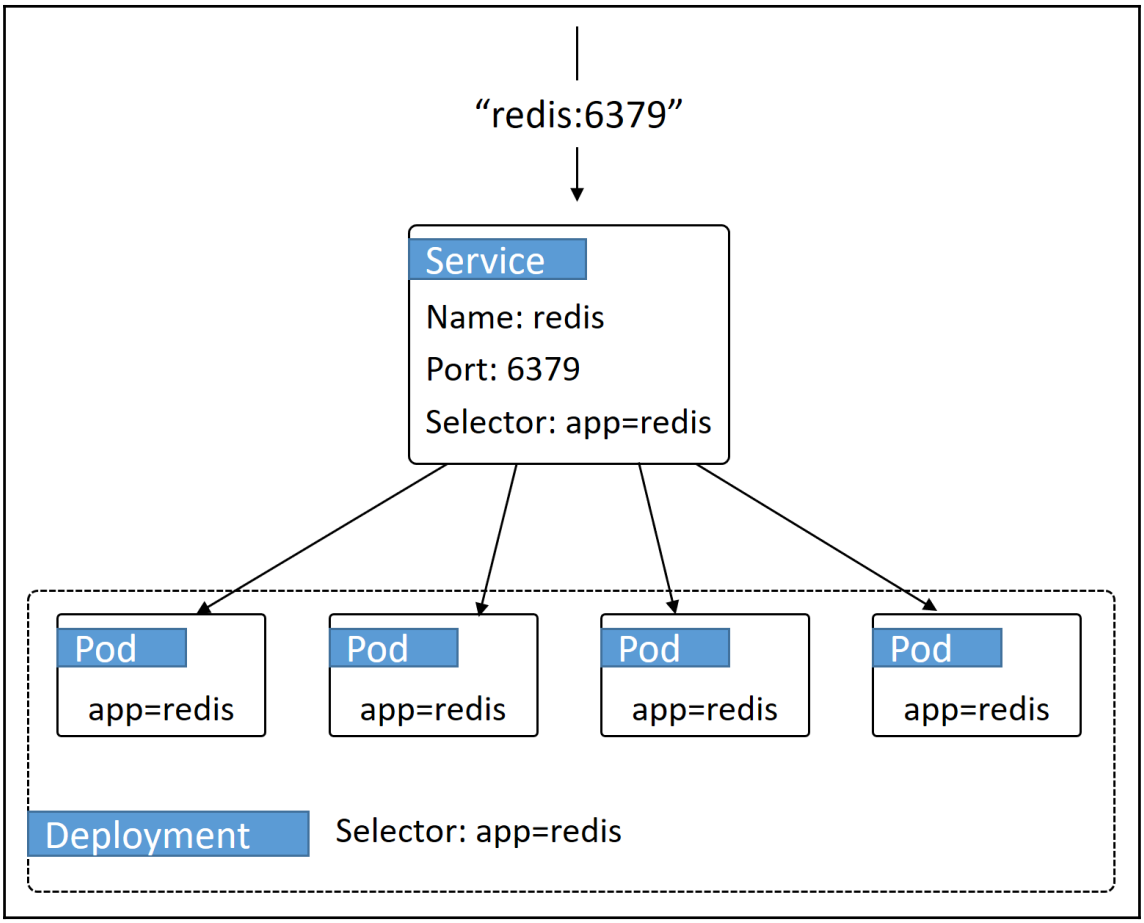
# Chapter 4: Preparing the Docker Enterprise Pilot Cluster

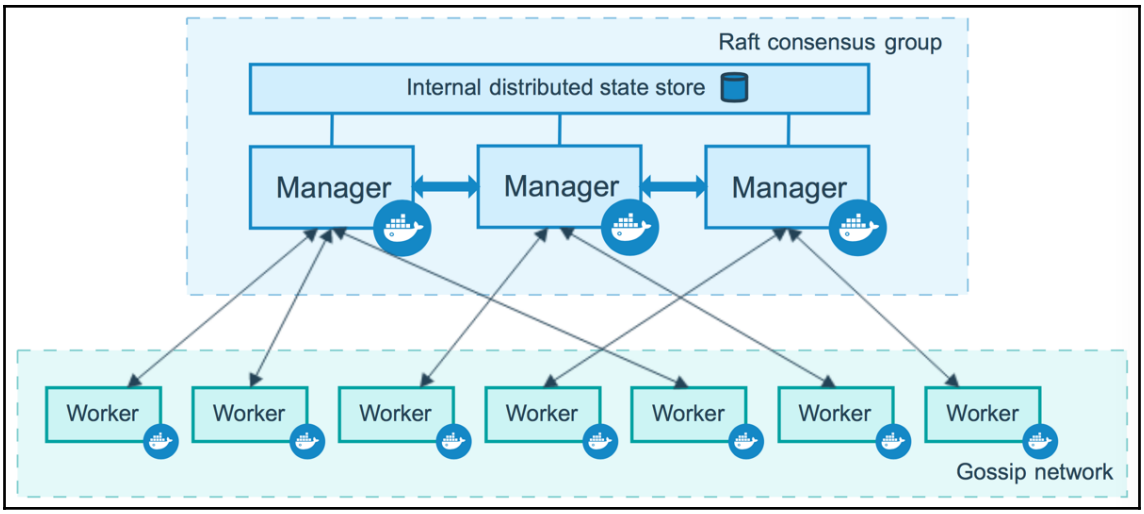


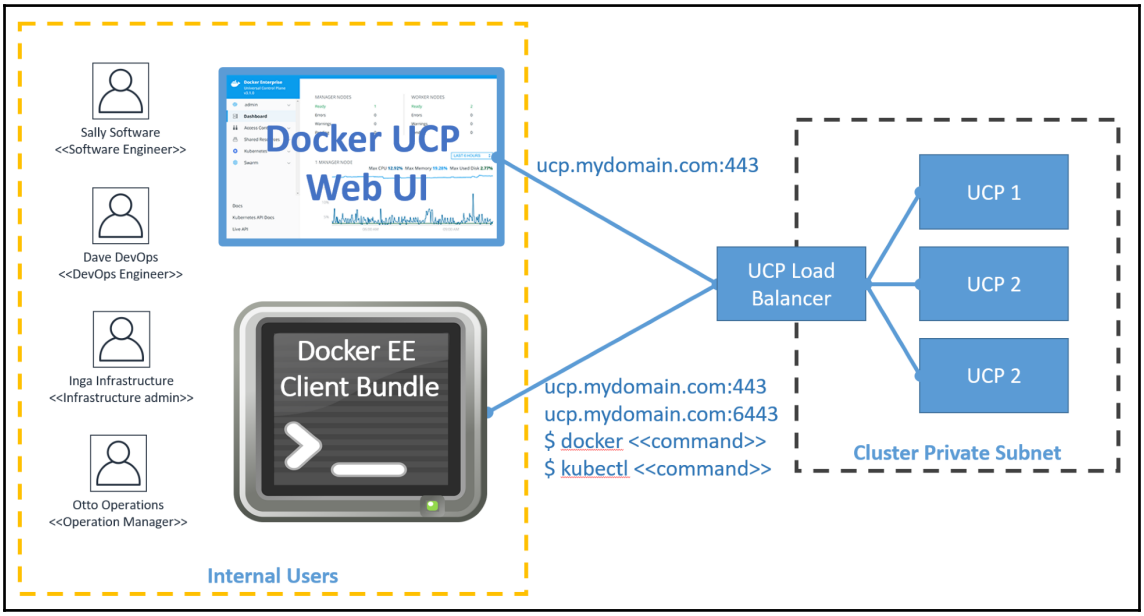

host
c1
c2
c3
eth0: 172.17.0.2
eth0: 10.0.0.2
eth0: 10.0.0.254
veth
veth
veth
docker0
my_bridge
eth0: 192.168.1.2

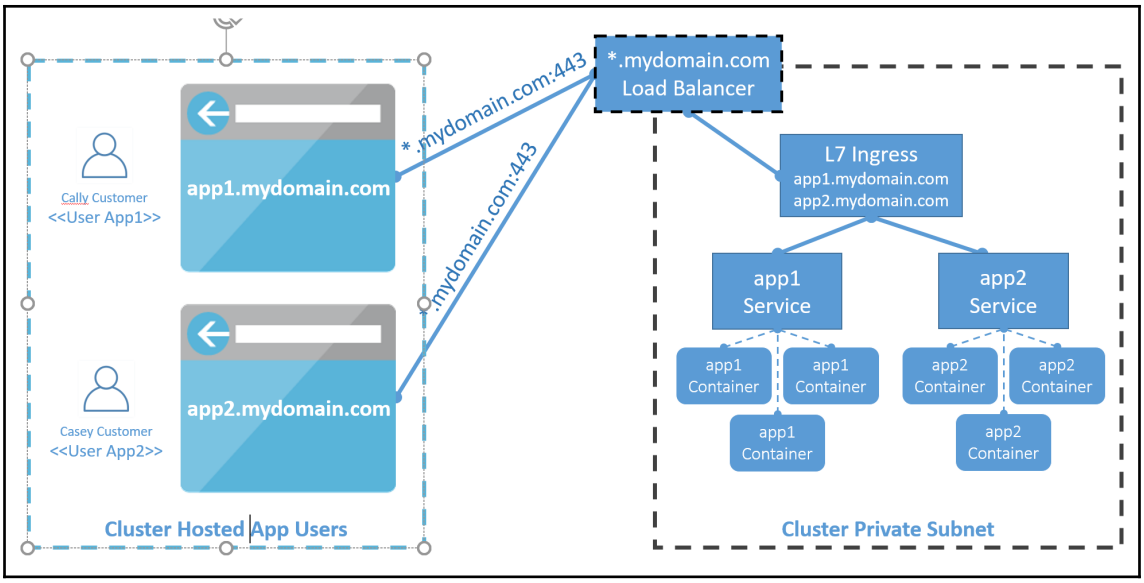

User Interface
RESTful API
Database
Front-end Network
Back-end Network

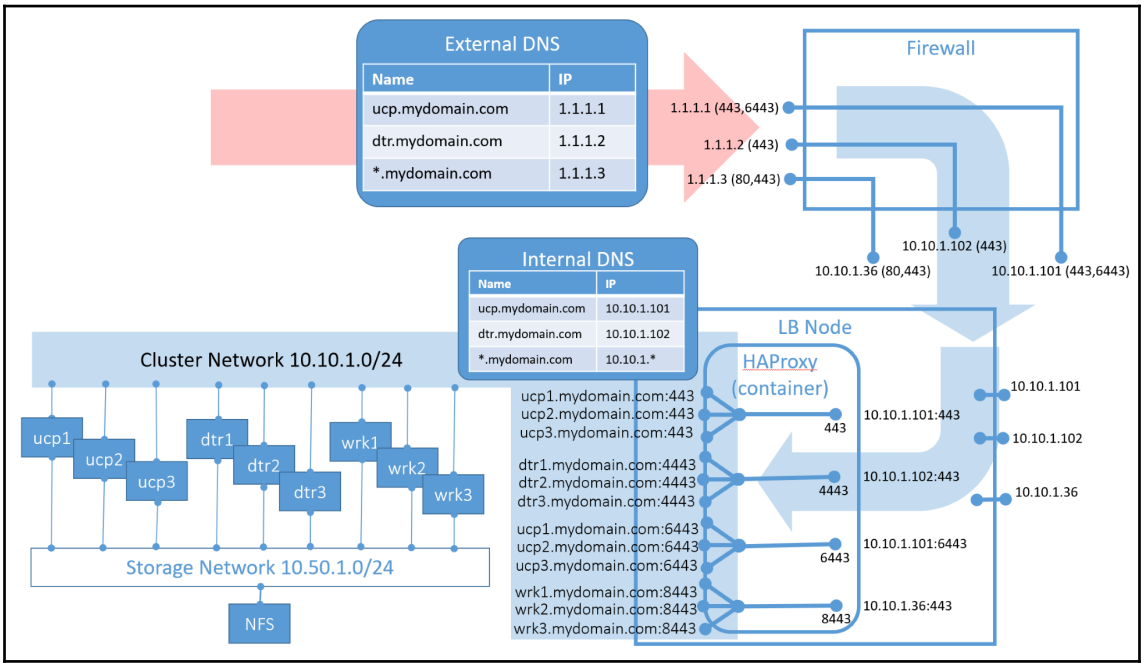

User Interface
RESTful API
Database
Pod Network
Front-end Policy
Back-end Policy

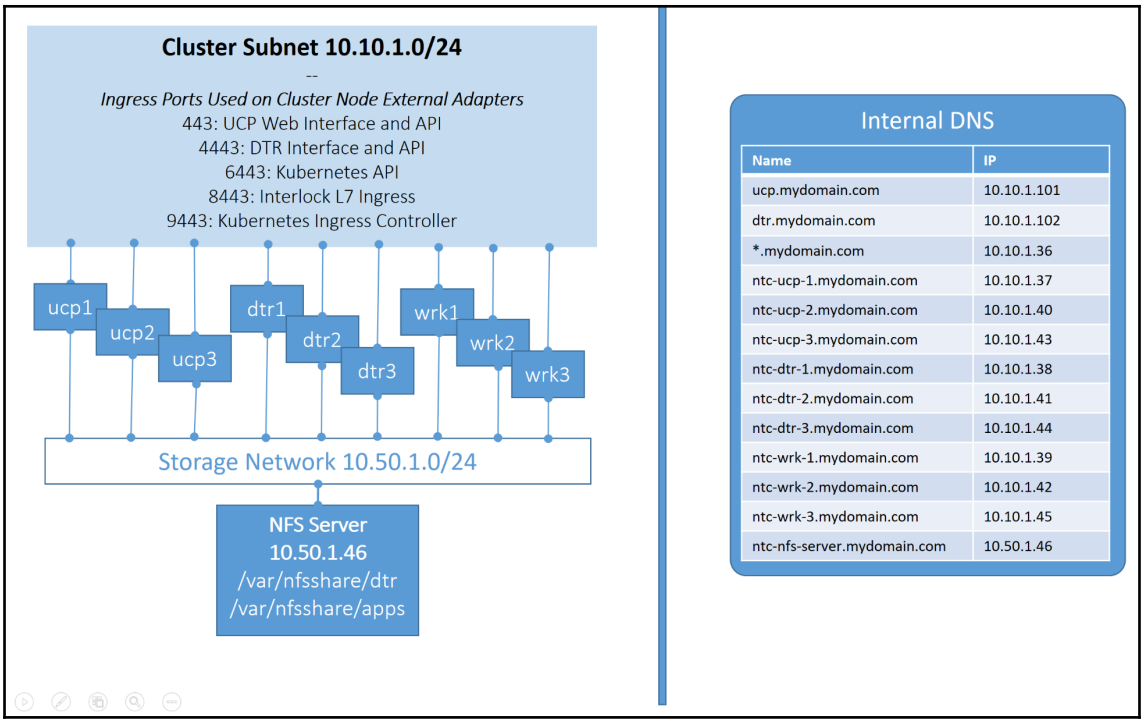

"redis:6379"
Service
Name: redis
Port: 6379
Selector: app=redis
Pod
app=redis
Pod
app=redis
Pod
app=redis
Pod
app=redis
Deployment
Selector: app=redis


Raft consensus group
Internal distributed state store
Manager
Manager
Manager
Worker
Worker
Worker
Worker
Worker
Worker
Worker
Gossip network

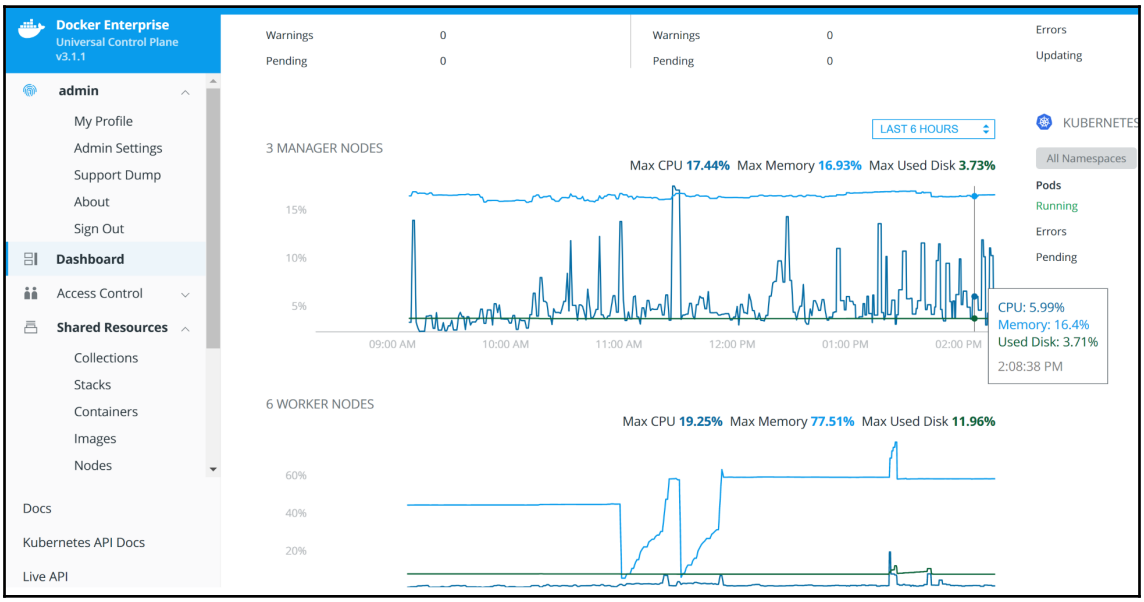

Sally Software
<<Software Engineer>>
Dave DevOps
<<DevOps Engineer>>
Inga Infrastructure
<<Infrastructure admin>>
Otto Operations
<<Operation Manager>>
Docker UCP
Web UI
Docker EE
Client Bundle
Internal Users
ucp.mydomain.com:443
ucp.mydomain.com:443
ucp.mydomain.com:6443
$ docker <<command>>
$ kubectl <<command>>
UCP Load
Balancer
UCP 1
UCP 2
UCP 2
Cluster Private Subnet

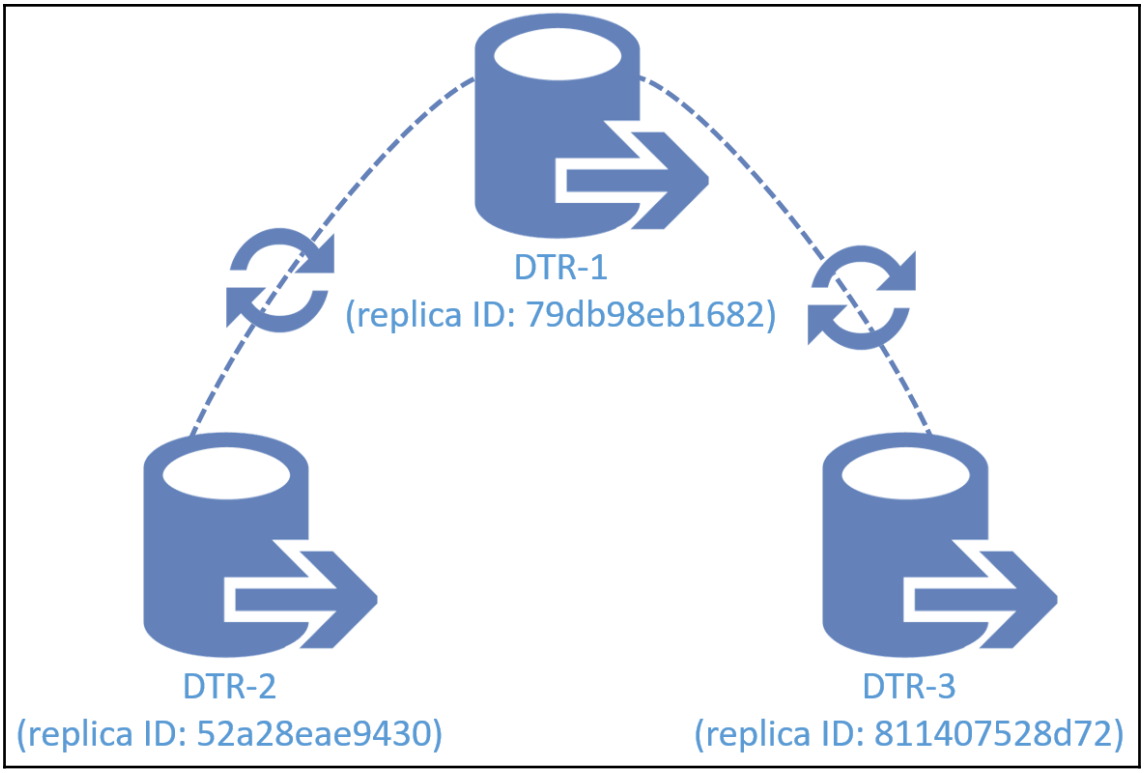

*.mydomain.com
Load Balancer
*.mydomain.com:443
*.mydomain.com:443
Cally Customer
<<User App1>>
app1.mydomain.com
Casey Customer
<<User App2>>
app2.mydomain.com
Cluster Hosted App Users
L7 Ingress
app1.mydomain.com
app2.mydomain.com
app1
Service
app2
Service
app1
Container
app1
Container
app1
Container
app2
Container
app2
Container
app2
Container
Cluster Private Subnet


External DNS
Name
IP
ucp.mydomain.com
1.1.1.1
dtr.mydomain.com
1.1.1.2
*.mydomain.com
1.1.1.3
Firewall
1.1.1.1 (443,6443)
1.1.1.2 (443)
1.1.1.3 (80,443)
10.10.1.36 (80,443)
10.10.1.102 (443)
10.10.1.101 (443,6443)
Internal DNS
Name
IP
ucp.mydomain.com
10.10.1.101
dtr.mydomain.com
10.10.1.102
*.mydomain.com
10.10.1.*
LB Node
HAProxy
(container)
Cluster Network 10.10.1.0/24
ucp1
ucp2
ucp3
dtr1
dtr2
dtr3
wrk1
wrk2
wrk3
Storage Network 10.50.1.0/24
NFS
ucp1.mydomain.com:443
ucp2.mydomain.com:443
ucp3.mydomain.com:443
443
10.10.1.101:443
dtr1.mydomain.com:4443
dtr2.mydomain.com:4443
dtr3.mydomain.com:4443
4443
10.10.1.102:443
ucp1.mydomain.com:6443
ucp2.mydomain.com:6443
ucp3.mydomain.com:6443
6443
10.10.1.101:6443
wrk1.mydomain.com:8443
wrk2.mydomain.com:8443
wrk3.mydomain.com:8443
8443
10.10.1.36:443
10.10.1.101
10.10.1.102
10.10.1.36

