Red Hat Summit

Connect

Migracja aplikacji pomiędzy chmurami

Regulacje / DORA / Exit-plan

Red Hat

Red Hat

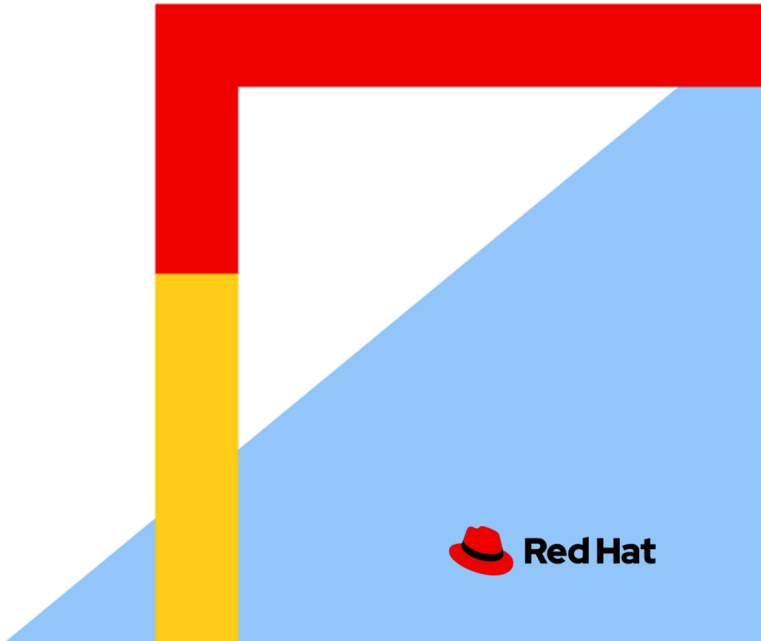
Artur Poczekalewicz

Senior Solution Architect
Red Hat

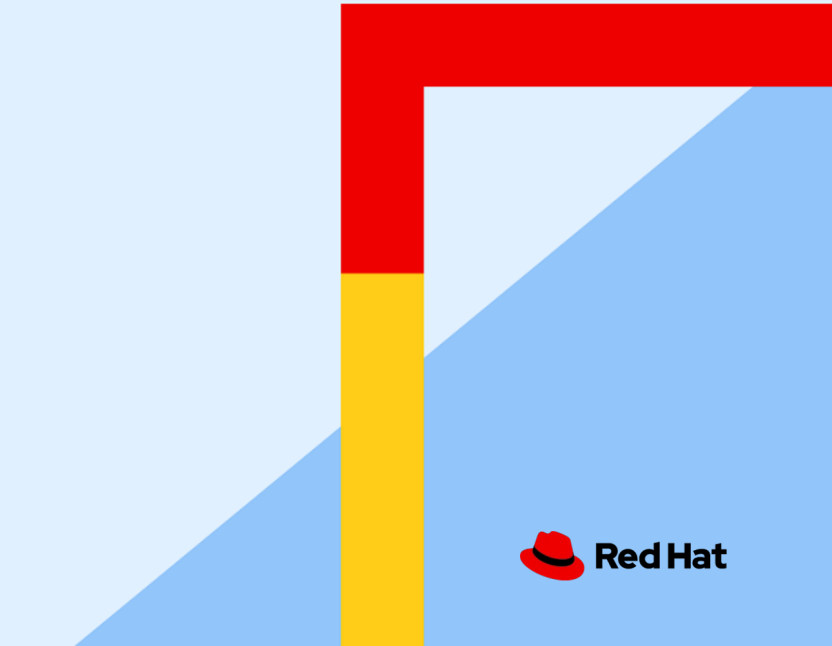
Red Hat

Agenda

- Regulacje - ogólnie
- DORA - słów kilka o niej
- Solucje Red Hat
- EXIT-PLAN: Migration Toolkit for Containers



Regulacje



Co to?

Red Hat

Co to? To "NIEBANAN"

Kształt ogórka: Zgodnie z tą regulacją ogórki klasy pierwszej nie mogły być **wygięte** bardziej niż o **10 mm** na każde **10 cm długości.**

Kształt banana: Podobnie jak w przypadku ogórków, UE wprowadziła przepisy dotyczące klasyfikacji bananów. Zgodnie z tymi przepisami banany musiały mieć minimalną **długość 14 cm** i **szerokość 27 mm**,

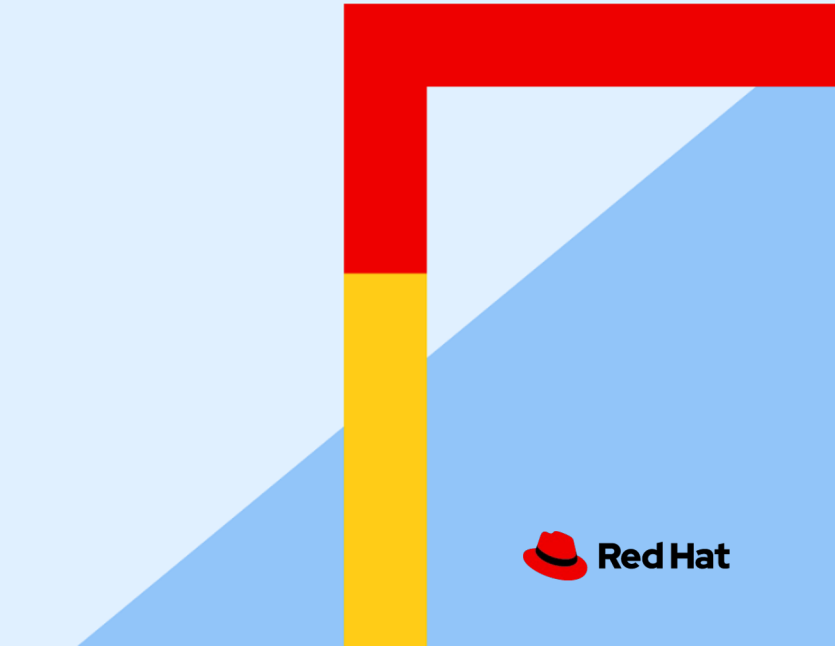
Kształt marchewki: Istniała również regulacja dotycząca klasyfikacji marchewek, które musiały mieć odpowiedni kształt i długość, aby były sprzedawane jako "klasa I". Na przykład, marchewki mogły mieć maksymalną **średnicę 20 mm**, aby były uznane za odpowiedniej jakości.

Red Hat

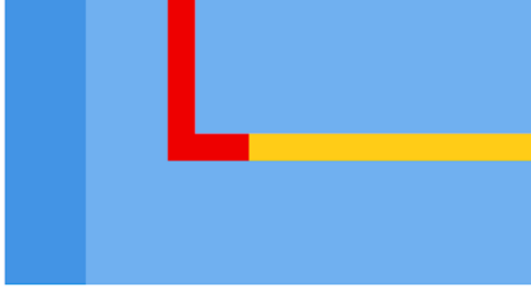
Regulacje - dobre czy złe?

Red Hat

DORA – QUIZ

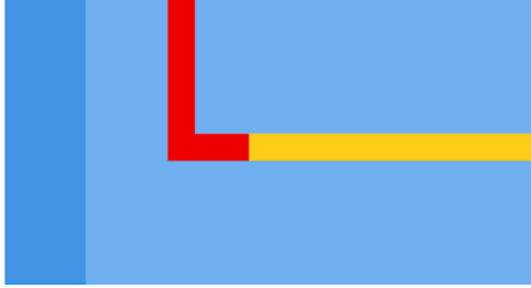


- DORA - skrót:



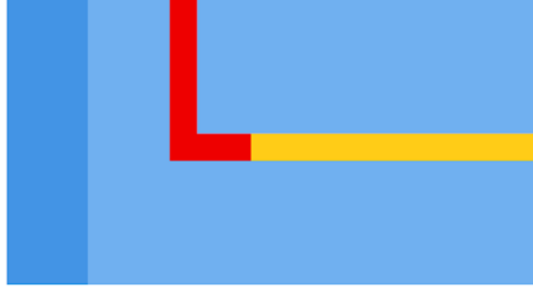
Red Hat

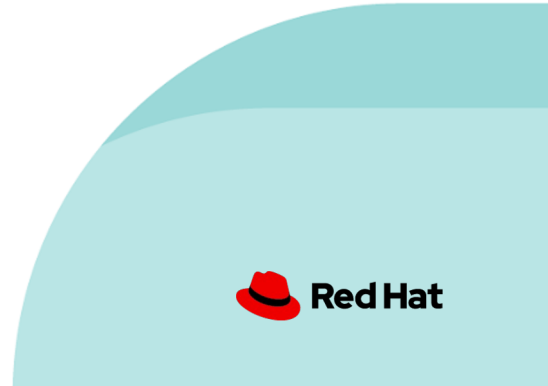
- DORA – skrót: **Digital Operational Resilience Act**



Red Hat

- DORA - skrót: **Digital Operational Resilience Act**
- Czym jest:





- DORA - skrót: **Digital Operational Resilience Act**
- Czym jest: **Europejska regulacja** dotycząca **odporności operacyjnej** w obszarze **IT**

