

7 июня 2023 📍 Москва, МЦК ЗИЛ

# БЕКОН<sup>23</sup>

Первая в России конференция  
по БЕзопасности КОНтейнеров и контейнерных сред

## ОС Talos Linux – путь к “тому самому” харденингу инфраструктуры для k8s

Николай Панченко

Тинькофф





Скачать  
Презентацию



# Панченко Николай

Ведущий специалист ИБ

Специализация – K8s



**TINKOFF**

nickrzaion@gmail.com

n.s.panchenko@tinkoff.ru



Telegram: @yours\_rage

# План

1. Общая информация о Talos Linux
2. Архитектура Talos Linux
3. Харденинг Talos Linux
4. Сравнение Talos Linux с другими OS
5. Рекомендации при переходе на Talos Linux
6. Вопросы =)



# Общая информация о Talos Linux



# Talos Linux

-----

это дистрибутив Linux,  
оптимизированный под работу  
с контейнерными нагрузками



**The Kubernetes Operating System**

# Talos Linux

-----

это дистрибутив Linux,  
оптимизированный под работу  
с контейнерными нагрузками



Текущая версия 1.4

Поддерживает версии k8s 1.25-1.27

**The Kubernetes Operating System**

# Talos Linux



**The Kubernetes Operating System**

-----

это дистрибутив Linux,  
оптимизированный под работу  
с контейнерными нагрузками

Текущая версия 1.4

Поддерживает версии k8s 1.25-1.27



## Кредо

«Имея меньшее,  
предлагай большее».



# Talos Linux



**The Kubernetes Operating System**

-----

это дистрибутив Linux,  
оптимизированный под работу  
с контейнерными нагрузками

Текущая версия 1.4

Поддерживает версии k8s 1.25-1.27



## Кредо

«Имея меньшее,  
предлагай большее».



## 4 кита OS:

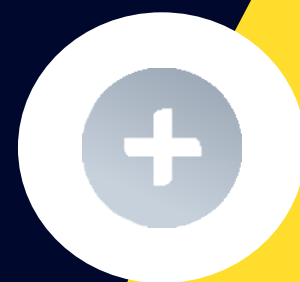
- Безопасность
- Эффективность
- Минимальность
- Стабильность



# Основные идеи Talos Linux



# Основные идеи Talos Linux



Максимально уменьшить  
поверхность атаки.

# Основные идеи Talos Linux



Максимально уменьшить  
поверхность атаки.



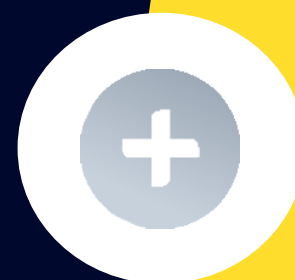
Перейти к неизменяемой  
(иммутабельной)  
инфраструктуре.



# Основные идеи Talos Linux



Максимально уменьшить поверхность атаки.



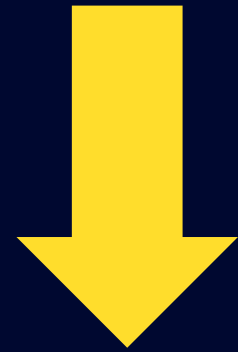
Перейти к неизменяемой (иммутабельной) инфраструктуре.



Сохранить максимальную эффективность и удобность работы с K8s.

# Используем ли мы Talos Linux в Тинькофф?

# Используем ли мы Talos Linux в Тинькофф?



## ДА



# Используем ли мы Talos Linux в Тинькофф?



## ДА



## Почему?

# Talos Linux – Основные преимущества

## 01

### Иммутабельность

неизменяемый состав OS  
после развертывания,  
конфигурация во  
временной директории

# Talos Linux – Основные преимущества

01

## Иммутабельность

неизменяемый состав OS  
после развертывания,  
конфигурация во  
временной директории

02

## Безопасность

Изначально создавалась  
для повышения  
безопасности  
контейнерных сред



# Talos Linux – Основные преимущества

01

## Иммутабельность

неизменяемый состав OS  
после развертывания,  
конфигурация во  
временной директории

02

## Безопасность

Изначально создавалась  
для повышения  
безопасности  
контейнерных сред

03

## Минимализм

минимальный набор  
компонентов для работы k8s,  
размер образа OS ~80Мб

# Talos Linux – Основные преимущества

01

## Иммутабельность

неизменяемый состав OS  
после развертывания,  
конфигурация во  
временной директории

02

## Безопасность

Изначально создавалась  
для повышения  
безопасности  
контейнерных сред

03

## Минимализм

минимальный набор  
компонентов для работы k8s,  
размер образа OS ~80Мб

04

## Только API

Есть только одна  
внешняя “ручка” управления,  
доступная по протоколу gRPCS

# Talos Linux – Основные преимущества

01

## Иммутабельность

неизменяемый состав OS  
после развертывания,  
конфигурация во  
временной директории

02

## Безопасность

Изначально создавалась  
для повышения  
безопасности  
контейнерных сред

03

## Минимализм

минимальный набор  
компонентов для работы k8s,  
размер образа OS ~80Мб

04

## Только API

Есть только одна  
внешняя “ручка” управления,  
доступная по протоколу gRPCS

05

## Версионность

Для каждой новой версии  
OS поддержка только трех  
последних версий k8s



# Talos Linux – Основные преимущества

01

## Иммутабельность

неизменяемый состав OS  
после развертывания,  
конфигурация во  
временной директории

02

## Безопасность

Изначально создавалась  
для повышения  
безопасности  
контейнерных сред

03

## Минимализм

минимальный набор  
компонентов для работы k8s,  
размер образа OS ~80Мб

04

## Только API

Есть только одна  
внешняя “ручка” управления,  
доступная по протоколу gRPCS

05

## Версионность

Для каждой новой версии  
OS поддержка только трех  
последних версий k8s

06

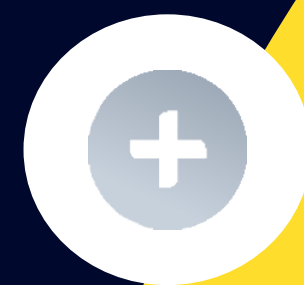
## Архитектура

Понятность взаимодействия  
компонентов и возможность  
дорабатывать под свои задачи

И все же,  
Почему?

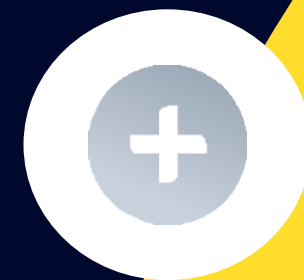


**И все же,  
Почему?**

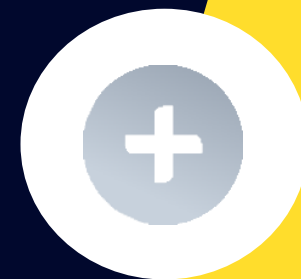


Нам нужна была безопасность –  
мы полезли в иммутабельность  
и максимальный харденинг

# И все же, Почему?



Нам нужна была безопасность –  
мы полезли в иммутабельность  
и максимальный харденинг



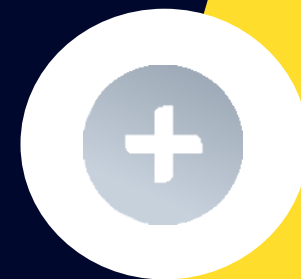
Мы хотели запретить шелл на ноду



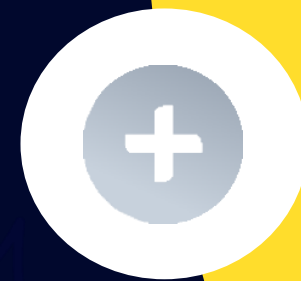
# И все же, Почему?



Нам нужна была безопасность –  
мы полезли в иммутабельность  
и максимальный харденинг



Мы хотели запретить шелл на ноду

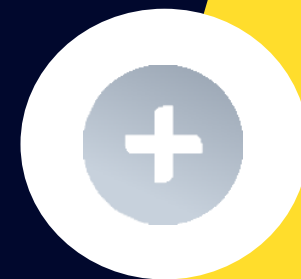


Мы хотели кубер на железе

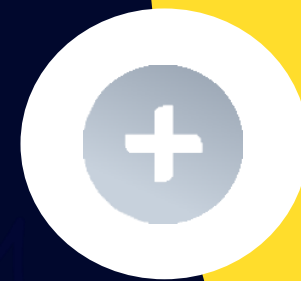
# И все же, Почему?



