



**RELAX,
WE CARE**



**RELAX,
WE CARE**

CONTAINERS ALL THE WAY DOWN: BOOTC AND KUBERNETES

andreas.tomaselli@nts.eu

\$ whoami

Andreas Tomaselli

- Platform Engineer @ NTS
- networking with Cisco ACI Fabrics
- building awesome stacks for awesome customers
- Yet another talk about containers ;)

Mail: andreas.tomaselli@nts.eu

Linkedin: <https://www.linkedin.com/in/andreas-tomaselli/>

LETS TALK ABOUT CONTAINERS

WHY CONTAINERS ?

- **K8S Applications ?**
 - 🖱 Developers / App Owner ?
 - CI/CD easy-peasy
 - Gitops
 - Container Registries & Scanning
 - <https://landscape.cncf.io/> some tools

**“CONTAINERS MAKE APPLICATION
DEPLOYMENT EASIER”**

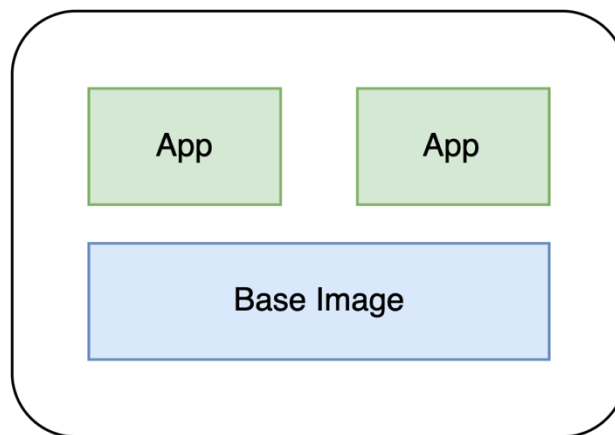




bootc

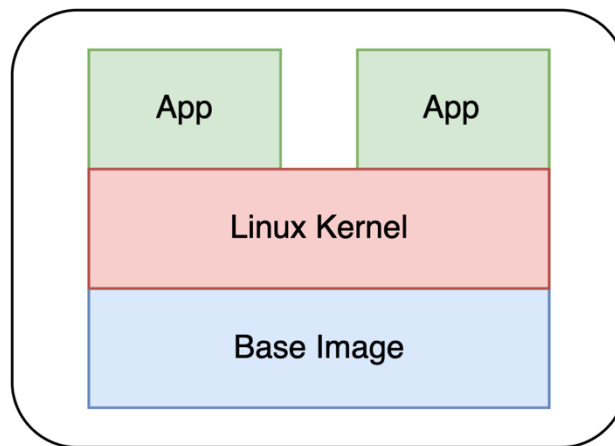
WHAT IF ... ?

Application Container



WHAT IF ... ?

Bootable Container



**“CONTAINERS MAKE OS
DEPLOYMENT EASIER”**



WHY ?

Complex and risky OS updates

Traditional OS updates can be complex, prone to corruption.

Bootc provides atomic, in-place updates that are either fully successful or cleanly reverted, minimizing corruption.

WHY ?

Inconsistent OS builds and deployments

Building and deploying operating systems often involves a complex mix of tools and formats.

Bootc standardizes OS builds into OCI container images, which are more consistent and easier to manage with existing CI/CD pipelines

WHY ?

Lack of immutability and rollback in OS

Unlike typical containers, traditional OSes are not inherently immutable or easily rollbacked.

Bootc creates immutable OS images, enabling single-command rollbacks and easier debugging.

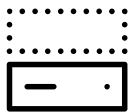
WHY ?

Slow and difficult OS image creation

Bootc allows users to build OCI-based OS images using familiar Dockerfiles.