Red Hat

- DORA - skrót: **Digital Operational Resilience Act**
- Czym jest: **Europejska regulacja** dotycząca **odporności operacyjnej** w obszarze **IT**
- Co zapewnia:

Red Hat

- DORA - skrót: **Digital Operational Resilience Act**
- Czym jest: **Europejska regulacja** dotycząca **odporności operacyjnej** w obszarze **IT**
- Co zapewnia: **Przygotowanie** podmiotów do **radzenia sobie** z **zagrożeniami cyfrowymi**

Red Hat

- DORA - skrót: **Digital Operational Resilience Act**
- Czym jest: **Europejska regulacja** dotycząca **odporności operacyjnej** w obszarze **IT**
- Co zapewnia: **Przygotowanie** podmiotów do **radzenia sobie** z **zagrożeniami cyfrowymi**
- Kiedy weszła w życie:

Red Hat

- DORA - skrót: **Digital Operational Resilience Act**
- Czym jest: **Europejska regulacja** dotycząca **odporności operacyjnej** w obszarze **IT**
- Co zapewnia: **Przygotowanie** podmiotów do **radzenia sobie** z **zagrożeniami cyfrowymi**
- Kiedy weszła w życie: **16 stycznia 2023**

Red Hat

- DORA - skrót: **Digital Operational Resilience Act**
- Czym jest: **Europejska regulacja** dotycząca **odporności operacyjnej** w obszarze **IT**
- Co zapewnia: **Przygotowanie** podmiotów do **radzenia sobie** z **zagrożeniami cyfrowymi**
- Kiedy weszła w życie: **16 stycznia 2023**
- Zgodność z DORA - termin:

Red Hat

- DORA - skrót: **Digital Operational Resilience Act**
- Czym jest: **Europejska regulacja** dotycząca **odporności operacyjnej** w obszarze **IT**
- Co zapewnia: **Przygotowanie** podmiotów do **radzenia sobie** z **zagrożeniami cyfrowymi**
- Kiedy weszła w życie: **16 stycznia 2023**
- Zgodność z DORA - termin: **17 stycznia 2025**

Red Hat

- DORA - skrót: **Digital Operational Resilience Act**
- Czym jest: **Europejska regulacja** dotycząca **odporności operacyjnej** w obszarze **IT**
- Co zapewnia: **Przygotowanie** podmiotów do **radzenia sobie** z **zagrożeniami cyfrowymi**
- Kiedy weszła w życie: **16 stycznia 2023**
- Zgodność z DORA - termin: **17 stycznia 2025**
- Jakie sektory obejmuje (4):

Red Hat

- DORA - skrót: **Digital Operational Resilience Act**
- Czym jest: **Europejska regulacja** dotycząca **odporności operacyjnej** w obszarze **IT**
- Co zapewnia: **Przygotowanie** podmiotów do **radzenia sobie** z **zagrożeniami cyfrowymi**
- Kiedy weszła w życie: **16 stycznia 2023**
- Zgodność z DORA - termin: **17 stycznia 2025**
- Jakie sektory obejmuje (4): **Banki**, **Ubezpieczenia**, **Firmy Inwestycyjne**, **Dostawcy ICT**

Red Hat

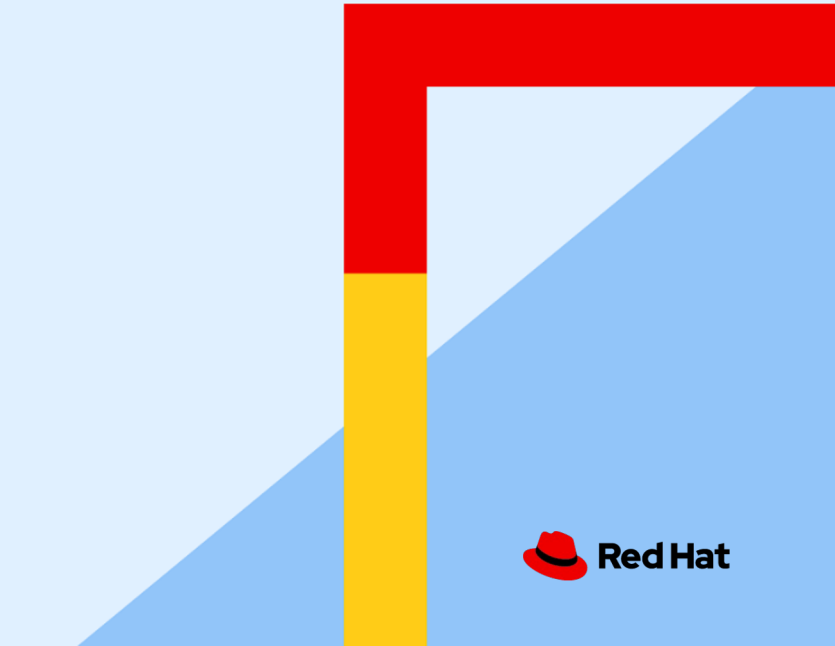
- DORA - skrót: **Digital Operational Resilience Act**
- Czym jest: **Europejska regulacja** dotycząca **odporności operacyjnej** w obszarze **IT**
- Co zapewnia: **Przygotowanie** podmiotów do **radzenia sobie** z **zagrożeniami cyfrowymi**
- Kiedy weszła w życie: **16 stycznia 2023**
- Zgodność z DORA - termin: **17 stycznia 2025**
- Jakie sektory obejmuje (4): **Banki**, **Ubezpieczenia**, **Firmy Inwestycyjne**, **Dostawcy ICT**
- Konsekwencje nieprzestrzegania (5):

Red Hat

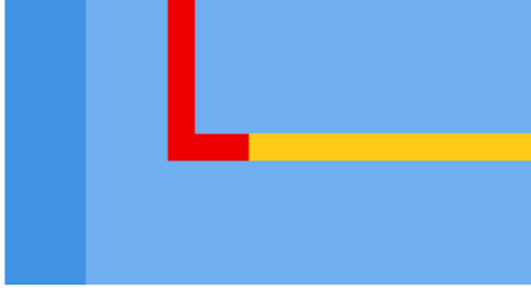
- DORA - skrót: **Digital Operational Resilience Act**
- Czym jest: **Europejska regulacja** dotycząca **odporności operacyjnej** w obszarze **IT**
- Co zapewnia: **Przygotowanie** podmiotów do **radzenia sobie** z **zagrożeniami cyfrowymi**
- Kiedy weszła w życie: **16 stycznia 2023**
- Zgodność z DORA - termin: **17 stycznia 2025**
- Jakie sektory obejmuje (4): **Banki**, **Ubezpieczenia**, **Firmy Inwestycyjne**, **Dostawcy ICT**
- Konsekwencje nieprzestrzegania (5):
  - **Finansowe**
  - **Ograniczenie działalności**
  - **Zwiększony nadzór**
  - **Odpowiedzialność prawna**
  - (*) **Utrata wizerunku/reputacji**

Red Hat

DORA – Rozdziały



- Chapter 2 -

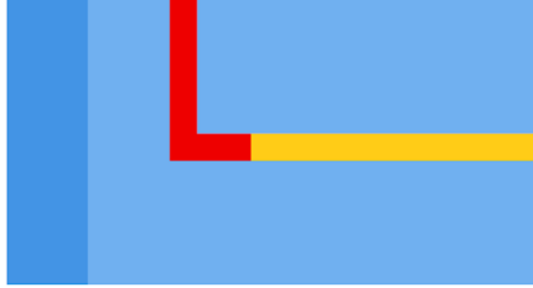


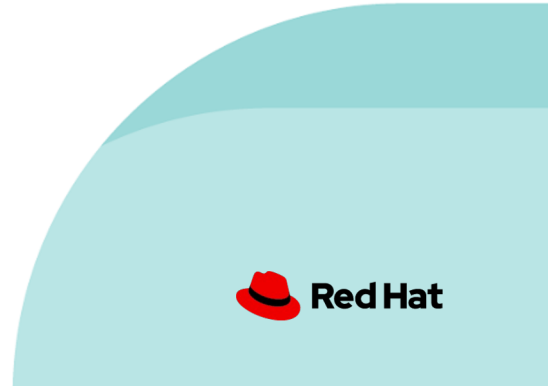
Red Hat

- Chapter 2 - **Risk Management**

Red Hat

- Chapter 2 - **Risk Management**
  - Cele (2):





- Chapter 2 - **Risk Management**
  - Cele (2):
    - **BCM** (Business Continuity Management) - **HA**, **DR**
    - **Data Integrity**

- Chapter 2 - **Risk Management**
  - Cele (2):
    - **BCM** (Business Continuity Management) - **HA**, **DR**
    - **Data Integrity**
- Chapter 3 -

- Chapter 2 - **Risk Management**
  - Cele (2):
    - **BCM** (Business Continuity Management) - **HA**, **DR**
    - **Data Integrity**
- Chapter 3 - **Incident Management**

- Chapter 2 - **Risk Management**
  - Cele (2):
    - **BCM** (Business Continuity Management) - **HA**, **DR**
    - **Data Integrity**
- Chapter 3 - **Incident Management**
  - Cele (2):

- Chapter 2 - **Risk Management**
  - Cele (2):
    - **BCM** (Business Continuity Management) - **HA**, **DR**
    - **Data Integrity**
- Chapter 3 - **Incident Management**
  - Cele (2): **identyfikacja**, **reagowanie**

