MICRO FOCUS

Data Protector for Cloud Workloads 5.1

September 2022

Legal Notice

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see https://www.microfocus.com/en-us/legal/.

© Copyright 2022 Micro Focus or one of its affiliates.

Table of contents

- Quick guide
  - “All-in-One" Installation
  - Launch Data Protector for Cloud Workloads
  - Typical Scenarios
- Overview
  - Main Features
  - Architecture
  - Support Matrix
  - Platform Requirements
  - High Availability
  - Sizing Guide
- Deployment
  - Installation Overview
    - “All-in-One" Installation
    - Installation using Ansible playbook
    - Installation with RPMs
  - Backup Destinations
    - File System
      - File system
        - Virtual Data Optimizer (VDO)
    - Synthetic File System
      - XFS
    - Deduplication Appliances
      - Dell EMC Data Domain
    - Object Storage
      - Alibaba Cloud OSS
      - AWS S3 or S3-compatible
      - Ceph Rados Gateway
      - Cloudian S3
      - Google Cloud Storage
      - IBM Cloud Object Storage
      - Microsoft Azure Blob Storage
      - Nutanix Objects
      - OpenStack SWIFT
      - Oracle Cloud Infrastructure Object Storage
      - Scality RING
    - Enterprise Backup Providers
      - Micro Focus Data Protector
  - Initial Configuration
  - Common tasks
    - Staging space configuration
    - Enabling HTTPS connectivity for nodes
    - LVM setup on Data Protector for Cloud Workloads Node for disk attachment backup mode
    - Full versions of libvirt/qemu packages installation
    - SSH public key authentication
- Protecting Virtual Environments
  - Virtual Machines
    - Nutanix Acropolis Hypervisor (AHV)

            - Red Hat Virtualization
            - oVirt
            - Oracle Linux Virtualization Manager
            - Oracle VM
            - Proxmox VE
            - KVM/Xen
            - OpenStack
            - Citrix Hypervisor (XenServer)
            - XCP-ng
            - Huawei FusionCompute
            - Scale Computing HC3
        - Cloud
            - AWS EC2
        - Containers
            - Kubernetes
            - Red Hat OpenShift
            - Proxmox VE
        - Backup & Restore
- Protecting Microsoft 365
    - Microsoft 365 organization management
        - Configure Microsoft 365 access
        - Add Microsoft 365 organization manually
        - Add Microsoft 365 organization using the Setup Assistant
        - Account auto-synchronization
    - Backup & Restore
    - Supported Sharepoint templates and limitations
- Protecting Applications
    - Applications
        - Relax and Recover - ReaR
        - Git
    - Backup and restore of Application
- Protecting Storage Providers
    - Storage Providers
        - Ceph RBD
        - Nutanix Files
        - Nutanix Volume Groups
    - Backup & Restore
- Administration
    - Dashboard
    - Virtual Environments
        - Instances
            - Backup on-demand
            - Restore on-demand
            - Snapshot Management
        - Infrastructure
        - Backup SLAs
            - Policies
            - Schedules
        - Snapshot SLAs
            - Policies
            - Schedules
        - Recovery Plans

            - Policies
            - Schedules
        - Mounted Backups (File-level Restore)
    - Storage Providers
        - Instances
            - Backup on-demand
            - Restore on-demand
        - Infrastructure
        - Backup SLAs
            - Policies
            - Schedules
        - Snapshot SLAs
            - Policies
            - Schedules
        - Mounted Backups (File-level Restore)
    - Cloud
        - Instances
        - Service Providers
        - Backup SLAs
            - Policies
            - Schedules
        - Download
    - Applications
        - Instances
        - Execution Configurations
        - Backup SLAs
    - Reporting
        - Virtual Environments
        - Storage
        - Cloud
        - Applications
        - Audit Log
    - Nodes
        - Instances
        - Node Configurations
    - Access Management
        - Users
        - Groups
        - Roles
        - OS Credentials
    - Settings
        - Global Settings
        - Internal DB Backup
        - Notification Rules
        - Mailing Lists
    - Upgrade
    - CLI Reference
- Integration
- Integration Plugins
    - Red Hat Virtualization UI Plugin
    - oVirt UI Plugin
    - Oracle Linux Virtualization Manager UI Plugin

    - OpenStack UI Plugin
- Troubleshooting
    - How to enable Data Protector for Cloud Workloads DEBUG mode
    - Collecting logs
    - External log targets
    - Disaster Recovery
- Known software issues and limitations
- Glossary

Quick guide

Data Protector for Cloud Workloads Server can be easily installed on a single server. It can be a physical or virtual machine. In both cases, the steps you need to follow are basically the same. Four steps required to deploy it are listed below:

1. Prepare server platform
2. Install Data Protector for Cloud Workloads
3. Select the area to backup
4. Perform backup & recovery

Before you start the installation process, you have to configure your machine and add disk space to store your backups. Go to the **Sizing Guide** chapter to prepare your server platform based on the size of the area to be backed up. After your system platform is configured you can proceed with Data Protector for Cloud Workloads installation.

Go to the All-in-One Installation section to learn about the swift installation of Data Protector for Cloud Workloads.

“All-in-One" Installation

Data Protector for Cloud Workloads can be easily installed on a single box quickly. This approach installs a server and node on the same box and generates an SSL certificate based on the hostname where it is installed. This corresponds to Ansible deployment, with the node and server roles installed on the same host. The end result should be the same as an RPM-based installation without a staging setup. Configuration (such as backup destination definition or hypervisor connectivity) still needs to be done after installation. You can also add more nodes in the future if necessary.

Installation

> Before installing Data Protector for Cloud Workloads we highly recommend doing a system update and reboot.

1. Install CentOS 8 Stream or RHEL 8 minimal with 6 GB of RAM and 2 vCPUs and some storage for staging space and optionally a backup destination:
    - use first disk for operating system
    - add a secondary disk, i.e. 200GB - 1 TB (depending on the size your VMs that you want to backup)
    - leave it empty, you'll initialize this space later
2. Log in as root over SSH to your machine, where you want to install it.
3. RHEL 8 requires active subscription.
4. Download Data Protector for Cloud Workloads package.
5. Extract this package on the host where you're installing it:

    ```
    tar xvf DP-for-Cloud-Workloads-XXX.tgz
    ```

6. Move extracted repository to temp directory:

    ```
    mv elX /tmp/DP-for-Cloud-Workloads-repo
    ```

7. As root run:

    ```
    ./DP-for-Cloud-Workloads-local-install.sh
    ```

8. Update the proxy details in /opt/vprotect/vprotect.env for cloud backup/restore and restart the server and node services.

> Use system command **hostnamectl** to obtain the proper name for host. Add this entry in section **no_proxy**.

With a proper repo url (this can be changed with DP_REPO environment variable) – by default repo URL points to local directory file:///tmp/DP-for-Cloud-Workloads-repo.

Now you should be able to log in to Data Protector for Cloud Workloads Server using https://<DP4CW_server_IP> with local node registered and running.

Update

This package replaces previous installation. Database model and any dependencies may be updated during update. All configuration stored in the database or migrated to the new model automatically if necessary.

Server Upgrade

1. Create database backup - run as root over SSH on the Data Protector for Cloud Workloads Server

```
/opt/vprotect/scripts/backup_db.sh /path/to/backup/file.tgz
```

2. Extract this package on the hosts with Data Protector for Cloud Workloads Server or Node:

```
tar xvf DP-for-Cloud-Workloads-XXX.tgz
```

3. Update Data Protector for Cloud Workloads Server using RPMs in elX folder

```
yum update elX/DP-for-Cloud-Workloads-server-XXX.elX.x86_64.rpm
```

4. Update each Data Protector for Cloud Workloads Nodes using RPMs in elX folder

```
yum update elX/DP-for-Cloud-Workloads-node-XXX.elX.x86_64.rpm
```

5. Update each Data Protector for Cloud Workloads Cloud Server:

```
yum update elX/DP-for-Cloud-Workloads-cloudserver-XXX.elX.x86_64.rpm
```

6. Update each Data Protector for Cloud Workloads Cloud Agent:

```
yum update elX/DP-for-Cloud-Workloads-cloudagent-XXX.elX.x86_64.rpm
```

7. Log in to the Data Protector for Cloud Workloads Server using https://<DP4CW_server_IP> with nodes updated and running.

Notice, that you may need to refresh your browser cache after update - for Chrome use CTRL+SHIFT+R (Windows/Linux) / CMD+SHIFT+R (MacOS)

Downgrade

1. Downgrade Server with yum:

```
yum downgrade vprotect-server
```

2. On the Data Protector for Cloud Workloads Server host stop the Server service, restore database using your DB password and start server again (these can be found in `/opt/vprotect/payara.properties` file)

```
systemctl stop vprotect-server
mysql -u vprotect -pDBPASSWORD -e "drop database vprotect"
mysql -u vprotect -pDBPASSWORD -e "create database vprotect"
gunzip < PATH_TO_GZIPPED_BACKUP | mysql -u vprotect -pDBPASSWORD vprotect
systemctl start vprotect-server
```

3. On the Data Protector for Cloud Workloads Nodes hosts - downgrade nodes with

```
yum downgrade vprotect-node
```

4. Make sure all nodes are running and optionally start service on each Data Protector for Cloud Workloads host

```
systemctl start vprotect-node
```

Deinstallation

1. Remove packages with yum:

```
yum remove vprotect-server
yum remove vprotect-node
```

2. To remove configuration files:

```
rm -rf /opt/vprotect
```

3. To remove all remaining MariaDB data:

```
yum remove mariadb mariadb-server
rm -rf /var/lib/mysql
rm /etc/my.cnf
Optional step:
rm ~/.my.cnf
rm -f /var/log/mariadb
rm -f /var/log/mariadb/mariadb.log.rpmsave
rm -rf /usr/lib64/mysql
rm -rf /usr/share/mysql
```

4. To remove users:

```
userdel vprotect
userdel mysql
```

Launch Data Protector for Cloud Workloads

Data Protector for Cloud Workloads will protect organizations in many different areas. It is possible to backup only one, mix the areas, or even backup all of them. Select the ones that interest you:

- Virtual Environments
- Cloud
- Applications
- Storage
- Endpoints

Typical Scenarios

Backup & Recovery

The core functionality of Data Protector for Cloud Workloads is an **agentless backup** for multiple virtualization, container, cloud platforms, storage providers and applications.

With snapshot-based backups, you don't have to install an agent inside VMs or customize your hypervisors.

Backups performed by Data Protector for Cloud Workloads usually are crash-consistent, but you can enable **application consistency** or enhance the backup process with your own **custom pre/post snapshot remote command execution**.

Snapshots are exported from your virtualization platform and can be stored in the backup provider of your choice. You can use enterprise-grade backup providers, object storage, or just a file system as your target.

This means that Data Protector for Cloud Workloads can act as a **stand-alone solution** or as a **proxy to your existing storage or enterprise backup provider.**

You also can periodically restore your VMs to verify if your backups are consistent.

With mounted backups, you can also **restore individual files** from your backups via a Web UI or directly from Data Protector for Cloud Workloads Node.

Disaster Recovery

Real disasters can sometimes happen - with Data Protector for Cloud Workloads you can configure your backups to be performed in one datacenter and - if necessary - restore them in a second datacenter.

Data Protector for Cloud Workloads can use replicated file systems or other built-in backup provider mechanisms to allow you to keep a copy in the secondary data center.

During DR, you can use Recovery Plans to restore multiple VMs to a predefined location.

Snapshot Management

Backups are usually quite an intensive operation. Snapshots have to be exported and stored, which usually means that you can't perform them too often. With Data Protector for Cloud Workloads, you can use Snapshot Management policies to periodically create additional snapshots on your VMs without the need to export them.

When you need to restore a VM to the most recent saved state, you can quickly revert to a snapshot that Data Protector for Cloud Workloads has created for you.

Application Backup & Recovery

There are many cases where VM-level backup may not be enough. Applications such as databases usually have their own mechanisms that guarantee consistent backups. As we are aware, in many situations you need to have the option to customize the backup process - therefore Data Protector for Cloud Workloads provides a **generic mechanism** for multiple scenarios.

You can prepare a custom script or invoke any backup command that produces backup artifacts (or just initiates the external backup process) on a remote host and stores backups to your backup provider.

With Application backup, you can extend your protection capabilities to:

- any remote applications with their own mechanisms
- hypervisor configuration

- files on remote hosts (physical, virtual, or containers)
    - this includes shares, mounted object-storage buckets, LVM block devices, or virtually anything which can be presented as a file
- initiating external backup processes such as RMAN

Overview

In this section, we'll briefly discuss the architecture and main features of Data Protector for Cloud Workloads as well as some typical use case scenarios.

The Main Features section briefly summarizes the key functionalities of the Data Protector for Cloud Workloads solution.

In the Architecture section, you will learn what the main components of the Data Protector for Cloud Workloads solution are, as well as find out how to place them in your deployment.

In the Support Matrix you can check versions of supported virtualization platforms, backup, and cloud providers.

Platform requirements present what are hardware and software requirements needed to run Data Protector for Cloud Workloads components.

High availaibility section provides guidance to plan Data Protector for Cloud Workloads solutions resistant to failures.

Sizing Guide is the place where we present key information that the user needs to collect before the installation process.

Main Features

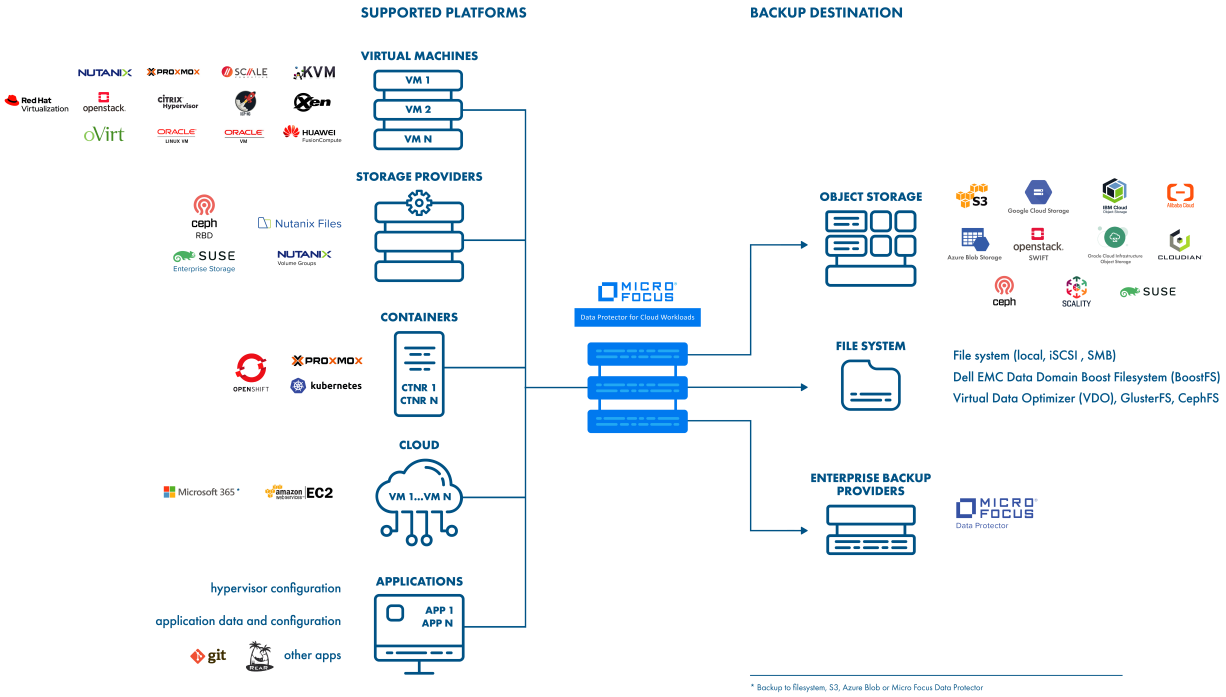
- VM-level, Container-level backup, and recovery
- Storage Provider (Ceph RBD, Nutanix Files, and Nutanix Volume Groups) backup & recovery
- Full and Incremental backups (with native CBT, CRT where available)
- VM data is exported in native (hypervisor-specific) format
- Backup only selected VM disk option
- Deployment protection (PVs and deployment metadata) for Kubernetes and OpenShift environments
- Support for a wide range of virtual platforms, containers, and cloud such as:
    - Microsoft 365
    - Red Hat Virtualization
    - oVirt
    - Oracle Linux Virtualization Manager
    - Nutanix Acropolis Hypervisor (AHV)
    - Citrix Hypervisor (XenServer)
    - XCP-ng
    - Proxmox VE
    - Oracle VM
    - OpenStack
    - libvirt hypervisors (KVM, PowerKVM, KVM for IBM z, Xen)
    - Kubernetes
    - Red Hat OpenShift
    - AWS EC2
    - Huawei FusionCompute
    - Scale Computing HC3
- Pre/post snapshot remote command execution on VM to enable operations such as DB quiesce
- Pre/post backup destination access command execution to allow mount/unmount operations on external storage providers
- Prioritized backup policies
- VM automatic policy assignment based on regular expressions and tags
- Snapshot Management (Copy Data Management)
- Snapshot consistent technology (quiesced snapshots)
- File-level restore using mountable backups
- Mounted backups - RAW disks shareable over iSCSI (for direct block-access to your backup data)
- Recovery plans for automated DR - on-demand restore of multiple VMs when needed, or on a scheduled basis for testing
- Generic application backup with your custom scripts with ready templates for commonly used databases
- OpenStack and KVM stand-alone with Ceph RBD storage support
- Multi-node support for better scalability or geographically dispersed environments
- Built-in Data Protector for Cloud Workloads DB backup
- Data encryption for file system backup destination
- Secondary backup destination to stare data to more than one location
- Immutable Backup (XFS-based backup destination) that protects backup data from being encrypted by ransomware
- LDAP authentication
- Integration with different backup destinations such as:
    - Any mounted file system (local or remote, especially GlusterFS for replication, CephFS, NFS, SMB, and many more)
    - Dell EMC Data Domain (BoostFS integration)
    - Amazon S3 (with Amazon Glacier as a 2nd tier archive storage),

    - S3-compliant storage (IBM Cloud, Oracle Cloud, Scality RING)
    - Google Cloud Storage
    - Microsoft Azure Blob Storage
    - OpenStack Swift
    - MicroFocus DataProtector
- Built-in data deduplication with Virtual Data Optimizer (VDO)
- Easy to use and modern management (HTML5 web UI and CLI)
- Open API for 3rd party software integration (REST API)

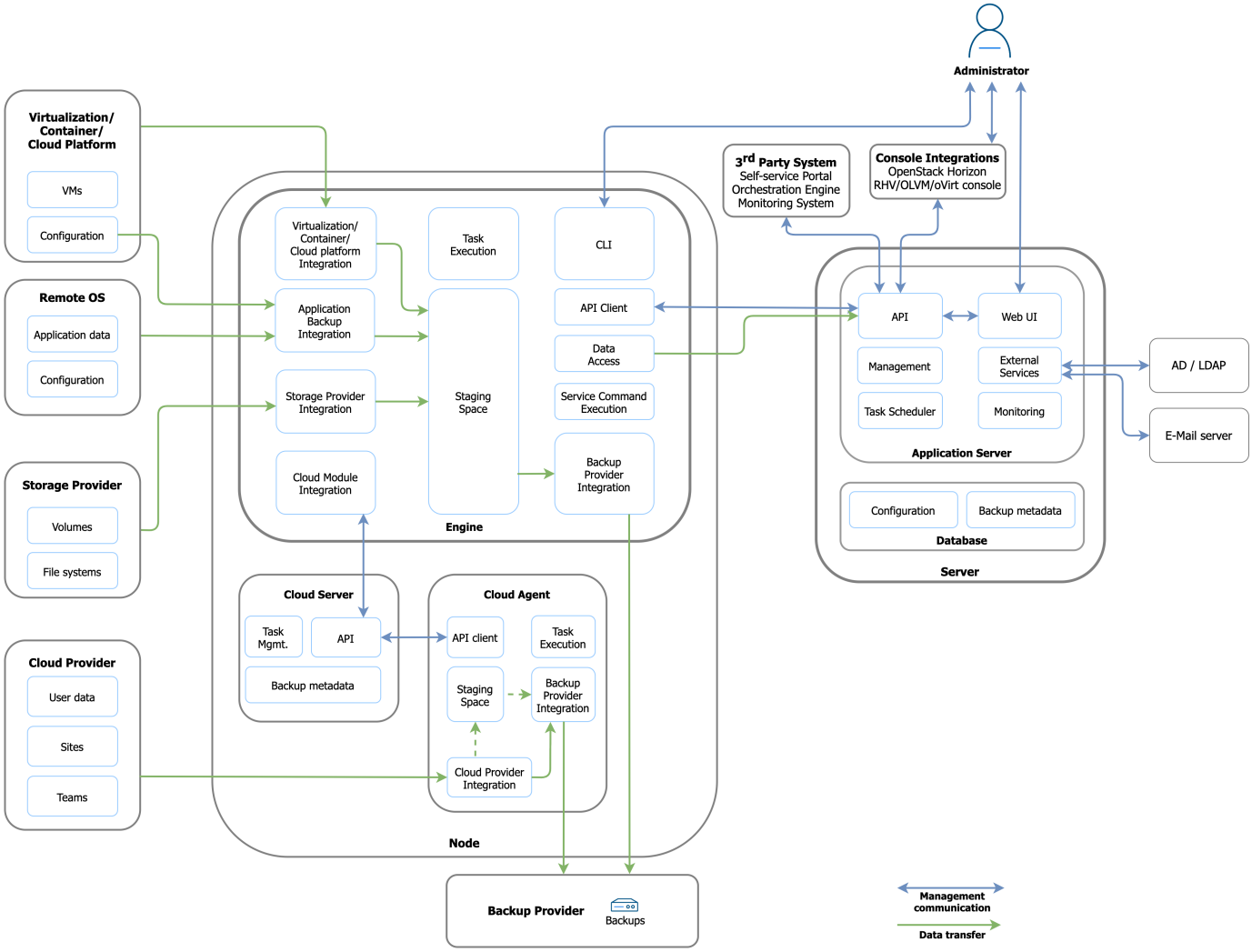
Architecture

High-level Architecture

Use Data Protector for Cloud Workloads to back up data from your virtualization platforms, M365 Cloud and storage providers. You can back up data to and recover data from a local filesystem or an NFS/CIFS share, object storage (cloud providers), or Micro Focus Data Protector.



Detailed Architecture



Data Protector for Cloud Workloads consists of 2 main components:

- **Data Protector for Cloud Workloads Server** - the central point of Data Protector for Cloud Workloads management, provides administrative Web UI, APIs and is a central repository of metadata
- **Data Protector for Cloud Workloads Node** - data mover that performs backups, restores, and mounts:
  - multiple nodes can be deployed for scalability or other reasons,
  - all nodes are managed by the server and need to be registered to the server.

Component placement

- **Data Protector for Cloud Workloads Server and Node can be installed on the same host.**
- The Server can be installed on a physical machine or VM - externally deployed nodes require network connectivity to the Server and PowerProtect DD target(s).
- Nodes may be deployed as physical or virtual systems unless the selected backup strategy requires the Node to be installed as a VM on a Hypervisor Cluster (especially when the "disk attachment" export mode is mentioned).
- Both components are installed on a CentOS 8 Stream or RHEL 8 minimal.

For detailed deployment scenarios refer to the following sections:

Virtual Environments

Microsoft 365

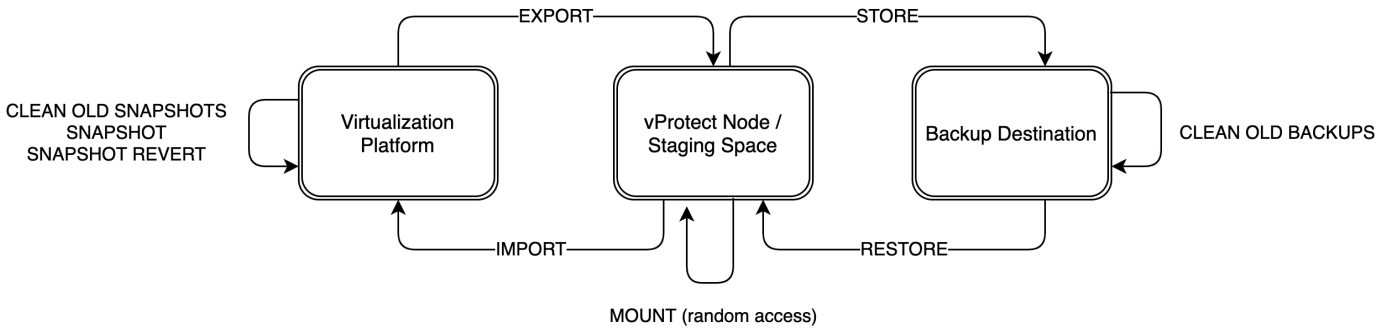
Applications

Storage Providers

Typical workflows

There are several standard workflows in Data Protector for Cloud Workloads and they result in a set of tasks:

- **Backup**
  - **Export** - a task that creates backup or snapshot and exports data to the staging space
  - **Store** - a task that moves data to the backup destination
- **Restore to filesystem**
  - **Restore** - a task that gets data from a backup provider and puts data in the staging space
- **Restore to a virtualization platform**
  - **Restore** - a task that gets data from a backup provider and puts data in the staging space (if it is a full backup that is being restored residing on the file system backup provider - this task just informs where files are waiting for import task)
  - **Import** - a task that imports data to the virtualization platform and recreates VM
- **Restore for a mount (file-level restore)**
  - **Restore** - a task that gets data from a backup provider and puts data in the staging space (if it is a full backup that is being restored residing on the file system backup provider - this task just informs where files are waiting for mount task)
  - **Mount** - mounts backup on the Data Protector for Cloud Workloads Node and either allows user to browse files or exposes backup over iSCSI, so that remote iSCSI initiator can access it)
- **Snapshot**
  - **Snapshot** - a task that creates a local persisted snapshot of a VM in the hypervisor environment according to a policy that was assigned to the VM - snapshots that are no longer needed (according to the policy) will be removed



Support Matrix

Backup Destination Support

Filesystem

Backup Provider	Supported version	Random Access	Deduplication	Encryption	Pre/post access command execution
Filesystem	N/A	✅	✅ (built-in VDO)	✅	✅
Filesystem (synthetic, XFS)	Linux kernel 4.15+, xfsprogs 4.17+	✅	✅ (built-in VDO)	❌	✅
PowerProtect DD	DD OS 7.x	✅	✅	✅	✅

Object storage

Backup Provider	Supported version	Random Access	Deduplication	Encryption	Pre/post access command execution
Amazon S3	Current	❌	N/A	✅	✅
S3 compatible	Current	❌	N/A	✅	✅
Cloudian S3	Current	❌	N/A	✅	✅
Alibaba Cloud OSS	Current	❌	N/A	✅	✅
Nutanix Objects	Current	❌	N/A	✅	✅
MS Azure Blob Storage	Current	❌	N/A	✅	✅
OpenStack Swift	API v2	❌	N/A	❌	✅
Scality Ring	6.4+	❌	N/A	Provider dependent	✅

Enterprise backup providers

Backup Provider	Supported version	Random Access	Deduplication	Encryption	Pre/post access command execution
Micro Focus Data Protector	11+	❌	✅	Provider dependent	✅

Virtualization Platforms - features and requirements

Nutanix AHV

	Disk-attachment

	Disk-attachment
Minimum version	5.5+ (Intel-only)
Status	In operation (**preferred**)
Last snapshot kept on hypervisor for inc. backups	yes
Hypervisor OS access needed	no
Proxy VM needed	yes

Feature	Disk-attachment
Incremental backup	✅
File-level restore	✅
VM disk exclusion	✅
Snapshot management	✅
Quiesced snapshot	✅
Pre/post snapshot command execution	✅
Backup disks sharable over iSCSI	✅
Name-based policy assignment	✅
Tag-based policy assignment	✅ (when using Prism Central)
Available space for snapshot check	❌ (hypervisor-dependent)
Power-on VM after restore	✅

Red Hat Virtualization

	Export storage domain	Disk-attachment	Disk Image Transfer	SSH Transfer	Changed-Block Tracking
Minimum version	3.5.1+	4.0+	4.3+	4.3+	4.4+
Status	To be deprecated	In operation	In operation	In operation (**preferred**)	Technical preview
Last snapshot kept on hypervisor for inc. backups	yes	yes	yes	yes	no
Hypervisor OS access needed	no	no	no	yes	no
Proxy VM needed	no	yes	no	no	no

	Export storage domain	Disk-attachment	Disk Image Transfer	SSH Transfer	Changed-Block Tracking
Key caveats	using old API v3 additional snapshot-cloning required	full backup only disk attachment process may be slow	data transfer via Manager	access to the hypervisor needed	using technical preview APIs incremental backup require QCOW2 disk format

Feature	Export storage domain	Disk-attachment	Disk Image Transfer	SSH Transfer	Changed-Block Tracking
Incremental backup	❌	❌	✅	✅	✅
File-level restore	✅	✅	✅	✅	✅
VM disk exclusion	❌	✅	✅	✅	✅
Snapshot management	✅	✅	✅	✅	✅
Quiesced snapshot	✅	✅	✅	✅	✅
Pre/post snapshot command execution	✅	✅	✅	✅	✅
Backup disks sharable over iSCSI	✅	✅	✅ (RAW-only)	✅ (RAW-only)	✅
Name-based policy assignment	✅	✅	✅	✅	✅
Tag-based policy assignment	✅	✅	✅	✅	✅
Available space for snapshot check	✅	✅	✅	✅	✅
Power-on VM after restore	❌	✅	✅	✅	✅

oVirt

	Export storage domain	Disk-attachment	Disk Image Transfer	SSH Transfer	Changed-Block Tracking
Minimum version	3.5.1+	4.0+	4.3+	4.3+	4.4+
Status	To be deprecated	In operation	In operation	In operation (**preferred**)	Technical preview

	Export storage domain	Disk-attachment	Disk Image Transfer	SSH Transfer	Changed-Block Tracking
Last snapshot kept on hypervisor for inc. backups	yes	yes	yes	yes	no
Hypervisor OS access needed	no	no	no	yes	no
Proxy VM needed	no	yes	no	no	no
Key Caveats	using old API v3 additional snapshot-cloning required	full backup only disk attachment process may be slow	data transfer via Manager	access to the hypervisor needed	using technical preview APIs incremental backup require QCOW2 disk format

Feature	Export storage domain	Disk-attachment	Disk Image Transfer	SSH Transfer	Changed-Block Tracking
Incremental backup	❌	❌	✅	✅	✅
File-level restore	✅	✅	✅	✅	✅
VM disk exclusion	❌	✅	✅	✅	✅
Snapshot management	✅	✅	✅	✅	✅
Quiesced snapshot	✅	✅	✅	✅	✅
Pre/post snapshot command execution	✅	✅	✅	✅	✅
Backup disks sharable over iSCSI	✅	✅	✅ (RAW-only)	✅ (RAW-only)	✅
Name-based policy assignment	✅	✅	✅	✅	✅
Tag-based policy assignment	✅	✅	✅	✅	✅
Available space for snapshot check	✅	✅	✅	✅	✅
Power-on VM after restore	❌	✅	✅	✅	✅

	Disk-attachment	Disk Image Transfer	SSH Transfer
Minimum version	4.3+	4.3+	4.3+
Status	In operation	In operation	In operation (**preferred**)
Last snapshot kept on hypervisor for inc. backups	yes	yes	yes
Hypervisor OS access needed	no	no	yes
Proxy VM needed	yes	no	no
Key Caveats	full backup only disk attachment process may be slow	data transfer via Manager	access to he hypervisor needed

Feature	Disk-attachment	Disk Image Transfer	SSH Transfer
Incremental backup	❌	✅	✅
File-level restore	✅	✅	✅
VM disk exclusion	✅	✅	✅
Snapshot management	✅	✅	✅
Quiesced snapshot	✅	✅	✅
Pre/post snapshot command execution	✅	✅	✅
Backup disks sharable over iSCSI	✅	✅ (RAW-only)	✅ (RAW-only)
Name-based policy assignment	✅	✅	✅
Tag-based policy assignment	✅	✅	✅
Available space for snapshot check	✅	✅	✅
Power-on VM after restore	✅	✅	✅

Proxmox VE

	Export storage repository	SSH Transfer
Minimum version	5.2+	5.2+
Status	In operation	In operation (**preferred**)
Last snapshot kept on hypervisor for inc. backups	yes	yes

	Export storage repository	SSH Transfer
Hypervisor OS access needed	yes	yes
Proxy VM needed	no	no
Key Caveats	using single image export file-level restore requires additional image extraction	only QCOW2 based disks supported

Feature	Export storage repository	SSH Transfer
Incremental backup	❌	✅
File-level restore	✅	✅
VM disk exclusion	✅	✅
Snapshot management	✅	✅
Quiesced snapshot	✅	✅
Pre/post snapshot command execution	✅	✅
Backup disks sharable over iSCSI	❌	✅
Name-based policy assignment	✅	✅
Tag-based policy assignment	❌	❌
Available space for snapshot check	❌ (hypervisor-dependent)	✅
Power-on VM after restore	✅	✅

KVM/Xen

	SSH Transfer
Minimum version	QEMU 2.1+ (qcow2-based VMs need libvirt with block commit feature), libvirt
Status	In operation (**preferred**)
Last snapshot kept on hypervisor for inc. backups	yes
Hypervisor OS access needed	yes
Proxy VM needed	no
VM storage formats	QCOW2/RAW file, Ceph RBD volume, LVM volume, LVM-thin volume

Feature	SSH Transfer
Incremental backup	✅
File-level restore	✅
VM disk exclusion	✅
Snapshot management	❌
Quiesced snapshot	❌ (hypervisor-dependent)
Pre/post snapshot command execution	✅
Backup disks sharable over iSCSI	✅
Name-based policy assignment	✅
Tag-based policy assignment	❌
Available space for snapshot check	❌ (hypervisor-dependent)
Power-on VM after restore	✅

OpenStack

	Disk-attachment	SSH Transfer
Minimum version	Queens	Queens, QEMU 2.1+ (qcow2-based VMs need libvirt with block commit feature)
Status	In operation (**preferred**)	In operation
Last snapshot kept on hypervisor for inc. backups	yes	yes
Hypervisor OS access needed	no	yes
Proxy VM needed	yes	no
Key Caveats	incremental backups only for Ceph RBD-based VMs, requires access to ceph monitors for incremental backup only	only QCOW2 based disks supported and Ceph RBD-based VMs, requires access to ceph monitors

Feature	Disk-attachment	SSH Transfer
Incremental backup	✅ (Ceph RBD volumes only)	✅
File-level restore	✅	✅
VM disk exclusion	✅	✅
Snapshot management	❌	❌

Feature	Disk-attachment	SSH Transfer
Quiesced snapshot	❌ (hypervisor-dependent)	❌ (hypervisor-dependent)
Pre/post snapshot command execution	✅	✅
Backup disks sharable over iSCSI	✅	✅ (RAW file/LVM only)
Name-based policy assignment	✅	✅
Tag-based policy assignment	✅	✅
Available space for snapshot check	❌ (hypervisor-dependent)	❌ (hypervisor-dependent)
Power-on VM after restore	❌ (always on)	❌ (always on)

Oracle VM

	Export storage repository
Minimum version	3.4+
Status	In operation (**preferred**)
Last snapshot kept on hypervisor for inc. backups	N/A
Hypervisor OS access needed	no
Proxy VM needed	no

Feature	Export storage repository
Incremental backup	❌
File-level restore	✅
VM disk exclusion	✅
Snapshot management	❌
Quiesced snapshot	❌
Pre/post snapshot command execution	❌
Backup disks sharable over iSCSI	✅
Name-based policy assignment	✅
Tag-based policy assignment	❌
Available space for snapshot check	❌ (hypervisor-dependent)
Power-on VM after restore	❌

Citrix Hypervisor (XenServer)

	Single image (XVA)	Changed-block Tracking
Minimum version	6.5+	6.5+ (incremental backup: 7.3+)
Status	In operation	In operation (**preferred**)
Last snapshot kept on hypervisor for inc. backups	yes	yes
Hypervisor OS access needed	no	no
Proxy VM needed	no	no
Key Caveats	file-level restore not supported	incremental backups may require Citrix XenServer license

Feature	Single image (XVA)	Changed-block Tracking
Incremental backup	✅	✅
File-level restore	❌	✅
VM disk exclusion	❌	✅
Snapshot management	✅	✅
Quiesced snapshot	✅	✅
Pre/post snapshot command execution	✅	✅
Backup disks sharable over iSCSI	❌	✅
Name-based policy assignment	✅	✅
Tag-based policy assignment	✅	✅
Available space for snapshot check	✅	✅
Power-on VM after restore	✅	✅

XCP-ng

	Single image (XVA)	Changed-block Tracking
Minimum version	7.4+	7.4+
Status	In operation	In operation (**preferred**)
Last snapshot kept on hypervisor for inc. backups	yes	yes
Hypervisor OS access needed	no	no
Proxy VM needed	no	no
Key Caveats	file-level restore not supported	

Feature	Single image (XVA)	Changed-block Tracking
Incremental backup	✅	✅
File-level restore	❌	✅
VM disk exclusion	❌	✅
Snapshot management	✅	✅
Quiesced snapshot	✅	✅
Pre/post snapshot command execution	✅	✅
Backup disks sharable over iSCSI	❌	✅
Name-based policy assignment	✅	✅
Tag-based policy assignment	✅	✅
Available space for snapshot check	✅	✅
Power-on VM after restore	✅	✅

Huawei FusionCompute

	Changed Block Tracking
Minimum version	8.0
Status	In operation
Last snapshot kept on hypervisor for inc. backups	yes
Hypervisor OS access needed	no
Proxy VM needed	no

Feature	Changed Block Tracking
Incremental backup	✅
File-level restore	✅
VM disk exclusion	✅
Snapshot management	✅
Quiesced snapshot	❌
Pre/post snapshot command execution	✅
Backup disks sharable over iSCSI	✅

Feature	Changed Block Tracking
Name-based policy assignment	✅
Tag-based policy assignment	❌
Available space for snapshot check	❌
Power-on VM after restore	❌

Scale Computing HC3

	Export Storage Domain	Disk-attachment
Minimum version	8.9.x	8.9.x
Status	In operation	In operation (**preferred**)
Last snapshot kept on hypervisor for inc. backups	no	yes
Hypervisor OS access needed	no	no
Proxy VM needed	no	yes

Feature	Export Storage Domain	Disk-attachment
Incremental backup	❌	✅
File-level restore	❌	✅
VM disk exclusion	✅	✅
Snapshot management	✅	✅
Quiesced snapshot	❌	❌
Pre/post snapshot command execution	✅	✅
Backup disks sharable over iSCSI	✅	✅
Name-based policy assignment	✅	✅
Tag-based policy assignment	✅	✅
Available space for snapshot check	❌	❌
Power-on VM after restore	✅	✅

Containers - features and requirements

Kubernetes

	Helper pod/Ceph RBD

	Helper pod/Ceph RBD
Minimum version	1.10+
Status	In operation (**preferred**)
Last snapshot kept on hypervisor for inc. backups	Yes
Hypervisor OS access needed	no
Proxy VM needed	no

Feature	Helper pod/Ceph RBD
Incremental backup	✅ (when using Ceph RBD as PV)
File-level restore	✅ (when using Ceph RBD as PV)
VM disk exclusion	✅
Snapshot management	❌
Quiesced snapshot	✅ (optional deployment pause)
Pre/post snapshot command execution	✅ (post export)
Backup disks sharable over iSCSI	✅ (when using Ceph RBD as PV)
Name-based policy assignment	✅
Tag-based policy assignment	✅
Available space for snapshot check	N/A
Power-on VM after restore	✅

Red Hat OpenShift

	Helper pod/Ceph RBD
Minimum version	4+
Status	In operation (**preferred**)
Last snapshot kept on hypervisor for inc. backups	Yes
Hypervisor OS access needed	no
Proxy VM needed	no

Feature	Helper pod/Ceph RBD
Incremental backup	✅ (when using Ceph RBD as PV)

Feature	Helper pod/Ceph RBD
File-level restore	✅ (when using Ceph RBD as PV)
VM disk exclusion	✅
Snapshot management	❌
Quiesced snapshot	✅ (optional deployment pause)
Pre/post snapshot command execution	✅ (post export)
Backup disks sharable over iSCSI	✅ (when using Ceph RBD as PV)
Name-based policy assignment	✅
Tag-based policy assignment	✅
Available space for snapshot check	N/A
Power-on VM after restore	✅

Proxmox VE

	Export storage repository
Minimum version	5+
Status	In operation (**preferred**)
Last snapshot kept on hypervisor for inc. backups	No
Hypervisor OS access needed	yes
Proxy VM needed	no

Feature	Export storage repository
Incremental backup	❌
File-level restore	❌
VM disk exclusion	✅
Snapshot management	✅
Quiesced snapshot	❌
Pre/post snapshot command execution	✅
Backup disks sharable over iSCSI	❌
Name-based policy assignment	✅
Tag-based policy assignment	❌
Available space for snapshot check	❌ (hypervisor-dependent)

Feature	Export storage repository
Power-on VM after restore	✅

Cloud - features and requirements

Microsoft 365

Data Protector for Cloud Workloads Server supports backups and restores of Microsoft 365 services.

Below you will find detailed information about what Microsoft 365 services can be protected by Data Protector for Cloud Workloads Server and what restore capabilities it holds:

	Backup	Item level restore	M365 restore	Restore to another account	Restore to a different path	Restore deleted elements	Restore with overwriting	Download
Mailbox	✅	✅	✅	✅	✅	✅	✅	✅
Calendar	✅	✅	✅	✅	✅	✅	✅	✅
Contact	✅	✅	✅	✅	✅	✅	✅	✅
Archive	✅	✅	✅	✅	✅	✅	✅	✅
OneDrive for Business	✅	✅	✅	✅	✅	✅	✅	✅
Sites	✅	✅	✅	❌	✅	✅	✅	✅
Pages	✅	✅	✅	❌	✅	✅	✅	✅
List items	✅	✅	✅	❌	✅	✅	✅	✅
Document Libraries	✅	✅	✅	❌	✅	✅	✅	✅
Teams Channel	✅	❌	✅	❌	❌	✅	❌	✅
Teams 1on1	✅	❌	✅	❌	❌	✅	❌	✅
Teams Files	✅	✅	✅	❌	✅	✅	✅	✅

Please also check supported Sharepoint templates and limitations.

> **Note:** Go to the Platform Requirements section to learn about platform requirements for Data Protector for Cloud Workloads Server.

AWS EC2

	Disk attachment
Minimum version	N/A
Status	In operation (**preferred**)
Last snapshot kept on hypervisor for inc. backups	yes
Hypervisor OS access needed	no
Proxy VM needed	yes

Feature	Disk attachment
Incremental backup	❌
File-level restore	✅
VM disk exclusion	✅
Snapshot management	✅
Quiesced snapshot	❌
Pre/post snapshot command execution	✅
Backup disks sharable over iSCSI	✅
Name-based policy assignment	✅
Tag-based policy assignment	✅
Available space for snapshot check	❌
Power-on VM after restore	✅

Storage Providers - features and requirements

Nutanix Files (AFS)

	File shares with CFT
Minimum version	N/A
Status	In operation (**preferred**)
Last snapshot kept in provider for inc. backups	N/A
Source type	NFS and SMB shares

Feature	File shares with CFT
Incremental backup	✅

Feature	File shares with CFT
Incremental backup change source	CFT API
File-level restore	✅
Snapshot management	❌
Pre/post snapshot command execution	✅
Backups sharable over iSCSI	✅
Name-based policy assignment	✅

Ceph RBD

	RBD export/RBD-NBD
Minimum version	Red Hat Ceph Storage 4.0+, Ceph nautilus+
Status	In operation (**preferred**)
Last snapshot kept in provider for inc. backups	Yes
Source type	RBD volume

Feature	Base
Incremental backup	✅
Incremental backup change source	RBD snap-diff
File-level restore	✅
Snapshot management	✅
Pre/post snapshot command execution	✅
Backups sharable over iSCSI	✅
Name-based policy assignment	✅

Nutanix Volume Groups

	Disk-attachment
Minimum version	N/A
Status	In operation (**preferred**)
Last snapshot kept in provider for inc. backups	Yes
Source type	Volume group

Feature	Disk-attachment
Incremental backup	✅
Incremental backup change source	CBT API
File-level restore	✅
Snapshot management	✅
Pre/post snapshot command execution	✅
Backups sharable over iSCSI	✅
Name-based policy assignment	✅

Conditions / Exclusion

File-level-restore:
When backing up CentOS 8 with a disk with the GPT partition scheme, you can use file-level restore only on the Data Protector for Cloud Workloads *node, which also runs on CentOS 8 operating system.*

Platform Requirements

Software Requirements

Operating Systems

RedHat Enterprise Linux

Versions: 8.x

Minimal install (Basic functionality)

CentOS

Versions: 8.x and Stream

Minimal install (Basic functionality)

Oracle Linux

Versions: 8.x

Minimal install (Basic functionality)

External packages

Data Protector for Cloud Workloads Server:

MariaDB 10.4 (installed from the official MariaDB repository)

> **Note:** MariaDB 10.6 is the latest version supported.

If you need to install MariaDB packages without accessing an external repository during Data Protector for Cloud Workloads installation you also can download RPMs and install them manually as described here

Hardware Requirements

Minimum requirements for all-in-one installation (Data Protector for Cloud Workloads Server and Node on the same machine):

CPU: 4 cores

RAM: 8 GB

HDD1: 20 GB for OS, and Data Protector for Cloud Workloads installation

HDD2: `X` GB for staging, where **`X`** = `size_of_biggest_VM` * `number_of_parallel_backups` - optionally can be skipped, when staging space is configured to be directly on external backup destination (eg. NFS-shared file system)

Minimum requirements for installation in the separated model - Data Protector for Cloud Workloads Server:

CPU: 2 cores

RAM: 6 GB

HDD1: 20 GB for OS, and Data Protector for Cloud Workloads installation

Minimum requirements for installation in the separated model - Data Protector for Cloud Workloads Node:

CPU: 2 cores

RAM: 4 GB

HDD1: 20 GB for OS, and Data Protector for Cloud Workloads installation

HDD2: `X` GB for staging, where **`X`** = `size_of_biggest_VM` * `number_of_parallel_backups` - optionally can be skipped, when staging space is configured to be directly on external backup destination (eg. NFS-shared file system)

Network Requirements

- Critical for data transfer, understand which paths are used for backups as in many cases you are going to use LAN. Depending on where the node is located you need to verify if data is not going to pass via low-bandwidth links.
- Internet is generally not required, but during the installation `yum` need to fetch packages from the repositories, so you need at least access to your internal repositories.
- Data Protector for Cloud Workloads Node needs access to the Server (ports **443** and/or **8181** depending on the setup).
- Data Protector for Cloud Workloads Node needs connectivity with backup providers (if they are external, such as Power Protect DD).
- Data Protector for Cloud Workloads Node needs connectivity with the Hypervisor or Hypervisor Manager.
- If netcat transfer is used for Red Hat Virtualization/oVirt/Oracle Linux VM/Proxmox VE/KVM stand-alone environments - **16000-16999** ports must be reachable from the hypervisors to the node which is responsible for those hypervisors.

General

Source	Destination	Ports	Description
Node	Server	443/tcp (or 8181/tcp)	Main Node-Server communication over HTTPS (443, 8181)
Server	Node	111/tcp, 111/UDP, 2049/tcp, 2049/UDP, ports specified in `/etc/sysconfig/nfs` - variables `MOUNTD_PORT` (TCP and UDP), `STATD_PORT` (TCP and UDP), `LOCKD_TCPPORT` (TCP), `LOCKD_UDPPORT` (UDP)	NFS access to browse mountable backups and logs from UI (using IP that is detected as the source IP - shown in the Node list in UI)

Nutanix AHV

Disk attachment

Connection URL: `https://PRISM_HOST:9440/api/nutanix/v3` (Prism Central or Prism Elements)

> **Note:** when connecting via Prism Central, the same credentials will be used to access all Prism Elements

Source	Destination	Ports	Description
Node	Prism Elements (and optionally Prism Central if used)	9440/tcp	API access to the Nutanix manager

OpenStack

Disk attachment

Connection URL: `https://KEYSTONE_HOST:5000/v3`

Source	Destination	Ports	Description
Node	Keystone, Nova, Glance, Cinder	ports that were defined in endpoints for OpenStack services	API access to the OpenStack management services - using endpoint type that has been specified in hypervisor manager details
Node	Ceph monitors	3300/tcp, 6789/tcp	if Ceph RBD is used as the backend storage - used to collect changed-blocks lists from Ceph

SSH transfer

Connection URL: `https://KEYSTONE_HOST:5000/v3`

> **Note:** You also must provide SSH credentials to all hypervisors that have been detected during inventory sync

Source	Destination	Ports	Description
Node	Hypervisor	22/tcp	SSH access
Hypervisor	Node	netcat port range defined in node configuration - by default 16000-16999/tcp	optional netcat access for data transfer
Node	Ceph monitors	3300/tcp, 6789/tcp, 10809/tcp	if Ceph RBD is used as the backend storage - used for data transfer over NBD

oVirt/RHV/OLVM

Export storage domain

Connection URL: `https://RHV_MGR_HOST/ovirt-engine/api`

Source	Destination	Ports	Description
Node	oVirt/RHV/OLVM manager	443/tcp	oVirt/RHV/OLVM API access
oVirt/RHV/OLVM host selected in export storage domain configuration	Node	If Node is hosting staging space: 111/tcp, 111/UDP, 2049/tcp, 2049/UDP, ports specified in `/etc/sysconfig/nfs` - variables `MOUNTD_PORT` (TCP and UDP), `STATD_PORT` (TCP and UDP), `LOCKD_TCPPORT` (TCP), `LOCKD_UDPPORT` (UDP), otherwise please check the documentation of your NFS storage provider	if staging space (export storage domain) is hosted on the Node - NFS access
Node and oVirt/RHV/OLVM host selected in export storage domain configuration	shared NFS storage	please check the documentation of your NFS storage provider	if staging space (export storage domain) is hosted on the shared storage - NFS access

Disk attachment

Connection URL: `https://MANAGER_HOST/ovirt-engine/api`

Source	Destination	Ports	Description
Node	oVirt/RHV/OLVM manager	443/tcp	oVirt/RHV/OLVM API access

Disk Image Transfer

Connection URL: `https://MANAGER_HOST/ovirt-engine/api`

Source	Destination	Ports	Description
Node	oVirt/RHV/OLVM manager	443/tcp	oVirt/RHV/OLVM API access
Node	oVirt/RHV/OLVM hypervisor	54322/tcp, 54323/tcp	oVirt/RHV/OLVM ImageIO services - for data transfer (primary source)
Node	oVirt/RHV/OLVM manager	54322/tcp, 54323/tcp	oVirt/RHV/OLVM ImageIO services - for data transfer (fallback to ImageIO Proxy)

SSH Transfer

Connection URL: `https://MANAGER_HOST/ovirt-engine/api`

> **Note:** You also must provide SSH credentials to all hypervisors that have been detected during inventory sync

Source	Destination	Ports	Description
Node	oVirt/RHV/OLVM manager	443/tcp	oVirt/RHV/OLVM API access
Node	oVirt/RHV/OLVM hypervisor	22/tcp	SSH access for data transfer
oVirt/RHV/OLVM hypervisor	Node	netcat port range defined in node configuration - by default 16000-16999/tcp	optional netcat access for data transfer

Change-Block Tracking

Connection URL: `https://MANAGER_HOST/ovirt-engine/api`

Source	Destination	Ports	Description
Node	oVirt/RHV/OLVM manager	443/tcp	oVirt/RHV/OLVM API access
Node	oVirt/RHV/OLVM hypervisor	54322/tcp, 54323/tcp	oVirt/RHV/OLVM ImageIO services - for data transfer
Node	oVirt/RHV/OLVM manager	54322/tcp, 54323/tcp	oVirt/RHV/OLVM ImageIO services - for data transfer

Oracle VM

Export storage domain

Connection URL: `https://MANAGER_HOST:7002`

Source	Destination	Ports	Description

Source	Destination	Ports	Description
Node	OVM manager	7002/tcp	OVM API access
Hypervisor	Node	If Node is hosting staging space: 111/tcp, 111/UDP, 2049/tcp, 2049/UDP, ports specified in `/etc/sysconfig/nfs` - variables `MOUNTD_PORT` (TCP and UDP), `STATD_PORT` (TCP and UDP), `LOCKD_TCPPORT` (TCP), `LOCKD_UDPPORT` (UDP), otherwise please check the documentation of your NFS storage provider	if staging space (export storage repository) is hosted on the Node - NFS access
Node and hypervisor	shared NFS storage	please check the documentation of your NFS storage provider	if staging space (export storage repository) is hosted on the shared storage - NFS access

Citrix XenServer/xcp-ng

> **Note:** all hosts in the pool must be defined

Single image (XVA-based)

Source	Destination	Ports	Description
Node	Hypervisor	443/tcp	API access (for data transfer management IP is used, unless `transfer NIC` parameter is configured in hypervisor details)

Changed-Block Tracking

Source	Destination	Ports	Description
Node	Hypervisor	443/tcp	API access (for data transfer management IP is used, unless `transfer NIC` parameter is configured in hypervisor details)
Node	Hypervisor	10809/tcp	NBD access (data transfer IP is returned by hypervisor)

KVM/Xen stand-alone

SSH transfer

Source	Destination	Ports	Description
Node	Hypervisor	22/tcp	SSH access
Hypervisor	Node	netcat port range defined in node configuration - by default 16000-16999/tcp	optional netcat access for data transfer
Node	Ceph monitors	3300/tcp, 6789/tcp, 10809/tcp	if Ceph RBD is used as the backend storage - used for data transfer over NBD

Proxmox VE

Export storage repository

Source	Destination	Ports	Description
Node	Hypervisor	22/tcp	SSH access
Hypervisor	Node	If Node is hosting staging space: 111/tcp, 111/UDP, 2049/tcp, 2049/UDP, ports specified in `/etc/sysconfig/nfs` - variables `MOUNTD_PORT` (TCP and UDP), `STATD_PORT` (TCP and UDP), `LOCKD_TCPPORT` (TCP), `LOCKD_UDPPORT` (UDP), otherwise please check the documentation of your NFS storage provider	if staging space (export storage domain) is hosted on the Node - NFS access
Node and hypervisor	shared NFS storage	please check the documentation of your NFS storage provider	if staging space (export storage domain) is hosted on the shared storage - NFS access

SSH transfer

Source	Destination	Ports	Description
Node	Hypervisor	22/tcp	SSH access
Hypervisor	Node	netcat port range defined in node configuration - by default 16000-16999/tcp	optional netcat access for data transfer

Security Requirements

User Permissions

User `vprotect` must be a member of group "disk".

Sudo privileges are required for the following commands:

Data Protector for Cloud Workloads Node:

- `/usr/bin/targetcli`
- `/usr/sbin/exportfs`
- `/usr/sbin/kpartx`
- `/usr/sbin/dmsetup`
- `/usr/bin/qemu-nbd`
- `/usr/bin/guestmount`
- `/usr/bin/fusermount`
- `/bin/mount`
- `/bin/umount`
- `/usr/sbin/parted`
- `/usr/sbin/nbd-client`
- `/usr/bin/tee`
- `/opt/vprotect/scripts/vs/privileged.sh`
- `/usr/bin/yum`
- `/usr/sbin/mkfs.xfs`
- `/usr/sbin/fstrim`

- `/usr/sbin/xfs_growfs`
- `/usr/bin/docker`
- `/usr/bin/rbd`
- `/usr/bin/chown`
- `/usr/sbin/nvme`
- `/bin/cp`
- `/sbin/depmod`
- `/usr/sbin/modprobe`
- `/bin/bash`
- `/usr/local/sbin/nbd-client`
- `/bin/make`

Data Protector for Cloud Workloads Server:

- `/opt/vprotect/scripts/application/vp_license.sh`
- `/bin/umount`
- `/bin/mount`

SELinux

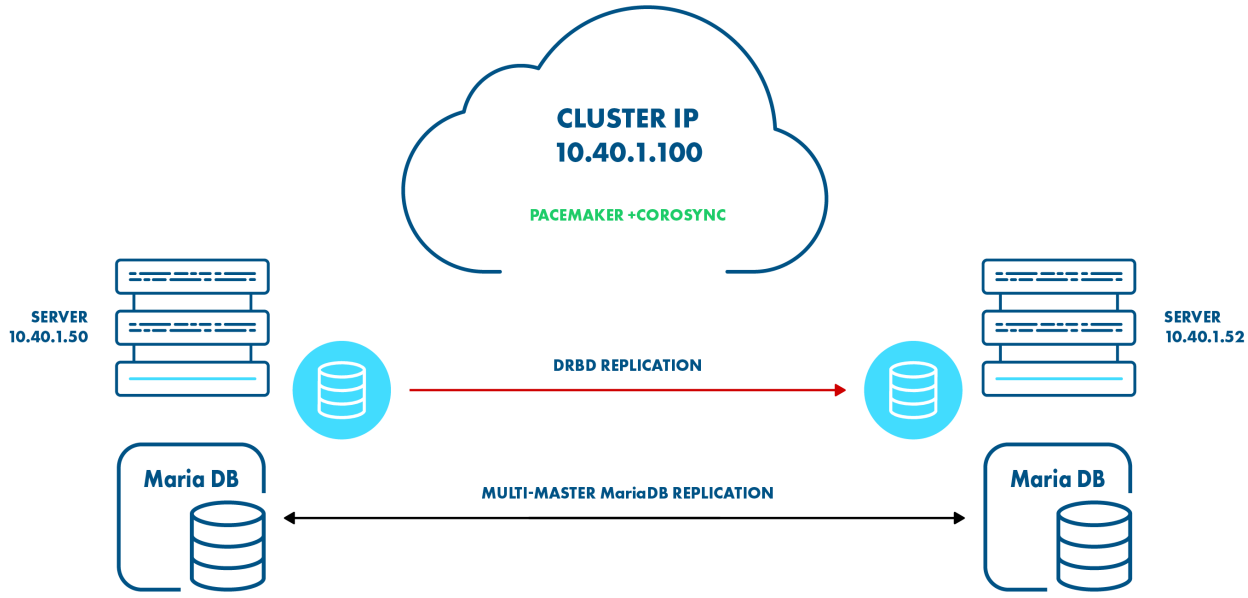
PERMISSIVE - currently it interferes with the mountable backups (file-level restore) mechanism. Optionally can be changed to ENFORCING if the file-level restore is not required.

High Availability

In this scenario, we are going to set up two Data Protector for Cloud Workloads Servers in High Availability, Active/Passive mode. This is possible by using techniques such as a pacemaker, corosync, and DRBD. At least a basic understanding of these is highly desirable. This how-to is intended for RPM-based systems such as Red Hat / CentOS. If you run Data Protector for Cloud Workloads on a different OS, you may need to refer to your distribution docs.

Our environment is built of the following elements:

1. server1 - first Data Protector for Cloud Workloads Server + Data Protector for Cloud Workloads Node, IP: 10.40.1.50
2. server2 - second Data Protector for Cloud Workloads Server + Data Protector for Cloud Workloads Node, IP: 10.40.1.52
3. Cluster IP: 10.40.1.100 - We will use this IP to connect to our **active** Data Protector for Cloud Workloads service. This IP will float between our servers and will point to an active instance.
4. DRBD (optionally with VDO) for data replication and deduplication between nodes.
5. MariaDB master <-> master replication



HA cluster setup

Preparing the environment

- Stop and disable the Data Protector for Cloud Workloads Server, node and database as the cluster will manage these resources.

```
systemctl disable vprotect-server vprotect-node mariadb
```

- **Use yum to check if you have any updates pending**

```
# yum update
```

- It is a good idea to check ***/etc/hosts,*** especially if you installed Data Protector for Cloud Workloads using the ***All in one quick installation*** method, as you might find an entry such as:

  ```
  127.0.0.1 <your_hostname_here>
  ```

  Delete it as this prevents the cluster from functioning properly (your nodes will not "see" each other).

Now we can proceed with installation of the required packages.

- **On both servers run**

```
# yum install -y pacemaker pcs psmisc policycoreutils-python
```

- **Add a firewall rule to allow HA traffic** - TCP ports 2224, 3121, and 21064, and UDP port 5405 (both servers)

```
# firewall-cmd --permanent --add-service=high-availability
success
# firewall-cmd --reload
success
```

While testing, depending on your environment, you may encounter problems related to network traffic, permissions, etc. While it might be a good idea to temporarily disable the firewall and SELinux, we do not recommend disabling that mechanism in the production environment as it creates significant security issues.
If you choose to disable the firewall, bear in mind that Data Protector for Cloud Workloads will no longer be available on ports 80/443. Instead, connect to ports 8080/8181 respectively.

```
# setenforce 0
# sed -i.bak "s/SELINUX=enforcing/SELINUX=permissive/g" /etc/selinux/config
# systemctl mask firewalld.service
# systemctl stop firewalld.service
# iptables --flush
```

- **Enable and start PCS daemon**

```
# systemctl enable pcsd.service
# systemctl start pcsd.service
```

Cluster configuration

Earlier installation of a pcs package automatically creates a user ***hacluster*** with no password authentication. While this may be good for running locally, we will require a password for this account to perform the rest of the configuration, so let's

- **configure the same password on both nodes**

```
# passwd hacluster
Changing password for user hacluster.
```

```
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

Corosync configuration

- On node 1, issue a command to authenticate as a **hacluster** user:

```
[root@vprotect1 ~]# pcs cluster auth vprotect1 vprotect2
Username: hacluster
Password:
vprotect1: Authorized
vprotect2: Authorized
```

- **Generate and synchronize the corosync configuration**

```
[root@vprotect1 ~]# pcs cluster setup --name mycluster vprotect1 vprotect2
```

Take a look at your output, which should look similar to below:

```
Destroying cluster on nodes: vprotect1, vprotect2...
vprotect1: Stopping Cluster (pacemaker)...
vprotect2: Stopping Cluster (pacemaker)...
vprotect1: Successfully destroyed cluster
vprotect2: Successfully destroyed cluster

Sending 'pacemaker_remote authkey' to 'vprotect1', 'vprotect2'
vprotect1: successful distribution of the file 'pacemaker_remote authkey'
vprotect2: successful distribution of the file 'pacemaker_remote authkey'
Sending cluster config files to the nodes...
vprotect1: Succeeded
vprotect2: Succeeded

Synchronizing pcsd certificates on nodes vprotect1, vprotect2...
vprotect1: Success
vprotect2: Success
Restarting pcsd on the nodes in order to reload the certificates...
vprotect1: Success
vprotect2: Success
```

- **Enable and start your new cluster**

```
[root@vprotect1 ~]# pcs cluster start --all && pcs cluster enable --all
vprotect1: Starting Cluster (corosync)...
vprotect2: Starting Cluster (corosync)...
vprotect1: Starting Cluster (pacemaker)...
vprotect2: Starting Cluster (pacemaker)...
vprotect1: Cluster Enabled
vprotect2: Cluster Enabled
```

OK! We have our cluster enabled. We have not created any resources (such as a floating IP) yet, but before we proceed we still have a few settings to modify.

Because we are using only two nodes, we need to

- **disable default quorum policy**

(this command should not return any output)

```
[root@vprotect1 ~]# pcs property set no-quorum-policy=ignore
```

We should also

- **define default failure settings**

```
[root@vprotect1 ~]# pcs resource defaults failure-timeout=30s
[root@vprotect1 ~]# pcs resource defaults migration-threshold=3
```

These two settings combined will define how many failures can occur for a node to be marked as ineligible for hosting a resource and after what time this restriction will be lifted. We define the defaults here, but it may be a good idea to also set these values at the resource level, depending on your experience.

As long we are not using any fencing device in our environment (and here we are not) we need to:

- **disable stonith**

```
[root@vprotect1 ~]# pcs property set stonith-enabled=false && crm_verify -L
```

The second part of this command verifies running-config. These commands normally do not return any output.

Resource creation

Finally, we have our cluster configured, so it's time to proceed to

- **resource creation**

First, we will create a resource that represents our ***floating IP*** 10.40.1.100. Adjust your IP and cidr_netmask, and you're good to go.

IMPORTANT: From this moment on we need to use this IP when connecting to our Data Protector for Cloud Workloads Server.

```
[root@vprotect1 ~]# pcs resource create "Failover_IP" ocf:heartbeat:IPaddr2
ip=10.40.1.100 cidr_netmask=22 op monitor interval=30s
```

Immediately, we should see our IP is up and running on one of the nodes (most likely on the one we issued this command for).

```
[root@vprotect1 ~]# ip a
[..]
```

```
2: ens160:  mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:a6:9f:c6 brd ff:ff:ff:ff:ff:ff
    inet 10.40.1.50/22 brd 10.40.3.255 scope global ens160
       valid_lft forever preferred_lft forever
    inet 10.40.1.100/22 brd 10.40.3.255 scope global secondary ens160
       valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:fea6:9fc6/64 scope link
       valid_lft forever preferred_lft forever
```

As you can see, our floating IP 10.40.1.100 has been successfully assigned as the second IP of interface ens160. This is what we wanted!

We should also check if the Data Protector for Cloud Workloads web interface is up and running. We can do this by opening the web browser and typing in https://<DP4CW_server_IP>. At this point we should see:

The next step is to

- **define a resource responsible for monitoring network connectivity**

```
[root@vprotect1 ~]# pcs resource create ping ocf:pacemaker:ping dampen=5s
multiplier=1000 host_list=10.40.0.1 clone
[root@vprotect1 ~]# pcs constraint location Failover_IP rule score=-INFINITY pingd lt
1 or not_defined pingd
```

Note that you need to use **your gateway IP** in the ***host_list*** parameter

Finally, we have to define a set of cluster resources responsible for other services crucial for Data Protector for Cloud Workloads as Data Protector for Cloud Workloads Node and the Data Protector for Cloud Workloads Server itself. We will logically link these services with our floating IP. Whenever the floating IP disappears from our server, these services will be stopped. We also have to define the proper order for services to start and stop, as for example starting the Data Protector for Cloud Workloads-server without a running database makes little sense.

- **Resource creation**

```
[root@vprotect1 ~]#  pcs resource create "vProtect-node" systemd:vprotect-node op
monitor timeout=300s on-fail="stop" --group vProtect-group
[root@vprotect1 ~]# pcs resource create "vProtect-server" service:vprotect-server op
start on-fail="stop" timeout="300s" op stop timeout="300s" on-fail="stop" op monitor
timeout="300s" on-fail="stop" --group vProtect-group
```

It is OK for these commands not to return any output.

- **Resource colocation**

```
[root@vprotect1 ~]# pcs constraint colocation add Failover_IP with vProtect-group
```

To finish with, we can set which server is more preferred for running our services

- **Set node preference**

```
[root@vprotect1 ~]# pcs constraint location Failover_IP prefers vprotect1=INFINITY
[root@vprotect1 ~]# pcs constraint location vProtect-group prefers vprotect1=INFINITY
```

We have made it to the end. At this point, our pacemaker HA cluster is functional.

However, there are still two things we need to consider, that is:

1. Creating DB replication
2. Setting up DRBD for /vprotect_data (optionally with VDO)

Setting up VDO+DRBD

In this section, we will prepare our deduplicated and replicated filesystem mounted in /vprotect_data.

Using a deduplicated FS is optional but highly recommended. If you don't intend to use it, skip the part regarding VDO configuration.

Note: If you are altering existing Data Protector for Cloud Workloads configuration it is very important to preserve the /vprotect_data contents and transfer them to the new filesystem. You may also need to re-create your backup_destination if you previously had one in this directory. Setting up VDO and DRBD will cause all data to be wiped from the configured volume.

Installation is split into the steps below that you need to follow to get the job done.

- **Stop the Data Protector for Cloud Workloads Server and node**

```
# systemctl stop vprotect-server vprotect-node
```

No output means everything went OK.

- **On both nodes install the equired repositories and packages**

```
# rpm --import https://www.elrepo.org/RPM-GPG-KEY-elrepo.org
# rpm -Uvh https://www.elrepo.org/elrepo-release-7.0-4.el7.elrepo.noarch.rpm
Retrieving https://www.elrepo.org/elrepo-release-7.0-4.el7.elrepo.noarch.rpm
Preparing...                          ################################# [100%]
Updating / installing...
   1:elrepo-release-7.0-4.el7.elrepo  ################################# [100%]
```

The next command can produce quite a few lines, so I've truncated the output, however the idea is simple: install drbd packages:

```
[root@vprotect1 ~]# yum install -y kmod-drbd84 drbd84-utils

Installed:
drbd84-utils.x86_64 0:9.6.0-1.el7.elrepo
kmod-drbd84.x86_64 0:8.4.11-1.1.el7_6.elrepo
```

If you have not disabled SELinux and the firewall, remember to

- **configure them on both nodes**

  ```
  # semanage permissive -a drbd_t
  # firewall-cmd --add-port=7788/tcp --permanent
  success
  # firewall-cmd --complete-reload
  success
  ```

  Don't forget to repeat these steps on the second node

Now that we have the necessary software installed, we must prepare an identical size block device on both nodes. A block device can be a hard drive, a hard drive partition, software RAID, LVM Volume, etc. In this scenario, we are going to use a hard drive connected as ***/dev/sdb***.

To add a DRBD resource we create the file ***/etc/drbd.d/vprotect.res*** with the content below. Be sure to change the "address" so that t reflects your network configuration.

Also, the node names (server1 and server2) must match your ***uname -n*** output.

```
resource replicate {
protocol C;
    on vprotect1 {
                device /dev/drbd0;
                disk /dev/sdb;
                address 10.40.1.50:7788;
                meta-disk internal;
        }
    on vprotect2 {
                device /dev/drbd0;
                disk /dev/sdb;
                address 10.40.1.52:7788;
                meta-disk internal;
        }
```

We now have config in place and can create and bring our resource online.

- **On both nodes, run**

```
# drbdadm create-md replicate
initializing activity log
initializing bitmap (4800 KB) to all zero
Writing meta data...
New drbd meta data block successfully created.
```

then bring the volume online

```
# drbdadm up replicate
```

You can verify if the device is up & running by issuing

```
# lsblk
NAME                    MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda                       8:0    0   16G  0 disk
├─sda1                    8:1    0    1G  0 part /boot
└─sda2                    8:2    0   15G  0 part
├─vg_vprotect-lv_root 253:0    0 13.4G  0 lvm  /
└─vg_vprotect-lv_swap 253:1    0  1.6G  0 lvm  [SWAP]
sdb                       8:16   0  150G  0 disk
└─drbd0                 147:0    0  150G  1 disk
```

However, if we check

```
[root@vprotect1 ~]# drbdsetup status replicate
replicate role:Secondary
disk:Inconsistent
peer role:Secondary
replication:Established peer-disk:Inconsistent
```

we will notice we need to start synchronization before we can use our volume.

- **On the first server, run**

```
[root@vprotect1 ~]# drbdadm primary --force replicate
[root@vprotect1 ~]# drbdsetup status replicate
replicate role:Primary
disk:UpToDate
peer role:Secondary
replication:SyncSource peer-disk:Inconsistent done:0.22
```

This way we have successfully started the process of replication between servers with vprotect1 as the ynchronization source.

If you don't want to create a VDO device, then create and mount your filesystem:

```
[root@vprotect1 ~]# mkfs.xfs -K /dev/drbd0
[root@vprotect1 ~]# mount /dev/mapper/drbd0 /vprotect_data/ && chown -R
vprotect:vprotect /vprotect_data
```

- **Create VDO volume** (optional)

  By issuing the command below we will create a VDO volume called ***vdo_data*** and put in at the top our DRBD volume. Afterwards, we format it with XFS and mount it in /vprotect_data.

```
[root@vprotect1 ~]# vdo create --name=vdo_data --device=/dev/drbd0 --
vdoLogicalSize=400G --compression=enabled --deduplication=enabled
Creating VDO vdo_data
Starting VDO vdo_data
Starting compression on VDO vdo_data
VDO instance 0 volume is ready at /dev/mapper/vdo_data

[root@vprotect1 ~]# mkfs.xfs -K /dev/mapper/vdo_data
meta-data=/dev/mapper/vdo_data   isize=512    agcount=4, agsize=26214400 blks
    =                       sectsz=4096  attr=2, projid32bit=1
    =                       crc=1        finobt=0, sparse=0
data     =                       bsize=4096   blocks=104857600, imaxpct=25
    =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0 ftype=1
log      =internal log           bsize=4096   blocks=51200, version=2
    =                       sectsz=4096  sunit=1 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0

[root@vprotect1 ~]# mount /dev/mapper/vdo_data /vprotect_data/ && chown -R
vprotect:vprotect /vprotect_data
```

- **Copy the VDO config to the second node**

```
[root@vprotect1 ~]# scp /etc/vdoconf.yml root@vprotect2:/etc/vdoconf.yml
```

- **Disable VDO automatic startup**

  As this resource will be managed by the cluster, we need to disable auto startup of this service ***on both nodes.***

```
# systemctl disable vdo
```

Final cluster settings

At this point, we have three components set up. To fully utilize our HAcluster and eliminate the need for manual intervention we should add the resources and settings below to our cluster.

Issue these commands on one node only as it will propagate to the cluster settings.

```
[root@vprotect1 ~]#  pcs cluster cib drbd_cfg
[root@vprotect1 ~]#  pcs -f drbd_cfg resource create replicate ocf:linbit:drbd \
        drbd_resource=replicate op monitor interval=10s --group fs_group
```

```
[root@vprotect1 ~]#  pcs -f drbd_cfg resource master replicateClone replicate \
         master-max=1 master-node-max=1 clone-max=2 clone-node-max=1 \
         notify=true --group fs_group

[root@vprotect1 ~]#  pcs -f drbd_cfg resource create vdo_resource ocf:heartbeat:vdo-
vol volume=vdo_data --group fs_group
[root@vprotect1 ~]#  pcs -f drbd_cfg resource create fs_resource
ocf:heartbeat:Filesystem device=/dev/mapper/vdo_data directory=/vprotect_data
fstype=xfs  --group fs_group
[root@vprotect1 ~]#  pcs cluster cib-push drbd_cfg --config

[root@vprotect1 ~]#  pcs constraint colocation add vdo_resource with replicateClone
[root@vprotect1 ~]#  pcs constraint order start vdo_resource then fs_resource
[root@vprotect1 ~]#  pcs constraint order start replicateClone then vdo_resource
[root@vprotect1 ~]#  pcs constraint colocation add vProtect-group with fs_group
[root@vprotect1 ~]#  pcs constraint colocation add vdo_resource with replicateClone
INFINITY with-rsc-role=Master
[root@vprotect1 ~]#  pcs constraint order promote replicateClone then start fs_group
```

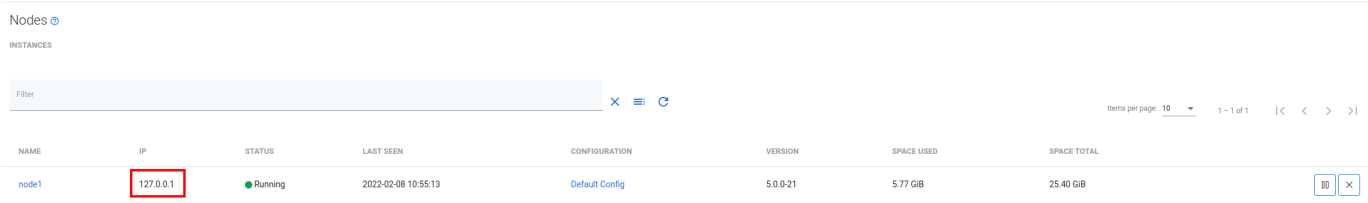
Here we have created a temporary file ***drbd_cfg*** and inside this file we have added our drbd_resource called ***replicate***, plus a Master/Slave set for this resource.

Afterwards, we have the definition of the vdo_resource and fs_resource in one fs_group followed by an update of the cluster configuration.

As a second step, we have put in place several resource colocations and constraints which allow us to control the order and existence of newly created resources.

We need still to

- Make sure that our node is pointed to a localhost address. Check the ***Nodes*** UI section.



If the node's IP is different than 127.0.0.1, delete the node and re-register it using

```
[root@vprotect1 ~]# vprotect node -e <Node_Name> admin http://127.0.0.1:8080/api
```

- copy our license and node information from the first node to the second node:

```
[root@vprotect1 ~]# scp -pr /opt/vprotect/.session.properties
[root@vprotect1 ~]# scp -pr /opt/vprotect/license.key
```

MariaDB replication

In this section, we will cover how to setup master<->master MariaDB replication.

- On both nodes, if you have the firewall enabled, allow communication via port **3306**

```
# firewall-cmd --add-port=3306/tcp --permanent
# firewall-cmd --complete-reload
```

Steps to run on the first server1 node: 10.40.1.50

This server will be the source of DB replication.

- **Stop the Data Protector for Cloud Workloads Server, node and database**

```
[root@vprotect1 ~]# systemctl stop vprotect-server vprotect-node mariadb
```

- **Edit the config file**, enable binary logging and start MariaDB again. Depending on your distribution, the config file location may vary, most likely it is /etc/my.cnf or /etc/my.cnf.d/server.cnf

  In the ***[mysqld]*** section, add the lines:

```
[root@vprotect1 ~]# vi /etc/my.cnf.d/server.cnf
log-bin
server_id=1
replicate-do-db=vprotect
[root@vprotect1 ~]# systemctl start mariadb
```

- Now **log in into your MariaDB**, create a user used for replication and assign appropriate rights to it.

  For the purpose of this task, we will set the username to 'replicator' and the password to 'R3pLic4ti0N'

```
[root@vprotect1 ~]# mysql -u root -p
Enter password:
[..]
MariaDB [(none)]> create user 'replicator'@'%' identified by 'R3pLic4ti0N';
Query OK, 0 rows affected (0.026 sec)

MariaDB [(none)]> grant replication slave on *.* to 'replicator'@'%';
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.001 sec)
```

Don't log out just yet, we need to check the master status and

- **write down the log file name and position**, as it is required for proper slave configuration.

```
MariaDB [(none)]> show master status;
+----------------------+----------+--------------+------------------+
| File                 | Position | Binlog_Do_DB | Binlog_Ignore_DB |
+----------------------+----------+--------------+------------------+
| vprotect1-bin.000007 |    46109 |              |                  |
+----------------------+----------+--------------+------------------+
```

- Dump the Data Protector for Cloud Workloads database and copy it onto the second server (vprotect2).

```
[root@vprotect1 ~]# mysqldump -u root -p vprotect > /tmp/vprotect.sql
[root@vprotect1 ~]# scp /tmp/vprotect_rep.sql root@vprotect2:/tmp/
```

Steps to run on the 2nd server, server2: 10.40.1.52

For the reader's convenience, I have only highlighted the differences in configuration between server1 and server2, and omitted the output of some commands if they are the same as on the previous node.

- **Stop the Data Protector for Cloud Workloads Server, Node and database**
- Edit the MariaDB config file. **Assign a different server id**, for example: 2. Then start MariaDB.

```
[root@vprotect2 ~]# vi /etc/my.cnf.d/server.cnf
log-bin
server_id=2
replicate-do-db=vprotect
[root@vprotect2 ~]# systemctl start mariadb
```

- **Load the database dump** copied from server1.

```
[root@vprotect2 ~]# mysql -u root -p vprotect < /tmp/vprotect.sql
```

At this point, we have two identical databases on our two servers.

- **Log in to the MariaDB instance, create a replication user with a password**. Use the same user as on server1. Grant the necessary permissions.
- Set the master host. You ***must*** use the user_master_log_file and master_log_pos written down earlier. Change the IP of the master host to match your network configuration.

```
MariaDB [(none)]> STOP SLAVE;
MariaDB [(none)]> CHANGE MASTER TO MASTER_HOST = '10.40.10.50', MASTER_USER =
'replicator',MASTER_PASSWORD='R3pLic4ti0N',MASTER_LOG_FILE = 'vprotect1-
bin.000007',MASTER_LOG_POS=46109;
Query OK, 0 rows affected (0.004 sec)
```

- Start the slave, check the master status and **write down the file name and position.**

```
MariaDB [(none)]> start slave;
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> SHOW MASTER STATUS;
+----------------------+----------+--------------+------------------+
| File                 | Position | Binlog_Do_DB | Binlog_Ignore_DB |
+----------------------+----------+--------------+------------------+
| vprotect2-bin.000002 |   501051 |              |                  |
+----------------------+----------+--------------+------------------+
1 row in set (0.000 sec)
```

Go back to the first server (server1)

- On **storreaw1**, stop the slave then change the master host using the parameters noted down in the previous step. Also, change the master host IP to match your network configuration.

```
MariaDB [(none)]> stop slave;
MariaDB [(none)]> MariaDB [(none)]>  change master to master_host='10.40.1.52',
master_user='replicator', master_password='R3pLic4ti0N',MASTER_LOG_FILE = 'vprotect2-
bin.000002', master_log_pos=501051;
Query OK, 0 rows affected (0.004 sec)
MariaDB [(none)]> start slave;
Query OK, 0 rows affected (0.001 sec)
```

At this point, you have successfully configured MariaDB master<->master replication.

Testing the setup

Automatic

The fastest way to test our setup is to invoke

```
# pcs node standby vprotect1
```

to put server1 into standby mode, which prevents it from hosting any cluster resources.

After a while, you should see your resources up and running on server2.

Note that if you perform normal OS shutdown (not a forced one), the pacemaker will wait for a long time for a node to come back online, which in fact will prevent completion of shutdown. As a result, resources ***will not*** switch correctly to the other node.

Manual

If you want to dive a little bit deeper, we have prepared instructions on how to manually move a filesystem resource from the first node to the second.

1. Stop vprotect services.

   ```
   systemctl stop vprotect-server && systemctl stop vprotect-node
   ```

2. Unmount the FS used by DRBD/VDO on the primary server (here server1).

   ```
   [root@vprotect1 ~]# drbdadm role replicate
   Primary/Secondary
   [root@vprotect1 ~]# umount /vprotect_data/
   ```

3. If you are using a VDO device, stop it.

   ```
   [root@vprotect1 ~]# vdo stop -n vdo_data
   Stopping VDO vdo_data
   ```

4. Demote the primary replication server (still server1) to secondary server.

```
[root@vprotect1 ~]# drbdadm secondary replicate
```

On the second server

1. Promote the second server (here server2) to the primary DRBD role.

```
[root@vprotect2 ~]# drbdadm    primary replicate
```

2. Start the VDO.

```
[root@vprotect2 ~]# vdo start -n vdo_data
Starting VDO vdo_data
Starting compression on VDO vdo_data
VDO instance 2 volume is ready at /dev/mapper/vdo_data
```

3. Mount the filesystem on the second server.

```
[root@vprotect2 ~]# mount /dev/mapper/vdo_data /vprotect_data/
```

Now you have your replicated volume mounted on the second node.

Sizing Guide

The best strategy is to **plan** your backup environment/procedure **before implementing** it. In this chapter, we have collected generic hints and guides which you might find useful while thinking about your Data Protector for Cloud Workloads implementation.

1. Collect information about the `TotalSizeOfData` to be protected in your environment
    - this is the size of your VMs/Storage that will be transferred within the backup window
        - for general sizing, assume all backups to be full
    - if your staging space is separate from the backup destination, please also check what are the biggest VMs/Storage that may end up in your staging area
2. Assume `BackupWindow` length - backups are usually executed overnight, so 10h-12h is common practice
3. Run a **test transfer** on a test file to estimate the maximum achievable bandwidth per thread (`SingleThreadTransfer`) from the hypervisor (or manager) to the node
    - we recommend 10 simultaneous transfers with the result divided by 10 threads to see if other limitations of the environment do not impact the total transfer rate (one such common limitation is disk read performance on the virtualization platform)
    - all the methods usually use snapshots to do backup - please check if snapshot removal in your environment does not take a significant amount of time, as it is a highly resource-intensive operation that impacts overall backup time - especially when running multiple export jobs in parallel
4. Estimate **the number of the nodes**
    - required bandwidth per node:

      ```
      RequiredBandwidth = TotalSizeOfData / BackupWindow
      ```

    - the total number of export tasks (note that other aspects such as snapshot handling, file system scanning during export, and infrastructure bottlenecks when using multiple threads will usually impact the overall speed):

      ```
      TotalNumberOfExportTasks = RequiredBandwidth / (70% * SingleThreadTransferSpeed)
      ```

    - the number of nodes:

      `NumberOfTheNodes = TotalNumberOfExportTasks / 10` **(10 is the recommended maximum number of export tasks per Node)**

    - note that the `TotalSizeOfData` does not mean that it is only a full backup, as you can mix full and incremental backups
    - granularity is a single hypervisor or storage provider, so at the maximum, you cannot have more nodes than hypervisor storage providers in your environment
    - if you have multiple clusters and you want to use the disk-attachment method, this automatically implies a minimum of 1 node per cluster
5. Estimate the total **store rate** in the backup destination
    - if multiple nodes are required, add up the total amount of data from all nodes
    - if your backup destination is accessible over LAN

        - do a test transfer from the node to the backup destination to verify if the performance on the backup destination is able to receive such a load

6. `NumberOfExportTasksPerNode`
    - we recommend using the same node configuration for multiple nodes, so the same limit value will be applied to all nodes sharing the configuration
    - this implies that we recommend assuming this value as follows (rounded down):

      `NumberOfExportTasksPerNode = TotalNumberOfExportTasks / NumberOfTheNodes`

7. `NumberOfStoreTasksPerNode` usually depends on destination backup performance
    - we recommend a value equal to the `NumberOfExportTasksPerNode` or higher
    - reduce this value only if your backup provider starts to have significant I/O latency eventually leading to a slower write rate than with the lower number of threads - this will typically result in higher staging space occupation as backups will be kept for a longer period of time in the temporary space

8. **Node resource requirements:**
    - **CPU**: Assume 0.5 CPU per task, minimum 2 cores - rounded up to get the full core count supported by the hypervisor or physical server (i.e. it may be required to round up 2.5 cores to 4 vCPUs if the hypervisor on which the node is deployed doesn't allow to 3 vCPUs to be assigned)
        - if SSH transfer (without netcat) or client-side deduplication is used (i.e. VDO) assume 1 CPU per task
    - **Memory**: 256 MB RAM per task, with a minimum of 2GB
    - **Staging space:** if not shared with the backup destination - the biggest VM/Storage multiplied by the number of tasks
    - when counting tasks for each node assume: `NumberOfExportTasksPerNode + NumberOfStoreTasksPerNode`

9. **Server resource requirements:**
    - **CPU**: Assume 0.5 CPU per task, minimum 2 cores - rounded up to full core count supported by the hypervisor or physical server (i.e. it may be required to round up 2.5 cores to 4 vCPUs if the hypervisor on which the node is deployed doesn't allow 3 vCPUs to be assigned)
    - **Memory**: 256 MB RAM per task, with a minimum of 6GB
    - when counting tasks assume:

      `TotalNumberOfExportTasks + TotalNumberOfStoreTasks`

10. Finally, if the resulting node count is too big:
    - divide your VMs into multiple backup policies with separate schedules so that some full backups of your VMs will be done on Monday, some on Tuesday, while the rest will run incremental backups at the same time - this will reduce the value of `TotalSizeOfData` in the previous equations
    - check if the backup window cannot be extended
        - exports usually impact infrastructure more, while store tasks can also safely be done during the day
        - Data Protector for Cloud Workloads will start backups only within the backup window, but once the tasks are started, they may continue even after your backup window ends

Notes on sizing using different setups

Disk-attachment methods

- read data from locally attached drives (which may use LAN or SAN behind the scenes depending on your virtualization platform setup) and write it to the staging space (local or remote)
- run a read test from one device to the staging storage to estimate the processing rate
- this method requires usually 1 node per cluster, so treat each cluster separately
- this method also requires time for attachment/detachment of drives

Export storage repository methods

- export data from a specific host to the staging space of Data Protector for Cloud Workloads via NFS
- run a test export on any VM to estimate the export speed in your environment
- export methods also usually have limitations on the hypervisor side, so OVM can process only 1 export job simultaneously using a specific set of storage repositories (on which the VM disks reside, and to which the VM is being exported), which may impact overall performance - please consult your hypervisor documentation to check for export process limitations
- it is common to share a backup destination with staging space from an external backup provider via NFS (not from each node) so that exports are done directly to the backup destination storage

Direct export from hypervisors or underlying storage

- if you can enable the netcat in SSH Transfer methods, it should result in 2-3 times faster transfer rates compared to standard SSH
- export tasks run against stand-alone hypervisors will be automatically balanced, while those managed by hypervisor managers will be subject to global and per source limits
    - this means that if you configure a maximum number of export tasks per source to 5 and the global number to 10, you will have no more than 5 export tasks running against a single manager regardless of the number of hosts
- when using Ceph RBD in KVM stand-alone or the OpenStack SSH Transfer method, the actual transfer is done directly from Ceph monitors, and this is the network path that needs to be checked when estimating bandwidth - use `rbd export` or mount a test volume over RBD-NBD to test it

Backup destination

- if you plan to use common storage for the staging space and backup destination, your reads from the source will be limited by the write speed of your backup destination
- make sure you have the appropriate bandwidth between the nodes and the backup destination
- verify if the backup destination is able to process IOPS coming from multiple sources - it is common to assume the export rate as the minimum required store rate

Deployment

In this section, you will find information about installing and configuring Data Protector for Cloud Workloads.

We recommend starting with the Installation Overview to see various options to install Data Protector for Cloud Workloads.

There are various options to install Data Protector for Cloud Workloads available, including Quick Install or Ansible.

Take a look and choose the method that best suits your needs and experiences.

Installation Overview

Quick Install

Installation using Ansible playbook

Installation with RPMs

> **Note:** We recommend doing an Initial Configuration after an installation.

Installation Overview

1. Choose your installation option. There are the following options:
    - All-in-one quick installation
    - Installation using Ansible playbook
    - Installation with RPMs
2. Regardless of the installation option you choose:
    - The node requires **staging space** - assume a number of concurrent export and store tasks and multiply it by the biggest VM size (**for example:** 6 export tasks + 4 store tasks * 100 GB should require around 1 TB)
    - The Staging space configuration will guide you to prepare storage on the spare drive
    - Data Protector for Cloud Workloads is installed in the `/opt/vprotect` folder and staging space is assumed to be in `/vprotect_data` - these are the defaults and should not be changed.
3. Now it is time for the Initial configuration
4. Add your Hypervisor(s) or Hypervisor Manager(s) and initiate the index to retrieve a list of VMs, storage, etc.:
    - by indexing Hypervisor Manager (RHV/oVirt/OLVM/Oracle VM/Nutanix Prism) you'll have hypervisors added automatically. Other hypervisors need to be entered one by one (KVM/Xen/Citrix Hypervisor/XCP-ng/Proxmox VE)
    - you can choose what platform you want to protect:
        - Virtual Environments
        - Microsoft 365
        - Applications
        - Storage Providers
5. Set up the backup provider:
    - you should check the backup destinations section for a detailed description of properties: Backup Destinations
6. Test basic operations to verify that integration is completed:
    - Backup
    - Restore
    - Mount

> **Note:** More information about how to do backup, restore or mount you will find in protected platforms chapters:
>
> - Virtual Environments
> - Applications
> - Microsoft 365
> - Storage Providers

“All-in-One" Installation

Data Protector for Cloud Workloads can be easily installed on a single box quickly. This approach installs a server and node on the same box and generates an SSL certificate based on the hostname where it is installed. This corresponds to Ansible deployment, with the node and server roles installed on the same host. The end result should be the same as an RPM-based installation without a staging setup. Configuration (such as backup destination definition or hypervisor connectivity) still needs to be done after installation. You can also add more nodes in the future if necessary.

Installation

> Before installing Data Protector for Cloud Workloads we highly recommend doing a system update and reboot.

1. Install CentOS 8 Stream or RHEL 8 minimal with 6 GB of RAM and 2 vCPUs and some storage for staging space and optionally a backup destination:
    - use first disk for operating system
    - add a secondary disk, i.e. 200GB - 1 TB (depending on the size your VMs that you want to backup)
    - leave it empty, you'll initialize this space later
2. Log in as root over SSH to your machine, where you want to install it.
3. RHEL 8 requires active subscription.
4. Download Data Protector for Cloud Workloads package.
5. Extract this package on the host where you're installing it:

    ```
    tar xvf DP-for-Cloud-Workloads-XXX.tgz
    ```

6. Move extracted repository to temp directory:

    ```
    mv elX /tmp/DP-for-Cloud-Workloads-repo
    ```

7. As root run:

    ```
    ./DP-for-Cloud-Workloads-local-install.sh
    ```

8. Update the proxy details in /opt/vprotect/vprotect.env for cloud backup/restore and restart the server and node services.

> Use system command **hostnamectl** to obtain the proper name for host. Add this entry in section **no_proxy**.

With a proper repo url (this can be changed with DP_REPO environment variable) – by default repo URL points to local directory file:///tmp/DP-for-Cloud-Workloads-repo.

Now you should be able to log in to Data Protector for Cloud Workloads Server using https://<DP4CW_server_IP> with local node registered and running.

Update

This package replaces previous installation. Database model and any dependencies may be updated during update. All configuration stored in the database or migrated to the new model automatically if necessary.

Server Upgrade

1. Create database backup - run as root over SSH on the Data Protector for Cloud Workloads Server

```
/opt/vprotect/scripts/backup_db.sh /path/to/backup/file.tgz
```

2. Extract this package on the hosts with Data Protector for Cloud Workloads Server or Node:

```
tar xvf DP-for-Cloud-Workloads-XXX.tgz
```

3. Update Data Protector for Cloud Workloads Server using RPMs in elX folder

```
yum update elX/DP-for-Cloud-Workloads-server-XXX.elX.x86_64.rpm
```

4. Update each Data Protector for Cloud Workloads Nodes using RPMs in elX folder

```
yum update elX/DP-for-Cloud-Workloads-node-XXX.elX.x86_64.rpm
```

5. Update each Data Protector for Cloud Workloads Cloud Server:

```
yum update elX/DP-for-Cloud-Workloads-cloudserver-XXX.elX.x86_64.rpm
```

6. Update each Data Protector for Cloud Workloads Cloud Agent:

```
yum update elX/DP-for-Cloud-Workloads-cloudagent-XXX.elX.x86_64.rpm
```

7. Log in to the Data Protector for Cloud Workloads Server using https://<DP4CW_server_IP> with nodes updated and running.

Notice, that you may need to refresh your browser cache after update - for Chrome use CTRL+SHIFT+R (Windows/Linux) / CMD+SHIFT+R (MacOS)

Downgrade

1. Downgrade Server with yum:

```
yum downgrade vprotect-server
```

2. On the Data Protector for Cloud Workloads Server host stop the Server service, restore database using your DB password and start server again (these can be found in `/opt/vprotect/payara.properties` file)

```
systemctl stop vprotect-server
mysql -u vprotect -pDBPASSWORD -e "drop database vprotect"
mysql -u vprotect -pDBPASSWORD -e "create database vprotect"
gunzip < PATH_TO_GZIPPED_BACKUP | mysql -u vprotect -pDBPASSWORD vprotect
systemctl start vprotect-server
```

3. On the Data Protector for Cloud Workloads Nodes hosts - downgrade nodes with

```
yum downgrade vprotect-node
```

4. Make sure all nodes are running and optionally start service on each Data Protector for Cloud Workloads host

```
systemctl start vprotect-node
```

Deinstallation

1. Remove packages with yum:

```
yum remove vprotect-server
yum remove vprotect-node
```

2. To remove configuration files:

```
rm -rf /opt/vprotect
```

3. To remove all remaining MariaDB data:

```
yum remove mariadb mariadb-server
rm -rf /var/lib/mysql
rm /etc/my.cnf
Optional step:
rm ~/.my.cnf
rm -f /var/log/mariadb
rm -f /var/log/mariadb/mariadb.log.rpmsave
rm -rf /usr/lib64/mysql
rm -rf /usr/share/mysql
```

4. To remove users:

```
userdel vprotect
userdel mysql
```

Installation using Ansible playbook

You can install the complete Data Protector for Cloud Workloads solution using the following 2 roles, available on Ansible Galaxy:

- Data Protector for Cloud Workloads Server: https://galaxy.ansible.com/xe0nic/ansible_vprotect_server
- Data Protector for Cloud Workloads Node: https://galaxy.ansible.com/xe0nic/ansible_vprotect_node

This approach installs a server and one or more nodes on remote hosts and generates an SSL certificate based on the server hostname. The end result should be the same as an RPM-based installation without the staging setup. Configuration (such as backup destination definition or hypervisor connectivity) still needs to be done after installation. You can also add more nodes in the future if necessary.

Prerequisites

You need to prepare CentOS 8/Stream or RHEL 8 minimal for Data Protector for Cloud Workloads (both roles can be installed on the same or different hosts). The Ansible control host should have Ansible installed so that it uses Python 3.x.0

This example assumes that you have `root` access to this host and you have configured your Ansible to connect with SSH public keys to your host. For example:

generate key:
`ssh-keygen -f ~/.ssh/id_rsa -P ""`

and copy it to your CentOS/RHEL box:
`ssh-copy-id -i ~/.ssh/id_rsa.pub root@YOUR_HOST`

The nodes will communicate with the Data Protector for Cloud Workloads Server via port 8181, so they need to be able to access it using the server's FQDN (this needs to be resolvable).

Installation

> Before installing Data Protector for Cloud Workloads we highly recommend doing a system update and reboot.

This example assumes that you want to install both the Data Protector for Cloud Workloads Server and Node **using a single playbook** and **on the same host.** However, keep in mind that you may also install them separately by providing different target hosts and using separate playbooks like in the examples in the readme roles (links above).

Run these on the system from which you run Ansible playbooks:

- Download the installation package from the Micro Focus download page
- Upload the installation package to all hosts (server and nodes)
- On each host, extract the archive:

```
tar xvf your-package.tgz
```

- The installation package contains a package repository in the `el8` folder which will be added automatically by the installation script. Move the extracted repository to the temp directory.

```
mv el8 /tmp/DP-for-Cloud-Workloads-repo
```

- Install Ansible roles:

```
ansible-galaxy install xe0nic.ansible_vprotect_server
ansible-galaxy install xe0nic.ansible_vprotect_node
```

- Install additional collections

```
ansible-galaxy install -r
~/.ansible/roles/xe0nic.ansible_vprotect_server/meta/collections.yml
ansible-galaxy install -r
~/.ansible/roles/xe0nic.ansible_vprotect_node/meta/collections.yml
```

- Create a playbook directory and change it to a working directory, i.e: `mkdir vprotect && cd vprotect`
- Create an inventory file - i.e. `hosts` and refer to the location to where you extracted the repository
    - in this example we have specified one node and server, but you can define more nodes (each one must be in a separate line and have a unique node name)
    - the server can be on a different host
    - we recommend having at least one node installed together with the server to run DB backups

```
[all:vars]
ansible_user = root
vprotect_repo = file:///tmp/DP-for-Cloud-Workloads-repo
admin_pass=password
db_pass=password

[server]
192.168.1.2

[nodes]
192.168.1.2 node_name=node1
```

where:

- `admin_pass` - password for admin user
- `db_pass` - password for mysql root user
- `node_name` - name under which node will be registered

> If you don't provide password for admin user and mysql root user, it will be set to **vPr0tect**

- Create a playbook file - `site.yml`:

```
---

- hosts: server
  roles:
  - xe0nic.ansible_vprotect_server

- hosts: nodes
```

```
    roles:
    - xe0nic.ansible_vprotect_node
```

- Run the playbook: `ansible-playbook -i hosts site.yml`
- After installation, you should be able to log in to your Data Protector for Cloud Workloads Server: `https://<DP4CW_server_IP>` and your nodes should be registered and running. By default, Data Protector for Cloud Workloads has one admin account - `admin` with the password `vPr0tect` (with a zero).
- Remember to prepare your staging space as described in the Staging space configuration.
- Now proceed with the Initial configuration instructions to configure access to the hypervisors and backup destinations.

Variables

These two roles use just a few variables. Both plays use the `server_fqdn` variable. If not defined, the server play sets the variable `server_fqdn` to the hostname reported by the OS on which it is installed. The server play will generate an SSL certificate for this FQDN, and node play will automatically use this value if defined. You can also provide this variable manually (either in the `hosts` file or with the extra vars switch in the `ansible-playbook` command, i.e. `-e "server_fqdn=vprotect.server.local"`

Node play needs a `node_name` for the registration process. If not provided, it will just use the hostname reported by the OS, however, keep in mind that it needs to be **unique** for each node. We recommend that you set them in the host inventory file.

Optionally, you may want to set a `db_password` for the root DB access which is set during server installation. Note, that the Server service uses its own account with an auto-generated password.

By default, Data Protector for Cloud Workloadst uses MariaDB 10.4 for CentOS - you can control the source, distribution and version of your MariaDB with the following variables (with their respective default values):

```
mariadb_version: "10.4"
mariadb_distro: "centos7-amd64"
mariadb_repo_url: "http://yum.mariadb.org/{{ mariadb_version }}/{{ mariadb_distro }}"
mariadb_repo_gpg_key: "https://yum.mariadb.org/RPM-GPG-KEY-MariaDB"
```

Installation with RPMs

Prerequisites

1. Install CentOS/RHEL 8 minimal
    - if you plan to use deduplication with VDO we recommend using RHEL to have Red Hat's support available
    - you also can use version CentOS/RHEL 7
2. Make sure your OS is up to date:

    ```
    dnf -y update
    ```

    If the kernel is updated, then you need to reboot your operating system.
3. Download the Data Protector for Cloud Workloads package from the Micro Focus download page.
4. Extract your package (replace the name with the downloaded package name):

    ```
    tar xvf your-package.tgz
    ```

5. Move the xtracted repository to the temp directory.

    ```
    mv el8 /tmp/DP-for-Cloud-Workloads-repo
    ```

6. Install the Data Protector for Cloud Workloads repository

- create a file `/etc/yum.repos.d/DP4CW.repo`:

    ```
    # Data Protector for Cloud Workloads - Enterprise backup solution for virtual
    environments repository
    [DP-for-Cloud-Workloads]
    name = Data Protector for Cloud Workloads
    baseurl = file:///tmp/DP-for-Cloud-Workloads-repo
    gpgcheck = 0
    ```

7. Install the MariaDB repository (Data Protector for Cloud Workloads **Server host only**

- generate .repo file at MariaDB download site
- copy and paste the generated repo file into `/etc/yum.repos.d/MariaDB.repo`, so it looks similar to this (this one for CentOS/RHEL 8):

    ```
    # MariaDB 10.4 CentOS repository list - created 2020-06-01 16:14 UTC
    # http://downloads.mariadb.org/mariadb/repositories/
    [mariadb]
    name = MariaDB
    baseurl = http://yum.mariadb.org/10.4/centos8-amd64
    ```

```
module_hotfixes=1
gpgkey=https://yum.mariadb.org/RPM-GPG-KEY-MariaDB
gpgcheck=1
```

Data Protector for Cloud Workloads Server installation

Data Protector for Cloud Workloads consists of a server (a central management point with a WebUI) and one or multiple nodes (which can be installed on the same host as the server or on other machines). The first step is always to install the server.

1. Install the Data Protector for Cloud Workloads Server using DNF package manager:

   ```
   dnf -y install vprotect-server
   ```

2. Set up the DB for Data Protector for Cloud Workloads:

   - Please provide a MariaDB password
   - Please remember to not re-run this command on running/production Data Protector for Cloud Workloads instance. This can cause problems with the Data Protector for Cloud Workloads database.

   ```
   vprotect-server-configure
   ```

3. Start the Data Protector for Cloud Workloads Server (it can take around a minute for the server to start):

   ```
   systemctl start vprotect-server
   ```

4. You may need to open the 8181 port (for HTTPS, HTTP requires port 8080) on your firewall. Here is an example:

   ```
   firewall-cmd --add-port=8181/tcp --permanent
   firewall-cmd --complete-reload
   # To check open ports:
   firewall-cmd --list-all
   ```

   or if you prefer to have the Data Protector for Cloud Workloads console running on the default HTTPS port (443), there is a script in the `/opt/vprotect/scripts` directory to set up forwarding from port 443 to 8181:

   ```
   cd /opt/vprotect/scripts
   ./ssl_port_forwarding_firewall-cmd.sh
   ```

5. Now you should be able to log in to the web console using the URL: `https://<DP4CW_server_IP>:8181`, where `<DP4CW_server_IP>` is the hostname or IP of your Data Protector for Cloud Workloads Server

   - by default, Data Protector for Cloud Workloads has one admin account - `admin` with the password `vPr0tect` (with a zero)

6. Optionally, if you are going to connect nodes running on remote hosts, proceed with the steps related to the Data Protector for Cloud Workloads Server described in the section: Enabling HTTPS connectivity for remote nodes

Data Protector for Cloud Workloads Node installation

Data Protector for Cloud Workloads Node is a component that executes all tasks. It can be installed together with the Server (it is common to have 1 server and just 1 node). More nodes can always be added later.

1. Install the Data Protector for Cloud Workloads Node using DNF:
   Remember to add our repository to the host machine

   ```
   dnf -y install vprotect-node
   ```

2. Prepare your staging space (on the Data Protector for Cloud Workloads Node host only):

   - If you just started with Data Protector for Cloud Workloads, and do not know what is staging space please follow the steps described in the Staging space configuration
   - **if your path is different than** `/vprotect_data` it is recommended to create a symlink `/vprotect_data` pointing to your staging space mount point, e.g.:

     ```
     ln -s /mnt/staging /vprotect_data
     ```

3. Register the node with the `NODE_NAME` of your choice, the `ADMIN_USER` user name which you would like to use and the URL to the Data Protector for Cloud Workloads API, and provide a password when prompted:

   - Syntax:

     ```
     vprotect node -r NODE_NAME ADMIN_USER http(s)://<DP4CW_server_IP>:PORT/api
     ```

   - If you are going to connect nodes running on remote hosts, please proceed with the steps related to the Data Protector for Cloud Workloads Node described in the section: Enabling HTTPS connectivity for remote nodes
   - Example for default local installation - over HTTP (port 8080):

     ```
     vprotect node -r node1 admin http://localhost:8080/api
     ```

4. Start the Data Protector for Cloud Workloads Node:

   ```
   systemctl start vprotect-node
   ```

   Now you should be able to see a new entry in the `Node` section of the web UI with your node in RUNNING state.

5. Run the script to configure the OS for Node, which includes changing the QEMU user/group to `vprotect`, disabling SELinux, adding Data Protector for Cloud Workloads to the disk group and sudoers to allow it to run privileged commands:

   ```
   vprotect-node-configure
   ```

6. Reboot the Data Protector for Cloud Workloads VM to apply the OS-specific settings:

```
reboot
```

Data Protector for Cloud Workloads is installed - you can now proceed with the steps described in the Initial configuration.

Backup Destinations

A backup destination is a storage location where Data Protector for Cloud Workloads keeps VMs, Containers, Cloud, and applications backup copies. To configure a backup destination, you can use the following storage types:

- File System
- Deduplication Appliances
- Object Storage
- Enterprise Backup Providers

The backup destination is defined by the backup provider configuration and retention settings. Each policy can be backed up to the selected backup destination. Backup destinations must be assigned to the nodes in the node configuration.

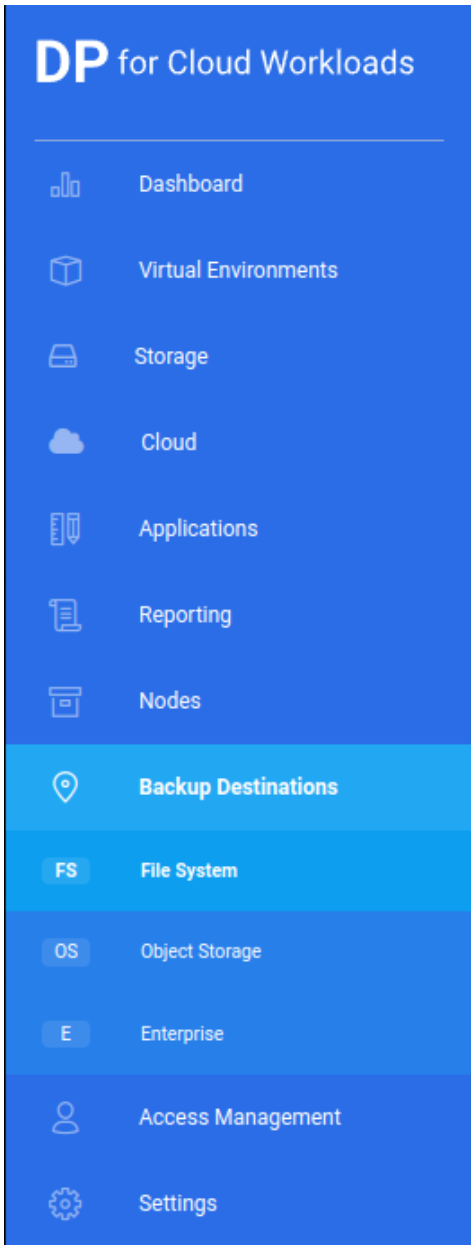
> **Note:** removal of any backup destination leaves data in the backup provider without an option to re-attach it in the future.

Retention

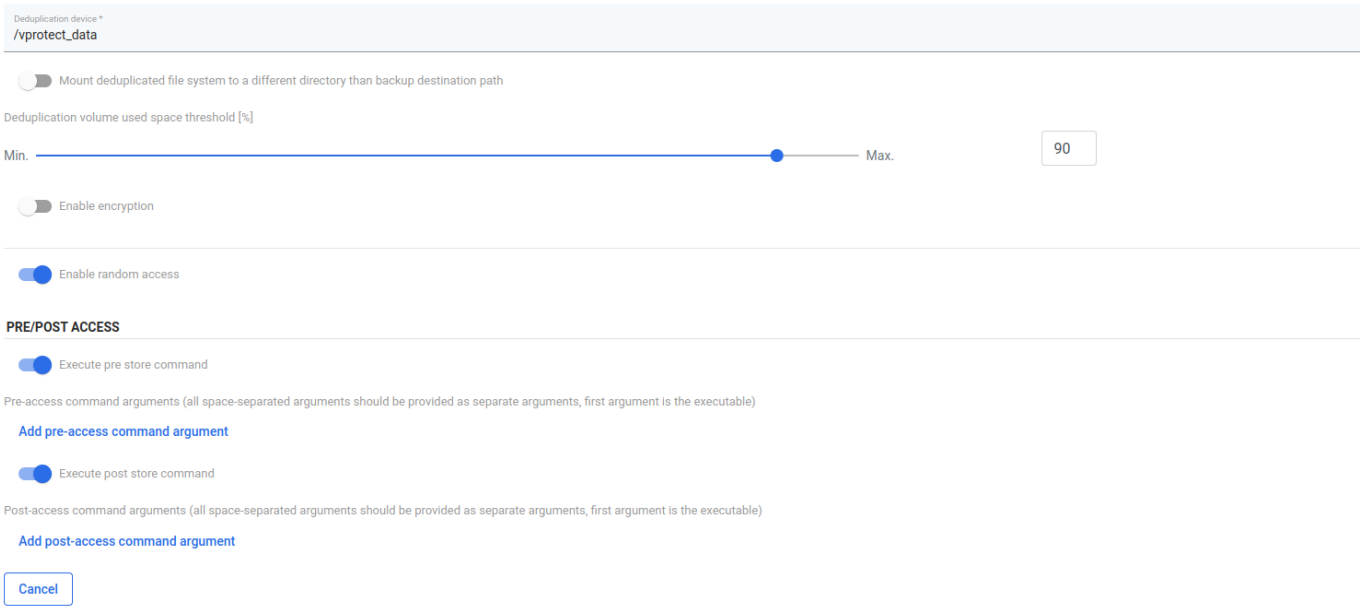
> **Note:** Retention settings are described in chapter Backup SLAs - Policy - Rule

Pre/post access command execution

- Prepare your scripts
  - the pre-script is invoked before every access to the Backup Destination - common usage - create and mount the remote volume
  - the post-script is executed after Node finishes store, restore, and clean-up operations
- The following environment variables are set before each execution - you can use them later in your scripts:
  - `VP_VM_GUID` - GUID of the VM in Data Protector for Cloud Workloads
  - `VP_VM_UUID` - UUID of the VM used by the hypervisor or hypervisor manager
  - `VP_VM_NAME` - the name of the VM
  - `VP_VM_TMP_DIR` - path to the folder containing files in the staging
  - `VP_BD_GUID` - GUID of the Backup Destination being accessed
  - `VP_BD_NAME` - the name of the Backup Destination being accessed
  - `VP_CONTAINER_NAME` - standard container name generated by Data Protector for Cloud Workloads that can be used for names of the volumes (format `<VM-NAME>__<PART-OF-UUID>`, i.e. `Centos 7__8d3ef6f1`, may contain special characters)
  - `VP_EXPORT_PATH` - an export path from Node Configuration, can be used as the mount root for backup destination volumes
  - `VP_TASK_TYPE` - the name of the task type, e.g.: STORE / RESTORE / DELETE_VM / OLD_BACKUPS_REMOVAL - to distinguish operation type when scripts are being invoked
- Upload your scripts to the **node**, where the `vprotect` user is able to access them
- Optionally, you may need to add a new file in the `/etc/sudoers.d/` directory to enable the `vprotect` user to execute privileged script (like chown operations in some file system locations): `%vprotect ALL=(root) NOPASSWD: /opt/vprotect/scripts/myscripts/privileged.sh`
- Open the "BACKUP DESTINATIONS" section from the left menu:



- Open your Backup Destination (click on the name)
- Provide pre/post access command arguments (the first argument is the command executed locally on the **node**):



File System

This section presents the key steps necessary for configuring a file system as your backup destination. You can use a:

- local File system or remote (NFS, SMB, etc.) or attach a block device with enabiling there Virtual Data Optimizer (VDO)
- Synthetic File System

File system

In this section, we'll show you how to set up a file system (it can be a local or remote file system, but this example assumes that you have a dedicated disk that you're going to use as a backup destination with a local XFS file system)

> **Note:**
>
> - Any remote FS like **NFS, SMB, etc.** - needs to be mounted by the user, and the vprotect user/group must own the directories within the backup destination. Data Protector for Cloud Workloads expects an already mounted file system and mount point in the backup destination.
> - You should add this file system to your /etc/fstab file on the node so that it gets mounted automatically if the OS is rebooted.
> - Consider using the same file system for the staging and backup destination (this boosts storage tasks, as no data needs to be copied again) - in such a scenario, the only difference would be that the presented /backupdestination mount point becomes a subdirectory of the staging space (usually /vprotect_data/backups).

Preparation

1. Log in to Data Protector for Cloud Workloads Node and create the mount directory as in the example `/backupdestination`

```
mkdir /backupdestination
```

2. List all existing disks and find your drive:

```
[root@vProtect01 ~]# fdisk -l | grep dev
Disk /dev/sda: 32.2 GB, 32212254720 bytes, 62914560 sectors
/dev/sda1   *        2048     1026047      512000   83  Linux
/dev/sda2         1026048    62914559    30944256   8e  Linux LVM
Disk /dev/sdc: 500 GB, 17179869184 bytes, 33554432 sectors
Disk /dev/sdb: 21.5 GB, 21474836480 bytes, 41943040 sectors
Disk /dev/mapper/centos-root: 28.5 GB, 28462546944 bytes, 55590912 sectors
Disk /dev/mapper/centos-swap: 3221 MB, 3221225472 bytes, 6291456 sectors
```

3. Prepare a filesystem on it:

```
mkfs.xfs -K /dev/sdc
```

4. Add permission for the Data Protector for Cloud Workloads user to access the directory `/backupdestination`

    - we assume here that you use a separate file system than your staging space
    - as an alternative, you also can point Data Protector for Cloud Workloads to use a subdirectory on the same file system as your staging space, i.e. `/vprotect_data/backups` (which you probably don't have to initialize at this point, as you may have already prepared it in the Staging space configuration, and you can just jump to the Web UI part in the next steps).

```
chown vprotect:vprotect -R /backupdestination
```

5. Add this line to the `/etc/fstab` file to automatically mount new the filesystem after reboot:

```
/dev/sdc    /backupdestination    xfs    defaults 0 0
```

   or if you want to store backups on NFS share then it will look like this (where 10.50.1.28 is your host):

```
10.50.1.28:/example_nfs_share /backupdestination nfs defaults  0 0
```

6. Check if the fstab entry is OK and mount the filesystem:

```
mount /backupdestination
```

7. Log in to the Data Protector for Cloud Workloads web UI.
8. Go to **Backup Destinations.**
9. Click on **Create Backup Destination**, choose a **File system.**
10. Type the name for the new backup destination, set the retention, and select at least one node configuration.
11. Usually, you have to decide if your backup destination is a separate entity from the staging space.
    - If the **staging space is different than your backup storage destination:**
      - In **Storage paths** type `/backupdestination` - this path will be used to mount the prepared file system (XFS) on top of the VDO volume.
    - If the **staging space needs to be the same as your backup storage destination:**
      - In **Storage paths** type `/vprotect_data/backups`, where you point to a subdirectory (i.e. `backups` on your staging space path, i.e. `/vprotect_data)`.
12. Save the configuration.

Virtual Data Optimizer (VDO)

In this section, you can find information on how to enable deduplication using basically any block storage available. We assume that you have prepared your storage provider and have exposed the block device to the system where Data Protector for Cloud Workloads Node is installed.

Preparation

> Secure Boot option must be disabled for the VM to allow VDO work properly. Run below command to check status of Secure Boot option:
>
> ```
> mokutil --sb-state
> ```

1. Log in to Data Protector for Cloud Workloads Node and create a mount directory as in the example `/backupdestination`

   ```
   mkdir /backupdestination
   ```

2. List all existing disks, and find your drive:

   ```
   [root@vProtect01 ~]# fdisk -l | grep dev
   Disk /dev/sda: 32.2 GB, 32212254720 bytes, 62914560 sectors
   /dev/sda1   *        2048     1026047      512000   83  Linux
   /dev/sda2         1026048    62914559    30944256   8e  Linux LVM
   Disk /dev/sdc: 500 GB, 17179869184 bytes, 33554432 sectors
   Disk /dev/sdb: 21.5 GB, 21474836480 bytes, 41943040 sectors
   Disk /dev/mapper/centos-root: 28.5 GB, 28462546944 bytes, 55590912 sectors
   Disk /dev/mapper/centos-swap: 3221 MB, 3221225472 bytes, 6291456 sectors
   ```

3. Let's assume `/dev/sdc` is your empty block device that you want to use.

4. Log in to the Data Protector for Cloud Workloads web UI.

5. Go to **Backup Destinations.**

6. Click on **Create Backup Destination**, choose a **File system.**

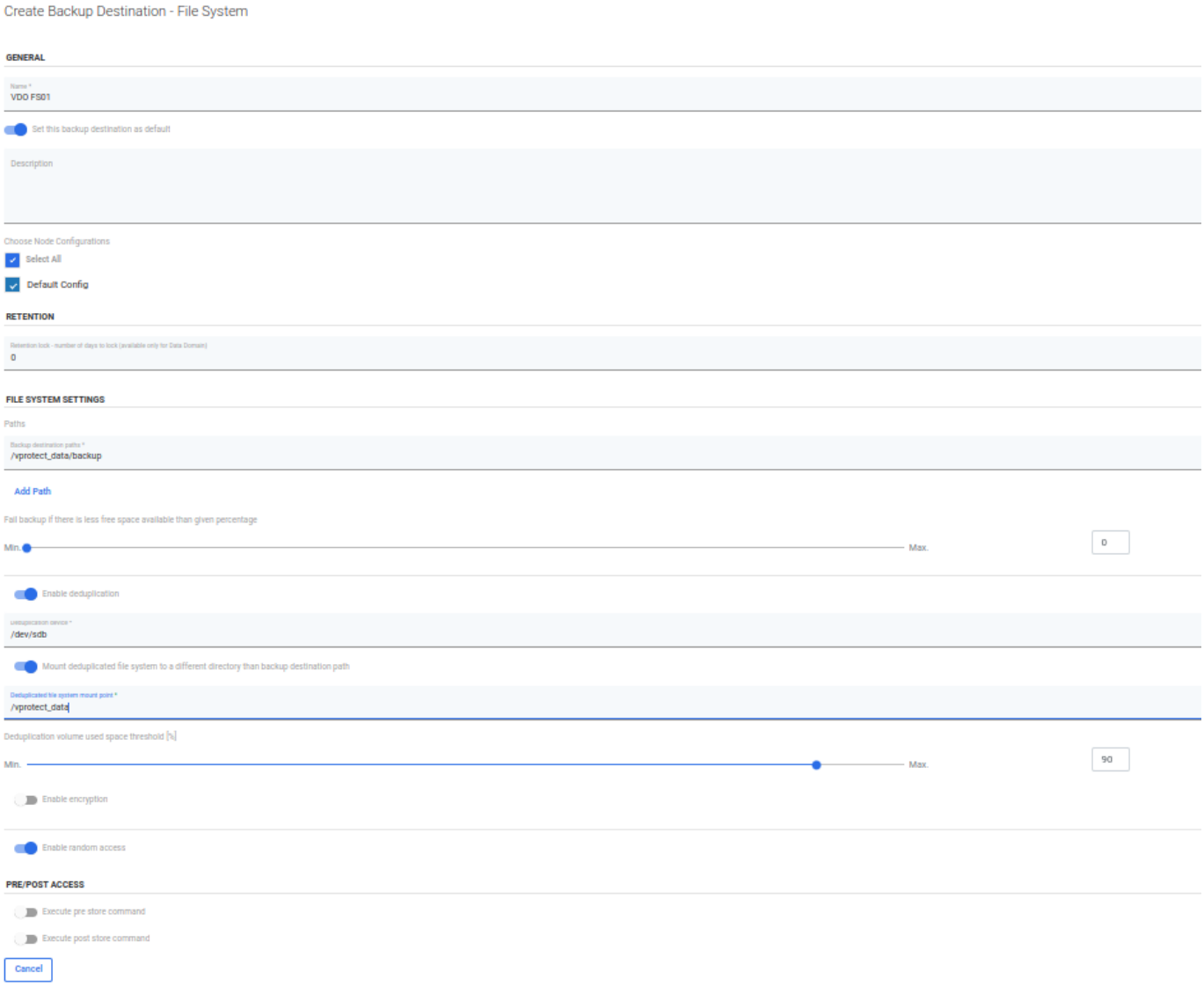
7. Type the name for the new backup destination, set the retention, and select at least one node configuration.

8. Usually, you have to decide if your backup destination is a separate entity from the staging space.

   - If the **staging space is different than your backup destination** storage:
     - In **Storage paths** type `/backupdestination` - this path will be used to mount the prepared file system (XFS) on top of the VDO volume.
     - Check **Enable deduplication.**
     - Provide your block device (i.e. `/dev/sdc`) as your Deduplication device.

9. If the **staging space needs to be the same as your backup destination** storage:

- In **Storage paths** type `/vprotect_data/backups` - this path assumes that `/vprotect_data` is your staging space path and `backups`is a subdirectory of the staging space.
- Check **Enable deduplication.**
- Provide your block device (i.e. `/dev/sdc`) as your **Deduplication device.**
- Enable **Mount deduplicated file system to a different directory than backup destination path** and provide the mount point - your staging space path, i.e. `/vprotect_data` - this will force Data Protector for Cloud Workloads to mount XFS on top of VDO in the staging space directory rather than in the backup subdirectory.



Note: Only one file system backup destination with deduplication using VDO pointing to a specific directory can be used.

- If you want to add another backup destination using the same VDO device, but just a different subdirectory, create it without deduplication enabled.
- Save the configuration.

Synthetic File System

A synthetic file system allows us to store and use incremental backups as if they were full backup files, but they take up a fraction of full file size.

To start using Synthetic File System read Prerequisites for Synthetic filesystem XFS

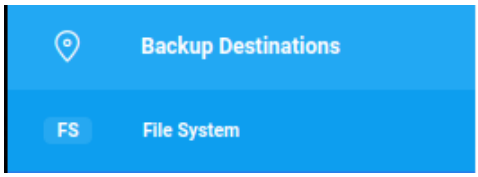
XFS

Prerequisites:

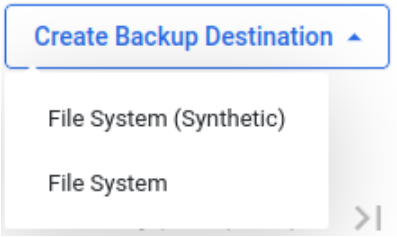
> **Note:**
>
> - The only prerequisite to using synthetic XFS as a backup destination is that the selected storage path is on the XFS
> - For a basic setup of file systems on the Node check File system

Creating a Synthetic Filesystem Backup Destination

1. Select File System from Backup Destinations,



2. Select Create Backup Destination -> File System (Synthetic),



3. The rest of the configuration is similar to a regular File system.

> **When setting the path, make sure it's actually on the XFS!**

Deduplication Appliances

This section presents the key steps necessary for configuring integration with deduplication appliances as your backup destination. You can use NFS or SMB to attach Dell EMC Data Domain.

Dell EMC Data Domain

Create a new Backup Destination (Dell EMC Data Domain)

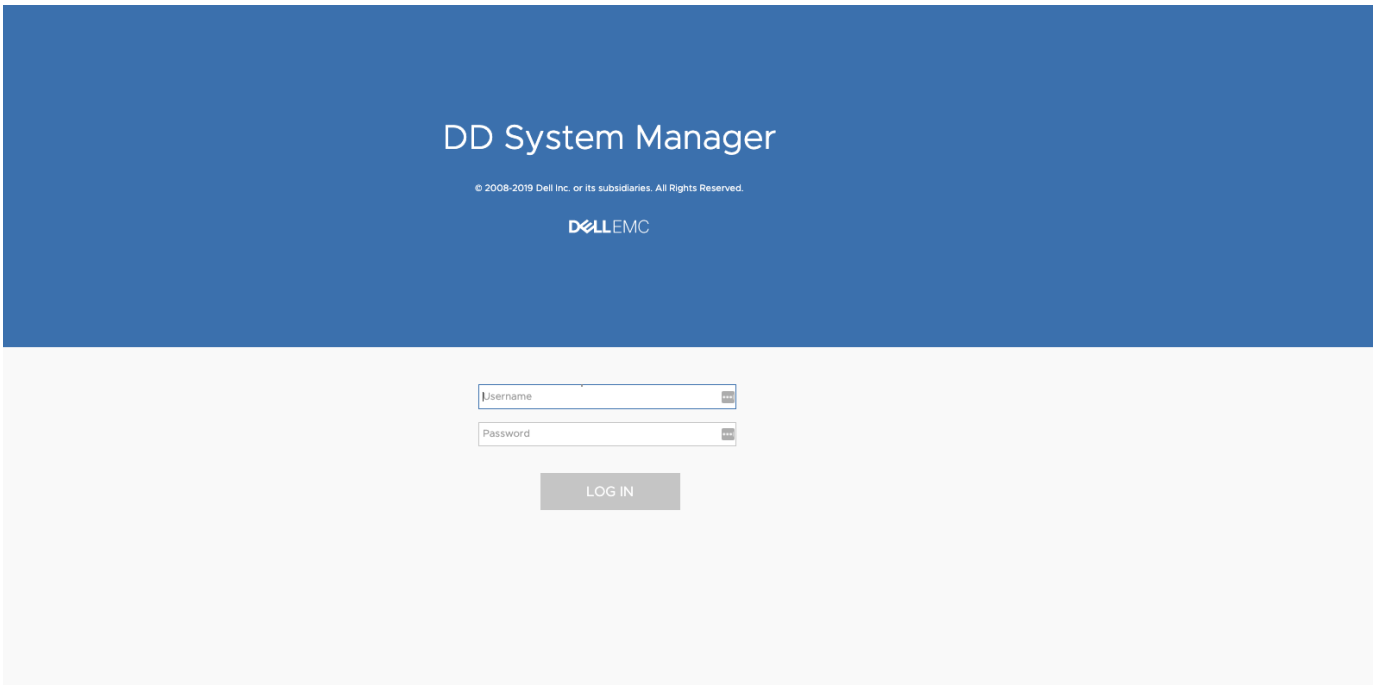
- Go into the backup destination menu and click on Create a backup destination.
- Provide a name and description for the new backup destination.
- Specify the retention days for full and incremental backups.
- Specify the retention versions for full and incremental backups.
- Choose and assign the node configuration to which you want to attach the new backup destination.
- Add to one or more storage paths.
    - `example - /vprotect_data/backupdestination`
- Save the configuration.

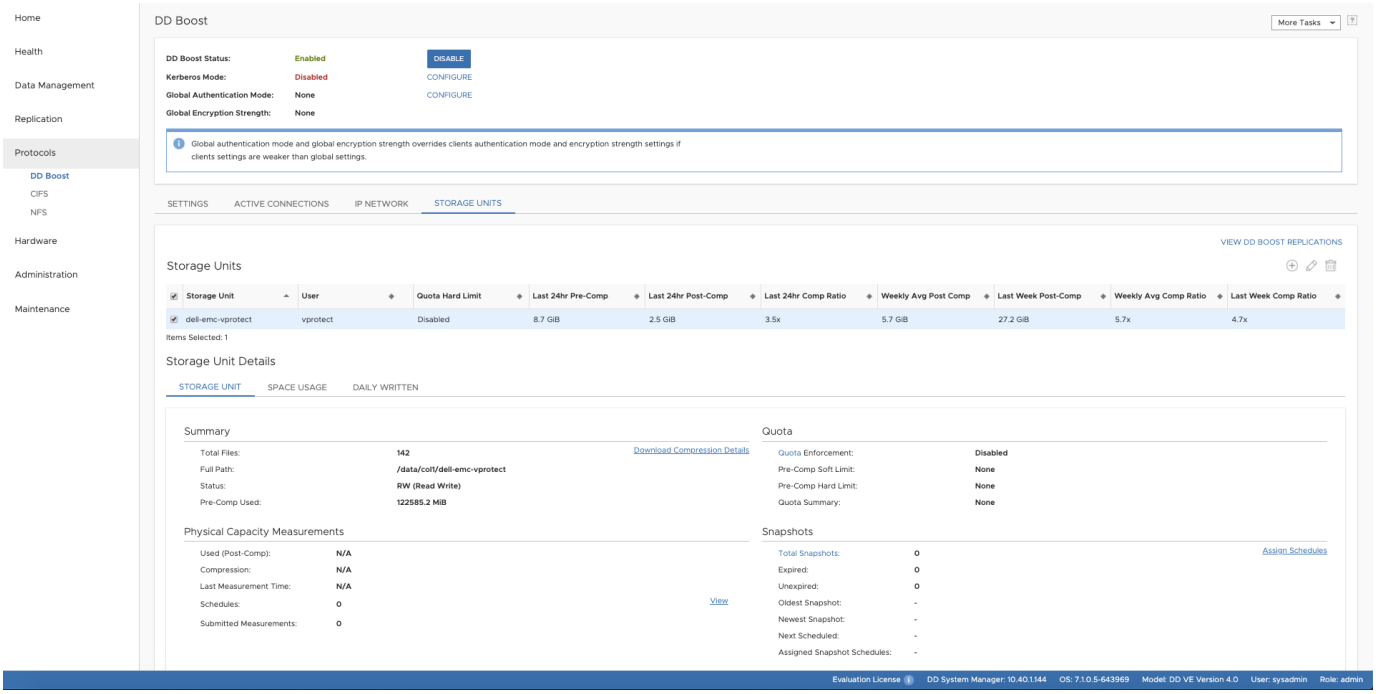
DD Boost FS Plugin

- To boost the backup process we recommend using a **single** Storage Unit and mtree, and subfolders on the BoostFS for multiple backup destinations (with possibly different retention settings).
    - No additional data copy is needed in the store phase if staging is using the same file system as the backup destination.
    - The Setup assumes a single Storage Unit and a single mtree for all backup destinations.
    - The staging space should always be a top directory, and all backup destinations should be defined as separate subfolders of this file system.
    - Data Protector for Cloud Workloads handles retention, and each backup destination may have different retention configured.
    - A single Storage Unit will also affect replication as it has to cover all backup destinations, and may replicate temporary data from the staging space or mounted backups.
- **Sharing** the same BoostFS across multiple nodes allows the administrator to create backups on one node (i.e. one host/environment) and restore using a different node (to a different host/environment).
    - UID/GID ownership and permissions must allow Data Protector for Cloud Workloads to read/write contents of the BoostFS share.
    - To meet these requirements, the user and group named vprotect that was created during the installation process must have the same UID and GID on each Data Protector for Cloud Workloads Node machine. You can create this before installing Data Protector for Cloud Workloads packages or change it after installation.

Prepare your PowerProtect DD as a backup destination:

- Login to PowerProtect DD and create an NFS Storage Unit called `DP-for-Cloud-Workloads`.





- Download BoostFS RPM from the Dell EMC site.
- Install BoostFS:

```
rpm -ivh DDBoostFS-7.0.0.0-633922.rhel.x86_64.rpm
```

- Save the password for BoostFS.

```
# Syntax
/opt/emc/boostfs/bin/boostfs lockbox set -d [DataDomain_IP_OR_DNS_NAME] -u
[Access_User_Name] -s [Storage_Area_Name]
# Example
/opt/emc/boostfs/bin/boostfs lockbox set -d 10.1.10.100 -u vprotect -s
vprotectbackup
```

- Add the /etc/fstab entry:

```
# Syntax
[DataDomain_IP_OR_DNS_NAME]:/[Storage_Area_Name] /[Mount_Point] boostfs
defaults,_netdev,bfsopt(allow-others=true) 0 0
# Example
10.1.10.100:/vprotectbackup /vprotect_data boostfs
defaults,_netdev,bfsopt(allow-others=true) 0 0
```

- Mount the fstab entry:

```
mount -a
```

- For a manual, one-time mount you can run this command:

```
# Syntax
/opt/emc/boostfs/bin/boostfs mount -o allow-others=true -d
[DataDomain_IP_OR_DNS_NAME] -s [Storage_Area_Name] /[Mount_Point]
# Example
/opt/emc/boostfs/bin/boostfs mount -o allow-others=true -d 10.1.10.100 -s
vprotectbackup /vprotect_data
```

- Confirm with `df -h` that your `/vprotect_data` is mounted
  Note: Remember to specify the backup destination path as a subdirectory of /vprotect_data if you would like to use the same storage unit as a staging space and backup destination - for example: /vprotect_data/my-backups.

```
mkdir /vprotect_data/my-backups
```

- Set ownership to the vprotect user on the directory /vprotect_data.

```
chown vprotect:vprotect -R /vprotect_data
```

- Set ownership to the vprotect user and data domain group on the directory /vprotect_data/my-backups.

```
chown vprotect:gid /vprotect_data/my-backups
```

where 'gid' is the GID of data domain user specified in Synthetic DD Boost backup destination configuration.

- Set read and write privileges for both user and group to the directory /vprotect_data/my-backups.

```
chmod 0775 /vprotect_data/my-backups
```

Object Storage

A backup destination is a storage location where Data Protector for Cloud Workloads keeps VMs, Containers, Cloud, and application backup copies. Data Protector for Cloud Workloads supports different types of object storage.

- Alibaba Cloud OSS
- AWS S3 or S3-compatible
- Ceph Rados Gateway
- Cloudian S3
- Wasabi
- Google Cloud Storage
- IBM Cloud Object Storage
- Microsoft Azure Blob Storage
- Nutanix Objects
- OpenStack SWIFT
- Oracle Cloud Infrastructure Object Storage
- Scality RING

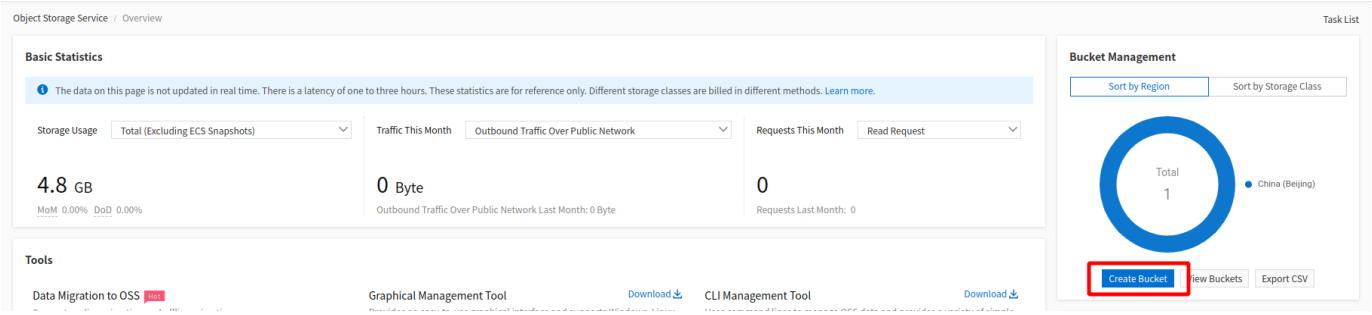
Alibaba Cloud OSS

Overview

Alibaba Cloud is an S3-compatible backup provider. Configuration as a backup destination is similar to AWS S3.

Example

After logging in, go to the Object Storage Service and create a new bucket.



Provide necessary details for your bucket and enable versioning.

Create Bucket

Create a bucket

Note: Storage Class, Region, and Zone-redundant Storage cannot be changed after the bucket is created.

Bucket Name

0/63

Region

China (Beijing)

Alibaba Cloud services in the same region can communicate with each other over an internal network. The region cannot be changed after the purchase. Exercise caution when you select a region.

Endpoint

oss-cn-beijing.aliyuncs.com

Storage Class

Standard | IA | Archive

Standard: high-performance, reliable, and highly available storage class. We recommend that you use this storage class for data that is frequently accessed.

How to Choose a Suitable Storage Class

Zone-redundant Storage Hot

Enable | Disable

OSS can back up your data to three zones within the same region to provide data center disaster recovery. Learn more.

Zone-redundant storage improves the availability of data. This feature incurs extra costs. For more information about the pricing of this feature, visit price details. This feature cannot be disabled after it is enabled.

Versioning Hot

Enable | Disable

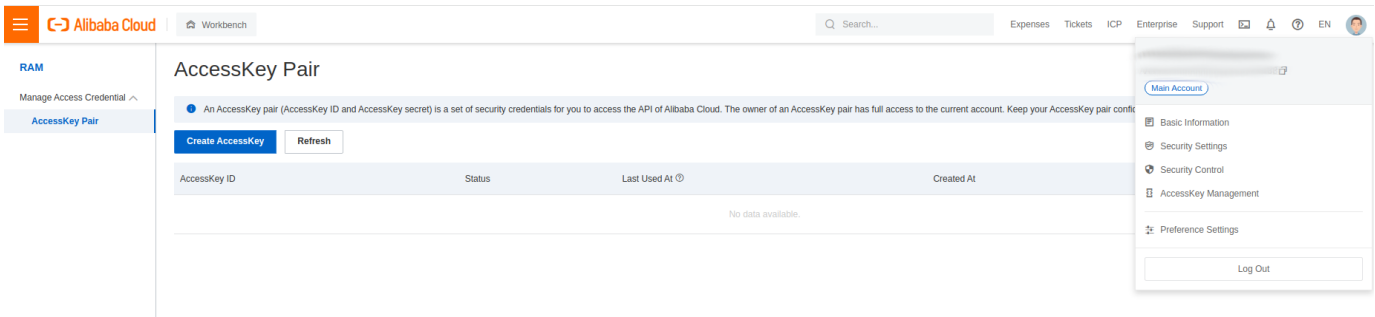
After versioning is enabled for a bucket, data that is overwritten or deleted in the bucket is saved as a previous version. If you enable versioning for a bucket, you are charged for the storage of the current and previous versions of objects in the bucket. Learn more.This feature cannot be disabled after it is enabled.

Access Control List (ACL)

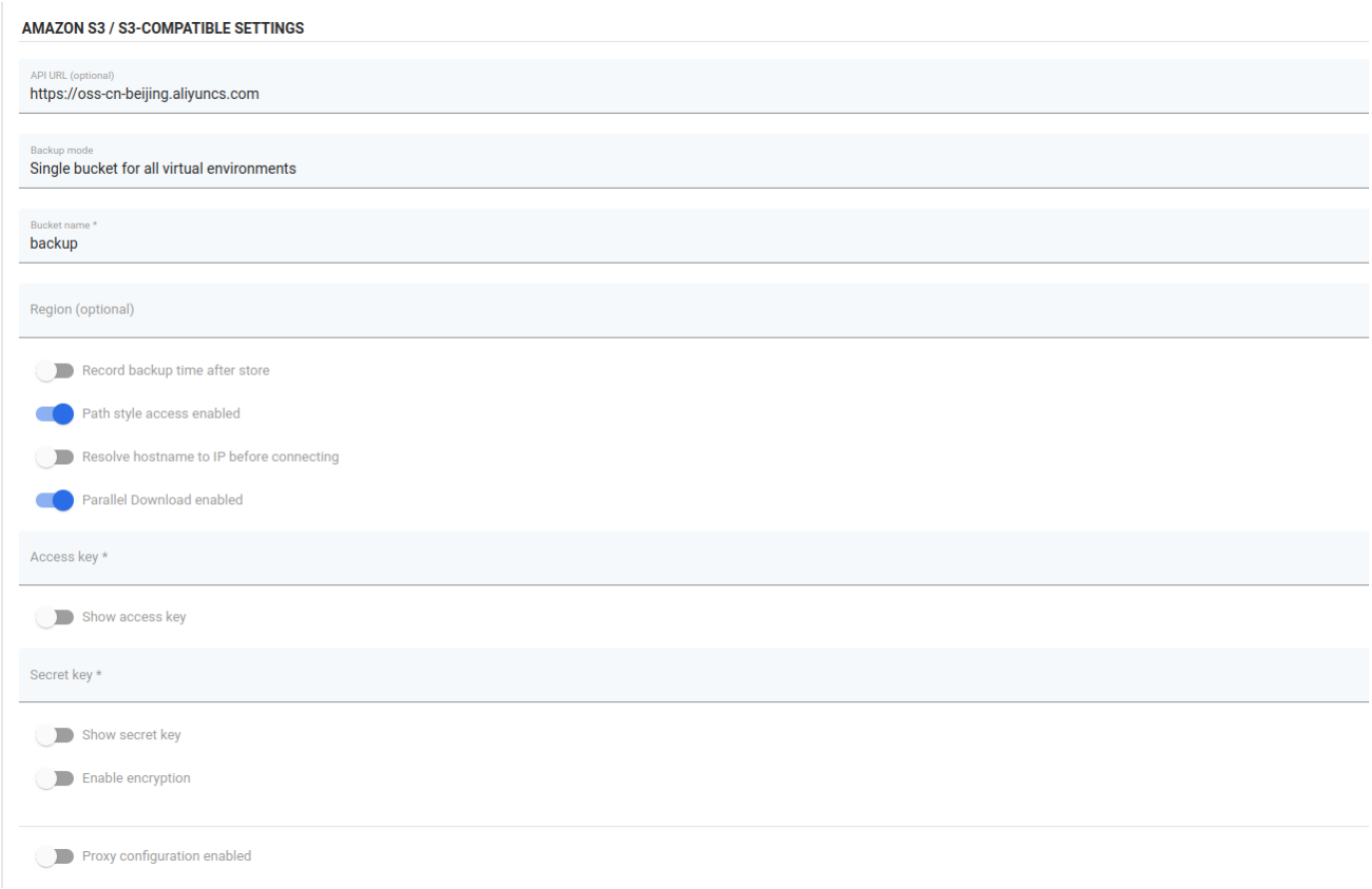
Private | Public Read | Public Read/Write

OK | Cancel

Next, go to Manage AccessKey Management and create new AccessKey



Now go to the Backup destination tab on the Data Protector for Cloud Workloads dashboard and change the sub-tab to object storage. Provide the bucket name and key credentials, and then configure the remaining options according to your requirements:



AWS S3 or S3-compatible

Overview

Data Protector for Cloud Workloads can store backups in AWS S3 or S3-compatible backup providers. In most cases, you just need to prepare a bucket (with versioning enabled if possible) and generate an access/secret key for Data Protector for Cloud Workloads. Data Protector for Cloud Workloads can be installed in AWS (if EC2 backup is used), but in most cases, S3 is used just as a cloud backup provider for on-prem environments.

Typical use cases are:

- When AWS is used - choose a single bucket with **versioning enabled** - all backup objects will have names in `/container_name/path/to/backup` format, where `container_name` typically is the VM name with an identifier.
- When a 3rd party is used - you need to verify:
  - Which strategy is supported by the vendor - i.e. Scality requires a single bucket without versioning.
  - When timestamp recording of the object should occur - i.e. Scality does it after data is stored (unlike AWS).

Data Protector for Cloud Workloads is also able to **encrypt** backups before sending backups (client-side encryption: SSE-C). Once enabled, new data is stored as encrypted with keys generated and kept by Data Protector for Cloud Workloads. For performance improvements, we also recommend using AWS Direct Connect to access S3. Otherwise, backups would be sent over the Internet, which could result in poor performance.

> **Note:** S3 has a **limit of 5TB** per object. This means that depending on the virtualization platform and backup format used by export/import mode you may have a limit of 5TB per VM (if it is Proxmox VMA or Citrix XVA image-based backup) or per VM disk (in most cases). Bigger files are currently not supported.

Permissions

Depending on the selected mode, you may have different permission sets. For a single bucket, you need to use the access keys of a user that has the ability to control objects within the bucket over the specific bucket - here is an example of IAM policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1568968204280",
      "Action": [
        "s3:DeleteObject",
        "s3:DeleteObjectTagging",
        "s3:DeleteObjectVersion",
        "s3:DeleteObjectVersionTagging",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetObject",
        "s3:GetObjectRetention",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:PutObjectTagging",
```

```
            "s3:PutObjectVersionTagging",
            "s3:RestoreObject"
        ],
        "Effect": "Allow",
        "Resource": "arn:aws:s3:::BACKUP_DESTINATION_BUCKET/*"
      }
    ]
}
```

You can also use a predefined role and create a user from the AWS console:
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html#Using_CreateAccessKey

> **Note:** It is recommended to periodically rotate your access/secret keys. More information can be found here: https://aws.amazon.com/blogs/security/how-to-rotate-access-keys-for-iam-users/. After changing the key in AWS, remember to update it in Data Protector for Cloud Workloads as well.

Bucket replication

Even though S3 is a highly available service, you may want to be prepared in case of a region failure. We recommend following this guide https://docs.aws.amazon.com/AmazonS3/latest/dev/replication.html to set up bucket replication so that your data is replicated to another region in a worst-case scenario. Remember to point Data Protector for Cloud Workloads to the replicated bucket in case of a disaster.

Glacier/Deep Archive support

Data Protector for Cloud Workloads is able to move older backups to a Glacier/Deep Archive storage tier. In the S3 backup provider settings, you need to enable the `Move old versions to other storage class` toggle and provide extended retention settings.

Keep in mind that Data Protector for Cloud Workloads will try to restore it to S3 with an expiration set to 2 days. You'll notice that although the task is running, no progress is taking place as it is waiting for the object to be restored from Glacier to S3. This **may take several hours** as Glacier doesn't provide instant access to archival data. Once this part is completed, Data Protector for Cloud Workloads will proceed with regular restore from a temporary S3 object.

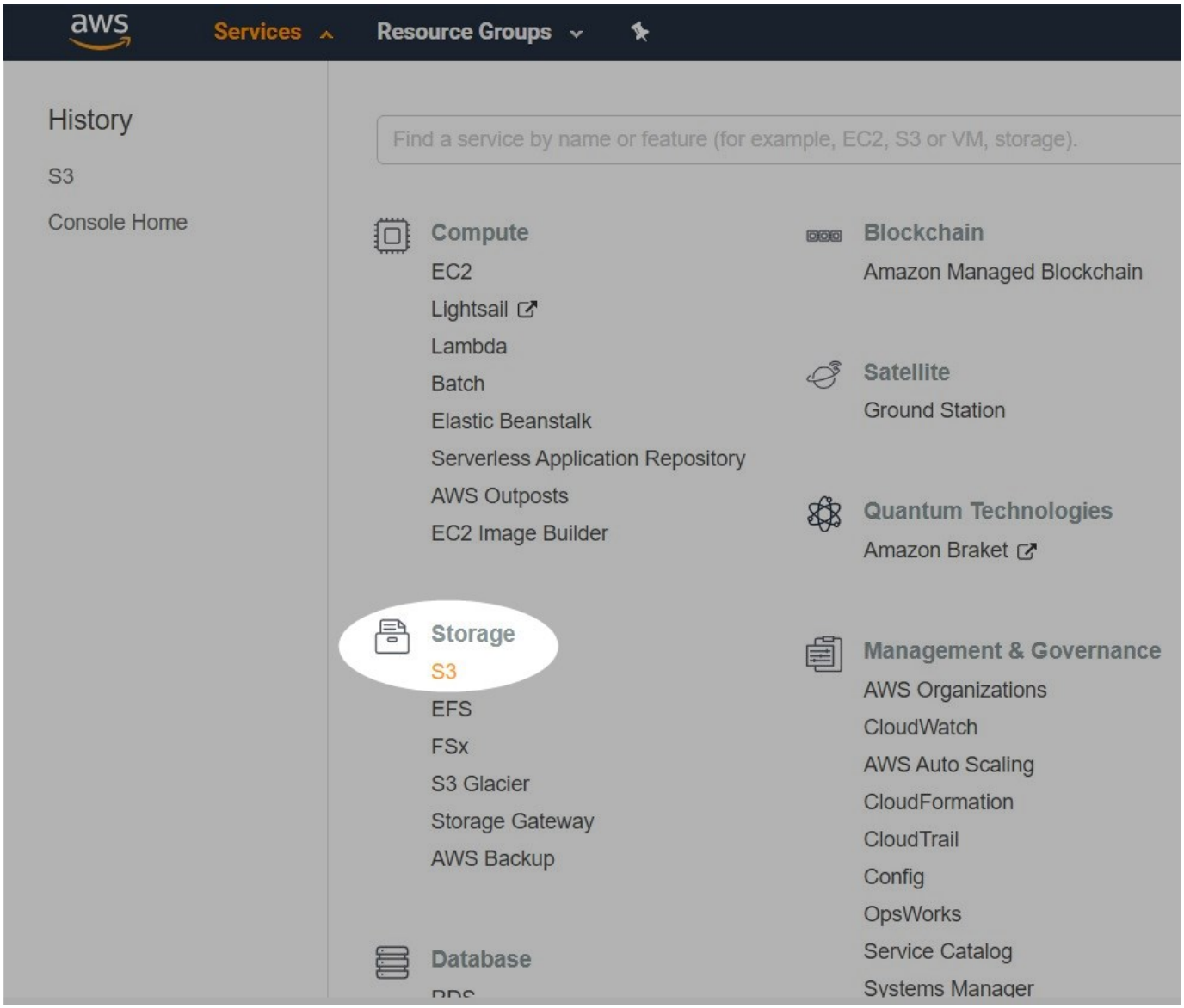
Costs

When storing backups in S3, additional charges will occur for stored backups. Retention setting in Data Protector for Cloud Workloads can limit the storage costs of stored backups. Currently, Data Protector for Cloud Workloads doesn't support Glacier (but it will appear in future releases).

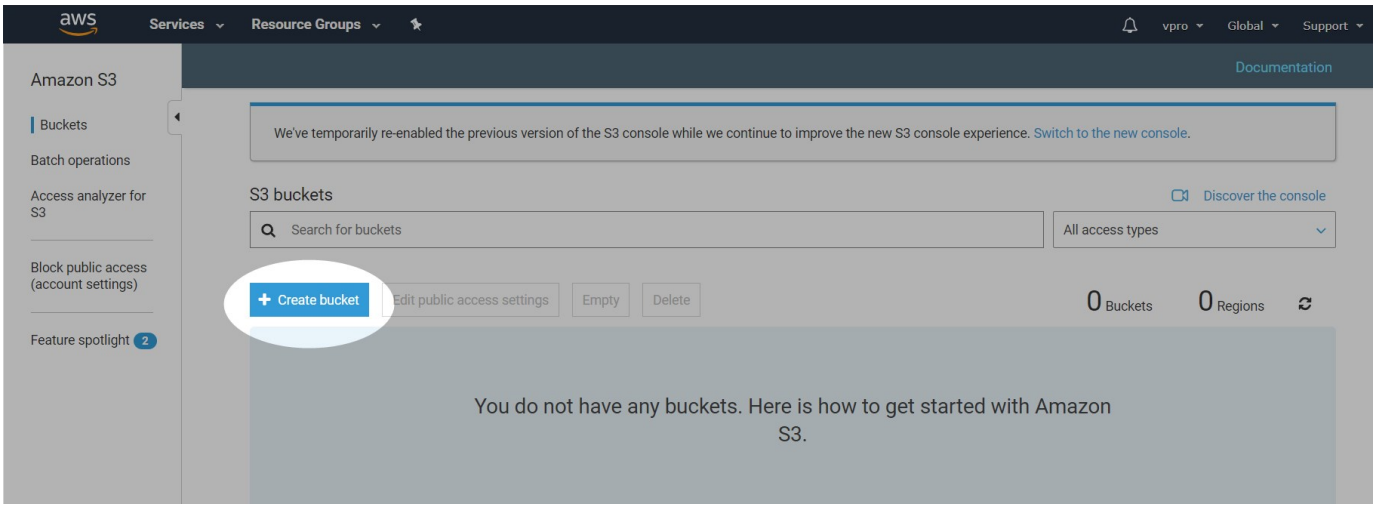
Please visit https://aws.amazon.com/s3/pricing/ to check current AWS S3 pricing.

Example

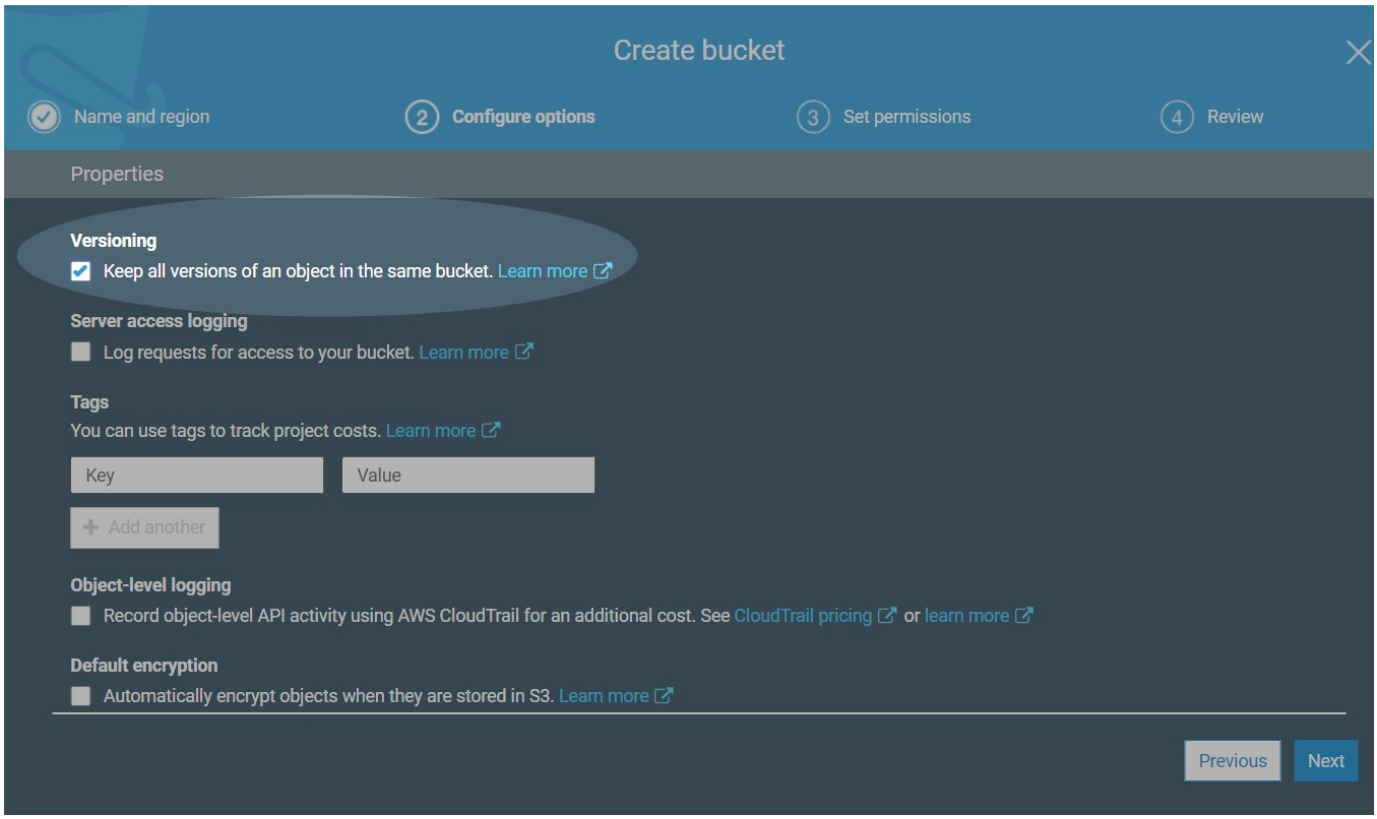
Now we will show you how to quickly create S3 storage and integrate it with Data Protector for Cloud Workloads as a backup destination.
After logging in, expand the services tab and choose S3 under the Storage section:



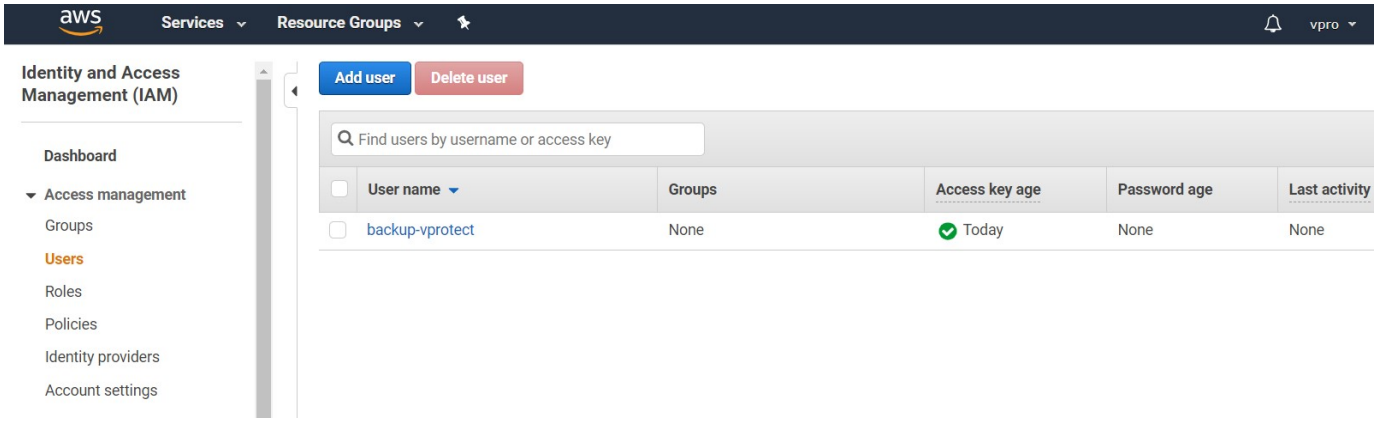
Now create a new bucket for your backups:



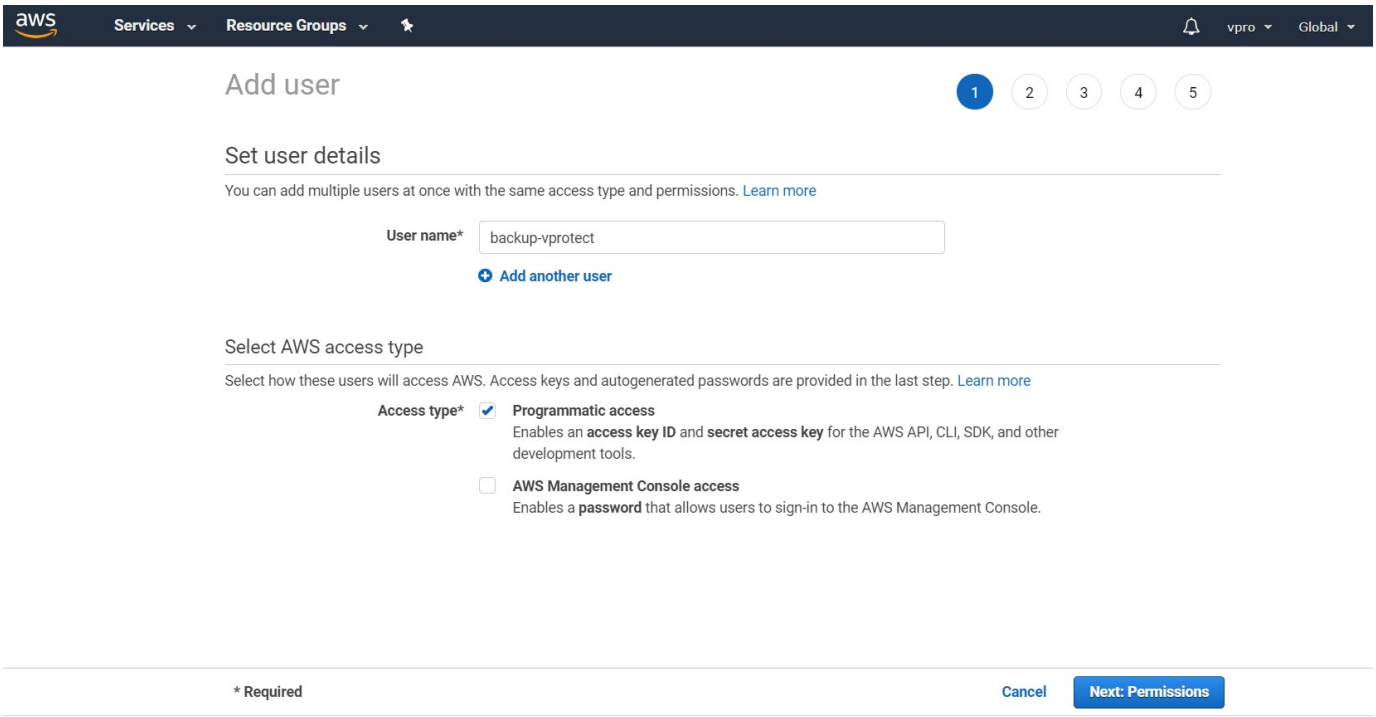
In "Configure options" activate versioning:
(In all other tabs, you can leave the default settings)



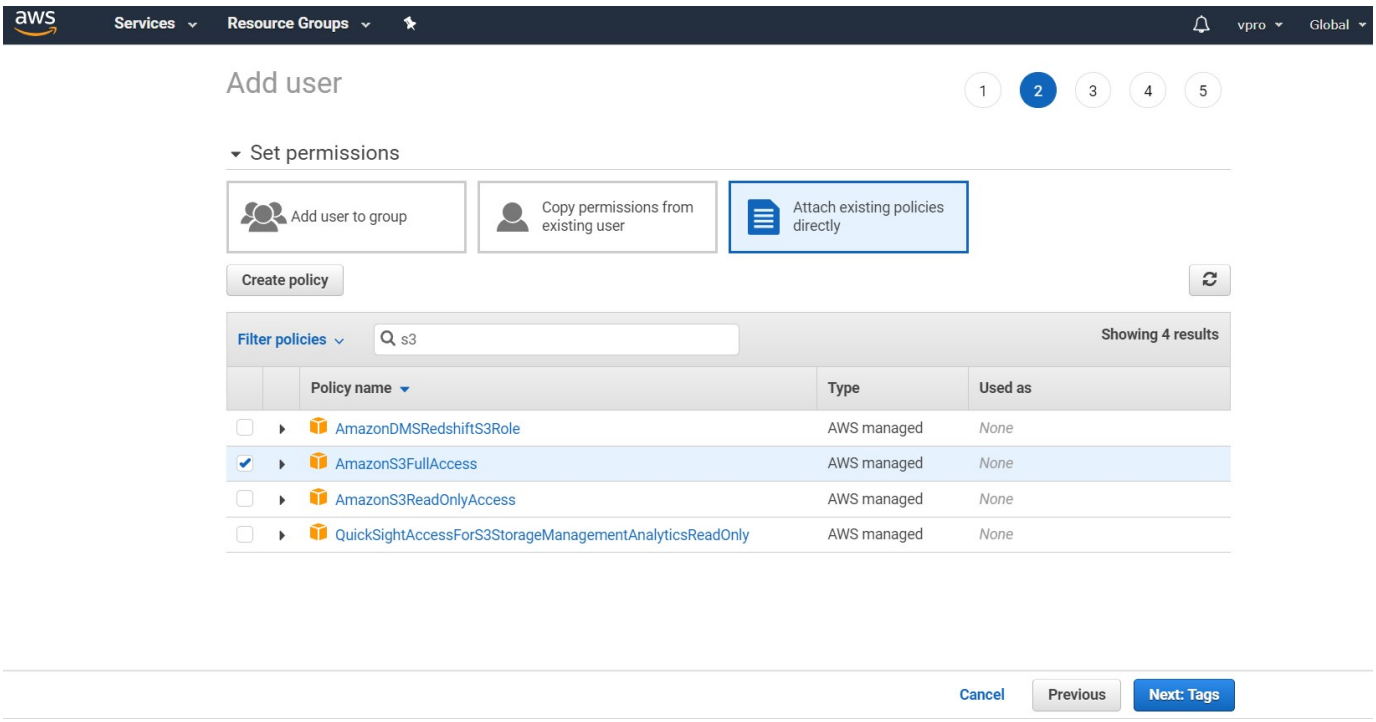
After creating a bucket, we need to create a new user with appropriate permissions:

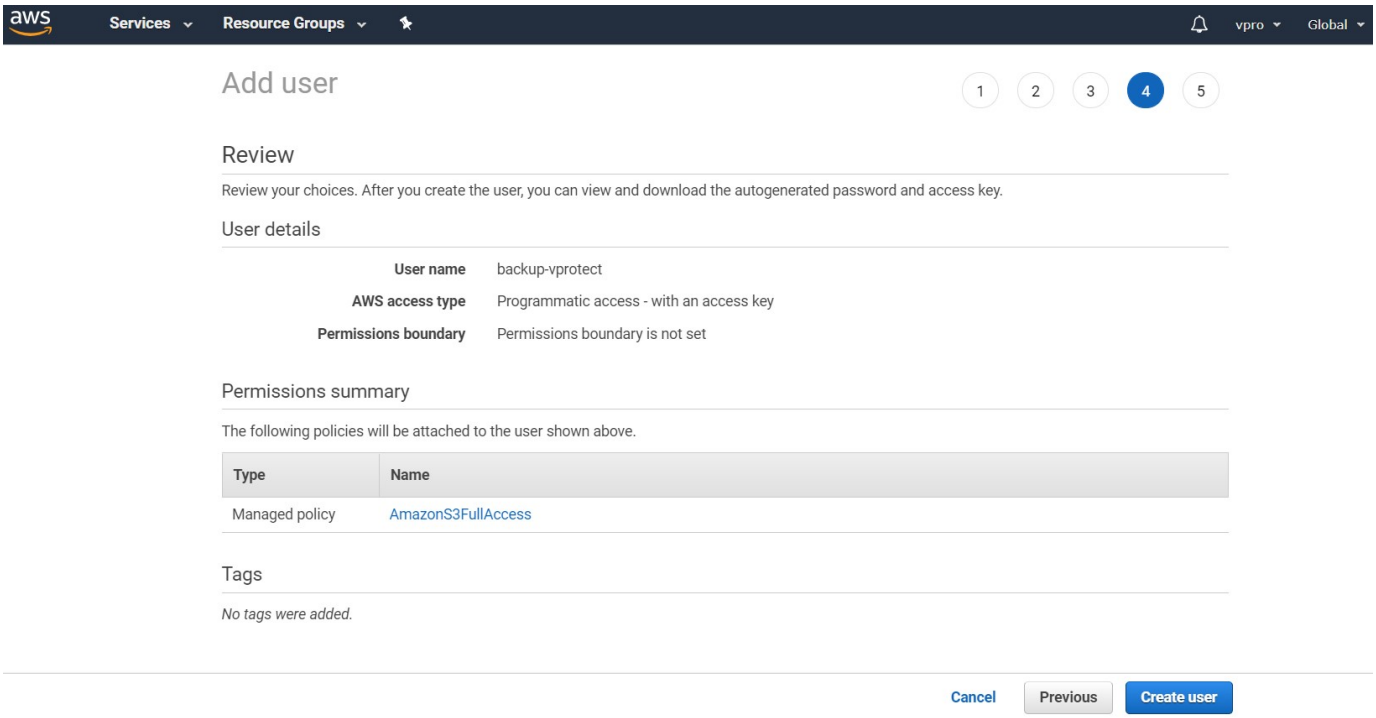


Remember to choose the "Programmatic access" account type:

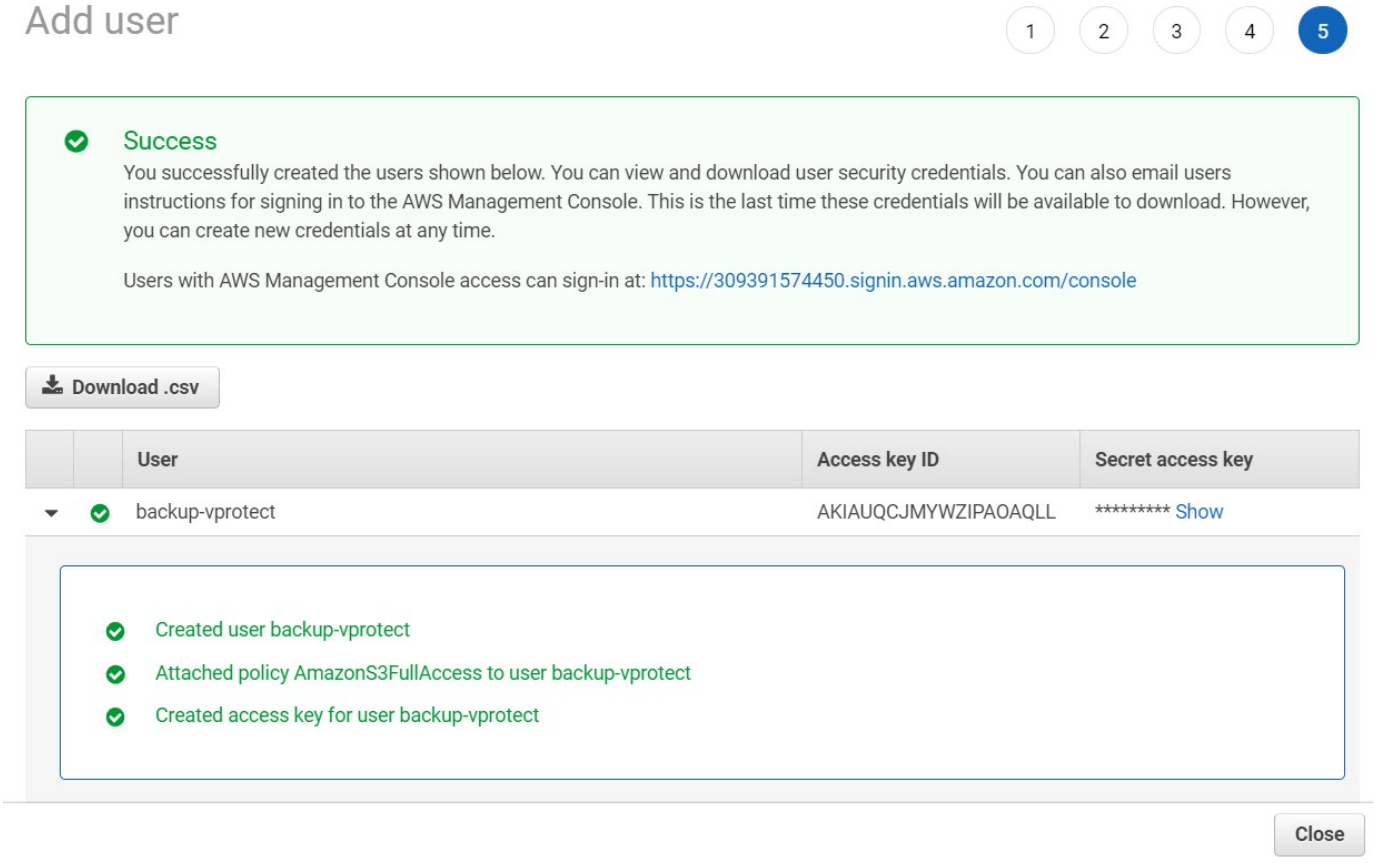


From the predefined roles, you can choose "AmazonS3FullAccess" or you can create a new one as described in the Permissions section:





Remember to download the .csv or copy the key credentials manually:



Now go to the Backup destination tab on the Data Protector for Cloud Workloads dashboard and change the sub-tab to object storage. Provide the bucket name and key credentials, and then configure the remaining options according to your requirements:

AMAZON S3 / S3-COMPATIBLE SETTINGS

API URL (optional)

Backup mode
Single bucket for all virtual environments

Bucket name *
backup

Region (optional)

Record backup time after store

Path style access enabled

Resolve hostname to IP before connecting

Parallel Download enabled

Access key *
••••••••••••••••••••

Show access key

Secret key *
••••••••••••••••••••••••••

Show secret key

Enable encryption

Proxy configuration enabled

PRE/POST ACCESS

Execute pre store command

Ceph Rados Gateway

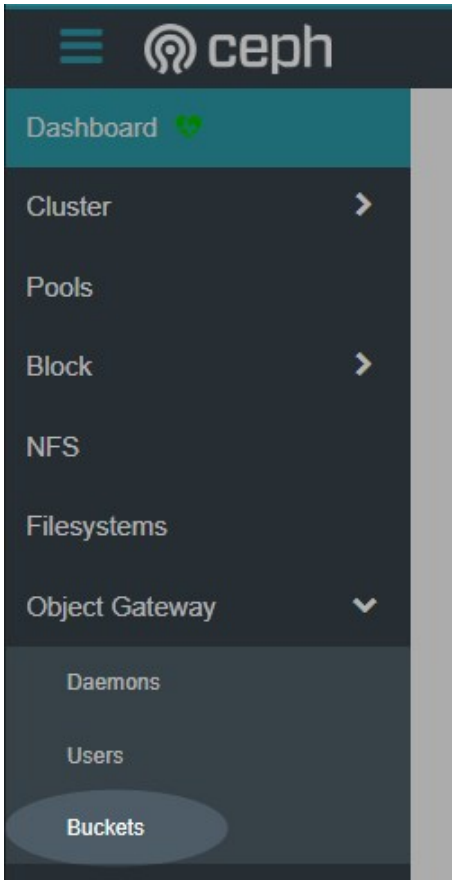
Overview

Ceph Object Gateway supports a RESTful API that is compatible with the basic data access model of the Amazon S3 API. Ceph Object Gateway is an object storage interface built on top of librados to provide applications with a RESTful gateway to Ceph Storage Clusters. Ceph Object Storage supports two interfaces:

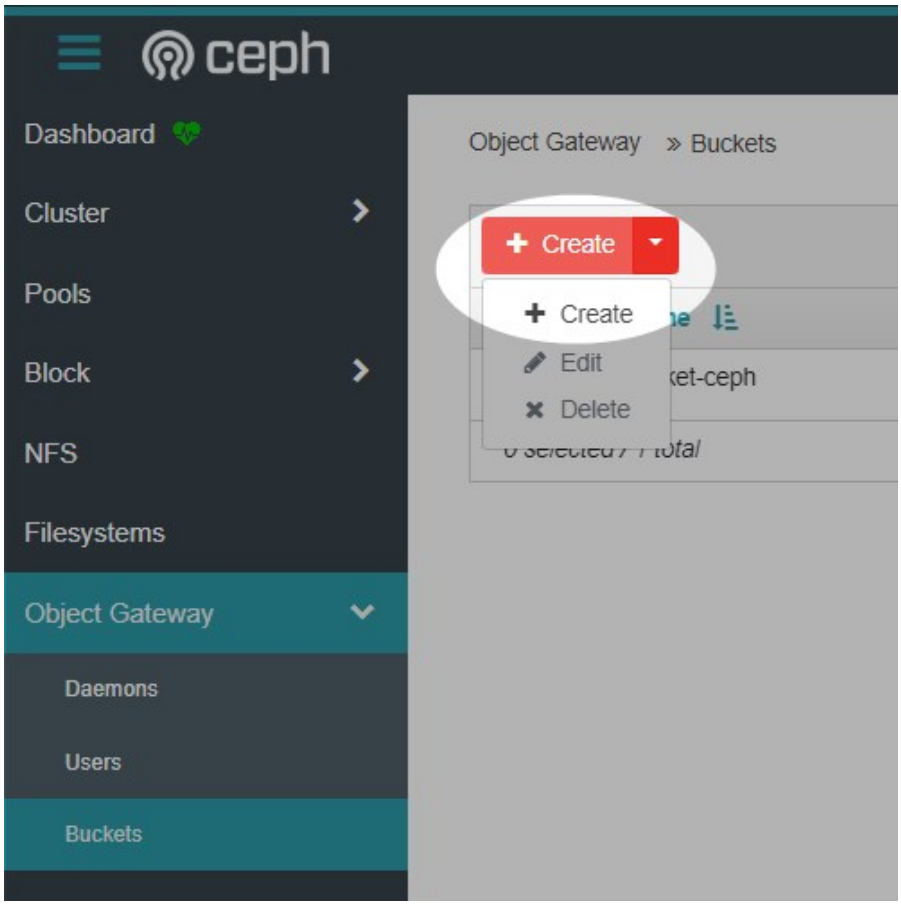
- **S3-compatible**: Provides object storage functionality with an interface that is compatible with a large subset of the Amazon S3 RESTful API.
- **Swift-compatible**: Provides object storage functionality with an interface that is compatible with a large subset of the OpenStack Swift API.