These images can then be exported to various cloud formats (like QCOW2, VMDK, AMI), accelerating the creation and deployment of operating systems on bare metal and public clouds

USECASES



1:1 App/Host

Manage the OS and the app as a single unit



Edge appliances

Manage a fleet of systems with registries and auto-updates



Standalone container hosts

Build containerized applications and the hosting OS



AI/ML Stacks

Perfectly version app dependencies from kernel, GPU and accelerator drivers, frameworks

- **Supported Linux Systems**

- Fedora
- CentOS Stream
- RHEL 9.6 / 10 (Image-mode)

- Bootc Project Contributed to CNCF by RedHat (Nov 2024)



bootc

BUILD – TEST – DEPLOY

SIMPLE CONTAINERFILE / DOCKERFILE

FROM registry.redhat.io/rhel9/rhel-bootc

RUN dnf -y install nginx cloud-init && \
dnf -y clean all && \
systemctl enable nginx.service cloud-init.service

COPY files/index.html /usr/share/nginx/html/index.html

```
index.html    <!DOCTYPE html>
               <html>
               <body style="background-color:green;">

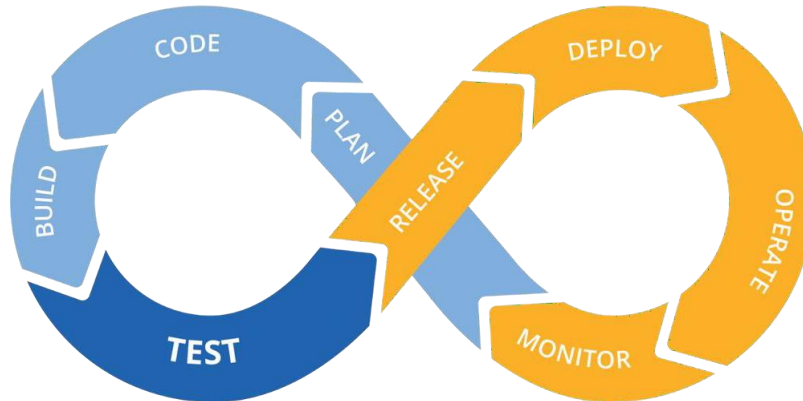
               </body>
               </html>
```

BUILD, TEST, DEPLOY

```
$ podman build -t quay.io/user/image-tag:base
```

```
$ podman run -privileged -d quay.io/user/image-tag:base
```

```
$ podman push quay.io/user/image-tag:base
```



Update releases

✓ Passed andreas tomaselli created pipeline for commit 5710d438 3 weeks ago, finished 3 weeks ago

For `main`

Scheduled latest 3 jobs 15 seconds, queued for 3 seconds

Pipeline

Jobs 3

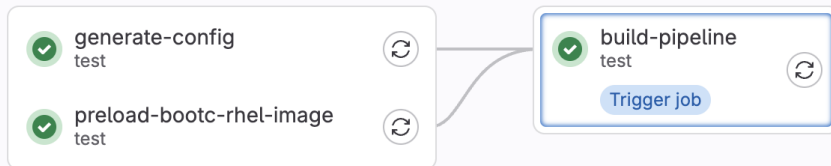
Tests 0

Group jobs by

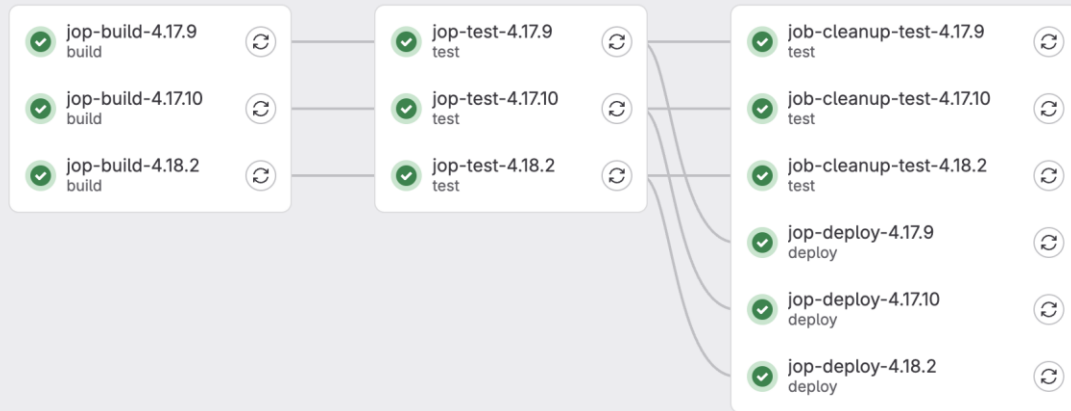
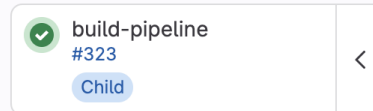
Stage

Job dependencies

Show dependencies ☒



Downstream



BOOTC

NTS

Repository Tags

Compact Expanded Show Signatures



1 - 3 of 3

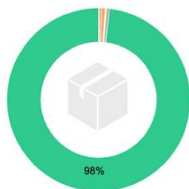


Filter Tags...