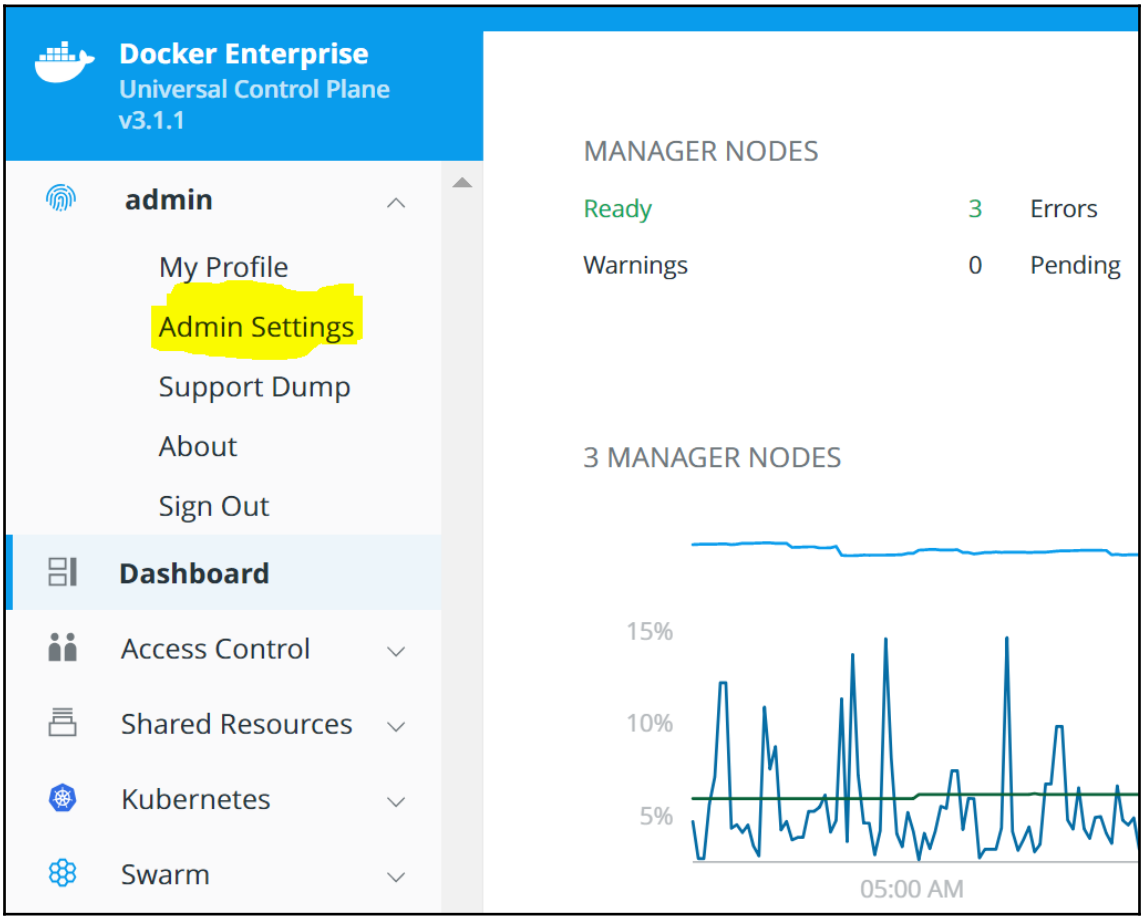


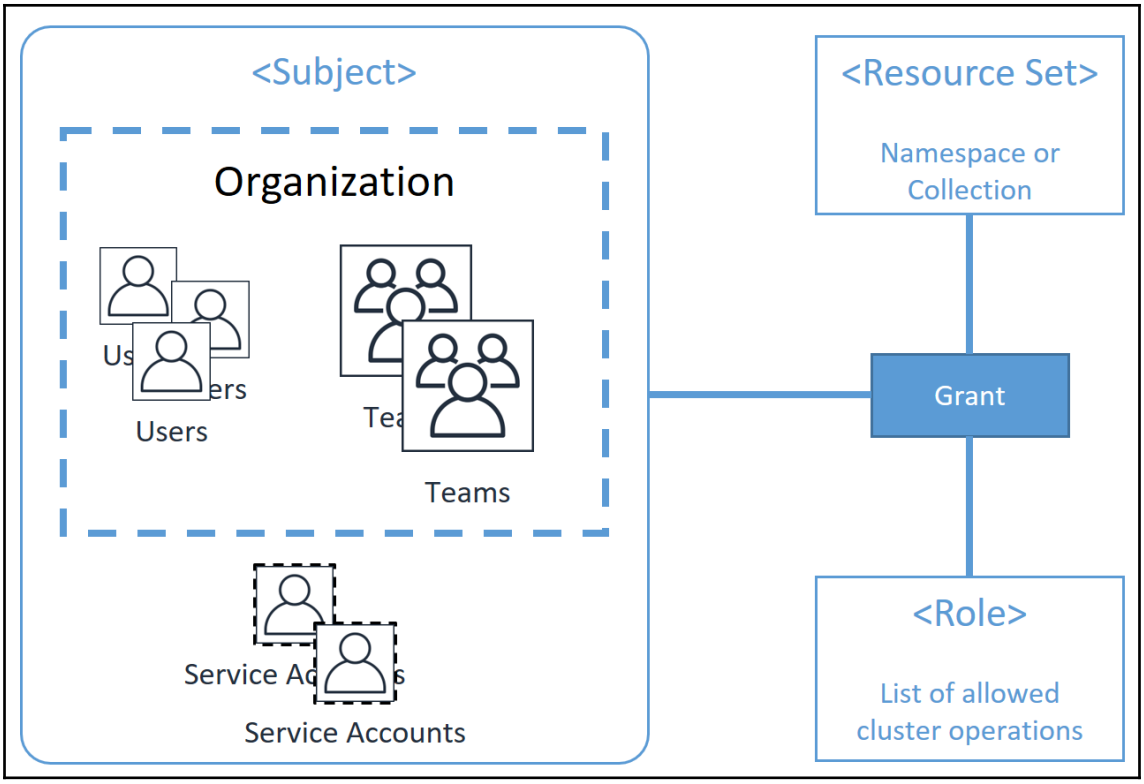

| Name | IP |
|---|---|
| ucp.mydomain.com | 10.10.1.101 |
| dtr.mydomain.com | 10.10.1.102 |
| *.mydomain.com | 10.10.1.36 |
| ntc-ucp-1.mydomain.com | 10.10.1.37 |
| ntc-ucp-2.mydomain.com | 10.10.1.40 |
| ntc-ucp-3.mydomain.com | 10.10.1.43 |
| ntc-dtr-1.mydomain.com | 10.10.1.38 |
| ntc-dtr-2.mydomain.com | 10.10.1.41 |
| ntc-dtr-3.mydomain.com | 10.10.1.44 |
| ntc-wrk-1.mydomain.com | 10.10.1.39 |
| ntc-wrk-2.mydomain.com | 10.10.1.42 |
| ntc-wrk-3.mydomain.com | 10.10.1.45 |
| ntc-nfs-server.mydomain.com | 10.50.1.46 |

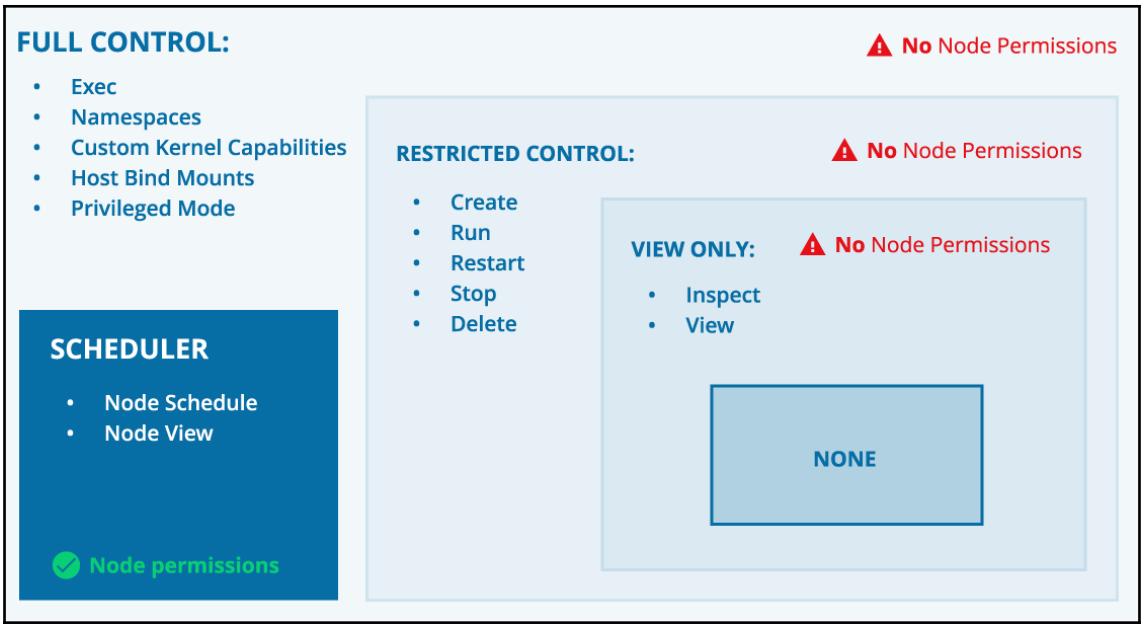


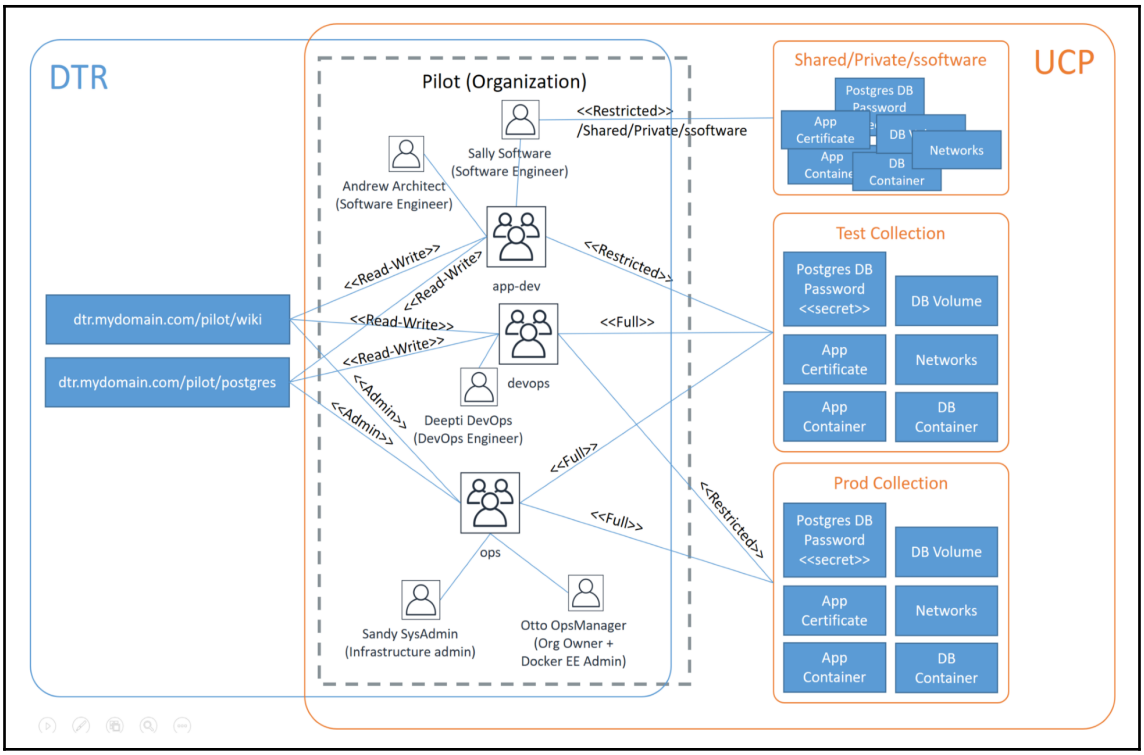

DTR-1
(replica ID: 79db98eb1682)
DTR-2
(replica ID: 52a28eae9430)
DTR-3
(replica ID: 811407528d72)

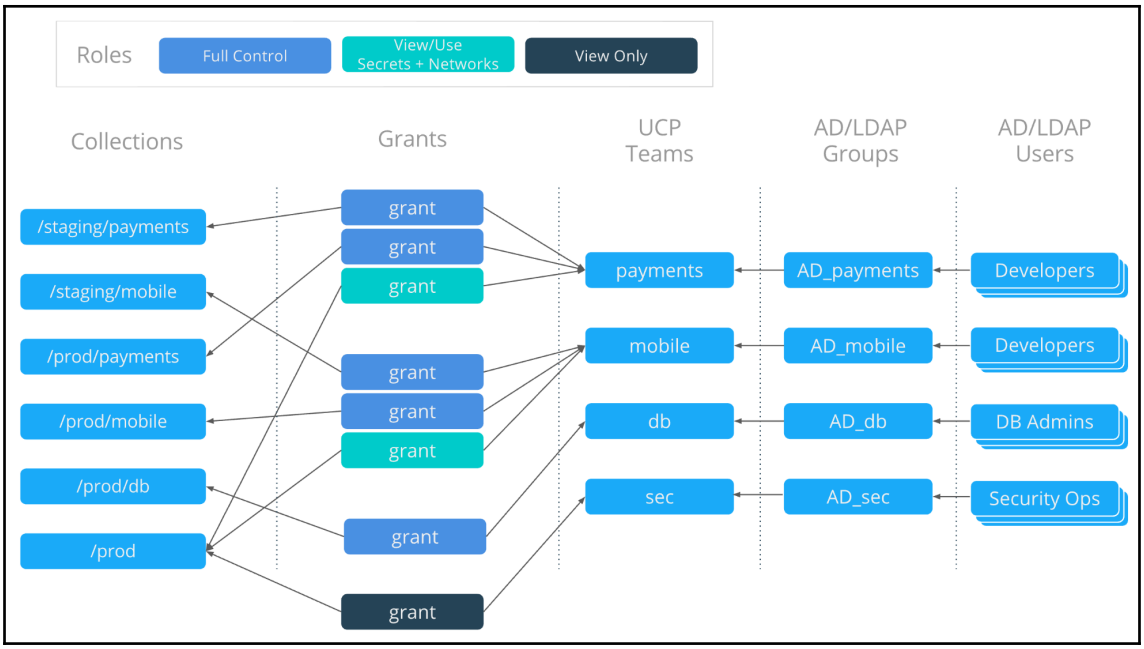
# Chapter 5: Prepare and Deploy a Docker Enterprise Pilot Application

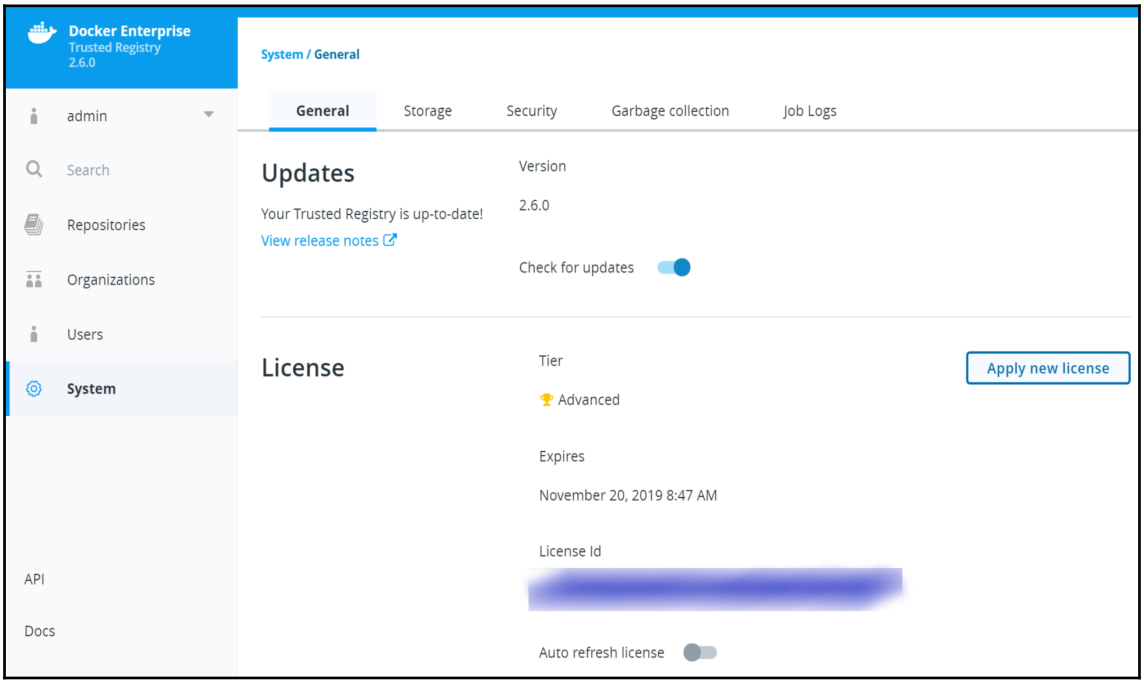


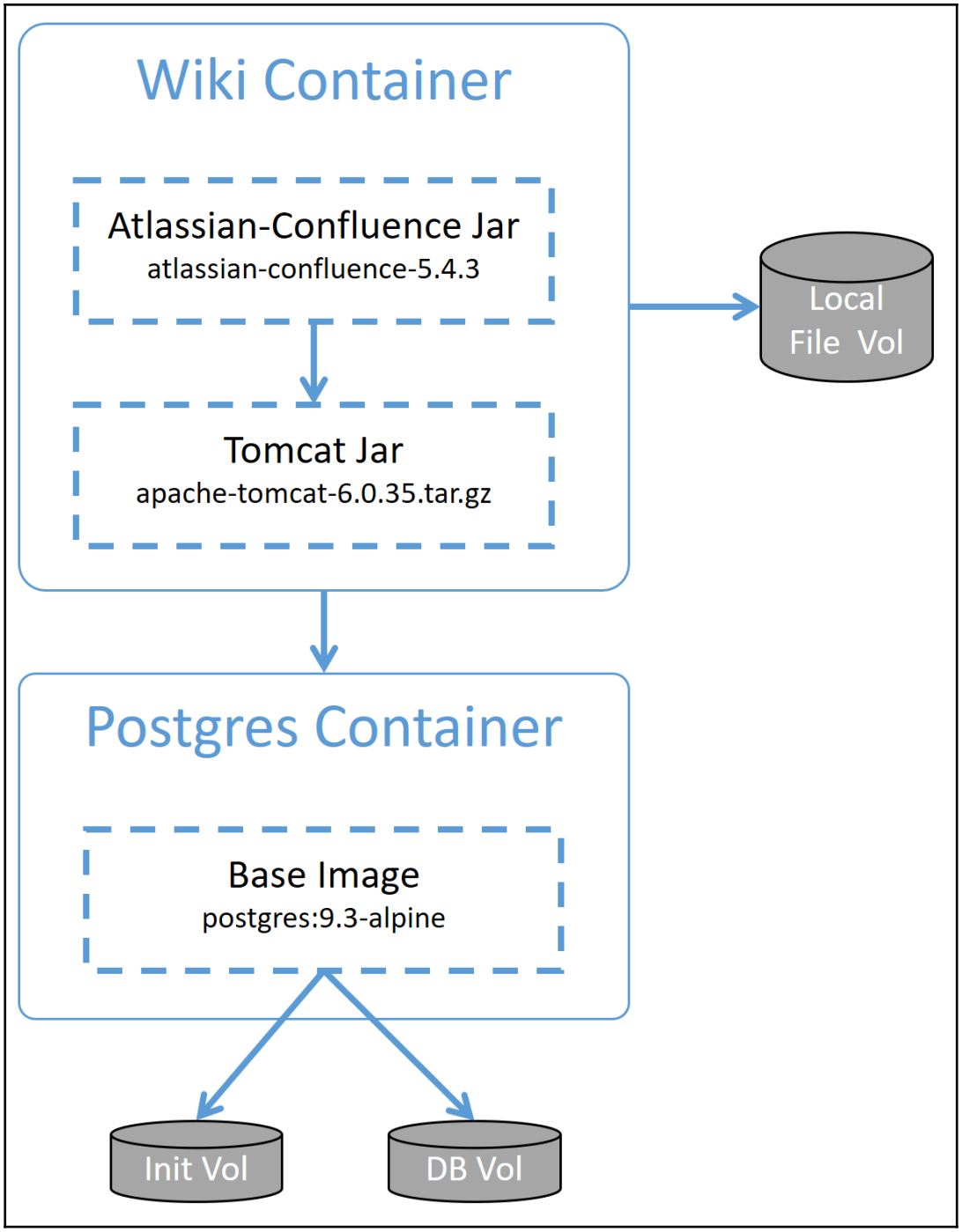

<Subject>
Organization
Users
Teams
Service Accounts
<Resource Set>
Namespace or Collection
Grant
<Role>
List of allowed cluster operations

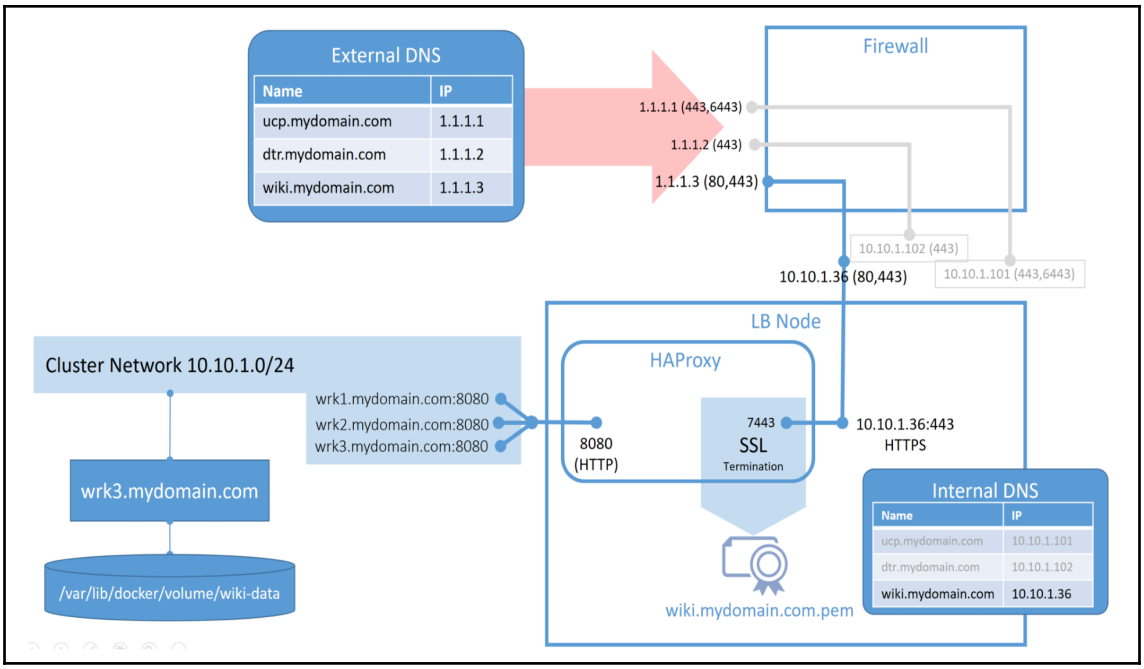

FULL CONTROL:
No Node Permissions
Exec
Namespaces
Custom Kernel Capabilities
Host Bind Mounts
Privileged Mode
RESTRICTED CONTROL:
No Node Permissions
Create
Run
Restart
Stop
Delete
VIEW ONLY:
No Node Permissions
Inspect
View
NONE
SCHEDULER
Node Schedule
Node View
Node permissions

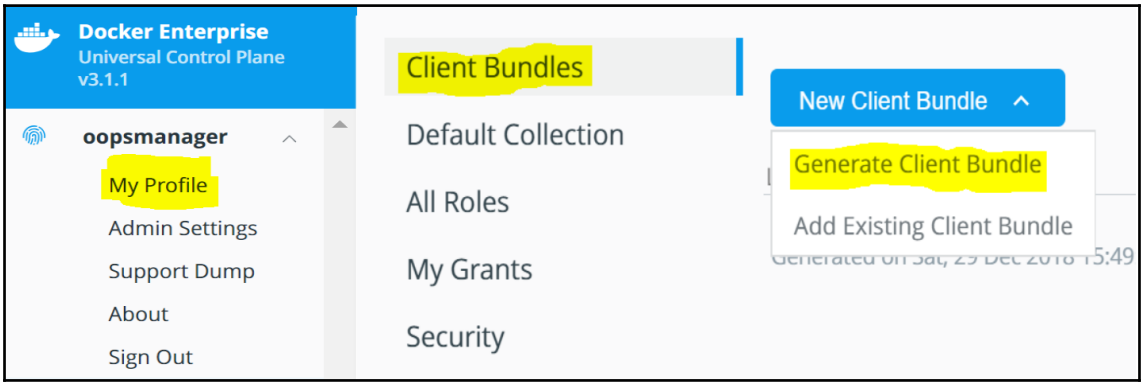

DTR
Pilot (Organization)
<<Restricted>>
/Shared/Private/ssoftware
Sally Software
(Software Engineer)
Andrew Architect
(Software Engineer)
app-dev
<<Restricted>>
<<Read-Write>>
<<Read-Write>>
<<Read-Write>>
<<Read-Write>>
<<Full>>
dtr.mydomain.com/pilot/wiki
dtr.mydomain.com/pilot/postgres
devops
Deepti DevOps
(DevOps Engineer)
<<Admin>>
<<Admin>>
<<Full>>
<<Full>>
<<Restricted>>
ops
Sandy SysAdmin
(Infrastructure admin)
Otto OpsManager
(Org Owner +
Docker EE Admin)
Shared/Private/ssoftware
Postgres DB
Password
App
Certificate
DB
Networks
App
Container
DB
Container
UCP
Test Collection
Postgres DB
Password
<<secret>>
DB Volume
App
Certificate
Networks
App
Container
DB
Container
Prod Collection
Postgres DB
Password
<<secret>>
DB Volume
App
Certificate
Networks
App
Container
DB
Container


Roles
Full Control
View/Use Secrets + Networks
View Only
Collections
Grants
UCP Teams
AD/LDAP Groups
AD/LDAP Users
/staging/payments
/staging/mobile
/prod/payments
/prod/mobile
/prod/db
/prod
grant
payments
mobile
db
sec
AD_payments
AD_mobile
AD_db
AD_sec
Developers
Developers
DB Admins
Security Ops

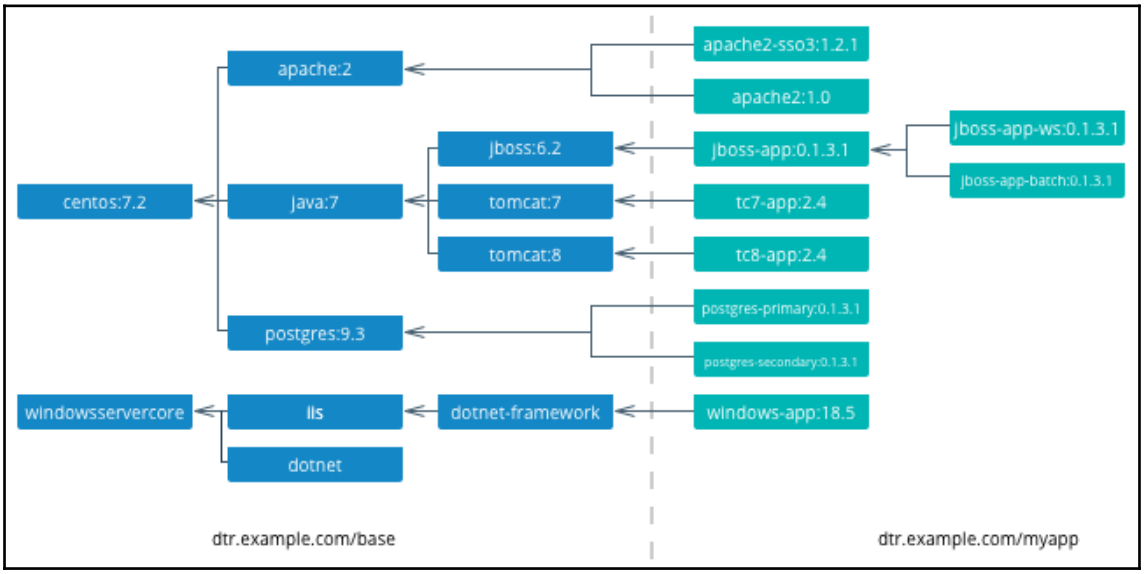

Docker Enterprise
Trusted Registry
2.6.0
admin
Search
Repositories
Organizations
Users
System
API
Docs
System / General
General
Storage
Security
Garbage collection
Job Logs
Updates
Your Trusted Registry is up-to-date!
View release notes
Version
2.6.0
Check for updates
License
Tier
Advanced
Apply new license
Expires
November 20, 2019 8:47 AM
License Id
Auto refresh license