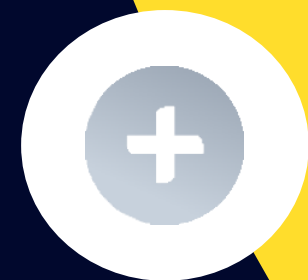
Нам нужна была безопасность – мы полезли в иммутабельность и максимальный харденинг



Мы хотели запретить шелл на ноду



Мы хотели кубер на железе



Мы были готовы дописывать компоненты, если потребуется

# Поддержка развертывания Talos Linux

**контейнер**



В основном  
используется  
для тестов

**облако**



Доступны как  
публичные,  
так и частные  
облака

**VM**



Поддержка  
развертывания  
на популярных  
системах  
виртуализации

**Железо**



Поддержка  
развертывания  
на железе через  
Sidero и  
ClusterAPI

# Требования к ресурсам для запуска

## Minimum Requirements

Role	Memory	Cores	System Disk
Control Plane	2 GiB	2	10 GiB
Worker	1 GiB	1	10 GiB

## Recommended

Role	Memory	Cores	System Disk
Control Plane	4 GiB	4	100 GiB
Worker	2 GiB	2	100 GiB

\*Сопоставимо с требованиями для развертывания k8s





# Архитектура Talos Linux

# Архитектура Talos Linux

За основу взяты идеи из OS Gentoo

# Архитектура Talos Linux

За основу взяты идеи из OS Gentoo

Распространяется как самодостаточный образ

# Архитектура Talos Linux

За основу взяты идеи из OS Gentoo

Распространяется как самодостаточный образ

версионизуемый



Для каждой новой версии  
Talos Linux есть  
поддержка только 3-х  
последних версий k8s

Например:

OS v1.3 -> k8s v1.24-1.26

# Архитектура Talos Linux

За основу взяты идеи из OS Gentoo

Распространяется как самодостаточный образ

версионированный



Для каждой новой версии  
Talos Linux есть  
поддержка только 3-х  
последних версий k8s

Например:

OS v1.3 -> k8s v1.24-1.26

подписанный



Образ и каждый  
компонент архитектуры  
изначально подписаны  
Cydero Labs



# Архитектура Talos Linux

За основу взяты идеи из OS Gentoo

Распространяется как самодостаточный образ

версионированный



Для каждой новой версии  
Talos Linux есть  
поддержка только 3-х  
последних версий k8s

Например:

OS v1.3 -> k8s v1.24-1.26

подписанный



Образ и каждый  
компонент архитектуры  
изначально подписаны  
Cydero Labs

неизменяемый



Образ собран с read-only  
файловой системой для  
обеспечения  
иммутабельности

# Архитектура Talos Linux

Talos Linux использует принцип модульности:  
модули связываются между собой по gRPCS

# Архитектура Talos Linux

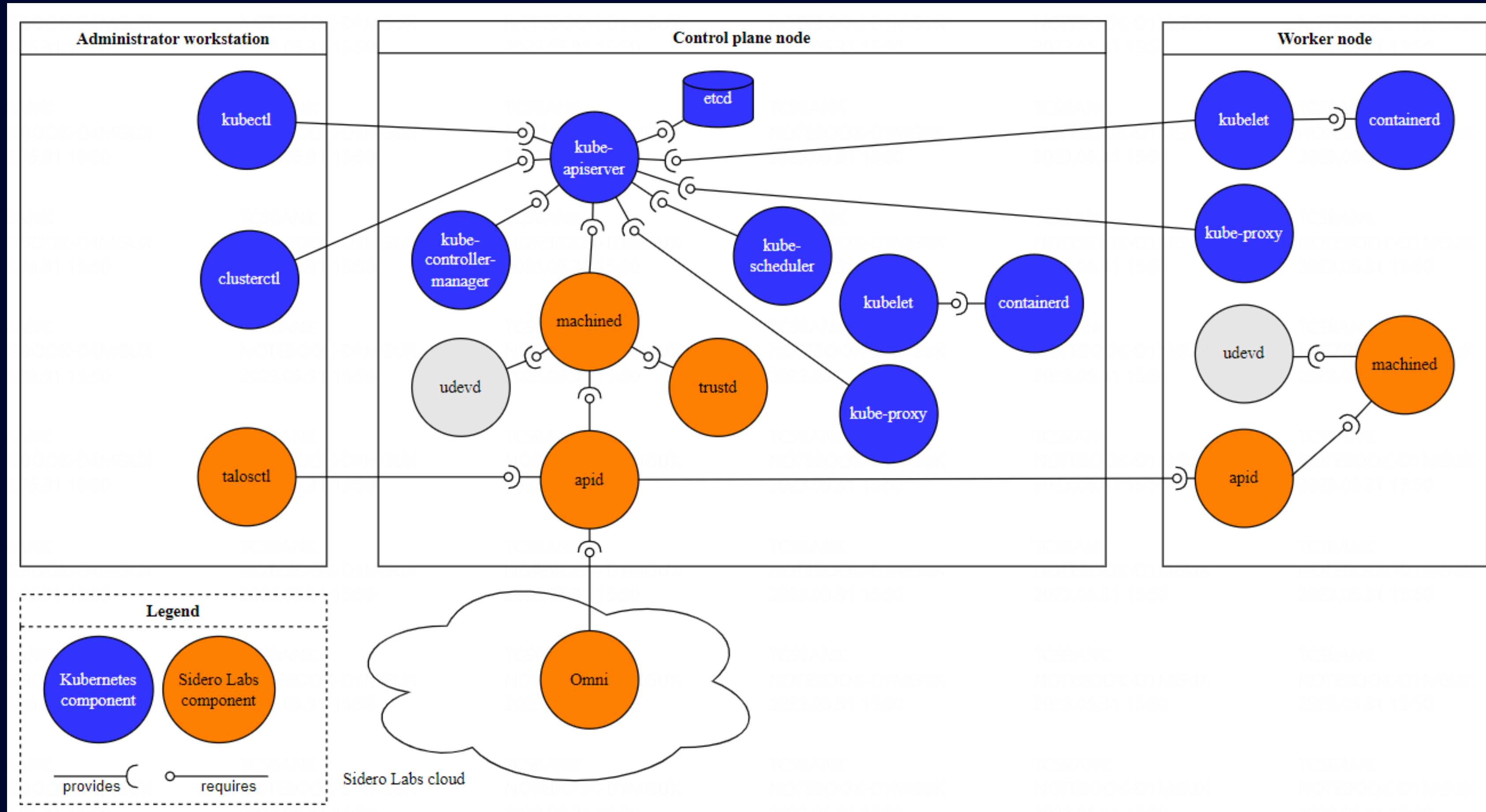
Talos Linux использует принцип модульности:  
модули связываются между собой по gRPCS



Это обеспечивает:

- Гарантированную доставку данных между модулями
- Удобность модификации их взаимодействия от версии к версии
- Возможность доработки архитектуры под свои задачи

# Архитектура Talos Linux



# Talos Linux - процессы

```
-talosctl2:~/configs$ talosctl service
```

SERVICE	STATE	HEALTH	LAST CHANGE	LAST EVENT
apid	Running	OK	1283h37m45s ago	Health check successful
containerd	Running	OK	1283h37m51s ago	Health check successful
cri	Running	OK	1283h37m49s ago	Health check successful
etcd	Running	OK	1283h37m44s ago	Health check successful
kubelet	Running	OK	1283h37m42s ago	Health check successful
machined	Running	OK	1283h37m52s ago	Health check successful
trustd	Running	OK	1283h37m49s ago	Health check successful
udev	Running	OK	1283h37m51s ago	Health check successful



# Talos Linux - процессы

```
-talosctl2:~/configs$ talosctl service
```

SERVICE	STATE	HEALTH	LAST CHANGE	LAST EVENT
apid	Running	OK	1283h37m45s ago	Health check successful
containerd	Running	OK	1283h37m51s ago	Health check successful
cri	Running	OK	1283h37m49s ago	Health check successful
etcd	Running	OK	1283h37m44s ago	Health check successful
kubelet	Running	OK	1283h37m42s ago	Health check successful
machined	Running	OK	1283h37m52s ago	Health check successful
trustd	Running	OK	1283h37m49s ago	Health check successful
udev	Running	OK	1283h37m51s ago	Health check successful

```
-talosctl2:~/configs$ talosctl containers -k
```