TAG	LAST MODIFIED ↓	SECURITY SCAN	SIZE	EXPIRES	MANIFEST
<input type="checkbox"/> 4.17.10	a day ago	2 Critical · 37 fixable	1.4 GiB	Never	SHA256 31cda8ec9ba4
<input type="checkbox"/> 4.18.2	a day ago	1 Critical · 29 fixable	1.4 GiB	Never	SHA256 2b322c2d4bbb
<input type="checkbox"/> latest	a day ago	1 Critical · 29 fixable	1.4 GiB	Never	SHA256 2b322c2d4bbb

← edge-nodes/flightctl

2b322c2d4bbb



Quay Security Scanner has recognized **856** packages.

- 1 packages with Critical-level vulnerabilities.
- 3 packages with High-level vulnerabilities.
- 6 packages with Medium-level vulnerabilities.
- 2 packages with Low-level vulnerabilities.
- 4 packages with Unknown-level vulnerabilities.
- 840** packages with no vulnerabilities.

Packages

PACKAGE NAME

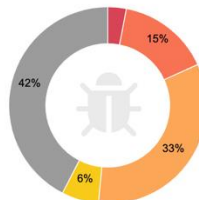
github.com/go-git/go-git/v5

PACKAGE

v5.11.0

← edge-nodes/flightctl

2b322c2d4bbb

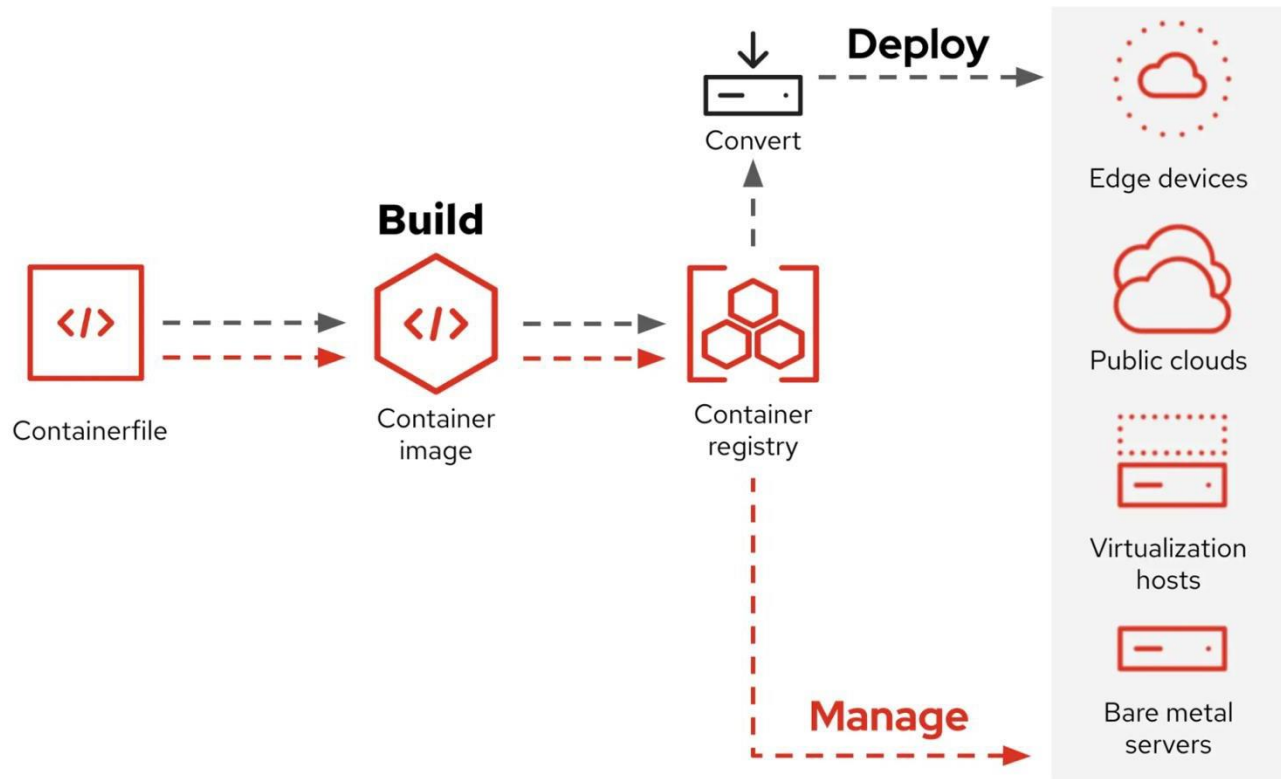


Quay Security Scanner has detected **33** vulnerabilities.
Patches are available for **29** vulnerabilities.

- 1 Critical-level vulnerabilities.
- 5 High-level vulnerabilities.
- 11 Medium-level vulnerabilities.
- 2 Low-level vulnerabilities.
- 14 Unknown-level vulnerabilities.

BOOTC

NTS



MANAGEMENT

CLI

Update OS

```
bash-5.1# bootc update