- Chapter 2 - **Risk Management**
  - Cele (2):
    - **BCM** (Business Continuity Management) - **HA**, **DR**
    - **Data Integrity**
- Chapter 3 - **Incident Management**
  - Cele (2): **identyfikacja**, **reagowanie**
  - Jakie incydenty (2):

- Chapter 2 - **Risk Management**
  - Cele (2):
    - **BCM** (Business Continuity Management) - **HA**, **DR**
    - **Data Integrity**
- Chapter 3 - **Incident Management**
  - Cele (2): **identyfikacja**, **reagowanie**
  - Jakie incydenty (2): **awarie**, **cyberataki**

- Chapter 2 - **Risk Management**
  - Cele (2):
    - **BCM** (Business Continuity Management) - **HA**, **DR**
    - **Data Integrity**
- Chapter 3 - **Incident Management**
  - Cele (2): **identyfikacja**, **reagowanie**
  - Jakie incydenty (2): **awarie**, **cyberataki**
- Chapter 4 -

- Chapter 2 - **Risk Management**
  - Cele (2):
    - **BCM** (Business Continuity Management) - **HA**, **DR**
    - **Data Integrity**
- Chapter 3 - **Incident Management**
  - Cele (2): **identyfikacja**, **reagowanie**
  - Jakie incydenty (2): **awarie**, **cyberataki**
- Chapter 4 - **Operational Resilience Testing**

- Chapter 2 - **Risk Management**
  - Cele (2):
    - **BCM** (Business Continuity Management) - **HA**, **DR**
    - **Data Integrity**
- Chapter 3 - **Incident Management**
  - Cele (2): **identyfikacja**, **reagowanie**
  - Jakie incydenty (2): **awarie**, **cyberataki**
- Chapter 4 - **Operational Resilience Testing**
  - Cele (3 testy):

- Chapter 2 - **Risk Management**
  - Cele (2):
    - **BCM** (Business Continuity Management) - **HA**, **DR**
    - **Data Integrity**
- Chapter 3 - **Incident Management**
  - Cele (2): **identyfikacja**, **reagowanie**
  - Jakie incydenty (2): **awarie**, **cyberataki**
- Chapter 4 - **Operational Resilience Testing**
  - Cele (3 testy): **HA**, **DR**, **Security** (Pentesting)

- Chapter 2 - **Risk Management**
  - Cele (2):
    - **BCM** (Business Continuity Management) - **HA**, **DR**
    - **Data Integrity**
- Chapter 3 - **Incident Management**
  - Cele (2): **identyfikacja**, **reagowanie**
  - Jakie incydenty (2): **awarie**, **cyberataki**
- Chapter 4 - **Operational Resilience Testing**
  - Cele (3 testy): **HA**, **DR**, **Security** (Pentesting)
- Chapter 5 -

- Chapter 2 - **Risk Management**
  - Cele (2):
    - **BCM** (Business Continuity Management) - **HA**, **DR**
    - **Data Integrity**
- Chapter 3 - **Incident Management**
  - Cele (2): **identyfikacja**, **reagowanie**
  - Jakie incydenty (2): **awarie**, **cyberataki**
- Chapter 4 - **Operational Resilience Testing**
  - Cele (3 testy): **HA**, **DR**, **Security** (Pentesting)
- Chapter 5 - **Third-party risk**

- Chapter 2 - **Risk Management**
  - Cele (2):
    - **BCM** (Business Continuity Management) - **HA**, **DR**
    - **Data Integrity**
- Chapter 3 - **Incident Management**
  - Cele (2): **identyfikacja**, **reagowanie**
  - Jakie incydenty (2): **awarie**, **cyberataki**
- Chapter 4 - **Operational Resilience Testing**
  - Cele (3 testy): **HA**, **DR**, **Security** (Pentesting)
- Chapter 5 - **Third-party risk**
  - Cele (3):

- Chapter 2 - **Risk Management**
  - Cele (2):
    - **BCM** (Business Continuity Management) - **HA**, **DR**
    - **Data Integrity**
- Chapter 3 - **Incident Management**
  - Cele (2): **identyfikacja**, **reagowanie**
  - Jakie incydenty (2): **awarie**, **cyberataki**
- Chapter 4 - **Operational Resilience Testing**
  - Cele (3 testy): **HA**, **DR**, **Security** (Pentesting)
- Chapter 5 - **Third-party risk**
  - Cele (3): **SLA**, **Multi-provider strategy**, **Exit-Plan**

- Chapter 2 - **Risk Management**
  - Cele (2):
    - **BCM** (Business Continuity Management) - **HA**, **DR**
    - **Data Integrity**
- Chapter 3 - **Incident Management**
  - Cele (2): **identyfikacja**, **reagowanie**
  - Jakie incydenty (2): **awarie**, **cyberataki**
- Chapter 4 - **Operational Resilience Testing**
  - Cele (3 testy): **HA**, **DR**, **Security** (Pentesting)
- Chapter 5 - **Third-party risk**
  - Cele (3): **SLA**, **Multi-provider strategy**, **Exit-Plan**
  - Dlaczego:

- Chapter 2 - **Risk Management**
  - Cele (2):
    - **BCM** (Business Continuity Management) - **HA**, **DR**
    - **Data Integrity**
- Chapter 3 - **Incident Management**
  - Cele (2): **identyfikacja**, **reagowanie**
  - Jakie incydenty (2): **awarie**, **cyberataki**
- Chapter 4 - **Operational Resilience Testing**
  - Cele (3 testy): **HA**, **DR**, **Security** (Pentesting)
- Chapter 5 - **Third-party risk**
  - Cele (3): **SLA**, **Multi-provider strategy**, **Exit-Plan**
  - Dlaczego: Aby **zewnętrzni dostawcy** usług **nie naruszyli odporności** operacyjnej podmiotów finansowych

- Chapter 2 - **Risk Management**
  - Cele (2):
    - **BCM** (Business Continuity Management) - **HA**, **DR**
    - **Data Integrity**
- Chapter 3 - **Incident Management**
  - Cele (2): **identyfikacja**, **reagowanie**
  - Jakie incydenty (2): **awarie**, **cyberataki**
- Chapter 4 - **Operational Resilience Testing**
  - Cele (3 testy): **HA**, **DR**, **Security** (Pentesting)
- Chapter 5 - **Third-party risk**
  - Cele (3): **SLA**, **Multi-provider strategy**, **Exit-Plan**
  - Dlaczego: Aby **zewnętrzni dostawcy** usług **nie naruszyli odporności** operacyjnej podmiotów finansowych
- Chapter 6 -

Red Hat

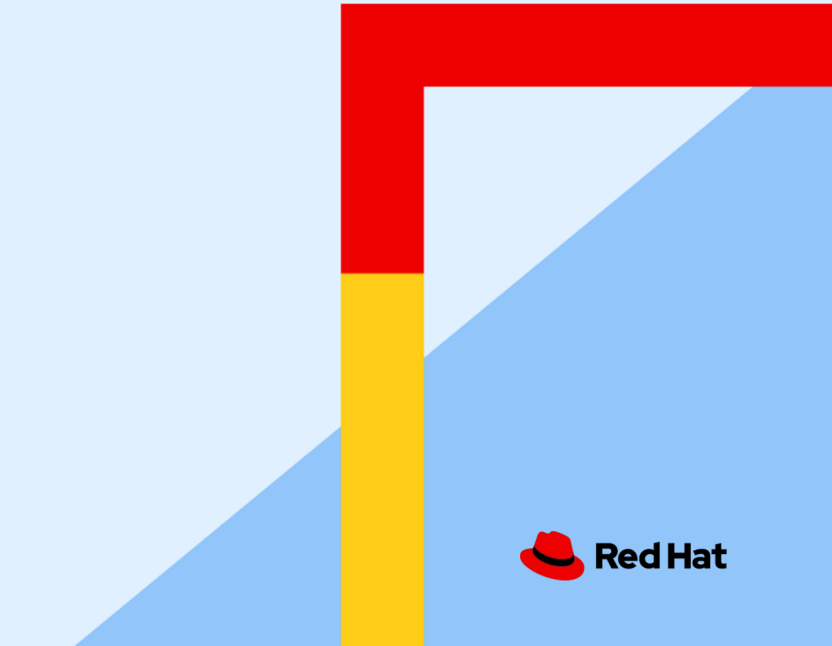
- Chapter 2 - **Risk Management**
  - Cele (2):
    - **BCM** (Business Continuity Management) - **HA**, **DR**
    - **Data Integrity**
- Chapter 3 - **Incident Management**
  - Cele (2): **identyfikacja**, **reagowanie**
  - Jakie incydenty (2): **awarie**, **cyberataki**
- Chapter 4 - **Operational Resilience Testing**
  - Cele (3 testy): **HA**, **DR**, **Security** (Pentesting)
- Chapter 5 - **Third-party risk**
  - Cele (3): **SLA**, **Multi-provider strategy**, **Exit-Plan**
  - Dlaczego: Aby **zewnętrzni dostawcy** usług **nie naruszyli odporności** operacyjnej podmiotów finansowych
- Chapter 6 - **Information exchange**

