vprotect by Storware

oVirt

# Disaster recovery strategies for oVirt

STORWARE

**Simplified Data Protection**

Storware provides highly efficient data protection solutions for all businesses.

# Key backup & disaster recovey areas

VM-level backup with snapshots

datacenter-level DR in oVirt

agent-less application protection

snapshot management

hypervisor configuration protection

# Backup strategy 1

## Export storage domain (RHV/oVirt/OLVM)

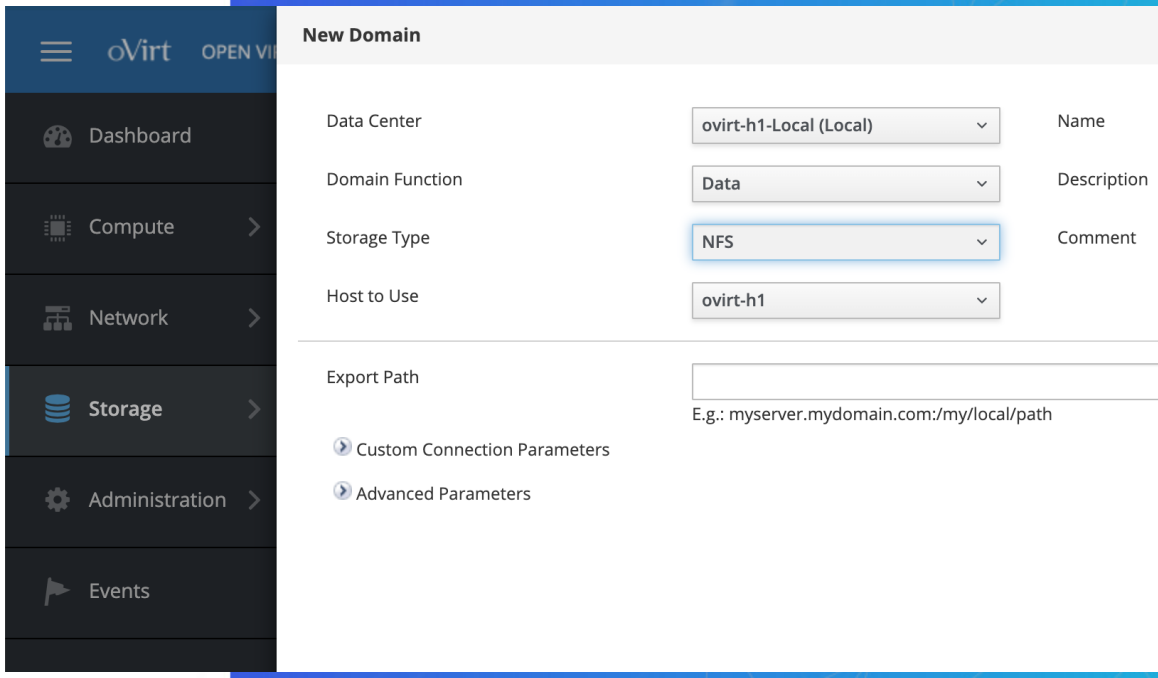
**Export storage domain/repository = staging space on the node**

**Pros:**

- supported since RHV/oVirt 3.5.1 (works with 4.0+)
- can be configured to write directly to the backup destination
  (file system)

**Cons:**

- RHV/oVirt requires additional VM cloning
- export storage domain management/setup
- no disk exclusion (RHV/oVirt)



# Backup strategy 2

## Disk attachment: Proxy VM

**vProtect Node installed as Proxy VM on the cluster**

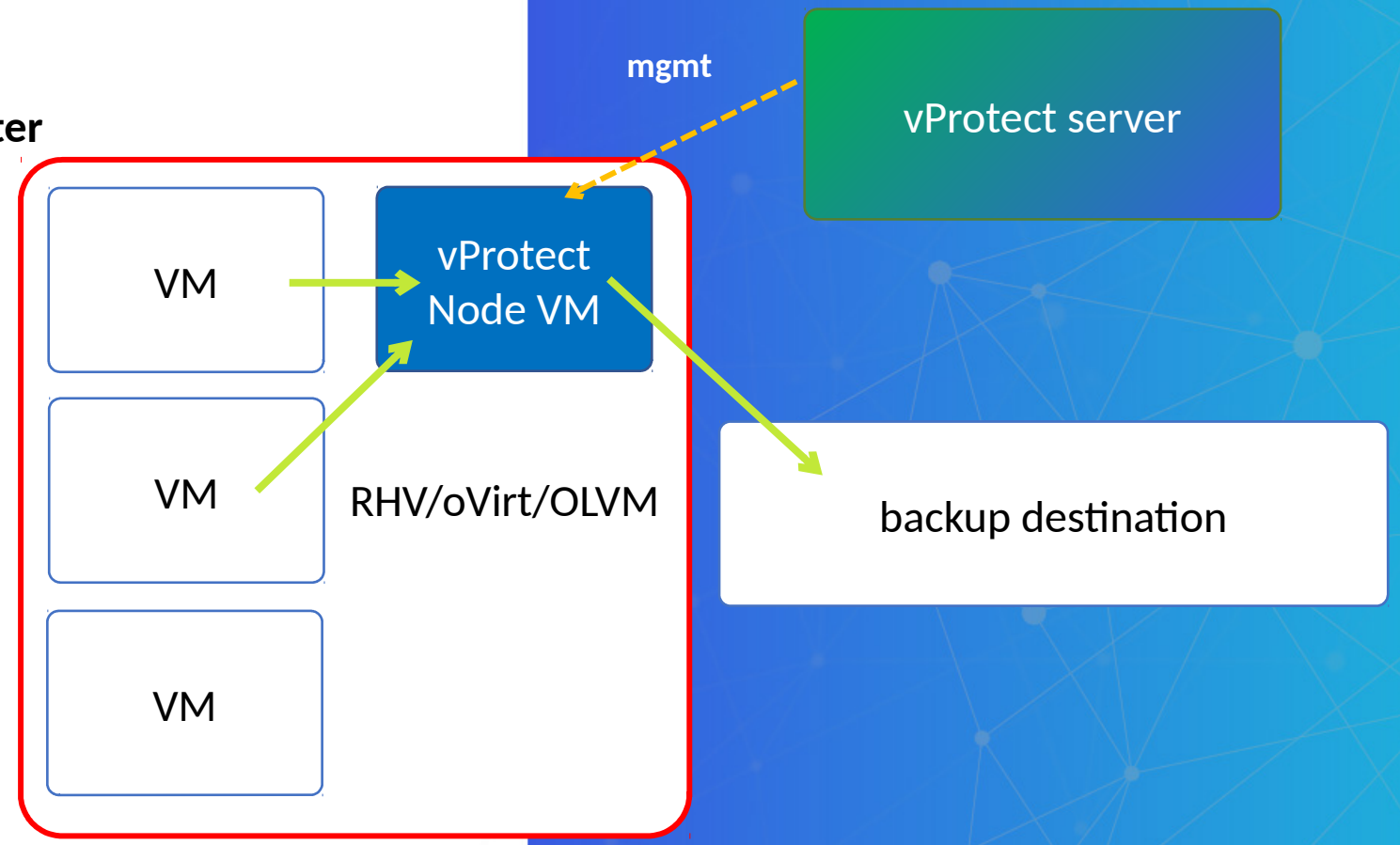
**VM disk snapshots attached and dumped via Proxy VM.**