Example

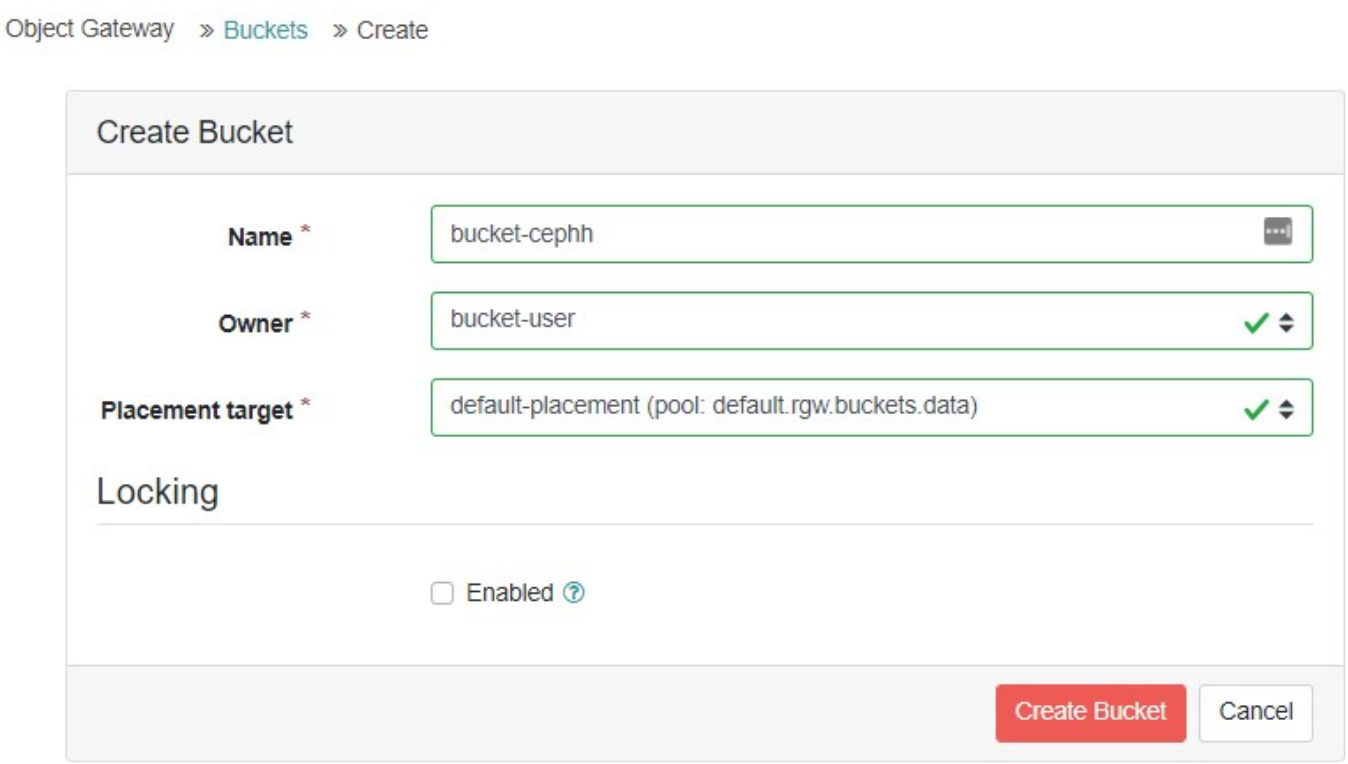
Log in to the ceph dashboard. Open Object gateway and then go to "Buckets".



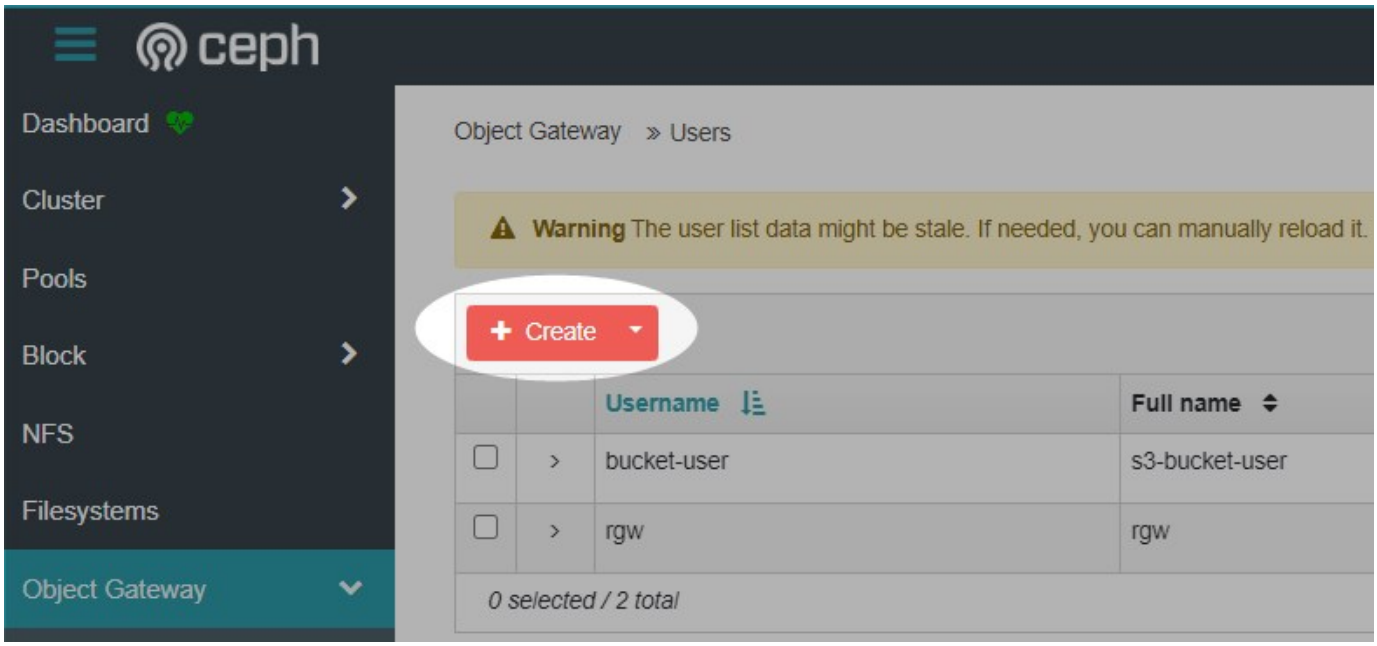
Then click on the "Create" button.



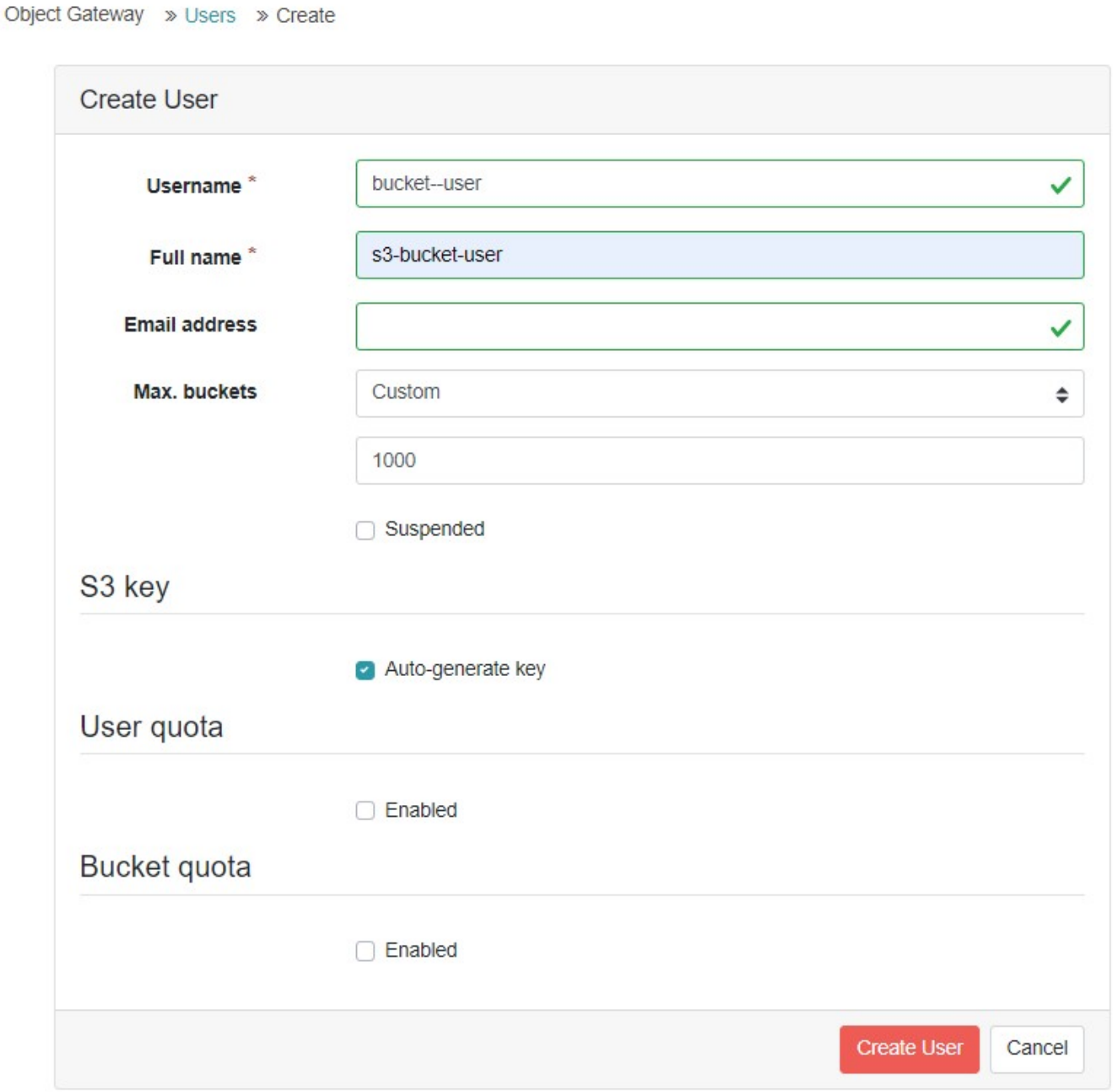
Fill in the required fields.



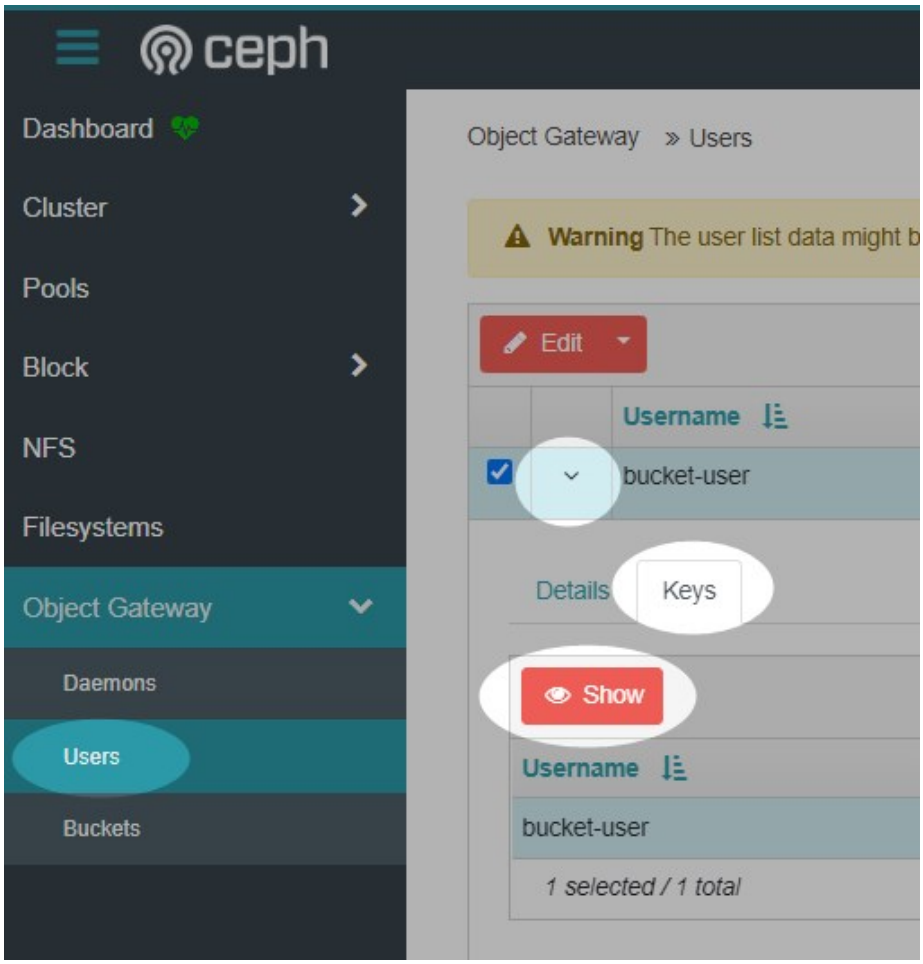
Now create a dedicated access account for the backup destination. Open the Users tab under the object gateway menu.



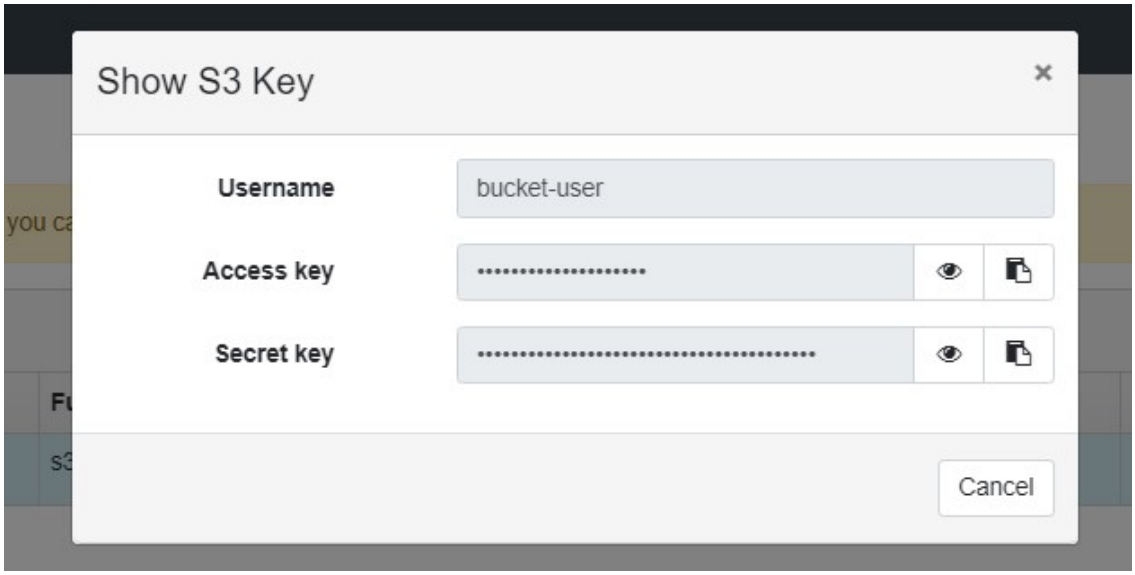
Fill in the username field, you can leave the other settings as default.



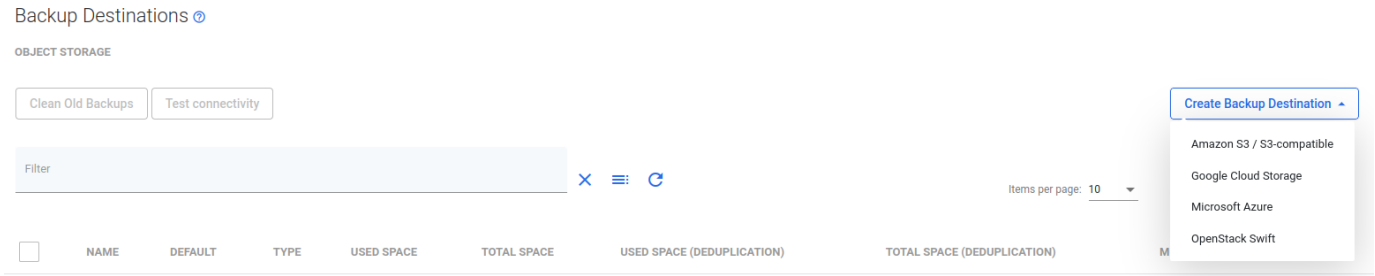
To see the account key and secret key, expand the user details and open the keys tab, click on the key, and then on the show button.



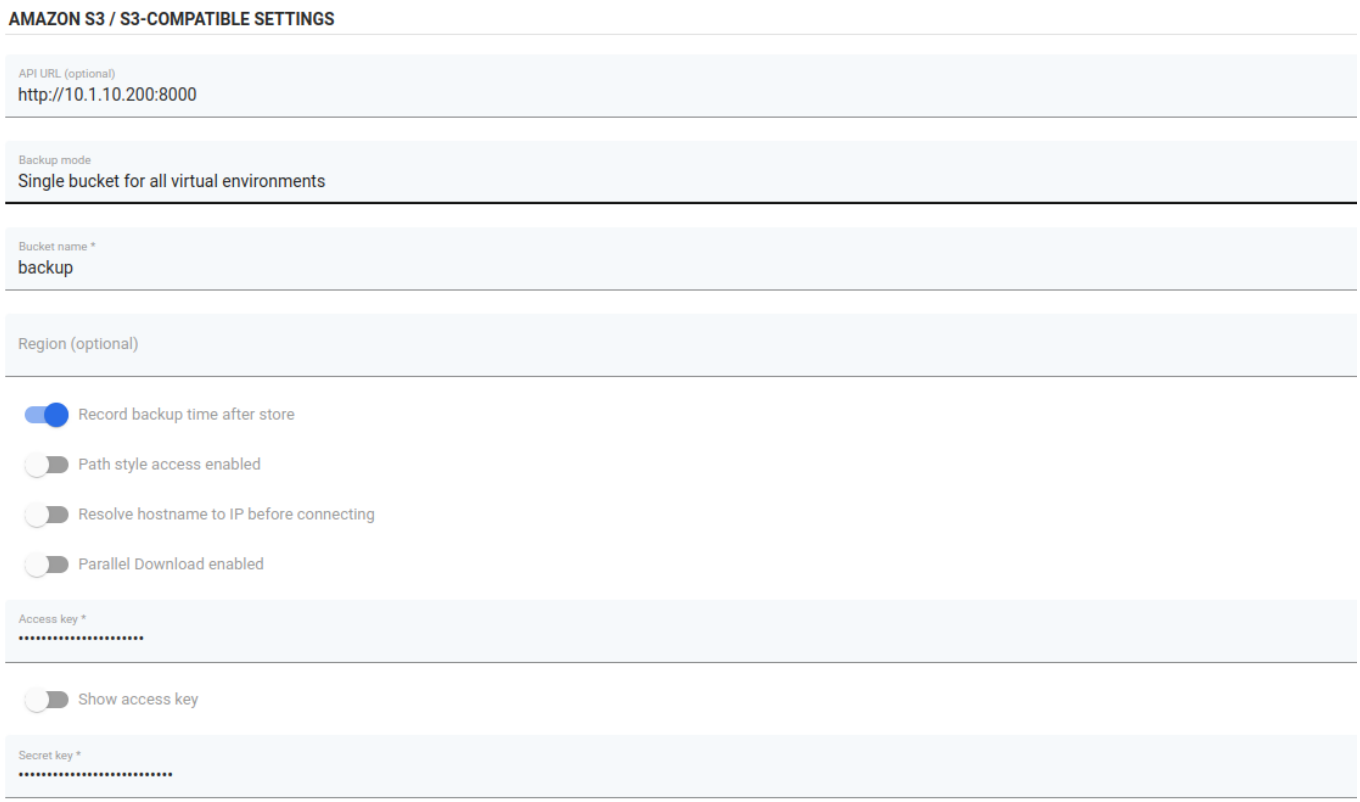
The access key and secret key will be needed to create a backup destination in Data Protector for Cloud Workloads.



Now we can go to the Data Protector for Cloud Workloads Dashboard. Open the "Backup Destination" tab from the left side menu and choose "Amazon S3 / S3-compatible" as the new type of backup destination.



By default, Ceph provides S3 via port 8000. Also, remember to enable the "record backup time after store" option.



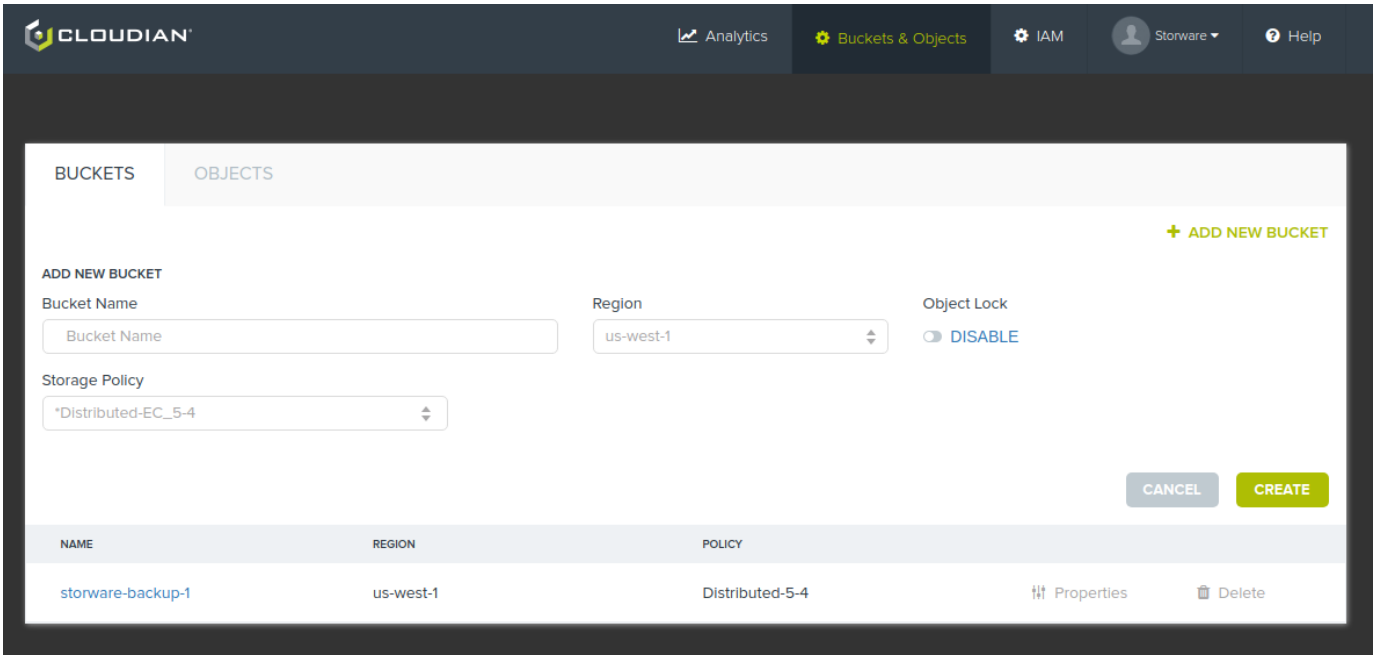
Cloudian S3

Overview

Cloudian is an S3-compatible backup provider. Configuration as the backup destination is similar to AWS S3.

Example

After logging in, create a new bucket for your backups



Next, go to security credentials and generate a new access key.

Now go to the Backup destination tab on the Data Protector for Cloud Workloads dashboard and change the sub-tab to object storage. Provide the bucket name and key credentials, and then configure the remaining options according to your requirements. Also, enable `Path style access enabled` option:

AMAZON S3 / S3-COMPATIBLE SETTINGS

API URL (optional)

Backup mode
Single bucket for all virtual environments

Bucket name *
backup

Region (optional)

Record backup time after store

Path style access enabled

Resolve hostname to IP before connecting

Parallel Download enabled

Access key *
••••••••••••

Show access key

Secret key *
••••••••••••••••••••

Show secret key

Enable encryption

Proxy configuration enabled

PRE/POST ACCESS

Execute pre store command

Execute post store command

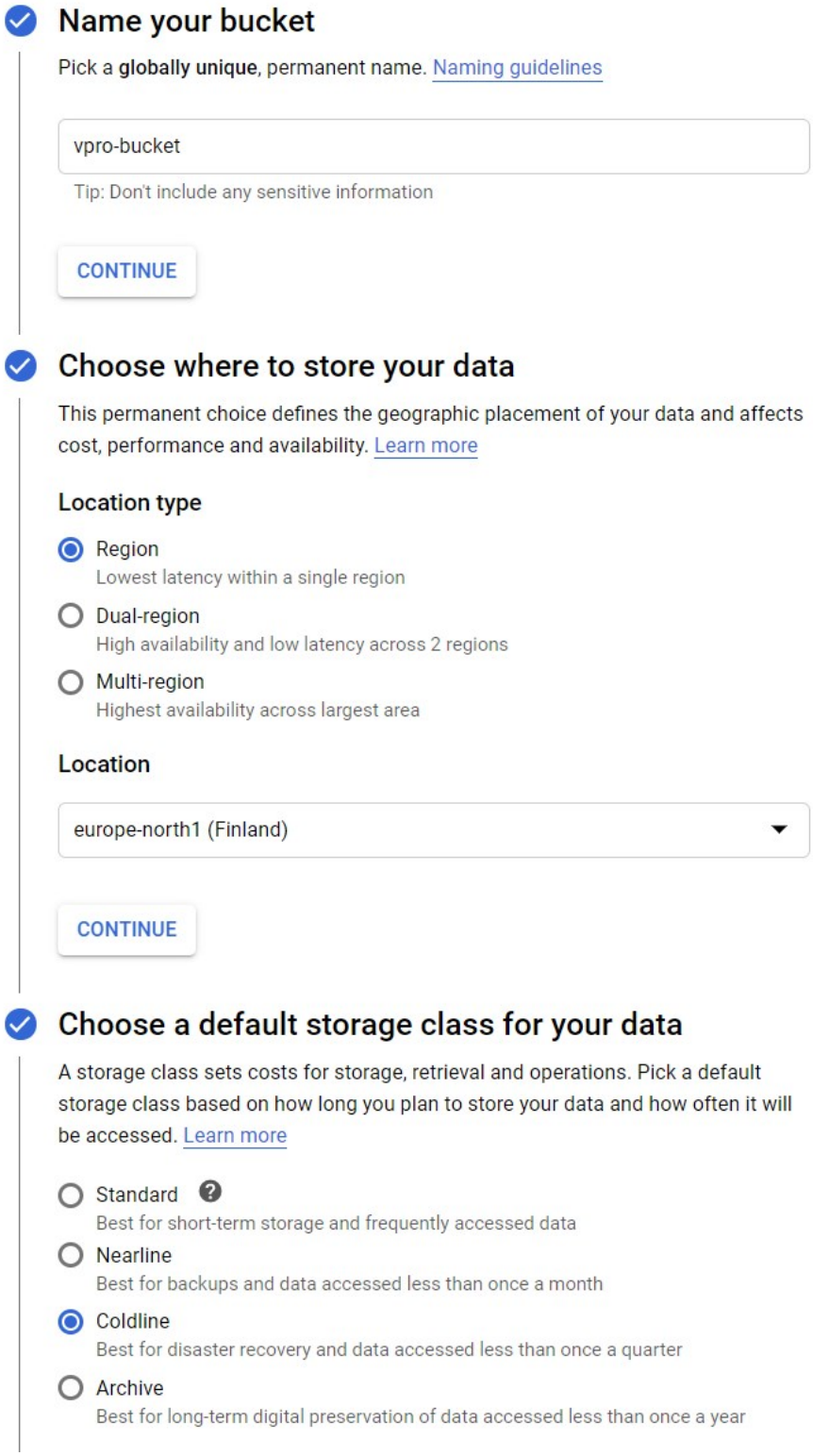
Cancel

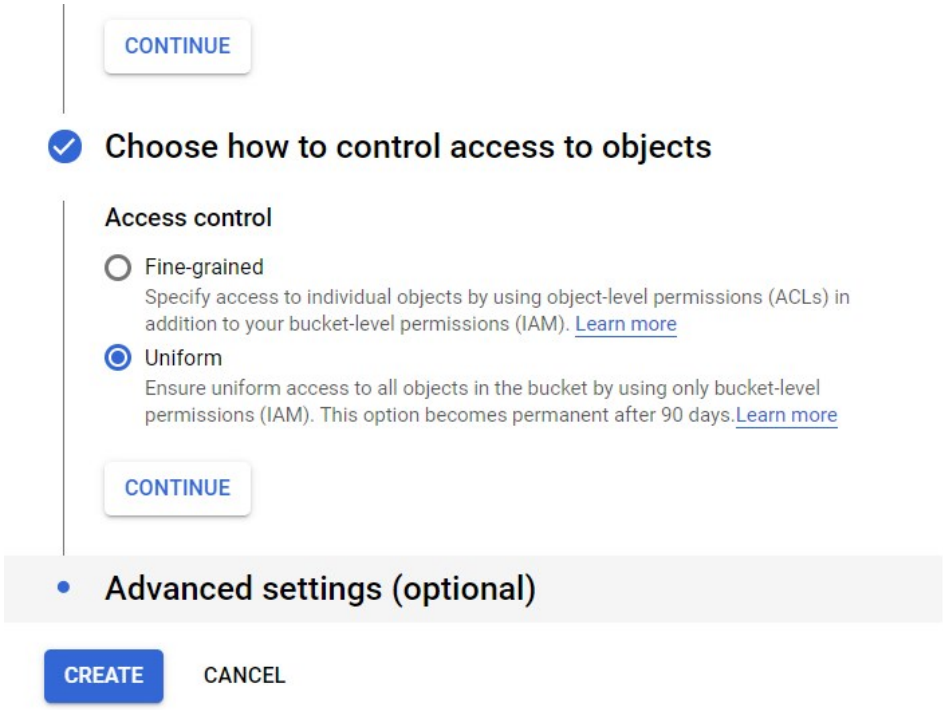
Google Cloud Storage

Google Cloud Storage allows data to be stored and accessed on Google Cloud Platform infrastructure. It combines the performance and scalability of Google's cloud with advanced security and sharing capabilities.

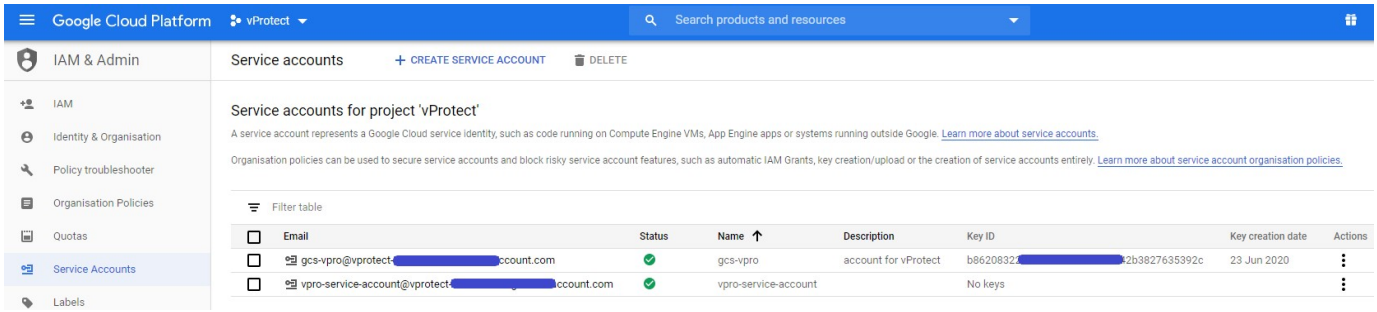
How to use **GCS** as a backup destination for Data Protector for Cloud Workloads:

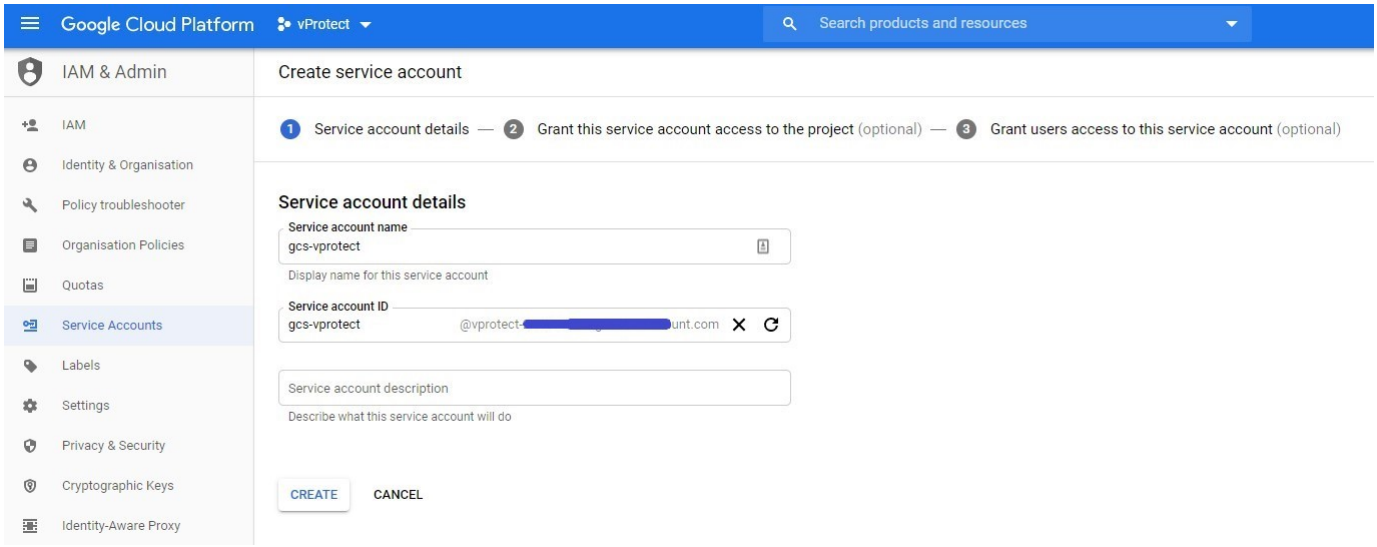
1. Create a project: Click here for more info about **Creating and Managing Projects**.
2. Create a bucket: Click here for more info about **Creating Storage Buckets**.

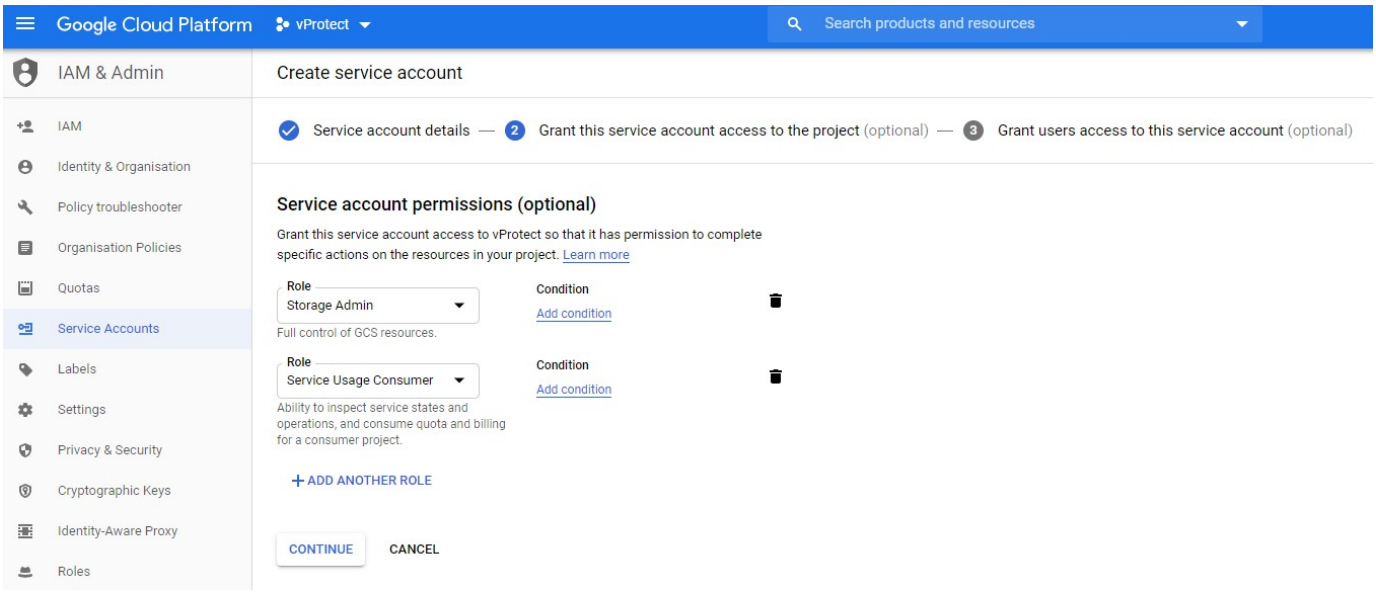




1. Enable versioning in your bucket: Click here for more info about **Enabling Object Versioning**. `gsutil versioning set on gs://[BUCKET_NAME]`
2. Generate a service account key: Click here for more info about **Creating service account keys**. The service account key should have the **Role** set to **Storage Admin and Service Usage Consumer**.

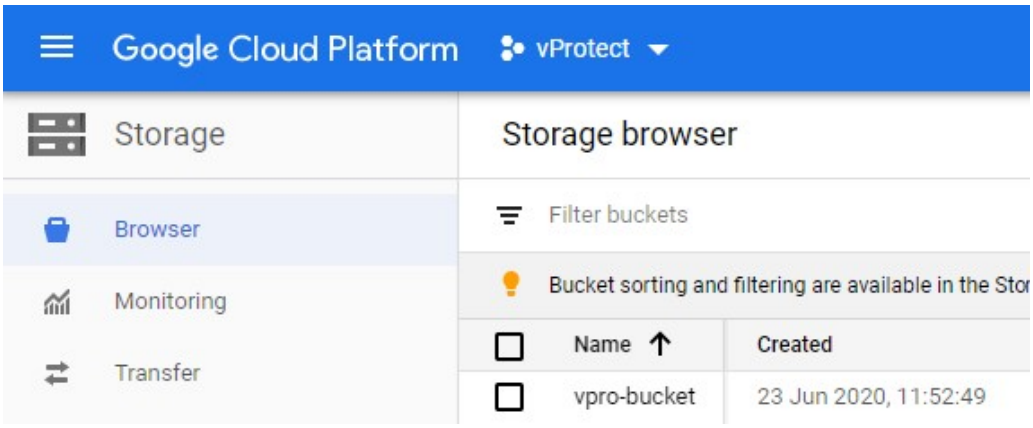


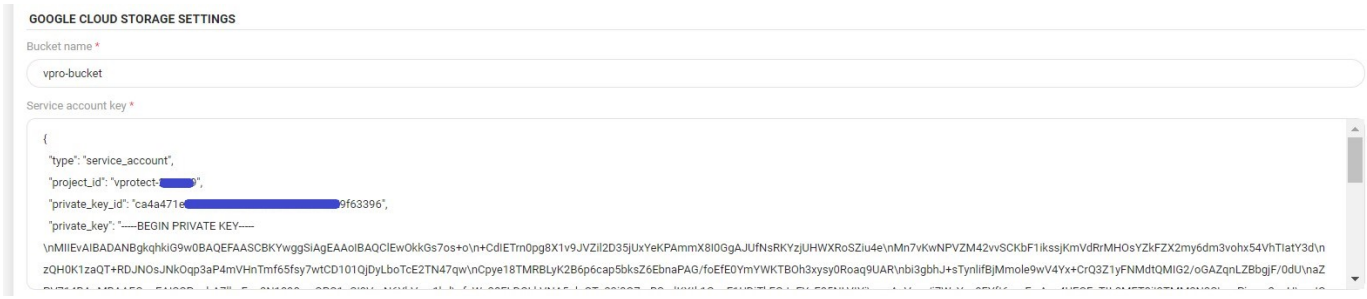




You can leave the third tab - Grant users access to this service account (optional).
To generate an account key, click on the "three-dot" button next to your service account and then click on "create key". You should then see the window below - click on create to download the JSON file. You'll need its content in the last step.

1. After the key is created, open your Data Protector for Cloud Workloads Web UI (you can also use **CLI**), click on **BACKUP DESTINATIONS**, then on the **Create Backup Destination** button, and then select **Google Cloud Storage** from the drop-down list. In addition to the standard properties, you need to specify:
2. The **Bucket name** was specified during bucket creation.
3. The **Service account key** - paste the content of the service account key .json file created before.





Now you can store Data Protector for Cloud Workloads backups on Google Cloud Storage.

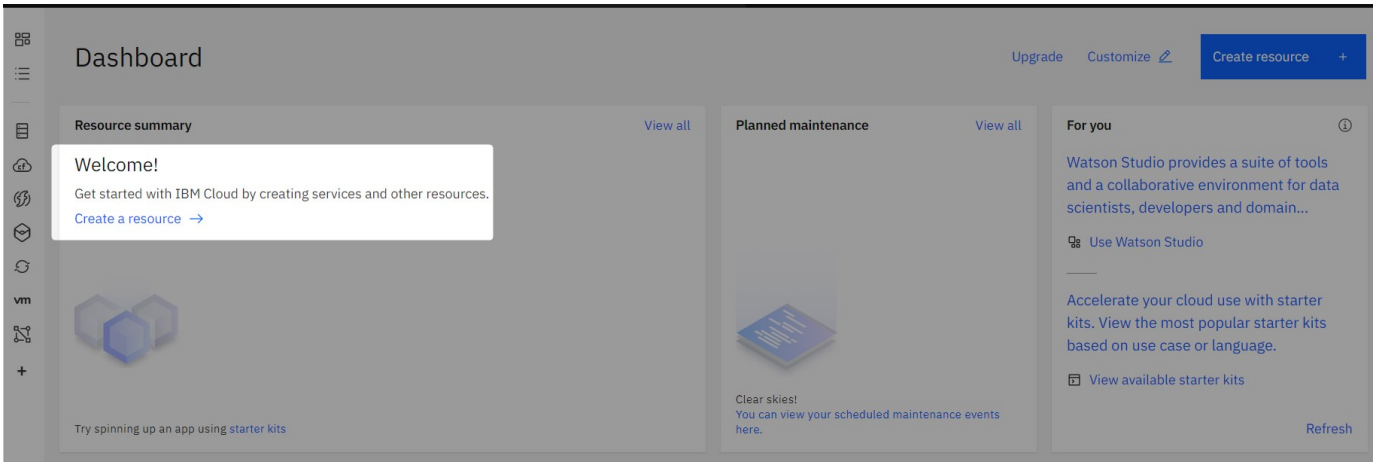
IBM Cloud Object Storage

Overview

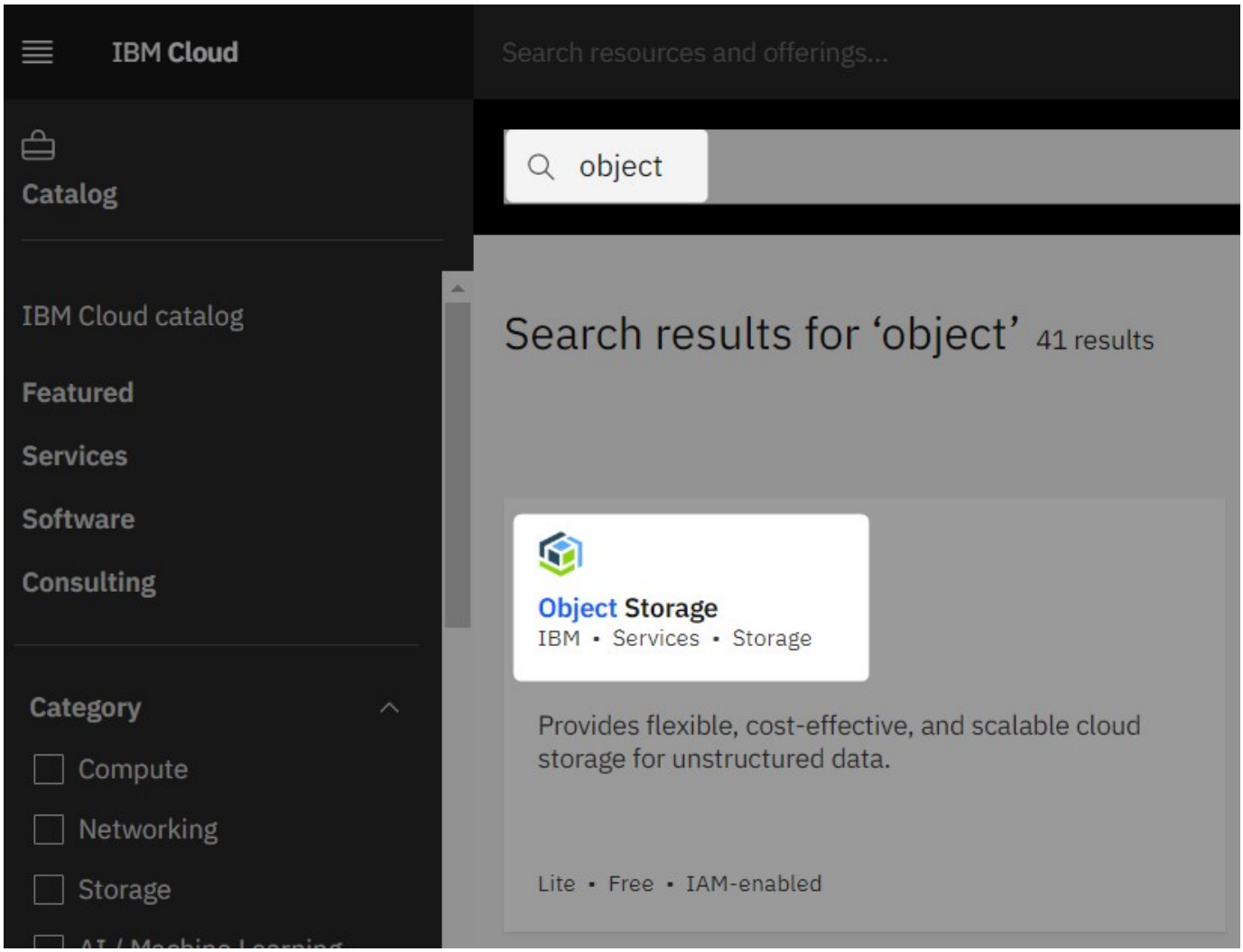
IBM Cloud Object Storage is a push-button deployed cloud storage service and is available in IBM Cloud global data centers. It offers leading data protection, high durability, and fast access to your data. You can use it to store and protect data with easy-to-use management features to organize your data and to configure finely-tuned access controls.

Example

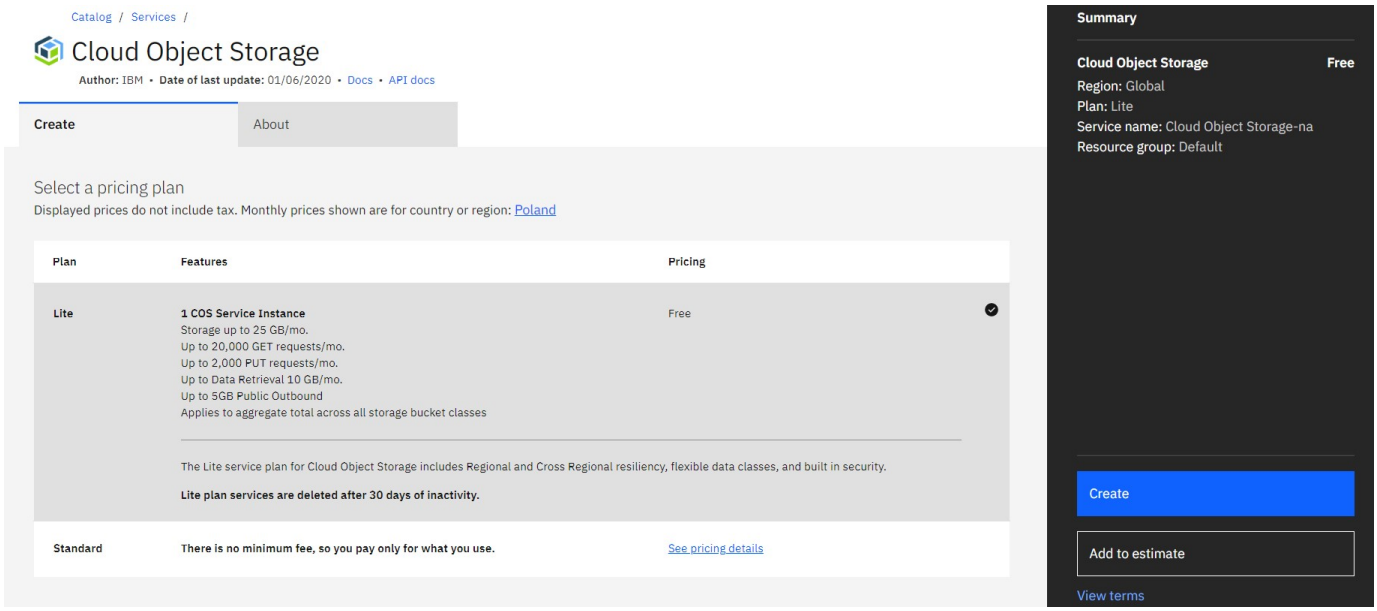
Log in to your IBM Cloud account. On the main dashboard, you will see the "Create a resource" button - Click on it.



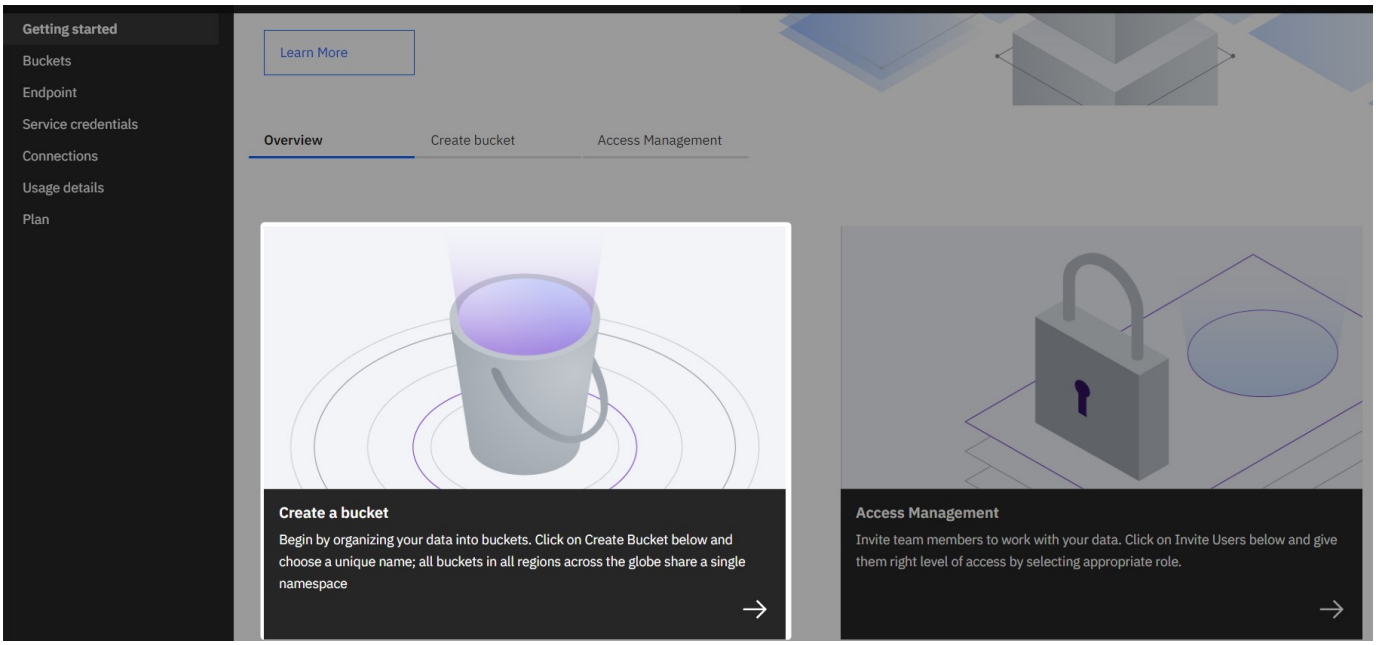
On the next screen, search for a resource named "Object Storage" and click on it.



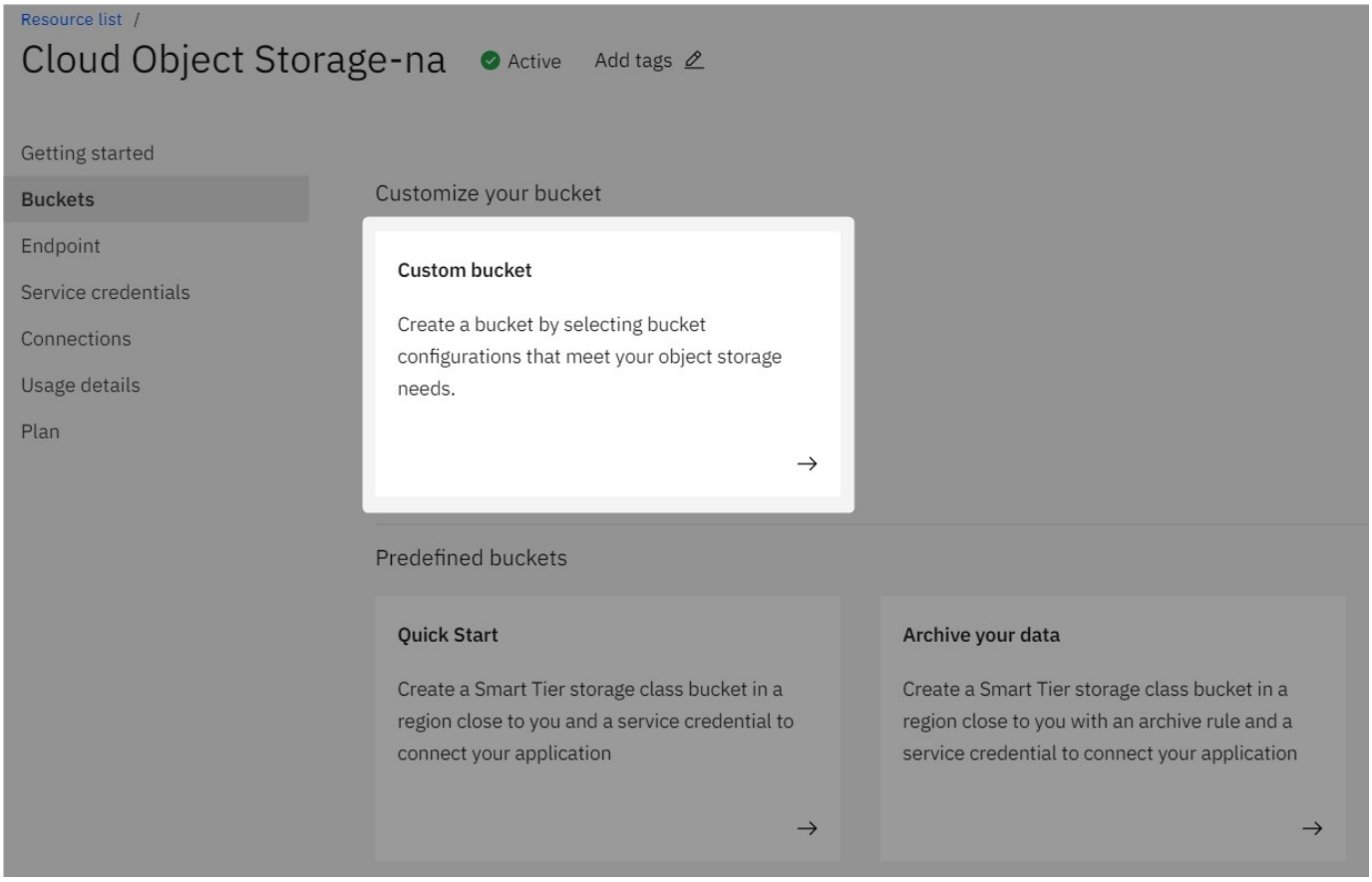
On the next screen, you can choose piercing plans, etc. Please select the options according to your requirements.



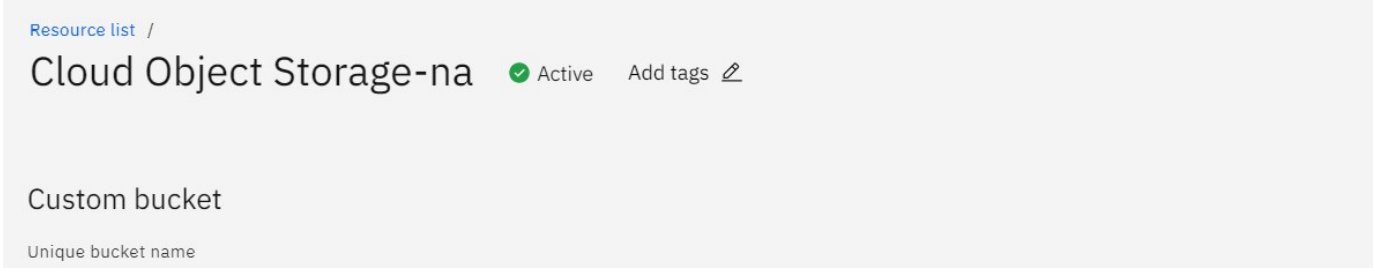
After creating a storage resource we need to create a bucket.



You can choose predefined templates or select the option to create a bucket with your own settings. In this example, we will choose "Custom bucket".



Data Protector for Cloud Workloads has no special requirements for the bucket, all options can be configured according to customer needs.



vprotect-bucket

Bucket naming rules:
- Must be unique across the **whole** IBM Cloud Object Storage system
- Do not use any personal information (any part of a name, address, financial or security accounts or SSN)

Resource list /

Cloud Object Storage-na

Active Add tags

Cross Region
Highest availability

Regional
Best performance

Single Site
Data sovereignty

Location

eu-de

Storage class View pricing

Smart Tier New!

Smart Tier automatically gives you the lowest storage rate based on your monthly activity.

Standard

For active workloads that require higher performance and low latency and where data needs to be accessed frequently.

Vault

For less active workloads that require infrequent data access (accessed once a month or less).

Cold Vault

For cold workloads where data is primarily archived (accessed a few times a year).

Advanced configurations

View services availability >

Optional

Rules & Policies

Archive Add rule

Create a rule to transition objects from their default storage class to Archive

Expiration Add rule

Creates rule to schedule deletion of objects after a specified amount of time after creation

Retention policy Add rule

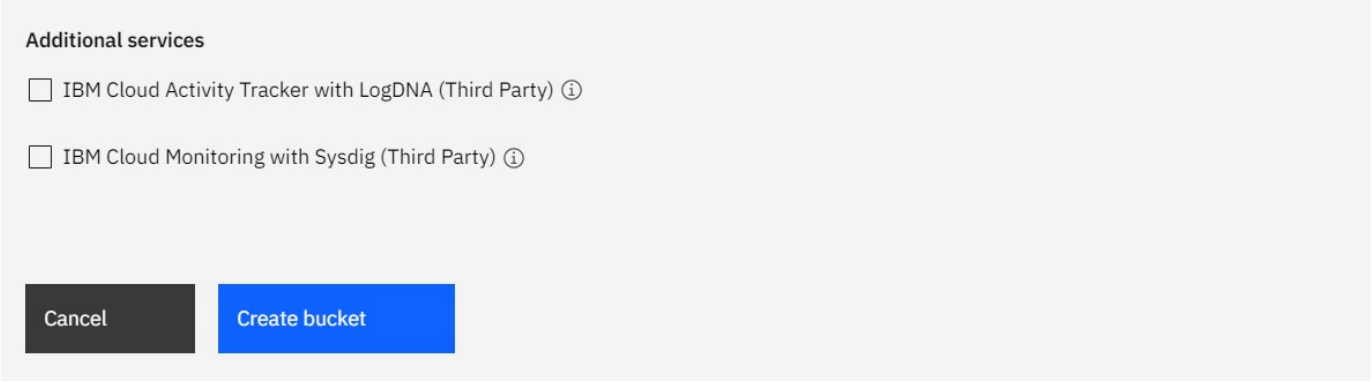
This feature is available for our Standard plan customers only. See pricing

Key management services

Key management services can only be added during bucket creation. If a key is deleted, all bucket data will become inaccessible.

☐ Key Protect

☐ Hyper Protect Crypto Services



After creating the bucket, you'll see the objects page. From the menu on the left select the configuration tab. You will see a summary of the resource you have created. To create a backup destination you will need the ***"public" address from the endpoints section*** from here.

Bucket configuration

Bucket details

Bucket name	vprotect-bucket	**Total bytes**	0 bytes
Service instance	cloud-object-storage	**Resiliency**	Regional
Total objects	0	**Location**	eu-de
Storage class	Smart Tier ⓘ	**Date created**	02/07/2020 10:38:57
Cloud Functions trigger	Disabled Learn more		

Bucket instance CRN

This value identifies the service instance when listing or creating buckets via the API. Learn more

```
crn:v1:bluemix:public:cloud-object-storage:global:[redacted]-fab3-40b1-98cb-682618778565:bucket:vprotect-bucket
```

Endpoints

Endpoints are used hand in hand with your credentials (i.e. keys, CRN, bucket name) to tell your service where to look for this bucket. Depending on where your service or applications is located you will want to use one of the below endpoint types.

Private ⓘ

Use private endpoints to point applications or services that are hosted in the IBM cloud (excluding Cloud Foundry services).

```
s3.private.eu-de.cloud-object-storage.appdomain.cloud
```

Public ⓘ

Use public endpoints to point applications or services that are hosted outside of the IBM cloud or for Cloud Foundry applications hosted in the IBM cloud.

```
s3.eu-de.cloud-object-storage.appdomain.cloud
```

Direct ⓘ

Use direct endpoints to connect from a VPC to Cloud Object Storage.

```
s3.direct.eu-de.cloud-object-storage.appdomain.cloud
```

Associated key management services

This bucket is not encrypted with key management key. Learn more

Activity Tracker

Add Activity Tracker

No Activity Tracker service instance is currently associated with this bucket.

Monitoring

Add Monitoring

No IBM Cloud Monitoring with Sysdig service instance is currently associated with this bucket.

Archive rule

Create

Archive lifecycle rules allow users to change their objects from their default bucket storage class to the archive storage class after a certain period. Archive is our lowest cost tier and is best for items that are not accessed often.

Expiration rule

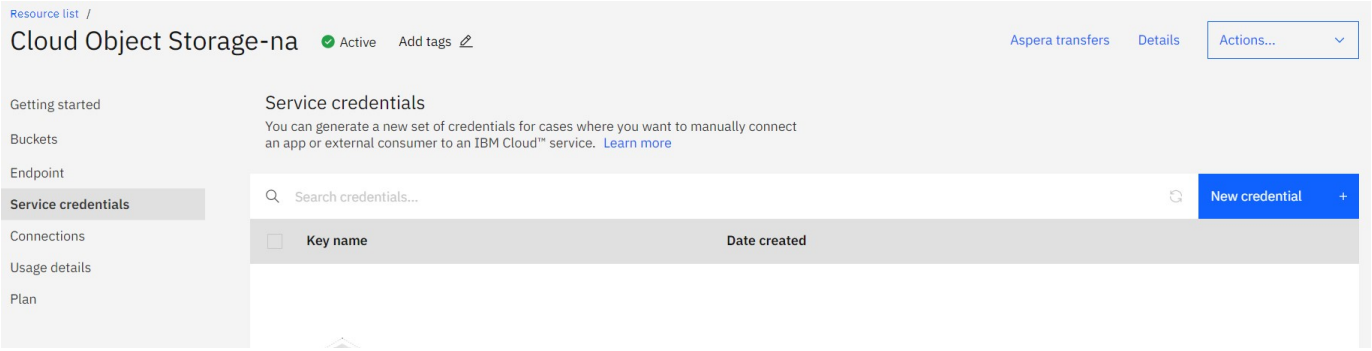
Add

Object Expiration rules allow you to manage storage costs by scheduling deletion of objects that are no longer needed after a specified amount of time. Learn more

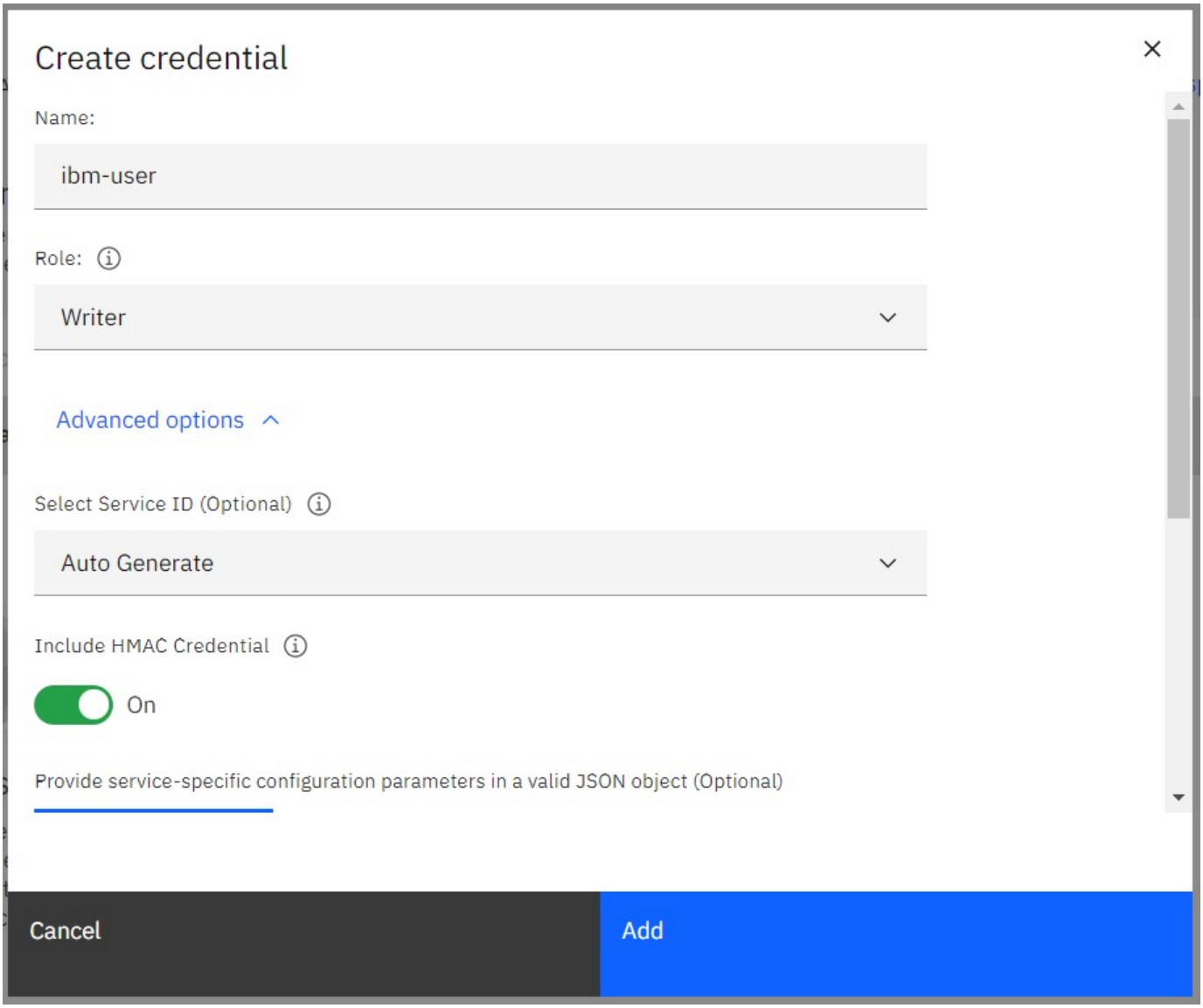
Add rule +

Rule name ⓘ ↑↓	Prefix filter(optional) ⓘ ↑↓	Expiration days/date ⓘ ↑↓	State ↑↓

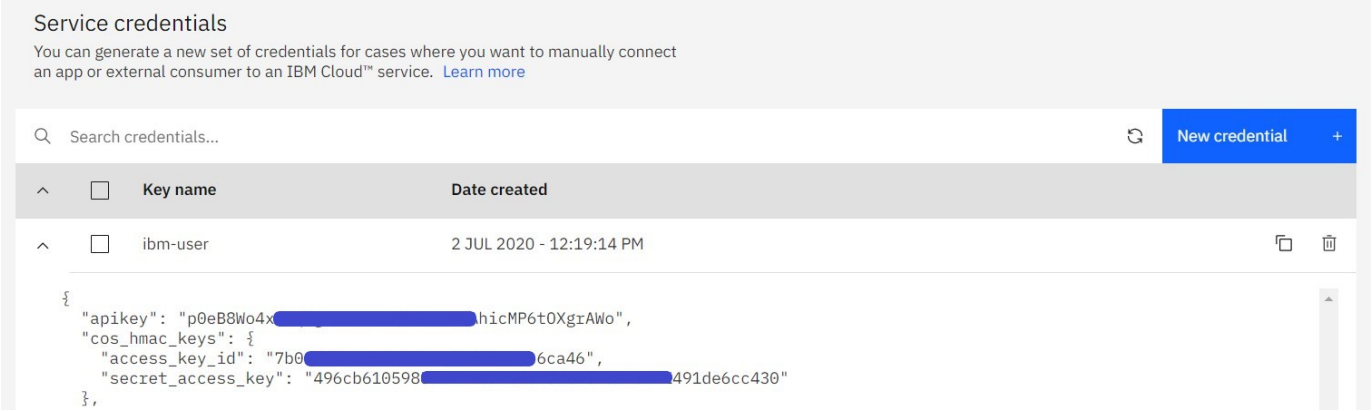
We are almost done here, now we need to create API access and a secret key. Go to "Service credentials" on the left side menu then create new credentials using the blue button on the right.



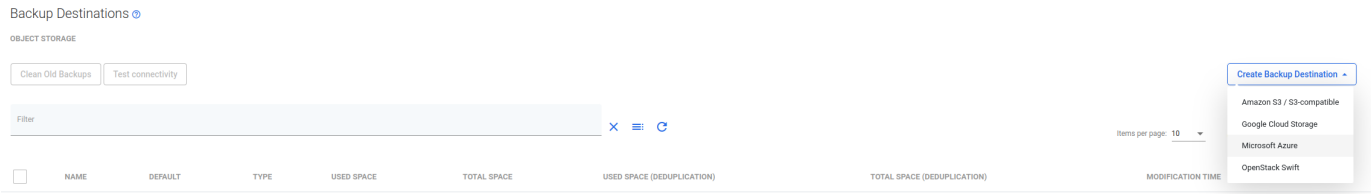
There are two important options on this screen. You must select the appropriate role (for Data Protector for Cloud Workloads it is the "Writer" role) and select the option "Include HMAC credential".



Now expand the detailed information about the created credentials by clicking on the arrow next to the name. What we need is "access_key_id" and "secret_access_key".



Now we can log in to the Data Protector for Cloud Workloads Dashboard and create a backup destination. Please go to the backup destination tab on the left side menu and then choose "Amazon S3 / S3-compatible".



As IBM cloud storage is compatible with Amazon-S3, many settings will be very similar. However, remember to enter the API URL (remember about "https://" at the beginning), select the "Record backup time after store" option, and enter the region.

AMAZON S3 / S3-COMPATIBLE SETTINGS

API URL (optional)
https://s3.eu-de.cloud-object.appdomain.cloud

Backup mode
Single bucket for all virtual environments

Bucket name *
backup

Region (optional)
eu-de

Record backup time after store

Path style access enabled

Resolve hostname to IP before connecting

Parallel Download enabled

Access key *
••••••••••••••

Show access key

Secret key *
••••••••••••••••••••••••••••••

Show secret key

Enable encryption

Proxy configuration enabled

PRE/POST ACCESS

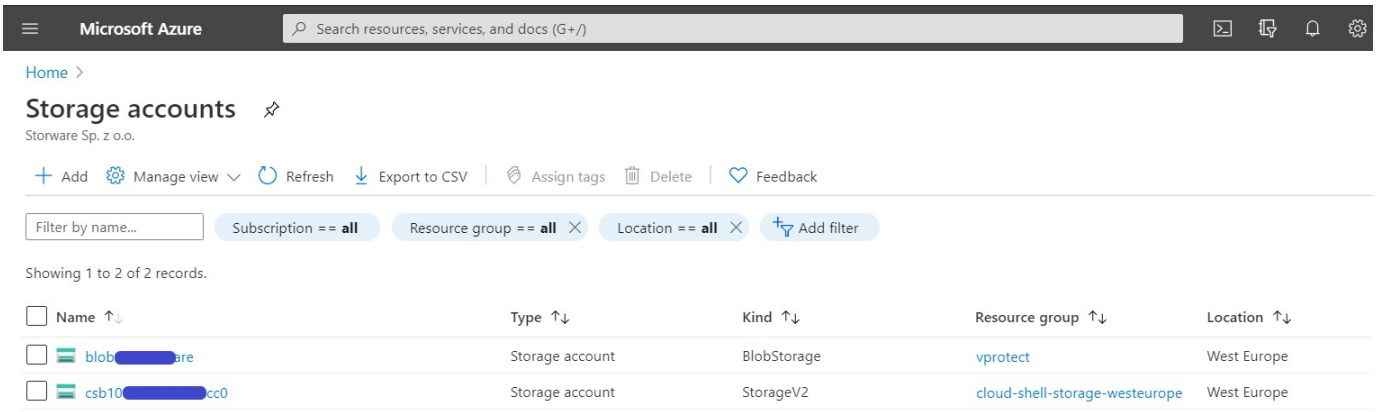
Execute pre store command

Execute post store command

Cancel

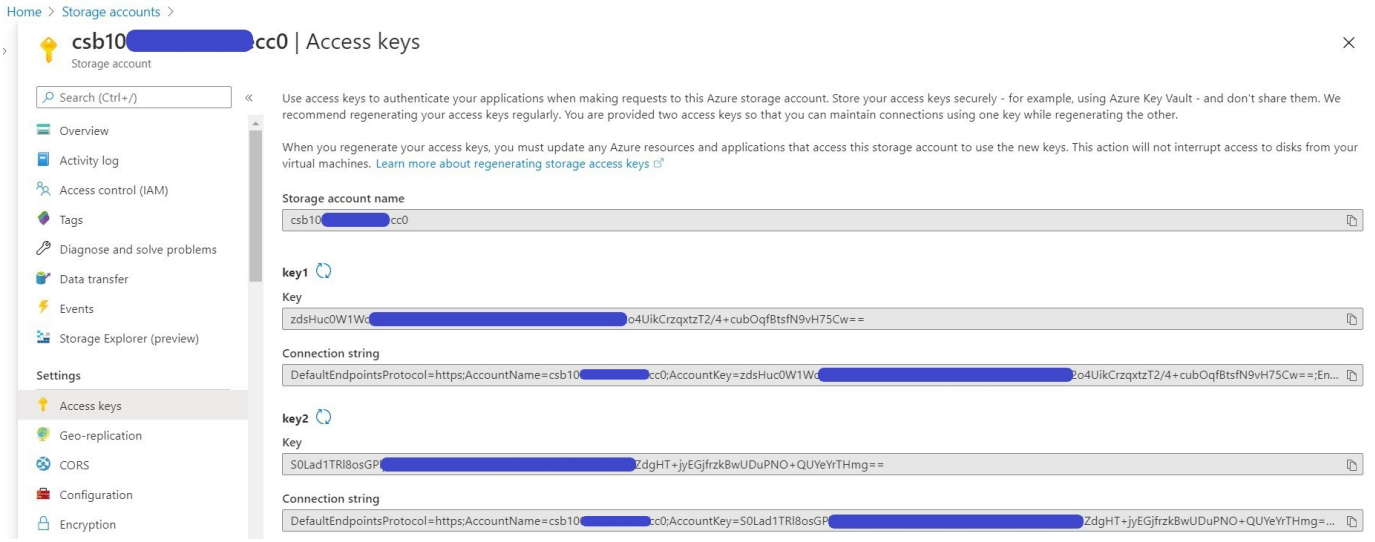
Microsoft Azure Blob Storage

Data Protector for Cloud Workloads supports integration with MS Azure Blob Storage. An Azure storage account contains all of your Azure Storage data objects: blobs, files, queues, tables, and disks. The storage account provides a unique namespace for your Azure Storage data that is accessible from anywhere in the world over HTTP or HTTPS. If you don't already know Azure Blob storage, please read this great documentation https://docs.microsoft.com/en-gb/azure/storage/blobs/.

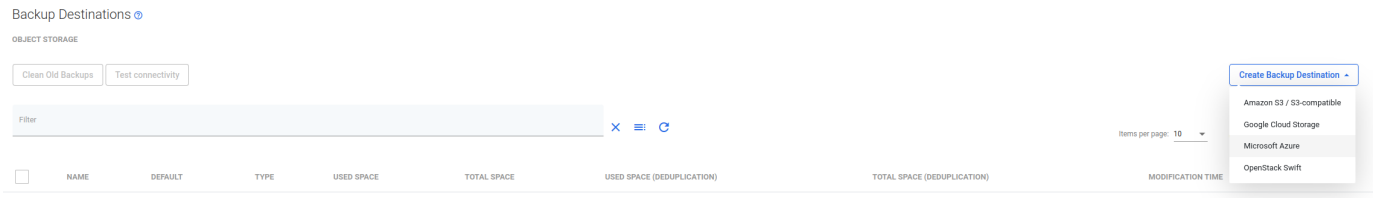


To configure Azure as a backup destination for Data Protector for Cloud Workloads, we just need:

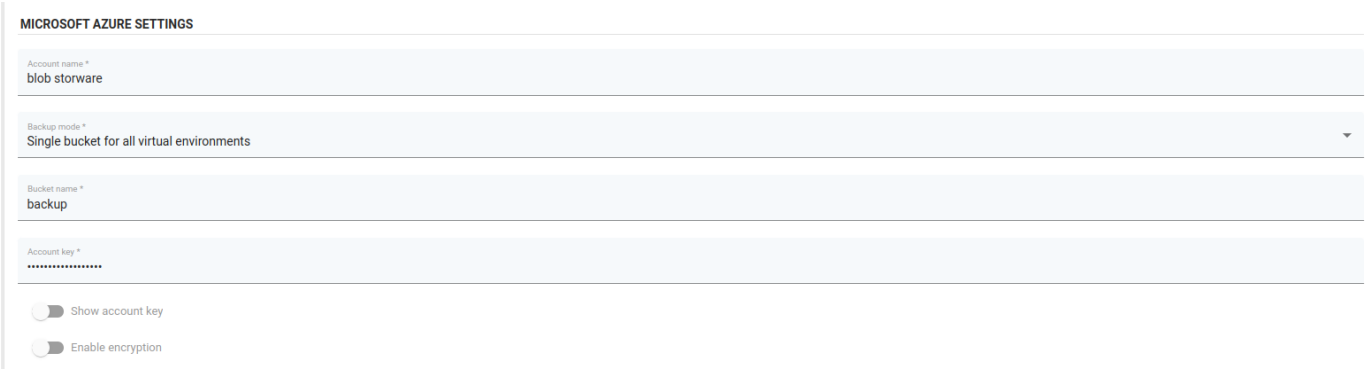
- The storage account name
- One of the account keys



Now you can go to the backup destinations tab in Data Protector for Cloud Workloads and create a new Microsoft Azure backup destination.



You just need to provide an account name, bucket name and key.



And that's all. As you see, in a few minutes you can integrate Data Protector for Cloud Workloads with Azure Blob storage to securely store your backups

Nutanix Objects

Nutanix Objects is an S3-compatible backup provider. Configuration as the backup destination is similar to AWS S3.

Example

In the Data Protector for Cloud Workloads system, go to the **Backup Destinations** -> **Object Storage** tab, then press the **Create Backup Destination** button and select the **Amazon S3 / S3-compatible** option.

In this step, complete the name, retention, add: API URL, Access key, and Secret key, indicate the name of the bucket to be used.

Then go to the **AMAZON S3/S3-COMPATIBLE SETTINGS** the segment in which you should **deselect** the **Parallel Download enabled** option for Nutanix Objects.

> When using Nutanix Objects version 3.5, the region "us-east-1" may be required.

After entering the settings, press the **Save** button to be able to use Nutanix Objects as Backup Destination.

OpenStack SWIFT

Data Protector for Cloud Workloads supports integration with OpenStack SWIFT.

Example

In the Data Protector for Cloud Workloads system, go to the **Backup Destinations** -> **Object Storage** tab, then press the **Create Backup Destination** button and select the **OpenStack Swift** option.

Enter the name of the new backup destination, assign it to **Node Configuration** and set up the retention.

Next, provide settings specific to **OpenStack Swift**:

- Authentication URL - URL pointing to authentication service, it should be similar to the following

  ```
  https://SWIFT_HOST:5000/v3/auth/tokens
  ```

- User name - domain formatted username used by Data Protector for Cloud Workloads to log into OpenStack Swift
- Authentication method - BASIC / TEMPAUTH / KEYSTONE / KEYSTONE_V3
  - in the case of KEYSTONE_V3 authentication method, you also need to enter **Authentication method scope**, **Domain** and **Project**
- Name of Swift service intended to be used
- Number of thread used (Swift connector supports multithreading)
- Endpoint interface type - type of interface used by connector (PUBLIC / INTERNAL / ADMIN)

OPENSTACK SWIFT SETTINGS

Enable encryption

Authentication URL *
https://swift.storware.local/v3/auth/tokens

User name *
storware@storware.local

Password *
••••••••••••••••

Show password

Authentication method *
KEYSTONE_V3

Authentication method scope *
DEFAULT

Domain
storware

Project
backup

Segment number length *
5

Segment size [MiB] *
200

Compression type *
DISABLED

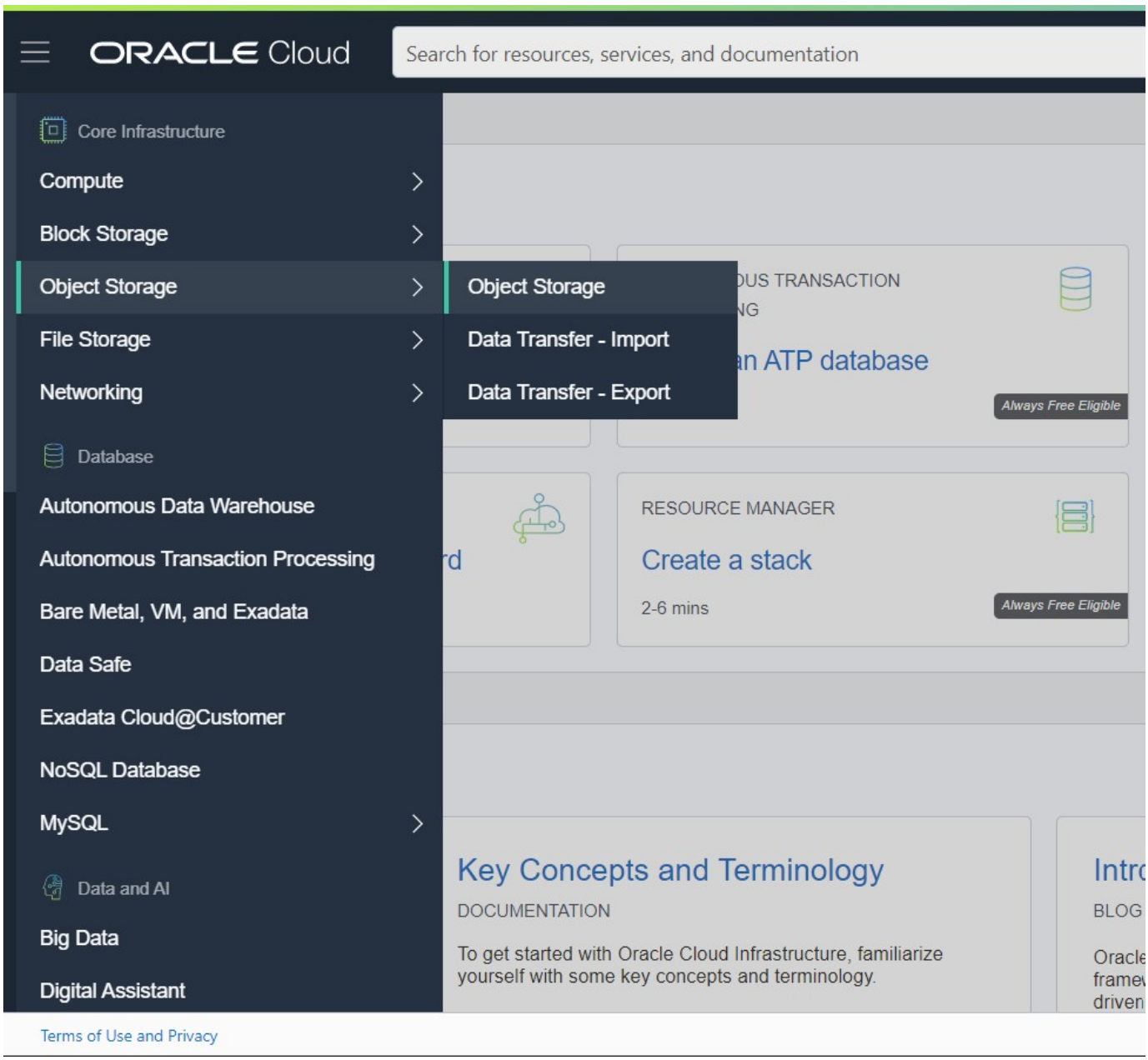
Oracle Cloud Infrastructure Object Storage

Overview

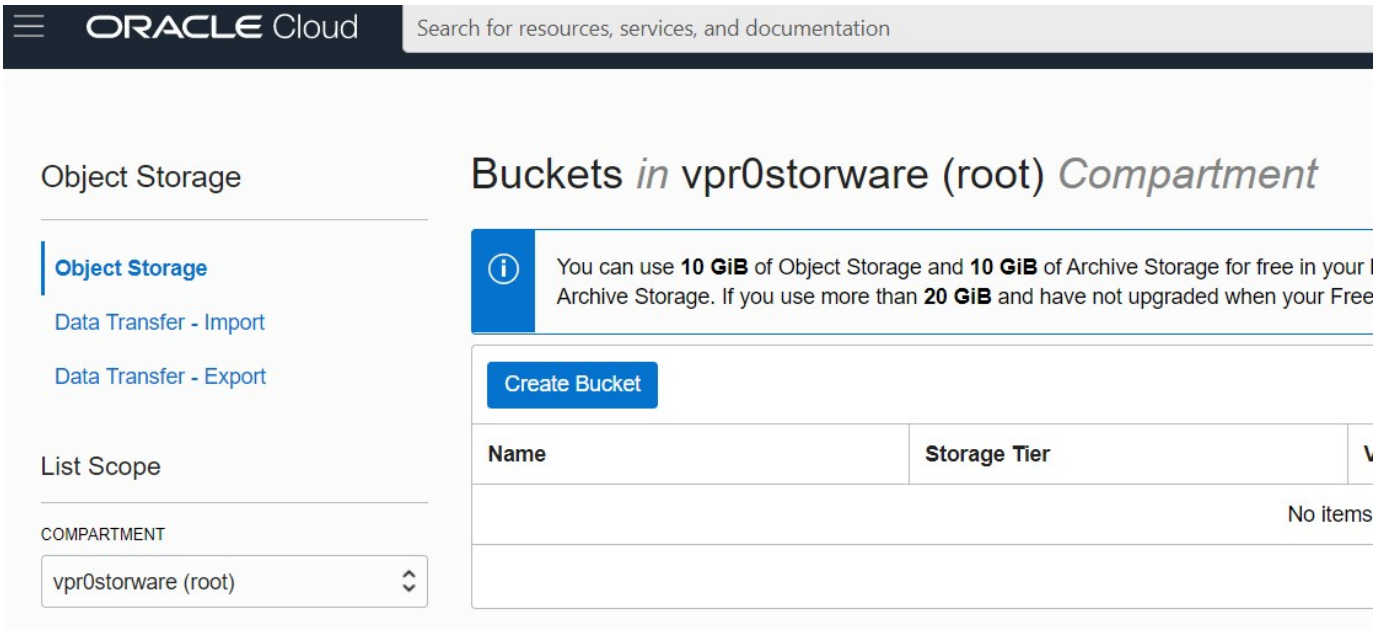
The Oracle Cloud Infrastructure Object Storage service is an internet-scale, high-performance storage platform that offers reliable and cost-efficient data durability. The Object Storage service can store an unlimited amount of unstructured data of any content type, including analytic data and rich content.

Example

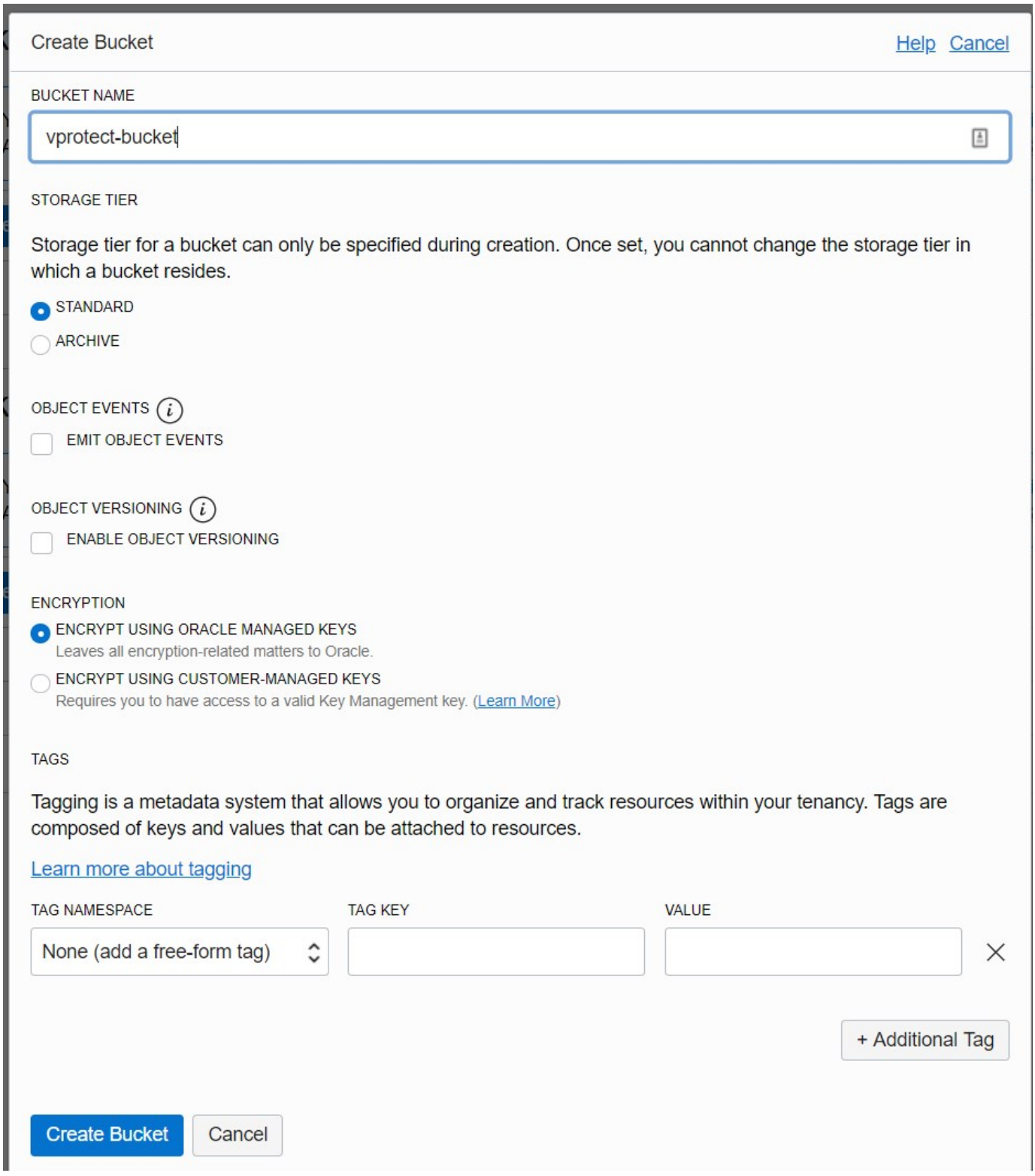
Log in to the Oracle cloud dashboard, expand the left side menu and go to the Object Storage tab.



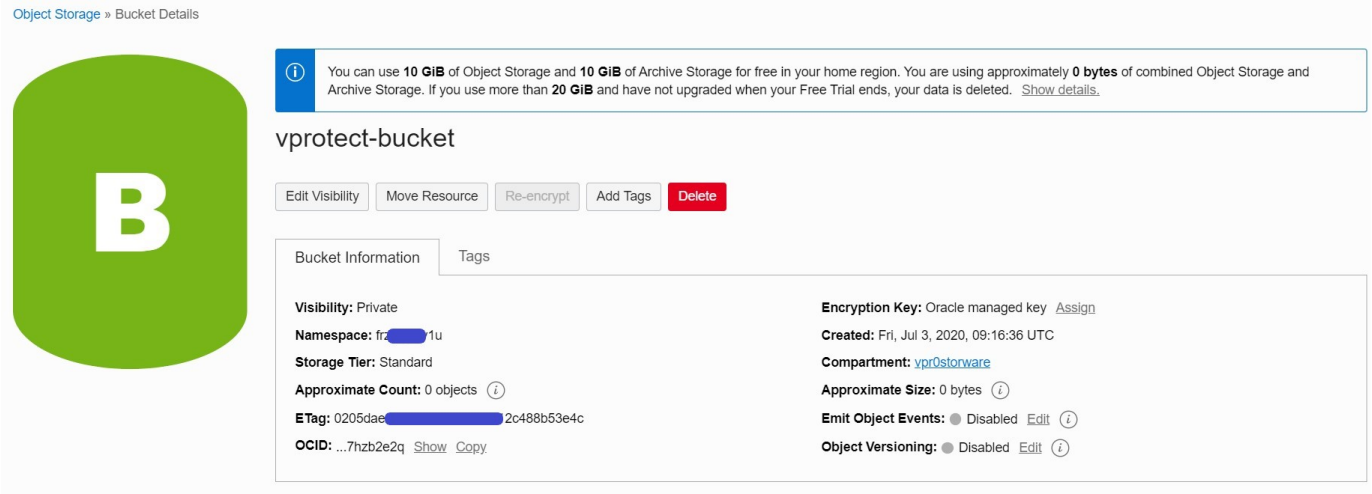
Now let's create a new bucket.



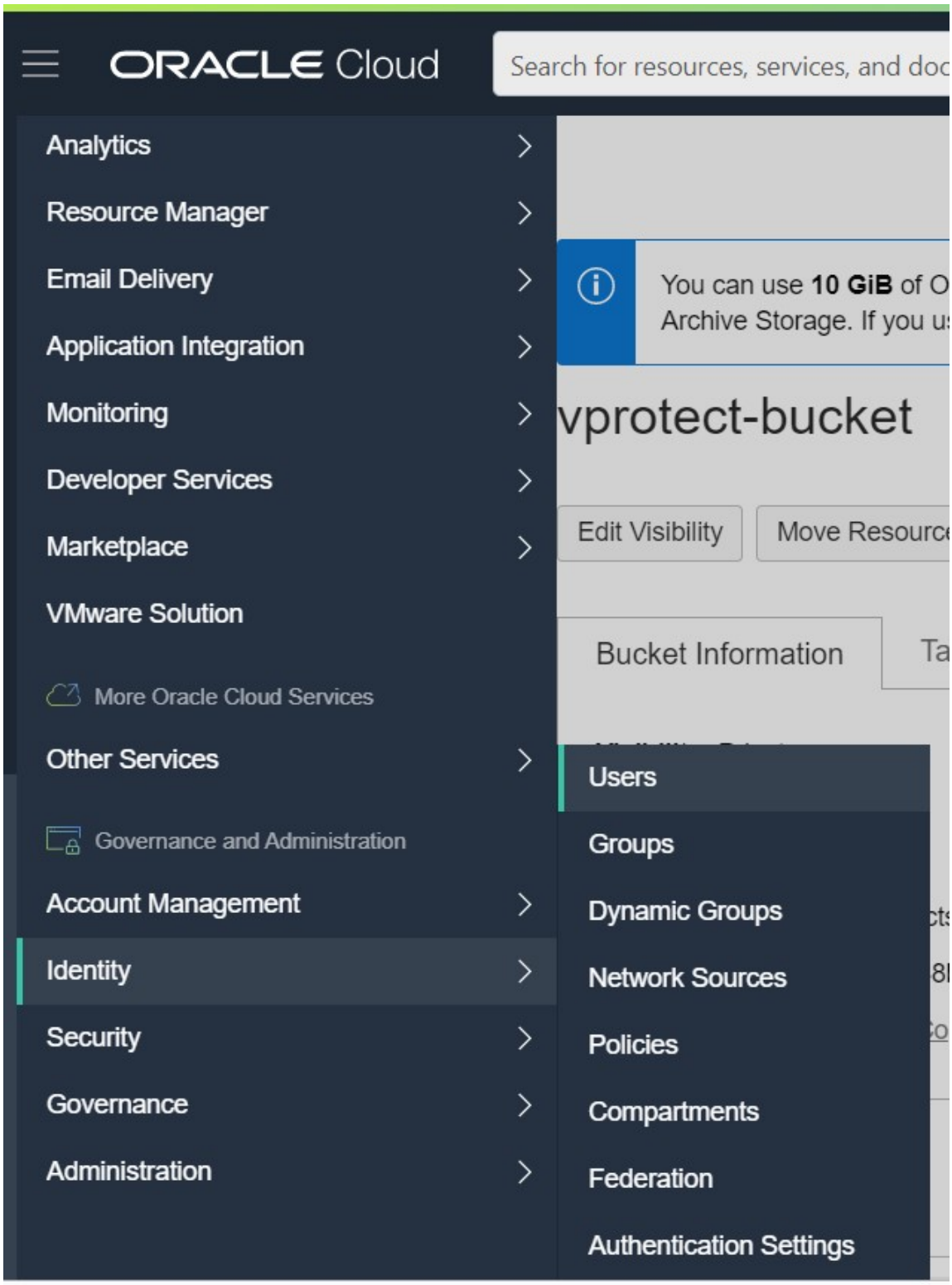
We do not require specific bucket settings for Data Protector for Cloud Workloads. The bucket name will be needed when we want to create a backup destination in Data Protector for Cloud Workloads.



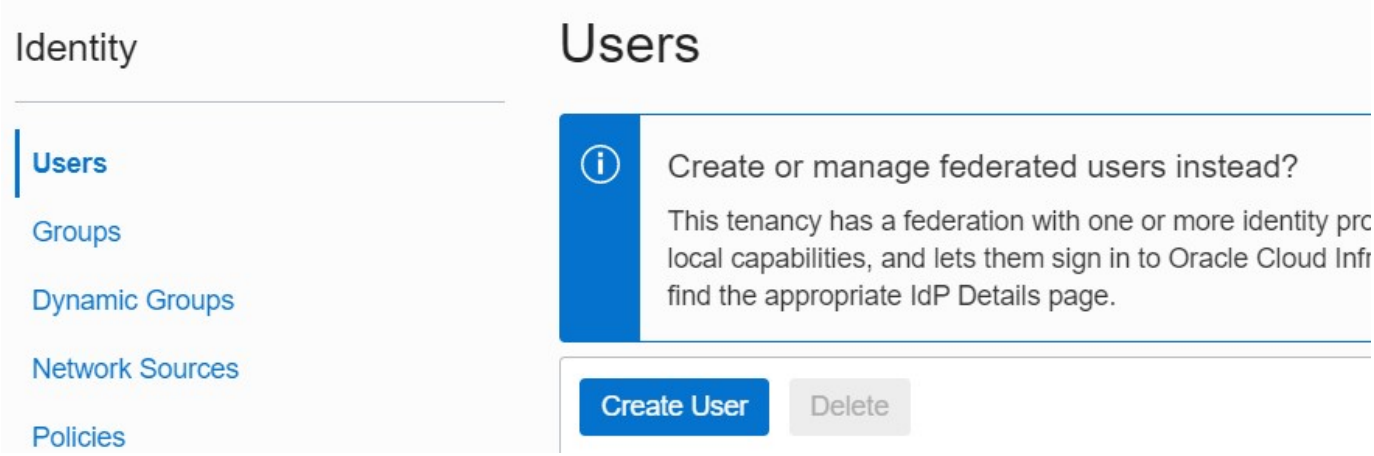
After creating the bucket, you'll see a list of buckets. Click on the name to view the details of the object. Remember the "namespace", we also need it when creating a backup destination.



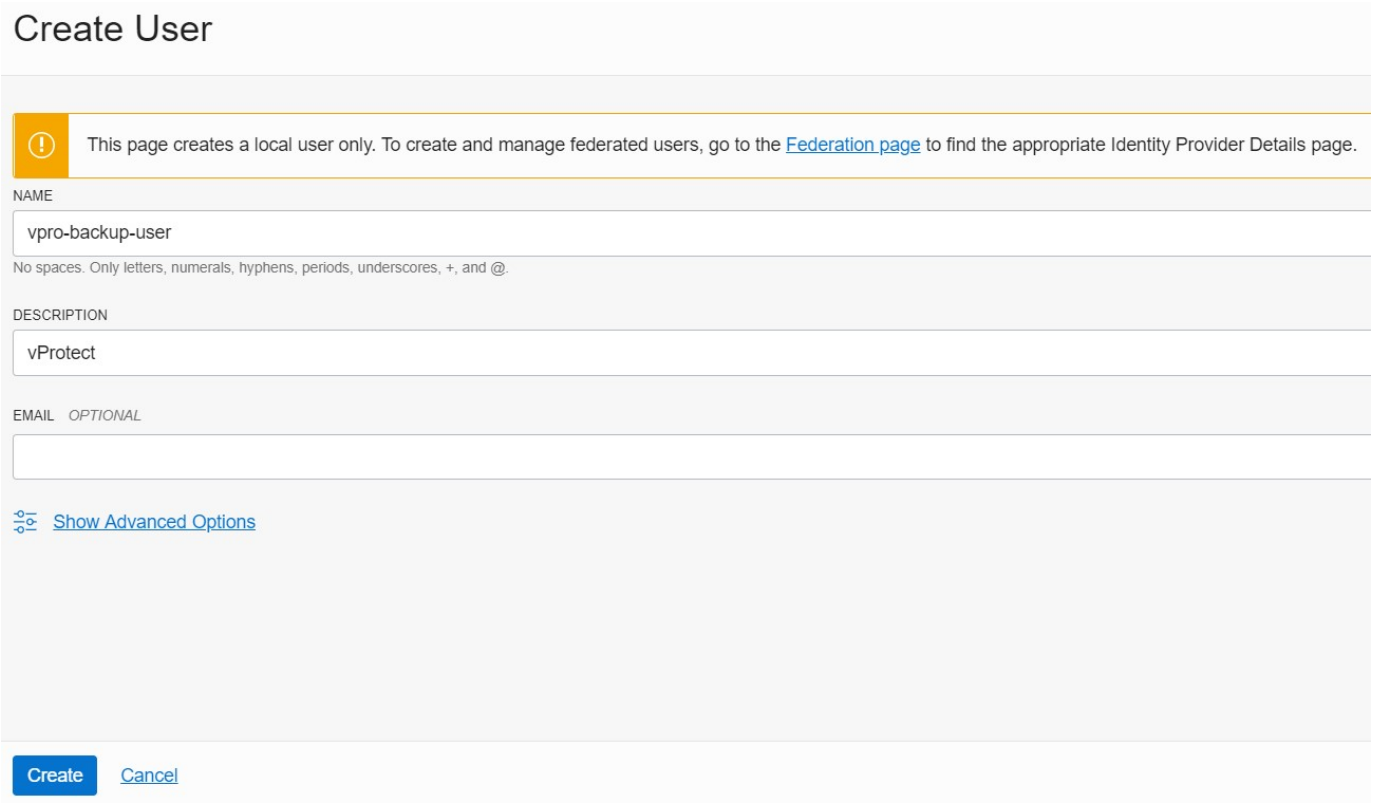
Now we need to create a user that we will use to authenticate our backup destination. Please go to the Users tab under the Identity tab in the menu on the left.



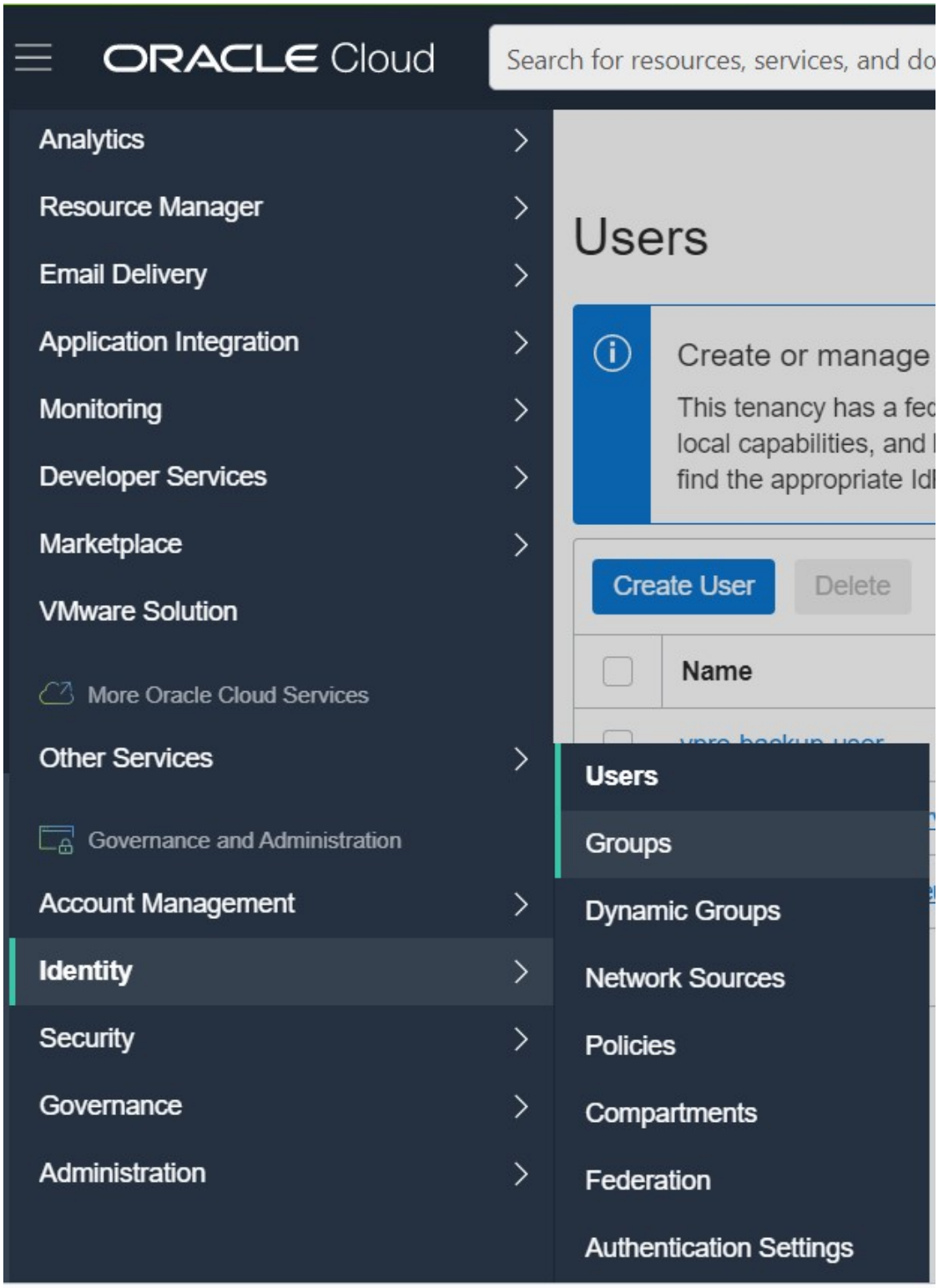
Now create a new user.



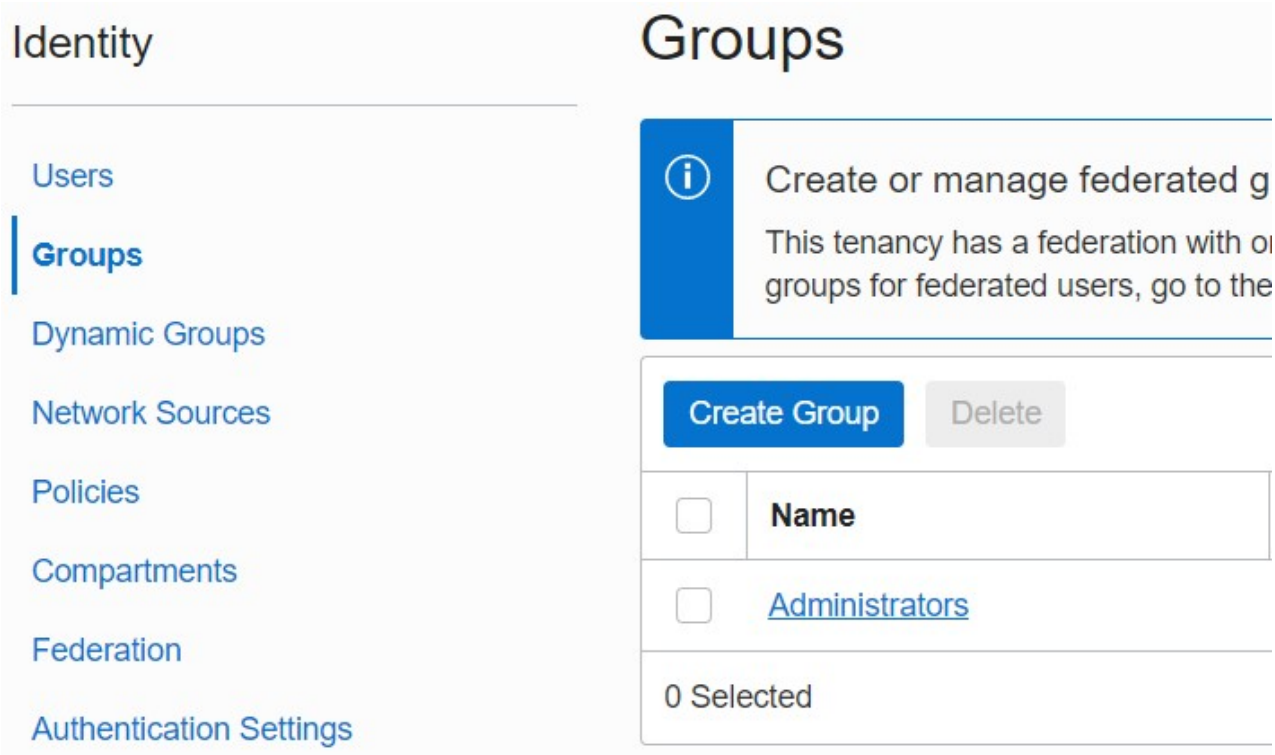
Fill in the required fields.



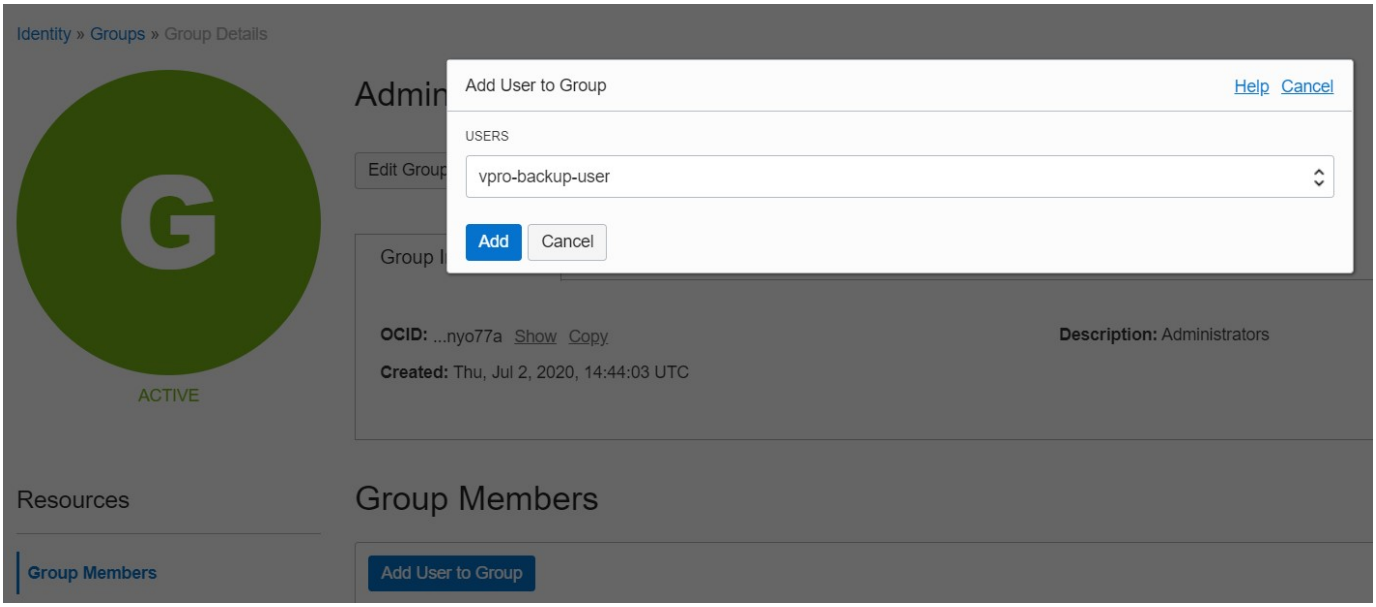
Then go to the Groups page, which you can also find under the identity tab in the left side menu.



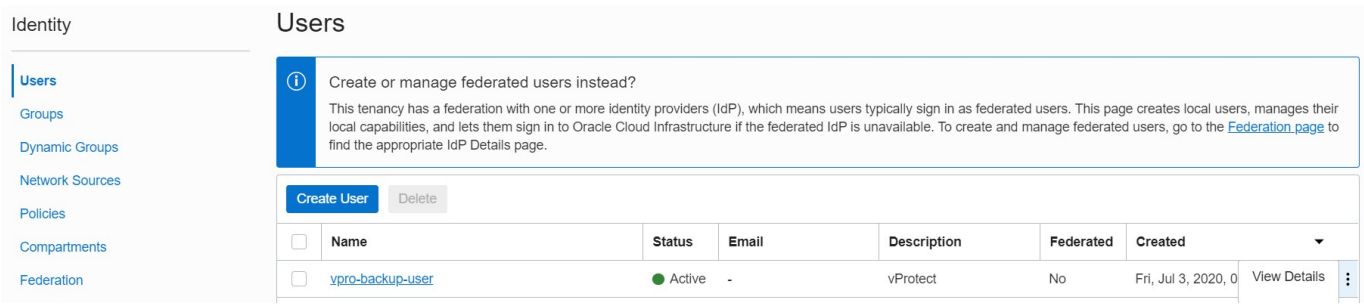
Now click on the existing group "Administrators".



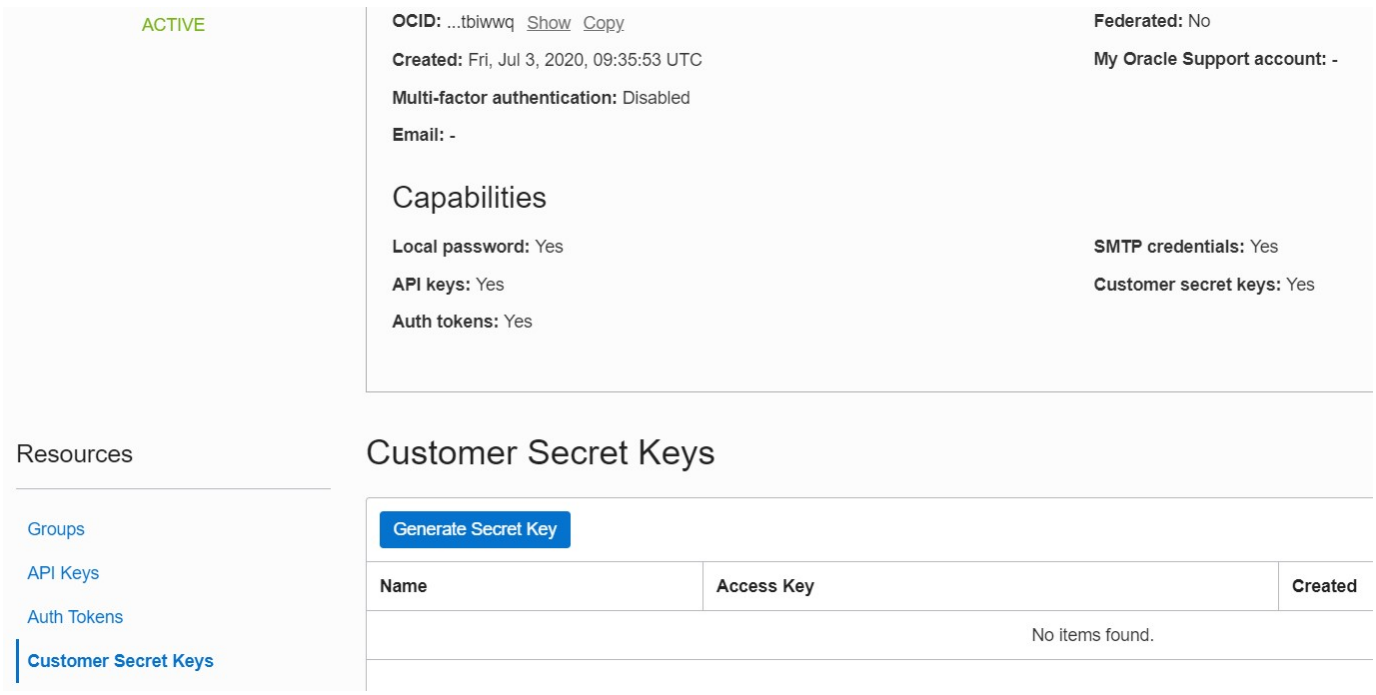
Now click on "Add User to Group" and choose the user you created previously.



Go back to the Users page and go to the details page of our user.

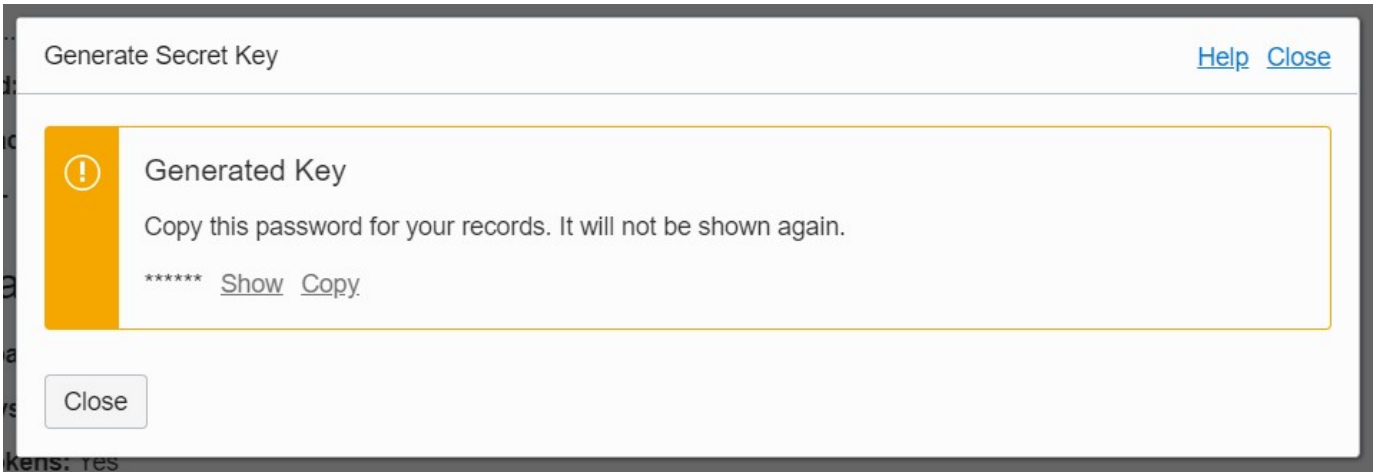


Scroll down and open the "Customer Secret Keys" tab. Click on "Generate Secret Key".

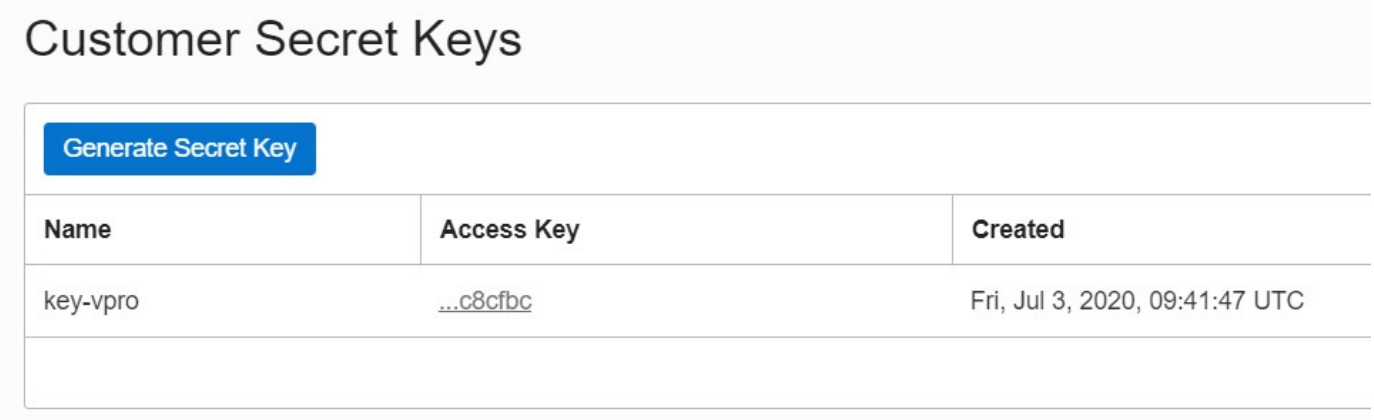


Enter any name.

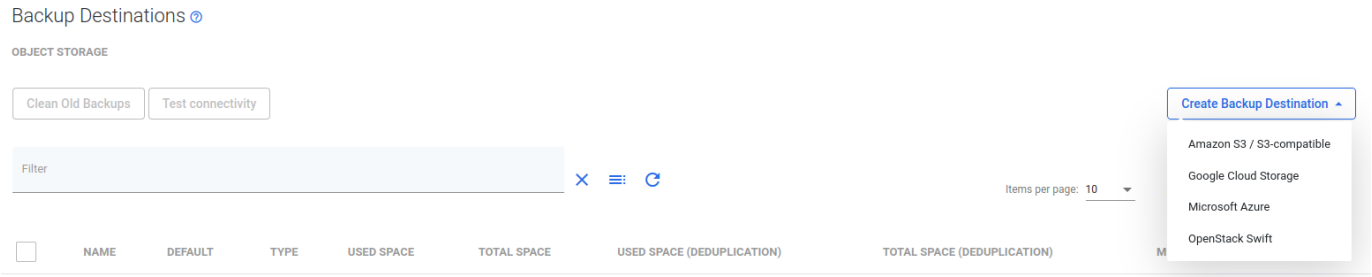
As you see in the note below, copy and save the secret key because you can only do this now.



After generating the secret key, you can view the access key, just move the mouse over it.



Now we can go to the Data Protector for Cloud Workloads Dashboard. Open the "Backup Destination" tab from the left side menu, then the sub-tab "Object Storage" and choose "Amazon S3 / S3-compatible" as the new type of backup destination.



First, let's focus on the "S3-Compatible" section.
To generate an API URL, you will need this site: https://docs.cloud.oracle.com/en-us/iaas/api/#/en/s3objectstorage/20160918/
As We mentioned earlier, you will need an object storage namespace (choose the API URL from the list according to your region).
Then provide your bucket name and region, and finally switch on "Record time after backup" and "Path style access enabled".
Configure the rest of the settings as desired.

AMAZON S3 / S3-COMPATIBLE SETTINGS

API URL (optional)
https://comcat.obejtstorage.ou.frankfurt1.oraclecloud.com

Backup mode
Single bucket for all virtual environments

Bucket name *
backup

Region (optional)
ou-frankfurt1

Record backup time after store

Path style access enabled

Resolve hostname to IP before connecting

Parallel Download enabled

Access key *

Show access key

Secret key *

Show secret key

Enable encryption

Proxy configuration enabled

PRE/POST ACCESS

Execute pre store command

Execute post store command

Cancel

Scality RING

Overview

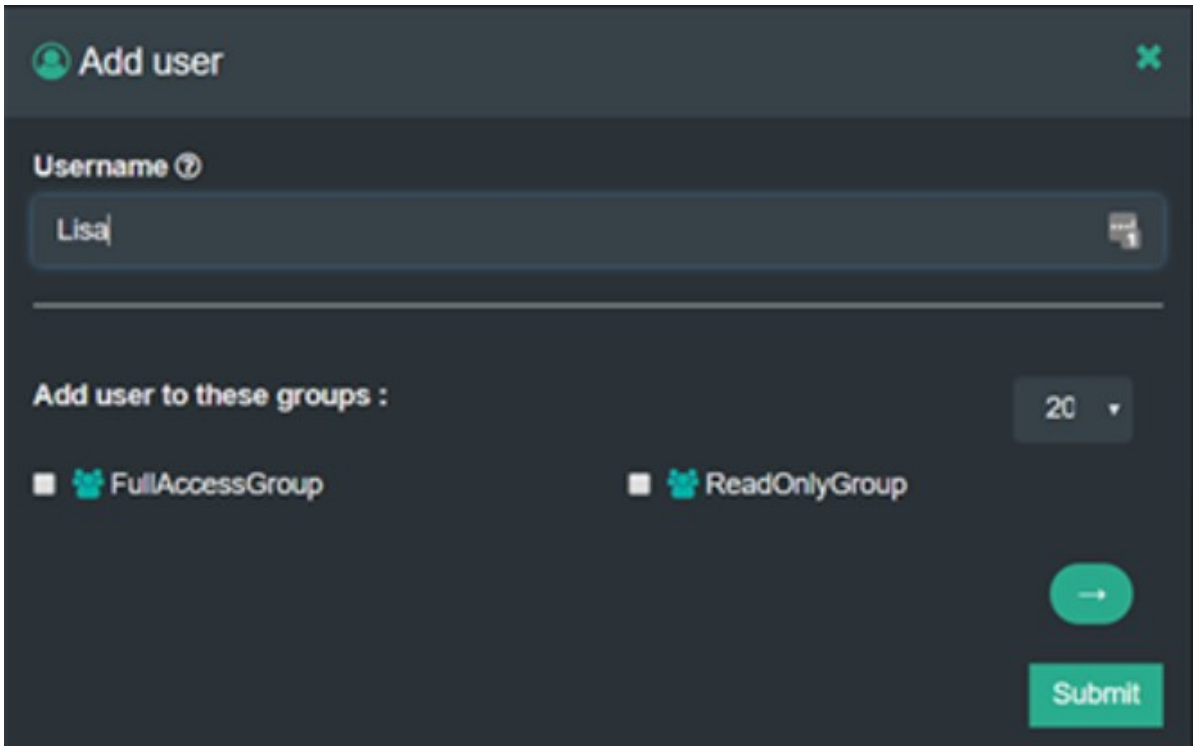
Scality Ring offers an object storage solution with a native and comprehensive S3 interface. Scality S3 Connector is the first AWS S3-compatible object storage for enterprise S3 applications with secure multi-tenancy and high performance.
AWS has achieved incredible traction with services such as S3 for a wide variety of cloud application and service provider businesses. However, for many service providers and enterprise corporations who require an on-premises deployment model in order to maintain control over sensitive data, for performance optimization, or for reasons of security or compliance – Scality's new S3 Connector for the RING provides an optimal solution. The S3 Connector offers a solution that is application-compatible with AWS S3 at both the data API level and also with the rapidly evolving AWS multi-tenancy model termed IAM (Identity and Access Management).

Example

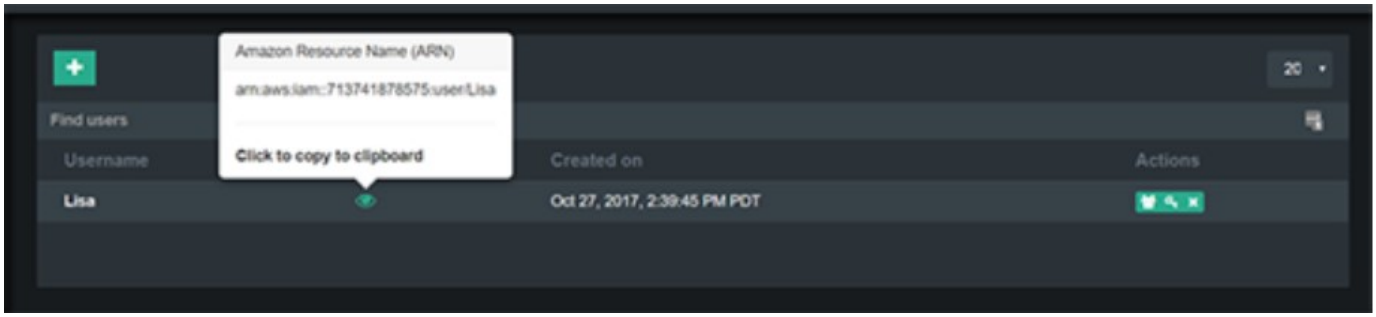
In this example, we will show you how to use the Scality S3 connector to create the backup destination for Data Protector for Cloud Workloads.
It assumes that the S3 connector is installed and configured

We will start by creating a user, please launch the S3 connector user interface.

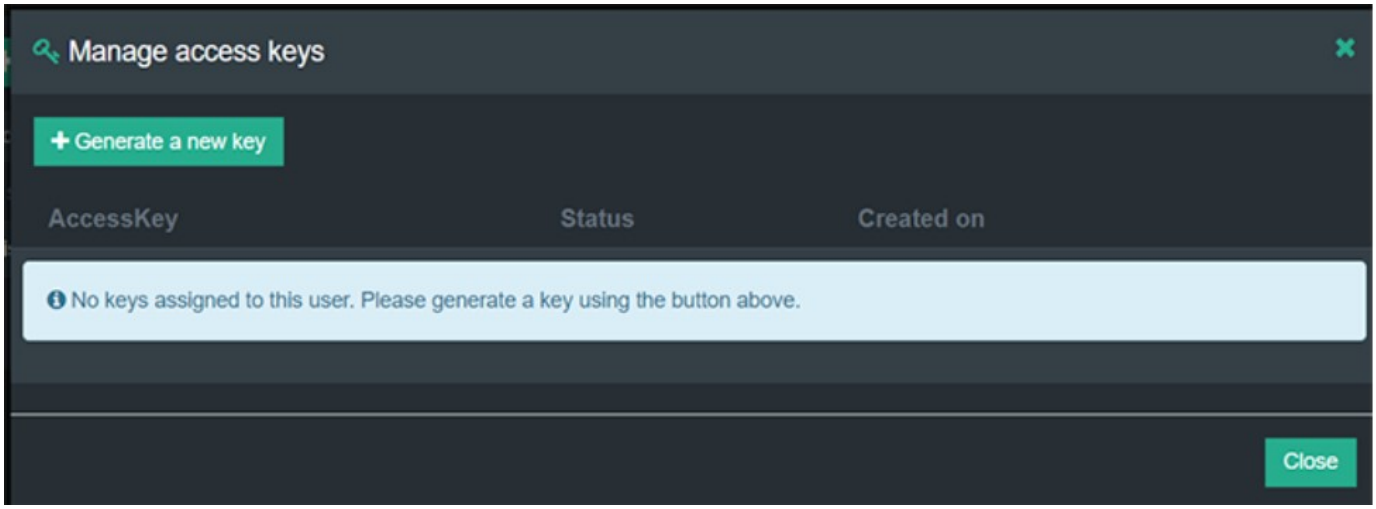
Log in as an account user using the password set in *Setting an account Password* from the S3 console GUI.
Select the user to open the user management window.
Click Add user to open the add user window.
Enter the user name and make sure to check the box for "FullAccessGroup".



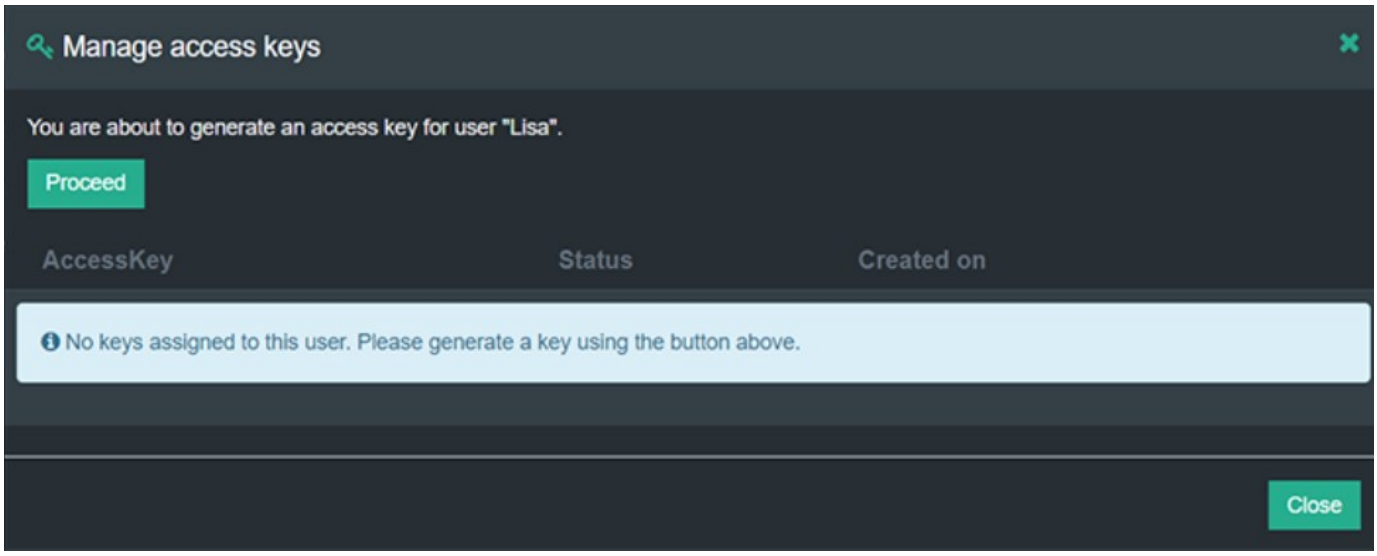
The user management panel displays the user name and the Amazon Resource Name (ARN).
Now we will generate the access and secret keys for the user.
Click on the key icon in the Actions column of the user row.



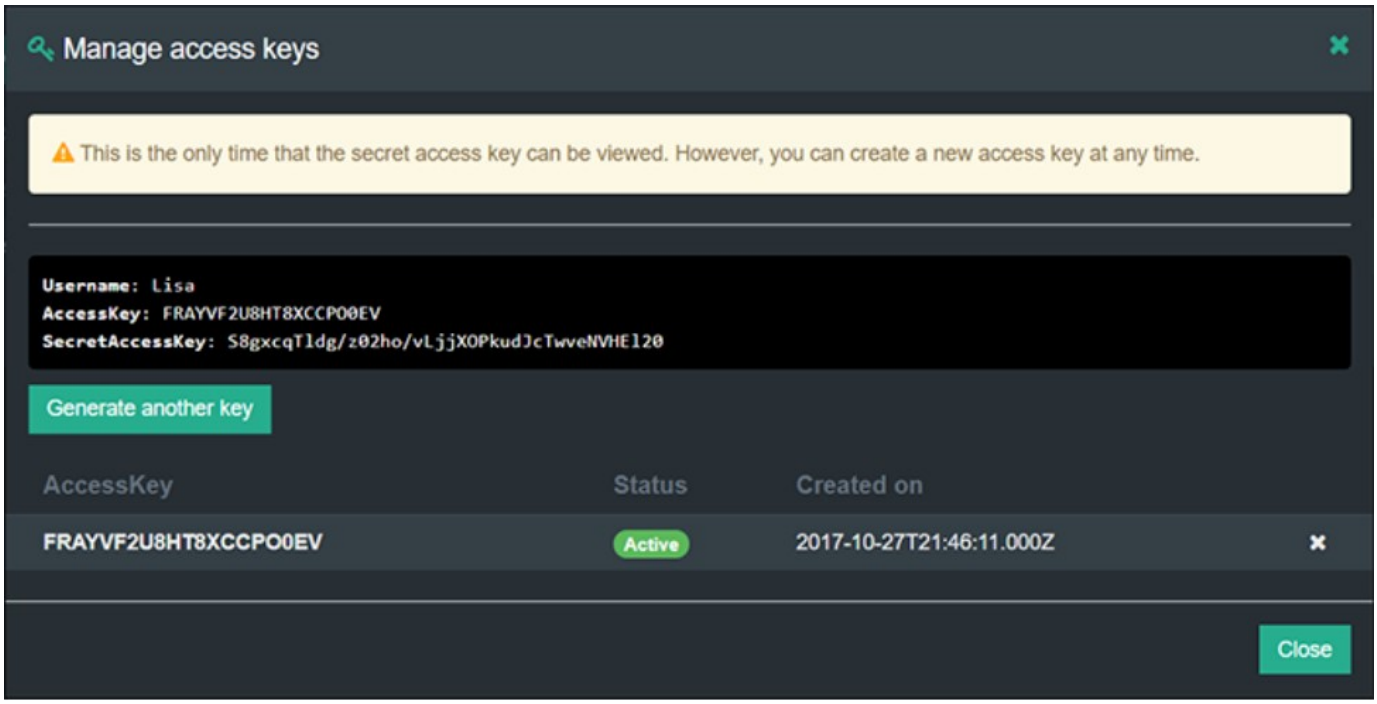
Click on Generate a new key.



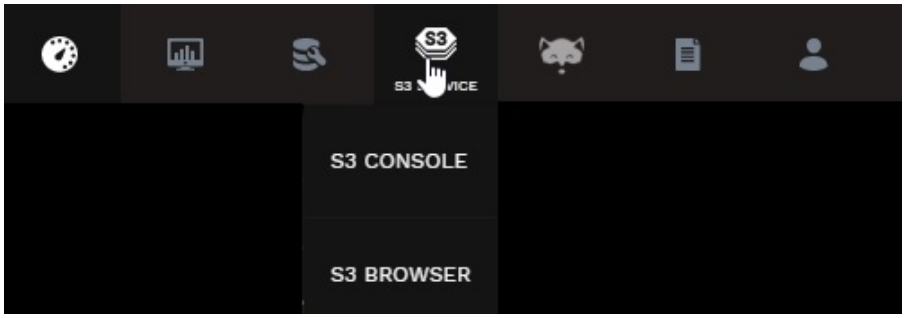
Click on Proceed to generate the user's AccessKey and SecretAccessKey.



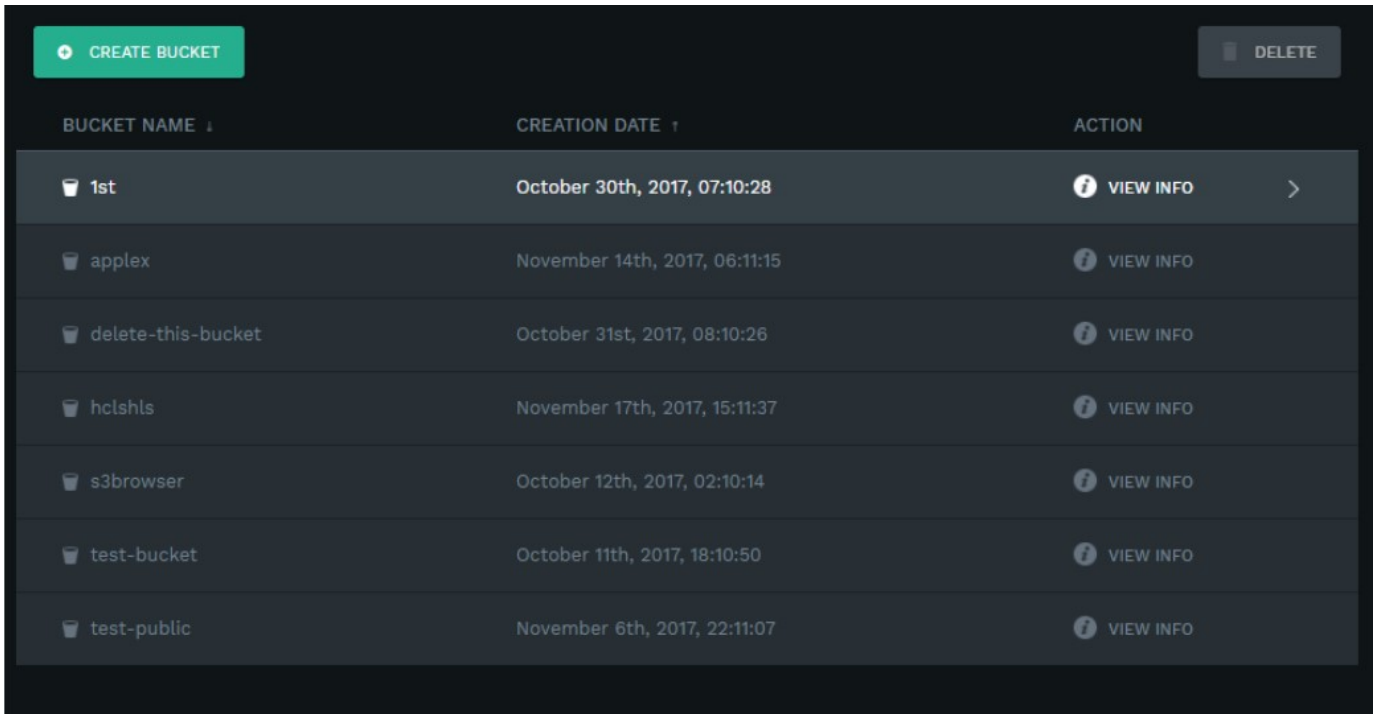
Copy and save the SecretAccessKey to a secure location. It is not shown again and cannot be recovered later.



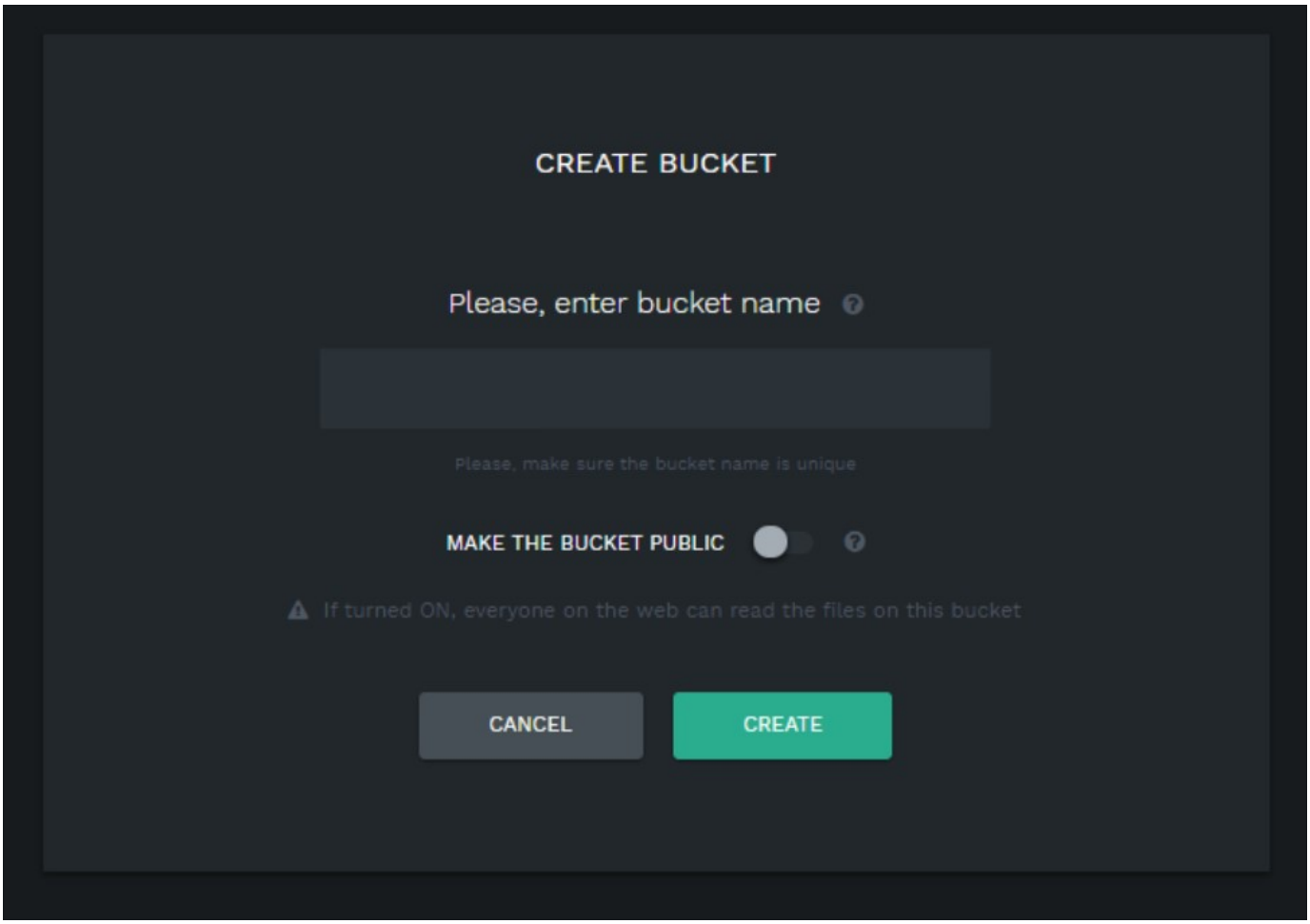
Now we can go to bucket creation. Please go to the S3 Browser interface.



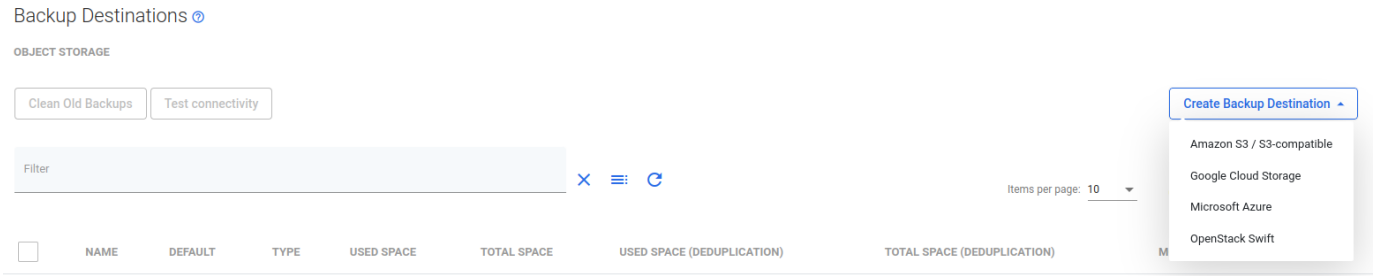
The S3 Browser opens the main window, from which one can see the entire roster of buckets.
Click the Create Bucket button in the top left of the main window.



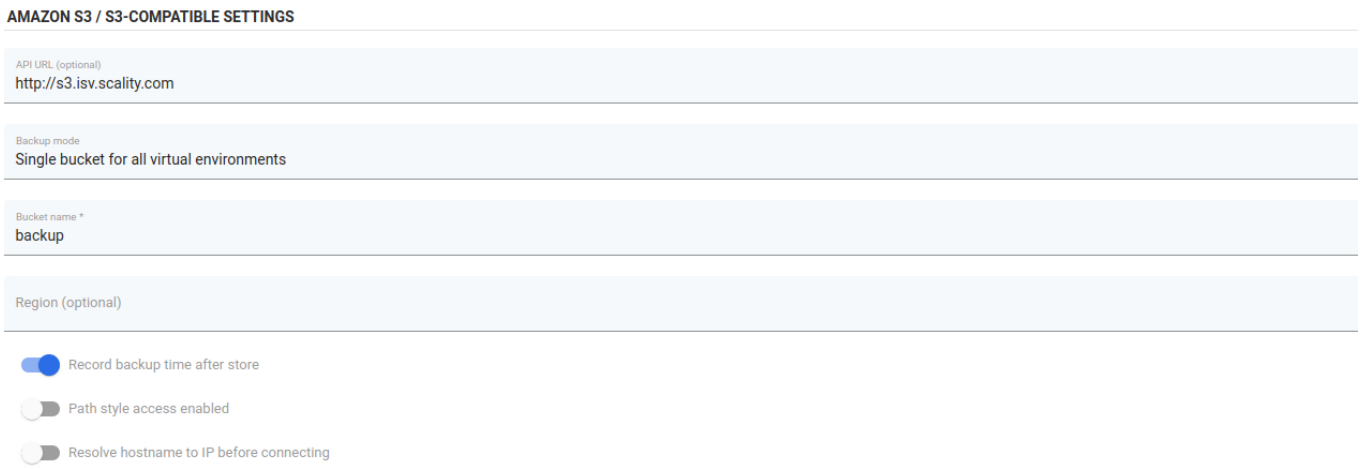
Enter a name for the new bucket and click on Create button.



That's all on the Scality side. Now we can go to Data Protector for Cloud Workloads.
Open the "Backup Destination" tab from the left side menu and choose "Amazon S3 / S3-compatible" as the new type of backup destination.



Like in other S3-compatible backup destinations, you have to fill in the fields below and provide the access and secret key.



That's it, you can now safely store your backups.

Enterprise Backup Providers

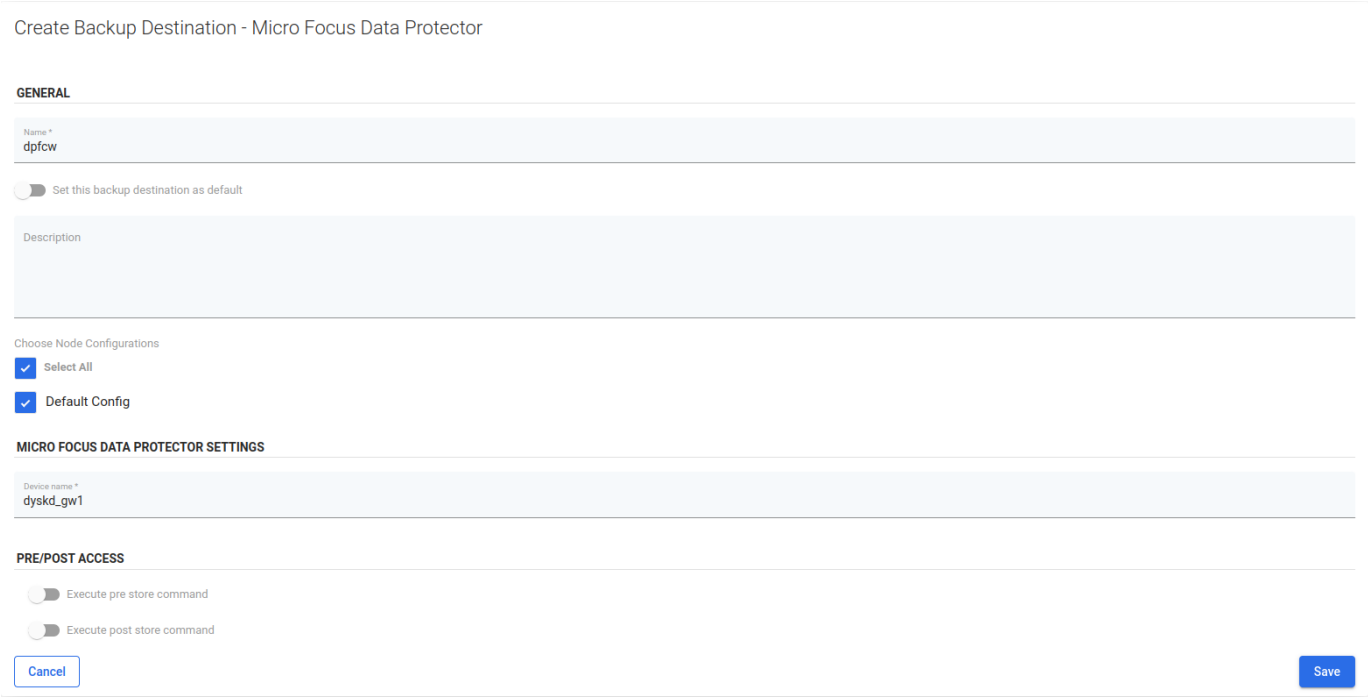
Micro Focus Data Protector

To integrate Data Protector for Cloud Workloads with Micro Focus Data Protector list device names by running following command on Data Protector for Cloud Workloads Node:

```
[root@protectorvp ~]# /opt/omni/bin/omnidownload -list_devices

Device Name                       Host
Device Type                           Pool Name
================================================================================
================================================================================
dyskd_gw1                         win-srv-proxy
Backup To Disk StoreOnce software de dyskd_MediaPool
vp_gw2                            protector11.lab.local
Backup To Disk StoreOnce software de vp_MediaPool
vp_protectorlab_gw1          protectorlab.lab.local
Backup To Disk StoreOnce software de vp_protectorlab_MediaPool
vp_protectorvp_gw1                protectorvp.lab.local
Backup To Disk StoreOnce software de vp_protectorvp_MediaPool
================================================================================
================================================================================
```

Next, go to Data Protector for Cloud Workloads and go to **Backup Destinations** -> **Enterprise**. Click **Create Backup destination** and choose **Micro Focus Data Protector**. Type the name for new backup destination and provide **Device name** which you get from first step.