- Chapter 2 - **Risk Management**
  - Cele (2):
    - **BCM** (Business Continuity Management) - **HA**, **DR**
    - **Data Integrity**
- Chapter 3 - **Incident Management**
  - Cele (2): **identyfikacja**, **reagowanie**
  - Jakie incydenty (2): **awarie**, **cyberataki**
- Chapter 4 - **Operational Resilience Testing**
  - Cele (3 testy): **HA**, **DR**, **Security** (Pentesting)
- Chapter 5 - **Third-party risk**
  - Cele (3): **SLA**, **Multi-provider strategy**, **Exit-Plan**
  - Dlaczego: Aby **zewnętrzni dostawcy** usług **nie naruszyli odporności** operacyjnej podmiotów finansowych
- Chapter 6 - **Information exchange**
  - Cel:

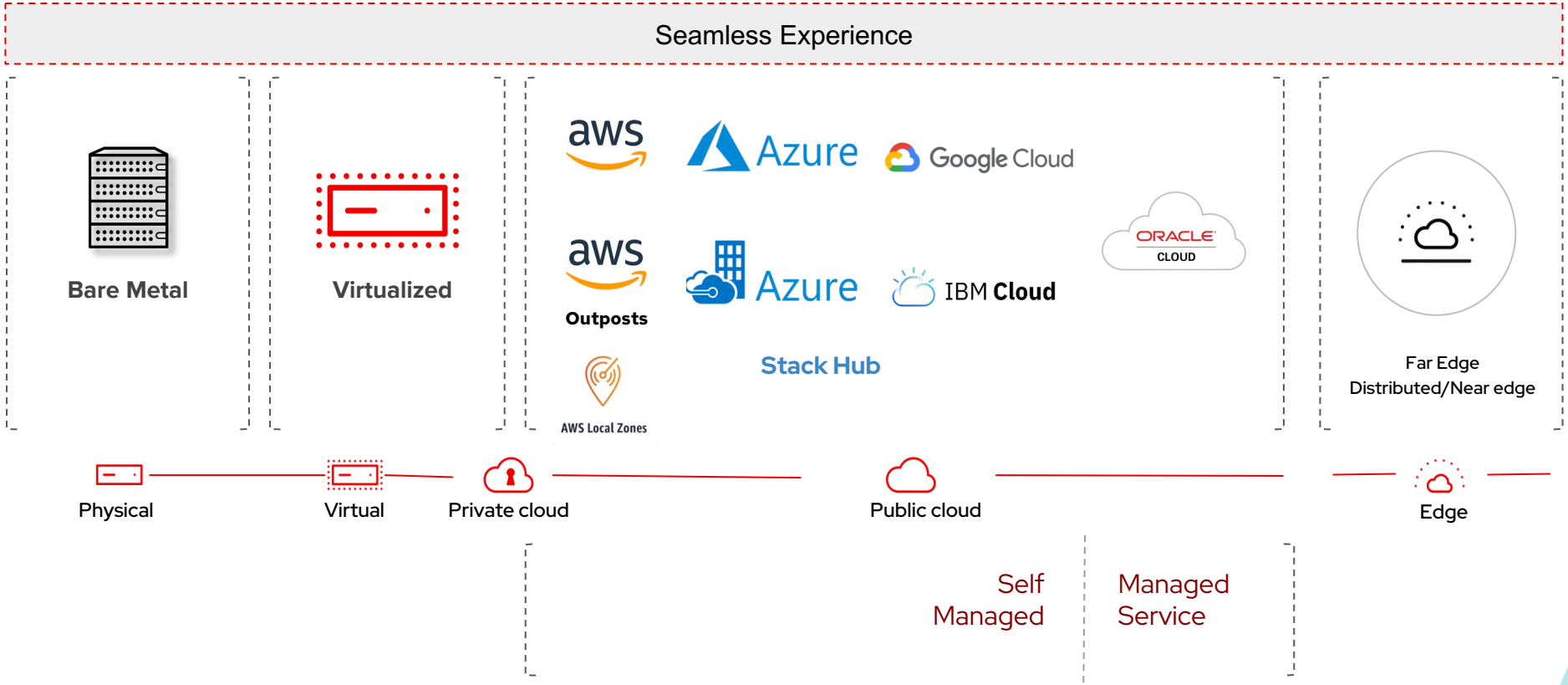
- Chapter 2 - **Risk Management**
  - Cele (2):
    - **BCM** (Business Continuity Management) - **HA**, **DR**
    - **Data Integrity**
- Chapter 3 - **Incident Management**
  - Cele (2): **identyfikacja**, **reagowanie**
  - Jakie incydenty (2): **awarie**, **cyberataki**
- Chapter 4 - **Operational Resilience Testing**
  - Cele (3 testy): **HA**, **DR**, **Security** (Pentesting)
- Chapter 5 - **Third-party risk**
  - Cele (3): **SLA**, **Multi-provider strategy**, **Exit-Plan**
  - Dlaczego: Aby **zewnętrzni dostawcy** usług **nie naruszyli odporności** operacyjnej podmiotów finansowych
- Chapter 6 - **Information exchange**
  - Cel: **Poufna wymiana informacji** pomiędzy instytucjami o **zagrożeniach**

- Chapter 2 - **Risk Management**
  - Cele (2):
    - **BCM** (Business Continuity Management) - **HA**, **DR**
    - **Data Integrity**
- Chapter 3 - **Incident Management**
  - Cele (2): **identyfikacja**, **reagowanie**
  - Jakie incydenty (2): **awarie**, **cyberataki**
- Chapter 4 - **Operational Resilience Testing**
  - Cele (3 testy): **HA**, **DR**, **Security** (Pentesting)
- Chapter 5 - **Third-party risk**
  - Cele (3): **SLA**, **Multi-provider strategy**, **Exit-Plan**
  - Dlaczego: Aby **zewnętrzni dostawcy** usług **nie naruszyli odporności** operacyjnej podmiotów finansowych
- Chapter 6 - **Information exchange**
  - Cel: **Poufna wymiana informacji** pomiędzy instytucjami o **zagrożeniach**

Solucje na wyzwania!



OpenShift Anywhere



Red Hat

OpenShift Anywhere

Red Hat

OpenShift Anywhere

- **Powód #1**
  - Wdrażanie aplikacji wszędzie takie samo (VM, containers, serverless)

Red Hat

OpenShift Anywhere

- **Powód #1**
  - Wdrażanie aplikacji wszędzie takie samo (VM, containers, serverless)
- **Powód #2**
  - Usprawnienia dla aplikacji takie same (ServiceMesh, ACS, Pipelines...)

Red Hat

OpenShift Anywhere

- **Powód #1**
  - Wdrażanie aplikacji wszędzie takie samo (VM, containers, serverless)
- **Powód #2**
  - Usprawnienia dla aplikacji takie same (ServiceMesh, ACS, Pipelines...)
- **Powód #3**
  - Możliwość centralnego zarządzania - Advanced Cluster Management / Advanced Cluster Security

OpenShift Anywhere

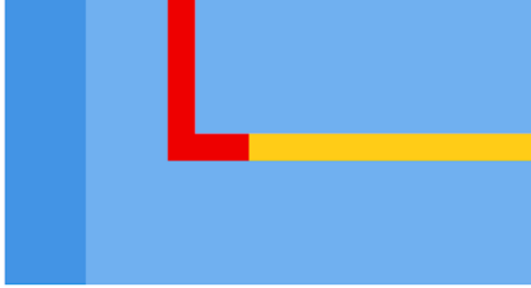
- **Powód #1**
  - Wdrażanie aplikacji wszędzie takie samo (VM, containers, serverless)
- **Powód #2**
  - Usprawnienia dla aplikacji takie same (ServiceMesh, ACS, Pipelines...)
- **Powód #3**
  - Możliwość centralnego zarządzania - Advanced Cluster Management / Advanced Cluster Security
- **Powód #4**
  - Możliwość szybkiej i łatwej zmiany środowiska (Exit Plan)

Red Hat

OpenShift Anywhere

- **Powód #1**
  - Wdrażanie aplikacji wszędzie takie samo (VM, containers, serverless)
- **Powód #2**
  - Usprawnienia dla aplikacji takie same (ServiceMesh, ACS, Pipelines...)
- **Powód #3**
  - Możliwość centralnego zarządzania - Advanced Cluster Management / Advanced Cluster Security
- **Powód #4**
  - Możliwość szybkiej i łatwej zmiany środowiska (Exit Plan)
- **Powód #5**
  - Jest jeszcze wiele powodów, ale trzeba gnać z czasem :)