NAMESPACE	ID
k8s.io	kube-system/cilium-dd9z4
k8s.io	└ kube-system/cilium-dd9z4:apply-sysctl-overwrites
k8s.io	└ kube-system/cilium-dd9z4:cilium-agent
k8s.io	└ kube-system/cilium-dd9z4:clean-cilium-state
k8s.io	└ kube-system/cilium-dd9z4:config
k8s.io	└ kube-system/cilium-dd9z4:install-cni-binaries
k8s.io	└ kube-system/cilium-dd9z4:mount-cgroup
k8s.io	kube-system/cilium-operator-8549c9f485-drwms
k8s.io	└ kube-system/cilium-operator-8549c9f485-drwms:cilium-operator
k8s.io	kube-system/coredns-fdddbdf46-mlhkg
k8s.io	└ kube-system/coredns-fdddbdf46-mlhkg:coredns
k8s.io	kube-system/coredns-fdddbdf46-ql6xz
k8s.io	└ kube-system/coredns-fdddbdf46-ql6xz:coredns
k8s.io	kube-system/kube-apiserver-talos-master
k8s.io	└ kube-system/kube-apiserver-talos-master:kube-apiserver
k8s.io	kube-system/kube-controller-manager-talos-master
k8s.io	└ kube-system/kube-controller-manager-talos-master:kube-controller-manager
k8s.io	└ kube-system/kube-controller-manager-talos-master:kube-controller-manager
k8s.io	kube-system/kube-scheduler-talos-master
k8s.io	└ kube-system/kube-scheduler-talos-master:kube-scheduler
k8s.io	└ kube-system/kube-scheduler-talos-master:kube-scheduler

```
-talosctl2:~/configs$ talosctl containers
```

NAMESPACE	ID	IMAGE	PID	STATUS
system	apid		1504	RUNNING
system	trustd		1505	RUNNING

# Talos Linux - процессы

```
-talosctl2:~/configs$ talosctl service
```

SERVICE	STATE	HEALTH	LAST CHANGE	LAST EVENT
apid	Running	OK	1283h37m45s ago	Health check successful
containerd	Running	OK	1283h37m51s ago	Health check successful
cri	Running	OK	1283h37m49s ago	Health check successful
etcd	Running	OK	1283h37m44s ago	Health check successful
kubelet	Running	OK	1283h37m42s ago	Health check successful
machined	Running	OK	1283h37m52s ago	Health check successful
trustd	Running	OK	1283h37m49s ago	Health check successful
udev	Running	OK	1283h37m51s ago	Health check successful

```
-talosctl2:~/configs$ talosctl containers -k
```

NAMESPACE	ID
k8s.io	kube-system/cilium-dd9z4
k8s.io	└ kube-system/cilium-dd9z4:apply-sysctl-overwrites
k8s.io	└ kube-system/cilium-dd9z4:cilium-agent
k8s.io	└ kube-system/cilium-dd9z4:clean-cilium-state
k8s.io	└ kube-system/cilium-dd9z4:config
k8s.io	└ kube-system/cilium-dd9z4:install-cni-binaries
k8s.io	└ kube-system/cilium-dd9z4:mount-cgroup
k8s.io	kube-system/cilium-operator-8549c9f485-drwms
k8s.io	└ kube-system/cilium-operator-8549c9f485-drwms:cilium-operator
k8s.io	kube-system/coredns-fdddbdf46-mlhkg
k8s.io	└ kube-system/coredns-fdddbdf46-mlhkg:coredns
k8s.io	kube-system/coredns-fdddbdf46-ql6xz
k8s.io	└ kube-system/coredns-fdddbdf46-ql6xz:coredns
k8s.io	kube-system/kube-apiserver-talos-master
k8s.io	└ kube-system/kube-apiserver-talos-master:kube-apiserver
k8s.io	kube-system/kube-controller-manager-talos-master
k8s.io	└ kube-system/kube-controller-manager-talos-master:kube-controller-manager
k8s.io	└ kube-system/kube-controller-manager-talos-master:kube-controller-manager
k8s.io	kube-system/kube-scheduler-talos-master
k8s.io	└ kube-system/kube-scheduler-talos-master:kube-scheduler
k8s.io	└ kube-system/kube-scheduler-talos-master:kube-scheduler

```
-talosctl2:~/configs$ talosctl containers
```

NAMESPACE	ID	IMAGE	PID	STATUS
system	apid		1504	RUNNING
system	trustd		1505	RUNNING

```
ubuntu@ubuntu-talosctl2:~/configs$ talosctl health
```

```
discovered nodes: ["10.0.0.152" "10.0.1.86"]
waiting for etcd to be healthy: ...
waiting for etcd to be healthy: OK
waiting for etcd members to be consistent across nodes: ...
waiting for etcd members to be consistent across nodes: OK
waiting for etcd members to be control plane nodes: ...
waiting for etcd members to be control plane nodes: OK
waiting for apid to be ready: ...
waiting for apid to be ready: OK
waiting for all nodes memory sizes: ...
waiting for all nodes memory sizes: OK
waiting for all nodes disk sizes: ...
waiting for all nodes disk sizes: OK
waiting for kubelet to be healthy: ...
waiting for kubelet to be healthy: OK
waiting for all nodes to finish boot sequence: ...
waiting for all nodes to finish boot sequence: OK
waiting for all k8s nodes to report: ...
waiting for all k8s nodes to report: OK
waiting for all k8s nodes to report ready: ...
waiting for all k8s nodes to report ready: OK
waiting for all control plane static pods to be running: ...
waiting for all control plane static pods to be running: OK
waiting for all control plane components to be ready: ...
waiting for all control plane components to be ready: OK
waiting for kube-proxy to report ready: ...
waiting for kube-proxy to report ready: SKIP
waiting for coredns to report ready: ...
waiting for coredns to report ready: OK
waiting for all k8s nodes to report schedulable: ...
waiting for all k8s nodes to report schedulable: OK
```

# Talos Linux – разделы

## EFI

Хранит загрузочные  
данные EFI

# Talos Linux – разделы

## EFI

Хранит загрузочные  
данные EFI

## BIOS

Используется для стадии  
загрузки Grub

# Talos Linux – разделы

## EFI

Хранит загрузочные  
данные EFI

## BIOS

Используется для стадии  
загрузки Grub

## BOOT

Используется загрузчиком,  
хранит initramfs и ядро

# Talos Linux – разделы

## EFI

Хранит загрузочные  
данные EFI

## BIOS

Используется для стадии  
загрузки Grub

## BOOT

Используется загрузчиком,  
хранит initramfs и ядро

## МЕТА

Хранит метаданные  
ноды Talos Linux,  
например ID ноды



# Talos Linux – разделы

## EFI

Хранит загрузочные данные EFI

## BIOS

Используется для стадии загрузки Grub

## BOOT

Используется загрузчиком, хранит initramfs и ядро

## МЕТА

Хранит метаданные ноды Talos Linux, например ID ноды

## STATE

Хранит настройки машины, информацию для определения роли машины в кластере и KubeSpan info

# Talos Linux – разделы

## EFI

Хранит загрузочные данные EFI

## BIOS

Используется для стадии загрузки Grub

## BOOT

Используется загрузчиком, хранит initramfs и ядро

## META

Хранит метаданные ноды Talos Linux, например ID ноды

## STATE

Хранит настройки машины, информацию для определения роли машины в кластере и KubeSpan info

## EPHEMERAL

Хранит временную информацию, смонтированную в /var, например данные созданного кластера