**Pros:**

- no export storage domain requirement
- new RHV/oVirt/OLVM API (v4) used
- no additional cloning required
- disk exclusion suport
- data read directly from the storage

**Cons:**

- more complex backup proces
- no incremental backups at the moment



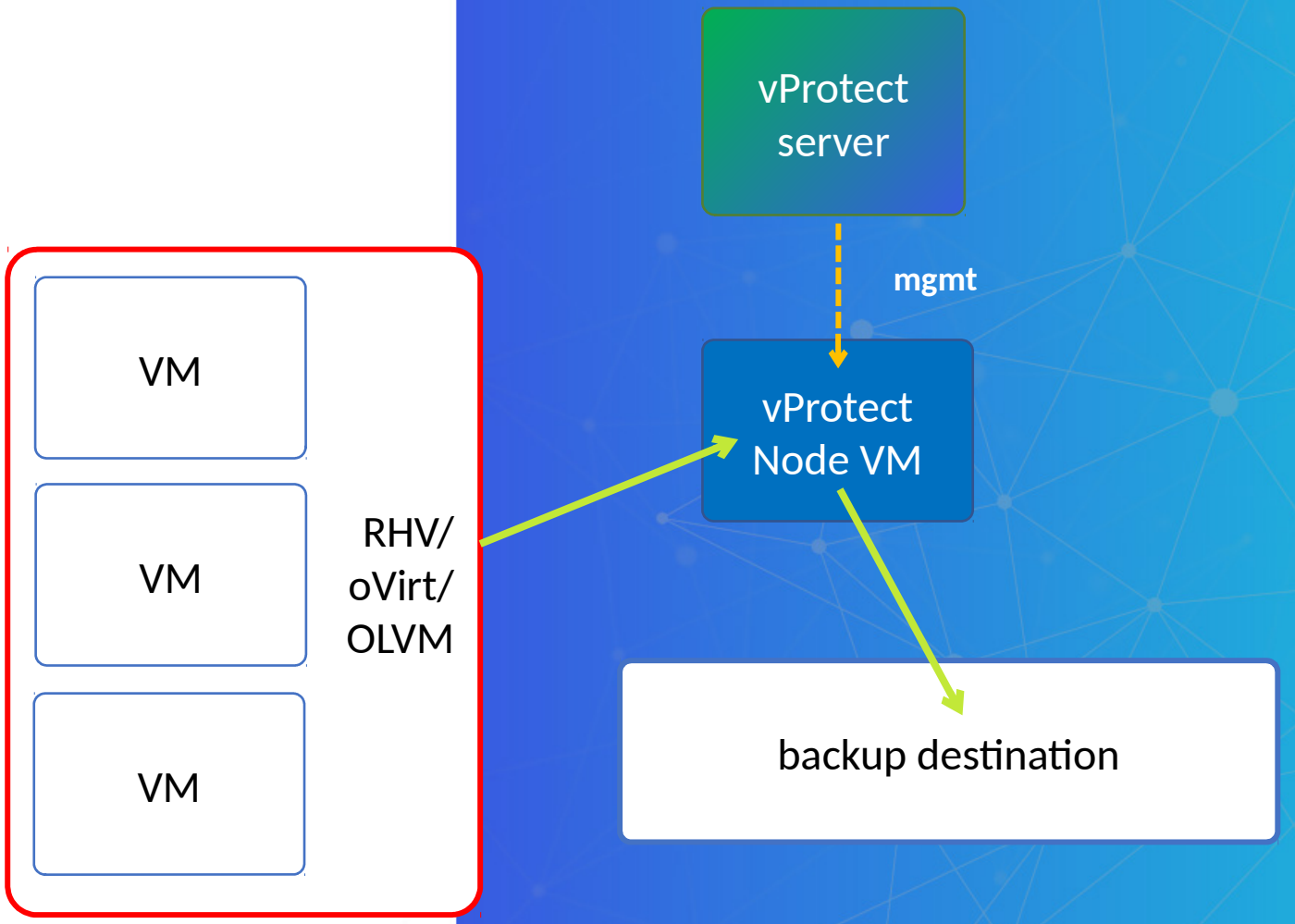
# Backup strategy 3

## Disk Image Transfer API

**vProtect Node talks with RHV/oVirt manager and requests snapshot export**

**Pros:**
- no export storage domain requirement
- new API (v4) used
- no additional cloning required
- disk exclusion support
- no proxy VM needed
- incremental backup option
- easy o setup