layers already present: 67; layers needed: 1 (285 bytes)
  Deploying: done (11 seconds)
  Version: 9.6
  Digest: sha256:20aeb6577bdfc95424b32faa76bc4435957abad34711a7e54839f61d
Total new layers: 68      Size: 1.2 GB
Removed layers:   1      Size: 279 bytes
Added layers:    1      Size: 285 bytes
bash-5.1#
```


CLI

Status

```
bash-5.1# bootc status
```

```
[ Staged image: quay.fdh.nts-lab.eu/bootc/rhel-baseimg:9.6
```

```
[ Digest: sha256:873ebcfdee3f60bebc5a87ad40e8fbe61c5303e90c4503066dae2889c715
```

```
[ Version: 9.6 (2025-09-24 07:21:27.103061176 UTC)
```

```
[
```

```
● Booted image: quay.fdh.nts-lab.eu/bootc/rhel-baseimg:9.6
```

```
    Digest: sha256:873ebcfdee3f60bebc5a87ad40e8fbe61c5303e90c4503066dae2889c715
```

```
    Version: 9.6 (2025-09-24 07:21:27.103061176 UTC)
```

```
[
```

```
[ Rollback image: quay.fdh.nts-lab.eu/bootc/rhel-baseimg:9.4
```

```
[ Digest: sha256:5a1201a8829bfb47293ce250450c679c4ff7b3923c6c16b562616abaff
```

```
[ Version: 9.20241104.0 (2025-09-23 15:04:32.145761143 UTC)
```

CLI

Switch Image

```
[bash-5.1# bootc switch quay.fdh.nts-lab.eu/bootc/rhel-baseimg:9.4-ev  
layers already present: 1; layers needed: 67 (934.0 MB)  
Fetching layers ██████████ 4/67  
└─ Fetching ██████████ 928.00 KiB/12.62 MiB (20.01 MiB/s) ostree chunk
```