Initial Configuration

Node

1. Set up the backup destinations (examples):
    - File System
    - Virtual Data Optimizer (VDO)
2. For backup strategies involving **disk attachment** mode, follow these steps: LVM setup on Data Protector for Cloud Workloads Node for disk attachment backup mode.

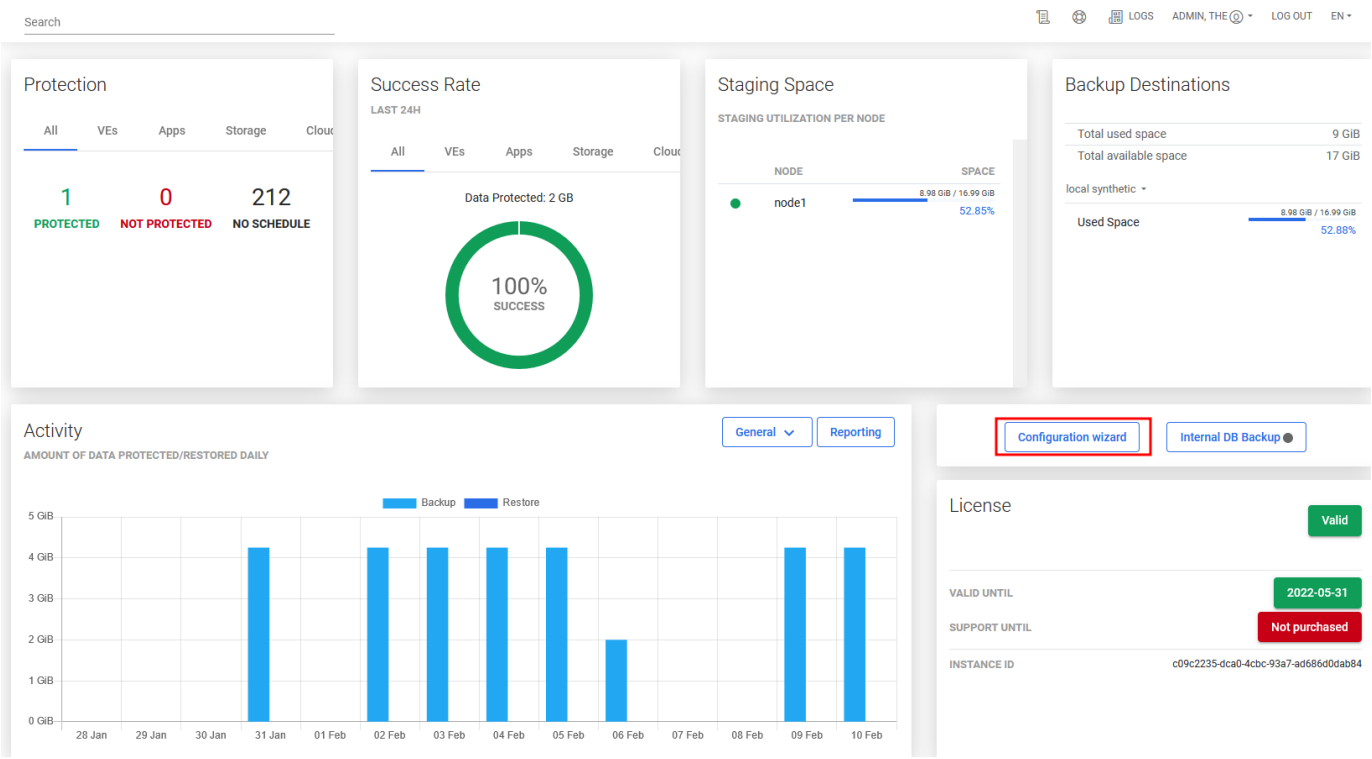
Server

1. Upload your license key:
    - if you don't have it, you can contact the Micro Focus team.
    - log in to the web UI and go to the **Settings** -> **License** and upload your `license.key` file.
2. It is **highly recommended** to set up Data Protector for Cloud Workloads DB backup - the database is key to restoring your Data Protector for Cloud Workloads environment and later all of the backups that you need.
3. Admin account setup:
    - for audit purposes, it is recommended to add individual admin accounts using the Access Management section

> **Note:** make sure to set the correct **time zone** for each user - the default admin account has **UTC** by default.

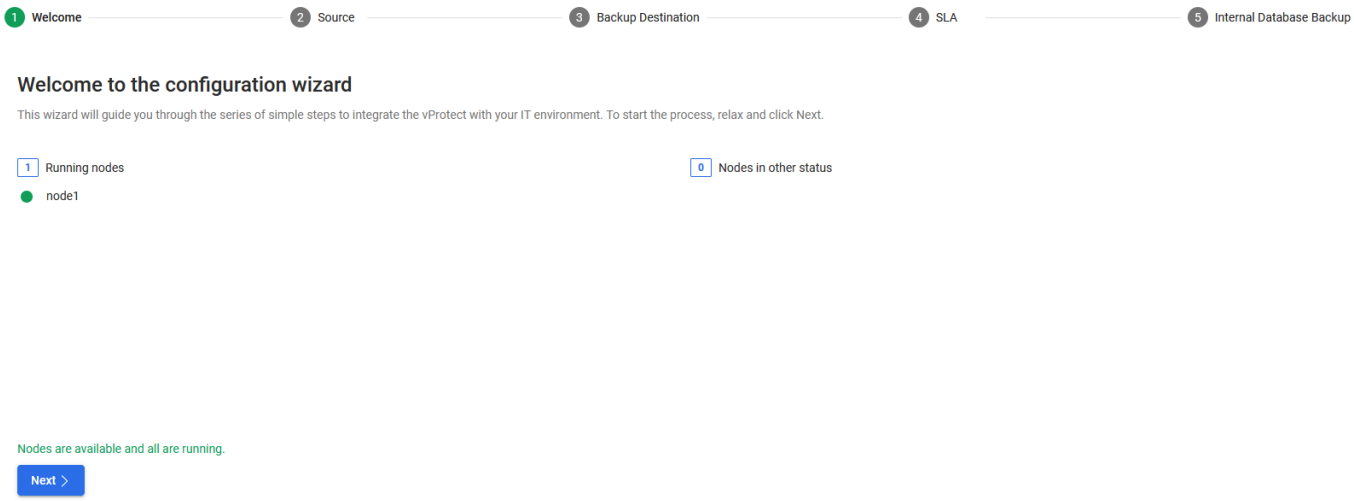
Configuration Wizard

- The configuration wizard can be accessed from the main dashboard by clicking on the "configuration wizard" button on the right.



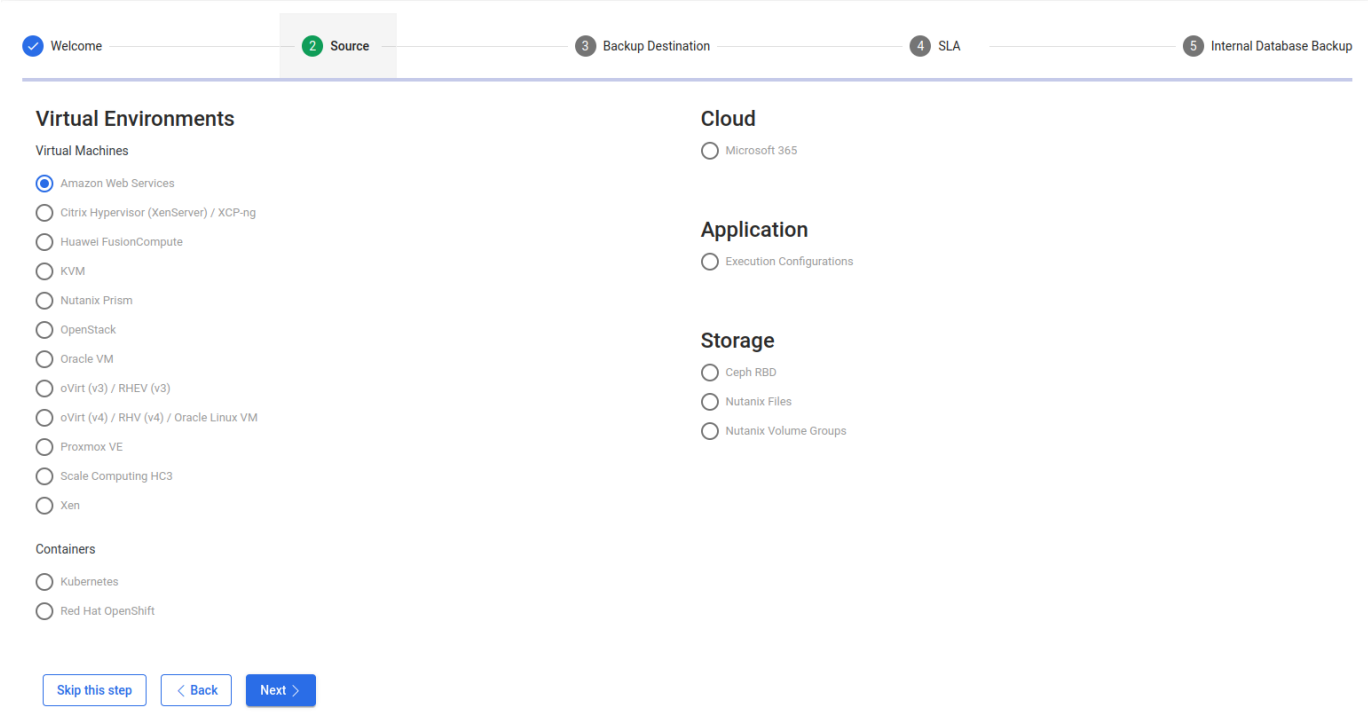
Welcome page - nodes

- On the welcome page, you should see the Data Protector for Cloud Workloads Nodes summary. You need at least one fully running node to continue. If you meet this requirement, please click on the Next button.

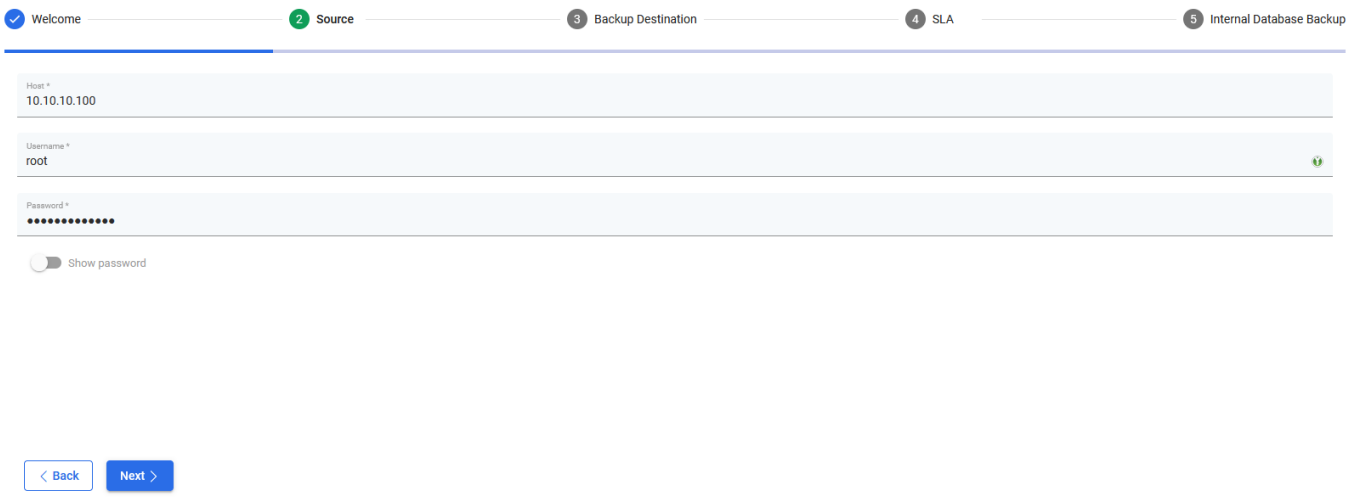


Add a hypervisor

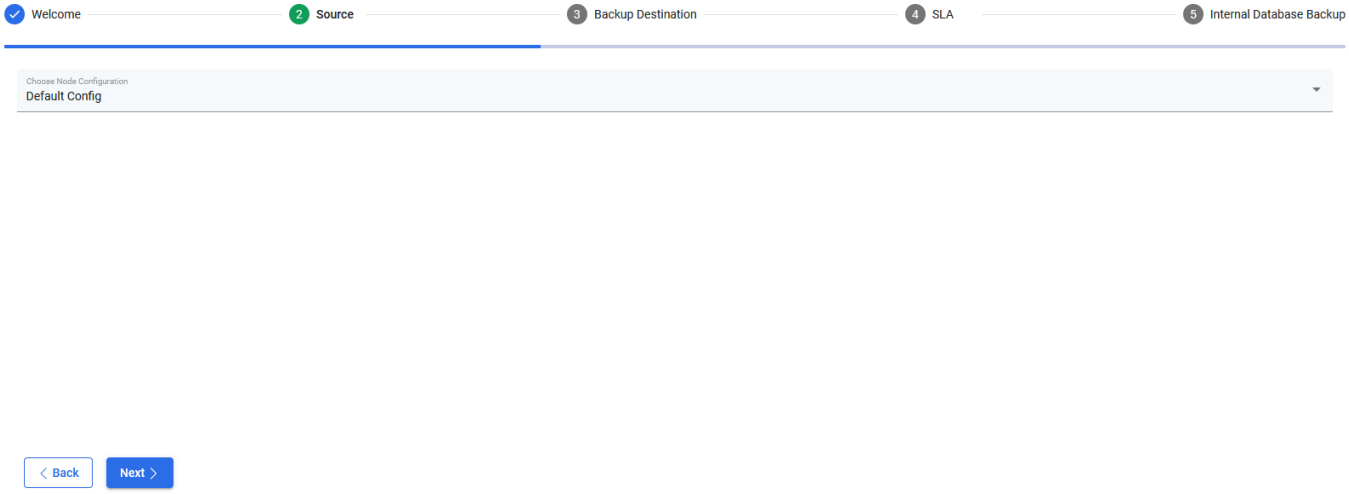
- In the Hypervisor section, you will start by selecting the hypervisor manager or hypervisor that you want to add. You can repeat this step if you have many types of virtualization providers.



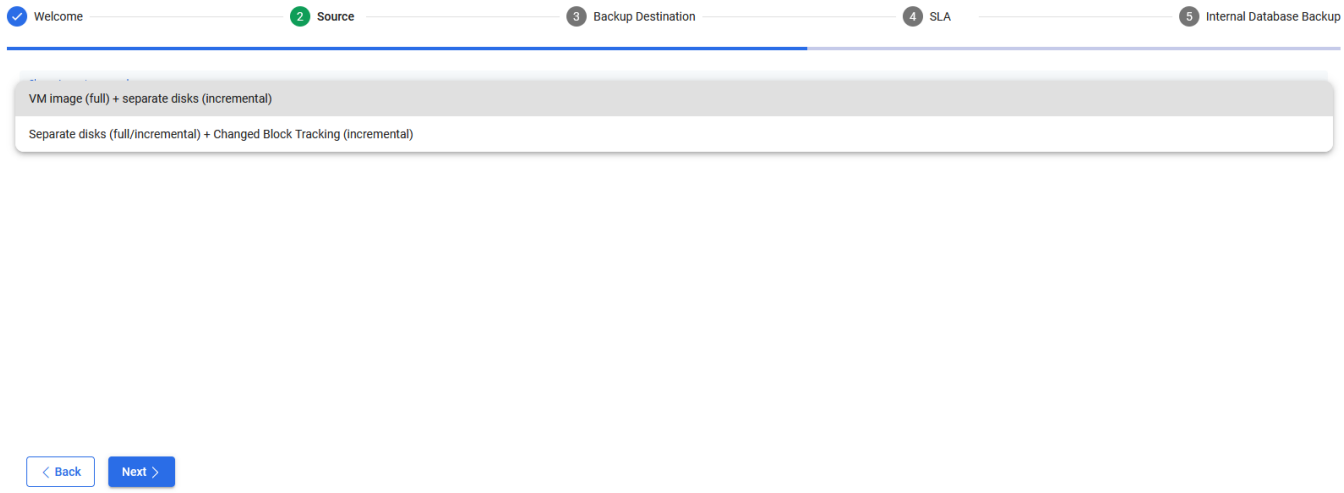
- For the Citrix hypervisor (as an example) you have to enter the following parameters



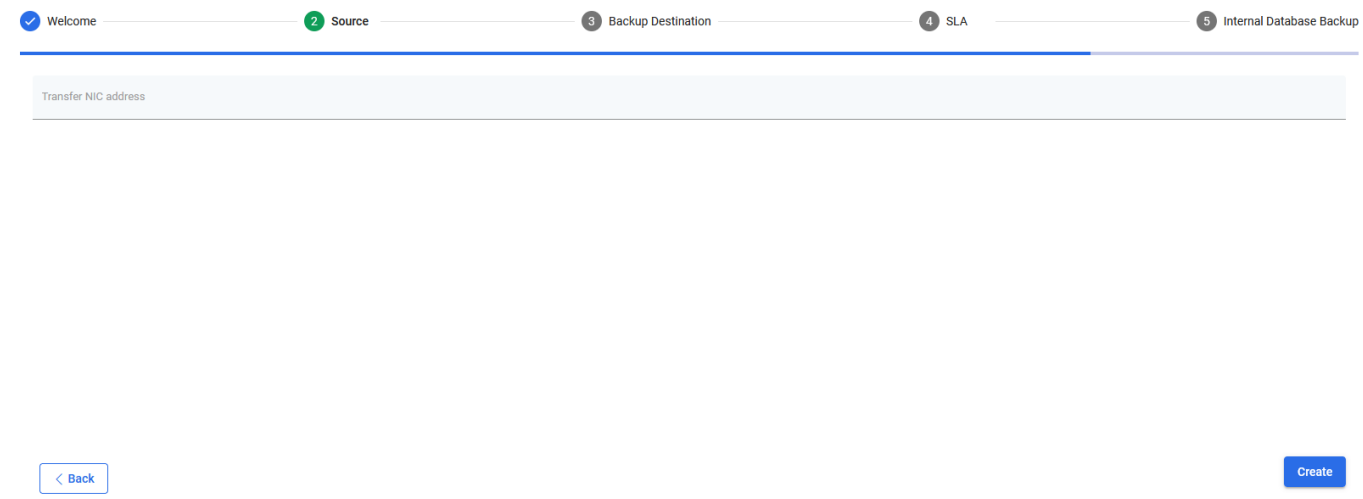
- Choose node configuration



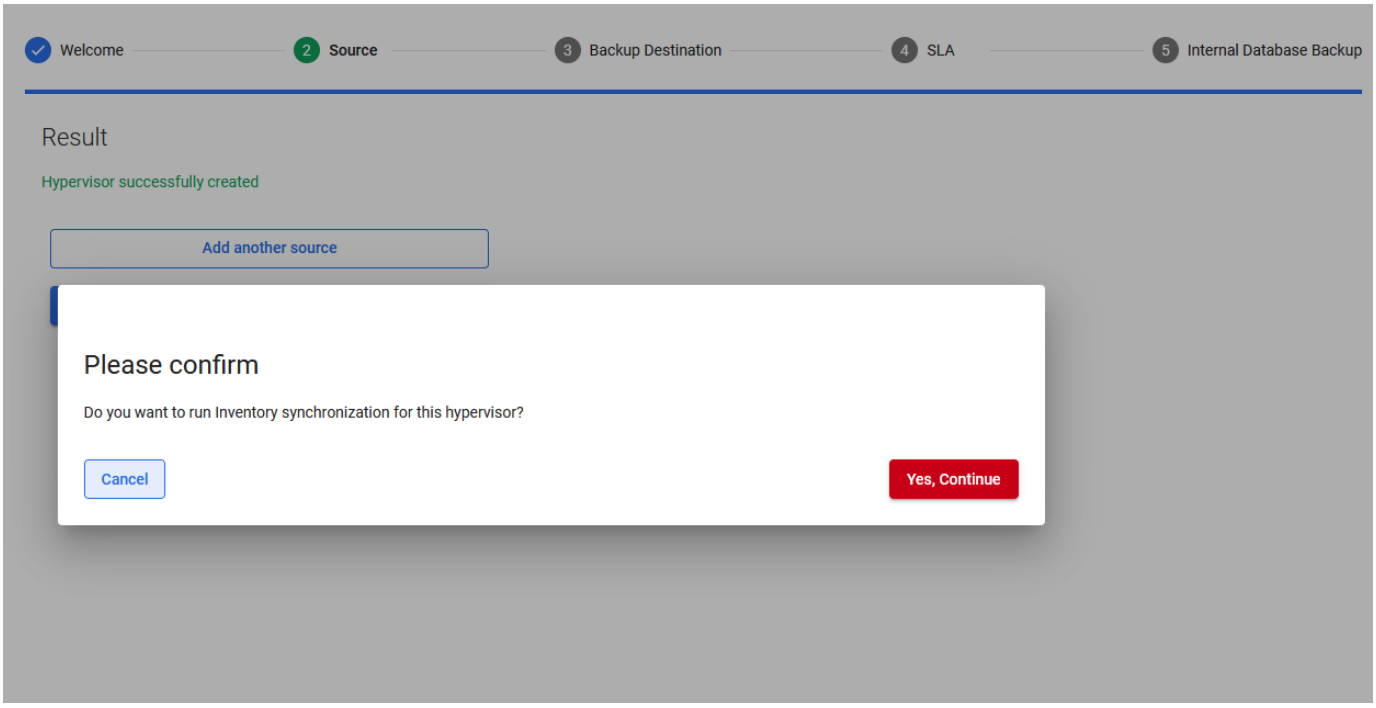
Select a backup strategy for your hypervisor



- Optionally, you can add an additional NIC for transfer purposes (provide IP address)

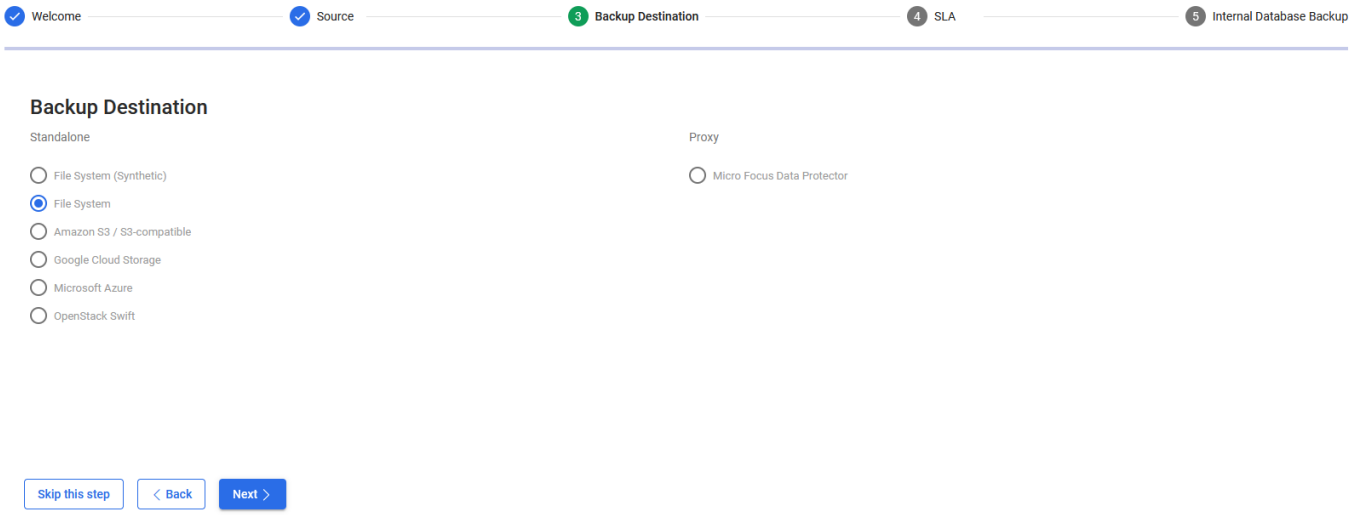


- At the end, you will see a popup window that allows you to run inventory synchronization. After that, you should see all the virtual machines from that hypervisor.

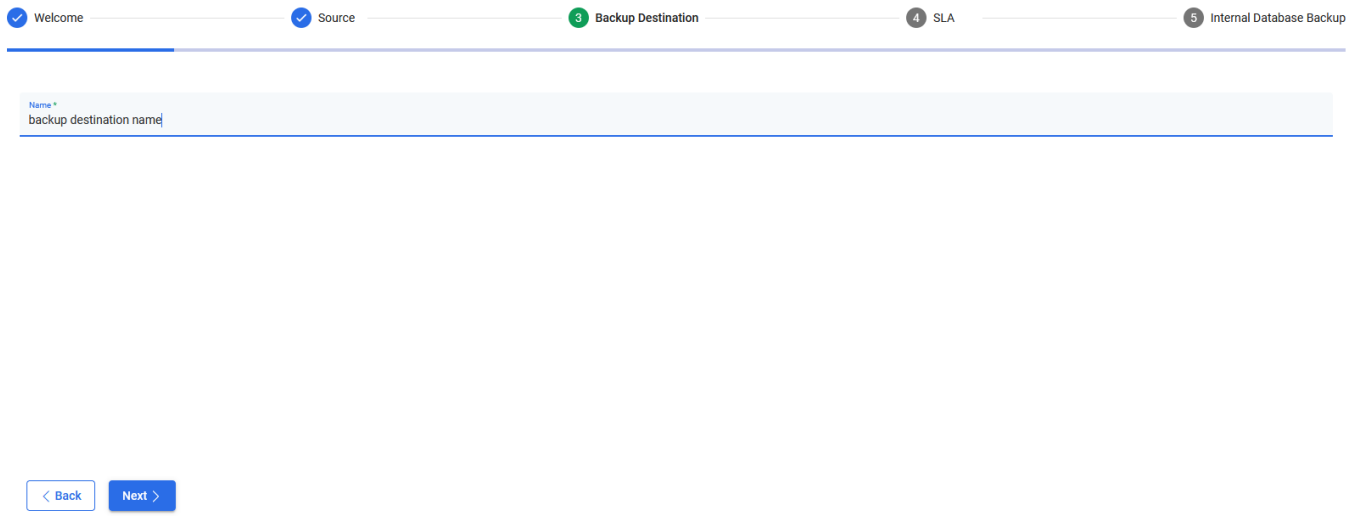


Add backup destination

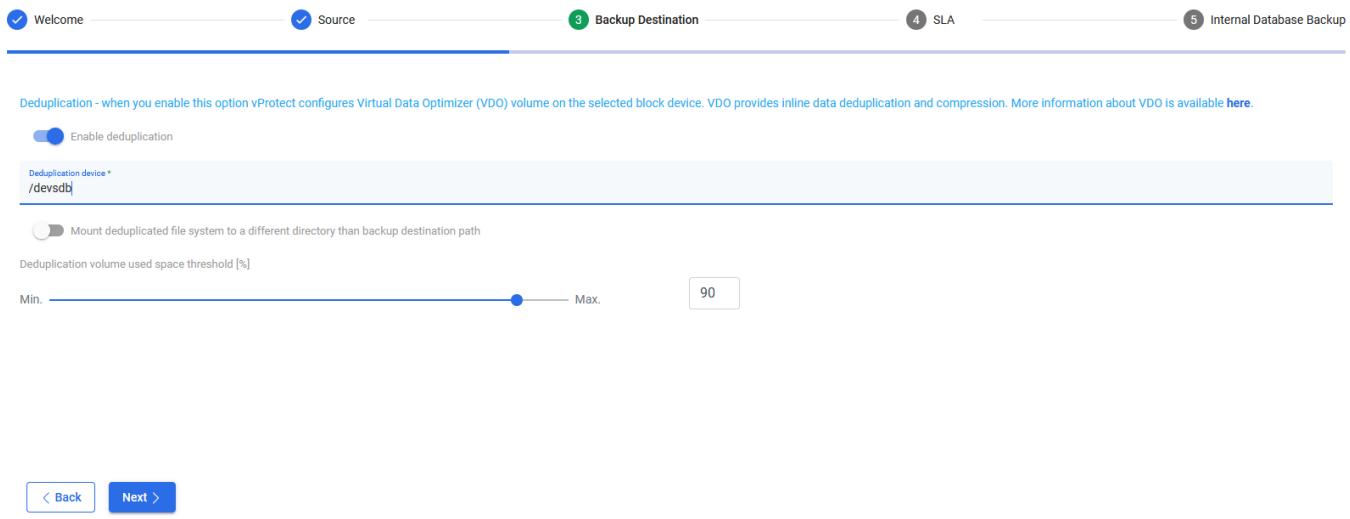
- In the next section, you can add a backup destination. In this case, you can also repeat the whole process so that you can add multiple providers using the wizard.
- Choose a backup destination (we used File System as an example)



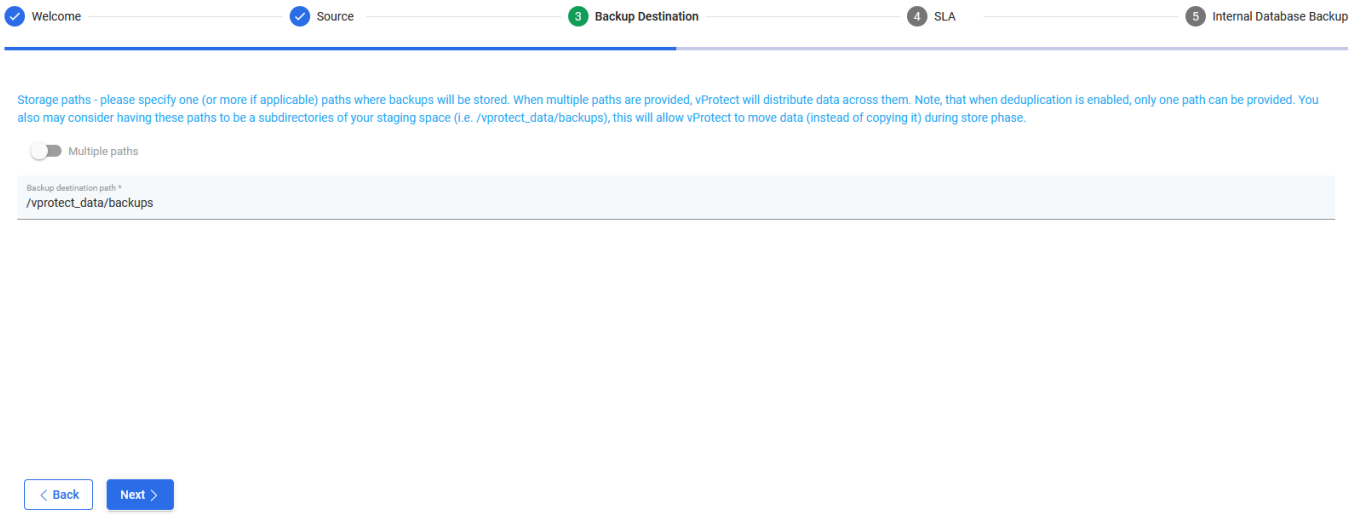
- First, enter a name for your backup destination



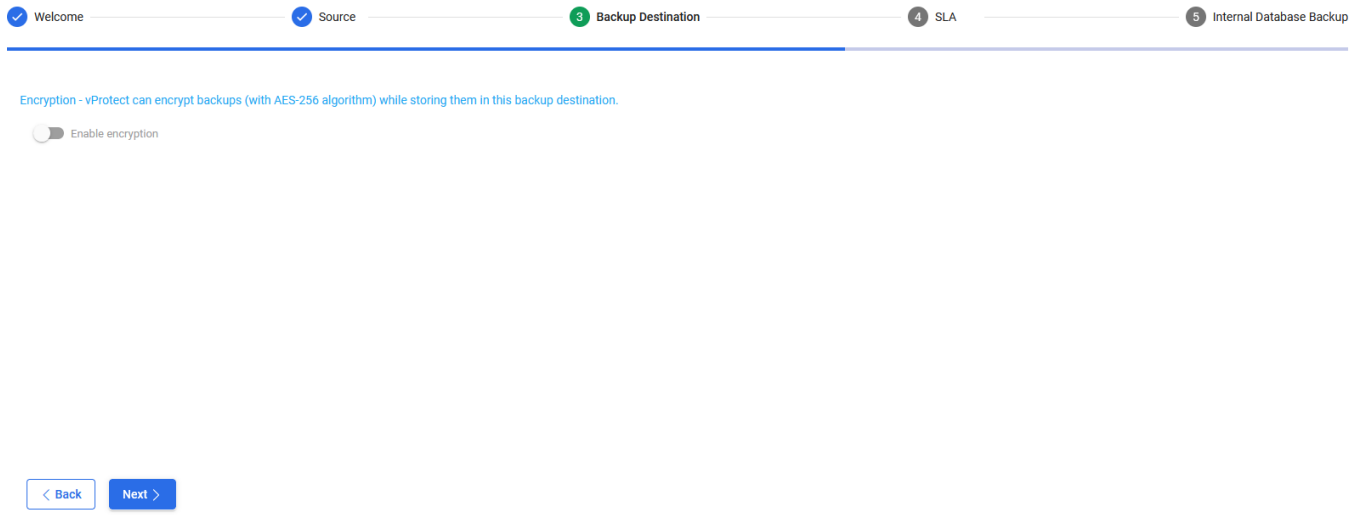
- Choose, if you want to use deduplication based on Virtual Data Optimizer (VDO)



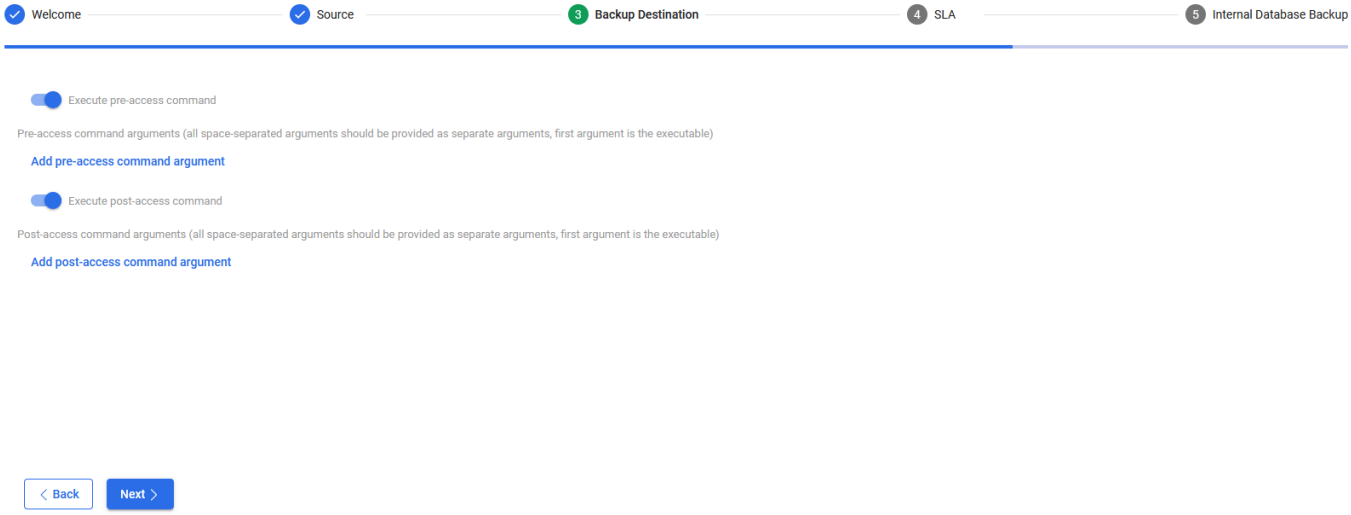
- Set up a storage path, where your data should be stored



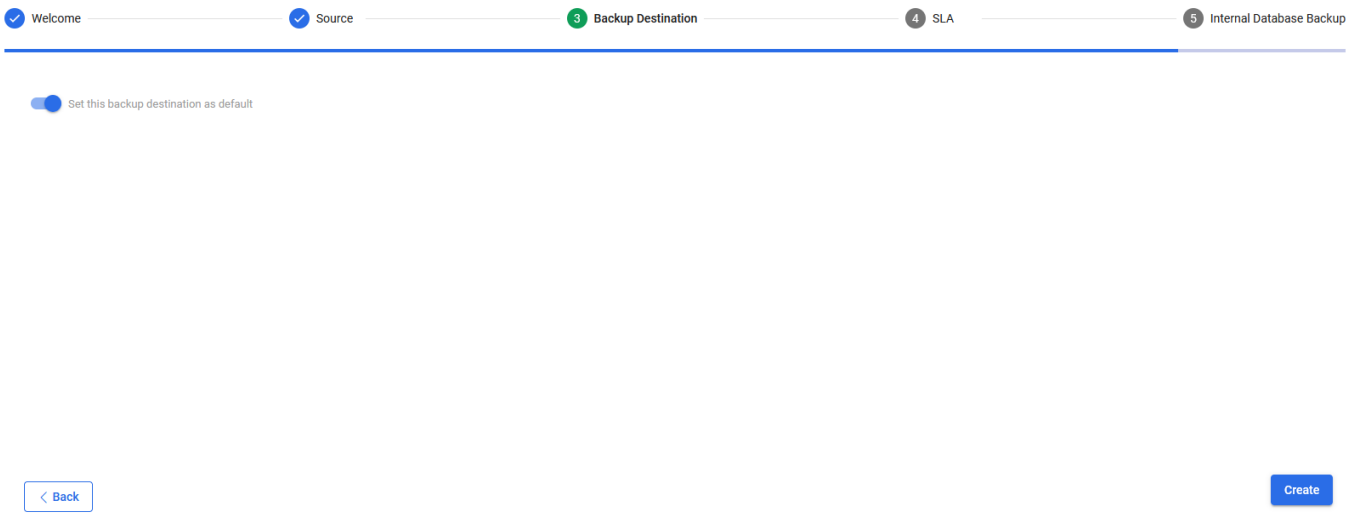
- Optionally you can enable encryption (AES-256 algorithm) - if you enable it, remember that you will not benefit from deduplication.



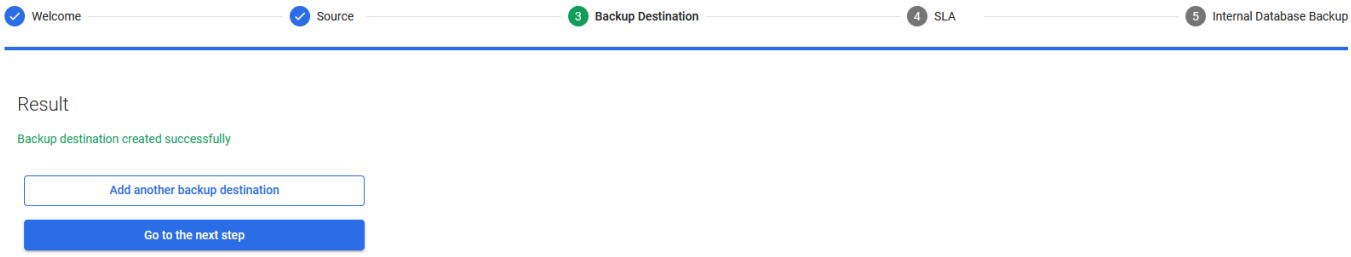
- configuration for pre/post execution command. If you use a File System with VDO, please skip this step.



- Decide if you want to set up this backup destination as the default one.

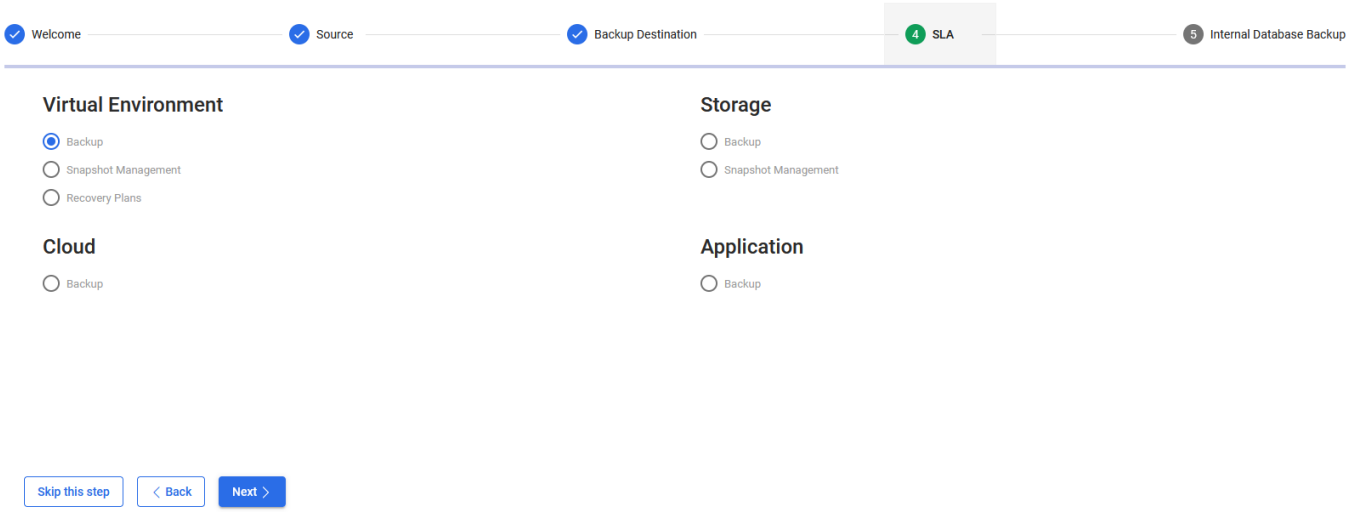


- Finish this step by going to the next section or adding another backup destination



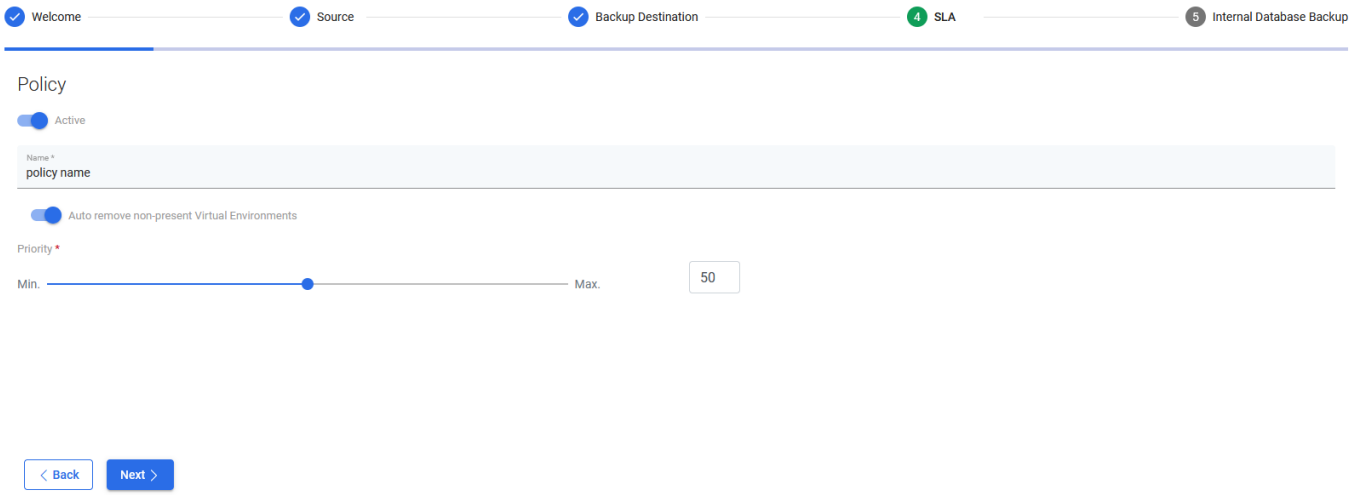
Add SLA

In this example, we will add SLA for Virtual Environment backup.



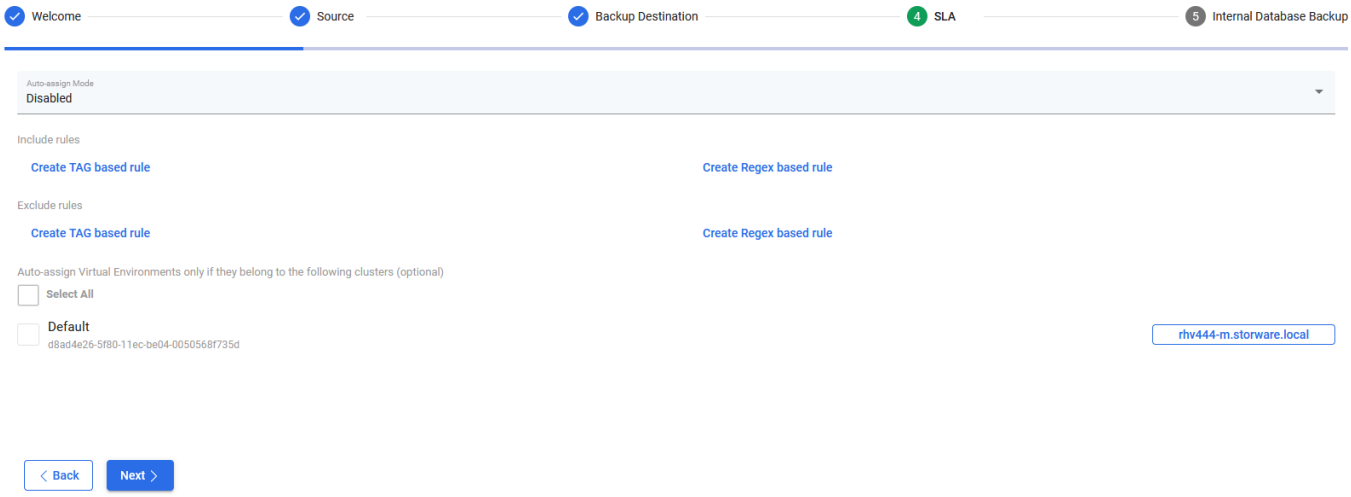
Add policy

- Choose a name for the policy, auto-remove non-present virtual environments (if Data Protector for Cloud Workloads should remove VM from a policy that no longer exists) tick the checkbox, and set the priority

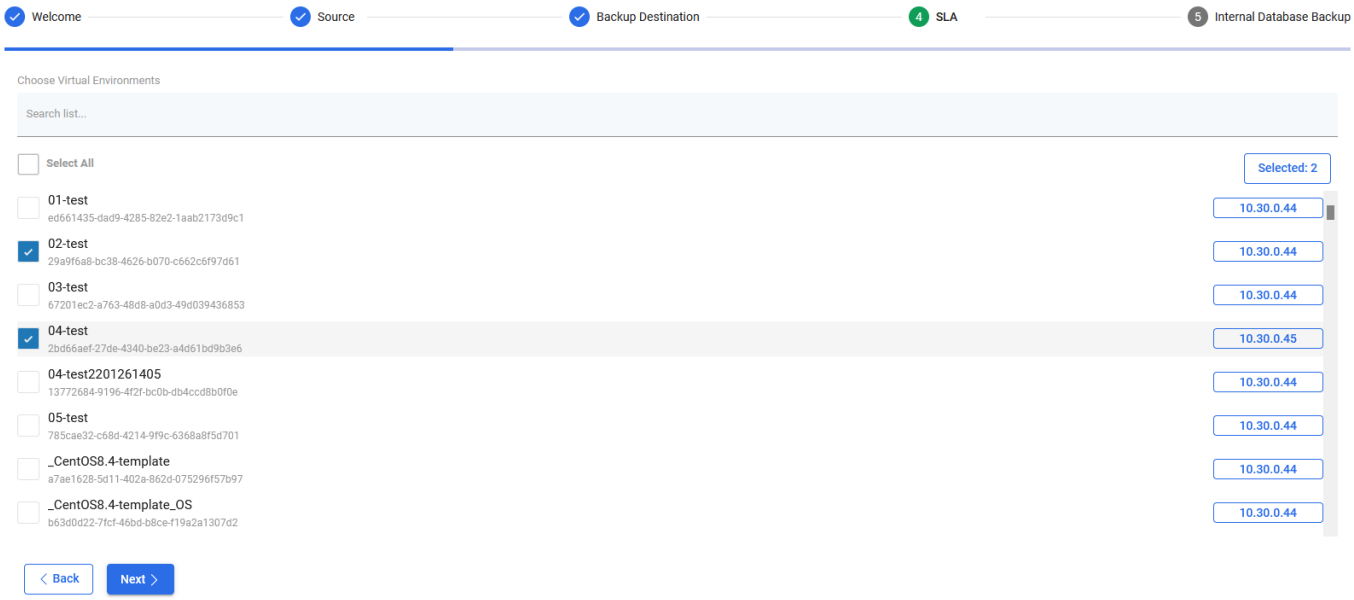


- Choose if you want to use auto assign mode based on tags and regular expressions (matched against the VM name, i.e. `.*` matches all characters 0 or more times)

> **Note:** check the Administration section for details of Backup SLAs to each protected platform

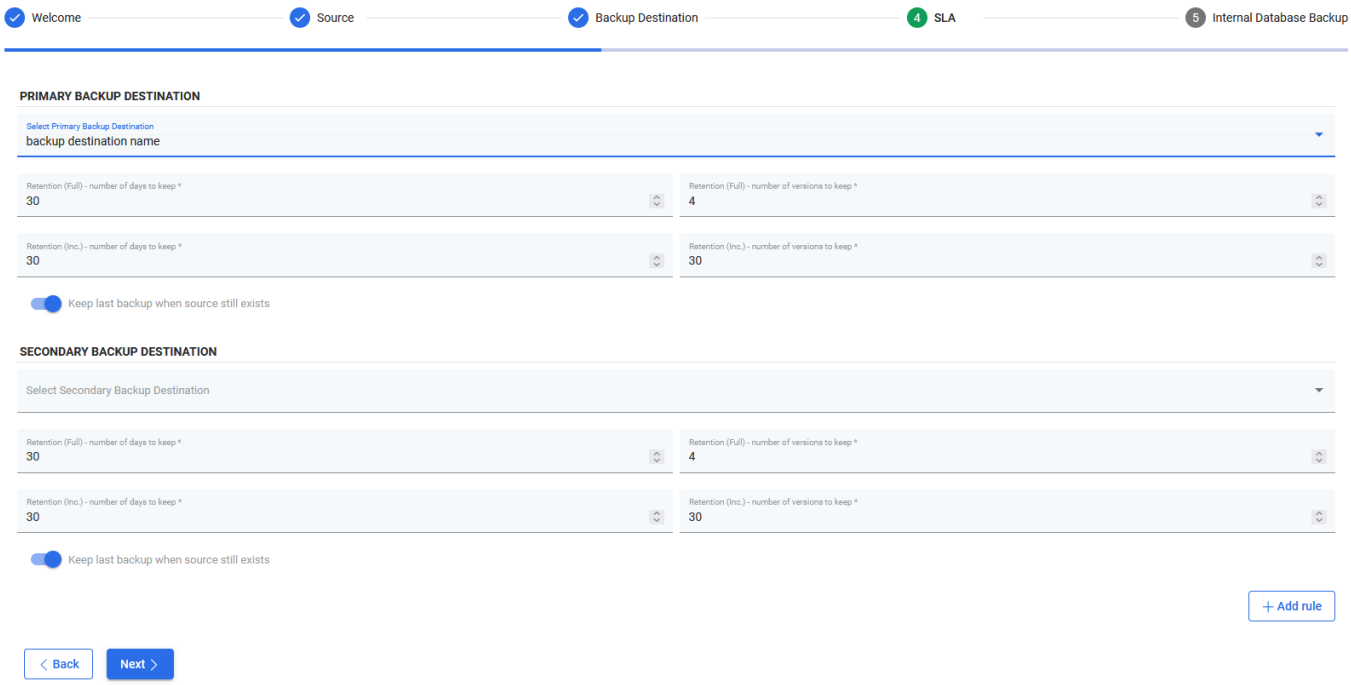


- Manually add the VMs if you do not want to use the auto-assignment mode

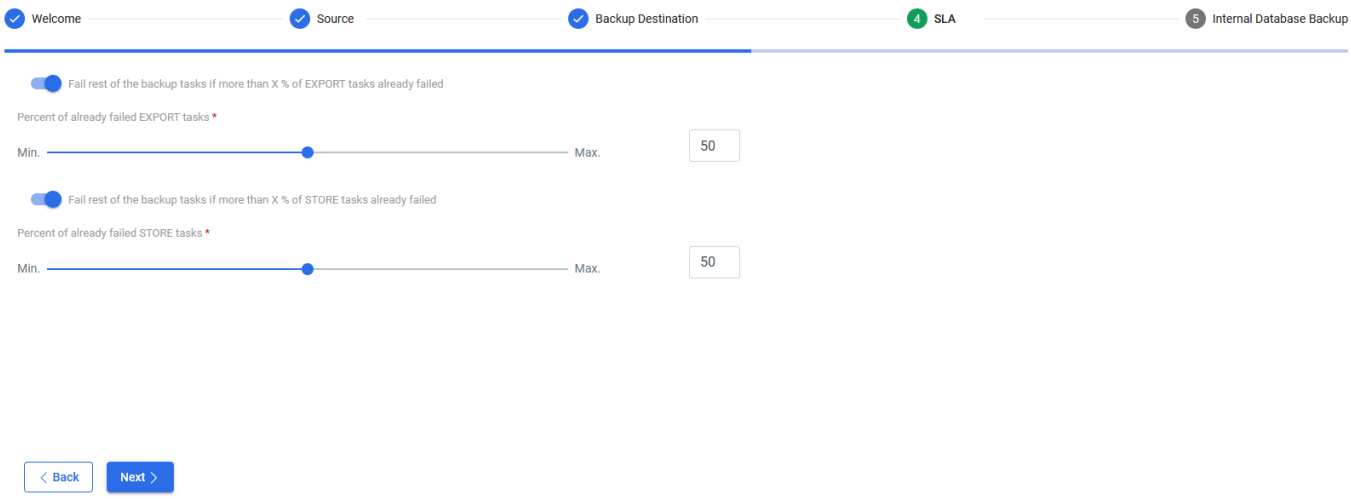


- Choose a backup destination target for this policy

Note: You can now customize retention. Each backup destination has its own retention settings. Whichever condition is met first (either number of versions has been reached or the backup is older than the given limit), it is removed from the backup destination.

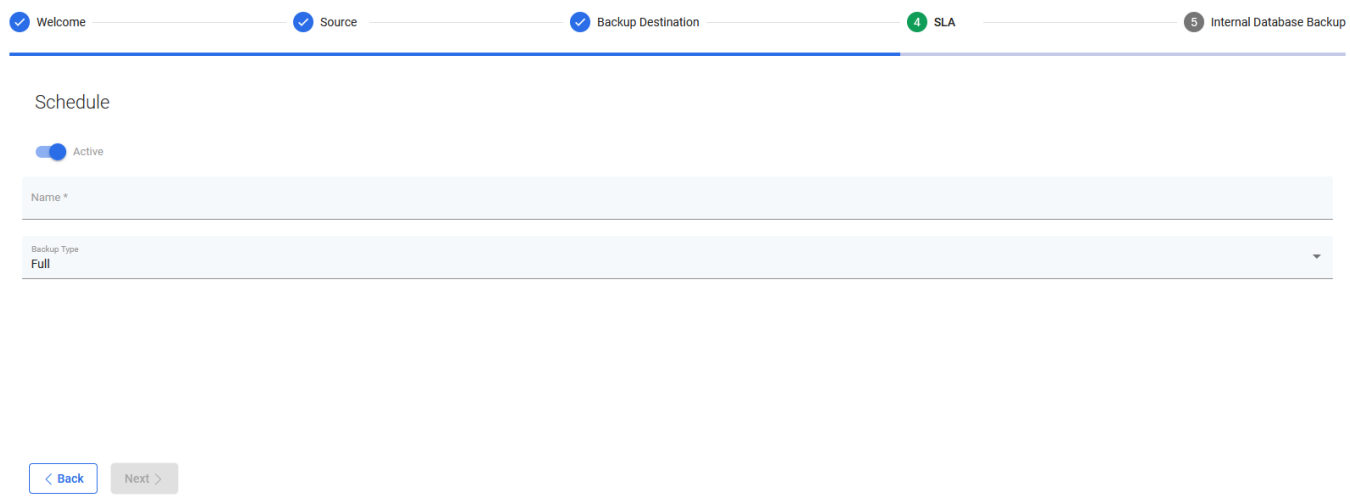


- Set up a threshold - the fail rest of backup tasks if more than X % of EXPORT tasks already failed
- Set up a threshold - fail rest of backup tasks if more than X % of the STORE tasks have already failed

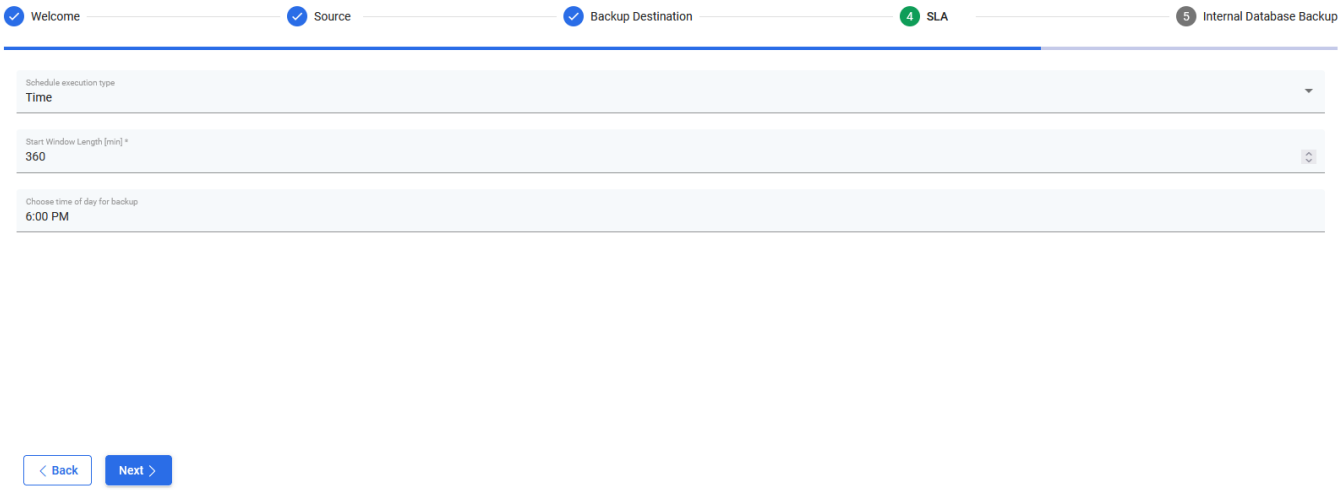


Add schedule

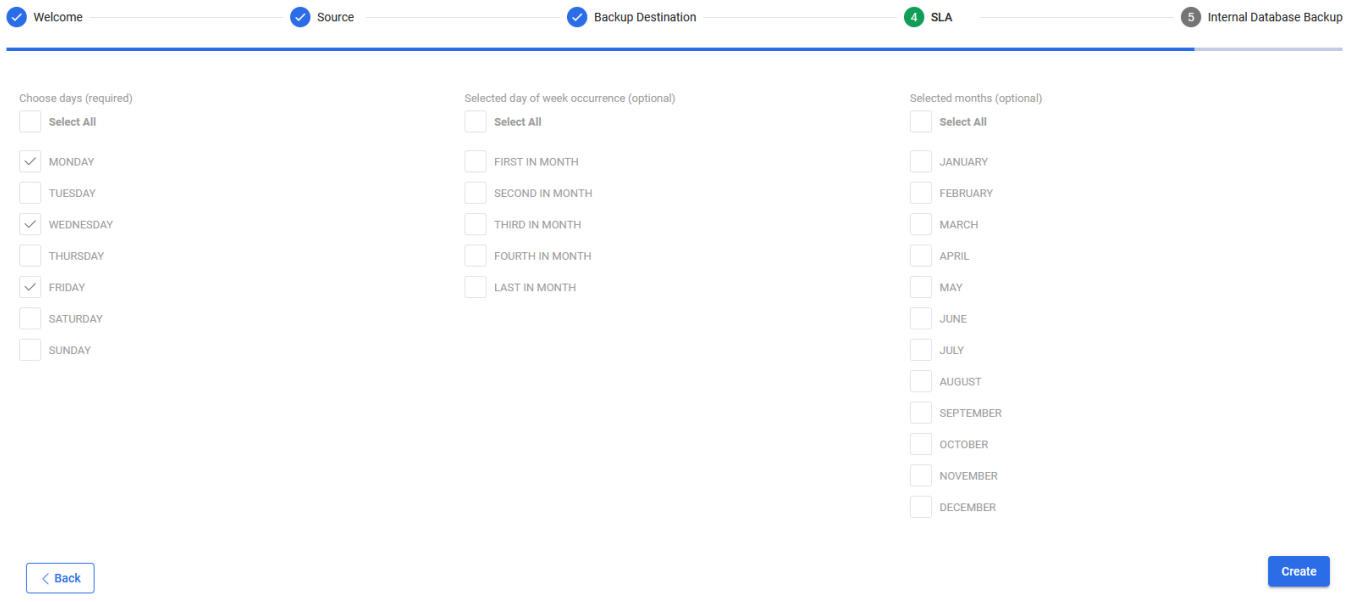
- Choose a name for the schedule and define the type:
    - Full
    - Incremental



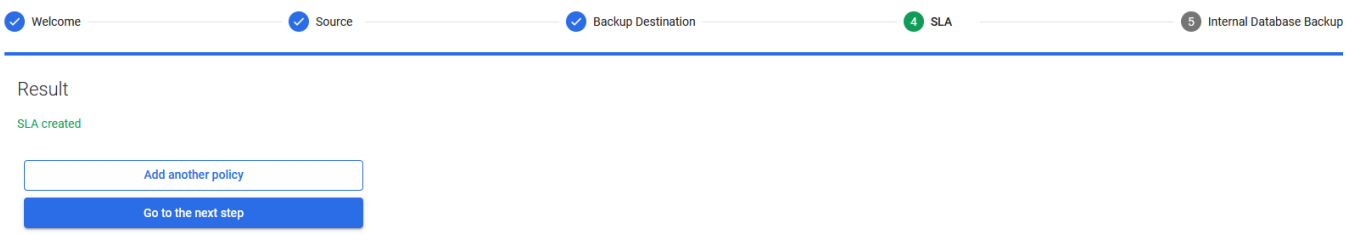
- Define the execution type:
    - time
    - interval
- Define the start window length
- Choose the time of day for backup



- Choose
    - days (required).
    - day of week occurrence (optional)
    - selected months (optional)

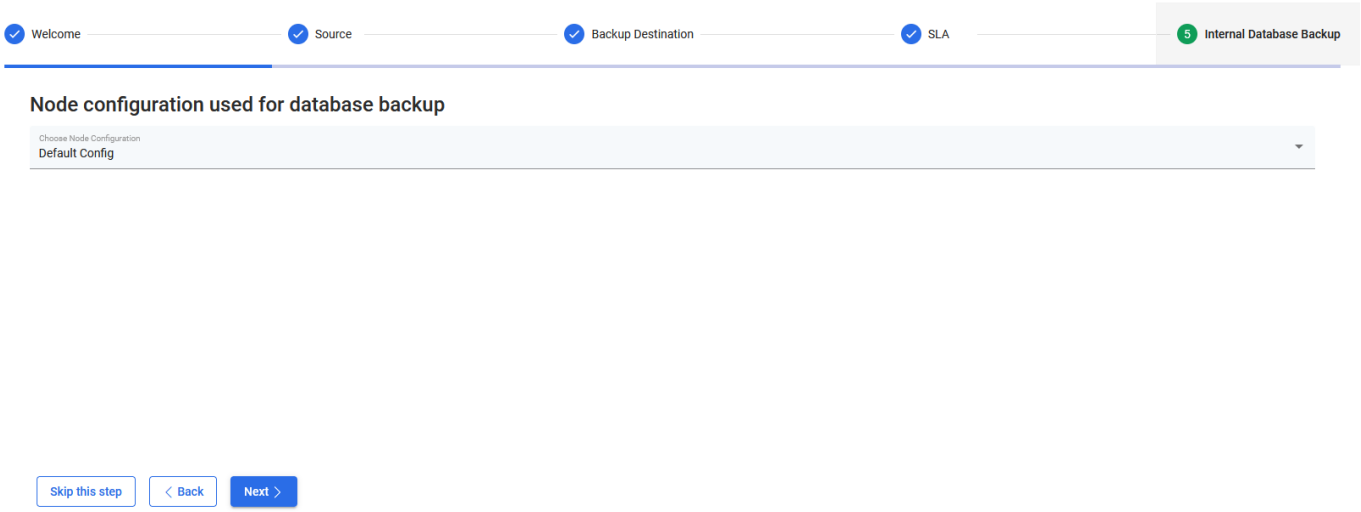


- Finish this step by going to the next section or adding another SLA.

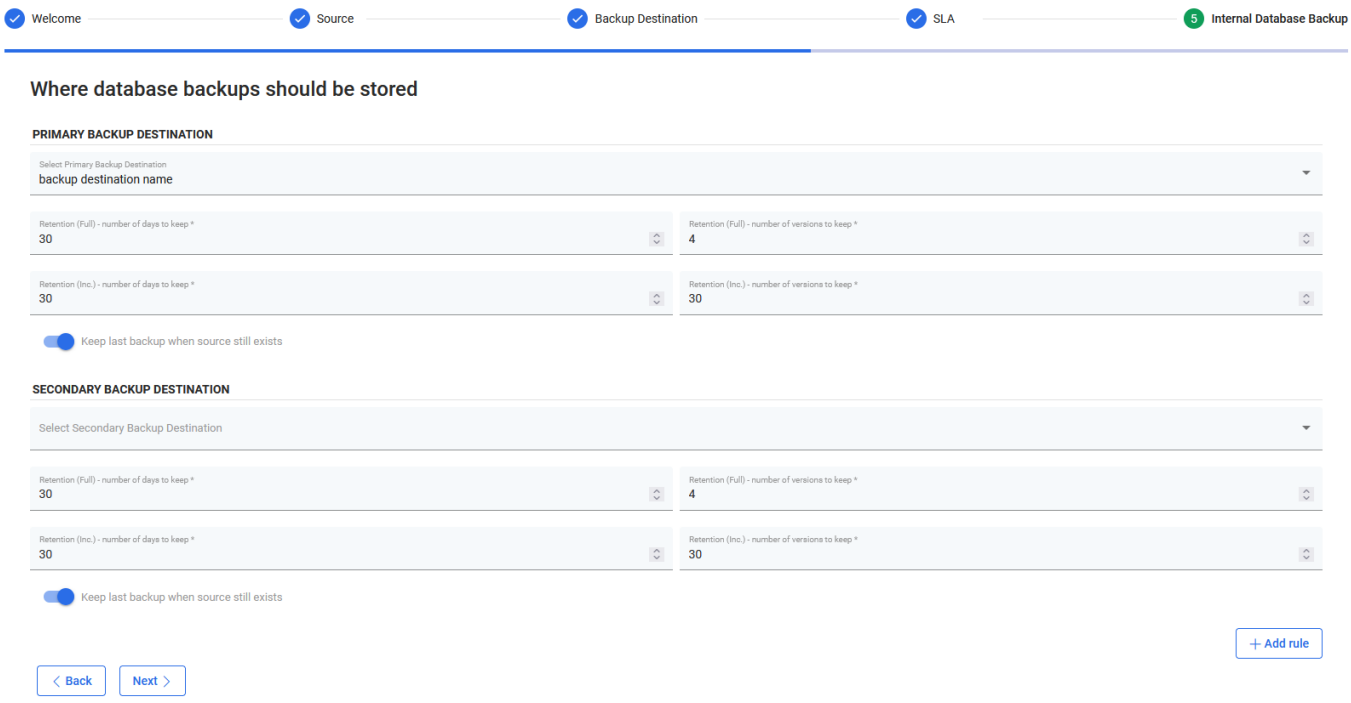


Add internal DB backup

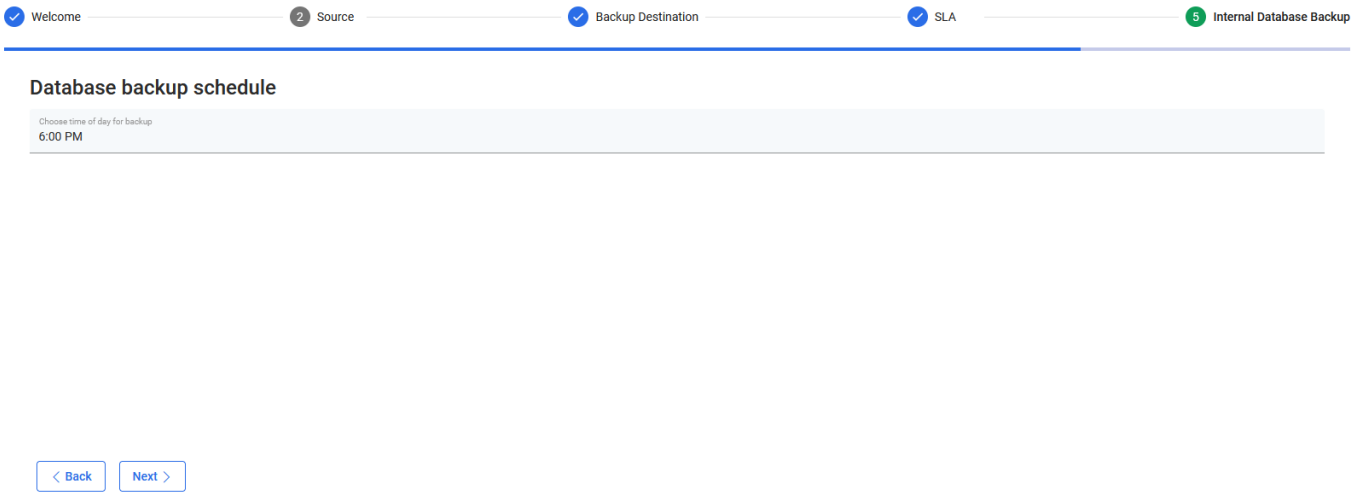
- Choose which node config should be used to perform a Data Protector for Cloud Workloads DB backup



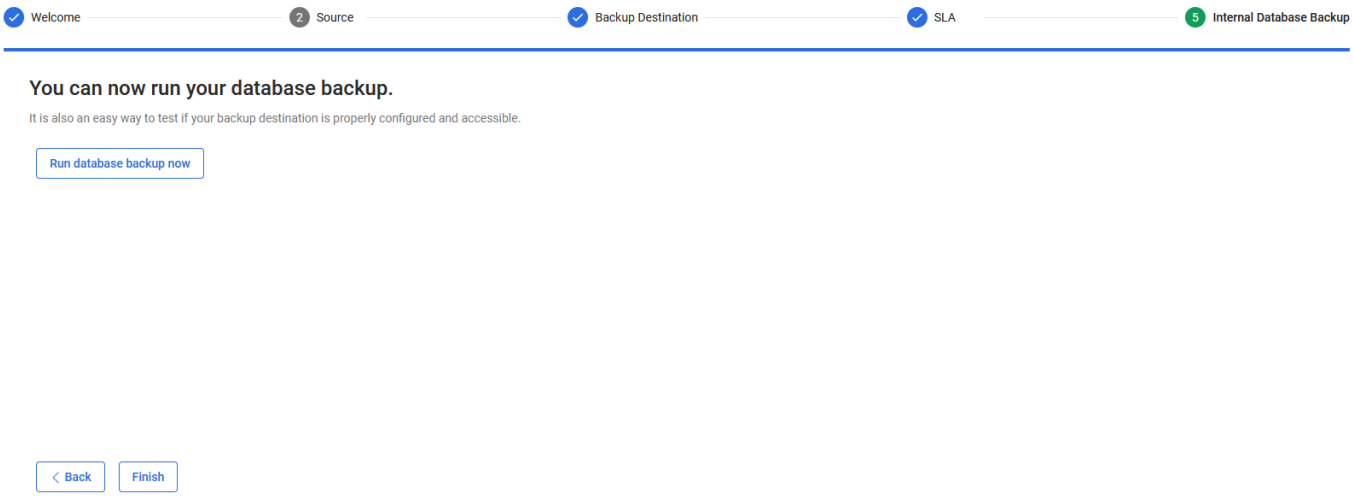
- Choose the backup destination for the DB backup



Choose when the DB backup should be run (daily basis)



- Finalize the configuration and/or run the backup manually (on demand)



- you are ready to go!

Well done!

Now let's launch some backup jobs.

Go back to dashboard

Common tasks

This section presents several supplementary tasks that may be needed in Data Protector for Cloud Workloads deployment. This includes tasks such as HTTPS setup, SSH public key authentication with your hypervisors, VMs or libvirt/qemu package installation.

Staging space configuration

Enabling HTTPS connectivity for nodes

LVM setup on Data Protector for Cloud Workloads Node for disk attachment backup mode

Full versions of libvirt/qemu packages installation

SSH public key authentication

Staging space configuration

General

Data Protector for Cloud Workloads Node needs staging space available in `/vprotect_data` by default. It is common to use PowerProtect DD for both the staging and backup destination. This will result in instant "store" processing, without the need to copy data from the staging space to the backup destinations. It is common to just attach an empty drive and mount it.

When using separate storage (usually local disks) for the staging space, please consider its requirements. Staging space size depends on the number and size of simultaneous backups - as a rule of thumb make it approximately equal to the number of expected simultaneous backup threads multiplied by the size of your biggest VM.

In any case - make sure the staging space is always mounted in the `/vprotect_data` folder, and that the vprotect user is able to have full permissions to this file system.

Example - Local filesystem

You also can use a plain file system for staging space (and optionally for backup destination). Here are steps assuming you have a local (physical or virtual) disk.

- List all existing disks, and find your dedicated disk (let's say - `/dev/sdc`):

```
[root@vProtect01 ~]# fdisk -l | grep dev
Disk /dev/sda: 32.2 GB, 32212254720 bytes, 62914560 sectors
/dev/sda1   *        2048     1026047      512000   83  Linux
/dev/sda2         1026048    62914559    30944256   8e  Linux LVM
Disk /dev/sdc: 500 GB, 17179869184 bytes, 33554432 sectors
Disk /dev/sdb: 21.5 GB, 21474836480 bytes, 41943040 sectors
Disk /dev/mapper/centos-root: 28.5 GB, 28462546944 bytes, 55590912 sectors
Disk /dev/mapper/centos-swap: 3221 MB, 3221225472 bytes, 6291456 sectors
```

- If you have a new clean disk prepare a filesystem on it:

```
mkfs.xfs -K /dev/sdc
```

- Test mount your existing filesystem in the created directory:

```
mount /dev/sdc /vprotect_data
```

- Set ownership to `vprotect` user on directory `/vprotect_data`:

```
chown vprotect:vprotect -R /vprotect_data
```

- Add a line to `/etc/fstab`file, to automatically mount new filesystem after reboot:

```
/dev/sdc    /vprotect_data    xfs    defaults 0 0
```

- Mount

```
mount -a
```

- Confirm with `df` that your `/vprotect_data` is mounted
- Restart your `vprotect-node`service:

```
systemctl restart vprotect-node
```

Enabling HTTPS connectivity for nodes

The default certificate presented by the application server uses `localhost.localdomain`. This works only for local node installations (server and node on a single host).

> **Note:**
>
> - When asked for the certificate/keystore password use: `changeit`.
> - You can use the default certificate - remember that you may need to use the `./node_add_ssl_cert.sh`script after future updates to refresh the certificate on the node
> - For the default certificate - jump to the Node configuration and use the `localhost.localdomain` instead of the `vprotectserver.local`example
> - When registering the node locally over HTTPS please note that the URL you should use is `localhost.localdomain` - **NOT** `localhost`

This section presents the steps necessary for generating an SSL certificate, for setup Data Protector for Cloud Workloads to use it and how to register a remote node.

Data Protector for Cloud Workloads Server (when using own certificate)

This section describes certificate generation and import on the Data Protector for Cloud Workloads Server side. It uses a self-signed certificate. If you would like to use CSR and your own CA instead - please check for additional steps described in the next section.

1. SSH to Data Protector for Cloud Workloads **Server** host
2. Generate the key and certificate (remember to provide a **valid** Data Protector for Cloud Workloads Server DNS hostname - in our example it was `vprotectserver.local`):

```
[root@localhost ~]# openssl req -x509 -newkey rsa:4096 -keyout vprotect.key -out
vprotect.crt -days 365
Generating a 4096 bit RSA private key
.....................................................................+
+
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.............++
writing new private key to 'vprotect.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:PL
State or Province Name (full name) []:
Locality Name (eg, city) [Default City]:Warsaw
Organization Name (eg, company) [Default Company Ltd]: your Company
Organizational Unit Name (eg, section) []:
```

```
Common Name (eg, your name or your server's hostname) []:vprotectserver.local
Email Address []:
```

3. Create the PKCS12 bundle from the certificate and the key:

```
[root@localhost ~]# openssl pkcs12 -export -in vprotect.crt -inkey vprotect.key
-out vprotect.p12 -name vprotect
Enter pass phrase for vprotect.key:
Enter Export Password:
Verifying - Enter Export Password:
```

4. Create a keystore for the Data Protector for Cloud Workloads Server with the PKCS12 bundle:

```
[root@localhost ~]# keytool -importkeystore -destkeystore
/opt/vprotect/keystore.jks -srckeystore vprotect.p12 -srcstoretype PKCS12 -alias
vprotect
Enter destination keystore password:
Re-enter new password:
Enter source keystore password:
```

5. Change ownership on the keystore to the `vprotect` user:

```
chown vprotect:vprotect /opt/vprotect/keystore.jks
```

6. Edit `/opt/vprotect/payara.properties` and change the path to the keystore:
`javax.net.ssl.keyStore=/opt/vprotect/keystore.jks`

7. Restart the Server:

```
systemctl stop vprotect-server
systemctl start vprotect-server
```

8. Make sure that your nodes resolve the hostname of the Data Protector for Cloud Workloads Server. You also can add an entry in the `/etc/hosts` like this (example IP: `1.2.3.4`):

```
1.2.3.4    vprotectserver.local
```

9. Check with your browser that `https://<DP4CW_server_IP>:8181` presents the certificate that you have just generated.
You also can execute the `openssl` client from the node to print it (check the hostname that you have provided in the certificate):

```
openssl s_client -connect vprotectserver.local:8181 < /dev/null
```

Notes on using your own certificate with CSR and your own CA

When using CSR to get a trusted certificate, you need to replace step 2 (self-signed certificate generation) with several steps including CSR generation, and download the CRT signed by your CA. The steps are as follows

1. Generate the CSR - answer the same set of questions as above:`openssl req -new -newkey rsa:2048 -nodes -keyout vprotect.key -out vprotect.csr`
2. Send your CSR and have it signed by your CA
3. Download your CRT file and save it as `vprotect.crt`(note that you should have your working directory set to`/opt/vprotect`)
4. Download your CA certificate chain (for example for a single`ca.crt`)and import it with the `CA_ALIAS` of your choice as follows:`keytool -import -trustcacerts -keystore /usr/lib/jvm/jre/lib/security/cacerts -storepass changeit -noprompt -alias CA_ALIAS -file ca.crt`
5. Now continue from PKCS12 bundle generation (step 3 in the section above).

Data Protector for Cloud Workloads Node (any SSL certificate)

1. SSH to **Data Protector for Cloud Workloads Node** host
2. Import the server certificate using the script under the `/opt/vprotect/scripts` folder:

```
cd /opt/vprotect/scripts
./node_add_ssl_cert.sh [SERVER_HOST] [PORT] [KEYSTORE_PASS]
```

where the defaults (if arguments have not been provided) are `SERVER_HOST` = `127.0.0.1`, `PORT` = `8181`, `KEYSTORE_PASS` = `changeit` (default java keystore password), examples:

- Default local installation (Server and Node on the same host):

```
./node_add_ssl_cert.sh
```

- Remote Server on the custom port:

```
./node_add_ssl_cert.sh vprotectserver.local 8181
```

3. Register the node with the `NODE_NAME` of your choice, the `ADMIN_USER` user name which you would like to use and the URL to Data Protector for Cloud Workloads API, and provide the password when prompted:

- Syntax:

```
vprotect node -r NODE_NAME ADMIN_USER http(s)://<DP4CW_server_IP>:PORT/api
```

- Remote server with a generated certificate:

```
vprotect node -r node1 admin https://vprotectserver.local:8181/api
```

- Local installation with default certificate:

```
vprotect node -r node1 admin https://localhost.localdomain:8181/api
```

LVM setup on Data Protector for Cloud Workloads Node for disk attachment backup mode

> **Note:** This is required for **Nutanix** and **RHV v4 API** (when using disk attachment mode)

Data Protector for Cloud Workloads Node attaches VM disks that potentially are clones of its own (i.e. if Node deployed from the template) - you need to configure LVM on the Node so that it doesn't scan for LVM volumes where disks are being attached.

1. Set the following variables in `/etc/lvm/lvm.conf` - so that only system volumes are being detected by LVM daemon (in this example sda disk with 2 partitions - sda1 and sda2):

   ```
   filter = [ "a|^/dev/sda|", "a|^/dev/sda1|", "a|^/dev/sda2|", "r|.*|" ]
   global_filter = [ "a|^/dev/sda|", "a|^/dev/sda1|", "a|^/dev/sda2|", "r|.*|" ]
   ```

2. Check with `vgscan -vvv` that your OS volumes are still being detected:

   ```
   Allocated VG vg_vprotect at 0x55914f19fac0.
   Importing logical volume vg_vprotect/lv_root.
   Importing logical volume vg_vprotect/lv_swap.
   ```

3. Reboot:

   ```
   reboot
   ```

Full versions of libvirt/qemu packages installation

Please make sure that your `libvirt` supports the `virsh blockcommit` operation. CentOS distribution requires you to install the full `libvirt` and `qemu-img` from the `oVirt` repository. This can be done like this:

1. Install oVirt repo:

```
yum install http://resources.ovirt.org/pub/yum-repo/ovirt-release42.rpm -y
```

2. Update the packages

```
yum update -y
```

which should replace `qemu` related packages with full versions from the oVirt repo.

SSH public key authentication

General

Instead of using password authentication - anywhere where you're able to provide SSH credentials (hypervisors, VMs applications, etc) you also have the public key alternative.**.
By default, Data Protector for Cloud Workloads uses the `/opt/vprotect/.ssh/id_rsa` path, however, you also can override it with your own path*.
***(this needs to be owned by `vprotect` user and make sure it has the `0400` permission set.**
****You don't have to pass a passphrase, you can leave this parameter blank.**

> **Note:** Data Protector for Cloud Workloads does not support keys other than "RSA"

Example

1. Generate a key or use yours and store it as `/opt/vprotect/.ssh/id_rsa` (make sure that the `vprotect` user and group own the file)

- example key generation:

```
[root@vProtect3 vprotect]# sudo -u vprotect ssh-keygen -t rsa -m PEM
Generating public/private rsa key pair.
Enter file in which to save the key (/opt/vprotect/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /opt/vprotect/.ssh/id_rsa.
Your public key has been saved in /opt/vprotect/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:86HSLKYwl7maDR7U1oIH1Y6VDtRFNJgHgfdjikg3VnQ vprotect@vProtect3
The key's randomart image is:
+---[RSA 2048]----+
|    .o=+XE       |
|    .o X...      |
|   .  O o        |
|   .+=.o +       |
|  .o+=o.oS..     |
|  ..o.+.o + .    |
|   = + + + .     |
|  . O + o        |
|   +.+           |
+----[SHA256]-----+
```

2. Use `ssh-copy-id` to upload your public key (as `vprotect` user) to the KVM host:

```
sudo -u vprotect ssh-copy-id -i /opt/vprotect/.ssh/id_rsa.pub root@HYPERVISOR
```

3. Check if you're able to log in to the hypervisor using the local `vprotect` user without being asked for the password:

```
[root@vProtect3]# sudo -u vprotect ssh -i /opt/vprotect/.ssh/id_rsa root@dkvm
Last failed login: Mon Jan 29 17:53:01 CET 2018 from 10.50.1.107 on ssh:notty
There was 1 failed login attempt since the last successful login.
```

```
Last login: Mon Jan 29 17:52:39 2018 from 10.50.1.107
[root@dKVM ~]# logout
```

4. Now you should be able to index VMs regardless of the password set for the hypervisor (the key should be used instead)

5. Provide path to key (default: /opt/vprotect/.ssh/id_rsa) in Data Protector for Cloud Workloads dashboard

Protecting Virtual Environments

Data Protector for Cloud Workloads supports multiple on-premise virtualization platforms. In this section, you will find what backup methods are supported and the specific steps that are needed for each of them to be integrated with Data Protector for Cloud Workloads.

- Virtual Machines
- Cloud
- Containers
- Backup & Restore

Virtual Machines

In this chapter, You will know how to add and protect your Virtual Machines such as:

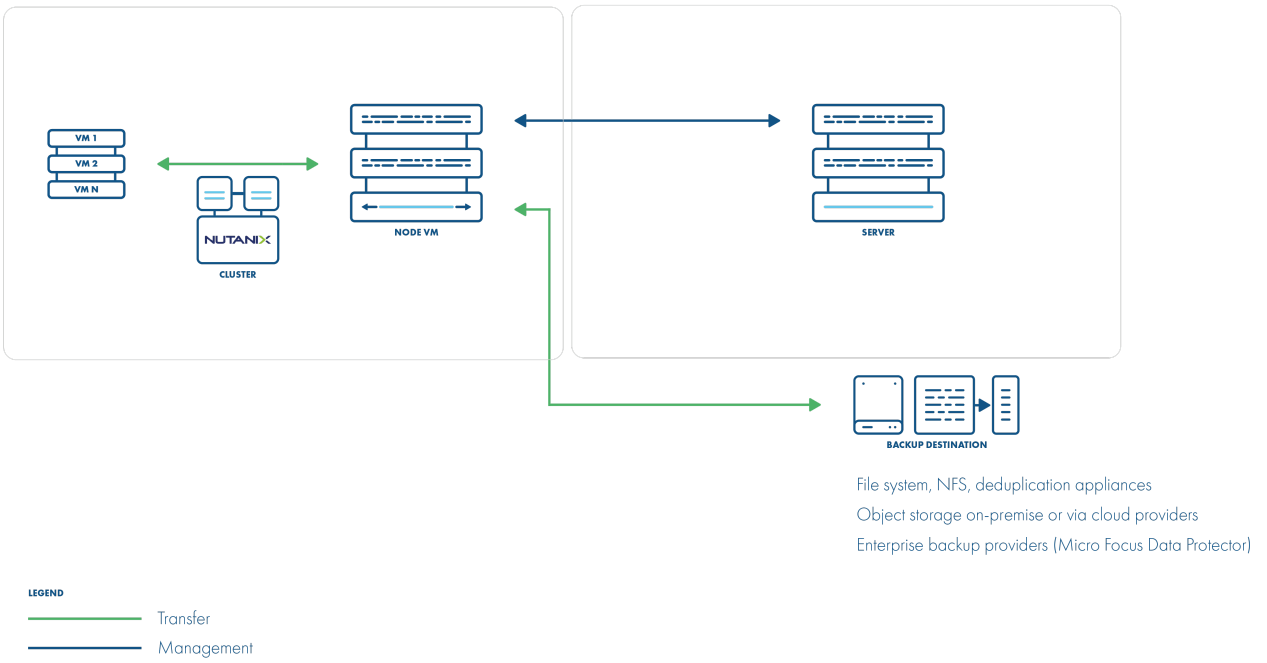
- Nutanix Acropolis Hypervisor (AHV)
- Red Hat Virtualization
- oVirt
- Oracle Linux Virtualization Manager
- Oracle VM
- Proxmox VE
- KVM/Xen
- OpenStack
- Citrix Hypervisor (XenServer)
- XCP-ng
- Huawei FusionCompute
- Scale Computing HC3

Nutanix Acropolis Hypervisor (AHV)

General

Data Protector for Cloud Workloads supports the Nutanix AHV platform by using a VM called “Proxy VM”. The node invokes commands on your hypervisor manager to snapshot and attach drives of a specific VM to itself (Proxy VM). The proxy VM is able to read the data from the attached disk snapshots and forward them to the backup provider.

This strategy allows you to exclude drives from a backup that you do not need. Remember that you need to install at least 1 Proxy VM per cluster so that the drives the node tries to attach are reachable.



Backup Process

- crash-consistent snapshot using hypervisor's API
- optionally application-consistent snapshot can be done if enabled and guest tools installed inside - the type of snapshot is selected based on is QuiesceBeforeSnapshot setting and passed as part of the snap request. The created snapshot might end up being of a different type (depending on the _**_presence of tools
- optional application consistency using pre/post snapshot command execution
- metadata exported from API
- snapshot disks are mounted one by one to the Proxy VM
- data read directly on the Proxy VM
- incremental backups using CBT API - only changed blocks are read from the attached disk
- the last snapshot kept on the hypervisor for the next incremental backup (if at least one schedule assigned to the VM has the backup type set to incremental)
- restore creates empty disks on the Proxy VM, imports merged data then recreates VM and reattaches volumes to the target VM

A general explanation of "The dynamically attached disks slot offset" parameter for Data Protector for Cloud Workloads Node proxy VM

Our best practice is to use a proxy machine with one disk device for the purposes of the operating system if you are using the "Disk attachment" backup strategy. Due to the simplification of the configuration of the environment, we also

do not achieve any benefits for this element of the environment.

Our experience shows that after adding a new node to the environment, is good to perform a test backup and check the logs from which disk device Data Protector for Cloud Workloads Node want to start the backup. Depending on the proxy virtual machine configuration, Data Protector for Cloud Workloads will select the appropriate disk or you need to manually set the offset parameter. Rather, we do not encounter this type of situation when a virtual machine has only one disk device.

Recommendations on how to set up the environment for Data Protector for Cloud Workloads

- As the backup strategy for the Nutanix environment depends on attaching and detaching disk devices to Proxy VM, we recommend simplifying the hardware configuration of this machine. If your backup destination allows having staging space on the same storage as the backup destination, one disk device should be sufficient for the proxy virtual machine's operating system purposes.
- If it is not possible to have only one disk device for Proxy VM, please read the Example section. We explained what you need to do to make sure your Data Protector for Cloud Workloads backups are good.
- If your backup destination requires that Proxy VM need to have staging space on a local disk device, then Staging space must be on a volume coming from container storage. Otherwise, Data Protector for Cloud Workloads may select the wrong device during backup.
- Our recommendation is also to configure LVM filters on Proxy VM. You need to add all OS disks and partitions, please follow these steps: LVM setup on Data Protector for Cloud Workloads Node for disk attachment backup mode

Things to Know About "How to Add Nutanix Hypervisor Manager to Data Protector for Cloud Workloads"

- When adding Nutanix hypervisor managers use a URL similar to the following:

```
https://PRISM_HOST:9440/api/nutanix/v3
```

- Nutanix environments require the Data Protector for Cloud Workloads Node to be installed in one of the VMs residing on the Nutanix cluster. Data Protector for Cloud Workloads should automatically detect the VM with the Data Protector for Cloud Workloads Node during the inventory synchronization operation.
- Data Protector for Cloud Workloads requires that there be a user with "cluster-admin" privileges on Prism, to process the backup/restore job.
- You can specify either a Prism Element or a Prism Central as hypervisor manager. If Prism Central is specified credentials for Prism Central and each Prism Element must be the same.
- Hypervisor tags are supported only with Prism Central
- Volume groups attached to the VMs are not affected by snapshot, hence neither backup nor snapshot revert on such volumes is going to include them.

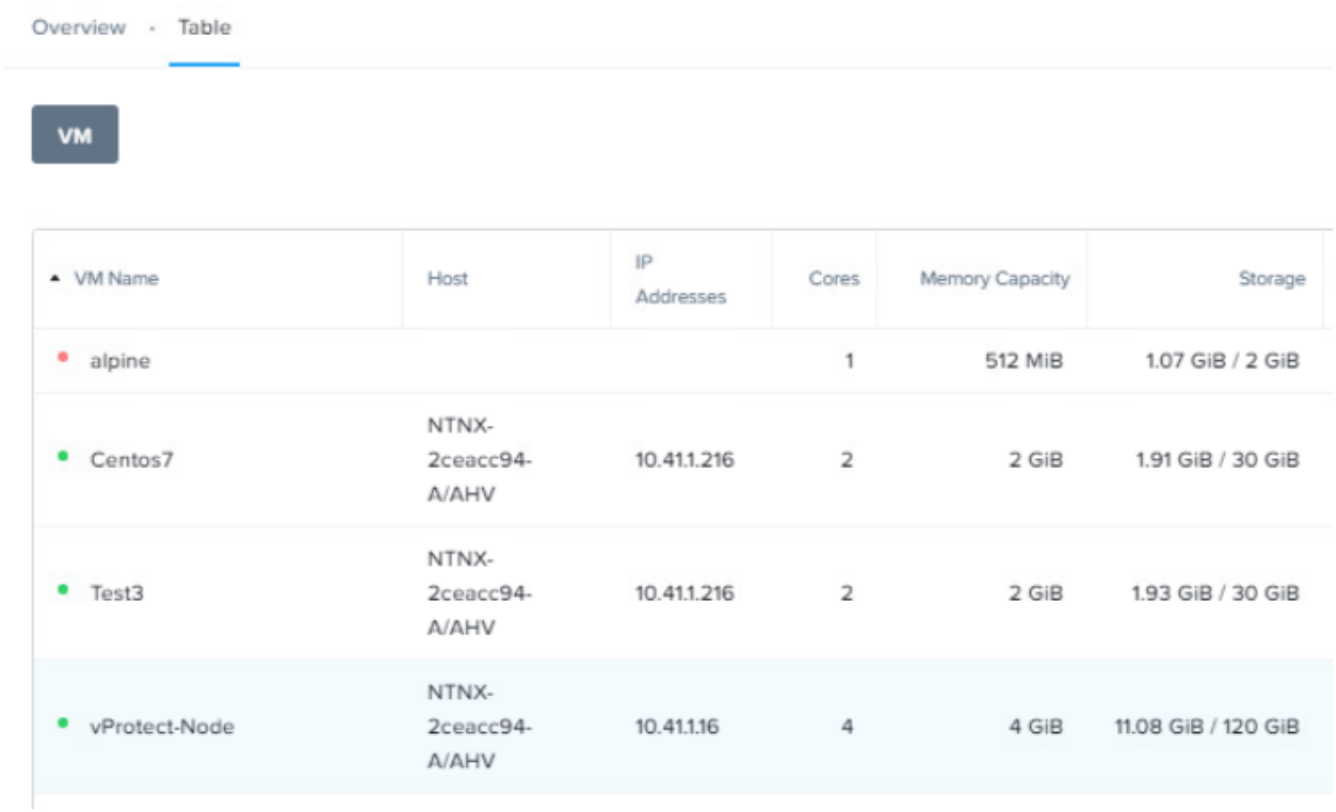
You can deploy more nodes in each cluster and map individual hypervisors to them:

- This should statically load balance jobs based on a hypervisor
- Each node will handle VMs that reside on the particular hypervisor (which because of data locality may be faster than backup of VMs from other hosts
- VMs that don't have hypervisor assigned are handled by the node from the hypervisor manager
- Each node needs to run inventory synchronization to record its Proxy VM UUID on which it is installed

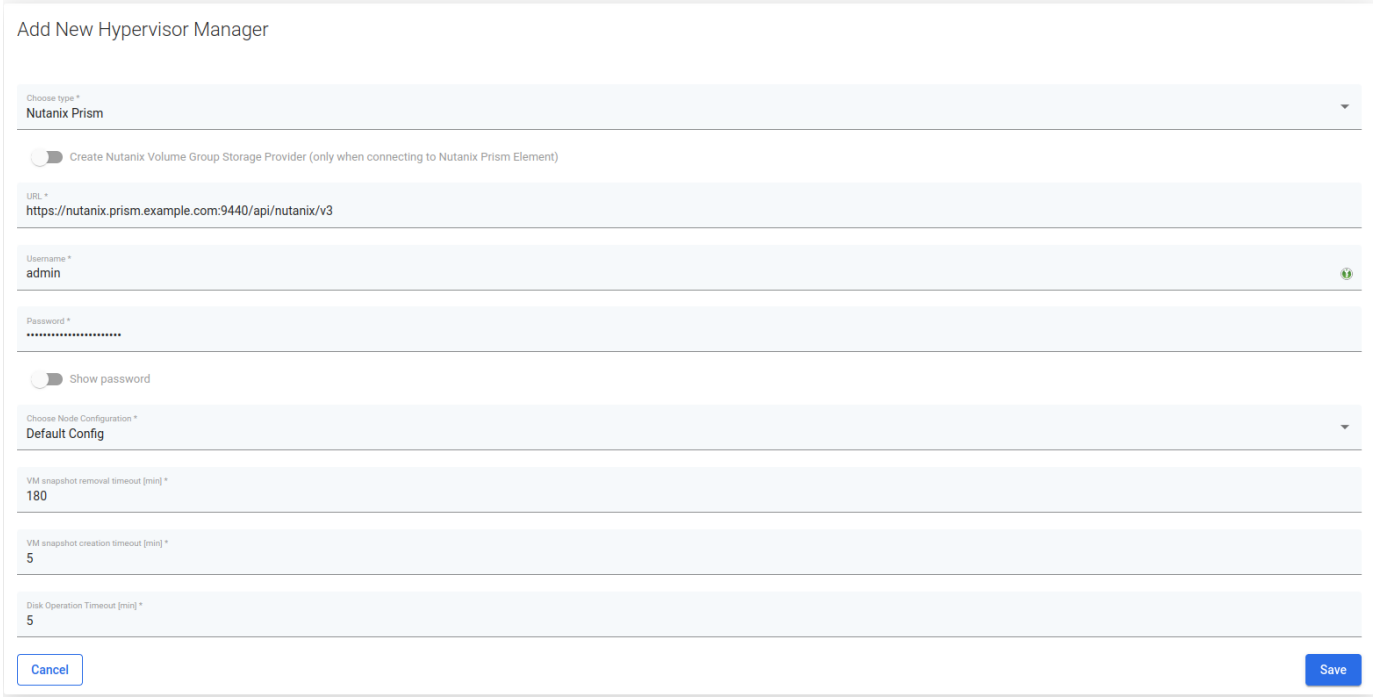
Example

How to start back up for Nutanix AHV Hypervisor

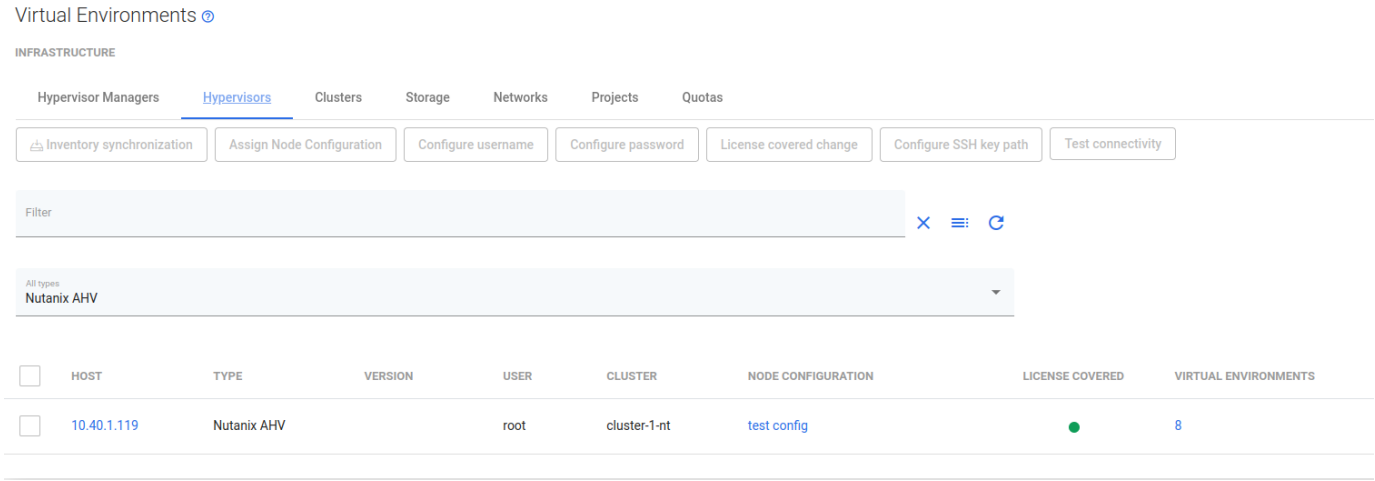
- Create Proxy VM into Nutanix cluster (with one of the supported OS: Platform Requirements)



- Install Data Protector for Cloud Workloads Node (How to install Data Protector for Cloud Workloads Node installation by RPM)
- Login to Data Protector for Cloud Workloads Dashboard and add hypervisor manager *Remember that if you add prism central all credentials must be the same (for prism elements and prism central)*



- Run inventory synchronization task, after that you should see all Nutanix hosts under the hypervisor tab

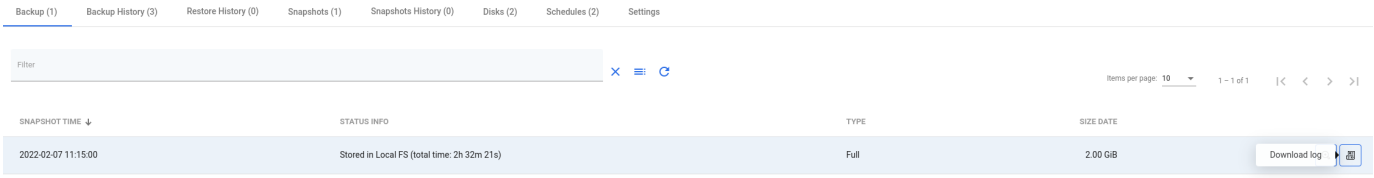


- As we describe above, we can back up Nutanix VMs thanks to the disk attachment backup strategy. As this is one of the most demanding methods, at this point we recommend that you perform a few easy tests to make sure that the backup you are going to perform is correct.
- Please connect via SSH to the Proxy VM. Enter "lsblk" to check the disk devices that belong to the machine. In this example, we have two disk devices:
    - 1. /dev/sda - with three partitions /dev/sda1, /dev/sda2, /dev/sda3
    - 2. /dev/sdb - with one partition /dev/sdb1

  This information will be needed for the next steps: configuring the lvm filter and checking if we need to correct the value of the parameter "dynamically disk attachment offset".

```
[root@vmnutanix ~]# lsblk
NAME        MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda           8:0    0   20G  0 disk
├─sda1        8:1    0  600M  0 part /boot/efi
├─sda2        8:2    0    1G  0 part /boot
└─sda3        8:3    0 18.4G  0 part
  ├─cl-root 253:0    0 16.5G  0 lvm  /
  └─cl-swap 253:1    0    2G  0 lvm  [SWAP]
sdb           8:16   0  100G  0 disk
└─sdb1        8:17   0  100G  0 part /vprotect_data
sr0          11:0    1 1024M  0 rom
[root@vmnutanix ~]#
```

- We'll start by configuring the lvm filter.
    - Global article about LVM: LVM setup manual
    - Remember to reboot VM after changes
    - Remember that the structure of this file is important and you need to put the filter lines back in their original place. Open in a text editor `/etc/lvm/lvm.conf` uncomment and replace the line: `filter = [ "a|.*|" ]` to `filter = [ "a|^/dev/sda|", "a|^/dev/sda1|", "a|^/dev/sda2|", "a|^/dev/sda3|", "a|^/dev/sdb|", "a|^/dev/sdb1|", "r|.|" ]` **and** `global_filter = [ "a|.*|" ]` **to** `global_filter = [ "a|^/dev/sda|", "a|^/dev/sda1|", "a|^/dev/sda2|", "a|^/dev/sda3|", "a|^/dev/sdb|", "a|^/dev/sdb1|", "r|.|" ]`
- Now we can move on to the "dynamically disk attachment offset" tests. *You need to do this only if Proxy VM has more than one disk device for OS purposes*
    - Switch Data Protector for Cloud Workloads Node logs (Proxy VM) to Debug mode: How to Enable Debug mode
    - Run a test backup - try to choose a small VM to not wait too long
    - After the backup is complete, download the log file from our dashboard



- As we can see in the logs, we do not need to correct the "offset" value. Data Protector for Cloud Workloads wants to start a backup from /dev/sdc, which is correct behavior because this disk device does not belong to Proxy VM.

```
[2021-04-08 14:51:40.959] INFO [Thread-47] IProxyVmProvider.waitForDevice:38
[ffc65c30-8952-4ffa-b5d5-eefcfe01f333] Checking if device '/dev/sdc' is  present...

[2021-04-08 14:51:45.959] DEBUG [Thread-47] CommandExecutor.exec:75
[ffc65c30-8952-4ffa-b5d5-eefcfe01f333] Exec: [lsblk, -l, /dev/sdc]

[2021-04-08 14:51:45.969] DEBUG [Thread-47] CommandExecutor.exec:102
[ffc65c30-8952-4ffa-b5d5-eefcfe01f333] [lsblk, -l, /dev/sdc]
Return code: 0
output:
[NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
sdc    8:32   0  20G  0 disk
sdc1   8:33   0   1G  0 part
sdc2   8:34   0  19G  0 part
]
error:
[]

[2021-04-08 14:51:45.970] INFO [Thread-47] IProxyVmProvider.waitForDevice:45
[ffc65c30-8952-4ffa-b5d5-eefcfe01f333] Device '/dev/sdc' is present

[2021-04-08 14:51:55.991] INFO [Thread-47] NutanixHypervisorManager.exportData:895
[ffc65c30-8952-4ffa-b5d5-eefcfe01f333] Data export of scsi.0
(917a15a2-5815-4d20-b693-6fb77ea59293)[20 GiB]: '/dev/sdc' ->
'/vprotect_data/vProtect-node__fb96db59/scsi.0.raw'...
```

- If you meet with a situation, when Data Protector for Cloud Workloads want to back up its own disk device, please read our knowledge base article: KB10037 How to change "Dynamically attached disks slot offset" parameter

Red Hat Virtualization

General

For RHV 4+ environments you can use API v4 for invoking all backup-related tasks.

Import/export mode defines the way the backups and restores are done. Red Hat Virtualization (with API v4) supports 4 modes:

1. **Disk attachment**, which exports VM metadata (in OVF format) with separate disk files (in RAW format) via the Proxy VM with the Node installed.
    - supports RHV 4.0+
    - no incremental backup
    - proxy VM required in each cluster - used for the disk attachment process
2. **Disk image transfer**, which exports VM metadata (in OVF format) with disk snapshot chains as separate files (QCOW2 format):
    - supports RHV 4.2+/oVirt 4.2.3+
    - supports incremental backup
    - disk images are transferred directly from API (no Proxy VM required)
3. **SSH Transfer,** this method assumes that all data transfers are directly from the hypervisor - over SSH
4. **Change Block Tracking,** this method backup only blocks with changes and skip zeroed sectors.
    - supports oVirt 4.4+ (with Libvirt 6+, qemu-kvm 4.2+ and vdsm 4.40+)
    - supports incremental backup

> **Note:** When using backup APIs - Red Hat highly recommends updating the RHV environment to the most recent version (4.4 - at the time of writing) - please refer to this article for more information.

When adding RHV 4.0+ hypervisor managers, use a URL similar to the following:

```
https://RHV_MGR_HOST/ovirt-engine/api
```

> **Note:** a username for RHV environments needs to be provided in the **user@domain** format - i.e. **admin@internal**. This user must have all permissions related to managing snapshots, creating/removing VMs, operating disks, and exporting data.

Backup Strategies

Red Hat Virtualization environments can be protected in several ways.

Note: Different strategies require a node to be installed either as a VM on the environment that you back up or installed separately.

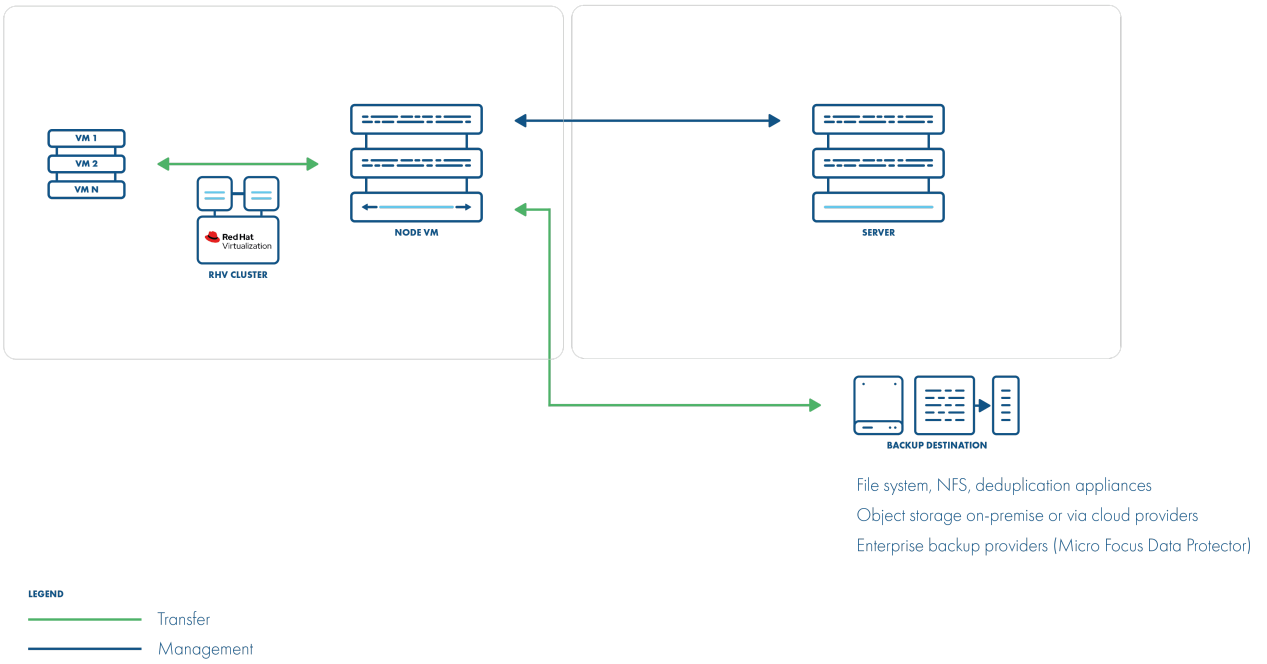
Note: All live snapshots are attempted with quiescing enabled. If the snapshot command fails because there is no compatible guest agent present, the live snapshot is re-initiated without the use-quiescing flag.

Disk attachment with Proxy VM

In this strategy, you have a VM called “Proxy VM” that invokes commands on your hypervisor manager to snapshot and attach drives of a specific VM to itself (Proxy VM). The Proxy VM is able to read the data from the attached disk snapshots and forward them to the backup provider.

This strategy allows you to exclude drives from the backup that you do not need. Remember that you need to install 1 Proxy VM per cluster so that the drives the node tries to attach are reachable.

Drawback - no incremental backup for now.



Backup Process

- crash-consistent snapshot using hypervisor's API
- optionally FS freeze can be executed before snapshot can be executed (FS thaw once the snapshot is completed) if enabled and guest tools installed inside
- optional application consistency using pre/post snapshot command execution
- metadata exported from API
- snapshot disks are mounted one by one to the Proxy VM
- data read directly on the Proxy VM
- incremental backups are _**_not supported
- restore creates empty disks on the Proxy VM, imports merged data then recreates VM and reattaches volumes to the target VM

Note: RHV API v4 environments require Data Protector for Cloud Workloads Node to be installed in one of the VMs residing on the RHV cluster. Data Protector for Cloud Workloads should automatically detect the VM with Data Protector for Cloud Workloads during the index operation.

Disk attachment mode requires `Virtio-SCSI` to be enabled on the Data Protector for Cloud Workloads Node VM (which can be enabled in `VM settings` -> `Resource Allocation` -> `VirtIO-SCSI Enabled` at the bottom).

During backup/restore operations, disks are transferred by attaching them to the proxy VM. This approach does not require an export storage domain to be set up.

Please make sure that you follow these steps: LVM setup on Data Protector for Cloud Workloads Node for disk attachment backup mode.

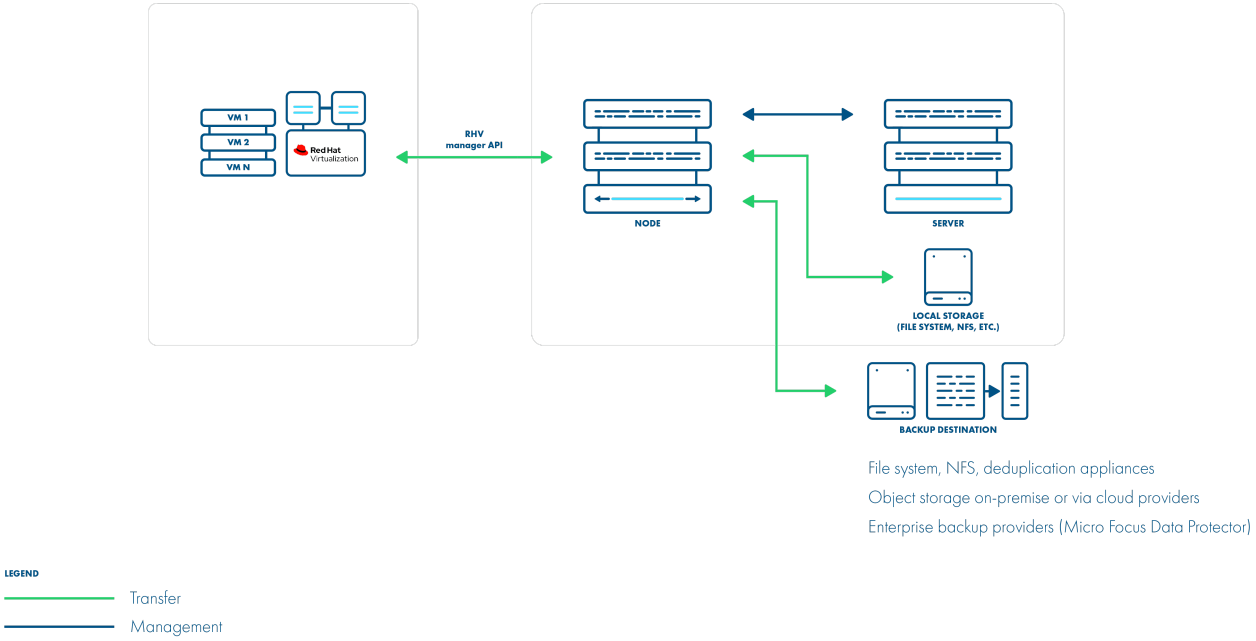
Disk image transfer API

This API appears in RHV 4.2 and allows the export of individual snapshots directly from the RHV manager. So instead of having to install multiple Proxy VMs, you can have a single external Node installation, which just invokes APIs via the

RHV manager.

This strategy supports incremental backups. Assuming you have RHV 4.2 or newer – just add your manager to Data Protector for Cloud Workloads and setup is done. From a network perspective, it requires two additional ports to be open - 54322 and 54323 - and your data to be pulled from the hypervisor manager.

Unfortunately, there are a few problems with the current architecture of this solution. The biggest issue is that all traffic passes via the RHV manager, which may impact the transfer rates that you can achieve during the backup process. To put this into perspective – in disk attachment, you can basically read data as if it is a local drive, where it could potentially be deduplicated even before transferring it to the backup destination.



Backup Process

- crash-consistent snapshot using hypervisor's API
- optionally FS freeze can be executed before snapshot can be executed (FS thaw once the snapshot is completed) if enabled and guest tools installed inside
- optional application consistency using pre/post snapshot command execution
- supported for oVirt/RHV/OLVM 4.3+
- metadata exported from API
- data transfer initiated on the manager and actual data exported from the hypervisor using imageio API
- incremental backups use the same APIs, but requests for changed blocks only
- the last snapshot kept on the hypervisor for the next incremental backup (if at least one schedule assigned to the VM has a backup type set to incremental)
- restore recreates VM from metadata using API and imports merged chain of data for each disk using imageio API

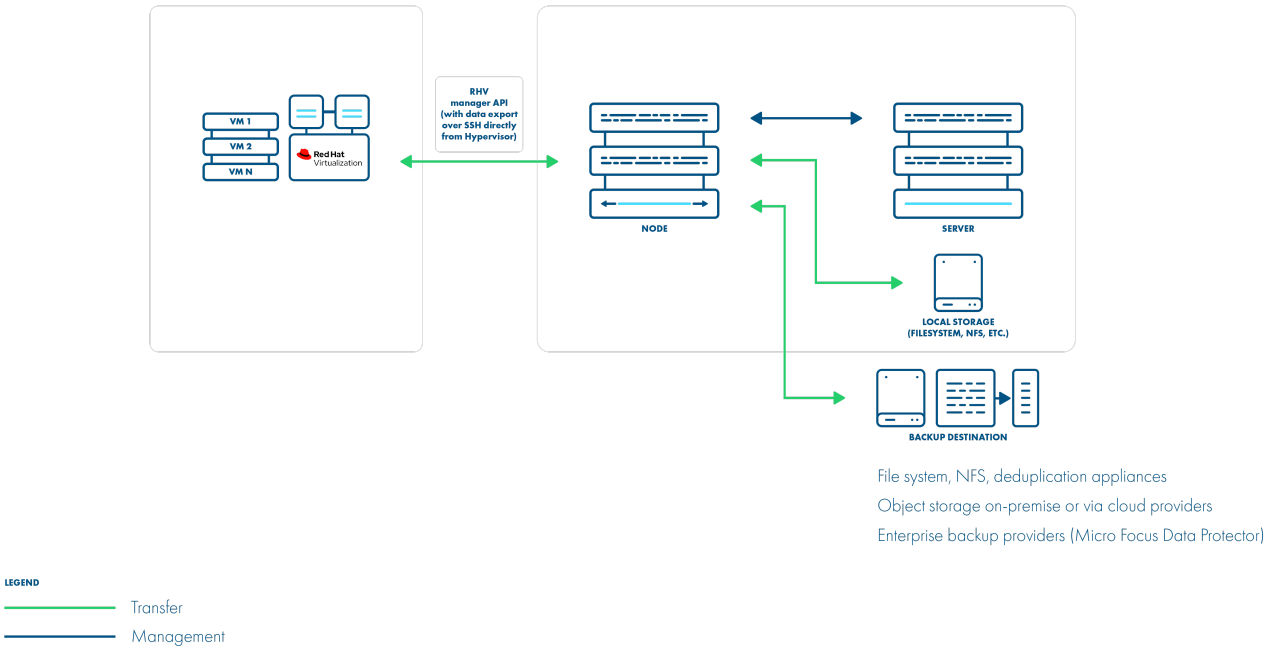
Disk image transfer mode exports data directly using RHV 4.2+ API. There is no need to set up an export storage domain or set up an LVM. This mode uses snapshot chains provided by RHV.

You may need to open communication for the additional port **54323** on the RHV manager - it needs to be accessible from Data Protector for Cloud Workloads Node. Also, make sure that your **ovirt-imageio-proxy** services are running and properly configured (you can verify this by trying to upload images with RHV UI).

Follow the steps in this section: Full versions of libvirt/qemu packages installation.

SSH transfer

This is an enhancement for the disk image transfer API strategy. It allows Data Protector for Cloud Workloads to use RHV API v4.2+ (HTTPS connection to RHV manager) only to collect metadata. Backup is done over SSH directly from the hypervisor (optionally using netcat for transfer), import is also using SSH (without netcat option). No need to install a node on the RHV environment. This method can boost backup transfers and supports incremental backups.



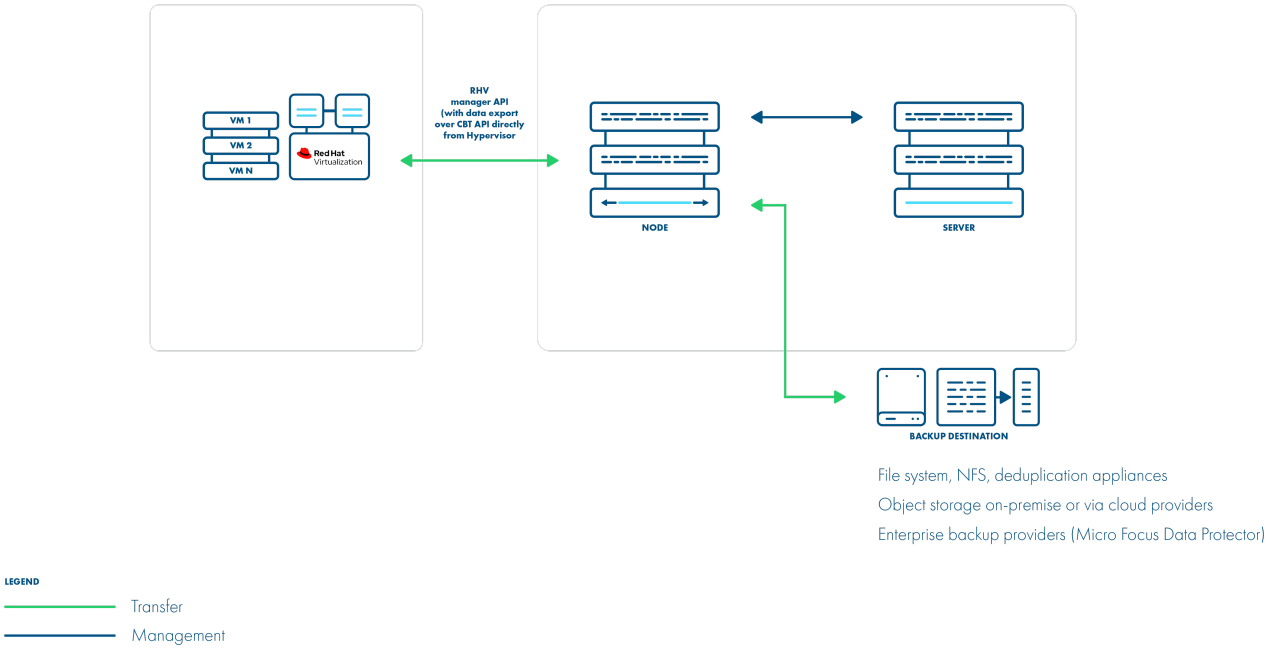
Backup Process

- crash-consistent snapshot using hypervisor's API
- optionally FS freeze can be executed before snapshot can be executed (FS thaw once the snapshot is completed) if enabled and guest tools installed inside
- optional application consistency using pre/post snapshot command execution • metadata exported from API
- data transfer via SSH (optional using netcat) - the full chain of disk snapshot files for each disk o if LVM-based storage is used, then node activates volumes if necessary to read data o if Gluster FS is used, then disk files are copied directly
- incremental backup export just sub-chain of QCOW2-deltas snapshots since last stored snapshot
- the last snapshot kept on the hypervisor for the next incremental backup (if at least one schedule assigned to the VM has the backup type set to incremental)
- restore recreates VM with empty storage from metadata using API and imports merged data over SSH to appropriate location on the hypervisor

This method assumes that all data transfers are directly from the hypervisor - over SSH. This means that after adding the RHV manager and detecting all available hypervisors - **you also need to provide SSH credentials or SSH keys for each of the hypervisors**. You can also use SSH public key authentication.

Change Block Tracking

This is a new method that is possible thanks to changes in RHV 4.4. It uses information about zeroed and changed blocks to reduce data size and make the process faster.



This strategy supports incremental backups.

The QCOW2 format is required for incremental backups so that disks enabled for incremental backup use the QCOW2 format instead of the raw format.

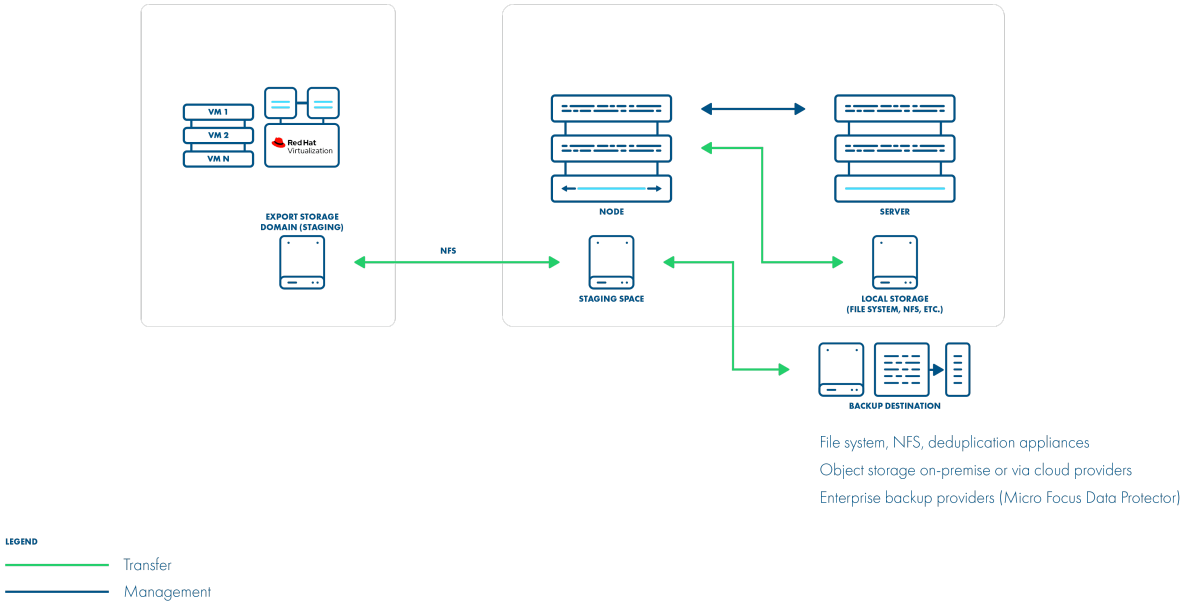
Also, this strategy doesn't need snapshots in the backup process. Instead, every incremental backup uses a checkpoint that is a point in time that was created after the previous backup.

Export storage domain (API v3)

This setup requires you to create a storage domain used for VM export. The export storage domain should also be accessible by Data Protector for Cloud Workloads Node in its staging directory. This implies that the storage space doesn't have to be exported by Data Protector for Cloud Workloads Node - it can be mounted from an external source. The only requirement is to have it visible from both the RHV host and the Node itself. Keep in mind that ownership of the files on the share should allow both Data Protector for Cloud Workloads and RHV to read and write files.

The backup process requires that once the snapshot is created, it will be cloned and exported (in fact to Data Protector for Cloud Workloads Node staging). The reason for additional cloning is that RHV doesn't allow you to export a snapshot directly. The Node can be outside of the environment that you back up.

This strategy is going to be deprecated, as Red Hat may no longer support it in future releases.



Backup Process

- crash-consistent snapshot is taken via API
- optional application consistency using pre/post snapshot command execution
- initial VM clone of the snapshot to the local repository is created
- cloned VM (data+metadata) exported by the manager to the Data Protector for Cloud Workloads staging space (visible as the export Storage Domain in managers UI)
- full backup only is supported
- restore is done to the export Storage Repository, the administrator needs to import the VM using manager UI

How to set up a backup with an export storage domain

RHV 3.5.1+ environments (using API v3) require an export storage domain to be set up.

1. Add a backup storage domain in RHEV (which points to the NFS export on Data Protector for Cloud Workloads Node)
    - If you have multiple data centers, you need to enable the **Multi DC export** a checkbox in the node configuration
        - Remember that you need to use named data centers in your RHV environment to avoid name conflicts
        - An RHV datacenter may use only one export storage domain, which is why you need to create subdirectories for each data center in the export path i.e. `/vprotect_data/dc01`, `/vprotect_data/dc02`, and use each sub-directory as NFS share for each data center export domain (separate NFS exports)
        - The export (staging) path in the above-mentioned scenario is still `/vprotect_data`, while `dc01` and `dc02` are data center names
        - Older versions of RHV (3.5.x) require you to specify a mapping between DC names and export storage domains - you need to provide pairs of a DC name and a corresponding SD name in the node configuration (section `Hypervisor`)
    - If you have only one data center and don't want to use the multiple data centers export feature in the future, you can use the default settings and set up the NFS export pointing to the staging path (e.g. `/vprotect_data`)

- Note that export must be set to use the UID and GID of the `vprotect` user
- Example export configuration in `/etc/exports` to a selected hypervisor in the RHV cluster:

  ```
  /vprotect_data
  10.50.1.101(fsid=6,rw,sync,insecure,all_squash,anonuid=993,anongid=990)
  ```

  where `anonuid=993` and `anongid=990` should have the correct UID and GID returned by command:

  ```
  [root@vProtect3 ~]# id vprotect
  uid=993(vprotect) gid=990(vprotect) groups=990(vprotect)
  ```

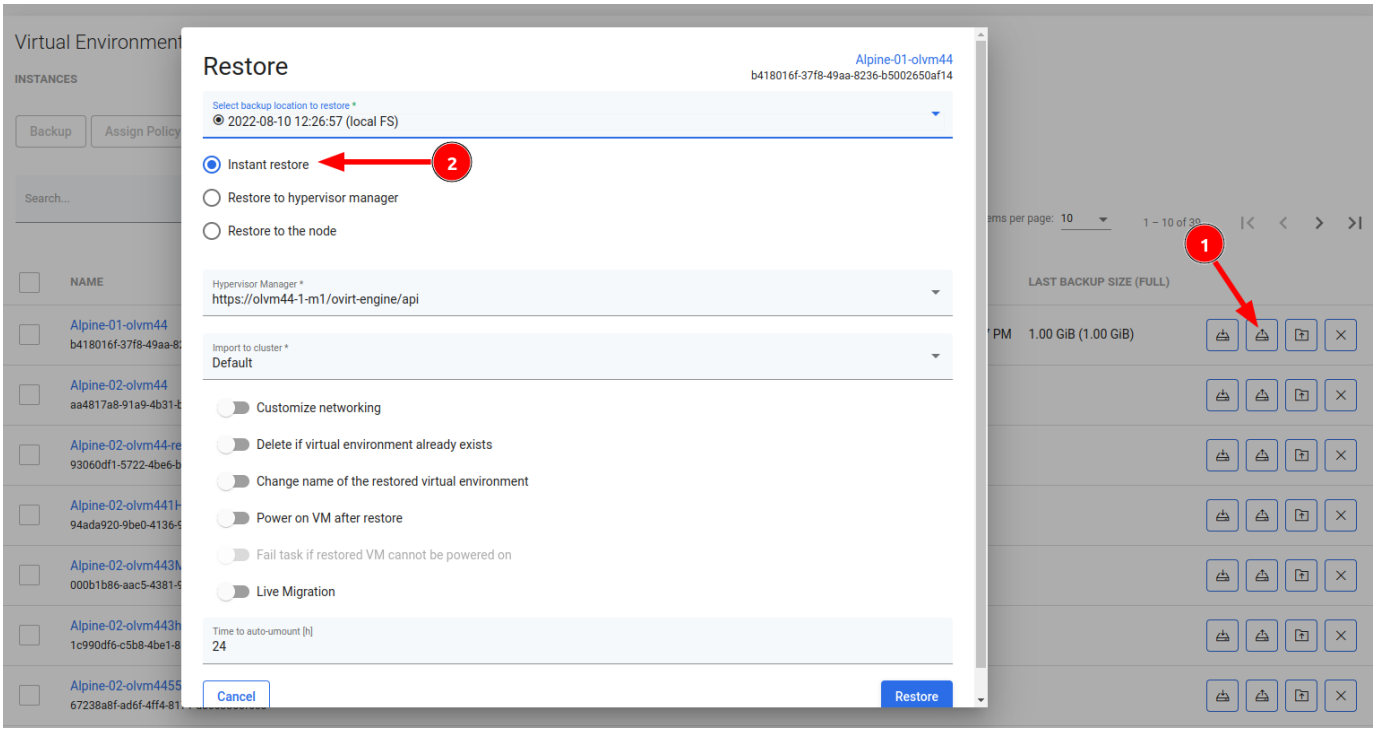
2. Both import and export operations will be done using this NFS share – restore will be done directly to this storage domain, so you can easily import the backup into RHV (shown below)
   - backups must be restored to the export path (the node automatically changes names to the original paths that are recognized by the RHV manager).
3. When adding RHV 4.0+ hypervisor managers, make sure you have a URL like the following:

   ```
   https://RHV_MGR_HOST/ovirt-engine/api/v3
   ```

> **Note:** Restore to RHV using SPARSE disk allocation format is not supported if backup files are in RAW format and destination storage domain type in either Fibre Channel or iSCSI. If such configuration is detected, then disk allocation format is automatically switched to PREALLOCATED

Instant restore

To use an instant restore feature, backup destination from which VM will be restored, has to be of a synthetic type. The restore process creates a NFS share on the Data Protector for Cloud Workloads node, later this share is attached to the RHV as a new storage domain. Then it creates a new virtual machine and attaches the disks from the newly created storage domain to it. To use instant restore you have to click the restore button in the instances list and choose the option **instant restore**.



Live migration

You can enable the live migration option during instant restore. It will automatically start the disks migration to the chosen storage after the VM is restored and powered on.

oVirt

General

For oVirt 4+ environments you can use API v4 for invoking all backup-related tasks.

Import/export mode defines the way the backups and restores are done. oVirt (with API v4) supports 4 modes:

1. **Disk attachment**, which exports VM metadata (in OVF format) with separate disk files (in RAW format) via Proxy VM with the Node installed.
    - supports oVirt 4.0+
    - no incremental backup
    - proxy VM required in each cluster - used for the disk attachment process
2. **Disk image transfer**, which exports VM metadata (in OVF format) with disk snapshot chains as separate files (QCOW2 format):
    - supports oVirt 4.2+/oVirt 4.2.3+
    - supports incremental backup
    - disk images are transferred directly from API (no Proxy VM required)
3. **SSH Transfer,** this method assumes that all data transfers are directly from the hypervisor - over SSH
4. **Change Block Tracking,** this method backs up only blocks with changes and skip zeroed sectors.
    - supports oVirt 4.4+ (with Libvirt 6+, qemu-kvm 4.2+ and vdsm 4.40+)
    - supports incremental backup
    - only disks marked with "enable incremental backup" in ovirt will be backed up

> **Note:** When using backup APIs - Red Hat highly recommends updating the oVirt environment to the most recent version (4.4 - at the time of writing) - please refer to this article for more information.

When adding oVirt 4.0+ hypervisor managers, use a URL similar to the following:

```
https://oVirt_MGR_HOST/ovirt-engine/api
```

> **Note:** a username for oVirt environments needs to be provided in the **user@domain** format - i.e. **admin@internal**. This user must have all permissions related to managing snapshots, creating/removing VMs, operating disks, and exporting data.

Backup Strategies

oVirt environments can be protected in several ways.

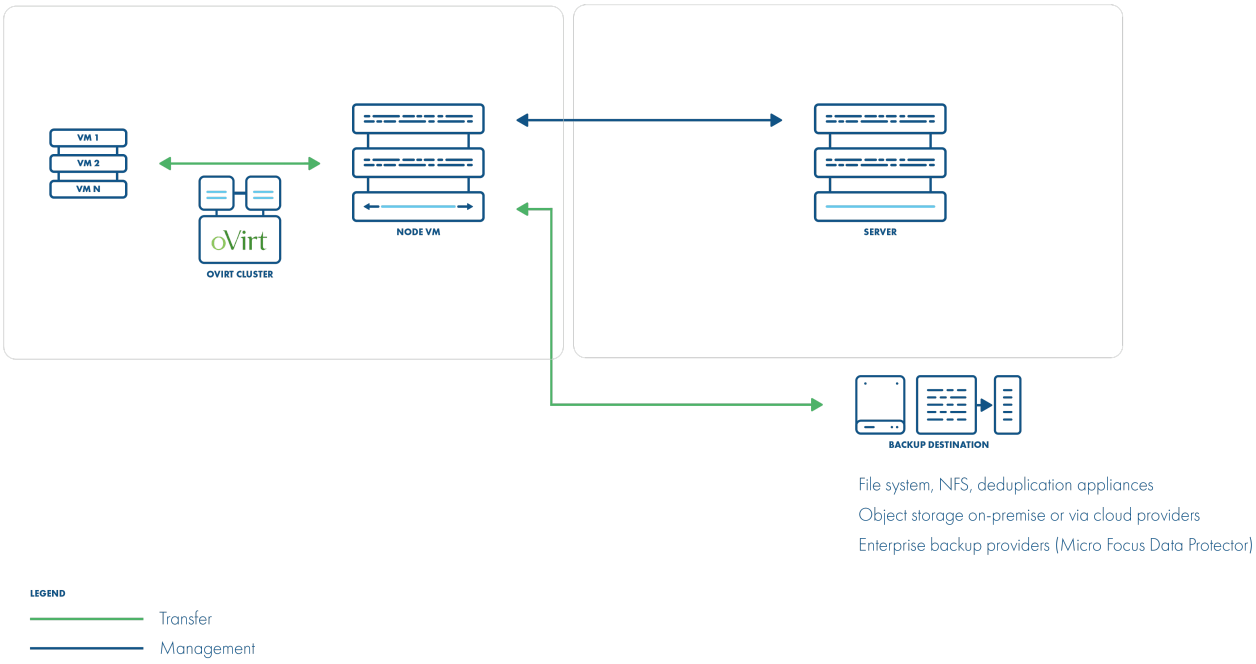
> **Note:**
>
> Different strategies require a node to be installed either as a VM on the environment that you back up or installed separately.
>
> All live snapshots are attempted with quiescing enabled. If the snapshot command fails because there is no compatible guest agent present, the live snapshot is re-initiated without the use-quiescing flag.

Disk attachment with Proxy VM

In this strategy, you have a VM called “Proxy VM” that invokes commands on your hypervisor manager to snapshot and attach drives of a specific VM to itself (Proxy VM). Proxy VM is able to read the data from the attached disk snapshots and forward them to the backup provider.

This strategy allows you to exclude drives from a backup that you do not need. Remember that you need to install 1 Proxy VM per cluster so that the drives the node tries to attach are reachable.

Drawback - no incremental backup for now.



Backup Process

- crash-consistent snapshot using hypervisor's API
- optionally FS freeze can be executed before snapshot can be executed (FS thaw once the snapshot is completed) if enabled and guest tools installed inside
- optional application consistency using pre/post snapshot command execution
- metadata exported from API
- snapshot disks are mounted one by one to the Proxy VM
- data read directly on the Proxy VM
- incremental backups are _**_not supported
- restore creates empty disks on the Proxy VM, imports merged data then recreates VM and reattaches volumes to the target VM

> **Note**: oVirt API v4 environments require Data Protector for Cloud Workloads Node to be installed in one of the VMs residing in the oVirt cluster. Data Protector for Cloud Workloads should automatically detect the VM with Data Protector for Cloud Workloads during the index operation.

Disk attachment mode requires `Virtio-SCSI` to be enabled on the Data Protector for Cloud Workloads Node VM (which can be enabled in `VM settings` -> `Resource Allocation` -> `VirtIO-SCSI Enabled` at the bottom).

During backup/restore operations, disks are transferred by attaching them to the proxy VM. This approach does not require an export storage domain to be set up.

Please make sure you follow these steps: LVM setup on Data Protector for Cloud Workloads Node for disk attachment backup mode.

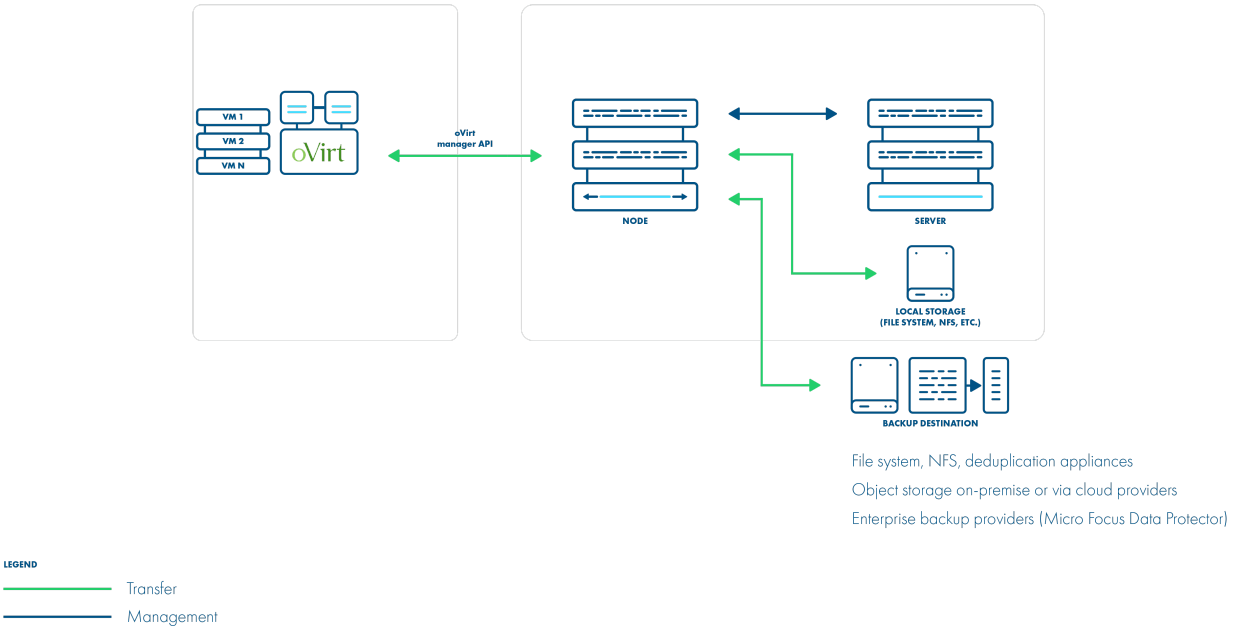
Disk image transfer API

This API appeared in oVirt 4.2 and allowed the export of individual snapshots directly from the oVirt manager. So instead of having to install multiple Proxy VMs, you can have a single external Node installation, which just invokes APIs via the

oVirt manager.

This strategy supports incremental backups. Assuming you have oVirt 4.2 or newer – just add your manager to Data Protector for Cloud Workloads and the setup is done. From a network perspective, it requires two additional ports to be opened - 54322 and 54323 - and your data to be pulled from the hypervisor manager.

Unfortunately, there are a few problems with the current architecture of this solution. The biggest issue is that all traffic passes via the oVirt manager, which may impact the transfer rates that you can achieve during the backup process. To put that into perspective – in disk attachment, you can basically read data as if it is a local drive, where it could potentially be deduplicated even before it is transferred to the backup destination.



Backup Process

- crash-consistent snapshot using hypervisor's API
- optionally FS freeze can be executed before snapshot can be executed (FS thaw once the snapshot is completed) if enabled and guest tools installed inside
- optional application consistency using pre/post snapshot command execution
- supported for oVirt/RHV/OLVM 4.3+
- metadata exported from API
- data transfer initiated on the manager and actual data exported from the hypervisor using imageio API
- incremental backups use the same APIs, but requests for changed blocks only
- the last snapshot kept on the hypervisor for the next incremental backup (if at least one schedule assigned to the VM has the backup type set to incremental)
- restore recreates VM from metadata using API and imports merged chain of data for each disk using imageio API

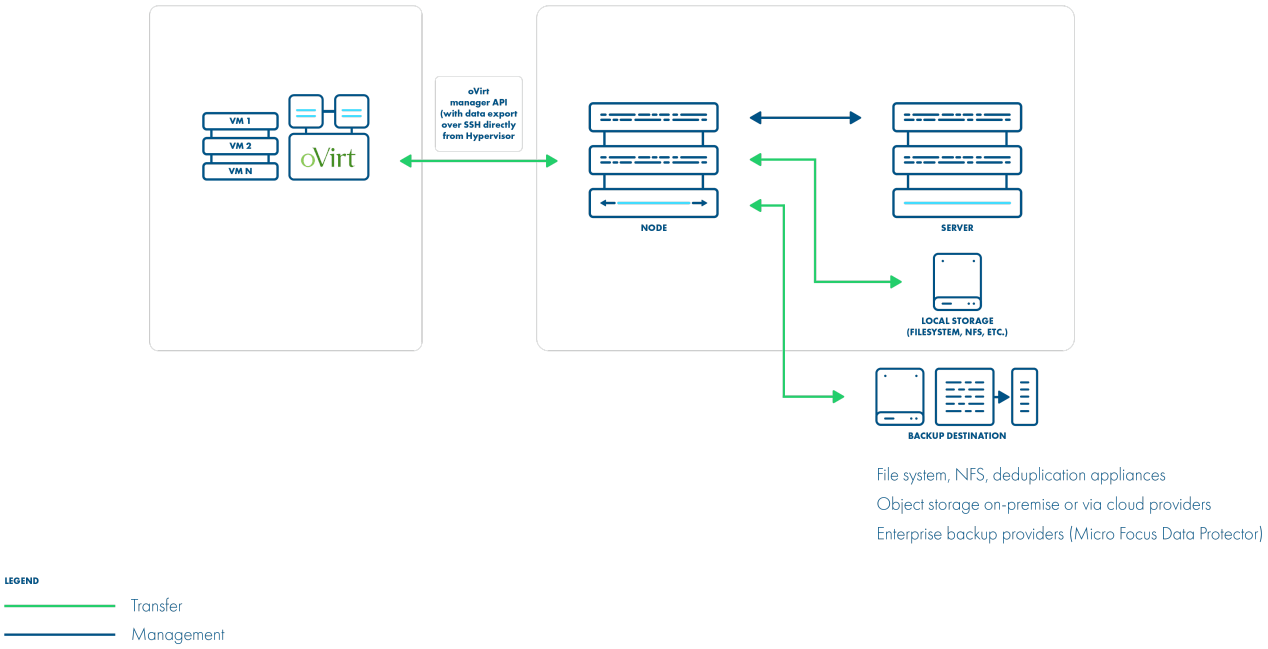
Disk image transfer mode exports data directly using oVirt 4.2+ API. There is no need to set up an export storage domain or setup LVM. This mode uses snapshot chains provided by oVirt.

You may need to open communication for the additional port **54323** on the oVirt manager - it needs to be accessible from Data Protector for Cloud Workloads Node. Also make sure that your **ovirt-imageio-proxy** services are running and properly configured (you can verify it by trying to upload images with oVirt UI).

Follow the steps in this section: Full versions of libvirt/qemu packages installation.

SSH transfer

This is an enhancement for disk image transfer API strategy. It allows Data Protector for Cloud Workloads to use oVirt API v4.2+ (HTTPS connection to oVirt manager) only to collect metadata. Backup is done over SSH directly from the hypervisor (optionally using netcat for transfer), import is also using SSH (without the netcat option). There is no need to install a node in the oVirt environment. This method can significantly boost backup transfers and supports incremental backups.



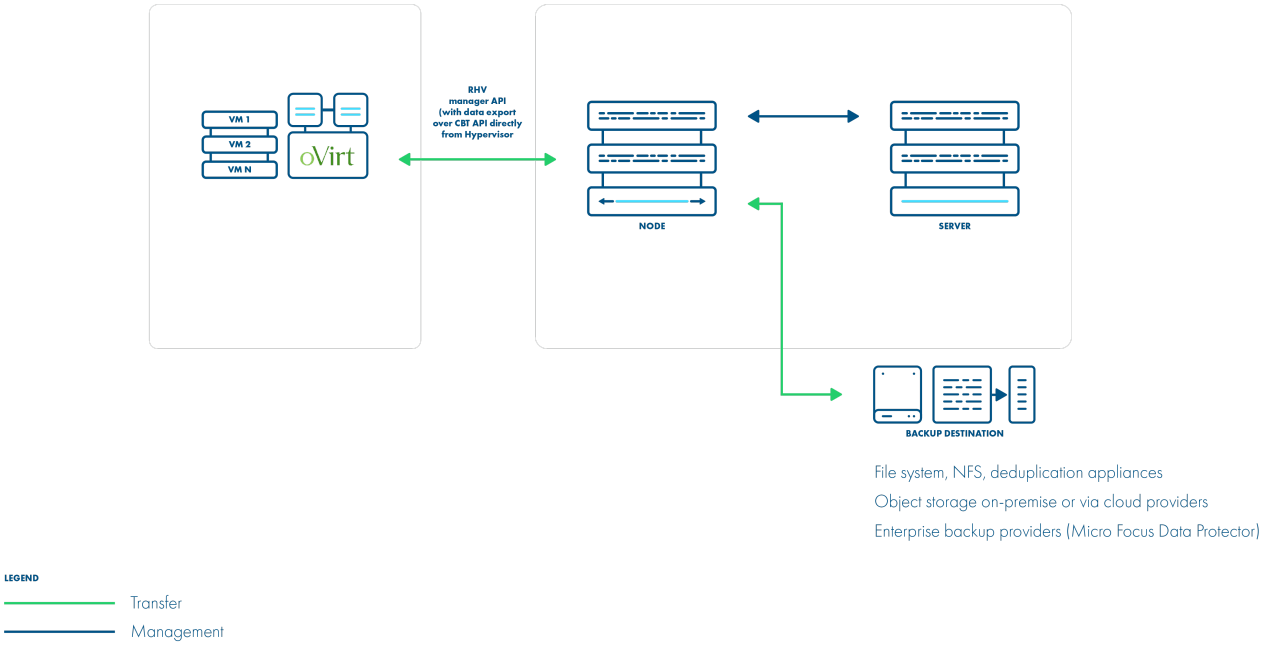
Backup Process

- crash-consistent snapshot using hypervisor's API
- optionally FS freeze can be executed before snapshot can be executed (FS thaw once the snapshot is completed) if enabled and guest tools installed inside
- optional application consistency using pre/post snapshot command execution • metadata exported from API
- data transfer via SSH (optional using netcat) - the full chain of disk snapshot files for each disk o if LVM-based storage is used, then node activates volumes if necessary to read data o if Gluster FS is used, then disk files are copied directly
- incremental backup export just sub-chain of QCOW2-deltas snapshots since last stored snapshot
- the last snapshot kept on the hypervisor for the next incremental backup (if at least one schedule assigned to the VM has the backup type set to incremental)
- restore recreates VM with empty storage from metadata using API and imports merged data over SSH to appropriate location on a hypervisor

This method assumes that all data transfers are directly from the hypervisor over SSH. This means that after adding oVirt manager and detecting all available hypervisors - **you also need to provide SSH credentials or SSH keys for each of the hypervisors**. You can also use SSH public key authentication.

Change Block Tracking

This is a new method which is possible thanks to changes in oVirt 4.4. It uses information about zeroed and changed blocks to reduce data size and make the process faster.



This strategy supports incremental backups.

The QCOW2 format is required for incremental backups, so disks enabled for the incremental backup will use the QCOW2 format instead of the raw format.

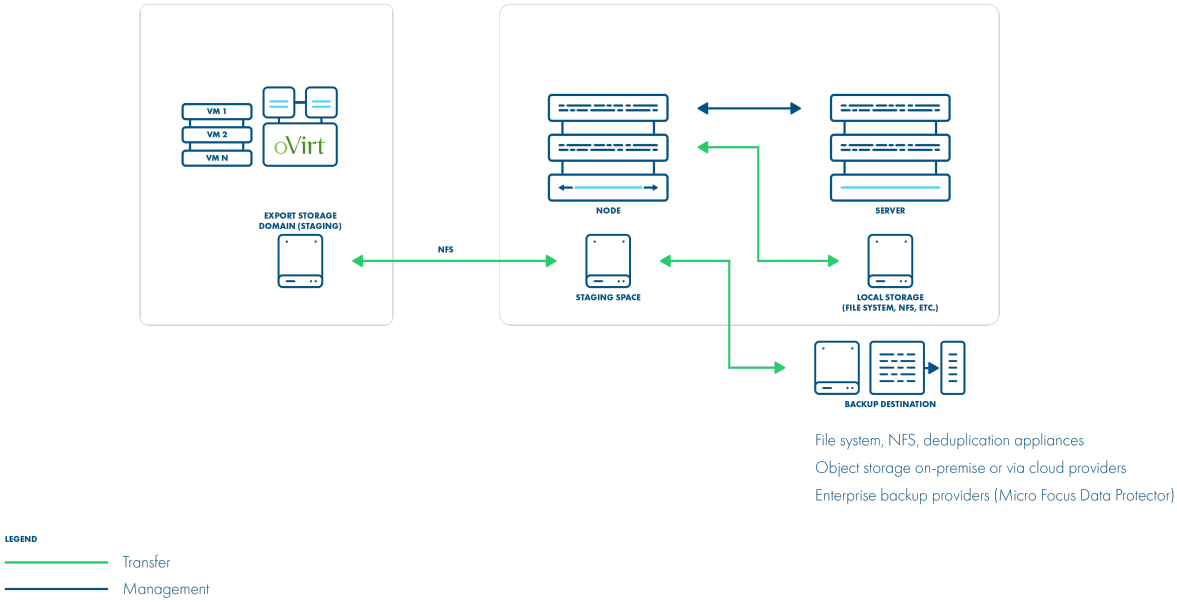
Also, this strategy doesn't need snapshots in the backup process. Instead, every incremental backup uses a checkpoint that is a point in time that was created after the previous backup.

Export storage domain (API v3)

This setup requires you to create a storage domain used for VM export. The export storage domain should also be accessible to Data Protector for Cloud Workloads Node in its staging directory. This implies that storage space doesn't have to be exported by Data Protector for Cloud Workloads Node - it can be mounted from an external source. The only requirement is to have it visible from both the oVirt host and the Node itself. Keep in mind that ownership of the files on the share should allow both Data Protector for Cloud Workloads and oVirt to read and write files.

The backup process requires that once a snapshot is created it will be cloned and exported (in fact to Data Protector for Cloud Workloads Node staging). The reason for additional cloning is that oVirt doesn’t allow you to export snapshots directly. The Node can be outside of the environment that you back up.

This strategy is going to be deprecated, as oVirt may no longer support it in future releases.



Backup Process

- crash-consistent snapshot is taken via API
- optional application consistency using pre/post snapshot command execution
- initial VM clone of the snapshot to the local repository is created
- cloned VM (data+metadata) exported by the manager to the Data Protector for Cloud Workloads staging space (visible as the export Storage Domain in managers UI)
- full backup only is supported
- restore is done to the export Storage Repository, the administrator needs to import the VM using manager UI

How to set up a backup with an export storage domain

oVirt 3.5.1+ environments (using API v3) require an export storage domain to be set up.

1. Add a backup storage domain in oVirt (which points to the NFS export in Data Protector for Cloud Workloads Node)
    - If you have multiple data centers, you need to enable the **Multi DC export** a checkbox in node configuration
        - Remember that you need to use named data centers in your oVirt environment to avoid name conflicts
        - An oVirt data center may use only one export storage domain, that is why you need to create sub-directories for each data center in the export path i.e. `/vprotect_data/dc01`, `/vprotect_data/dc02`, and use each sub-directory as NFS share for each data center export domain (separate NFS exports)
        - The export (staging) path in the above-mentioned scenario is still `/vprotect_data`, while `dc01` and `dc02` are data center names
        - Older versions of oVirt (3.5.x) require you to specify the mapping between DC names and export storage domains - you need to provide pairs of a DC name and a corresponding SD name in the node configuration (section `Hypervisor`)
    - If you have only one data center and don't want to use the multiple data centers export feature in the future, you can use the default settings and setup NFS export pointing to the staging path (e.g. `/vprotect_data`)
    - Note that the export must be set to use the UID and GID of `vprotect` user

- Example export configuration in `/etc/exports` to a selected hypervisor in the oVirt cluster:

```
/vprotect_data
10.50.1.101(fsid=6,rw,sync,insecure,all_squash,anonuid=993,anongid=990)
```

where `anonuid=993` and `anongid=990` should have the correct UID and GID returned by command:

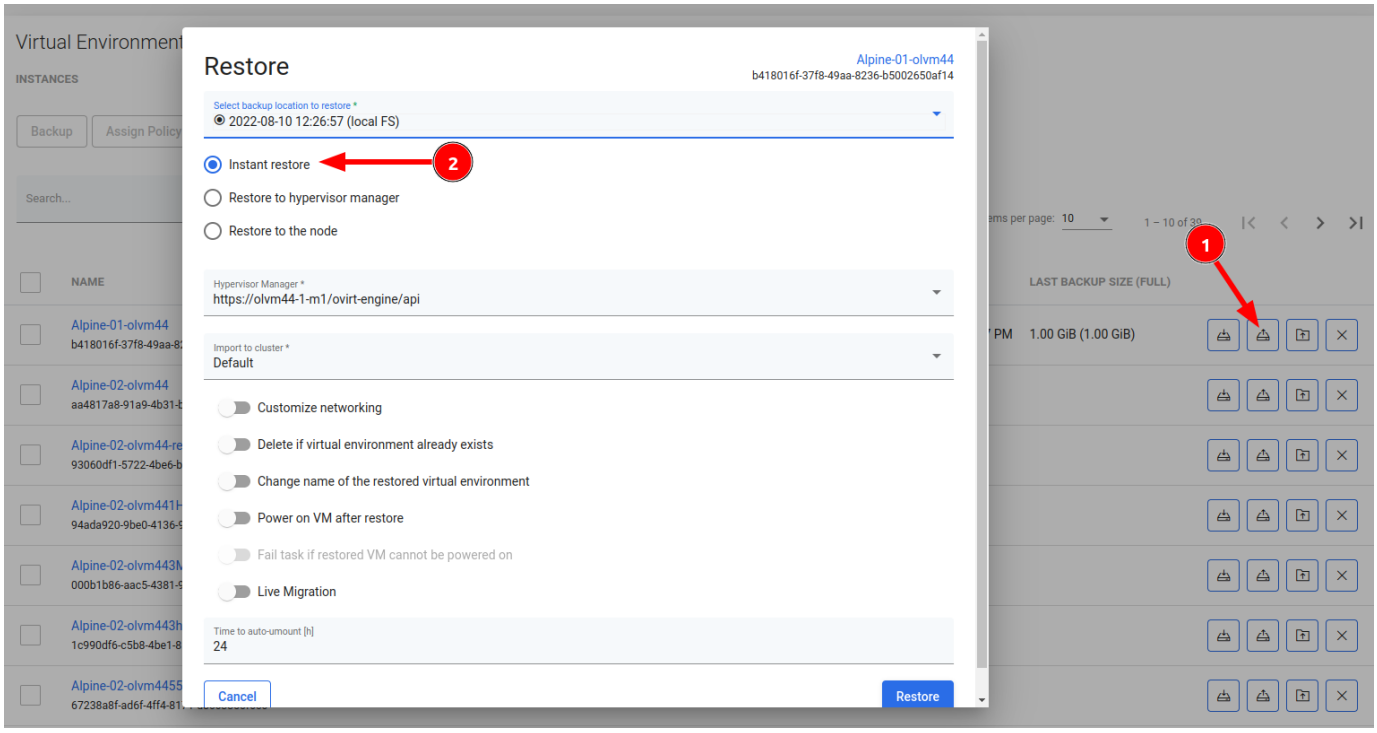
```
[root@vProtect3 ~]# id vprotect
uid=993(vprotect) gid=990(vprotect) groups=990(vprotect)
```

2. Both import and export operations will be done using this NFS share – restore will be done directly to this storage domain, so you can easily import the backup into oVirt (shown below)
    - backups must be restored to the export path (the node automatically changes names to the original paths that are recognized by the oVirt manager.
3. When adding oVirt 4.0+ hypervisor managers, make sure you have a URL like the following:

```
https://oVirt_MGR_HOST/ovirt-engine/api/v3
```

Instant restore

To use an instant restore feature, backup destination from which VM will be restored, has to be of a synthetic type. The restore process creates a NFS share on the Data Protector for Cloud Workloads node, later this share is attached to the RHV as a new storage domain. Then it creates a new virtual machine and attaches the disks from the newly created storage domain to it. To use instant restore you have to click the restore button in the instances list and choose the option **instant restore**.



Live migration

You can enable the live migration option during instant restore. It will automatically start the disks migration to the chosen storage after the VM is restored and powered on.

Oracle Linux Virtualization Manager

General

For Oracle Linux Virtualization Manager (OLVM) 4+ environments you can use API v4 for invoking all backup-related tasks.

Import/export mode defines the way the backups and restores are done. OLVM (with API v4) supports 3 modes:

1. **Disk attachment**, which exports VM metadata (in OVF format) with separate disk files (in RAW format) via Proxy VM with the Node installed.
    - supports OLVM 4.0+
    - no incremental backup
    - proxy VM required in each cluster - used for the disk attachment process
2. **Disk image transfer**, which exports VM metadata (in OVF format) with disk snapshot chains as separate files (QCOW2 format):
    - supports OLVM 4.2+/oVirt 4.2.3+
    - supports incremental backup
    - disk images are transferred directly from the API (no Proxy VM required)
3. **SSH Transfer,** this method assumes that all data transfers are directly from the hypervisor over SSH

When adding OLVM hypervisor managers, use a URL similar to the following:

```
https://OLVM_MGR_HOST/ovirt-engine/api
```

> **Note:** a username for OLVM environments needs to be provided in the **user@domain** format - i.e. **admin@internal**. This user must have all permissions related to managing snapshots, creating/removing VMs, operating disks, and exporting data.

Backup Strategies

OLVM environments can be protected in several ways.

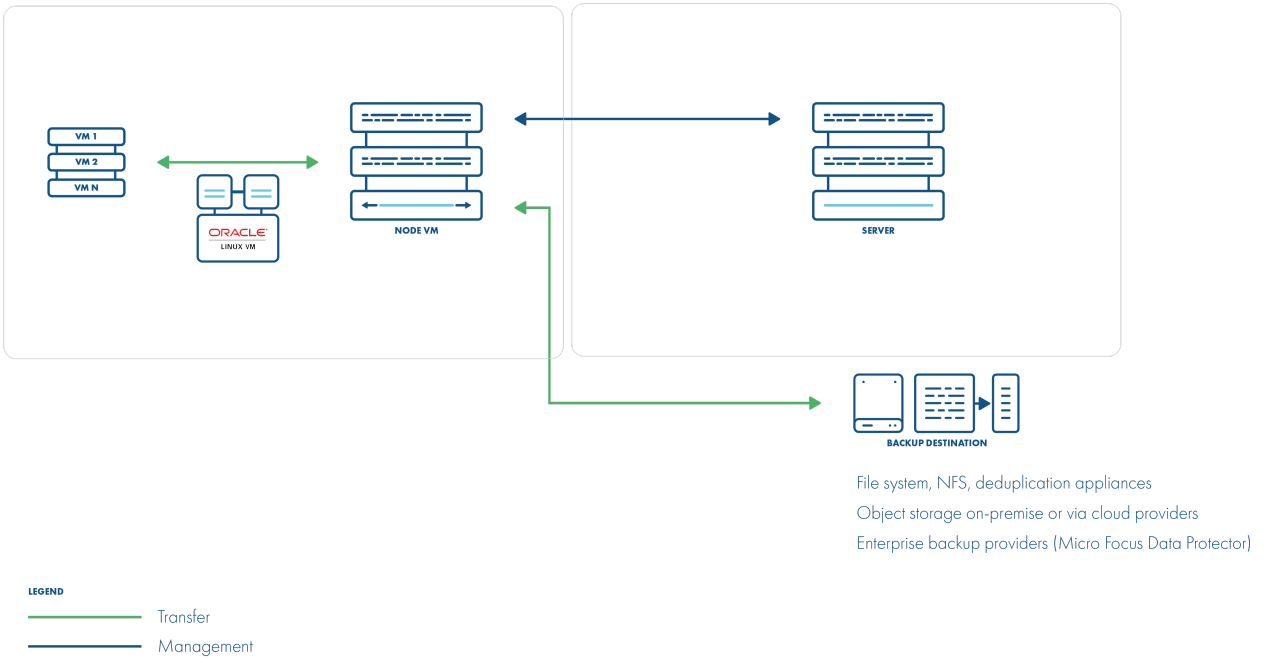
> **Note:**
>
> Different strategies require a node to be installed either as a VM in the environment that you back up or installed separately.
>
> All live snapshots are attempted with quiescing enabled. If the snapshot command fails because there is no compatible guest agent present, the live snapshot is re-initiated without the use-quiescing flag.

Disk attachment with Proxy VM

In this strategy, you have a VM called “Proxy VM” that invokes commands on your hypervisor manager to snapshot and attach drives of a specific VM to itself (Proxy VM). The proxy VM is able to read the data from the attached disk snapshots and forward them to the backup provider.

This strategy allows you to exclude drives from a backup that you do not need. Remember that you need to install 1 Proxy VM per cluster so that the drives the node tries to attach are reachable.

Drawback - no incremental backup for now.



Backup Process

- crash-consistent snapshot using hypervisor's API
- optionally FS freeze can be executed before snapshot can be executed (FS thaw once the snapshot is completed) if enabled and guest tools installed inside
- optional application consistency using pre/post snapshot command execution
- metadata exported from API
- snapshot disks are mounted one by one to the Proxy VM
- data read directly on the Proxy VM
- incremental backups are _**_not supported
- restore creates empty disks on the Proxy VM, imports merged data then recreates VM and reattaches volumes to the target VM

> **Note**: OLVM API v4 environments require Data Protector for Cloud Workloads Node to be installed in one of the VMs residing in the OLVM cluster. Data Protector for Cloud Workloads should automatically detect the VM with Data Protector for Cloud Workloads during the index operation.

The disk attachment mode requires `Virtio-SCSI` to be enabled on the Data Protector for Cloud Workloads Node VM (which can be enabled in `VM settings` -> `Resource Allocation` -> `VirtIO-SCSI Enabled` at the bottom).