**Cons:**
- requires RHV/oVirt/OLVM 4.2
- data transfer passing through manager
- requires snapshot merge



# Backup strategy 4

## SSH transfer (RHV/oVirt/OLVM)

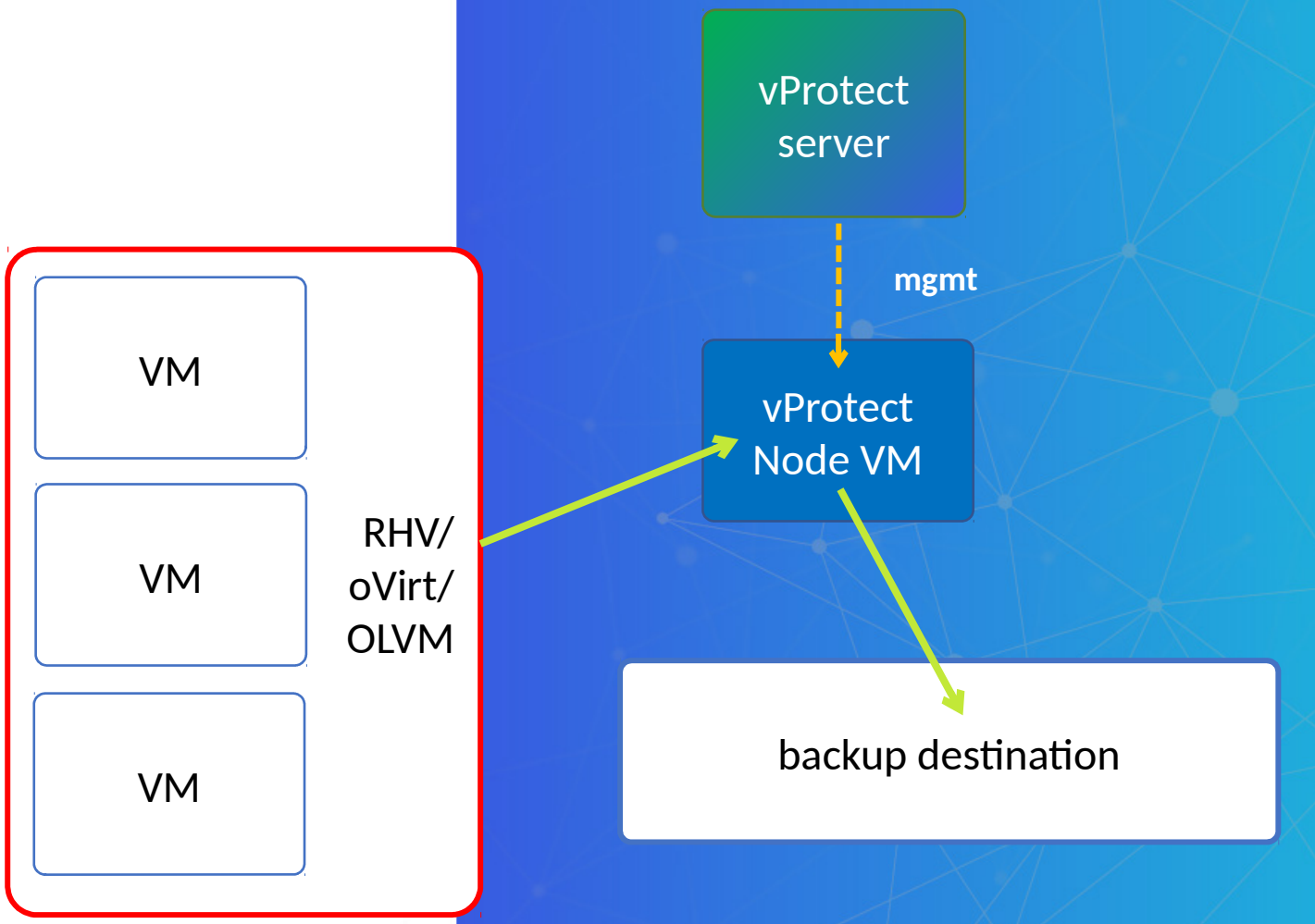
**vProtect Node talks with RHV/oVirt manager and requests snapshot export**

**Pros:**

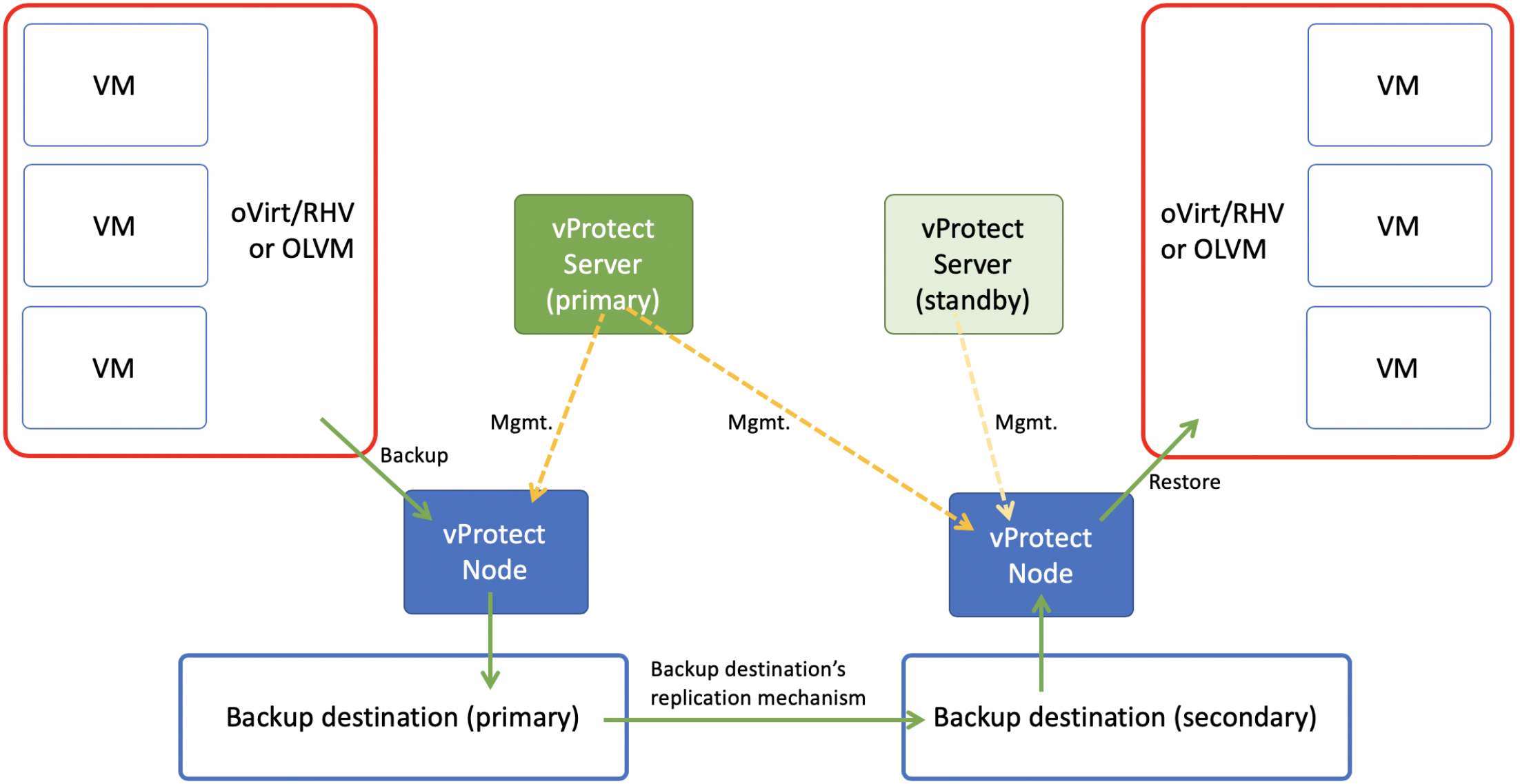
- no export storage domain requirement
- new API (v4) used
- no additional cloning required
- disk exclusion support
- no proxy VM needed
- incremental backup option
- direct data transfer from hypervisor
    - option to enhance transfer with netcat