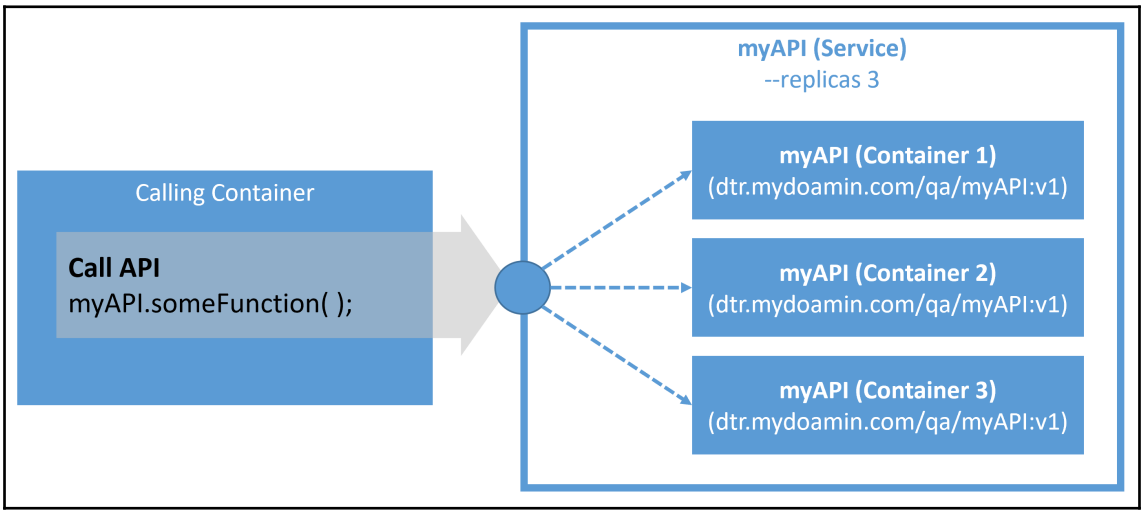

Wiki Container
Atlassian-Confluence Jar
atlassian-confluence-5.4.3
Tomcat Jar
apache-tomcat-6.0.35.tar.gz
Local
File Vol
Postgres Container
Base Image
postgres:9.3-alpine
Init Vol
DB Vol

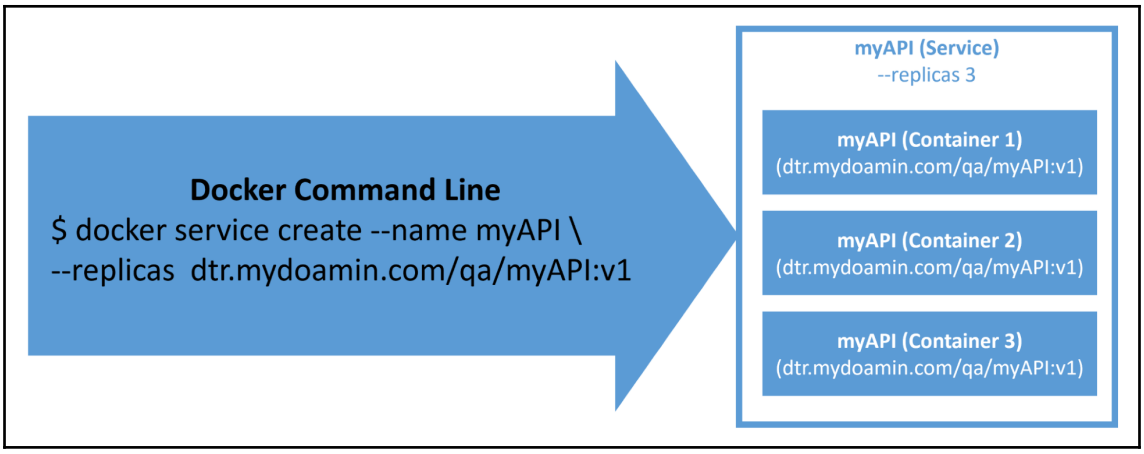

External DNS
Name
IP
ucp.mydomain.com
1.1.1.1
dtr.mydomain.com
1.1.1.2
wiki.mydomain.com
1.1.1.3
Firewall
1.1.1.1 (443,6443)
1.1.1.2 (443)
1.1.1.3 (80,443)
10.10.1.102 (443)
10.10.1.36 (80,443)
10.10.1.101 (443,6443)
LB Node
HAProxy
Cluster Network 10.10.1.0/24
wrk1.mydomain.com:8080
wrk2.mydomain.com:8080
wrk3.mydomain.com:8080
8080
(HTTP)
7443
SSL
Termination
10.10.1.36:443
HTTPS
wrk3.mydomain.com
/var/lib/docker/volume/wiki-data
Internal DNS
Name
IP
ucp.mydomain.com
10.10.1.101
dtr.mydomain.com
10.10.1.102
wiki.mydomain.com
10.10.1.36
wiki.mydomain.com.pem

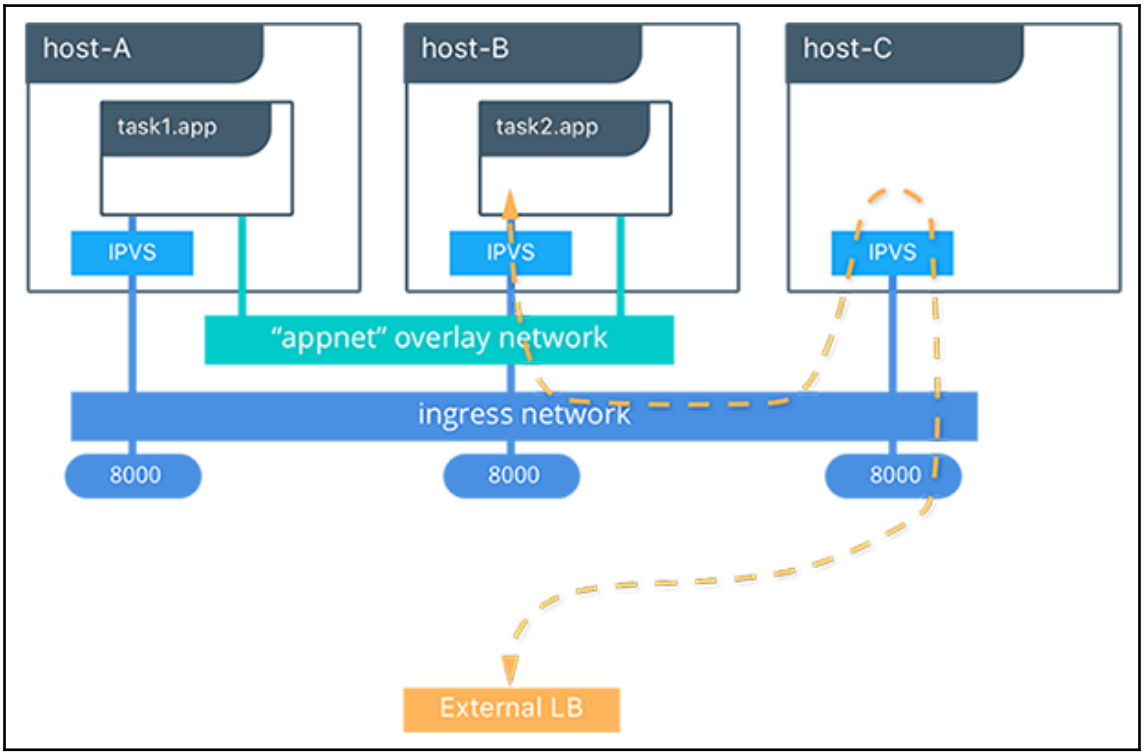

Docker Enterprise
Universal Control Plane
v3.1.1
oopsmanager
My Profile
Admin Settings
Support Dump
About
Sign Out
Client Bundles
Default Collection
All Roles
My Grants
Security
New Client Bundle
Generate Client Bundle
Add Existing Client Bundle

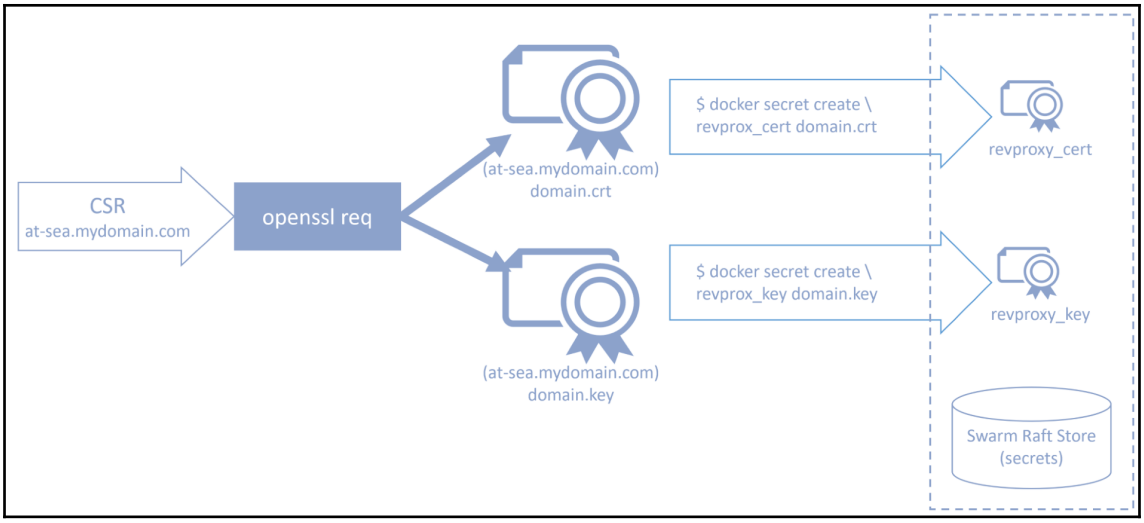
# Chapter 6: Design and Pilot a Docker Enterprise CI Pipeline

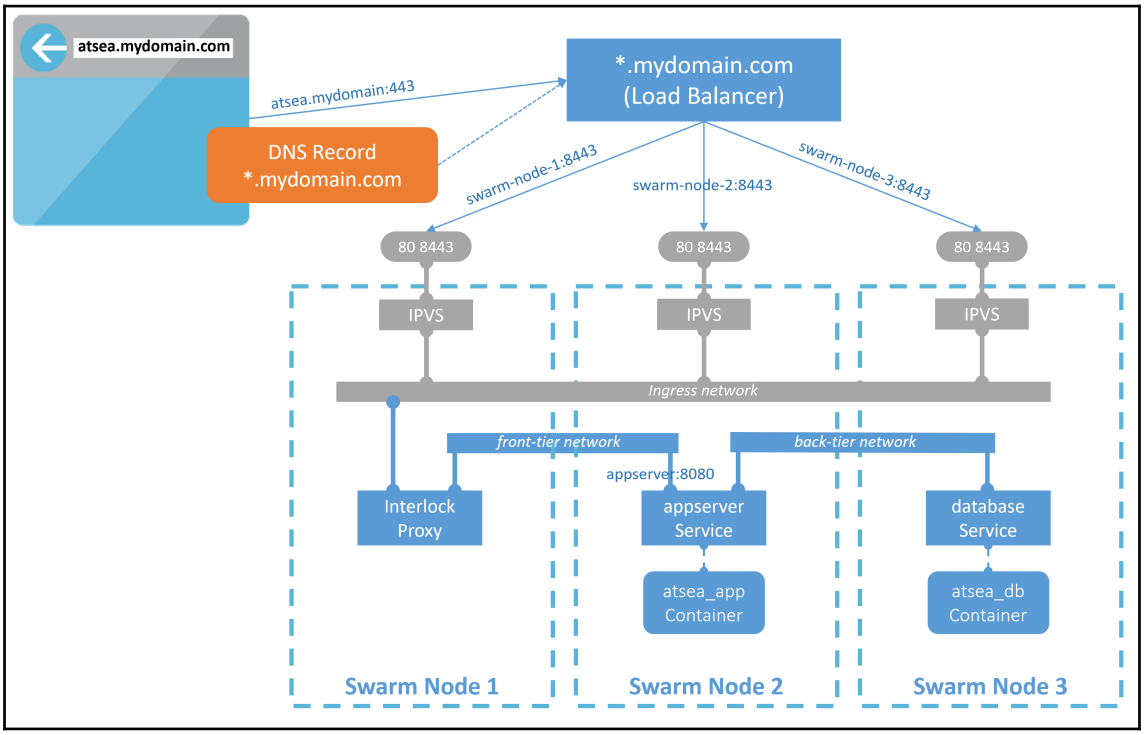


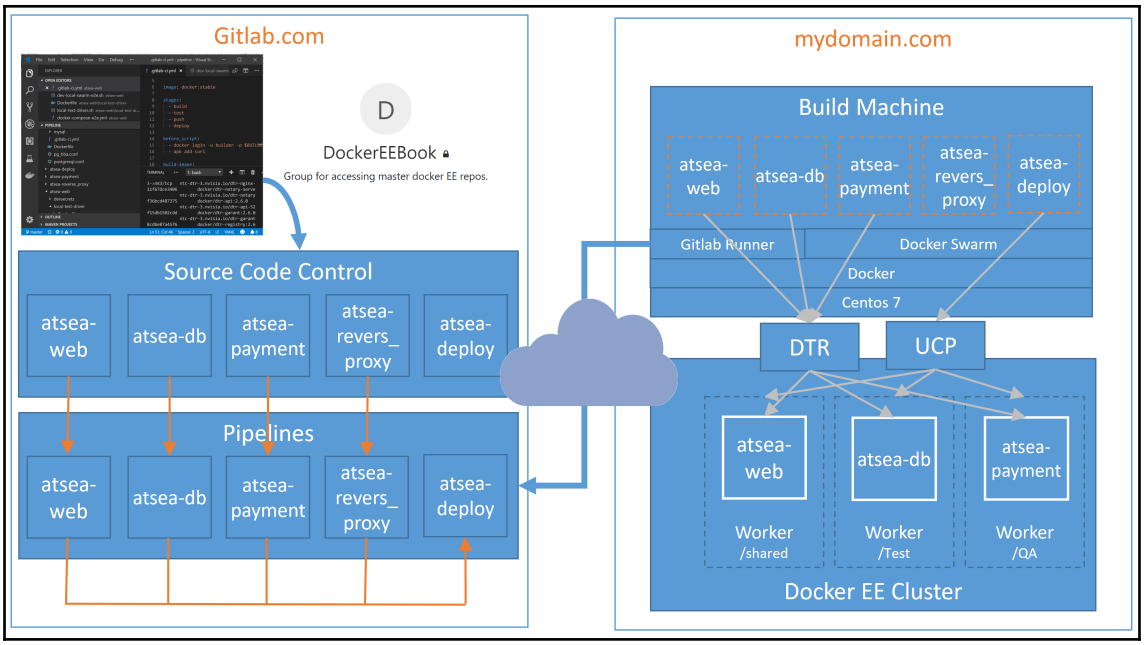




Docker Command Line
$ docker service create --name myAPI \
--replicas dtr.mydoamin.com/qa/myAPI:v1
myAPI (Service)
--replicas 3
myAPI (Container 1)
(dtr.mydoamin.com/qa/myAPI:v1)
myAPI (Container 2)
(dtr.mydoamin.com/qa/myAPI:v1)
myAPI (Container 3)
(dtr.mydoamin.com/qa/myAPI:v1)


host-A
task1.app
IPVS
host-B
task2.app
IPVS
host-C
IPVS
"appnet" overlay network
ingress network
8000
8000
8000
External LB


CSR
at-sea.mydomain.com
openssl req
(at-sea.mydomain.com)
domain.crt
(at-sea.mydomain.com)
domain.key
$ docker secret create \
revprox_cert domain.crt
$ docker secret create \
revprox_key domain.key
revproxy_cert
revproxy_key
Swarm Raft Store
(secrets)


atsea.mydomain.com
DNS Record
*.mydomain.com
atsea.mydomain:443
*.mydomain.com
(Load Balancer)
swarm-node-1:8443
swarm-node-2:8443
swarm-node-3:8443
80 8443
80 8443
80 8443
IPVS
IPVS
IPVS
Ingress network
front-tier network
back-tier network
appserver:8080
Interlock
Proxy
appserver
Service
database
Service
atsea_app
Container
atsea_db
Container
Swarm Node 1
Swarm Node 2
Swarm Node 3


Gitlab.com
DockerEEBook
Group for accessing master docker EE repos.
Source Code Control
atsea-web
atsea-db
atsea-payment
atsea-revers_proxy
atsea-deploy
Pipelines
atsea-web
atsea-db
atsea-payment
atsea-revers_proxy
atsea-deploy
mydomain.com
Build Machine
atsea-web
atsea-db
atsea-payment
atsea-revers_proxy
atsea-deploy
Gitlab Runner
Docker Swarm
Docker
Centos 7
DTR
UCP
atsea-web
atsea-db
atsea-payment
Worker /shared
Worker /Test
Worker /QA
Docker EE Cluster

DockerEEBook > **Projects**

**DockerEEBook** projects: New project

**DockerEEBook / atsea-web**
6.5 MB Members Edit Remove

**DockerEEBook / atsea-db**
533 KB Members Edit Remove

**DockerEEBook / atsea-deploy**
1.1 MB Members Edit Remove

**DockerEEBook / atsea-reverse_proxy**
265 KB Members Edit Remove

**DockerEEBook / atsea-payment**
297 KB Members Edit Remove

GitLab Projects Groups Activity Milestones Snippets

D DockerEEBook

Overview

Issues 0

Merge Requests 0

Kubernetes

Members

Settings

General

Projects

CI / CD

Webhooks

Billing

To start serving your jobs you can add Runners to your group

## Group Runners

GitLab Group Runners can execute code for all the projects in this group. They can be managed using the Runners API.

### Set up a group Runner manually

1. Install GitLab Runner
2. Specify the following URL during the Runner setup: `https://gitlab.com/`
3. Use the following registration token during setup:

Reset runners registration token

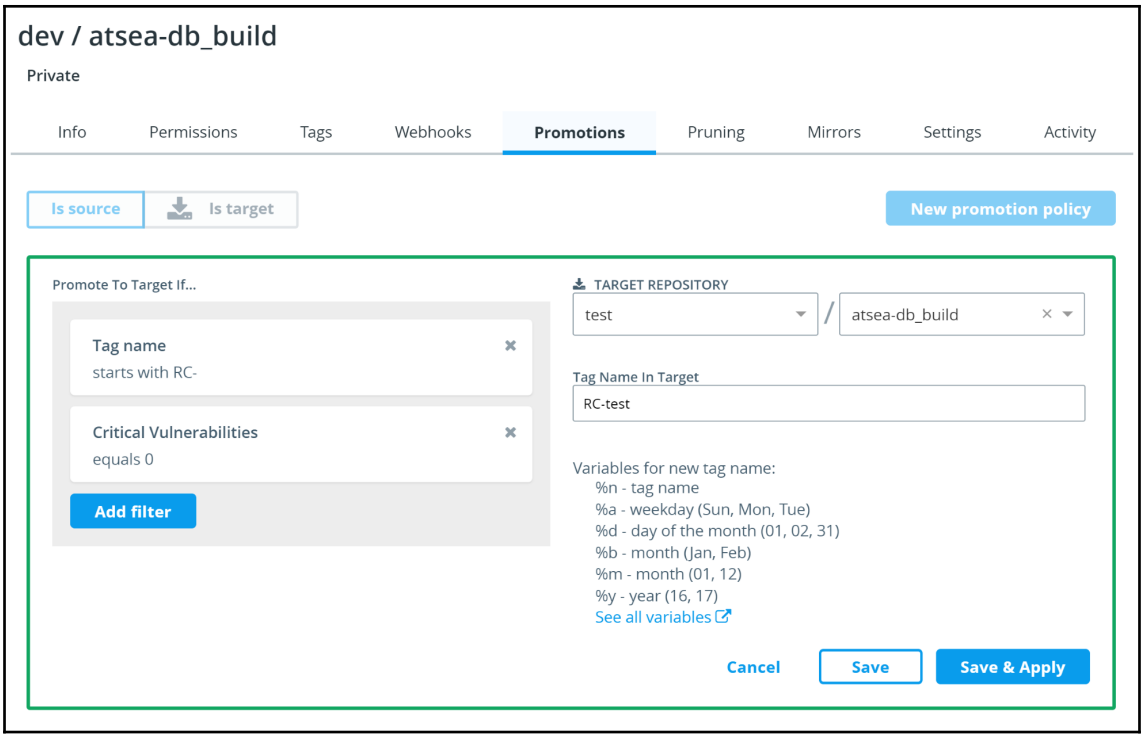
4. Start the Runner!

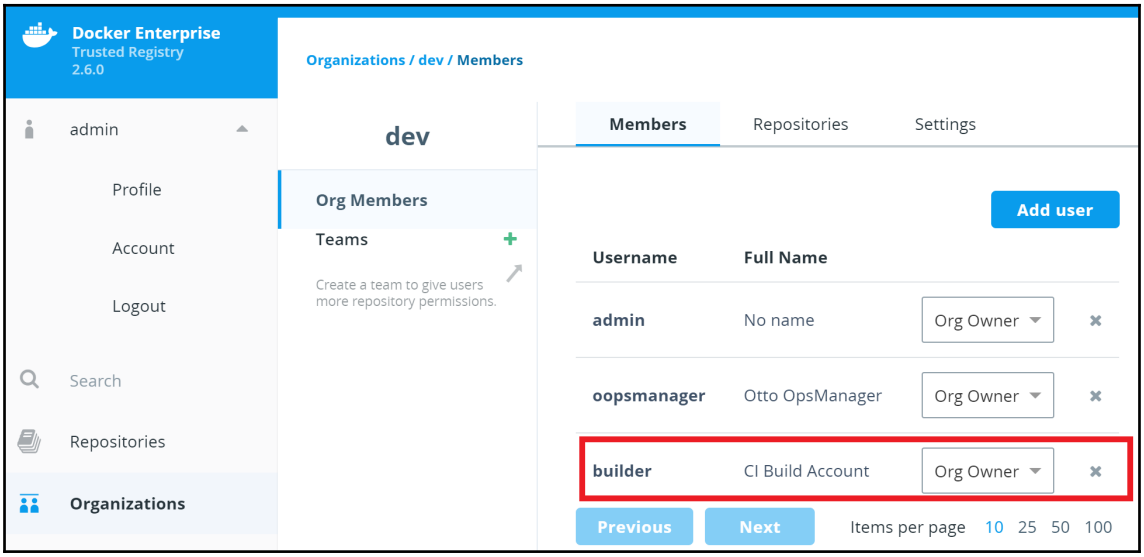
### Available group Runners : 1.