# Talos Linux – работа с файловой системой

# Talos Linux – работа с файловой системой

read-only



Для всего кроме  
/system и /var

# Talos Linux – работа с файловой системой

read-only



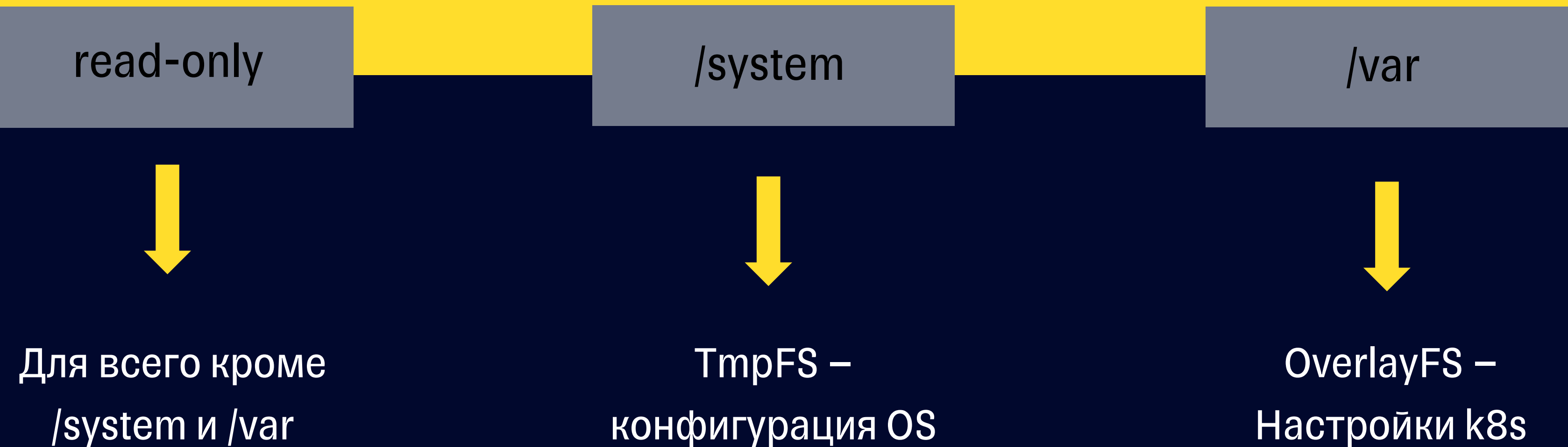
Для всего кроме  
/system и /var

/system



TmpFS –  
конфигурация OS

# Talos Linux – работа с файловой системой





# Talos Linux – файловая система

```
ubuntu@ubuntu-talosctl2:~/configs$ talosctl cat /etc/os-release

NAME="Talos"
ID=talos
VERSION_ID=v1.3.7
PRETTY_NAME="Talos (v1.3.7)"
HOME_URL="https://www.talos.dev/"
BUG_REPORT_URL="https://github.com/siderolabs/talos/issues"
ubuntu@ubuntu-talosctl2:~/configs$ talosctl cat /etc/machine-id ; echo
9b3f67b6d77a331410f6284a7534d4d9
```

# Talos Linux – файловая система

```
ubuntu@ubuntu-talosctl2:~/configs$ talosctl cat /etc/os-release

NAME="Talos"
ID=talos
VERSION_ID=v1.3.7
PRETTY_NAME="Talos (v1.3.7)"
HOME_URL="https://www.talos.dev/"
BUG_REPORT_URL="https://github.com/siderolabs/talos/issues"
ubuntu@ubuntu-talosctl2:~/configs$ talosctl cat /etc/machine-id ; echo
9b3f67b6d77a331410f6284a7534d4d9
```

```
ubuntu@ubuntu-talosctl2:~/configs$ talosctl ls /system/state/
NAME
.
config.yaml
node-identity.yaml
platform-network.yaml
ubuntu@ubuntu-talosctl2:~/configs$ talosctl ls /system/config/
NAME
.
kubernetes
ubuntu@ubuntu-talosctl2:~/configs$ talosctl ls /system/config/kubernetes/kube-apiserver
NAME
.
admission-control-config.yaml
auditpolicy.yaml
```

# Talos Linux – файловая система

```
ubuntu@ubuntu-talosctl2:~/configs$ talosctl cat /etc/os-release

NAME="Talos"
ID=talos
VERSION_ID=v1.3.7
PRETTY_NAME="Talos (v1.3.7)"
HOME_URL="https://www.talos.dev/"
BUG_REPORT_URL="https://github.com/siderolabs/talos/issues"
ubuntu@ubuntu-talosctl2:~/configs$ talosctl cat /etc/machine-id ; echo
9b3f67b6d77a331410f6284a7534d4d9
```

```
-talosctl2:~/configs$ talosctl ls /system/state/
NAME
.
config.yaml
node-identity.yaml
platform-network.yaml
-talosctl2:~/configs$ talosctl ls /system/config/
NAME
.
kubernetes
-talosctl2:~/configs$ talosctl ls /system/config/kubernetes/kube-apiserver
NAME
.
admission-control-config.yaml
auditpolicy.yaml
```

# Talos Linux – файловая система

```
ubuntu@ubuntu-talosctl2:~/configs$ talosctl cat /etc/os-release

NAME="Talos"
ID=talos
VERSION_ID=v1.3.7
PRETTY_NAME="Talos (v1.3.7)"
HOME_URL="https://www.talos.dev/"
BUG_REPORT_URL="https://github.com/siderolabs/talos/issues"
ubuntu@ubuntu-talosctl2:~/configs$ talosctl cat /etc/machine-id ; echo
9b3f67b6d77a331410f6284a7534d4d9
```

```
-talosctl2:~/configs$ talosctl ls /system/state/
NAME
.
config.yaml
node-identity.yaml
platform-network.yaml
-talosctl2:~/configs$ talosctl ls /system/config/
NAME
.
kubernetes
-talosctl2:~/configs$ talosctl ls /system/config/kubernetes/kube-apiserver
NAME
.
admission-control-config.yaml
auditpolicy.yaml
```

```
-talosctl2:~/configs$ talosctl ls /var/system/overlays
NAME
.
etc-cni-diff
etc-cni-workdir
etc-kubernetes-diff
etc-kubernetes-workdir
opt-diff
opt-workdir
usr-etc-udev-diff
usr-etc-udev-workdir
usr-libexec-kubernetes-diff
usr-libexec-kubernetes-workdir
-talosctl2:~/configs$ talosctl ls /var/log
NAME
.
audit
containers
pods
-talosctl2:~/configs$ talosctl ls /var/run
NAME
.
cilium
lock
netns
```

# Talos Linux – файловая система

```
ubuntu@ubuntu-talosctl2:~/configs$ talosctl cat /etc/os-release

NAME="Talos"
ID=talos
VERSION_ID=v1.3.7
PRETTY_NAME="Talos (v1.3.7)"
HOME_URL="https://www.talos.dev/"
BUG_REPORT_URL="https://github.com/siderolabs/talos/issues"
ubuntu@ubuntu-talosctl2:~/configs$ talosctl cat /etc/machine-id ; echo
9b3f67b6d77a331410f6284a7534d4d9
```

```
-talosctl2:~/configs$ talosctl ls /system/state/
NAME
.
config.yaml
node-identity.yaml
platform-network.yaml
-talosctl2:~/configs$ talosctl ls /system/config/
NAME
.
kubernetes
-talosctl2:~/configs$ talosctl ls /system/config/kubernetes/kube-apiserver
NAME
.
admission-control-config.yaml
auditpolicy.yaml
```

```
-talosctl2:~/configs$ talosctl ls /var/system/overlays
NAME
.
etc-cni-diff
etc-cni-workdir
etc-kubernetes-diff
etc-kubernetes-workdir
opt-diff
opt-workdir
usr-etc-udev-diff
usr-etc-udev-workdir
usr-libexec-kubernetes-diff
usr-libexec-kubernetes-workdir
-talosctl2:~/configs$ talosctl ls /var/log
NAME
.
audit
containers
pods
-talosctl2:~/configs$ talosctl ls /var/run
NAME
.
cilium
lock
netns
```

# Talos Linux – logs

```
talosctl2:~/configs$ talosctl ls /var/log/audit/kube
NAME
.
kube-apiserver-2023-06-05T00-04-39.111.log
kube-apiserver-2023-06-05T02-34-24.669.log
kube-apiserver-2023-06-05T05-04-11.017.log
kube-apiserver-2023-06-05T07-33-56.064.log
kube-apiserver-2023-06-05T10-03-46.692.log
kube-apiserver-2023-06-05T12-33-27.606.log
kube-apiserver-2023-06-05T15-03-06.783.log
kube-apiserver-2023-06-05T17-32-57.132.log
kube-apiserver-2023-06-05T20-02-32.592.log
kube-apiserver-2023-06-05T22-32-22.112.log
kube-apiserver.log
```