**Cons:**

- requires snapshot merge
- root access to the hypervisor

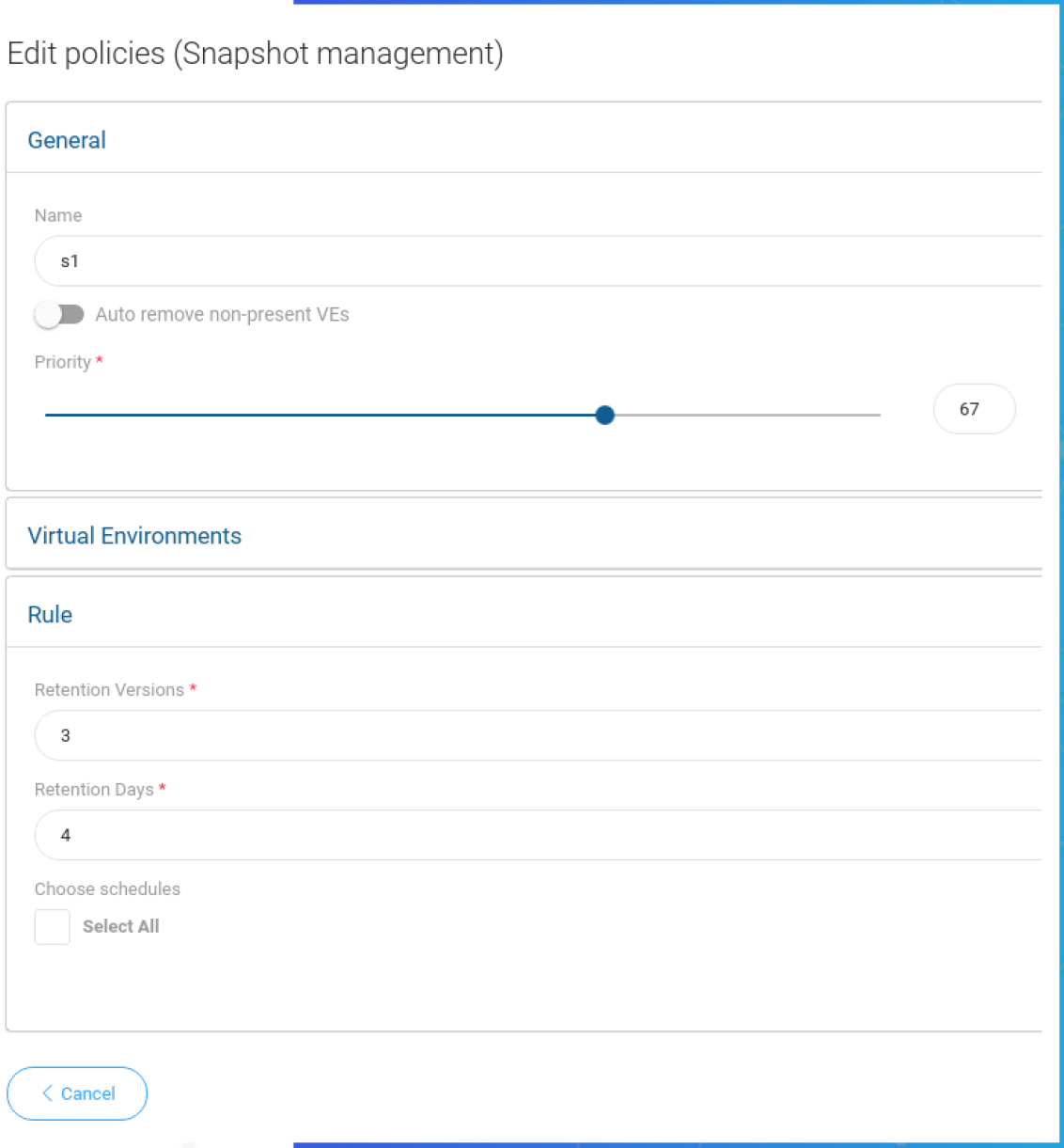


# Backup replication

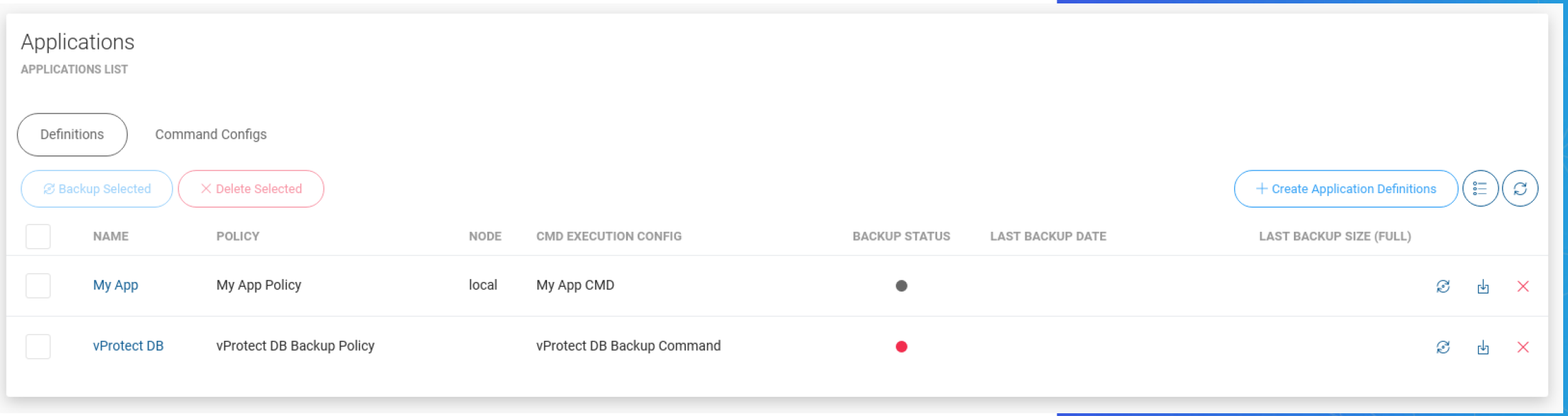


# Snapshot management

- Restore state of the VM without the need to restore data from the backup provider.
- vProtect creates snapshots periodically according to the policy (schedule and retention settings).
- Admin reverts VM using admin console of each Hypervisor platform or vProtect UI.