Red Hat



Red Hat

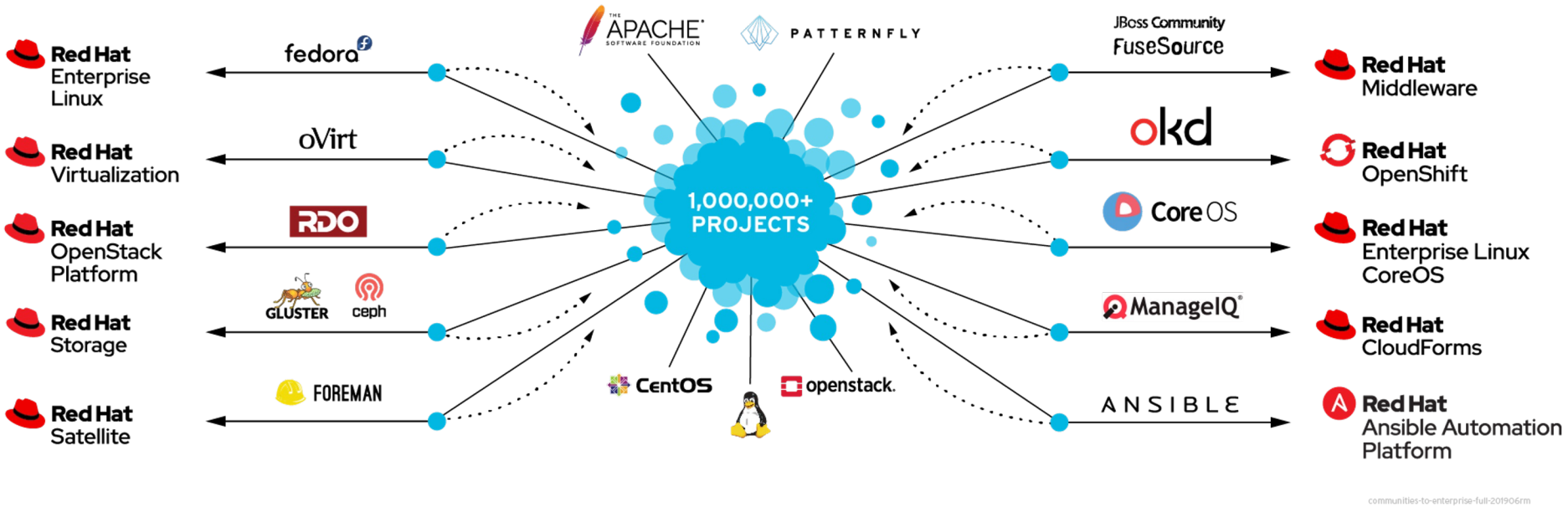
- Chapter 2 - **Risk Management**
  - Cele (2):
    - **BCM** (Business Continuity Management) - **HA**, **DR**
    - **Data Integrity**
- Chapter 3 - **Incident Management**
  - Cele (2): **identyfikacja**, **reagowanie**
  - Jakie incydenty (2): **awarie**, **cyberataki**
- Chapter 4 - **Operational Resilience Testing**
  - Cele (3 testy): **HA**, **DR**, **Security** (Pentesting)
- Chapter 5 - **Third-party risk**
  - Cele (3): **SLA**, **Multi-provider strategy**, **Exit-Plan**
  - Dlaczego: Aby **zewnętrzni dostawcy** usług **nie naruszyli odporności** operacyjnej podmiotów finansowych
- Chapter 6 - **Information exchange**
  - Cel: **Poufna wymiana informacji** pomiędzy instytucjami o **zagrożeniach**

Multi-provider Strategy

Co błyskotliwy autor tego slajdu ma na myśli pod kątem vendor-lockingu?

Red Hat

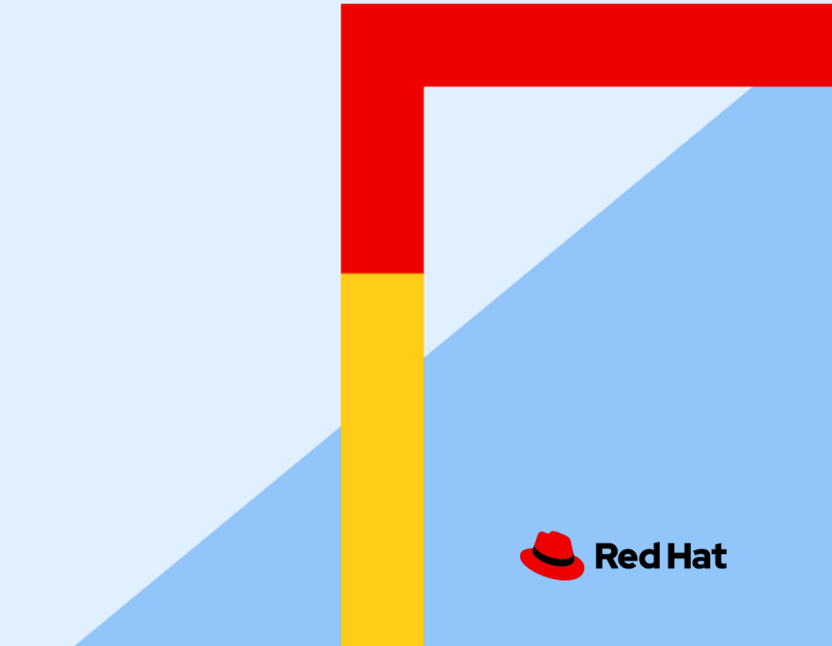
Od zawsze Open Source



communities-to-enterprise-full-201906rm

Red Hat

<tech>
Solucje na wyzwania!
</tech>



Provisioning (Physical/Logical) (as a Code)

- Cluster as a Service
  - Different platforms (on-prem, AWS, Azure, GCP..)
  - Different deployments (Normal, Compat, SNO)
- Namespace as a Service
  - Quota
  - Limits
  - RBAC
  - NetworkPolicy (Egress/Ingress)
  - ExternalServices
- Cloud native services
  - PostgreSQL
  - Firewall

Service HA, Service Resiliency

- ServiceMesh (circuit breaker)
- ACM (submariner)
- Red Hat Service Interconnect
- OpenShift (ExternalService)
- OpenShift (HPA)
- ACM (cluster sets)

Incident Reporting

- **Policy Violation (ACM)**
- **Incident reporting (ACS)**
- **OpenSCAP**
- **OpenShift Monitoring (AlertManager)**
- **Red Hat Satellite / Red Hat Insights**

Continuous Monitoring & Auditing

- **OpenShift Logging**
- **OpenShift Monitoring**
- **ACM (clusters overview)**
- **ACM (governance)**
- **ACS**
- **Compliance Operator**
- **Red Hat Satellite / Red Hat Insights**

Compliance Check

- **ACS**
- **Compliance Operator**
- **ACM (governance)**
- **Red Hat Automation Platform (with ACM)**
- **Red Hat Automation Platform (dry-run)**
- **Red Hat Trusted Profile Analyzer (SBOM)**

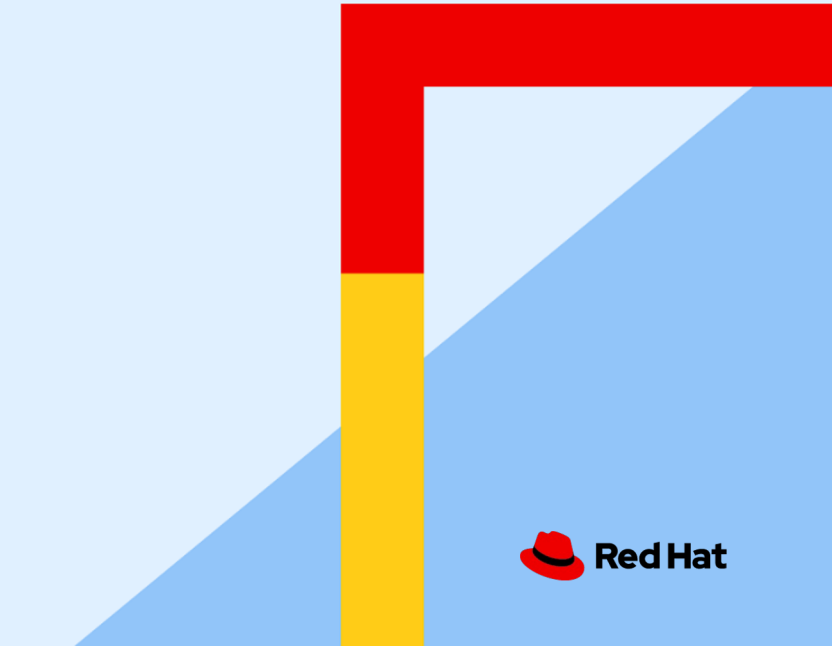
Data Integrity

- OpenShift OADP (OpenShift APIs for Data Protection)
- LUKS (Linux Unified Key Setup)
- Red Hat Trusted Software Supply Chain
- Red Hat Trusted Artifact Signer
- Red Hat Pipelines + Tekton Chains

Exit-Plan

- **OpenShift MTV - Migration Toolkit for Virtualization**
- **OpenShift MTC - Migration Toolkit for Containers**

Migration Toolkit for Containers



Migracja - ogólnie

- **Cel**: na klastrze docelowym muszą się znaleźć:
  - Definicje aplikacji (k8s **Resources**)
  - Dane (**Persistent Volumes - PV**) / (**Images!**)
- **Resources**:
  - Manual deployment (oc/kubectl)
  - GitOps - np. OpenShift Gitops (ArgoCD), ACM
  - Odtworzenie z backup
- Ewentualne **transformacje** (np. różne wersje k8s - różne wersje API lub inne StorageClass)
- **Persistent Volumes:**
  - Odtworzenie z backup
  - Transfer PV
  - Dostępny storage z lokalizacji docelowej (np. NFS lub EBS snapshots)
  - Replikowany Storage