# Talos Linux – logs

```
talosctl2:~/configs$ talosctl ls /var/log/audit/kube
NAME
-
kube-apiserver-2023-06-05T00-04-39.111.log
kube-apiserver-2023-06-05T02-34-24.669.log
kube-apiserver-2023-06-05T05-04-11.017.log
kube-apiserver-2023-06-05T07-33-56.064.log
kube-apiserver-2023-06-05T10-03-46.692.log
kube-apiserver-2023-06-05T12-33-27.606.log
kube-apiserver-2023-06-05T15-03-06.783.log
kube-apiserver-2023-06-05T17-32-57.132.log
kube-apiserver-2023-06-05T20-02-32.592.log
kube-apiserver-2023-06-05T22-32-22.112.log
kube-apiserver.log
```

```
talosctl2:~/configs$ talosctl ls /var/log/containers
NAME
-
cilium-dd9z4_kube-system_apply-sysctl-overwrites-fdab64e591b4856235ed4b8b61743bc726fe9cfb265900b7a931b606888c3890.log
cilium-dd9z4_kube-system_cilium-agent-c22a82044ffe9f86b9b83874f2590b8b93dbcd9012af9ec9c4c0e25c1ad50c84.log
cilium-dd9z4_kube-system_clean-cilium-state-e3666cc5bcd131c7220ac46837737c32325b052befd59422475798fb01f31cf6.log
cilium-dd9z4_kube-system_config-e29bb79872f1e551dd50662fde4e2bb1965dca6b09aa9fbcaafe3b7a7937cea3.log
cilium-dd9z4_kube-system_install-cni-binaries-b3de9dd95c016ea5667eeb6513ef009684a617e94da835cb03228ff446121803.log
cilium-dd9z4_kube-system_mount-cgroup-20a3f1bd546ca2e82e426b4922e2190a0f4d3c14ffa62ddbda55d09e580c1324.log
cilium-operator-8549c9f485-drwms_kube-system_cilium-operator-55429d412a448366ee890b9127f45c60bd04efb8e543fe6ec5255d098b4fa7ff.log
coredns-fdddbdf46-mlhkg_kube-system_coredns-bc5fab352b85b12d8c01ec78f9efd713bbd2417effcda64442414f505386800e.log
coredns-fdddbdf46-ql6xz_kube-system_coredns-6198cb31bf000a42db7b097d7de6be88d4144cbbda5cc9b813404f914df533f8.log
kube-apiserver-talos-master_kube-system_kube-apiserver-81172e20c947cbc00d219436b82fe2ac43703dfdea0bb16b7426f40b527b0919.log
kube-controller-manager-talos-master_kube-system_kube-controller-manager-2db144e3883d30d1fbb3995ed07d3483dabce734a2d8f8dea93df8be5e60ab47.log
kube-controller-manager-talos-master_kube-system_kube-controller-manager-81534e1937b232d4c1d4b567c333ecf9d178a0ec85e07aa4784a8a82287d770c.log
kube-scheduler-talos-master_kube-system_kube-scheduler-34395c3f49b07d246e64b39e392a5c4bd5797219355a5b09464d87d654cf8d4f.log
kube-scheduler-talos-master_kube-system_kube-scheduler-96e58ef0edb360cea78365c28470e7145c6e65e842d27609c27625d58489ddd4.log
```



# Talos Linux – logs

```
talosctl2:~/configs$ talosctl ls /var/log/audit/kube
NAME
*
kube-apiserver-2023-06-05T00-04-39.111.log
kube-apiserver-2023-06-05T02-34-24.669.log
kube-apiserver-2023-06-05T05-04-11.017.log
kube-apiserver-2023-06-05T07-33-56.064.log
kube-apiserver-2023-06-05T10-03-46.692.log
kube-apiserver-2023-06-05T12-33-27.606.log
kube-apiserver-2023-06-05T15-03-06.783.log
kube-apiserver-2023-06-05T17-32-57.132.log
kube-apiserver-2023-06-05T20-02-32.592.log
kube-apiserver-2023-06-05T22-32-22.112.log
kube-apiserver.log
```

```
talosctl2:~/configs$ talosctl ls /var/log/containers
NAME
*
cilium-dd9z4_kube-system_apply-sysctl-overwrites-fdab64e591b4856235ed4b8b61743bc726fe9cfb265900b7a931b606888c3890.log
cilium-dd9z4_kube-system_cilium-agent-c22a82044ffe9f86b9b83874f2590b8b93dbcd9012af9ec9c4c0e25c1ad50c84.log
cilium-dd9z4_kube-system_clean-cilium-state-e3666cc5bcd131c7220ac46837737c32325b052befd59422475798fb01f31cf6.log
cilium-dd9z4_kube-system_config-e29bb79872f1e551dd50662fde4e2bb1965dca6b09aa9fbcaafe3b7a7937cea3.log
cilium-dd9z4_kube-system_install-cni-binaries-b3de9dd95c016ea5667eeb6513ef009684a617e94da835cb03228ff446121803.log
cilium-dd9z4_kube-system_mount-cgroup-20a3f1bd546ca2e82e426b4922e2190a0f4d3c14ffa62ddbda55d09e580c1324.log
cilium-operator-8549c9f485-drwms_kube-system_cilium-operator-55429d412a448366ee890b9127f45c60bd04efb8e543fe6ec5255d098b4fa7ff.log
coredns-fdddbdf46-mlhkg_kube-system_coredns-bc5fab352b85b12d8c01ec78f9efd713bbd2417effcda64442414f505386800e.log
coredns-fdddbdf46-ql6xz_kube-system_coredns-6198cb31bf000a42db7b097d7de6be88d4144cbbda5cc9b813404f914df533f8.log
kube-apiserver-talos-master_kube-system_kube-apiserver-81172e20c947cbc00d219436b82fe2ac43703dfdea0bb16b7426f40b527b0919.log
kube-controller-manager-talos-master_kube-system_kube-controller-manager-2db144e3883d30d1fbb3995ed07d3483dabce734a2d8f8dea93df8be5e60ab47.log
kube-controller-manager-talos-master_kube-system_kube-controller-manager-81534e1937b232d4c1d4b567c333ecf9d178a0ec85e07aa4784a8a82287d770c.log
kube-scheduler-talos-master_kube-system_kube-scheduler-34395c3f49b07d246e64b39e392a5c4bd5797219355a5b09464d87d654cf8d4f.log
kube-scheduler-talos-master_kube-system_kube-scheduler-96e58ef0edb360cea78365c28470e7145c6e65e842d27609c27625d58489ddd4.log
```

```
talosctl2:~/configs$ talosctl dmesg
kern: notice: [2023-04-13T11:09:23.343645116Z]: Linux version 5.15.106-talos (@buildkitsandbox) (gcc (GCC) 12.2.0, GNU ld (GNU Binutils) 2.39) #1 SMP Wed Apr 5 15:23:01 UTC 2023
kern: info: [2023-04-13T11:09:23.343645116Z]: Command line: BOOT_IMAGE=/A/vmlinuz talos.platform=openstack console=tty1 console=ttyS0 init_on_alloc=1 slab_nomerge pti=on console
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: Supporting XSAVE feature 0x020: 'AVX-512 opmask'
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: Supporting XSAVE feature 0x040: 'AVX-512 Hi256'
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: Supporting XSAVE feature 0x080: 'AVX-512 ZMM_Hi256'
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: Supporting XSAVE feature 0x200: 'Protection Keys User registers'
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[2]: 576, xstate_sizes[2]: 256
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[5]: 832, xstate_sizes[5]: 64
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[10]: 1088, xstate_sizes[10]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[11]: 1216, xstate_sizes[11]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[12]: 1344, xstate_sizes[12]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[13]: 1472, xstate_sizes[13]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[14]: 1600, xstate_sizes[14]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[15]: 1728, xstate_sizes[15]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[16]: 1856, xstate_sizes[16]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[17]: 1984, xstate_sizes[17]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[18]: 2112, xstate_sizes[18]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[19]: 2240, xstate_sizes[19]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[20]: 2368, xstate_sizes[20]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[21]: 2496, xstate_sizes[21]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[22]: 2624, xstate_sizes[22]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[23]: 2752, xstate_sizes[23]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[24]: 2880, xstate_sizes[24]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[25]: 3008, xstate_sizes[25]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[26]: 3136, xstate_sizes[26]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[27]: 3264, xstate_sizes[27]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[28]: 3392, xstate_sizes[28]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[29]: 3520, xstate_sizes[29]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[30]: 3648, xstate_sizes[30]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[31]: 3776, xstate_sizes[31]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[32]: 3904, xstate_sizes[32]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[33]: 4032, xstate_sizes[33]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[34]: 4160, xstate_sizes[34]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[35]: 4288, xstate_sizes[35]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[36]: 4416, xstate_sizes[36]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[37]: 4544, xstate_sizes[37]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[38]: 4672, xstate_sizes[38]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[39]: 4800, xstate_sizes[39]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[40]: 4928, xstate_sizes[40]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[41]: 5056, xstate_sizes[41]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[42]: 5184, xstate_sizes[42]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[43]: 5312, xstate_sizes[43]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[44]: 5440, xstate_sizes[44]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[45]: 5568, xstate_sizes[45]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[46]: 5696, xstate_sizes[46]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[47]: 5824, xstate_sizes[47]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[48]: 5952, xstate_sizes[48]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[49]: 6080, xstate_sizes[49]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[50]: 6208, xstate_sizes[50]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[51]: 6336, xstate_sizes[51]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[52]: 6464, xstate_sizes[52]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[53]: 6592, xstate_sizes[53]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[54]: 6720, xstate_sizes[54]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[55]: 6848, xstate_sizes[55]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[56]: 6976, xstate_sizes[56]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[57]: 7104, xstate_sizes[57]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[58]: 7232, xstate_sizes[58]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[59]: 7360, xstate_sizes[59]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[60]: 7488, xstate_sizes[60]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[61]: 7616, xstate_sizes[61]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[62]: 7744, xstate_sizes[62]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[63]: 7872, xstate_sizes[63]: 128
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[64]: 7999, xstate_sizes[64]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[65]: 8126, xstate_sizes[65]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[66]: 8253, xstate_sizes[66]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[67]: 8380, xstate_sizes[67]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[68]: 8507, xstate_sizes[68]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[69]: 8634, xstate_sizes[69]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[70]: 8761, xstate_sizes[70]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[71]: 8888, xstate_sizes[71]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[72]: 9015, xstate_sizes[72]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[73]: 9142, xstate_sizes[73]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[74]: 9269, xstate_sizes[74]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[75]: 9396, xstate_sizes[75]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[76]: 9523, xstate_sizes[76]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[77]: 9650, xstate_sizes[77]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[78]: 9777, xstate_sizes[78]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[79]: 9904, xstate_sizes[79]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[80]: 10031, xstate_sizes[80]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[81]: 10158, xstate_sizes[81]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[82]: 10285, xstate_sizes[82]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[83]: 10412, xstate_sizes[83]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[84]: 10539, xstate_sizes[84]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[85]: 10666, xstate_sizes[85]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[86]: 10793, xstate_sizes[86]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[87]: 10920, xstate_sizes[87]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[88]: 11047, xstate_sizes[88]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[89]: 11174, xstate_sizes[89]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[90]: 11301, xstate_sizes[90]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[91]: 11428, xstate_sizes[91]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[92]: 11555, xstate_sizes[92]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[93]: 11682, xstate_sizes[93]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[94]: 11809, xstate_sizes[94]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[95]: 11936, xstate_sizes[95]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[96]: 12063, xstate_sizes[96]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[97]: 12190, xstate_sizes[97]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[98]: 12317, xstate_sizes[98]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[99]: 12444, xstate_sizes[99]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[100]: 12571, xstate_sizes[100]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[101]: 12698, xstate_sizes[101]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[102]: 12825, xstate_sizes[102]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[103]: 12952, xstate_sizes[103]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[104]: 13079, xstate_sizes[104]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[105]: 13206, xstate_sizes[105]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[106]: 13333, xstate_sizes[106]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[107]: 13460, xstate_sizes[107]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[108]: 13587, xstate_sizes[108]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[109]: 13714, xstate_sizes[109]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[110]: 13841, xstate_sizes[110]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[111]: 13968, xstate_sizes[111]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[112]: 14095, xstate_sizes[112]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[113]: 14222, xstate_sizes[113]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[114]: 14349, xstate_sizes[114]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[115]: 14476, xstate_sizes[115]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[116]: 14603, xstate_sizes[116]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[117]: 14730, xstate_sizes[117]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[118]: 14857, xstate_sizes[118]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[119]: 14984, xstate_sizes[119]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[120]: 15111, xstate_sizes[120]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[121]: 15238, xstate_sizes[121]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[122]: 15365, xstate_sizes[122]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[123]: 15492, xstate_sizes[123]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[124]: 15619, xstate_sizes[124]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[125]: 15746, xstate_sizes[125]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[126]: 15873, xstate_sizes[126]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[127]: 15999, xstate_sizes[127]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[128]: 16126, xstate_sizes[128]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[129]: 16253, xstate_sizes[129]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[130]: 16380, xstate_sizes[130]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[131]: 16507, xstate_sizes[131]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[132]: 16634, xstate_sizes[132]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[133]: 16761, xstate_sizes[133]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[134]: 16888, xstate_sizes[134]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[135]: 17015, xstate_sizes[135]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[136]: 17142, xstate_sizes[136]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[137]: 17269, xstate_sizes[137]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[138]: 17396, xstate_sizes[138]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[139]: 17523, xstate_sizes[139]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[140]: 17650, xstate_sizes[140]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[141]: 17777, xstate_sizes[141]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[142]: 17904, xstate_sizes[142]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[143]: 18031, xstate_sizes[143]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[144]: 18158, xstate_sizes[144]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[145]: 18285, xstate_sizes[145]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[146]: 18412, xstate_sizes[146]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[147]: 18539, xstate_sizes[147]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[148]: 18666, xstate_sizes[148]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[149]: 18793, xstate_sizes[149]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[150]: 18920, xstate_sizes[150]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[151]: 19047, xstate_sizes[151]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[152]: 19174, xstate_sizes[152]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[153]: 19301, xstate_sizes[153]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[154]: 19428, xstate_sizes[154]: 127
kern: info: [2023-04-13T11:09:23.343645116Z]: x86/fpu: xstate_offset[155]: 1955
```