During backup/restore operations, disks are transferred by attaching them to the proxy VM. This approach does not require an export storage domain to be set up.

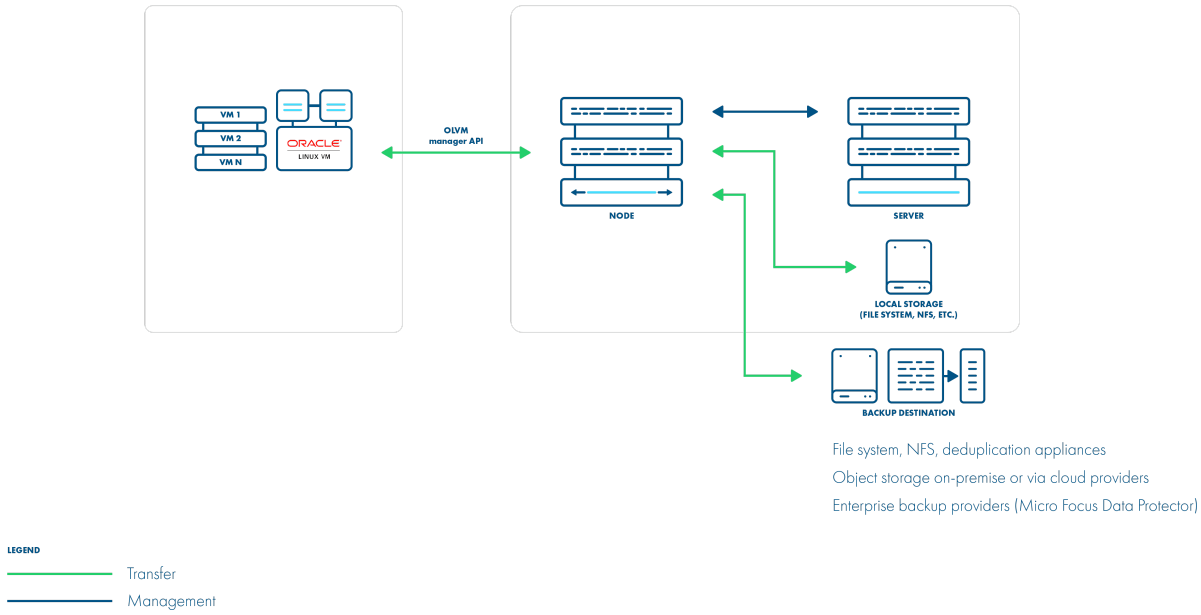
Please make sure you follow these steps: LVM setup on Data Protector for Cloud Workloads Node for disk attachment backup mode.

Disk image transfer API

This API appeared in OLVM 4.2 and allowed the export of individual snapshots directly from the OLVM manager. So instead of having to install multiple Proxy VMs, you can have a single external Node installation, which just invokes APIs via the OLVM manager.

This strategy supports incremental backups. Assuming you have OLVM 4.2 or newer – just add your manager to Data Protector for Cloud Workloads and setup is done. From a network perspective, it requires two additional ports to be opened - 54322 and 54323 - and your data to be pulled from the hypervisor manager.

Unfortunately, there are a few problems with the current architecture of this solution. The biggest issue is that all traffic passes via the OLVM manager, which may impact the transfer rates that you can achieve during the backup process. To put that into perspective – in disk attachment, you can basically read data as if it is a local drive, where it could potentially be deduplicated even before it is transferred to the backup destination.



Backup Process

- crash-consistent snapshot using hypervisor's API
- optionally FS freeze can be executed before snapshot can be executed (FS thaw once the snapshot is completed) if enabled and guest tools installed inside
- optional application consistency using pre/post snapshot command execution
- supported for oVirt/RHV/OLVM 4.3+
- metadata exported from API
- data transfer initiated on the manager and actual data exported from the hypervisor using imageio API
- incremental backups use the same APIs, but requests for changed blocks only
- the last snapshot kept on the hypervisor for the next incremental backup (if at least one schedule assigned to the VM has a backup type set to incremental)
- restore recreates VM from metadata using API and imports merged chain of data for each disk using imageio API

Disk image transfer mode exports data directly using OLVM 4.2+ API. There is no need to set up an export storage domain or setup LVM. This mode uses snapshot chains provided by OLVM.

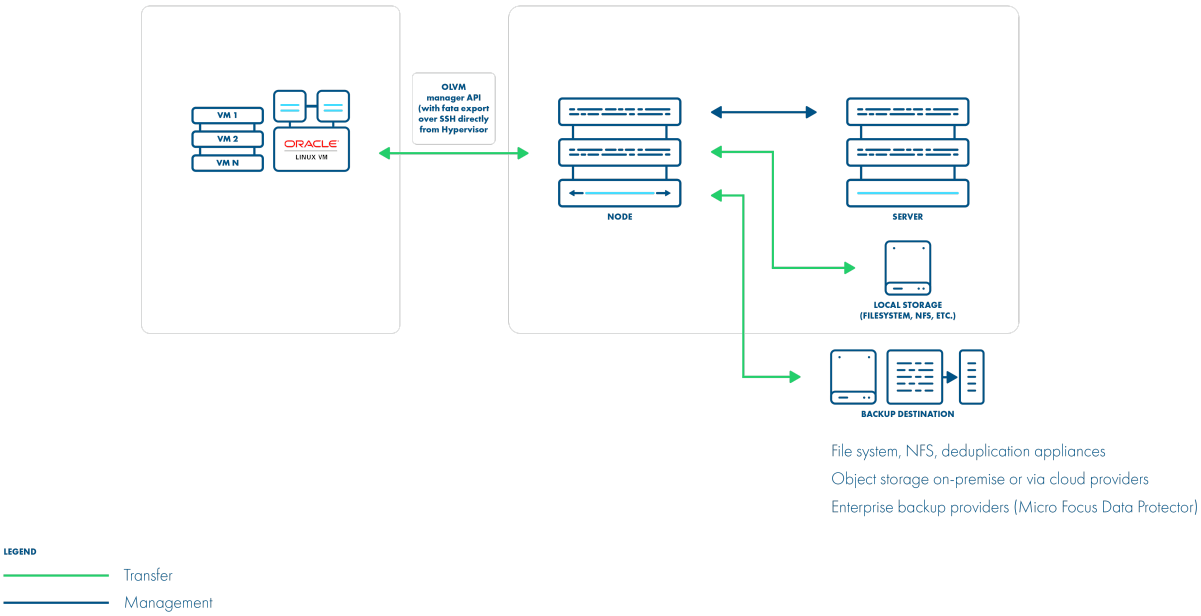
You may need to open communication for the additional port **54323** on the OLVM manager - it needs to be accessible from Data Protector for Cloud Workloads Node. Also, make sure that your **ovirt-imageio-proxy** services are running and properly configured (you can verify it by trying to upload images with OLVM UI).

Follow the steps in this section: Full versions of libvirt/qemu packages installation.

SSH transfer

This is an enhancement to the disk image transfer API strategy. It allows Data Protector for Cloud Workloads to use OLVM API v4.2+ (HTTPS connection to OLVM manager) only to collect metadata. Backup is done over SSH directly from the hypervisor (optionally using netcat for transfer), import is also using SSH (without the netcat option). There is no

need to install a node on the OLVM environment. This method can significantly boost backup transfers and supports incremental backups.



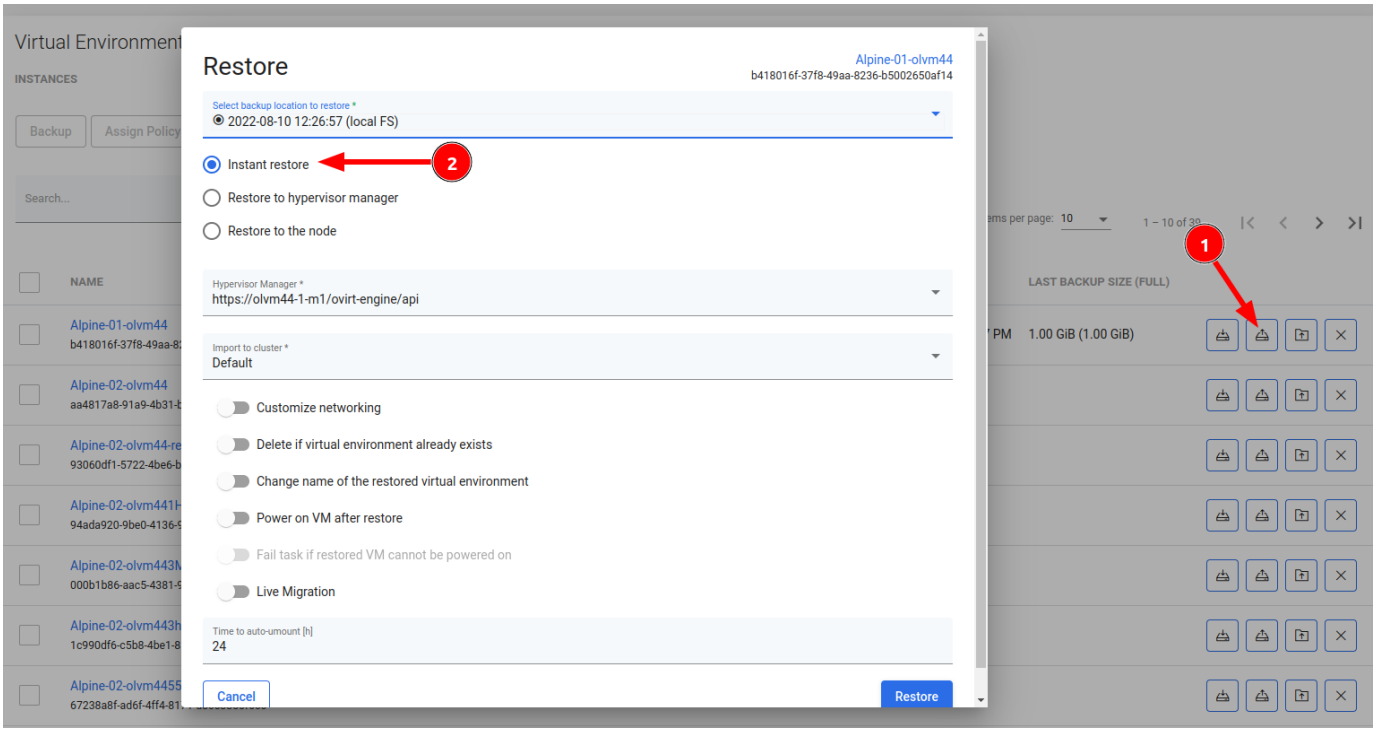
Backup Process

- crash-consistent snapshot using hypervisor's API
- optionally FS freeze can be executed before snapshot can be executed (FS thaw once the snapshot is completed) if enabled and guest tools installed inside
- optional application consistency using pre/post snapshot command execution • metadata exported from API
- data transfer via SSH (optional using netcat) - the full chain of disk snapshot files for each disk o if LVM-based storage is used, then node activates volumes if necessary to read data o if Gluster FS is used, then disk files are copied directly
- incremental backup export just sub-chain of QCOW2-deltas snapshots since last stored snapshot
- the last snapshot kept on the hypervisor for the next incremental backup (if at least one schedule assigned to the VM has a backup type set to incremental)
- restore recreates VM with empty storage from metadata using API and imports merged data over SSH to appropriate location on a hypervisor

This method assumes that all data transfers are directly from the hypervisor over SSH. This means that after adding OLVM manager and detecting all available hypervisors - **you also need to provide SSH credentials or SSH keys for each of the hypervisors**. You can also use SSH public key authentication.

Instant restore

To use an instant restore feature, backup destination from which VM will be restored, has to be of a synthetic type. The restore process creates a NFS share on the Data Protector for Cloud Workloads node, later this share is attached to the RHV as a new storage domain. Then it creates a new virtual machine and attaches the disks from the newly created storage domain to it. To use instant restore you have to click the restore button in the instances list and choose the option **instant restore**.



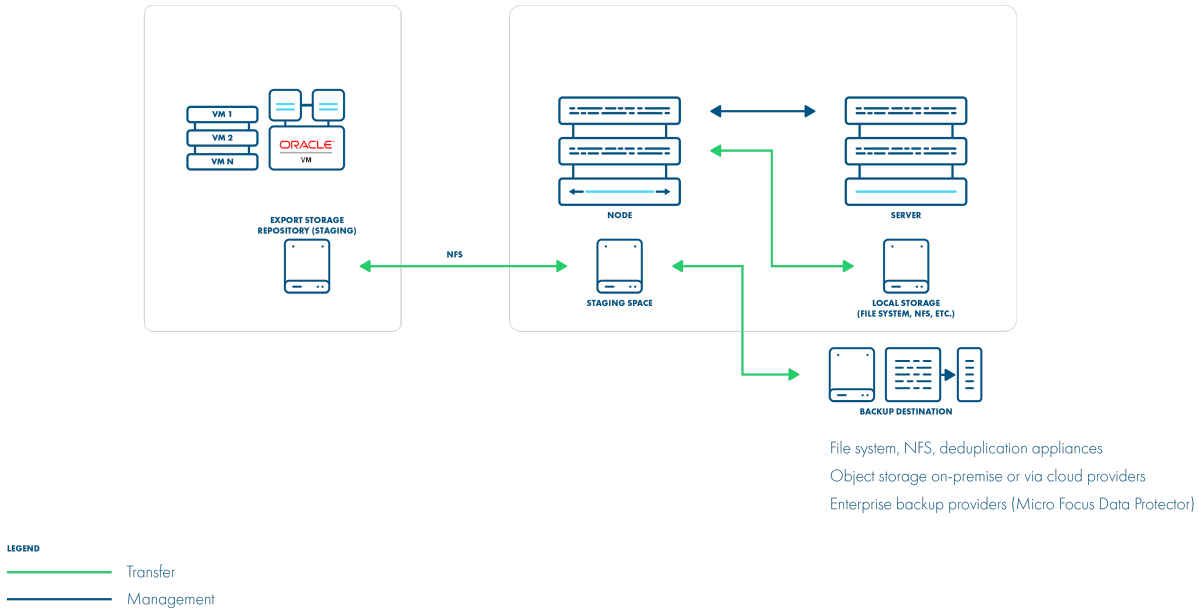
Live migration

You can enable the live migration option during instant restore. It will automatically start the disks migration to the chosen storage after the VM is restored and powered on.

Oracle VM

Deployment in Oracle VM environment

The Oracle VM environment requires you to create storage used for VM export. The export storage repository should also be accessible by Data Protector for Cloud Workloads Node in its staging directory. This implies that storage space doesn't have to be exported by Data Protector for Cloud Workloads Node - it can be mounted from an external source. The only requirement is to have it visible from both OVM hosts and Node itself. Keep in mind that ownership of the files on the share should allow both Data Protector for Cloud Workloads and OVM to read and write files.



Backup Process

- crash-consistent snapshot is taken by OVM during hot-clone of the VM
- data + metadata exported by the manager to the Data Protector for Cloud Workloads staging space (visible as the export Storage Repository in OVM)
- full backup only is supported
- OVM exports are limited to 1 task per Storage Repository being used by VM (this is the _**_limitation of OVM)
- restore is done to the export Storage Repository, the administrator needs to clone the VM using manager UI

> **Note:**
>
> - If the virtual machines are running on NFS storage, you must shut down the Oracle virtual machines to perform the backup
> - Make sure the NFS share have the Data Protector for Cloud Workloads user UID and GID
> - The directory under / vprotect_data needs to be the same name as the OVS server pool name
> - Oracle VM needs to disable services (nfslock , rpcbind**)**
> - Restore of VM is multi-step
> - Restore to the staging space on vNode
> - Move VM from the staging space to the Oracle protection repository
> - Migrate the VM into the Oracle server pool

Oracle VM environments require storage repositories to be defined for each server pool and must be mounted on Data Protector for Cloud Workloads Node.

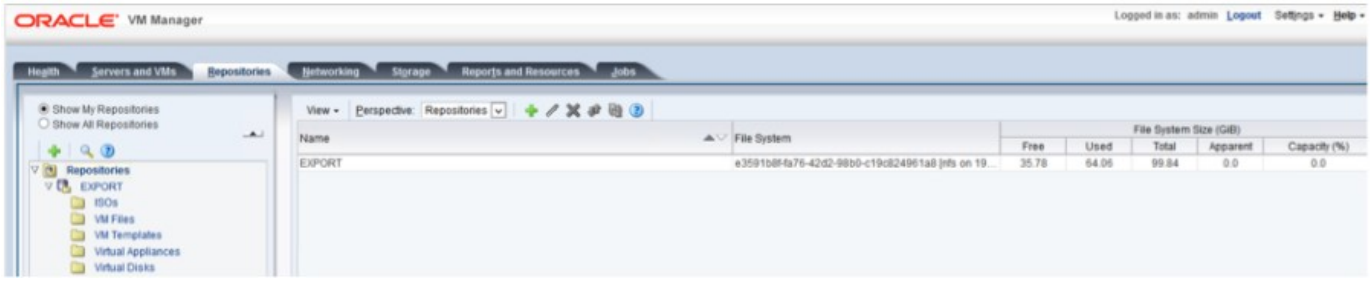
1. Create a repository from NFS share on Data Protector for Cloud Workloads Node
    - One server pool should have a separate subdirectory in the export path i.e. `/vprotect_data/pool01`, `/vprotect_data/pool2` - each subdirectory is a separate NFS share
    - The export (staging) path in the above-mentioned scenario is still `/vprotect_data`, while `pool01` and `pool02` are server pool names
    - Specify mapping between server pool names and storage repository names in the hypervisor manager configuration
    - Note that the export must be set to use the UID and GID of the `vprotect` user
    - Example export configuration in `/etc/exports` to the selected hypervisor in the RHV cluster:

      ```
      /vprotect_data/pool01    10.50.1.101(fsid=6,rw,sync,insecure,
      all_squash,anonuid=993,anongid=990)
      /vprotect_data/pool02    10.50.1.102(fsid=7,rw,sync,insecure,
      all_squash,anonuid=993,anongid=990)
      ```

      where `anonuid=993` and `anongid=990` should have the correct UID and GID returned by command:

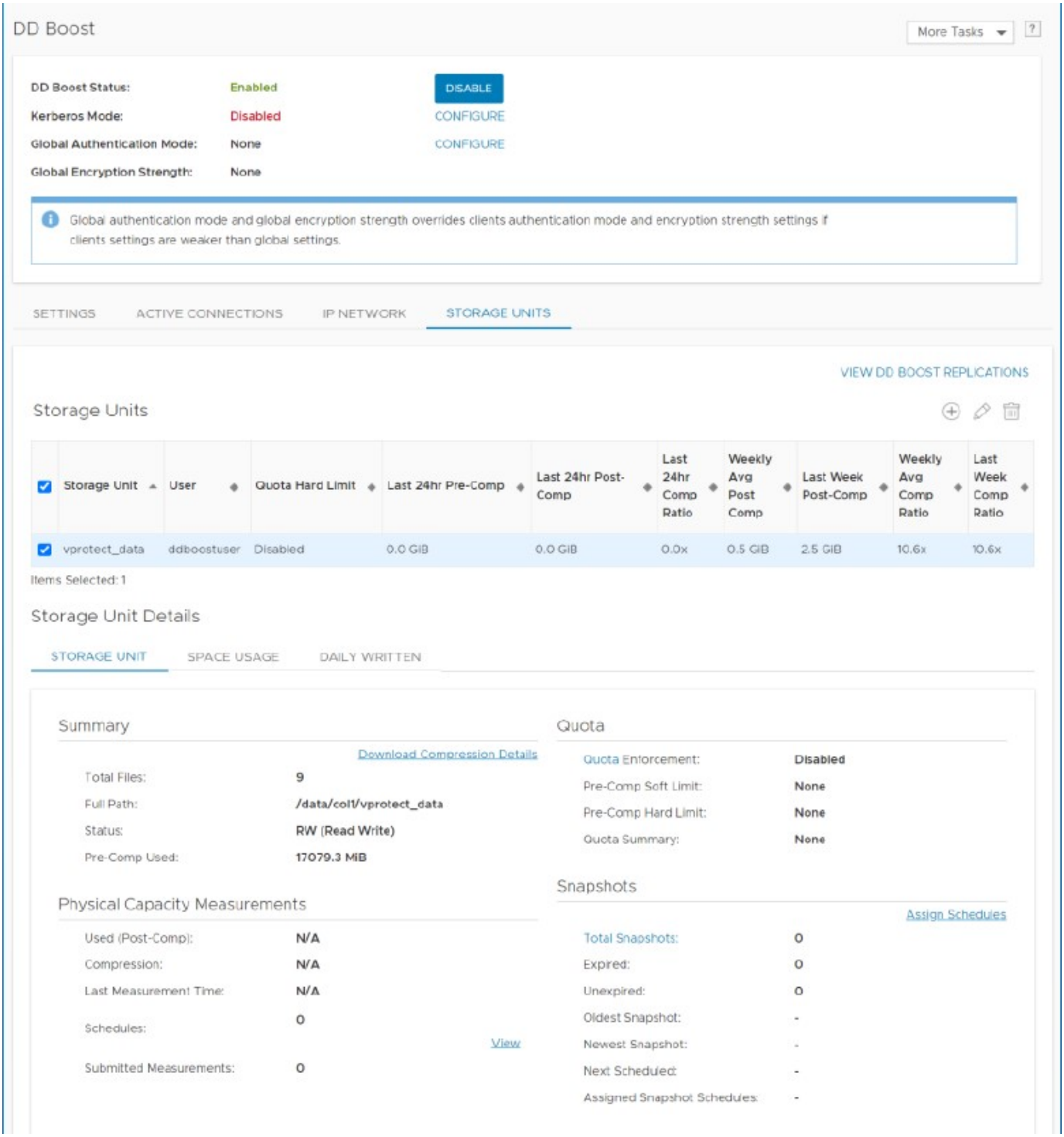
      ```
      [root@vProtect3 ~]# id vprotect
      uid=993(vprotect) gid=990(vprotect) groups=990(vprotect)
      ```

2. Both import and export operations will be done using these NFS shares – restore will be done directly to this storage domain, so you can easily import the backup into the Oracle VM environment
    - Backups must be restored to the export path (the node automatically changes the names to the original paths that are recognized by the OVM manager.

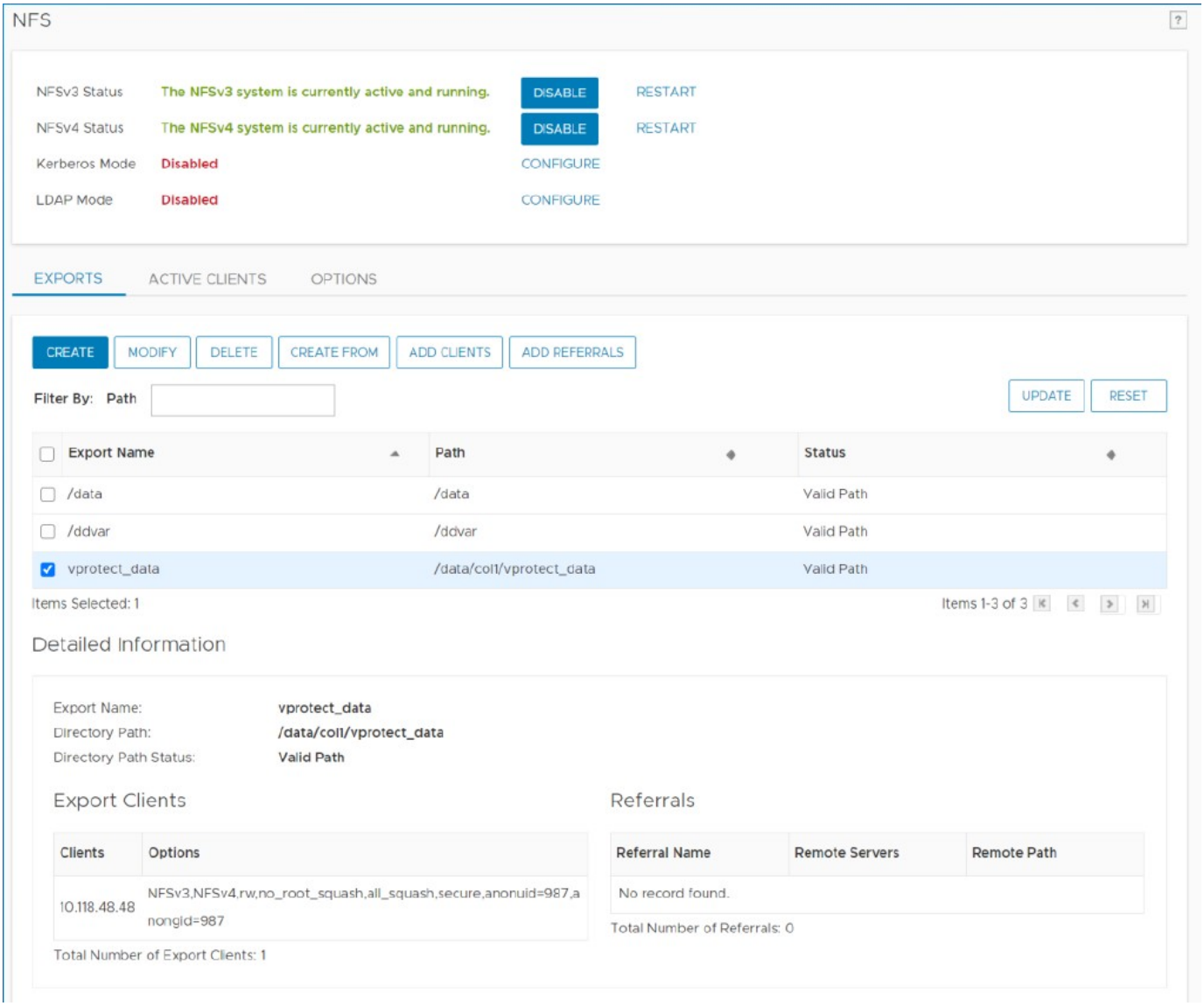


Example - How to configure OVM protection with PowerProtect DD

- Create a DDBoost device



- Create NFS share



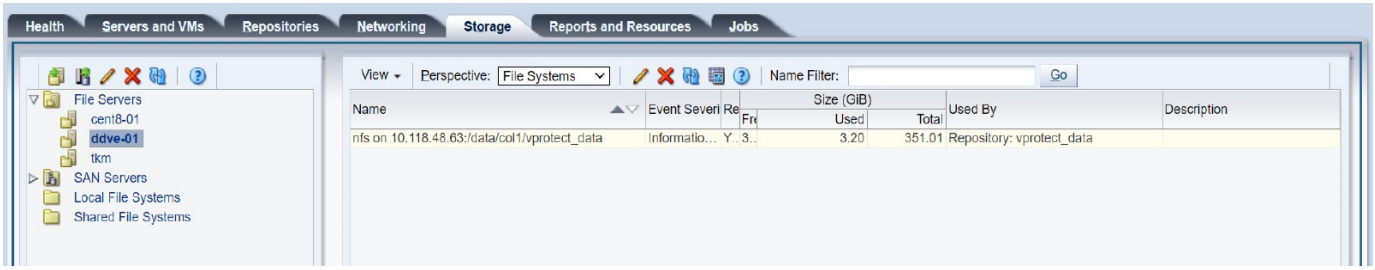
- Mount the DDBoost device on Data Protector for Cloud Workloads Node

```
#
# /etc/fstab
# Created by anaconda on Thu Oct  8 19:19:19 2020
#
# Accessible filesystems, by reference, are maintained under '/dev/disk/'.
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info.
#
# After editing this file, run 'systemctl daemon-reload' to update systemd
# units generated from this file.
#
/dev/mapper/cl-root                       /              xfs     defaults                                0 0
UUID=a41bae84-ba8d-4b6a-86fa-9d4f5b3a0396 /boot          ext4    defaults                                1 2
/dev/mapper/cl-swap                       swap           swap    defaults                                0 0
10.118.48.63:/vprotect_data               /vprotect_data boostfs defaults,_netdev,bfsopt(allow-others=true)  0 0
[root@cent8-02 MyServerPool]#
```

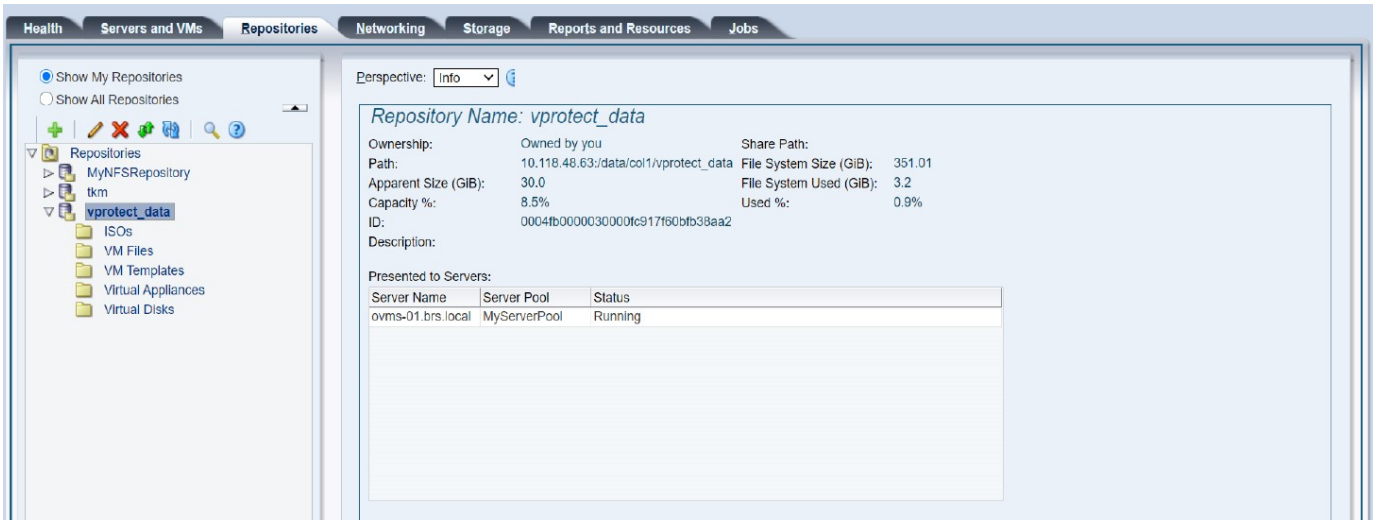
- Create symbolic links for the OVM Pool name (MyServerPool) to BoostFS mount point command, for example: ln -s /vprotect_data /MyServerPool

```
[root@cent8-02 MyServerPool]# ls -l
合計 5
drwx------ 2 vprotect vprotect 101 12月   7 11:43 Assemblies
drwx------ 2 vprotect vprotect 101 12月   7 11:43 ISOs
lrwxrwxrwx 1 root     root      14 12月   7 11:30 MyServerPool -> /vprotect_data
drwx------ 2 vprotect vprotect 101 12月   7 11:43 Templates
drwx------ 2 vprotect vprotect 101 12月   7 14:52 VirtualDisks
drwx------ 2 vprotect vprotect 101 12月   7 14:52 VirtualMachines
drwxr-xr-x 2 vprotect vprotect 101 12月   7 13:00 app-e87278af-a794-493e-be44-56a610094f9a
drwxr-xr-x 3 vprotect vprotect 156 12月   7 11:36 backups
drwxr-xr-x 2 vprotect vprotect 101 12月   7 11:32 import
drwxr-xr-x 2 vprotect vprotect 101 12月   7 11:32 mount
```

- Create a Storage Server for DD NFS Share



- Create a Repository using DD



- Add the OVM Hypervisor Manager to Data Protector for Cloud Workloads

> ***Note:*** *You can get the "Storage Repository ID" from the "OVM repositories" menu shown in the previous step*

Add New Hypervisor Manager

Choose type
Oracle VM

URL *
https://ovmm-01.brs.local:7002

Username *
admin

Password *
••••••••••••

Show password

Choose Node Configuration
Default Config

Job status polling interval [s] *
3

Pool to Repository mappings

Add Mapping

Server Pool name *
MyServerPool

Storage Repository ID
00004fb0000030000fc0bfb38aa2

Override export clone type

Cancel

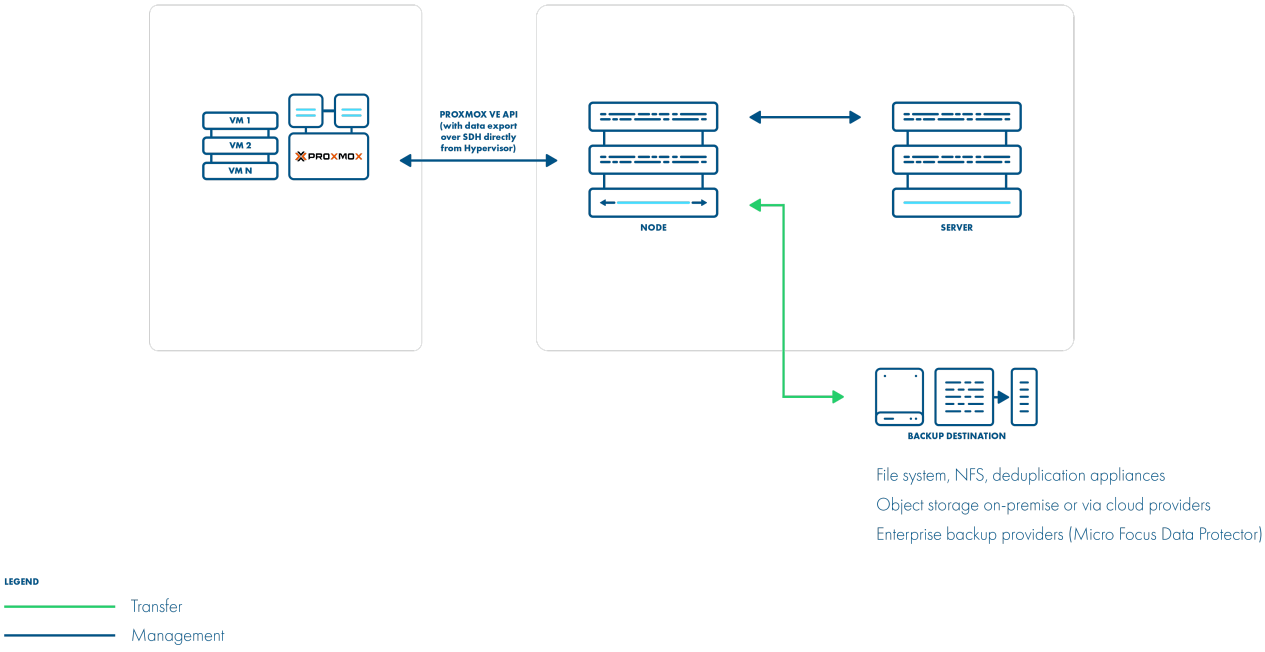
Save

Proxmox VE

SSH Transfer

SSH Transfer strategy:

- supports Proxmox 5.0+
- supports only QCOW2 disk images
- supports incremental backups
- supports over iSCSI



Backup is done by transferring QCOW2 disk images over SSH directly from the hypervisor (optionally using Netcat for transfer). Metadata is backed up only in the full backup. This method supports incremental backups where the last snapshot is required for the next incremental backups. The resulting backup has separate files for each disk + metadata, so you have the option to exclude specific drives as well.

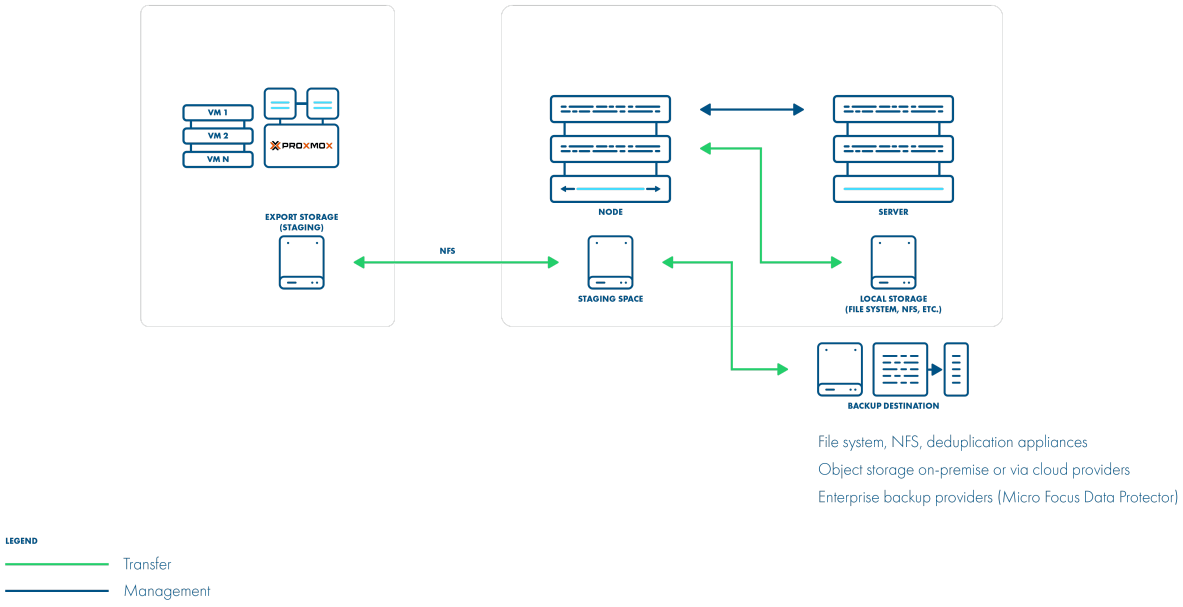
Backup Process

- QCOW2 - file-based storage only
- crash-consistent snapshots created using hypervisor CLI over SSH
- optionally FS freeze can be executed before snapshot can be executed (FS thaw once the snapshot is completed) if enabled and guest tools installed inside
- QCOW2 snapshots mounted locally on the hypervisor and exported via SSH (optionally with netcat)
- for incremental backups, both last and currently created snapshots are mounted and block-difference is sent via SSH
- metadata exported via SSH • restore imports metadata and overwrites empty disks with data from a merged backup over SSH

Export storage repository

The Proxmox virtual environment requires you to create storage used for VM export. Export storage should also be accessible to Data Protector for Cloud Workloads Node in its staging directory. This implies that storage space doesn't have to be exported by Data Protector for Cloud Workloads Node - it can be mounted from an external source. The only

requirement is to have it visible from both Proxmox VE hosts and the Node itself. Keep in mind that ownership of the files on the share should allow both Data Protector for Cloud Workloads and Proxmox VE to read and write files.



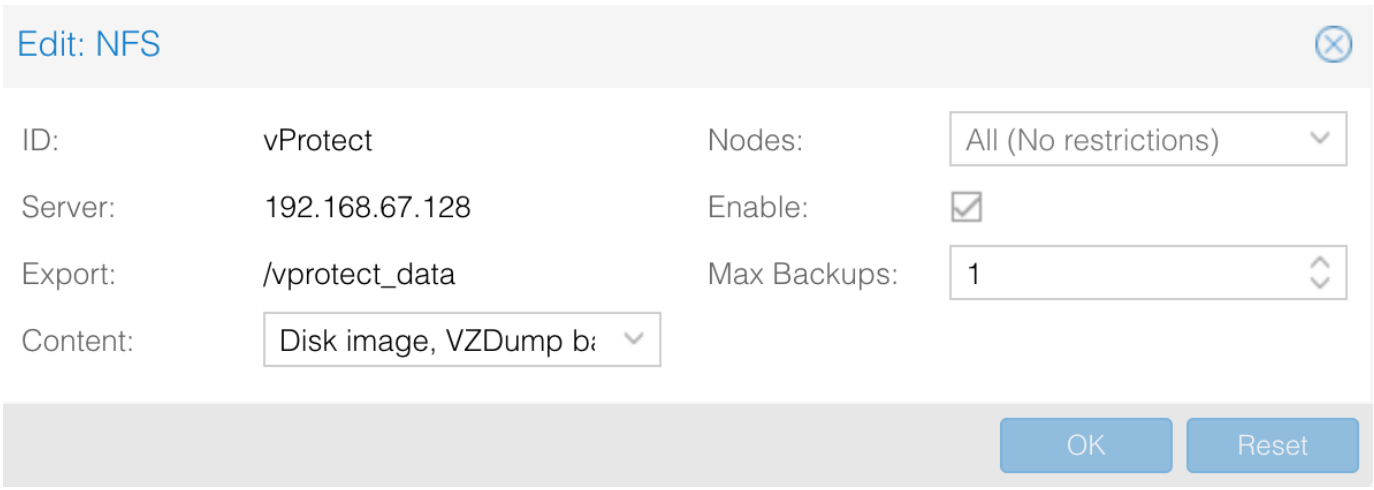
Backup Process

- native VM export is done to the prepared NFS storage (staging space on Data Protector for Cloud Workloads) using SSH access to the hypervisor
- crash-consistency - FS freeze used for VMs, LVM snapshot for containers
- optional application consistency using pre/post export command execution for VMs (pre/post snapshot) for containers
- data and metadata are in a single VMA image
- only full backups are supported • restore imports VMA image to the hypervisor

How to set up export storage repository backup

Proxmox virtual environments require backup storage to be defined on each server. This storage must be a location accessible from Data Protector for Cloud Workloads Node (the simplest setup, when you use only 1 node, is to create NFS share for the staging path on Data Protector for Cloud Workloads Node)

1. Create storage from NFS share (Content-type: **only VZDump**)



- Export share must be set to use the UID and GID of the `vprotect` user

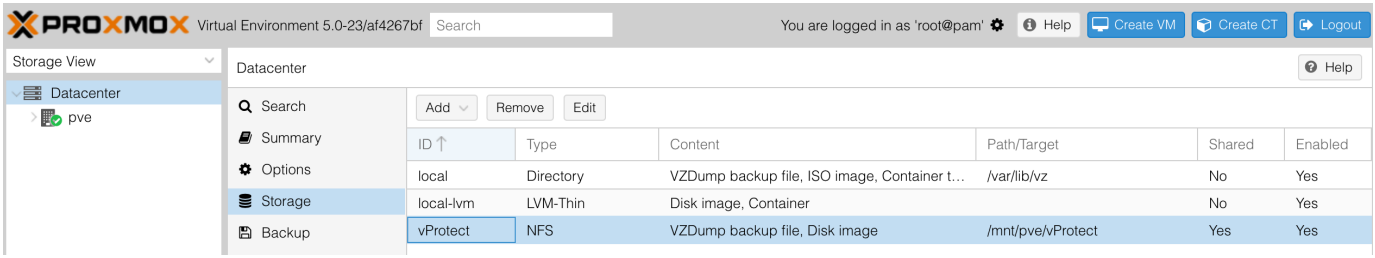
- Example export configuration in `/etc/exports` to the selected hypervisor in the cluster:

  ```
  /vprotect_data     PROXMOX_HOSTS(fsid=6,rw,sync,insecure,all_squash,
  anonuid=993,anongid=990)
  ```

  where `anonuid=993` and `anongid=990` should have correct UID and GID returned by command:

  ```
  [root@vProtect3 ~]# id vprotect
  uid=993(vprotect) gid=990(vprotect) groups=990(vprotect)
  ```

- Both import and export operations will be done using these NFS shares – restore will be done directly to this storage domain, so you can easily import the backup into Proxmox VE
  - backups must be restored to the export path (the node automatically changes names to the original paths that are recognized by Proxmox VE.
- A name for storage must be provided later in the **Virtual Environments** -> **Infrastructure** -> **Hypervisors**



File-level restore support for VMA images

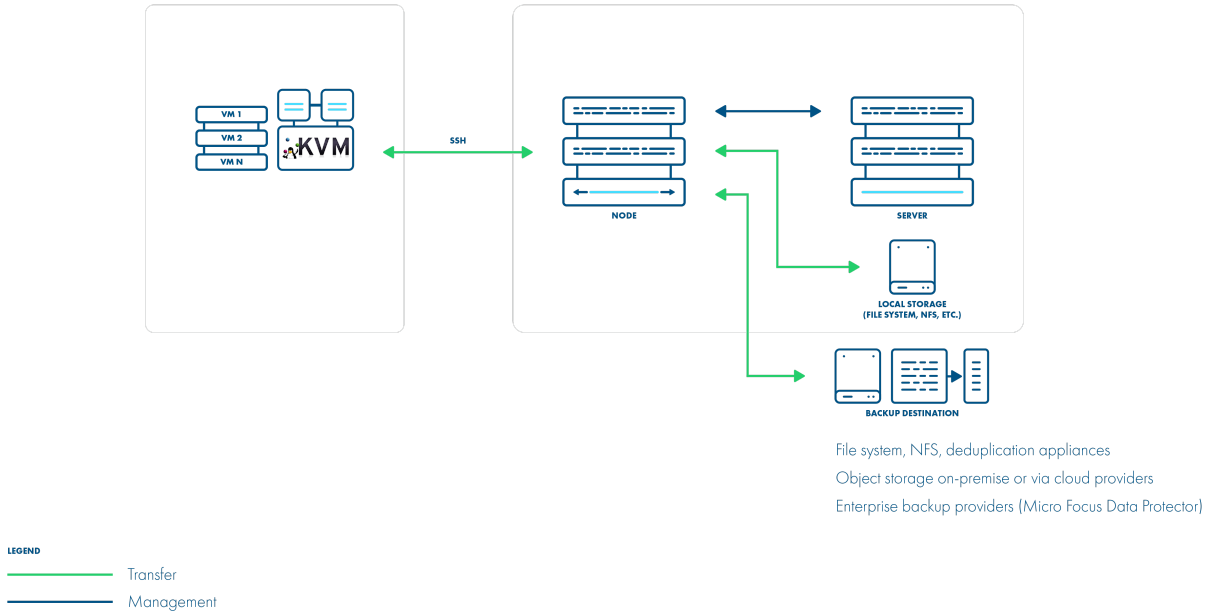
Prepare the VMA extractor on Data Protector for Cloud Workloads Node:

- build VMA extractor like this (requires Internet on the **node**):

  ```
  cd /opt/vprotect/scripts/vma
  ./setup_vma.sh
  ```<div style="page-break-after: always;"></div>
  ```

# KVM/Xen

Data Protector for Cloud Workloads access KVM/Xen (stand-alone libvirt) hosts over SSH. The Data Protector for Cloud Workloads Node can be installed outside of the environment.
  ```



Backup Process

- direct access to the hypervisor over SSH
- crash-consistent snapshot taken directly using virsh (QCOW2/RAW file), lvcreate (LVM), rbd snapshot for Ceph (separate call for each storage backend) For QCOW2/RAW file, virsh snapshot-create-as is used when VM is running - otherwise, qemu-img create is used
- optional application consistency using pre/post snapshot command execution
- QCOW2/RAW-file/LVM data exported over SSH (optionally with netcat)
- Ceph RBD data exported using rbd export or RBD-NBD when incremental is used If last stored snapshot is not missing, snapshot diffs are downloaded using rbd diff, then changes are written to inc file and diff file. If it is missing, export is treated as full, and then rbd export is used.
- libvirt XML metadata saved • last snapshot kept on the hypervisor for the next incremental backup (if at least one schedule assigned to the VM has backup type set to incremental)
- restore recreates files/volumes according to their backend (same transfer mechanism as used in backup) and then defines VM on the hypervisor

KVM/Xen (libvirt) environments require to have the correct entry in known_hosts on the **node**:

- it must be `known_hosts` file that belongs to `vprotect` user
- the algorithm must be set to `ssh-rsa`
- make sure to have in your Node Configuration `known_hosts` file-path set to the location that is accessible for `vprotect` user - default `/opt/vprotect/.ssh/known_hosts`
- if your user/group used on the KVM host is other than `qemu:qemu` then please provide them in hypervisor details form when you add/update the hypervisor

KVM - VG scanning

Used with LVM-based VMs only. In order to allow VG scanning please make sure to have your LVM packages up to date **on the hypervisor**. LVM reporting was one of the features added in RHEL/CentOS 7.3 and is used by Data Protector for Cloud Workloads to collect information about VGs.

KVM - full libvirt installation

CentOS-based KVM hypervisors may not have full libvirt available, specifically libvirt's `blockcommit` operation. If you need to change libvirt to the full version, please make sure to follow the steps in this section: Full versions of libvirt/qemu packages installation.

Public key authentication

If you prefer to authenticate by using public keys instead of a password, follow the steps described in SSH public key authentication section.

OpenStack

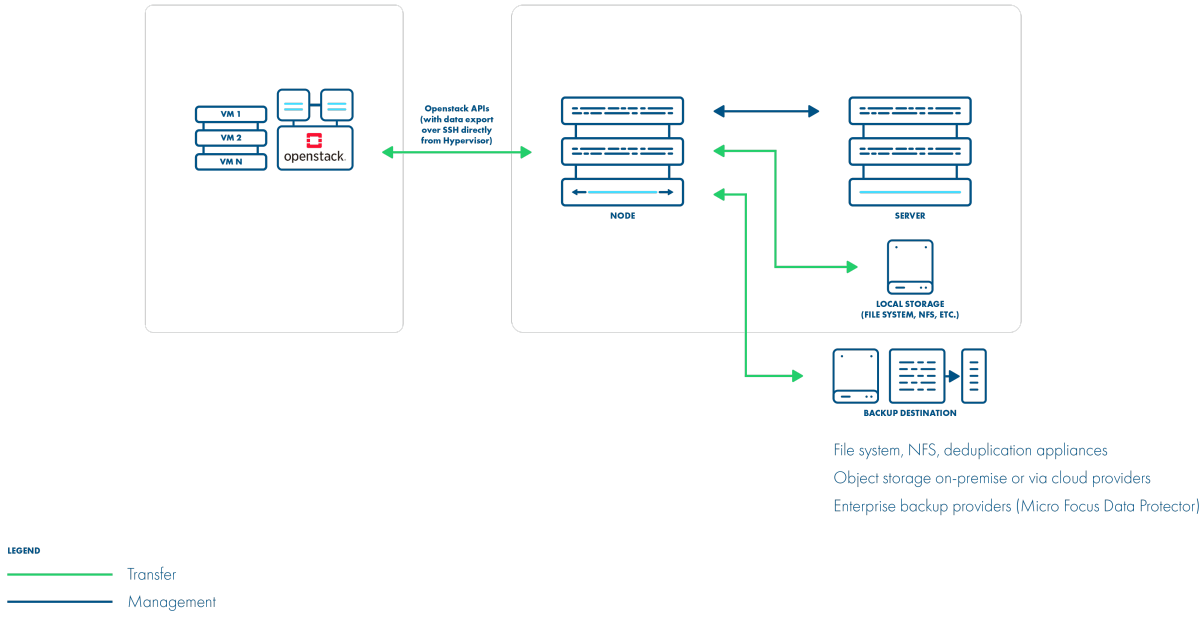
Data Protector for Cloud Workloads supports backup for OpenStack:

- Disk image transfer - for KVM hypervisors with VMs using QCOW2
- Volumes or Ceph-based storage:
    - supports incremental backup
    - disk images are transferred directly from API (no Proxy VM required)
- Disk attachment through Cinder:
    - supports all hypervisors and storages
    - no incremental backup
    - proxy VM is required - used for the disk attachment process.

Backup Strategies

Libvirt strategy

Data Protector for Cloud Workloads supports OpenStack environments that use KVM hypervisors and VMs running on QCOW2 or RAW files. Data Protector for Cloud Workloads communicates with OpenStack APIs such as Nova and Glance to collect metadata and for the import of the restored process. However, the actual backup is done over SSH directly from the hypervisor. The process is exactly the same as in Deployment in the KVM/Xen environment. Data Protector for Cloud Workloads Node can be installed anywhere - it just needs to have access to the OpenStack APIs and hypervisor SSH via a network. Both full and incremental backups are supported.



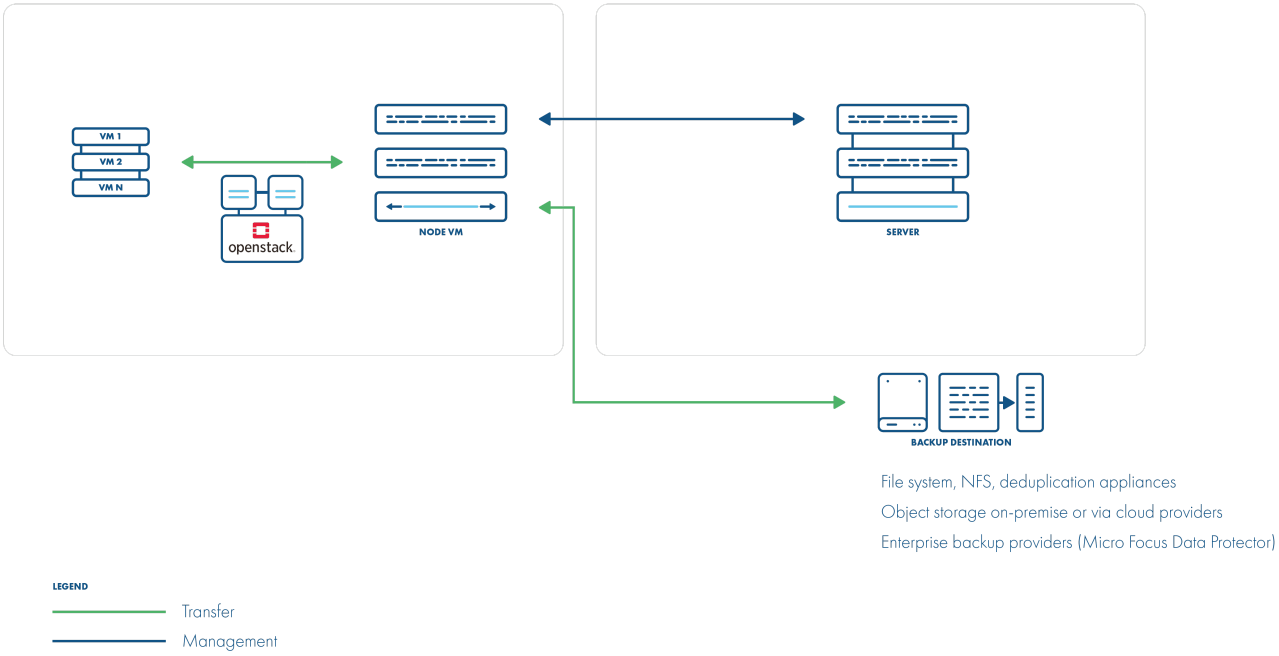
Backup Process

- direct access to the hypervisor over SSH
- crash-consistent snapshot taken directly using virsh (QCOW2/RAW file), rbd snapshot for Ceph (separate call for each storage backend)
- optional application consistency using pre/post snapshot command execution • QCOW2/RAW-file data exported over SSH (optionally with netcat)
- Ceph RBD data exported using rbd export or RBD-NBD when incremental is used

- metadata exported from OpenStack APIs (nova, glance, cinder)
- the last snapshot kept on the hypervisor for the next incremental backup (if at least one schedule assigned to the VM has backup type set to incremental)
- restore recreates files/volumes according to their backend (same transfer mechanism as used in backup) and then defines VM on the hypervisor

Disk attachment

Data Protector for Cloud Workloads also supports the disk-attachment method using cinder. This should allow you to use cinder-compatible storage and still allow Data Protector for Cloud Workloads to create backups. Currently, only a full backup is supported. Data Protector for Cloud Workloads needs to communicate OpenStack service's API to attach drives to the proxy VM with Data Protector for Cloud Workloads Node installed.



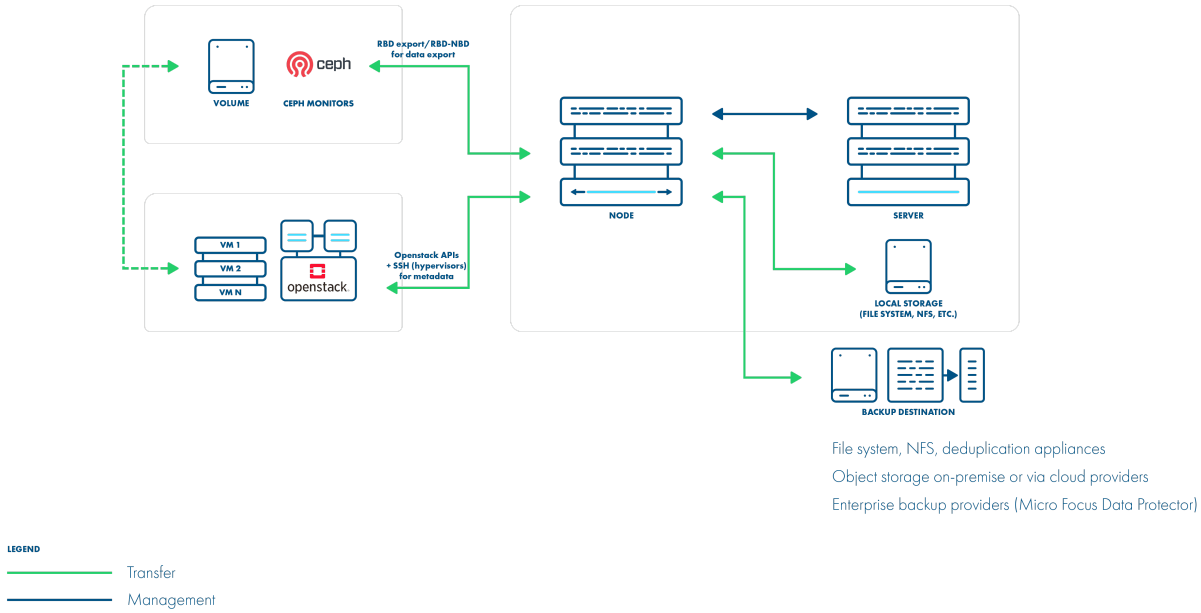
Backup Process

- crash-consistent snapshot using cinder API
- optional application consistency using pre/post snapshot command execution
- metadata exported from API
- volumes created from snapshotted disks are mounted one by one to the Proxy VM
- data read directly on the Proxy VM
- incremental backups are only supported for Ceph RBD - a list of the changed blocks are fetched from the monitors, and only these blocks are read from the attached disk on the Proxy VM
- if an instance is created from the glance image and "download image from glance" option is enabled data is downloaded from glance API, instance is created from the instance metadata and the images which is fetched from the glance API
- restore creates empty disks on the Proxy VM, imports merged data then recreates the VM using these volumes, it will try to use the image from a glance if present in the target environment or it will upload the image to the glance and register it with the restored VM

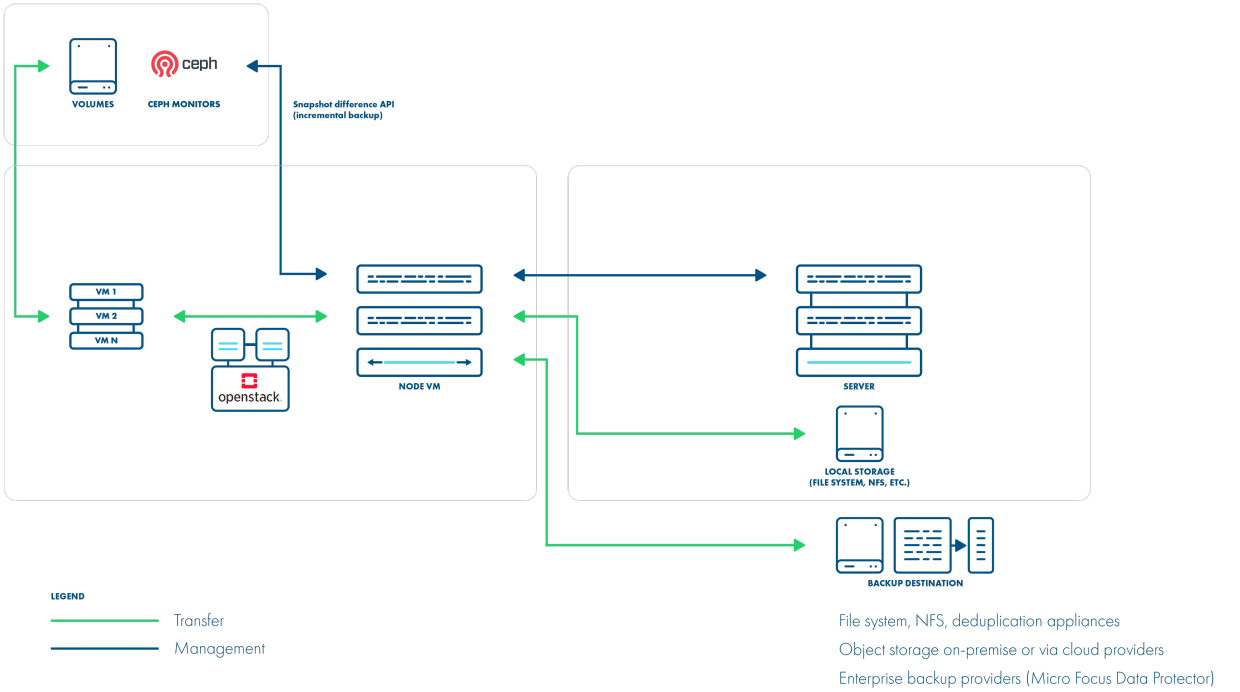
Ceph RBD storage backend

Data Protector for Cloud Workloads also supports deployments with Ceph RBD as a storage backend. Data Protector for Cloud Workloads communicates directly with Ceph monitors using RBD export/RBD-NBD when used with the Libvirt strategy or - when used with the Disk-attachment method - only during incremental backups (snapshot difference).

Libvirt strategy



Disk attachment strategy



Data Protector for Cloud Workloads supports OpenStack with Ceph RBD volumes. Here is an example of a typical (expected) section that needs to be added in **cinder.conf**for Ceph in the OpenStack environment:

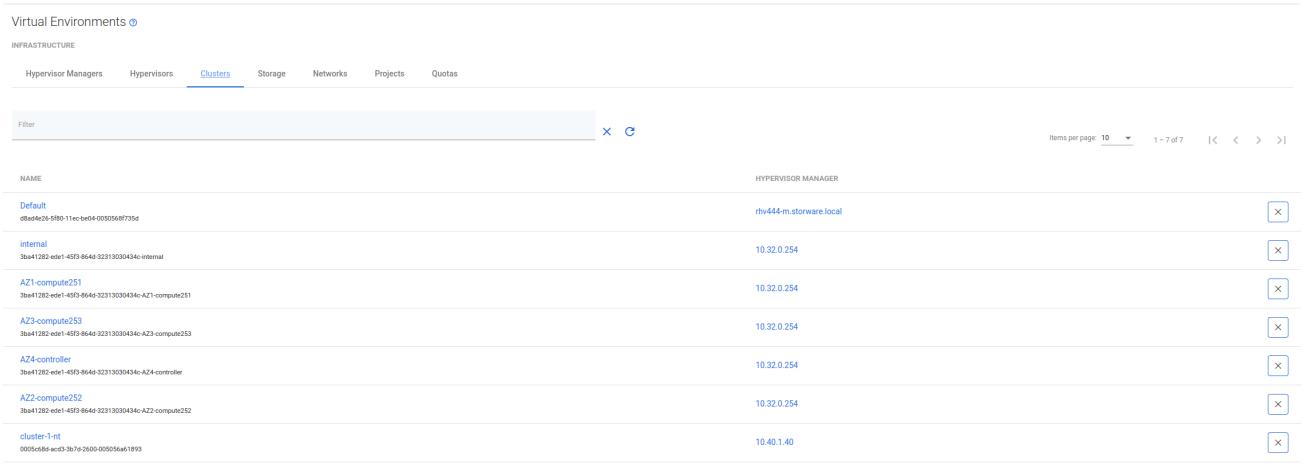
```
[rbd]
volume_backend_name = rbd
volume_driver = cinder.volume.drivers.rbd.RBDDriver
rbd_pool = volumes
rbd_ceph_conf = /etc/ceph/ceph.conf
```

```
rbd_flatten_volume_from_snapshot = false
rbd_max_clone_depth = 5
rbd_store_chunk_size = 4
rados_connect_timeout = -1
glance_api_version = 2
rbd_user = volumes
rbd_secret_uuid = ce6d1549-4d63-476b-afb6-88f0b196414f
```

A good article on how to set up Ceph with OpenStack can be found here.

To set up the Openstack HVM with Ceph RBD volumes in Data Protector for Cloud Workloads:

1. Add Ceph storage as described here
2. Add the hypervisor manager as described here.
3. Go to **Virtual Environments**-> **Infrastructure**-> **Clusters**and select cluster that is used by Openstack.



4. In **Storage Provider** field select previously added Ceph storage.

Now you can save and sync the inventory - if Ceph communication works properly you should be able to see Hypervisor Storage entries (in Hypervisors -> Storage tab) representing your Ceph storage pools.

QCOW2 files on NFS storage

Example: scenario QCOW2 files residing on NFS

You can configure the NFS volume backend here:

https://docs.openstack.org/cinder/rocky/admin/blockstorage-nfs-backend.html

Make sure the QCOW2 volumes are enabled.

For an NFS backend, it's recommended to set these values in **/etc/cinder/cinder.conf**:

```
default_volume_type=nfs nfs_sparsed_volumes = true nfs_qcow2_volumes = true volume_driver = cinder.volume.drivers.nfs.NfsDriver enabled_backends = nfs
```

Nova volumes

Data Protector for Cloud Workloads is able to backup nova volumes using libvirt strategy. In the hypervisor manager settings there is an option **Download image from glance**. When this option is enabled the original image from glance is downloaded, if it is disabled than the image is not downloaded, however the nova volume created from it is backed up.

Adding hypervisor managers

When creating the hypervisor manager, provide the following data in the fields:

URL - Keystone API URL, e.g. **http://10.201.32.40:5000/v3**

Authentication domain:

- name - name of domain
- domainId - optional domain id
- user - OpenStack user.
- password - password for that user.
- default project - name of default project in domain.

Scope VMs to Domain - you can create one or more Authentication Domains based on this setting, as described in the **Authentication Domains** section below.

Download image from glance - allows Data Protector for Cloud Workloads to use images from glance as described in the disk attachment strategy

When you index the hypervisor manager, **make sure you provide the correct SSH credentials** for each hypervisor that appeared on the Hypervisors tab. You can also use SSH public key authentication.

> **Note:** When restoring the instances, make sure that the provided user is a member of the target tenant.

Authentication Domains

Data Protector for Cloud Workloads supports OpenStack environments with multiple domains. Each OpenStack Hypervisor Manager needs to have at least one Authentication Domain provided.

Data Protector for Cloud Workloads supports two types of domain authorization:

- Unscoped - single credentials to multiple domains
- Scoped - single credentials to single domain

Single credentials to single domain

Scoping VMs to Domain option needs to be turned on.

In that setup user can create Authentication Domains for every Domain in OpenStack environment. Projects and Virtual Machines are only scanned in provided Authentication Domains.

Single credentials to multiple domains

Scoping VMs to Domain option needs to be turned off.

In that setup user need to create only one Authentication Domain. Projects and Virtual Machines are scanned in every domain that provided user has access to.

Openstack tags

To list tags for specific instance:

```
root@c254:~# nova show d6787375-ea0c-49fd-878b-35b71747c62a |grep tags
| tags                                 | ["test"]
```

Tags for Openstack requires nova API version >= 2.26.

Openstack Access Keys

During Inventory Synchronization Data Protector for Cloud Workloads scans all Keypairs (to which a user has access) and stores them as Access Keys. When restoring an instance, the user can specify the Access Key.

> **Note:** If the access key selected for restore is no longer present in the Openstack environment, it will be restored.

Openstack Flavor

During Inventory Synchronization Data Protector for Cloud Workloads scans all Flavors and saves their configuration. When restoring an instance, the user can specify the flavor.

> **Note:** If the flavor selected for restore is no longer present in the Openstack environment, it will be restored with the same configuration and availability as the original flavor.

Limitations

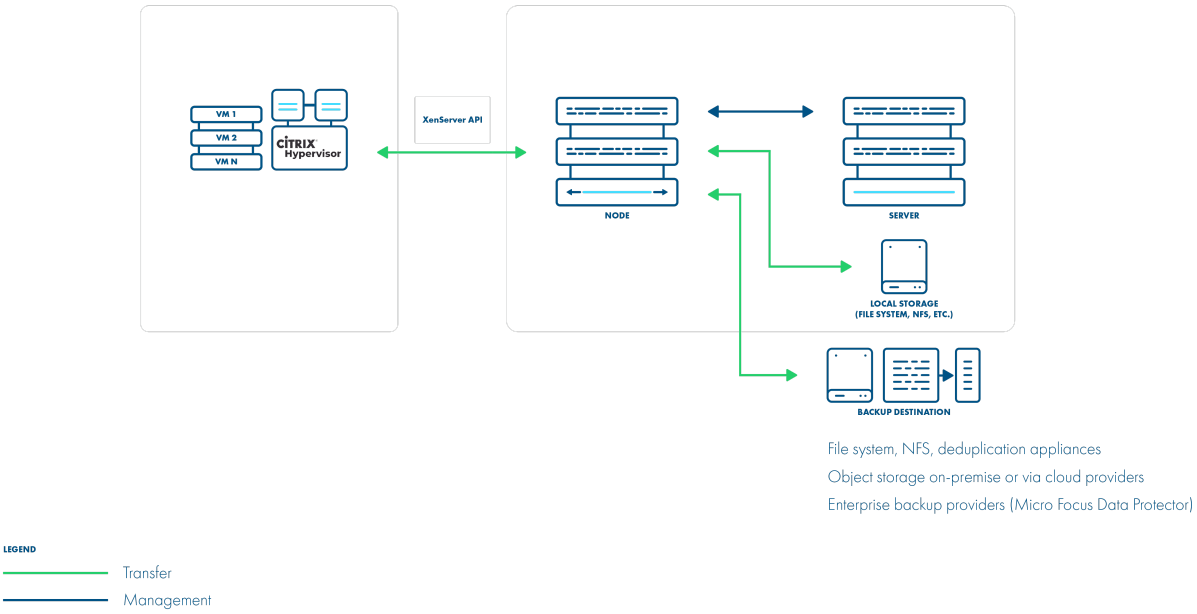
- Data Protector for Cloud Workloads does not backup and restores keypairs that were created by other OpenStack users than the one used in Data Protector for Cloud Workloads. The restored instance will have no keypairs assigned. In such a case, the keypairs have to be backed up and restored manually under the same name before restoring the instance.
- For the libvirt strategy only, QCOW2/RAW files or Ceph RBD are supported as the backend.
- The disk attachment method with Ceph requires access to the monitors from the Proxy VM.

Citrix Hypervisor (XenServer)

Backup Strategies

XVA-based

In this strategy, the VM is exported as a single XVA bundle containing all of the data. Incremental backup is also supported. Data is transferred directly from the XenServer API without the need to set up anything on the hosts.



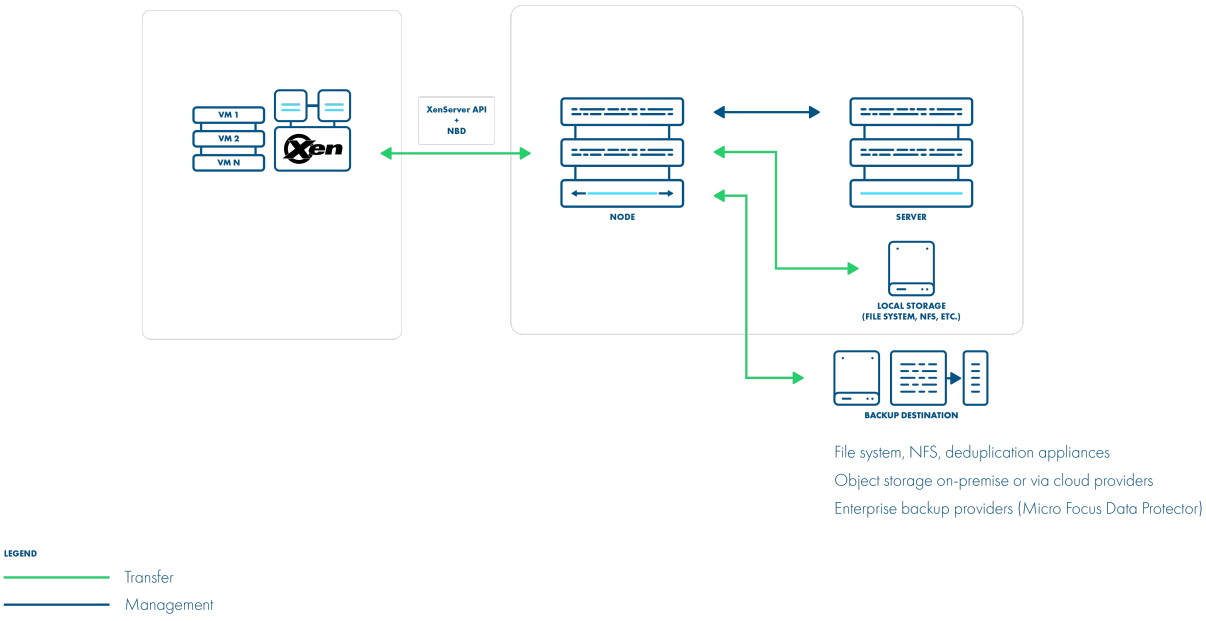
Backup Process

- crash-consistent snapshot using hypervisor's API only for full backups
- optionally quiesced snapshot can be done if enabled and guest tools installed inside - if quiesced snapshot has been failed we are doing regular one
- optional application consistency using pre/post snapshot command execution
- data export directly from the hypervisor using hypervisor's API - both full (XVA) and delta (VHD for each disk)
- full backup (XVA) contains metadata
- snapshot taken with full backup is kept on the hypervisor for the next incremental backup - if at least one schedule assigned to the VM has backup type set to incremental
- incremental backups are cumulative (all data since last full backup)
- restore recreates VM from XVA, and then applies changes from each incremental backup using Hypervisor APIs

Changed-Block Tracking

In this strategy, the VM is exported using XenServer API (full backup) and the Network Block Device service (NBD, incremental backups) on the XenServer hosts. The CBT feature in Citrix XenServer 7.3+ may require an additional license. The resulting backup has separate files for each disk + metadata, so you also have the option to exclude specific drives.

> **Note:** For full backups only you can still use this strategy without CBT enabled on the hypervisor.



Backup Process

- crash-consistent snapshot using hypervisor's API
- optionally quiesced snapshot can be done if enabled and guest tools installed inside - if quiesced snapshot has been failed we are doing regular one
- optional application consistency using pre/post snapshot command execution
- CBT enabled during full backup on each disk if it wasn't done earlier
- metadata exported from API
- full backup - each disk exported from API (RAW format)
- incremental backup - each disk queried for changed blocks and which are exported over NBD
- last snapshot kept on the hypervisor for the next incremental backup - if at least one schedule assigned to the VM has backup type set to incremental
- restore recreates VM from metadata using API and imports merged chain of data for each disk using API

Change Block Tracking setup

Citrix introduced the CBT mechanism in XenServer 7.3. In order to enable CBT backups, the following requirements must be met:

1. Citrix XenServer 7.3 or above must be used - note that CBT is a licensed feature
2. The NBD server must be enabled on the hypervisor
3. The NBD client and NBD module must be installed on Data Protector for Cloud Workloads Node

Notes on restore

1. When image-based backups (XVA) are used - Data Protector for Cloud Workloads restore VMs as templates and renames them appropriately after the restore
2. When separate disk backups are used:
    - if there is already a VM in the infrastructure with the UUID of the VM being restored (check `present` flag in VM list) - Data Protector for Cloud Workloads restores it as a new VM (MAC addresses will be generated)
    - otherwise Data Protector for Cloud Workloads attempts to restore the original configuration including MAC addresses

NBD Server setup (on XenServer)

1. Get the Network UUID that you intend to use for communication with Data Protector for Cloud Workloads - run on the XenServer shell:

```
[root@xenserver-cbt ~]# xe network-list
uuid ( RO)             : e16b4e34-47d4-9a6e-371b-65beb7252d69
       name-label ( RW): Pool-wide network associated with eth0
 name-description ( RW):
           bridge ( RO): xenbr0
..........
uuid ( RO)             : 244a2fa7-ae7c-e45c-819a-44cecf51e8fa
       name-label ( RW): Host internal management network
 name-description ( RW): Network on which guests will be assigned a private
link-local IP address which can be used to talk XenAPI
           bridge ( RO): xenapi
```

   For example: `e16b4e34-47d4-9a6e-371b-65beb7252d69`

2. Enable the NBD service on your hypervisor:

```
xe network-param-add param-name=purpose param-key=nbd
uuid=<network-uuid>
```

NBD Client setup (on Data Protector for Cloud Workloads Node)

Data Protector for Cloud Workloads comes with a pre-built RPM and modules for CentOS 7 distribution.

1. Go to the NBD directory:

```
cd /opt/vprotect/scripts/nbd
```

2. Use `yum` to install the NBD client:

```
yum -y install nbd-3.16.1-1.el7.centos.x86_64.rpm
```

3. If your Linux does not have the NBD module installed you may try to build one yourself (there is a script for Red Hat based distributions that downloads the kernel, enables the NBD module, and builds it) or use an already provided module:

   - you can compile the module by running:

```
./compile_nbd_module.sh
```

   - if you have Centos 7, you also may use a pre-built module (for CentOS 7.4.1708 with kernel 3.10.0-693.5.2) - which is `nbd.ko`

4. Enable the module by invoking the script (the following command will either use a module in your kernel or copy the provided `nbd.ko`):

```
./enable_nbd.sh
```

5. Verify that you have `/dev/nbd*` devices available on your Data Protector for Cloud Workloads Node host:

```
[root@localhost nbd]# ls /dev/nbd*
/dev/nbd0  /dev/nbd1  /dev/nbd10  /dev/nbd11  /dev/nbd12  /dev/nbd13
/dev/nbd14  /dev/nbd15  /dev/nbd2  /dev/nbd3  /dev/nbd4  /dev/nbd5
/dev/nbd6  /dev/nbd7  /dev/nbd8  /dev/nbd9
```

6. Restart your Data Protector for Cloud Workloads Node:

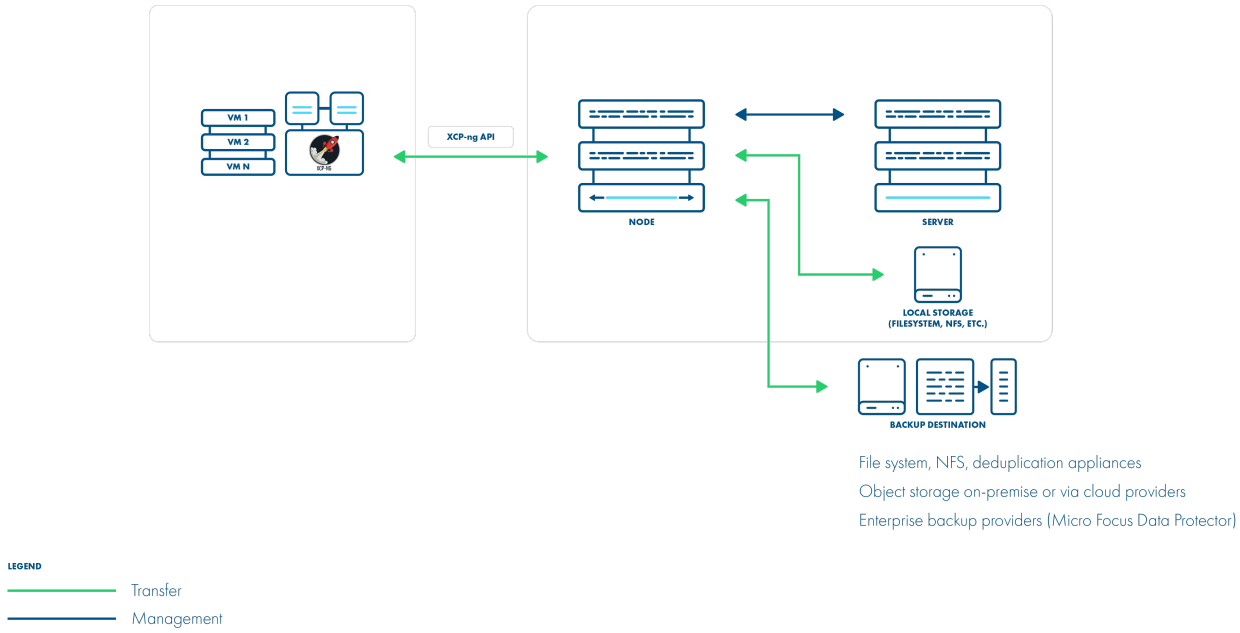
```
systemctl restart vprotect-node
```

XCP-ng

Backup Strategies

XVA-based

In this strategy, the VM is exported as a single XVA bundle containing all of the data. Incremental backup is also supported. Data is transferred directly from the XenServer API without the need to set up anything on the hosts.



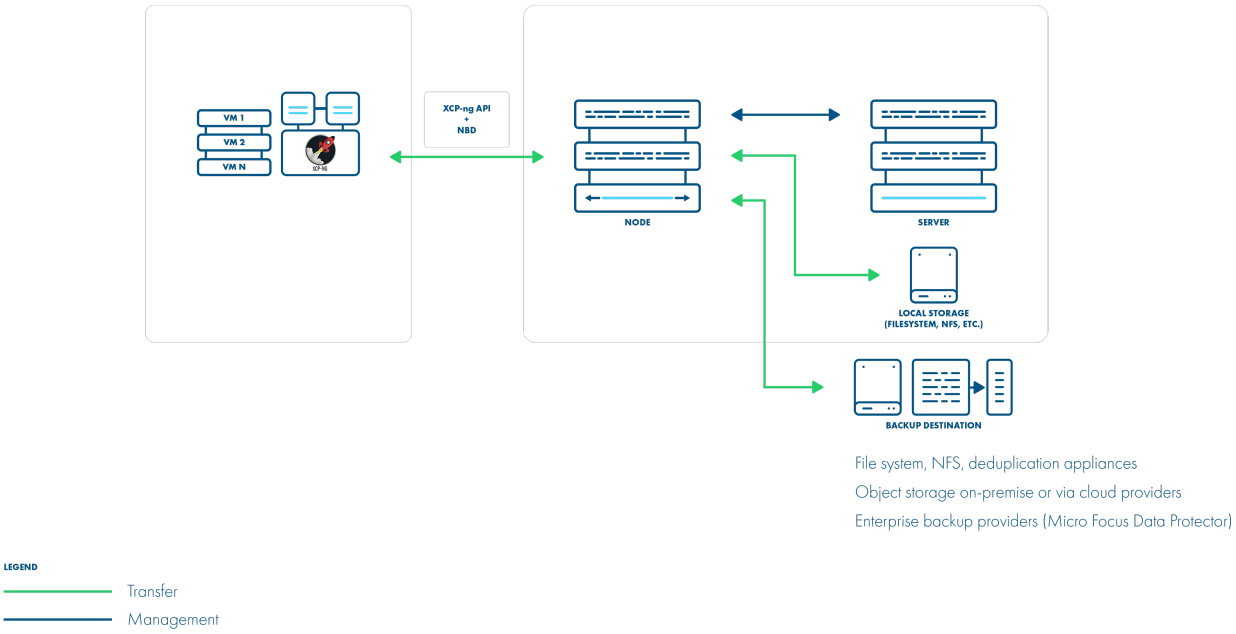
Backup Process

- crash-consistent snapshot using hypervisor's API only for full backups
- optionally quiesced snapshot can be done if enabled and guest tools installed inside - if the quiesced snapshot has been failed we are doing regular one
- optional application consistency using pre/post snapshot command execution
- data export directly from the hypervisor using hypervisor's API - both full (XVA) and delta (VHD for each disk)
- full backup (XVA) contains metadata
- snapshot taken with full backup is kept on the hypervisor for the next incremental backup - if at least one schedule assigned to the VM has backup type set to incremental
- incremental backups are cumulative (all data since last full backup)
- restore recreates VM from XVA, and then applies changes from each incremental backup using Hypervisor APIs

Changed-Block Tracking

In this strategy, the VM is exported using XenServer API (full backup) and the Network Block Device service (NBD, incremental backups) on the XenServer hosts. The CBT feature in Citrix XenServer 7.3+ may require an additional license. The resulting backup has separate files for each disk + metadata, so you also have the option to exclude specific drives.

> **Note:** For full backups only you can still use this strategy without CBT enabled on the hypervisor.



Backup Process

- crash-consistent snapshot using hypervisor's API
- optionally quiesced snapshot can be done if enabled and guest tools installed inside - if the quiesced snapshot has been failed we are doing regular one
- optional application consistency using pre/post snapshot command execution
- CBT enabled during full backup on each disk if it wasn't done earlier
- metadata exported from API
- full backup - each disk exported from API (RAW format)
- incremental backup - each disk queried for changed blocks and which are exported over NBD
- the last snapshot is kept on the hypervisor for the next incremental backup - if at least one schedule assigned to the VM has a backup type set to incremental
- restore recreates VM from metadata using API and imports merged chain of data for each disk using API

Change Block Tracking setup

Citrix introduced the CBT mechanism in XenServer 7.3. In order to enable CBT backups, the following requirements must be met:

1. Citrix Hypervisor 7.3 (XCP-ng 7.4) or above must be used - note that CBT is a licensed feature
2. The NBD server must be enabled on the hypervisor
3. The NBD client and NBD module must be installed on Data Protector for Cloud Workloads Node (Data Protector for Cloud Workloads should take care of this automatically during installation)

Notes on restore

1. When image-based backups (XVA) are used - Data Protector for Cloud Workloads restore VMs as templates and renames them appropriately after the restore
2. When separate disk backups are used:
    - if there is already a VM in the infrastructure with the UUID of the VM being restored (check `present` flag in VM list) - Data Protector for Cloud Workloads restore it as a new VM (MAC addresses will be generated)

- otherwise Data Protector for Cloud Workloads attempts to restore the original configuration including MAC addresses

NBD Server setup (on XenServer)

1. Get the Network UUID that you intend to use for communication with Data Protector for Cloud Workloads - run on the XenServer shell:

```
[root@xenserver-cbt ~]# xe network-list
uuid ( RO)             : e16b4e34-47d4-9a6e-371b-65beb7252d69
       name-label ( RW): Pool-wide network associated with eth0
 name-description ( RW):
           bridge ( RO): xenbr0
.....
uuid ( RO)             : 244a2fa7-ae7c-e45c-819a-44cecf51e8fa
       name-label ( RW): Host internal management network
 name-description ( RW): Network on which guests will be assigned a private
link-local IP address which can be used to talk XenAPI
           bridge ( RO): xenapi
```

   For example: `e16b4e34-47d4-9a6e-371b-65beb7252d69`

2. Enable the NBD service on your hypervisor:

```
xe network-param-add param-name=purpose param-key=nbd
uuid=<network-uuid>
```

NBD Client setup (on Data Protector for Cloud Workloads Node)

> **Note:** This part is done by Data Protector for Cloud Workloads automatically during installation. The article may be helpful in case of problems with the NBD module.

Data Protector for Cloud Workloads comes with a pre-built RPM and modules for CentOS 7 distribution.

1. Go to the NBD directory:

```
cd /opt/vprotect/scripts/nbd
```

2. Use `yum` to install the NBD client:

```
yum -y install nbd-3.16.1-1.el7.centos.x86_64.rpm
```

3. If your Linux does not have the NBD module installed you may try to build one yourself (there is a script for Red Hat based distributions that downloads the kernel, enables the NBD module, and builds it) or use the already provided module:

   - you can compile the module by running:

```
./compile_nbd_module.sh
```

- if you have Centos 7, you also may use the pre-built module (for CentOS 7.4.1708 with kernel 3.10.0-693.5.2) - which is `nbd.ko`

4. Enable the module by invoking the script (the following command will either use a module in your kernel or copy the provided `nbd.ko`):

```
./enable_nbd.sh
```

5. Verify that you have `/dev/nbd*` devices available on your Data Protector for Cloud Workloads Node host:

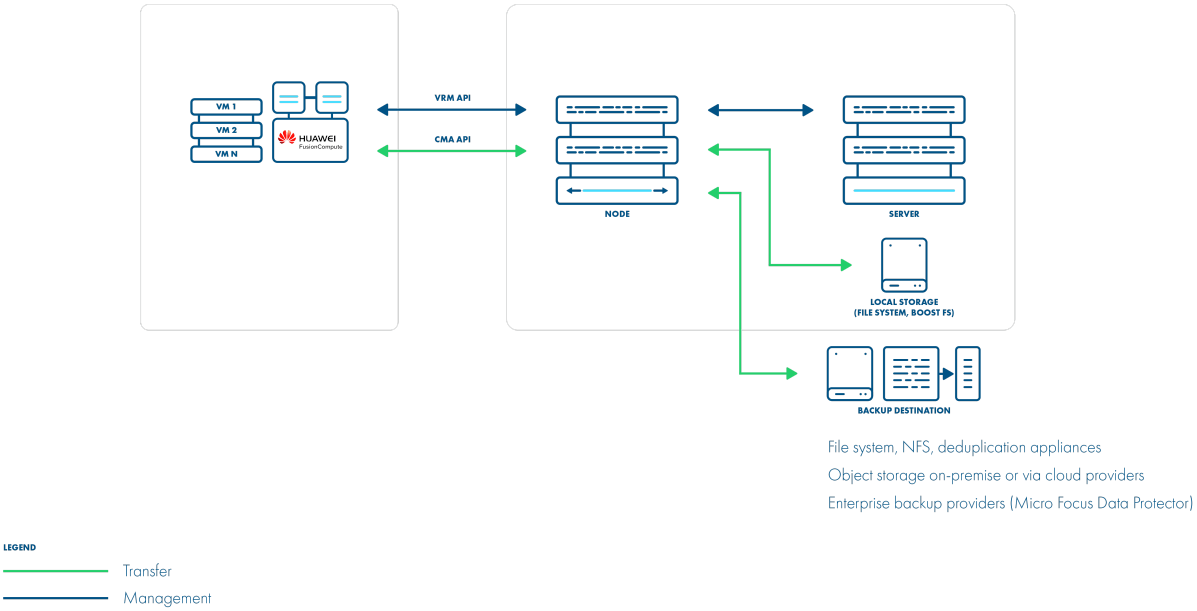
```
[root@localhost nbd]# ls /dev/nbd*
/dev/nbd0  /dev/nbd1  /dev/nbd10  /dev/nbd11  /dev/nbd12  /dev/nbd13
/dev/nbd14  /dev/nbd15  /dev/nbd2  /dev/nbd3  /dev/nbd4  /dev/nbd5
/dev/nbd6  /dev/nbd7  /dev/nbd8  /dev/nbd9
```

6. Restart your Data Protector for Cloud Workloads Node:

```
systemctl restart vprotect-node
```

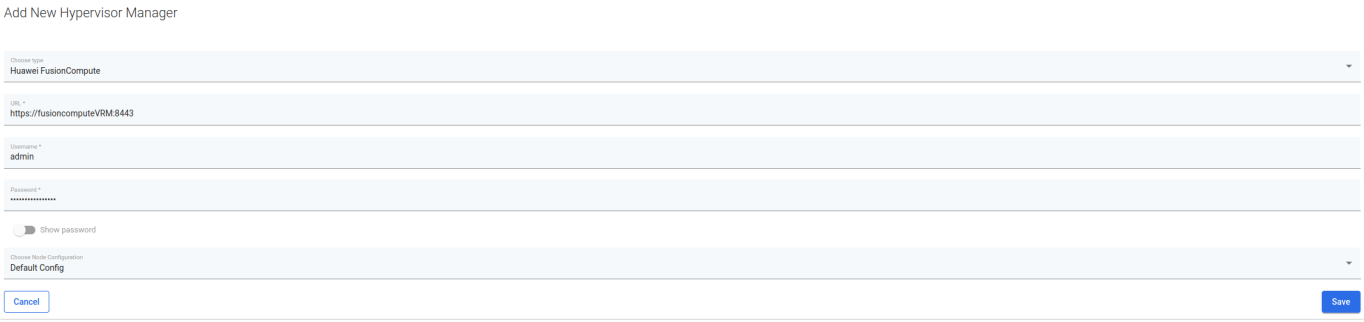
Huawei FusionCompute

- Supported version: 8.x.
- The node can be installed outside of the environment, but not behind a NAT.
- Incremental backup uses the CBT functionality of VRM. This means that currently, incremental backup can only be performed on VMs with installed VMTools (You can find instructions on how to install VMTools on VRM's Help page).



Creating a FusionCompute Hypervisor Manager

- Fill in the URL field:
  - https
  - address of VRM server, hostname, or IP, with port (default is 8443)
- Fill in the admin username and password for VRM.



Backup and Restore

- Backup and restore use LANSSL transfer mode for communication with CNAs.
- Requires a connection to each Hypervisor (data transfer during the backup/restore process will be performed directly between the node and the CNA/Hypervisor on which the VM is running).

Backup process

- A snapshot of the VM is performed. (type 'normal' when the VM is without VMTools or type 'CBTbackup' if the VM has VMTools installed).
- The metadata of VM is backed up in json format.
- Each disk is then backed up sequentially, using LANSSL transfer mode. During this process, the node communicates with the specific CNA directly.
- If the incremental backup is performed: additionally the CBT map for each disk is backed up.
- The last snapshot is kept on the hvm for incremental backup.

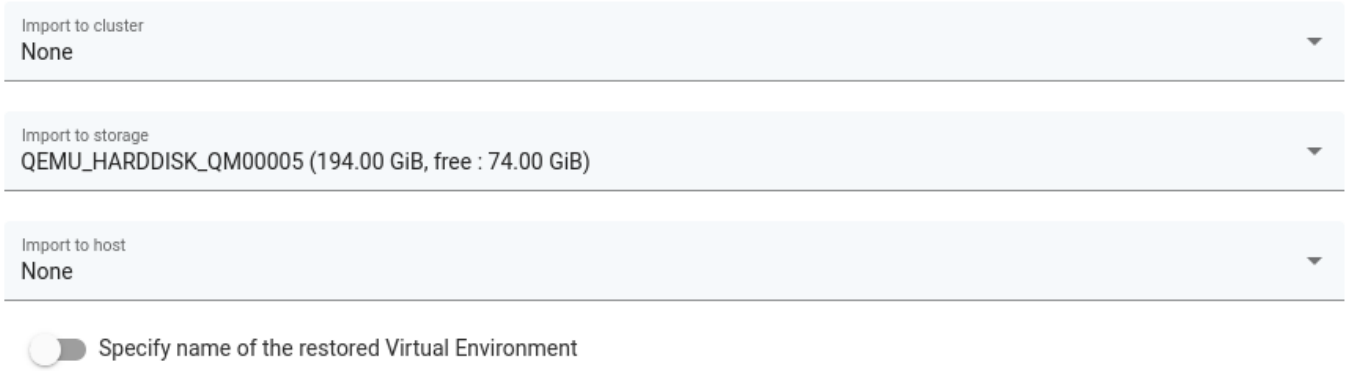
Restore process

- The node sends a request to the VRM to create a new VM based on the metadata stored during the backup process. The VRM automatically creates the required disks.
- For each disk, the node sends data using LANSSL transfer mode directly to the CNA, restoring the backup content.

Restore settings

*Restore to hypervisor manager

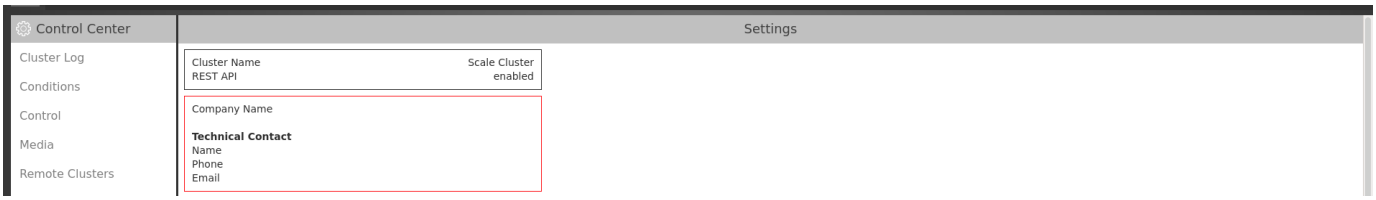
- Select the storage to which disks will be restored
- Cluster and host selection:
    - If the host is selected then the VM will be restored to that host and bound to it.
    - If the host is set to None, then a cluster must be selected and the VM will be restored to that cluster
- You can specify the name for the restored VM.



Scale Computing HC3

General

All the operations are using REST API to communicate with the HC3 cluster. Because of this, the cluster intended to be used by Data Protector for Cloud Workloads has to have the REST API enabled in the settings.



Before taking a snapshot, the current state of the *disableSnapshotting* flag of every disk in the virtual machine is checked. If even one of the disks has disabled snapshotting, the snapshot task ends with the error. All disks with disabled snapshotting are listed in the error message.


```
{
  "uuid": "7add7112-df10-499d-9c60-2f1462b7386e",
  "virDomainUUID": "121a4382-67b7-4bf2-8bcd-a4bcf45a10db",
  "type": "IDE_DISK",
  "cacheMode": "WRITETHROUGH",
  "capacity": 2000683008,
  "allocation": 1017118720,
  "physical": 0,
  "shareUUID": "",
  "path": "scribe/7add7112-df10-499d-9c60-2f1462b7386e",
  "slot": 1,
  "name": "",
  "disableSnapshotting": false,
  "tieringPriorityFactor": 8,
  "mountPoints": [],
  "createdTimestamp": 1631880304,
  "readOnly": false
},
```


Backup Strategies

Export Storage Domain Strategy

Export storage domain strategy performs the export using a Samba server running on a node machine. This strategy does not require a proxy VM.

> **Note:**
>
> - supported version: 8.9.x
> - no incremental backup
> - backup files are transferred to the SMB file share created on the node host (no Proxy VM required

In general, the export process is as follows:

• A snapshot of the virtual machine is taken

• Samba server is started on the node machine and export share is added

• Export of the VM to created SMB share is ordered

• Export share is removed and Samba server is stopped after Data Protector for Cloud Workloads finishes copying files

• Metadata of the excluded disks is exported

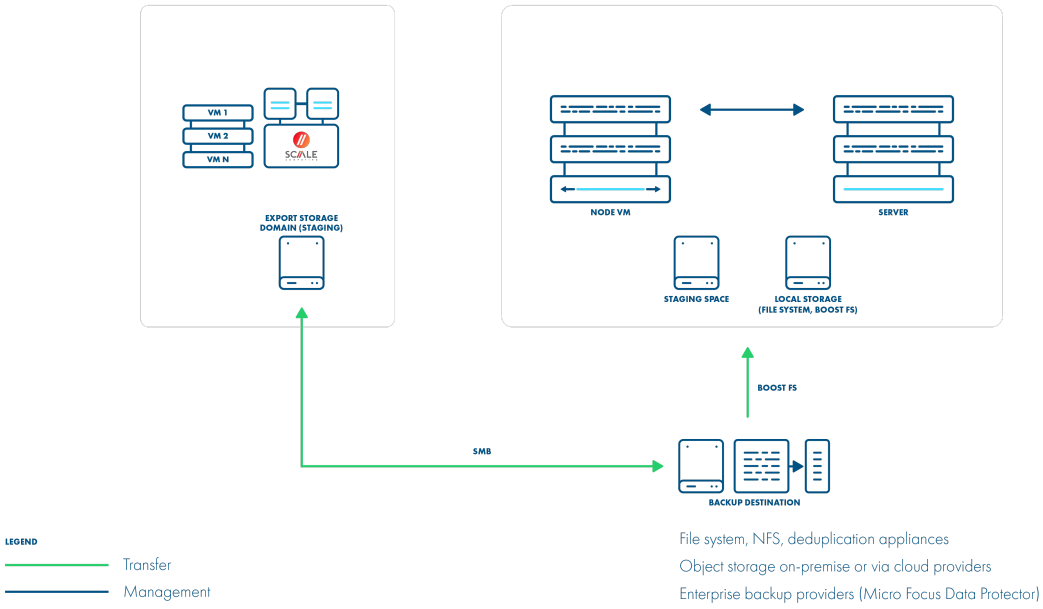
In general, the restore process is as follows:

• Samba server is started on the node machine and import share is added

• Import of the VM to the created SMB share is ordered

• Empty disks for excluded disks are added to the restored VM

• Import share is removed and Samba server is stopped



Disk Attachment Strategy

Disk attachment strategy performs the export using proxy VM running on the HC3 cluster.

> **Note:**
>
> - supported version: 8.9.x
> - incremental backup available
> - a proxy VM is required - used for the disk attachment process.

In general, the export process is as follows:

• A snapshot of the virtual machine is taken

• The disks from the taken snapshot that were not excluded are attached to the proxy VM

• If full export is being performed, then the whole content of the attached disks is saved to the backup files. If incremental export is being performed, then the list of changed blocks is first retrieved and then only the content of these blocks is saved.

• The disks are detached from the proxy VM

In general, the restore process is as follows:

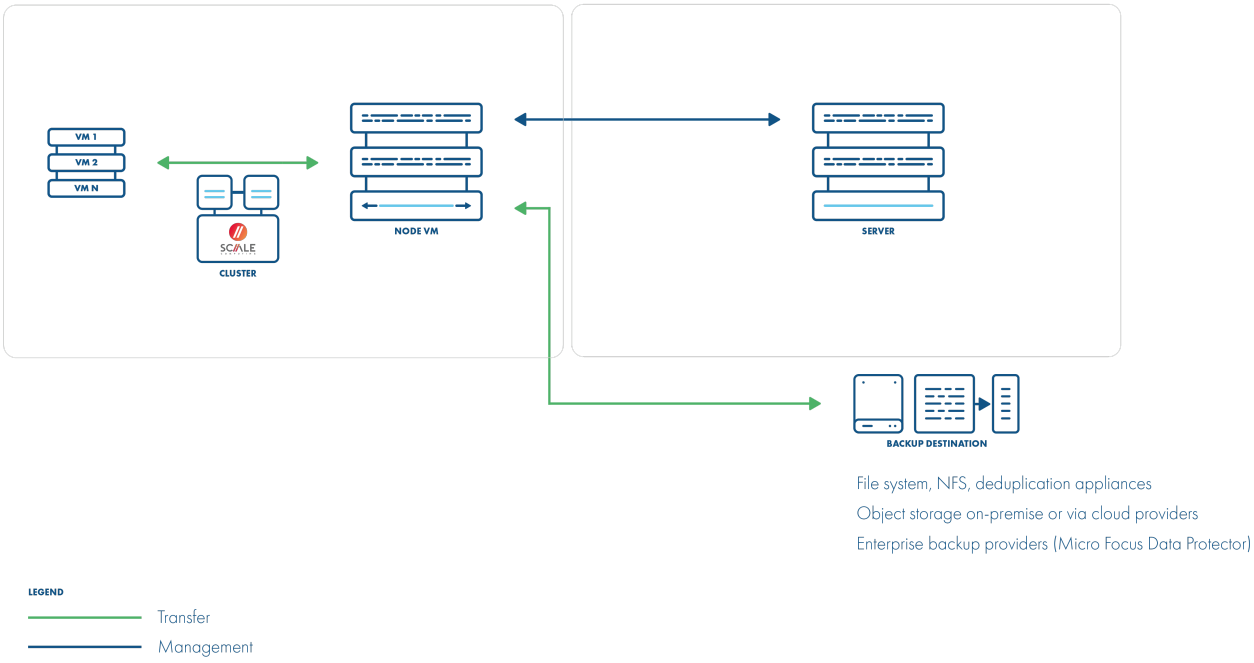
• A new virtual machine is created using exported metadata

• Empty disks are attached to the proxy VM

• Content of the exported disk files is written to the attached disks

• The restored disks are then reattached from the proxy VM to the restored VM

• List of boot devices for the restored VM is set



Adding HC3 as Hypervisor Manager

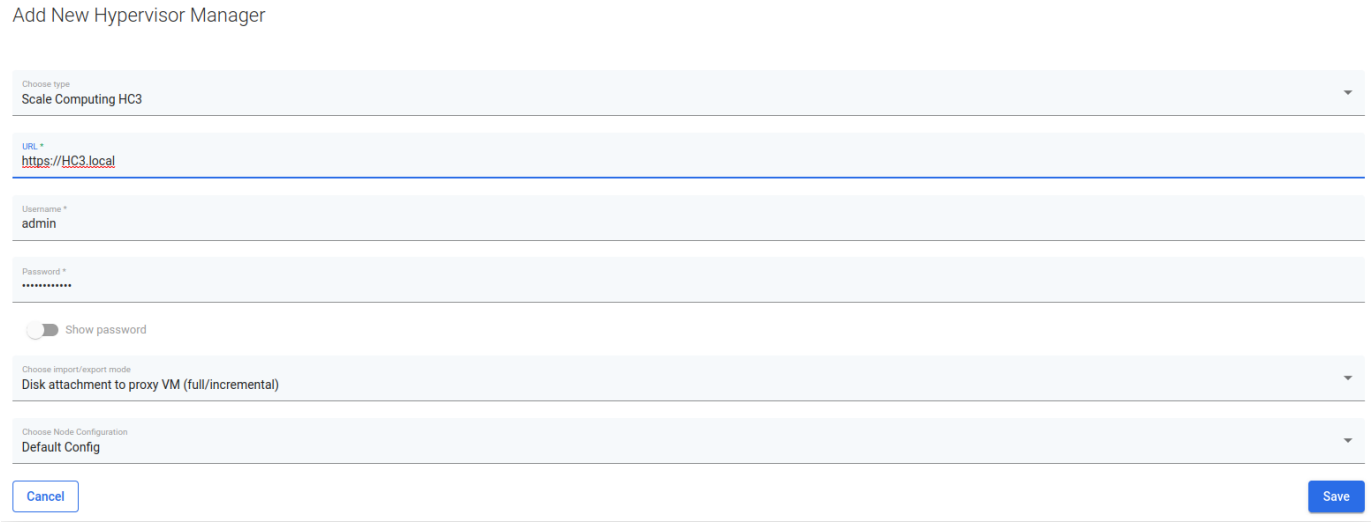
When adding a new Scale HC3 as Hypervisor Manager in Data Protector for Cloud Workloads, configure the following fields:

• URL: Address of HC3 hypervisor server: hostname or IP with HTTPS

• Fill in the admin username and password for HC3

• Select the export method

• The node configuration responsible for backup operations



Cloud

Data Protector for Cloud Workloads currently only supports the AWS EC2 cloud and Microsoft 365.

In this section, you will find information about the AWS EC2 backup strategy and specific steps needed to use it with Data Protector for Cloud Workloads.

> **Note:** Information about protecting Microsoft 365 you can find in the chapter Protecting Microsoft 365

AWS EC2

Data Protector for Cloud Workloads supports the AWS EC2 cloud platform by using a VM called “Proxy VM”. The node invokes commands on the AWS to snapshot and attach EBS drives of a specific VM to itself (Proxy VM). The proxy VM is able to read the data from the attached disk snapshots and forward them to the backup provider.

This means that you need to create an EC2 instance (Proxy VM) in each region. Keep in mind that if you don't want to transfer data between AZ during the backup you may want to deploy Proxy VMs in each AZ.

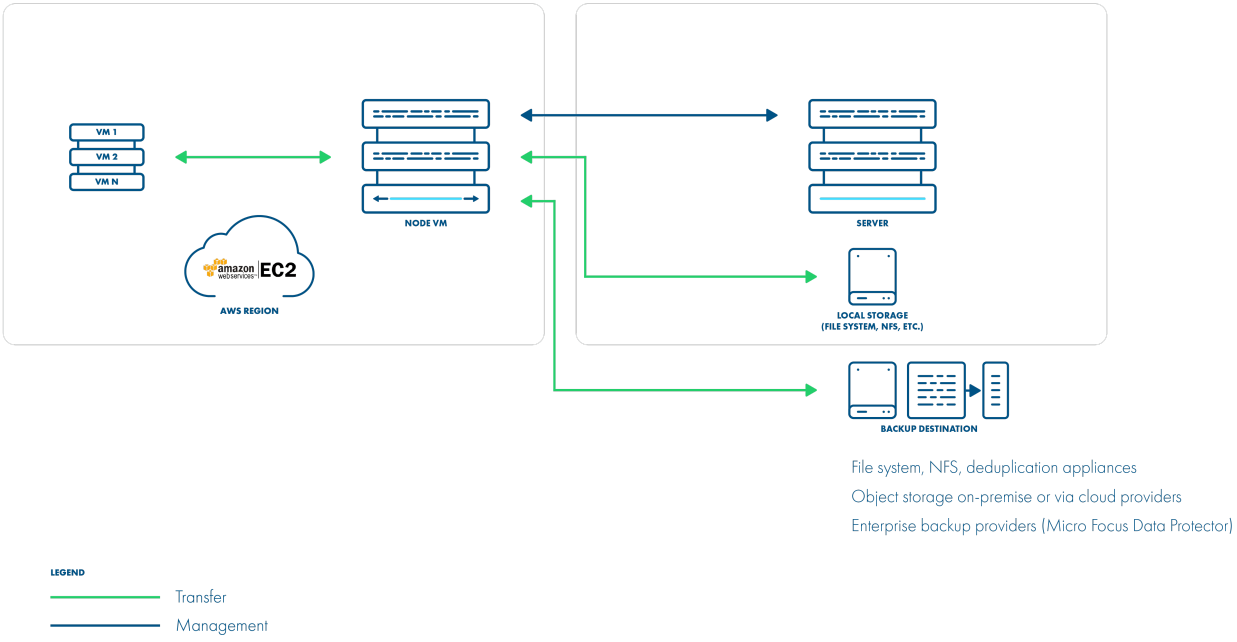
The Data Protector for Cloud Workloads Server can be deployed anywhere, but keep in mind that Nodes need to be able to call the server over HTTP(S) on the port you have specified.

The AWS backup strategy allows you to exclude drives from backup which you don’t need. Remember that you need to install 1 Proxy VM per AWS region so that drives that the Node tries to attach are reachable.

All backup destinations can be used, but keep in mind that you may be charged for transferring data between regions, AZs and external backup providers.

Data Protector for Cloud Workloads Node has access to instances only in the **region where it is hosted**.

Data Protector for Cloud Workloads Node requires the **account ID, access key** and **secret key** to connect to the AWS account.



Typical use scenarios

There are several scenarios for AWS which may be suitable for your case:

- **Backup EC2 to S3** - in this case after dumping backup, Data Protector for Cloud Workloads can push them to the S3 bucket. You may consider using a VPC endpoint to boost your store operation performance.
- **Backup EC2 to EBS volume on the proxy** - you can use PowerProtect DD to deduplicate data and optimize your storage consumption significantly. Keep in mind that you may want to protect your EBS volume using EBS snapshots as well.

- **Backup EC2 to your local backup provider** - if you already have a central enterprise backup solution, you may want to use it as a backup provider for EC2 instances running in AWS. You should consider using Direct connect to have a higher bandwidth available.
- **Backup EC2 to your other cloud provider** - If you're using multiple clouds, you also may consider storing data in GCS or Azure backup providers.

> **Note**: In all cases, depending on your target, you may be charged for data transfers.

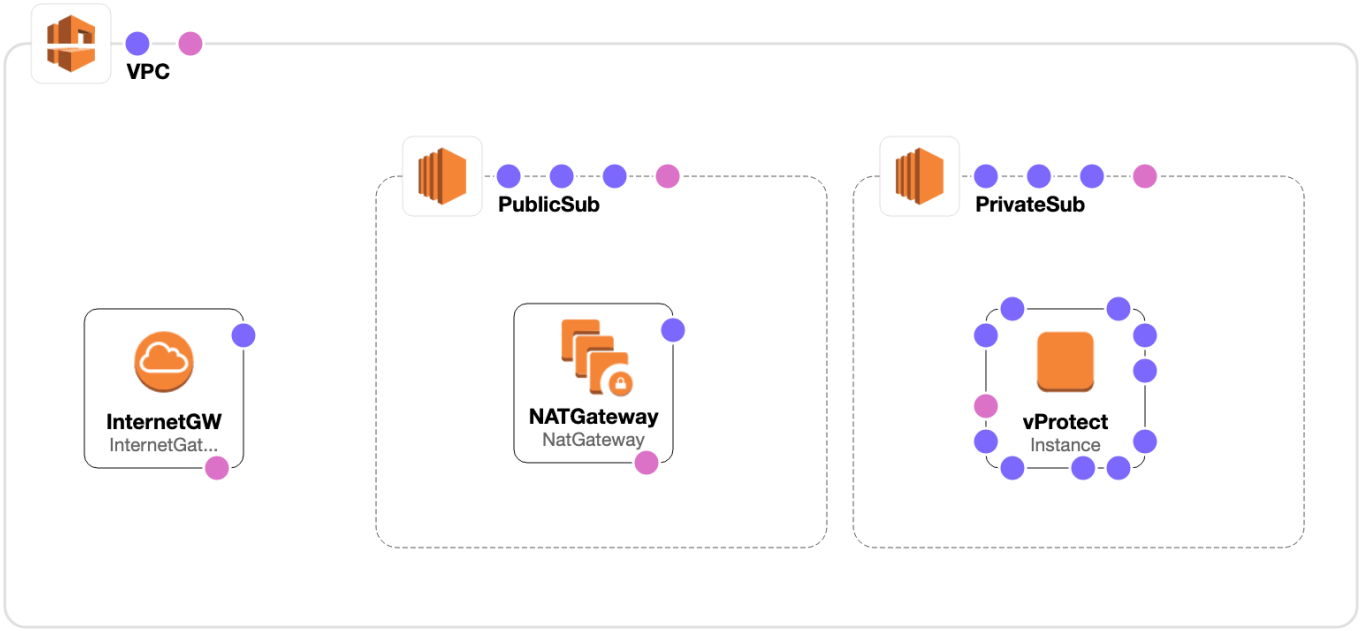
Setup considerations

It is assumed that you have working experience with AWS EC2 to be able to deploy Data Protector for Cloud Workloads components. You also need to have an IAM user with permissions that allow you to deploy an instance and generate access/secret keys for Data Protector for Cloud Workloads.

Remember to use **CentOS 8 AMI** as a base image - both for the Server and Nodes. For a typical installation, we recommend 2 virtual processors and 4 GB of RAM. This means that **t3.medium** or **m5.large** should cover general use cases. For better performance, however, we recommend using storage optimized instances such as **i3.large** or bigger, where I/O intensive operations should perform better.

Both Data Protector for Cloud Workloads components are assumed to be deployed without HA (more precisely, all the nodes or server will probably be in separate AZs, and only need to communicate over HTTP). There is no requirement for multi-AZ deployment for now. While the Node is stateless and can be lost without data loss, the Server needs DB to be protected. Data Protector for Cloud Workloads provides a built-in automatic DB backup mechanism, which can be used to protect backup metadata. Please refer to the Disaster recovery section for more details.

From a networking perspective, Data Protector for Cloud Workloads requires communicating with AWS EC2 API, but it is still recommended to put in a private subnet and allow communication over a NAT Gateway.



You add AWS EC2 as a Hypervisor Manager. You need to provide the account ID and access/secret keys of a user that has permissions to handle snapshot, AMI and EBS volume operations and EC2 instance creation.

On the same screen, you also specify if the AMIs of root volumes should be created during the backup process. For Windows instances, we recommend also keeping an AMI image with each backup to have the option to restore the original root volume as well. You can also skip AMI creation, but this means that during restore you need to specify the appropriate AMI ID that you want to boot from.

Permissions

Here are the IAM permissions that Data Protector for Cloud Workloads needs to have for backup/restore operations.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1565003475859",
      "Action": [
        "ec2:AttachNetworkInterface",
        "ec2:AttachVolume",
        "ec2:CreateImage",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSnapshot",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DeleteSnapshot",
        "ec2:DeleteVolume",
        "ec2:DeregisterImage",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:DetachVolume",
        "ec2:RegisterImage",
        "ec2:RunInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    }
  ]
}
```

Adding a hypervisor manager

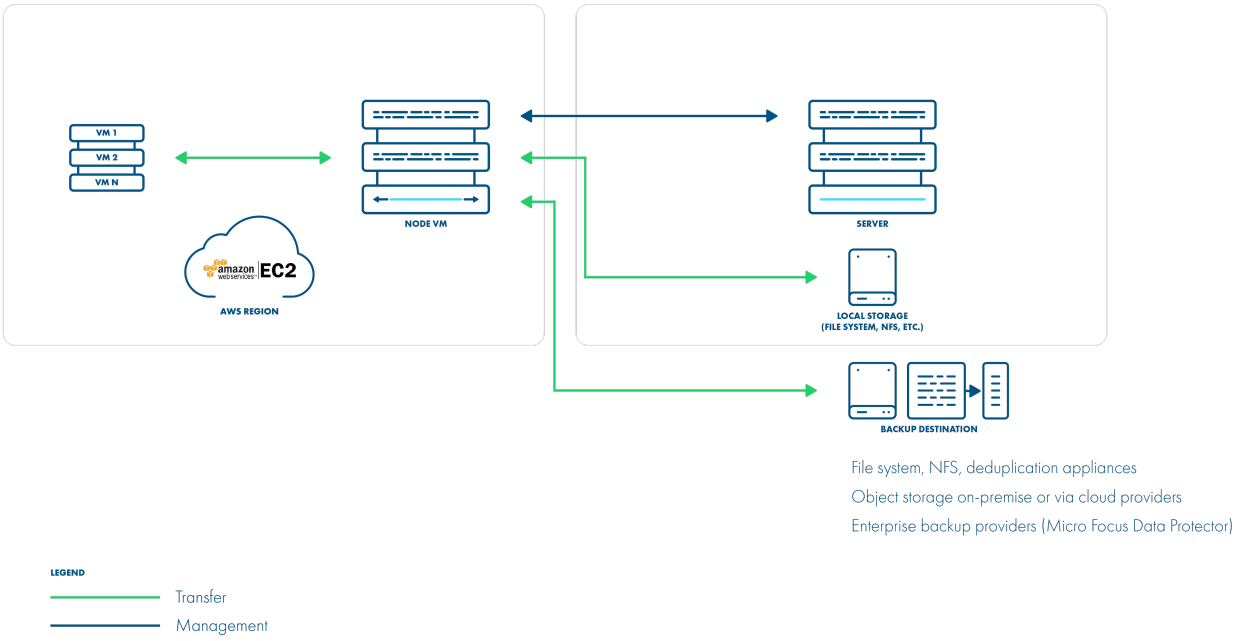
To properly configure your AWS account, go to Data Protector for Cloud Workloads -> Virtual Environments -> Infrastructure -> add hypervisor manager

Enter parameters such as:

- Account ID

https://docs.aws.amazon.com/IAM/latest/UserGuide/console_account-alias.html#FindingYourAWSId"

- Access key
- Secret Key
- Enable/disable Windows, Linux image



> **Note:** When Data Protector for Cloud Workloads creates a backup, some operating systems, such as Windows, may require an AMI for later restores in order to keep your OS settings. With this option, Data Protector for Cloud Workloads will keep the AMI necessary for future restores in your AWS account. Without this image, a new instance will have to be started with a fresh root device and additional volumes attached, which may not contain your OS-related settings, licenses, or data that were stored on the root device.

Backup modes

These settings regarding Windows or Linux images are required to define the way backups and restores are done. AWS supports 2 ways:

1. Using AMI and AWS snapshots:
    - During Export or Snapshot tasks an AMI is created for the root volume, other volumes are snapshotted.
    - The AMI is stored in AWS until Data Protector for Cloud Workloads snapshot or backup removal is initiated.
    - During Restore, a new instance is launched from a previously exported AMI, and imported non-root volumes are attached.
2. Using AWS snapshots:
    - During Export or Snapshot tasks, all volumes are snapshotted.
    - During Restore, an AMI is created from the imported root volume, a new instance is launched and imported non-root volumes are attached. The AMI is then removed.

In both cases, volume snapshots are kept in AWS only if the Data Protector for Cloud Workloads Snapshot task is completed.

> **Note:** A Windows AMI created from a snapshot is not launchable, hence it is recommended to **enable using AMI for the Windows platform**.

Restore

It is possible to specify another AMI for attaching non-root volumes during restore. You can also specify an availability zone (within the region of the Data Protector for Cloud Workloads Node) for a new instance.

Costs

From the AWS perspective, you need to take inot account several additional costs that may be incurred:

- EC2 instance costs for the Data Protector for Cloud Workloads Server and Nodes:
  - depends on the number of nodes (assume at least one node per region)
  - to reduce costs we recommend to use reserved instances for production use
  - https://aws.amazon.com/ec2/pricing/
- Backup destination and staging space storage on EBS:
  - staging space is necessary and we recommend it to be at least the size of the biggest VM multiplied by the number of export and store threads
  - if you want to store backups on EBS you also need to have additional storage
  - you can have both using the same EBS volume
  - we encourage you to use deduplication, as it may even result in over 95% of storage savings
  - https://aws.amazon.com/ebs/pricing/
- Data transfer costs:
  - if you upload data to external backup providers, or if a node needs to transfer a lot of data between AZs - this can be reduced by deploying one node per AZ
  - https://aws.amazon.com/ec2/pricing/on-demand/#Data_Transfer

Containers

Data Protector for Cloud Workloads can back up data residing on Persistent Volumes in Red Hat OpenShift/Kubernetes environments or containers running on Proxmox VE (using its native backup mechanism).

- Kubernetes
- Red Hat OpenShift
- Proxmox VE

Kubernetes

Data Protector for Cloud Workloads Node preparation

Data Protector for Cloud Workloads Node requires `kubectl` installed (you have to add Kubernetes repository to install `kubectl`) and `kubeconfig` with valid certificates (placed in `/home/user/.kube`) to connect to the Kubernetes cluster.

1. Check if your kubeconfig looks the same as below.

Example:

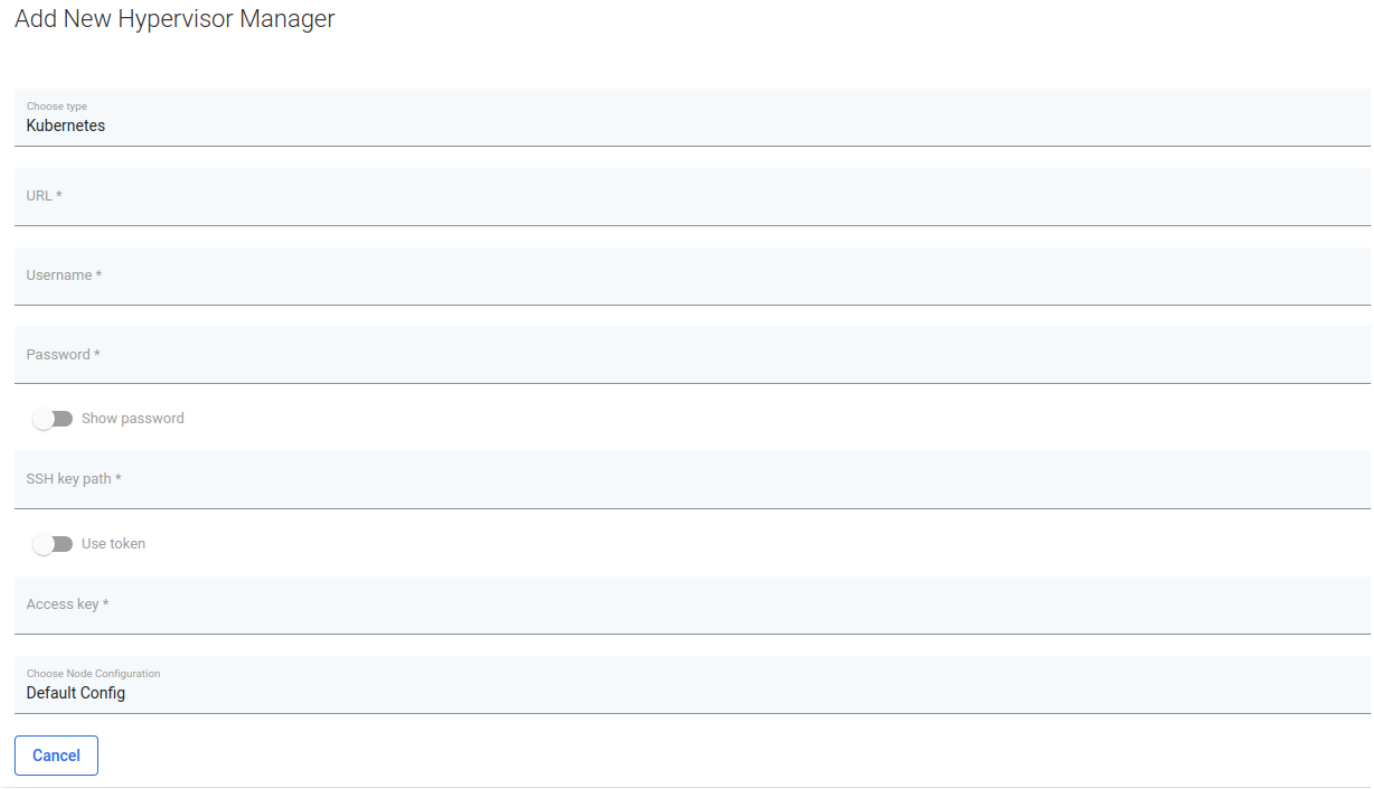
```
    current-context: admin-cluster.local
    kind: Config
    preferences: {}
    users:
    - name: admin-cluster.local
      user:
        client-certificate-data: <REDACTED>
        client-key-data: <REDACTED>
```

1. Copy configs to Data Protector for Cloud Workloads Node. (**Skip this and point 2 if you don't use Minikube**)
    - If you use Minikube, you can copy the following files to Data Protector for Cloud Workloads: `sudo cp /home/user/.kube/config /opt/vprotect/.kube/config sudo cp /home/user/.minikube/{ca.crt,client.crt,client.key} /opt/vprotect/.kube`
2. Modify the paths in `config` so they point to `/opt/vprotect/.kube` instead of `/home/user/.minikube`. Example:

```
- name: minikube
  user:
    client-certificate: /opt/vprotect/.kube/client.crt
    client-key: /opt/vprotect/.kube/client.key
```

1. Afterward, give permissions to the `vprotect` user:

```
chown -R vprotect:vprotect /opt/vprotect/.kube
```



Kubernetes Nodes should appear in Data Protector for Cloud Workloads after indexing the cluster.

> **Note**: Please provide the URL to the web console and SSH credentials to the master node when creating the OpenShift hypervisor manager in Data Protector for Cloud Workloads WebUI. You can also use SSH public key authentication. This is needed for Data Protector for Cloud Workloads to have access to your cluster deployments.

> **Note:** Valid SSH admin credentials should be provided **for every Kubernetes node** by the user (called *Hypervisor* in the Data Protector for Cloud Workloads WebUI). If Data Protector for Cloud Workloads is unable to execute docker commands on the Kubernetes node, it means that it is logged as a user lacking admin privileges. Make sure you added your user to sudo/wheel group (so it can execute commands with `sudo`).

> **Note:** If you want to use Ceph you must provide ceph keyring and configuration. Ceph requires ceph-common and rbd-nbd packages installed.

Persistent volumes restore/backup

There are two ways of restoring the volume content.

1. The user should deploy an automatic provisioner which will create persistent volumes dynamically. If Helm is installed, the setup is quick and easy https://github.com/helm/charts/tree/master/stable/nfs-server-provisioner.
2. The user should manually create a pool of volumes. Data Protector for Cloud Workloads will pick one of the available volumes with proper storage class to restore the content.

Limitations

- currently, we support only backups of Deployments/DeploymentConfigs (persistent volumes and metadata)
- **all deployment's pods will be paused during the backup operation** - this is required to achieve consistent backup data
- for a successful backup, every object used by the Deployment/DeploymentConfig should have an `app` label assigned appropriately

Red Hat OpenShift

Log in to the web interface and add a new OpenShift Hypervisor Manager:

Data Protector for Cloud Workloads Node preparation

The Openshift Nodes should appear in Data Protector for Cloud Workloads after indexing the cluster.

> **Note**:
>
> 1. Please provide the URL to the web console and SSH credentials to the master node when creating the OpenShift hypervisor manager in Data Protector for Cloud Workloads WebUI. You can also use SSH public key authentication. This is needed for Data Protector for Cloud Workloads to have access to your cluster deployments.
> 2. Valid SSH admin credentials should be provided **for every Openshift node** by the user (called *Hypervisor* in the Data Protector for Cloud Workloads WebUI). If Data Protector for Cloud Workloads is unable to execute docker commands on the Openshift node, it means that it is logged as a user lacking admin privileges. Make sure you have added your user to the sudo/wheel group (so they can execute commands with sudo).

Persistent volumes restore/backup

There are two ways of restoring the volume content.

1. The user should deploy an automatic provisioner which will create persistent volumes dynamically. If Helm is installed, the setup is quick and easy https://github.com/helm/charts/tree/master/stable/nfs-server-provisioner.
2. The user should manually create a pool of volumes. Data Protector for Cloud Workloads will pick one of the available volumes to restore the content.

OpenShift troubleshooting

The user from the current context should have cluster-admin permissions.

```
oc adm policy add-cluster-role-to-user cluster-admin admin --as system:admin
```

In this case, you should stay logged in as `admin` for the connection to be successful.

The following error might occur if the token in the kubeconfig file is invalid:

```
Failure executing: GET at: https://192.168.42.206:8443/api/v1/persistentvolumes. Message:
Unauthorized! Token may have expired! Please log-in again. Unauthorized.
```

Solution:

In the OpenShift master node, execute `oc login -u admin` (or any other user with cluster-admin permissions) and index the OpenShift hypervisor manager in Data Protector for Cloud Workloads WebUI again.

If indexing/export fails because no Pods could be found, please make sure they have the `app` label assigned appropriately.

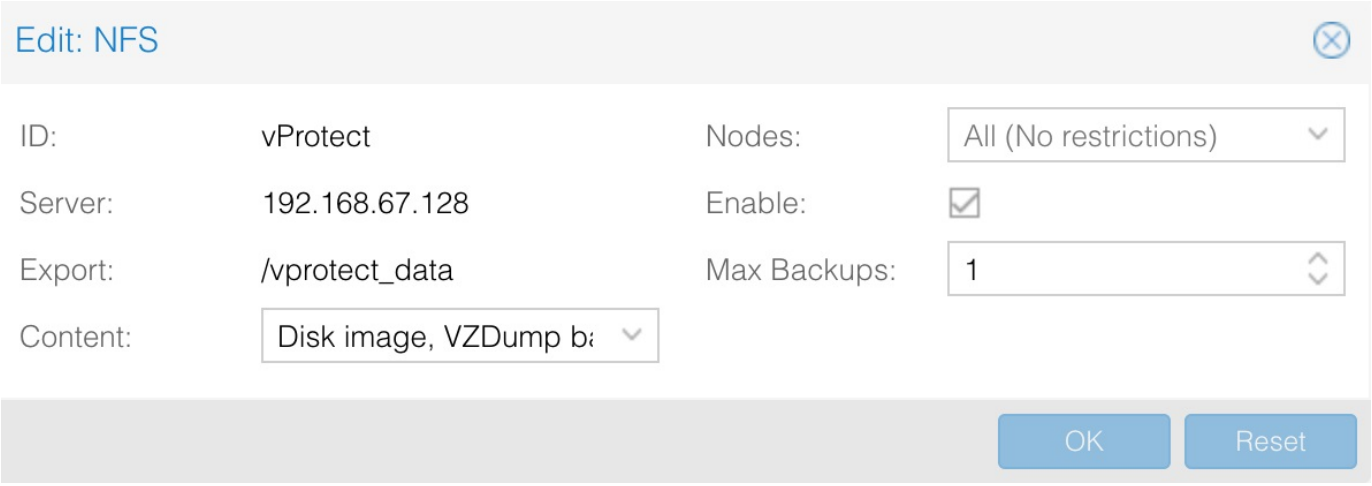
Limitations

- Currently, we only support backups of Deployments/DeploymentConfigs (persistent volumes and metadata)
- **All deployment pods will be paused during the backup operation** - this is required to achieve consistent backup data.
- For a successful backup, every object used by the Deployment/DeploymentConfig should have a `app` label assigned appropriately.

Proxmox VE

Proxmox environments require backup storage to be defined on each server. This storage must be a location accessible from Data Protector for Cloud Workloads Node (the simplest setup, when you use only 1 node, is to create NFS share for the staging path on Data Protector for Cloud Workloads Node).

1. Create storage from NFS share (Content-type: VZDump)



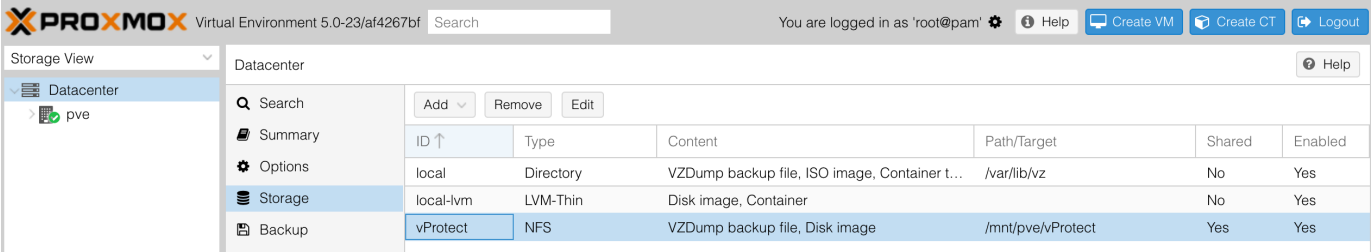
- The export share must be set to use the UID and GID of the `vprotect` user.
- Example export configuration in `/etc/exports` to the selected hypervisor in the RHV cluster:

  ```
  /vprotect_data
  PROXMOX_HOSTS(fsid=6,rw,sync,insecure,all_squash,anonuid=993,anongid=990)
  ```

  where `anonuid=993` and `anongid=990` should have the correct UID and GID returned by command:

  ```
  [root@vProtect3 ~]# id vprotect
  uid=993(vprotect) gid=990(vprotect) groups=990(vprotect)
  ```

- Both import and export operations will be done using these NFS shares – restore will be done directly to this storage domain, so you can easily import the backup into the Proxmox environment
  - Backups must be restored to the export path (the node automatically changes the names to the original paths that are recognized by Proxmox).
- The name for storage must be provided later in the node configuration (`Hypervisor -> Proxmox`)section.



File-level restore support for VMA images

1. Prepare the VMA extractor on Data Protector for Cloud Workloads Node - you have 2 options:
    - Build a VMA extractor like this (requires Internet on the **node**):

```
cd /opt/vprotect/scripts/vma
./setup_vma.sh
```

2. - Download the VMA extractor from the Micro Focus download page and install it.

```
cd /opt/vprotect/scripts/vma
./setup_vma.sh PATH_TO_VMA_ARCHIVE
```

Public key authentication

The details are described in the SSH public key authentication section.

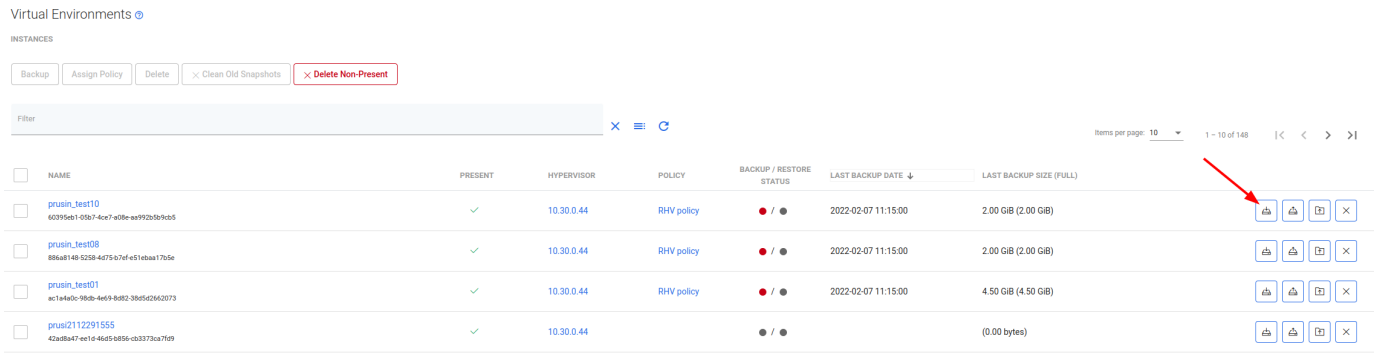
Backup & Restore

This section is a simple step-by-step guide on how to use Data Protector for Cloud Workloads to protect your Virtual Environments.

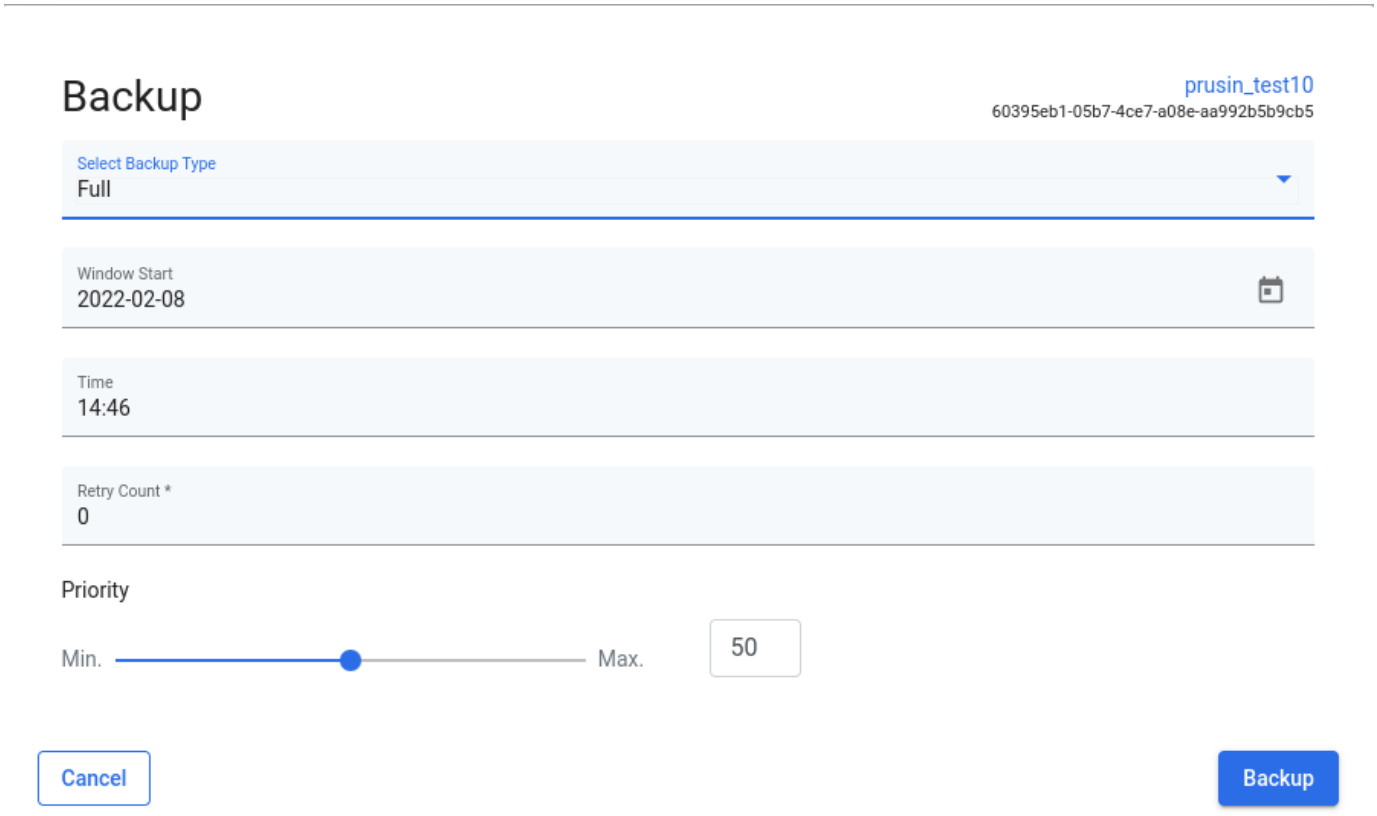
Manual backup

> **Note:** to perform a manual backup, a target VE instance must be assigned to Backup SLA

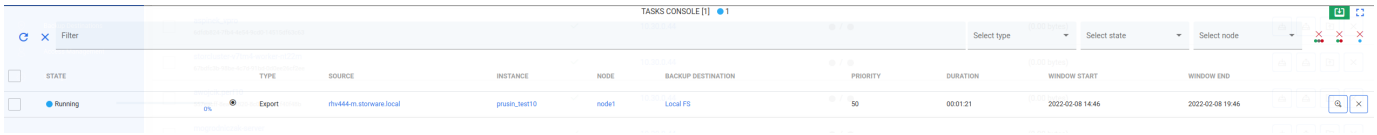
Search for VE instance you want to backup and click **Backup** the button next to it.



In the next window, choose backup type and click **Backup** button.

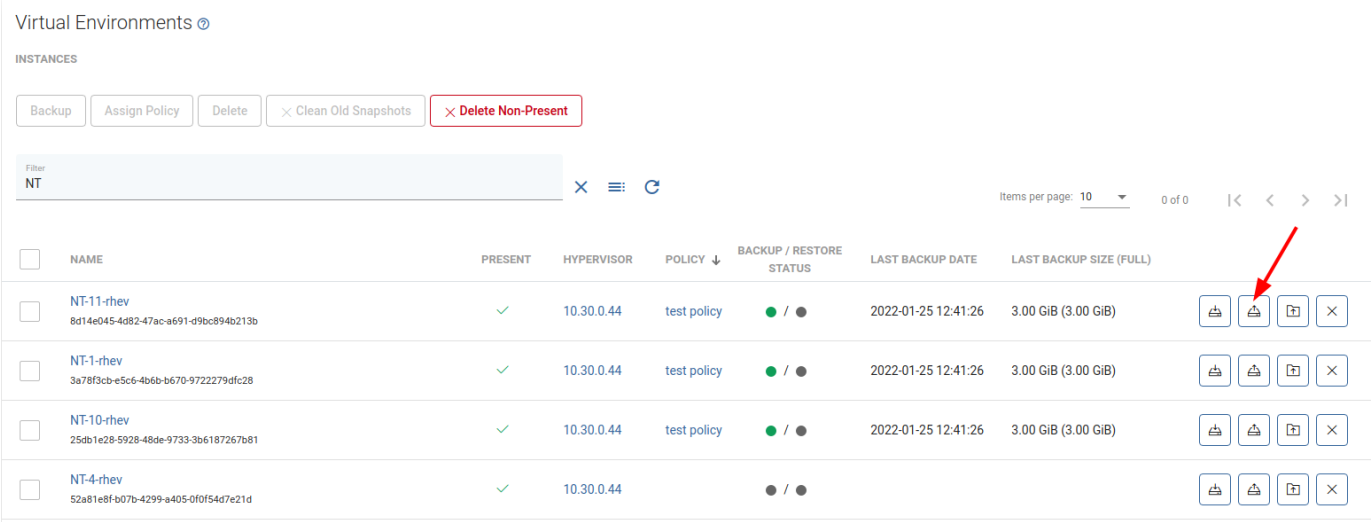


You can track the progress of the task in **tasks console**

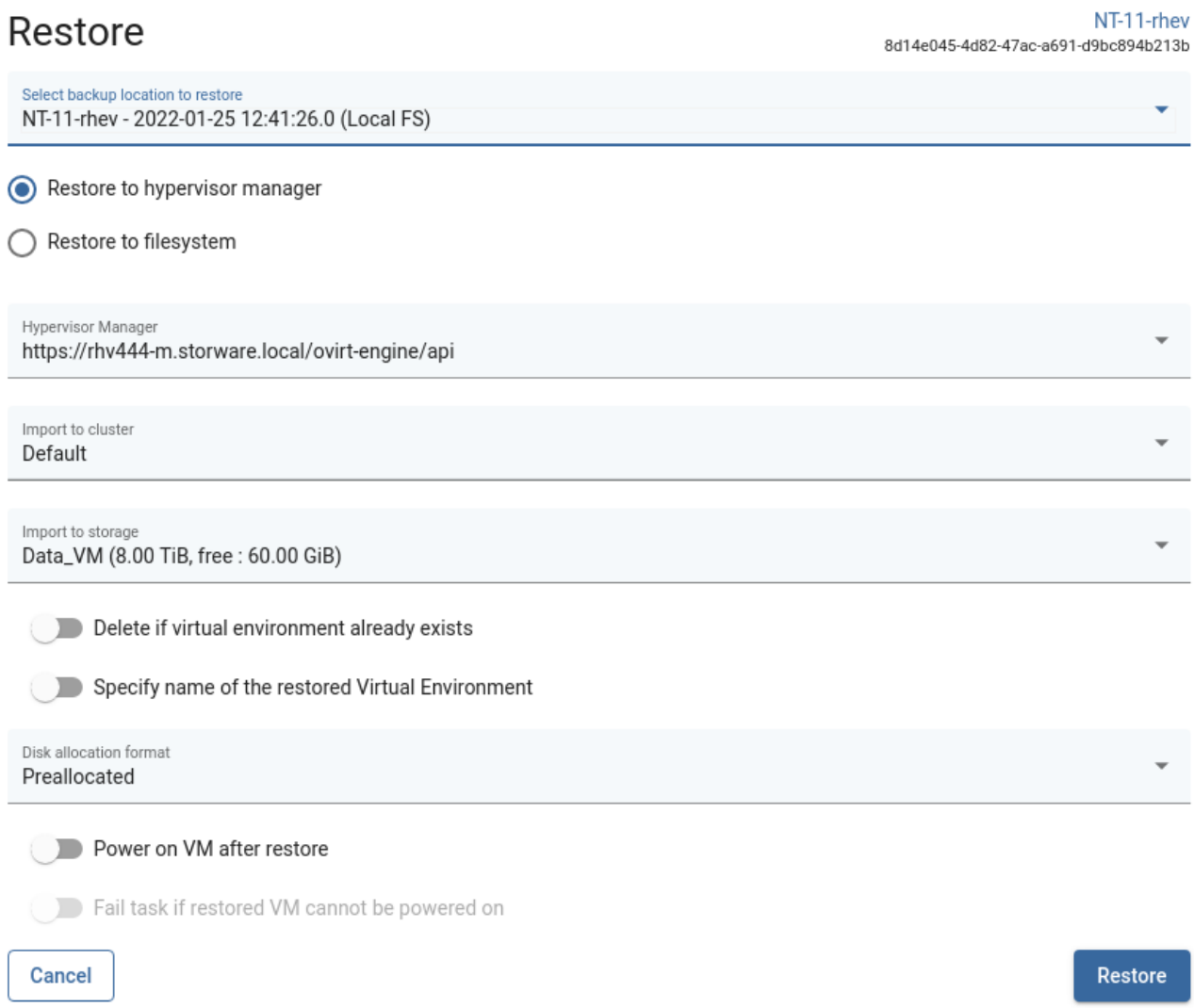


Manual restore

Search for VE instance you want to restore and click **Restore** the button next to it.



In the next window, choose if you want to restore to the file system or directly to the hypervisor (or hypervisor manager). Enter the rest parameters according to your needs and click **Restore** the button. The available parameters may differ depending on the hypervisor.



Note: More information about Virtual Environments you can find in the administration chapter.

Protecting Microsoft 365

Data Protector for Cloud Workloads Server allows you to protect multiple Microsoft 365 organizations within a single server instance. Before you add the Microsoft 365 organization to Data Protector for Cloud Workloads Server, you have to configure all required permissions of your application in the Microsoft 365 service.

Go to the Microsoft 365 organization management section to learn how to configure Microsoft 365 organization permissions to be able to add them to Data Protector for Cloud Workloads Server.

After that, you can go to Backup & Restore to start protecting Yours Microsoft 365 organizations.

Microsoft 365 organization management

You can add a Microsoft 365 organization manually or using the Setup assistant.

To add the organization log into Data Protector for Cloud Workloads go to the **Cloud** menu and select **Service Providers**. Now you can choose one of the options: **Create** to add manually or use **Setup Assistant**.

How to add Microsoft 365 organization manually

How to add Microsoft 365 organization using the Setup Assistan

> **Note:** We recommend using the setup assistant to add Microsoft 365 organizations

Configure Microsoft 365 access

Before you start to configure Backup SLAs, Data Protector for Cloud Workloads Server has to get access to your Microsoft 365 organization configuration first.

Access to data is performed via an application configured in your Microsoft 365 organization.

> **Note:**
>
> - You can skip this step if you want to add your Microsoft 365 organization to Data Protector for Cloud Workloads Server using the Setup Assistant. If not, please proceed with the next steps.
> - Data Protector for Cloud Workloads does not store your Microsoft 365 administrative id and password.

Manually registering an application with Azure Active Directory

A new Microsoft 365 application has to be registered and configured in Azure Active Directory. When it's done, in the next step you can add the application (organization) to Data Protector for Cloud Workloads Server.

The instruction is as follow:

1. Go to the Azure portal (https://portal.azure.com/) page and sign in to your Microsoft account by using your Microsoft 365 administrative user ID and password.
2. In the home view, go to **Manage Azure Active Directory** (click the **View** button).
3. To open the Azure Active Directory admin center, in the left pane, click the ellipsis to expand the Show all menu, and then click **Admin centers** > **Azure Active Directory**.
4. In the tenant dashboard menu, click **App registrations** and then click **New registration**.
5. Specify a user-facing name for the Microsoft 365 application, on the **Register an application** page by entering a name in the **Name** field.
6. Use the default options for the remaining fields, and click **Register**. The app registration is set up with the user-facing name that you entered.
7. To obtain the application (**client**) ID, and directory (**tenant**) ID string, go to **Azure Active Directory > tenant - App registrations > Owned applications**. Click the application name, copy the application ID string and directory ID. These strings will be required later when you register the Microsoft 365 service on Data Protector for Cloud Workloads Server.
8. To create a client secret for this application ID, click **Certificates & secrets** > **New client secret**.
9. On the "**Add a client secret**" pane, enter any user name in the **Description** field, and click **Add**. A client secret is generated, and the value is then displayed in the Client secrets pane.
10. Copy the client secret to the clipboard by using the copy icon next to the Client secret value field. This character string is also used for registration with Data Protector for Cloud Workloads Server.
11. To add permissions for this application ID, click **API permissions** > **Add permission**.
12. Specify permissions for each API in the following table by taking the following actions. Select the API name, for example, Azure Active Directory Graph.

API	Permission name	Permission type

API	Permission name	Permission type
Azure Active Directory Graph	Calendars.ReadWrite	Application
Microsoft Graph	Channel.Create	Application
Microsoft Graph	Channel.ReadBasic.All	Application
Microsoft Graph	ChannelMember.Read.All	Application
Microsoft Graph	ChannelMember.ReadWrite.All	Application
Microsoft Graph	ChannelMessage.Read.All	Application
Microsoft Graph	Chat.Read.All	Application
Microsoft Graph	Chat.ReadBasic.All	Application
Microsoft Graph	Chat.ReadWrite.All	Application
Microsoft Graph	ChatMember.Read.All	Application
Microsoft Graph	ChatMember.ReadWrite.All	Application
Microsoft Graph	Contacts.ReadWrite	Application
Microsoft Graph	Directory.ReadWrite.All	Application
Microsoft Graph	Files.ReadWrite.All	Application
Microsoft Graph	Group.Create	Application
Microsoft Graph	Group.ReadWrite.All	Application
Microsoft Graph	GroupMember.Read.All	Application
Microsoft Graph	GroupMember.ReadWrite.All	Application
Microsoft Graph	Mail.ReadWrite	Application
Microsoft Graph	MailboxSettings.Read	Application
Microsoft Graph	MailboxSettings.ReadWrite	Application
Microsoft Graph	Member.Read.Hidden	Application
Microsoft Graph	Sites.FullControl.All	Application
Microsoft Graph	Sites.Manage.All	Application
Microsoft Graph	Sites.Read.All	Application
Microsoft Graph	Sites.ReadWrite.All	Application
Microsoft Graph	Team.Create	Application
Microsoft Graph	Team.ReadBasic.All	Application
Microsoft Graph	TeamMember.Read.All	Application
Microsoft Graph	TeamMember.ReadWrite.All	Application
Microsoft Graph	TeamMember.ReadWriteNonOwnerRole.All	Application
Microsoft Graph	TeamsApp.ReadWrite.All	Application
Microsoft Graph	TeamSettings.ReadWrite.All	Application

API	Permission name	Permission type
Microsoft Graph	TeamsTab.Create	Application
Microsoft Graph	TeamsTab.ReadWrite.All	Application
Microsoft Graph	TeamsTab.ReadWriteForChat.All	Application
Microsoft Graph	TeamsTab.ReadWriteForTeam.All	Application
Microsoft Graph	TeamsTab.ReadWriteForUser.All	Application
Microsoft Graph	User.Read.All	Application
Microsoft Graph	User.ReadWrite.All	Application
Office 365 Exchange Online	full_access_as_app	Application
SharePoint	Sites.FullControl.All	Application
SharePoint	Sites.Manage.All	Application
SharePoint	Sites.Read.All	Application
SharePoint	Sites.ReadWrite.All	Application
SharePoint	User.ReadWrite.All	Application

13. To set the permission "**full_access_as_app**" in the Office 365 Exchange Online API, click "**Add a permission**" option and in the "**Request API permissions**" window go to "**APIs my organization uses**" and search for "**Office 365 Exchange Online**", then select "**Application permissions**" and check "**full_access_as_app**" from "**Other permissions**".

14. To save the selected permissions, click **Grant admin consent for <your organization name>**.

15. Since you're granting tenant scoped permissions this granting can only be done via the **appinv.aspx** page on the tenant administration site. You can reach this site by typing the address: **https://tenantName-admin.sharepoint.com/_layouts/15/appinv.aspx**. (replace the **tenantName** with your tenant name). Once the page is loaded, do as follow:

    1. Enter your App Id (client ID) and click the **Lookup** button.
    2. Enter the App Domain name.
    3. In the "**App's Permission Request XML"** window enter the following lines:

```
<AppPermissionRequests AllowAppOnlyPolicy="true">
    <AppPermissionRequest Scope="http://sharepoint/content/tenant"
     Right="FullControl" />
 </AppPermissionRequests>
```

16. When you click on the **Create** button you'll be presented with a permission consent dialog. Press the **Trust It** button to grant the permissions.

17. Open Powershell command prompt and execute the command:

```
Install-Module -Name Microsoft.Online.SharePoint.Powershell
```

or download and install the module directly from this site

then

```
Connect-SPOService https://tenantName-admin.sharepoint.com
Set-SPOTenant -LegacyAuthProtocolsEnabled $True
Set-SPOTenant -DisableCustomAppAuthentication $false
```

It enables the **LegacyAuthProtocolsEnabled** setting.

Add Microsoft 365 organization manually

To add your Microsoft 365 organization to Data Protector for Cloud Workloads Server, do as follow:

1. Log into Data Protector for Cloud Workloads WebUi and select tab **Cloud**.
2. Go to the **Service Providers** menu.
3. Click the **Create** button.
4. In the **Microsoft 365 Configuration** window you have to enter information as follow:
    1. Tenant ID
    2. Client ID
    3. Client secret
5. Chose node configuration which will be assigned to this organization
6. Save your settings by clicking the **Save** button.
7. Click the **Synchronize** button to synchronize users/sites/teams from your organization with Data Protector for Cloud Workloads Server.
8. Now you can go to the **Instances** menu and see synchronize results.

Go to the Add Microsoft 365 organization using the Setup Assistant chapter to learn how to add Microsoft 365 organization using dedicated Setup Assistant.

> **Note:** Go to the Account auto-synchronization to learn how to synchronize Microsoft 365 accounts.

Add Microsoft 365 organization using the Setup Assistant

To add your Microsoft 365 organization to Data Protector for Cloud Workloads Server using Setup Assistant, do as follow:

1. Go to the **Cloud** menu -> **Service Providers** -> click the **Setup Assistant** button.
2. In the **Wizard** window read the information and click the **Next** button to go to the next step.
3. Copy the authorization code -> click the link **https://microsoft.com/devicelogin** and enter it -> sign in to your Microsoft 365 organization as a user with administrator's rights. Now close the tab and go back to **Setup Assistant**.
4. Provide number of application and click **Create** button. The application tenant is created. Click the **Next** button to go to the next step.
5. Follow the instructions in **Setup Assistant**. If the **Lookup** button is not working and fields are not automatically populated the user needs to put there the following:
    - for the Title field: DP4CW
    - for the App domain field: localhost
6. In the next step, click **Grant permissions** button. You will be redirected to the the page where you need to accept permissions.
7. Execute provided PowerShell commands and click **Save** button.
8. The configuration is now complete. Save your settings by clicking the **Save** button.

Required permissions

1. Since you're granting tenant scoped permissions this granting can only be done via the **appinv.aspx** page on the tenant administration site. You can reach this site by typing the address: **https://tenantName-admin.sharepoint.com/_layouts/15/appinv.aspx**. (replace the **tenantName** with your tenant name). Once the page is loaded, do as follow:

2. Enter your App Id (client ID) and click the **Lookup** button.

3. Enter the App Domain name.

4. In the "**App's Permission Request XML"** window enter the following lines:

    ```
    <AppPermissionRequests AllowAppOnlyPolicy="true">
        <AppPermissionRequest Scope="http://sharepoint/content/tenant"
         Right="FullControl" />
     </AppPermissionRequests>
    ```

5. When you click on the **Create** button you'll be presented with a permission consent dialog. Press the **Trust It** button to grant the permissions.

6. Open Powershell command prompt and execute the command:

    ```
    Install-Module -Name Microsoft.Online.SharePoint.Powershell
    ```

    or download and install the module directly from this site

    then