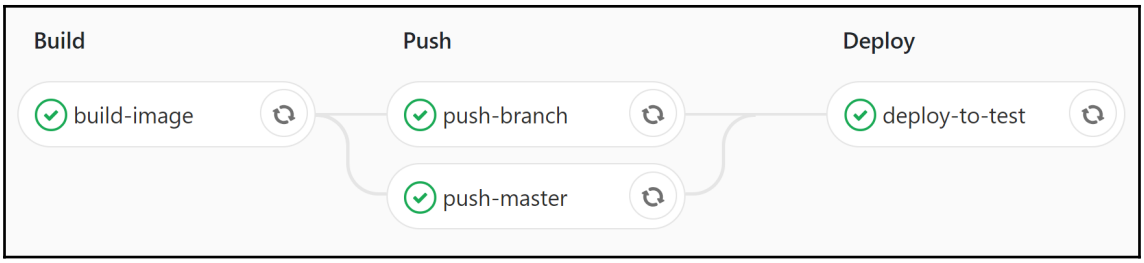
DUdA7V-y Pause Remove Runner

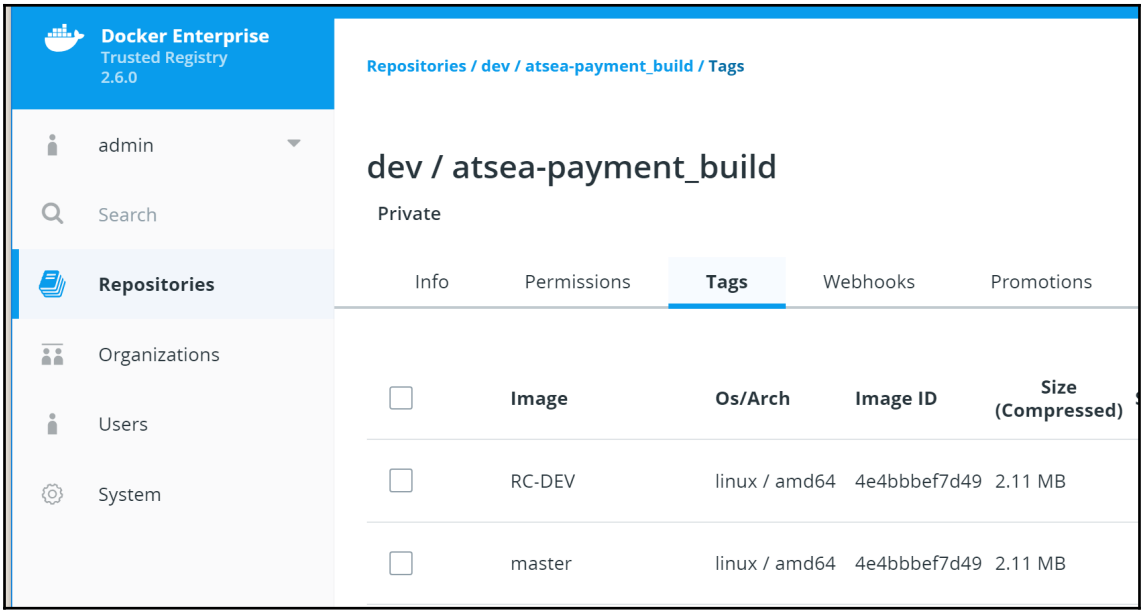
docker-iscsi-runner #670581

docker ntc


dev / atsea-db_build
Private
Info
Permissions
Tags
Webhooks
Promotions
Pruning
Mirrors
Settings
Activity
Is source
Is target
New promotion policy
Promote To Target If...
Tag name
starts with RC-
Critical Vulnerabilities
equals 0
Add filter
TARGET REPOSITORY
test
atsea-db_build
Tag Name In Target
RC-test
Variables for new tag name:
%n - tag name
%a - weekday (Sun, Mon, Tue)
%d - day of the month (01, 02, 31)
%b - month (Jan, Feb)
%m - month (01, 12)
%y - year (16, 17)
See all variables
Cancel
Save
Save & Apply


Docker Enterprise
Trusted Registry
2.6.0
admin
Profile
Account
Logout
Search
Repositories
Organizations
Organizations / dev / Members
dev
Org Members
Teams
Create a team to give users more repository permissions.
Members
Repositories
Settings
Add user
Username
Full Name
admin
No name
Org Owner
oopsmanager
Otto OpsManager
Org Owner
builder
CI Build Account
Org Owner
Previous
Next
Items per page
10
25
50
100


Build
Push
Deploy
build-image
push-branch
push-master
deploy-to-test


Docker Enterprise
Trusted Registry
2.6.0
admin
Search
Repositories
Organizations
Users
System
Repositories / dev / atsea-payment_build / Tags
dev / atsea-payment_build
Private
Info
Permissions
Tags
Webhooks
Promotions
Image
Os/Arch
Image ID
Size (Compressed)
RC-DEV
linux / amd64
4e4bbbef7d49
2.11 MB
master
linux / amd64
4e4bbbef7d49
2.11 MB

GitLab Projects Groups Activity Milestones Snippets

A atsea-db

Project
Repository
Issues 0
Merge Requests 0
CI / CD
Pipelines

DockerEEBook > atsea-db > Pipelines

All 14 Pending 0 Running 0 Finished 14 Branches Tags

| Status | Pipeline | Commit | Stages |
|---|---|---|---|
| passed | #46121337 by latest | master bd29e042 Clean up... | |
| passed | #46074572 by | master a771c3e8 Final cleanup | |

Docker Enterprise
Trusted Registry
2.6.2

admin
Search
Repositories
Organizations
Users
System
API

Repositories / test / atsea-db_build / Tags

test / atsea-db_build

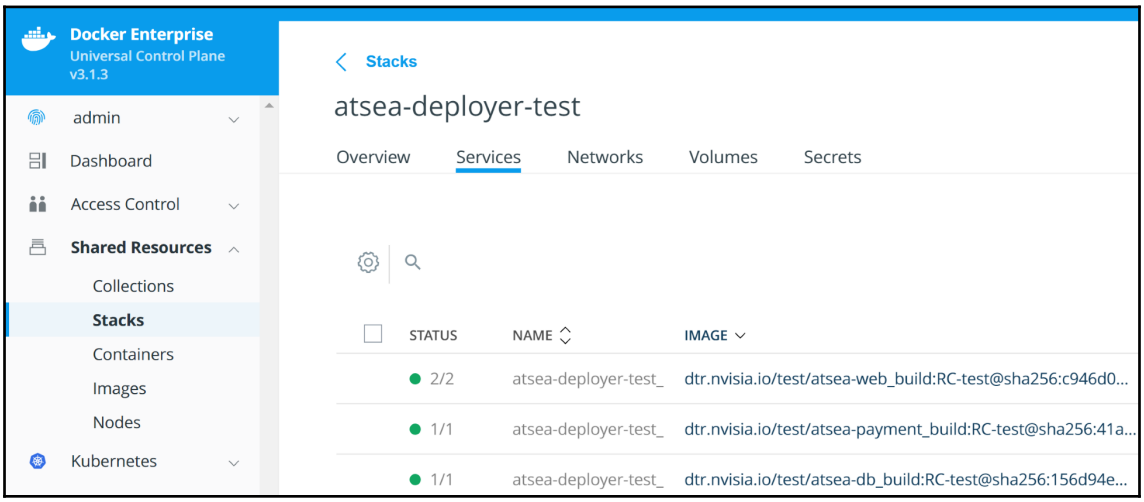
Private

Info Permissions Tags Webhooks Promotions Pruning Mirrors Settings Act

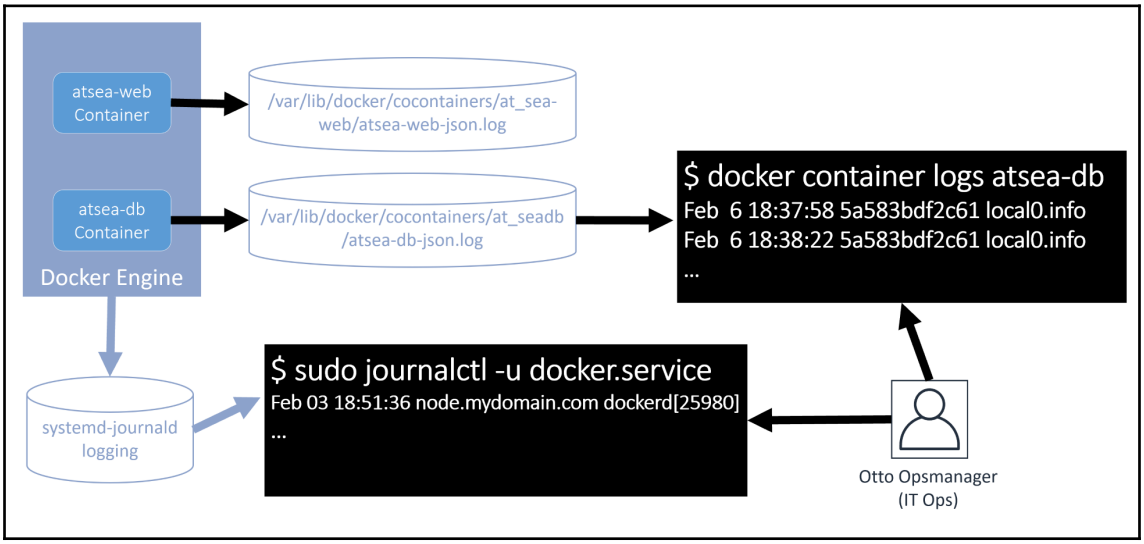
| Image | Os/Arch | Image ID | Size (Compressed) | Signed | Last Pushed | Vulnerabilities | |
|---|---|---|---|---|---|---|---|
| RC-test (Promoted) | linux / amd64 | 77edfb0f774a | 116.87 MB | | 21 minutes ago by builder | 6 Critical 24 Major 18 Minor | View details |
| kV1 | linux / amd64 | 77edfb0f774a | 116.87 MB | | 5 days ago by admin | Scan out of date. Rescan | View details |

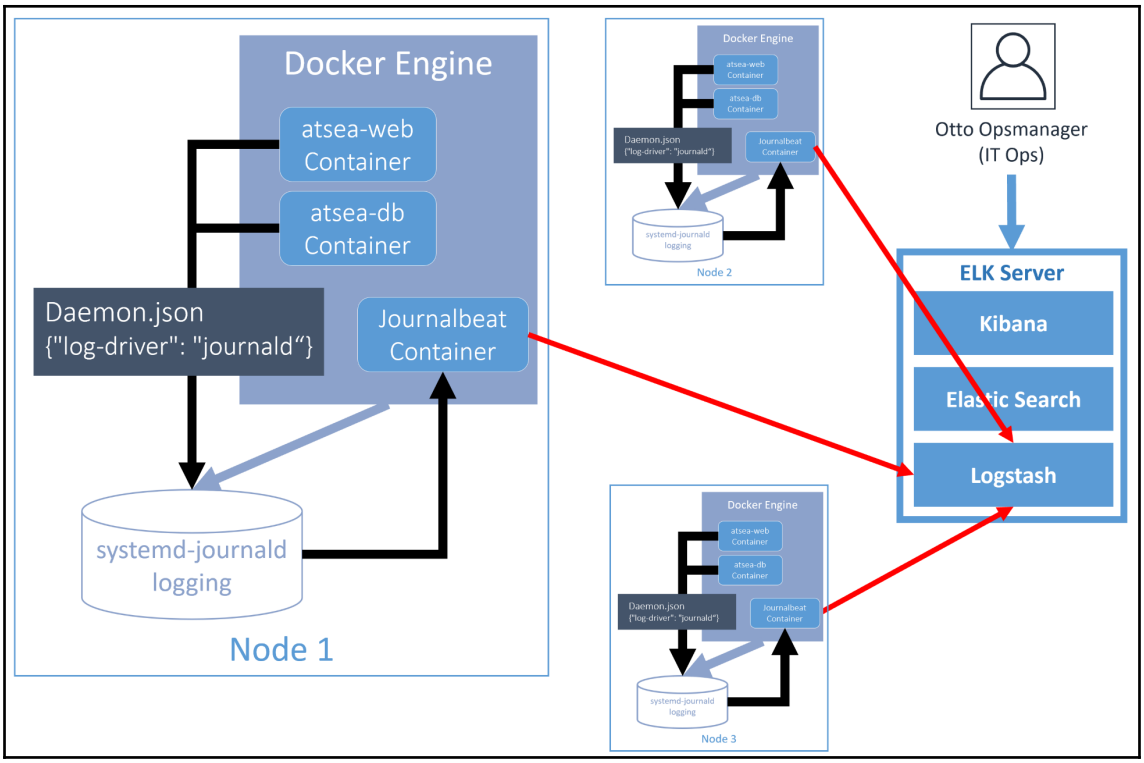
```
$ docker container run --network atsea-web-${CI_PIPELINE_ID}_front-tier --name l
driver:${CI_PIPELINE_ID}
Running after script...
$ docker stack rm atsea-web-${CI_PIPELINE_ID}
Removing service atsea-web-46142493_appserver
Removing service atsea-web-46142493_database
Removing service atsea-web-46142493_payment_gateway
Removing secret atsea-web-46142493_postgres_password
Removing secret atsea-web-46142493_payment_token
Removing network atsea-web-46142493_front-tier
Removing network atsea-web-46142493_payment
Removing network atsea-web-46142493_back-tier
$ docker container rm -f local-test-driver-container-${CI_PIPELINE_ID}
local-test-driver-container-46142493
$ docker image rm local-test-driver:${CI_PIPELINE_ID}
Untagged: local-test-driver:46142493
Deleted: sha256:5e461fa057d3cdb2314a3867f8239334b7b19c0ad1dffad2de01ba1f42dee23
Deleted: sha256:0a80c51bcaab25cd7f6c1488d486625415d2d25fc00f4fb0c6e7f32d83e1986
Deleted: sha256:75b67a25798e2382ecaa5b66e6adec06ea9ba1cdcda5292f7461e82ada7e224
Deleted: sha256:942acb39c5c1fbcd1f14e44e1f7934c3bc3c5953ede45235541078cb0fe6fc6
Deleted: sha256:23bc8b904a9fcb795183696a0783f402e6dc419816c69ac6f8717c3f6036f45
ERROR: Job failed: exit code 1
```

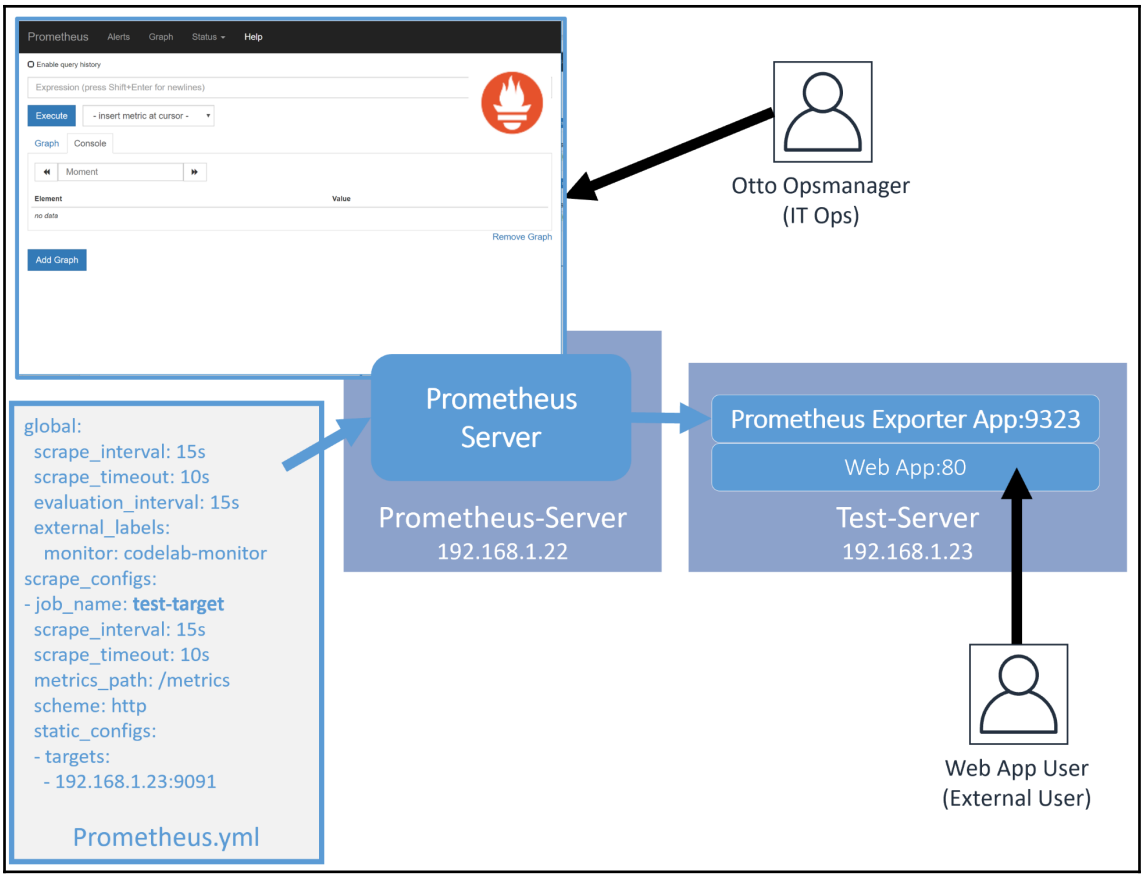
```
$ docker container run --network atsea-web-${CI_PIPELINE_ID}_front-tier -
driver:${CI_PIPELINE_ID}
Running after script...
$ docker stack rm atsea-web-${CI_PIPELINE_ID}
Removing service atsea-web-46142789_appserver
Removing service atsea-web-46142789_database
Removing service atsea-web-46142789_payment_gateway
Removing secret atsea-web-46142789_payment_token
Removing secret atsea-web-46142789_postgres_password
Removing network atsea-web-46142789_back-tier
Removing network atsea-web-46142789_payment
Removing network atsea-web-46142789_front-tier
$ docker container rm -f local-test-driver-container-${CI_PIPELINE_ID}
local-test-driver-container-46142789
$ docker image rm local-test-driver:${CI_PIPELINE_ID}
Untagged: local-test-driver:46142789
Job succeeded
```

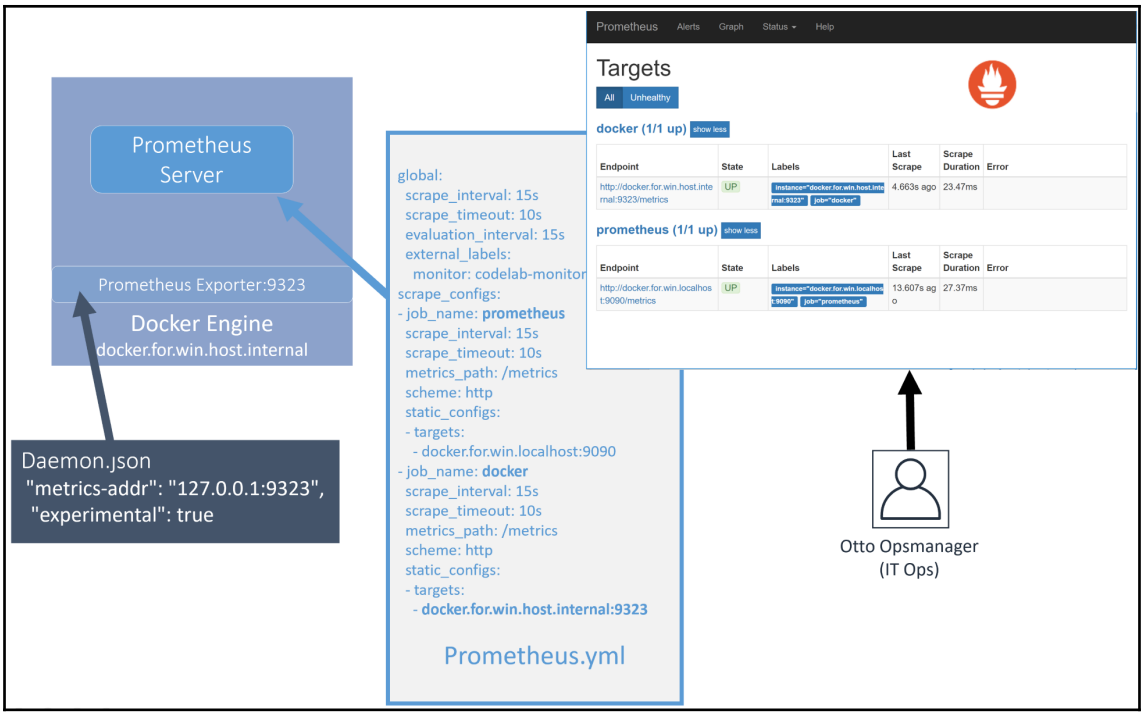


# Chapter 7: Pilot Docker Enterprise Platform Monitoring and Logging

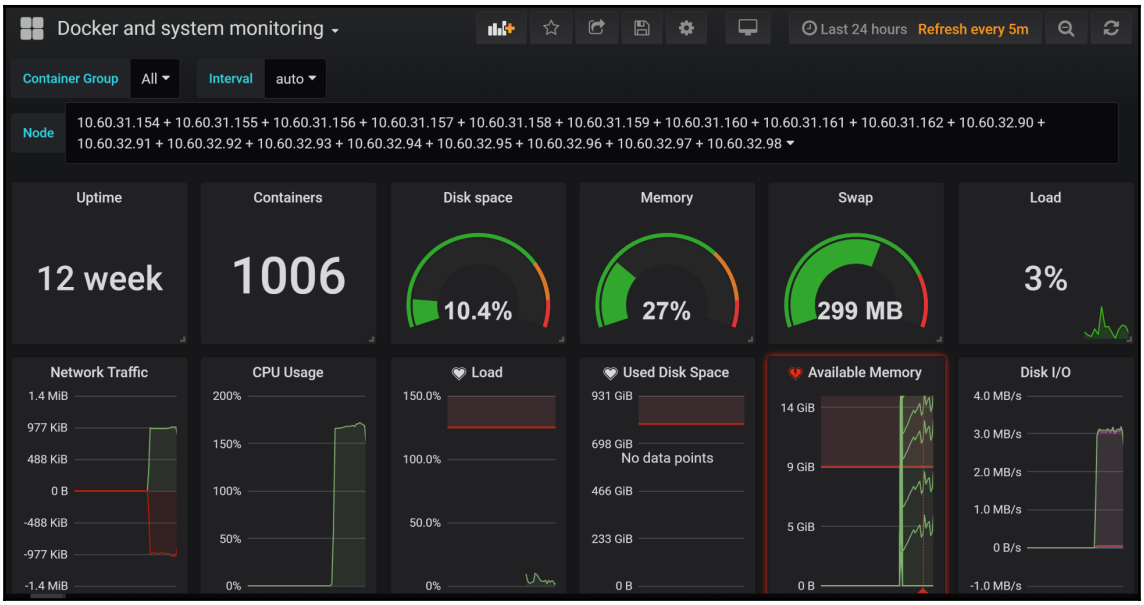


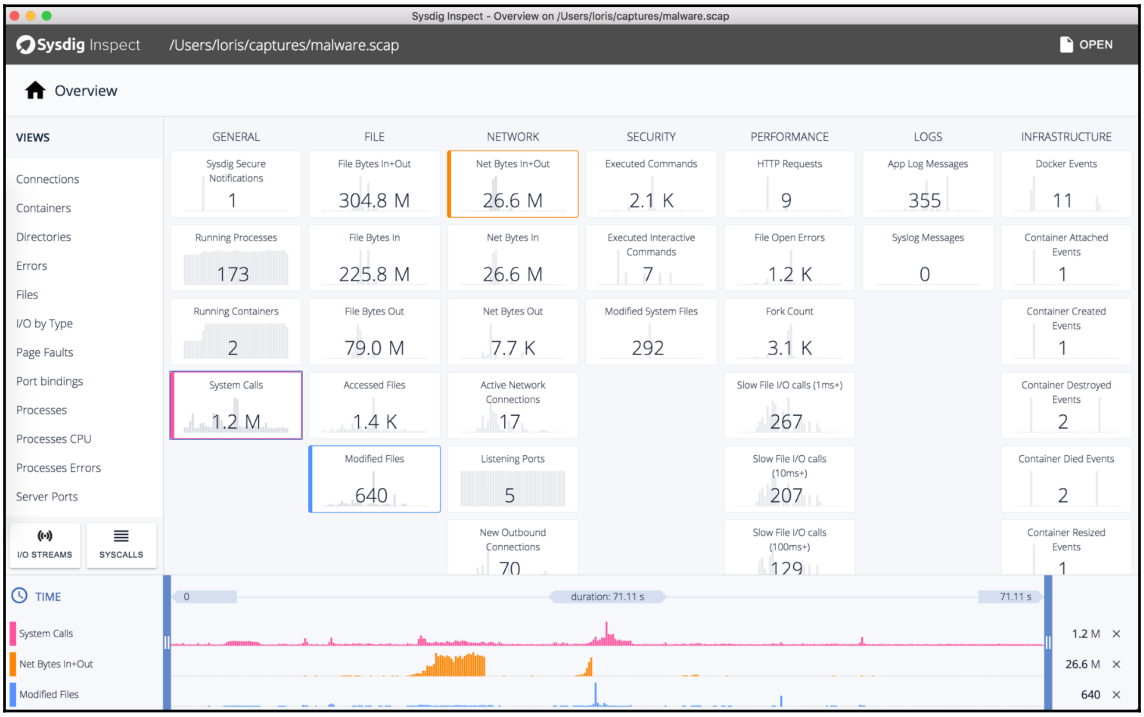

Docker Engine
atsea-web Container
atsea-db Container
Daemon.json
{"log-driver": "journald"}
Journalbeat Container
systemd-journald logging
Node 1
Docker Engine
atsea-web Container
atsea-db Container
Daemon.json
{"log-driver": "journald"}
Journalbeat Container
systemd-journald logging
Node 2
Otto Opsmanager
(IT Ops)
ELK Server
Kibana
Elastic Search
Logstash
Docker Engine
atsea-web Container
atsea-db Container
Daemon.json
{"log-driver": "journald"}
Journalbeat Container
systemd-journald logging
Node 3

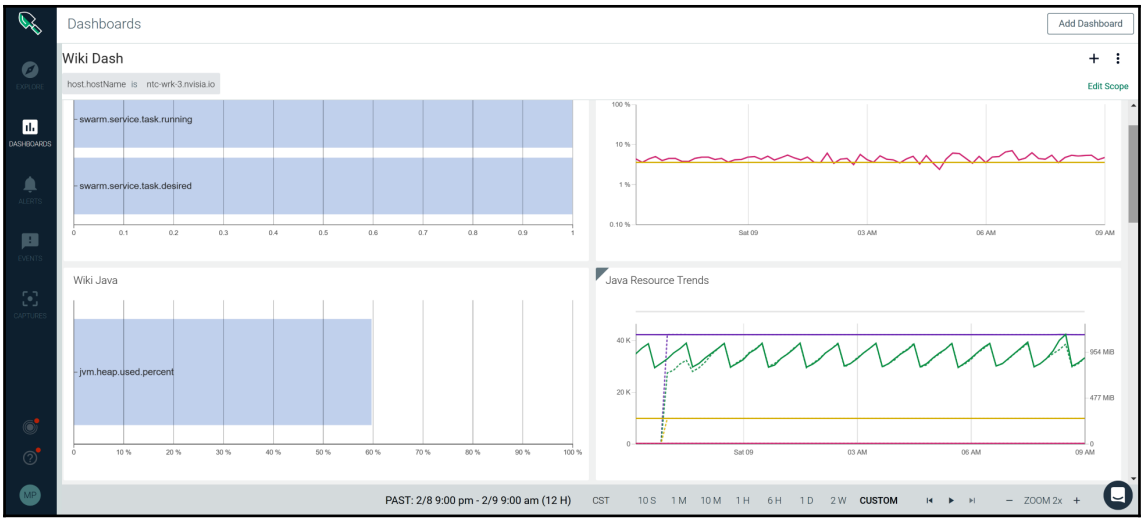

Prometheus
Alerts
Graph
Status
Help
Enable query history
Expression (press Shift+Enter for newlines)
Execute
- insert metric at cursor -
Graph
Console
Moment
Element
Value
no data
Remove Graph
Add Graph
Otto Opsmanager
(IT Ops)
global:
scrape_interval: 15s
scrape_timeout: 10s
evaluation_interval: 15s
external_labels:
monitor: codelab-monitor
scrape_configs:
- job_name: test-target
scrape_interval: 15s
scrape_timeout: 10s
metrics_path: /metrics
scheme: http
static_configs:
- targets:
- 192.168.1.23:9091
Prometheus.yml
Prometheus Server
Prometheus-Server
192.168.1.22
Prometheus Exporter App:9323
Web App:80
Test-Server
192.168.1.23
Web App User
(External User)