# Talos Linux - Dashboard



59

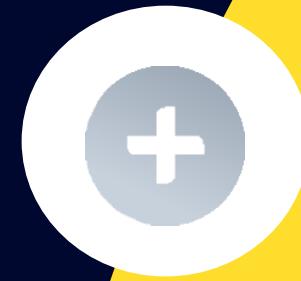


# Харденинг Talos Linux

# Харденинг

## 01

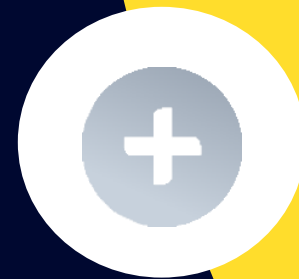
Развертывание всех машин с Talos Linux должно осуществляться только с подконтрольных серверов.



Контроль периметра



Уменьшение поверхности атаки



Доступ только у минимального количества администраторов

# Харденинг

02

**apid** должен запускаться с параметрами:

**--enable-rbac**

**--enable-ext-key-usage-check**



Включаем RBAC, появляется возможность понизить права подключения к **apid**



Включаем проверку ключа



Всегда проверяем параметры запуска **apid**



# Харденинг

## 03

При включенном **--enable-rbac** для **apid** роль **admin** должна быть минимизирована.



Понижаем права пользователей при подключении к **apid**



Доступ до мониторинга рекомендуется выдавать с пониженными правами, например с ролью **user**



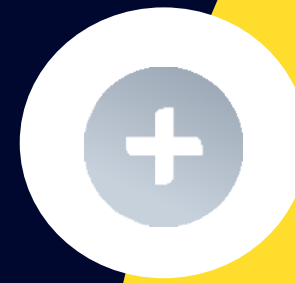
Всегда проверяем кому мы выдали роль **admin**

# Харденинг

## 04

Режим отладки в PROD окружении  
должен быть отключен:

**debug: false**



Убираем с PROD окружения  
возможность получения  
sensitive информации о работе  
ноды Talos Linux



Иногда для воспроизведения  
кейса нужен debug в PROD.  
Он может быть выдан на время,  
но для этого потребуется  
перезапуск ноды!  
Помните об этом!