FLIGHTCTRL

ACM: EDGE-MANAGER

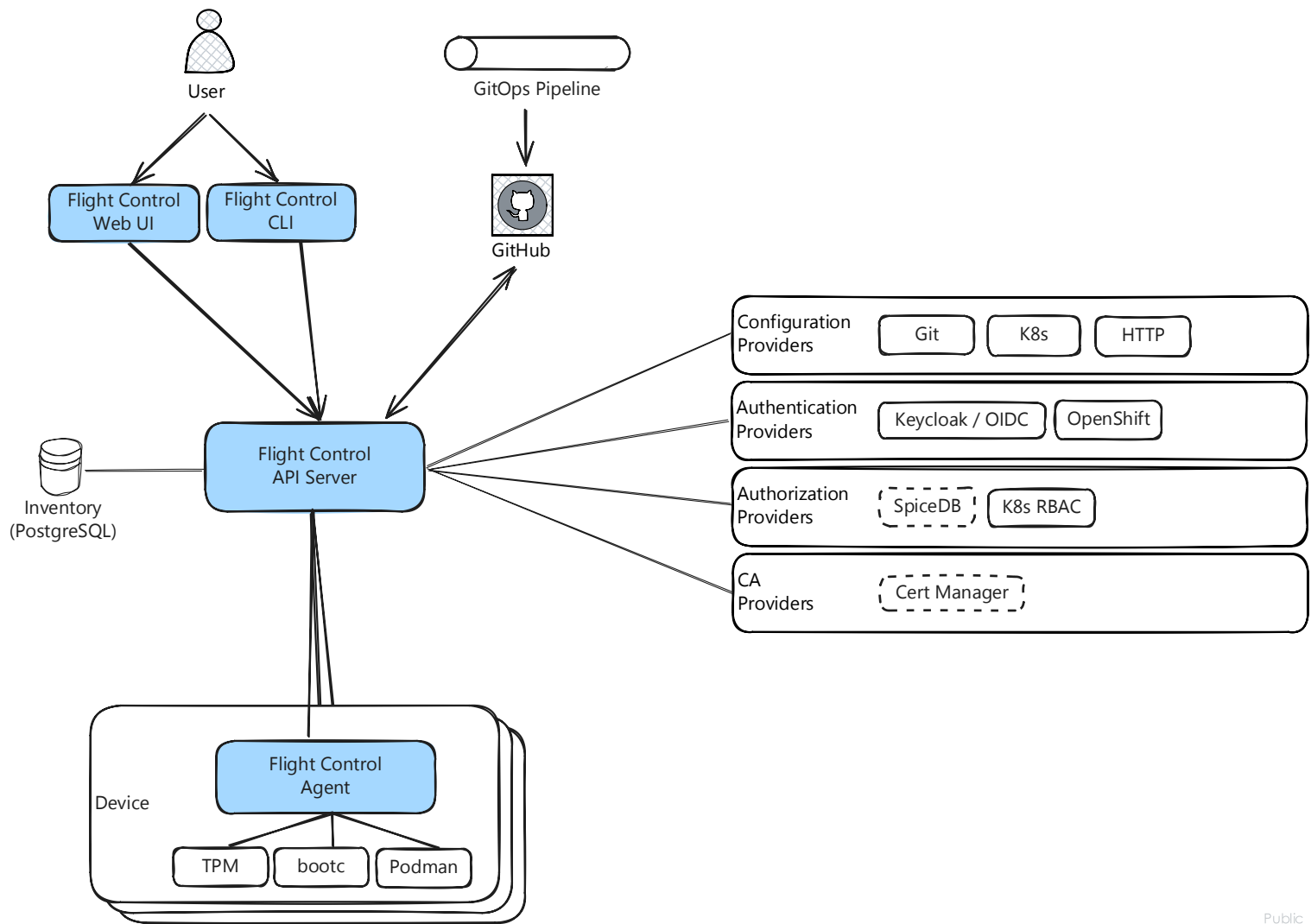
WHAT IS FLIGHTCONTROL ?

Flight Control is a service for declarative management of **fleets** of edge devices and their workloads

- Included with ACM 2.13+ (TP) – (**Edge Manager**)
- Requires flightctrl agent on the edge device
- <https://github.com/flightctl/flightctl>

FLIGHTCTRL

NTS



FLIGHTCTRL

NTS

```
Red Hat Enterprise Linux 9.20241104.0.4 (Plow)  
Kernel 5.14.0-427.42.1.el9_4.x86_64 on an x86_64
```

```
enp1s0: 10.0.2.2 fe80::71:55ff:fe00:8
```



Enroll your device to flightctl by scanning
the above QR code or following this URL:

<https://console-openshift-console.apps.c13.k8s.fdh.nts-lab.eu/edge/enroll/tqsvqu02r9gcnskrp4onsj5v292i11j2i8uqlc91aa7kq2>

rhel9-chocolate-hornet-98 login:

Home >

Search

Infrastructure >

Edge Management ▾

Fleets

Devices

Repositories

Applications

Governance

Credentials

You are logged in as a temporary administrative user. Update the [cluster OAuth configuration](#) to allow others to log in.