```
Connect-SPOService https://tenantName-admin.sharepoint.com
Set-SPOTenant -LegacyAuthProtocolsEnabled $True
Set-SPOTenant -DisableCustomAppAuthentication $false
```

It enables the **LegacyAuthProtocolsEnabled** setting.

> **Note:** Go to the Account auto-synchronization to learn how to synchronize Microsoft 365 accounts.

Account auto-synchronization

This feature allows Microsoft 365 service accounts to be automatically synchronized with the Data Protector for Cloud Workloads Server. It means, that every newly created Microsoft 365 account will be synchronized with the server.

To configure this feature on the server do as follow:

1. Log onto Data Protector for Cloud Workloads WebUI
2. Go to the **Settings** menu
3. Select the **Global Settings** tab
4. Set the **Periodic inventory synchronization** interval (by default is 8 hours)
5. Click the **Save** button

From now on all new Users, SharePoint sites, and Teams added to Microsoft 365 service are also available in the Protection menu on Data Protector for Cloud Workloads Server after automatic inventory synchronization.

Backup & Restore

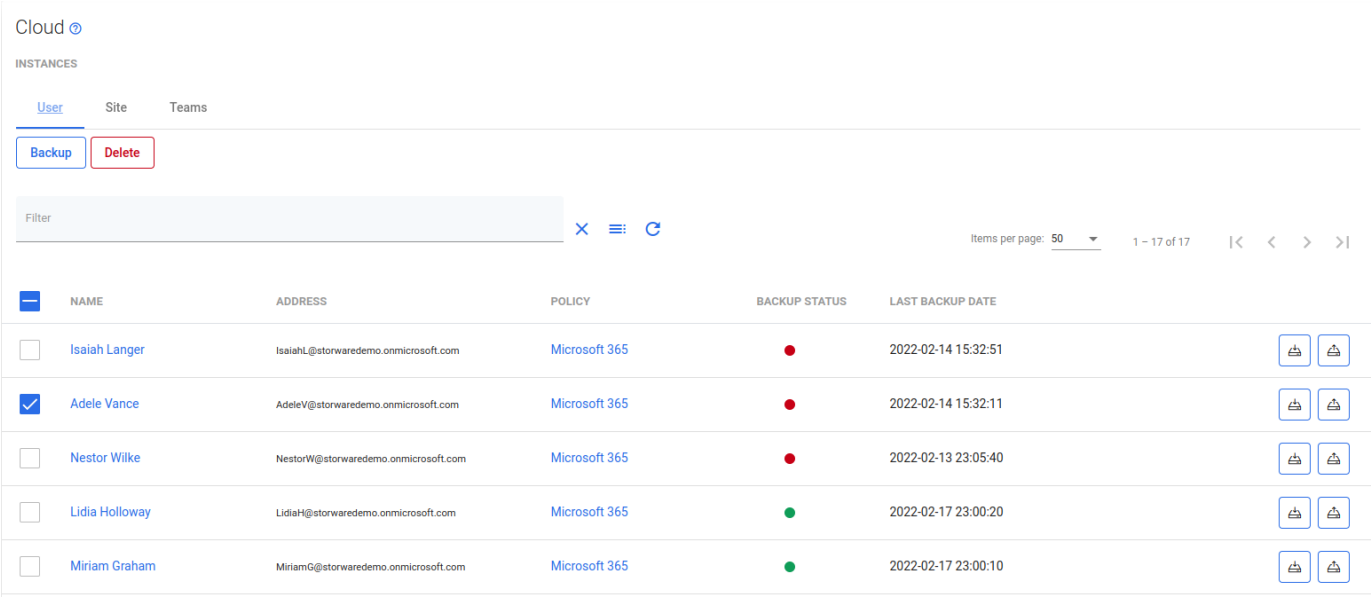
This section is a simple step-by-step guide on how to use Data Protector for Cloud Workloads to protect your Microsoft 365.

Backup and restore of Microsoft 365

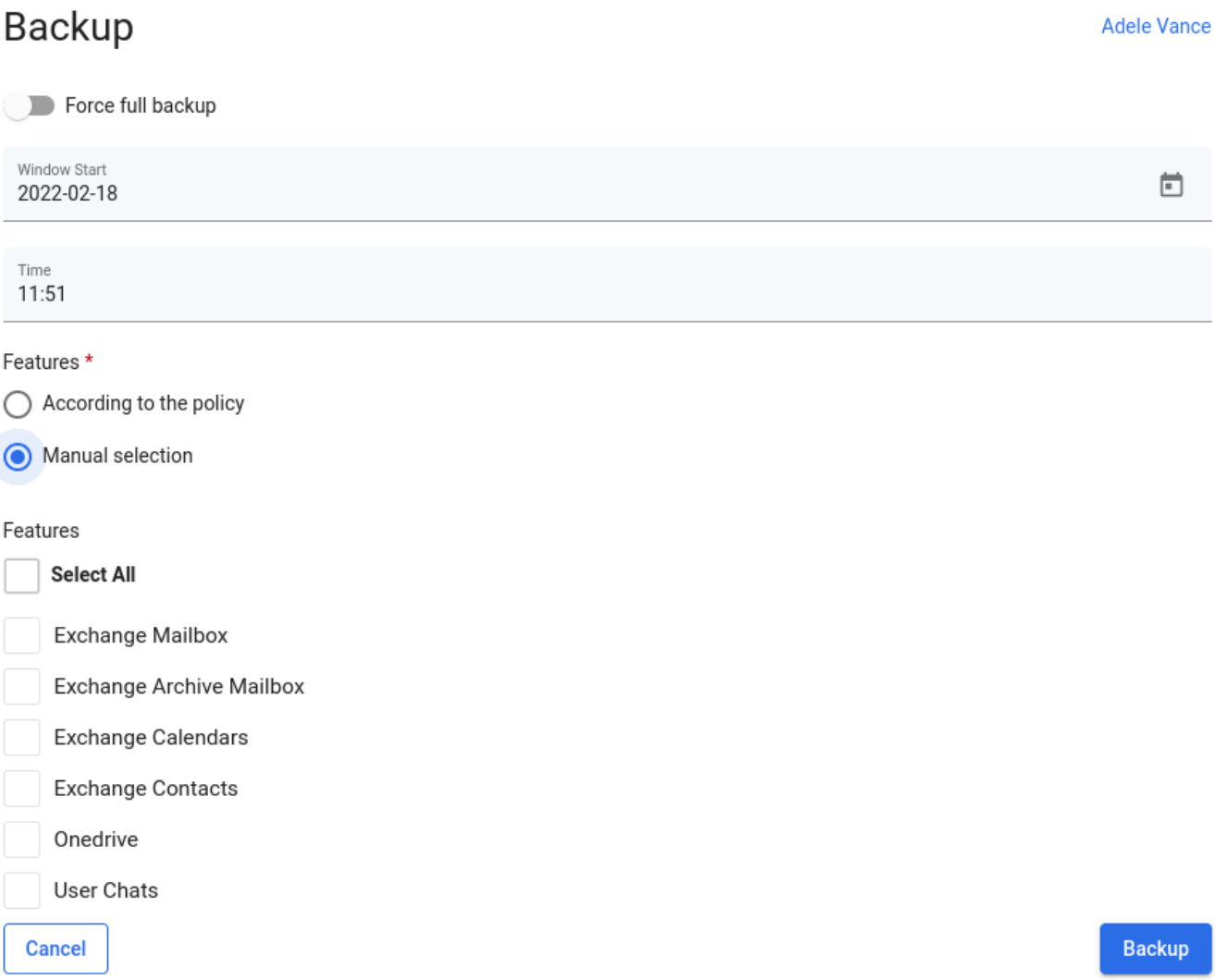
Manual backup

> **Note:** to perform a manual backup, a target account, site or team instance must be assigned to Backup SLA

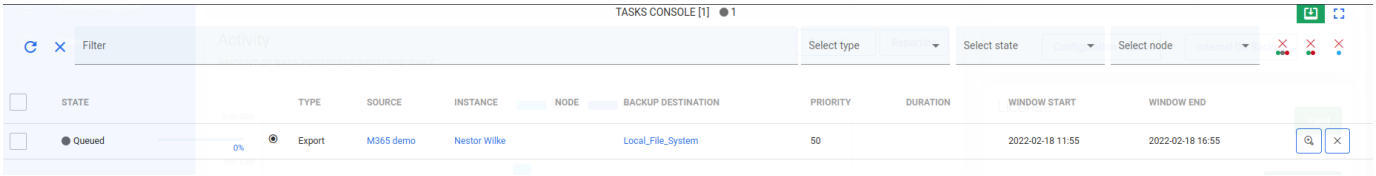
Search for one of the cloud instances you want to backup and click **Backup** the button next to it.



In the next window, choose backup type and what features you want to protect. If you want a backup of just one or more features use **manual selection** or use **according to the policy** to backup all features selected in Backup SLA then click **Backup** button.

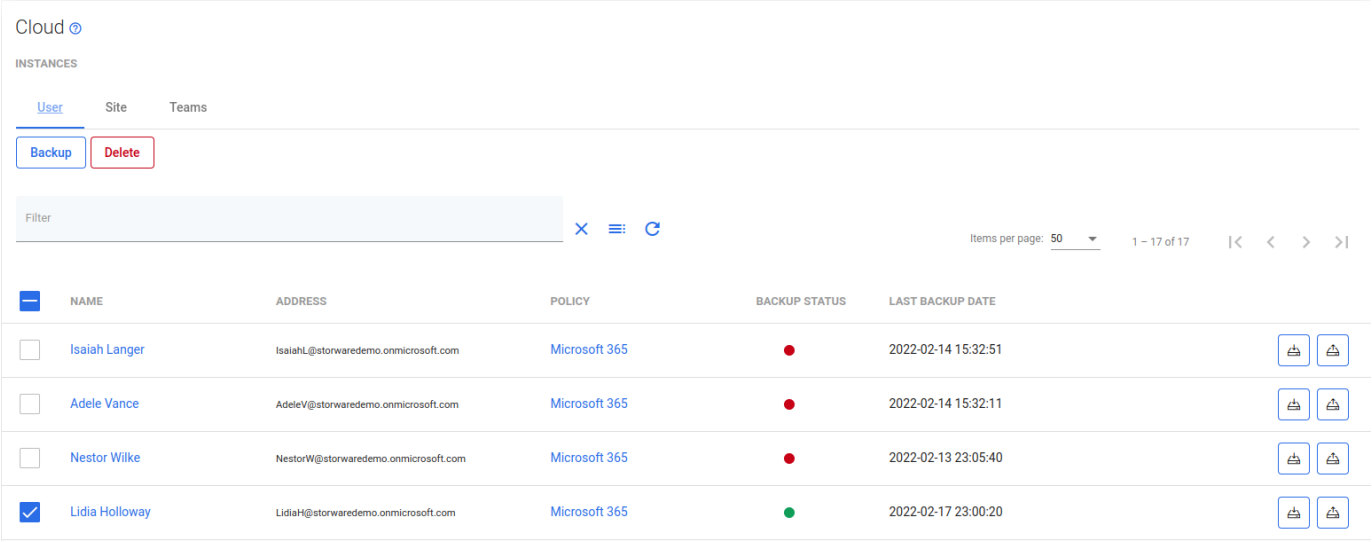


You can track the progress of the task in **tasks console**

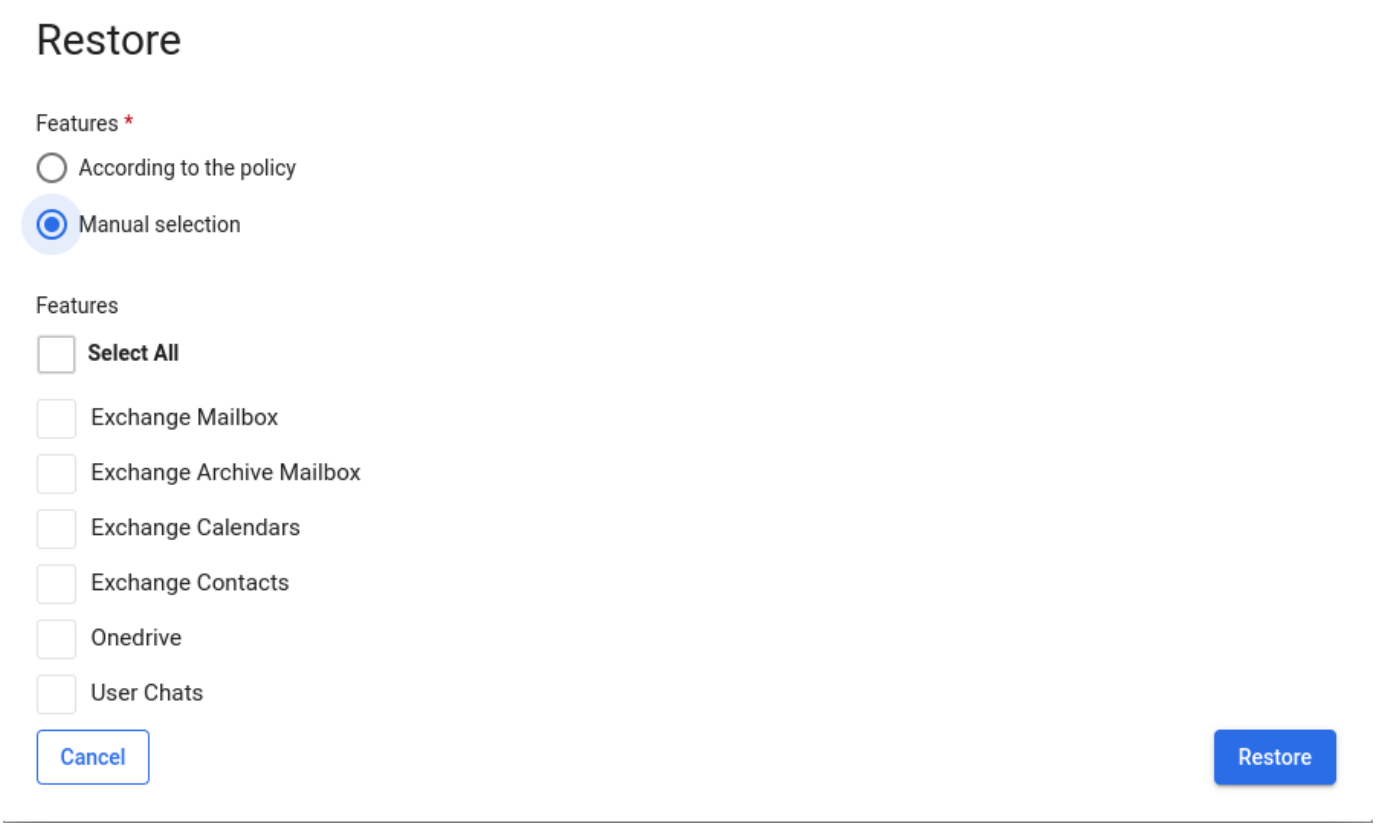


Manual restore

Search for cloud instance you want to restore and click **Restore** the button next to it.



In the next window, choose if you want to restore **according to the policy** or use **manual selection** to restore one specific feature directly to the restored account and click **Restore** the button.



Note: More information about Cloud you can find in the administration chapter.

Supported Sharepoint templates and limitations

Templates and apps supported for backup in Microsoft SharePoint Online

Supported site type:

- Teams site
- Communication site

Supported templates - Team site

	Event planning	**Project management**	**Retail management team**	**Store collaboration**	**Training and courses**	**Training and development team**	**Team collaboration**
List	yes	yes	yes	yes	yes	yes	yes
Document library	yes	yes	yes	yes	yes	yes	yes
Page	yes	yes	yes	yes	yes	yes	yes
Space	no	no	no	no	no	no	no
News post	yes (it is pages)	yes (it is pages)	yes (it is pages)	yes (it is pages)	yes (it is pages)	yes (it is pages)	yes (it is pages)
News link	yes (it is pages)	yes (it is pages)	yes (it is pages)	yes (it is pages)	yes (it is pages)	yes (it is pages)	yes (it is pages)
Plans	no	no	no	no	no	no	no
Event list	yes	yes	yes	yes	yes	yes	yes
App	no	no	no	no	no	no	no

List Template	**backup**	**restore**
Issue tracker	✅	✅
Employee onboarding	✅	✅
Event itinerary	✅	✅
Asset manager	✅	✅
Recruitment tracker	✅	✅
Travel requests	✅	✅
Work progress tracker	✅	✅
Content scheduler	✅	✅
Gift ideas	✅	✅
Expense tracker	✅	✅

List Template	backup	restore
Recipe tracker	✅	✅
Export - from excel	❌	❌
Blank list	✅	✅
Events	✅	✅
Progress tracker list	✅	✅
Inventory list	❌	❌

Supported templates - Communication site

	Crisis management	Leadership connection	Learning central	Showcase	Topic	Volunteer center
List	Yes	Yes	Yes	Yes	Yes	Yes
Document library	Yes	Yes	Yes	Yes	Yes	Yes
Page	Yes	Yes	Yes	Yes	Yes	Yes
Space	No	No	No	No	No	No
News post	Yes	Yes	Yes	Yes	Yes	Yes
New link	Yes	Yes	Yes	Yes	Yes	Yes
Event list	Yes	Yes	Yes	Yes	Yes	Yes
App	No	No	No	No	No	No

List Template	backup	restorer
Issue tracker	✅	✅
Employee onboarding	✅	✅
Event itinerary	✅	✅
Asset manager	✅	✅
Recruitment tracker	✅	✅
Travel requests	✅	✅
Work progress tracker	✅	✅
Content scheduler	✅	✅
Gift ideas	✅	✅
Expense tracker	✅	✅
Recipe tracker	✅	✅

List Template	backup	restorer
Export - from excel	❌	❌
Blank list	✅	✅

Unsupported templates:

- Communication site template - Department
- Communication site template - New employee onboarding

Unsupported elements on templates:

- Space
- Plans
- App

Limitations

- Contacts photos are not supported. Contacts are restored without photos.
- Marking messages as read or not read is not supported. Restored messages are always marked as read.
- OneNote files are not supported.
- Sharepoint comments are not supported.
- Calendar Groups are not supported.
- Site comments and likes are not supported.
- Messages for a private channel are not supported.
- Only parent Sharepoint sites can be restored. All subsites won't be restored.
- Wiki content is not supported

Protecting Applications

This section describes Data Protector for Cloud Workloads **generic mechanism** for multiple scenarios where VM-level backup may not be enough.

With Data Protector for Cloud Workloads you can prepare a custom script or invoke any backup command that produces backup artifacts (or just initiates an external backup process) on a remote host and stores backups to your backup provider.

With Application the backup you can extend your protection capabilities to:

- any remote applications with their own mechanisms
- hypervisor configuration
- files on remote hosts (physical, virtual, or containers)
    - this includes shares, mounted object-storage buckets, LVM block devices, or virtually anything which can be presented as a file
- initiating external backup processes such as RMAN

Data Protector for Cloud Workloads internal DB backup mechanism also uses Application backup. The mechanism uses predefined artifacts that simply need to be configured according to your needs.

In the Application section, you can read how the **generic mechanism** works and know what application Data Protector for Cloud Workloads can protect.

In the Backup & Restore section, you can find information about using Data Protector for Cloud Workloads to protect your application.

Applications

Data Protector for Cloud Workloads can protect Applications and others likes:

- Relax and Recover - ReaR
- Git

Main concepts

There are 2 main concepts that Data Protector for Cloud Workloads uses to execute backups:

- Command Execution Configuration
- Application Definition

Command Execution Configuration

This describes **how** to perform a backup operation. That is how to execute a command that produces a backup artefact which Data Protector for Cloud Workloads later stores in a backup provider. Multiple Application definitions share Command Execution Configuration but with different parameter values.

Command Execution Configuration properties come in several sections:

1. **General:**
    - **Name** - Name of your configuration
    - **Execution type**:
        - Node - execute this command directly on the node
        - Remote SSH - execute this command over SSH using credentials provided in the Application definition
    - **Timeout** - fail execution if a command doesn't complete within the time given
        - if you think that your backup should take longer, increase this value
        - this timeout is for whole command execution - if you have several steps in your script and you need additional timeouts for these steps - add them to your script
2. **Command arguments:**
    - add arguments that contain spaces as separate arguments
    - the first argument is the path to your executable
    - make sure this command is accessible on the remote host, and Data Protector for Cloud Workloads credentials will suffice to execute it
    - remote commands (over SSH) will invoke shell so you can use bash-style expressions (built-in commands such as `echo`, environmental variables or redirections) within the command argument
    - commands executed on the node are executed natively by OS, so if you want to use bash-style expressions (built-in commands such as `echo`, environmental variables or redirections) you need to split your command at least into 3 arguments: `/bin/bash`, `-c` and `your command > with some redirections`
3. **Data export:**
    - **Export data** - when enabled, Data Protector for Cloud Workloads will expect artefacts to be collected as a result of a command
    - **Source type:**
        - FILE - result will be a file, directory or path with `*` wildcard
        - STREAM - output of your command
    - **Source path:**
        - path to your artefacts that need to be collected
        - file, directory or path with `*` wildcard - more than 1 file on the source will result in files being stored as a single tar archive
    - **Remove files after export:**

        - if artefacts (files or source directory) need to be removed once exported
        - be careful when providing a path in the source directory, the whole directory will be removed when this setting is enabled
4. **Applications:**
    - select which applications will use this command execution config
5. **Parameters:**
    - this section allows you to define the parameters that will be expected to be entered in each application definition
    - each parameter will eventually become an environment variable in the application definition
    - each parameter has several properties
        - Name - Name of the resulting environmental variable
        - User-friendly hint - a hint what this parameter is to be shown later in the application definition
        - Default value - the default value, entered during initialization in the application definition form
        - Show in UI - if the value should be shown as dotted or not - useful for passwords
        - Obligatory - if we expect that its value should always be provided in the application definition form
6. **Error handling**
    - Standard error output stream handling (when non-empty):
        - Don't ignore it - will fail if anything is in the standard error output
        - Ignore without warning - will ignore it silently
        - Ignore with a warning - will ignore it but a warning indicator in the backup history will contain this output
    - Ignored Exit Codes:
        - error codes that should be ignored and not treated by Data Protector for Cloud Workloads as errors
        - by default, only 0 is assumed as a success

Application Definition

Once you have your command execution configuration defined (or you choose to use the predefined ones provided with Data Protector for Cloud Workloads), you should define the instances of your application.

There are a few parameters for application definition that come in several sections:

1. **General:**
    - Name - Name of your application instance
    - Choose node - which node is going to execute this command
    - Backup policy - optionally set policy for scheduled backups
    - Command execution configuration
        - configuration of your command used for this application
        - **Note:** when you create a definition for the first time, you select a configuration and click **Save** - you will be redirected to the Settings tab for additional details
2. **Environment variables**
    - shown only when the definition has been saved on the Settings tab
    - defines a list of environment variables that will be passed to your command/script during its invocation
    - parameters from the command execution config will be populated automatically
    - each parameter has several properties:
        - Key - name of the environmental variable
        - Value - Value of the environment variable
        - Show - if the value should be shown as dotted or not - useful for passwords
3. **SSH access:**
    - shown when Remote SSH is chosen as the execution type in command execution configuration
    - parameters:
        - SSH host - host where the command will be executed
        - SSH port - port on which the SSH service is running (by default 22)

        - SSH user - user used to connect via SSH
        - SSH key path:
            - path to your key - needs to be a file only accessible by Data Protector for Cloud Workloads with `400` permissions
            - alternatively, you can use the password access method
4. **Password:**
    - shown when Remote SSH is chosen as the execution type in command execution configuration
    - set your SSH password here if you're not using the public-key authentication method

Enabling WinRM on Windows machines

The Windows Remote Management (a.k.a. WinRM) interface is a network service that allows remote management access to computers via the network. It's used to allow remote management of computers via PowerShell. As a result, WinRM is not enabled by default on Windows Server.

There is an `enable_winrm.ps1` script in the `/opt/vprotect/scripts/winrm` directory

A Power Shell script performs the following steps:

- Automatically starts the WinRM service
- Adds all addresses to trusted hosts. This can be changed in line 7, replacing the aseterix symbol with the appropriate address, e.g.

Add all computers to the TrustedHosts list

```
Set-Item WSMan:\localhost\Client\TrustedHosts -Value *
```

Add all domain computers to the TrustedHosts list

```
Set-Item WSMan:\localhost\Client\TrustedHosts *.yourdomain.com
```

Add specific computers to the TrustedHosts list

```
Set-Item WSMan:\localhost\Client\TrustedHosts -Value DESKTOP-R88J8V5, MacBookPro19
```

Add computers to the TrustedHosts list using the IP address

```
Set-Item WSMan:\localhost\Client\TrustedHosts -Value 192.168.100.69
```

- Adds an exception in Windows Firewall, which is used by WinRm over HTTPS (port 5986).
- Creates a self-signed certificate and creates Create HTTPS listener.

The `enable_winrm.ps1` script must be run on the Hyper-V server in the PowerShell console.

PowerShell for Linux must be installed on the machine where Node is installed. You can download it from GitHub at:

{% embed url="https://github.com/PowerShell/PowerShell" %}

More about installation and versions for different Linux distributions here:

{% embed url="https://docs.microsoft.com/en-us/powershell/scripting/install/installing-powershell-core-on-linux?view=powershell-7.1" %}

After the correct installation, we can test the connection. On Linux, run PowerShell with the pwsh command.

Then we connect to the Hyper-V server:

```
Enter-PSSession -ComputerName IP_ADDRESS -UseSSL -SessionOption (New-PSSessionOption -SkipCNCheck -SkipCACheck) -Authentication Basic -Credential (Get-Credential)
```

After providing the correct credentials, the PowerShell console will start on the remote machine. We end the session with the "exit" command. We can also try a test PowerShell script on a remote machine:

```
Invoke-Command -Session (New-PSSession -ComputerName SERVER_ADDRESS -UseSSL -SessionOption (New-PSSessionOption -SkipCNCheck -SkipCACheck) -Authentication Basic -Credential (Get-Credential)) -ScriptBlock {Get-ChildItem Env:}
```

or

```
Enter-PSSession -ComputerName SERVER_ADDRESS -UseSSL -SessionOption (New-PSSessionOption -SkipCNCheck -SkipCACheck) -Authentication Basic -Credential (Get-Credential)
```

Relax and Recover - ReaR

To create a new application for Relax and Recover database backup, go to the tab: **Applications -> Instances**

Then select the **Create** button. The Creating an Application Definition section will be displayed, which needs to be completed.

This is a description of how your script is going to be invoked - you need to specify:

- **Name** - unique name of the application in the Data Protector for Cloud Workloads system
- **Choose Node Config** - select which node should perform the task
- **Backup policy** - specify which backup policy should be used for this application
- **Command execution configuration** - select a prepared template for backup or create a new one yourself

In the SSH access subtab, complete the following fields:

- **Host** - set the address of the host where the instance exists
- **Port** - set the host port
- **User** - indicate a user for connecting to the ssh
- **Password** - enter the connection password
- **SSH key path** - alternatively you can specify the ssh key path for authorization

After **saving** the changes to the application, you need to configure the **environment variables** in the **settings section** of your application as needed.

When using the built-in script for database backup, define:

- **VP_REAR_OUTPUT** - Defines where the rescue image should be sent
- **VP_REAR_LOGFILE** - Path to the target server, where Data Protector for Cloud Workloads can place the log file from the backup job.
- **VP_REAR_MOUNTPATH** - Path where the NFS directory will be mounted
- **VP_REAR_STOREPATH** - Path to the Relax and Recover server, where Data Protector for Cloud Workloads can place the backup file.
- **VP_REAR_METHOD** - Relax and Recover backup method
- **VP_REAR_RETENTION** - Number of days to keep the copy
- **VP_REAR_NFSSERVER** - IP address of the NFS server
- **VP_REAR_SCRIPTPATH** - Path to the target server, where Data Protector for Cloud Workloads can place and execute the backup script.

> **Note:** After the new application is fully configured, **save** the changes and go to the Backup SLAs configuration.

Git

To create a new application for Git Repository instances backup, go to the tab: **Applications -> Instances** Then select the **Create** button. The 'Creating an Application Definition' section will be displayed, which needs to be completed. This is a description of how your script is going to be invoked - you need to specify:

- **Name** - unique name of the application in the Data Protector for Cloud Workloads system
- **Choose Node Config** - select which node should perform the task
- **Backup policy** - specify which backup policy should be used for this application
- **Command execution configuration** - select a prepared template for Git Repository backup or create a new one yourself

After **saving** the changes to the application, you need to configure the **environment variables** in the **settings section** of your application as needed. When using the built-in script for database backup, define:

- **VP_GITREPO_ADDRESS** - The git clone address (ssh/https) of the repository.
- **VP_GITREPO_USERNAME** - Git name of the user with access to the specified repository.
- **VP_GITREPO_PASSWORD** - Git password of the user with access to the specified repository.
- **VP_GITREPO_STOREPATH** - Path on the server with connection to the Git repository, where Data Protector for Cloud Workloads can place the temporary backup file. No other files should be stored in the given path since everything is removed after the backup is finished.
- **VP_GITREPO_SCRIPTPATH** - Path on Data Protector for Cloud Workloads node, where the backup script is located.

> **Note:** After the new application is fully configured, **save** the changes and go to the Backup SLAs configuration.

Backup & Restore

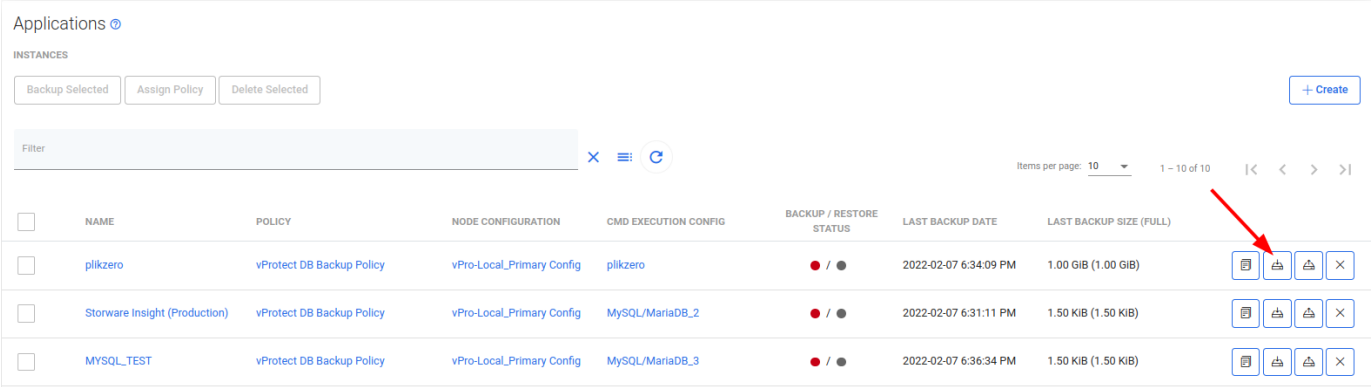
This section is a simple step-by-step guide on how to use Data Protector for Cloud Workloads to protect your Applications.

Backup and restore of Application

Manual backup

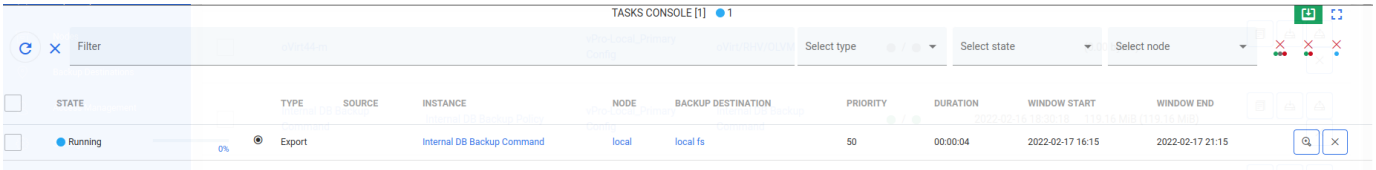
Note: to perform a manual backup, a target Application instance must be assigned to Backup SLA

1. Search for Application instance you want to backup and click **Backup** the button next to it.



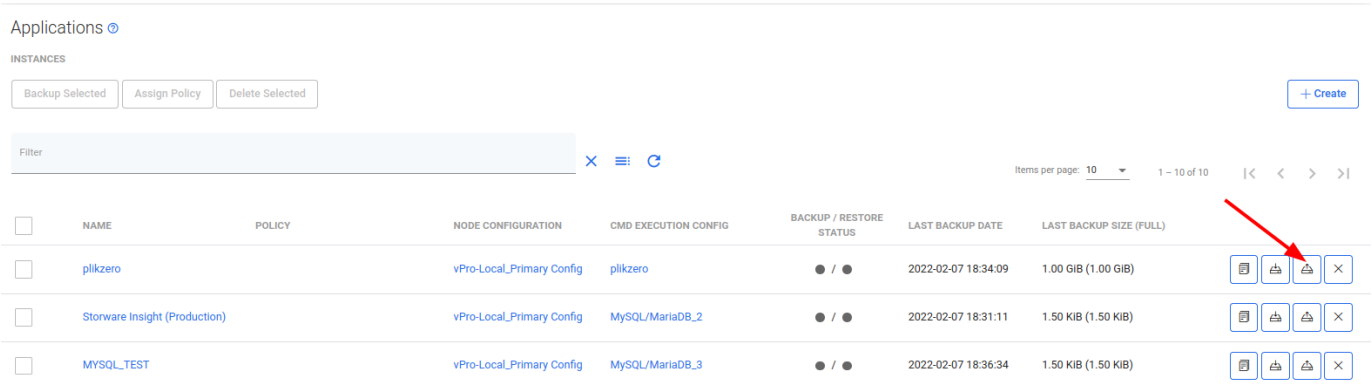
2. In the next window, choose backup type and click **Backup** button.

3. You can track the progress of the task in **tasks console**

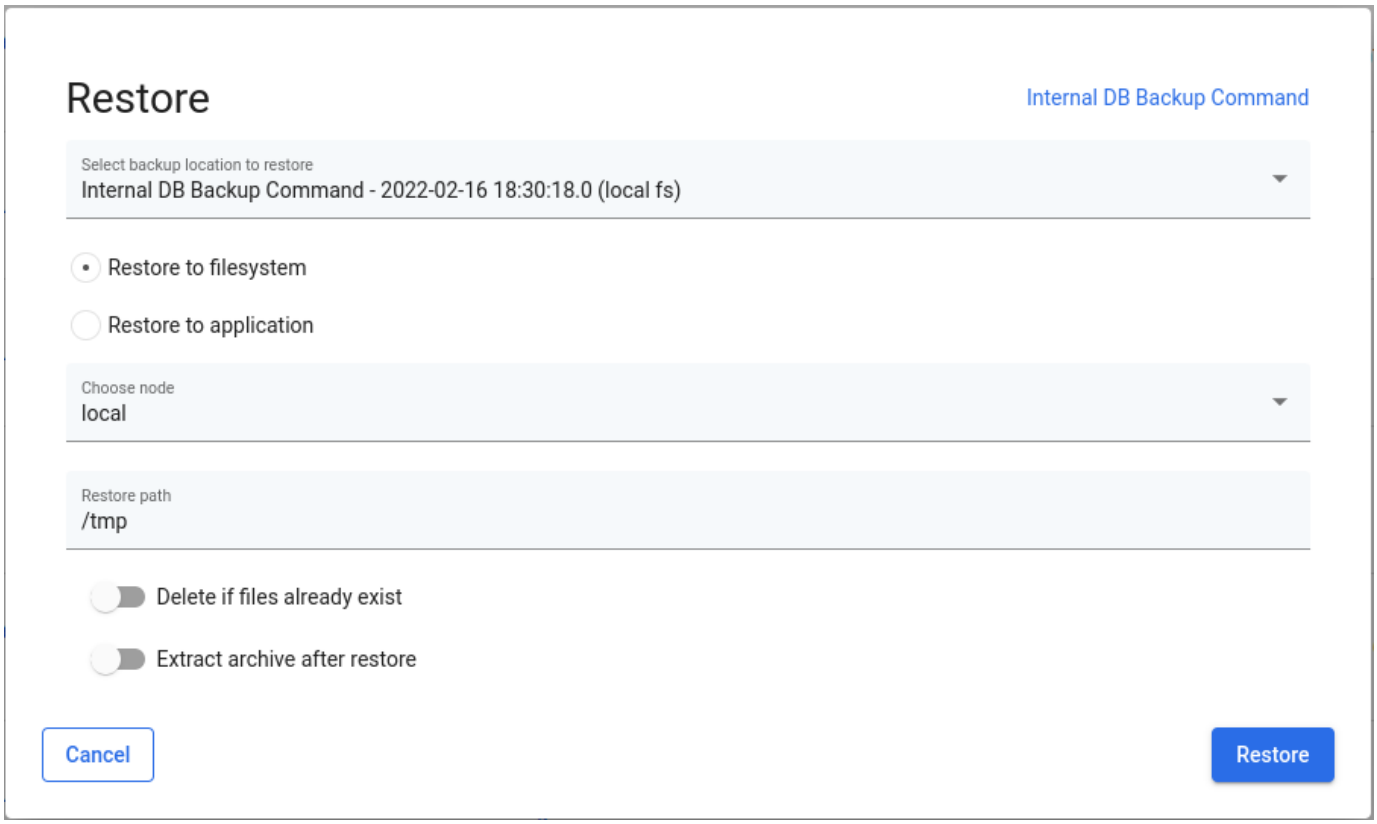


Manual restore

1. Search for Application instance you want to restore and click **Restore** the button next to it.



2. In the next window, choose if you want to restore to the file system or to the application instance host. Enter the rest parameters according to your needs and click **Restore** button.



Note: More information about protecting Applications you can find in the administration chapter.

Protecting Storage Providers

Data Protector for Cloud Workloads supports data protection for several storage providers.

In the chapter Storage Providers you can read how to use Data Protector for Cloud Workloads to protect Storage Providers and how to protect them you can read in chapter Backup & Restore

Storage Providers

This feature allows you to protect file systems mounted on Data Protector for Cloud Workloads Nodes, Ceph RBD volumes, and more.

- Ceph RBD
- Nutanix Files
- Nutanix Volume Groups

> **Note**: Synthetic backup destination is not available for Storage Providers

Ceph RBD

General

In order to connect to Ceph RBD you need to provide the keyring and configuration files. The Ceph RBD storage provider should detect the volumes and pools in the environment and allow you to assign backup policies. Data Protector for Cloud Workloads uses the RBD-NBD approach to mount a remote RBD snapshot over NBD and read data.

> **Note:**
>
> - Data Protector for Cloud Workloads needs access to the monitors specified in the Ceph configuration file.
> - When creating Ceph RBD storage provider for the OpenStack environment only the credentials specified in the storage provider form are used by the OpenStack backup process - the actual technique (RBD-NBD mount or cinder in disk-attachment strategy) and **node** for connecting and the backup volumes depend on the OpenStack hypervisor manager settings, not in the storage provider settings

Example

Please complete the following steps to add the Ceph RBD storage provider:

- Data Protector for Cloud Workloads Node supports Ceph RBD, for which you will need to install ceph libraries:
  - On Data Protector for Cloud Workloads **Node** enable the required repositories:

For Data Protector for Cloud Workloads Node installed on RHEL7:

```
sudo subscription-manager repo --enable=rhel-7-server-rhceph-4-tools-rpms
```

For Data Protector for Cloud Workloads Node installed on RHEL8:

```
sudo subscription-manager repo --enable=rhceph-4-tools-for-rhel-8-x86_64-rpms
```

For Data Protector for Cloud Workloads Node installed on CentOS7:

```
sudo yum install epel-release
sudo rpm --import 'https://download.ceph.com/keys/release.asc'
sudo yum install https://download.ceph.com/rpm-octopus/el7/noarch/ceph-release-1-
1.el7.noarch.rpm
```

For Data Protector for Cloud Workloads Node installed on CentOS8:

```
sudo yum install epel-release
sudo rpm --import 'https://download.ceph.com/keys/release.asc'
sudo yum install https://download.ceph.com/rpm-octopus/el8/noarch/ceph-release-1-
1.el8.noarch.rpm
```

- Install the rbd-nbd and ceph-common package, with all dependencies:

```
yum install rbd-nbd ceph-common
```

- Go to **Storage** -> **Infrastructure** and click **Add Storage Provider**
- Choose **Ceph RBD** as the type and select the node responsible for backup operations
- Provide `Ceph keyring file contents` which is the contents of your keyring file from the Cinder host - `/etc/ceph/ceph.client.admin.keyring`, for example:

> **Note:** Remember, both contents need to end with the new line sign.

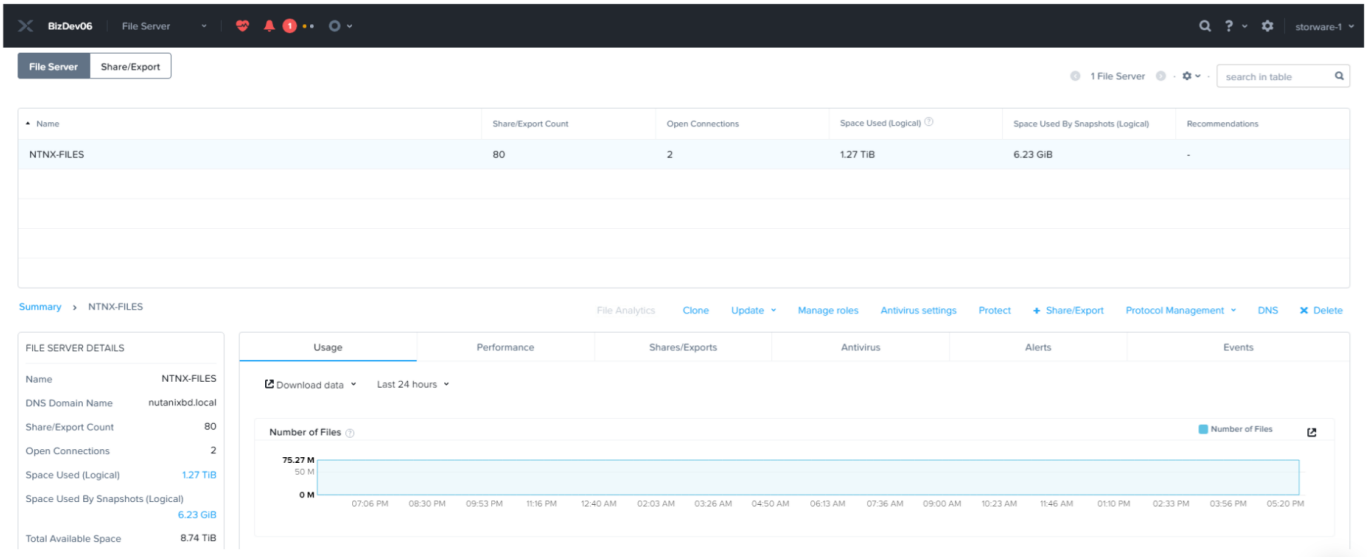
```
[client.admin]
key = AQCCQG5dGKhUFBAA9G7TTQWfFXbF1ywbqpA1Vw==
caps mds = "allow *"
caps mgr = "allow *"
caps mon = "allow *"
caps osd = "allow *"
```

- Provide `Ceph configuration file contents`, for example:

```
[global]
cluster network = 10.40.0.0/16
fsid = cc3a4e9f-d2ca-4fec-805d-2c40605723b3
mon host = ceph-mon.domain.local
mon initial members = ceph-00
osd pool default crush rule = -1
public network = 10.40.0.0/16
[client.images]
keyring = /etc/ceph/ceph.client.images.keyring
[client.volumes]
keyring = /etc/ceph/ceph.client.volumes.keyring
[client.nova]
keyring = /etc/ceph/ceph.client.nova.keyring
```

- Click **Save** - now you can initiate inventory synchronization (pop-up message) to collect information about available volumes and pools
    - later you can use the **Inventory Synchronization** button on the right of the newly created provider on the list.
- Your volumes will appear in the **Instances** section in the submenu on the left, from which you can initiate backup/restore/mount tasks or view volume backup history and its details.

Nutanix Files



General

Nutanix Files offers file system storage in the form of network shares (SMB or NFS). With Data Protector for Cloud Workloads, you can easily back up and recover these shares.

> **Note:**
>
> - there must be an account defined in both Prism Central and File Server with the same credentials
> - each File Server is considered as a separate Storage Provider
> - Data Protector for Cloud Workloads tracks changes for each file system change using the Nutanix CFT mechanism
> - this shortens backup times because it does not need to perform a metadata scan across your file server, which could contain millions of files and directories.
> - only regular files, symlinks, and directories are backup
> - for file systems, Data Protector for Cloud Workloads currently build images for each backup before uploading data to the specific backup provider so that it doesn't have to upload objects one-by-one - these images will be merged automatically in restore tasks

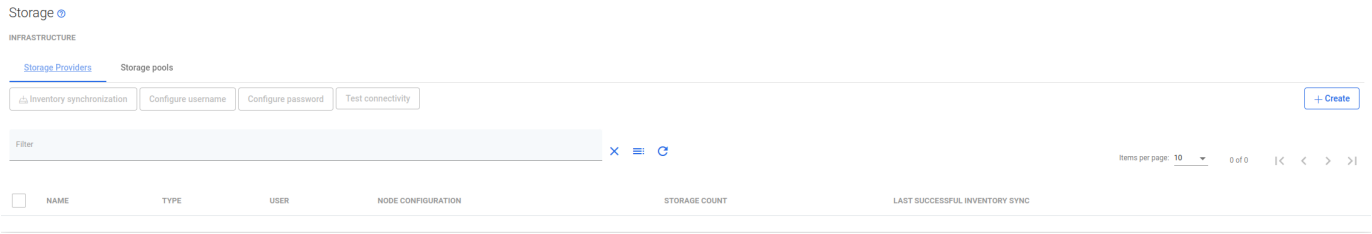
In general, the process looks as follows:

- the user adds a new storage provider (Nutanix files)
- inventory synchronization retrieves all the information about storage (of two types: SMB and NFS)
- the user can then do a full backup (storage is mounted and all files are extracted from it)
- incremental backup uses CFT from the API, and based on this list Data Protector for Cloud Workloads only downloads changed files.

Example

Please complete the following steps to add the Nutanix Files storage provider:

Go to **Storage** -> **Infrastructure** and click on **Create**



In the form, provide:

- `Nutanix Files` as the type
- The File Server URL in the `host` field (i.e. `https://FILE_SERVER:9440`)
- The URL to the Prism Element Host (i.e. `https://PRISM_ELEMENT:9440`)
- The login and password
    - The `admin` account **cannot** be used
    - The same credentials will be used to access Prism Element and File Server
    - In Prism Element, there is a dedicated account with a Cluster Admin role
    - Create an API account for the file server (e.g. in Prism Element, go to the File Server tab, select Manage Roles, add an API user and add the user to the file server administration group)
    - If you want to use domain account, enter it in this form - `domain\username`
- The node responsible for backup operations

Click **Storage** - now you can run inventory synchronization to detect file systems (storage instances) - they will be visible in **Storage** -> **Instances** view

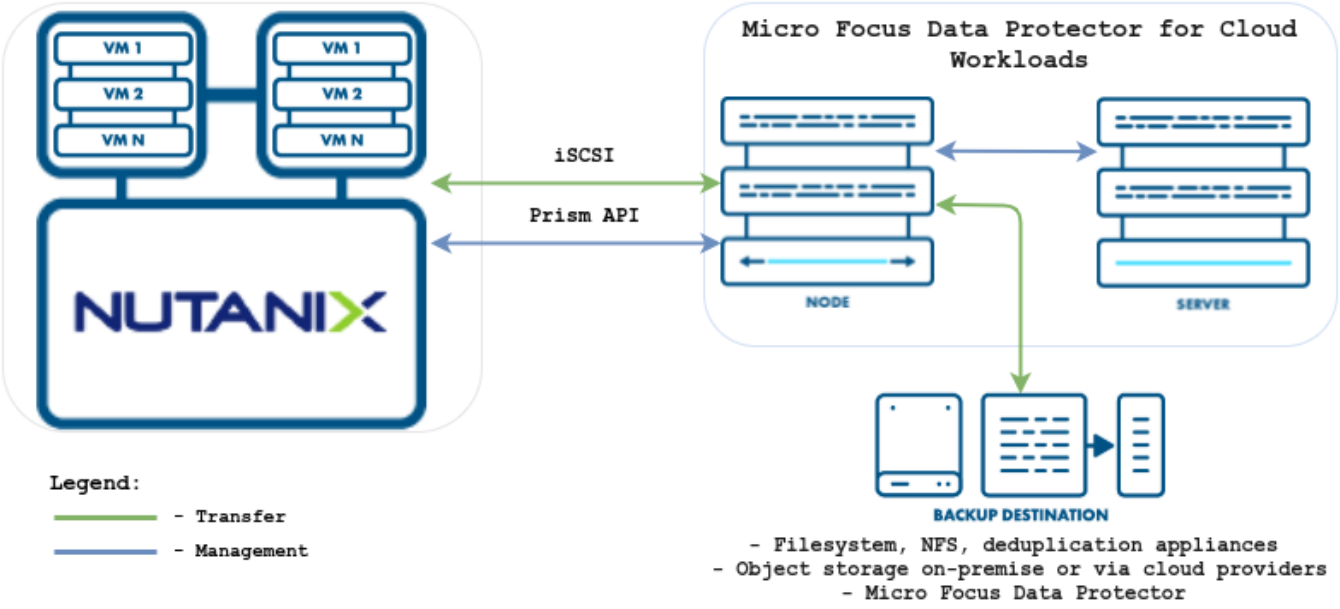
Now you can assign backup SLAs in **Storage** -> **Backup SLAs** to schedule periodic backups of these shares. You are also able to mount backups to restore individual files using Mounted Backups (File-level Restore).

Nutanix Volume Groups

General

Data Protector for Cloud Workloads supports volume groups for the Nutanix platform. Disk snapshots are being attached to the host with Data Protector for Cloud Workloads Node using iSCSI. Thanks to this backups and restores can be performed remotely without Proxy VM.

This storage provider also allows excluding disks for backups.



In general, the export process looks as follows:

- A Snapshot of the volume group is taken
- A Temporary volume group with disk snapshots is created
- Disks from the temporary volume group are attached to Data Protector for Cloud Workloads Node host using iSCSI
- Disks content is exported to RAW files
- Disks are then detached and temporary volume group is deleted

In general, the restore process looks as follows:

- A new volume group is created with yet empty disks
- Disks from a new volume group are attached to Data Protector for Cloud Workloads Node host using iSCSI
- Content from RAW files of backup is imported to attached disks
- Disks are detached from Data Protector for Cloud Workloads Node host

> **Note:** iSCSI uses `iSCSI Data Services IP` defined on the Nutanix platform to discover targets, which means that exception will be thrown if this value is missing.

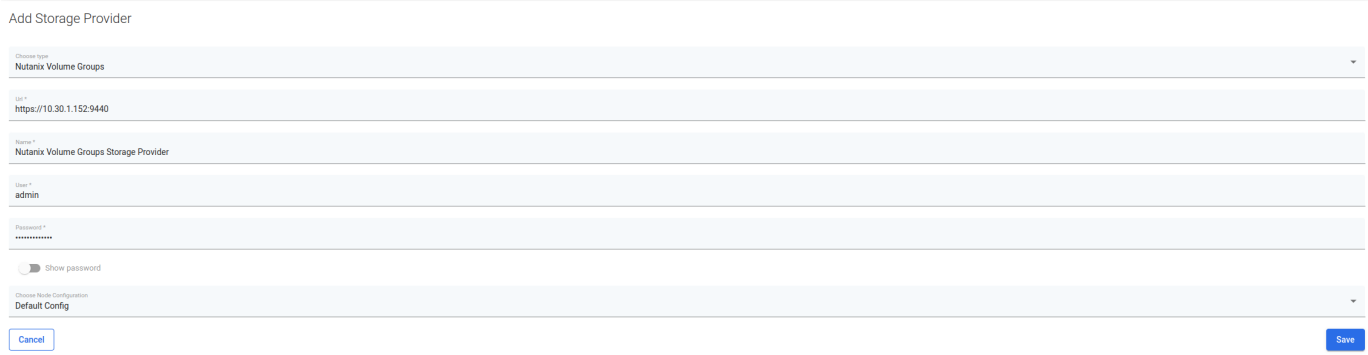
Example

Please complete the following steps to add the Nutanix Volume Groups storage provider:

Go to **Storage** -> **Infrastructure** and add click on **Create**

In the form provide:

- `Nutanix Volume Groups` as a type
- URL to Prism Element Host (i.e. `https://PRISM_ELEMENT:9440`)
- Name of the storage provider
- Login and password
- The node configuration responsible for backup operations



Click **Save** - now you can run inventory synchronization to detect volume groups - they will be visible in **Storage** -> **Instances** view

Now you can create a backup task for the chosen volume group.

Backup & Restore

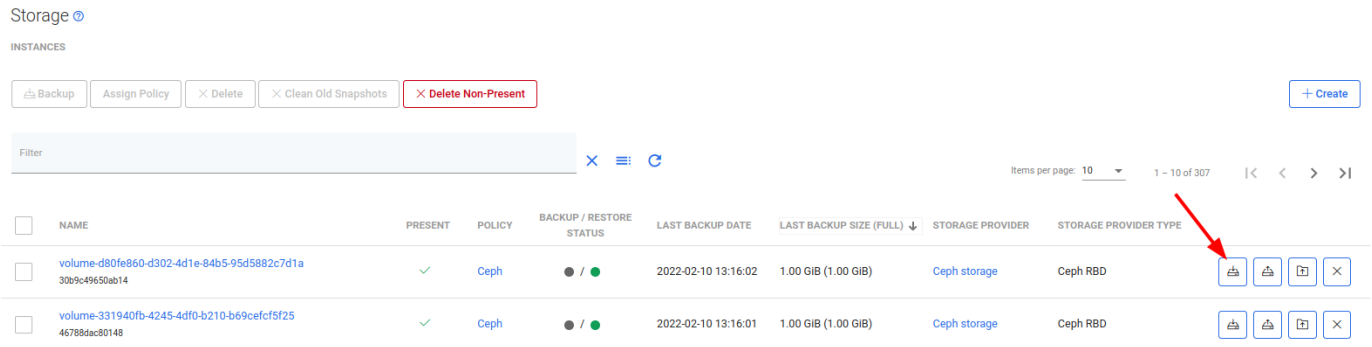
This section is a simple step-by-step guide on how to use Data Protector for Cloud Workloads to protect your Storage Providers.

Bacup and restore of Storage Provider

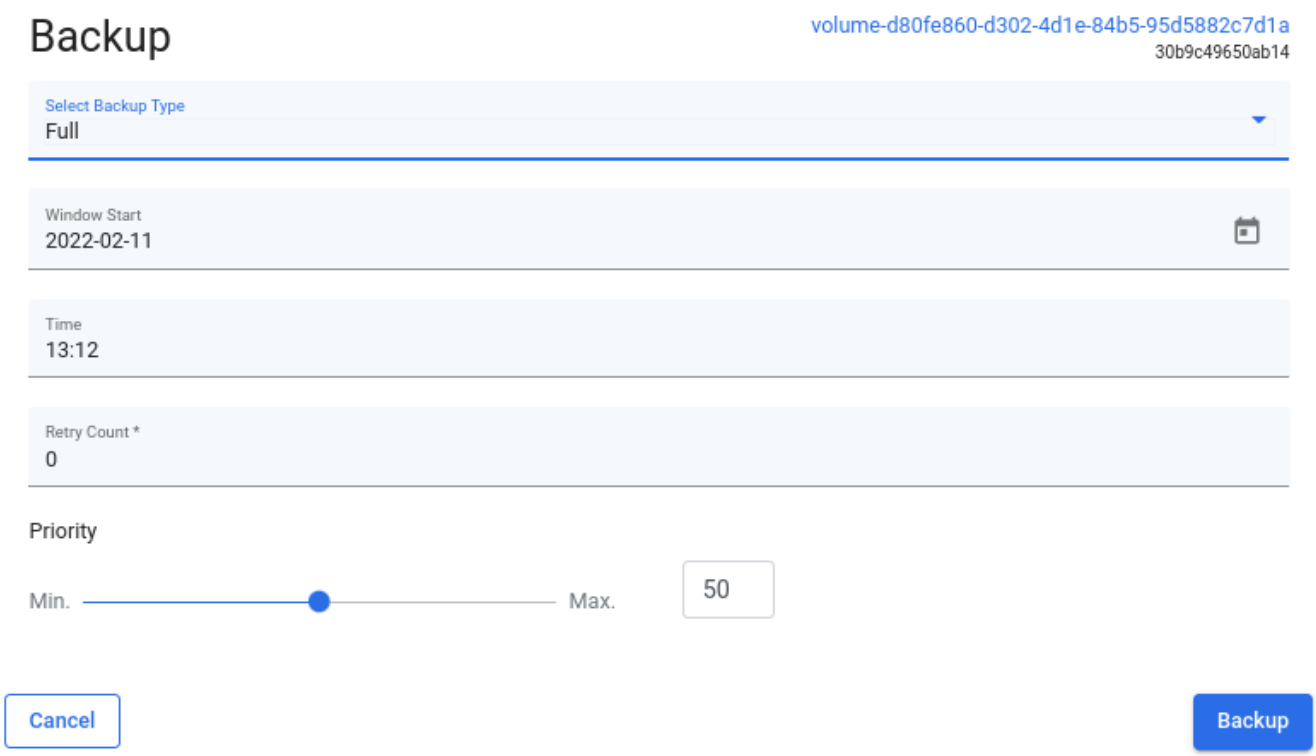
Manual backup

Note: to perform a manual backup, target Storage Provider instance must be assigned to Backup SLA

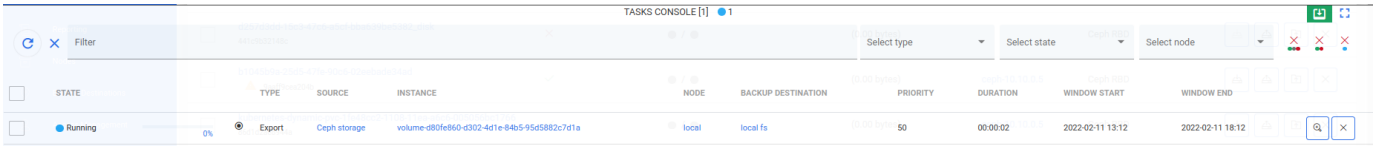
1. Search for Storage Provider instance you want to backup and click the **Backup** button next to it.



2. In the next window, choose backup type and click **Backup** button.

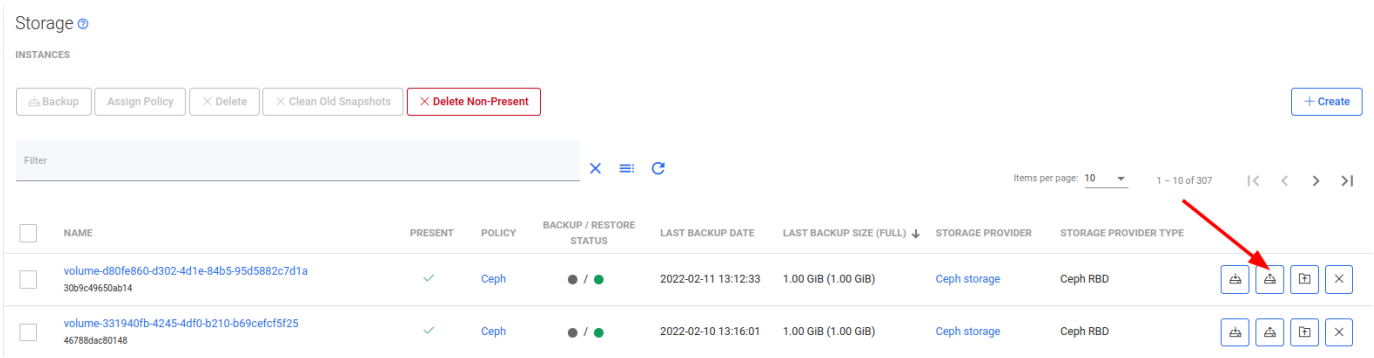


3. You can track the progress of the task in **tasks console**



Manual restore

1. Search for Storage Provider instance you want to restore and click the **Restore** button next to it.



2. In the next window, choose if you want to restore to File System or directly to the storage provider. Enter the rest parameters according to your needs and click the **Restore** button. The available parameters may differ depending on the storage provider.

Note: More information about protecting Storage Providers you can find in the administration chapter.

Administration

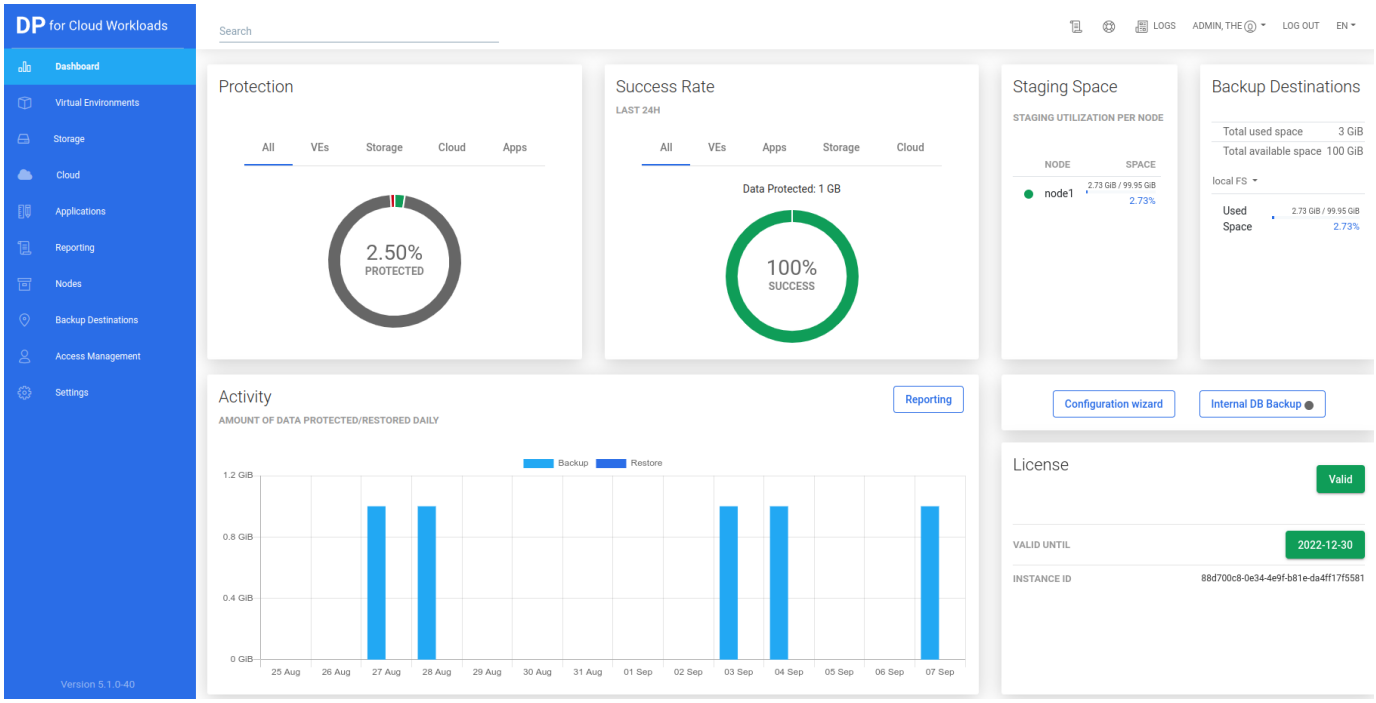
This section provides information about administrative tasks such as how to backup, restore, or manage key elements using Web UI of Data Protector for Cloud Workloads like:

- Dashboard
- Virtual Environments
- Storage Providers
- Cloud
- Applications
- Reporting
- Nodes
- Access Management
- Settings

We also recommend reading the Disaster Recovery section carefully to be sure that you understand how to recover Data Protector for Cloud Workloads installation in case of losing the node or even server.

For a complete list of CLI commands, check CLI Reference.

Dashboard



Overview

The primary Data Protector for Cloud Workloads interface is the WEB UI accessible via a web browser.

Divided into a few sections, it makes it possible to view and set the most vital options related to management, monitoring and reporting.

The left pane contains the main menu (see below for a more detailed description).

The **Protection** field present the overall statistics about protection of your environment. The instance is considered protected when it is attached to Backup SLA and the backup has been done in the last 24 hours.

The upper right corner provides access to documentation, support and system logs.

The lower part provides the option to view the (sliding) task console.

The menu on the left provides access to the most important sections:

- Dashboard - the main screen with a general summary and the configuration wizard
- Virtual Environments - page where you can add and protect your Environments
- Storage - page where you can add and protect your Storage
- Cloud - page where you can add and protect your Microsoft 365 organization
- Applications - page where you can add and protect your Applications
- Reporting - page where you can see all reports from Data Protector for Cloud Workloads
- Nodes - node management and node configurations
- Backup Destination - create and manage backup destinations
- Access Management - create and manage your accounts (Language, time zones, etc.)
- Settings - From here, you can manage global settings, licenses, email, authentication, and internal DB backup.

Virtual Environments

This section provides information about administrative tasks like:

Instances - list of currently known virtual machines and access to the details page of each object.

Infrastructure - access configuration for hypervisors and hypervisor managers, basic info about the inventoried environment, such as clusters and storage.

Backup SLAs - allows you to set up a correlation between virtual machines, the backup destination, and schedules (Policies tab). It also allows you to configure policy schedules (schedules tab).

Snapshot SLAs - allows you to set up a correlation between virtual machines, snapshot retention, and schedules (Policies tab). It also allows you to configure policy schedules (schedules tab).

Recovery Plans - this allows you to set up a number of rules to restore your virtual machines into a hypervisor or filesystem to test your backups (Policies tab). It also allows you to configure policy schedules (schedules tab).

Mounted Backups (File-level Restore) - browse and download files from mounted backups.

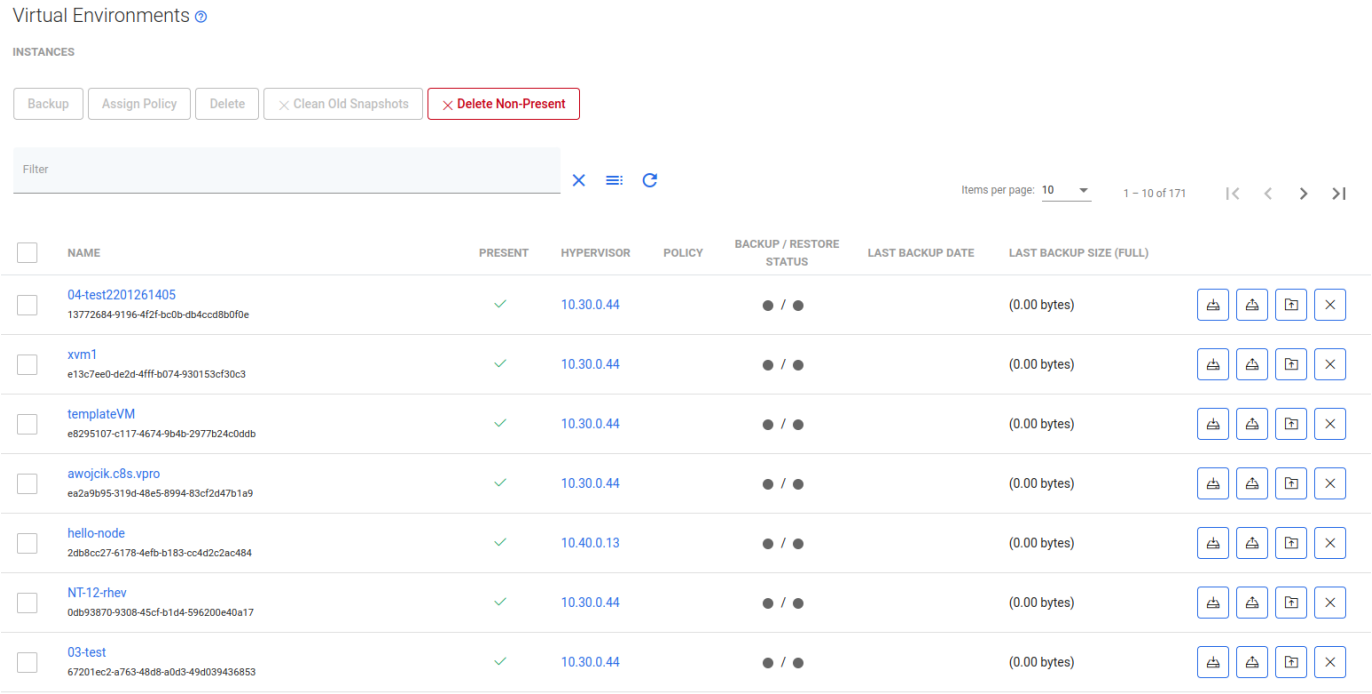
Instances

General

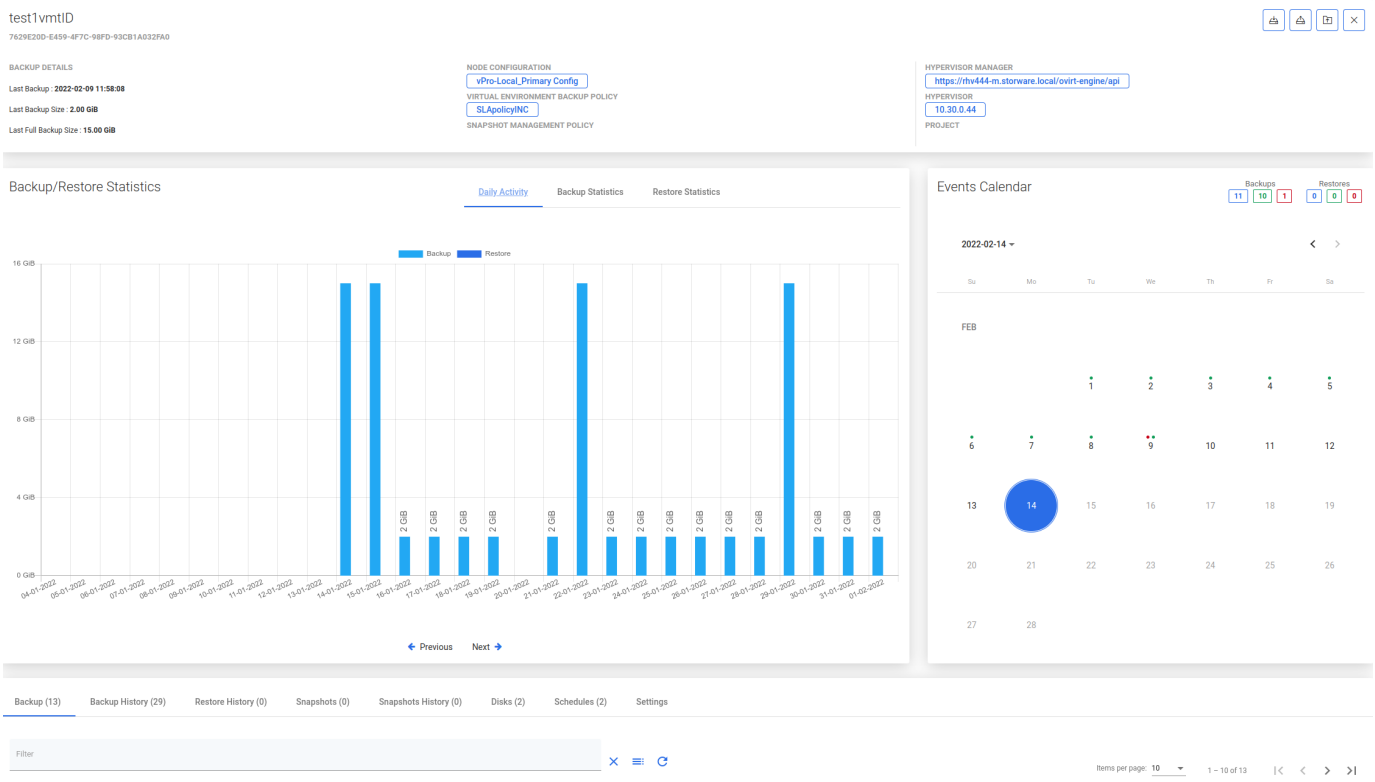
A list of currently known virtual machines and access to the details page of each object. From this place, you can also perform on-demand actions such as backup, restore and file-level restore.

The field lets the user filter the virtual machines by their:

- Name
- UUID
- GUID
- Tags
- Url of a linked hypervisor manager
- Node configuration name linked via hypervisor manager
- Host field of a linked hypervisor
- Node configuration name linked via a hypervisor
- Name field of a linked VM Backup Policy
- Name field of a linked Snapshot Management Policy

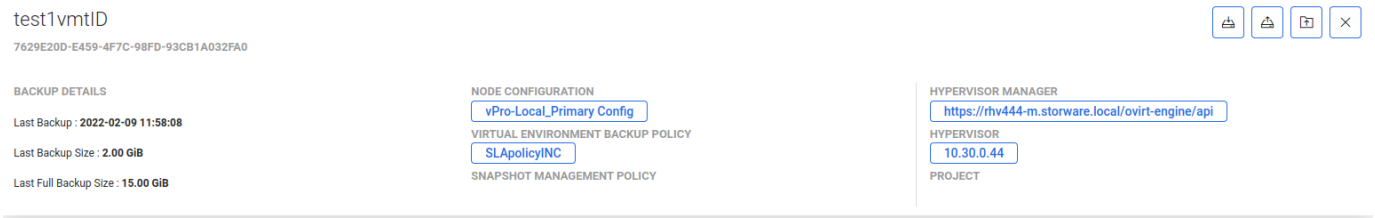


Returning to the VM details page, this is what it looks like:



As you can see, the window has been divided into several areas:

VM Summary



At the top, you can see summarized pieces of information about the VM, such as:

- the ID of the VM object into Data Protector for Cloud Workloads
- to which hypervisor the VM belongs
- which node is backing up this virtual machine
- short information about the last backup actions
- whether the virtual machine has tags or policies assigned to it

You can also use several function buttons:

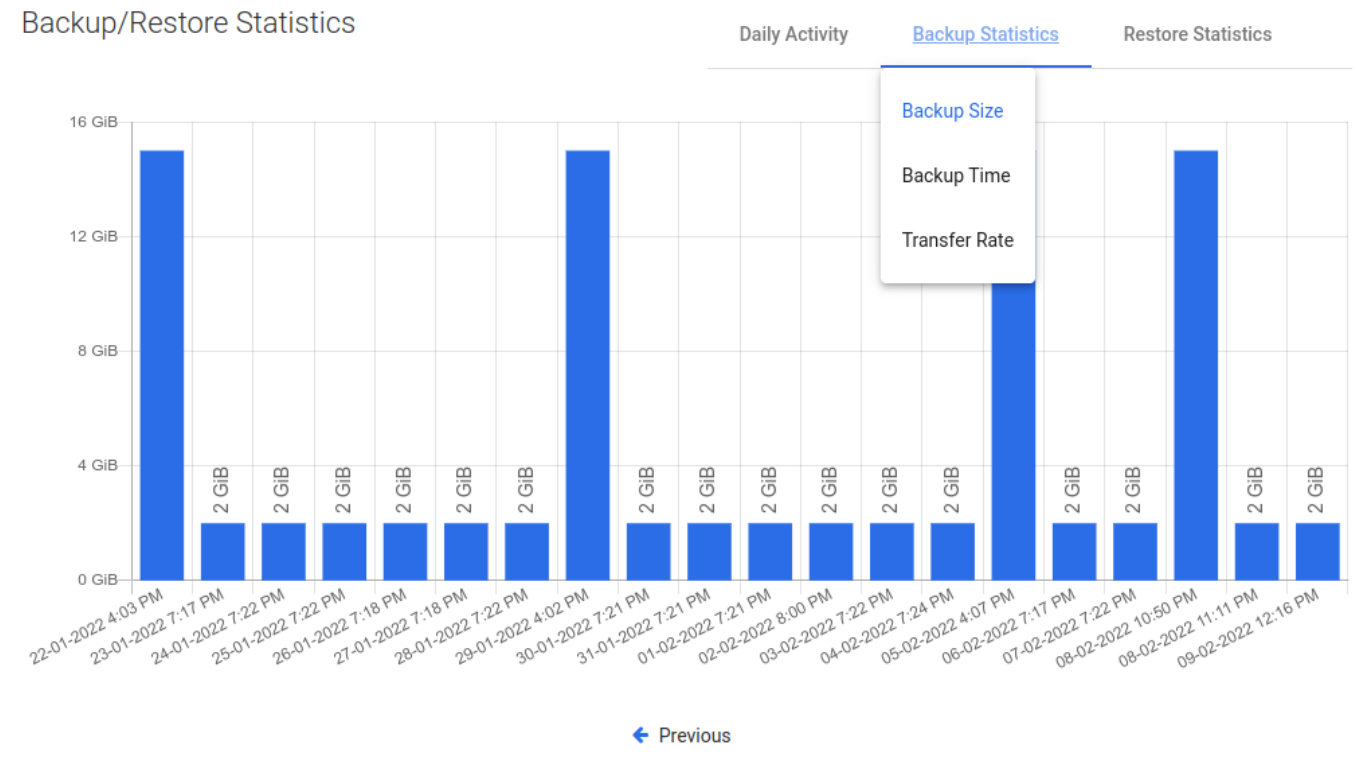
- refresh
- back to list
- backup
- restore
- mount
- delete

Backup/Restore Statistics

Daily activity

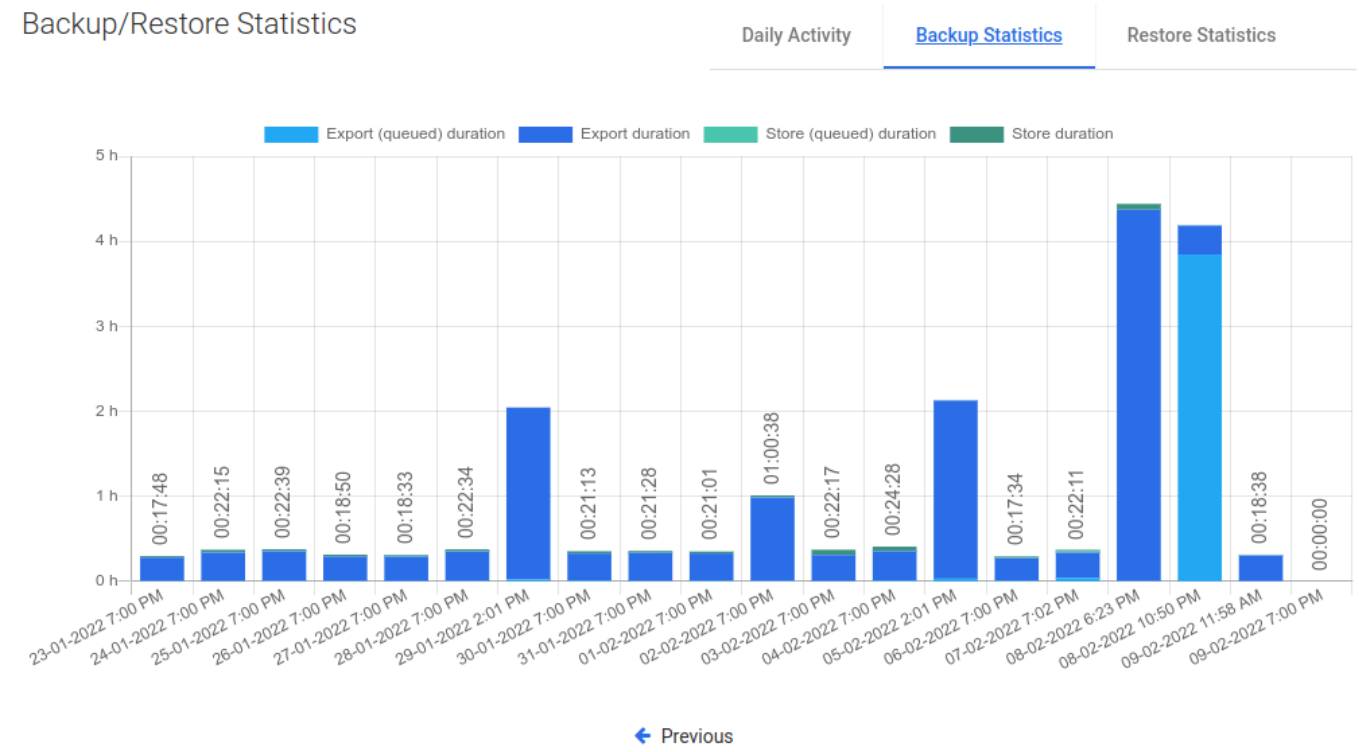
First, you'll see a daily summary of the backup and restore operations for the last month. This view is called "Daily Summary" and is the default view. You can switch the report between four views.

Backup Size



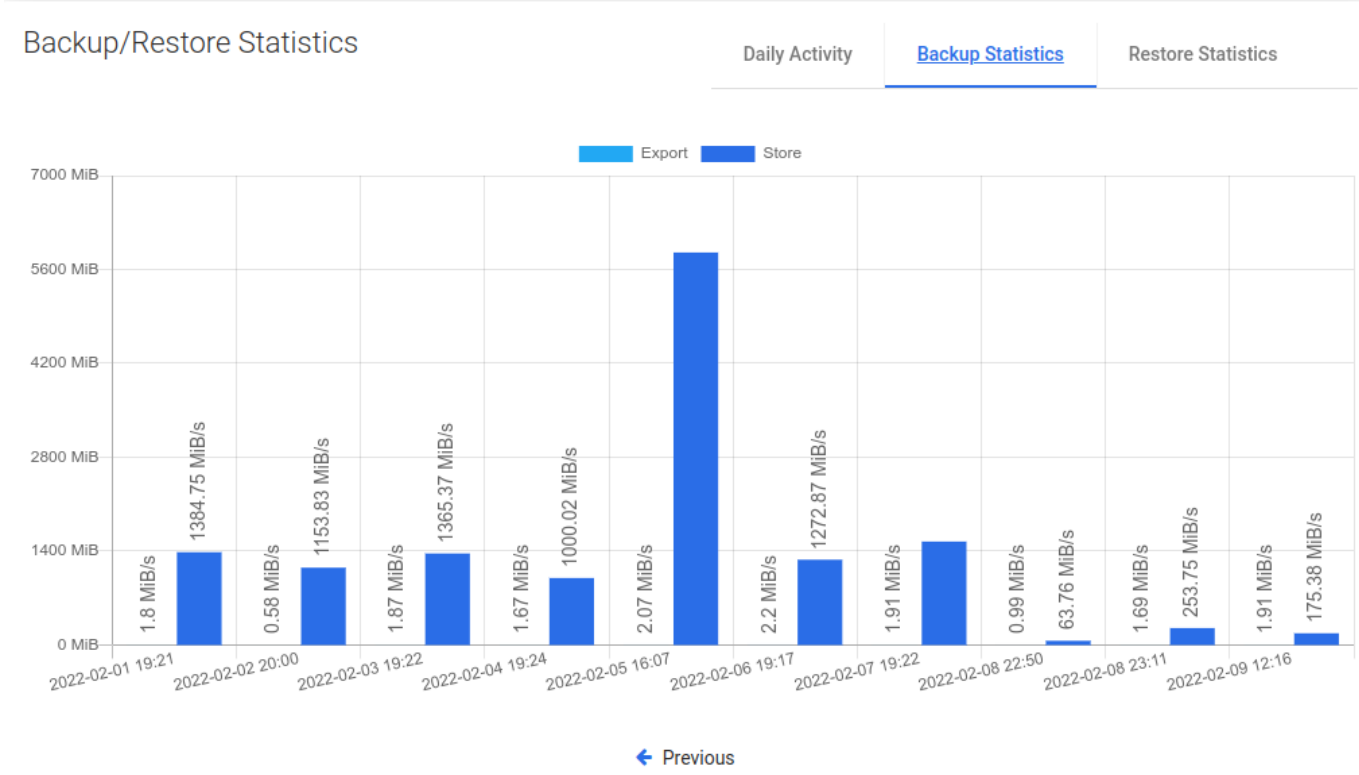
This view shows separate columns for each backup made to the virtual machine. Thanks to this, you can easily determine what data increase occurs on a given machine.

Backup Time



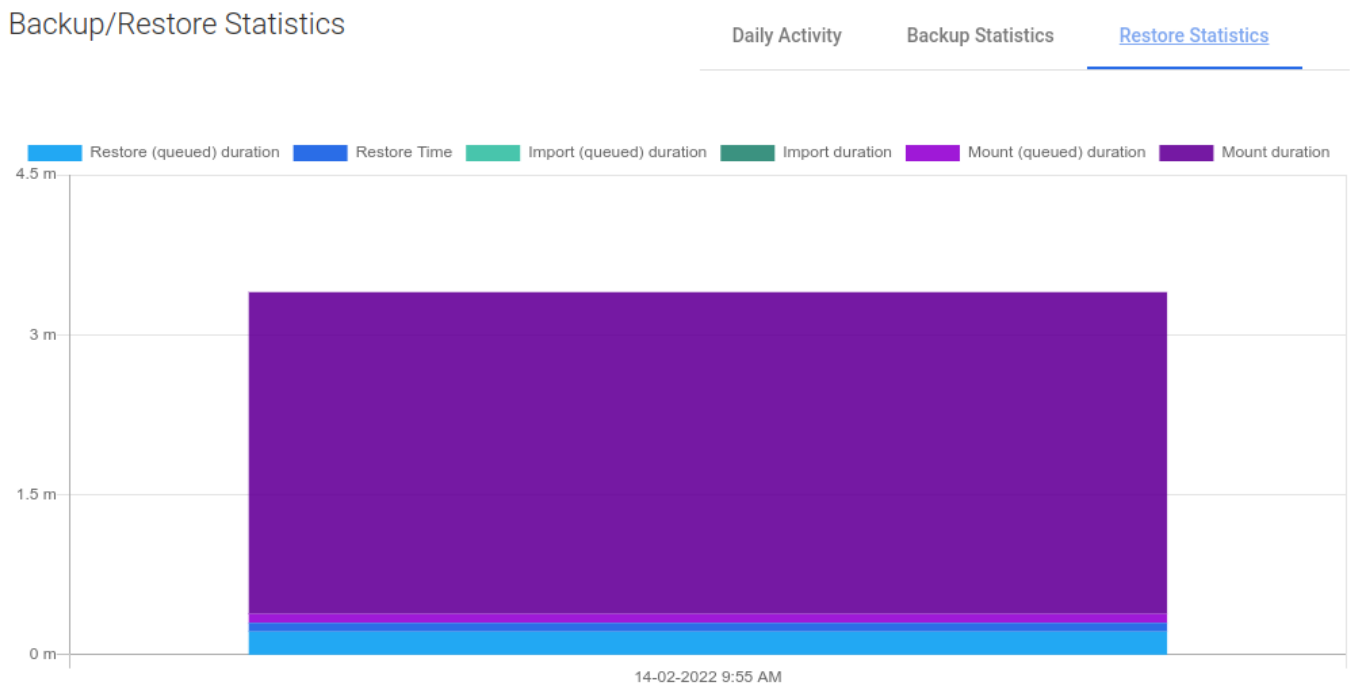
A very useful report. It allows you to determine the required window length for backups or, based on the time of individual phases, it is easy to deduce the cause of slow backups.

Transfer Rate



One of the latest reports, now you can easily see how fast data transfer is.

Restore Time



A view with the same properties as "Backup Time". It allows us to estimate how long it will take to restore the machine in the event of a failure.

Transfer Rate

As in the previous case, we also have the transfer speed for the restore job.

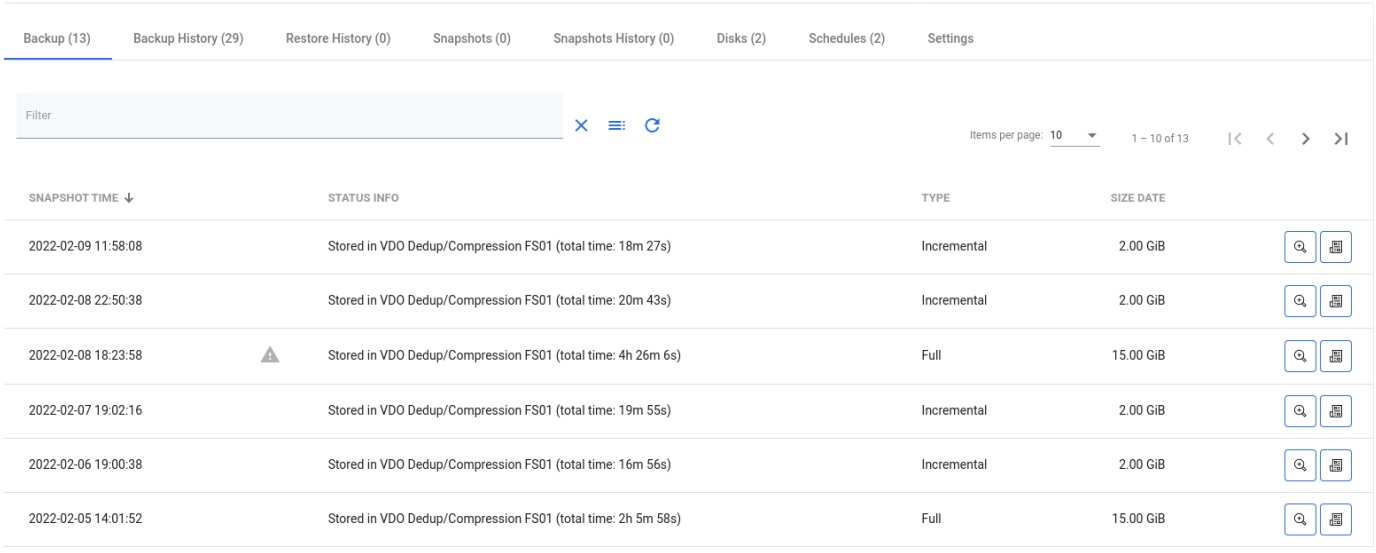
Events Calendar

The calendar extends the possibilities of adjacent statistics. It allows you to neatly define the range of days you want to see, additionally makes a quick summary of the number of backups and restores (top right corner).
Blue - the sum of all backups, **Green** - the sum of successes, **Red** - the sum of failures.

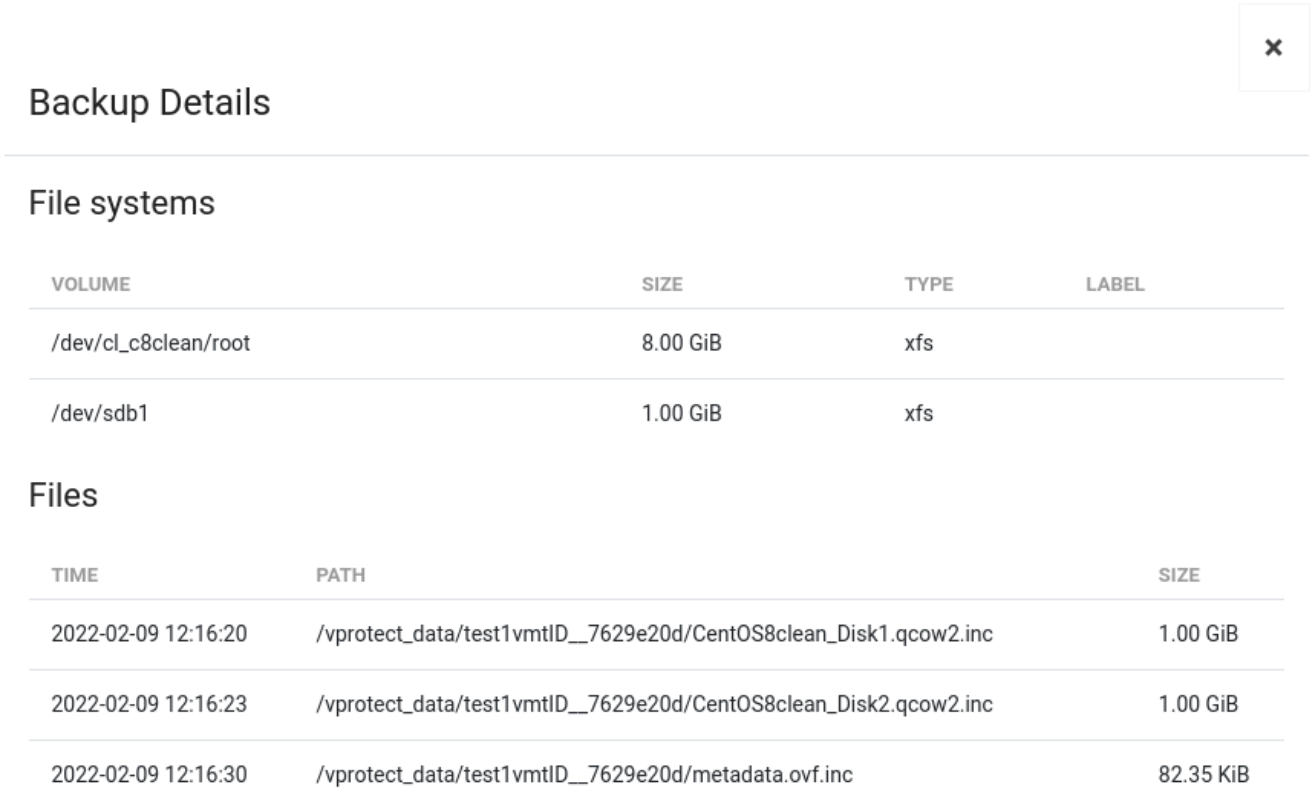
Bottom menu

In the bottom menu, you can find a large number of tabs, each of which will present different information or will allow you to change the configuration of this particular virtual machine.

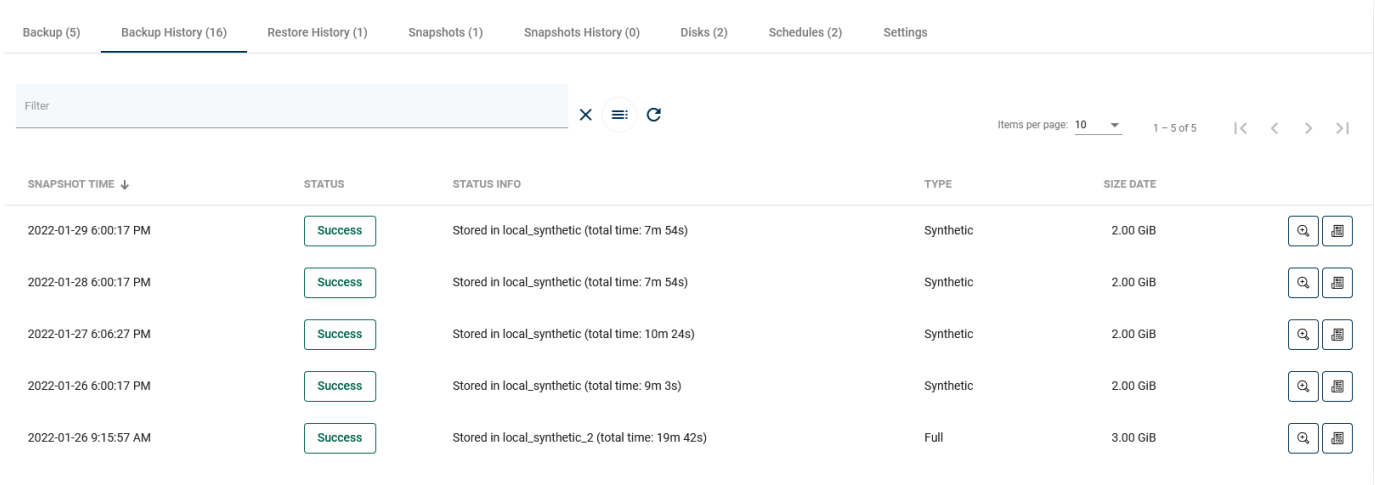
Backup



The first tab shows all virtual machine backups that are currently available and all basic information about them in a list. After clicking on the magnifying glass button, you will see additional information. The button next to it allows you to download logs in the form of a .txt file.

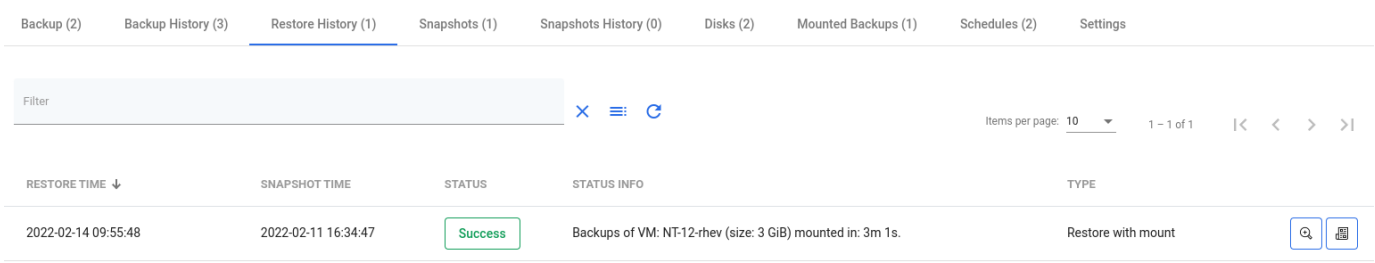


Backup History



This tab shows information about all backups made for this virtual machine, as well as information about failed, removed (because of retention), or currently executing backups.

Restore History



This tab is similar to "Backup History". This is a list with basic information about the virtual machine restores performed. When you open the details of the selected restore, you will see more detailed information.

Restore details

Node	local
Protected Entity	NT-12-rhev
Restore Time	2022-02-14 09:55:48
Status	Success
Status Info	Backups of VM: NT-12-rhev (size: 3 GiB) mounted in: 3m 1s.
Backup Type	Full
Restore Type	Restore and mount

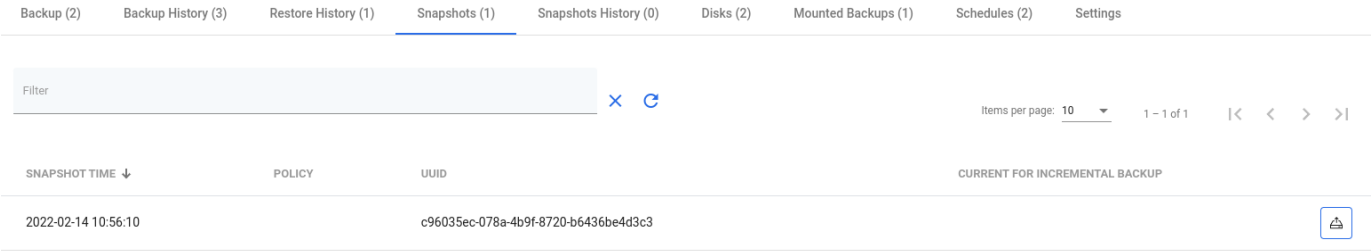
Task Time Stats

Mount duration	03:01 s
Mount (queued) duration	00:05 s

Backup

Backup Time	2022-02-11 18:04:22
Protected Entity	NT-12-rhev
Size	3.00 GiB
Snapshot time	2022-02-11 16:34:47
Status	Success
Status Info	Stored in local fs (total time: 1h 29m 35s)
Type	Full

Snapshots

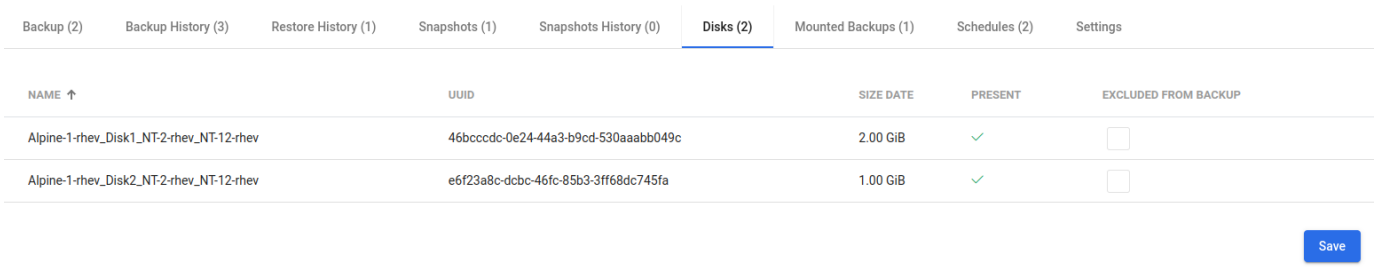


This tab shows virtual machine snapshots (remember - snapshots are stored on the hypervisor). The snapshot can be divided into two categories:

1. As you can see in the list above, there is a green dot next to the snapshot. This means that this snapshot is created for incremental backup purposes. This is an automatic operation and we only keep the last snapshot.
2. The second one on the list is a snapshot created at the user's request (scheduled or manual).

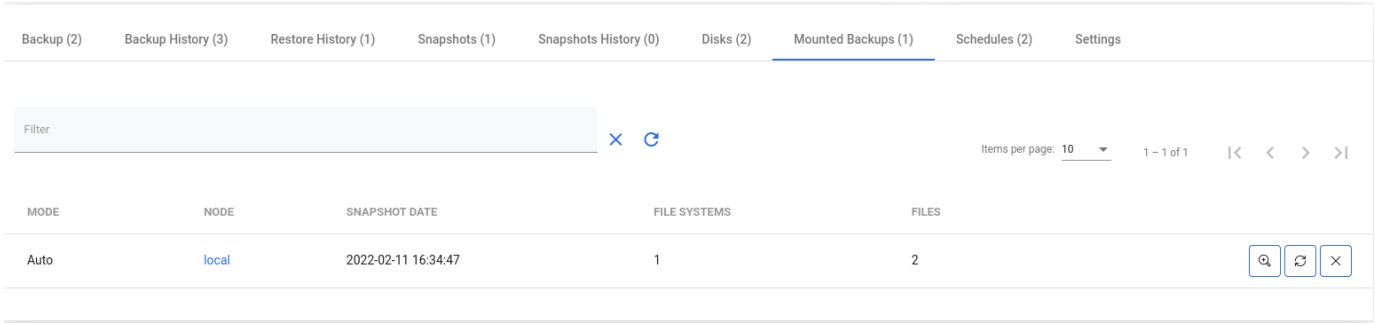
Next to the snapshot is a button that allows you to restore the virtual machine. It actually creates a new virtual machine and keeps the old one (security considerations to protect against the human factor).

Disks



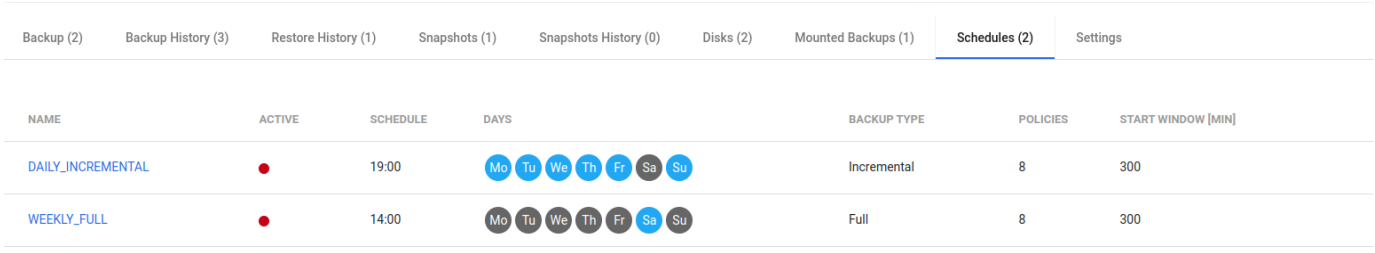
It is worth remembering that if such a virtual machine is restored, the excluded disks will be created from scratch and connected to the machine.

Mounted Backups



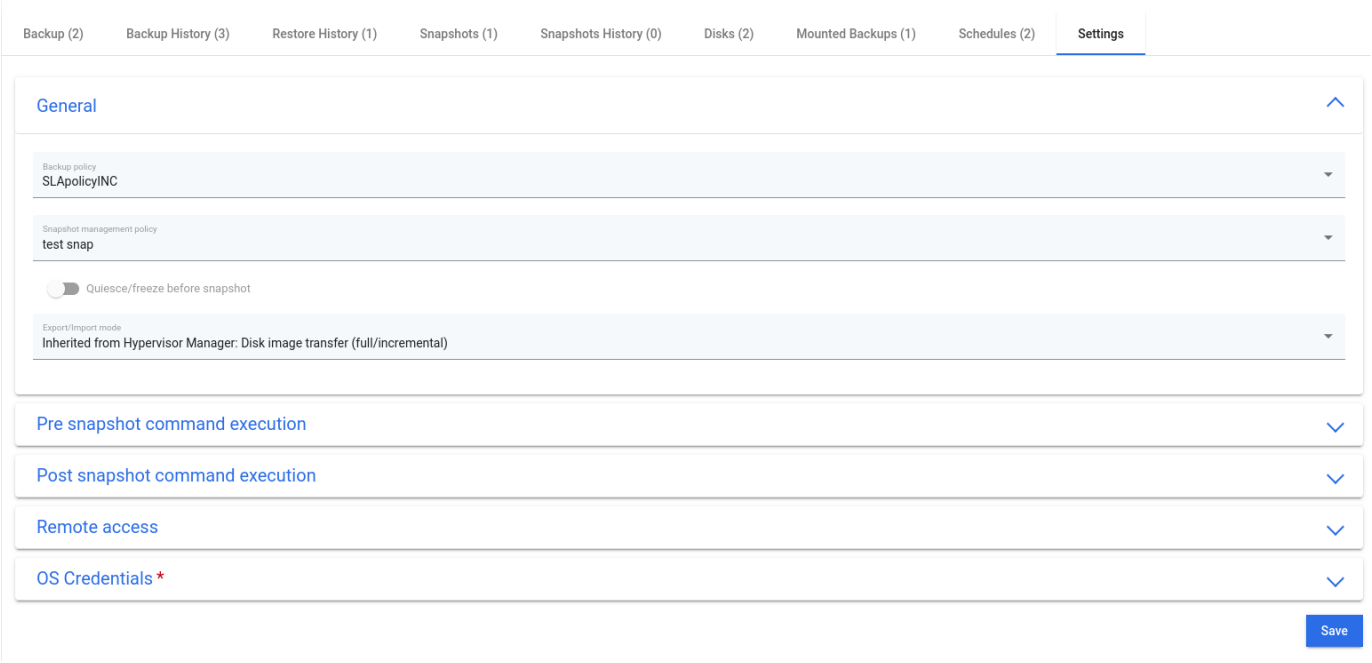
This tab shows a list of mounted backups for this virtual environment.

Schedules



In this tab, you can see all the schedules assigned to the virtual machine.

Settings



Finally, the last tab. The first two options allow you to change the policies assigned to the virtual machine. The third is a toggle to turn on or off the "Snapshot consistent technology" feature. Below You can change the transfer mode which is used for this VM.

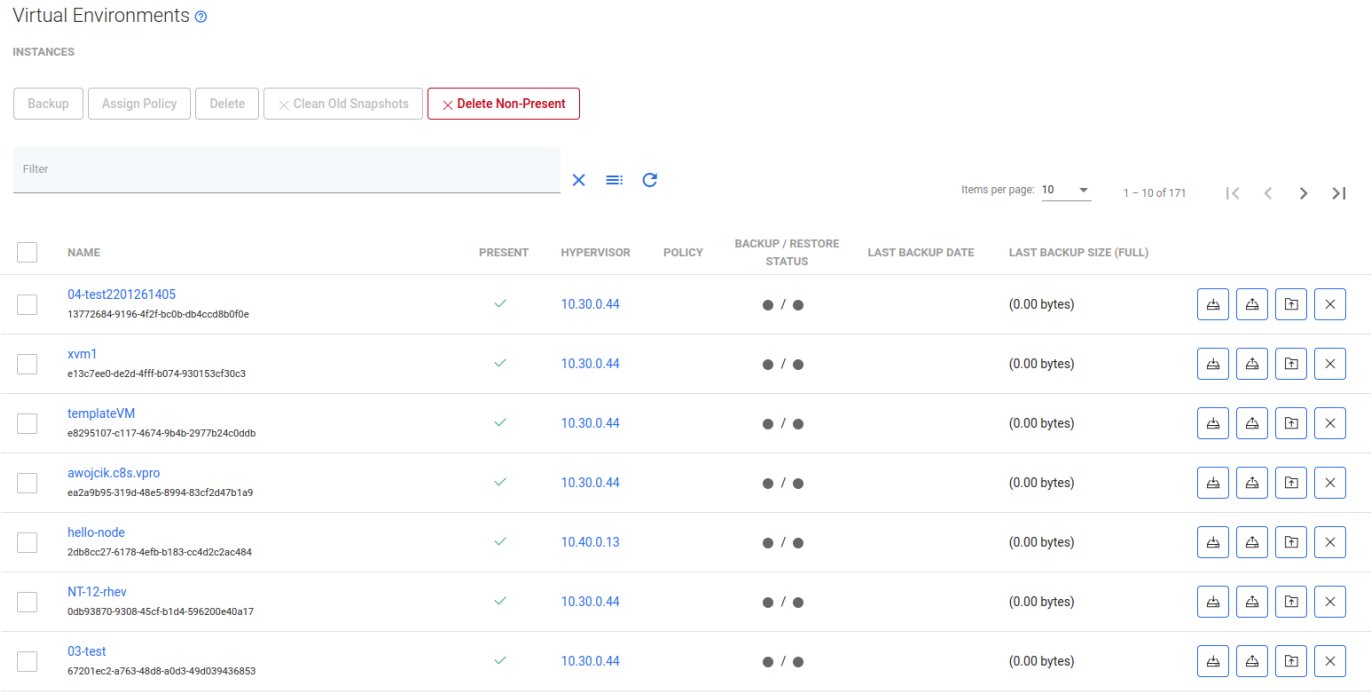
Performing pre/post snapshot commands is a function intended for advanced users. As the name implies, it allows us to execute scripts via an ssh connection, either before or after taking a snapshot.

Backup on-demand

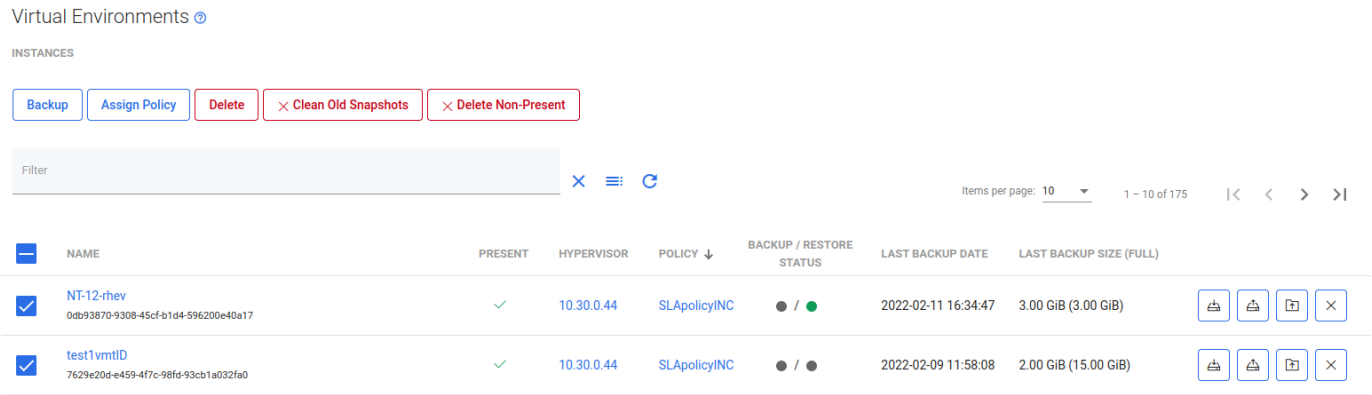
Virtual Environments

To perform on-demand backup go to the Instances tab under the Virtual Environment section.

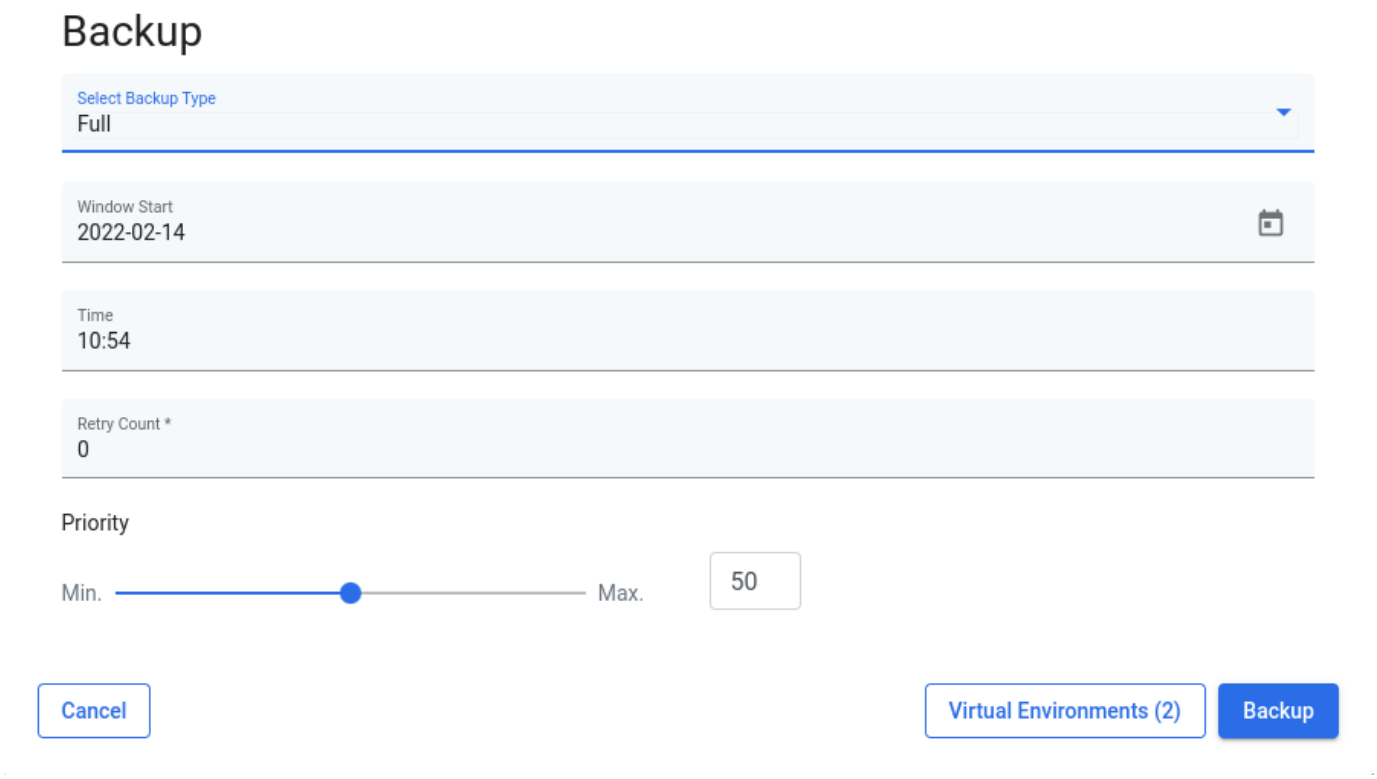
You can click on icon to backup one VM



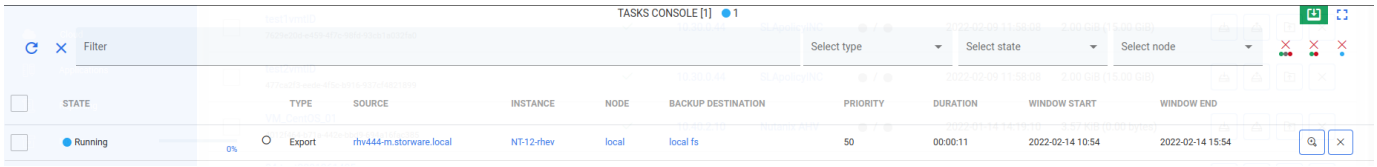
or select multiple virtual machines and click on icon to backup it.



Finally select a backup type, backup destination, when a task should start, priority and click on **Backup** button.



On the Tasks Console, you can see the progress of the backup task.

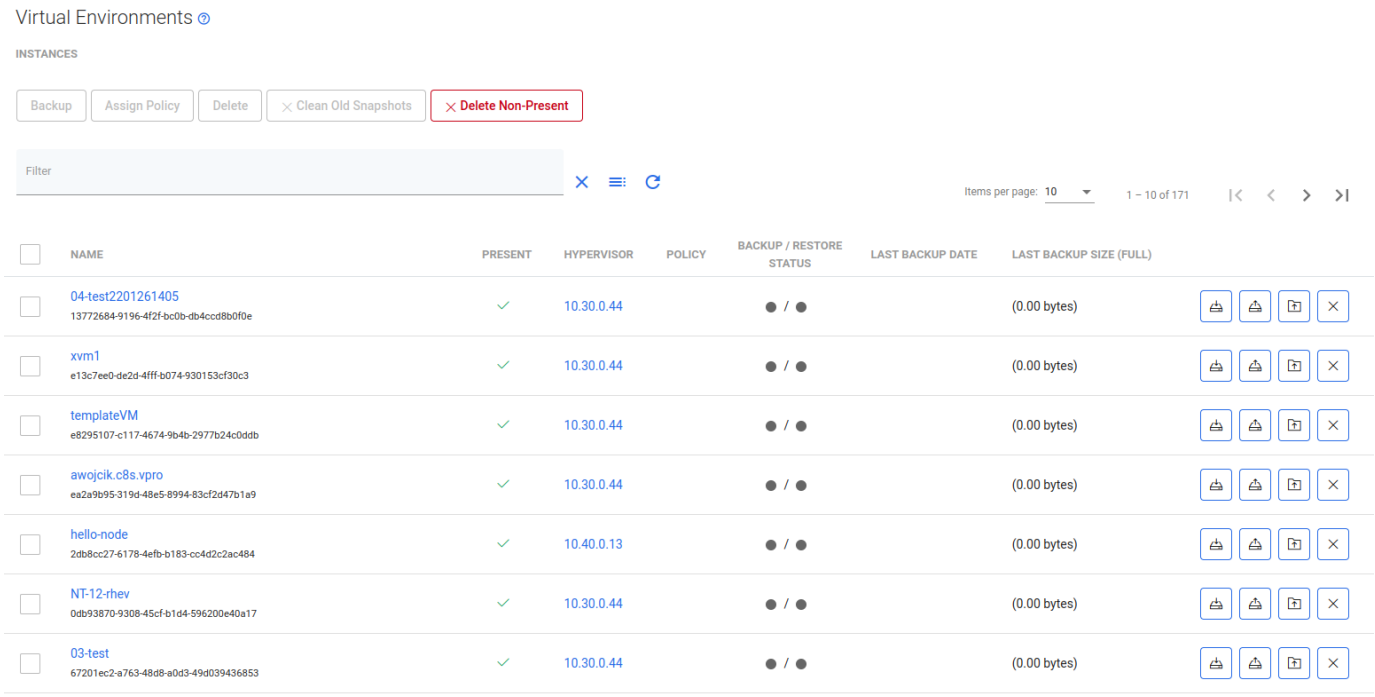


> **Note:** You can also perform the same action thanks to the CLI interface: CLI Reference

Restore on-demand

Restore from virtual environment menu

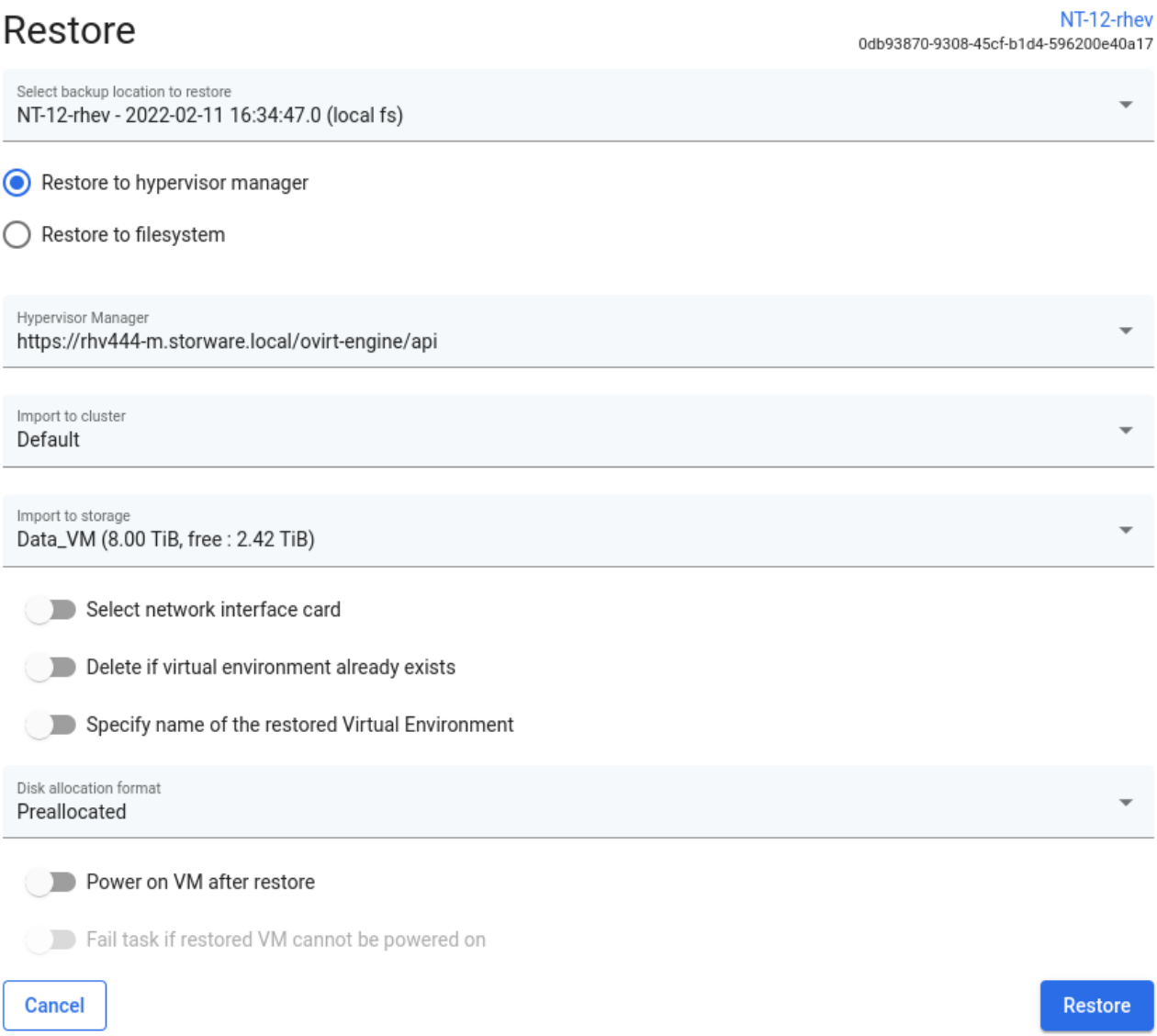
To restore a single virtual machine on-demand, go to the instances tab under Virtual Environment section. Click on the restore icon next to the virtual machine



Now you should see a popup window where you might customize restore settings.

Restoring to the filesystem is an option to restore VMs directly to the Data Protector for Cloud Workloads Node storage. (Remember, the Data Protector for Cloud Workloads user must have the appropriate write permissions to the given path.)

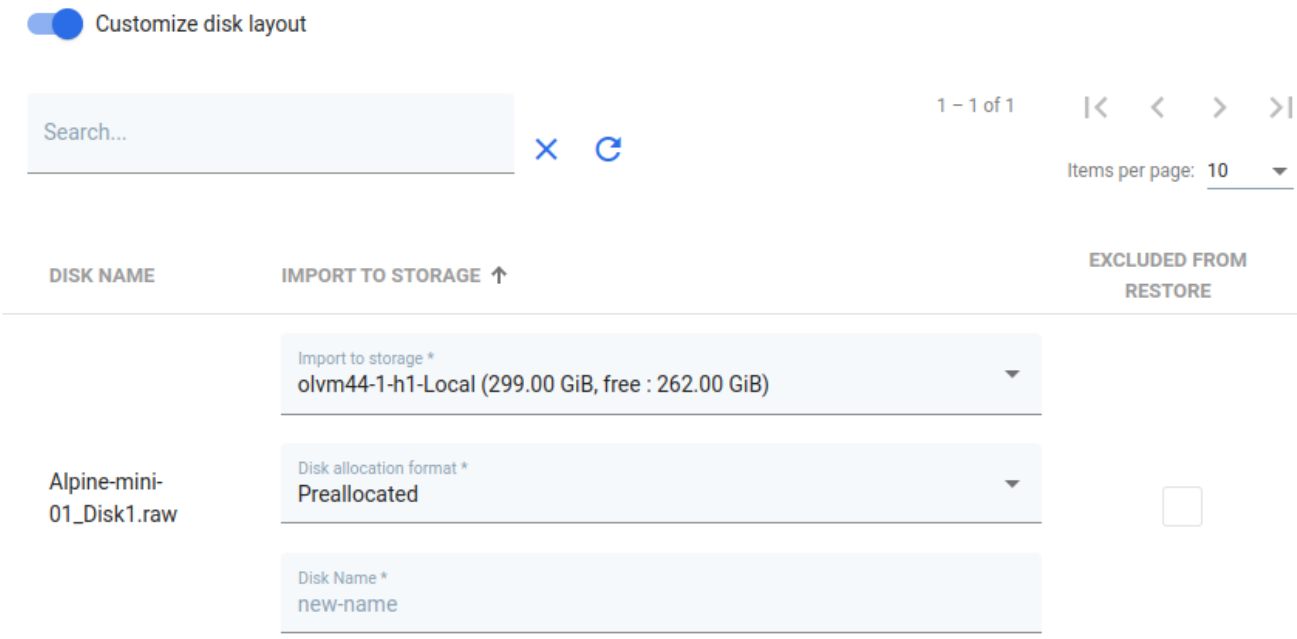
Restoring to a hypervisor or hypervisor manager is allowed for several providers, but not for all (for detailed info go to Data Protector for Cloud Workloads Support Matrix).



When you restore a virtual machine, disks of this machine can be:

- Restored to specified destination. It can be the same or diffrent datastore/volume type for each disk.
- Restored with changed disk name

Supported platforms: RHV, Openstack.



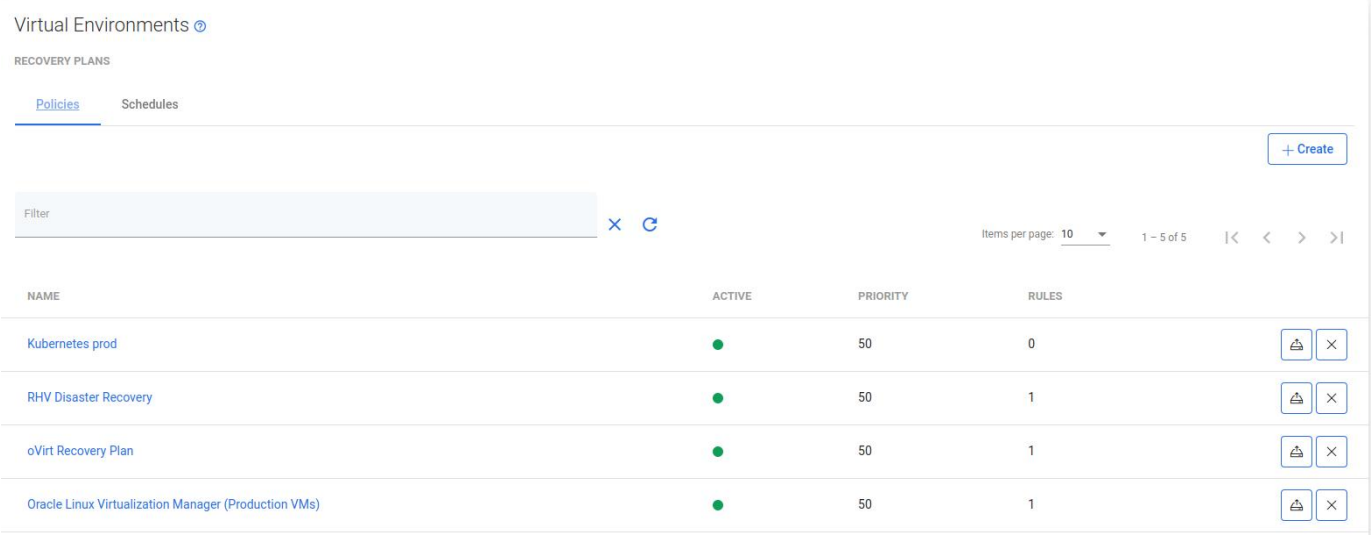
Finally, after customizing the restore, click the restore button.

> **Note:** every platform has some restrictions imposed on the VM name, such as length or characters that can be used. Please verify these limits before restoring with a custom name.

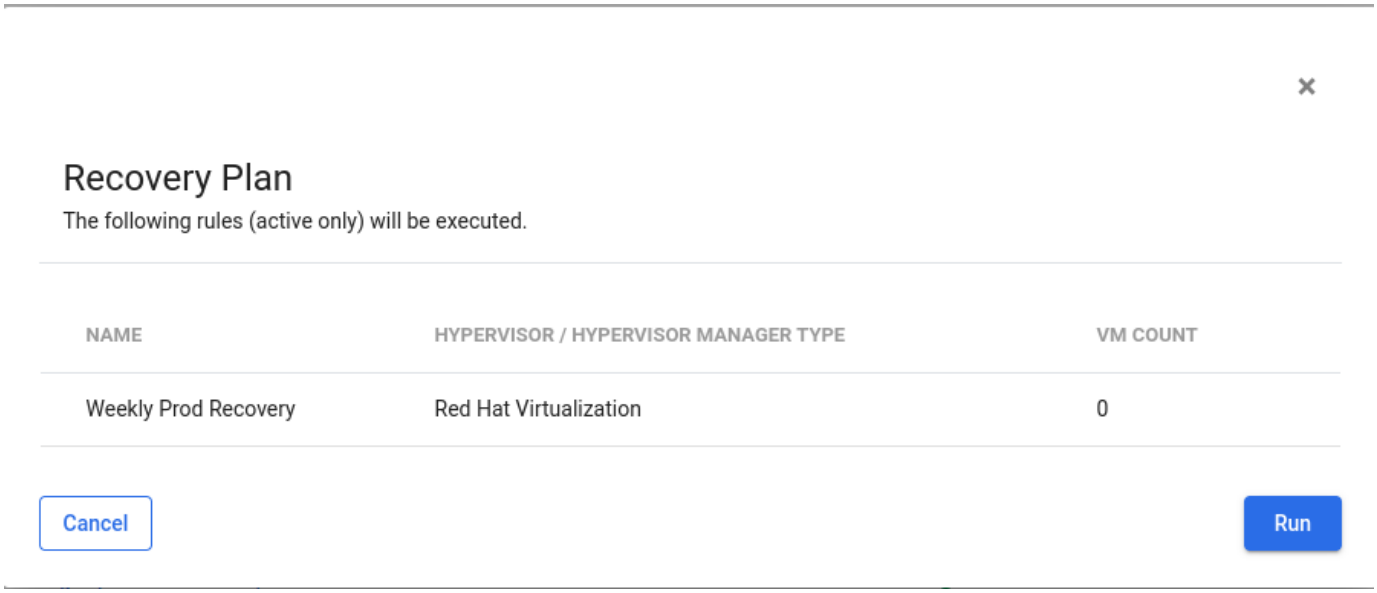
> **Note:** You can also perform the same action thanks to the CLI interface: CLI Reference

Restore on-demand using recovery plans

To restore several virtual machines, you have to use recovery plans. As you can see on the below screenshot, next to the recovery plan policy you can find the same icon that allows you to restore virtual machines



After clicking on it you will see a summary window showing what will be restored.



Click Run to start the restore process.

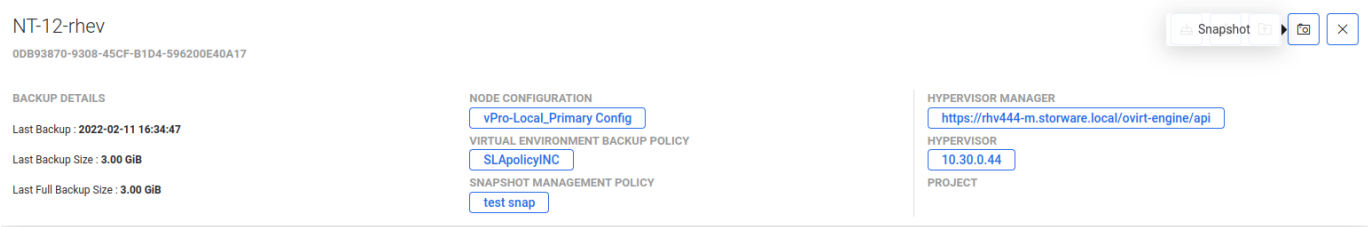
Snapshot Management

Data Protector for Cloud Workloads can periodically create snapshots and keep several of them on every VM. To see which hypervisor support this feature please go to Data Protector for Cloud Workloads Support Matrix.

Snapshots are kept in the virtualization platform and are not exported with the backup. It allows quick recovery of a VM without the need to restore and import data backup to the hypervisor. Snapshots cannot replace backup, but allow to increase RPO when used together with backups. Snapshot chains may impact VM performance and occupy significant additional space depending on the storage setup in the environment, so we recommend keeping low values for the number of kept snapshots in the policy, i.e. less than 3, and check the documentation of your environment and storage setup for aspects related to possible implications of keeping snapshots.

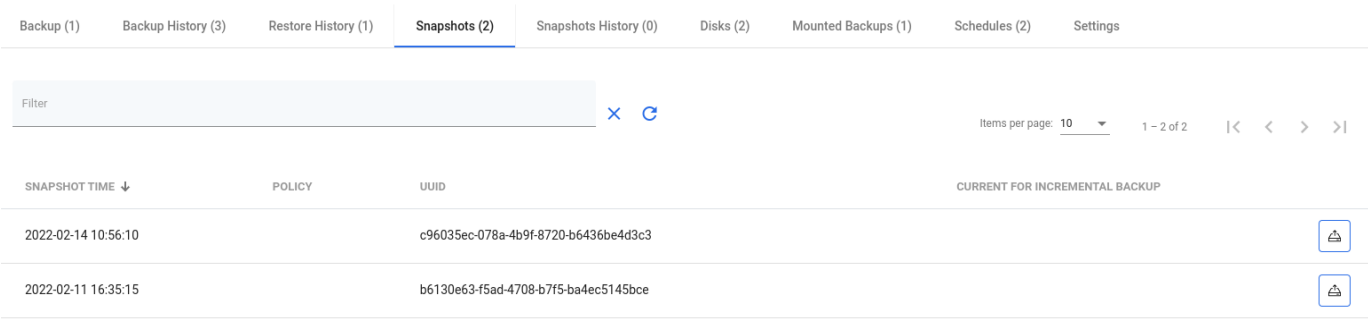
> **Note:**
>
> Snapshot management for on-demand or scheduled operations is not available until the virtual machine has a snapshot management policy assigned to it.
>
> In order to enable snapshot management for VM, you need to follow the steps in this article: Snapshot SLAs

Once VM is assigned, you'll have new buttons that allow on-demand operations. After opening the virtual machine details page, you can see the camera button in the upper right corner.



After pressing the button, the snapshot will be taken immediately, without additional confirmation.

You can also revert the snapshot from the virtual machine details page.

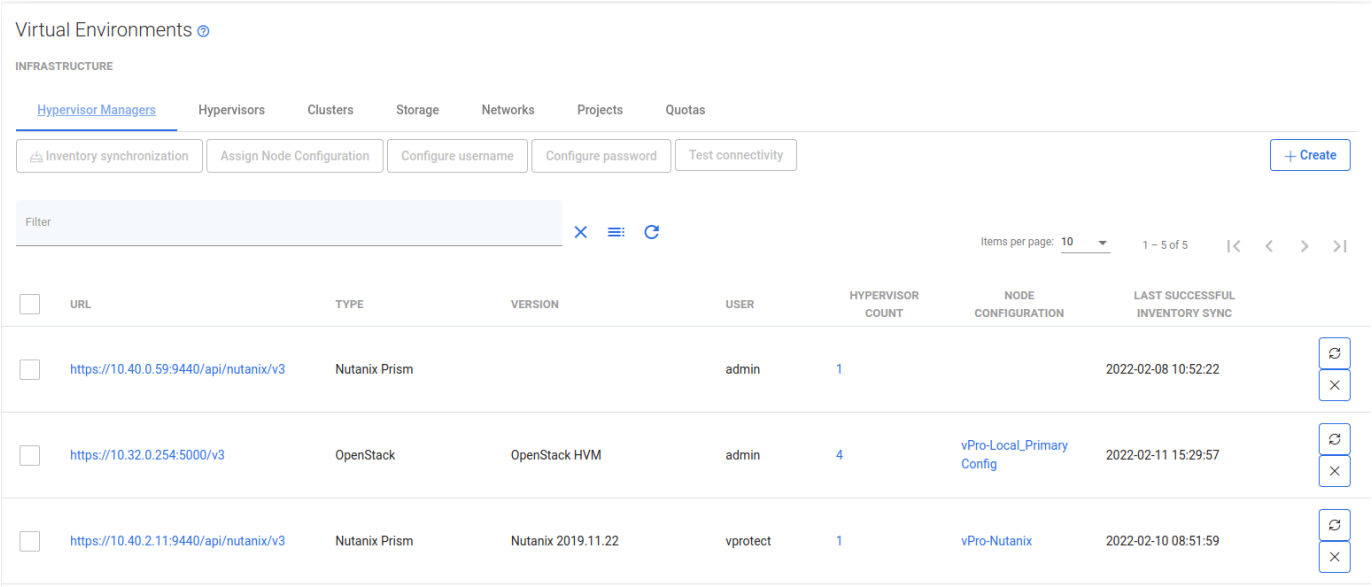


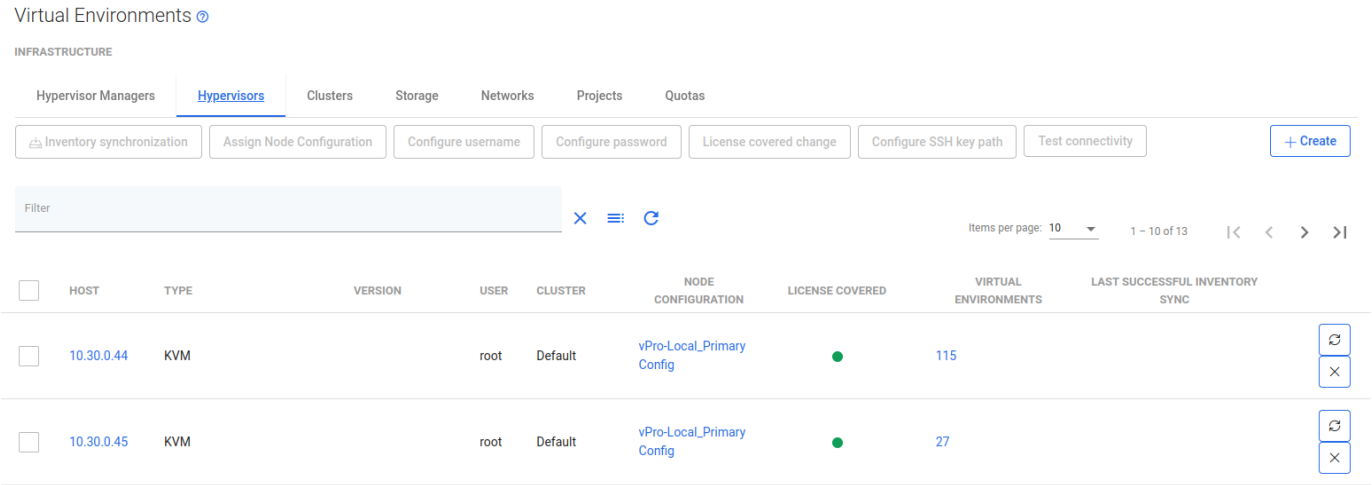
Next to the snapshot is a button that allows you to restore the virtual machine. It actually creates a new virtual machine and keeps the old one (security considerations to protect against the human factor).

> **Note:** You can also perform the same action thanks to the CLI interface: CLI Reference

Infrastructure

This section describes how to manage hypervisors and their managers in Data Protector for Cloud Workloads. Inventory that Data Protector for Cloud Workloads needs first to be populated. The first step is always to add a hypervisor manager (if it virtualization platform supports a dedicated manager) or individual hypervisors (if these are not managed, but are stand-alone).





You also can verify if your Hypervisor Storage (datastores/storage repositories/storage domains, depending on how different platforms call it) or Hypervisor Clusters (which corresponds to server pools/ clusters/availability zones) that have been detected.

Click Add Hypervisor Manager / Add Hypervisor to add entries and in general, you always need to provide:

- URL (hypervisor manager - valid URLs are described in the sections describing the setup of a particular virtual platform type) or hostname/IP (hypervisor)
- the node which is responsible for executing tasks in this environment
- backup strategy - if available for a particular platform

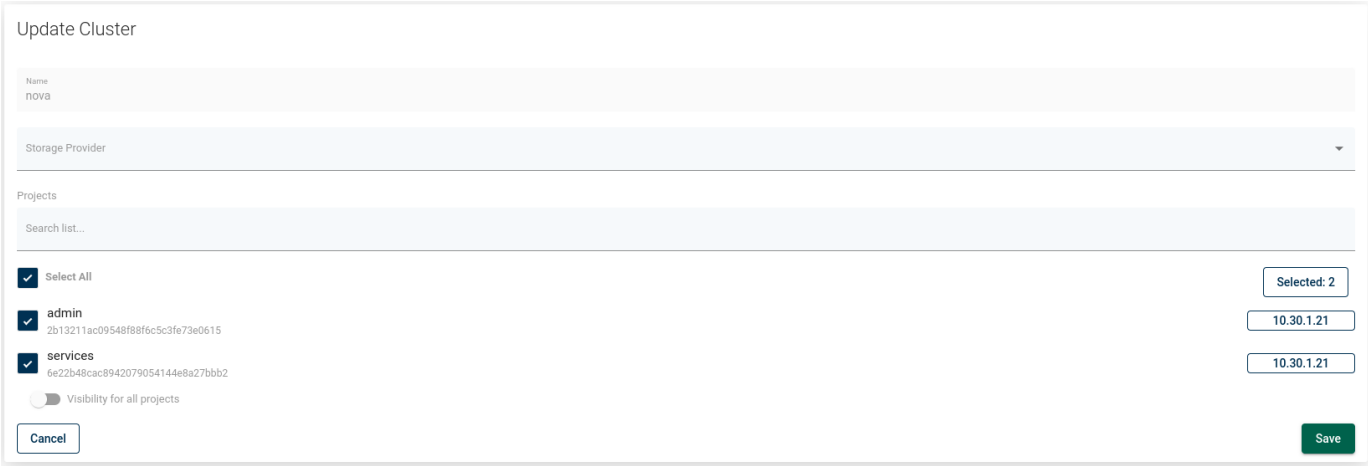
Then synchronize inventory (either automatically - there will be a dialog box shown just after saving the form or manually with the button on the right of hypervisor or manager). If Inventory Synchronization tasks (visible in the console at the bottom) completes successfully it also proves that connection was successful, credentials are correct and all of the inventory items have been collected successfully.

Check Hypervisor Storage, Hypervisor Clusters tabs, as well as Virtual Environments -> Instances to see the results of inventory synchronization.

> **Note:**
>
> - inventory synchronization executed on the manager level assigns the same node as used for the manager to all hypervisors - you can override it in the Hypervisor tab and assign a different node to handle VMs that reside on a specific hypervisor - this is especially important for scalability and when environments are divided into multiple clusters (disk-attachments strategies may not be able to access disks from different clusters)
> - if you use **disk-attachment** strategy - always execute **inventory synchronization at least once from each hypervisor** - the end result will be the same from the inventory point of view, but each node needs to detect its own Proxy VM ID in the environment to attach disks to the correct VM

Hypervisor clusters and storages

When using Openstack, for each hypervisor cluster and hypervisor storage you can select projects for which it is going to be available in horizon plugin restore dialog.



Selecting "Visible for all projects" will make a cluster/storage visible for all projects, regardless of their time of creation (including ones added after editing this setting).

Deselecting "Visible for all projects" option and selecting some (or all) of existing projects will result in cluster/storage being visible just for selected, already existing projects. The cluster/storage will not be automatically visible for any newly added projects.

This setting will also affect filtering clusters and storages by project selected in restore modal dialog or while editing restore setting for recovery plan rule.

Quotas

Quotas manage the number of VM backups and restores in projects. Quotas uses user-defined rules to control the number of backups. Each Rule has two thresholds: **SOFT** and **HARD**. **SOFT** limits only warn you when a certain limit is exceeded. **HARD** limits prevent the execution of tasks that have exceeded the specified limits. When any of the rules are exceeded, the task fails or warnings are placed on the VM and on backup or restore. For each limit type you need to specify time frame in which rule will be applied. Quotas can be activated or deactivated at any moment, additionally each rule can be activated or deactivated.

To create new Quota, please open **Infrastructure** tab under **Virtual Environments** section and go to **Quotas** then click on **Create** button on the right.

Backup SLAs

Backup SLAs allow you to group backup policies and schedules for multiple VMs. In general, a VM can have at most only one backup policy to always have easy-to-interpret configuration.

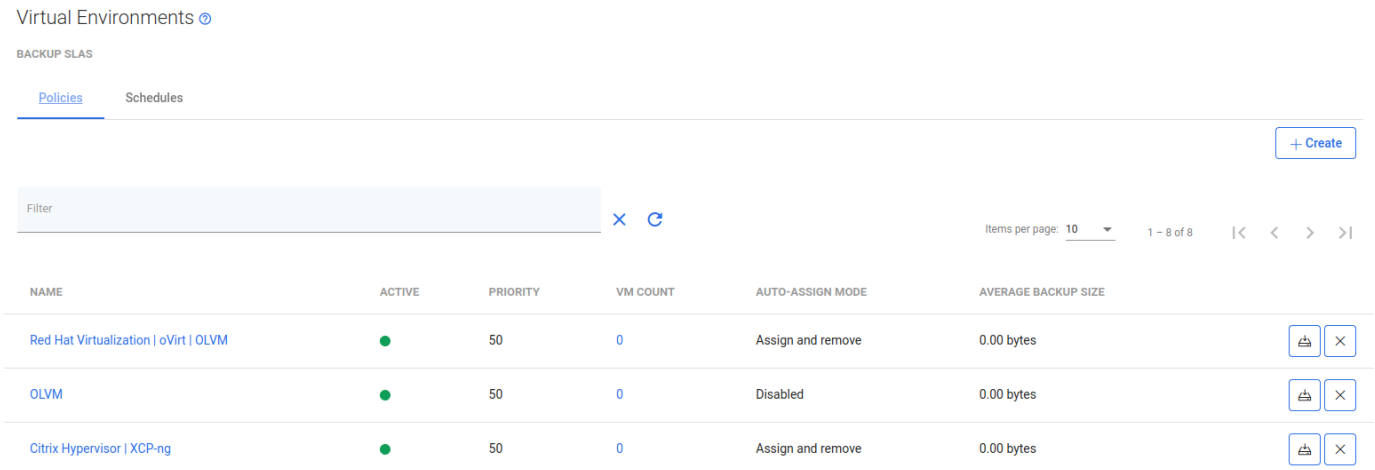
Each policy can have multiple schedules assigned so that you can define more complex schedules in which backups are executed even multiple times each day and with a different backup type.

> **Note:**
>
> - schedules define the type of backup - full or incremental
> - the approach we highly recommend is to create a schedule for **periodic full** backup and always assign at least 1 such schedule in backup SLAs
> - in order to create incremental backups, you always need to have **at least 1 incremental backup schedule** and run at least one full backup
> - in most virtualization platforms supported by Data Protector for Cloud Workloads, it is required to **keep the last snapshot** for future incremental backups

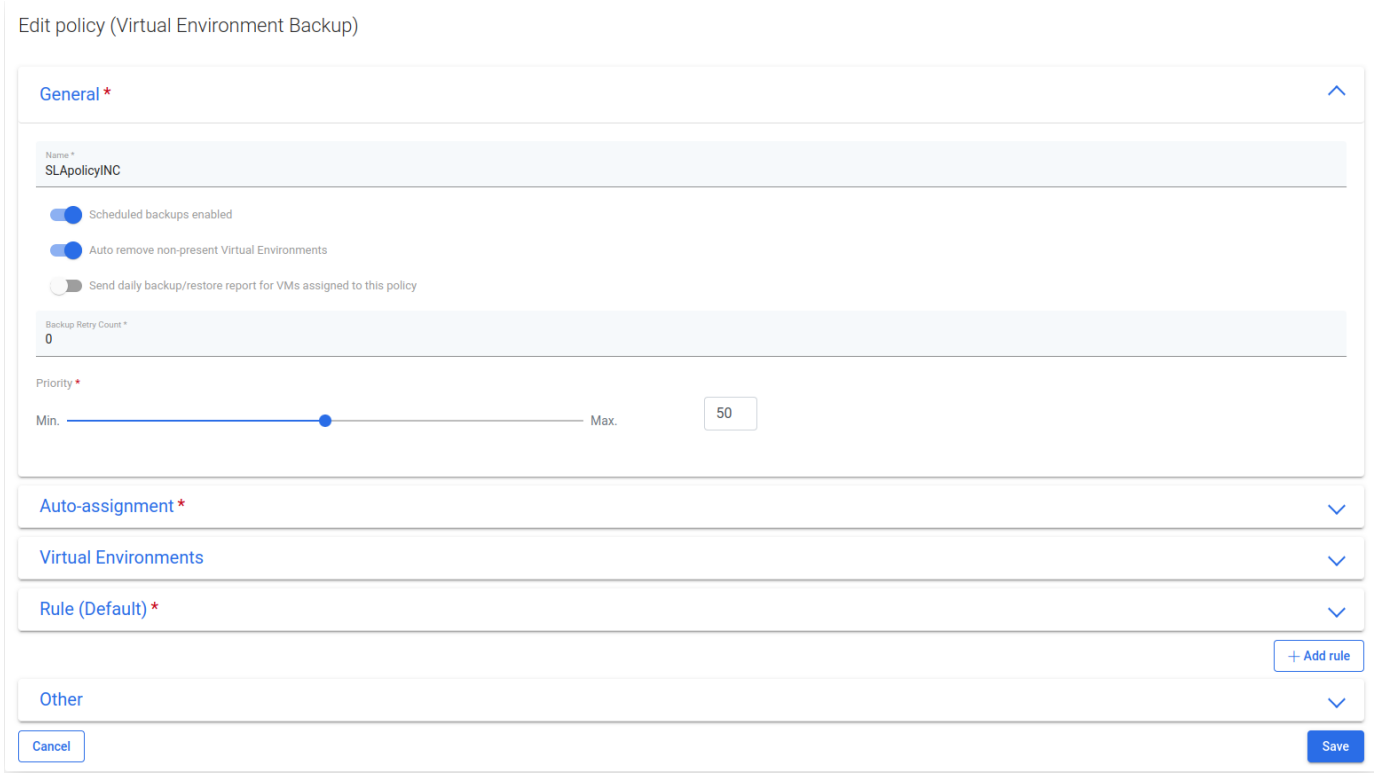
Policies

Policies allows you to group virtual machines in many ways. For example, based on the type of hypervisor.

To create a new backup policy, please open the Backup SLAs tab under the Virtual Environments section and click on **Create** the button on the right.



Now you should see the policy wizard with 5 main sections.



General

Under this section you can set up:

- The policy name
- Switch on/off auto-remove non-present virtual environments
- Set the priority for tasks
- Backup retry count

Auto-assignment

In this section you can configure automatic policy assignment based on certain criteria:

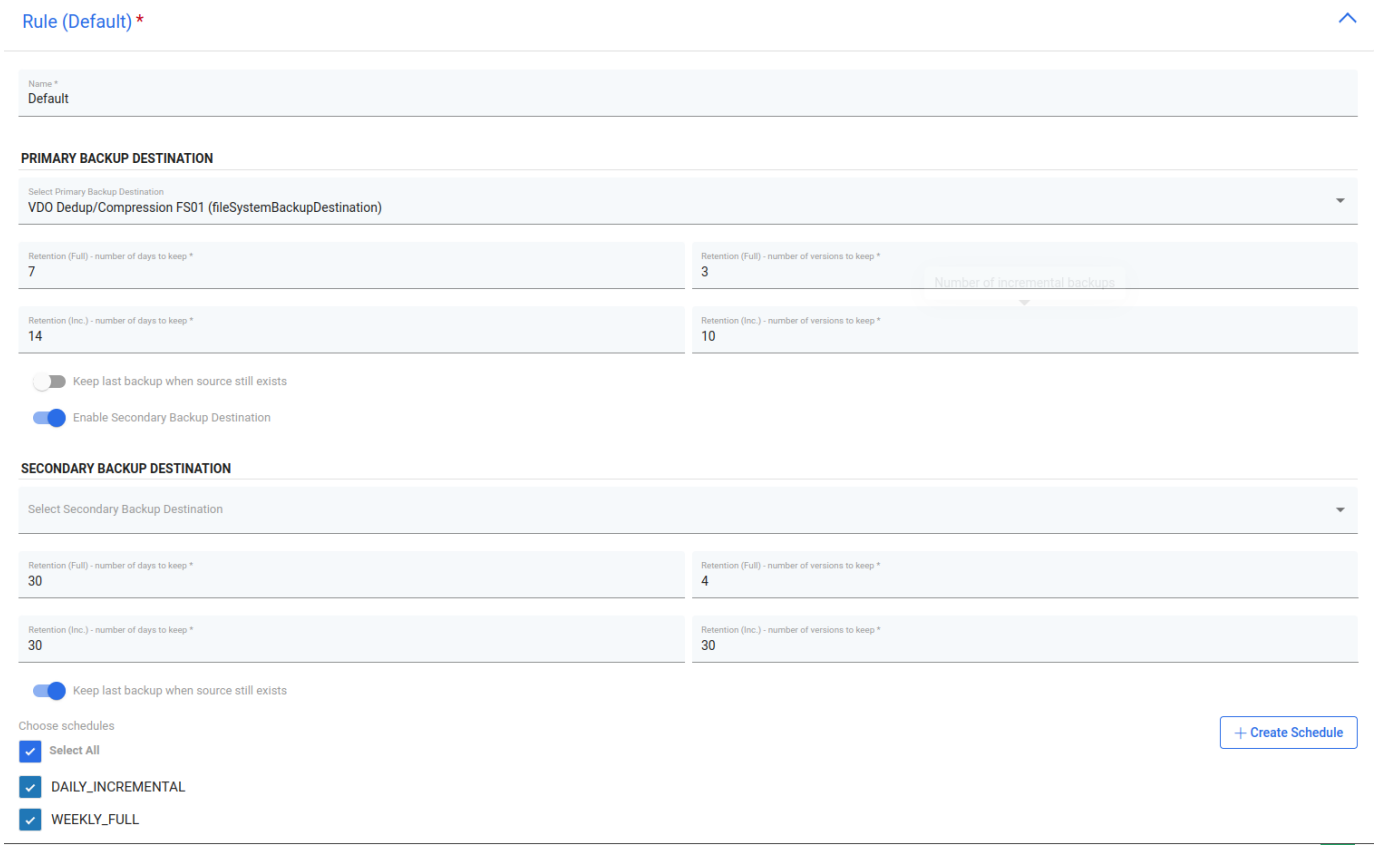
- Mode
  - Disabled
  - Assign only
  - Assign and remove
- Include or exclude rules based on hypervisor tags or regular expressions matching the VM name, such as:
  - regular expression examples:
    - `.*` match any character any number of times
    - `vm-[0-9][0-9][0-9]` - match the name that starts with `vm-` and 3 digits
    - `(prod|uat|dev)-[0-9][0-9][0-9][a-z]?` - match the name that starts with `prod` or `uat` or `dev` prefix, then `-`, then 3 digits and an optional lower-case letter (matching is case-sensitive)
  - exclude rules always take precedence over include rules
  - VMs will not be reassigned to a different policy if they already have a matching policy assigned
  - VMs will be reassigned to a different policy only if the mode is `Assign and remove`, the current policy assignment rules don't match, and other's policy rules match
  - rules are joined with the OR operator, so
    - if **any** rule (tag or matched regular expression) excludes the VM - it will be excluded
    - if **no** rule (tag or matched regular expression) excludes the VM, and **any** rule (tag or matched regular expression) includes the VM - it will be included
- You can also select clusters to match only VMs that belong to them.

Virtual Environments

Here you can easily select virtual machines manually.

Rule

This section is used to select the backup destination.



> **Note:** You can select Primary and Secondary Backup Destintanion in one Rule

You can also set here **Retention** settings for your backups. You can use a number of days and versions for full and incremental backups.

If you have already created a schedule, you can also select it or Create New Schedule.

Retention

Data Protector for Cloud Workloads handles retention for all backup destinations. There are 4 properties that define how long backup should be kept in the backup destination:

- `Retention (Full) - no. of versions to keep` - number of full backups
- `Retention (Inc.) - no. of versions to keep` - number of incremental backups
- `Retention (Full) - no. of days to keep` - number of days to keep a full backup
- `Retention (Inc.) - no. of days to keep` - number of days to keep an incremental backup

> If you are using Synthetic File System backup destination, you have only two options for retention:
>
> - `Retention - no. of versions to keep` - number of full backups
> - `Retention - no. of days to keep` - number of days to keep a full backup

Whichever condition is met first (either number of versions has been reached or the backup is older than the given limit), it is removed from the backup destination.

Other

This is an optional section with two switches:

- Fail the rest of the backup tasks if more than xx% of the EXPORT tasks have already failed
- Fail the rest of the backup tasks if more than xx% of the STORE tasks have already failed

These are two examples of when using switches is useful. It is very likely that if 30% of the backup tasks fail, the remaining tasks will also fail because the environment has failed. Or, if you are backing up a set of machines, and even if only one is not secured, there is no point in backing up the rest.

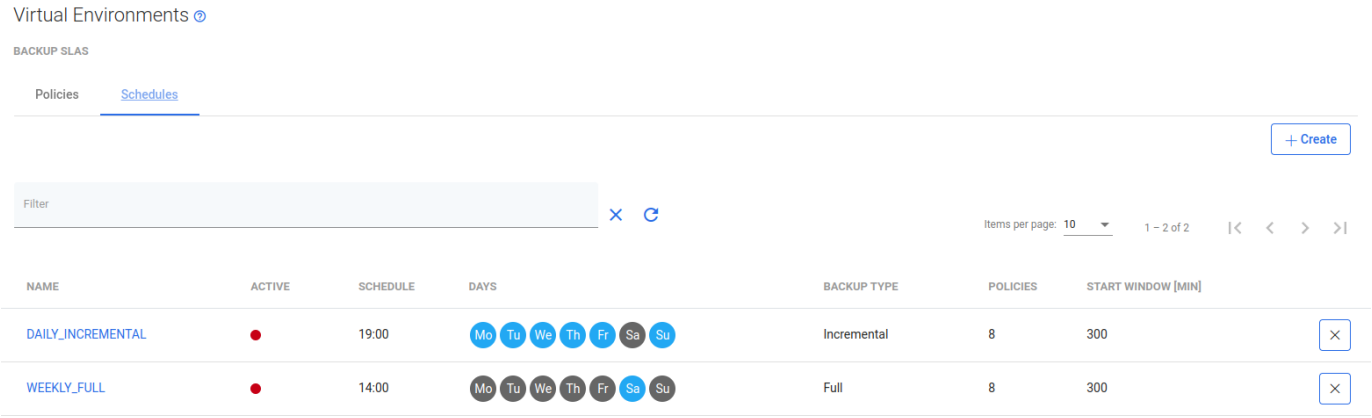
At the end, save the settings.

> **Note:** You can also perform the same action thanks to the CLI interface: CLI Reference

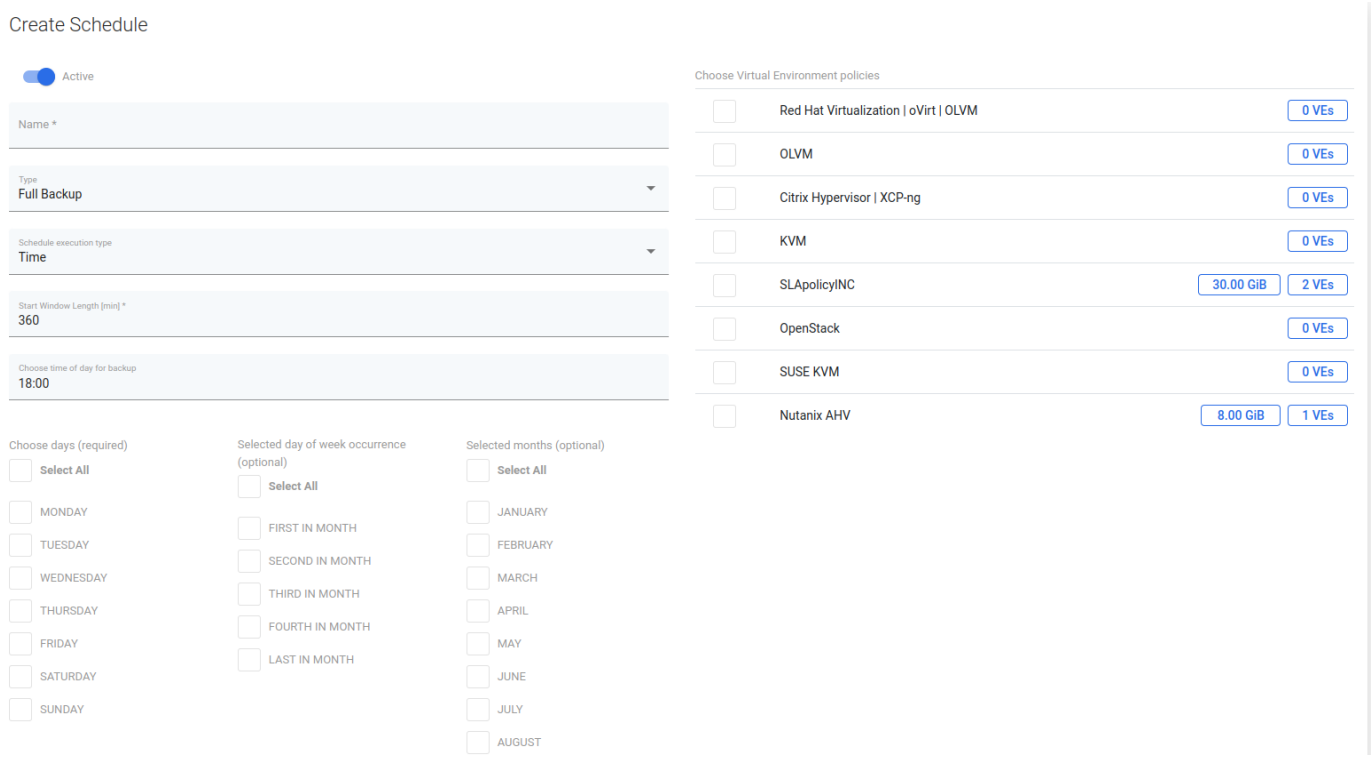
Schedules

Schedules allow you to invoke specific policies periodically. This allows you to back up multiple VMs automatically.

A schedule defines when and on which days VMs should be backed up. To define a new schedule, open Backup SLAs under the Virtual Environments section and go to the Schedules tab, then use the + Create button.



Now enter the properties:



- `Schedule Active` - enable or disable executing schedule
- `Name` - schedule name
- `Backup Type` - defines the backup type: full or incremental
- `Execution Type` - choose the time or interval mode
- `Start Window` - defines for how long since the task start time scheduled tasks are allowed to be executed
- `Choose time of day` - for the time execution mode, this defines when the task should be added to the queue
- `Choose time of interval start` - for the interval execution mode, this defines when tasks should start
- `Choose time of interval end` - for the interval execution mode, this defines when tasks should end
- `Frequency` - defines how often the task will be executed during the interval

- `Choose days` - the last required parameter, select the days of the week on which the task will be performed

You can also use optional parameters to further personalize the backup time or select a virtual environment policy if it has been previously created.

> **Note:** You can also perform the same action thanks to the CLI interface: CLI Reference

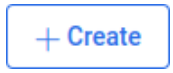
Snapshot SLAs

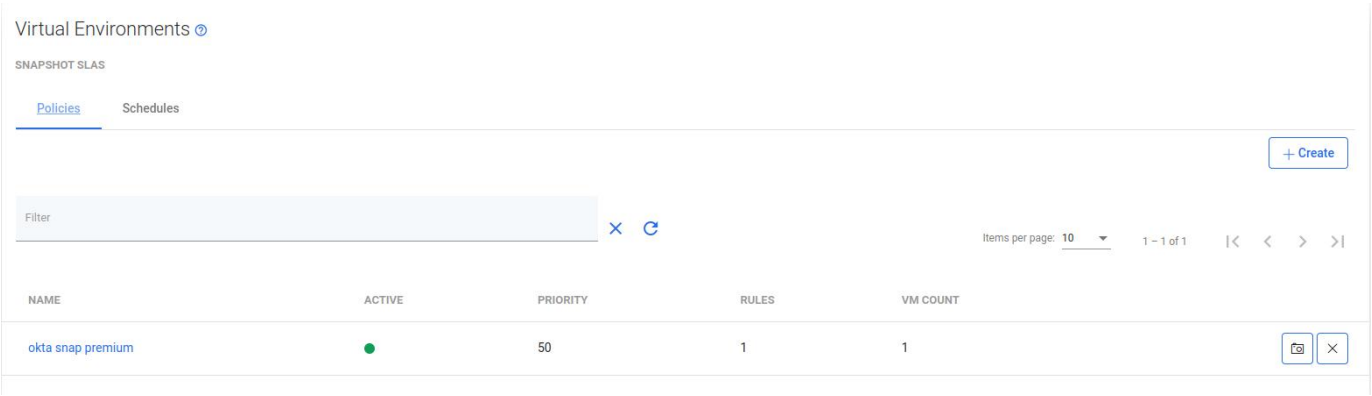
Data Protector for Cloud Workloads can periodically create snapshots and keep several of them for every VM. To see which hypervisor support this feature please go to Data Protector for Cloud Workloads Support Matrix.

> **Note:** Snapshot management for on-demand or scheduled operations is not available until the virtual machine has a snapshot management policy assigned to it.

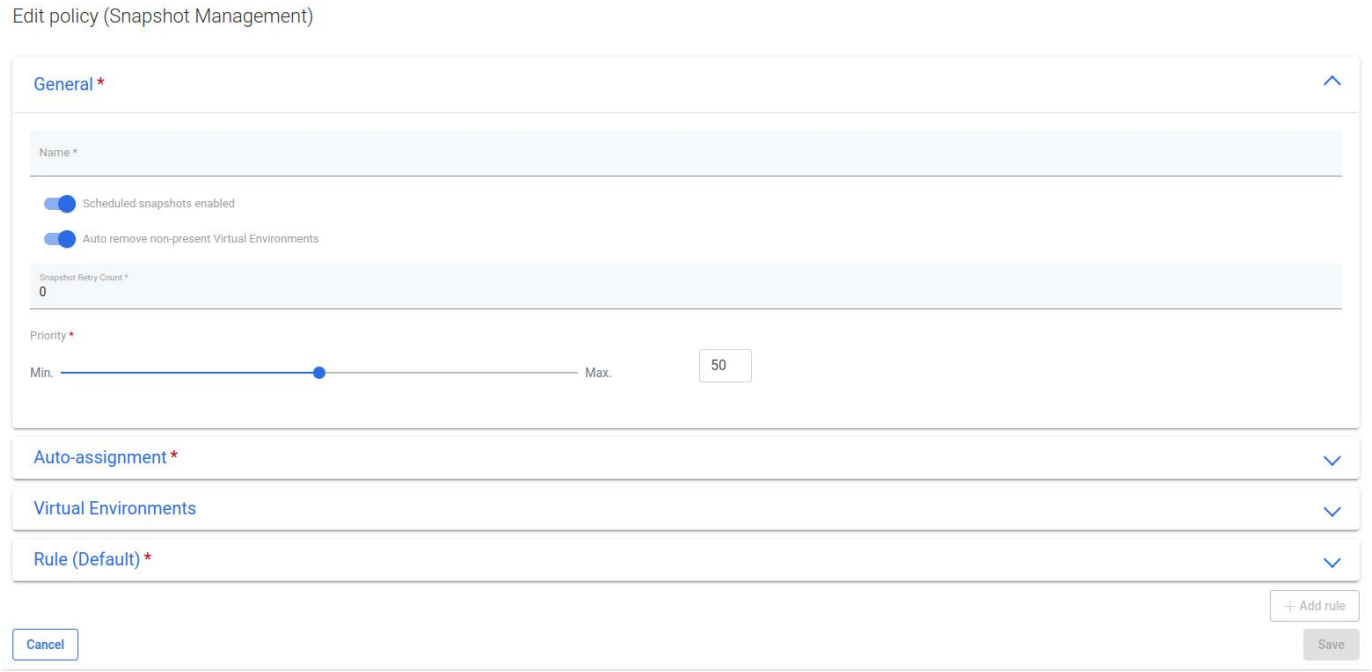
Policies

In order to enable snapshot management for VM you need to do the following steps:

Go to Snapshot SLAs under Virtual Environment section and create a new Snapshot Management policy 



As well as other types of Policies, you'll also find 4 main sections here.



General

Under this section you can set up:

- Name of policy
- Switch on/off auto remove non-present virtual environments
- Set priority for tasks

Auto-assignment

In this section you can set up:

- Mode
    - Disabled
    - Assign only

    - Assign and remove
- Include or exclude rules based on hypervisor tag's or regular expression matching VM name, i.e.:
    - regular expression examples:
        - `.*` match any character any number of times
        - `vm-[0-9][0-9][0-9]` - match name that starts with `vm-` and 3 digits
        - `(prod|uat|dev)-[0-9][0-9][0-9][a-z]?` - match name that starts with `prod` or `uat` or `dev` prefix, then `-`, then 3 digits and optional lower-case letter (matching is case-sensitive)
    - exclude rules always take precedence over include rules
    - VMs may will not be reassigned to the different policy if they already have matching policy assigned
    - VMs may will be reassigned to the different policy only if mode is `Assign and remove`, current policy assignment rules don't match, and other's policy rules match
    - rules are joined with OR operatorator, so
        - if **any** rule (tag or matched regular expression) excludes VM - it will be excluded
        - if **no** rule (tag or matched regular expression) excludes VM, and **any** rule (tag or matched regular expression) includes VM - it will be included
- You can also select clusters to match only VMs that belong to them

Virtual Environments

In this place, you can select virtual machines manually in a simple way.

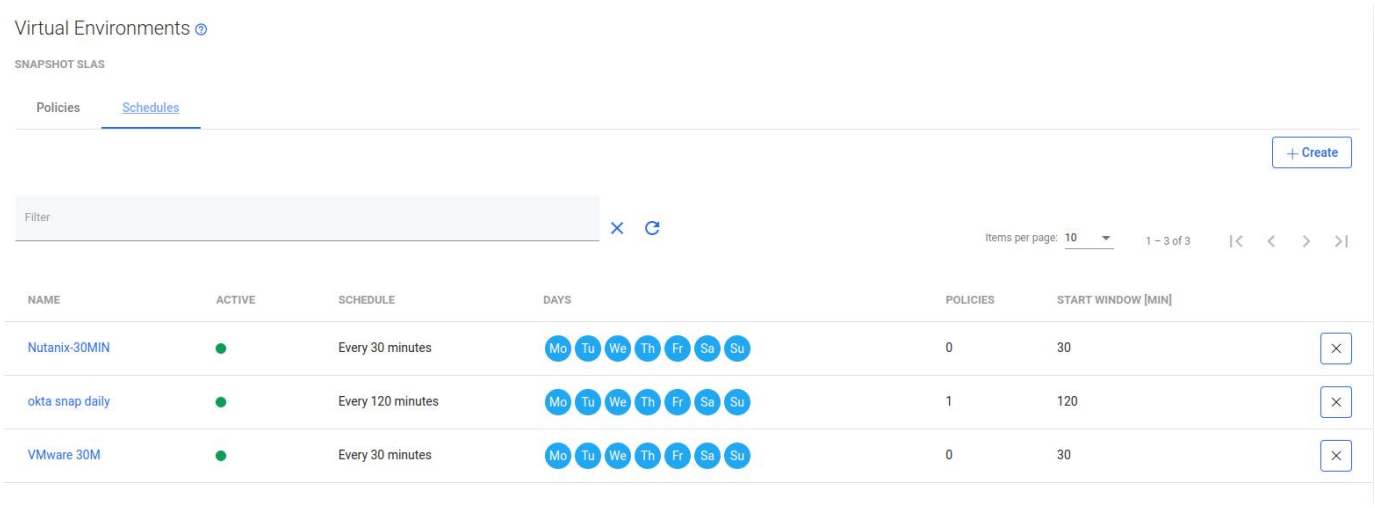
Rule

Provide retention settings - how many snapshots (created by this policy) will be kept and for how long. If you have already created a schedule, you can also select it.

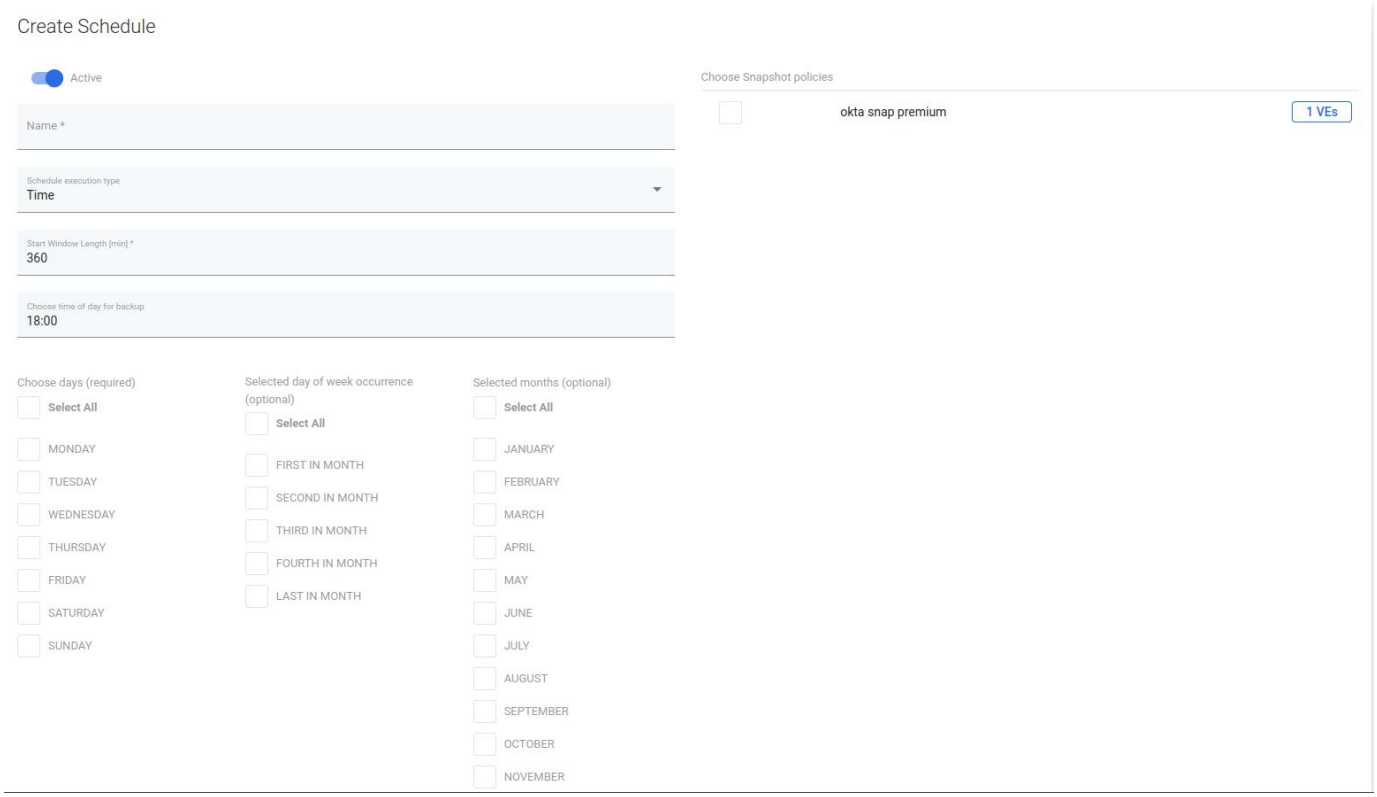
> **Note:** You can also perform the same action thanks to the CLI interface: CLI Reference

Schedules

Schedule defines when and on which days snapshots should be created. To define new schedule use the + Create button.



Now provide properties:



- `Schedule Active` - enable or disable executing schedule
- `Name` - schedule name
- `Execution Type` - choose time or interval mode
- `Start Window` - defines for how long since task start time scheduled tasks are allowed to be executed
- `Choose time of day` - for time execution mode defines when the task should be added to queue
- `Choose time of interval start` - for interval execution mode defines when tasks should start
- `Choose time of interval end` - for interval execution mode defines when tasks should end
- `Frequency` - defines how often task will be executed during the interval
- `Choose days` - last required parameter, select days of the week on which the task will be performed

You can also use optional parameters to further personalize the backup time or select a virtual environment policy if it has been previously created.

Recovery Plans

Recovery plans are used to automate DR process so that Data Protector for Cloud Workloads executes multiple restore operations to the target environment with preconfigured settings.

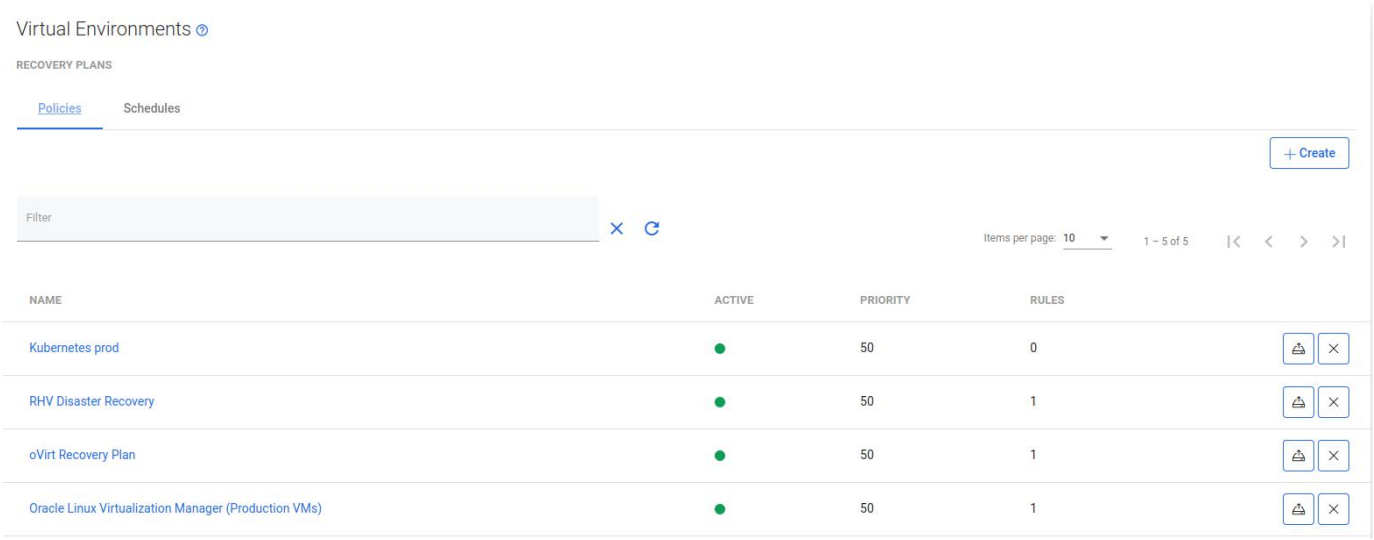
Recovery plans can be executed on-demand or on a scheduled basis (for instance to test the recovery process periodically). Recovery plans consist of rules, each one for a particular virtualization platform, which specify VMs, restore settings, and optionally schedules. Only rules marked as active are executed.

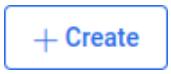
Restore operations will be performed according to the restore/import task limits set in Node Configuration. In target environment new VMs will be created. Names are generated by default (with optional prefix/suffix), optionally original name can be used. For periodic restores, it is common to replace previous VM, which typically means that options to use original VM name and deletion of virtual environment with the same name are checked.

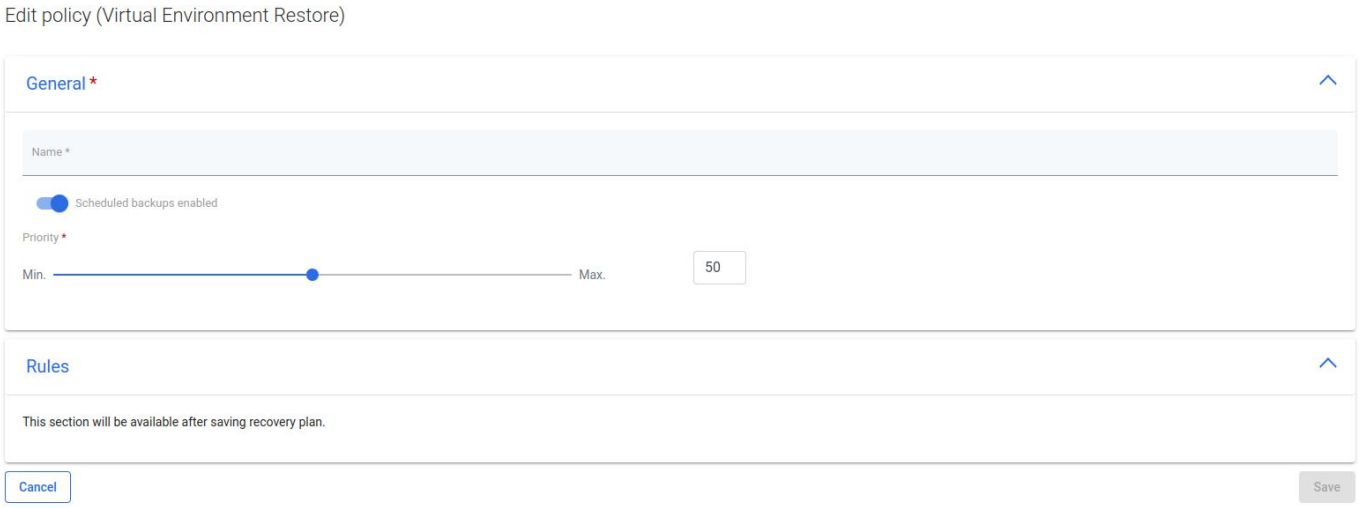
Policies

To schedule a VM restore using a recovery plan (or execute a recovery plan manually), you must first create a policy.

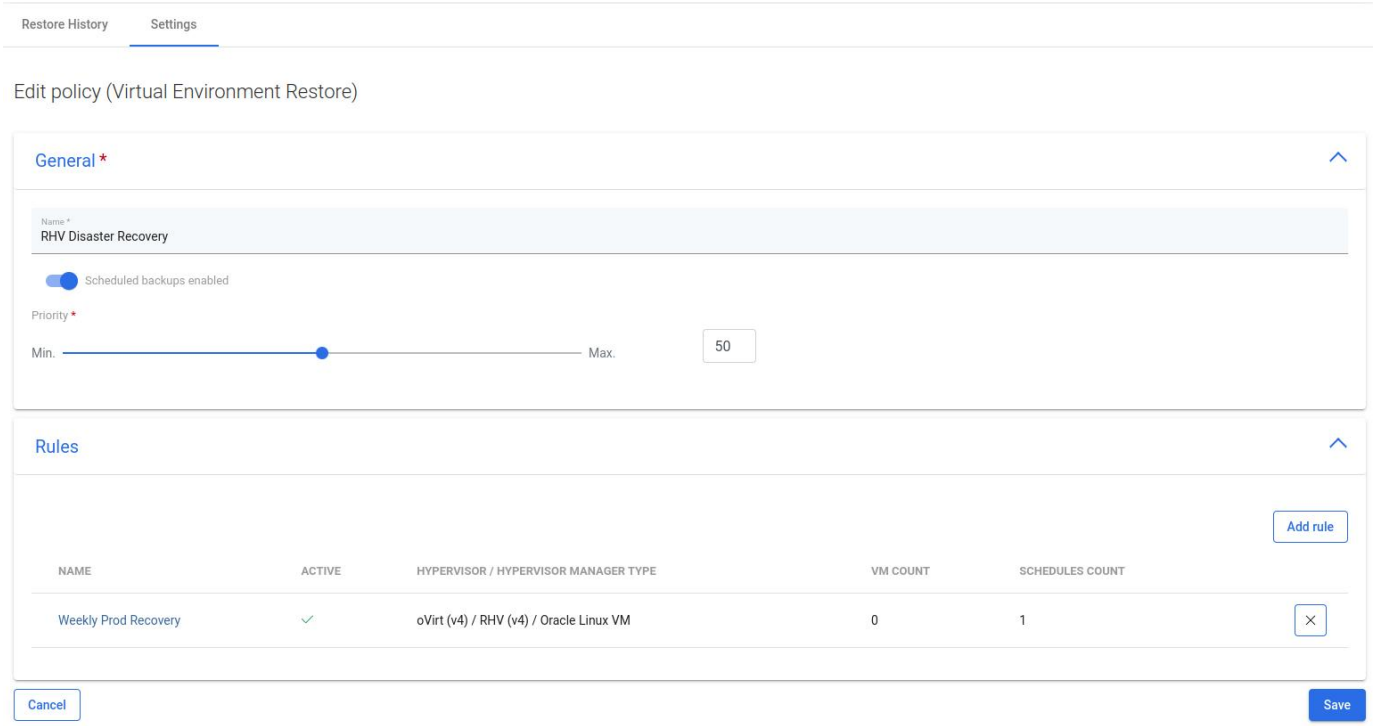
Go to the Recovery Plans from the left menu under the Virtual Environments section.



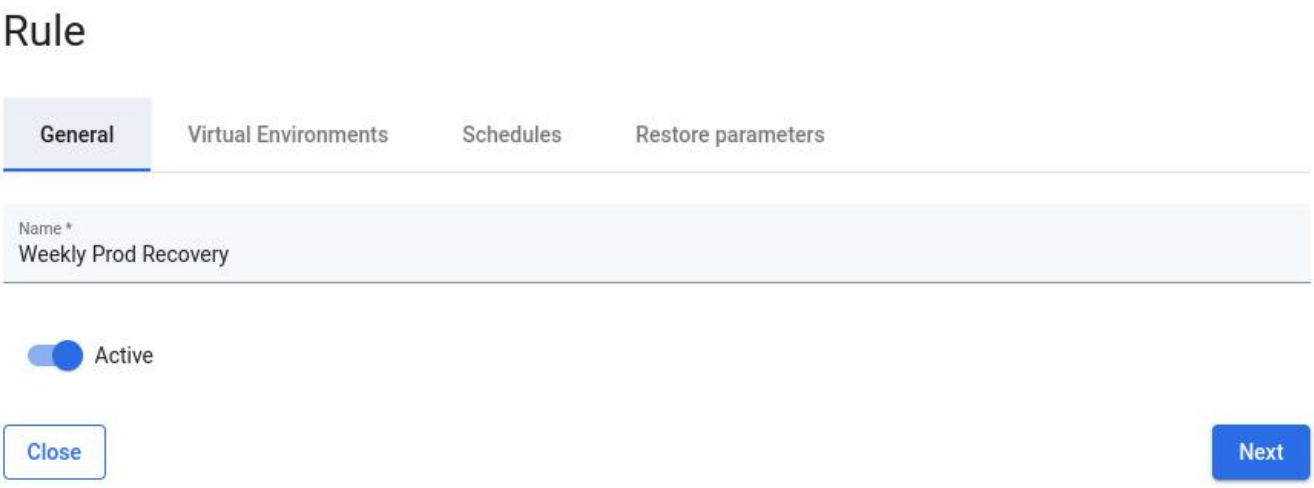
After clicking on  provide the name of the policy and set priority. After saving you will be able to add rules using the new button on the right.



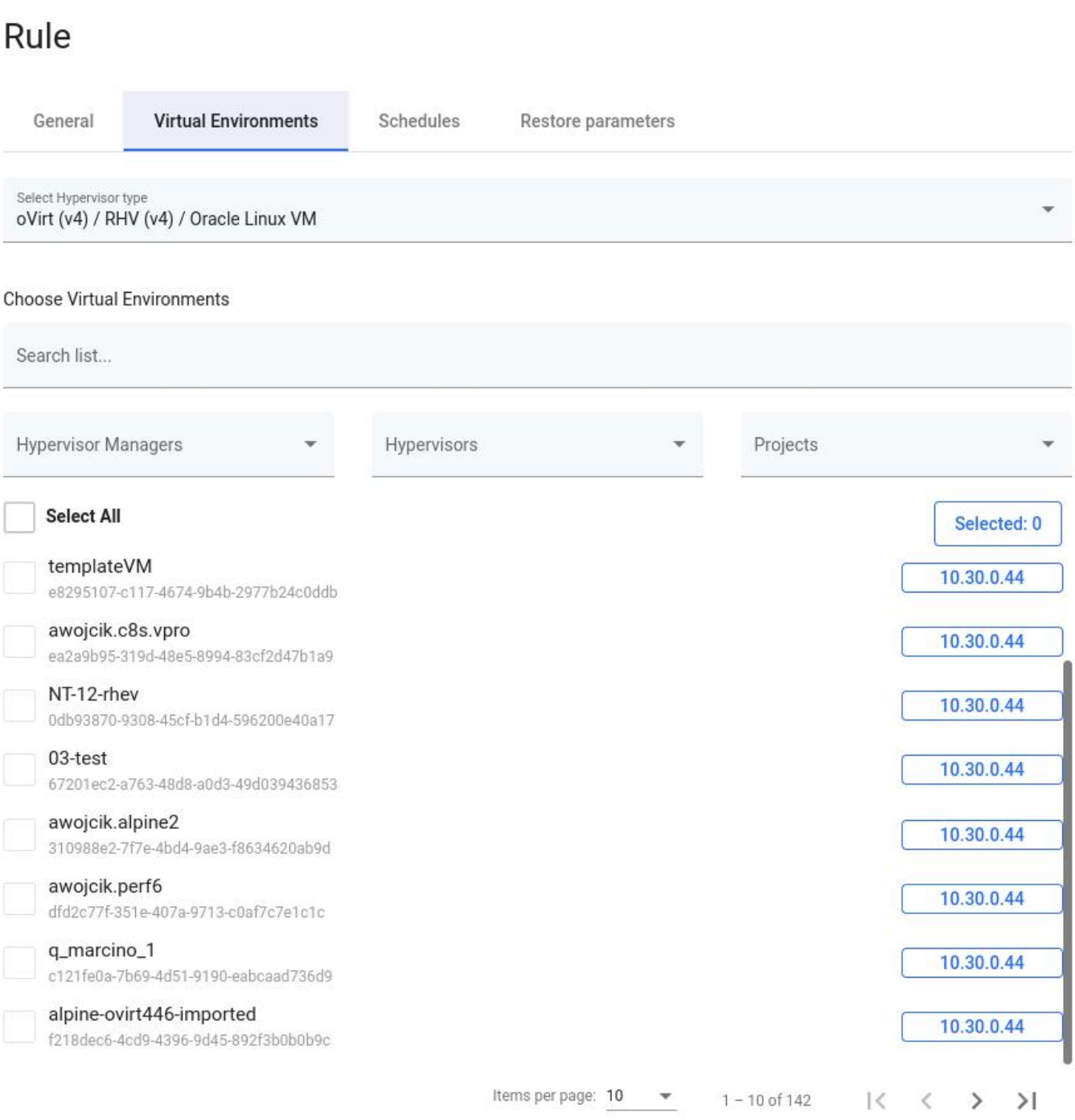
Click on it and customize restore settings.



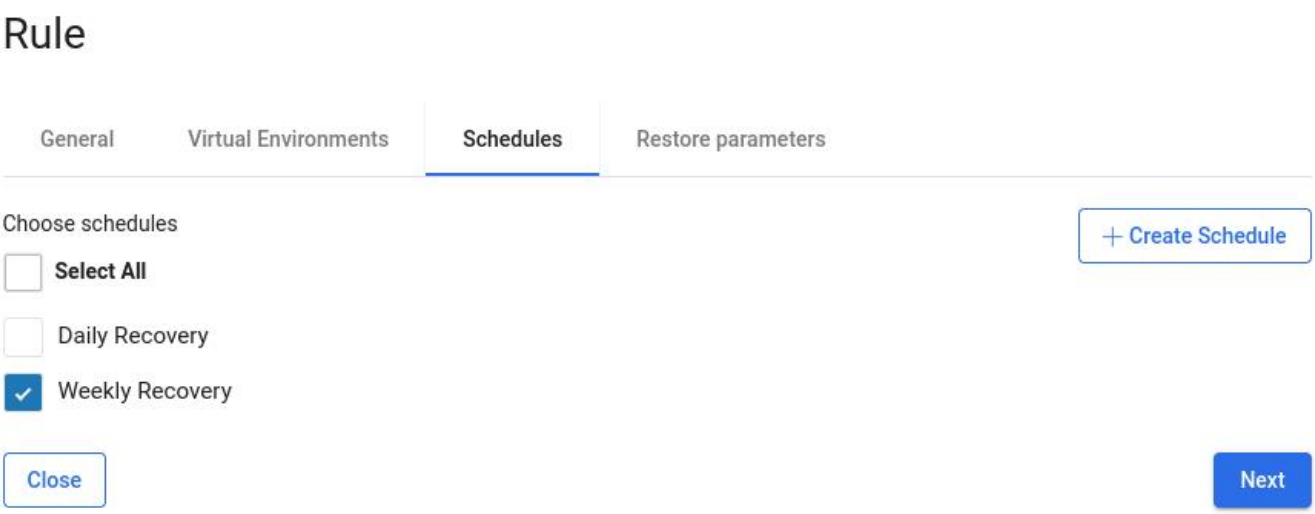
Each rule requires a **name** for easier identification later



In the **Virtual Environments** tab, you need to select **Hypervisor type** for this rule and corresponding **virtual environments** of this type



If you previously defined any schedules for recovery plans you can select them in **Schedules** tab



In **Restore Parameters** tab you specify where VMs are going to be restored - compared to regular restore parameters provided in manual restore window, notice that:

- you need to choose ****which backup to restore -** last (regardless of status) **or** last successful
- you may want to use **Delete if Virtual Environment already exists** - which allows Data Protector for Cloud Workloads to remove VM with the same name as the one being restored

Rule

General | Virtual Environments | Schedules | **Restore parameters**

Select backup to restore
Last successful

- (•) Restore to hypervisor manager
- ( ) Restore to filesystem

Hypervisor Manager
https://rhv444-m.storware.local/ovirt-engine/api

Import to cluster
Default

Import to storage
Data_VM (8.00 TiB, free : 2.42 TiB)

- [ ] Generate VM name automatically

Prefix for the name of the virtual machine being restored
DR_Weekly

Suffix for the name of the virtual machine being restored
Webinar

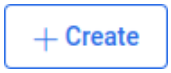
- [ ] Delete if virtual environment already exists

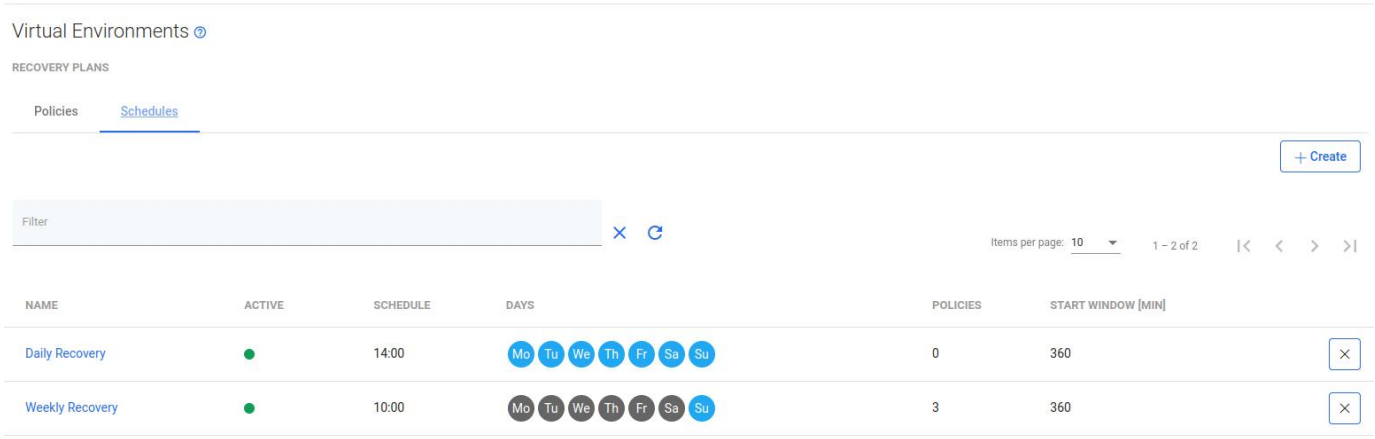
Disk allocation format
PREALLOCATED

- [ ] Power on VM after restore
- [ ] Fail task if restored VM cannot be powered on

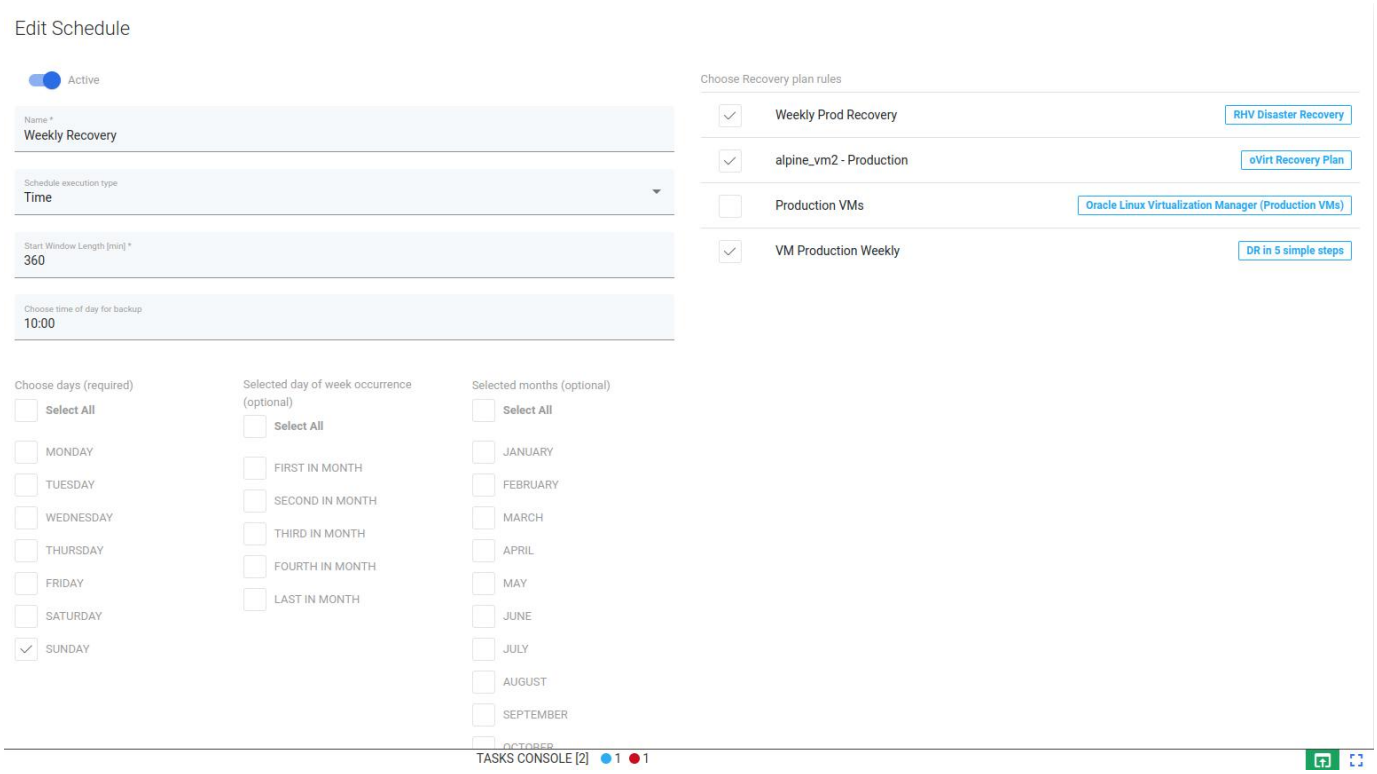
Schedules

The Schedule defines when and on which days recovery plans should run. To define a new schedule use the





Now provide properties:



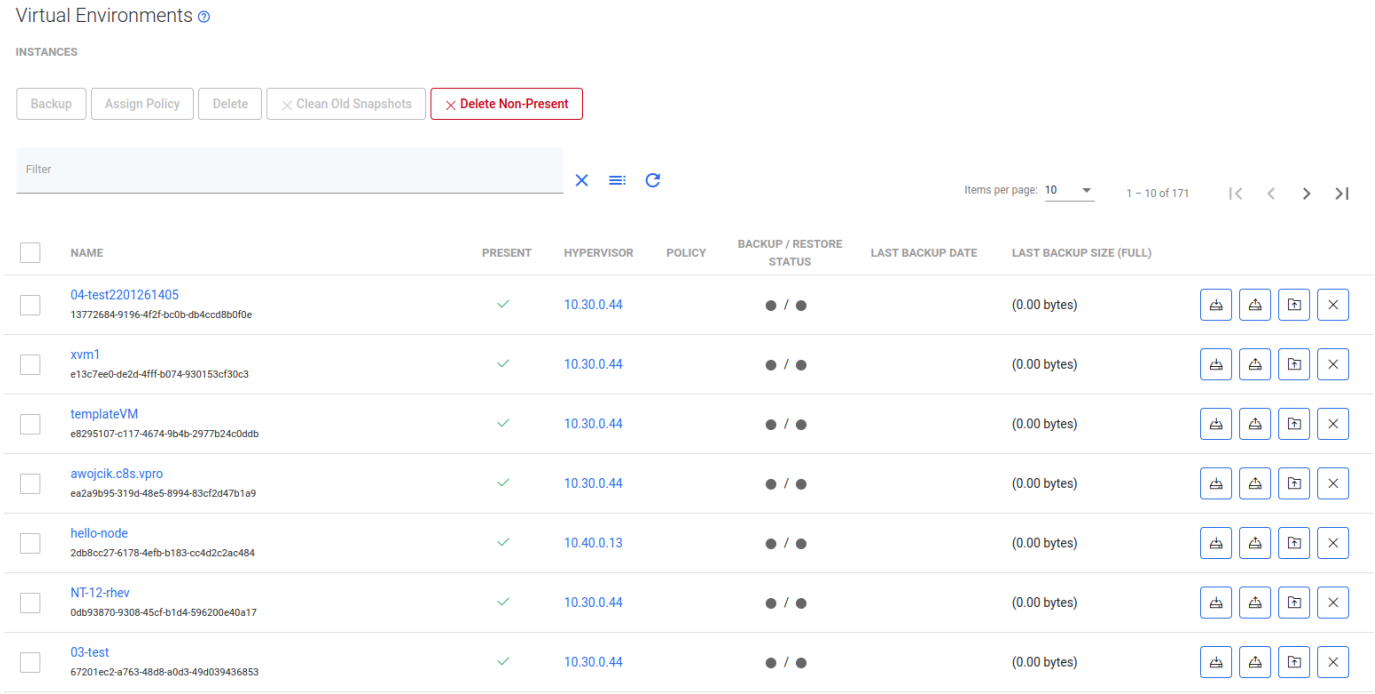
- `Schedule Active` - enable or disable executing schedule
- `Name` - schedule name
- `Execution Type` - choose time or interval mode
- `Start Window` - defines for how long since task start time scheduled tasks are allowed to be executed
- `Choose time of day` - for time execution mode defines when the task should be added to the queue
- `Choose time of interval start` - for interval execution mode defines when tasks should start
- `Choose time of interval end` - for interval execution mode defines when tasks should end
- `Frequency` - defines how often task will be executed during the interval
- `Choose days` - last required parameter, select days of the week on which the task will be performed

You can also use optional parameters to further personalize the backup time or select a virtual environment policy if it has been previously created.

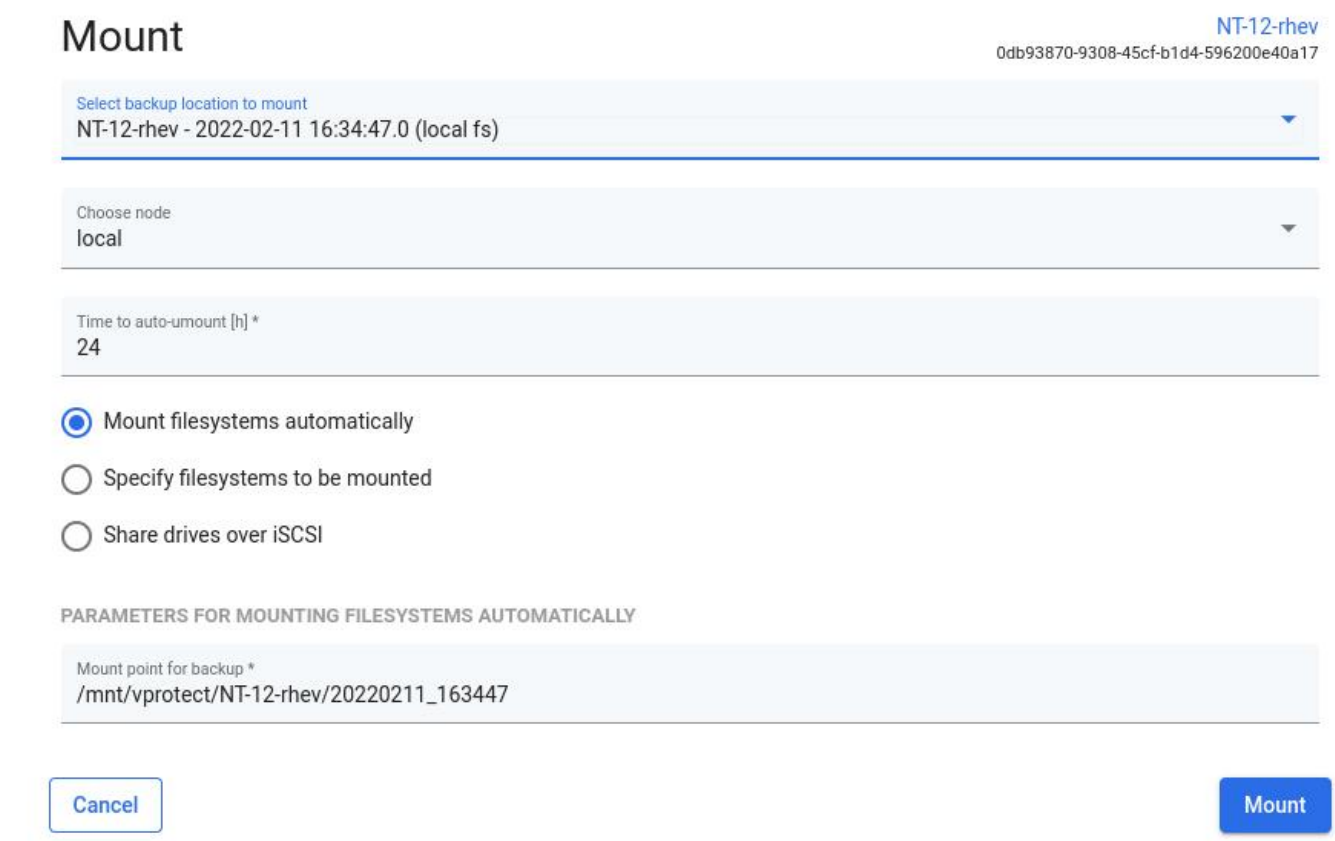
Mounted Backups (File-level Restore)

> **Note:** To see which hypervisor support this feature please go to Data Protector for Cloud Workloads Support Matrix.

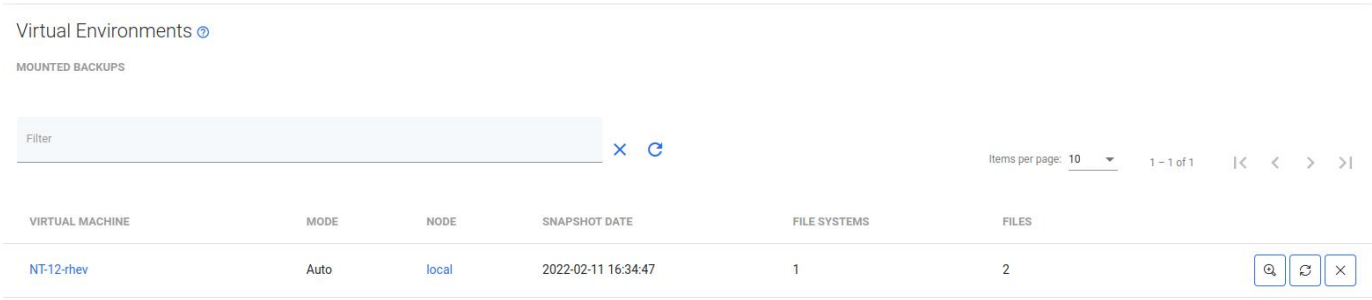
To mount backup go to the Instances tab under Virtual Environment section on the left side menu, then click on the mount icon next to a chosen virtual machine



On the popup window, you can select which backup you want to mount and on which node. You can also change the mounting method, but we recommend leaving the default setting "Mount filesystem automatically".



The Mounted Backups tab show mounted Virtual Machine backups on the Data Protector for Cloud Workloads Node.



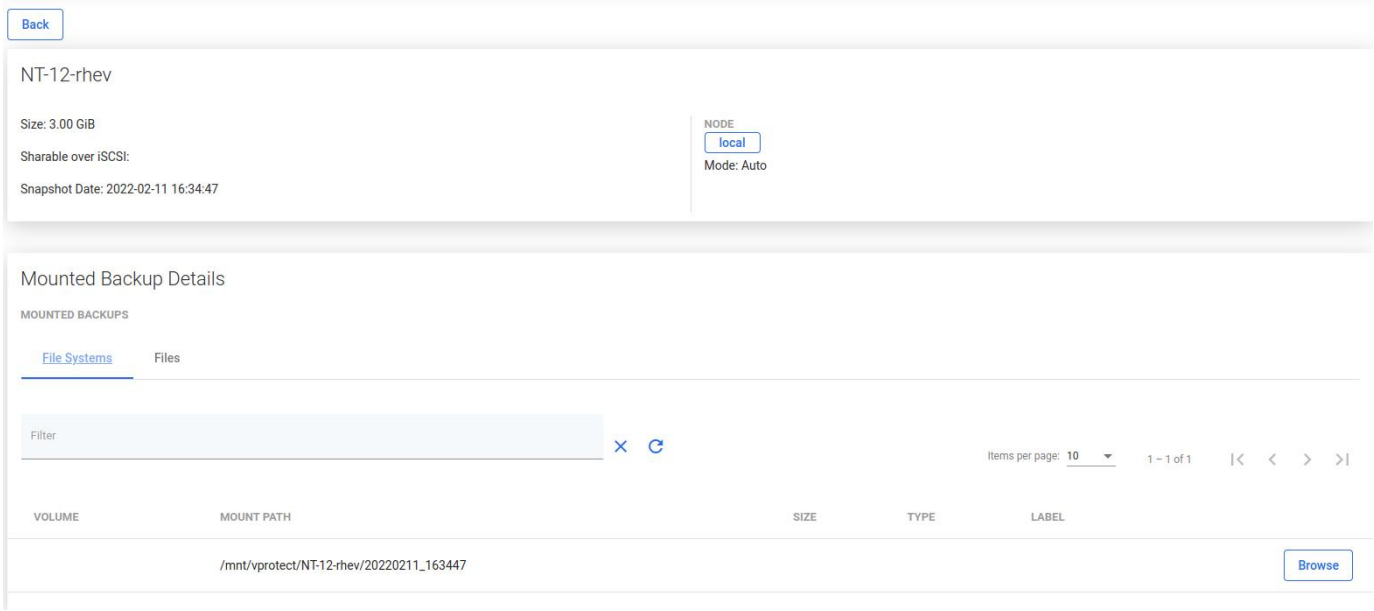
- `VIRTUAL MACHINE` - mounted virtual machine name
- `MODE` - Auto - Data Protector for Cloud Workloads auto-detect filesystems and mount it on path "/mnt/vprotect/". In Manual mode, the user chose a mount point for selected filesystems.
- `NODE` - Data Protector for Cloud Workloads Node responsible for mount job.
- `SNAPSHOT DATE` - date of mounted backup of the VM.
- `FILE SYSTEMS` - a number of mounted filesystems.
- `FILES` - a number of mounted virtual disk images.

Next to every mounted backup you can see three buttons: To unmount backup click on

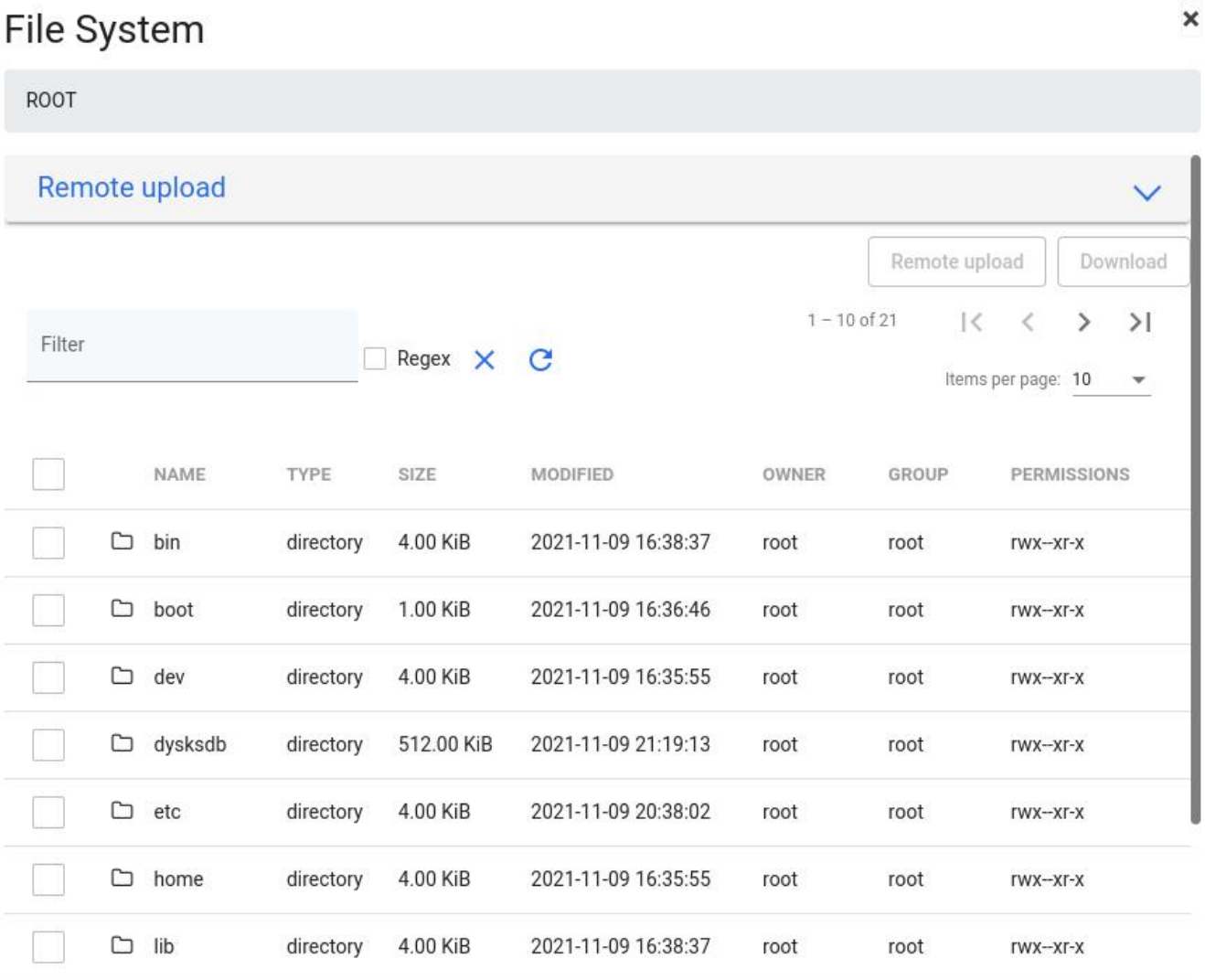
To remount backup click on

To go to the details page of mounted backup click on

On the details page, you can view some basic information or go deeper and browse files.



With a web browser, you can obtain even a single file from inside of your virtual machine backup.



Note: You can also perform the same action thanks to the CLI interface: CLI Reference

Storage Providers

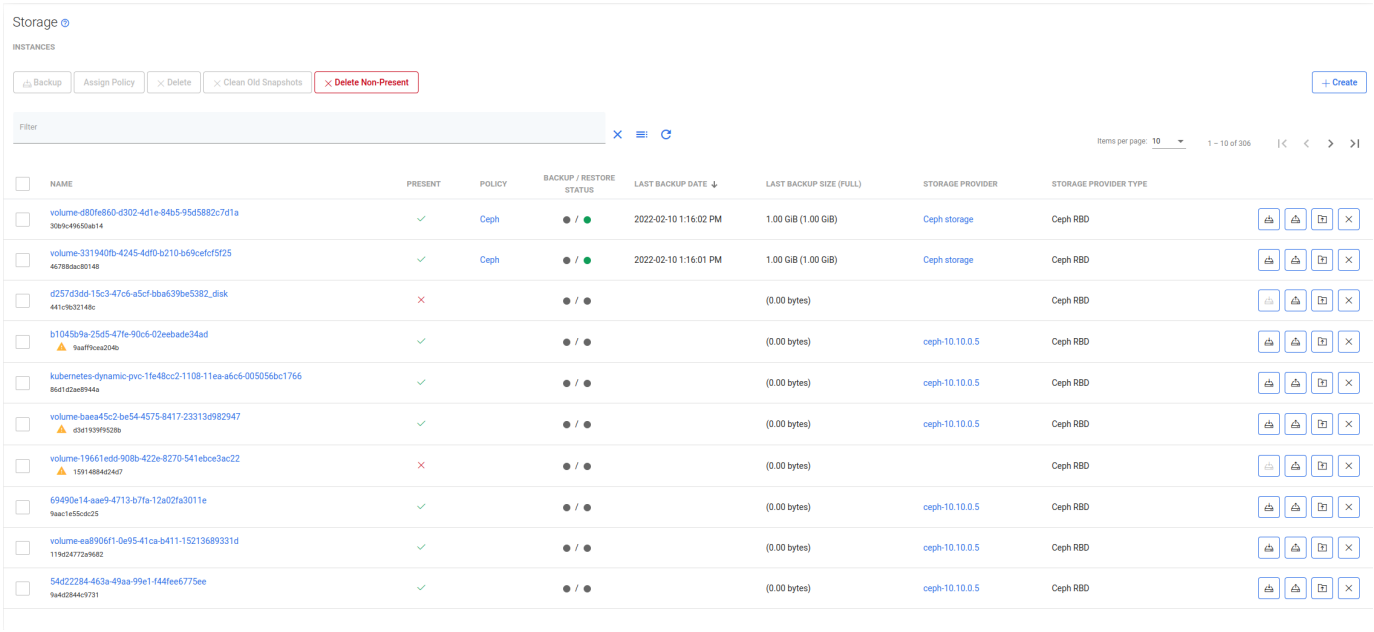
Data Protector for Cloud Workloads allows backup of multiple storage providers. You can protect Ceph RBD volumes, plain file systems, Nutanix Files (AFS), and Nutanix Volume Groups.

You can execute full and incremental backups, and recover individual files using mounted backups or share them over iSCSI.

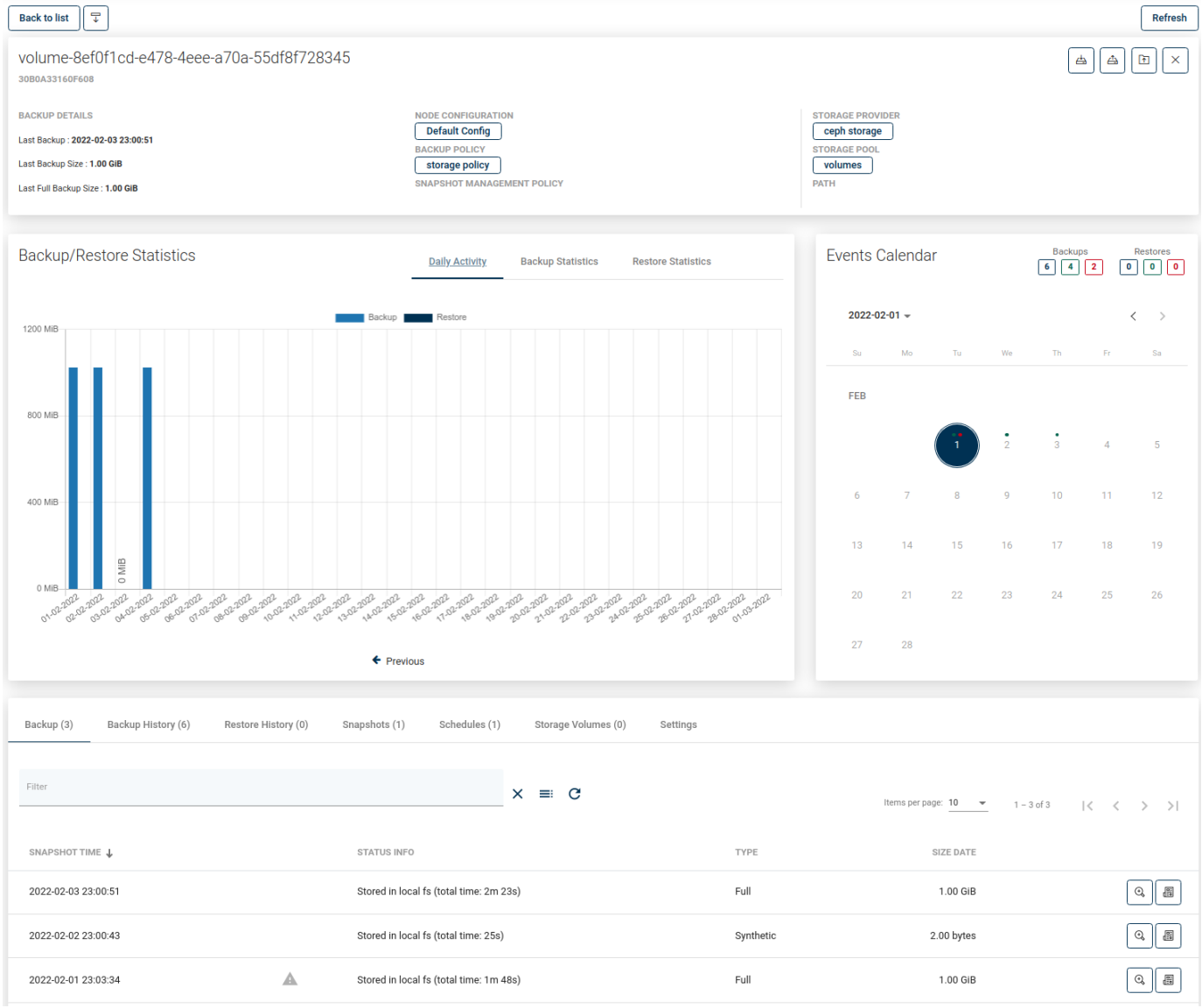
Instances

General

A list of currently known storage instances and access to the details page of each object. From this place, you can also perform on-demand actions such as backup, restore and file-level restore.

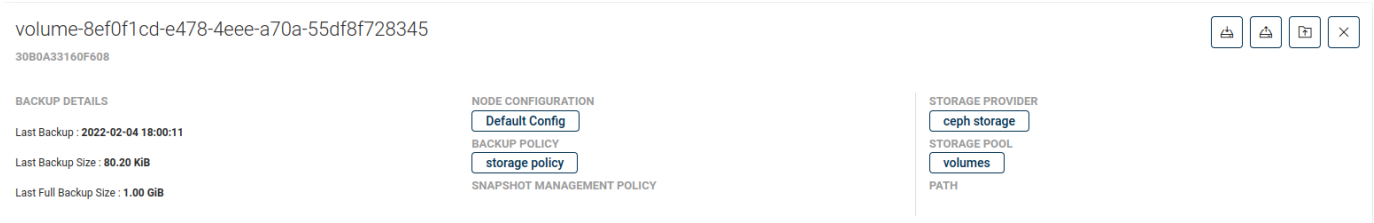


Going back to the Storage details page, this is what it looks like:



As you can see, the window has been divided into several areas:

Storage instance summary



At the top, you can see summarized pieces of information, such as:

- ID of Storage instance into Data Protector for Cloud Workloads
- to which Provider the instance belongs
- to which Pool the instance belongs
- which node is responsible for backup
- short information about the last backup actions
- whether the storage instance has policies assigned to it

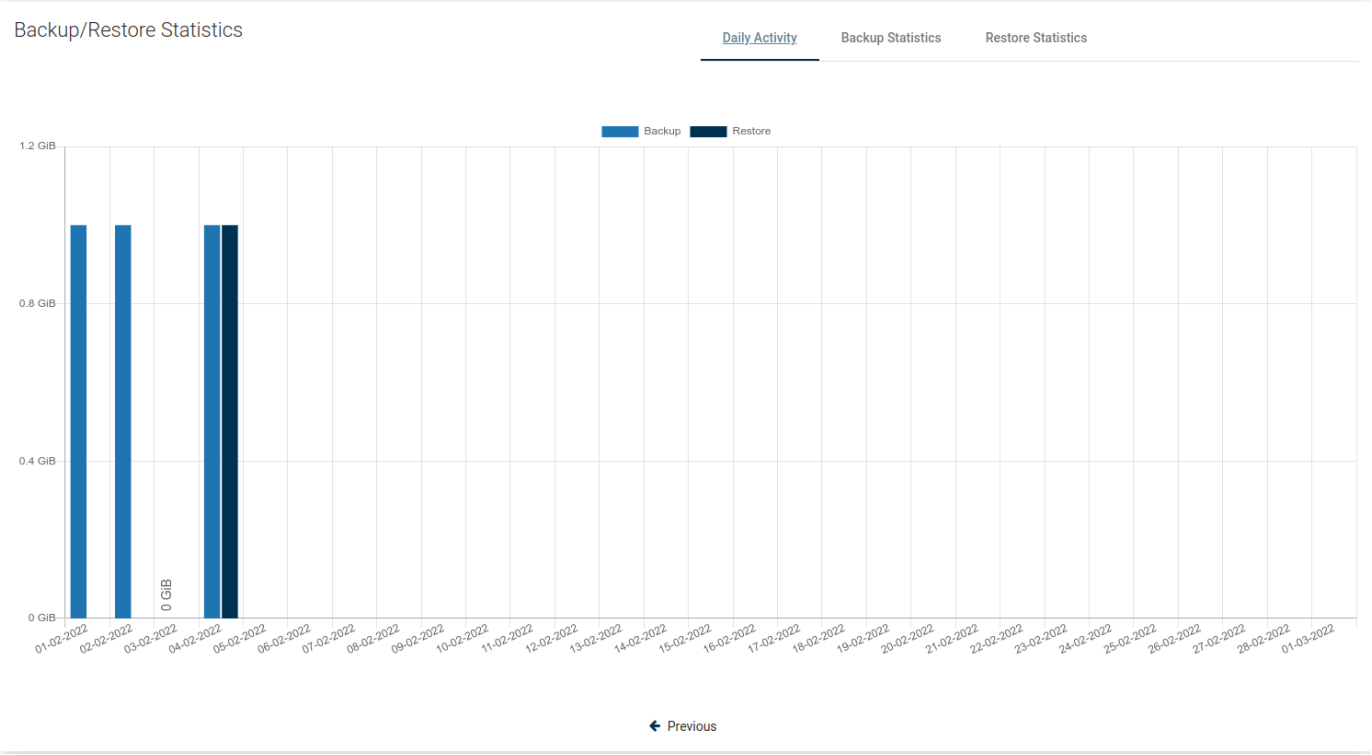
You can also use several function buttons, such as:

- refresh
- back to list

- change section order
- backup
- restore
- mount
- delete

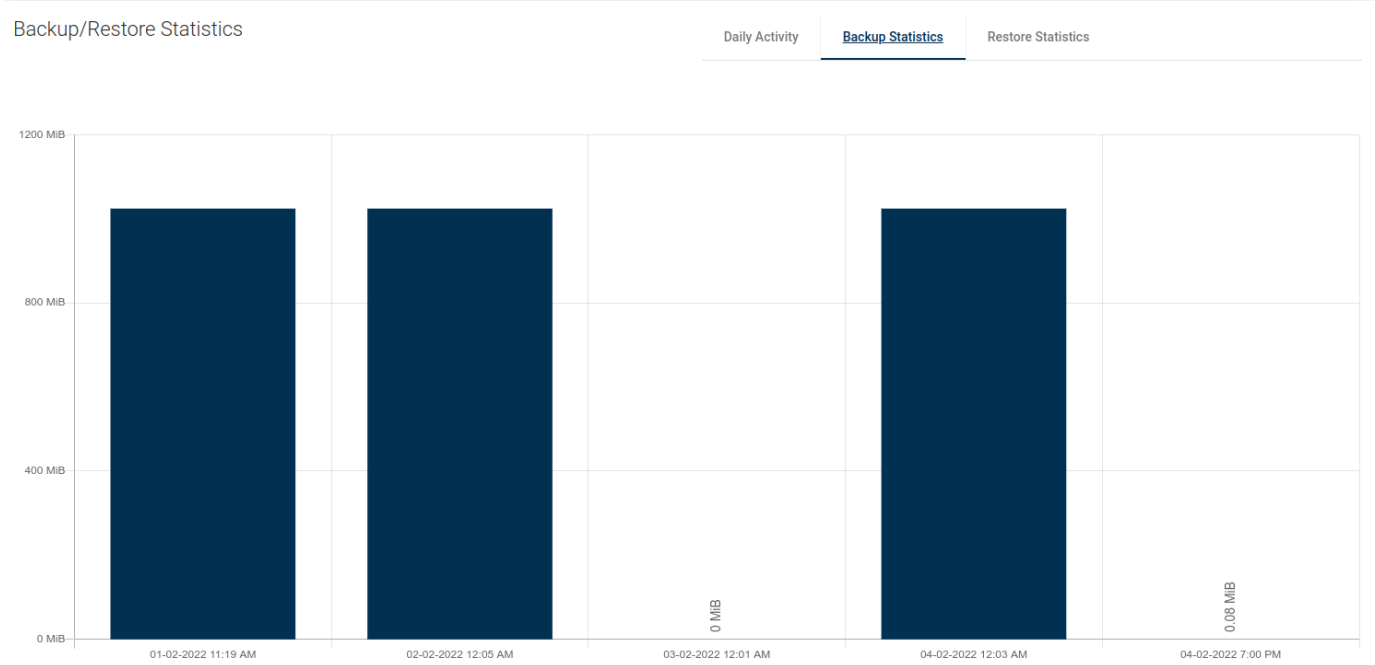
Backup/Restore Statistics

Daily activity



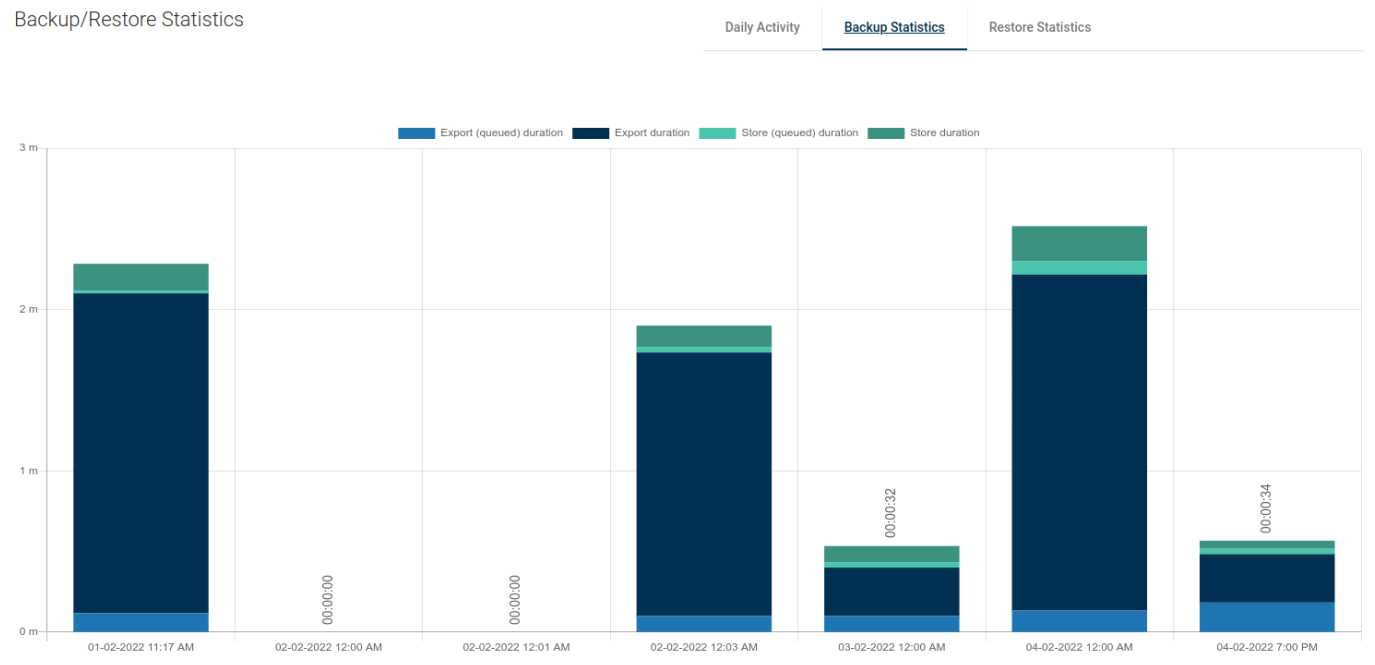
First, you'll see a daily summary of the backup and restore operations for the last month. This view is called "Daily Summary" and is the default view. You can switch the report between multiple views.

Backup Size



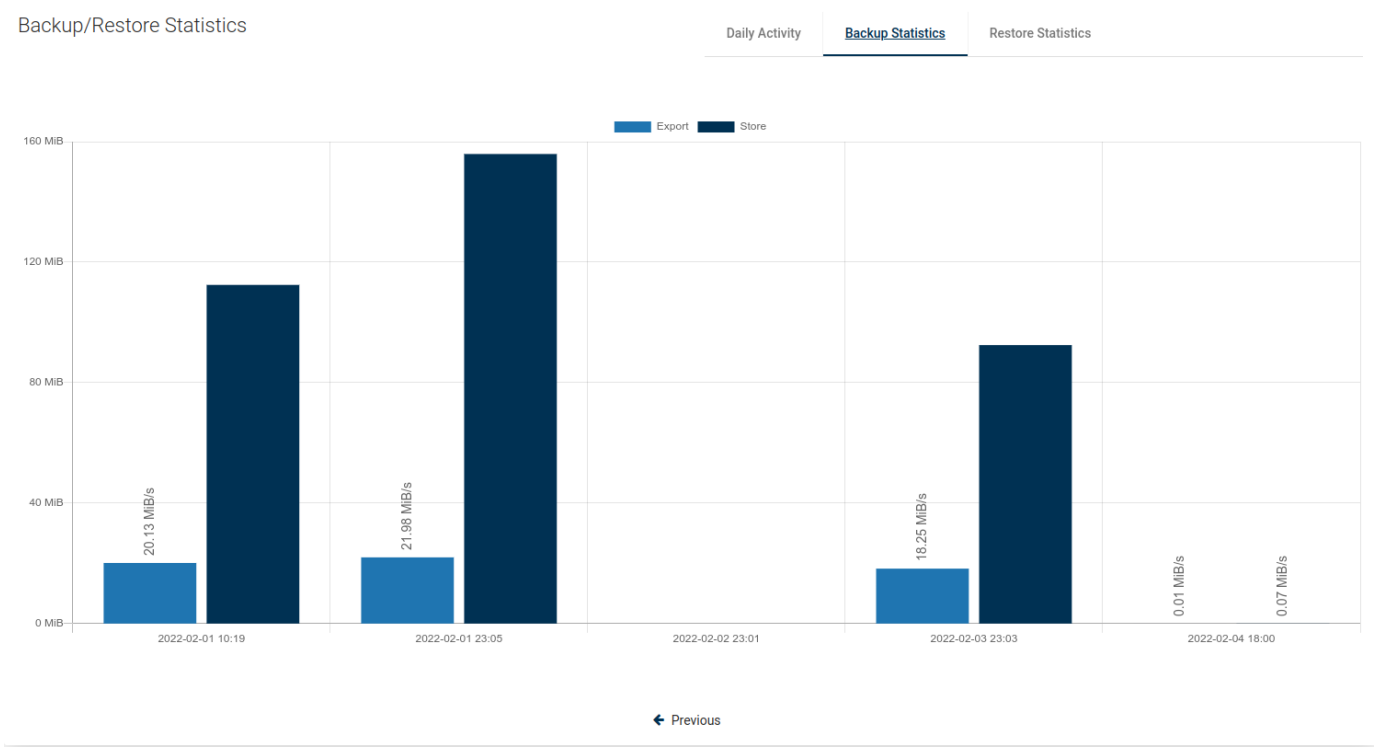
This view shows separate columns for each backup made. Thanks to this, you can easily determine what data increase occurs on a given machine.

Backup Time



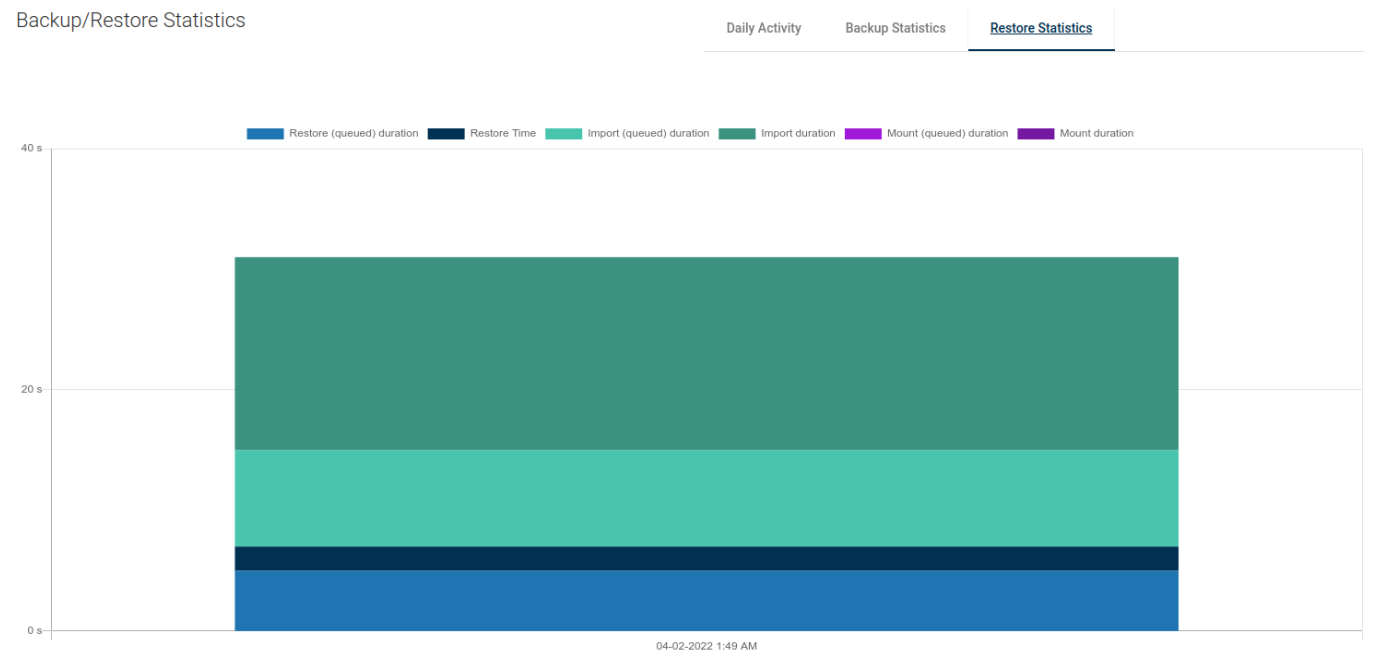
A very useful report. It allows you to determine the required window length for backups or, based on the time of individual phases, it is easy to deduce the cause of slow backups.

Transfer Rate



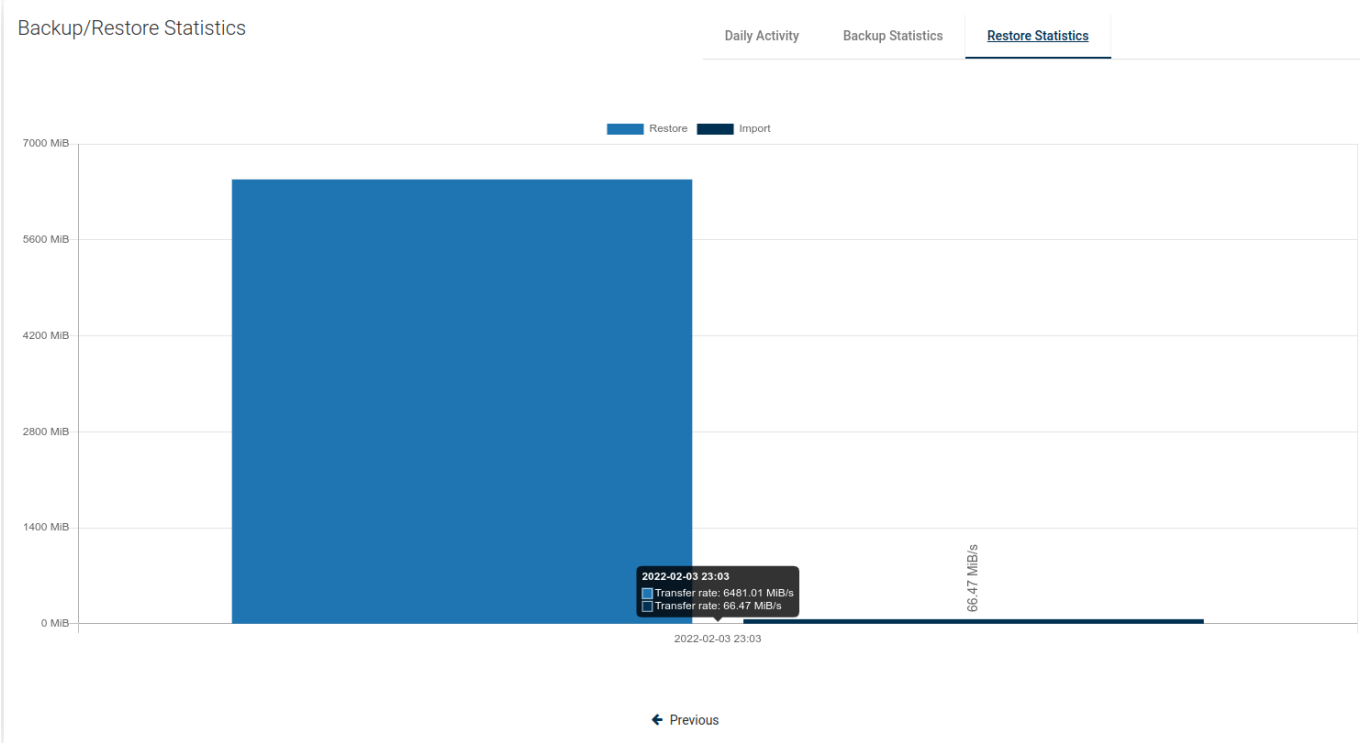
One of the latest reports, now you can easily see how fast data transfer is.

Restore Duration



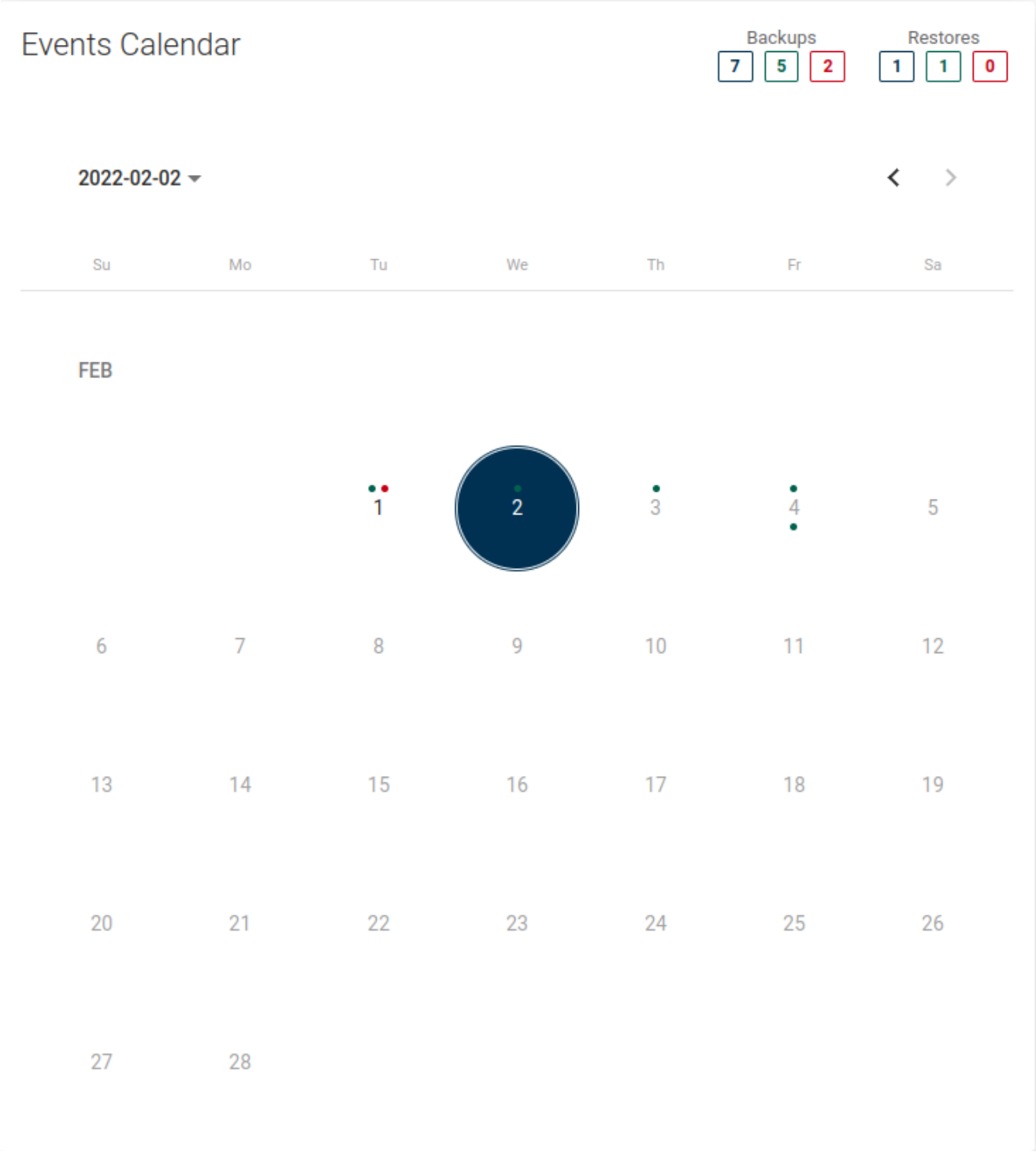
A view with the same properties as "Backup Time". It allows us to estimate how long it will take to restore the storage instance in the event of a failure.

Restore Rate



As in the previous case, we also have the transfer speed for the restore job.

Events Calendar

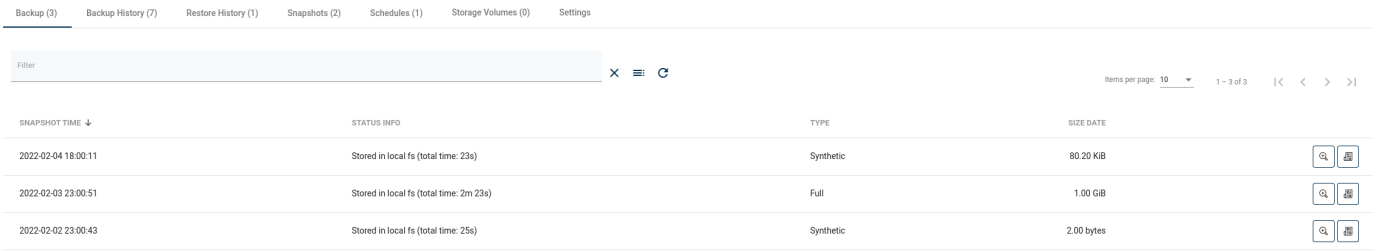


The calendar extends the possibilities of adjacent statistics. It allows you to neatly define the range of days you want to see, additionally makes a quick summary of the number of backups and restores (top right corner).
Blue - the sum of all backups, **Green** - the sum of successes, **Red** - the sum of failures.

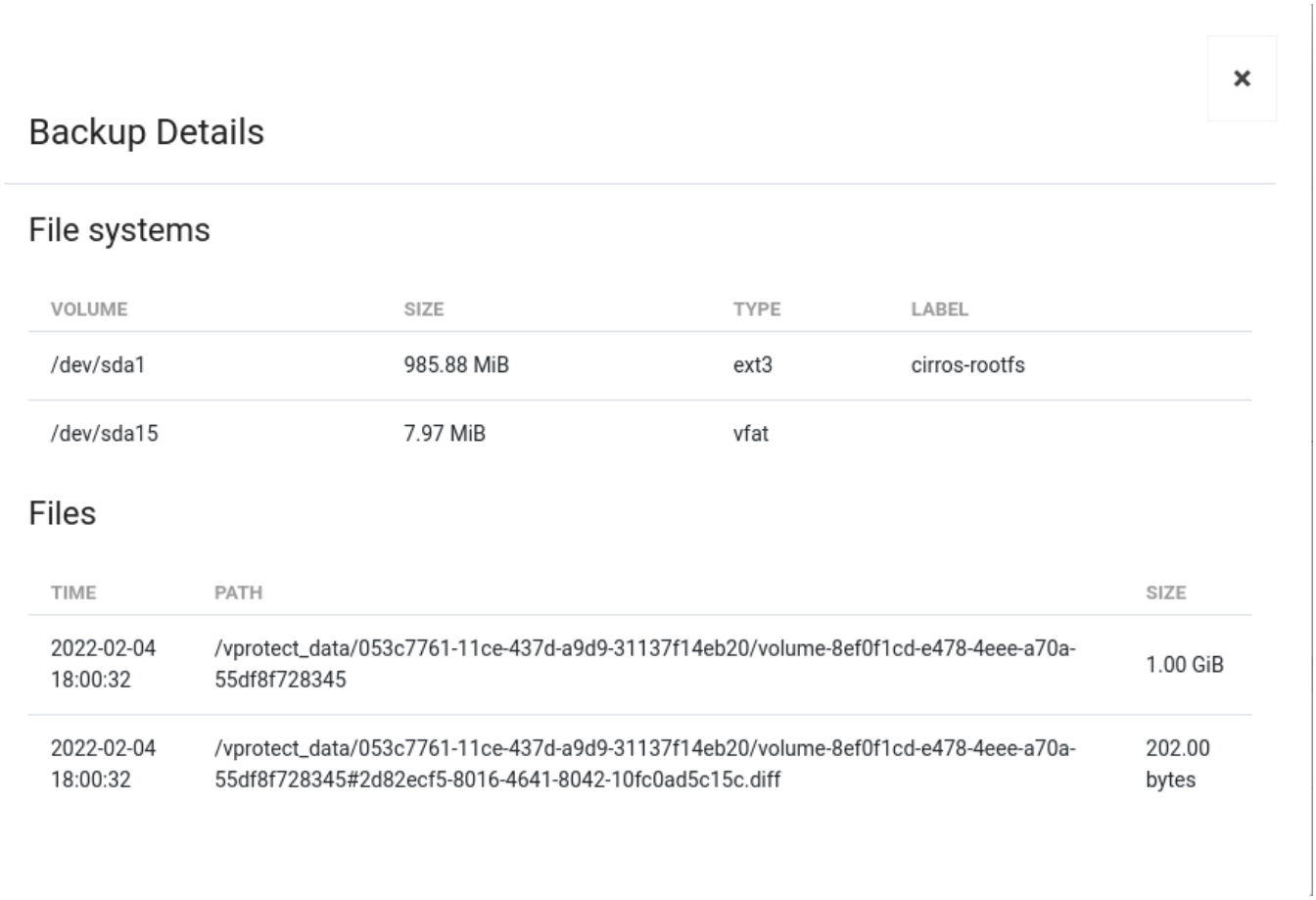
Bottom menu

In the bottom menu, you can find a large number of tabs, each of which will present different information or will allow you to change the configuration of this particular storage instance.

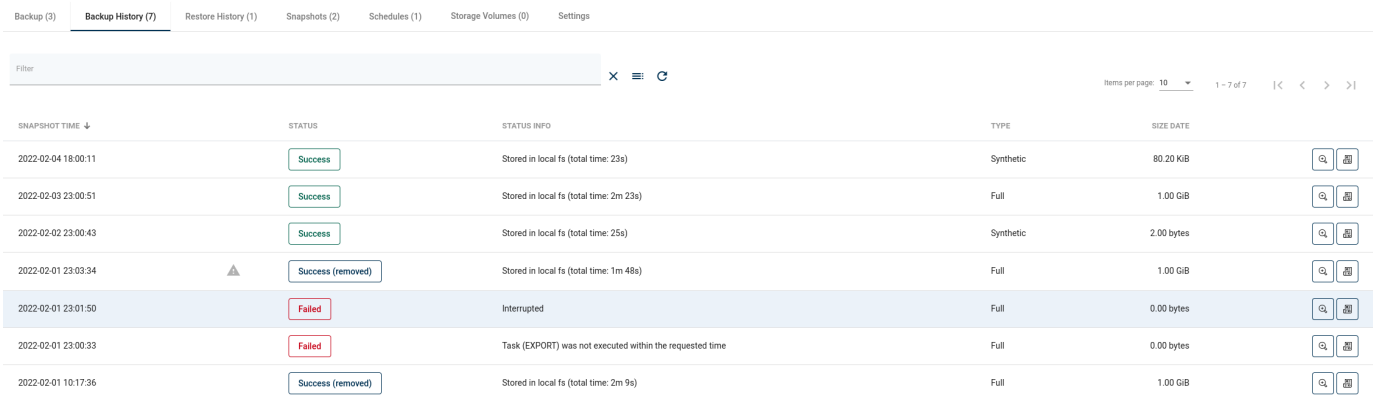
Backup



The first tab shows all backups that are currently available and all the basic information about them in a list. After clicking on the magnifying glass button, you will see additional information. The button next to it allows you to download logs in the form of a .txt file.



Backup History



This tab shows information about all backups made. Also about those that failed, were removed (because of retention) or are currently executing.

Restore History

This tab is similar to "Backup History". This is a list with basic information about the storage instance restores performed. When you open the details of the selected restore, you will see much more detailed information.

Restore details

Node	node1
Protected Entity	volume-8ef0f1cd-e478-4eee-a70a-55df8f728345
Restore Time	2022-02-04 00:49:47
Status	Success
Status Info	Backups of STORAGE: volume-8ef0f1cd-e478-4eee-a70a-55df8f728345 (size: 1 GiB) imported in: 15s.
Backup Type	Full
Restore Type	Restore and import

Task Time Stats

Import duration	00:16 s
Import (queued) duration	00:08 s

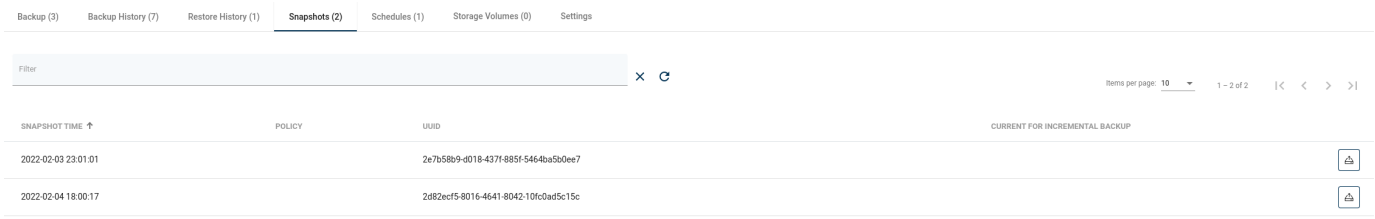
Backup

Backup Time	2022-02-03 23:03:14
Protected Entity	volume-8ef0f1cd-e478-4eee-a70a-55df8f728345
Size	1.00 GiB
Snapshot time	2022-02-03 23:00:51
Status	Success
Status Info	Stored in local fs (total time: 2m 23s)
Type	Full

Backup - task time stats

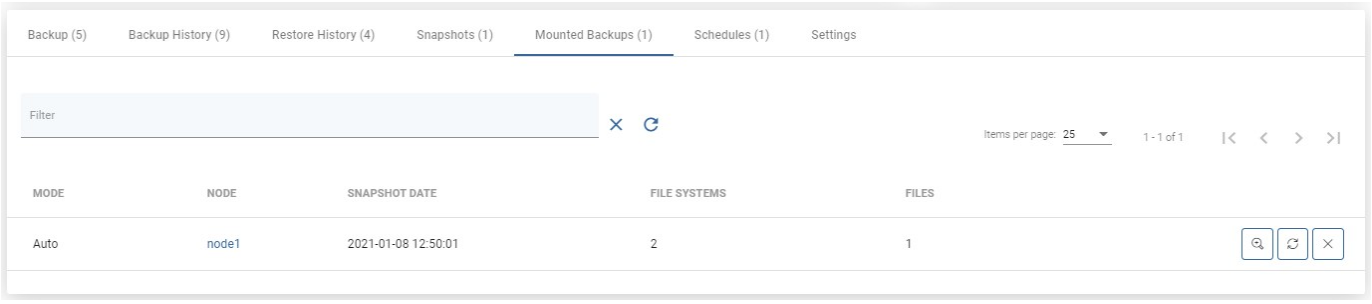
Export time	02:05 s
Queued Export Time	00:08 s
Queued Store Time	00:05 s
Store time	00:13 s

Snapshots



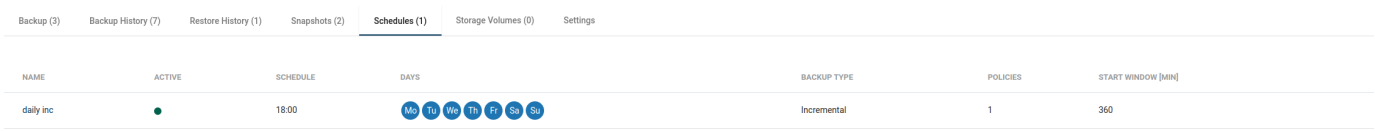
This tab shows the storage instance snapshot - the tab is visible only for the ceph and nutanix Storage Provider.
As you can see in the list above, there is a green dot next to the snapshot. This means that the snapshot is created for incremental backup purposes. This is an automatic operation and we only keep the last snapshot.

Mounted Backups



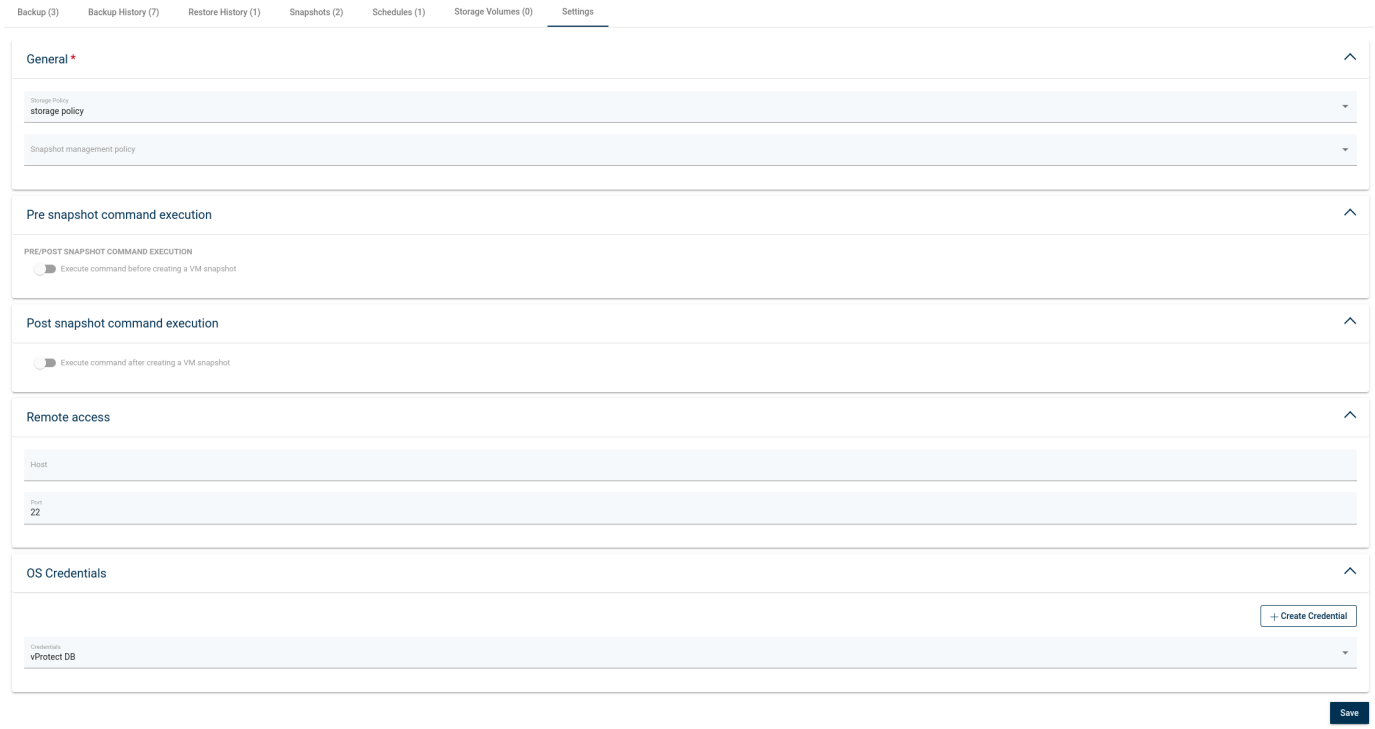
This tab lists all mounted backups of this particular storage instance. With the buttons on the right, you can browse/remount/delete it.

Schedules



On this tab, you can see all the schedules assigned to the instance.

Settings



Finally, the last tab. The first option allows you to change the policies assigned to the storage instance.

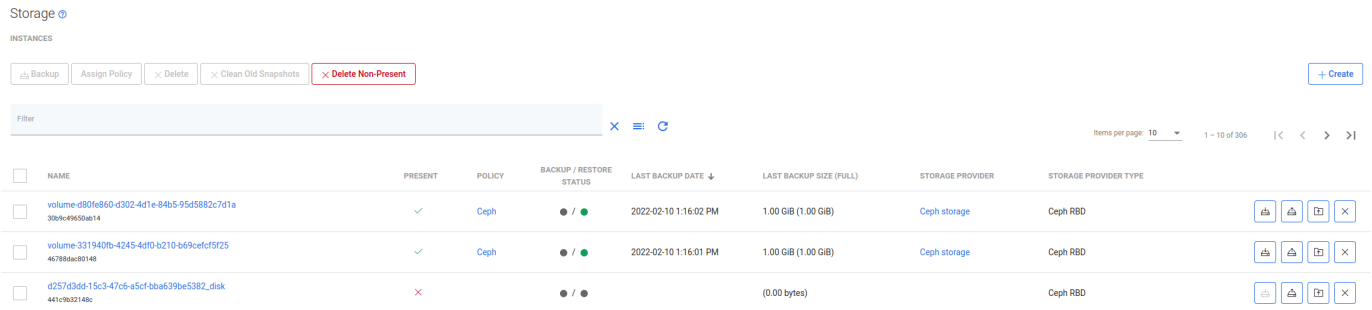
Performing pre/post snapshot commands is a function intended for advanced users. As the name implies, it allows us to execute scripts via an ssh connection, either before or after taking a snapshot.

Backup on-demand

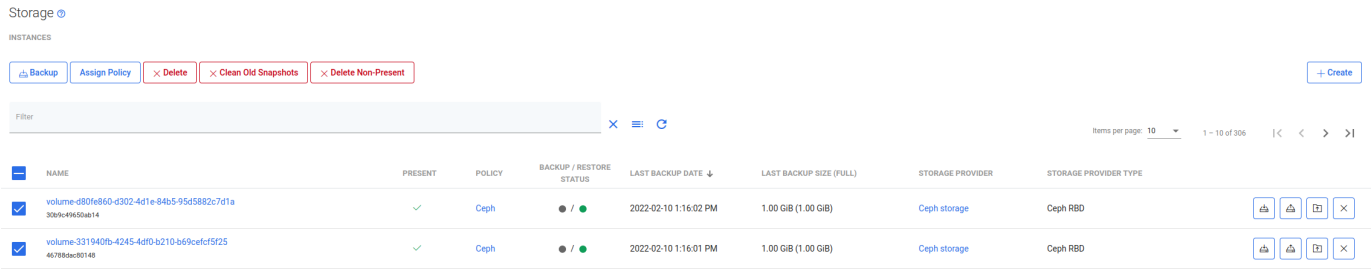
Storage List

To perform on-demand backup, go to the instances tab under the Storage Providers section.

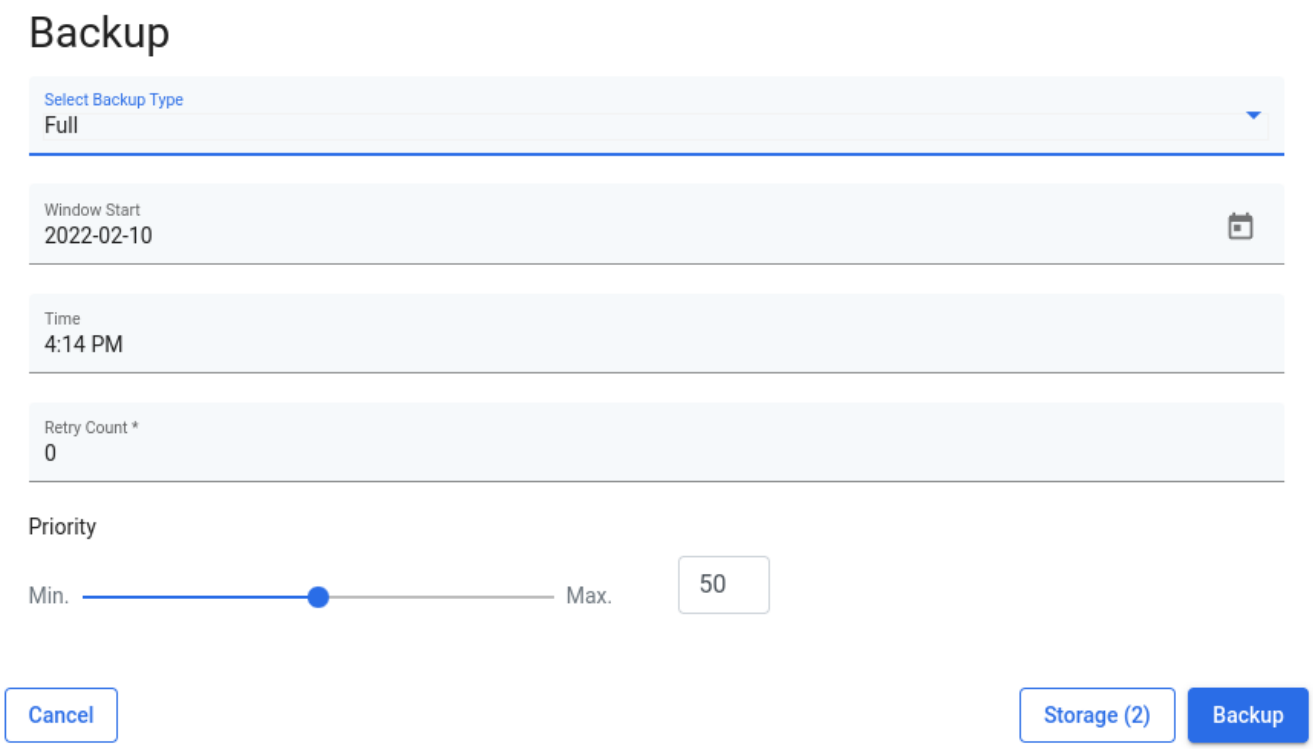
You can click on the icon to back up a single storage instance



Or select multiple instances and click on the icon to back them up.



Finally select the backup type, backup destination, when a task should start, the priority, and click on the backup button.

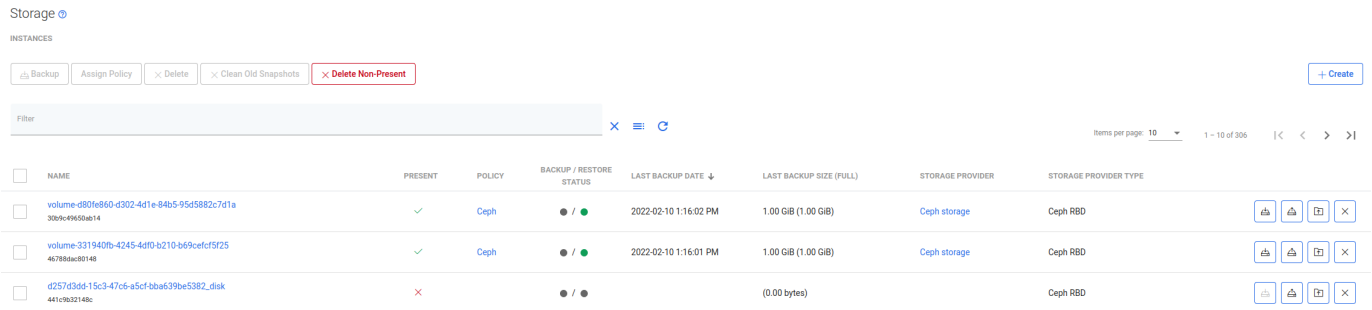


> **Note:** You can also perform the same action thanks to the CLI interface: CLI Reference

Restore on-demand

Restore from Storage Providers menu

To restore a single storage instance on-demand, go to the instances tab under the Storage Providers section. Click on the restore icon next to the object



Now you should see a popup window where you can customize the restore settings.

Restoring to the filesystem is an option to restore directly to the Data Protector for Cloud Workloads Node storage. (Remember, the Data Protector for Cloud Workloads user must have the appropriate write permissions to the given path.)

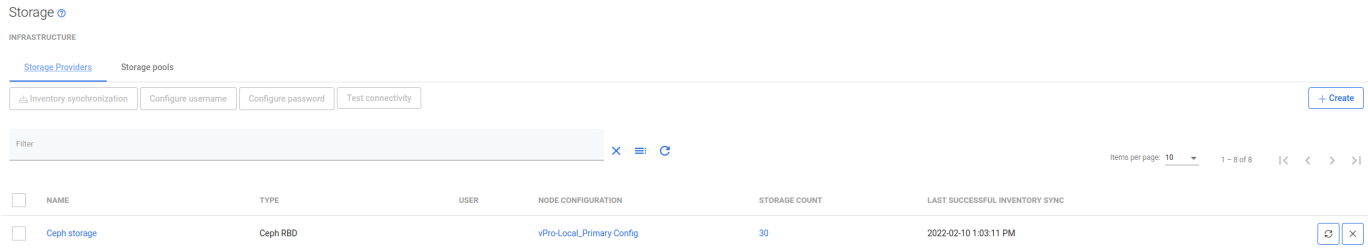
You can also restore the backup to the storage provider from which the backup was created.

Finally, after customizing the restore, click the restore button.

> **Note:**
>
> - every platform has some restrictions imposed on the storage instance name, such as length or characters that can be used. Please check these limits before restoring with a custom name.
> - You can also perform the same action thanks to the CLI interface: CLI Reference

Infrastructure

This section describes how to manage Storage Providers in Data Protector for Cloud Workloads. The inventory that Data Protector for Cloud Workloads needs first has to be populated. The first step is always to add a storage provider or file system visible on the Data Protector for Cloud Workloads Node.

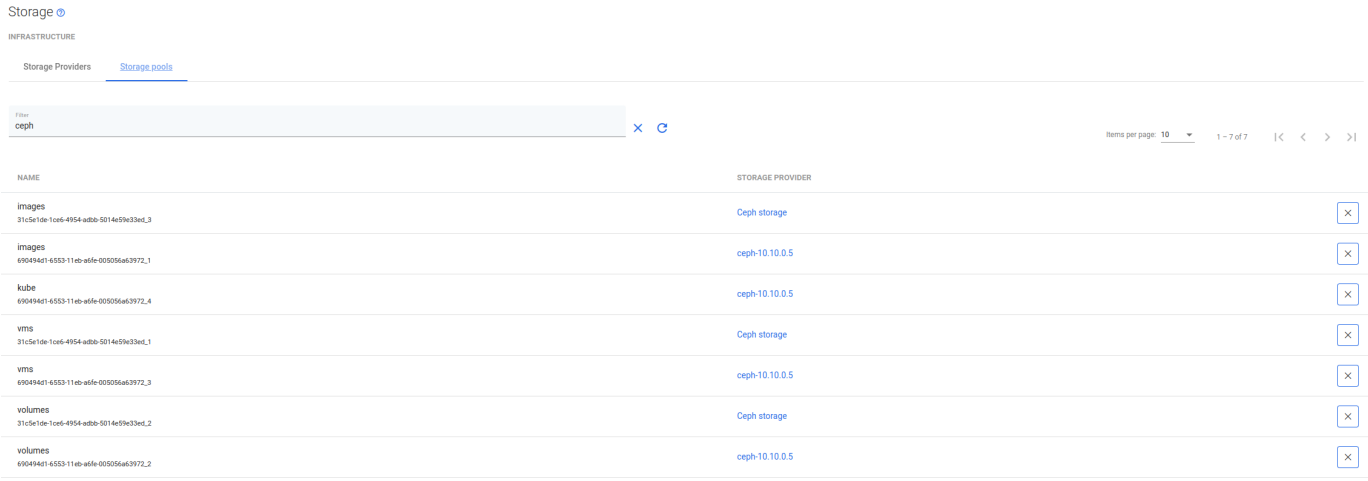


Click Add Storage Provider to add entries

Then synchronize the inventory (either automatically - a dialog box will be shown just after saving the form, or manually with the button on the right of the storage provider).

If the inventory synchronization tasks (visible on the console at the bottom) were completed successfully, this also proves that the connection was successful, authentication is correct and all of the inventory items have been collected successfully.

Check the storage pools as well as Storage -> Instances to see the results of the inventory synchronization.



> **Note:** You can also perform the same action thanks to the CLI interface: CLI Reference

Backup SLAs

Backup SLAs allow you to group backup policies and schedules for multiple storage instances. In general, a storage instance should have only one backup policy so as to always have an easy-to-interpret configuration.

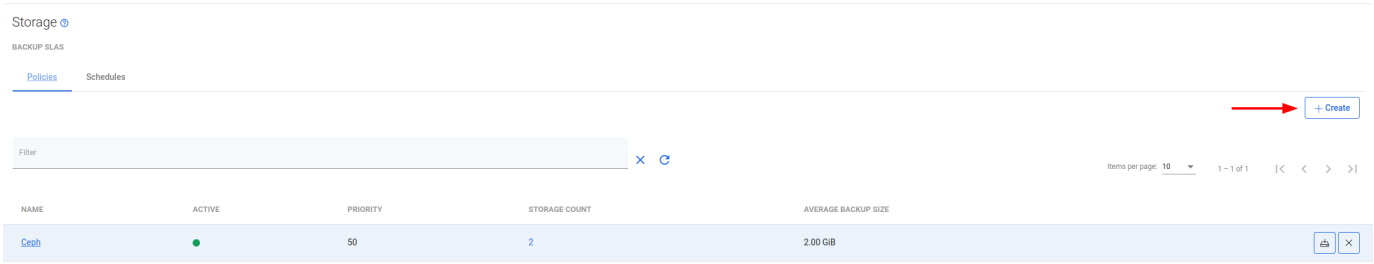
Each policy can have multiple schedules assigned so that you can define more complex schedules so that backups are executed even multiple times each day and with different backup types.

> **Note:**
>
> - schedules define the type of backup - full or incremental
> - the approach we highly recommend is to create a schedule for **periodic full** backup and always assign at least 1 such schedule in the backup SLAs
> - in order to create incremental backups, you need to always have **at least 1 incremental backup schedule** and run at least one full backup

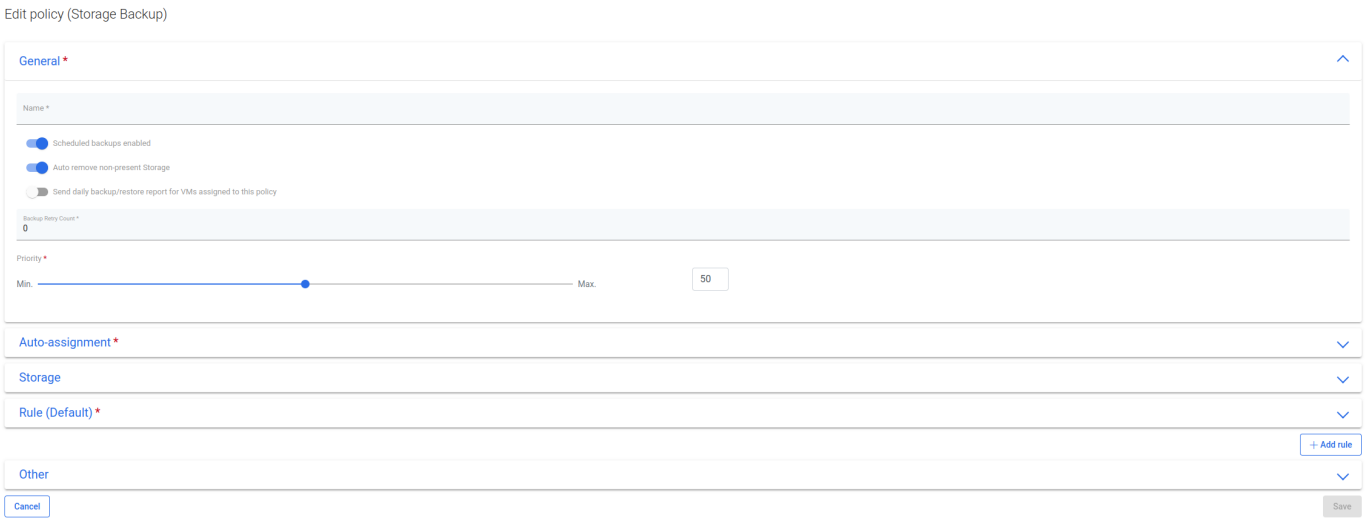
Policies

Policies allow you to group storage instances in many ways. For example, based on the type of storage provider.

To create a new backup policy, please open the Backup SLAs tab under the Storage Provider section and click on the + Create button on the right.



Now you should see the policy wizard with 5 main sections.



General

Under this section you can set up:

- Name of policy
- Switch on/off auto-remove non-present virtual environments
- Set the priority for tasks

Auto-assignment

In this section you can configure automatic policy assignment based on certain criteria:

- Mode
  - Disabled
  - Assign only
  - Assign and remove
- Include or exclude rules based on regular expressions matching storage instance names, i.e.:
  - regular expression examples:
    - `.*` match any character any number of times
    - `st-[0-9][0-9][0-9]` - match names that start with `st-` and 3 digits

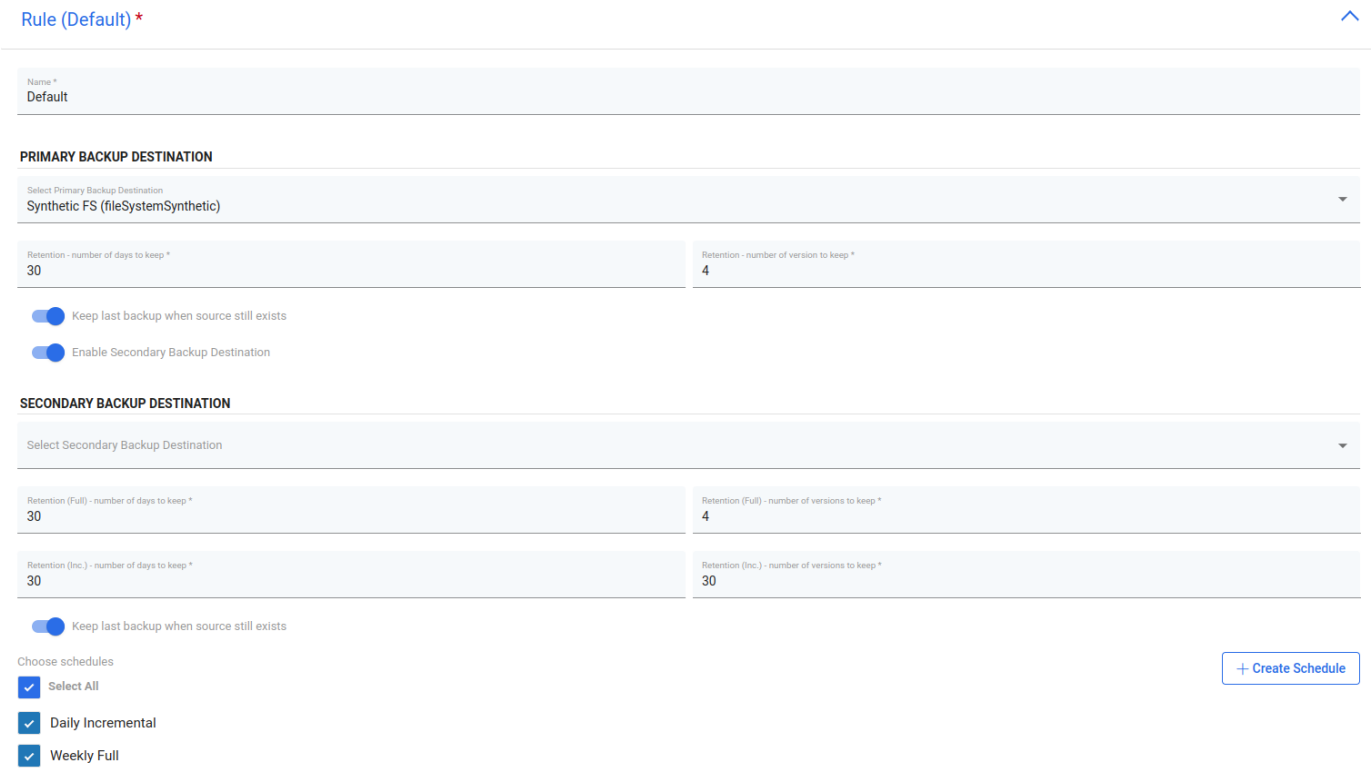
        - `(prod|uat|dev)-[0-9][0-9][0-9][a-z]?` - match names that start with the `prod` or `uat` or `dev` prefix, then `-`, then 3 digits and an optional lower-case letter (matching is case-sensitive)
    - exclude rules always take precedence over include rules
    - objects may not be reassigned to a different policy if they already have a matching policy assigned
    - objects may be reassigned to a different policy only if the mode is `Assign and remove`, the current policy assignment rules don't match, and the other policy's rules do match
    - rules are joined with the OR operator, so
        - if **any** rule (tag or matched regular expression) excludes the storage instance - it will be excluded
        - if **no** rule (tag or matched regular expression) excludes the storage instance, and **any** rule (tag or matched regular expression) includes the VM - it will be included
- You can also select clusters to match only VMs that belong to them

Storage

Here you can easily select storage instances manually.

Rule

This section is used to select the backup destination.



> **Note:** You can select Primary and Secondary Backup Destintanion in one Rule

You can also set here **Retention** settings for your backups. You can use a number of days and versions for full and incremental backups.

Retention

Data Protector for Cloud Workloads handles retention for all backup destinations. There are 4 properties that define how long backup should be kept in the backup destination:

- `Retention (Full) - no. of versions to keep` - number of full backups
- `Retention (Inc.) - no. of versions to keep` - number of incremental backups
- `Retention (Full) - no. of days to keep` - number of days to keep a full backup

- `Retention (Inc.) - no. of days to keep` - number of days to keep an incremental backup

> **Note:** If you are using Synthetic File System backup destination, you have only two options for retention:
>
> - `Retention - no. of versions to keep` - number of full backups
> - `Retention - no. of days to keep` - number of days to keep a full backup

Whichever condition is met first (either number of versions has been reached or the backup is older than the given limit), it is removed from the backup destination.

Other

This is an optional section with two switches:

- Fail the rest of the backup tasks if more than xx% of EXPORT tasks have already failed
- Fail the rest of the backup tasks if more than xx% of STORE tasks have already failed

Here are two examples of when using switches is very useful: It is very likely that if 30% of the backup tasks fail, the remaining tasks will also fail because the environment has failed. Or, if you are backing up a set of storage instances, and if even one is not secured, there is no point in backing up the rest.

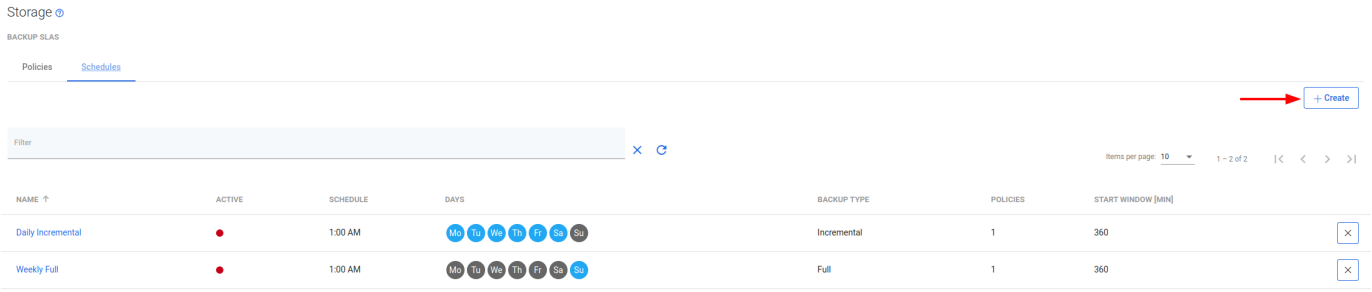
At the end, save the settings.

> **Note:** You can also perform the same action thanks to the CLI interface: CLI Reference

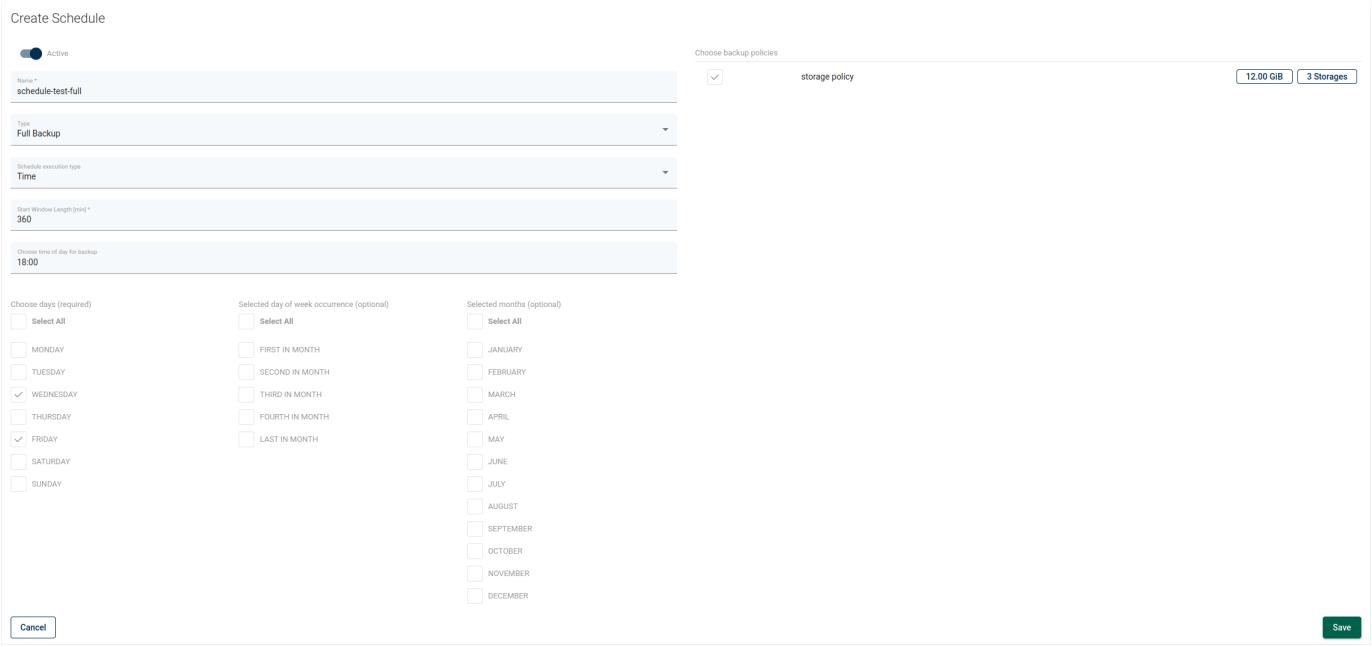
Schedules

Schedules allow you to invoke specific policies periodically. This allows you to backup multiple storage instances automatically.

A schedule defines when and on which days instances should be backed up. To define a new schedule, open Backup SLAs under the Storage section and go to the Schedules tab, then use the **Create** button.



Now enter the properties:



- `Schedule Active` - enable or disable executing schedule
- `Name` - schedule name
- `Backup Type` - defines backup type: full or incremental
- `Execution Type` - choose time or interval mode
- `Start Window` - defines for how long since the task start time scheduled tasks are allowed to be executed
- `Choose time of day` - for the time execution mode, this defines when the task should be added to the queue
- `Choose time of interval start` - for the interval execution mode, this defines when tasks should start
- `Choose time of interval end` - for the interval execution mode, this defines when tasks should end
- `Frequency` - defines how often the task will be executed during the interval
- `Choose days` - last required parameter, select days of the week on which the task will be performed

You can also use optional parameters to further personalize the backup time or select a storage instance policy if it has been previously created.

> **Note:** You can also perform the same action thanks to the CLI interface: CLI Reference

Snapshot SLAs

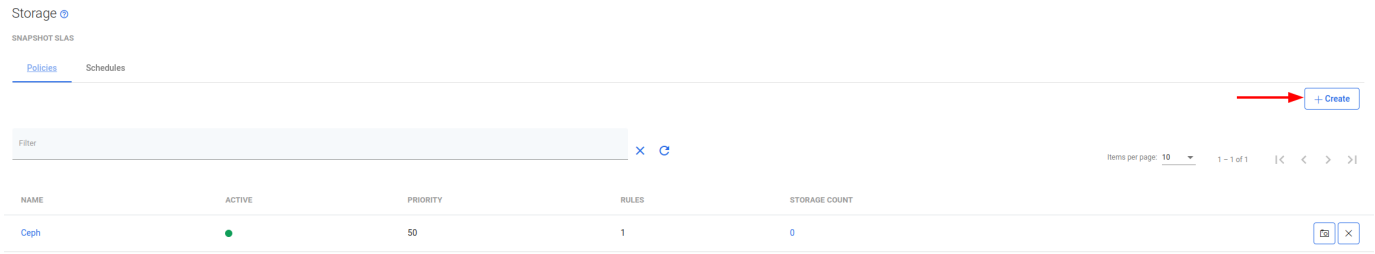
Data Protector for Cloud Workloads can periodically create snapshots and keep several of them for every Storage Provider instance. To see which Storage Provider support this feature please go to SData Protector for Cloud Workloads Support Matrix.

> **Note:**
> Snapshot management for on-demand or scheduled operations is not available until the storage instance has a snapshot management policy assigned to it

Policies

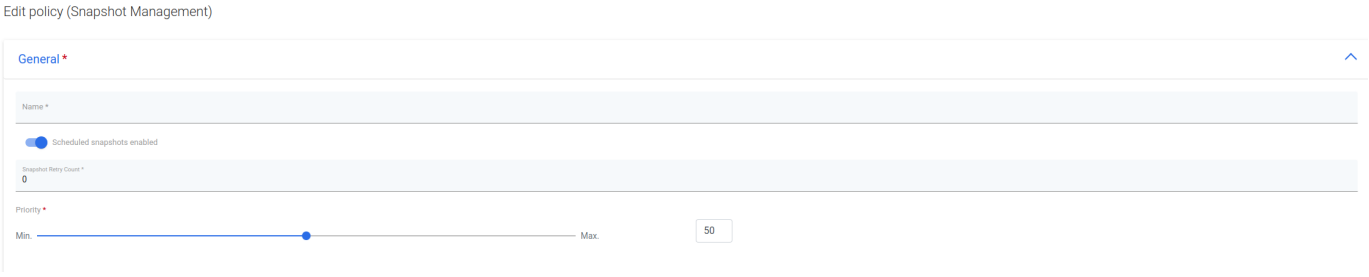
In order to enable snapshot management for Storage Instance you need to do the following steps:

Go to Snapshot SLAs under the Storage section and create a new Snapshot Management policy:



As well as other types of Policies, you'll also find 4 main sections here:

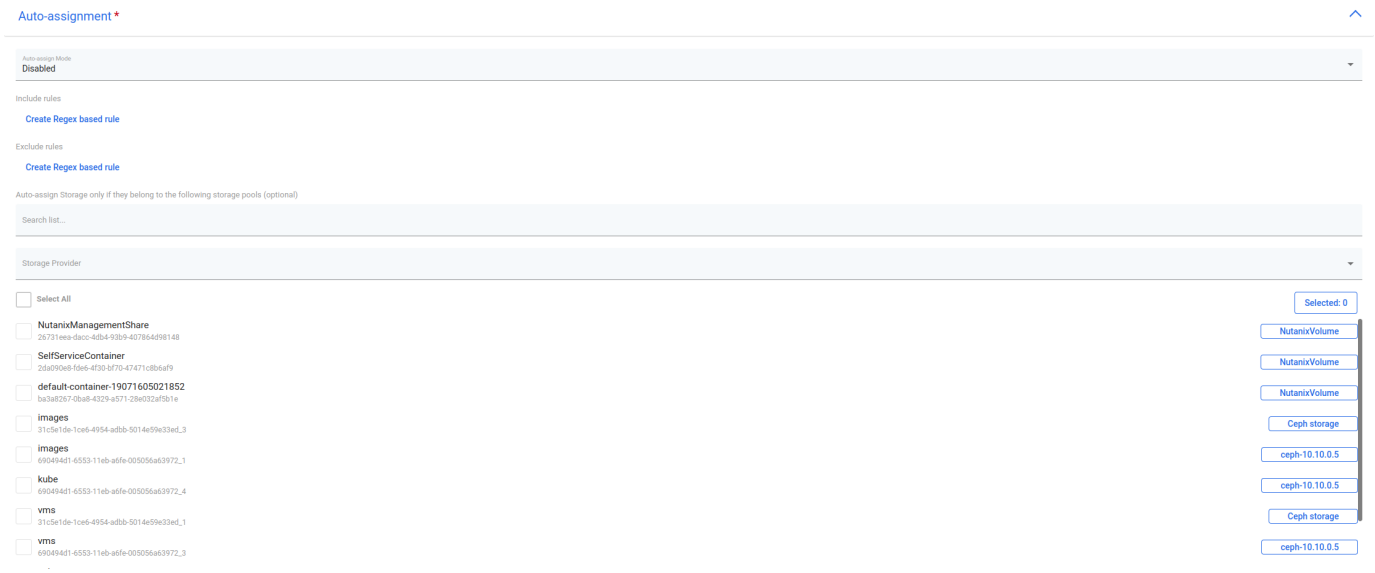
General



Under this section you can set up:

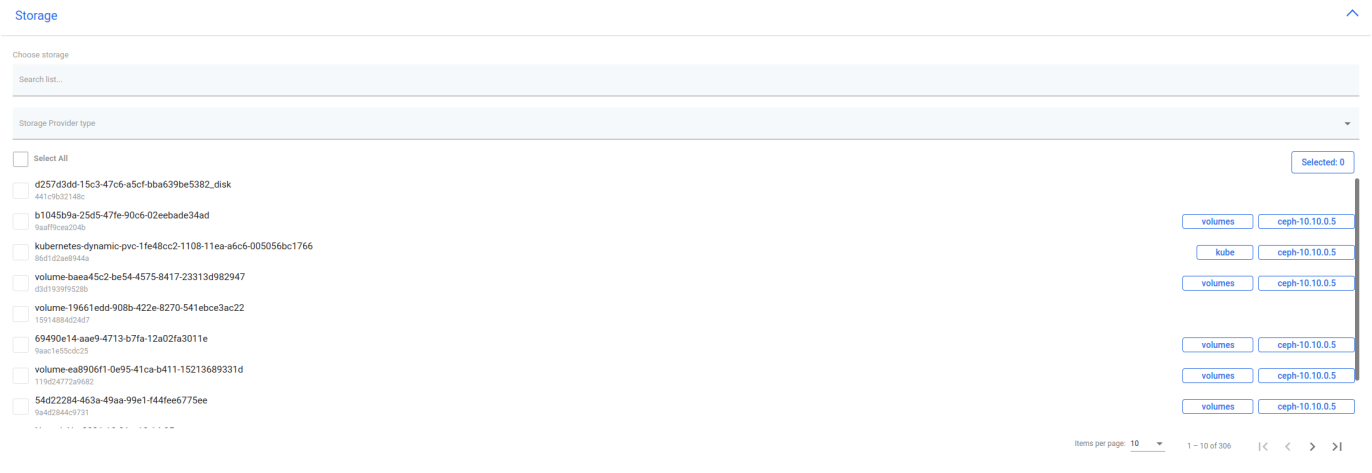
- Name of policy
- Enable/disable this policy
- **Snapshot Retry Count** - how many times, Data Protector for Cloud Workloads will try to repeat the snapshot task
- Set priority for the task

Auto-assignment

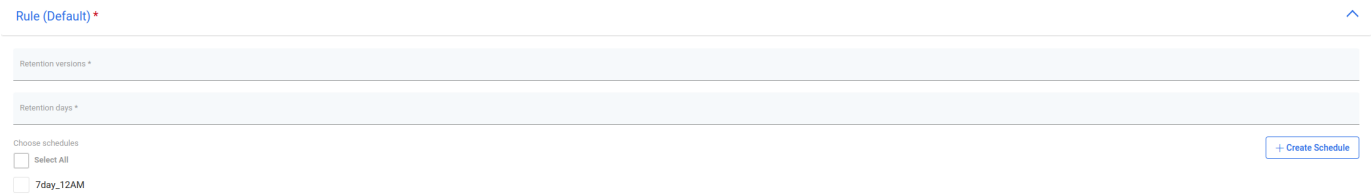


In this section you can set up:

- Mode
  - Disabled
  - Assign only
  - Assign and remove
- Include or exclude rules based on regular expression matching Storage Instance name, i.e.:
  - regular expression examples:
    - **.*** match any character any number of times
    - **storage-[0-9][0-9][0-9]** - match name that starts with storage- and 3 digits
    - **(prod|uat|dev)-[0-9][0-9][0-9][a-z]?** - match the name that starts with prod or uat or dev prefix, then -, then 3 digits and optional lower-case letter (matching is case-sensitive)
  - exclude rules always take precedence over include rules
  - Storage Instances may not be reassigned to the different policy if they already have a matching policy assigned
  - Storage Instances may be reassigned to the different policy only if mode is assigned and remove, current policy assignment rules don't match, and other's policy rules match
  - rules are joined with OR operator, so
    - if any rule (tag or matched regular expression) excludes Storage Instance - it will be excluded
    - if no rule (tag or matched regular expression) excludes Storage Instance, and any rule (tag or matched regular expression) includes Storage Instance - it will be included
  - You can also select Storage Pools to match only Storage Instances that belong to them



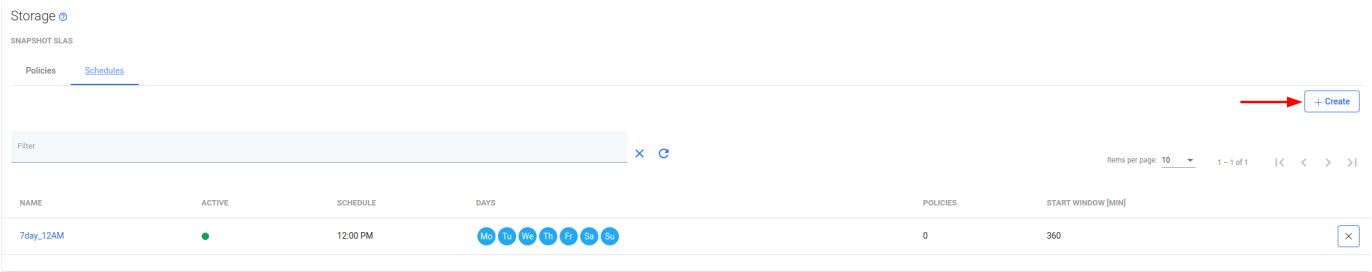
In this place, you can select storage instances manually in a simple way.



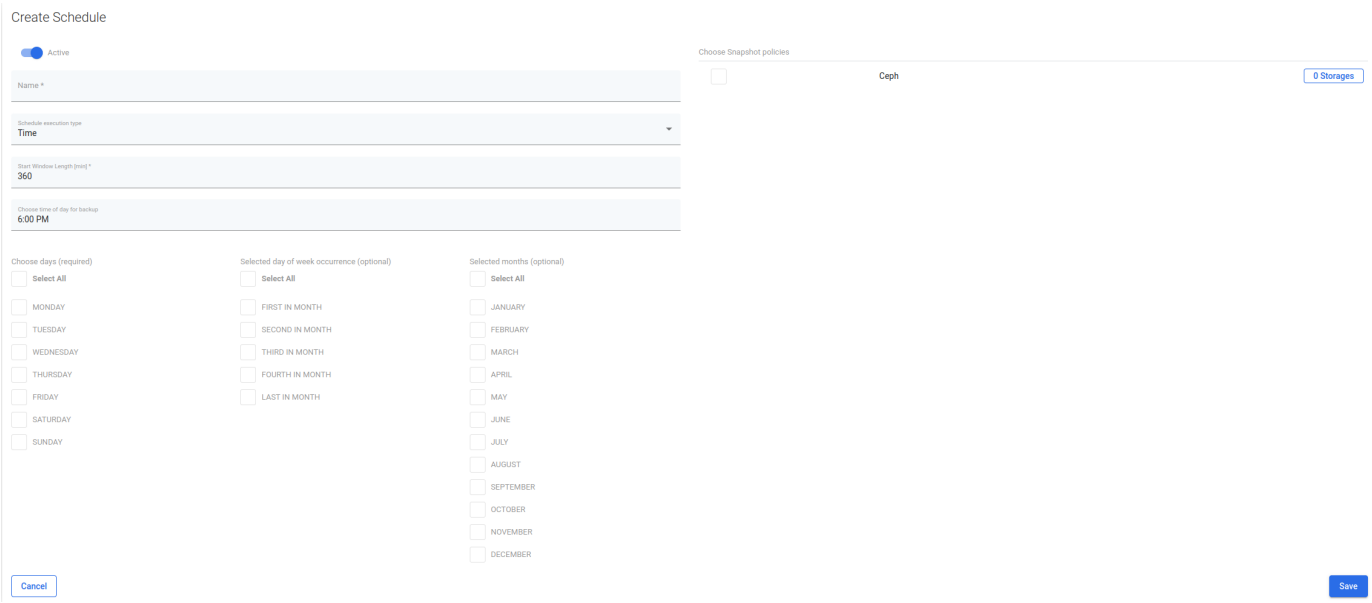
Provide retention settings - how many snapshots (created by this policy) will be kept and for how long. If you have already created a schedule, you can also select it. You can also create another rule with different retention settings with different schedules.

Schedules

The schedule defines when and on which days snapshots should be created. To define a new schedule click Create Schedule button.



Now provide properties:

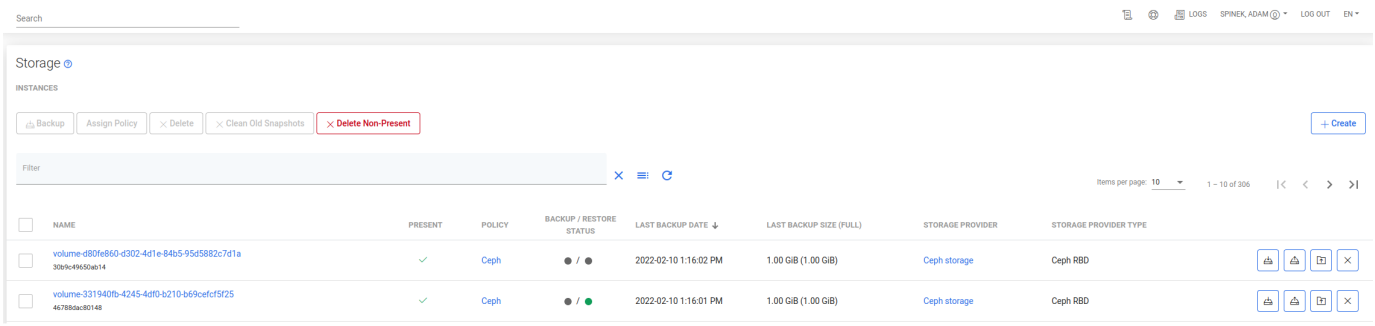


- Schedule Active - enable or disable executing schedule
- Name - schedule name
- Execution Type - choose time or interval mode
- Start Window - defines for how long since task start time scheduled tasks are allowed to be executed
- Choose a time of day - for time execution mode defines when the task should be added to the queue
- Choose a time of interval start - for interval execution mode defines when tasks should start
- Choose a time of interval end - for interval execution mode defines when tasks should end
- Frequency - defines how often the task will be executed during the interval
- Choose days - last required parameter, select days of the week on which the task will be performed

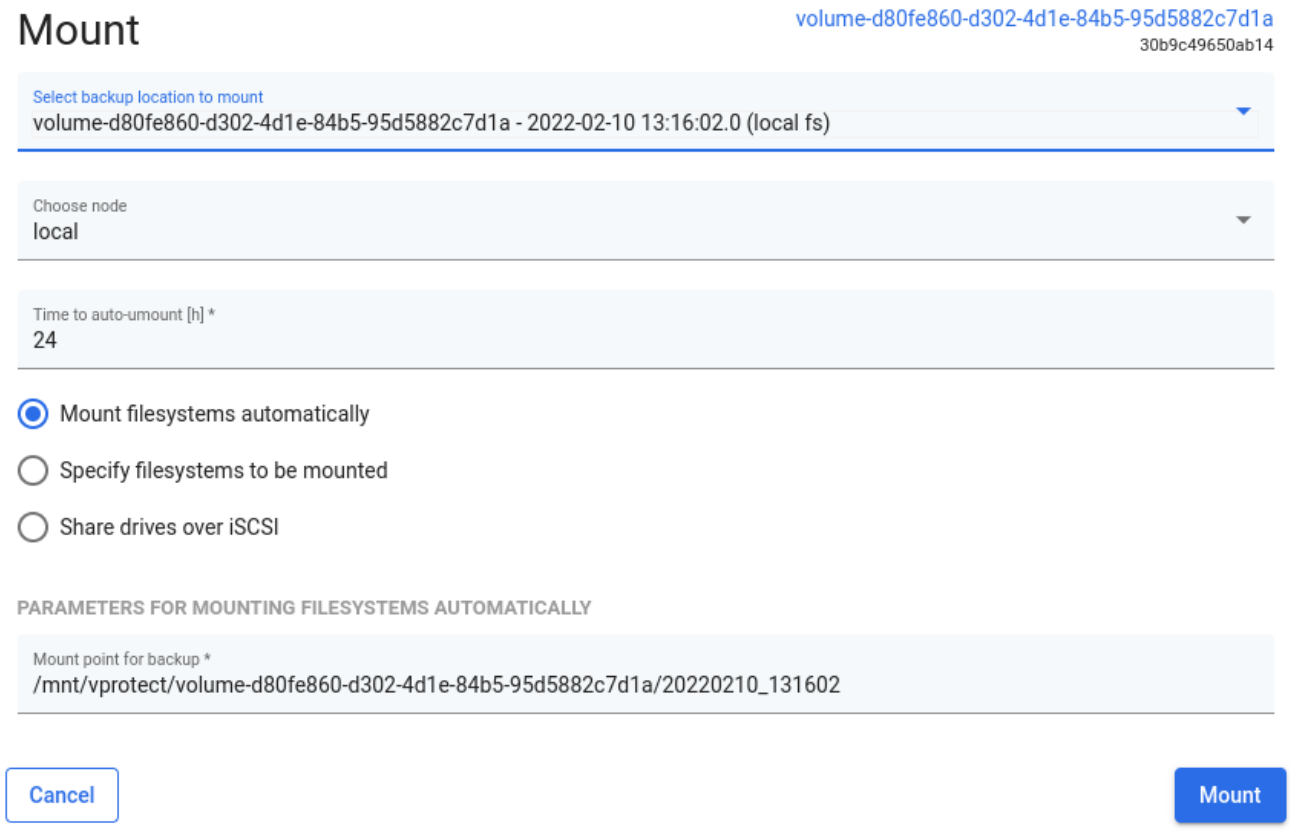
You can also select a Storage Snapshot policy if it has been previously created

Mounted Backups (File-level Restore)

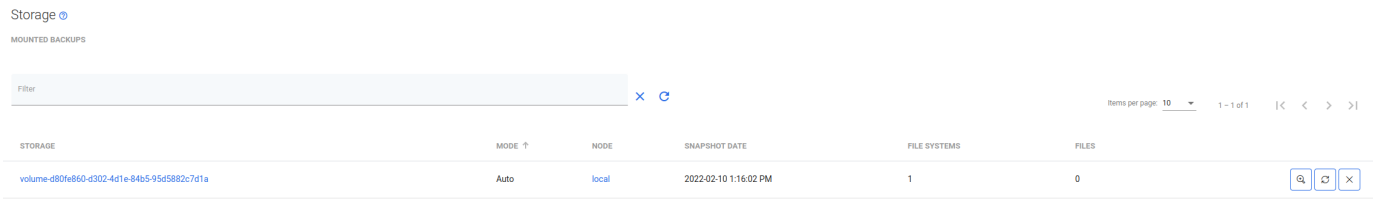
To mount backup, go to the Instances tab under the Storage Providers section on the left side menu, then click on the mount icon next to the chosen storage instance



In the popup window, you can select which backup you want to mount and on which node.



The Mounted Backups tab shows mounted storage-instance backups on the Data Protector for Cloud Workloads Node.



- `Storage` - mounted instance name

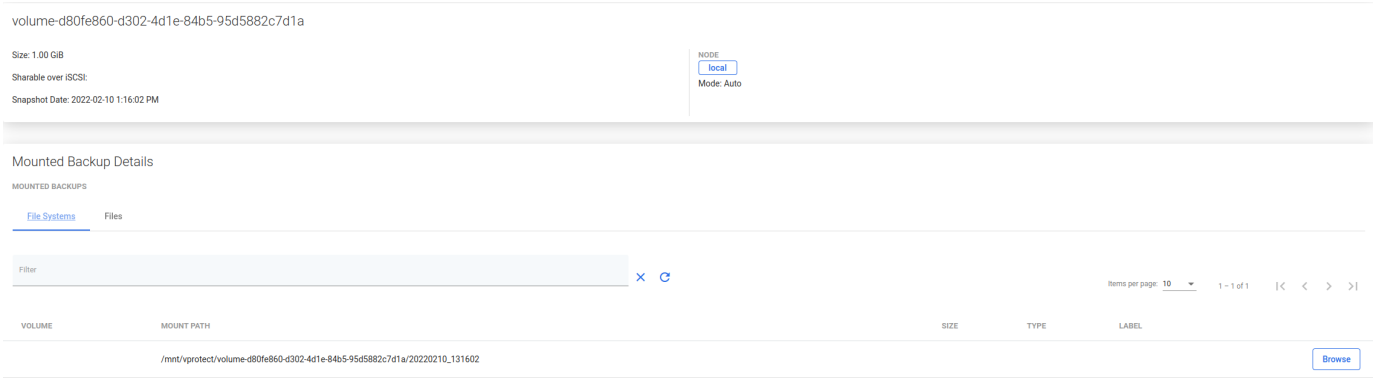
- `MODE` - Auto - Data Protector for Cloud Workloads auto-detects filesystems and mounts them on the path "/mnt/vprotect/". In Manual mode, the user chooses the mount point for selected filesystems.
- `NODE` - the Data Protector for Cloud Workloads Node is responsible for the mounting job.
- `SNAPSHOT DATE` - the date when the backup was created.
- `FILE SYSTEMS` - the number of mounted filesystems.
- `FILES` - the number of mounted virtual disk images.

Next to every mounted backup you can see three buttons: To unmount backup click on

To remount backup click on

To go to the details page of mounted backup click on

On the details page, you can view basic information or you can go deeper and browse the files.



With a web browser, you can even obtain a single file from your storage instance backup.

Cloud

This section provides information about administrative tasks like:

Instances - list of currently known entities and access to the details page of each object

Service Providers - access configuration for Microsoft365 organization.

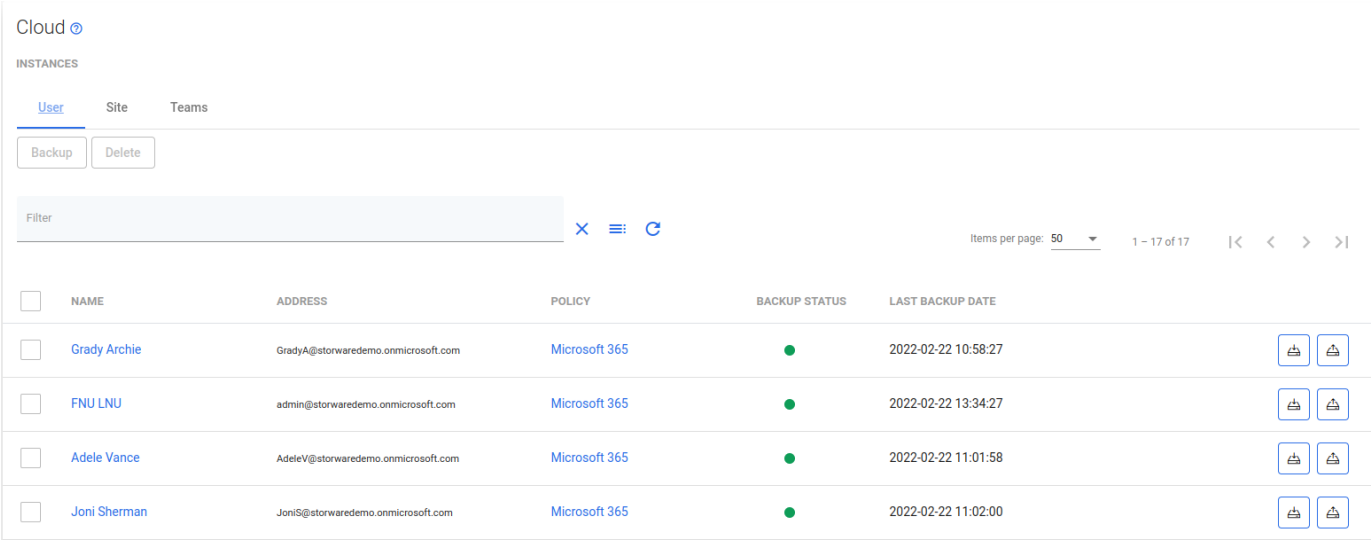
Backup SLAs - allows you to setup a correlation between protected entities, the backup destination and schedules (Policies tab). It also allows you to configure policy schedules (schedules tab).

Instances

In this view, you can see all users and sites, and teams synchronized (imported) from the defined organization (Microsoft 365)

Click **Synchronize** button on cloud service providers or use account auto-synchronization to import users or sites and teams from Microsoft 365 organization.

Switch to the **Users, Site,** or **Teams** view to see only selected instances.

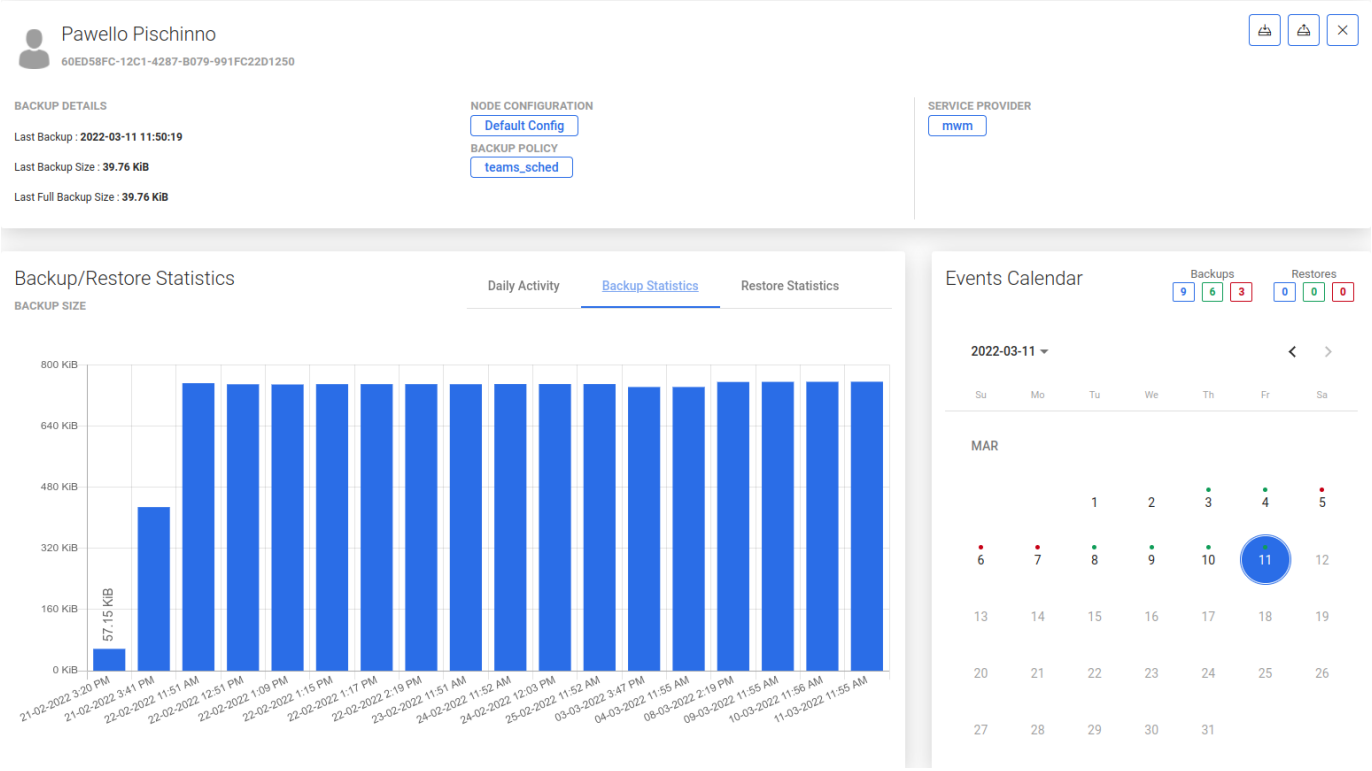


You can do the following activities on the protected entities (users or sites):

- **Backup** - to start a backup process for the selected entities
- **Delete** - to delete selected entities
- **Restore** - to restore entities data

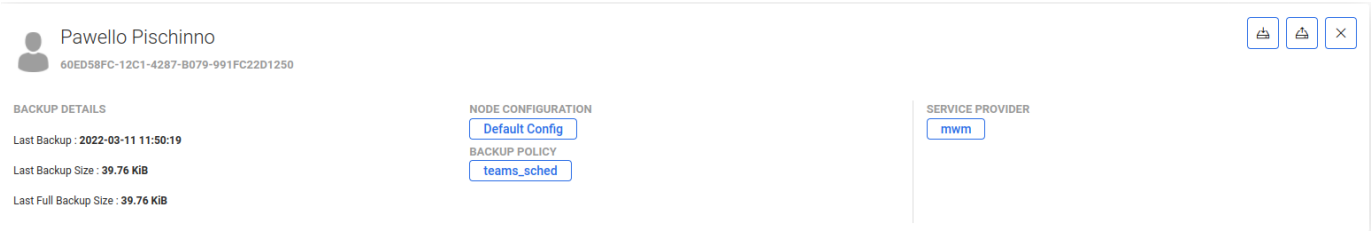
> **Note:** Go to the Backup SLAs section to learn about how to configure a backup of your organization's data.

You can go into User/Site/Teams to see the details page, this is what it looks like:



As you can see, the window has been divided into several areas:

Summary



At the top, you can see summarized pieces of information about the selected entity, such as:

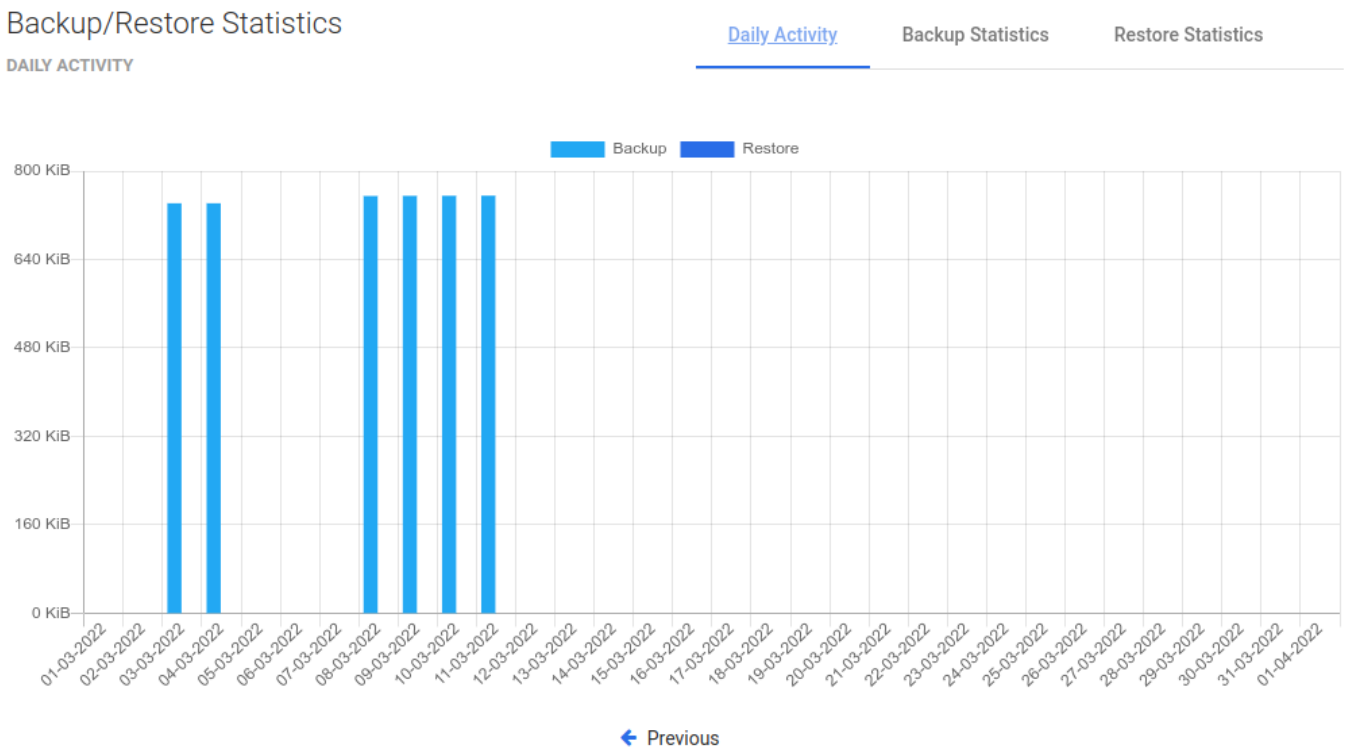
- the ID of the entity object in Data Protector for Cloud Workloads
- to which service provider belongs
- which node is assign to backup this entity
- short information about the last backup actions
- whether the entity has tags or policies assigned to it

You can also use several function buttons:

- refresh
- back to list
- change view
- backup
- restore
- delete

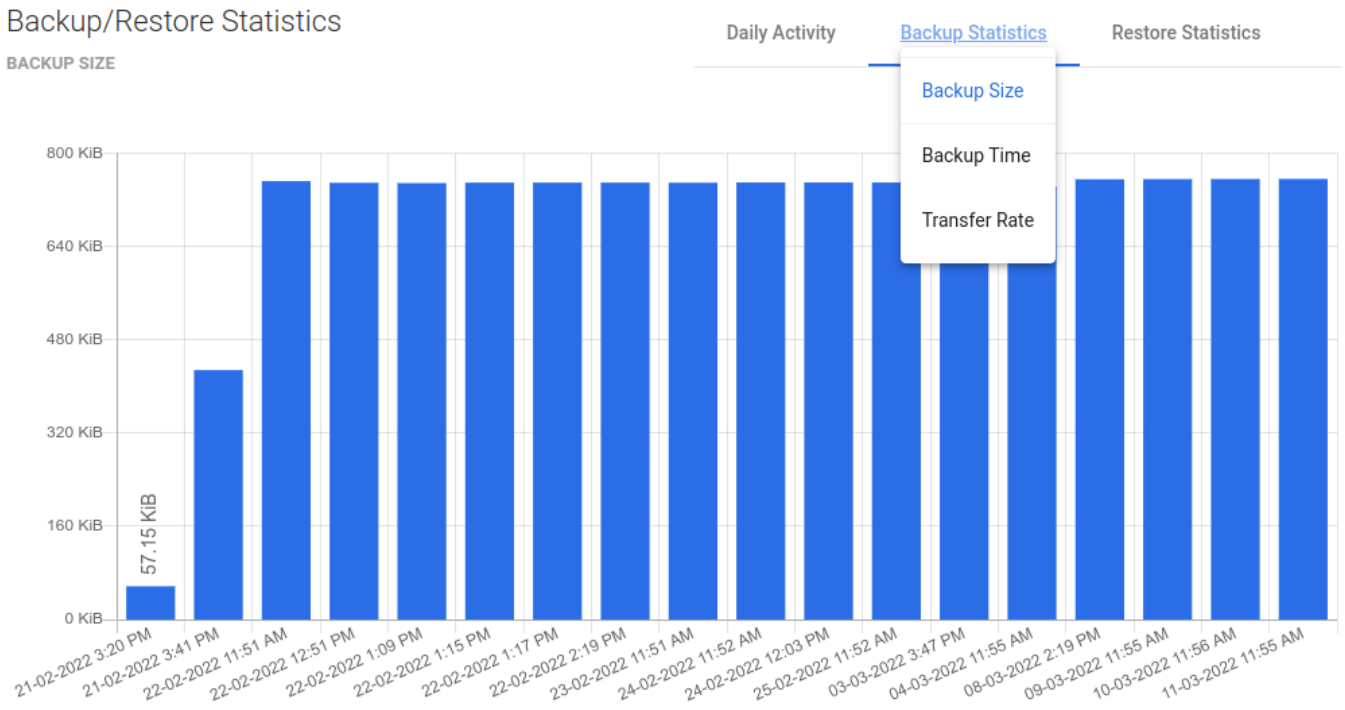
Backup/Restore Statistics

Daily activity



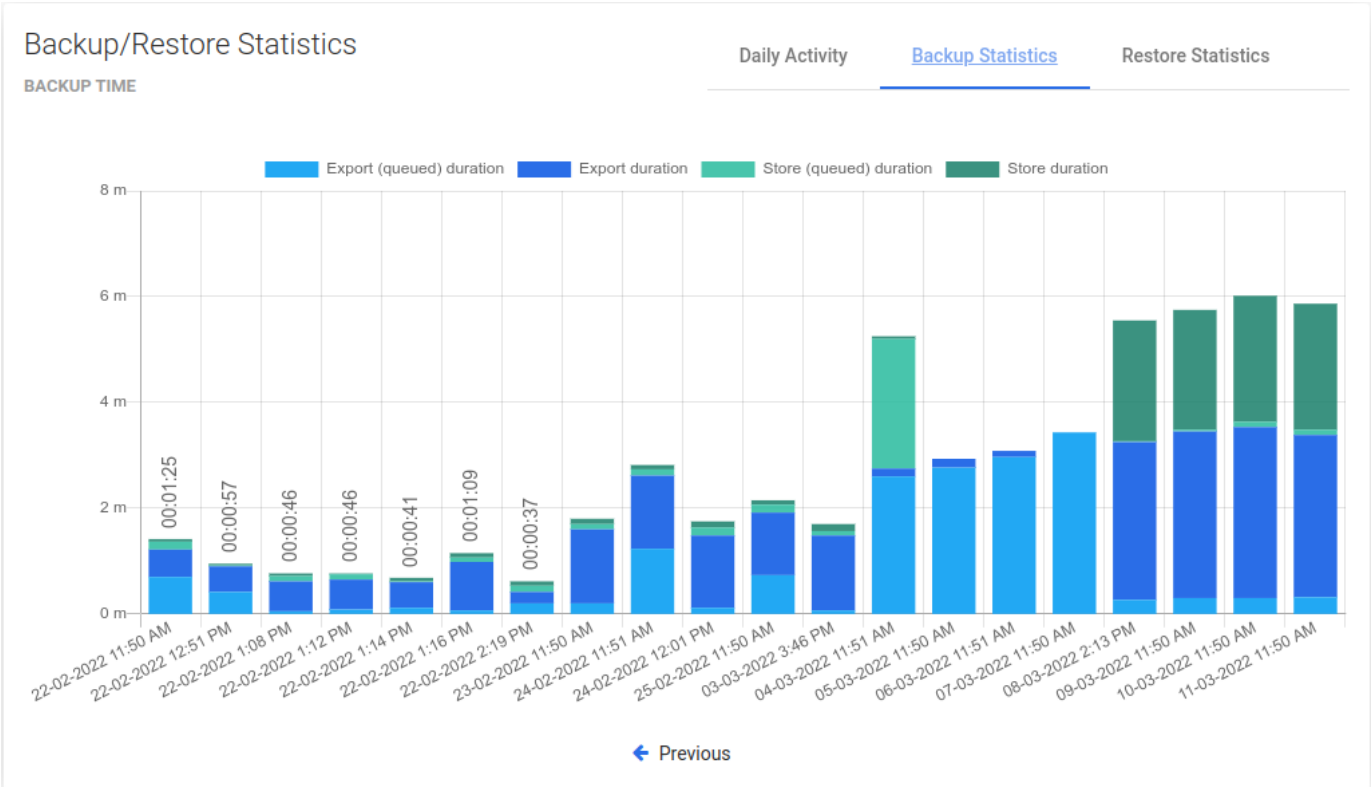
First, you'll see a daily summary of the backup and restore operations for the last month. This view is called "Daily Summary" and is the default view. You can switch the report between four views.

Backup Size



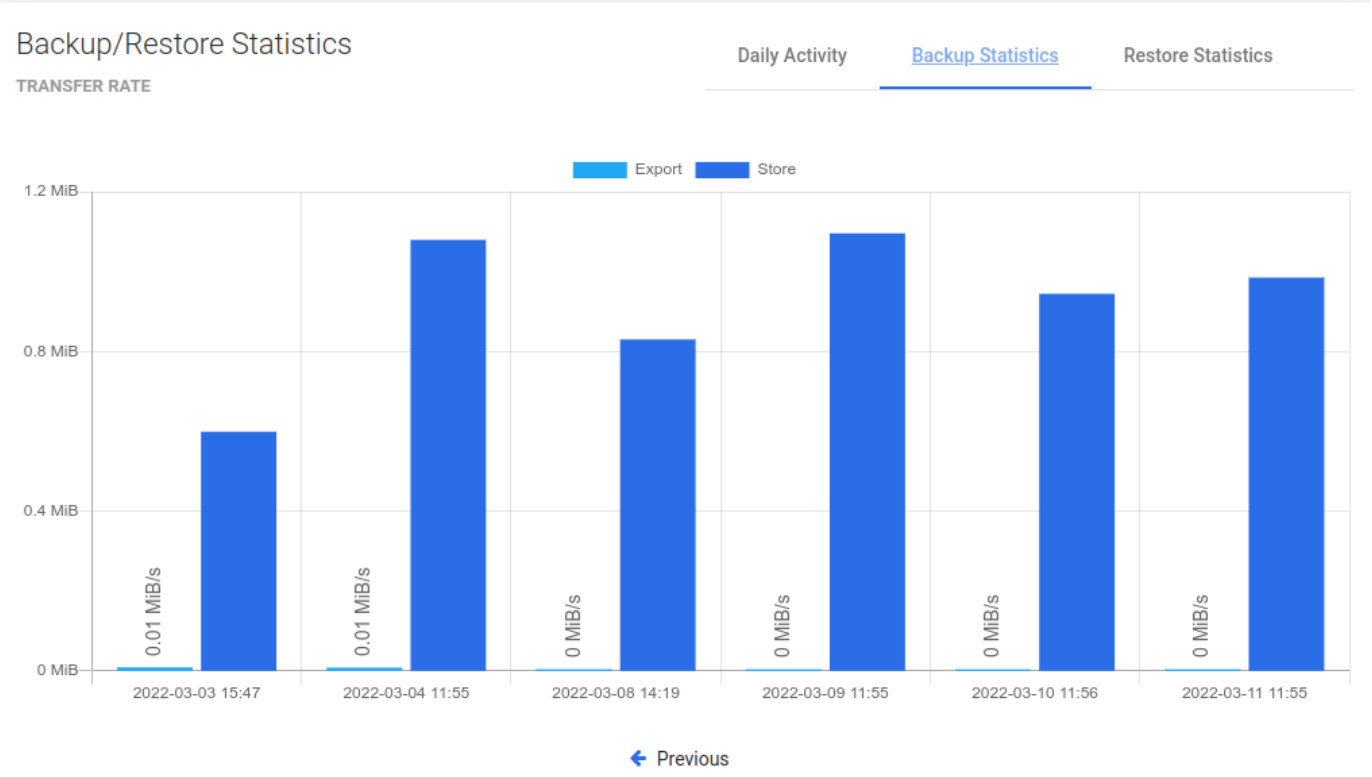
This view shows separate columns for each backup made to the virtual machine. Thanks to this, you can easily determine what data increase.

Backup Time



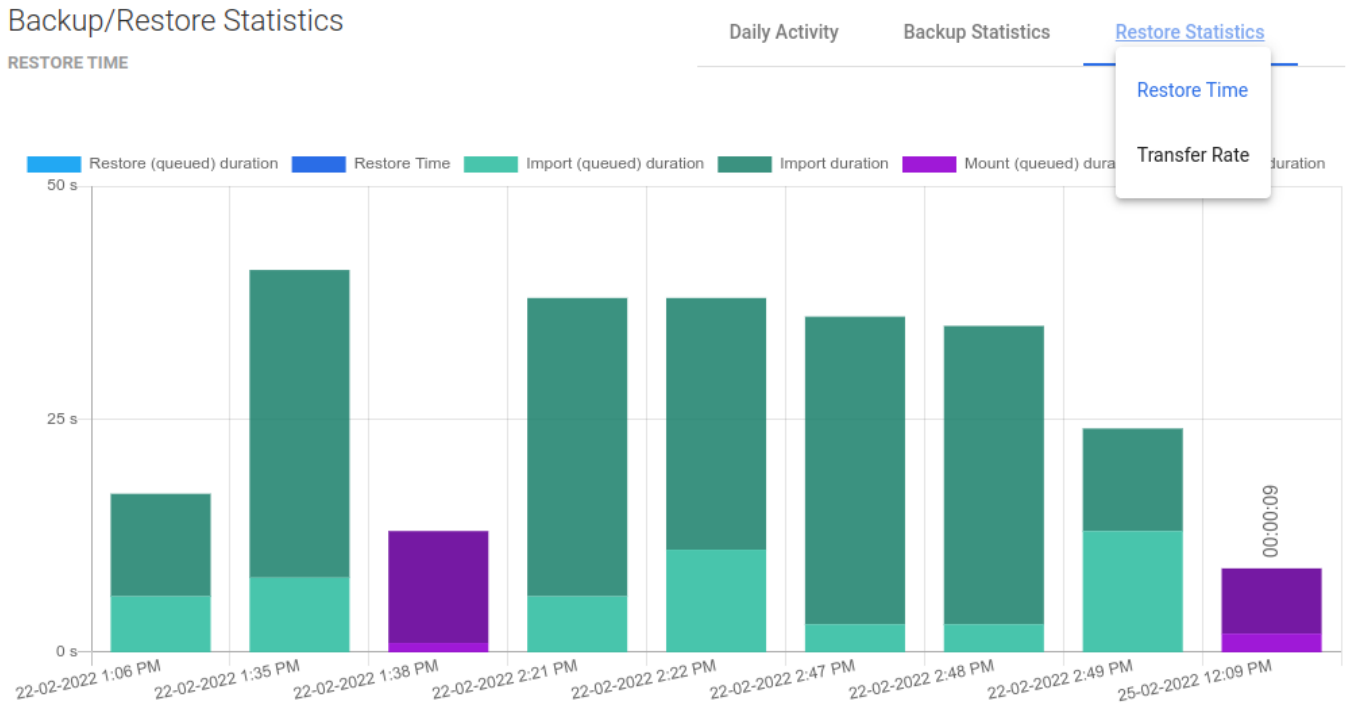
A very useful report. It allows you to determine the required window length for backups or, based on the time of individual phases, it is easy to deduce the cause of slow backups.

Transfer Rate



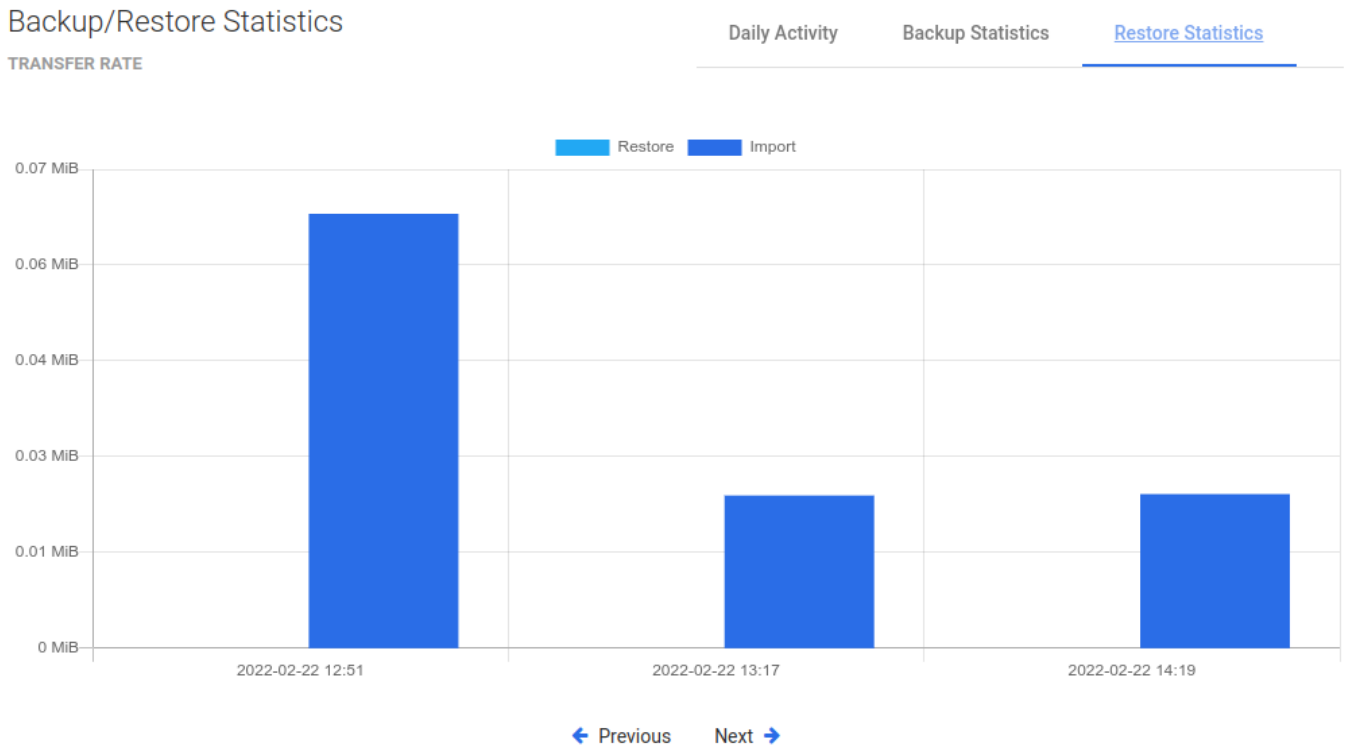
One of the latest reports, now you can easily see how fast data transfer is.

Restore Time



A view with the same properties as "Backup Time". It allows us to estimate how long it will take to restore the machine in the event of a failure.

Transfer Rate



As in the previous case, we also have the transfer speed for the restore job.

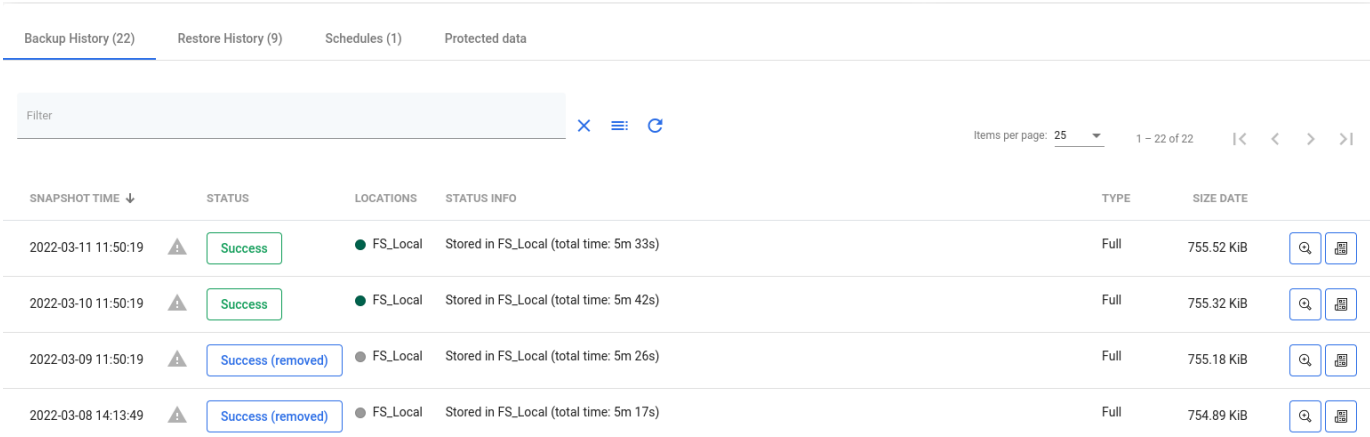
Events Calendar

The calendar extends the possibilities of adjacent statistics. It allows you to neatly define the range of days you want to see, additionally makes a quick summary of the number of backups and restores (top right corner).
Blue - the sum of all backups, **Green** - the sum of successes, **Red** - the sum of failures.

Bottom menu

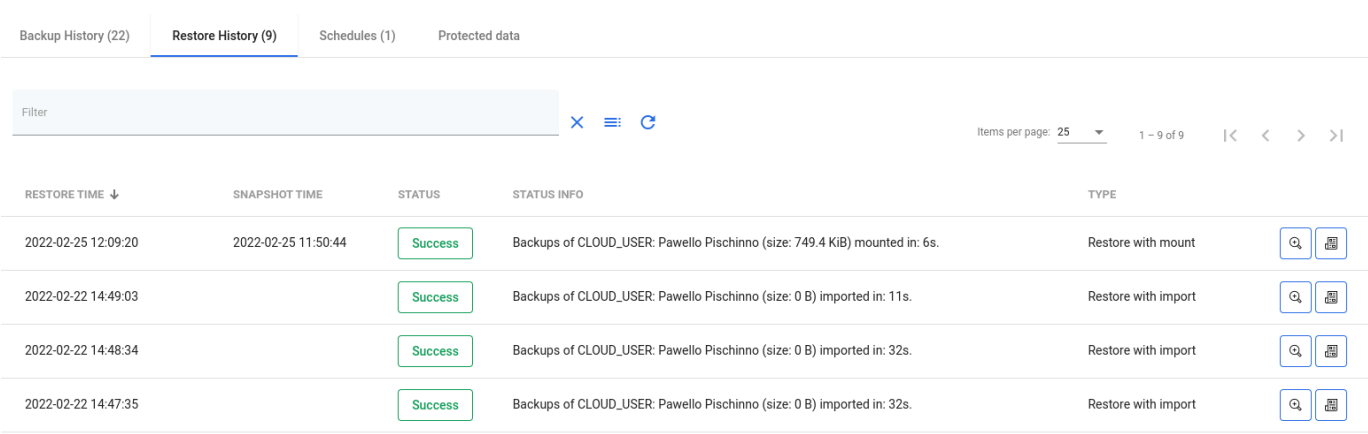
In the bottom menu, you can find a large number of tabs, each of which will present different information or will allow you to restore one or more objects from the selected user, site, team.

Backup History



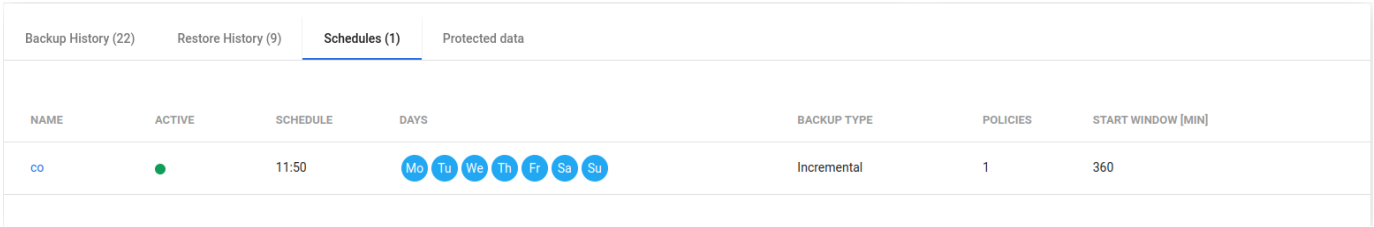
This tab shows information about all backups made, as well as information about failed, removed (because of retention), or currently executing backups.

Restore History



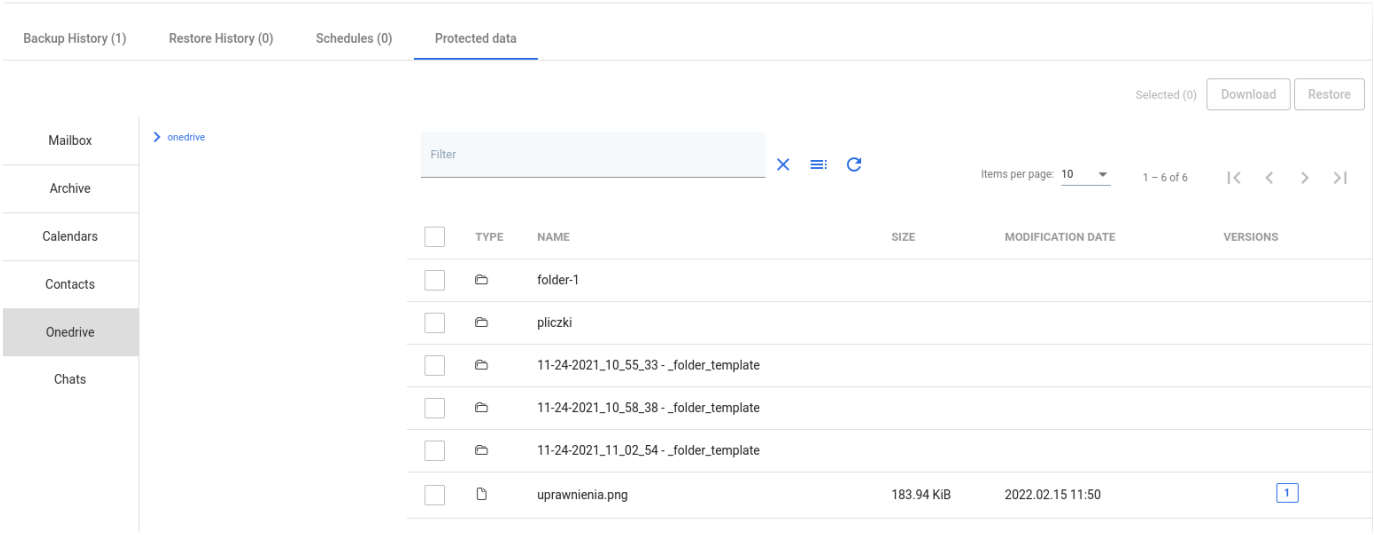
This tab is similar to "Backup History". This is a list with basic information about restores performed. When you open the details of the selected restore, you will see more detailed information.

Schedules



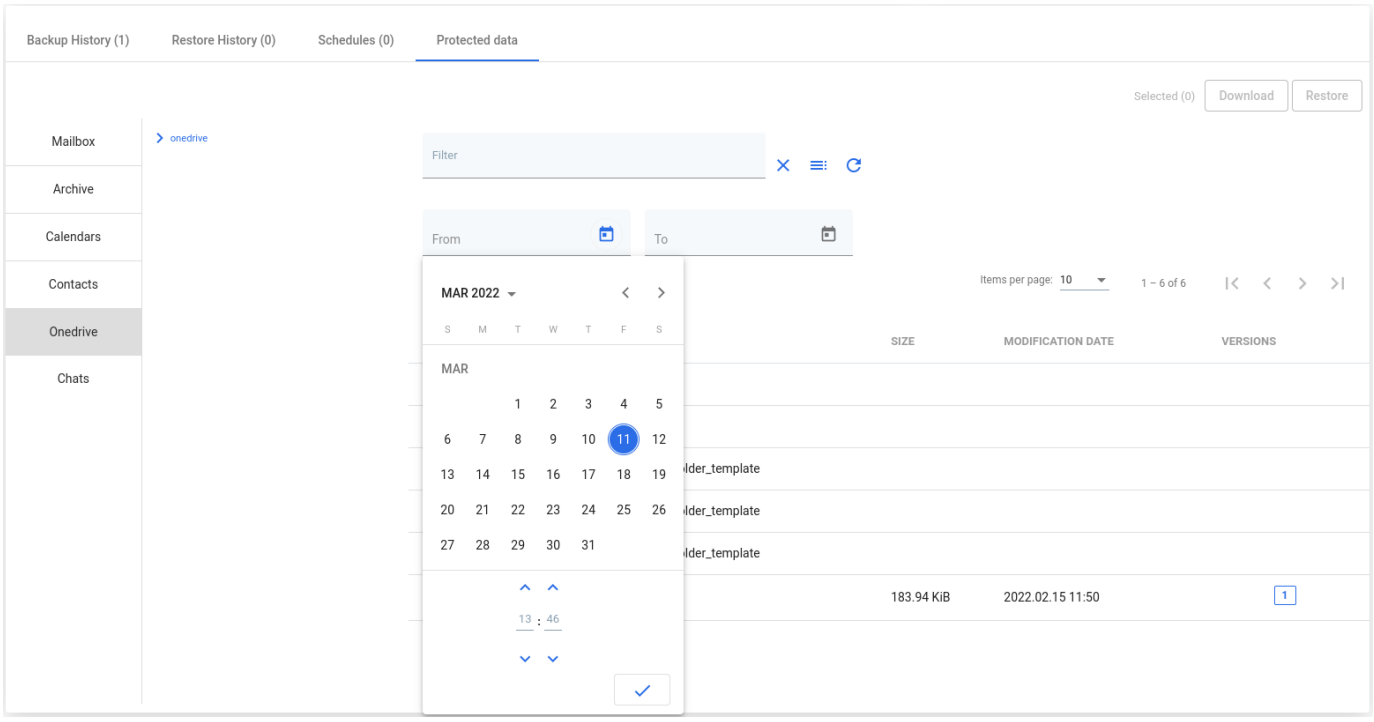
In this tab, you can see all the schedules assigned to this entity.

Protected data



In this tab, you can see all backup data which you can select for restore or download.

You can always use the filters to move back in time to select the exact moment from the calendar and restore or download data.



Export to PST

This feature allow you to download data and save it as PST file. Currently available only for Mailboxes.

Requirements

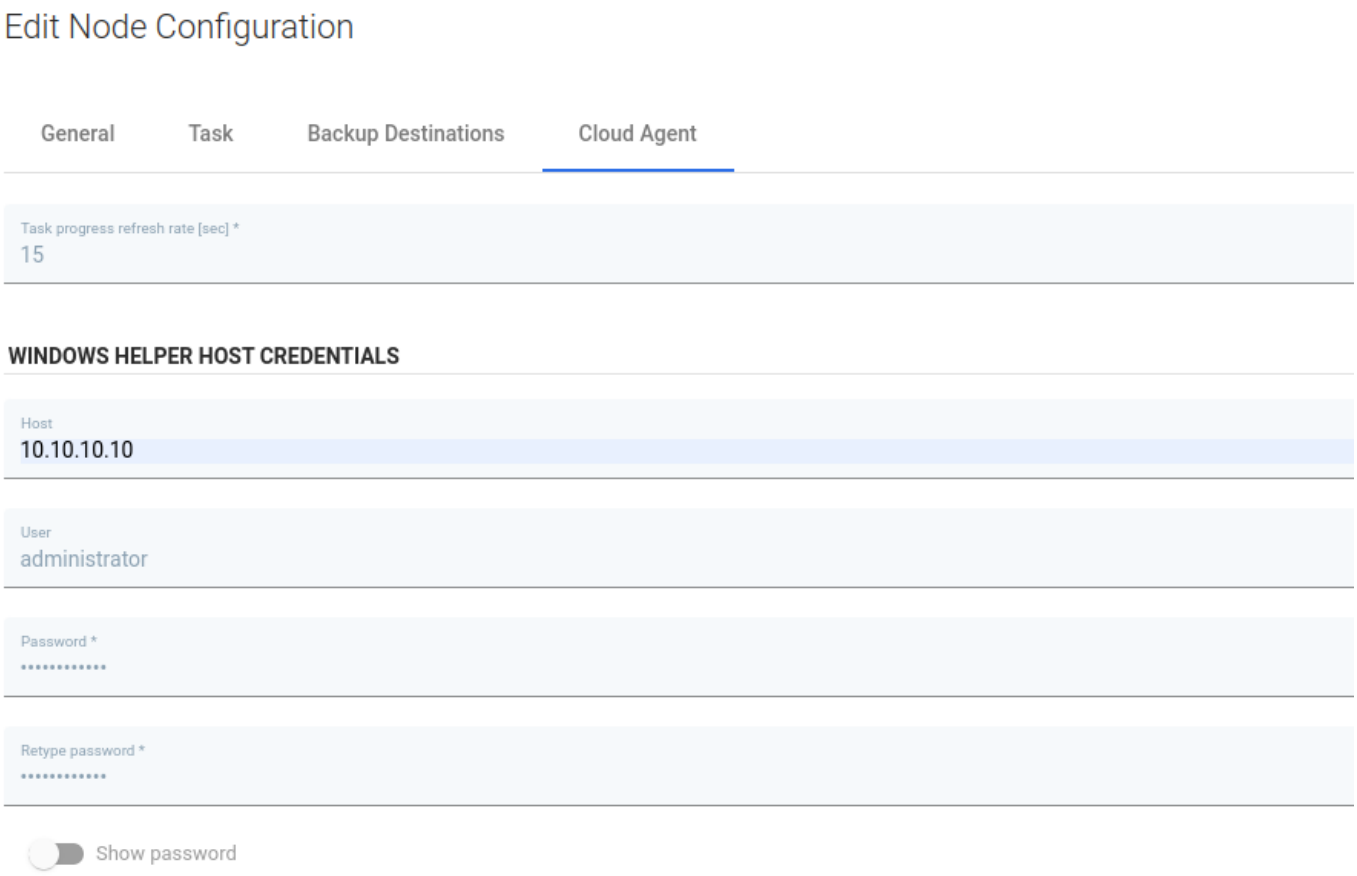
- Machine with Windows OS
- Microsoft Outlook 64-bit installed on mentioned machine

You need to enable WinRM and add firewall rules on the Windows machine. You can use ready scripts to do it. You can find these scripts in `/opt/vprotect/` directory:

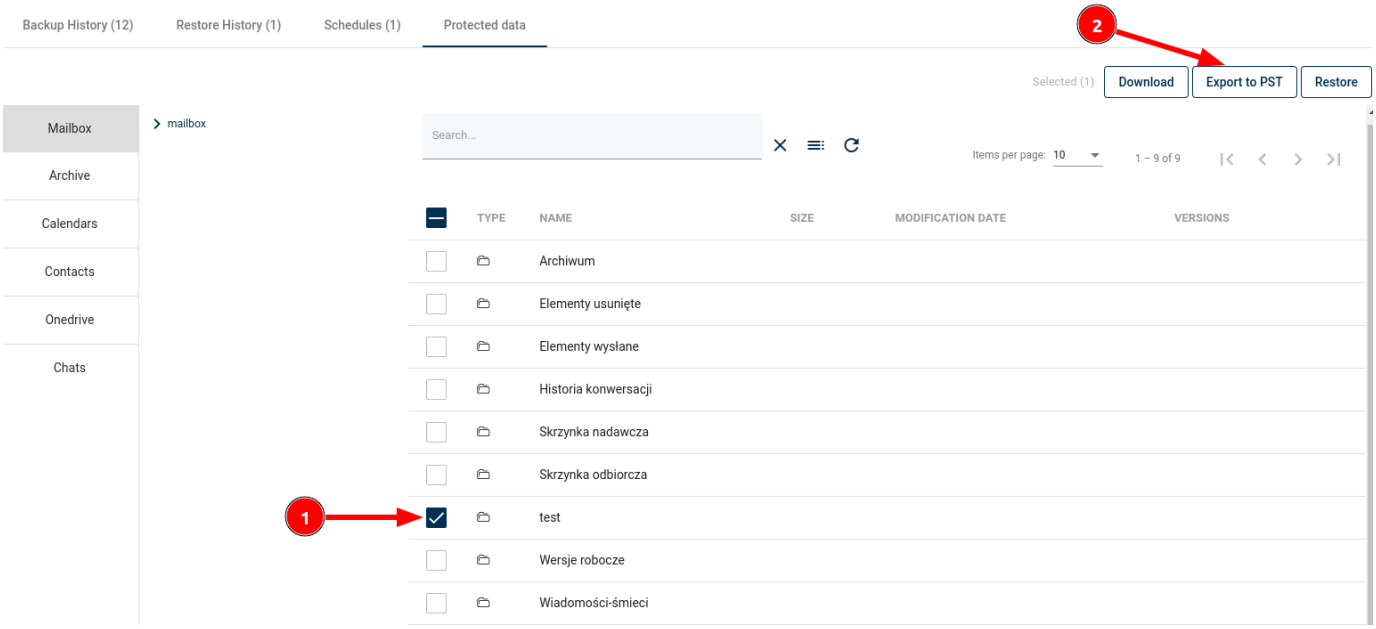
- scripts/winrm_firewall_windows.ps1 - copy from node to target Windows host and execute
- scripts/winrm.ps1 - copy from node to target Windows host and execute

Exporting to PST

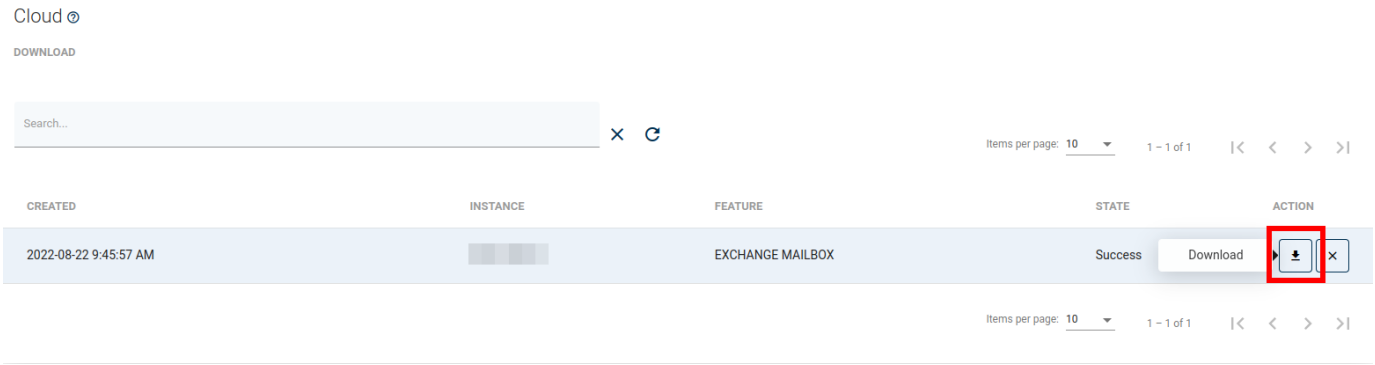
1. Go to **Nodes** -> **Node Configurations** and edit existing node configuration. Click on **Cloud Agent** tab and type access credentials to your Windows machine which will be used to generate PST.



2. In the **Protected data** tab of the selected M365 user, click on item you want to export and then click **Export to PST** button. The download task will be created.

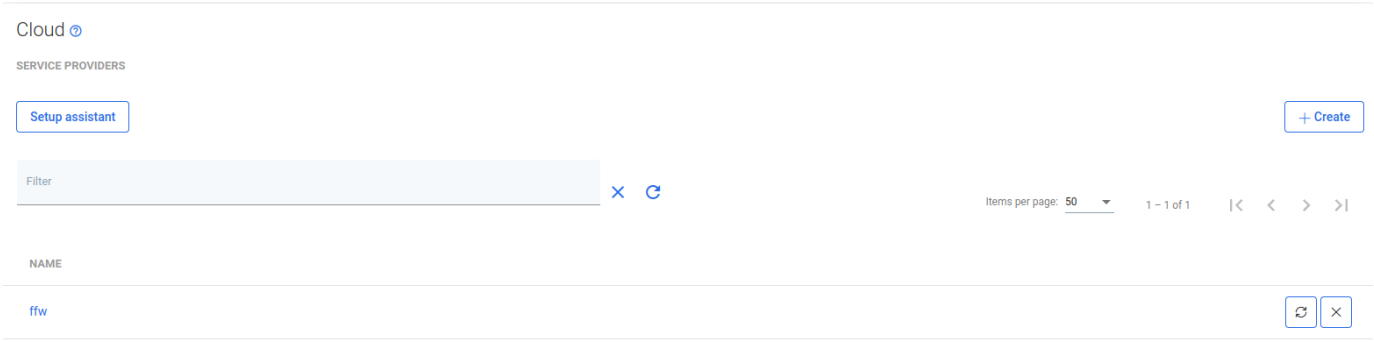


3. After download task is complete, go to **Cloud** -> **Download**. Here, click on the **Download** button to download your exported PST file.



Service Providers

On this page, you can add, edit, or delete Microsoft 365 organizations.



You can add more than one Microsoft 365 cloud service provider.

You can also on this tab do manual synchronization.

> **Note:** How to add new service providers we describe in the chapters manual or by using the setup assistant

Backup SLAs

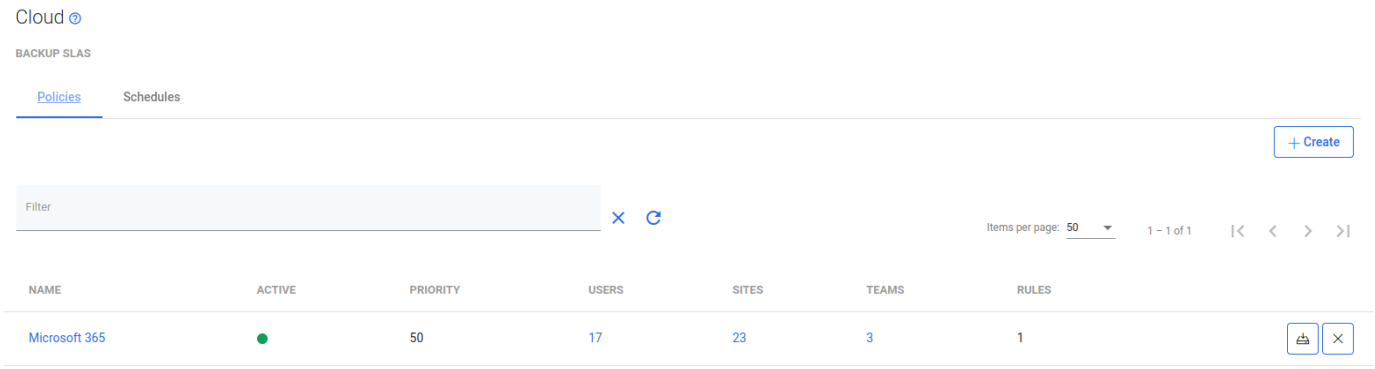
Backup SLAs policy allows you to configure the following settings:

- Set backup retention in day(s), month(s), year(s)
- Number of protected item(s) or file(s) versions
- Select the desired backup destination
- Protected Microsoft 365 services (SLA):
    - Exchange Online Mailboxes
    - Exchange Online Archives
    - Exchange Online Calendars
    - Exchange Online Contacts
    - OneDrive for Business
    - User Chats
    - Sharepoint Online
    - Microsoft Teams

If you need to add organization user(s) or site(s)to the policy go to Users, Sites, or Teams Tabs and select required instances.

> **Note:** There must be at least one Backup SLAs policy on Data Protector for Cloud Workloads Server to do a backup.

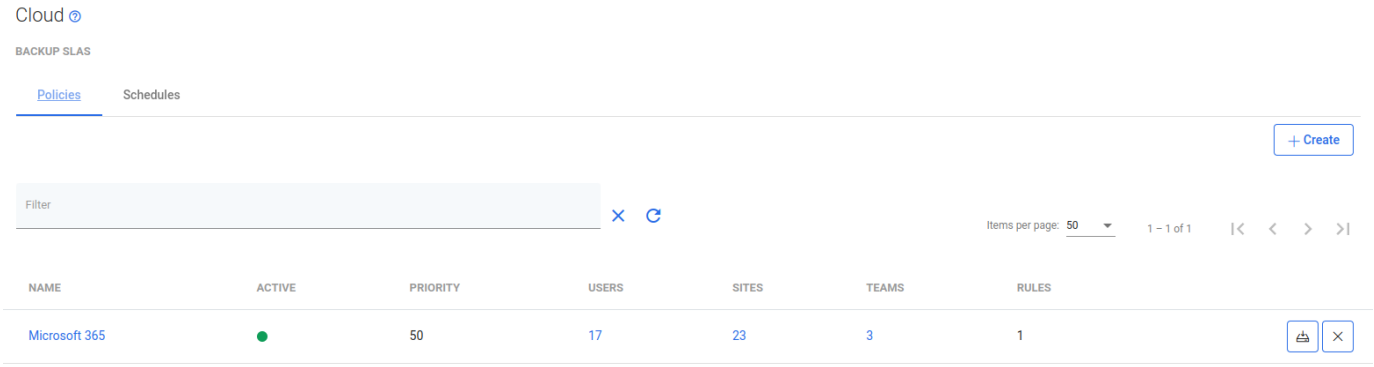
Use `Create` button to create a new policy.



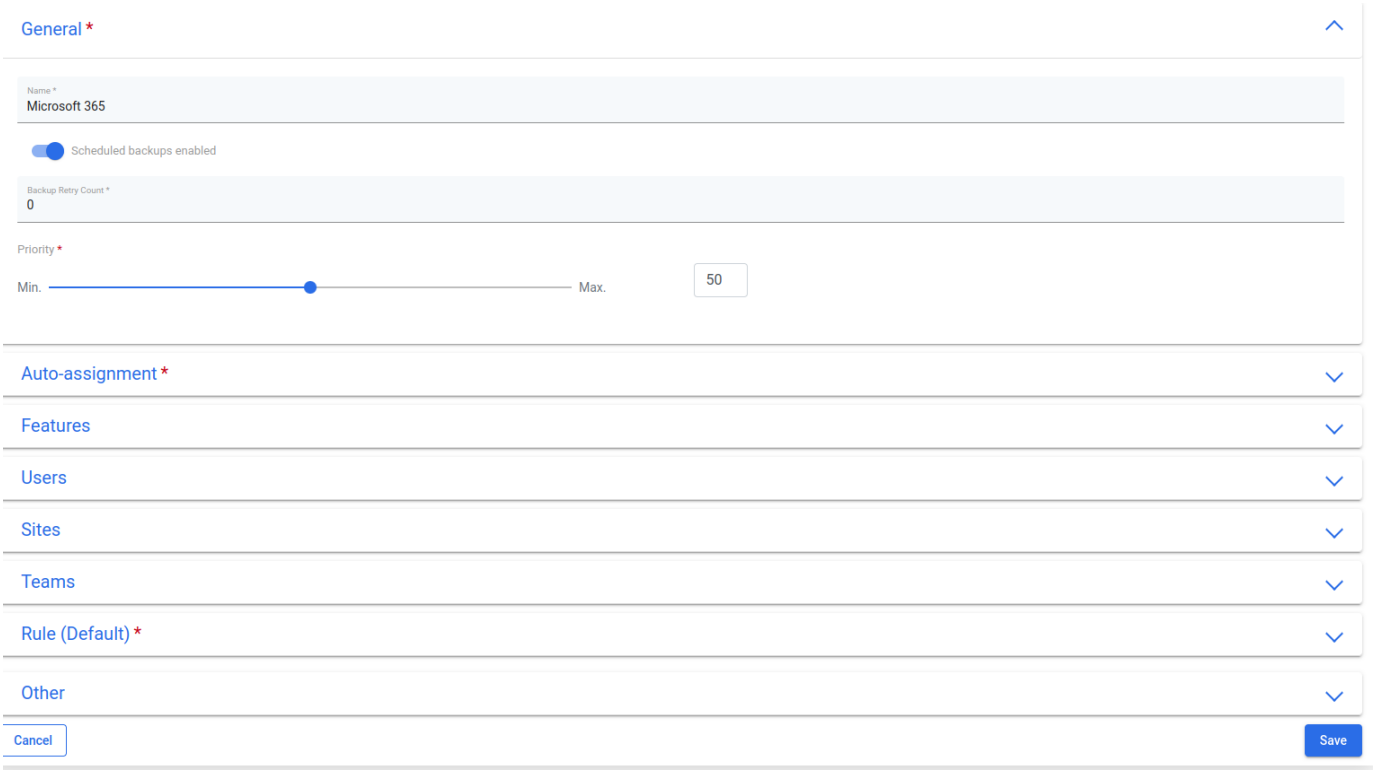
Policies

Policies allow you to group cloud instances in many ways. For example, based on the cloud features.

To create a new backup policy, please open the Backup SLAs tab under the Cloud section and click on + Create the button on the right.



Now you should see the policy wizard with 8 main sections.



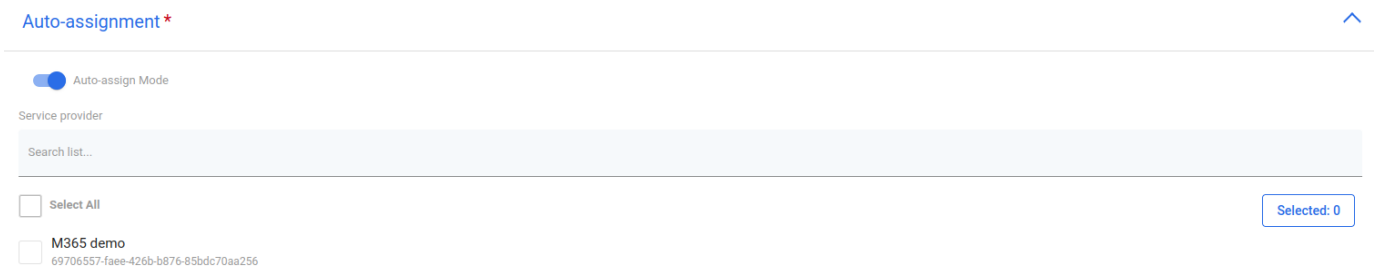
General

Under this section you can set up:

- The policy name
- Switch on/off scheduled backups enabled
- Set the priority for tasks

Auto-assignment

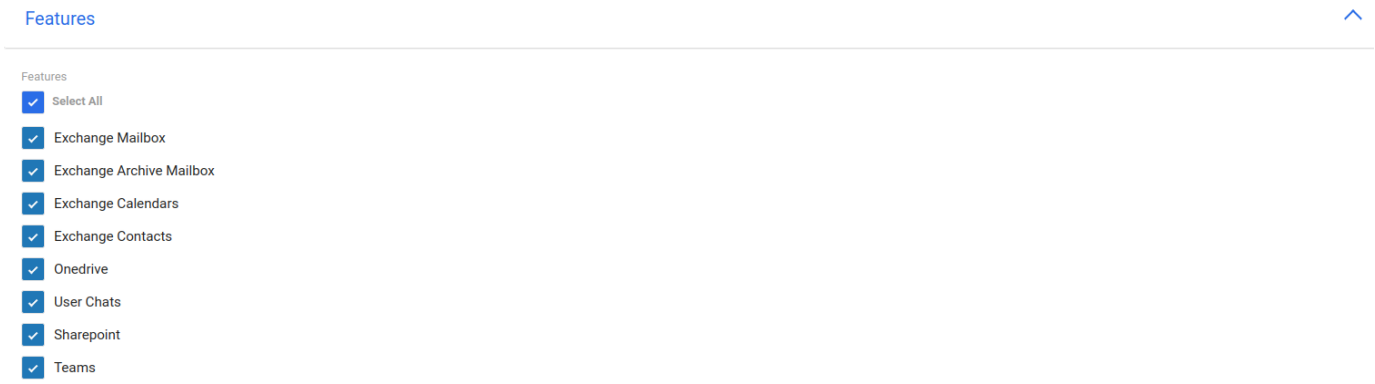
In this section, you can switch on/off automatic policy assignments to cloud service providers



> **Note:** Go to the Account auto-synchronization to learn how to synchronize Microsoft 365 accounts.

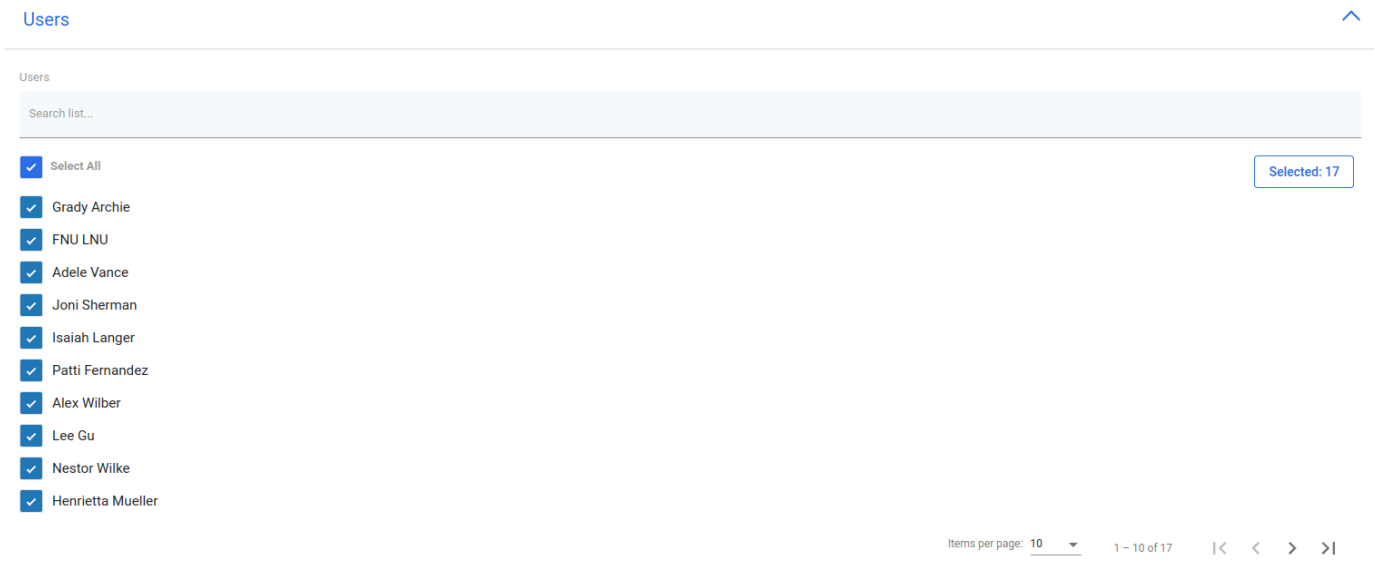
Features

Here you can easily select features that will be backup according to policy.



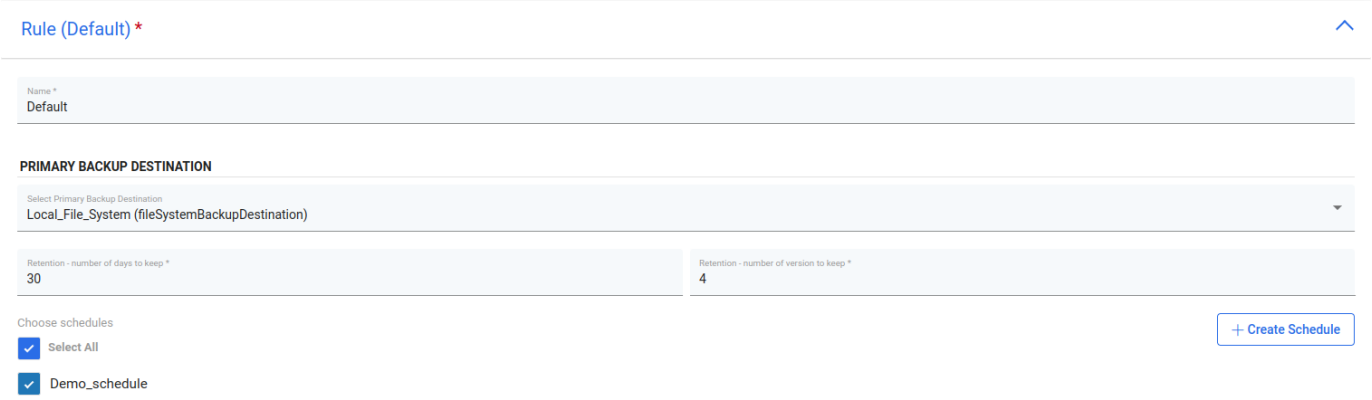
Users / Sites / Teams

These sections are used to select instances that will be protected in policy.



Rule

This section is used to select the backup destination.



> **Note:** You can use only File System, Microsoft Azure Blob Storage, Micro Focus Data Protector as a backup destination.

You can also set here **Retention** settings for your backups. You can use a number of days and versions to keep.

If you have already created a schedule, you can also select it or Create New Schedule.

Retention

Data Protector for Cloud Workloads handles retention for all backup destinations. There are 2 properties that define how long backup should be kept in the backup destination:

- `Retention - no. of versions to keep` - number of versions to keep
- `Retention - no. of days to keep` - number of days to keep

Other

This is an optional section with two switches:

- Fail the rest of the backup tasks if more than xx% of the EXPORT tasks have already failed
- Fail the rest of the backup tasks if more than xx% of the STORE tasks have already failed

Two examples when using switches is useful It is very likely that if 30% of the backup tasks fail, the remaining tasks will also fail because the environment has failed. Or you are backing up a set of machines, and if even one is not secured, there is no point in backing up the rest.

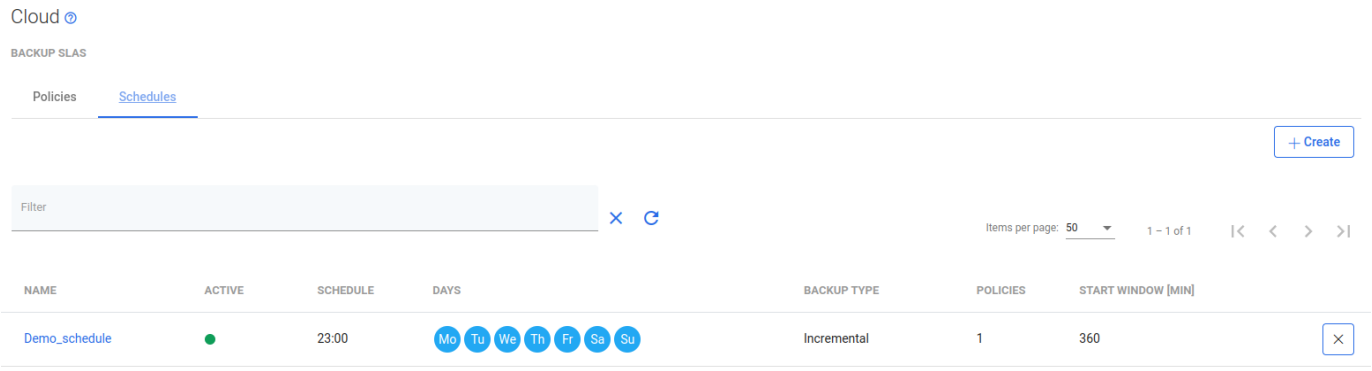
In the end, save settings.

> **Note:** You can also perform the same action thanks to the CLI interface: CLI Reference

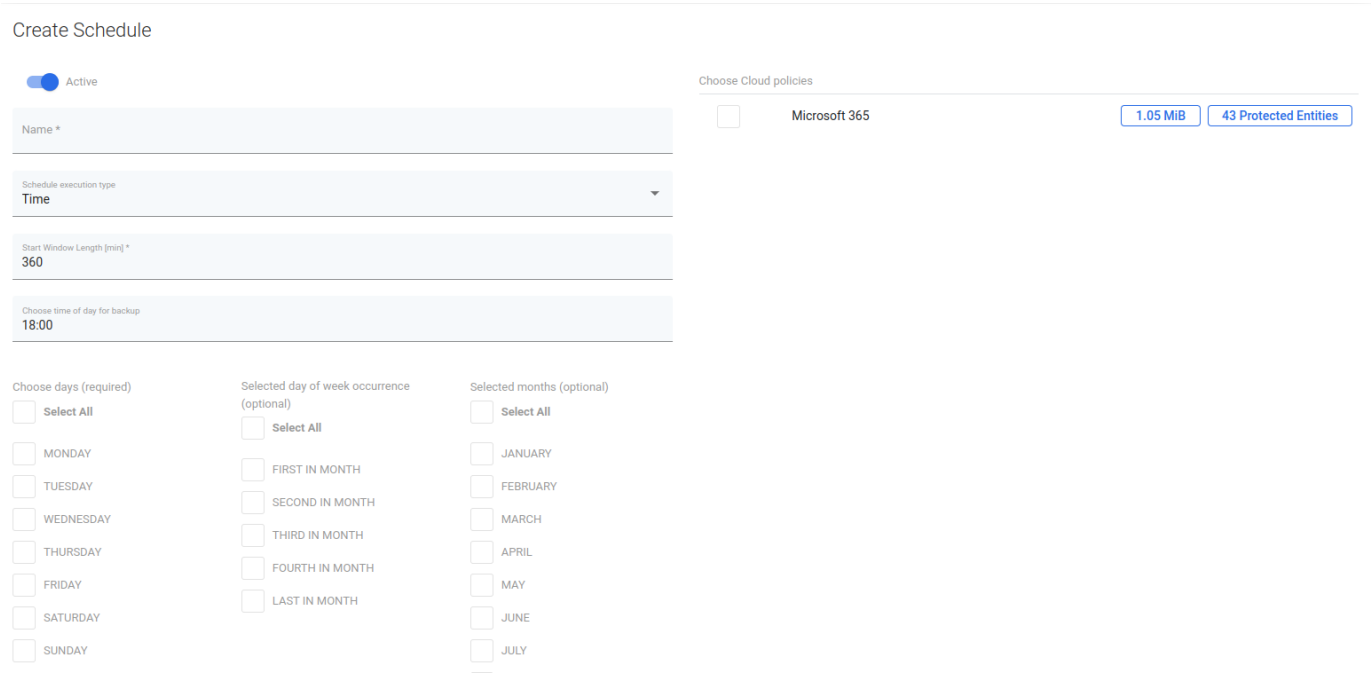
Schedules

The schedules allow you to invoke specific policies periodically. This allows you to back up multiple Cloud instances automatically.

A schedule defines when and on which days cloud instances should be backup. To define a new schedule, open Backup SLAs under the Cloud section and go to the Schedules tab, then use the + Create button.



Now enter the properties:



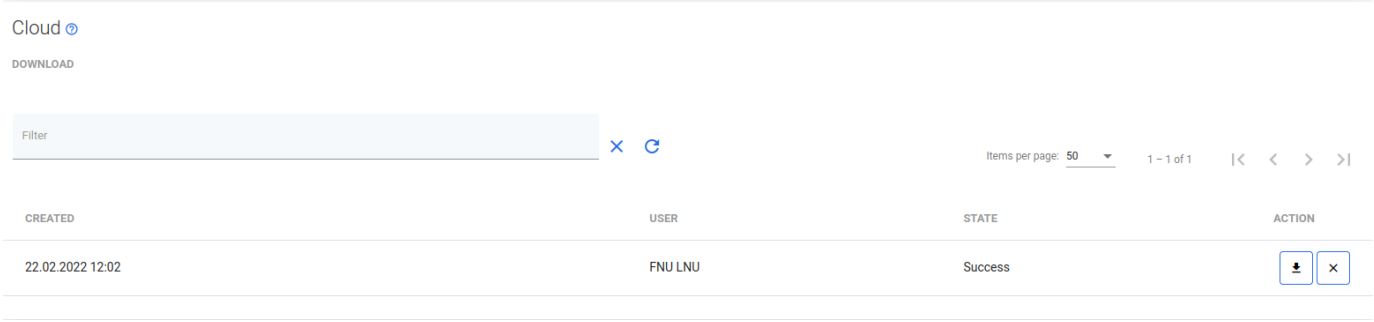
- `Schedule Active` - enable or disable executing schedule
- `Name` - schedule name
- `Execution Type` - choose the time or interval mode
- `Start Window` - defines for how long since the task start time scheduled tasks are allowed to be executed
- `Choose time of day` - for the time execution mode, this defines when the task should be added to the queue
- `Choose time of interval start` - for the interval execution mode, this defines when tasks should start
- `Choose time of interval end` - for the interval execution mode, this defines when tasks should end
- `Frequency` - defines how often the task will be executed during the interval
- `Choose days` - the last required parameter, select the days of the week on which the task will be performed

You can also use optional parameters to further personalize the backup time or select a cloud policy if it has been previously created.

> **Note:** You can also perform the same action thanks to the CLI interface: CLI Reference

Download

All downloads tasks that have been will be, or are being performed on the Data Protector for Cloud Workloads Cloud are collected in the **Downloads** view.



Here you can download the elements you selected previously and that has been prepared by the Data Protector for Cloud Workloads agent.

Applications

Data Protector for Cloud Workloads allows you to setup periodic backup with your own scripts or application-native backup commands. These can be executed either on the Node or remotely over SSH.

The Application can reside anywhere - it can be in a VM, Kubernetes deployment, or on a physical box.

> **Note:** The only requirement is to allow Data Protector for Cloud Workloads to execute a set of commands over SSH or on the node to access data remotely.

In this section are:

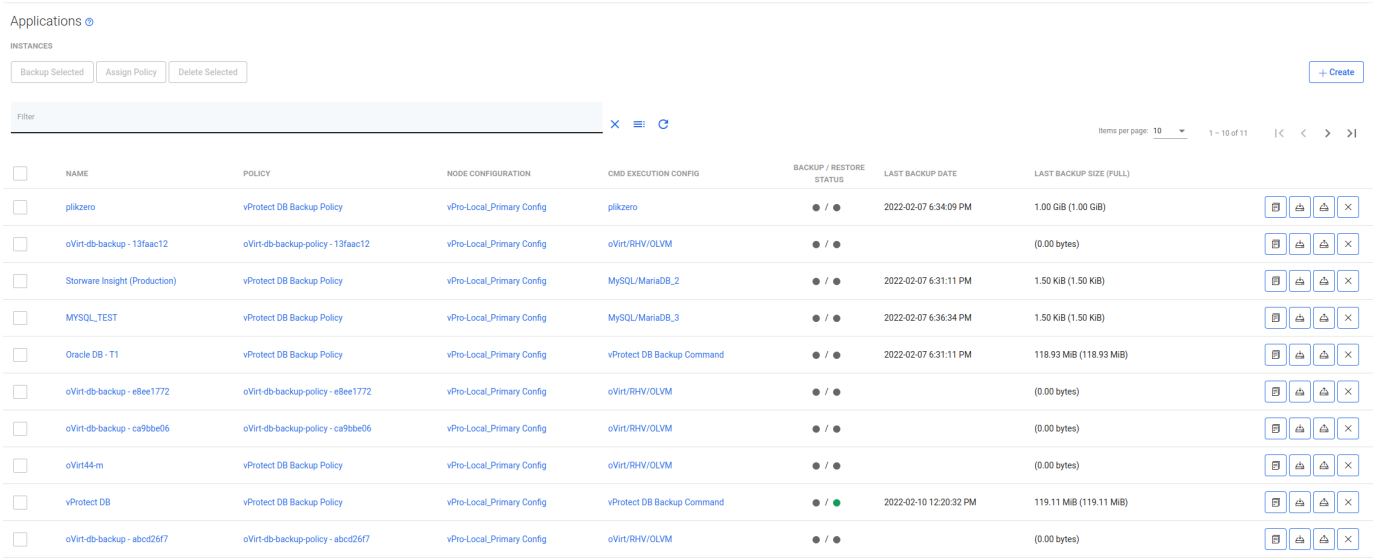
Instances - Create Application definition (at least its name and Command Execution Configuration and select node which is going to do the work)

Execution Configurations - Prepare script or commands (this is a description of how your script is going to be invoked)

Backups SLAs - allow you to setup a correlation between applications, backup destinations, and schedules. It also allows you to configure policy schedules (schedules tab).

Instances

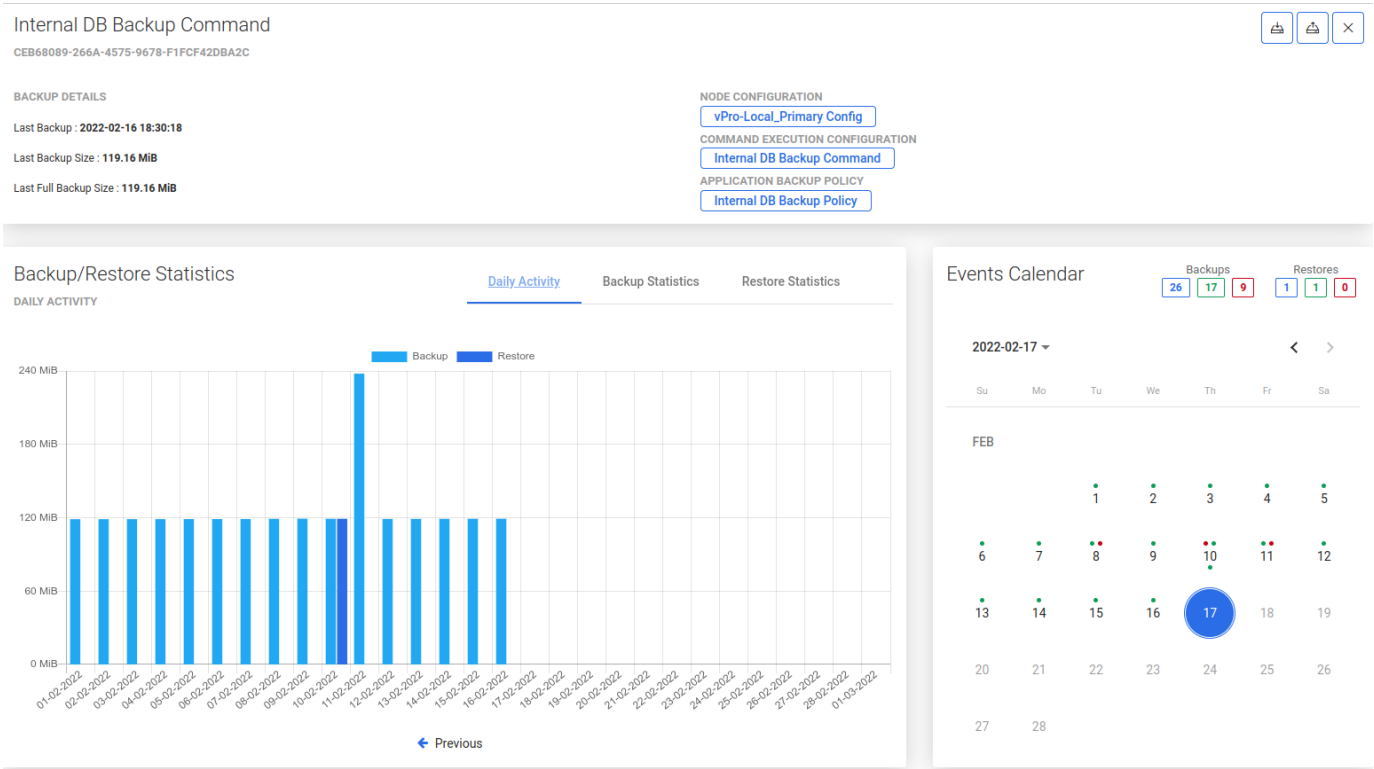
General



This tab allows you to create an "Application definition" and execute on-demand actions like:

- Clone
- Backup
- Restore
- Delete

Details page



As you can see, the window is divided into several areas like

Application summary

At the top, you can see summarized pieces of information about the Application, such as:

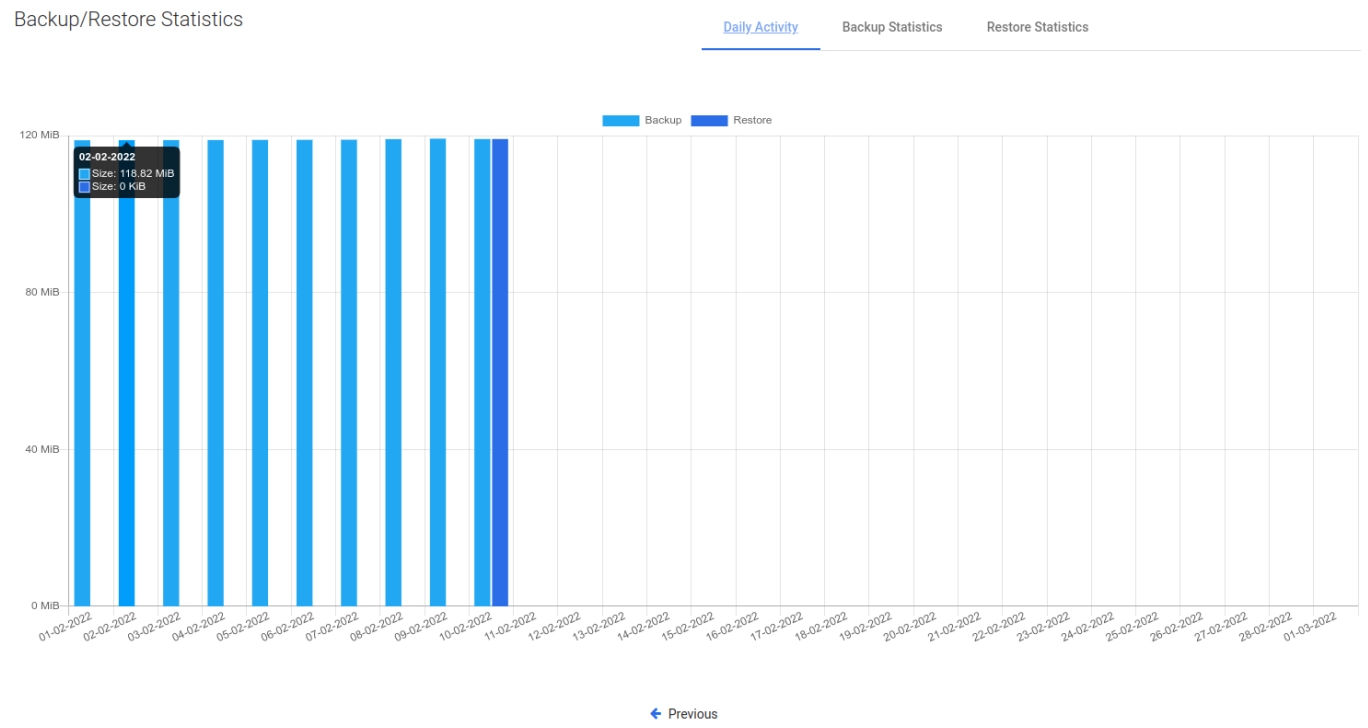
- Name of application object in Data Protector for Cloud Workloads
- To which command the execution is assigned
- Which node is backing up this application
- Short information about the last backup actions

You can also use several function buttons, such as:

- refresh
- back to instances list
- backup
- restore
- delete

Backup/Restore Statistics

Daily activity

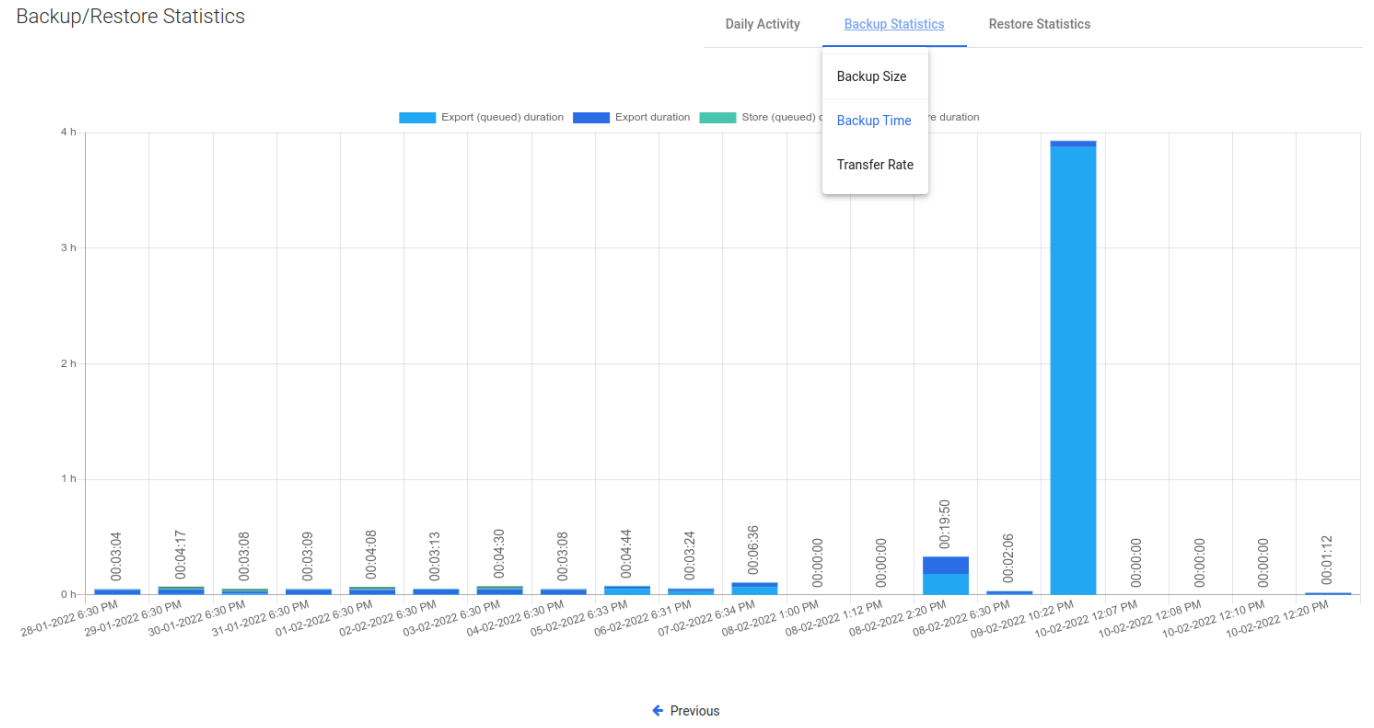


First, you'll see a daily summary of the backup and restore operations for the last month. This view is called "Daily Summary" and is the default view. You can switch the report between multiple views.

Backup Size

This view shows separate columns for each backup made to the application. Thanks to this, you can easily determine what data increase has occurred on a given app.

Backup Time

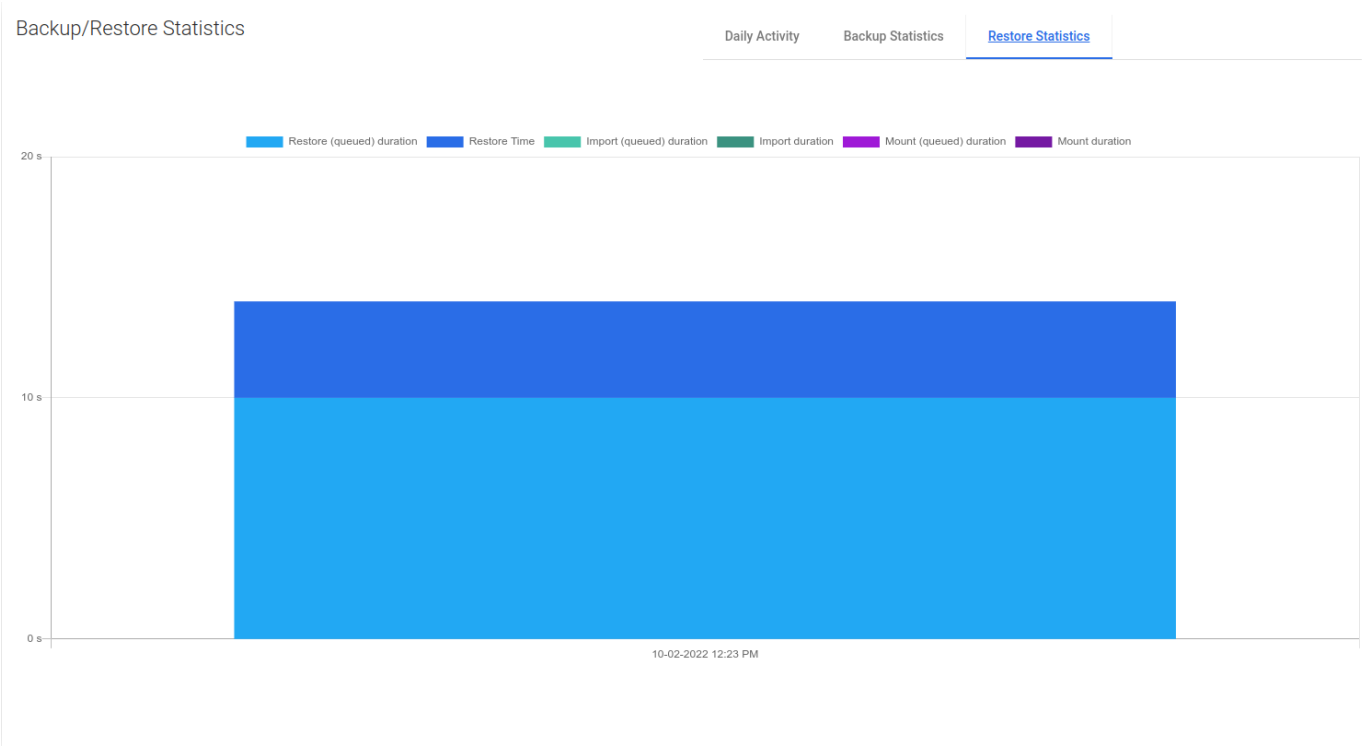


A very useful report. It allows you to determine the required window length for backups or, based on the time of individual phases, it is easy to deduce the cause of slow backups.

Transfer Rate

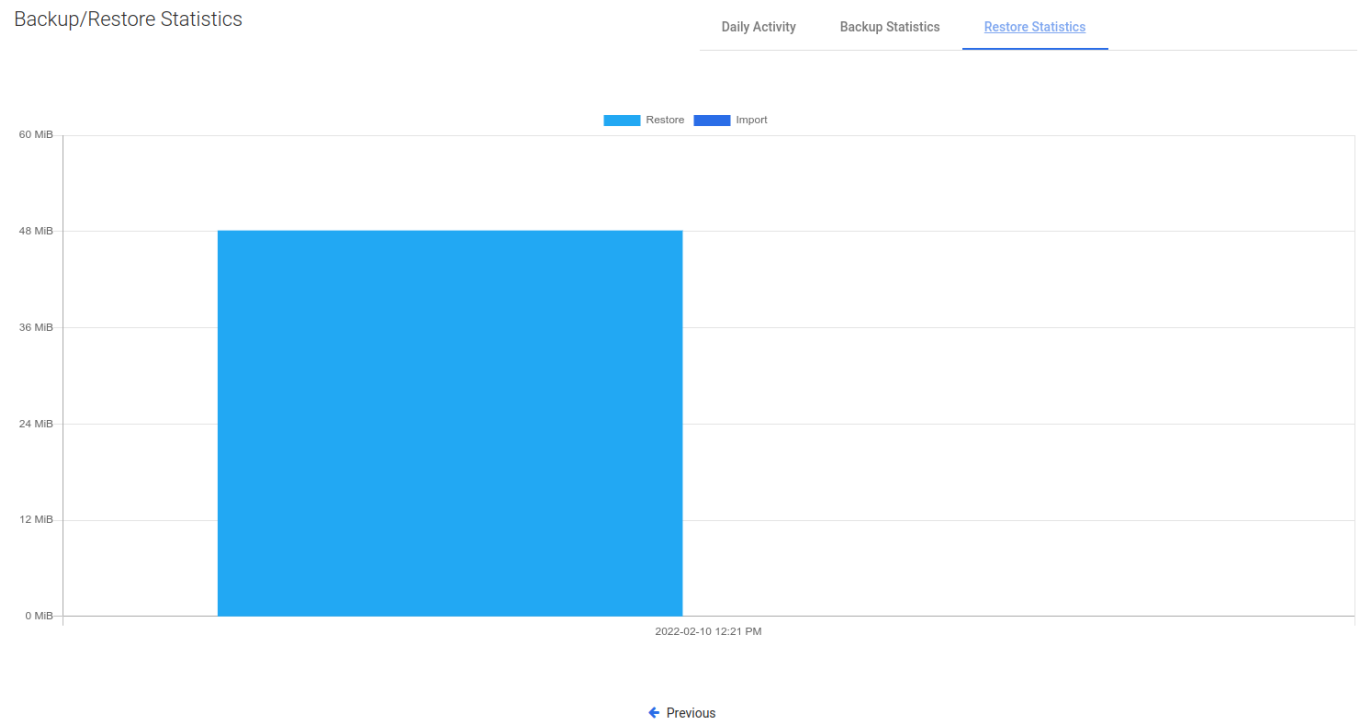
One of the newest reports - now you can easily see how fast the data transfer is.

Restore Duration



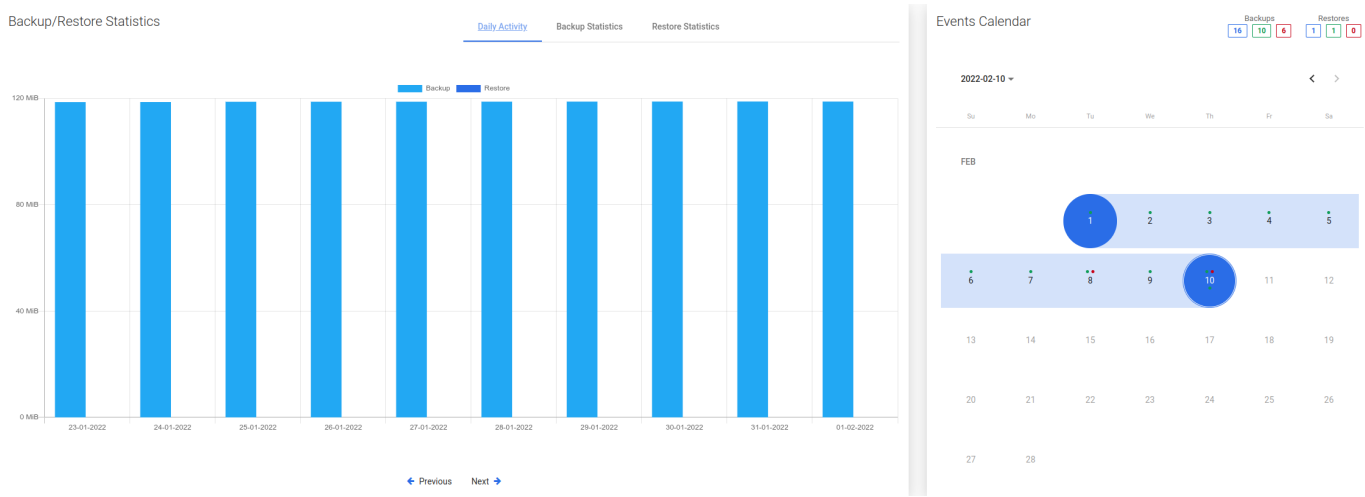
A view with the same properties as "Backup Time". It allows us to estimate how long it will take to restore the application backup files in the event of a failure.

Restore Rate



As in the previous case, we also have the transfer speed for the restore job.

Events Calendar

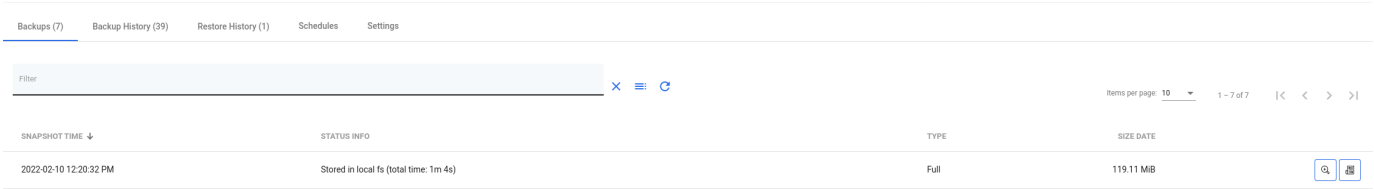


The calendar extends the possibilities of adjacent statistics. It allows you to neatly define the range of days you want to see, and additionally makes a quick summary of the number of backups and restores (top right corner).
Blue - the sum of all backups, **Green** - the sum of successes, **Red** - the sum of failures.

Bottom menu

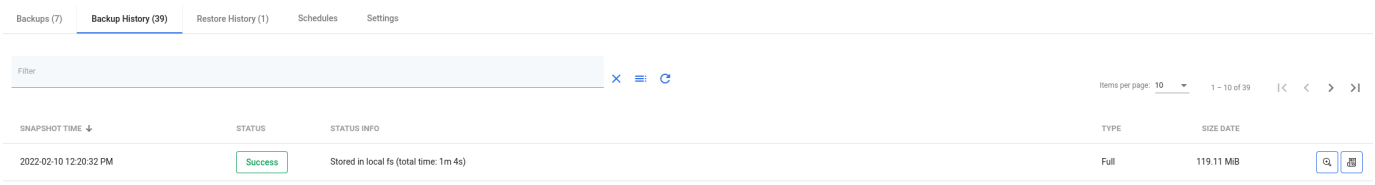
In the bottom menu, you can find a large number of tabs, each of which will present different information or will allow you to change the configuration of the particular application.

Backup



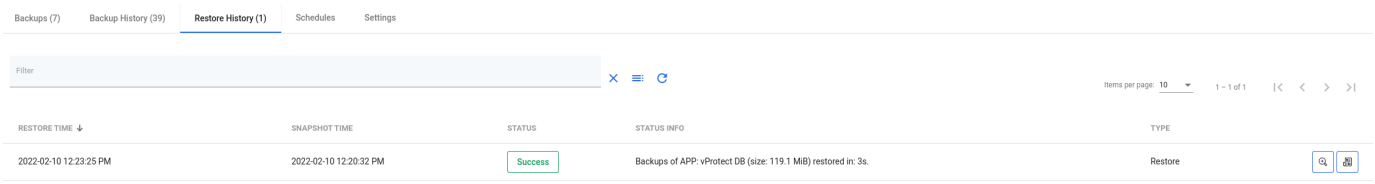
The first tab shows all application backups that are currently available and all basic information about them in a list. After pressing the magnifying glass button, you will see additional information. The button next to it allows you to download logs in the form of a .txt file.

Backup History



This tab shows information about all backups made for this application, including those failed, removed (because of retention), or currently executing.

Restore History



This tab is similar to "Backup History". This is a list with basic information about the application restores performed. When you open the details of the selected restore, you will see much more detailed information.

Restore details

Node	local
Protected Entity	Internal DB Backup Command
Restore path	/tmp
Restore Time	2022-02-10 12:23:25
Status	Success
Status Info	Backups of APP: vProtect DB (size: 119.1 MiB) restored in: 3s.
Backup Type	Full
Restore Type	Restore

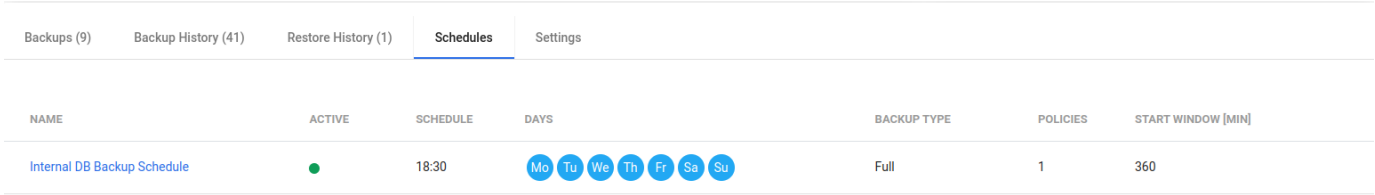
Task Time Stats

Restore (queued) duration	00:10 s
Restore Time	00:04 s

Backup

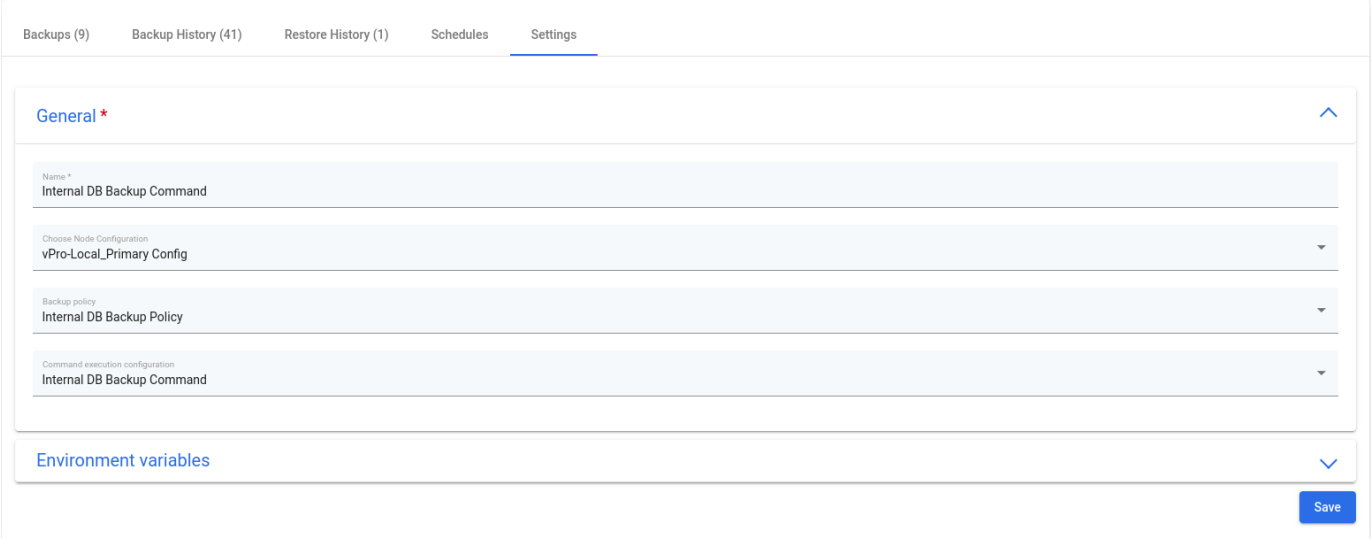
Backup Time	2022-02-10 12:21:36
Protected Entity	Internal DB Backup Command
Size	119.11 MiB
Snapshot time	2022-02-10 12:20:32
Status	Success
Status Info	Stored in local fs (total time: 1m 4s)

Schedules



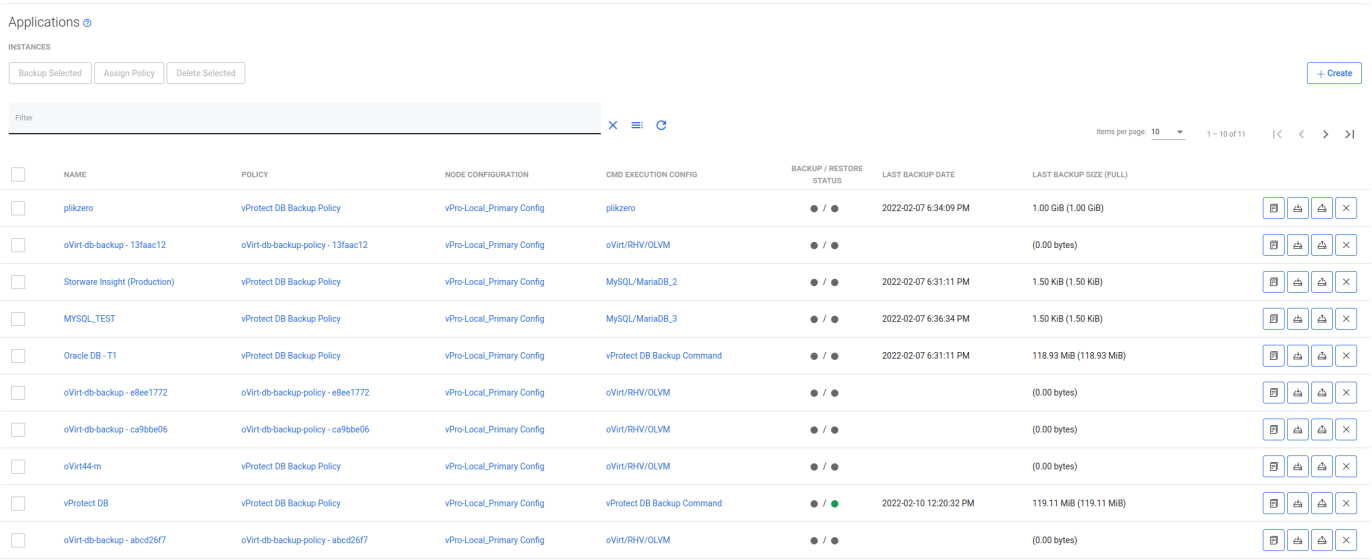
In this tab, you can see all the schedules assigned to the application.

Settings



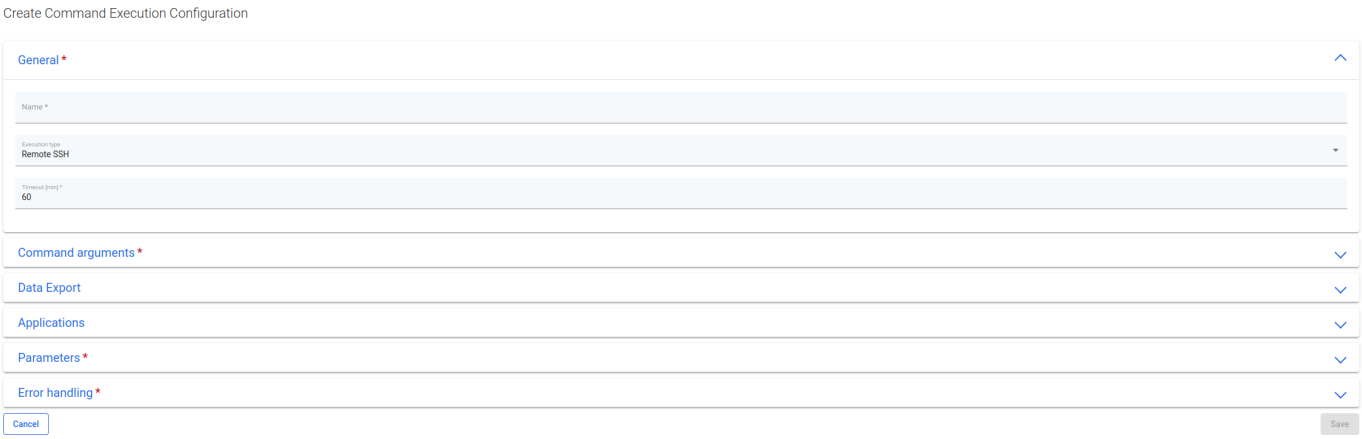
Finally, the last tab. The first two options allow you to change the node selected to perform backups and policies assigned to the application. The third allows you to choose the execution configuration.

Example - How to create an application definition



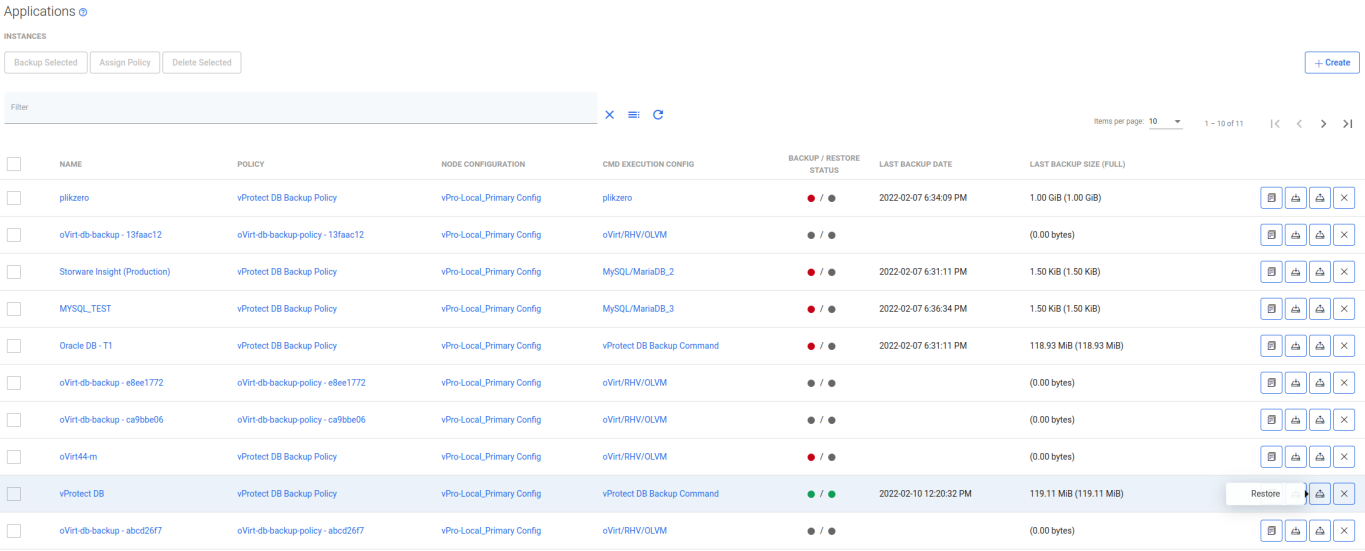
You need to provide its **name** and the **Command Execution Configuration** and select the **node** which is going to do the work - for "node" type command executions.
If the command execution type is "remote ssh", you also need to provide ssh access.
To schedule application backup, you need to select the backup policy.

> **Note:** You can find more about policies and schedules in this article: Backup SLAs.

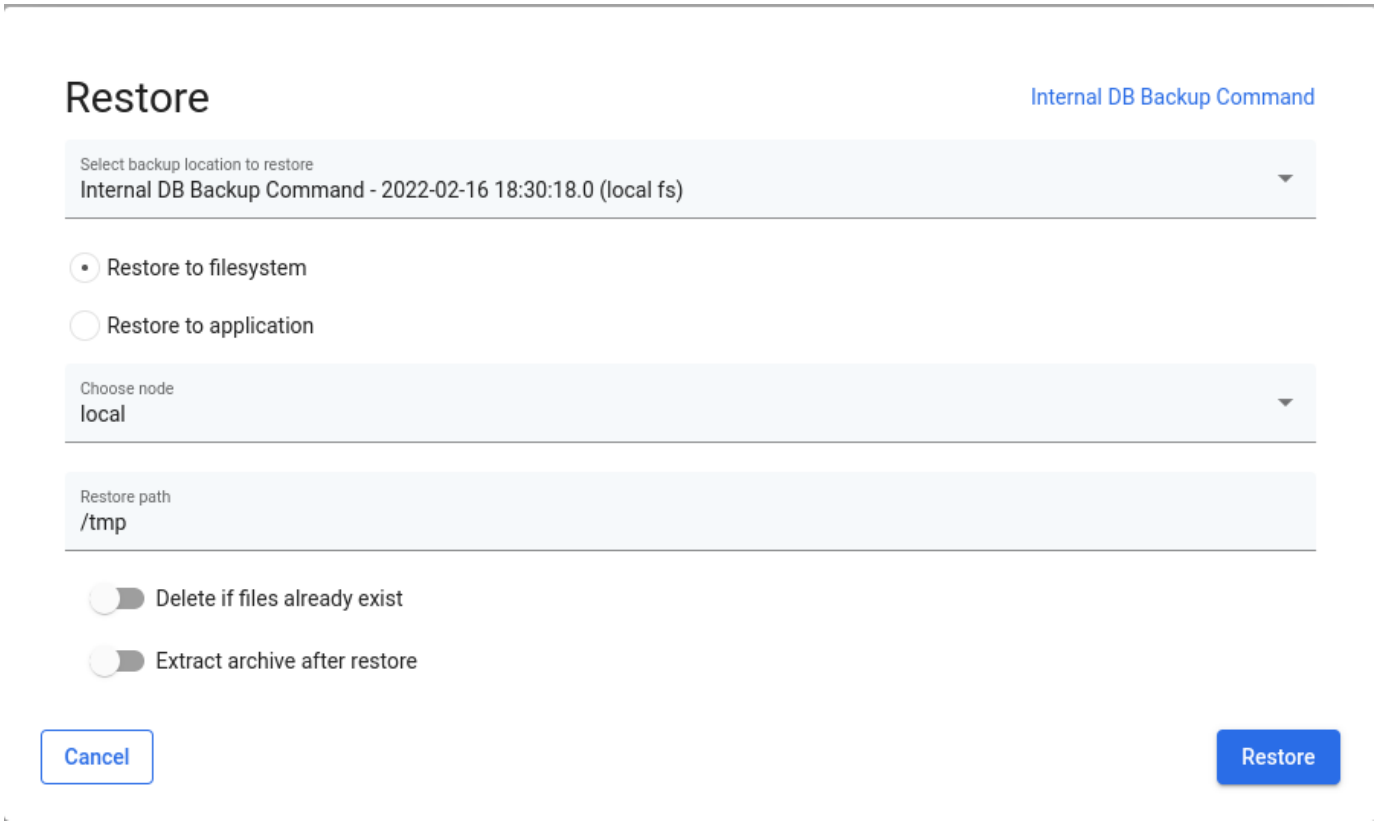


Example - How to restore an application

To perform an on-demand application restore, click the restore button on the right side of the application line.

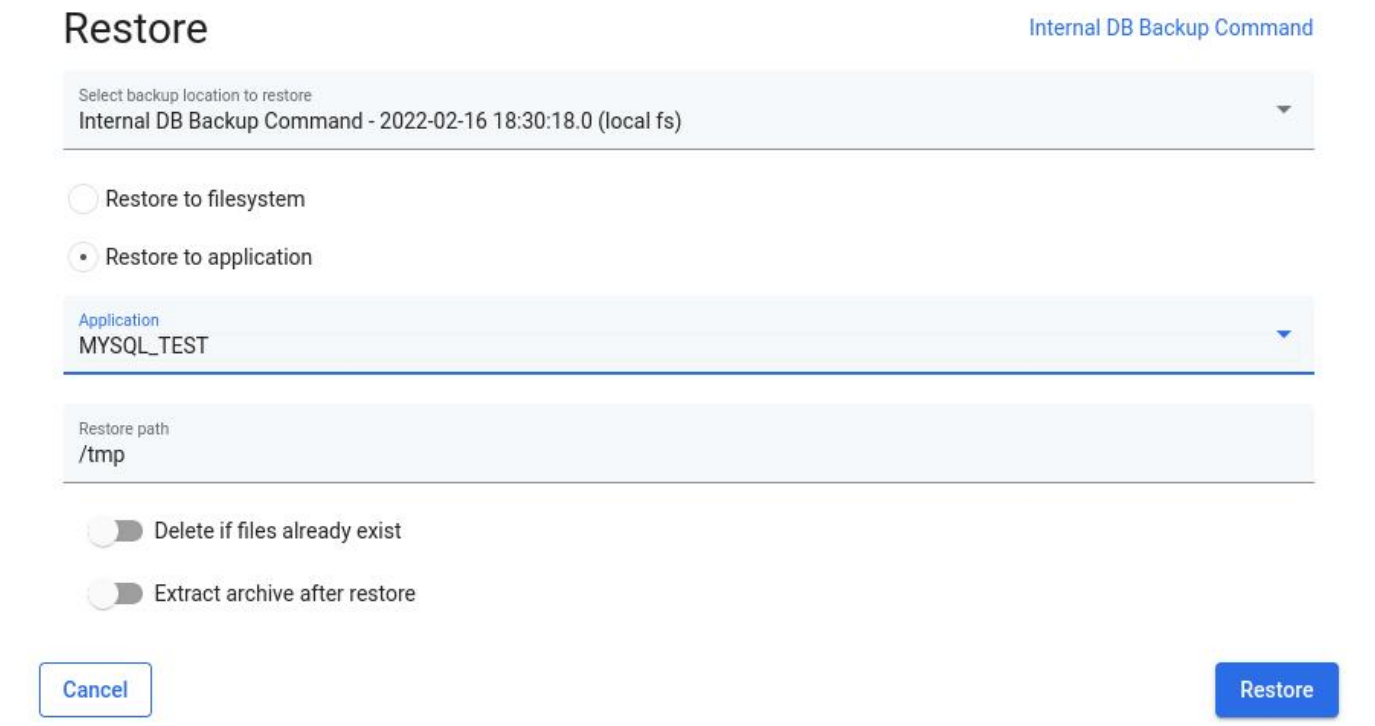


After clicking on it, you will see a pop-up window where you can customize the restore options.



If you choose the "Restore to filesystem" option, you can select things such as which backup you want to restore, on which node you want to restore files, etc.

The "Restore to application" option differs in that it allows you to restore files to the server where the application is located.**



**This option is available for applications using "Remote SSH" in the command execution configuration

Settings Command Execution Configuration

General *

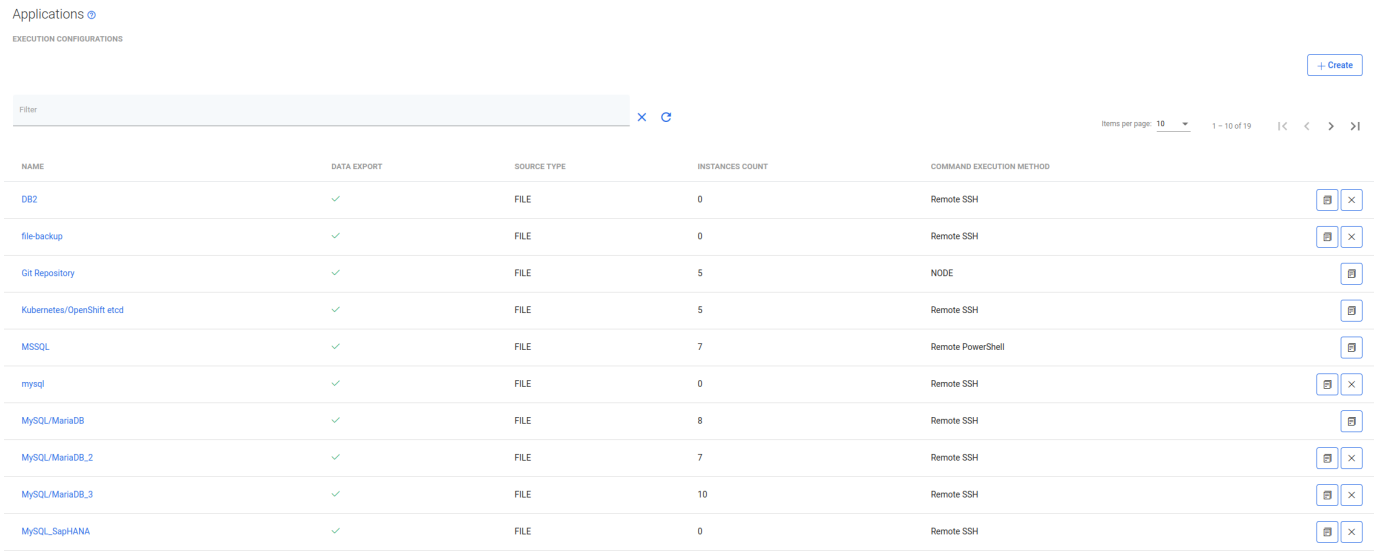
Name *
DB2

Execution type
Remote SSH

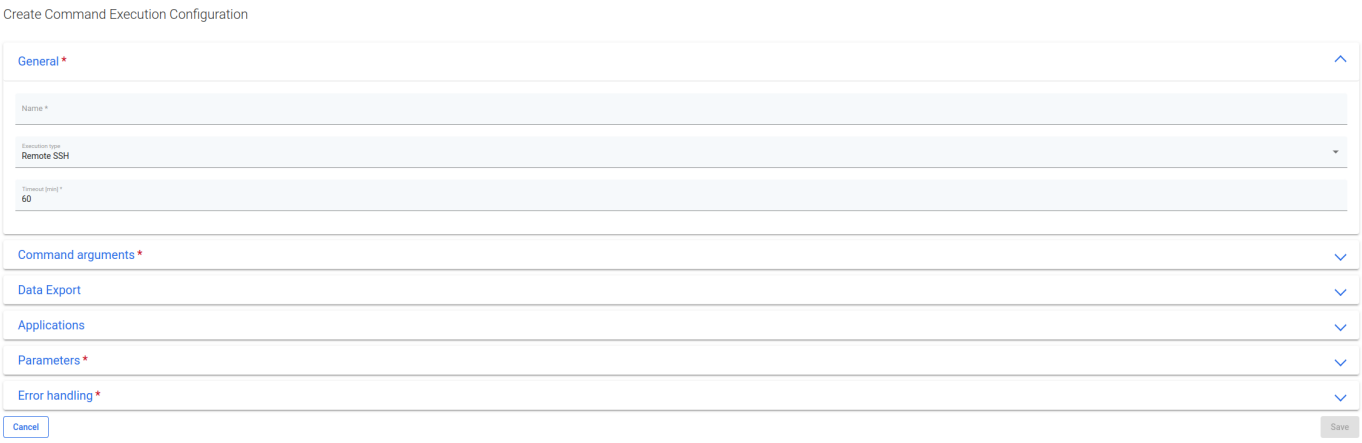
Timeout [min] *
60

Execution Configurations

Using this tab, you can create a command execution configuration, i.e. commands executed for the proper backup of your application (or directed to the script file).



1. Prepare the script or commands, and (if remote SSH execution is required) put them on the remote machine with your application.
2. In the Applications section, create a new **Command Execution Configuration.**



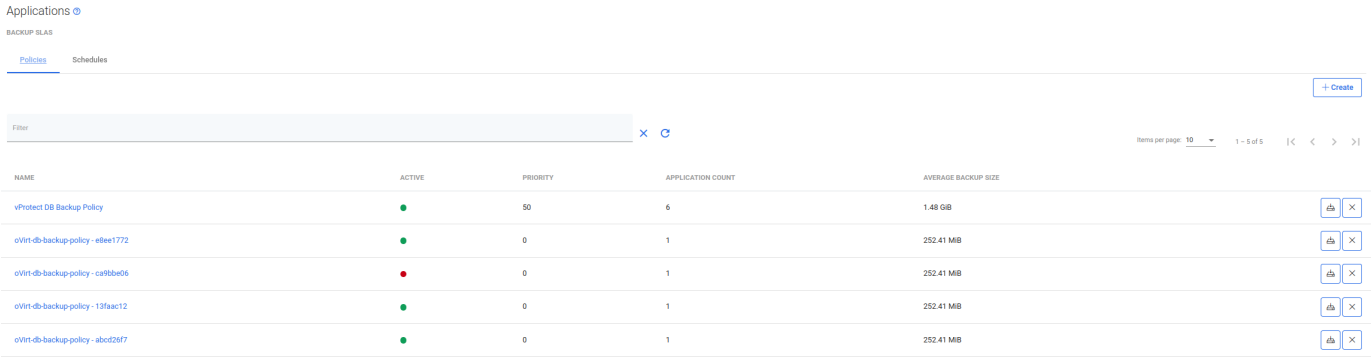
This is a description of how your script is going to be invoked - you need to specify:

- **Execution Type -** either on the Node or a command to be executed remotely.
- **Timeout** - for script/command execution - make sure to have this timeout set to a value high enough to allow your command to complete its execution.
- **Command arguments** (the first one is the actual executable) - all arguments should be provided separately - Data Protector for Cloud Workloads assumes that they can contain spaces.
- **Data export** - this switch allows you to export (or not) data that will be generated by the command (sometimes you may want Data Protector for Cloud Workloads just to execute commands without transferring anything).
- **Source type** (if you export data)
    - **FILE** - select if your command produces a single file/directory (or multiple files) - if you provide a directory or path with wildcards, Data Protector for Cloud Workloads will create a TAR archive - you have to specify the **Source Path** for this source type.
    - **STREAM** - select if your command generates backup to the standard output.
- Select existing **Applications** (or skip this for now - it can be assigned later).

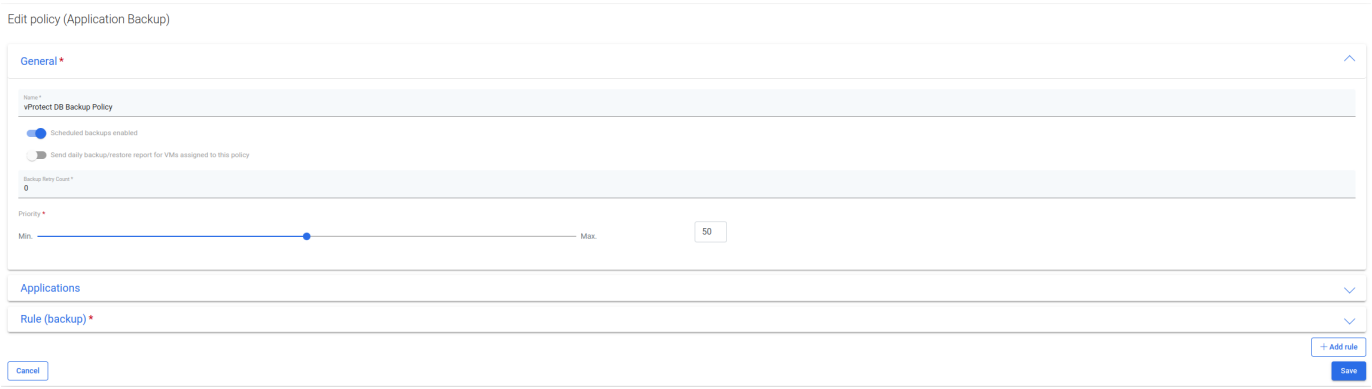
- You can define the **Parameters** that you'll later be able to use in your commands/scripts. Note that the variable name should not contain white-space characters.**
- **Error handling** - you can decide what do you want to do with errors in your output stream

Backup SLAs

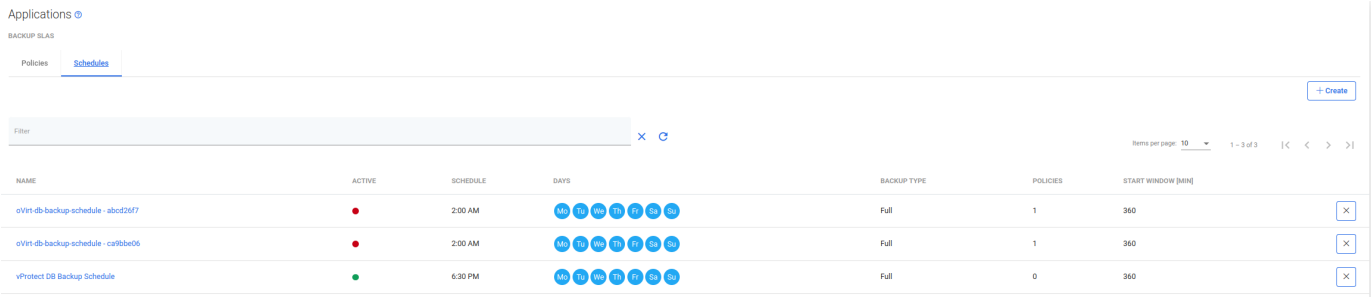
To backup your application periodically:

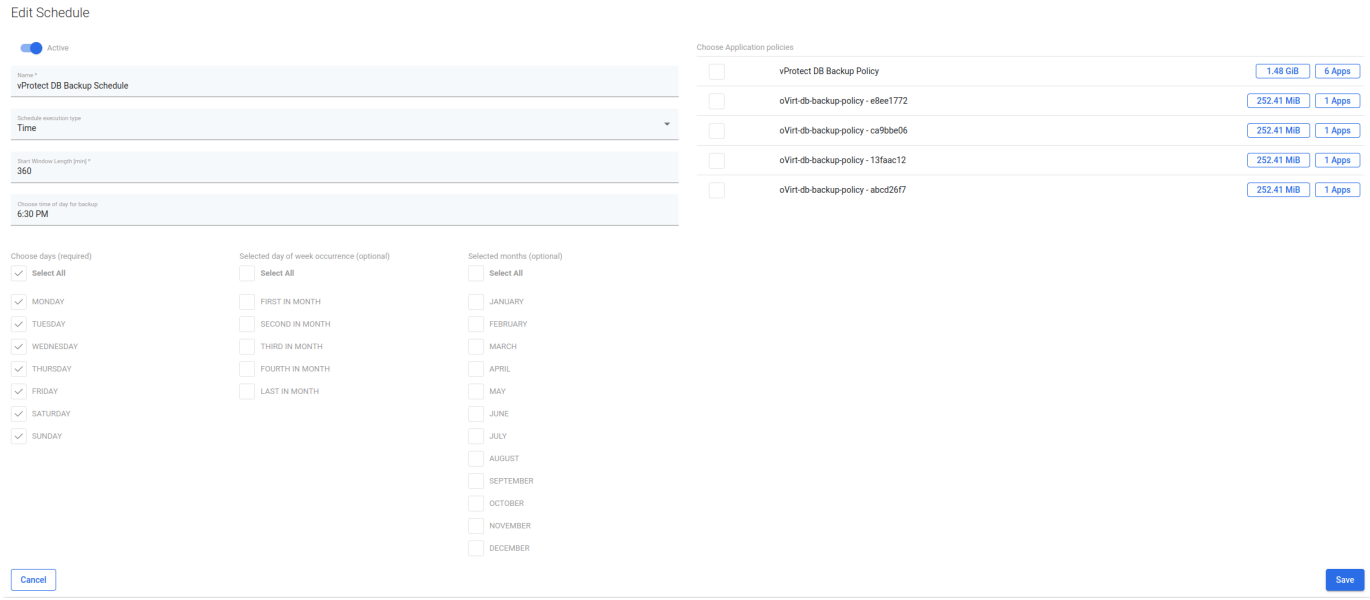


- You need to create a Policy:
  - Go to Applications from the left side menu and then to Backup SLAs
  - Provide a policy name
  - Select your application from the list
  - Specify backup rule details - especially backup destination and schedules



- The second part is a schedule for policy:
  - Change tab from Policies to Schedules
  - Create a new schedule for application policy - create it just like other schedules, enter a name, choose execution time (time or interval) and days of the week. *optionally you can select policy if already exists





Now your application backups will be done periodically according to your policy.

Reporting

Reporting features allow users to view statistics, especially for backup and restore tasks. They also provide the possibility to view what has happened lately in the Data Protector for Cloud Workloads environment.

Reporting is divided into five sections:

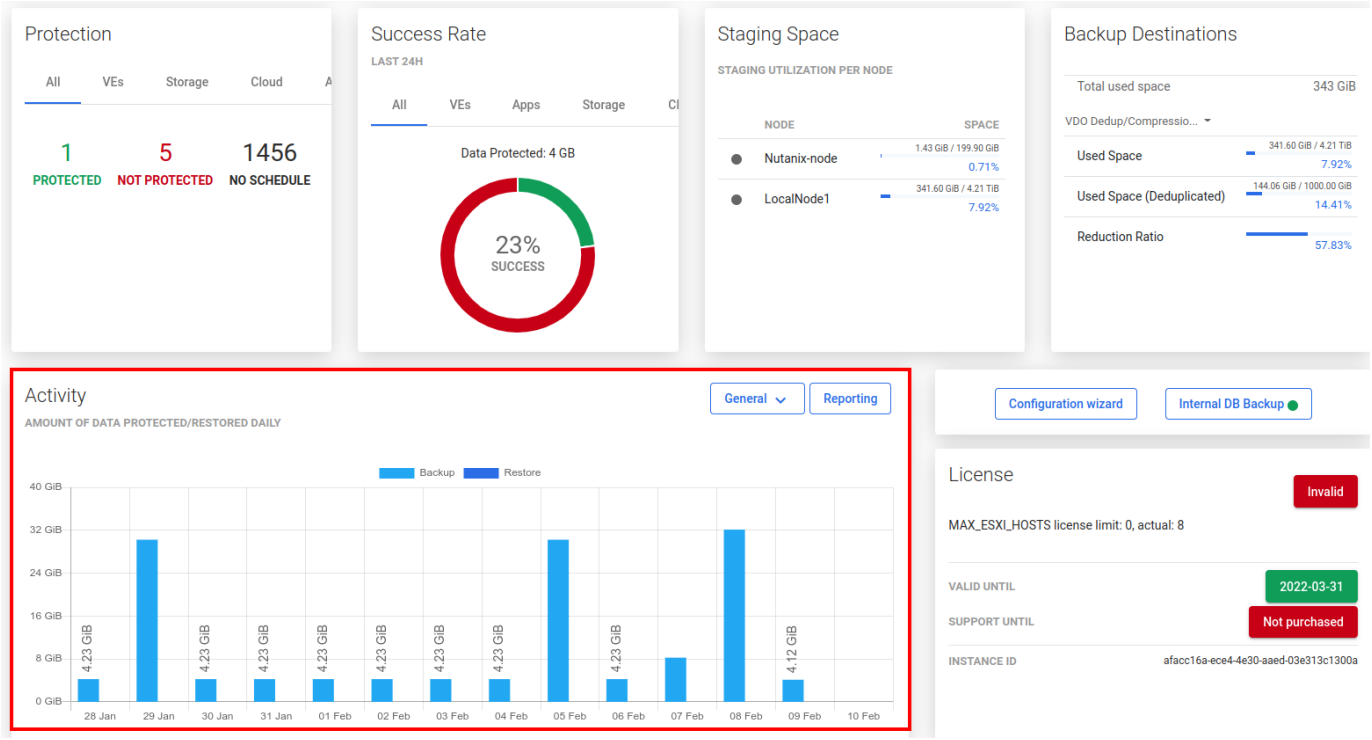
- Virtual Environment - for general statistics about data from virtual machines
- Storage - for general statistics about data from storage providers
- Cloud - for general statistics about data from Cloud (Microsoft 365)
- Applications - for general statistics about data from applications
- Audit logs - for important events in terms of security and system administration.

Detailed information on these individual sections can be found directly in the related articles.

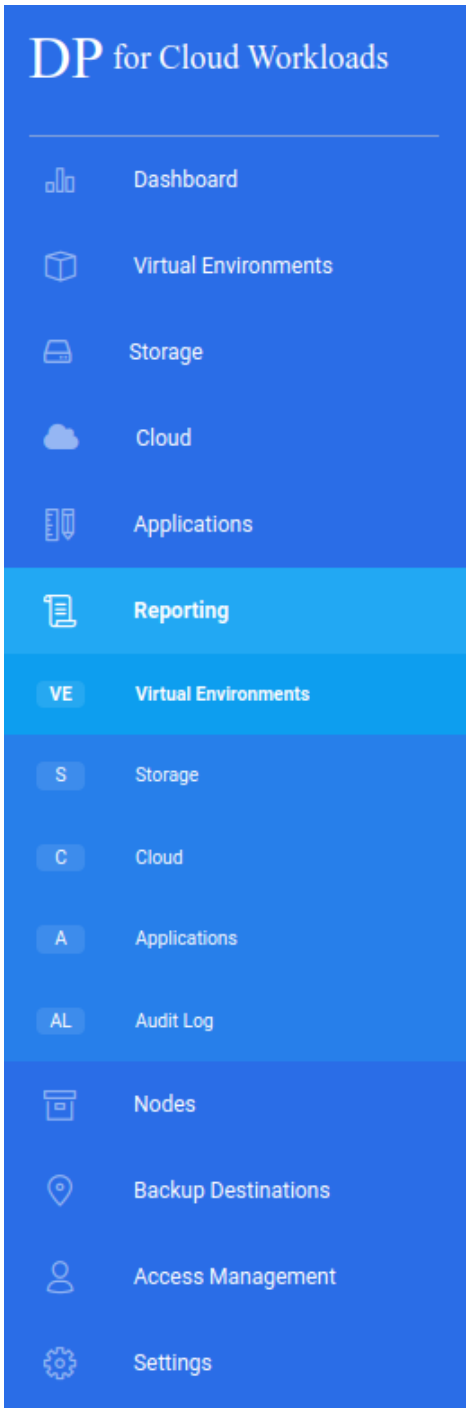
Virtual Environments

General

Data Protector for Cloud Workloads provides a reporting feature for obtaining information about historical activities. You can reach this from the main dashboard under the Activity section via the **Reporting** button.

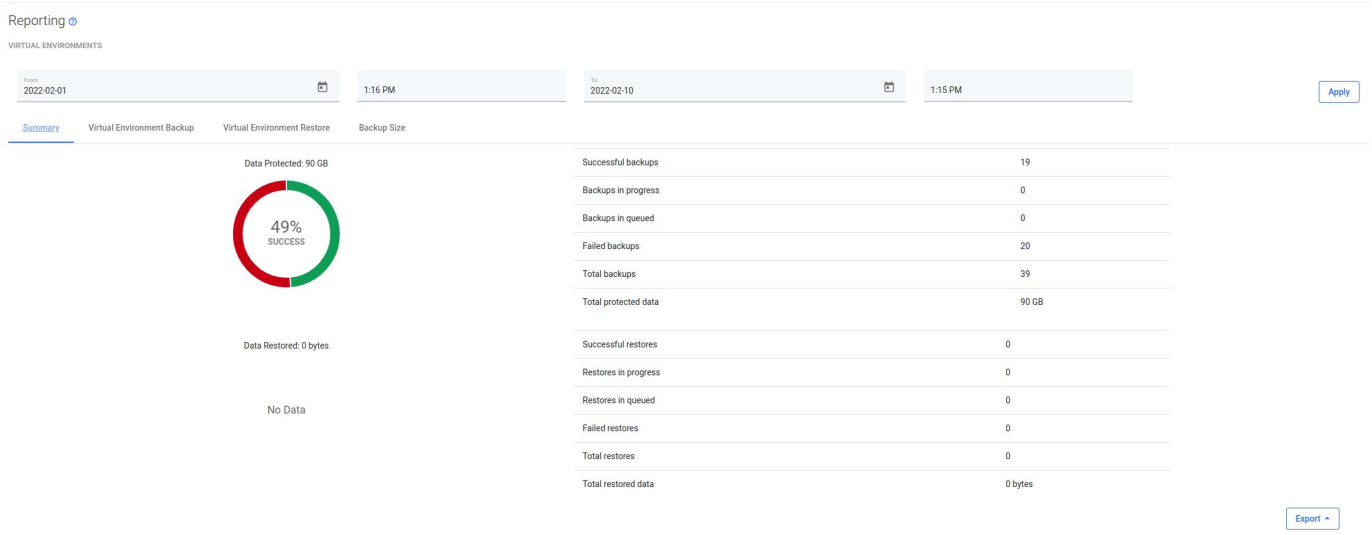


Or on the left side menu - **Reporting** -> **Virtual Environments**.

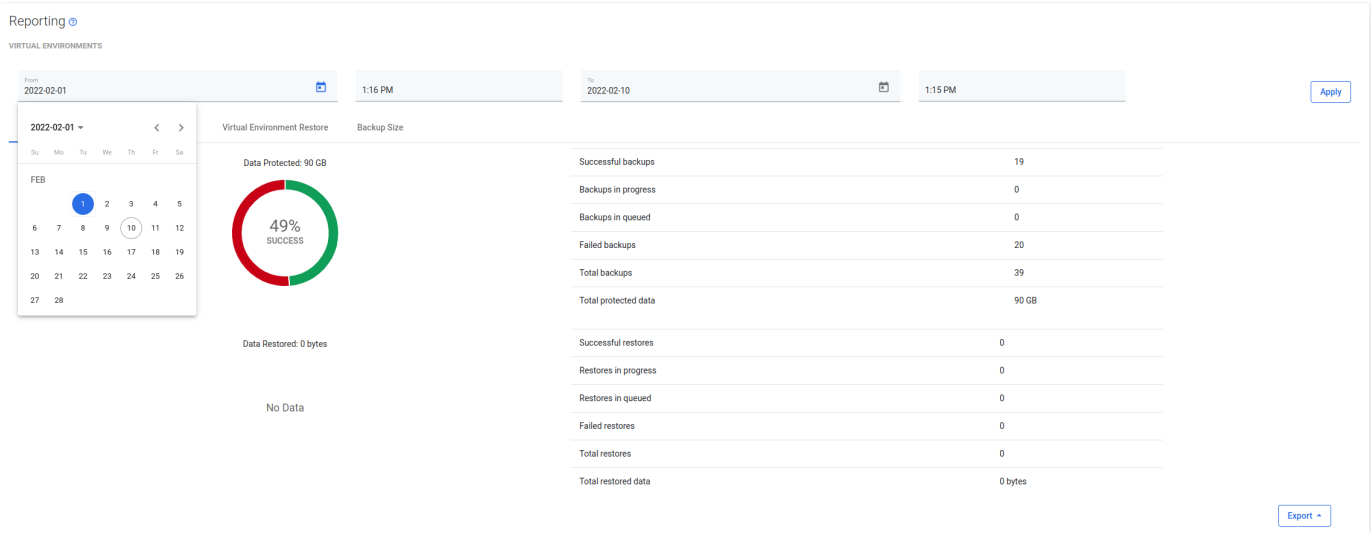


Summary

At the beginning, you should see the summary page.



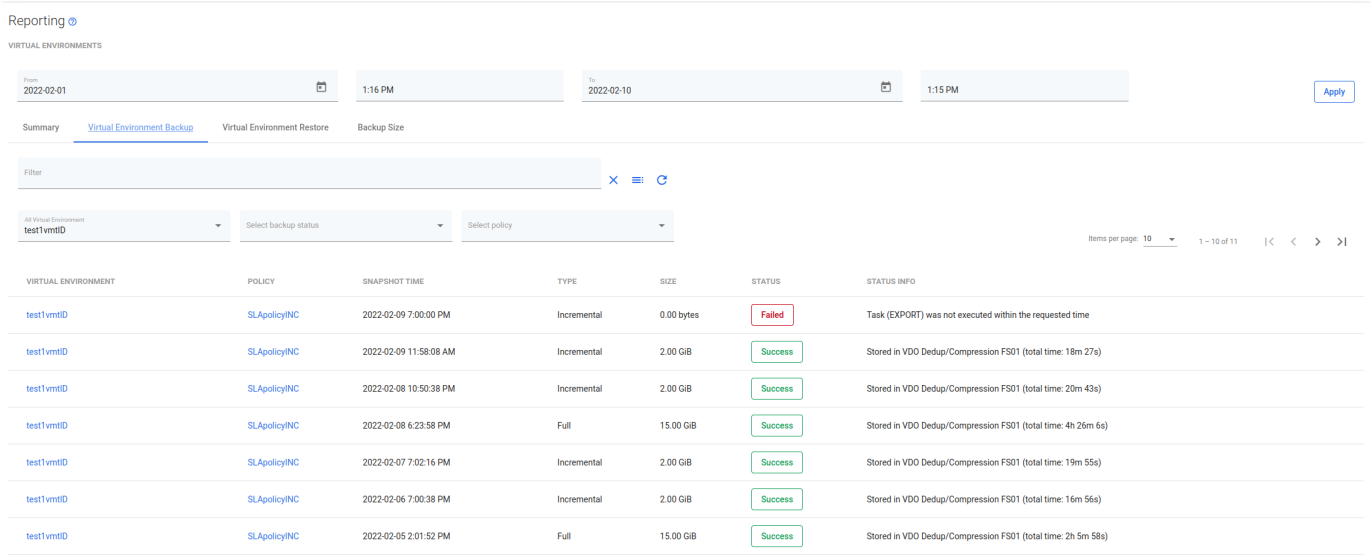
From here, you can set a date range or go to a detailed summary of backup, restore jobs, and backup size.



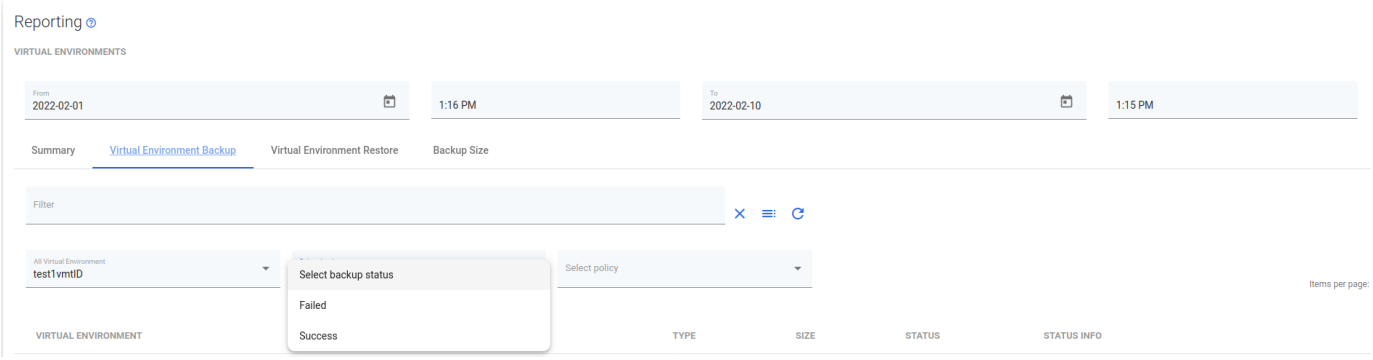
Now that you have set the date you are interested in, you can move to the next tabs to view details of each task performed by Data Protector for Cloud Workloads.

Backup Statistics

Now you can see all the tasks completed within the set date, or ...

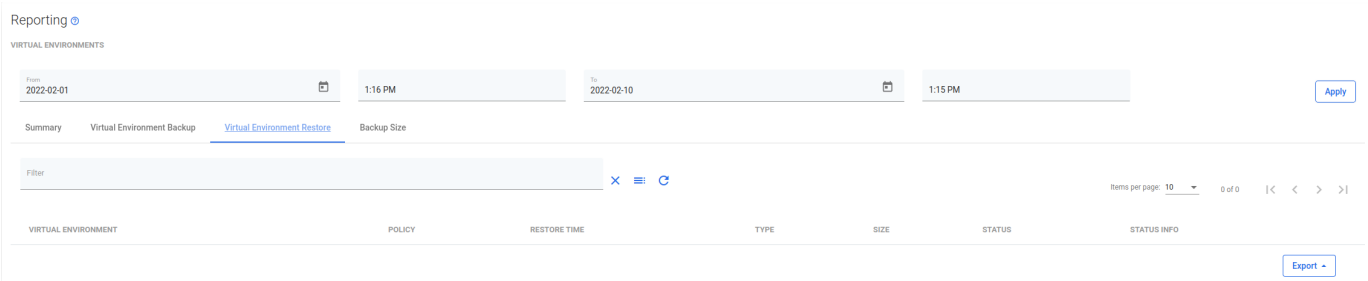


additionally filter them by status, rules or instance.



Restore Statistics

The functionality is the same as for the backup statistics, you can see all the tasks completed within the set deadline or filter them by status, policy, or instance.



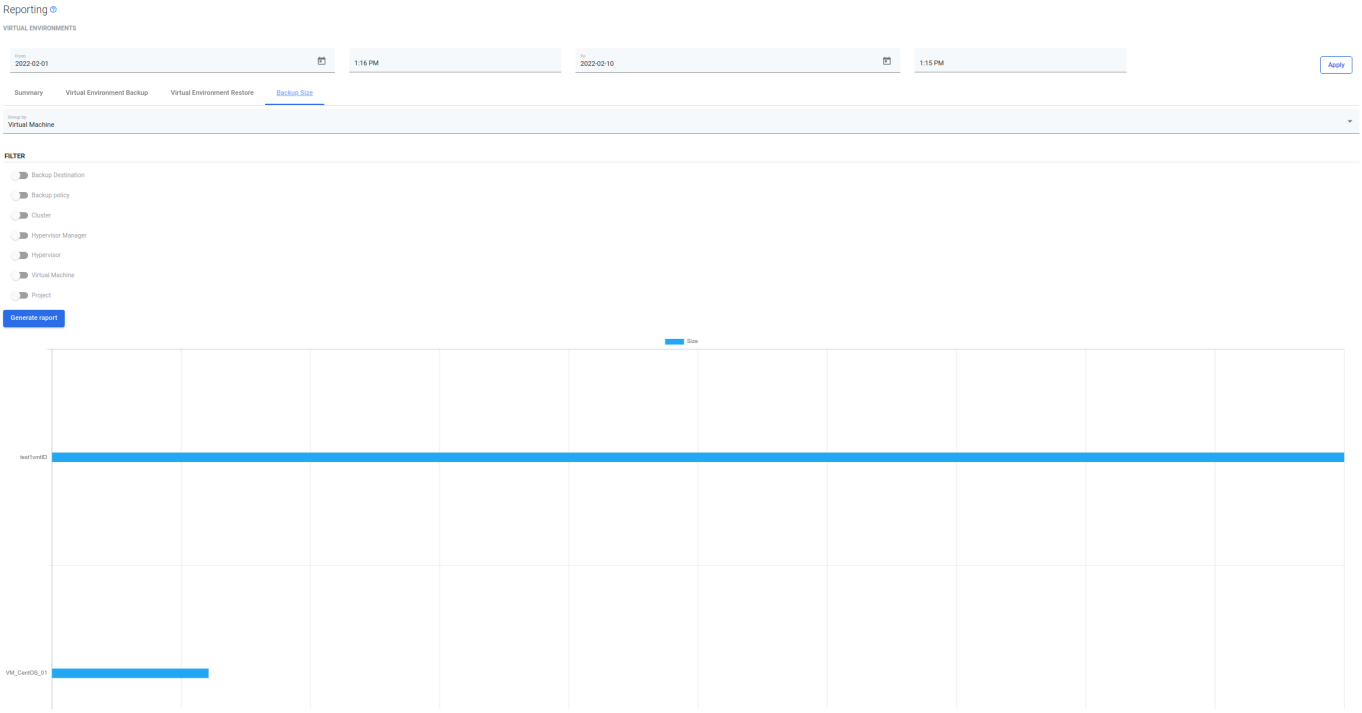
Report sections that you might need for chargeback reporting:

Transfer Size

Transfer size tab shows the amount of data transferred during the backup operations.

Backup Size

Backup Size section shows the current exported data.

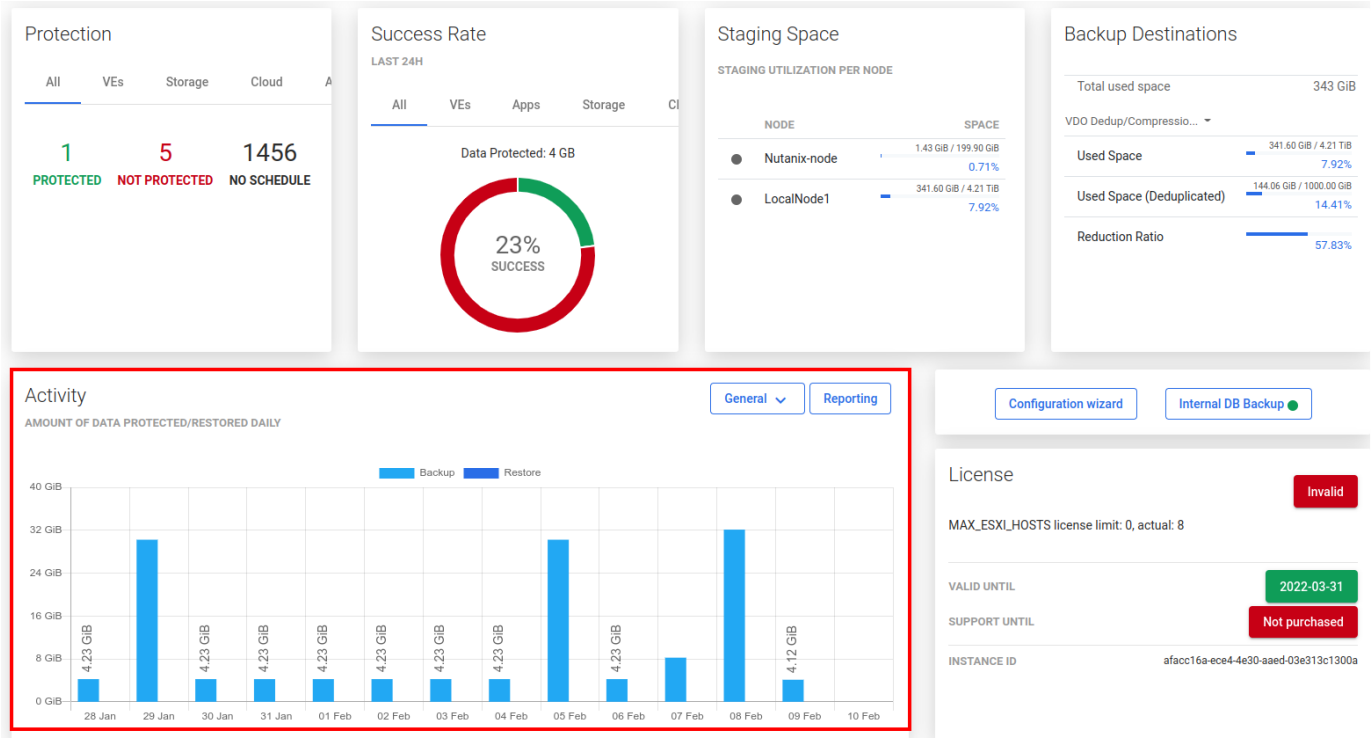


Note: You can use the **Export** button to send reports with backup and restore statistics by email or export them as PDF or HTML.

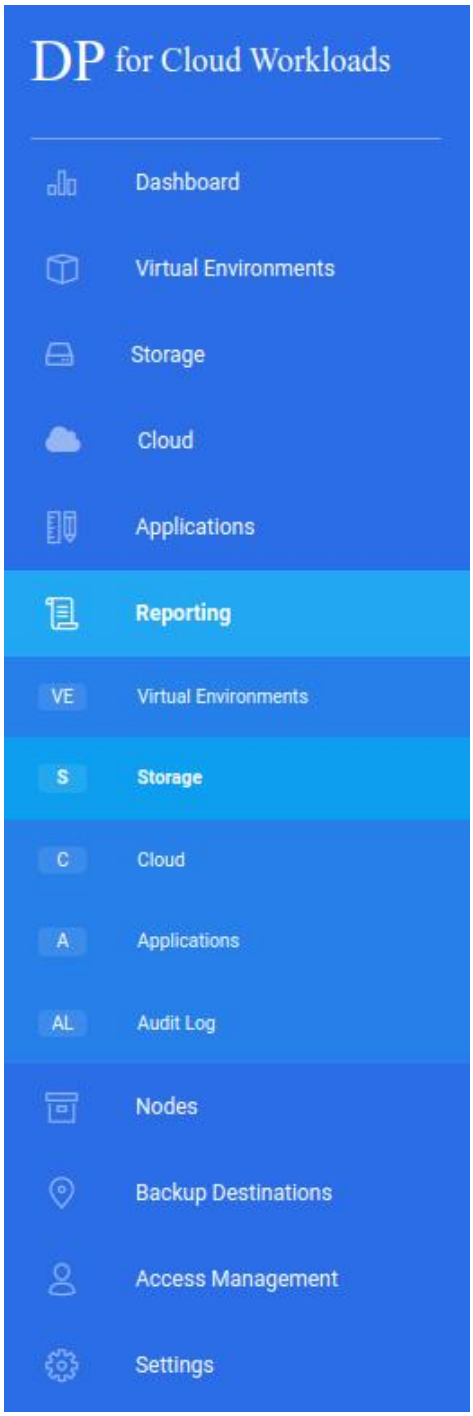
Storage

General

Data Protector for Cloud Workloads provides reporting functionality for obtaining information on historical activity. You can reach this from the main dashboard in the Activity section via the button `Reporting`.

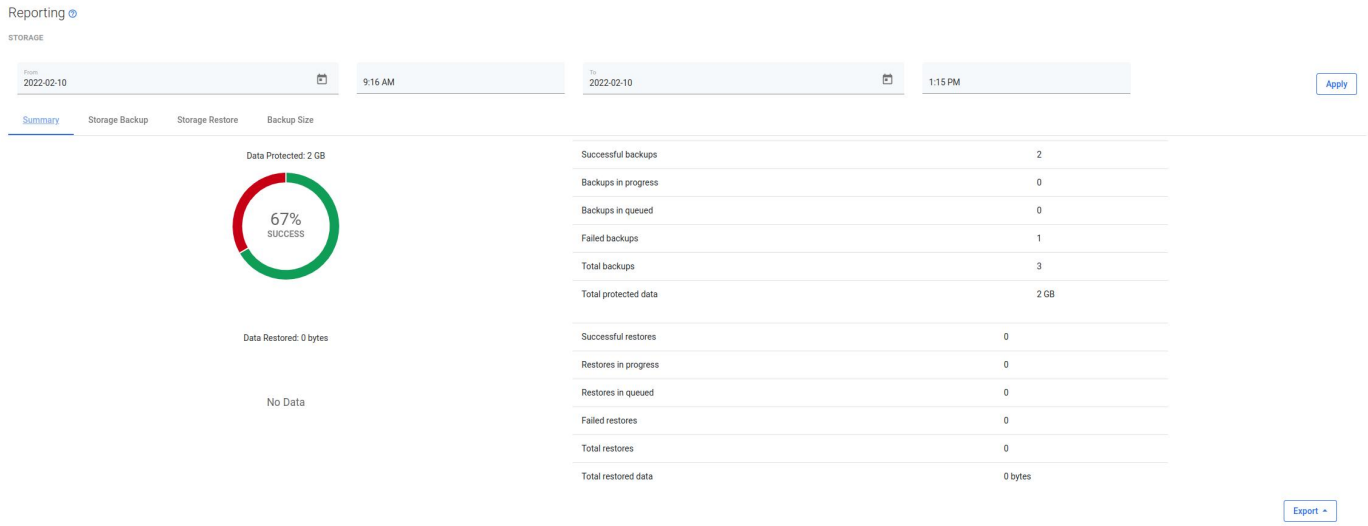


You can also open the storage reports in the reporting section using the left menu.

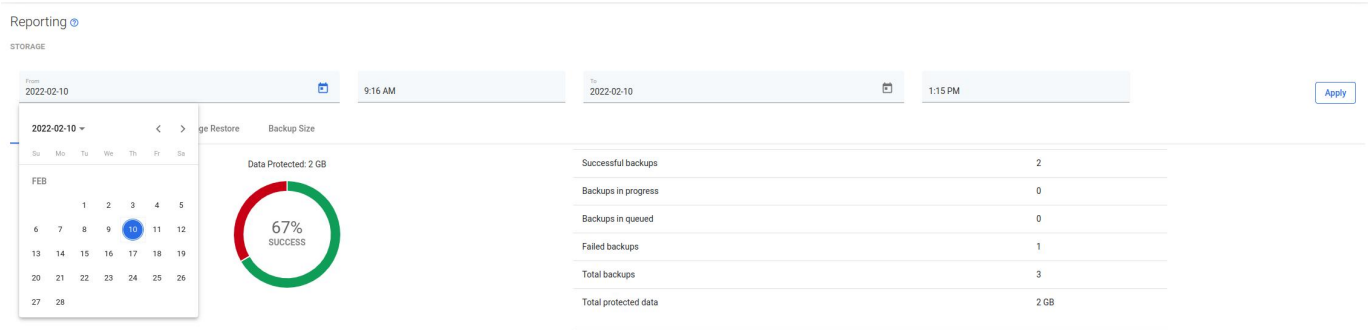


Summary

In the beginning, you should see the summary page.



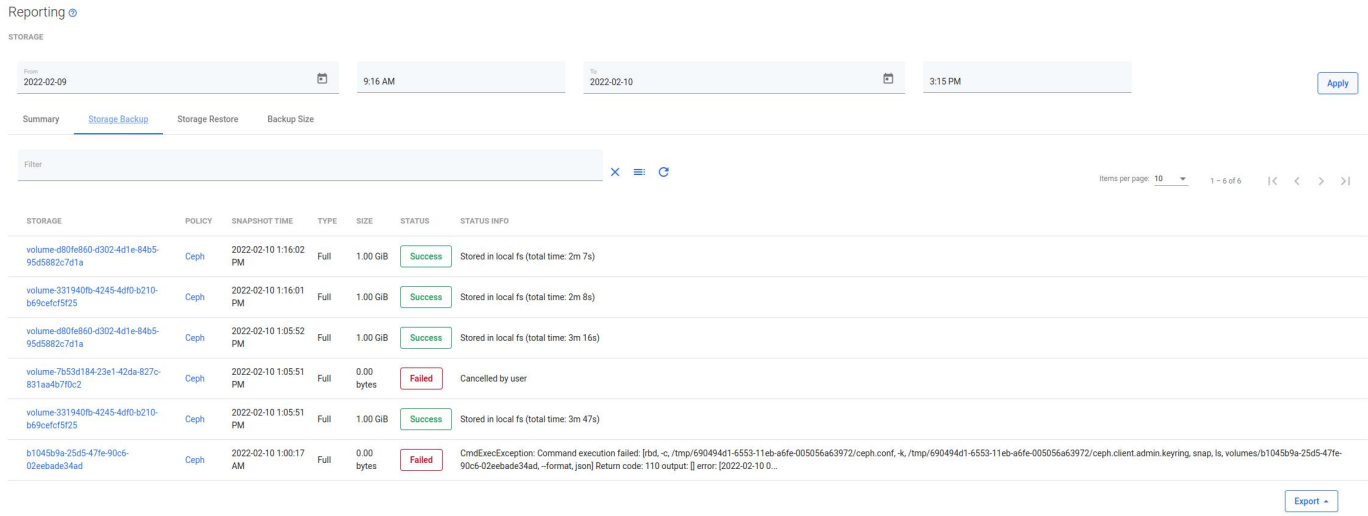
From here, you can set a date range or go to a detailed summary of backup, restore jobs and backup size.



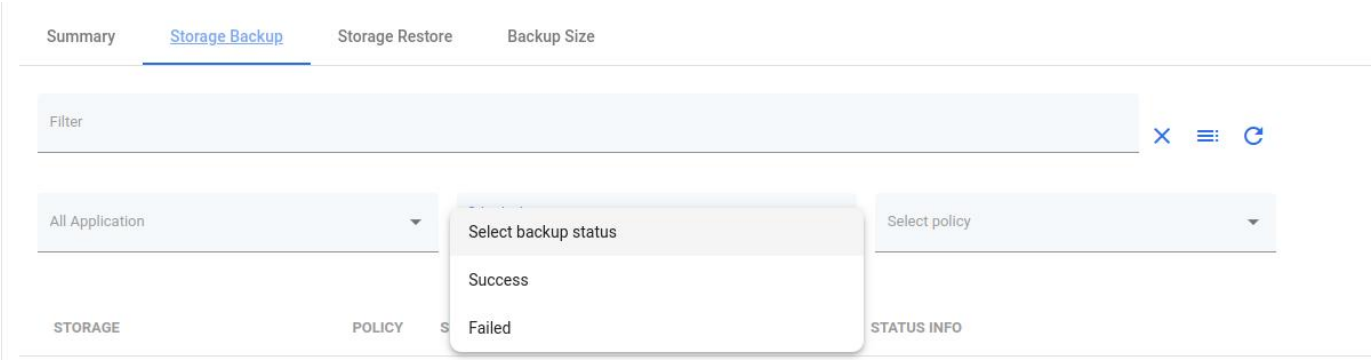
Now that you have set the date you are interested in, you can move to the next tabs to view the details of each task performed by Data Protector for Cloud Workloads.

Backup Statistics

Now you can see all the tasks completed within the set date, or ...

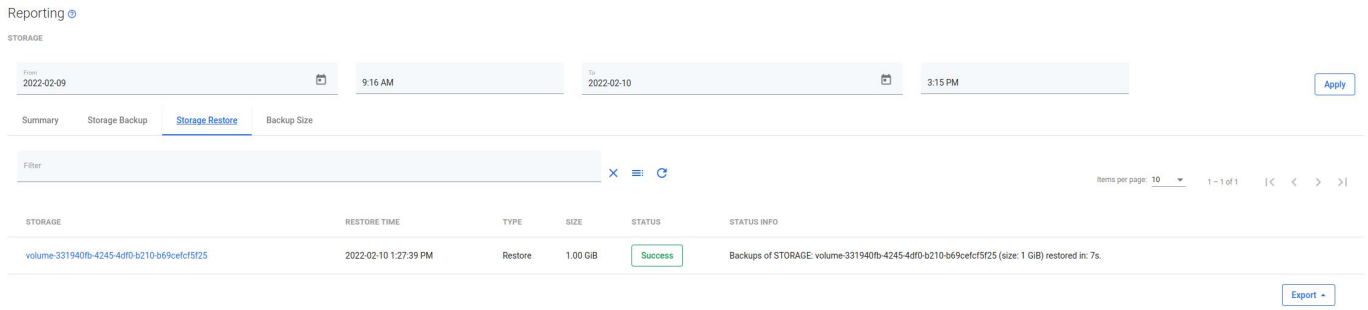


additionally filter them by status, rules or instance.



Restore Statistics

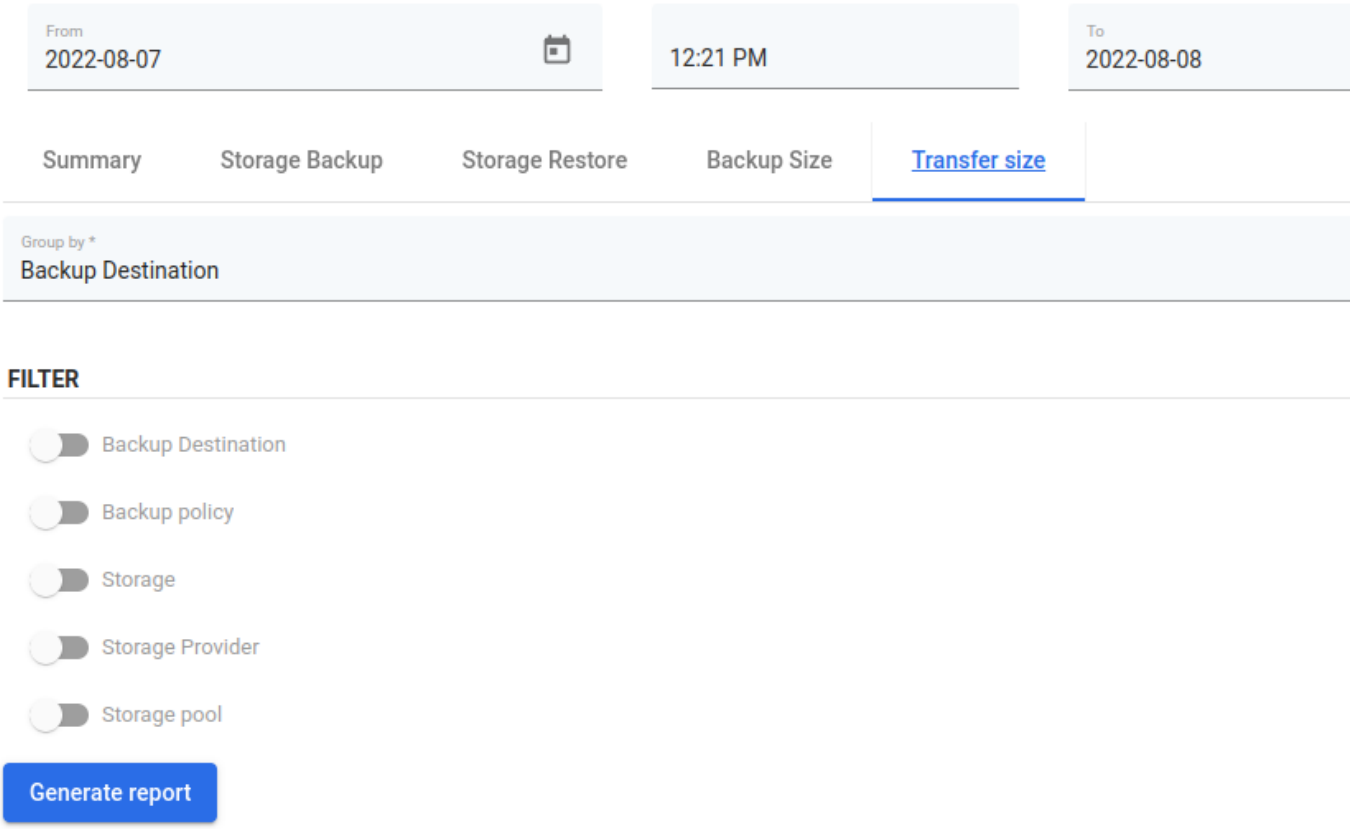
The functionality is the same as for the backup statistics, you can see all the tasks completed within the set deadline, or filter them by status, policy or instance.



Report sections that you might need for chargeback reporting:

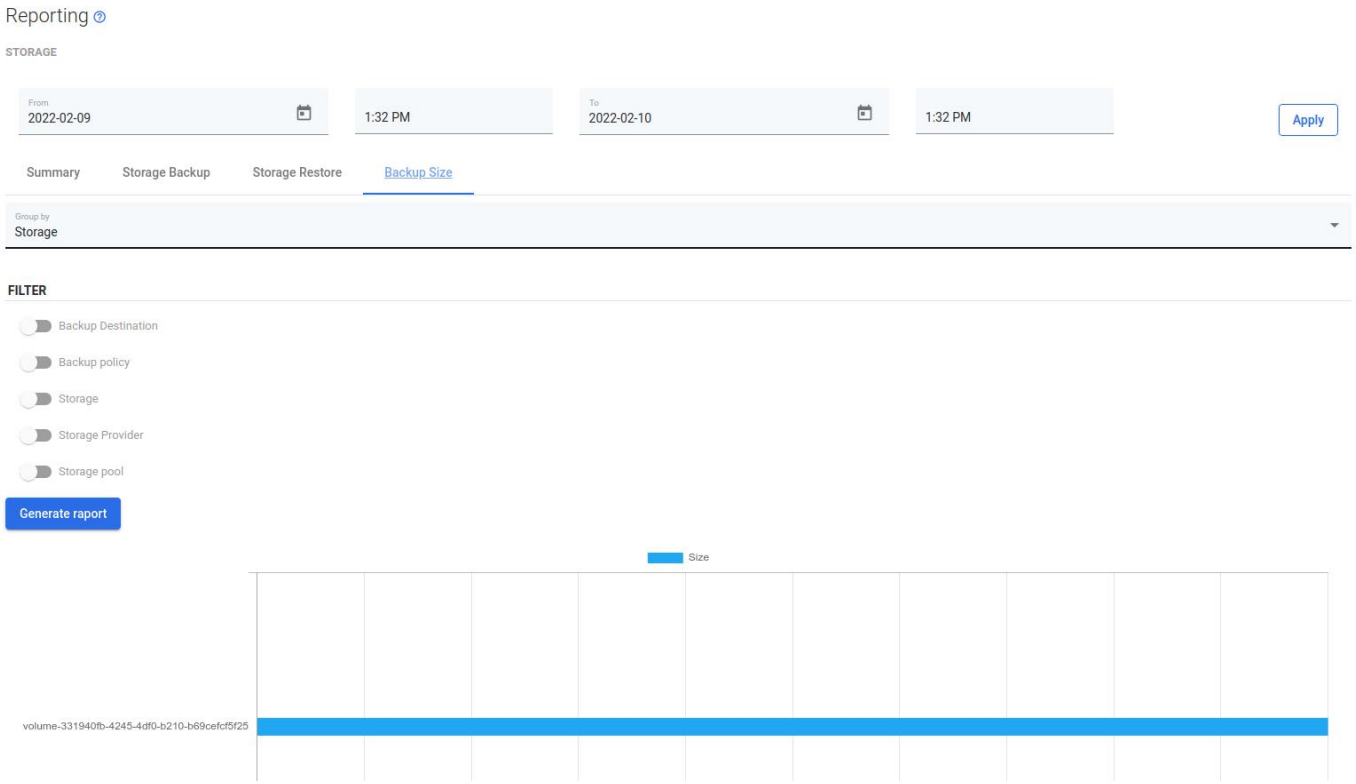
Transfer Size

Transfer size tab shows the amount of data transferred during the backup operations.



Backup Size

Backup Size section shows the current exported data.

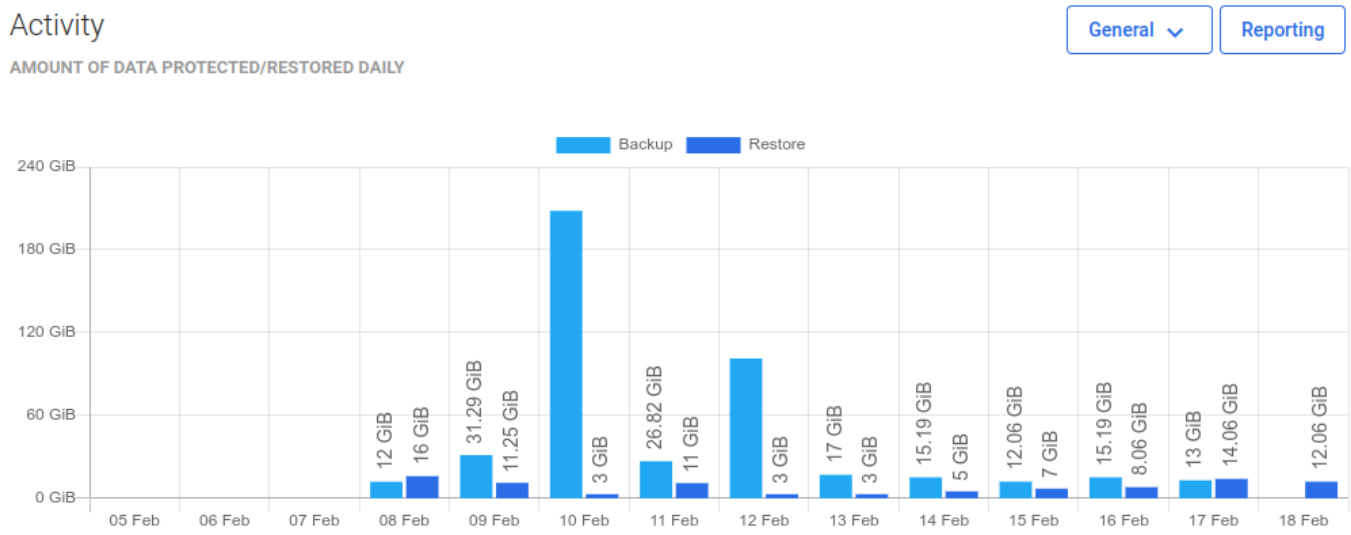


Note: You can use the **Export** button to send reports with backup and restore statistics by email or export them as PDF or HTML.

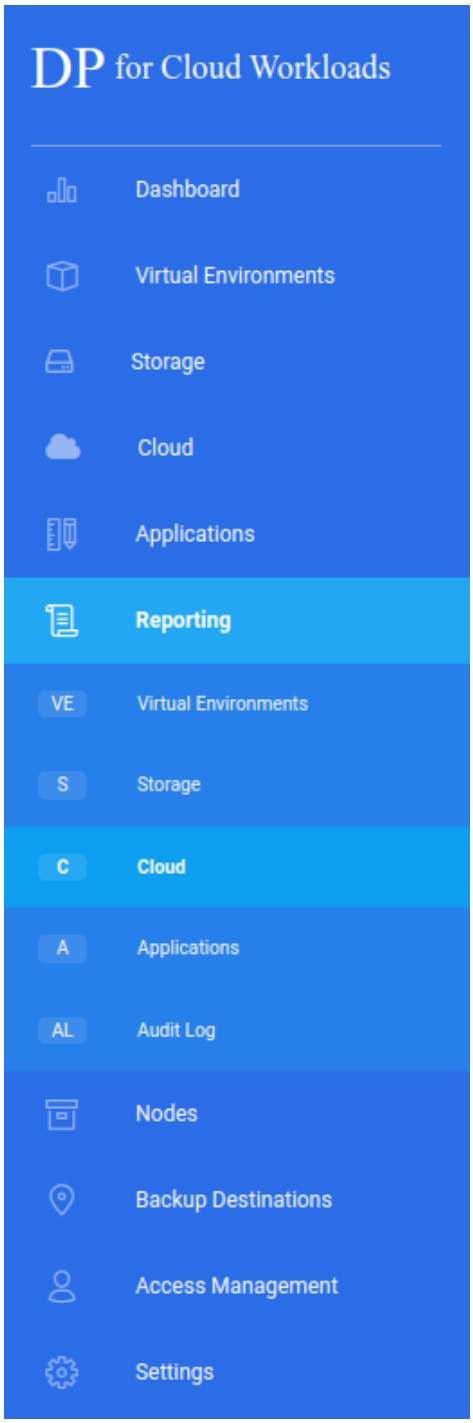
Cloud

General

Data Protector for Cloud Workloads provides a reporting feature for obtaining information about historical activities. You can reach this from the main dashboard under the Activity section via the **Reporting** button.

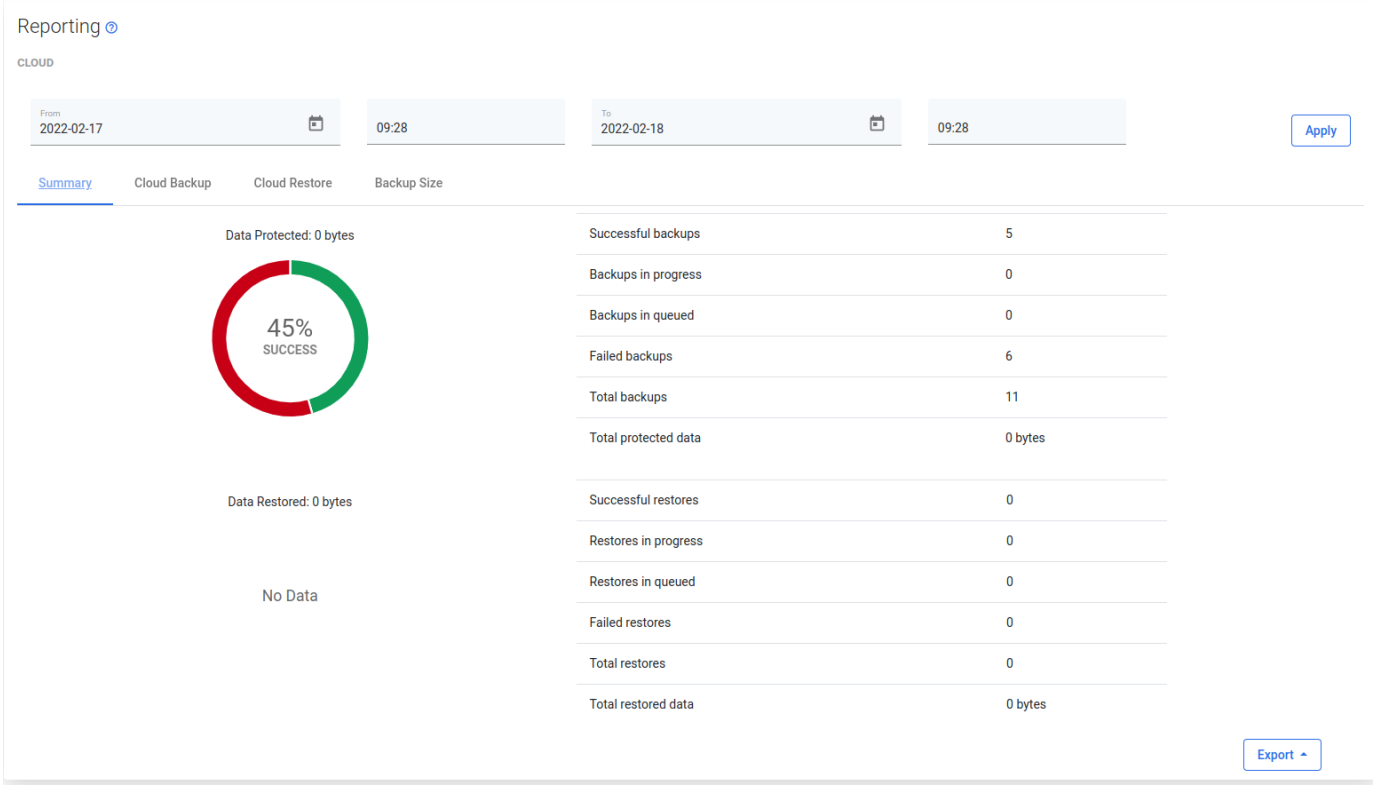


Or on the left side menu - **Reporting** -> **Cloud**.

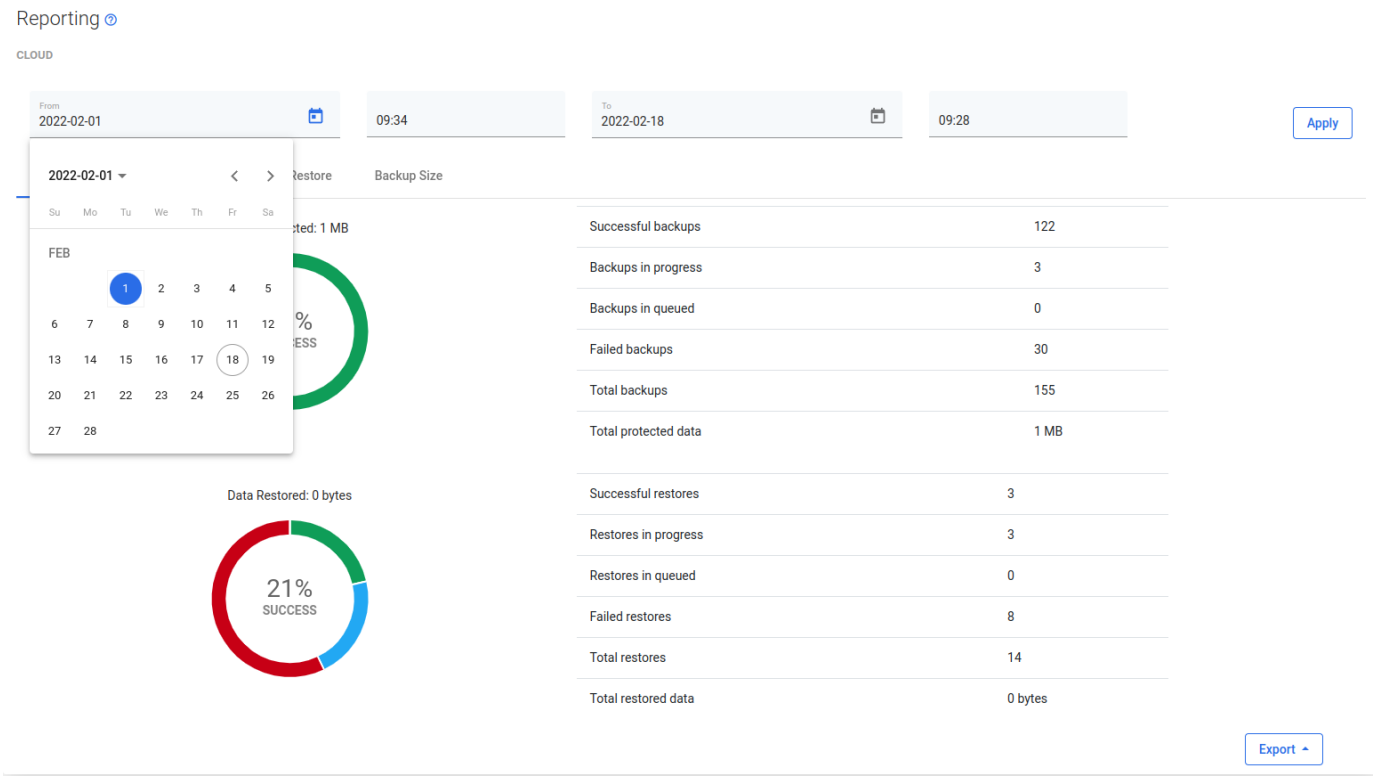


Summary

In the beginning, you should see the summary page.



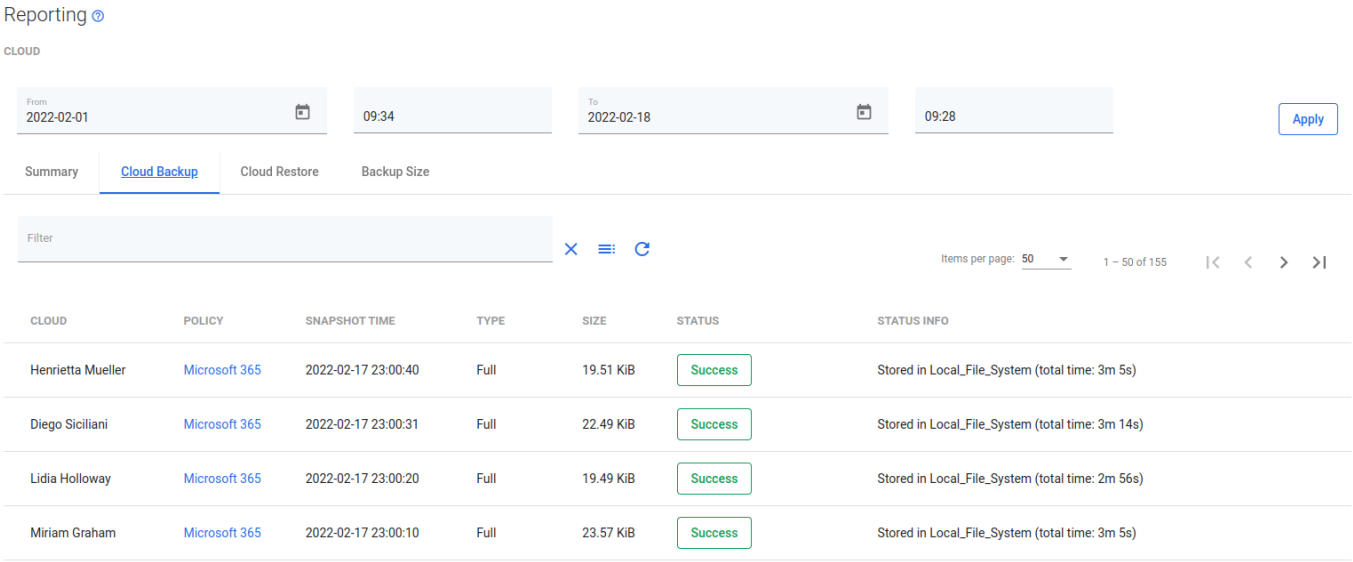
From here, you can set a date range or go to a detailed summary of backup, restore jobs, and backup size.



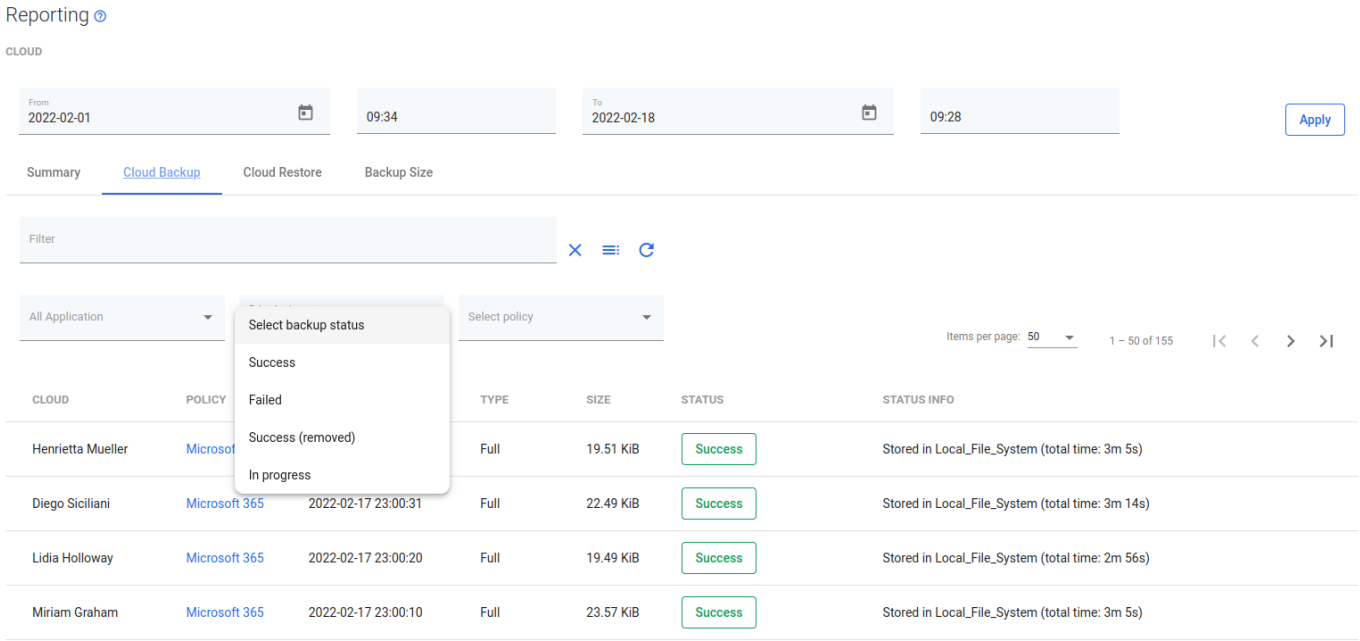
Now that you have set the date you are interested in, you can move to the next tabs to view details of each task performed by Data Protector for Cloud Workloads.

Backup Statistics

Now you can see all the tasks completed within the set date, or ...

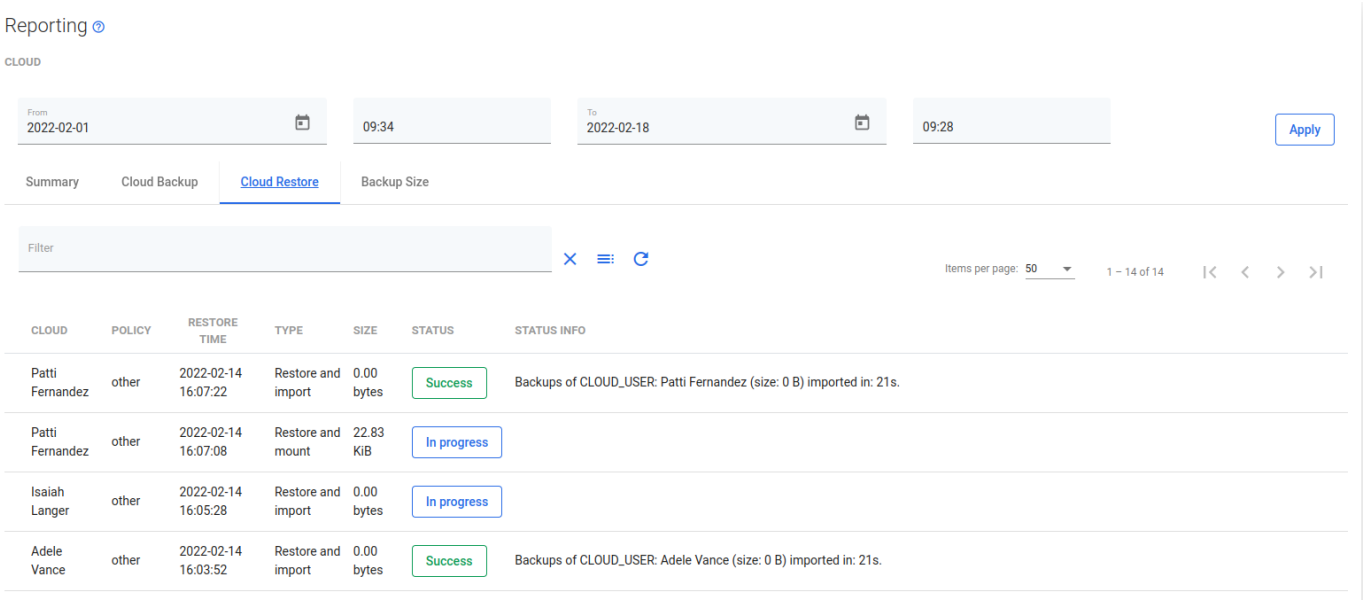


additionally filter them by status, rules, or instance.



Restore Statistics

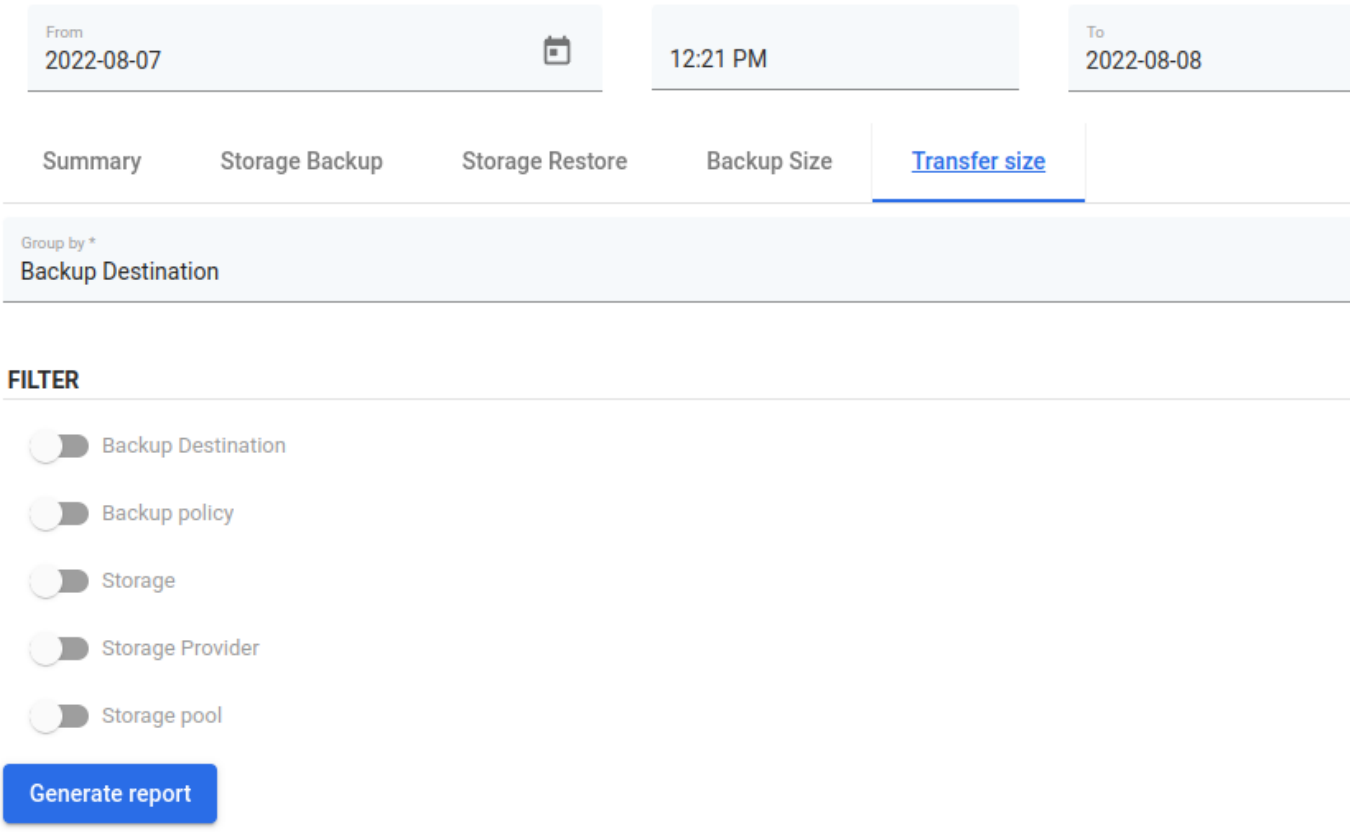
The functionality is the same as for the backup statistics, you can see all the tasks completed within the set deadline or filter them by status, policy, or instance.



Report sections that you might need for chargeback reporting:

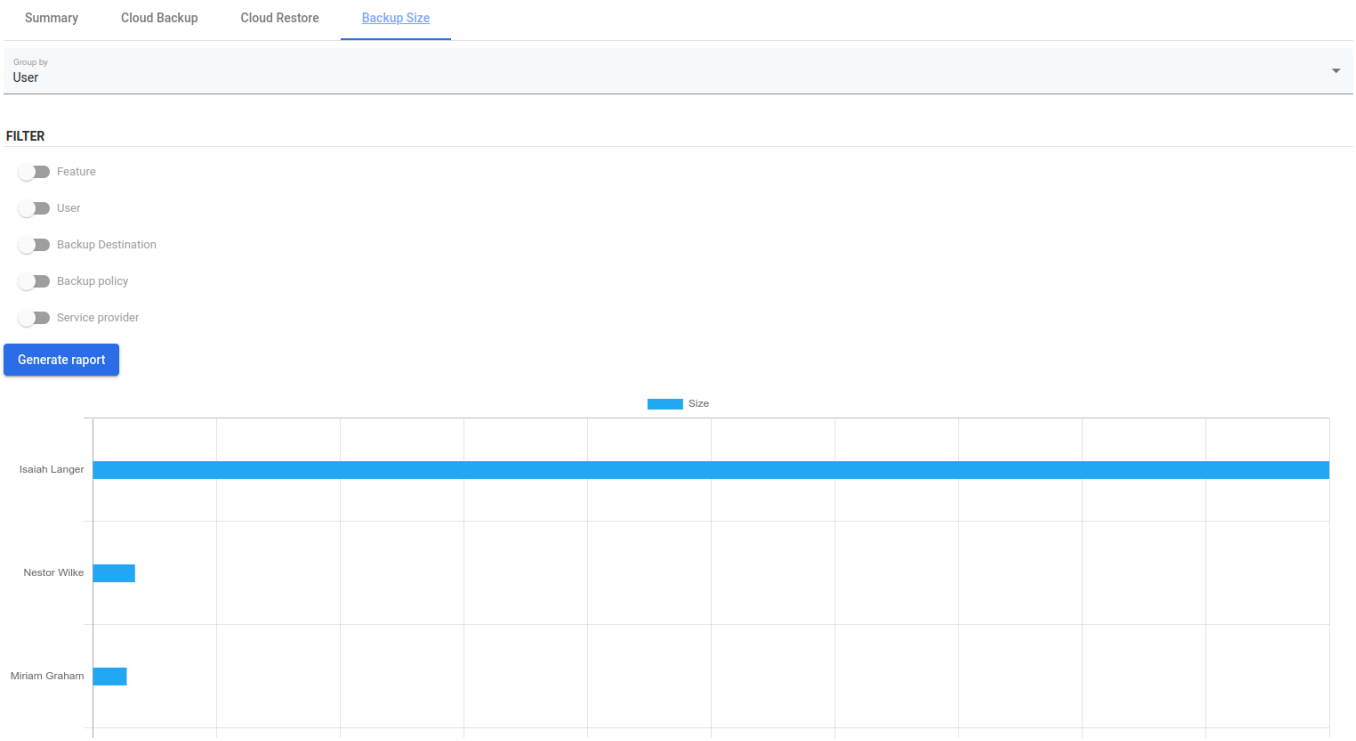
Transfer Size

Transfer size tab shows the amount of data transferred during the backup operations.



Backup Size

Backup Size section shows the current exported data.

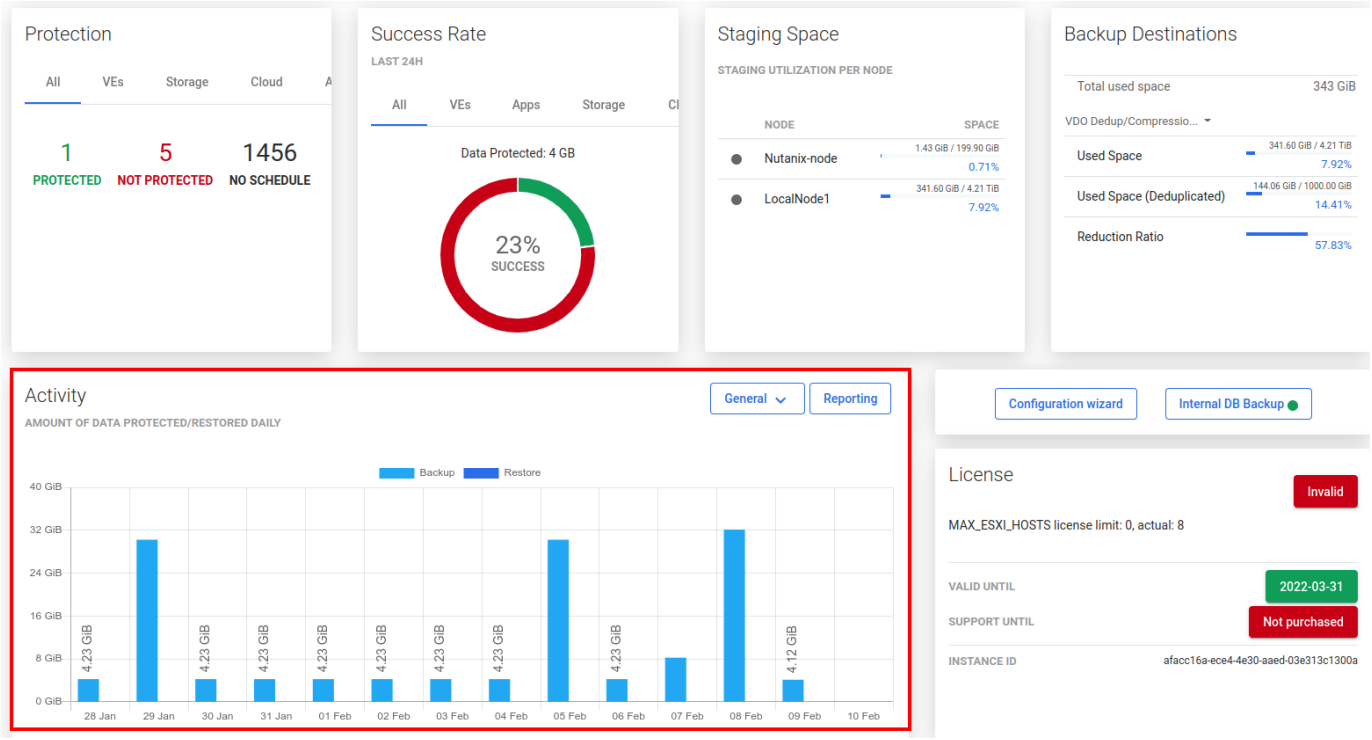


Note: You can use the **Export** button to send reports with backup and restore statistics by email or export them as PDF or HTML.

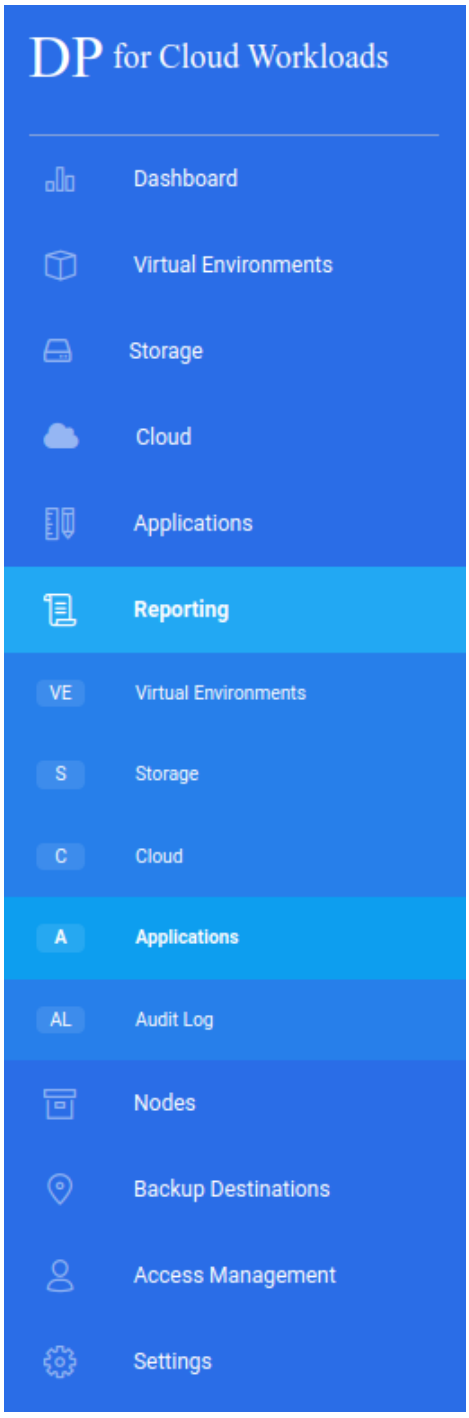
Applications

General

Data Protector for Cloud Workloads provides reporting functionality to obtain information on historical activity.
You can reach them from the main dashboard in the "Activity" section with the button **Reporting**.

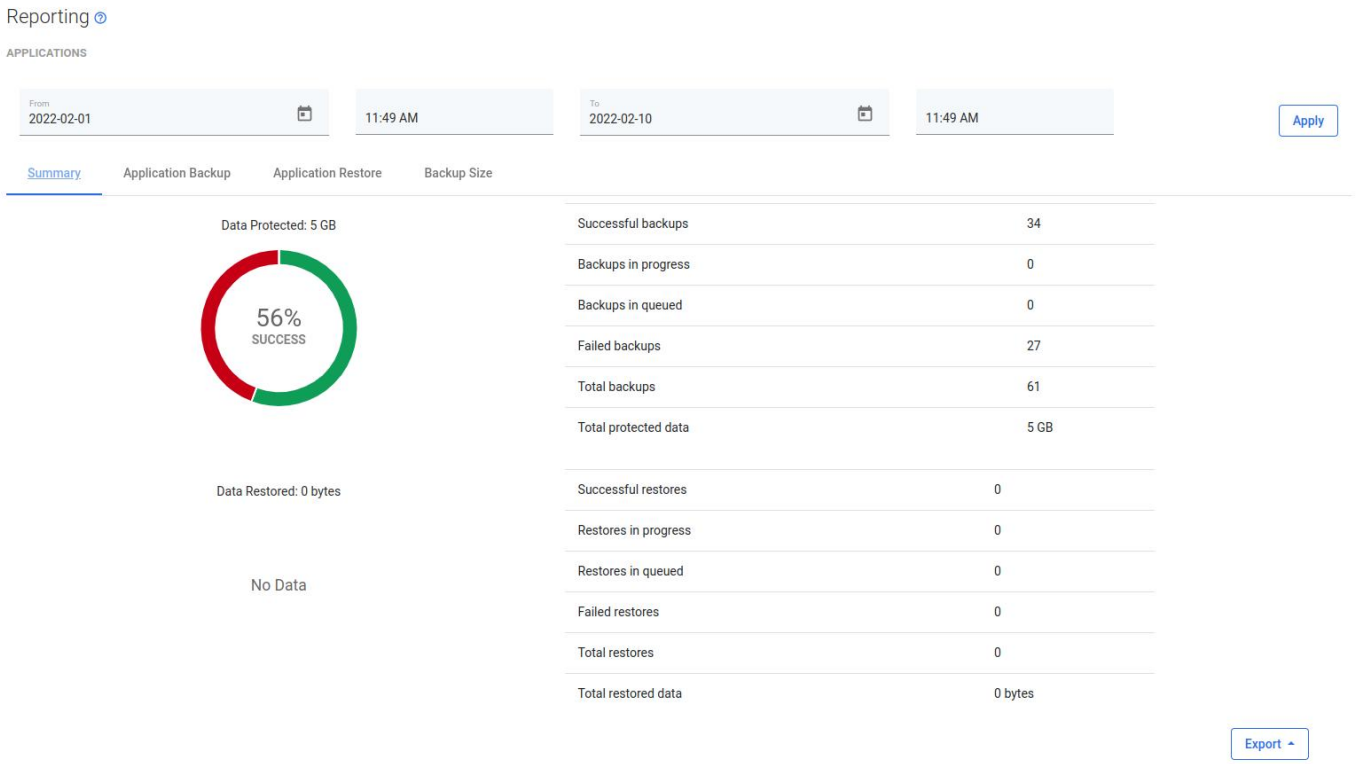


You can also open the Application reports in the reporting section from the left menu.

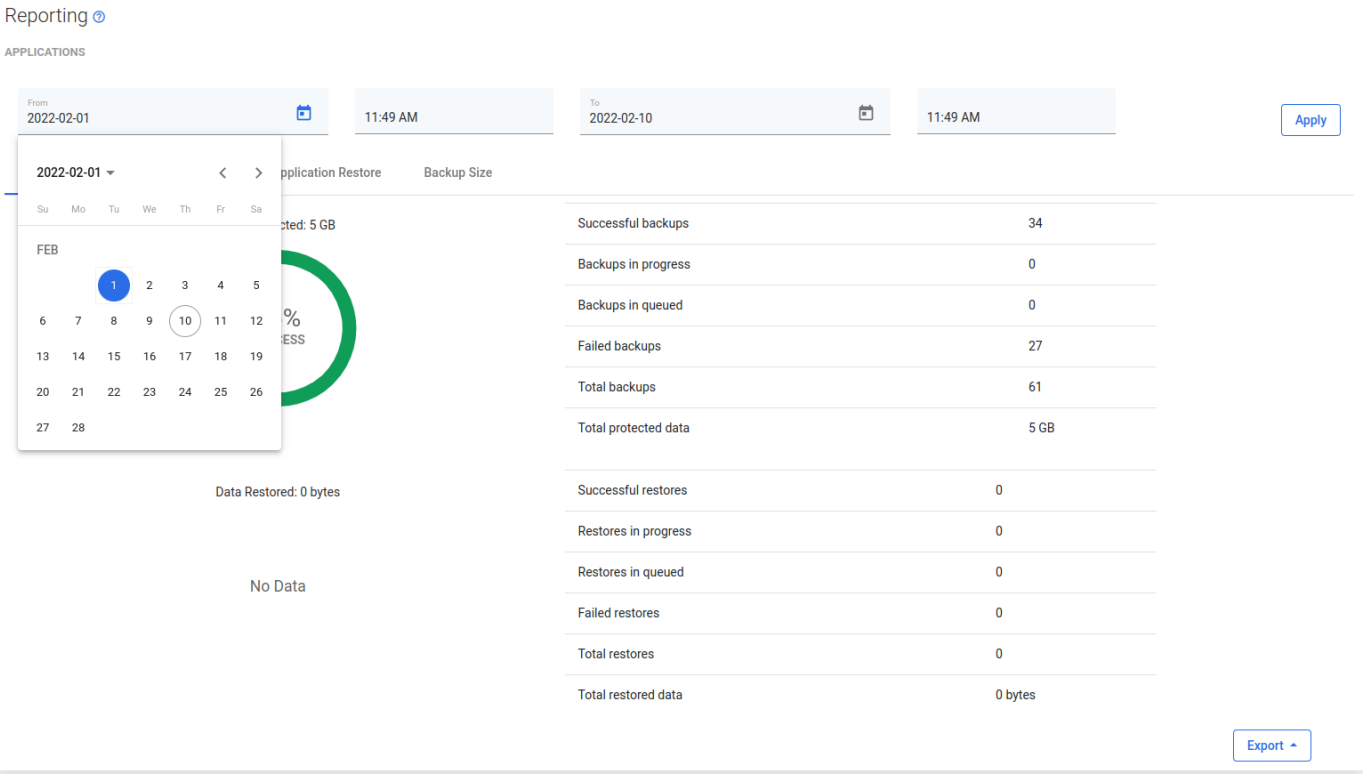


Summary

In the beginning, you should see the summary page



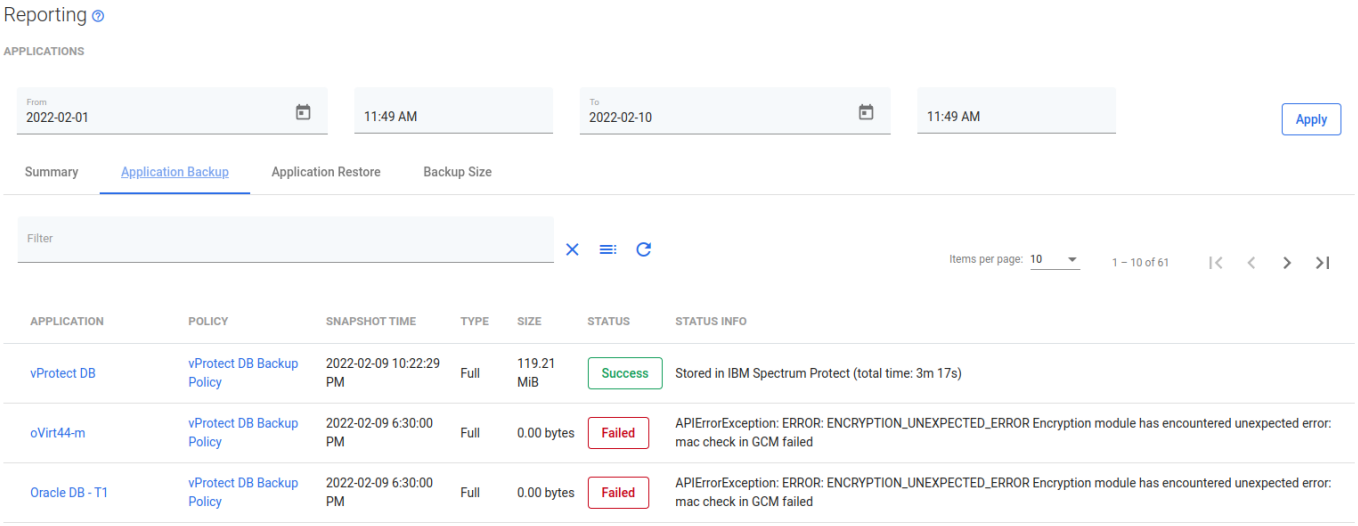
From here, you can set a date range or go to a detailed summary of backup, restore jobs, and backup size.



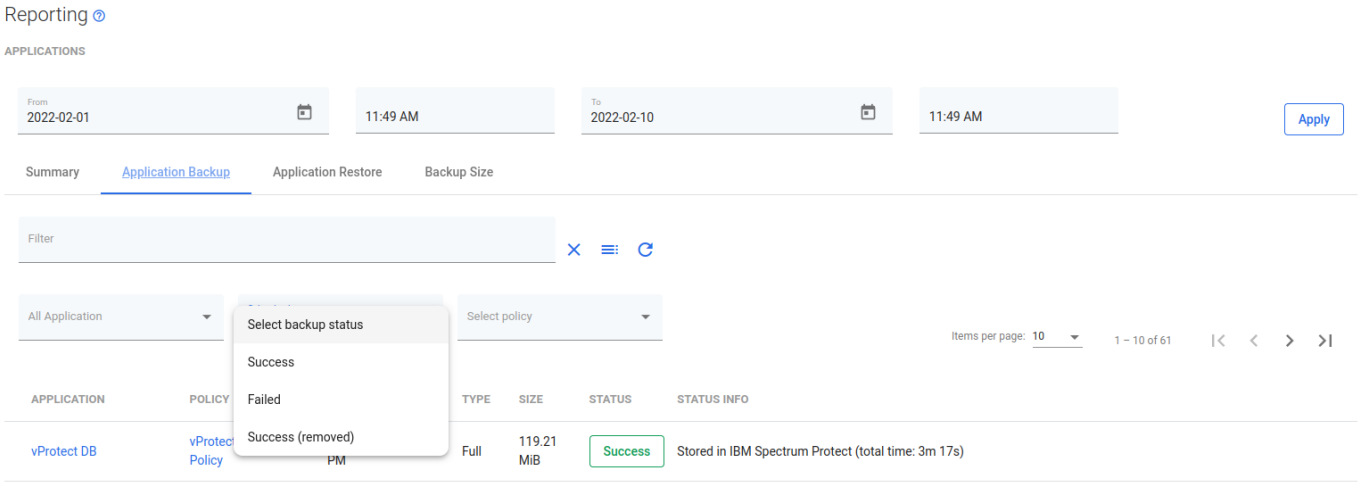
Now that you have set the date you are interested in, you can move to the next tabs to view details of each task performed byData Protector for Cloud Workloads.

Backup Statistics

Now you can see all tasks completed within the set date or ...

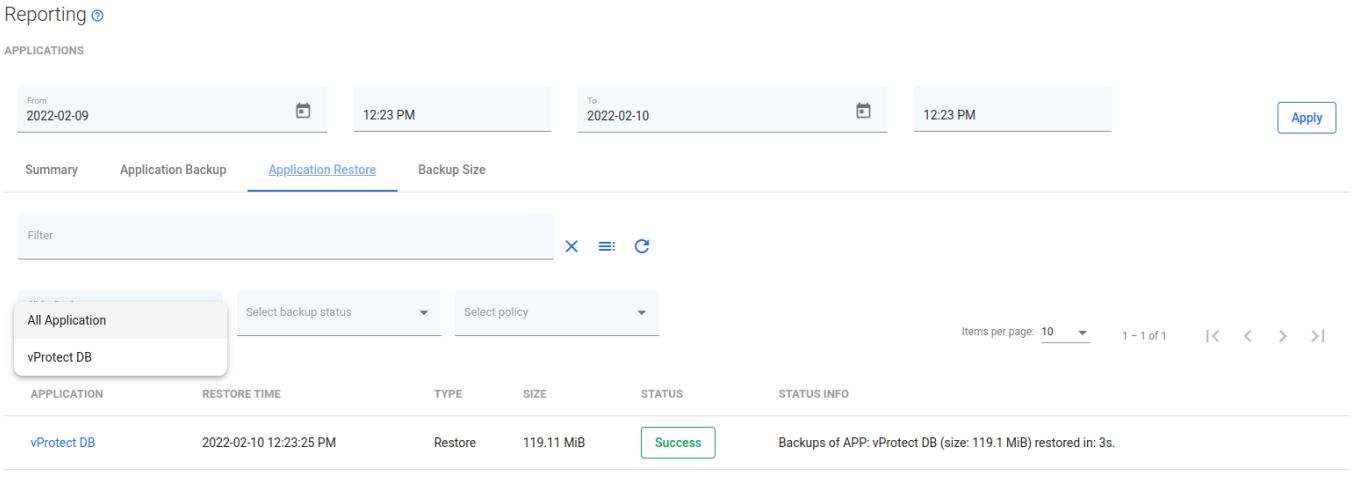


additionally filter them by status, rules, or instance.



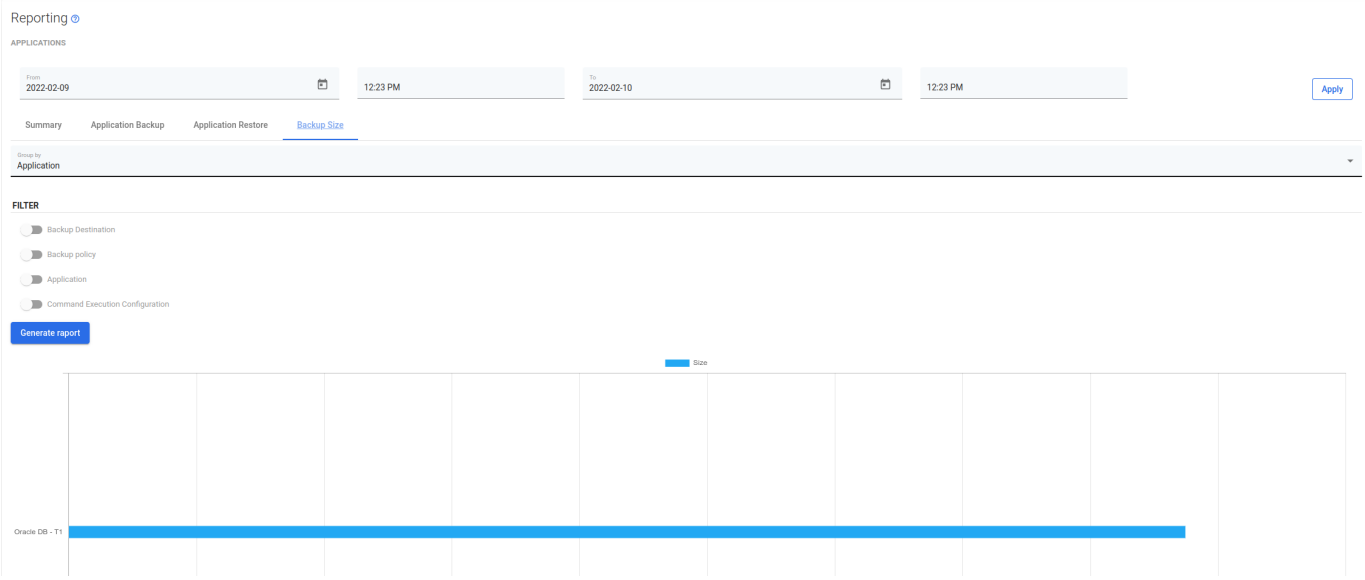
Restore Statistics

The functionality is the same as for the backup statistics, you can see all tasks completed within the set deadline or filter them by status, policy, or instance.



Backup Size

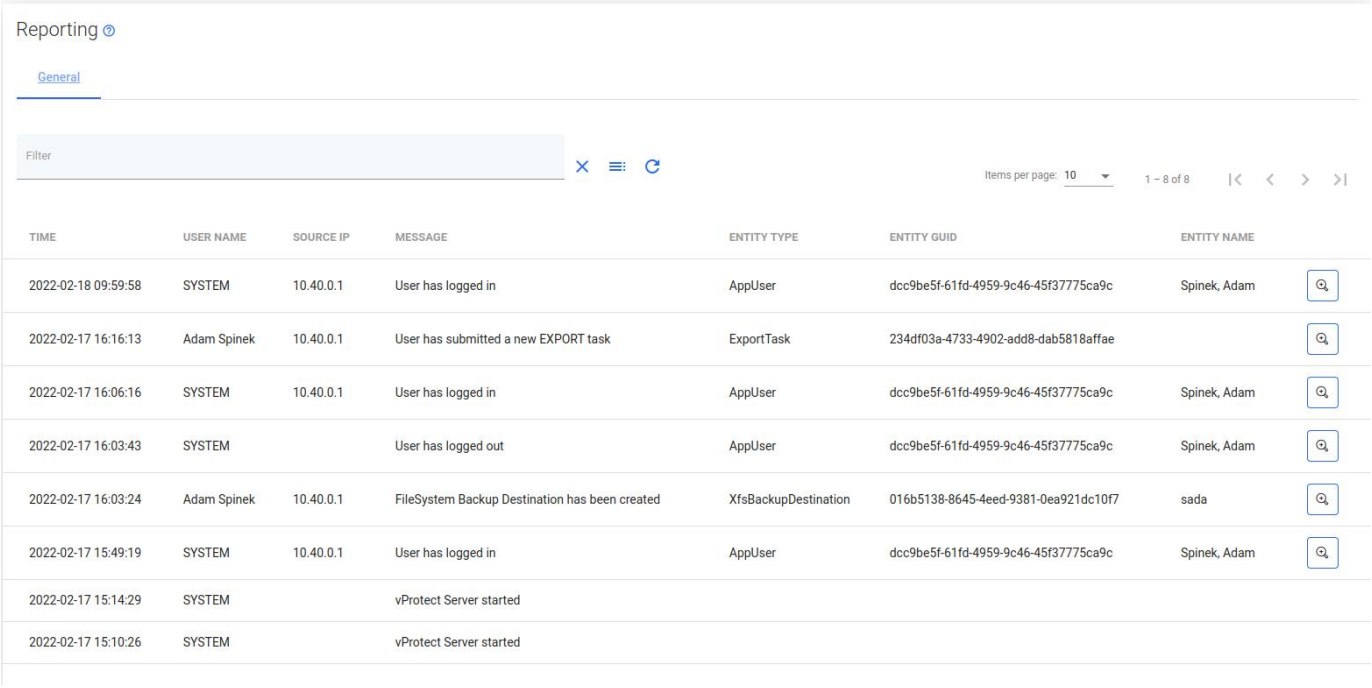
This is a backup size report that you might need for chargeback reporting.



Note: You can use the **Export** button to send reports with backup and restore statistics by email or export them as PDF or HTML.

Audit Log

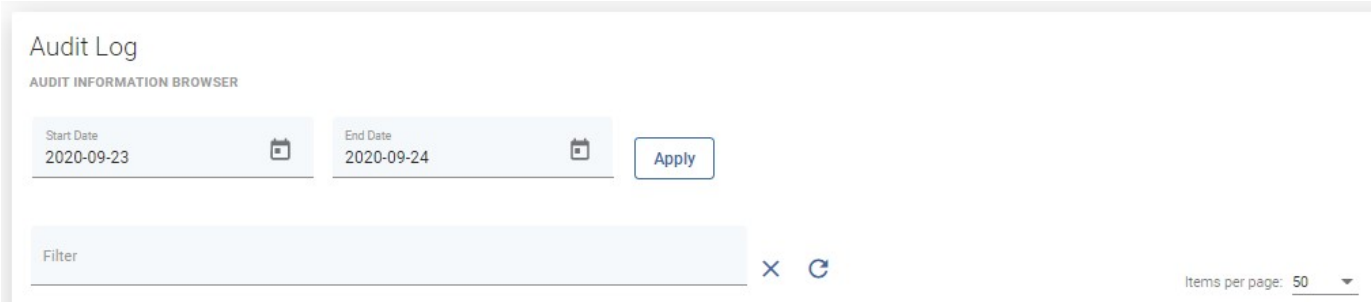
You can open the Audit log under the reporting section using the left side menu to see what has happened lately in the Data Protector for Cloud Workloads environment.



TIME	USER NAME	SOURCE IP	MESSAGE	ENTITY TYPE	ENTITY GUID	ENTITY NAME
2022-02-18 09:59:58	SYSTEM	10.40.0.1	User has logged in	AppUser	dcc9be5f-61fd-4959-9c46-45f37775ca9c	Spinek, Adam
2022-02-17 16:16:13	Adam Spinek	10.40.0.1	User has submitted a new EXPORT task	ExportTask	234df03a-4733-4902-add8-dab5818affae	
2022-02-17 16:06:16	SYSTEM	10.40.0.1	User has logged in	AppUser	dcc9be5f-61fd-4959-9c46-45f37775ca9c	Spinek, Adam
2022-02-17 16:03:43	SYSTEM		User has logged out	AppUser	dcc9be5f-61fd-4959-9c46-45f37775ca9c	Spinek, Adam
2022-02-17 16:03:24	Adam Spinek	10.40.0.1	FileSystem Backup Destination has been created	XfsBackupDestination	016b5138-8645-4eed-9381-0ea921dc10f7	sada
2022-02-17 15:49:19	SYSTEM	10.40.0.1	User has logged in	AppUser	dcc9be5f-61fd-4959-9c46-45f37775ca9c	Spinek, Adam
2022-02-17 15:14:29	SYSTEM		vProtect Server started			
2022-02-17 15:10:26	SYSTEM		vProtect Server started			

As you can see, you can easily check who logged in / out or what task was done.

Thanks to the filter section at the top of the page, you can easily choose a date range or enter a keyword.



You can also open the task details page using the magnifier icon on the right.

Details