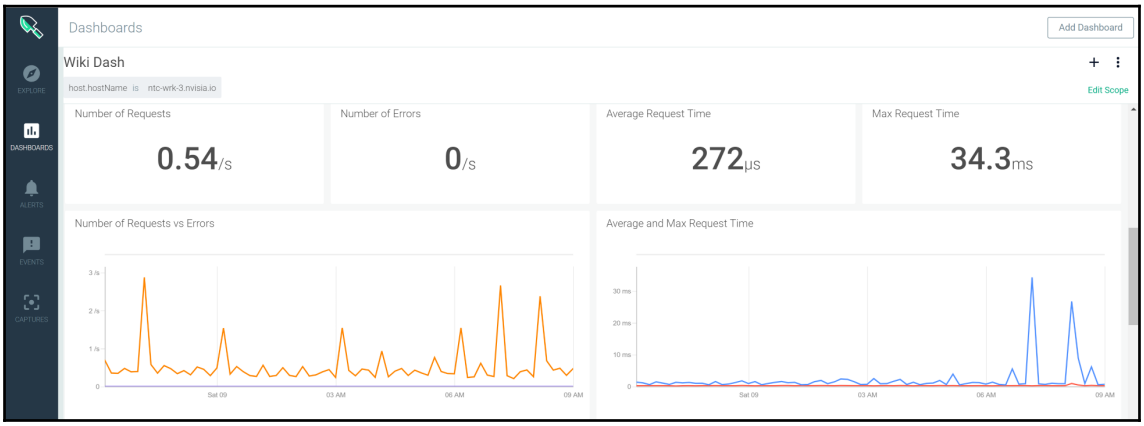

Prometheus Server
Prometheus Exporter:9323
Docker Engine
docker.for.win.host.internal
Daemon.json
"metrics-addr": "127.0.0.1:9323",
"experimental": true
global:
scrape_interval: 15s
scrape_timeout: 10s
evaluation_interval: 15s
external_labels:
monitor: codelab-monitor
scrape_configs:
- job_name: prometheus
scrape_interval: 15s
scrape_timeout: 10s
metrics_path: /metrics
scheme: http
static_configs:
- targets:
- docker.for.win.localhost:9090
- job_name: docker
scrape_interval: 15s
scrape_timeout: 10s
metrics_path: /metrics
scheme: http
static_configs:
- targets:
- docker.for.win.host.internal:9323
Prometheus.yml
Prometheus
Alerts
Graph
Status
Help
Targets
All
Unhealthy
docker (1/1 up)
show less
Endpoint
State
Labels
Last Scrape
Scrape Duration
Error
http://docker.for.win.host.internal:9323/metrics
UP
instance="docker.for.win.host.internal:9323"
job="docker"
4.663s ago
23.47ms
prometheus (1/1 up)
show less
Endpoint
State
Labels
Last Scrape
Scrape Duration
Error
http://docker.for.win.localhost:9090/metrics
UP
instance="docker.for.win.localhost:9090"
job="prometheus"
13.607s ago
27.37ms
Otto Opsmanager
(IT Ops)


Docker Enterprise
Universal Control Plane
v3.1.3
admin
Dashboard
Access Control
Shared Resources
Kubernetes
Swarm
Docs
Kubernetes API Docs
Live API
MANAGER NODES
Ready 3
Errors 0
Warnings 0
Pending 0
WORKER NODES
Ready 6
Errors 0
Warnings 0
Pending 0
SWARM
Services
Active 2
Errors 0
Updating 0
LAST 6 HOURS
3 MANAGER NODES
Max CPU 16.19% Max Memory 18.17% Max Used Disk 7.47%
15%
10%
5%
07:00 AM
08:00 AM
09:00 AM
10:00 AM
11:00 AM
12:00 PM
KUBERNETES
All Namespaces
Pods
Running 0
Errors 0
Pending 0
Controllers
None
6 WORKER NODES
Max CPU 7.59% Max Memory 59.72% Max Used Disk 10.61%
40%
20%
07:00 AM
08:00 AM
09:00 AM
10:00 AM
11:00 AM
12:00 PM


Docker and system monitoring
Last 24 hours
Refresh every 5m
Container Group
All
Interval
auto
Node
10.60.31.154 + 10.60.31.155 + 10.60.31.156 + 10.60.31.157 + 10.60.31.158 + 10.60.31.159 + 10.60.31.160 + 10.60.31.161 + 10.60.31.162 + 10.60.32.90 + 10.60.32.91 + 10.60.32.92 + 10.60.32.93 + 10.60.32.94 + 10.60.32.95 + 10.60.32.96 + 10.60.32.97 + 10.60.32.98
Uptime
12 week
Containers
1006
Disk space
10.4%
Memory
27%
Swap
299 MB
Load
3%
Network Traffic
1.4 MiB
977 KiB
488 KiB
0 B
-488 KiB
-977 KiB
-1.4 MiB
CPU Usage
200%
150%
100%
50%
0%
Load
150.0%
100.0%
50.0%
0%
Used Disk Space
931 GiB
698 GiB
No data points
466 GiB
233 GiB
0 B
Available Memory
14 GiB
9 GiB
5 GiB
0 B
Disk I/O
4.0 MB/s
3.0 MB/s
2.0 MB/s
1.0 MB/s
0 B/s
-1.0 MB/s


Sysdig Inspect - Overview on /Users/loris/captures/malware.scap
Sysdig Inspect
/Users/loris/captures/malware.scap
OPEN
Overview
VIEWS
Connections
Containers
Directories
Errors
Files
I/O by Type
Page Faults
Port bindings
Processes
Processes CPU
Processes Errors
Server Ports
I/O STREAMS
SYSCALLS
GENERAL
FILE
NETWORK
SECURITY
PERFORMANCE
LOGS
INFRASTRUCTURE
Sysdig Secure Notifications
1
File Bytes In+Out
304.8 M
Net Bytes In+Out
26.6 M
Executed Commands
2.1 K
HTTP Requests
9
App Log Messages
355
Docker Events
11
Running Processes
173
File Bytes In
225.8 M
Net Bytes In
26.6 M
Executed Interactive Commands
7
File Open Errors
1.2 K
Syslog Messages
0
Container Attached Events
1
Running Containers
2
File Bytes Out
79.0 M
Net Bytes Out
7.7 K
Modified System Files
292
Fork Count
3.1 K
Container Created Events
1
System Calls
1.2 M
Accessed Files
1.4 K
Active Network Connections
17
Slow File I/O calls (1ms+)
267
Container Destroyed Events
2
Modified Files
640
Listening Ports
5
Slow File I/O calls (10ms+)
207
Container Died Events
2
New Outbound Connections
70
Slow File I/O calls (100ms+)
129
Container Resized Events
1
TIME
0
duration: 71.11 s
71.11 s
System Calls
Net Bytes In+Out
Modified Files
1.2 M
26.6 M
640


Dashboards
Add Dashboard
Wiki Dash
host.hostName is ntc-wrk-3.nvisia.io
Edit Scope
swarm.service.task.running
swarm.service.task.desired
Wiki Java
jvm.heap.used.percent
Java Resource Trends
PAST: 2/8 9:00 pm - 2/9 9:00 am (12 H)
CST
10 S
1 M
10 M
1 H
6 H
1 D
2 W
CUSTOM
ZOOM 2x


Dashboards
Add Dashboard
Wiki Dash
host.hostName is ntc-wrk-3.nvisia.io
Edit Scope
Number of Requests
0.54/s
Number of Errors
0/s
Average Request Time
272µs
Max Request Time
34.3ms
Number of Requests vs Errors
Average and Max Request Time

# Wiki Service is Down

One or more Swarm services are down

High

## 1 Define

### a Select entity to monitor

Alert if any swarm.service.name ×

Select a label... is down.

### b Scope

swarm.service.label.stack.na... is nvisia-wiki

Select a label...

### c Trigger

If entity is down for the last 1 minute for 100 % of the time

# Prod Worker Is Down

Insert alert description

High

## 1 Define

### a Select entity to monitor

Alert if any host.hostName ×

Select a label... is down.

### b Scope

swarm.node.label.com.nvisia.... is prod

Select a label...

### c Trigger

If entity is down for the last 2 minute for 100 % of the time

## 3 Act

Activate Sysdig Capture

| | | |
|---|---|---|
| **Storage** | Sysdig Monitor Storage | (Go to Sysdig Storage to review setting) |
| **File Name** | alert-capture.scap | |
| **Time frame** | 15 | seconds |
| **Filter** | Sysdig Capture Filter | |

# [Swarm] Task with No Containers Running

No running containers available for one or more Swarm services

Medium

## 1 Define

### a Metric

Average of swarm.service.task.running

### b Scope

everywhere

### c Trigger

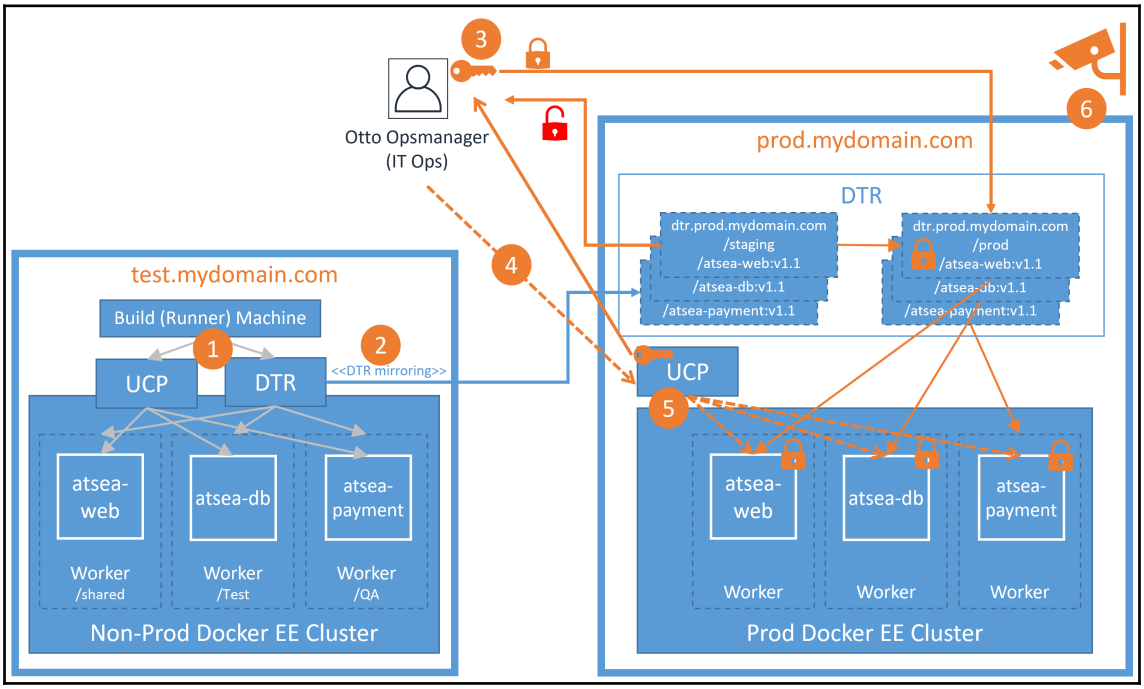
If metric < 0.8 for the last 3 minute on average

Multiple Alerts

Trigger a separate alert for each **segment**: swarm.service.name

Select a label...

# Chapter 8: First Application in Production with Docker Enterprise



Docker Enterprise
Trusted Registry
2.6.0

admin
Search
Repositories
Organizations
Users
System

Repositories / qa / atsea-web_stage / Mirrors / New

## qa / atsea-web_stage

Private

### Mirror direction

**Push to remote registry**
Images will push from this registry to the remote registry

**Pull from remote registry**
Images will pull from the remote registry to this registry

### Connect to a remote repository

Registry type
Docker Trusted Registry

Registry URL
https:// http://
dtr.prod.mydomain.com

Username
prod-stager

Password or access token
••••••••••••

Repository
staging / atsea-web

### Triggers

Copy image to remote repository if it has...

**Tag name**
starts with v

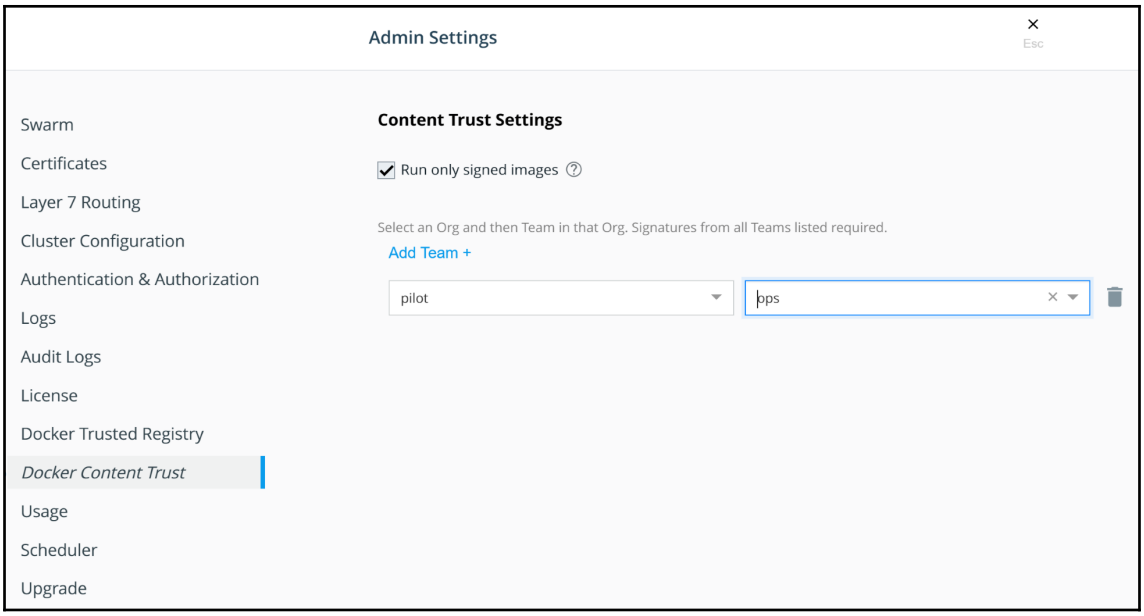
Add criteria:

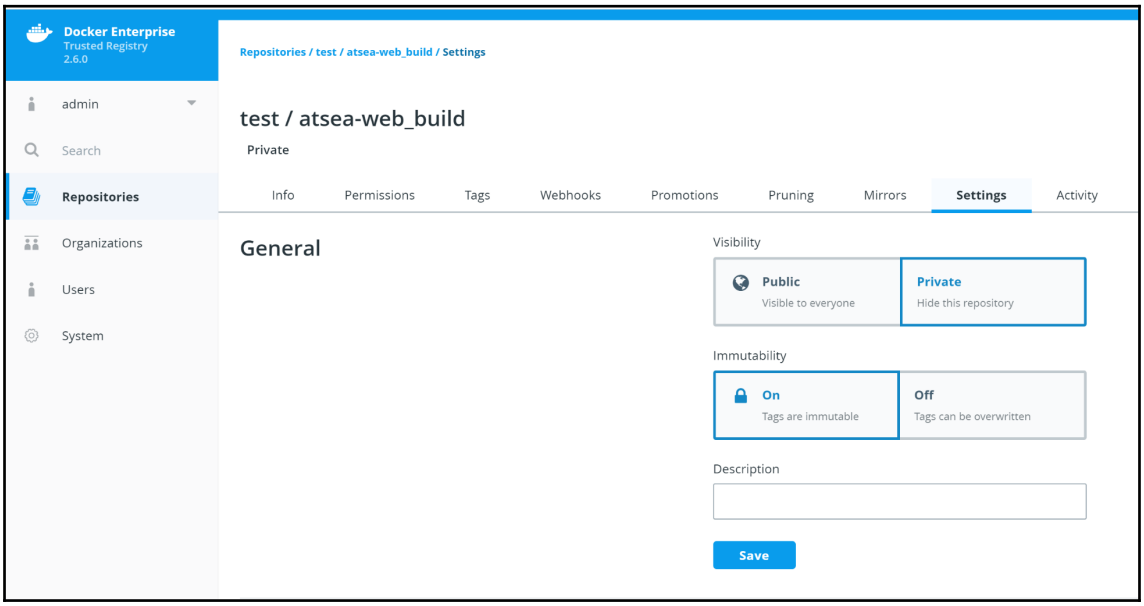
- Tag name
- Component name
- All vulnerabilities
- Critical vulnerabilities
- Major vulnerabilities
- Minor vulnerabilities
- License name
- Last updated at

### Mirrored image's tag

%n

Variables for tag name: %n = tag name | %d = day of the month (01, 02, 31) | %m = month (01, 02) | See all variables
%a = weekday (Sun, Mon, Tue) | %b = month (Jan, Feb) | %y = year (16, 17)


Admin Settings
Esc
Swarm
Certificates
Layer 7 Routing
Cluster Configuration
Authentication & Authorization
Logs
Audit Logs
License
Docker Trusted Registry
Docker Content Trust
Usage
Scheduler
Upgrade
Content Trust Settings
Run only signed images
Select an Org and then Team in that Org. Signatures from all Teams listed required.
Add Team +
pilot
ops


Docker Enterprise
Trusted Registry
2.6.0
admin
Search
Repositories
Organizations
Users
System
Repositories / test / atsea-web_build / Settings
test / atsea-web_build
Private
Info
Permissions
Tags
Webhooks
Promotions
Pruning
Mirrors
Settings
Activity
General
Visibility
Public
Visible to everyone
Private
Hide this repository
Immutability
On
Tags are immutable
Off
Tags can be overwritten
Description
Save

Docker Enterprise
Trusted Registry
2.6.0

admin
Search
Repositories
Organizations
Users
System
API
Docs

Repositories / test / atsea-payment_build / RC-test / Components

test / atsea-payment_build : RC-test

Private

linux / amd64 | 0367cd2eeab4 | 2.63 MB | Pushed 14 days ago by builder | 2 major | All layers already scanned | Delete | Promote | Scan

Layers | Components

busybox
1.29.3-r10
1 Major

busybox
1.29.3-r12
1 Major

apk-tools
2.10.3-r1
Clean

openssl
1.1.1a-r1
Clean

busybox
Version: 1.29.3-r10
License: GPL

| Vulnerabilities | Severity | Description | |
|---|---|---|---|
| CVE-2018-20679 | 5 | An issue was discovered in BusyBox before 1.30.0. An out of bounds read in udhcp components (consumed by the DHCP server, client, and relay) allows a remote attacker to leak sensitive information from the stack by sending a crafted DHCP message. This is related to verification in udhcp_get_option() in networking/udhcp/common.c that 4-byte options are indeed 4 bytes. | Show layers affected |

Docker Enterprise
Universal Control Plane
v3.1.3

admin
My Profile
Admin Settings
Support Dump
About
Sign Out
Dashboard
Access Control
Shared Resources
Collections
Stacks
Containers
Images
Nodes
Kubernetes
Swarm
Docs

Stacks

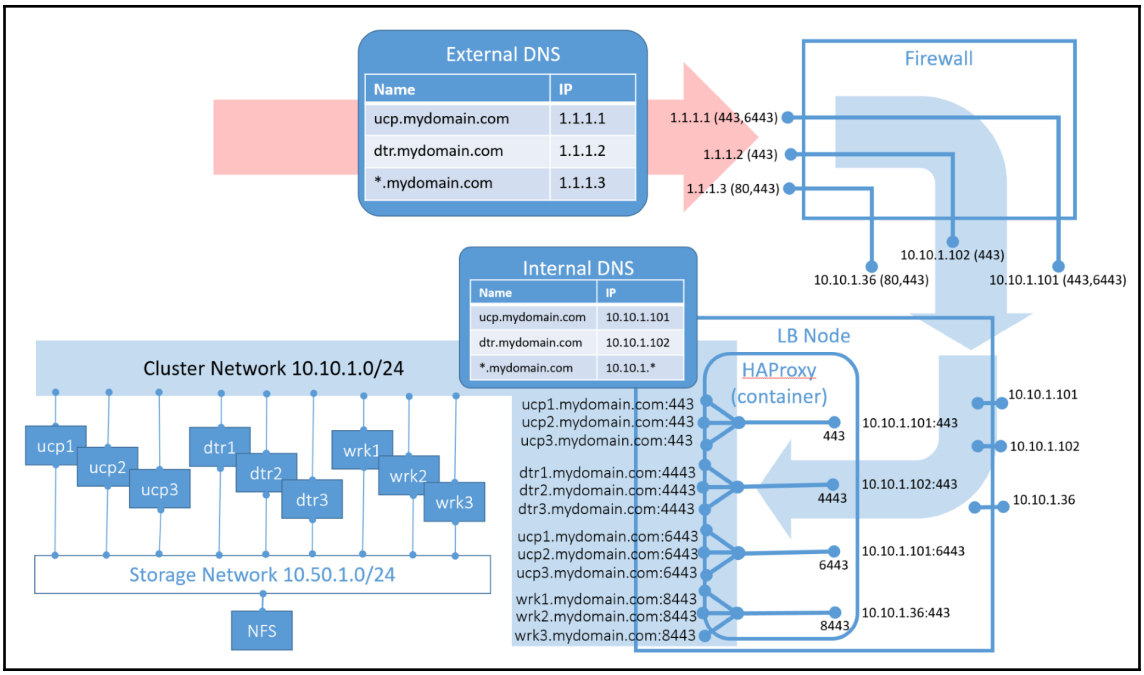
atsea-deployer-test

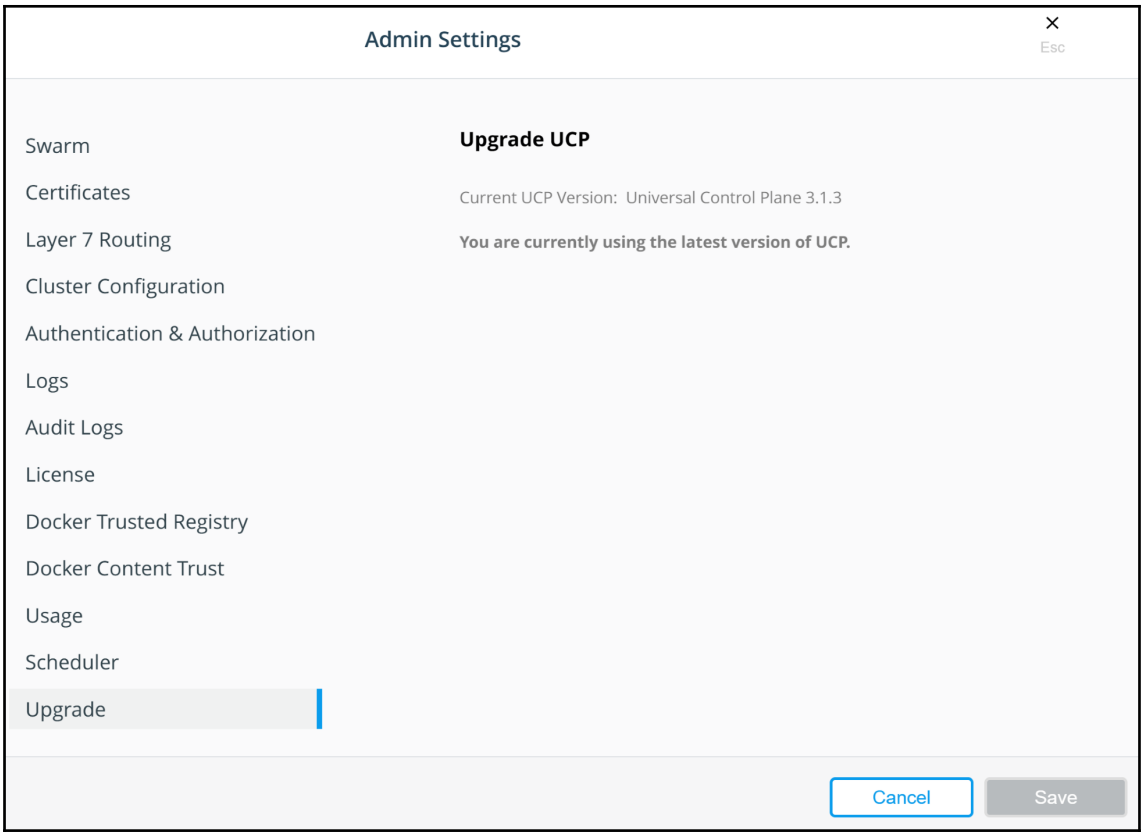
Overview | Services | Networks | Volumes | Secrets