# Application backup

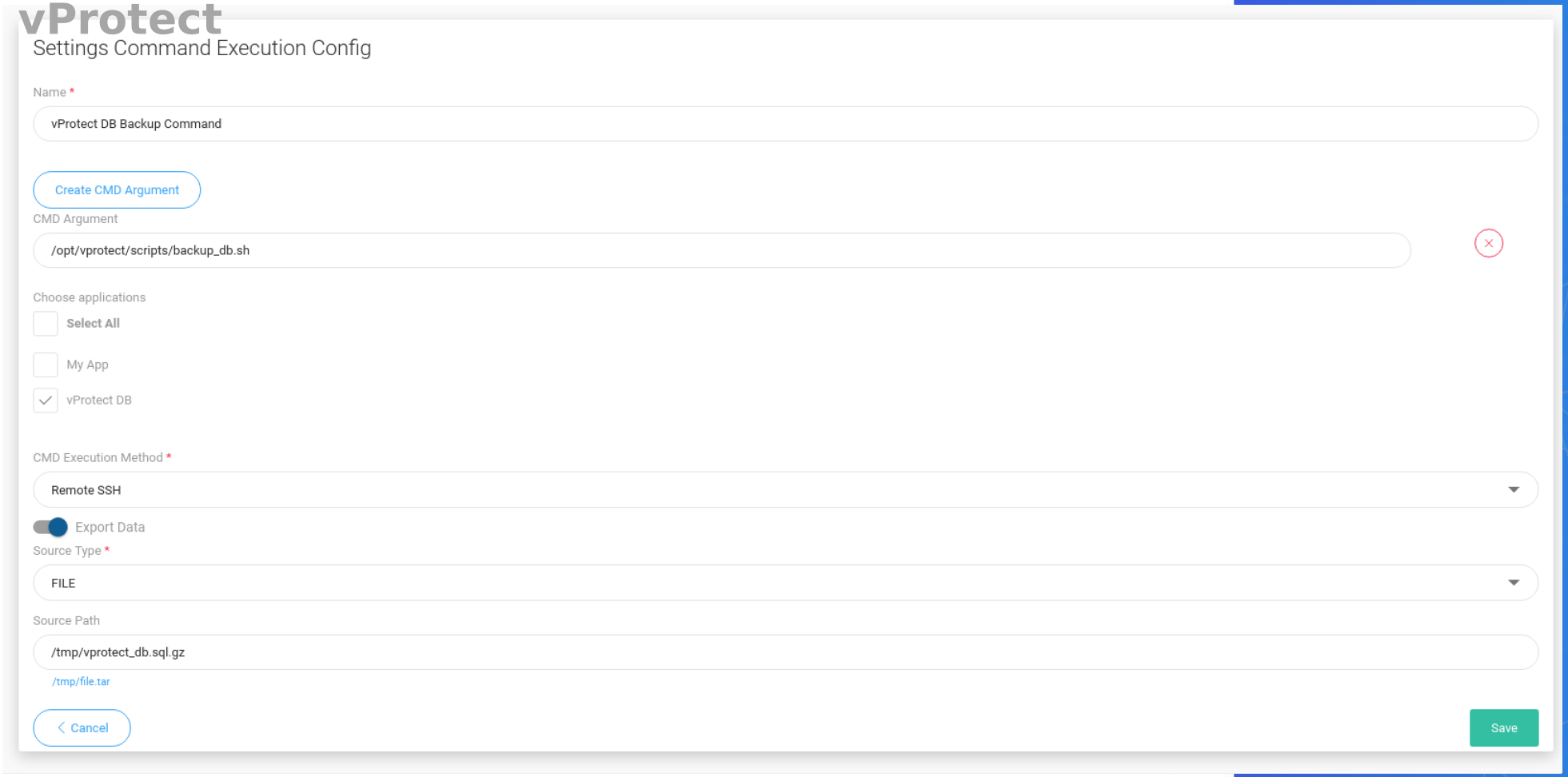



**Use case:**

- Generic backup using custom scripts provided by administrator.
- Scripts executed on the Node or via SSH on the target machine.
- Target application can be VM, Container or even physical.
- Apps can be anything: databases, custom applications, or just set of files.

# Application backup

## how to configure commands to be executed by vProtect



# Application backup – use cases

oVirt metadata protection

with engine-backup.