Devices pending approval

Technology preview

 Search by name

Actions ▾

<input type="checkbox"/>	Name	Created	
<input type="checkbox"/>	tqsvqv...2ucatu0	< 1 minute ago	Approve ⋮
1 of 1 ▾ < >			

Devices

Technology preview

Filter by status ▾

Labels and fleets ▾

Add devices

Decommission devices

☐ Show only decommissioned devices

<input type="checkbox"/>	Alias	Name	Fleet	Application...	Device st...	Update status ?	Last seen
<input type="checkbox"/>	edge-device-flightctl	4sa99m...snu1lf0	None ?	✓ Healthy	✓ Online	✓ Up-to-date	< 1 minute ago ⋮

Home >

Search

Infrastructure >

Edge Management ▾

Fleets

Devices

Repositories

Applications

Governance

Credentials

You are logged in as a temporary administrative user. Update the [cluster OAuth configuration](#) to allow others to log in.

Devices

 Technology preview

Filter by status ▾

Labels and fleets ▾












Add devices

Decommission devices



Show only decommissioned devices

<input type="checkbox"/>	Alias	Name	Fleet	Applicati...	Device s...	Update status...	Last seen
<input type="checkbox"/>	edge-device-flightctl	4sa99m...snu1lf0	None 	 Healthy	 Online	 Up-to-date	1 minute ago 
<input type="checkbox"/>	edgy1	rf4pb9...stgar90	clickops-fleet	 Healthy	 Online	 Up-to-date	< 1 minute ago 

1 of 1 ▾



- Home >
- Search
- Infrastructure >
- Edge Management ▾
 - Fleets
 - Devices
 - Repositories
- Applications
- Governance
- Credentials

You are logged in as a temporary administrative user. Update the [cluster OAuth configuration](#) to allow others to log in.

Details

Url

<https://gitlab.fdh.nts-lab.eu/rhel-edge-device/flightctl-repo>

Status

✓ Accessible

Type

Git repository

Privacy

🔒 Public repository

Last transition

15 hours ago

Resource syncs ?

🔍 Search by name

Actions ▾

☐

Name

Path

Target re...

Status

Observed h...

☐

anwendertreffen-fleet

/anwendertreffen-fleet/fleet.yaml

main

✓ Synced

8f4d39b

⋮

[+ Add a resource sync](#)

Home >

Search

Infrastructure >

Edge Management ▾

Fleets

Devices

Repositories

Applications

Governance

Credentials

You are logged in as a temporary administrative user. Update the [cluster OAuth configuration](#) to allow others to log in.

[Fleets](#) > [clickops-fleet](#) > Edit fleet

Edit fleet

- 1 General info
- 2 **Device template**
- 3 Updates
- 4 Review and save

Application 1

Image ⓘ *

quay.fdh.ntsllab.eu/bootc/example-app:v1

Application name ⓘ

nginx-on-bootc

+ Add a variable

+ Add application

Tracked systemd services

Add service

☐ Register all MicroShift devices to ACM ⓘ

Next

Back

Cancel

Home

Search

Infrastructure

Clusters

Automation

Host inventory

Virtual machines

Edge Management

Fleets

Devices

Repositories

Applications

Governance

Credentials

Clusters

Cluster list Cluster sets Cluster pools Discovered clusters

Get started with Multicuster Hub

	15 more
Nodes	5
Add-ons	8
Creation date	25. Sept. 2024, 19:34

Name	us21qf5t7..s23nsv9s7f0doqh93g	
Namespace	us21qf5t7..s23nsv9s7f0doqh93g	
Status	Ready	
Infrastructure	Red Hat Device Edge	
Control plane type	Standalone	
Distribution version	MicroShift 4.18.2	
Labels	microshiftVersion=4.18.2	
	10 more	
Nodes	1	
Add-ons	1 6	
Creation date	7. Mai 2025, 20:14	

Edit fleet

- 1 General info
- 2 Device template
- 3 Updates
- 4 Review and save

Update timeout ? *

Timeout devices that fail to update after minutes.

▼ Batch 1 ⊖

Select devices using labels

[Add label](#)

Select a subset using

%

Success threshold ? *

If % of the batch devices pass the success threshold, move to next batch or the rest of fleet's devices.

[+ Add batch](#)

☐ Set disruption budget ?

Next

Back

Cancel

☒ Set disruption budget [?](#)

Group devices by label keys [?](#)

[Add label key](#)

Use only the 'key' part of the labels to group same values.

Leaving this empty will apply the disruption budget to all fleet's devices.

Minimum number of available devices [?](#)

−		+
---	--	---

Maximum number of unavailable devices [?](#)

−		+
---	--	---

Q&A