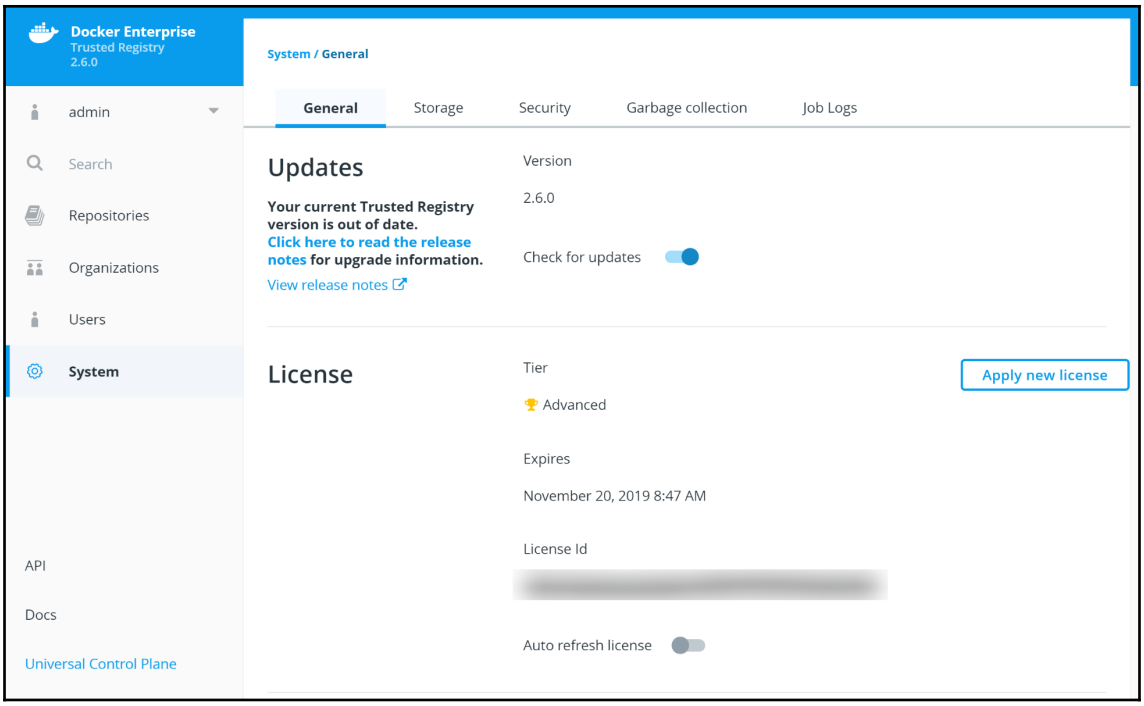
Actions

| STATUS | NAME | IMAGE | VULNERABILITIES | | | MODE | UPDATED AT | LAST E |
|---|---|---|---|---|---|---|---|---|
| 2/2 | atsea-depl | dtr.nvisia.io/test/atsea-web_build... | 29 Critical | 51 Major | 1 Minor | Replicated | 29 minutes ... | |
| 1/1 | atsea-depl | dtr.nvisia.io/test/atsea-db_build:R... | 5 Critical | 20 Major | 4 Minor | Replicated | 29 minutes ... | |
| 1/1 | atsea-depl | dtr.nvisia.io/test/atsea-payment_... | 0 Critical | 2 Major | 0 Minor | Replicated | 29 minutes ... | |

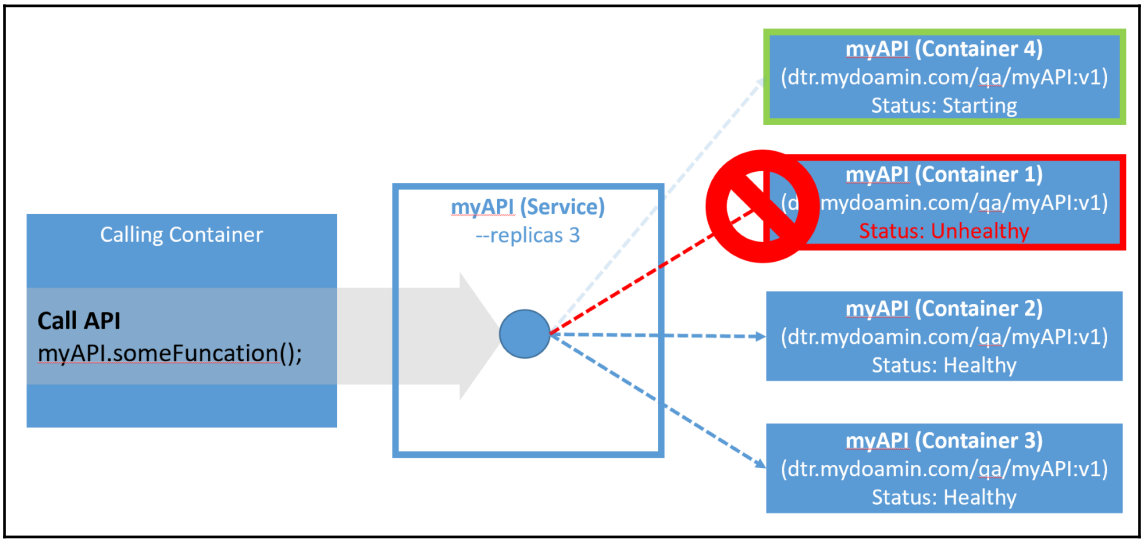

Avg. CPU %
13.5%
Avg. Memory Usage %
9.73%
Avg. Network Bytes
556KiB/s
Avg. Network Conne...
34.6/s
Avg. Disk Usage
3.70%
Avg. File Bytes
1.86MiB/s
CPU %
100 %
50 %
0
Sat 09
12 PM
Feb 10
12 PM
Memory Usage %
100 %
50 %
0
Sat 09
12 PM
Feb 10
12 PM
Network Bytes Total
488 KiB/s
0
Sat 09
12 PM
Feb 10
12 PM
Number of Network Connections
40 /s
20 /s
0
Sat 09
12 PM
Feb 10
12 PM
Disk Usage
100 %
50 %
0
Sat 09
12 PM
Feb 10
12 PM
File Bytes Total
1.91 MiB/s
0
Sat 09
12 PM
Feb 10
12 PM


External DNS
Name
IP
ucp.mydomain.com
1.1.1.1
dtr.mydomain.com
1.1.1.2
*.mydomain.com
1.1.1.3
Firewall
1.1.1.1 (443,6443)
1.1.1.2 (443)
1.1.1.3 (80,443)
10.10.1.102 (443)
10.10.1.36 (80,443)
10.10.1.101 (443,6443)
Internal DNS
Name
IP
ucp.mydomain.com
10.10.1.101
dtr.mydomain.com
10.10.1.102
*.mydomain.com
10.10.1.*
LB Node
HAProxy
(container)
Cluster Network 10.10.1.0/24
ucp1
ucp2
ucp3
dtr1
dtr2
dtr3
wrk1
wrk2
wrk3
Storage Network 10.50.1.0/24
NFS
ucp1.mydomain.com:443
ucp2.mydomain.com:443
ucp3.mydomain.com:443
443
10.10.1.101:443
dtr1.mydomain.com:4443
dtr2.mydomain.com:4443
dtr3.mydomain.com:4443
4443
10.10.1.102:443
ucp1.mydomain.com:6443
ucp2.mydomain.com:6443
ucp3.mydomain.com:6443
6443
10.10.1.101:6443
wrk1.mydomain.com:8443
wrk2.mydomain.com:8443
wrk3.mydomain.com:8443
8443
10.10.1.36:443
10.10.1.101
10.10.1.102
10.10.1.36


Admin Settings
Esc
Swarm
Certificates
Layer 7 Routing
Cluster Configuration
Authentication & Authorization
Logs
Audit Logs
License
Docker Trusted Registry
Docker Content Trust
Usage
Scheduler
Upgrade
Upgrade UCP
Current UCP Version: Universal Control Plane 3.1.3
You are currently using the latest version of UCP.
Cancel
Save


Docker Enterprise
Trusted Registry
2.6.0
admin
Search
Repositories
Organizations
Users
System
API
Docs
Universal Control Plane
System / General
General
Storage
Security
Garbage collection
Job Logs
Updates
Your current Trusted Registry version is out of date.
Click here to read the release notes for upgrade information.
View release notes
Version
2.6.0
Check for updates
License
Tier
Advanced
Apply new license
Expires
November 20, 2019 8:47 AM
License Id
Auto refresh license

# Chapter 9: Important Docker Enterprise Production Topics



Docker Enterprise
Universal Control Plane
v3.1.3

Stacks
Containers
Images
Nodes
Kubernetes
Create
Namespaces
All Namespaces
Service Accounts
Controllers
Load Balancers
Pods
Configurations
Storage
Swarm
Services
Volumes
Networks
Secrets
Docs
Kubernetes API Docs

Services

atsea-deployer-test_appserver

2 / 2 Last Updated an hour ago / Last Error: --

Overview Metrics

Vulnerabilities: image was not in DTR scanning data response

UPDATE CONFIGURATION

Failure action
rollback

Max failure ratio
0

Parallelism
1

Order
stop-first

LIMITS

CPUs
1

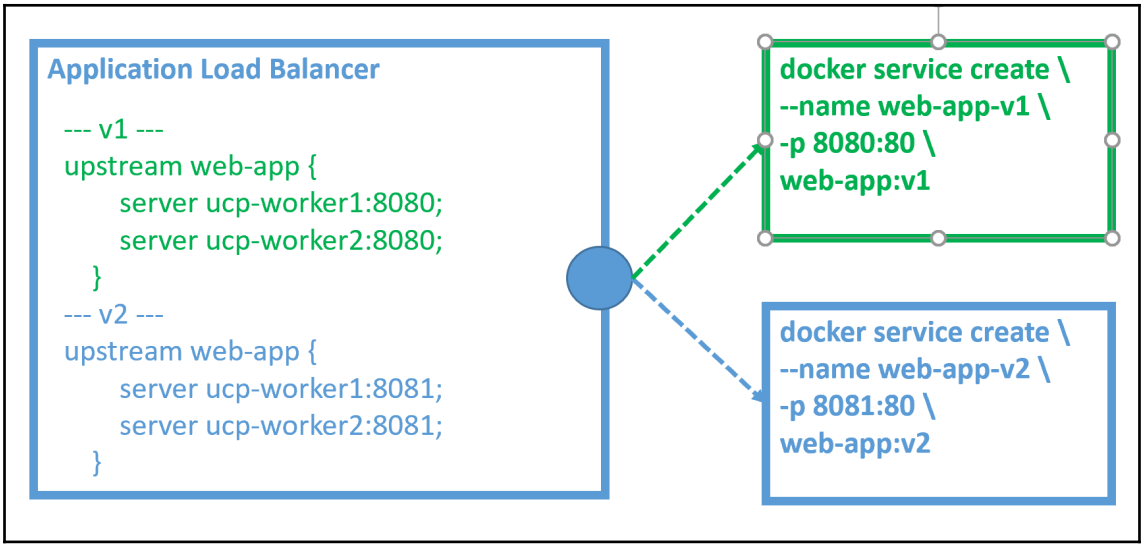
Memory
1.5 GB

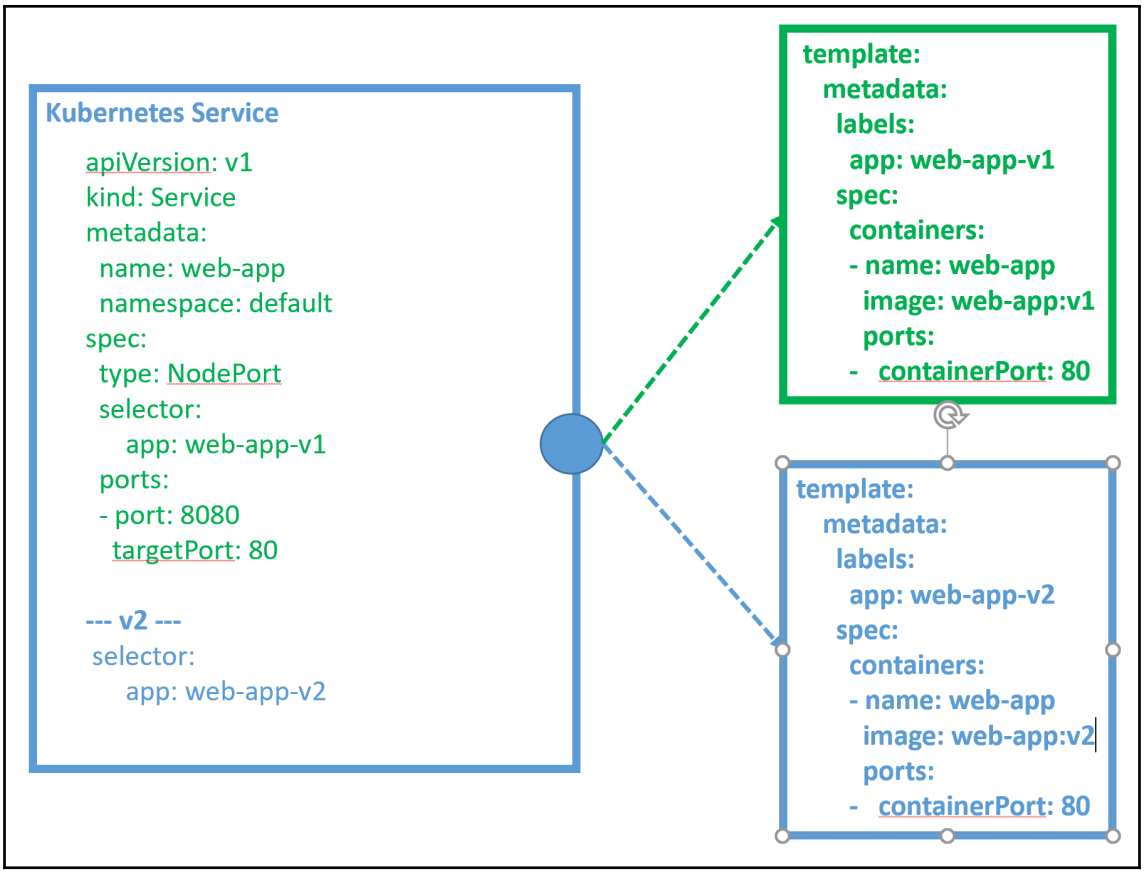
RESERVATIONS

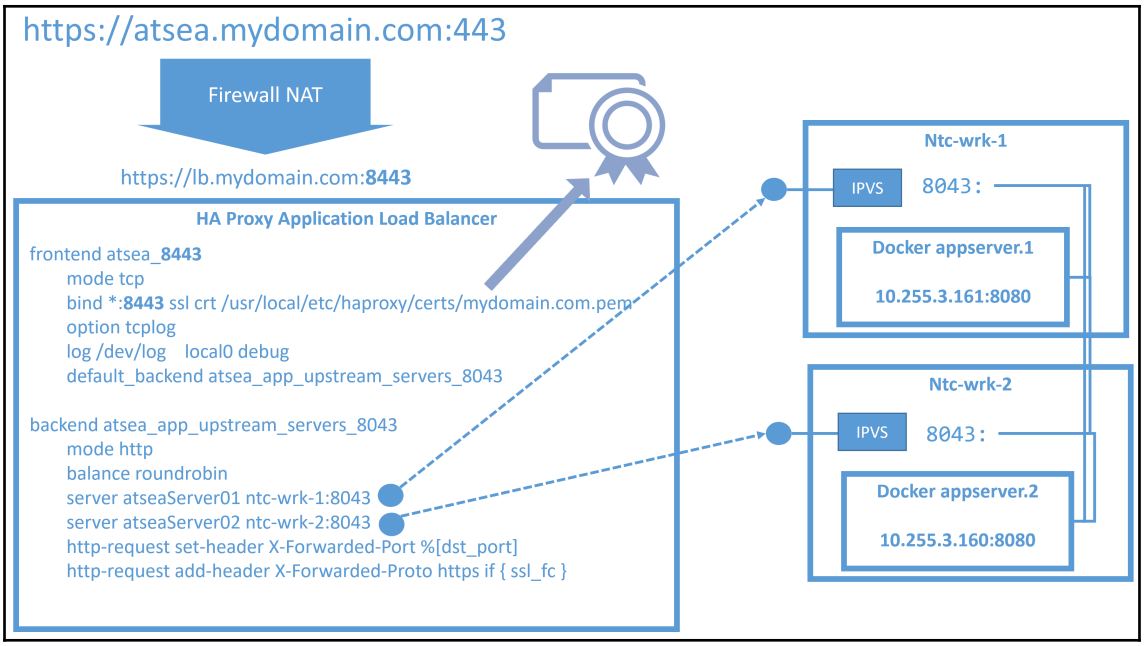
CPUs
1

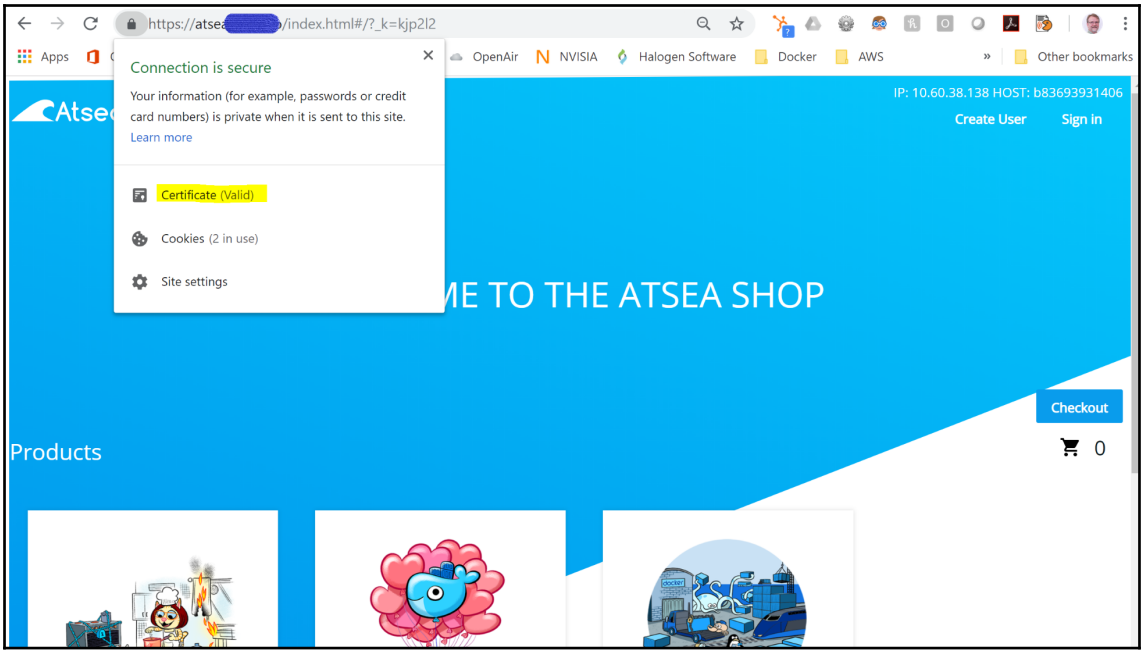
Memory
1.5 GB


JVM
Scope: host.hostName = 'ntc-wrk-2.nvisia.io'
Heap Usage Over Time
954 MiB
477 MiB
0
07 PM
08 PM
09 PM
10 PM
11 PM
Tue 19
Heap Usage by Process
- /app/AtSea-0.0.1-SNAPSHOT.jar
0
50 MiB
100 MiB
150 MiB
200 MiB
250 MiB
Garbage Collector: Collection Time
100 %
50 %
0
Garbage Collector: Collection Count
Thread Count
LIVE: 2/18 6:40 pm - 2/19 12:40 am (6 H)
CST
10 S
1 M
10 M
1 H
6 H
1 D
2 W
CUSTOM
ZOOM 2x


Application Load Balancer
--- v1 ---
upstream web-app {
server ucp-worker1:8080;
server ucp-worker2:8080;
}
--- v2 ---
upstream web-app {
server ucp-worker1:8081;
server ucp-worker2:8081;
}
docker service create \
--name web-app-v1 \
-p 8080:80 \
web-app:v1
docker service create \
--name web-app-v2 \
-p 8081:80 \
web-app:v2


Kubernetes Service
apiVersion: v1
kind: Service
metadata:
name: web-app
namespace: default
spec:
type: NodePort
selector:
app: web-app-v1
ports:
- port: 8080
targetPort: 80
--- v2 ---
selector:
app: web-app-v2
template:
metadata:
labels:
app: web-app-v1
spec:
containers:
- name: web-app
image: web-app:v1
ports:
- containerPort: 80
template:
metadata:
labels:
app: web-app-v2
spec:
containers:
- name: web-app
image: web-app:v2
ports:
- containerPort: 80


https://atsea.mydomain.com:443
Firewall NAT
https://lb.mydomain.com:8443
HA Proxy Application Load Balancer
frontend atsea_8443
mode tcp
bind *:8443 ssl crt /usr/local/etc/haproxy/certs/mydomain.com.pem
option tcplog
log /dev/log local0 debug
default_backend atsea_app_upstream_servers_8043
backend atsea_app_upstream_servers_8043
mode http
balance roundrobin
server atseaServer01 ntc-wrk-1:8043
server atseaServer02 ntc-wrk-2:8043
http-request set-header X-Forwarded-Port %[dst_port]
http-request add-header X-Forwarded-Proto https if { ssl_fc }
Ntc-wrk-1
IPVS
8043:
Docker appserver.1
10.255.3.161:8080
Ntc-wrk-2
IPVS
8043:
Docker appserver.2
10.255.3.160:8080


Connection is secure
Your information (for example, passwords or credit card numbers) is private when it is sent to this site.
Learn more
Certificate (Valid)
Cookies (2 in use)
Site settings
IP: 10.60.38.138 HOST: b83693931406
Create User
Sign in
ME TO THE ATSEA SHOP
Checkout
0
Products

Server Hostname

atsea.[redacted] Check SSL

atsea[redacted] resolves to 38.140.113.29

Server Type: Apache/2.2.15 (CentOS)

The certificate should be trusted by all major web browsers (all the correct intermediate certificates are installed).

The certificate was issued by DigiCert. Write review of DigiCert

The certificate will expire in 273 days. Remind me

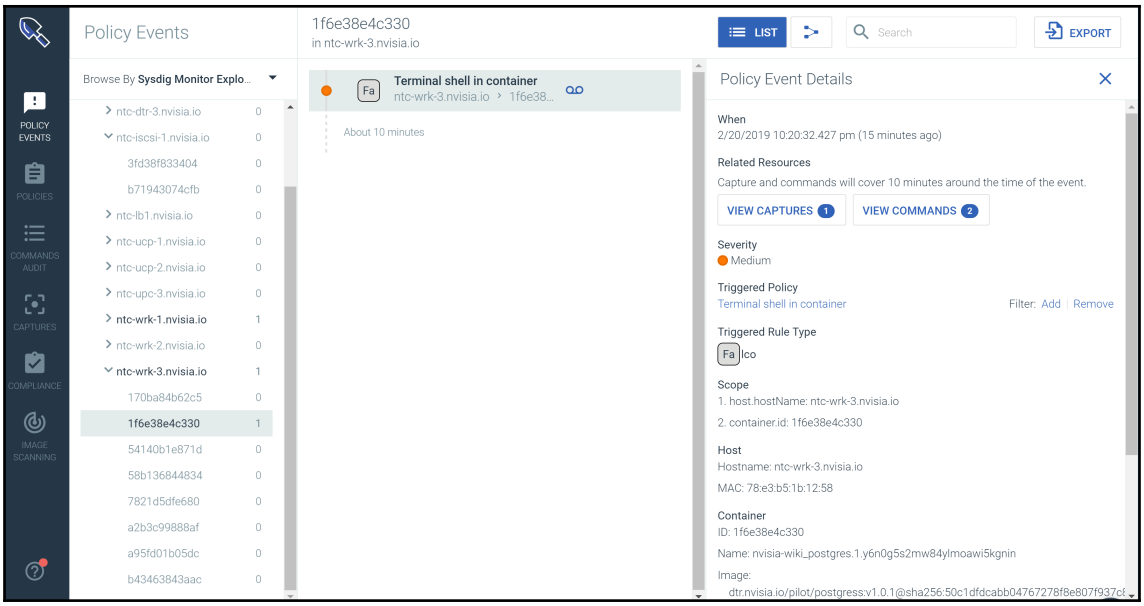
The hostname (atsea.[redacted]) is correctly listed in the certificate.