# Харденинг



**.machine.ca** – свой  
сертификат на основе **CA**  
сертификата компании

**05**

Работа с сертификатами

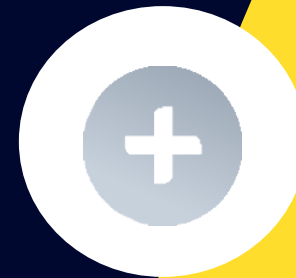
# Харденинг

05

Работа с сертификатами



**.machine.ca** – свой сертификат на основе **CA** сертификата компании



Сертификаты кластера **k8s** для секции **.cluster.ca** должны быть отличны от **.machine.ca**

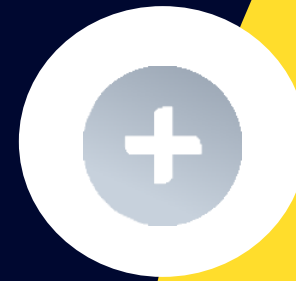
# Харденинг

05

Работа с сертификатами



**.machine.ca** – свой сертификат на основе **CA** сертификата компании



Сертификаты кластера **k8s** для секции **.cluster.ca** должны быть отличны от **.machine.ca**



Сертификаты должны генерироваться на стойких алгоритмах шифрования

# Харденинг

05

Работа с сертификатами



**.machine.ca** – свой сертификат на основе **CA** сертификата компании



Сертификаты кластера **k8s** для секции **.cluster.ca** должны быть отличны от **.machine.ca**



Сертификаты должны генерироваться на стойких алгоритмах шифрования



На каждую ноду должен быть добавлен Certificate Authority компании (в идеале – заменен)

# Харденинг

## 05

Работа с сертификатами



**.machine.ca** – свой сертификат на основе **CA** сертификата компании



Сертификаты кластера **k8s** для секции **.cluster.ca** должны быть отличны от **.machine.ca**



Сертификаты должны генерироваться на стойких алгоритмах шифрования



На каждую ноду должен быть добавлен Certificate Authority компании (в идеале – заменен)



На каждый кластер нужен свой пул сертификатов

# Talos system extensions

Talos system extension – это кастомно-собранный контейнерный образ,  
расширяющий возможности Talos Linux

# Talos system extensions

Talos system extension – это кастомно-собранный контейнерный образ,  
расширяющий возможности Talos Linux

У него:

- определённая структура директорий, потому что будет наложение на root файловую систему;
- фичи активируются только в процессе установки или обновления системы;
- после завершения установки всех extensions файловая система root будет иммутабельна (read-only)
- <https://github.com/siderolabs/extensions> – описание работы с системными расширениями Talos Linux

# Talos system extensions

Talos system extension – это кастомно-собранный контейнерный образ,  
расширяющий возможности Talos Linux

У него:

- определённая структура директорий, потому что будет наложение на root файловую систему;
- фичи активируются только в процессе установки или обновления системы;
- после завершения установки всех extensions файловая система root будет иммутабельна (read-only)
- <https://github.com/siderolabs/extensions> – описание работы с системными расширениями Talos Linux

machine:

install:

extensions:

- image: ghcr.io/siderolabs/gvisor:33f613e
- image: ghcr.io/siderolabs/nvidia-open-gpu-kernel-modules:530.41.03-v1.4.5
- image: ghcr.io/siderolabs/nvidia-container-toolkit:v1.5.0-alpha.0



# Talos Extensions - примеры

## Container Runtimes

Name	Image	Description	Version Format
<a href="#">gvisor</a>	<a href="#">ghcr.io/siderolabs/gvisor</a>	<a href="#">gVisor</a> container runtime	upstream version - talos version

## Firmware

Name	Image	Description	Version Format
<a href="#">amd-ucode</a>	<a href="#">ghcr.io/siderolabs/amd-ucode</a>	AMD CPU microcode updates	linux firmware version
<a href="#">i915-ucode</a>	<a href="#">ghcr.io/siderolabs/i915-ucode</a>	Intel GPU firmware	linux firmware version
<a href="#">bnx2-bnx2x</a>	<a href="#">ghcr.io/siderolabs/bnx2-bnx2x</a>	Broadcom NetXtreme firmware	linux firmware version
<a href="#">intel-ucode</a>	<a href="#">ghcr.io/siderolabs/intel-ucode</a>	Intel CPU microcode updates	upstream version

## Drivers

Name	Image	Description	Version Format
<a href="#">gasket</a>	<a href="#">ghcr.io/siderolabs/gasket-driver</a>	Driver for Google Coral PCIe devices	gasket driver upstream short commit - talos version
<a href="#">nvidia</a>	<a href="#">ghcr.io/siderolabs/nvidia-open-gpu-kernel-modules</a>	NVIDIA OSS Driver	nvidia driver upstream version - talos version

# Talos Extensions - примеры

## Storage

Name	Image	Description	Version Format
<a href="#">iscsi-tools</a>	<a href="#">ghcr.io/siderolabs/iscsi-tools</a>	Open iSCSI tools	<code>v0.1.0</code>
<a href="#">drbd disabled</a>	<a href="#">ghcr.io/siderolabs/drbd</a>	DRBD driver module	<code>v0.1.0</code>

## Power

Name	Image	Description	Version Format
<a href="#">nut-client</a>	<a href="#">ghcr.io/siderolabs/nut-client</a>	Network UPS Tools upsmon client	<code>upstream version - talos version</code>

## NVIDIA GPU

Name	Description	Version Format
<a href="#">nvidia-container-toolkit</a>	Tools to run <a href="#">NVIDIA GPU workloads</a> in containers	<code>driver version - toolkit version</code>
<a href="#">nvidia-fabricmanager</a>	<a href="#">NVIDIA fabric manager</a> support for GPU workloads	<code>driver version</code>
<a href="#">nvidia-open-gpu-kernel-modules</a>	NVIDIA driver kernel modules	<code>driver version - talos version</code>

# Безопасность Talos Extensions

## 06

Все новые самописные модули для Talos Linux должны подключаться с согласованием команды ИБ.

# Безопасность Talos Extensions

## 06

Все новые самописные модули для Talos Linux должны подключаться с согласованием команды ИБ.



Подключаемые расширения работают в privileged режиме

# Безопасность Talos Extensions

## 06

Все новые самописные модули для Talos Linux должны подключаться с согласованием команды ИБ.



Подключаемые расширения работают в privileged режиме



Они ложатся новым слоем при установке системы на файловую систему в **/root**


# Безопасность Talos Extensions

## 06


Все новые самописные модули для Talos Linux должны подключаться с согласованием команды ИБ.



Подключаемые расширения работают в privileged режиме



Они ложатся новым слоем при установке системы на файловую систему в **/root**



Да, **/root** после установки будет иммутабельна, но фича уже добавлена

# Безопасность Talos Extensions

## 06

Все новые самописные модули для Talos Linux должны подключаться с согласованием команды ИБ.



Подключаемые расширения работают в `privileged` режиме



Они ложатся новым слоем при установке системы на файловую систему в **`/root`**



Да, **`/root`** после установки будет иммутабельна, но фича уже добавлена



Валидации подписи нового расширения по умолчанию в Talos Linux нет!

# Безопасность Talos Extensions

## 06

Все новые самописные модули для Talos Linux должны подключаться с согласованием команды ИБ.

Вывод:

Командой ИБ должен быть организован процесс анализа системных расширений Talos Linux для обеспечения контроля безопасности экосистемной инфраструктуры.



Подключаемые расширения работают в privileged режиме



Они ложатся новым слоем при установке системы на файловую систему в **/root**



Да, **/root** после установки будет иммутабельна, но фича уже добавлена



Валидации подписи нового расширения по умолчанию в Talos Linux нет!





# Сравнение Talos Linux с другими OS

# Сравнительная таблица возможностей OS

Критерий	Ubuntu	Flatcar	Talos Linux
Иммутабельная	нет	да	да
Запуск на bare-metal	да	да	да
Размер серверного ISO-образа	~1.8Gb	353Mb	78,3Mb
Модификация логирования/debug туллинга	нет	нет	да
Работа с пакетными менеджерами	да	да/нет	нет
Классический интерактивный shell	да	да	нет
Динамически загружаемые модули	да	да	нет
Корневая директория с правами на запись	да	да	нет
Автоматические обновления (A-B)	нет	да	да
Многоуровневая изоляция работы k8s	нет	нет	да

# Сравнительная таблица возможностей OS

Критерий	Ubuntu	Flatcar	Talos Linux
Иммутабельная	нет	да	да
Запуск на bare-metal	да	да	да
Размер серверного ISO-образа	~1.8Gb	353Mb	78,3Mb
Модификация логирования/debug туллинга	нет	нет	да
Работа с пакетными менеджерами	да	да/нет	нет
Классический интерактивный shell	да	да	нет
Динамически загружаемые модули	да	да	нет
Корневая директория с правами на запись	да	да	нет
Автоматические обновления (A-B)	нет	да	да
Многоуровневая изоляция работы k8s	нет	нет	да

# Сравнительная таблица возможностей OS

Критерий	Ubuntu	Flatcar	Talos Linux
Иммутабельная	нет	да	да
Запуск на bare-metal	да	да	да
Размер серверного ISO-образа	~1.8Gb	353Mb	78,3Mb
Модификация логирования/debug туллинга	нет	нет	да
Работа с пакетными менеджерами	да	да/нет	нет
Классический интерактивный shell	да	да	нет
Динамически загружаемые модули	да	да	нет
Корневая директория с правами на запись	да	да	нет
Автоматические обновления (A-B)	нет	да	да
Многоуровневая изоляция работы k8s	нет	нет	да