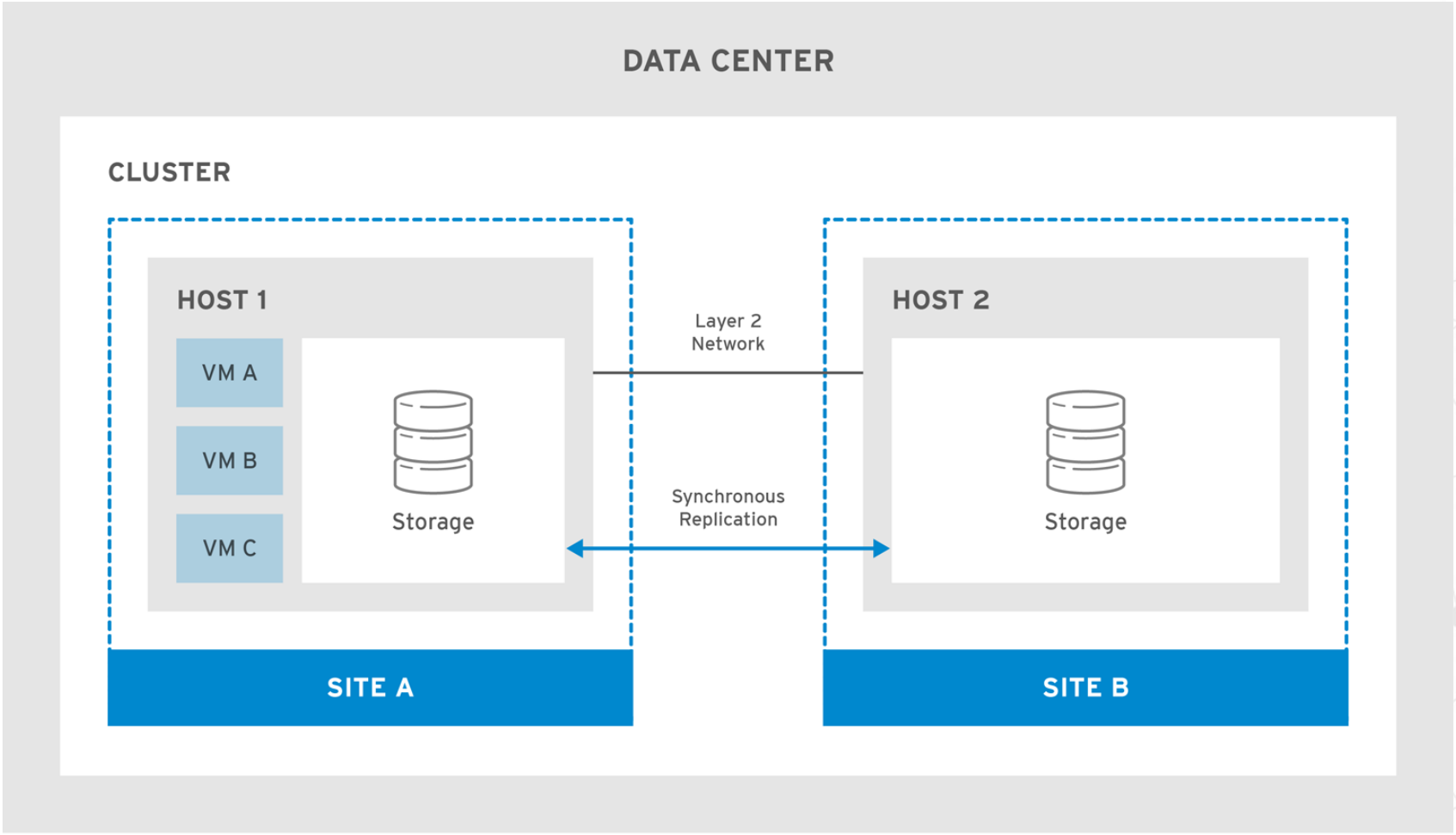
Existing old script-based backups

centralized for scheduling and reporting.

Databases and other applications running on VMs:

- native mechanisms to provide consistent backups
- when crash-consistent snapshots are not an option