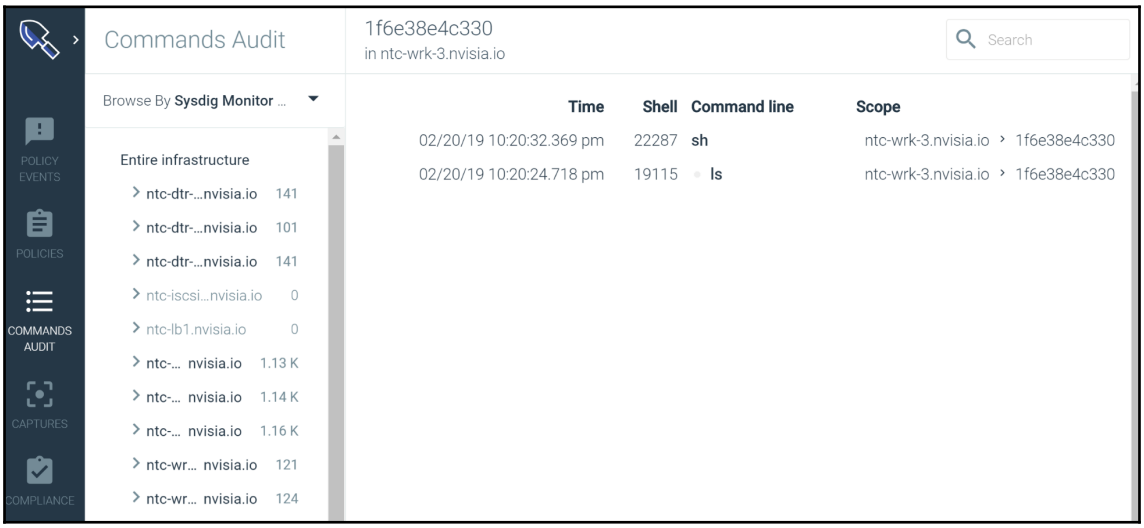
Server

**Common name:** *[redacted]
**SANs:** *[redacted]
**Valid** from November 20, 2018 to November 21, 2019
**Serial Number:** 0e274b7af77ebd961af056452af0e2d9
**Signature Algorithm:** sha256WithRSAEncryption
**Issuer:** RapidSSL RSA CA 2018

Chain

**Common name:** RapidSSL RSA CA 2018
**Organization:** DigiCert Inc **Org. Unit:** www.digicert.com
**Location:** US
**Valid** from November 6, 2017 to November 6, 2027
**Serial Number:** 08a5a246cd4b5c8c83d702b4bbab5349
**Signature Algorithm:** sha256WithRSAEncryption
**Issuer:** DigiCert Global Root CA


Policy Events
1f6e38e4c330
in ntc-wrk-3.nvisia.io
LIST
Search
EXPORT
Browse By Sysdig Monitor Explo...
POLICY EVENTS
POLICIES
COMMANDS AUDIT
CAPTURES
COMPLIANCE
IMAGE SCANNING
ntc-dtr-3.nvisia.io 0
ntc-iscsi-1.nvisia.io 0
3fd38f833404 0
b71943074cfb 0
ntc-lb1.nvisia.io 0
ntc-ucp-1.nvisia.io 0
ntc-ucp-2.nvisia.io 0
ntc-upc-3.nvisia.io 0
ntc-wrk-1.nvisia.io 1
ntc-wrk-2.nvisia.io 0
ntc-wrk-3.nvisia.io 1
170ba84b62c5 0
1f6e38e4c330 1
54140b1e871d 0
58b136844834 0
7821d5dfe680 0
a2b3c99888af 0
a95fd01b05dc 0
b43463843aac 0
Fa
Terminal shell in container
ntc-wrk-3.nvisia.io › 1f6e38...
About 10 minutes
Policy Event Details
When
2/20/2019 10:20:32.427 pm (15 minutes ago)
Related Resources
Capture and commands will cover 10 minutes around the time of the event.
VIEW CAPTURES 1
VIEW COMMANDS 2
Severity
Medium
Triggered Policy
Terminal shell in container
Filter: Add | Remove
Triggered Rule Type
Fa lco
Scope
1. host.hostName: ntc-wrk-3.nvisia.io
2. container.id: 1f6e38e4c330
Host
Hostname: ntc-wrk-3.nvisia.io
MAC: 78:e3:b5:1b:12:58
Container
ID: 1f6e38e4c330
Name: nvisia-wiki_postgres.1.y6n0g5s2mw84ylmoawi5kgnin
Image:


Commands Audit
1f6e38e4c330
in ntc-wrk-3.nvisia.io
Search
Browse By Sysdig Monitor ...
POLICY EVENTS
POLICIES
COMMANDS AUDIT
CAPTURES
COMPLIANCE
Entire infrastructure
ntc-dtr-...nvisia.io 141
ntc-dtr-...nvisia.io 101
ntc-dtr-...nvisia.io 141
ntc-iscsi...nvisia.io 0
ntc-lb1.nvisia.io 0
ntc-... nvisia.io 1.13 K
ntc-... nvisia.io 1.14 K
ntc-... nvisia.io 1.16 K
ntc-wr... nvisia.io 121
ntc-wr... nvisia.io 124
Time
Shell
Command line
Scope
02/20/19 10:20:32.369 pm 22287 sh ntc-wrk-3.nvisia.io › 1f6e38e4c330
02/20/19 10:20:24.718 pm 19115 ls ntc-wrk-3.nvisia.io › 1f6e38e4c330


Sysdig Inspect
Terminal shell in container-63dcfb53-5bea-4f39-8688-db315999fd21.scap
Overview
VIEWS
Directories
Errors
Files
I/O by Type
Page Faults
Port bindings
Processes
Processes CPU
Processes Errors
Server Ports
I/O STREAMS
SYSCALLS
GENERAL
FILE
NETWORK
SECURITY
PERFORMANCE
INFRASTRUCTURE
Running Processes
89
File Bytes In+Out
451.0 K
Net Bytes In+Out
152
Executed Commands
6
File Open Errors
143
Docker Events
1
Running Containers
9
File Bytes In
450.9 K
Net Bytes In
76
Deleted Files
3
Fork Count
32
System Calls
10.4 K
File Bytes Out
60
Net Bytes Out
76
Accessed Files
104
Active Network Connections
2
Modified Files
Listening Ports
TIME
0
duration: 624.87 ms
624.87 ms
Accessed Files
Executed Commands
File Bytes In+Out

COMPLIANCE

Results > Docker Node Compliance

Download CSV

POLICY EVENTS
POLICIES
COMMANDS AUDIT
CAPTURES
COMPLIANCE
IMAGE SCANNING

HIGH RISK

0 Fail | 38 Warn | 66 Pass

Completed on Feb 18, 2019 - 12:00 am

Host Mac b4:b5:2f:65:f0:8c

1. Host Configuration
2. Docker daemon configuration
3. Docker daemon configuration files
4. Container Images and Build File
5. Container Runtime
6. Docker Security Operations
7. Docker Swarm Configuration

## 5. Container Runtime

5.1 Ensure AppArmor Profile is enabled

Containers with no AppArmorProfile:
- sysdig-agent
- gitlab-runner

5.2 Ensure SELinux security options are set, if applicable

Containers with no SecurityOptions:
- gitlab-runner

5.3 Ensure Linux Kernel Capabilities are restricted within containers

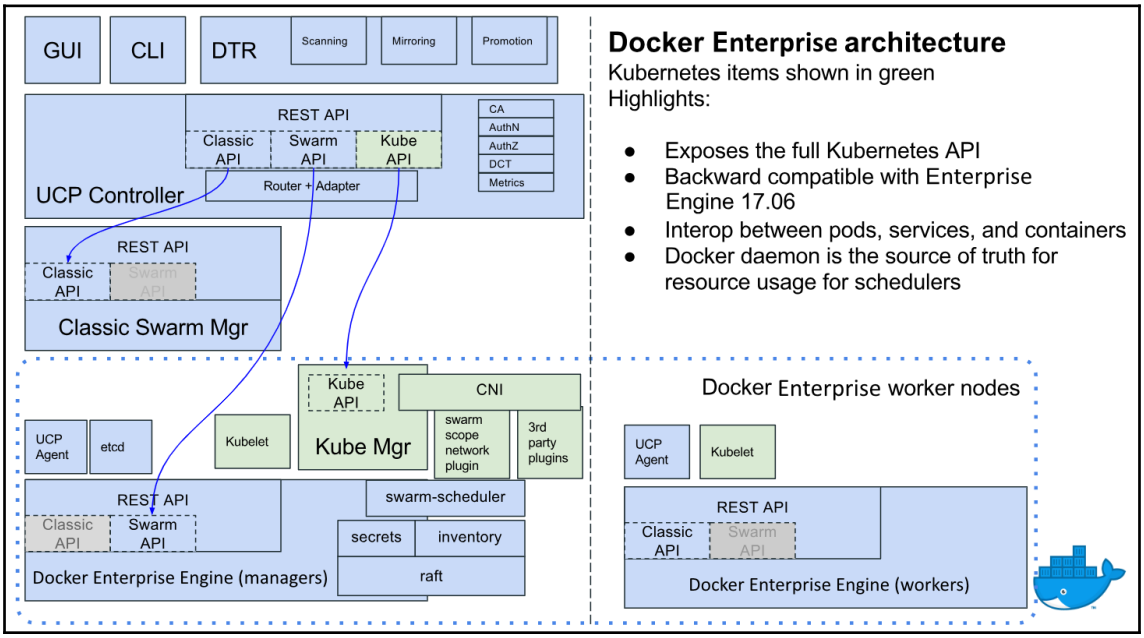
5.4 Ensure privileged containers are not used

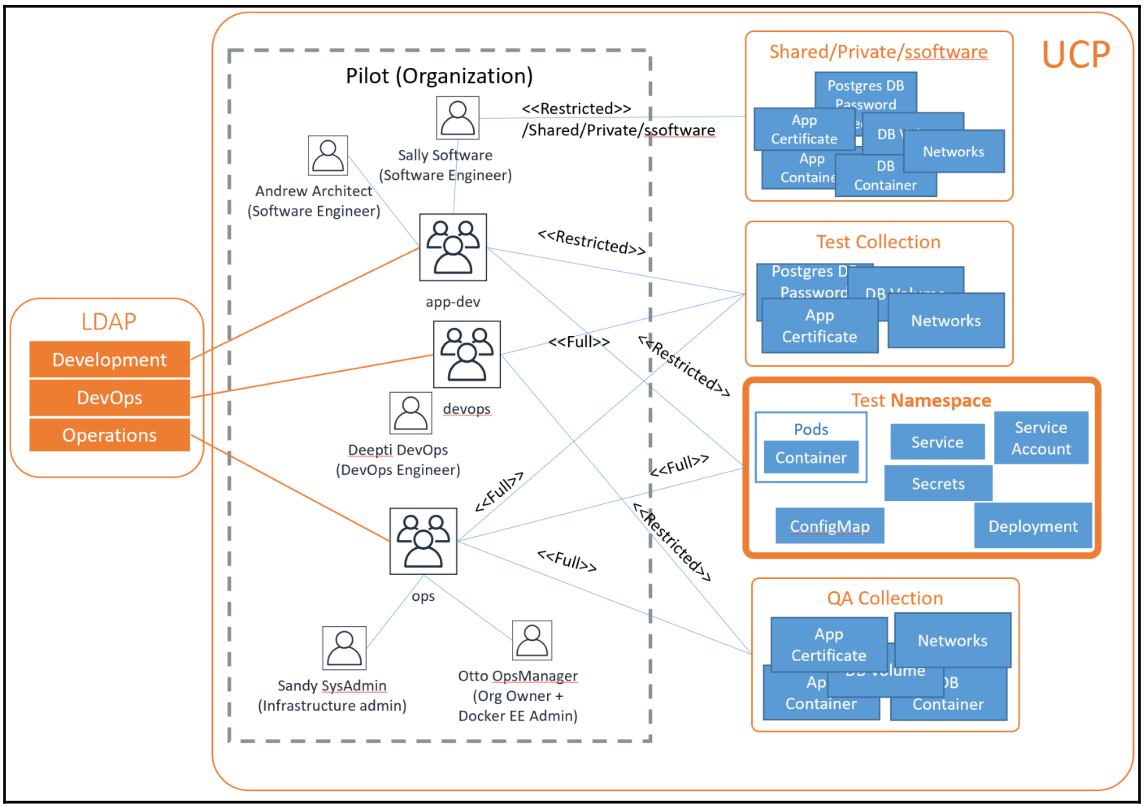
Containers running in privileged mode:
- sysdig-agent

5.5 Ensure sensitive host system directories are not mounted on containers

5.6 Ensure ssh is not run within containers

# Chapter 10: More on Kubernetes with Docker Enterprise




UCP
Pilot (Organization)
Sally Software
(Software Engineer)
Andrew Architect
(Software Engineer)
app-dev
devops
Deepti DevOps
(DevOps Engineer)
ops
Sandy SysAdmin
(Infrastructure admin)
Otto OpsManager
(Org Owner +
Docker EE Admin)
<<Restricted>>
/Shared/Private/ssoftware
<<Restricted>>
<<Full>>
<<Full>>
<<Restricted>>
<<Full>>
<<Full>>
<<Restricted>>
LDAP
Development
DevOps
Operations
Shared/Private/ssoftware
Postgres DB
Password
App
Certificate
Networks
App
Container
DB
Container
Test Collection
App
Certificate
Networks
Test Namespace
Pods
Container
Service
Service
Account
Secrets
ConfigMap
Deployment
QA Collection
App
Certificate
Networks
App
Container
DB
Container

Kubernetes

## ClusterRole: system:aggregate-to-view

Created 3 months ago

Overview

RULES

API Groups
N/A

Resources
**configmaps, endpoints, persistentvolumeclaims, pods, replicationcontrollers, replicationcontrollers/scale, serviceaccounts, services**

Verbs
**get, list, watch**

API Groups
N/A

Resources
**bindings, events, limitranges, namespaces/status, pods/log, pods/status, replicationcontrollers/status, resourcequotas, resourcequotas/status**

Verbs
**get, list, watch**

API Groups
N/A

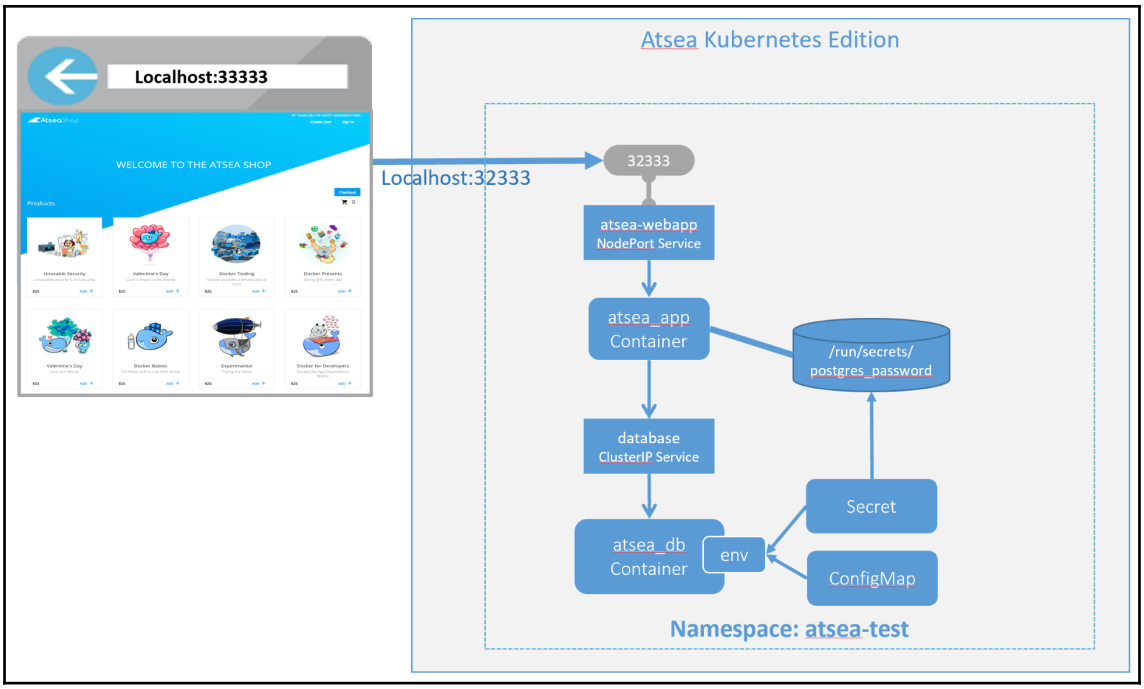
Resources
**namespaces**

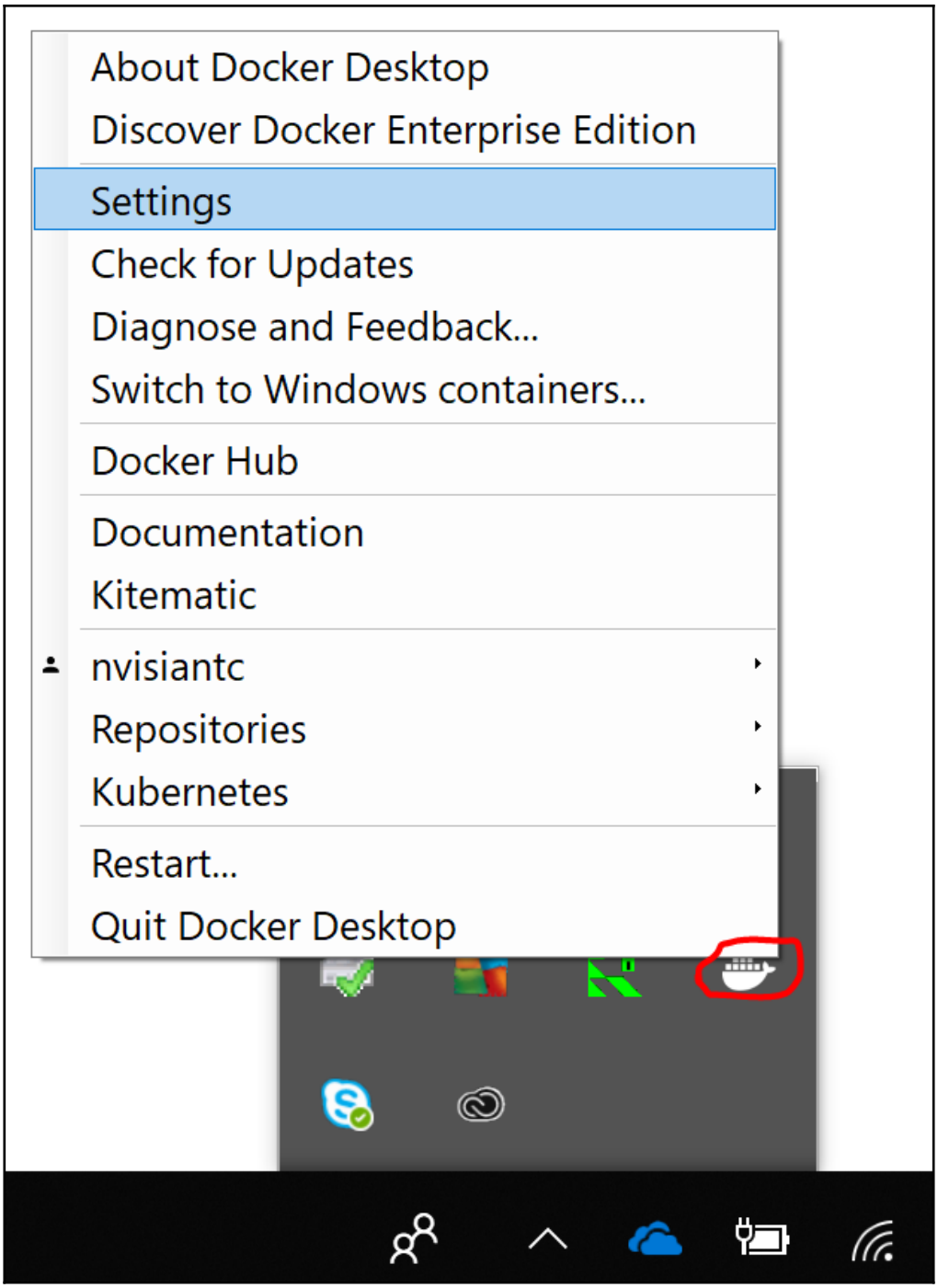
Verbs
**get, list, watch**

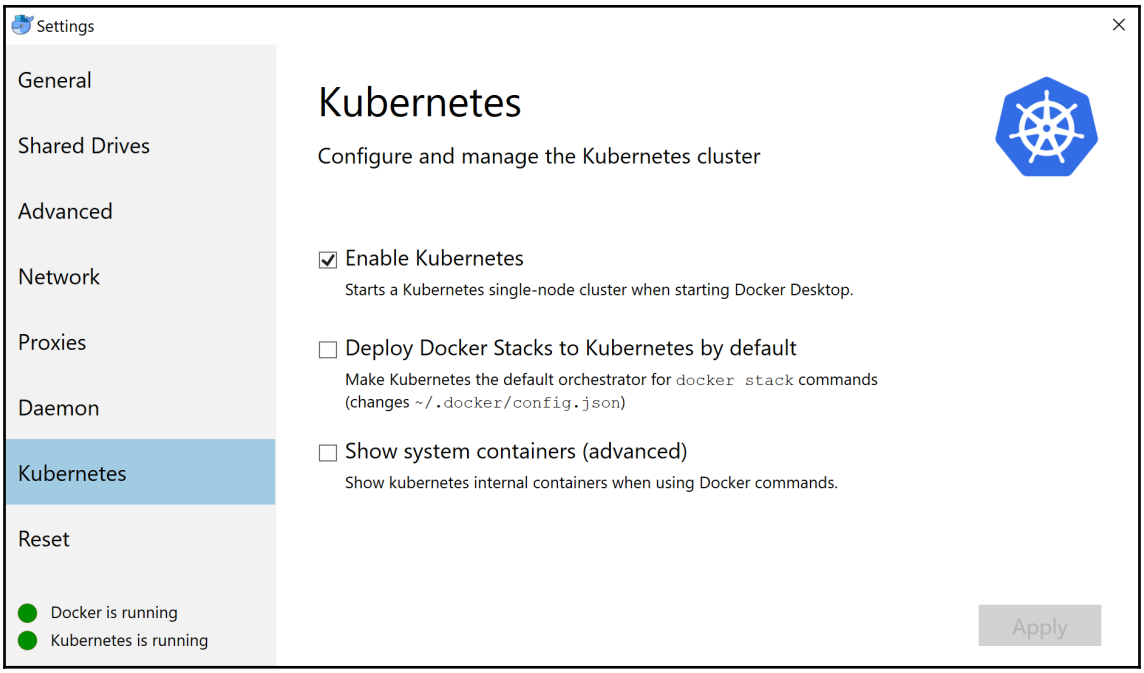
API Groups
**apps**

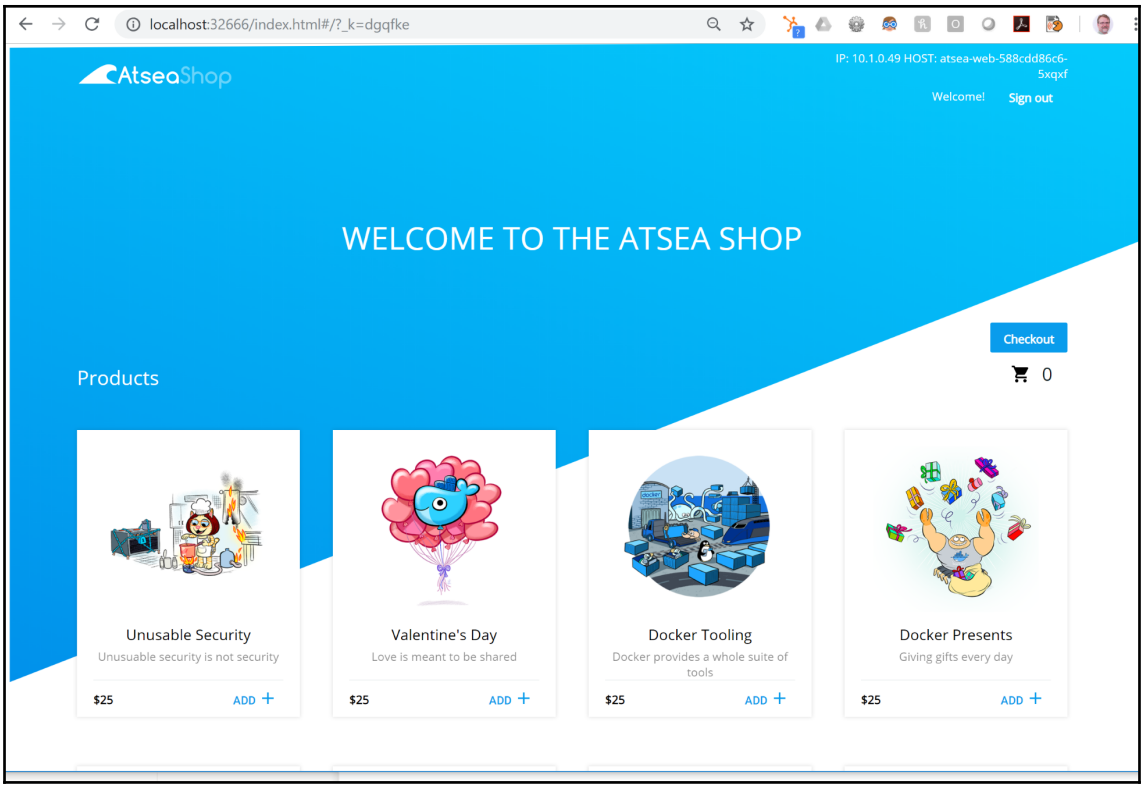
Resources
**daemonsets, deployments, deployments/scale, replicasets, replicasets/scale, statefulsets, statefulsets/scale**