MTC - Migration Toolkit for Containers

- **OpenShift - Migration Toolkit for Containers** (Crane + Restic + Volsync + Ansible)
- Migracja: Resources, PV, internal images - automatycznie (bez GitOps)
- Pre i post hooks
- WebUI oraz API
- Techniki migracji PV:
  - Copy - **Direct Volume Migration** (Volsync/Rsync)
  - Copy - z serwerem pośredniczącym (**S3**)
  - **Snapshot** (odtworzenie PV ze snapshota dostępnego z obu lokalizacji)
  - **Move** (przy współdzielonym storage pomiędzy lokalizacjami - np. NFS) - przeniesienie tylko definicji PV na drugi klaster
- Transformacje storageclass, PV resizing
- Stage migration + Cut over

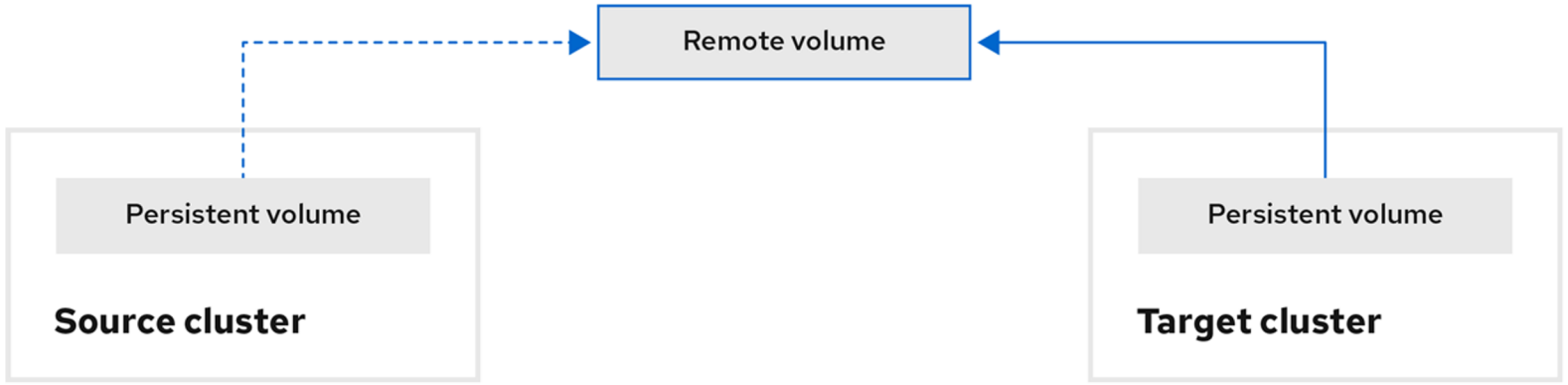
Red Hat

MTC - Recreate from snapshot

Benefits	Limitations
• Faster than the file system copy method.	• Cloud provider must support snapshots. • Clusters must be on the same cloud provider. • Clusters must be in the same location or region. • Clusters must have the same storage class. • Storage class must be compatible with snapshots. • Does not support direct volume migration.

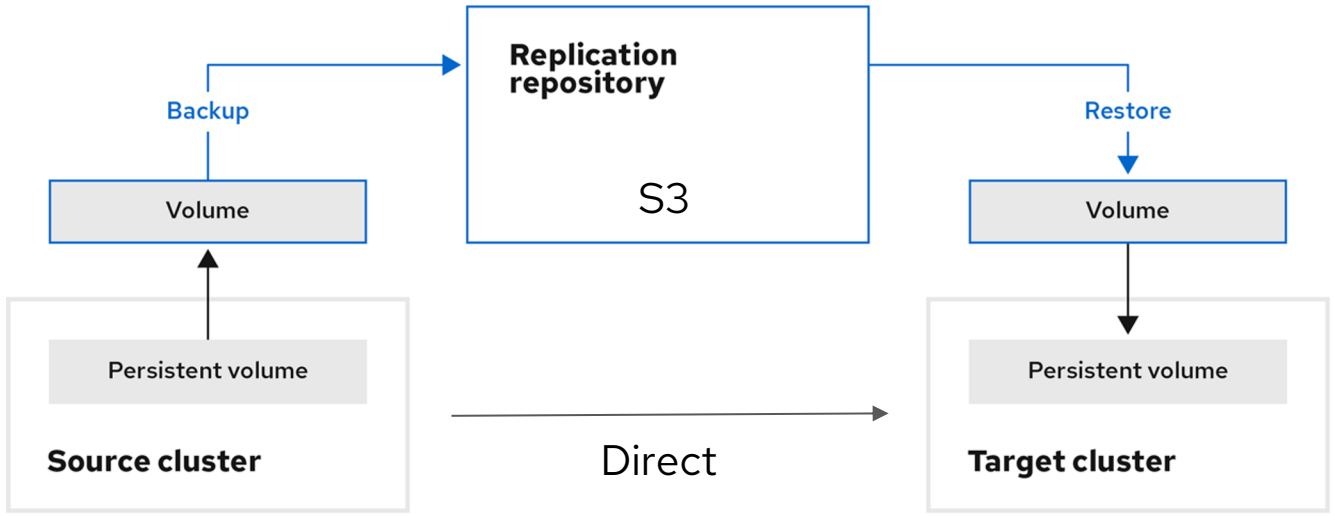
Red Hat

MTC – Move

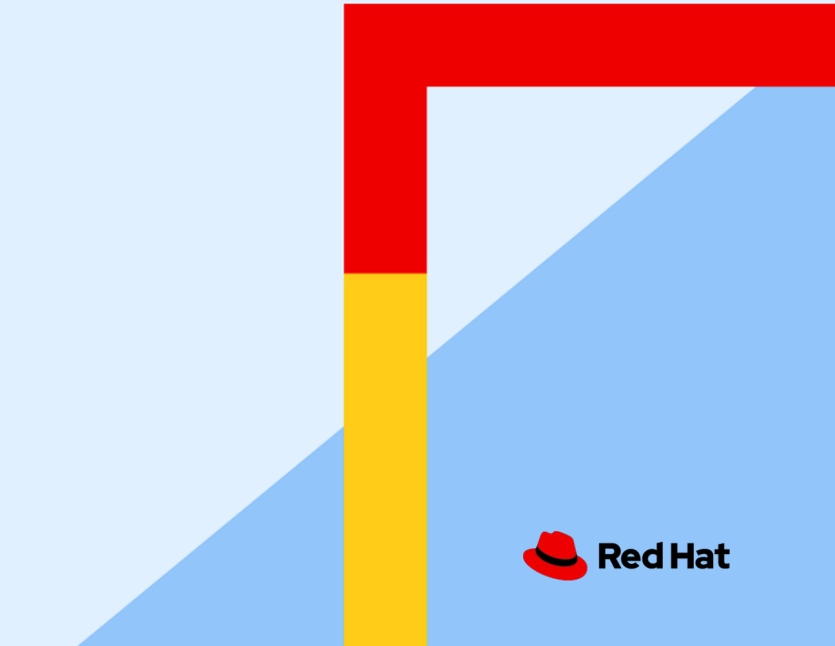


Move: MTC unmounts a remote volume, for example, NFS, from the source cluster, creates a PV resource on the target cluster pointing to the remote volume, and then mounts the remote volume on the target cluster. Applications running on the target cluster use the same remote volume that the source cluster was using. The remote volume must be accessible to the source and target clusters.

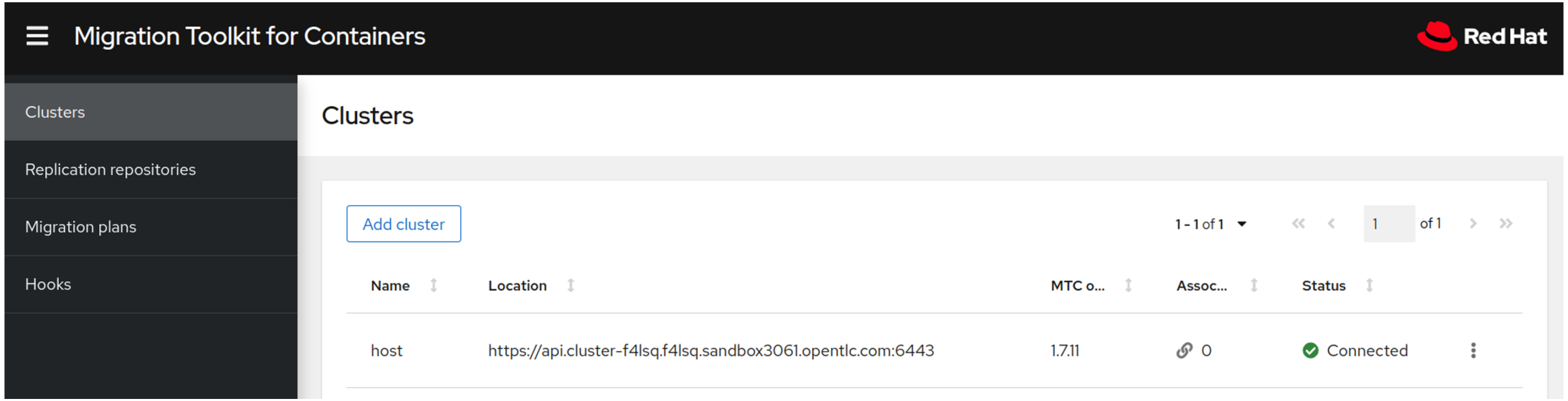
MTC - Copy (S3 or Direct)



Migration Toolkit for Containers - DEMO



Migration Toolkit for Containers - DEMO



Red Hat

Add cluster

cluster2

Is this an azure cluster?