```
guid: "9e96b226-ba7d-44af-9f85-4d3914b766e4"
parentTask: null
type: "EXPORT"
restoreType: null
state: "QUEUED"
statusInfo: null
windowStart: 1644491280000
windowEnd: 1644509280000
progressChange: null
creationTime: 1644491300000
startTime: null
finishTime: null
progress: 0
priority: 50
retryCount: 0
processedObjectCount: null
totalObjectCount: null
▸ protectedEntity: Object {"guid":"ceb68089-266a-4575-9678-f1fcf42dba2c","name":"vProtect DB","typ
protectedEntityDisplayName: "vProtect DB"
dstProtectedEntity: null
protectedEntitySnapshot: null
hypervisor: null
hypervisorManager: null
storageProvider: null
cloudServiceProvider: null
▸ backup: Object {"guid":"e50b8d80-611a-40f3-88f9-5235150748f2","name":"vProtect DB - 2022-02-10 1
```

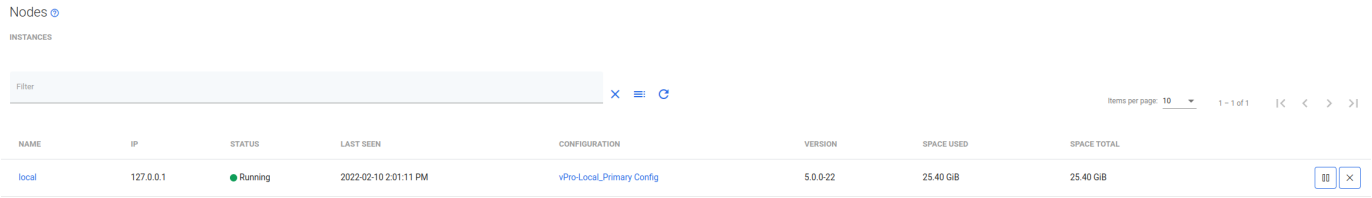
Nodes

In this chapter, You will know how to manage Data Protector for Cloud Workloads Node and how to create Data Protector for Cloud Workloads Node configurations

Instances

Node Instances

Node instances are a list of the Data Protector for Cloud Workloads Nodes that currently exist in your environment. You can easily check basic information about the nodes or change the assigned node configuration.

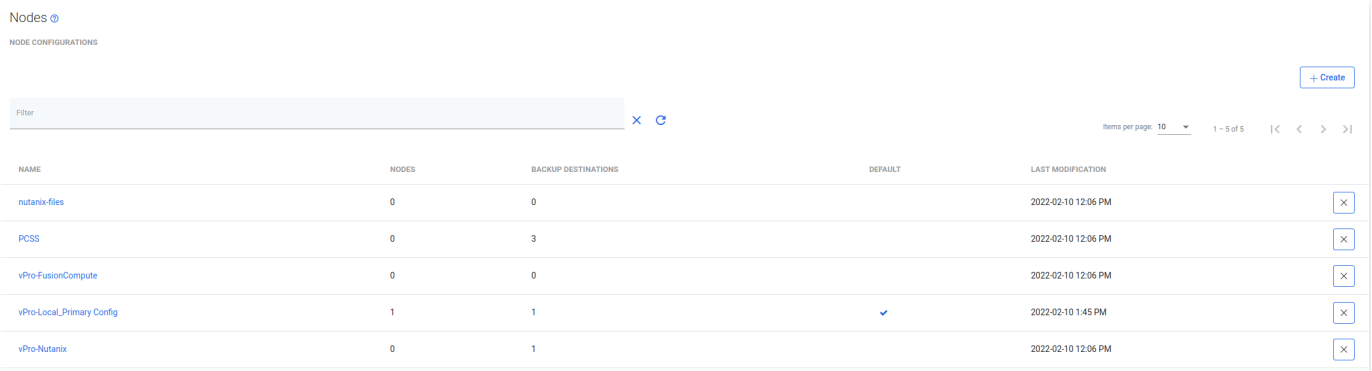


Node Configurations

> **Note:** You can also perform the same action thanks to the CLI interface: CLI Reference

Node configurations are groups of settings assignable to a set of nodes. This is so that you don't have to change them on every node separately.

> **Note:**
>
> - The task-to-node assignment will be executed via the task's hypervisor/hypervisor manager/storage provider/application/cloud related to the node configuration where the system will decide on the specific node assigned to the aforementioned configuration responsible for executing the task.



Available settings

General

- `Name` - unique name identifying the configuration
- `Set as default` - set default configuration to be assigned to new nodes

Storage

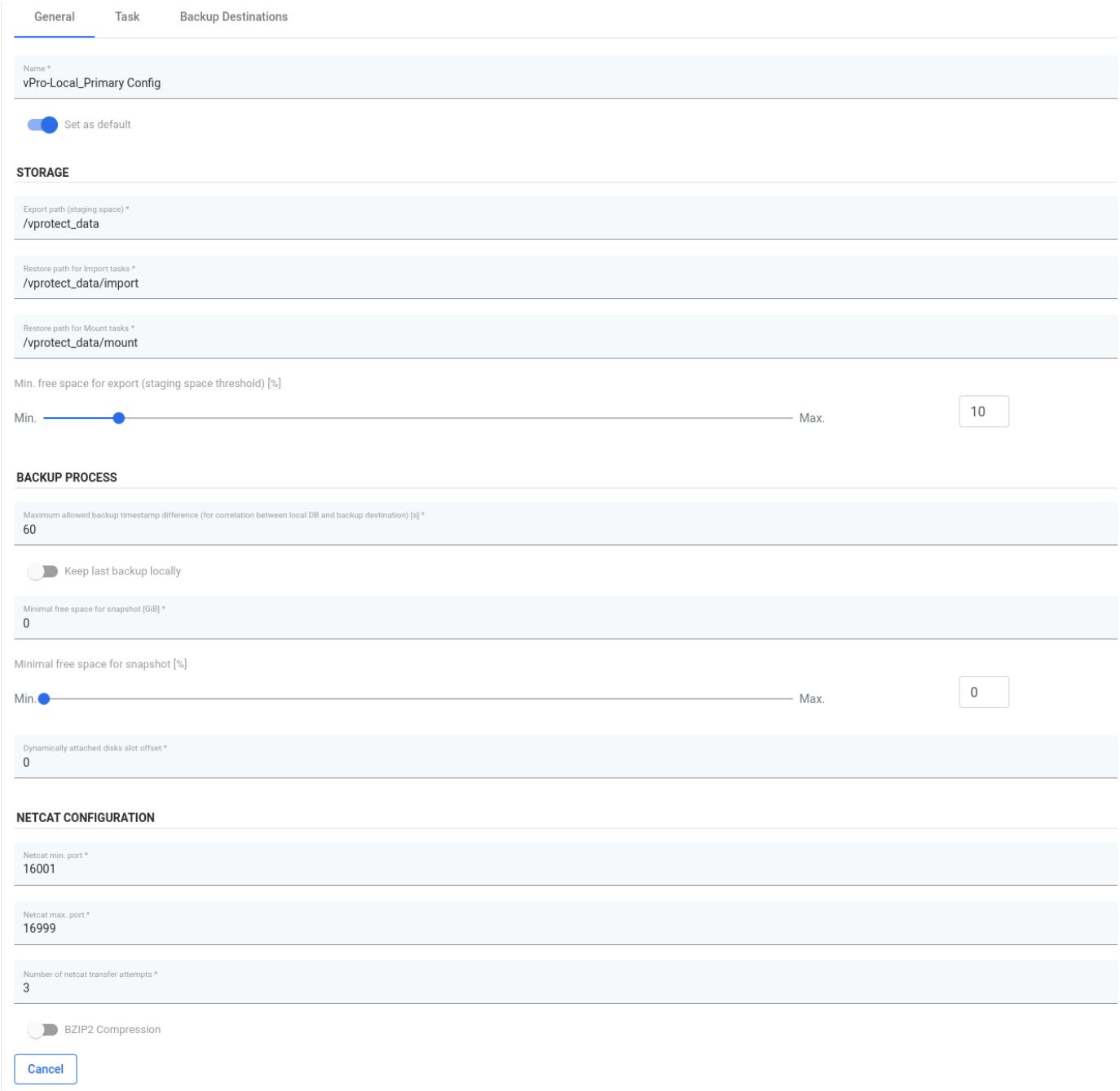
- `Export path (staging space)` - staging path (must be owned by the `vprotect` user)
- `Restore path for import tasks` - in rare cases, you may want to restore backups to a custom location within the node before the import process begins
- `Restore path for mount tasks` - in rare cases, you may want to restore backups to a custom location within the node before the mounting process begins
- `Min. free space for export [%]` - the amount of storage space left in order to force a node to wait before starting another export task

Backup Process

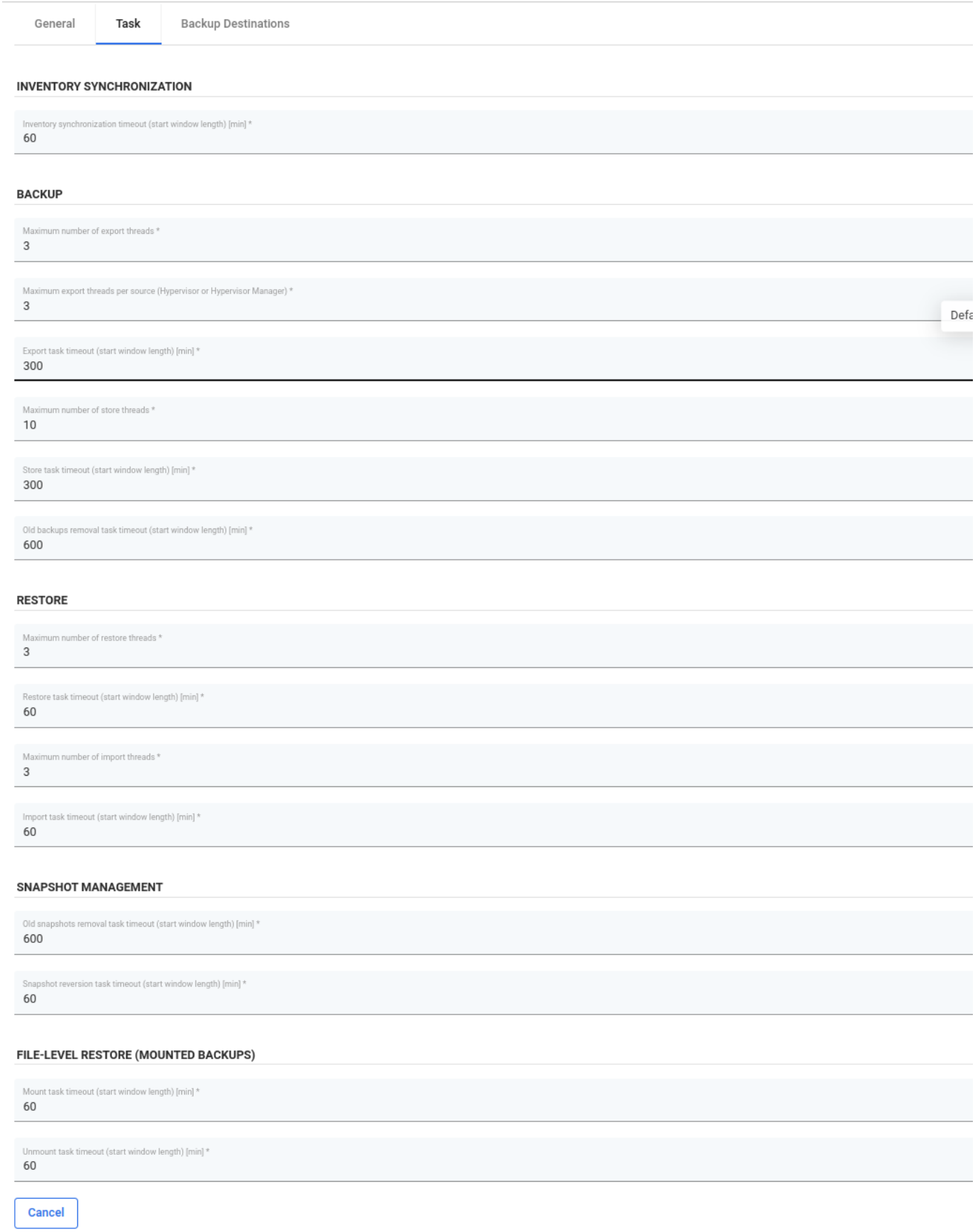
- `Max. allowed backup timestamp difference [s]`- maximum time difference between the timestamp of a backup in Data Protector for Cloud Workloads and the backup destination in order to match the local version of the backup with the remote one
- `Minimal free space for snapshot [GB]` - the amount of storage space left in order to force a node to wait before starting another task
- `Minimal free space for snapshot [%]` - the amount of storage space left in order to force a node to wait before starting another task
- `Dynamically attached disks slot offset` - this setting forces a shift of a disk slot number that the node reads/writes from when the disk-attachment method is used - currently used in the Nutanix disk-attachment method when you have block devices not reported by the hypervisor API, such as iSCSI mounted block devices. When set to 0, Data Protector for Cloud Workloads will mount drives just after the last occupied (and reported by

the hypervisor API) slot (which means that block device number 3 in API will be /dev/sdc in OS). In general, N means that Data Protector for Cloud Workloads will shift N slots, so 1 will make the 3rd device be treated as the 4th in OS /dev/sdd)

- `Netcat min. port` - min. Netcat port range
- `Netcat max. port` - max. Netcat port range
- `Number of netcat transfer attempts` - maximum number of attempts
- `BZIP2 Compression` - compress backup files with bzip2



Task



INVENTORY SYNCHRONIZATION

- `Inventory synchronization timeout (start window length) [min]` - default length of the start window for index tasks

BACKUP

- `Maximum number of export threads` - max. number of export tasks per node (total)

- `Maximum export threads per source (HV or HVM)` - max. number of export tasks per node and per HV/HVM
- `Export task timeout (start window length) [min]` - default length of the start window for export tasks
- `Maximum number of store threads` - max. number of store tasks per node
- `Store task timeout (start window length) [min]` - default length of the start window for store tasks
- `Old backups removal task timeout (start window length) [min]` - default length of start window for old backup removal tasks

RESTORE

- `Maximum number of restore threads` - max. number of restore tasks per node (total)
- `Restore task timeout (start window length) [min]` - default length of start window for restore tasks
- `Maximum number of import threads` - max. number of import tasks per node (total)
- `Import task timeout (start window length) [min]` - default length of the start window for import tasks

SNAPSHOT MANAGEMENT

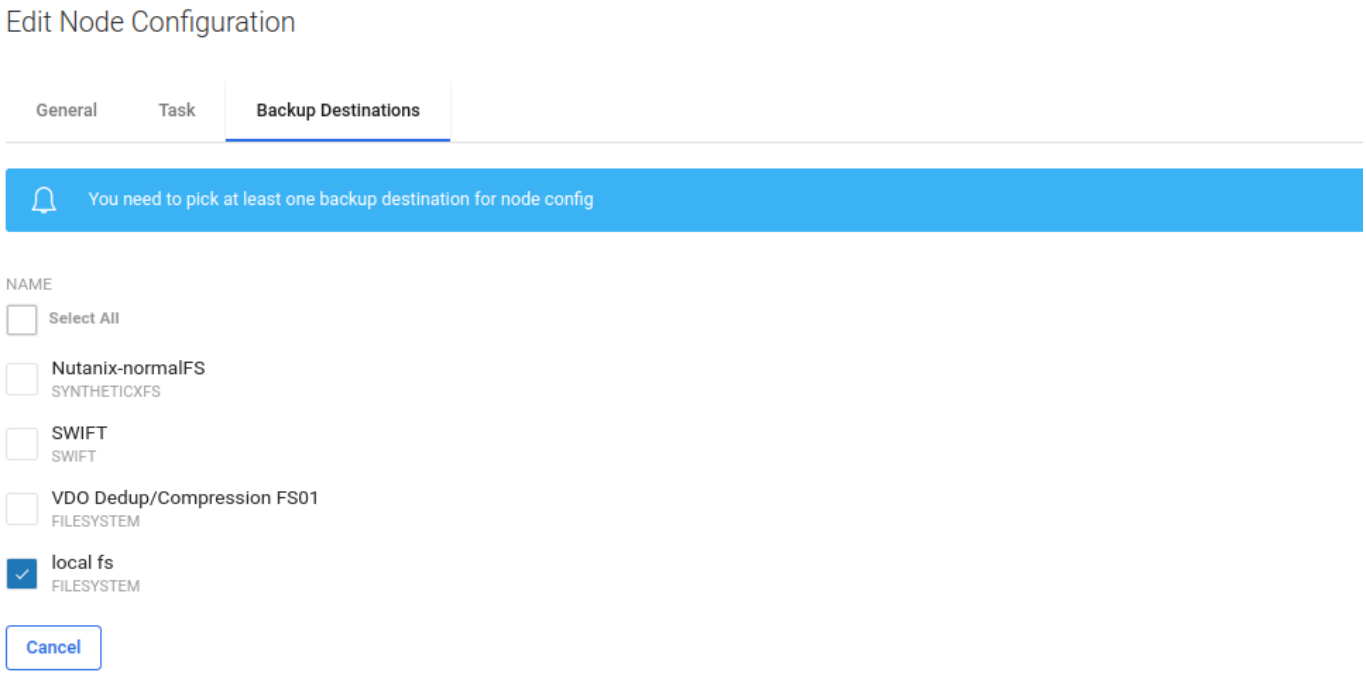
- `Old snapshot removal task timeout (start window length) [min]` - default length of start window for old snapshot removal tasks
- `Snapshot reversion task timeout (start window length) [min]` - default length of start window for snapshot reversion tasks

FILE-LEVEL RESTORE (MOUNTED BACKUPS)

- `Mount task timeout (start window length) [min]` - default length of start window for mount tasks
- `Unmount task timeout (start window length) [min]` - default length of start window for unmount tasks

Backup destinations

This section is used to add/remove backup destinations to the nodes using this configuration. Only backup destinations enabled here can be used by the nodes.



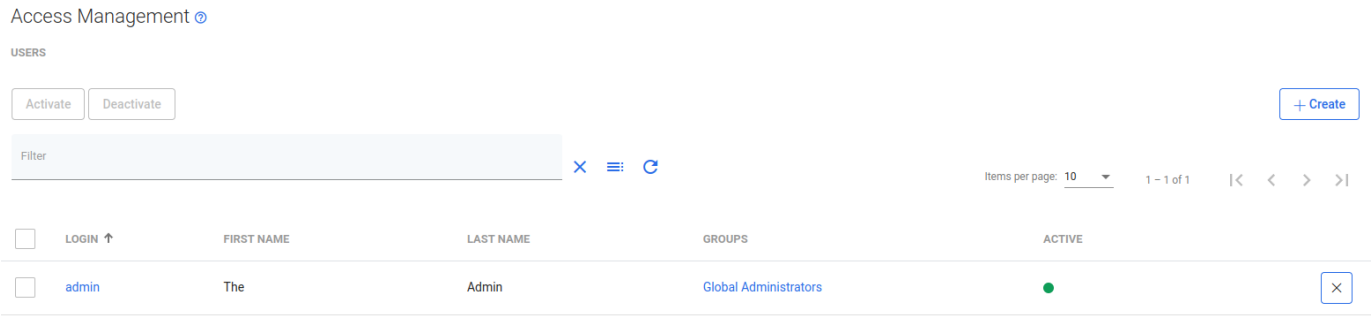
Access Management

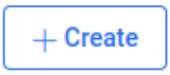
This section allows you to manage Users, Groups, and Roles. The role is a set of permissions in Data Protector for Cloud Workloads. Users can belong to multiple groups. Each group can have multiple roles assigned.

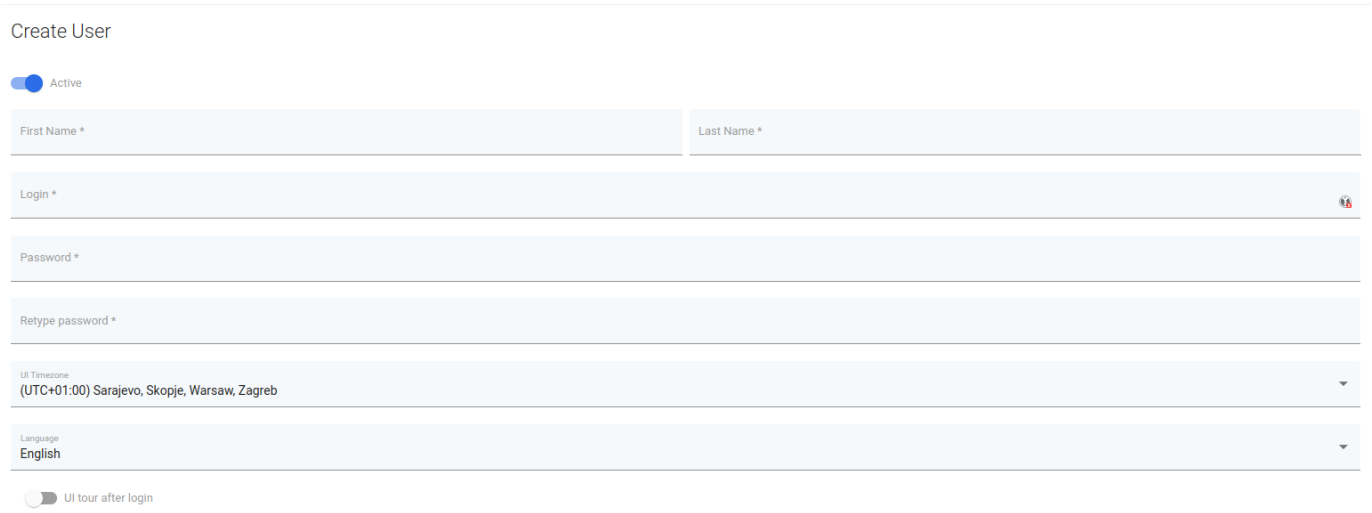
Users

There are two types of users:

- local users
- LDAP users (please refer to how setup LDAP authentication)



To create a new user, click the button on the right 



Complete the following parameters:

- First Name
- Last Name
- Password
- Timezone
- Language

Save, and now you can add this account to the specific group. In the Groups section, click on the name of the group and add a user.

Groups

Group is a central place to bind together a set of roles with users. There are already a set of predefined groups in Data Protector for Cloud Workloads.

> **Note:**
>
> - Automatically created accounts based on LDAP logins will have the `Operator` role by default.
> - Current group management is available in Data Protector for Cloud Workloads WebUI only (they are not mapped to LDAP groups)

Roles

The Role is a set of permissions to the different sections and actions in Data Protector for Cloud Workloads. When multiple roles are assigned to the Group, the resulting permissions will be the sum of all permissions from all assigned roles.

> **Note:**
>
> - It is mandatory to have always at least one account with permission to manage Users
> - in other words: at least one account must be assigned to the group, which has a role with this permission.

Permissions

Section (Name)	Permission	Allows
Nodes	Instances	Read - allows you to view the list of instances and basic information Register - allows you to register new nodes in the environment Write - allows you to change selected node config Delete - allows you to remove a node from the environment
Nodes	Node Configurations	Read - allows you to browse the list of configs and open them Write - allows you to modify existing configs and create new ones
Virtual Environments	Instances	Read - allows you to browse the list of instances and open them Write - allows you to modify virtual machine settings Backup - allows you to perform a manual backup Restore - allows you to perform a manual restore Snapshot - allows you to perform a manual snapshot Mount - allows you to mount a backup for file-level restore Clean old Snapshot - allows you to perform the "Clean old snapshot" task
Virtual Environments	Infrastructure	Read - allows you to browse the list of infrastructure objects for all tabs Write - allows you to modify settings for existing objects and to add new ones Test Connectivity - This permission allows you to enable or disable access to the connectivity test
Virtual Environments	Backup SLAs	Read - allows you to browse the list of policies and schedules Write - allows you to modify the existing and add new ones

Section (Name)	Permission	Allows
Virtual Environments	Snapshot SLAs	Read - allows you to browse the list of policies and schedules Write - allows you to modify the existing and add new ones
Virtual Environments	Recovery Plans	Read - allows you to browse the list of policies and schedules Write - allows you to modify the existing and add new ones
Virtual Environments	Mounted Backups	Read - allows you to browse the list of mounted backups and also to download files Unmount - allows you to unmount a backup
Applications	Instances	Read - allows you to browse the list of instances and open them Write - allows you to modify virtual machine settings Backup - allows you to perform a manual backup Restore - allows you to perform a manual restore
Applications	Execution Configurations	Read - allows you to browse the list of execution configs Write - allows you to modify the existing and add new ones
Applications	Backup SLAs	Read - allows you to browse the list of policies and schedules Write - allows you to modify the existing and add new ones
Storage	Instances	Read - allows you to browse the list of instances and open them Write - allows you to modify storage instance settings Backup - allows you to perform a manual backup Restore - allows you to perform a manual restore Snapshot - allows you to perform a manual snapshot Mount - allows you to mount a backup for file-level restore Clean old Snapshot - allows you to perform the "Clean old snapshot" task

Section (Name)	Permission	Allows
Storage	Infrastructure	Read - allows you to browse the list of infrastructure objects for all tabs Write - allows you to modify settings for existing objects and to add new ones Test Connectivity - This permission allows you to enable or disable access to the connectivity test
Storage	Backup SLAs	Read - allows you to browse the list of policies and schedules Write - allows you to modify the existing and add new ones
Storage	Snapshot SLAs	Read - allows you to browse the list of policies and schedules Write - allows you to modify the existing and add new ones
Storage	Mounted Backups	Read - allows you to browse the list of mounted backups and also to download files Unmount - allows you to unmount a backup
Reporting	Reporting	Read - allows you to view report data for virtual machines and storage providers Send report - This permission allows you to enable or disable the ability to send the report by mail
Reporting	Audit Log	Read - This permission allows you to enable or disable access to the audit log report
Backup Destinations	Backup Destination	Read - allows you to browse the list of backup destinations Write - allows you to modify settings for existing objects and to add new ones Test Connectivity - This permission allows you to enable or disable access to the connectivity test Clean old backups - This permission allows you to enable or disable the ability to perform this task
Access Management	Access Management	Read - allows you to browse the list of objects for all access management tabs Write - allows you to modify existing objects and to add new ones Change passwords - allows you to change user passwords

Section (Name)	Permission	Allows
Settings	Settings	Read - allows you to view selected settings for all tabs in the "settings" section Write - allows you to modify settings for all tabs in the "settings" section
Tasks Console	Tasks Console	Read - this permission allows you to hide or show the "Task Console" floating panel Write - allows you to remove/cancel tasks from the list
Restore Job	Restore Job	Read - This permission allows you to enable or disable access to the information about restore tasks - under tasks console, details of virtual machine or storage instance and from recovery plans

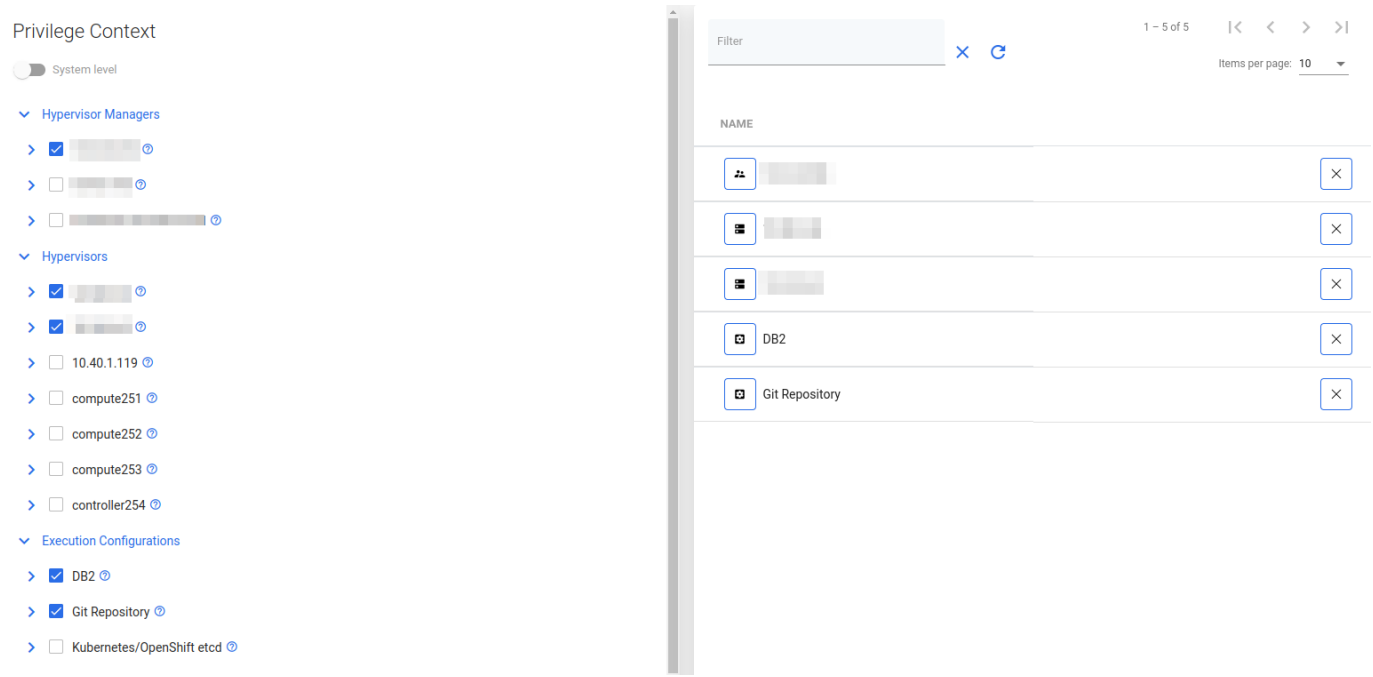
Security contexts

The security context defines the set of system objects that can be accessed with defined permissions.

The object hierarchy is constructed in a way that any defined privileges will apply to the specified object and to all the downstream objects, therefore the `System Level` security context defines the access to all objects across the platform and disables the choice of lower-level objects.

Security contexts have been aggregated into the specified hierarchy. Different system object types can have different parental objects (or none) and so will appear in the different sections of the tree.

Selected objects will be visible in the table on the right-hand side.



The full hierarchy:

- Hypervisor Managers
  - Projects
    - Virtual Environments
  - Data Centers
    - Hypervisors

            - Virtual Environments
        - Clusters
            - Hypervisors
            - Virtual Environments
        - Virtual Environments
    - Clusters
        - Hypervisors
        - Virtual Environments
    - Hypervisors
        - Virtual Environments
    - Virtual Environments
- Hypervisors
    - Virtual Environments
- Application Configurations
    - Applications
- Storage Providers
    - Storages

OS Credentials

OS Credentials are center managed settings, that let you using them for :

- executing pre or post snapshot commands
- uploading files from mounted backup

Main place when you can mange OS Credentials is **Access Management** -> **OS Credentials**. To add new credentials click **Create** button.

In the form provide:

- Name
- User
- Password
- SSH key path (optional)

Settings

In this section, you can find various general settings for Data Protector for Cloud Workloads as:

Global Settings

Internal DB Backup

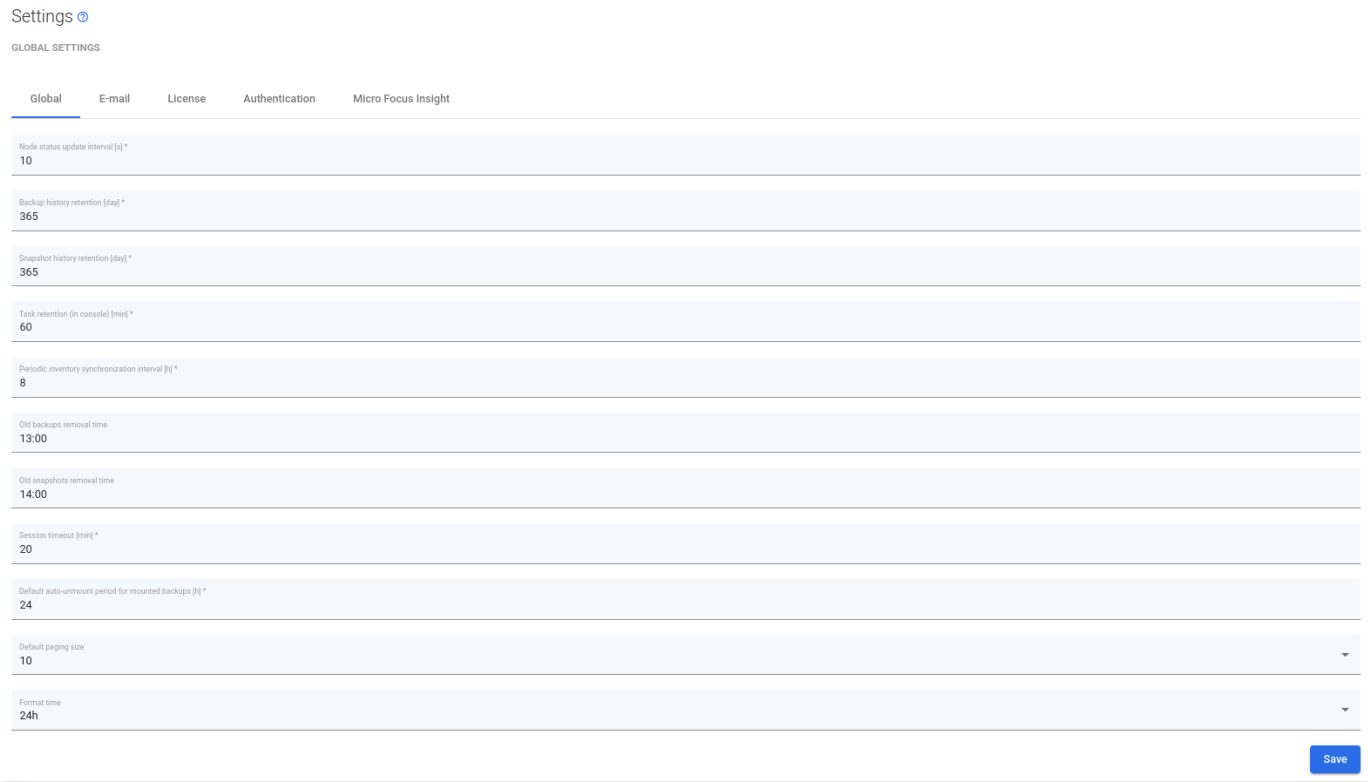
Notification Rules

Mailing Lists

Global Settings

Global

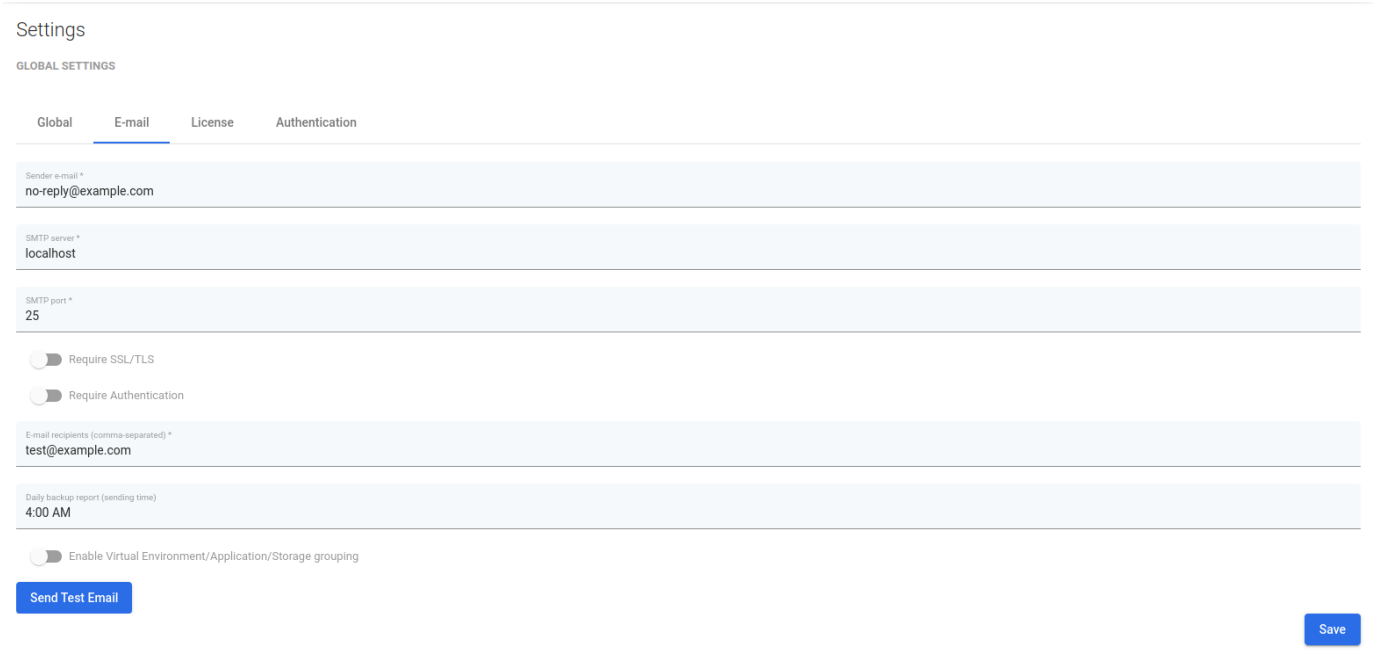
Global value settings for some retentions and schedules:



- `Node status update interval` - how often nodes should update their status
- `Backup history retention` - how long should the history of backups be kept (even removed from backup provider)
- `Task retention (in console)` - how long finished/failed tasks should be kept in the console in UI/CLI
- `Periodic inventory synchronizarion interval` - how often Data Protector for Cloud Workloads should scan for changes in VM inventory on HV/HVMs and Microsoft 365 users accounts, sites, and teams
- `Old backups removal time` - time, when daily backup destination cleanup should be invoked (for all backup destinations)
- `Old snapshots removal time` - time, when daily snapshots cleanup should be invoked (for all VMs with any policy assigned)
- `Session timeout [min]` - Session timeout [min] - the time after which you will be logged out of the WebUI
- `Default paging size` - Default value of items shown on lists
- `Format time` - you can choose between 12h and 24h time format

E-mail

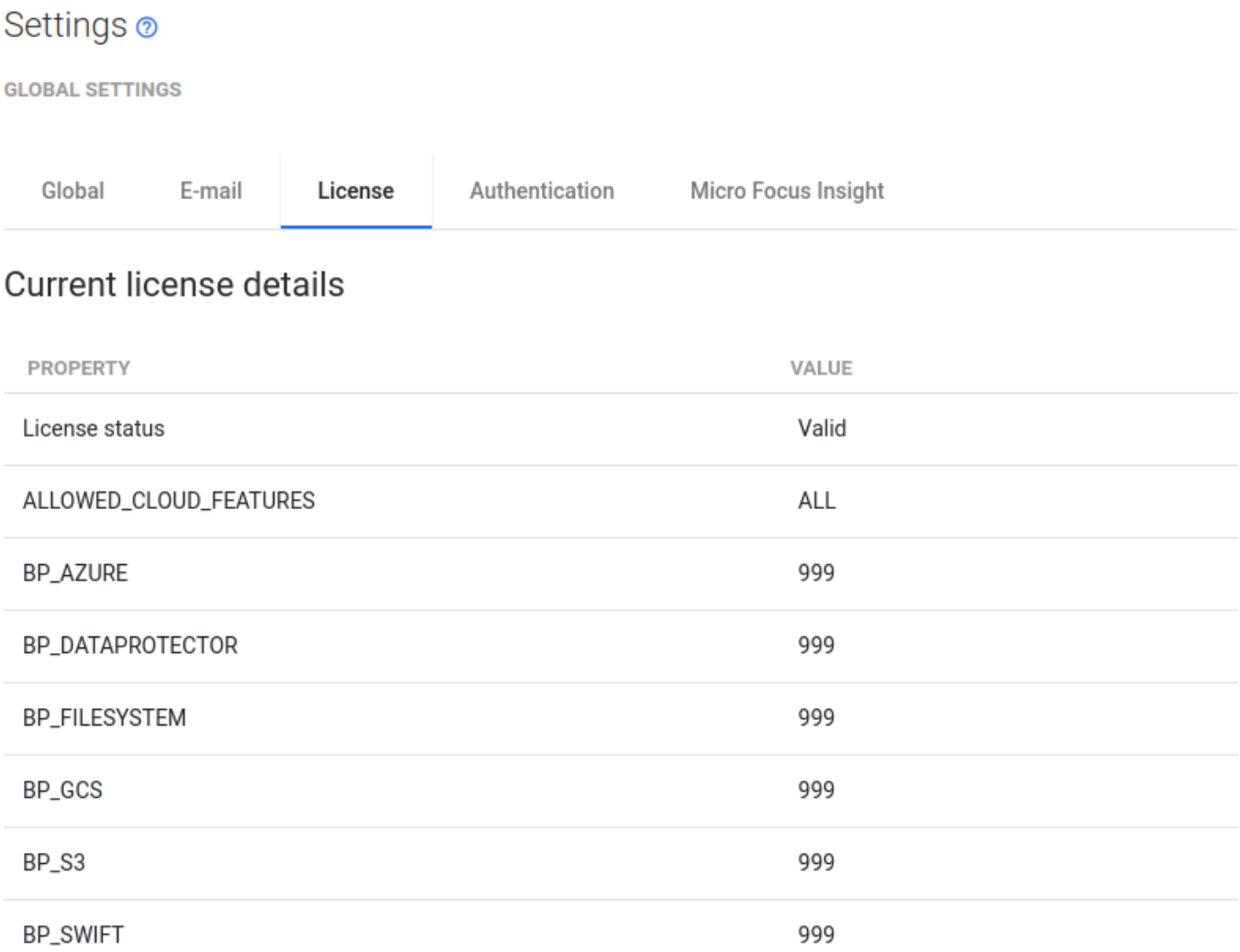
Email configuration for reports purposes



- `Sender e-mail` - address from which should e-mail be sent
- `SMTP server` - SMTP server address
- `SMTP port` - SMTP server port
- `SMTP SSL port` - SMTP SSL port (if enabled)
- `SMTP user` - SMTP account used to send e-mails
- `E-mail recipients (comma-separated)` - list of recipients of daily backup report
- `Daily backup report (sending time)` - time when daily backup report should be sent
- `Daily backup report` - sending time for summary report
- `Enable virtual environment/application grouping` - you can group environment by selected parameter

License

This section enables you to view current license status and upload a new license if necessary.

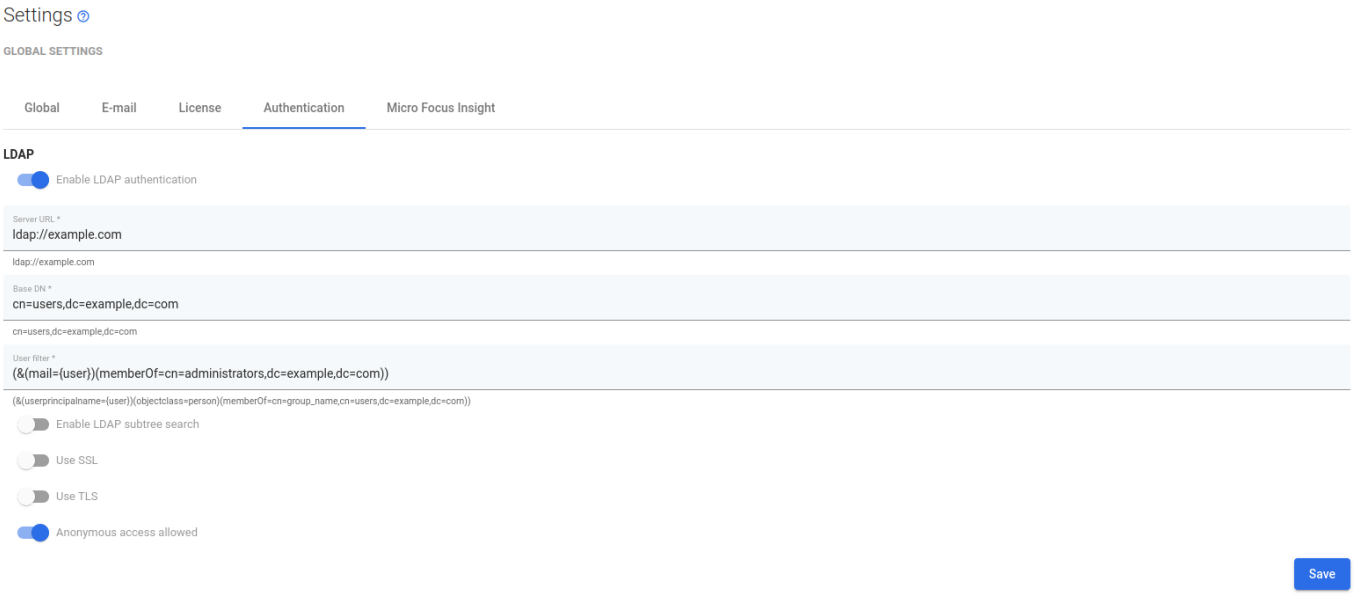


License details:

- `MAX_xxx_HOSTS` - maximum number of hosts for given platform
- `BP_xxx` - maximum number of backup destinations per backup provider type
- `EXPIRE_DATE` - trial period expiration date

Authentication

This section enables you to setup LDAP authentication for administrative accounts in Data Protector for Cloud Workloads:

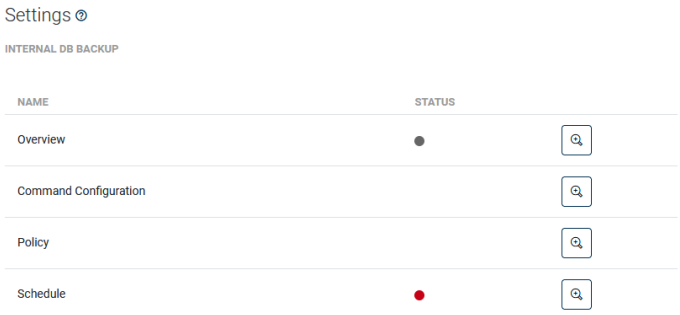


> **Note:** accounts will be added to Data Protector for Cloud Workloads automatically with the first successful login

- `Enable LDAP authentication` - enables LDAP authentication, Data Protector for Cloud Workloads will try to check for non-existing accounts in LDAP, and if authenticated successfully, a new account will appear on the list
- `Server URL` - LDAP server URL
- `Base DN` - Base DN that needs to be searched
- `User filter` - filter to be used to authenticate only users in a specific group
- `Enable LDAP subtree search` - when disabled, only 1 level below base DN is being searched
- `Use SSL` - enables SSL for LDAP connection
- `Use TLS` - enables TLS for LDAP connection
- `Anonymous access allowed` - if users are not allowed to anonymously browse LDAP directory you need to provide account which has that privilege:
- `Service account DN` - DN of the user
- `Service account password` - password of that user

Internal DB Backup

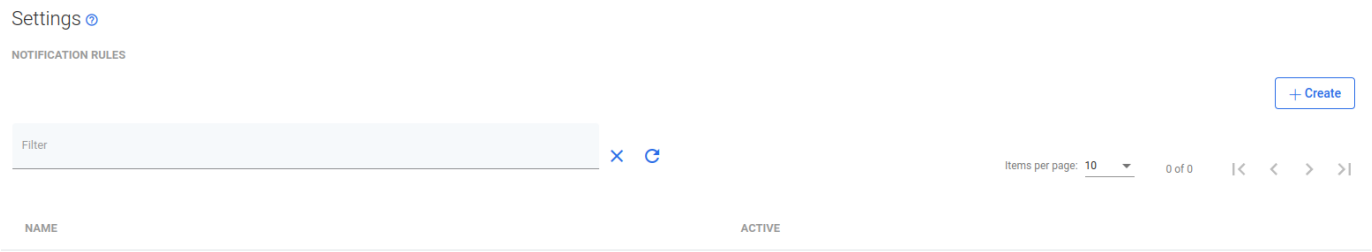
This allows you to control the process of creating an internal database backup from one place. Clicking on the magnifying glass icon will take you to the appropriate menu.



Notification Rules

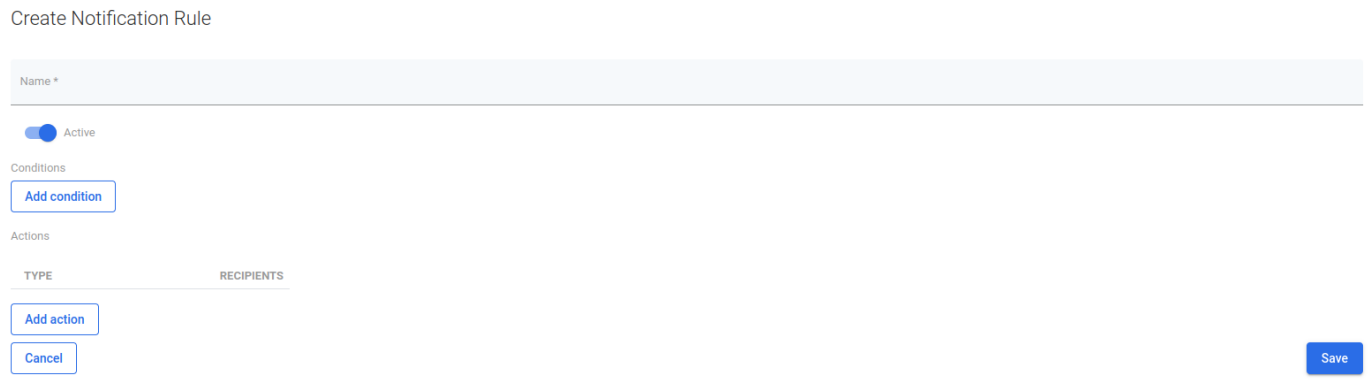
General

Data Protector for Cloud Workloads allows a Notification Rules feature to create a semi-custom rule that will send notification triggered by an event specified in rule.
Go to Settings on a left menu and then click on Notification Rules button.

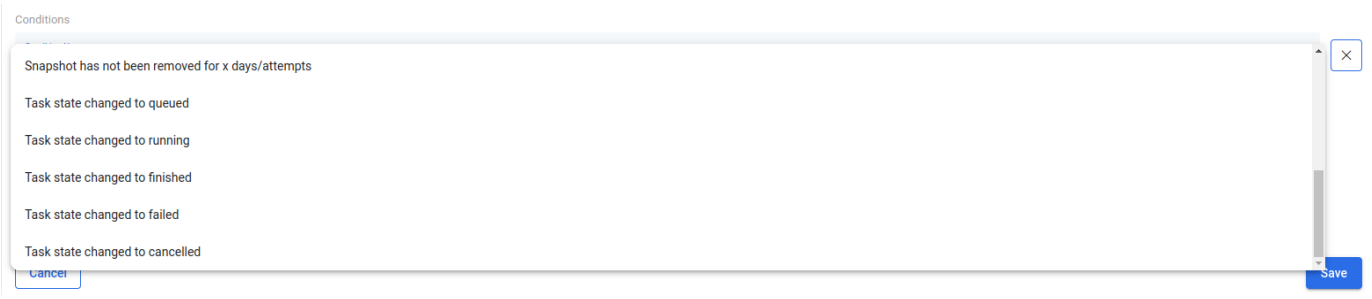


Creating new Notification Rule

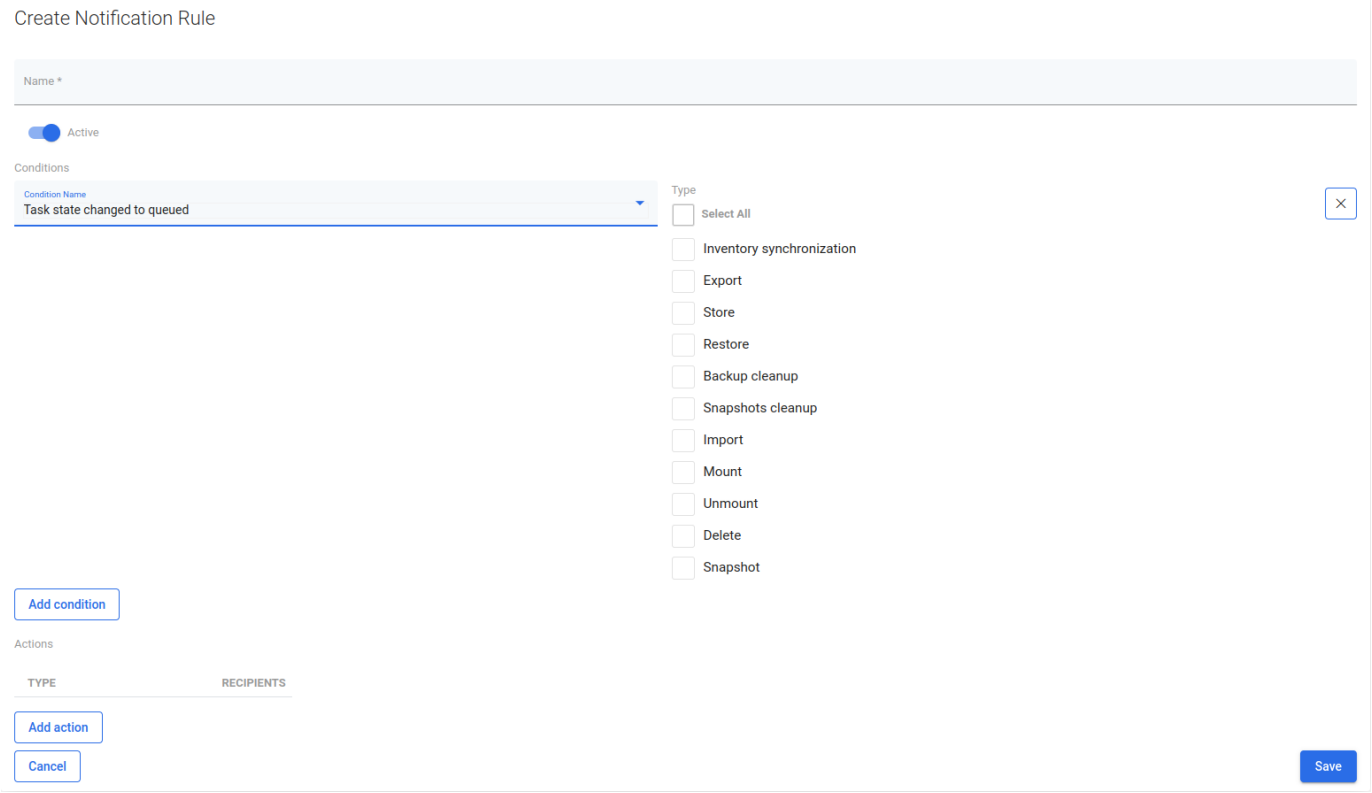
To create new rule, simply click on **Create** button. A new window will appear.



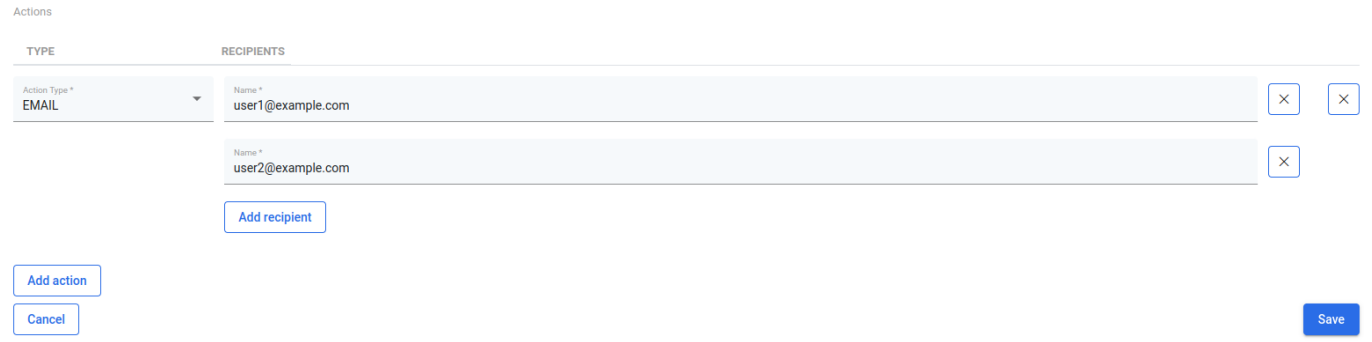
Fill in a name for your rule, set your notification to active and add one or more conditions from a list.



For some conditions, you will need to provide more information, for example, choose TaskType.



The last step is to add an action with related recipients.
Click **Add Action** button, choose **Action Type** from a list, add one or more recipients passing their email addresses.

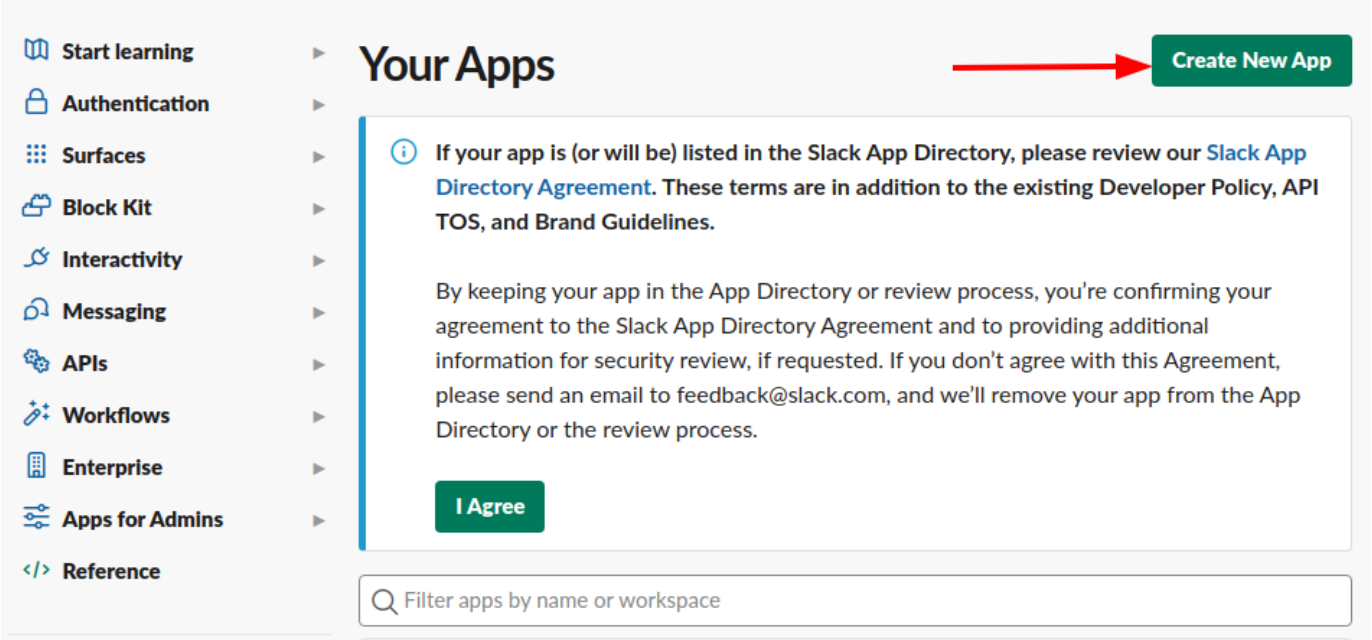


After an event that will trigger a notification, all recipients who have been added to the notification rule will receive an email notification.

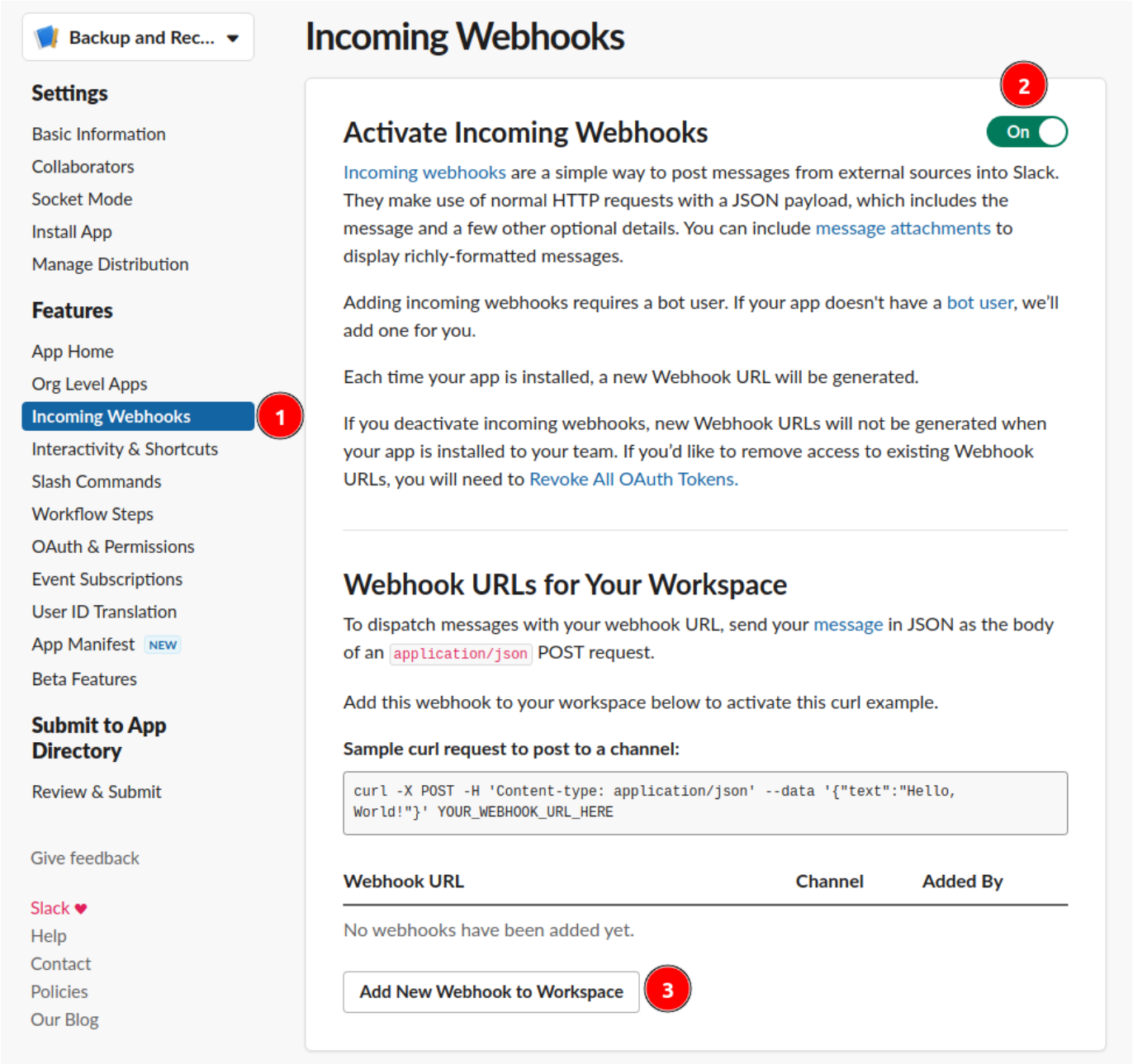
Slack integration

From Data Protector for Cloud Workloads version 5.0, there is a possibility to send notifications to the Slack channel. Follow these steps to authorize platform in your Slack workspace:

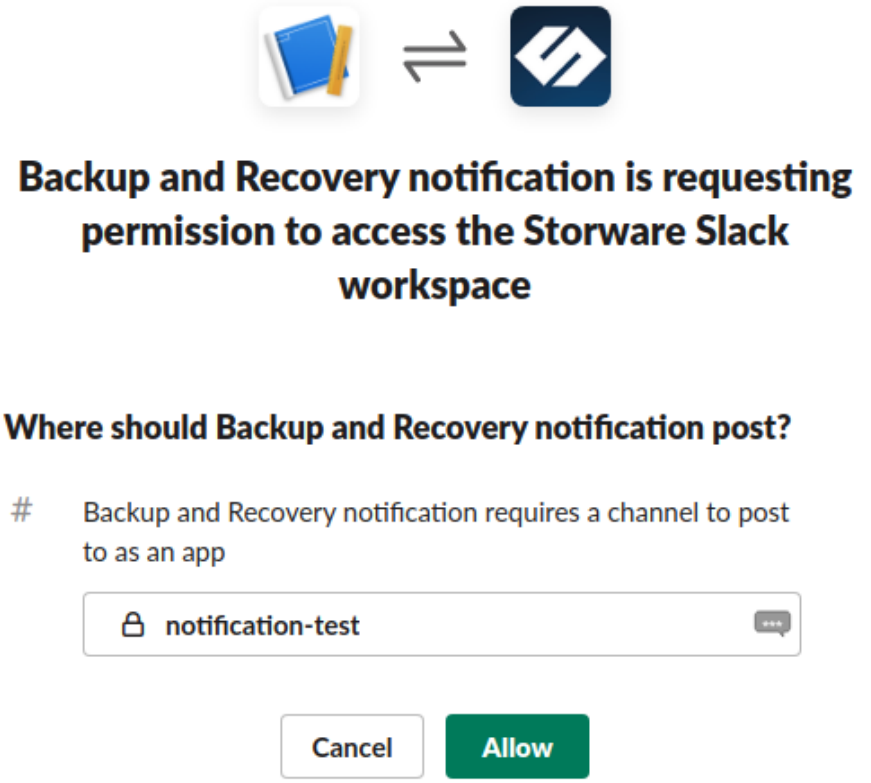
1. Go to this page and create a new Slack app in the workspace where you want to post messages. Select From scratch option and Enter the **App Name** and **Workspace** in which you want to use this app



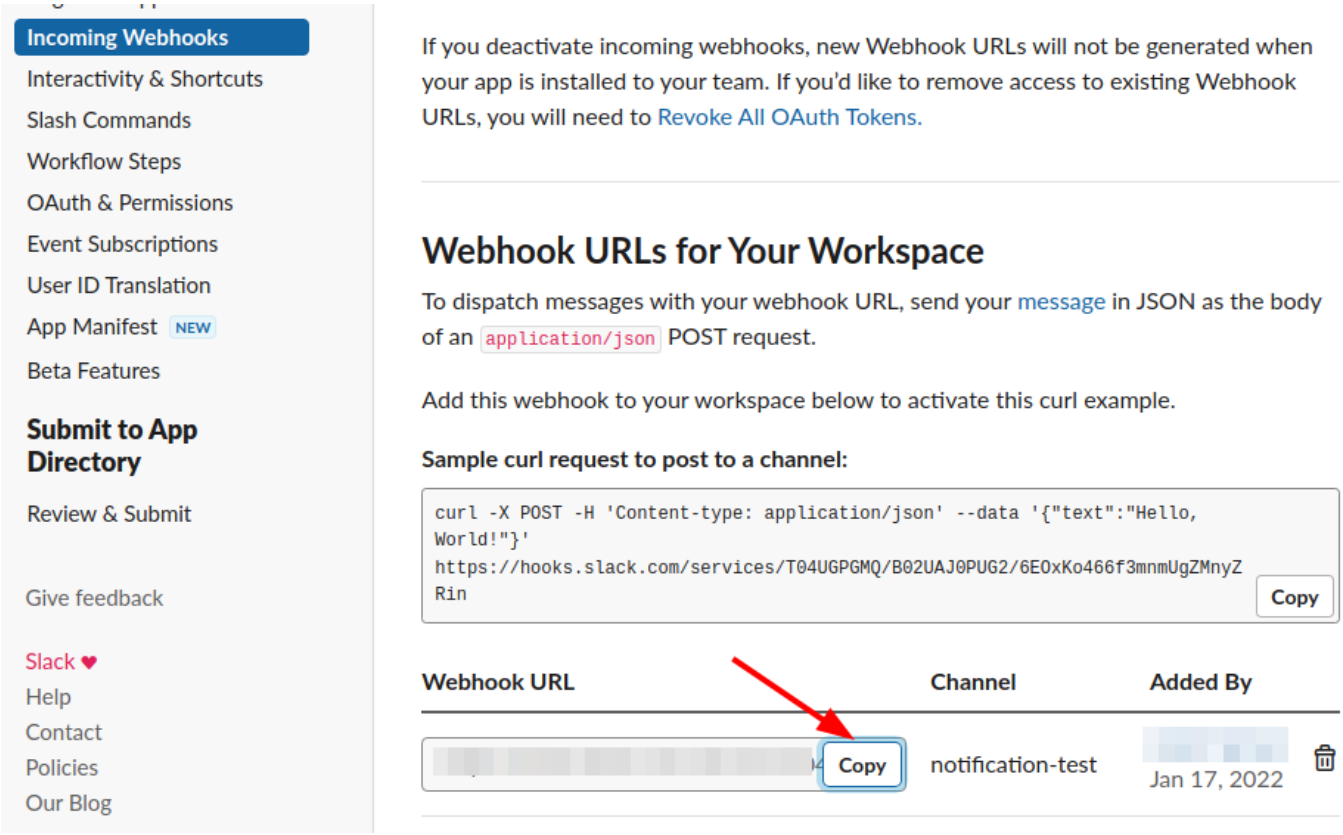
2. From the Features page, toggle Activate Incoming Webhooks on. Click Add New Webhook to Workspace.

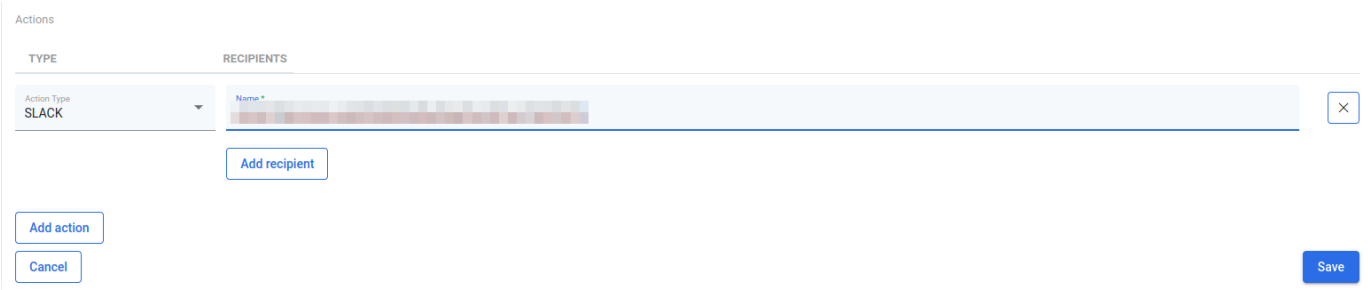


3. Pick a channel that the app will post to, then click Allow.



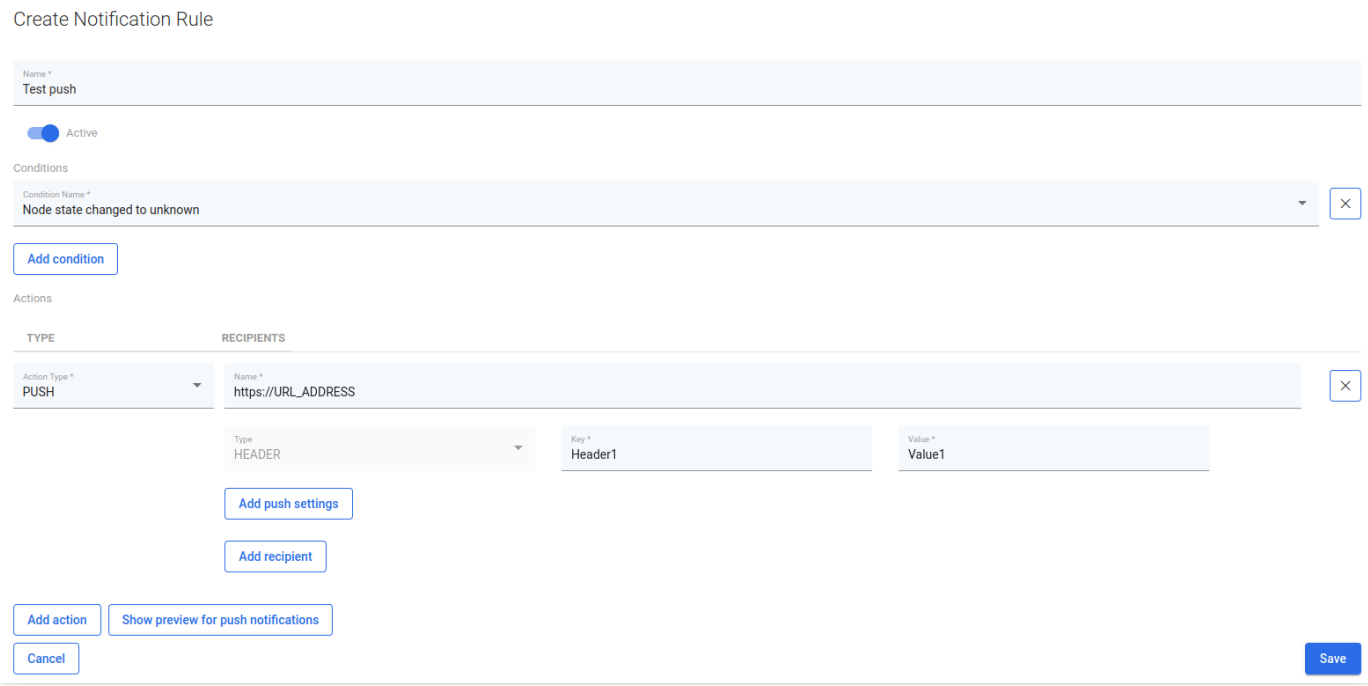
4. Copy the Webhook URL and use its Notification rules. Select Action Type as SLACK and paste the URL in the **Name** field.





Configuration of Push Notification

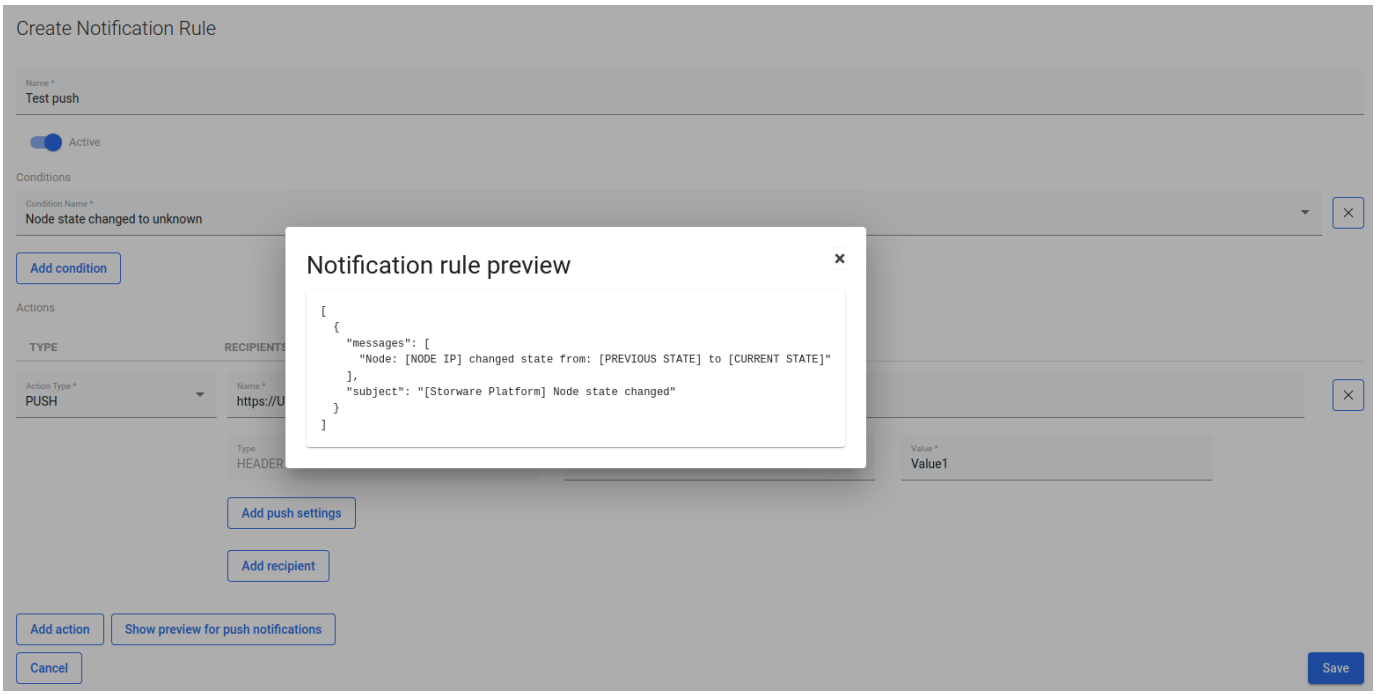
To configure a push notification, provide URL of endpoint address, where you want to receive notifications and add if needed custom headers that will be added to POST request with notification.



Body of notification will contain two fields:

- **subject**
- **messages** - list of notification messages that have been generated base on notification policy and triggered during run of program

To check how your notification will be looking please click on button **Show preview for push notifications**

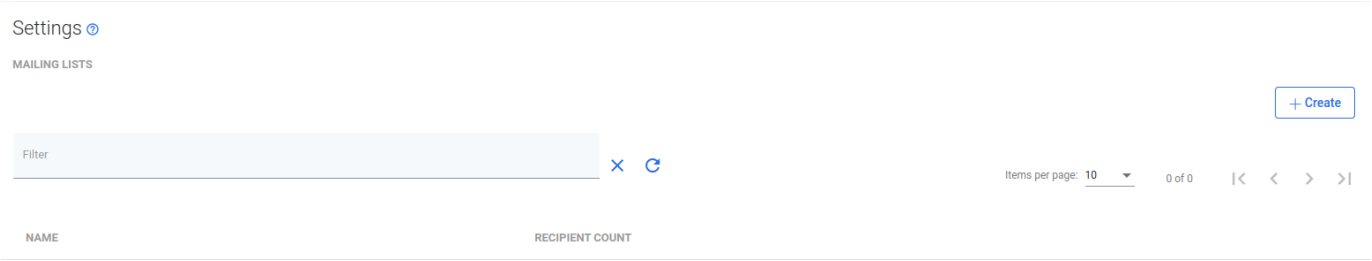

Create Notification Rule
Name *
Test push
Active
Conditions
Condition Name *
Node state changed to unknown
Add condition
Actions
TYPE
RECIPIENTS
Action Type *
PUSH
Name *
https://U
Type
HEADER
Value *
Value1
Add push settings
Add recipient
Add action
Show preview for push notifications
Cancel
Save
Notification rule preview
[
{
"messages": [
"Node: [NODE IP] changed state from: [PREVIOUS STATE] to [CURRENT STATE]"
],
"subject": "[Storware Platform] Node state changed"
}
]

Mailing Lists

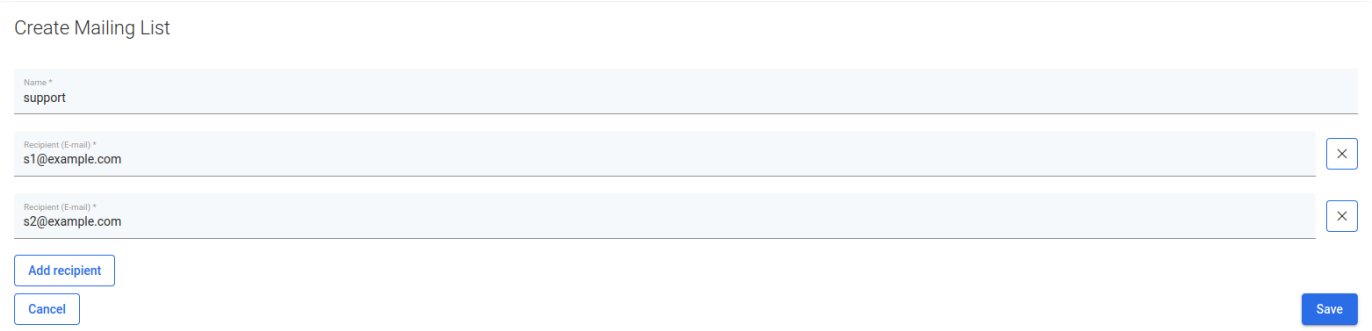
This allows you to create a mailing list which can be used for sending group report e-mails.

Creating a new mailing list

To create a new list, click on **Create** button. A new window will appear.



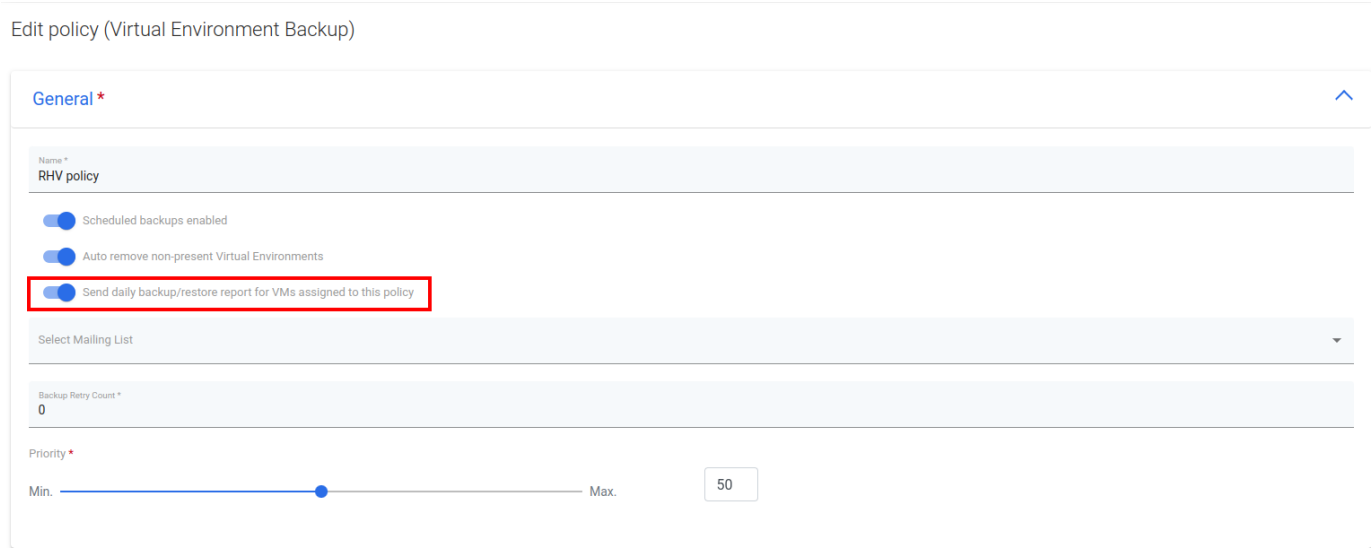
Fill the name for your list and add recipients e-mails by clicking **Add recipient** button.



After you have finished adding recipients, click on the **Save** button.

Mailing list usage

Find the backup policy in which you want to use the mailing list and click on it to enter the **Edit policy** page. Enable the **Send daily backup/restore report for VMs assigned to this policy** option and select the mailing list.



Upgrade

Before every update, check the version of installed packages. The database version is particularly important.