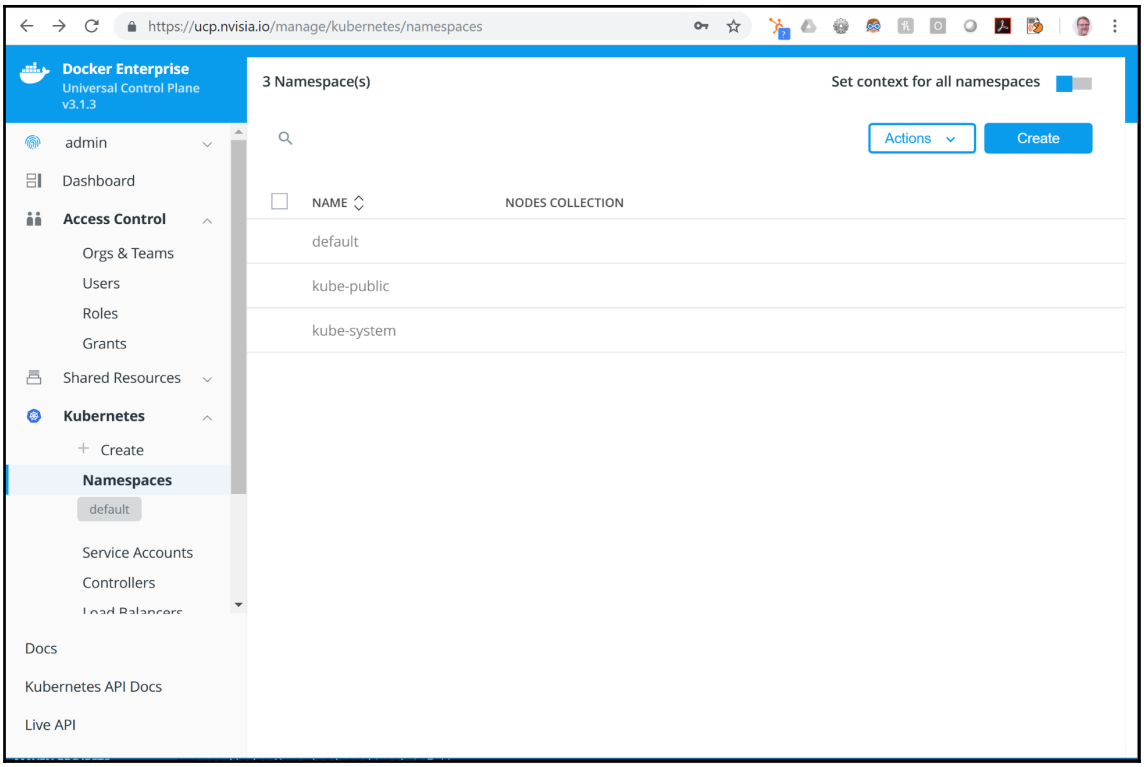
Verbs
**get, list, watch**

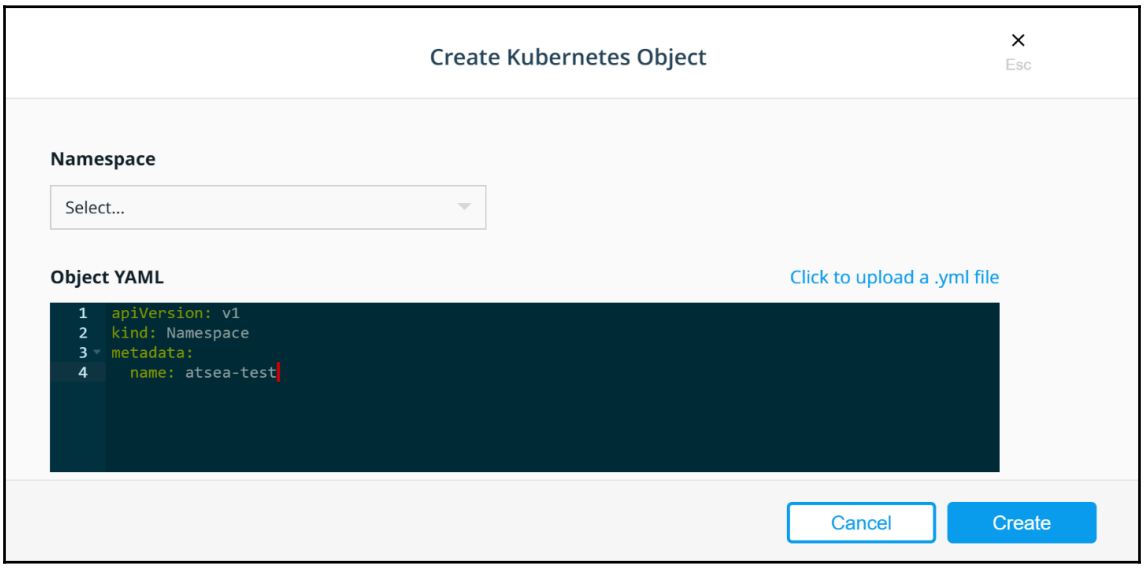

Localhost:33333
WELCOME TO THE ATSEA SHOP
Localhost:32333
Atsea Kubernetes Edition
32333
atsea-webapp
NodePort Service
atsea_app
Container
/run/secrets/
postgres_password
database
ClusterIP Service
Secret
atsea_db
Container
env
ConfigMap
Namespace: atsea-test


About Docker Desktop
Discover Docker Enterprise Edition
Settings
Check for Updates
Diagnose and Feedback...
Switch to Windows containers...
Docker Hub
Documentation
Kitematic
nvisiantc
Repositories
Kubernetes
Restart...
Quit Docker Desktop


Settings
General
Shared Drives
Advanced
Network
Proxies
Daemon
Kubernetes
Reset
Docker is running
Kubernetes is running
Kubernetes
Configure and manage the Kubernetes cluster
Enable Kubernetes
Starts a Kubernetes single-node cluster when starting Docker Desktop.
Deploy Docker Stacks to Kubernetes by default
Make Kubernetes the default orchestrator for docker stack commands
(changes ~/.docker/config.json)
Show system containers (advanced)
Show kubernetes internal containers when using Docker commands.
Apply


localhost:32666/index.html#/?_k=dgqfke
AtseaShop
IP: 10.1.0.49 HOST: atsea-web-588cdd86c6-5xqxf
Welcome!
Sign out
WELCOME TO THE ATSEA SHOP
Checkout
0
Products
Unusable Security
Unusuable security is not security
$25
ADD +
Valentine's Day
Love is meant to be shared
$25
ADD +
Docker Tooling
Docker provides a whole suite of tools
$25
ADD +
Docker Presents
Giving gifts every day
$25
ADD +


https://ucp.nvisia.io/manage/kubernetes/namespaces
Docker Enterprise
Universal Control Plane
v3.1.3
admin
Dashboard
Access Control
Orgs & Teams
Users
Roles
Grants
Shared Resources
Kubernetes
Create
Namespaces
default
Service Accounts
Controllers
Docs
Kubernetes API Docs
Live API
3 Namespace(s)
Set context for all namespaces
Actions
Create
NAME
NODES COLLECTION
default
kube-public
kube-system


Create Kubernetes Object
Esc
Namespace
Select...
Object YAML
Click to upload a .yml file
1 apiVersion: v1
2 kind: Namespace
3 metadata:
4 name: atsea-test
Cancel
Create

4 Namespace(s)

Set context for all namespaces

Actions

Create

| NAME | NODES COLLECTION |
| --- | --- |
| atsea-test | |
| default | |
| kube-public | |
| kube-system | |

## Create User

### Details

Newly added users will automatically be added to the "docker-datacenter" organization; this organizati
priviledges. These users will have restrictedcontrol to their own private collections.

**Username**

mpanthofer

**Password**

••••••••••••••••

**Full Name**

Mark Panthofer (no-admin)

☐ Is a Docker Enterprise admin

Create Role Binding

× Esc

A grant defines who (subject) has a specific access (role or cluster role) to a resource set (Kubernetes namespace).

✓ 1. Subject

**User**
mpanthofer

Edit

✓ 2. Resource Set

**Namespace**
atsea-test

Edit

3. Role

**Role Type**

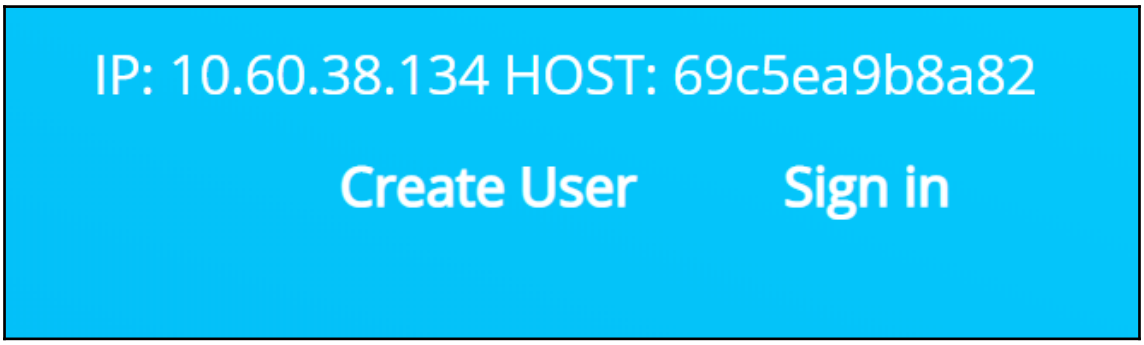
ROLE CLUSTER ROLE

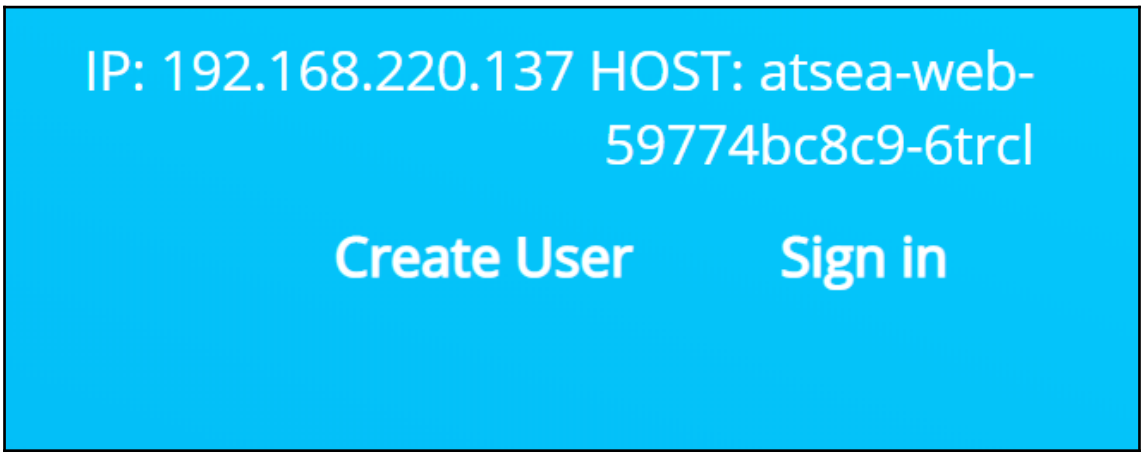
**Select Cluster Role**

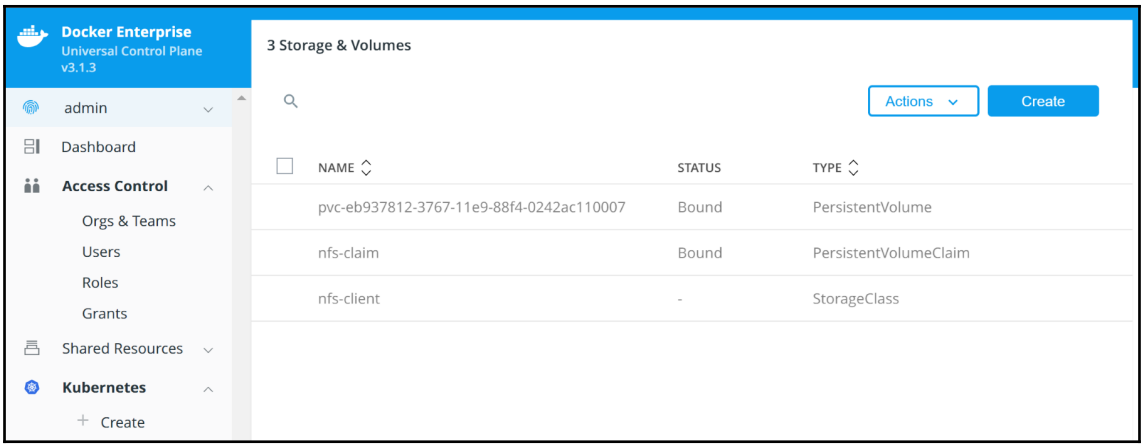
admin

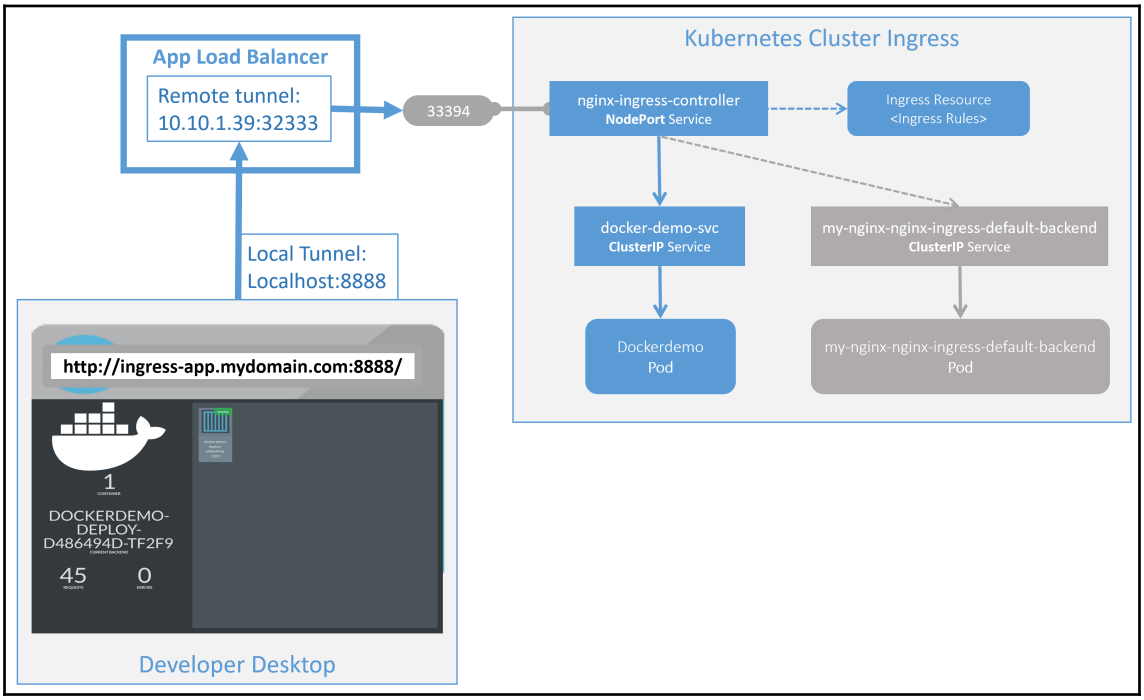
Cancel Create

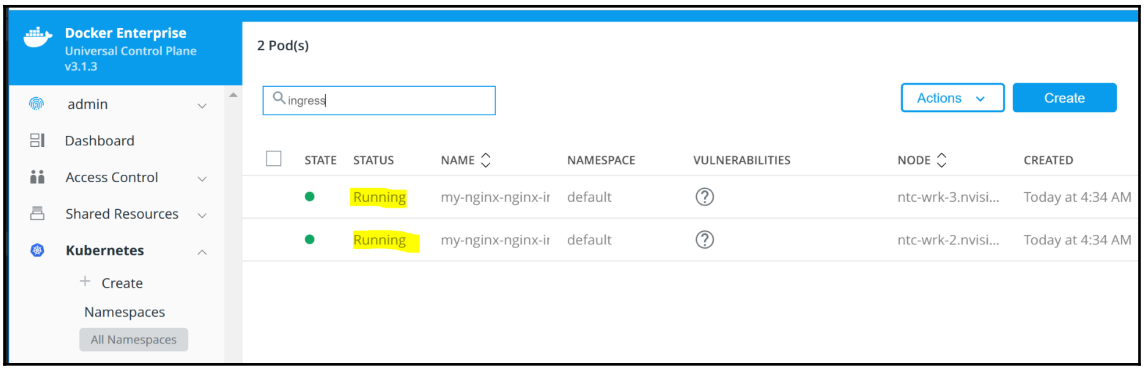
```
mpanthofer@xps-bash::cli-mpanthofer-no-admin$ kubectl get all
Error from server (Forbidden): pods is forbidden: User "2177a148-729b-4aa2-aa28-eeeb1e701c55" cannot li
Error from server (Forbidden): replicationcontrollers is forbidden: User "2177a148-729b-4aa2-aa28-eeeb1
Error from server (Forbidden): services is forbidden: User "2177a148-729b-4aa2-aa28-eeeb1e701c55" cannc
Error from server (Forbidden): daemonsets.apps is forbidden: User "2177a148-729b-4aa2-aa28-eeeb1e701c55
Error from server (Forbidden): deployments.apps is forbidden: User "2177a148-729b-4aa2-aa28-eeeb1e701c5
Error from server (Forbidden): replicasets.apps is forbidden: User "2177a148-729b-4aa2-aa28-eeeb1e701c5
Error from server (Forbidden): statefulsets.apps is forbidden: User "2177a148-729b-4aa2-aa28-eeeb1e701c
Error from server (Forbidden): horizontalpodautoscalers.autoscaling is forbidden: User "2177a148-729b-4
e "default": access denied
Error from server (Forbidden): jobs.batch is forbidden: User "2177a148-729b-4aa2-aa28-eeeb1e701c55" car
Error from server (Forbidden): cronjobs.batch is forbidden: User "2177a148-729b-4aa2-aa28-eeeb1e701c55"
mpanthofer@xps-bash::cli-mpanthofer-no-admin$ kubectl -n atsea-test get all
No resources found.
mpanthofer@xps-bash::cli-mpanthofer-no-admin$
```

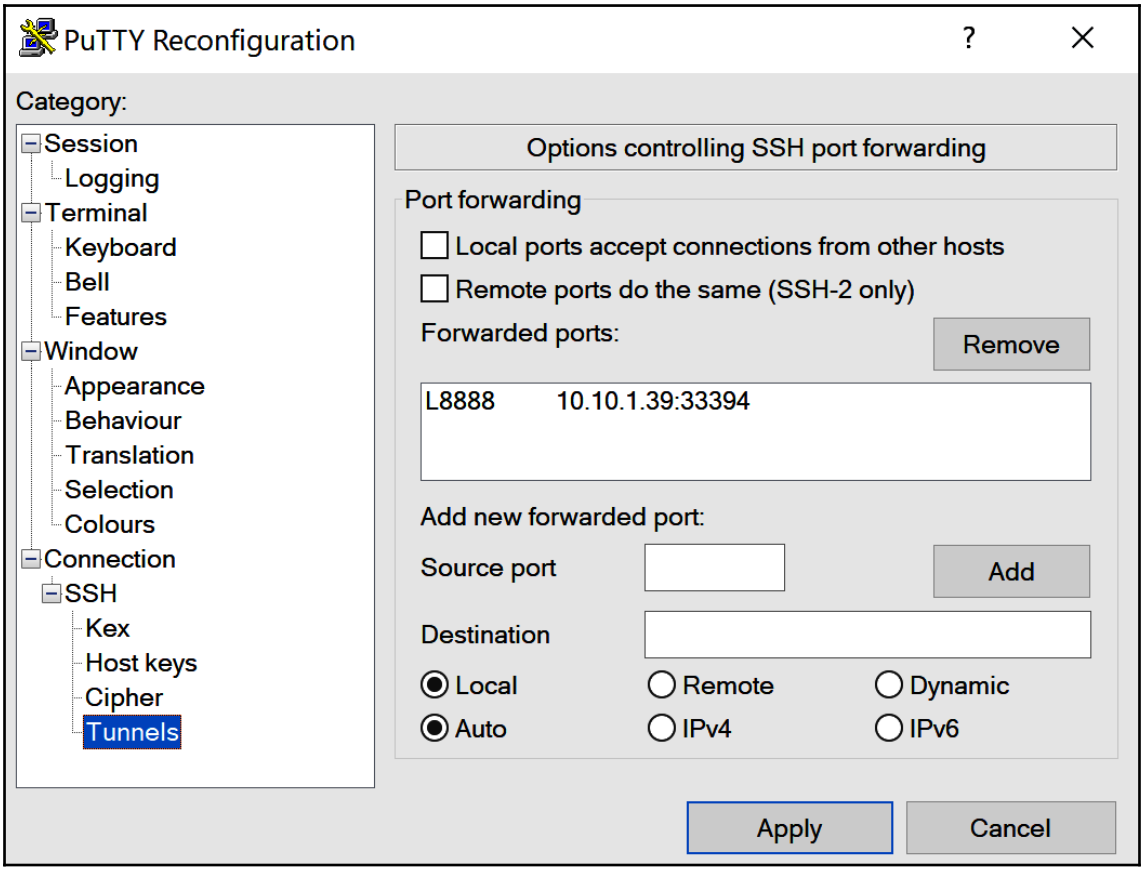


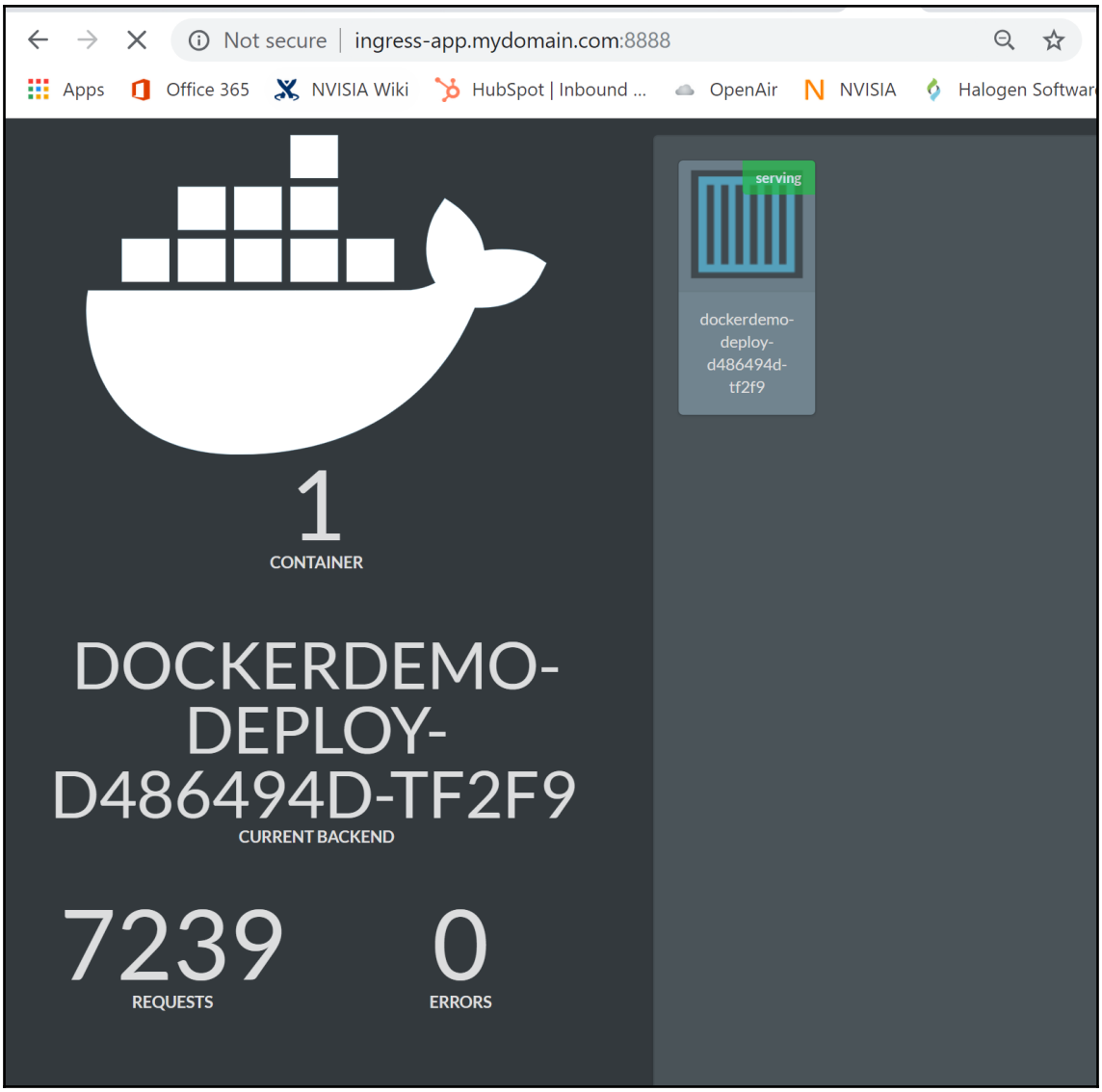




Docker Enterprise
Universal Control Plane
v3.1.3
admin
Dashboard
Access Control
Orgs & Teams
Users
Roles
Grants
Shared Resources
Kubernetes
Create
3 Storage & Volumes
Actions
Create
NAME
STATUS
TYPE
pvc-eb937812-3767-11e9-88f4-0242ac110007
Bound
PersistentVolume
nfs-claim
Bound
PersistentVolumeClaim
nfs-client
-
StorageClass


App Load Balancer
Remote tunnel:
10.10.1.39:32333
33394
Kubernetes Cluster Ingress
nginx-ingress-controller
NodePort Service
Ingress Resource
<Ingress Rules>
docker-demo-svc
ClusterIP Service
my-nginx-nginx-ingress-default-backend
ClusterIP Service
Dockerdemo
Pod
my-nginx-nginx-ingress-default-backend
Pod
Local Tunnel:
Localhost:8888
http://ingress-app.mydomain.com:8888/
1
DOCKERDEMO-
DEPLOY-
D486494D-TF2F9
45
0
Developer Desktop


Docker Enterprise
Universal Control Plane
v3.1.3
admin
Dashboard
Access Control
Shared Resources
Kubernetes
Create
Namespaces
All Namespaces
2 Pod(s)
ingress
Actions
Create
STATE
STATUS
NAME
NAMESPACE
VULNERABILITIES
NODE
CREATED
Running
my-nginx-nginx-ir
default
ntc-wrk-3.nvisi...
Today at 4:34 AM
Running
my-nginx-nginx-ir
default
ntc-wrk-2.nvisi...
Today at 4:34 AM


PuTTY Reconfiguration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
SSH
Kex
Host keys
Cipher
Tunnels
Options controlling SSH port forwarding
Port forwarding
Local ports accept connections from other hosts
Remote ports do the same (SSH-2 only)
Forwarded ports:
Remove
L8888 10.10.1.39:33394
Add new forwarded port:
Source port
Add
Destination
Local
Remote
Dynamic
Auto
IPv4
IPv6
Apply
Cancel


Not secure
ingress-app.mydomain.com:8888
Apps
Office 365
NVISIA Wiki
HubSpot | Inbound ...
OpenAir
NVISIA
Halogen Softwar
serving
dockerdemo-deploy-d486494d-tf2f9
1
CONTAINER
DOCKERDEMO-DEPLOY-D486494D-TF2F9
CURRENT BACKEND
7239
REQUESTS
0
ERRORS

# Chapter 11: Taking the Docker Enterprise Platform into the Future