☐ Azure cluster

URL *

https://api.cluster2.sandbox577.opentlc.com:6443

URL of the cluster's API server

Service account token *

••

Copy and paste the cluster's service account token.

Exposed route host to image registry

Optional route to the cluster's image registry

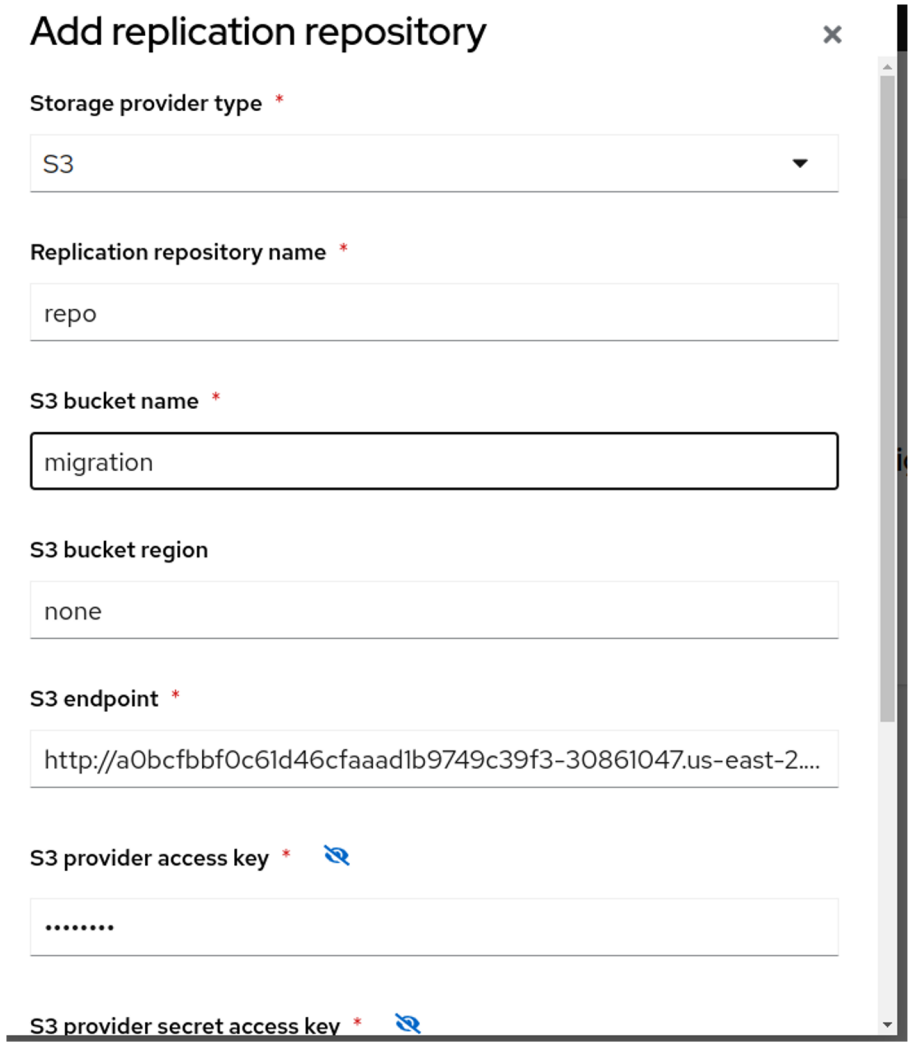
Red Hat

Add cluster

1 - 2 of 2 | 1 of 1

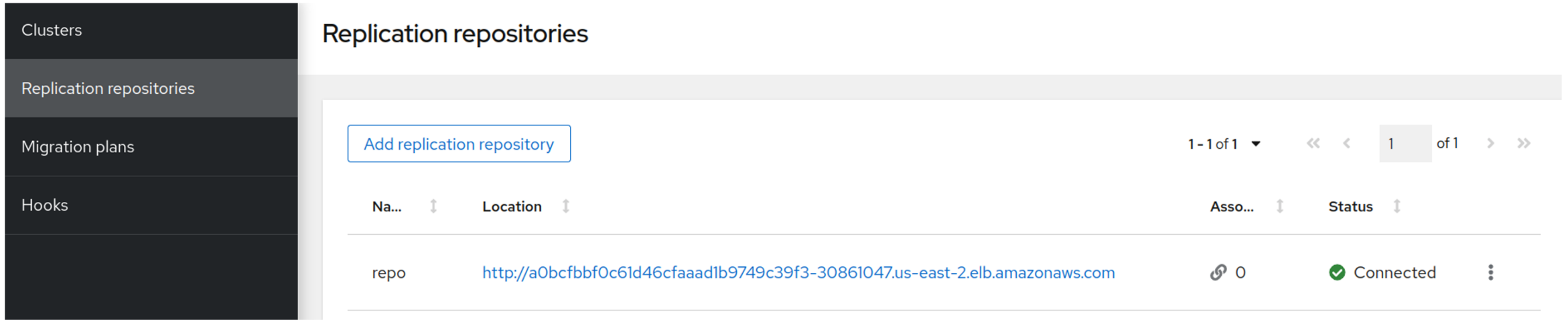
Name	Location	MTC o...	Assoc...	Status
cluster2	https://api.cluster2.sandbox577.opentlc.com:6443	1.7.11	0	Connected
host	https://api.cluster-f4lsq.f4lsq.sandbox3061.opentlc.com:6443	1.7.11	0	Connected

Red Hat


Add replication repository
Storage provider type *
S3
Replication repository name *
repo
S3 bucket name *
migration
S3 bucket region
none
S3 endpoint *
http://a0bcfbbf0c61d46cfaaad1b9749c39f3-30861047.us-east-2....
S3 provider access key *
••••••••
S3 provider secret access key *

Red Hat

Migration Toolkit for Containers - DEMO



Red Hat

General

All fields are required.

Plan name *

plan1

Migration type *

Select...

- Full migration - migrate namespaces, persistent volumes (PVs) and Kubernetes resources from one cluster to another
- State migration - migrate only PVs between namespaces in the same cluster or different clusters
- Storage class conversion - convert PVs to a different storage class within the same cluster and namespace

Red Hat

Plan name *

plan1

Migration type *

Full migration - migrate namespaces, persistent volumes (PVs) and Kubernetes resources from one cluster to another

Source cluster *

cluster2

Target cluster *

host

Repository *

repo

Migration Toolkit for Containers - DEMO

1 General
2 Namespaces
3 Persistent volumes
4 Copy options
5 Migration options
6 Hooks

	Source name	Pods	PV claims	Services	Target name
☐	cluster2	0	0	0	cluster2
☐	open-cluster-management-agent	7	0	0	open-cluster-management-agent
☐	open-cluster-management-agent-addon	9	0	6	open-cluster-management-agent-addon
☑	persistent-app	1	1	1	persistent-app

Red Hat

Persistent volumes

Choose to move or copy persistent volumes associated with selected namespaces.

PV name | Filter by PV name... | 1 - 1 of 1 | 1 of 1

	PV name	Claim	Namespace	Storage cl...	Size	PV migration type	Details
☑	pvc-ad69fccc-b3d8-47a2-bae1-736a99fc5031	persistent-app	persistent-app	gp3-csi	1Gi	Filesystem copy	View JSON

Filesystem copy ✓
Volume snapshot

1 - 1 of 1

Red Hat

Copy options

For each persistent volume to be copied, you can optionally change the target PVC and target storage class.

PV name | Filter by PV name... | 1 - 1 of 1 | 1 of 1

PV name	Source PVC	Source stora...	Target PVC	Target storage class	Verify copy ...
pvc-ad69fccc-b3d8-47a2-bae1-736a99fc5031	persistent-app	gp3-csi	persistent-app	gp3-csi:ebs.csi.aws.com	

gp2-csi:ebs.csi.aws.com
gp3-csi:ebs.csi.aws.com ✓

of 1

Red Hat

1 General
2 Namespaces
3 Persistent volumes
4 Copy options
5 Migration options
6 Hooks

Migration options

Images

Direct image migration Available

Use direct image migration

Persistent volumes

Direct PV migration Available

Use direct PV migration for filesystem copies

Red Hat

Hooks

Hooks are commands that can be run at various steps in the migration process. They are defined in a container image or an Ansible playbook and can be run on either the source or target cluster.

Add an existing hook or create a new one *

Create a new hook

Hook name *

Hook definition

Ansible playbook

Upload your Ansible playbook file or paste its contents below. *

Drag a file here or browse to upload | Browse... | Clear

Migration Toolkit for Containers - DEMO

Ansible runtime image *

registry.redhat.io/rhmtc/openshift-migration-hook-runner-rhel8@sha256:bd4432109c59d14ad683e11d19790cc33b5722ff042d6e02aef35c96201c1cd1

This is the default Ansible runtime image. You can change it to a custom image with your own modules.