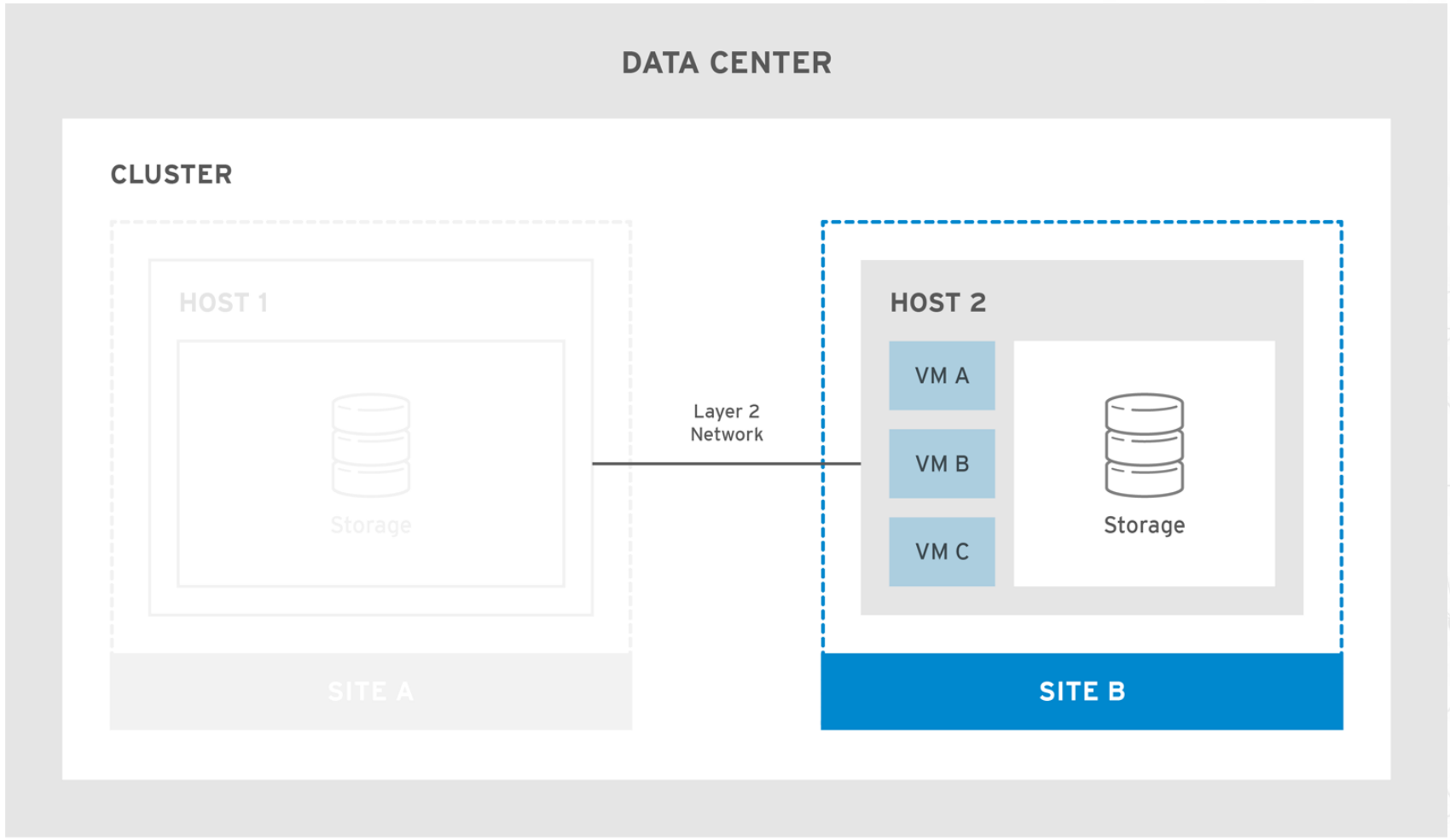
# DC replication - active-active DR




RHV_460251_1017

All the hosts belong to the same oVirt cluster.

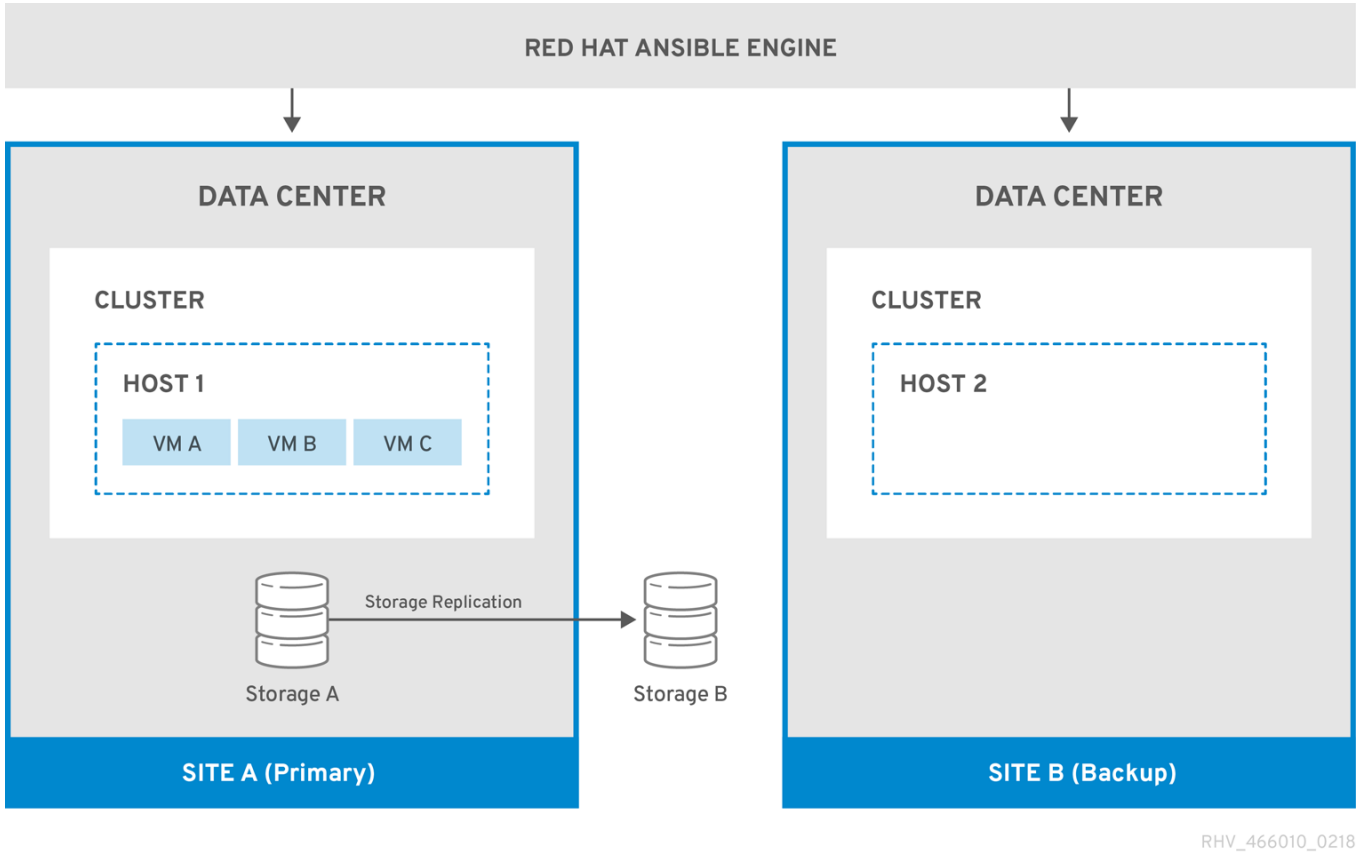
# DC replication - active-active DR




RHV_460251_1017

VMs will automatically failback to the primary site when the site becomes available and the storage is replicated in both sites.

# DC replication - active-passive DR




2 environments: the active primary, and the passive secondary (backup).