# Сравнительная таблица возможностей OS

Критерий	Ubuntu	Flatcar	Talos Linux
Иммутабельная	нет	да	да
Запуск на bare-metal	да	да	да
Размер серверного ISO-образа	~1.8Gb	353Mb	78,3Mb
Модификация логирования/debug туллинга	нет	нет	да
Работа с пакетными менеджерами	да	да/нет	нет
Классический интерактивный shell	да	да	нет
Динамически загружаемые модули	да	да	нет
Корневая директория с правами на запись	да	да	нет
Автоматические обновления (A-B)	нет	да	да
Многоуровневая изоляция работы k8s	нет	нет	да

# Сравнительная таблица возможностей OS

Критерий	Ubuntu	Flatcar	Talos Linux
Иммутабельная	нет	да	да
Запуск на bare-metal	да	да	да
Размер серверного ISO-образа	~1.8Gb	353Mb	78,3Mb
Модификация логирования/debug туллинга	нет	нет	да
Работа с пакетными менеджерами	да	да/нет	нет
Классический интерактивный shell	да	да	нет
Динамически загружаемые модули	да	да	нет
Корневая директория с правами на запись	да	да	нет
Автоматические обновления (A-B)	нет	да	да
Многоуровневая изоляция работы k8s	нет	нет	да

# Сравнительная таблица возможностей OS

Критерий	Ubuntu	Flatcar	Talos Linux
Иммутабельная	нет	да	да
Запуск на bare-metal	да	да	да
Размер серверного ISO-образа	~1.8Gb	353Mb	78,3Mb
Модификация логирования/debug туллинга	нет	нет	да
Работа с пакетными менеджерами	да	да/нет	нет
Классический интерактивный shell	да	да	нет
Динамически загружаемые модули	да	да	нет
Корневая директория с правами на запись	да	да	нет
Автоматические обновления (A-B)	нет	да	да
Многоуровневая изоляция работы k8s	нет	нет	да

# Сравнительная таблица возможностей OS

Критерий	Ubuntu	Flatcar	Talos Linux
Иммутабельная	нет	да	да
Запуск на bare-metal	да	да	да
Размер серверного ISO-образа	~1.8Gb	353Mb	78,3Mb
Модификация логирования/debug туллинга	нет	нет	да
Работа с пакетными менеджерами	да	да/нет	нет
Классический интерактивный shell	да	да	нет
Динамически загружаемые модули	да	да	нет
Корневая директория с правами на запись	да	да	нет
Автоматические обновления (A-B)	нет	да	да
Многоуровневая изоляция работы k8s	нет	нет	да



# Сравнительная таблица возможностей OS

Критерий	Ubuntu	Flatcar	Talos Linux
Иммутабельная	нет	да	да
Запуск на bare-metal	да	да	да
Размер серверного ISO-образа	~1.8Gb	353Mb	78,3Mb
Модификация логирования/debug туллинга	нет	нет	да
Работа с пакетными менеджерами	да	да/нет	нет
Классический интерактивный shell	да	да	нет
Динамически загружаемые модули	да	да	нет
Корневая директория с правами на запись	да	да	нет
Автоматические обновления (A-B)	нет	да	да
Многоуровневая изоляция работы k8s	нет	нет	да

# Сравнительная таблица возможностей OS

Критерий	Ubuntu	Flatcar	Talos Linux
Иммутабельная	нет	да	да
Запуск на bare-metal	да	да	да
Размер серверного ISO-образа	~1.8Gb	353Mb	78,3Mb
Модификация логирования/debug туллинга	нет	нет	да
Работа с пакетными менеджерами	да	да/нет	нет
Классический интерактивный shell	да	да	нет
Динамически загружаемые модули	да	да	нет
Корневая директория с правами на запись	да	да	нет
Автоматические обновления (A-B)	нет	да	да
Многоуровневая изоляция работы k8s	нет	нет	да

# Сравнительная таблица возможностей OS

Критерий	Ubuntu	Flatcar	Talos Linux
Иммутабельная	нет	да	да
Запуск на bare-metal	да	да	да
Размер серверного ISO-образа	~1.8Gb	353Mb	78,3Mb
Модификация логирования/debug туллинга	нет	нет	да
Работа с пакетными менеджерами	да	да/нет	нет
Классический интерактивный shell	да	да	нет
Динамически загружаемые модули	да	да	нет
Корневая директория с правами на запись	да	да	нет
Автоматические обновления (A-B)	нет	да	да
Многоуровневая изоляция работы k8s	нет	нет	да

# Сравнительная таблица возможностей OS

Критерий	Ubuntu	Flatcar	Talos Linux
Иммутабельная	нет	да	да
Запуск на bare-metal	да	да	да
Размер серверного ISO-образа	~1.8Gb	353Mb	78,3Mb
Модификация логирования/debug туллинга	нет	нет	да
Работа с пакетными менеджерами	да	да/нет	нет
Классический интерактивный shell	да	да	нет
Динамически загружаемые модули	да	да	нет
Корневая директория с правами на запись	да	да	нет
Автоматические обновления (A-B)	нет	да	да
Многоуровневая изоляция работы k8s	нет	нет	да



# Рекомендации при переходе на Talos Linux

# Рекомендации при переходе на Talos Linux

## 01

Проанализируйте  
готовность Вашей текущей  
инфраструктуры к переходу  
в неизменяемый режим,  
«стоит ли игра свеч?»

# Рекомендации при переходе на Talos Linux

## 01

Проанализируйте готовность Вашей текущей инфраструктуры к переходу в неизменяемый режим, «стоит ли игра свеч?»

## 02

Оцените готовность инфраструктурной команды к обеспечению необходимых процессов

# Рекомендации при переходе на Talos Linux

## 01

Проанализируйте готовность Вашей текущей инфраструктуры к переходу в неизменяемый режим, «стоит ли игра свеч?»

## 02

Оцените готовность инфраструктурной команды к обеспечению необходимых процессов

## 03

Проверьте, соответствует ли архитектура Talos Linux Вашим ожиданиям, оцените, потребуются ли внутренние доработки



# Рекомендации при переходе на Talos Linux

**01**

Проанализируйте готовность Вашей текущей инфраструктуры к переходу в неизменяемый режим, «стоит ли игра свеч?»

**02**

Оцените готовность инфраструктурной команды к обеспечению необходимых процессов

**03**

Проверьте, соответствует ли архитектура Talos Linux Вашим ожиданиям, оцените, потребуются ли внутренние доработки

**04**

Выберите подходящий для Вас режим развертывания:  
Cloud, VM, Bare-metal

# Рекомендации при переходе на Talos Linux

**01**

Проанализируйте готовность Вашей текущей инфраструктуры к переходу в неизменяемый режим, «стоит ли игра свеч?»

**04**

Выберите подходящий для Вас режим развертывания:  
Cloud, VM, Bare-metal

**02**

Оцените готовность инфраструктурной команды к обеспечению необходимых процессов

**05**

Не забывайте о харденинге настроек операционной системы и обеспечении ее безопасного развертывания

**03**

Проверьте, соответствует ли архитектура Talos Linux Вашим ожиданиям, оцените, потребуются ли внутренние доработки

# Рекомендации при переходе на Talos Linux

**01**

Проанализируйте готовность Вашей текущей инфраструктуры к переходу в неизменяемый режим, «стоит ли игра свеч?»

**02**

Оцените готовность инфраструктурной команды к обеспечению необходимых процессов

**03**

Проверьте, соответствует ли архитектура Talos Linux Вашим ожиданиям, оцените, потребуются ли внутренние доработки

**04**

Выберите подходящий для Вас режим развертывания:  
Cloud, VM, Bare-metal

**05**

Не забывайте о харденинге настроек операционной системы и обеспечении ее безопасного развертывания

**06**

Правильно настройте процесс работы с внедрением новых extensions, ибо root =)



Вопросы?



7 июня 2023 📍 Москва, МЦК ЗИЛ

Первая в России конференция  
по БЕзопасности КОНтейнеров и контейнерных сред



## Contacts:

nickrzaion@gmail.com

n.s.panchenko@tinkoff.ru

Telegram: @yours\_rage



## Наше сообщество



@k8security

@k8security – канал о (не)безопасности Kubernetes + микросервисных, контейнеризированных приложений. Ценим и любим reliability и security, а также observability.