○ Custom container image

Run in

◉ Source cluster

○ Target cluster

Service account name *

Service account namespace *

Migration step when the hook should be run *

Select a phase

PreBackup

Red Hat

Migration Toolkit for Containers - DEMO

Name	Migrations	Type	Source	Target	Repos...	Namespaces	Last state
plan1	0	Full migrati...	cluster2	host	repo	1	Ready

1 - 1 of 1

1

Logs

Edit

Delete

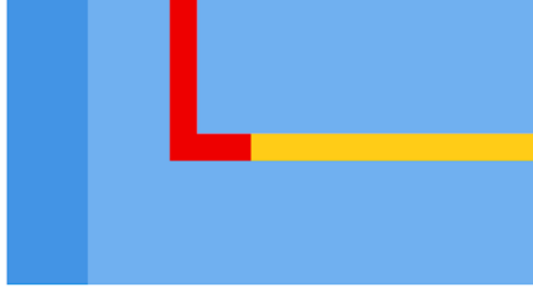
Migrations

Stage

Cutover

Rollback

Red Hat



Stage migration

During a stage migration:

- PV data is copied to the target cluster.
- PV references are **not** moved.
- Source pods continue running.

Stage Cancel

Migration Toolkit for Containers - DEMO

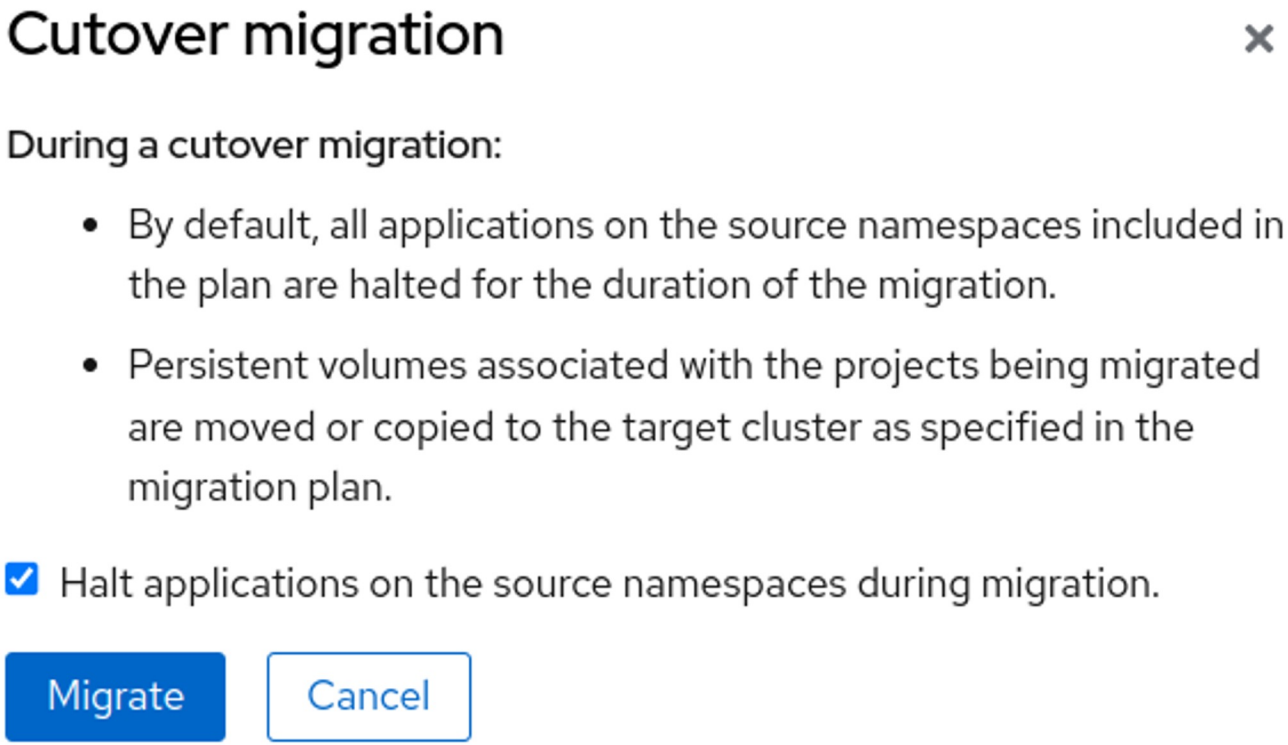
DirectImage	a few seconds	Complete	
DirectVolume	a few seconds	Complete	View Details
Cleanup	a few seconds	Complete	

Migration resources

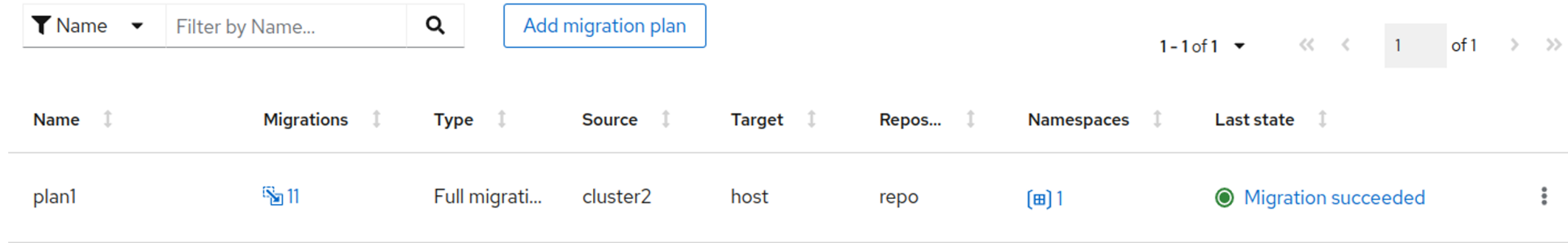
Type to search

- Plan: host/openshift-migration/plan1 — Stage succeeded
  - Migration: host/openshift-migration/stage-b40d9 — Completed
    - DirectVolumeMigration: host/openshift-migration/stage-b40d9-8lgkw — Completed
      - DirectVolumeMigrationProgress: host/openshift-migration/1dc838ee3531e61344e2ba7733f5a44b — Completed
    - DirectImageMigration: host/openshift-migration/stage-b40d9-8jdsv — Completed

Red Hat


Cutover migration
During a cutover migration:
By default, all applications on the source namespaces included in the plan are halted for the duration of the migration.
Persistent volumes associated with the projects being migrated are moved or copied to the target cluster as specified in the migration plan.
Halt applications on the source namespaces during migration.
Migrate
Cancel

Migration Toolkit for Containers - DEMO - SUKCES

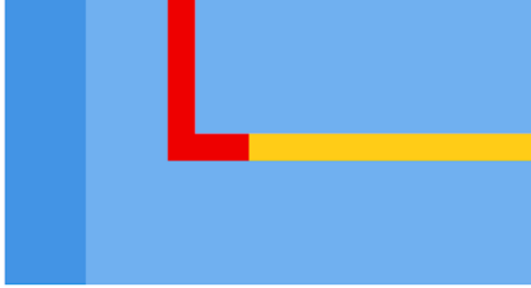


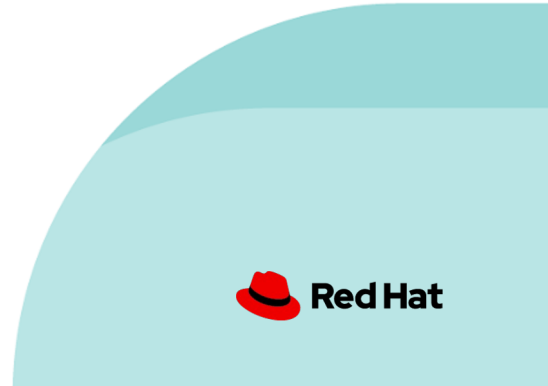
Przedstawiony zrzut ekranu w sposób niepodważalny odzwierciedla wielki sukces osiągnięty na drodze naszego wspólnego wysiłku, który stanowi chlubny przykład realizacji wyznaczonych celów i strategii.

Jest to dowód na skuteczność przyjętej linii działania oraz na harmonijną współpracę wszystkich zaangażowanych czynników tego rozwiązania.

Red Hat

Q & A





MTC - Migration Toolkit for Containers

- **OpenShift - Migration Toolkit for Containers** (Crane + Restic + Volsync + Ansible)
- Migracja: Resources, PV, internal images - automatycznie (bez GitOps)
- Pre i post hooks
- WebUI oraz API
- Techniki migracji PV:
  - Copy - **Direct Volume Migration** (Volsync/Rsync)
  - Copy - z serwerem pośredniczącym (**S3**)
  - **Snapshot** (odtworzenie PV ze snapshota dostępnego z obu lokalizacji)
  - **Move** (przy współdzielonym storage pomiędzy lokalizacjami - np. NFS) - przeniesienie tylko definicji PV na drugi klaster
- Transformacje storageclass, PV resizing
- Stage migration + Cut over

Red Hat

Red Hat Summit

Connect

Thank you

 linkedin.com/company/red-hat

 facebook.com/redhatinc

 youtube.com/user/RedHatVideos

 twitter.com/RedHat

Red Hat