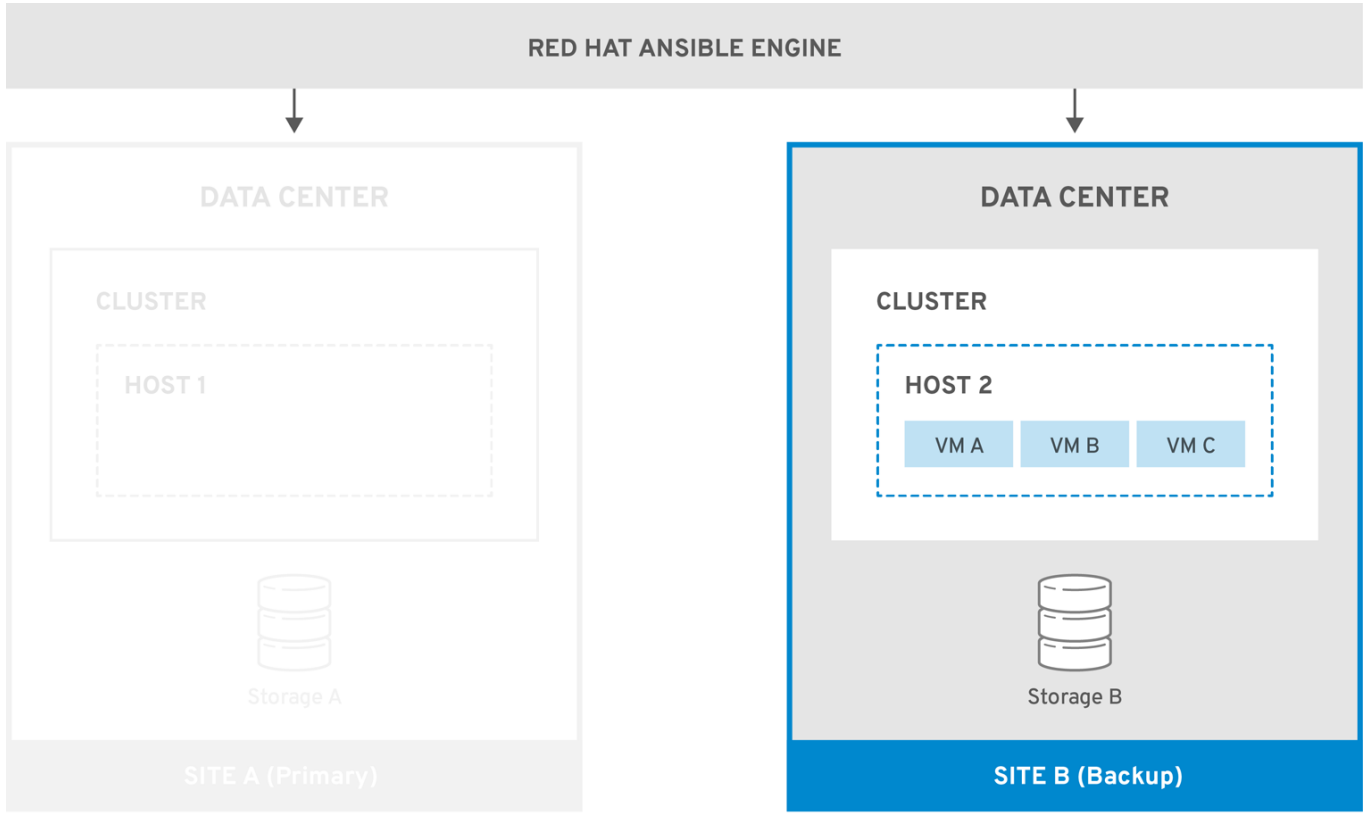
1. **Playbook to generate the mappin File**
   - create an Ansible playbook

   **ansible-playbook dr-rhv-setup.y --tags "generate_mapping”**
   - configure the mapping file (site details, clusters, storage domain etc.)

2. **Failover and Failback Playbooks**
   - create playbook and select sourc and target site

   **ansible-playbook dr-rhv-failover.yml --tags "fail_over"**

# DC replication - active-passive DR

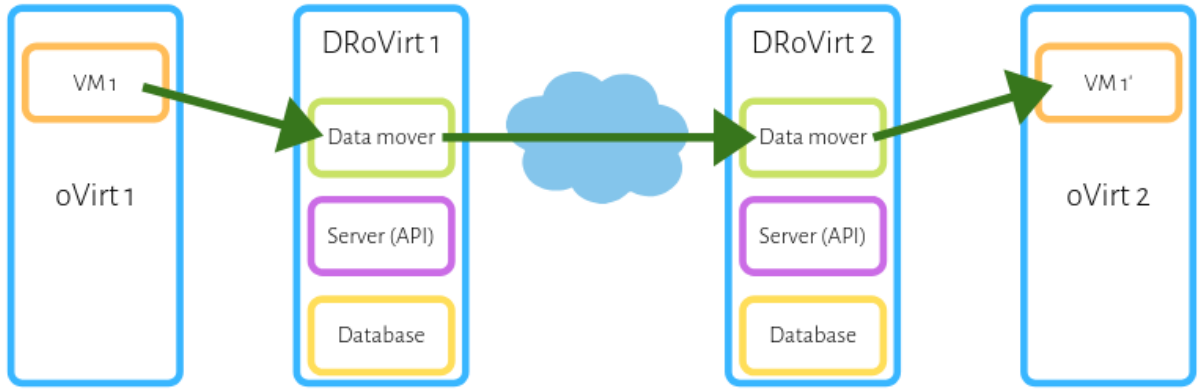



https://github.com/oVirt/ovirt-ansible-disaster-recovery

The **primary storage domain's block devices or shares** that contain virtual machine disks or templates **must be replicated**.

The **secondary storage must not be attached to any data center**, and will be added to the backup site's data center during failover.

# DRoVirt




Disaster Recovery / Replication for oVirt/RHV – storage agnostic

Planned 3 components:

- **Data-mover** - responsible for grabbing data periodically and transferring it
- **Server/API** - central management point to invoke tasks
- **Database** - small DB to store current tasks
- **CLI** - utility to easier manage the replication configuration tasks

The actual implementation of the replication is subject to discussion. Initially we want to start with oVirt/RHV 4.2 Disk Image Transfer API / SSH Transfer and later add additional strategies.

https://github.com/Storware/drovirt

# Key takeaways

**Snapshots** are **not a backups**

If you loose parts of your infrastructure, that affect VM – you'll use snapshot anyway.

**Replication** is **not a backup**

Any user error or ransomware activity is going to be replicated anyway.

**Agents cost time** to install them and manage

Agent-less approach is easier maintain.

**Conclusions:**

- you always need a backup
- best if it can be handled in an agent-less way
- enhance RTO/RPO with snapshot management or replication

STORWARE Sp. z o.o.

Leszno St. 8/44

01-192 Warsaw

Poland

info@storware.eu

mobile: +48 725 602 679

**Simplified Data Protection**

Storware provides highly efficient data protection solutions for all businesses.