```
yum info vprotect-server vprotect-node mariadb-server
# Or
rpm -qa | egrep -e "vprotect|Maria"
```

If the host computer has an internet connection, use the yum command - you'll also see the new package versions provided by the repositories.

Server Upgrade

- Make sure you have the Data Protector for Cloud Workloads database backup.
    - You can use this command manually to back it up on-demand on the Data Protector for Cloud Workloads Server:`/opt/vprotect/scripts/backup_db.sh /path/to/backup/file.sql.gz`
- If Data Protector for Cloud Workloads was installed on a virtual machine (not a physical one), it would be a good move to take a snapshot.
- After backing up the database, you should carefully stop the Data Protector for Cloud Workloads service to make sure that you don't have any tasks running (a running task may cause problems updating the database).
    - View all tasks, if you see even one on the list, clear it (wait for the ongoing tasks to finish)
    - You can do this from the WebUI (it's faster)

```
[root@vprotect ~]# vprotect task -L

                GUID                    Type    State    [%]    Window start
Window end     Pri.     Node       VM/APP
------------------------------------  ------  --------  ---  ----------------  ------
----------  ----  ----------  -----------
e3bb2496-3928-417c-a604-8c61b64df90e  Export  Running   0    2020-06-19 12:27  2020-
06-19 17:27  50    vPro-Local  VM_01_Apine
05c1d6cc-fe3b-40fb-9811-94b976571d8e  Store   Finished  100  2020-06-19 12:10  2020-
06-19 17:10  50    vPro-Local  VM_01_Apine
cb47190d-cf10-4cf9-8d1d-418eed5accf9  Export  Finished  100  2020-06-19 12:09  2020-
06-19 17:09  50    vPro-Local  VM_01_Apine

#To delete a task from the list
[root@vprotect ~]# vprotect task -d cb47190d-cf10-4cf9-8d1d-418eed5accf9
```

- Now, if you don't have any tasks on the list, you can stop the service.

```
[root@vprotect ~]# systemctl stop vprotect-server --now
```

- To make sure that no scheduler has started a task before stopping the service, let's query the database.
    - If the table is not empty, start the Data Protector for Cloud Workloads-Server service and clear the tasks again.

```
mysql -u root -p -e "Select * FROM vprotect.task;"
```

- Make sure you have MariaDB up-to-date - currently Data Protector for Cloud Workloads by default uses version **10.4**, while 10.2.31 is the minimum version supported.
    - If you need to migrate between versions (i.e. 10.3 to 10.4) - we recommend updating it as described here, but when you uninstall MariaDB packages you **SHOULD NOT** remove the Data Protector for Cloud Workloads Server package (as a dependency) i.e. try the `--noautoremove` option: *As centos/rhel 7 do not have the --noautoremove option natively, please use the rpm method.*
    - Otherwise, minor MariaDB versions should be updated with `yum update`
    - `rpm -e --nodeps "MariaDB-server-YOUR_VERSION_OF_PACKAGE"`
    - Update the MariaDB repository to the correct version `vi /etc/yum.repos.d/MariaDB.repo`
    - Install the new MariaDB-Server `yum install -y mariadb-server`
    - Update all other components of MariaDB `yum update -y mariadb`
    - Start the MariaDB engine `systemctl enable mariadb --now`
    - Run mysql_upgrade to update the Data Protector for Cloud Workloads Database `mysql_upgrade --user=root --password`
- If the database update is successful, now you can start with the Data Protector for Cloud Workloads Update.
- Extract this package on the hosts with Data Protector for Cloud Workloads Server or Node:

```
tar xvf DP-for-Cloud-Workloads-XXX.tgz
```

- Update Data Protector for Cloud Workloads Server using RPMs in elX folder

```
yum update elX/DP-for-Cloud-Workloads-server-XXX.elX.x86_64.rpm
```

- If the server service was not running before update, you may also need to execute:

```
systemctl start vprotect-server --now
```

Node Upgrade

1. Copy the Node RPM to all hosts with Data Protector for Cloud Workloads Node installed.
2. Update each Node:

```
systemctl stop vprotect-node
yum update elX/DP-for-Cloud-Workloads-node-XXX.elX.x86_64.rpm
```

3. If the node service was not running before the update, you may also need to execute:

```
systemctl start vprotect-node --now
```

4. Log in to the web UI and check if the nodes are running.

- **Note:** You may need to refresh your browser cache after update - for Chrome use `CTRL+SHIFT+R` (Windows/Linux) / `CMD+SHIFT+R` (MacOS)

Cloud Server Upgrade

1. Copy the Cloud Server RPM to all hosts with Data Protector for Cloud Workloads Node installed.
2. Update each Cloud Server:

```
yum update elX/DP-for-Cloud-Workloads-cloudserver-XXX.elX.x86_64.rpm
```

Cloud Agent Upgrade

1. Copy the Cloud Agent RPM to all hosts with Data Protector for Cloud Workloads Node installed.
2. Update each Cloud Agent:

```
yum update elX/DP-for-Cloud-Workloads-cloudagent-XXX.elX.x86_64.rpm
```

CLI Reference

Overview

Every node provides CLI that can be used to manage configuration and invoke tasks on Data Protector for Cloud Workloads Node. All of the commands are executed using `vprotect` command. The general syntax is as shown below:

```
[root@vProtect3 ~]# vprotect
usage: vprotect <COMMAND> -<ARG_1> ... -<ARG_N>
COMMAND is one of the following:
 node                    Node management
 config                      Node configuration management
 hv                          Hypervisor management
 hvm                         Hypervisor manager management
 hc                          Hypervisor cluster management
 hs                          Hypervisor storage management
 vm                          Virtual machine management
 vmpolicy                    VM backup policy management
 bd                          Backup destination management
 sched                       Schedule management
 brvm                        VM backup & restore
 st                          Storage management
 stpool                      Storage pool management
 stprovider                   Storage provider management
 brapp                       Application backup & restore
 mnt                         Mounted backup management
 task                        Task management
 login                       User login
 logout                      Node and user logout
 stop                        Safely stops node
 vm-snappolicy               Snapshot policy management for VMs
 storage-snappolicy           Snapshot policy management for storages
 app                         Application backup management
 appconf                     App command execution management
 apppolicy                   Application backup policy management
 restorejob                   Restore jobs
 recplan                     Recovery plan policies
 brst                        Storage backup & restore
 quota                       Quota management
 project                     Project management
 user                        User management
 rbac                        Rbac management
 role                        AppUser Role management
 group                       AppUser Group management
 status                      Shows node status
 start                       Starts node
```

Starting and stopping node

- To check if Data Protector for Cloud Workloads Node is running, run:

```
systemctl status vprotect-node
```

or

```
vprotect status
```

- To start Data Protector for Cloud Workloads Node run:

  ```
  systemctl start vprotect-node
  ```

  or

  ```
  vprotect start
  ```

- To safely stop Data Protector for Cloud Workloads Node (this command waits for all tasks to be canceled, so that temporary objects are cleaned up) run:

  ```
  systemctl stop vprotect-node
  ```

  or

  ```
  vprotect stop
  ```

- In emergency cases you may need to kill the engine without task clean up - get PID of the node by running:

  ```
  vprotect status
  ```

  and kill process using:

  ```
  kill <PID>
  ```

User login

- To log in to CLI use the following command:

  ```
  vprotect login -u USER_NAME
  ```

where `USER_NAME` is your admin account in Data Protector for Cloud Workloads. You will be prompted for a password. From this moment you are able to execute commands.

- Once you completed working with CLI, you can log out by running:

  ```
  vprotect logout -u
  ```

Note about GUIDs

All of the commands require GUID of the object that you want to refer to in the command. GUID is found in the first column of typical list command, e.g.:

1. Let's list VMs and get VM GUID:

```
 [root@vProtect3 ~]# vprotect vm -l
                GUID                                 Name
Hypervisor       Present   VM group    Protected       Last backup
 ------------------------------------  ----------------------------  ----------
---------  -------  -----------  ---------  ---------------------
 b2555a74-97bb-44e4-9c68-ed1ac2ddffcd  Windows 7 (32-bit)            xcp-ng.DP-
for-Cloud-Workloads.local  true    PM-T1_Group  false      2020-06-03 00:30
(Tue)
```

2. Now let's show details of the VM:

```
[root@vprotect ~]# vprotect vm -g b2555a74-97bb-44e4-9c68-ed1ac2ddffcd
Property                                    Value
------------------------------------------  ----------------------------------
--------------------------

GUID                                        b2555a74-97bb-44e4-9c68-
ed1ac2ddffcd
Name                                        Windows 7 (32-bit)
UUID                                        9a486d85-c5c6-868b-50f4-
3b27f4e4f968
Present                                     true
HV type                                     CITRIX
HVM type                                    -
Inc. backup snapshot                        Windows 7 (32-bit): 2020-06-15
19:10:22.0 (6626e7d9-0900-4bfa-a961-85f5379b48d4)
Tags                                        [vPro-Citrix]
Hypervisor                                  10.40.0.29 (1048d561-b0f5-4f1d-
b558-856b28e0283e)
HV manager                                  -
Backups                                     29
VM backup policies                          Citrix Hypervisor | XCP-ng
(1f02821f-75f9-433f-9698-5694f130e1df)
Protected                                   true
Last backup                                 2020-06-15 19:10 (Mon)
Warnings present                            true
VM export/import mode                       INHERIT
Quiesce/freeze before snapshot              false
SSH host                                    -
SSH port                                    22
SSH user                                    -
SSH key path                                -
Pre-snapshot CMD exec. enabled              false
Pre-snapshot CMD                            []
Post-snapshot CMD exec. enabled             false
Post-snapshot CMD                           []
Pre-snapshot ignored exit codes             -
Pre-snapshot standard error output handling   DONT_IGNORE
```

```
Post-snapshot ignored exit codes                -
Post-snapshot standard error output handling  DONT_IGNORE
```

Note: that UUID is the ID used by the hypervisor or HV manager, while GUID is the ID used by Data Protector for Cloud Workloads to uniquely identify objects.

Node GUID can be replaced by `this` keyword to state that action such as restore or mount is going to be run on the node where the command is executed from. For instance, to restore or backup with given GUID on current node to `/vprotect_data`:

```
vprotect br -r 2132182d-e9ab-4478-a1db-48222b0e515b this /vprotect_data
```

Similarly, backup destinations can be referred to by names. So a backup of some VM with given GUID to backup destination with name `ISP` can be done like this:

```
vprotect br -b b6f96d43-6f55-468f-a7a0-8aa6219fdf4e ISP
```

Nodes

To list or register node use `vprotect node` sub-command:

```
[root@vprotect ~]# vprotect node
Incorrect syntax: Missing required option: [-r Register node, -R Check and Register
node, -d Delete node, -e Register existing node, -l List nodes]

usage: node -d <GUID | NAME> | -e <NODE_NAME> <ADMIN_LOGIN> <API_URL> <[PASSWORD]> |
-l | -r <NODE_NAME> <ADMIN_LOGIN> <API_URL> <[PASSWORD]> | -R <NODE_NAME>
<ADMIN_LOGIN> <API_URL> <[PASSWORD]>
Node management
 -d,--delete <GUID | NAME>                                                  Delete
node
 -e,--register-existing <NODE_NAME> <ADMIN_LOGIN> <API_URL> <[PASSWORD]>    Register
existing node
 -l,--list                                                                  List
nodes
 -r,--register <NODE_NAME> <ADMIN_LOGIN> <API_URL> <[PASSWORD]>             Register
node
 -R,--check-and-register <NODE_NAME> <ADMIN_LOGIN> <API_URL> <[PASSWORD]>   Check and
Register node
```

Examples

- To list all nodes registered

  ```
  vprotect node -l
  ```

- Example node registration

```
vprotect node -r node1 admin https://localhost:8181/api
```

- You may need to re-register a node if Data Protector for Cloud WorkloadsServer address changes

```
vprotect node -e node1 admin https://localhost:8181/api
```

Node configurations

Use `vprotect config` sub-command add/remove backup destinations from node config, list, or show details of node configs.

```
[root@vProtect ~]# vprotect config
Incorrect syntax: Missing argument for option: s

usage: config -b <CONFIG_GUID> <[BD_GUID|BD_NAME],...,[BD_GUID|BD_NAME]> | -c <NAME>
| -d <GUID> | -g <GUID> | -l | -r <CONFIG_GUID> <[BD_GUID|BD_NAME],...,
[BD_GUID|BD_NAME]> | -s <GUID> <PROPERTY_NO.> <VALUE |
"MAPPING1=VALUE1;MAPPING2=VALUE2">

Node configuration management
 -b,--add-backup-destinations <CONFIG_GUID> <[BD_GUID|BD_NAME],...,[BD_GUID|BD_NAME]>
Add backup destinations
 -c,--create <NAME>
Create node config
 -d,--delete <GUID>
Delete node config
 -g,--details <GUID>
Show config details
 -l,--list
List node configs
 -r,--remove-backup-destinations <CONFIG_GUID> <[BD_GUID|BD_NAME],...,
[BD_GUID|BD_NAME]>   Remove backup destinations
 -s,--set <GUID> <PROPERTY_NO.> <VALUE | "MAPPING1=VALUE1;MAPPING2=VALUE2">
Modify node config.
```

Setting up parameters for node configuration

In general `vprotect config -s <GUID> <PROPERTY_NO.> <VALUE>` command sets the value of a property with the given number of node configurations with `GUID`. Property numbers are returned in a detailed view of each node configuration. After you create node configuration, show default values with `-g`. Then use property numbers (the first number in the property/value line of the detailed view).

Examples

- To list all node configurations

```
vprotect config -l

                GUID                            Name       Default  Nodes  Backup
destinations  Modification time
------------------------------------  --------------  -------  -----  ----------
```

```
---------  -----------------
c95fb3cc-e567-11eb-8446-566fc400002d  Default Config  true     1      1
2021-07-16 11:41
```

- To show details of the given node config (by GUID)

```
vprotect config -g c95fb3cc-e567-11eb-8446-566fc400002d

Property                                                    Value
----------------------------------------------------------  -------------------
----------------------------------------

GUID                                                        c95fb3cc-e567-11eb-
8446-566fc400002d
Modification time                                           2021-07-16 11:41:54
1. Name                                                     Default Config
2. Default                                                  true
3. Export path                                              /vprotect_data
4. Import path
/vprotect_data/import
5. Mount path
/vprotect_data/mount
6. Max. backup time diff. [sec.]                            60
7. Keep last backups locally                                false
8. Min. free space for export (staging space threshold) [%] 10
9. Minimal free space for snapshot in bytes                 0
10. Minimal free space for snapshot in percentages          0
11. Max. no. of inventory synchronization threads           1
12. Max. no. of export threads                              3
13. Max. no. of export threads                              3
14. Max. no. of export threads per source                   2
15. Max. no. of store threads                               3
16. Max. no. of restore threads                             3
17. Inventory synchronization task timeout [min.]           1h
18. Export task timeout [min.]                              5h
19. Store task timeout [min.]                               5h
20. Restore task timeout [min.]                             1h
21. Unmount task timeout [min.]                             1h
22. Mount task timeout [min.]                               1h
23. Import task timeout [min.]                              1h
24. Old backups removal task timeout [min.]                 1h
25. Snapshot reversion task timeout [min.]                  1h
26. Old snapshot removal task timeout [min.]                1h
27. Task snapshot timeout [min.]                            1h
28. Max. no. of snapshot threads                            5
29. Max. no. of snapshots threads per source                2
Backup destinations                                         [backup
[FILESYSTEM] (bb0524fe-40a1-4ca3-bbc9-7f0be8ac73cc)]
```

- To add backup destination (second GUID) to the given node configuration (first GUID):

```
vprotect config -b c95fb3cc-e567-11eb-8446-566fc400002d f27b6018-ce1c-4d67-991e-
31d9f4f6662b
```

More backup destinations can be added by separating GUIDs with commas.

Backup destinations

The Backup destination management module is used to add, remove backup destinations (i.e. backup provider instances with retention settings). The Backup destination must be assigned to the group for the scheduler to know where to put backups during automatic backup. For backup on-demand, you just need to specify which backup destination should be used.

Backup destinations are assigned to the node configuration. This means that nodes using such configuration are configured to store backups in the selected backup destinations.

Note that the backup task will fail if it is not able to assign a node because the given BD is not assigned to the node config of the node that is required to be used for the given hypervisor.

To manage backup destinations in the system used `vprotect bd` sub-command.

```
[root@vprotect ~]# vprotect bd
Required option: [-r Reinitialize backup destination, -c Create backup destination
(type = ["filesystem", "netbackup", "networker", "s3", "swift", "isp", "azure",
"gcs", "avamar"]), -s Modify backup destination, -d Delete backup destination, -D
Remove old backups, -g Show backup destination details, -l List backup destinations]

usage: bd -c <NAME> <TYPE> | -d <GUID | NAME> | -D <[GUID | NAME],...,[GUID | NAME]>
| -g <GUID | NAME> | -l | -r <[GUID]> | -s <GUID |
       NAME> <PROPERTY_NO.> <VALUE>
Backup destination management
 -c,--create <NAME> <TYPE>                                      Create backup
destination (type = ["filesystem", "netbackup", "networker",
                                                                "s3", "swift", "isp",
"azure", "gcs", "avamar"])
 -d,--delete <GUID | NAME>                                      Delete backup
destination
 -D,--remove-old-backups <[GUID | NAME],...,[GUID | NAME]>      Remove old backups
 -g,--details <GUID | NAME>                                     Show backup destination
details
 -l,--list                                                      List backup destinations
 -r,--reinit <[GUID]>                                           Reinitialize backup
destination
 -s,--set <GUID | NAME> <PROPERTY_NO.> <VALUE>                  Modify backup
destination
```

Setting up parameters for backup destinations

In general `vprotect bd -s <GUID> <PROPERTY_NO.> <VALUE>` command sets value of property with the given number of BD with `GUID`. Property numbers are returned in detailed view of each BD (fields obviously are different for each backup provider). After you create backup destination, show default values with `-g`. Then use property numbers (first number in the property/value line of the detailed view).

Retention time settings are interpreted in days (just give a number without any additional suffixes).

There are however some mode/type fields that require a string to be typed in the correct format:

1. Amazon S3 - `Backup mode` - must be either:
    - `SINGLE_BUCKET` - single bucket for all VMs
    - `ONE_BUCKET_PER_VM` - separate bucket for each VM (note that default limit is 100 buckets in Amazon S3)

2. Swift - `Auth method` - authentication method used to authenticate Swift BD:
    - `BASIC`
    - `TEMPAUTH`
    - `KEYSTONE`
3. Time zones must be specified in the format shown in this table: List of tz database time zones

Examples

- To list all backup destinations

```
vprotect bd -l
```

- To show details of the given HV manager (by GUID) - **note** that each BD has a different set of fields - numbers at the beginning of a line indicate an identifier of a field you want to set from CLI. Remember that to use a BD you need to create a new entry of a given type and then configure its properties:

```
[root@vprotect ~]# vprotect bd -c backup filesystem
[root@vprotect ~]# vprotect bd -g 3263b196-056e-4485-9e8f-932798b58eb3
Property                                                                Value
-------------------------------------------------------------  ------------------
------------------

GUID
bb0524fe-40a1-4ca3-bbc9-7f0be8ac73cc
Node configs                                                            1
Type
FILESYSTEM
Total available space                                                   181
GiB
Total used space                                                        9,1
GiB
1. Name
backup
2. Pre-access CMD exec. enabled                                         false
3. Pre-access CMD                                                       []
4. Post-access CMD exec. enabled                                        false
5. Post-access CMD                                                      []
6. Default                                                              false
7. Retention (full) - keep last N backups                               4
8. Retention (full) - keep newer than                                   30d
9. Retention (inc.) - keep last N backups                               30
10. Retention (inc.) - keep newer than                                  30d
11. Paths
[/backup]
12. Deduplication enabled                                               false
13. Deduplication device                                                 -
14. Deduplicated filesystem mount point (set as 'default' to use BD path)
/backup
15. Deduplication volume used space threshold percentage                 -
16. Encryption enabled
```

HV managers (oVirt/RHV/Oracle VM/Nutanix/Kubernetes)

Hypervisor manager management module is used to add, remove hypervisor managers (currently only oVirt and RHV managers) and invoke indexing task. Indexing tasks gathers information about hypervisors and VMs running in the managed environment and updates their location if the VM has been moved to the different hypervisor.

To manage HV managers in the system used `vprotect hvm` sub-command.

Note that if you're using RHV/oVirt/Oracle VM/Nutanix/Kubernetes then hypervisors will be detected automatically as a part of the index task. So there is no need to define every hypervisor manually as they will be detected automatically.

```
[root@vprotect ~]# vprotect hvm
Incorrect syntax: Missing required option: [-c Create hypervisor manager (type =
["rhev", "rhv", "ovm", "nutanix", "openstack"]), -d Delete hypervisor manager, -e Set
export/import mode for HV manager, -g Show HV manager details, -l List hypervisor
managers, -L List hypervisors managed by hypervisor manager, -m Modify hypervisor
manager, -n Set node config for hypervisor, -sC Modify hypervisor manager
configuration, -s Index inventory on hypervisor manager, -u Set user/password or
access key/secret key, -V List VMs managed by hypervisor manager, -sK Set SSH key
path]

usage: hvm -c <URL | ACCOUNT_ID> <TYPE> | -d <GUID | HOST> | -e <GUID | HOST>
<DEFAULT|DISK_ATTACHMENT|DISK_IMAGE_TRANSFER|SSH_TRANSFER> | -g <GUID | HOST> | -l |
-L <GUID | HOST> | -m <GUID | HOST> <URL> | -n <GUID | HOST> <NODE_CONFIG_GUID |
NODE_CONFIG_NAME> | -s <GUID | HOST> |
       -sC <GUID> <PROPERTY_NO.> <VALUE | "MAPPING1=VALUE1;MAPPING2=VALUE2"> | -sK
<GUID> <SSH_KEYPATH> | -u <GUID | HOST> <USER/ACCESS_KEY> <PASSWORD/SECRET_KEY> | -V
<GUID | HOST>
Hypervisor manager management
 -c,--create <URL | ACCOUNT_ID> <TYPE>
Create hypervisor manager (type = ["rhev", "rhv", "ovm", "nutanix", "openstack"])
 -d,--delete <GUID | HOST>
Delete hypervisor manager
 -e,--set-export-import-mode <GUID | HOST>
<DEFAULT|DISK_ATTACHMENT|DISK_IMAGE_TRANSFER|SSH_TRANSFER>   Set export/import mode
for HV manager
 -g,--details <GUID | HOST>
Show HV manager details
 -l,--list
List hypervisor managers
 -L,--list-hvs <GUID | HOST>
List hypervisors managed by hypervisor manager
 -m,--modify <GUID | HOST> <URL>
Modify hypervisor manager
 -n,--set-node-config <GUID | HOST> <NODE_CONFIG_GUID | NODE_CONFIG_NAME>
Set node config for hypervisor
 -s,--sync <GUID | HOST>
Index inventory on hypervisor manager
 -sC,--configuration <GUID> <PROPERTY_NO.> <VALUE |
"MAPPING1=VALUE1;MAPPING2=VALUE2">                  Modify hypervisor manager
configuration
 -sK,--set-ssh-key-path <GUID> <SSH_KEYPATH>
Set SSH key path
 -u,--credentials <GUID | HOST> <USER/ACCESS_KEY> <PASSWORD/SECRET_KEY>
Set user/password or access key/secret key
 -V,--list-vms <GUID | HOST>
```

Examples

- To list all hypervisor managers

```
vprotect hvm -l
```

- To show details of the given HV manager (by GUID)

```
vprotect hvm -g 4c999c85-e223-4df3-9c40-7b0115234c8c
```

- To index VMs and hypervisors on the given HV manager:

```
vprotect hvm -s 4c999c85-e223-4df3-9c40-7b0115234c8c
```

- To create a HV manager you need to execute the following commands:
    - Create HV manger entry with given type:

```
vprotect hvm -c https://dovirt-m.lab.local/ovirt-engine/api/v3 rhev
```

    - Use GUID returned to set credentials:

```
vprotect hvm -u 4c999c85-e223-4df3-9c40-7b0115234c8c admin@internal
password
```

    - By default current node configuration is used for created HV manager - you may change it with this command (first HV GUID, then node configuration GUID):

```
vprotect hvm -n 4c999c85-e223-4df3-9c40-7b0115234c8c e2673e8f-66fc-4e9f-
aaef-20958c4c2b01
```

      Hypervisors connected to the HV manager will have node configuration of the HV manager assigned by default. For backup export always node configuration assigned to the HV is used.

Hypervisors

The Hypervisor management module is used to add, remove hypervisors and invoke indexing tasks. Indexing tasks gather information about VMs running on the hypervisor and update their location if the VM has been moved within the pool.

To manage hypervisors in the system used `vprotect hv` sub-command.

Note that if you're using RHV/oVirt/Oracle VM then hypervisors will be detected automatically as a part of the index task. So there is no need to define OVM hypervisors and for RHV/oVirt KVM hosts will be detected automatically.

```
[root@vprotect ~]# vprotect hv
Incorrect syntax: Missing required option: [-sC Modify hypervisor configuration, -c
```

```
Create hypervisor (type = ["citrix", "nutanix", "proxmox", "ovm", "kvm", "xen"]), -s
Synchronize inventory with hypervisor, -d Delete hypervisor, -nC Set node config for
hypervisor, -e Set export/import mode for hypervisor, -u Set user/password, -g Show
hypervisor details, -sK Set SSH key path, -l List hypervisors, -L List VMs for
hypervisor, -m Modify hypervisor]

usage: hv -c <HOST> <TYPE> | -d <GUID | HOST> | -e <GUID | HOST>
<DEFAULT|VM_IMAGE_PLUS_INCREMENTAL_DISKS|CHANGED_BLOCK_TRACKING|SSH_TRANSFER|EXPORT_S
TORAGE_REPO> | -g <GUID | HOST> | -l | -L <GUID | HOST> | -m <GUID | HOST> <NEW_HOST>
| -nC <GUID | HOST> <NODE_CONFIG_GUID> | -s
       <GUID | HOST> | -sC <GUID> <PROPERTY_NO.> <VALUE> | -sK <GUID> <SSH_KEYPATH> |
-u <GUID | HOST> <USER> <PASSWORD>

Hypervisor management
 -c,--create <HOST> <TYPE>
Create hypervisor (type = ["citrix", "nutanix", "proxmox", "ovm", "kvm", "xen"])
 -d,--delete <GUID | HOST>
Delete hypervisor
 -e,--set-export-import-mode <GUID | HOST>
<DEFAULT|VM_IMAGE_PLUS_INCREMENTAL_DISKS|CHANGED_BLOCK_TRACKING|SSH_TRANSFER|EXPORT_S
TORAGE_REPO>   Set export/import mode for hypervisor
 -g,--details <GUID | HOST>
Show hypervisor details
 -l,--list
List hypervisors
 -L,--list-vms <GUID | HOST>
List VMs for hypervisor
 -m,--modify <GUID | HOST> <NEW_HOST>
Modify hypervisor
 -nC,--set-node-config <GUID | HOST> <NODE_CONFIG_GUID>
Set node config for hypervisor
 -s,--sync <GUID | HOST>
Synchronize inventory with hypervisor
 -sC,--configuration <GUID> <PROPERTY_NO.> <VALUE>
Modify hypervisor configuration
 -sK,--set-ssh-key-path <GUID> <SSH_KEYPATH>
Set SSH key path
 -u,--credentials <GUID | HOST> <USER> <PASSWORD>
Set user/password
```

Examples

- To list all hypervisors

```
vprotect hv -l
```

- To show details of the given hypervisor (by GUID)

```
vprotect hv -g c93140b8-a898-4aff-8eef-645587ca8289
```

- To index VMs on the given HV:

```
vprotect hv -s c93140b8-a898-4aff-8eef-645587ca8289
```

- To create a hypervisor you need to execute the following commands:
    - Create HV entry with given type:

```
vprotect hv -c 1.2.3.4 citrix
```

    - Use GUID returned to set credentials:

```
vprotect hv -u a757c6e8-ece0-467b-b912-dfe393d1e421 root password
```

    - By default current node configuration is used for created hypervisor - you may change it with this command (first HV GUID, then node configuration GUID):

```
vprotect hv -n a757c6e8-ece0-467b-b912-dfe393d1e421 e2673e8f-66fc-4e9f-
aaef-20958c4c2b01
```

Hypervisor clusters

Hypervisor clusters management module enables you to view and remove clusters detected on RHV/oVirt/Nutanix/OVM/XenServer environments.

To view or delete them use `vprotect hc` sub-command.

```
[root@localhost ~]# vprotect hc
Incorrect syntax: Missing required option: [-d Delete HV cluster, -l List HV
clusters]

usage: hc -d <GUID> | -l
Hypervisor cluster management
 -d,--delete <GUID>                                                Delete HV cluster
 -l,--list                                                         List HV clusters
 -sn,--set-name <GUID> <NAME>                                      Change Hypervisor
Cluster name
 -sp,--set-storage-provider <GUID> <STORAGE_PROVIDER_GUID>>     Assign Storage
Provider to Hypervisor Cluster. No value unassigns Storage Provider
```

Examples

- To list all detected clusters:

```
vprotect hc -l
```

- To delete a cluster with GUID `107bc87a-9adf-4d6c-b732-345dd06c59e9`:

```
vprotect hc -d 107bc87a-9adf-4d6c-b732-345dd06c59e9
```

Hypervisor storage

Hypervisor storage management module enables you to view and remove storage detected on RHV/oVirt/Nutanix/OVM/XenServer environments. You can select storage in the restore dialog box for XenServer/Nutanix and RHV/oVirt (v4) platforms.

To view or delete them used `vprotect hs` sub-command.

```
[root@localhost ~]# vprotect hs
Incorrect syntax: Missing required option: [-d Delete HV storage, -l List HV storage]

usage: hs -d <GUID> | -l
Hypervisor storage management
 -d,--delete <GUID>   Delete HV storage
 -l,--list            List HV storage
```

Examples

- To list all detected storage volumes:

  ```
  vprotect hs -l
  ```

- To delete a storage volume with GUID `6b5aa45a-5436-47cd-82ce-1c4250742323`:

  ```
  vprotect hs -d 6b5aa45a-5436-47cd-82ce-1c4250742323
  ```

Virtual machines

The Virtual machine management module is used to provide information about VMs that has been detected on hypervisors, report the status of the last backup of your VMs (and all backups for a particular VM) and set priority for operations invoked on VM.

To manage VMs in the system used `vprotect vm` sub-command.

VMs are detected automatically during `Index` tasks executed on the HV or HV manager.

```
[root@vprotect ~]# vprotect vm
Incorrect syntax: Missing required option: [-A Assign VM to the policy, -D List
detected VM disks, -xC Set pre-snapshot CMD as semi-colon-separated string, i.e.
"cmd;-a;-b", -wb Acknowledge warnings related to the backup, -L List backups of the
VM, -xE Set pre-snapshot CMD exec enabled (1) / disabled (0), -rvS Revert snapshot, -
cS Create VM snapshot, -se Set handling for pre-snap standard error. Values:
DONT_IGNORE, IGNORE_WITH_WARNING, IGNORE_WITHOUT_WARNING, -S List managed VM
snapshots, -T List tasks related to the VM, -si Set pre-snap ignored command exit
codes e.g. '15, 101-150' or '*', -gb Show backup details, -d Delete VM, -g Show
virtual machine details, -XC Set post-snapshot CMD as semi-colon-separated string,
i.e. "cmd;-a;-b", -l List VMs, -XE Set post-snapshot CMD exec enabled (1) / disabled
(0), -sC Set SSH access credentials, -sE Set handling for post-snap standard error.
Values: DONT_IGNORE, IGNORE_WITH_WARNING, IGNORE_WITHOUT_WARNING, -sH Set SSH access
host/port, -sI Set post-snap ignored command exit codes e.g. '15, 101-150' or '*', -w
Acknowledge all backup warnings related to the VM, -sK Set SSH key path, -rmS Remove
```

```
old snapshots, -eD Exclude disk from backup excluded (1) / included (0)]

usage: vm -A <GUID> <VM_POLICY_GUID> | -cS <GUID> <RULE_GUID> <PRIORITY> | -D <GUID>
| -d <GUID> | -eD <DISK_GUID> <0|1> | -g <<VM_GUID>> | -gb <BACKUP_GUID> | -L <GUID>
| -l | -rmS <VM_GUID,...,VM_GUID> | -rvS <SNAPSHOT_GUID> | -S <GUID> | -sC <GUID>
<SSH_USER> <SSH_PASS> | -se
       <GUID> <HANDLING> | -sE <GUID> <HANDLING> | -sH <GUID> <SSH_HOST> <SSH_PORT> |
-si <GUID> <IGNORED_EXIT_CODES> | -sI <GUID> <IGNORED_EXIT_CODES> | -sK <GUID>
<SSH_KEYPATH> | -T <GUID> | -w <GUID> | -wb <BACKUP_GUID> | -xC <GUID> <CMD_STRING> |
-XC <GUID> <CMD_STRING> | -xE
       <GUID> <0|1> | -XE <GUID> <0|1>

Virtual machine management
 -A,--assign-vm-policy <GUID> <VM_POLICY_GUID>              Assign VM to the policy
 -cS,--create-snapshot <GUID> <RULE_GUID> <PRIORITY>        Create VM snapshot
 -D,--list-disks <GUID>                                     List detected VM disks
 -d,--delete <GUID>                                         Delete VM
 -eD,--exclude-disk <DISK_GUID> <0|1>                       Exclude disk from backup
excluded (1) / included (0)
 -dnp,--delete-non-present <[PROJECT_UUID]>                 Delete non-present
Virtual Machines. Project UUID is optional
 -g,--details <<VM_GUID>>                                   Show virtual machine
details
 -gb,--show-backup-details <BACKUP_GUID>                    Show backup details
 -L,--list-backups <GUID>                                   List backups of the VM
 -l,--list                                                  List VMs
 -rmS,--remove-snapshot <VM_GUID,...,VM_GUID>               Remove old snapshots
 -rvS,--revert-snapshot <SNAPSHOT_GUID>                     Revert snapshot
 -S,--list-snapshots <GUID>                                 List managed VM snapshots
 -sC,--set-ssh-credentials <GUID> <SSH_USER> <SSH_PASS>     Set SSH access
credentials
 -se,--set-pre-std-error-out <GUID> <HANDLING>              Set handling for pre-snap
standard error. Values: DONT_IGNORE, IGNORE_WITH_WARNING, IGNORE_WITHOUT_WARNING
 -sE,--set-post-std-error-out <GUID> <HANDLING>             Set handling for post-
snap standard error. Values: DONT_IGNORE, IGNORE_WITH_WARNING, IGNORE_WITHOUT_WARNING
 -sH,--set-ssh-host <GUID> <SSH_HOST> <SSH_PORT>            Set SSH access host/port
 -si,--set-pre-ignored-codes <GUID> <IGNORED_EXIT_CODES>    Set pre-snap ignored
command exit codes e.g. '15, 101-150' or '*'
 -sI,--set-post-ignored-codes <GUID> <IGNORED_EXIT_CODES>   Set post-snap ignored
command exit codes e.g. '15, 101-150' or '*'
 -sK,--set-ssh-key-path <GUID> <SSH_KEYPATH>                Set SSH key path
 -T,--list-tasks <GUID>                                     List tasks related to the
VM
 -w,--ack-all-backup-warnings <GUID>                        Acknowledge all backup
warnings related to the VM
 -wb,--ack-backup-warnings <BACKUP_GUID>                    Acknowledge warnings
related to the backup
 -xC,--set-pre-snap-cmd <GUID> <CMD_STRING>                 Set pre-snapshot CMD as
semi-colon-separated string, i.e. "cmd;-a;-b"
 -XC,--set-post-snap-cmd <GUID> <CMD_STRING>                Set post-snapshot CMD as
semi-colon-separated string, i.e. "cmd;-a;-b"
 -xE,--set-pre-snap-cmd-exec-enabled <GUID> <0|1>           Set pre-snapshot CMD exec
enabled (1) / disabled (0)
 -XE,--set-post-snap-cmd-exec-enabled <GUID> <0|1>          Set post-snapshot CMD
exec enabled (1) / disabled (0
```

Examples

- To list all VMs

```
vprotect vm -l
```

- To show details of the given VM (by GUID)

```
vprotect vm -g 0f36f40c-6427-4035-9f2b-1ead6aca3597
```

- To add VM (first GUID) to the given policy (second GUID):

```
vprotect vm -A 0f36f40c-6427-4035-9f2b-1ead6aca3597 3afcd507-a4f5-484d-8d34-
53c73d7a5809
```

- To show backup history of a VM with given GUID:

```
vprotect vm -L 0f36f40c-6427-4035-9f2b-1ead6aca3597
```

- To create snapshot of a VM with given GUID (VM must have snapshot policy already assigned):

```
vprotect vm -cS 0f36f40c-6427-4035-9f2b-1ead6aca3597
```

Storage backup management

This module is responsible for managing storage instances and actions related to backups/schedules/policies etc.

```
[root@localhost ~]# vprotect st
Incorrect syntax: Missing required option:
[-A Assign Storage to the policy, -a Assign Storage to the snapshot policy,
 -d Delete Storage, -g Show Storage details, -wb Acknowledge warnings related
 to the backup, -xC Set pre-snapshot CMD as semi-colon-separated string,
 i.e. "cmd;-a;-b", -XC Set post-snapshot CMD as semi-colon-separated string,
 i.e. "cmd;-a;-b", -l List Storages, -L List backups of the Storage,
 -sC Set SSH access credentials, -se Set handling for pre-snap standard error.
 Values: DONT_IGNORE, IGNORE_WITH_WARNING, IGNORE_WITHOUT_WARNING,
 -sE Set handling for post-snap standard error. Values: DONT_IGNORE,
 IGNORE_WITH_WARNING, IGNORE_WITHOUT_WARNING, -s Modify Storage configuration,
 -T List tasks related to the Storage, -w Acknowledge all backup warnings
 related to the Storage, -gb Show backup details]

usage: st -A <GUID> <STORAGE_POLICY_GUID> | -a <GUID> <SNAPSHOT_POLICY_GUID> |
  -d <GUID> | -g <GUID> | -gb <BACKUP_GUID> | -l | -L <GUID> |
  -s <GUID> <PROPERTY_NO.> <VALUE> | -sC <GUID> <SSH_USER> <SSH_PASS> |
  -se <GUID> <HANDLING> | -sE <GUID> <HANDLING> |-T <GUID> | -w <GUID> |
  -wb <BACKUP_GUID> | -xC <GUID> <CMD_STRING> | -XC <GUID> <CMD_STRING>
Storage management
 -A,--assign-storage-policy <GUID> <STORAGE_POLICY_GUID>
    #Assign Storage to the policy
 -a,--assign-snapshot-policy <GUID> <SNAPSHOT_POLICY_GUID>
    #Assign Storage to the snapshot policy
 -d,--delete <GUID>
```

```
    #Delete Storage
 -g,--details <GUID>
    #Show Storage details
 -gb,--show-backup-details <BACKUP_GUID>
    #Show backup details
 -l,--list
    #List Storages
 -L,--list-backups <GUID>
    #List backups of the Storage
 -s,--configuration <GUID> <PROPERTY_NO.> <VALUE>
    #Modify Storage configuration
 -sC,--set-ssh-credentials <GUID> <SSH_USER> <SSH_PASS>
    #Set SSH access credentials
 -se,--set-pre-std-error-out <GUID> <HANDLING>
    #Set handling for pre-snap standard error. Values: DONT_IGNORE,
    #IGNORE_WITH_WARNING, IGNORE_WITHOUT_WARNING
 -sE,--set-post-std-error-out <GUID> <HANDLING>
    #Set handling for post-snap standard error. Values: DONT_IGNORE,
    #IGNORE_WITH_WARNING, IGNORE_WITHOUT_WARNING
 -T,--list-tasks <GUID>
    #List tasks related to the Storage
 -w,--ack-all-backup-warnings <GUID>
    #Acknowledge all backup warnings related to the Storage
 -wb,--ack-backup-warnings <BACKUP_GUID>
    #Acknowledge warnings related to the backup
 -xC,--set-pre-snap-cmd <GUID> <CMD_STRING>
    #Set pre-snapshot CMD as semi-colon-separated string, i.e. "cmd;-a;-b"
 -XC,--set-post-snap-cmd <GUID> <CMD_STRING>
    #Set post-snapshot CMD as semi-colon-separated string, i.e. "cmd;-a;-b"
```

Examples

Storage pool management

This small module allows us to list and deleting inventoried storage pools.

```
[root@localhost ~]# vprotect stpool
Incorrect syntax: Missing required option: [-d Delete Storage Pool,
-l List Storage Pools]

usage: stpool -d <GUID> | -l
Storage pool management
 -d,--delete <GUID>        Delete Storage Pool
 -l,--list                 List Storage Pools
```

Examples

To list storage pools

```
[root@localhost ~]# vprotect stpool -l

                GUID                    Name                      UUID
Storage Provider
-----------------------------------  -------  ------------------------------------
----------------
```

```
b1171aba-aeb3-4e10-84dd-f3e3c0dc3235  backups  537e00c8-620d-4256-8d6c-e5e031327caa_1
last-ceph
86f41229-6f13-41b3-b1ce-c5841df7b4c7  images   537e00c8-620d-4256-8d6c-e5e031327caa_4
last-ceph
55832390-1779-483b-8023-88bb9a79b6ed  vms      537e00c8-620d-4256-8d6c-e5e031327caa_3
last-ceph
ff3a9f65-0b5f-4a78-8b97-b883cb971f81  volumes  537e00c8-620d-4256-8d6c-e5e031327caa_2
last-ceph
```

Storage providers management

This module is responsible for managing the storage provider's infrastructure. So performing tasks such as adding/removing / inventorying, etc.

```
[root@localhost ~]# vprotect stprovider
Incorrect syntax: Missing required option: [-sC Modify Storage Provider
configuration, -c Create Storage Provider, -s Synchronize inventory with Storage
Provider, -d Delete Storage Provider, -u Set user/password, -nC Set node config for
Storage Provider, -g Show Storage Providers details, -h Set host for Storage
Provider, -l List Storage Providers, -L List Storages for Storage Provider, -n Set
node for Storage Provider]

usage: stprovider -c <HOST> <TYPE> | -d <GUID> | -g <GUID> | -h <GUID> <HOST> | -l |
-L <GUID> | -n <GUID> <NODE_GUID> | -nC <GUID> <NODE_CONFIG_GUID> | -s <GUID> | -sC
<GUID> <PROPERTY_NO.> <VALUE> | -u <GUID> <USER> <PASSWORD>
+Storage provider management
 -c,--create <HOST> <TYPE>                          Create Storage Provider
 -d,--delete <GUID>                                 Delete Storage Provider
 -g,--details <GUID>                                Show Storage Providers details
 -h,--set-host <GUID> <HOST>                        Set host for Storage Provider
 -l,--list                                          List Storage Providers
 -L,--list-storages <GUID>                          List Storages for Storage
Provider
 -n,--set-node <GUID> <NODE_GUID>                   Set node for Storage Provider
 -nC,--set-node-config <GUID> <NODE_CONFIG_GUID>    Set node config for Storage
Provider
 -s,--sync <GUID>                                   Synchronize inventory with
Storage Provider
 -sC,--configuration <GUID> <PROPERTY_NO.> <VALUE>  Modify Storage Provider
configuration
 -u,--credentials <GUID> <USER> <PASSWORD>          Set user/password
```

Examples

VM backup policies

Virtual machine backup policies management module is used to define backup policies of VMs. You can assign different backup priorities for a policy when the scheduler invokes a backup task. You need first to define a VM policy and then add VMs to it. VM can belong only to a single backup policy.

To manage VM policies in the system use `vprotect vmpolicy` sub-command.

VMs are assigned automatically to the policy only if VM has no policy assigned already. If an automatic assignment has been turned on for a policy and either name of the VM matches the regular expression, or tag-detected

(Citrix/oVirt/RHV/Oracle VM) matches tag defined for the policy, VM is assigned to the policy, and all schedules for a policy will also be automatically invoked for this VM.

Note: it is important to assign a backup destination for a policy (required for a node to know where to store backups)

```
[root@vprotect ~]# vprotect vmpolicy
Required option: [-rR Remove auto-assignment RE, -rT Remove auto-assignment tag, -aC
Set auto-assignment HV clusters, -b Set backup destination for the VM policy, -c
Create a new policy, -d Delete a policy, -g Show details, -l List policies, -L List
VMs in the policy, -aM Set auto-assignment mode, -m Modify policy, -aN Set auto-
removal of non-present VMs flag, -p Set policy's backup task priority (0-100, 50 =
default), -aR Add auto-assignment RE, -aT Add auto-assignment tag, -S List schedules
for the policy, -s Set schedules for the VM policy, -U Unassign VMs from the policy,
-V Assign VMs to the policy]

usage: vmpolicy -aC <GUID > <[HV_CLUSTER_GUID,...,HV_CLUSTER_GUID]> | -aM <GUID>
<DISABLED|ASSIGN_ONLY|ASSIGN_AND_REMOVE> | -aN <GUID> <0|1> | -aR <GUID>
       <inc|exc> <REG_EXP> | -aT <GUID> <inc|exc> <TAG> | -b <GUID> <BD_GUID |
BD_NAME>> | -c <NAME> | -d <GUID> | -g <GUID> | -l | -L <GUID> | -m <GUID>
       <NAME> | -p <GUID> <PRIORITY> | -rR <GUID> <inc|exc> <REG_EXP> | -rT <GUID>
<inc|exc> <TAG> | -S <GUID> | -s <GUID> <SCHED_GUID,...,SCHED_GUID> | -U
       <VM_GUID,...,VM_GUID> | -V <GUID> <VM_GUID,...,VM_GUID>
VM backup policy management
 -aC,--set-auto-assign-hv-clusters <GUID > <[HV_CLUSTER_GUID,...,HV_CLUSTER_GUID]>
Set auto-assignment HV clusters
 -aM,--set-auto-assign-mode <GUID> <DISABLED|ASSIGN_ONLY|ASSIGN_AND_REMOVE>
Set auto-assignment mode
 -aN,--set-auto-remove-non-present <GUID> <0|1>
Set auto-removal of non-present VMs flag
 -aR,--add-auto-assign-re <GUID> <inc|exc> <REG_EXP>
Add auto-assignment RE
 -aT,--add-auto-assign-tag <GUID> <inc|exc> <TAG>
Add auto-assignment tag
 -b,--set-backup-destination <GUID> <BD_GUID | BD_NAME>>
Set backup destination for the VM policy
 -c,--create <NAME>
Create a new policy
 -d,--delete <GUID>
Delete a policy
 -g,--details <GUID>
Show details
 -l,--list
List policies
 -L,--list-vms <GUID>
List VMs in the policy
 -m,--modify <GUID> <NAME>
Modify policy
 -p,--set-priority <GUID> <PRIORITY>
Set policy's backup task priority (0-100, 50 = default)
 -rR,--remove-auto-assign-re <GUID> <inc|exc> <REG_EXP>
Remove auto-assignment RE
 -rT,--remove-auto-assign-tag <GUID> <inc|exc> <TAG>
Remove auto-assignment tag
 -S,--list-schedules <GUID>
List schedules for the policy
 -s,--set-schedules <GUID> <SCHED_GUID,...,SCHED_GUID>
Set schedules for the VM policy
 -U,--unassign-vms <VM_GUID,...,VM_GUID>
Unassign VMs from the policy
```

```
  -V,--assign-vms <GUID> <VM_GUID,...,VM_GUID>
Assign VMs to the policy
```

Examples

- To list all VM policies

```
vprotect vmpolicy -l
```

- To show details of the given VM (by GUID)

```
vprotect vmpolicy -g 3afcd507-a4f5-484d-8d34-53c73d7a5809
```

- To create a new policy

```
vprotect vmpolicy -c "My Policy"
```

- To add `policy1` tag (include) for a policy:

```
vprotect vmpolicy -aT 3afcd507-a4f5-484d-8d34-53c73d7a5809 inc policy1
```

- To remove `policy1` tag (include) for a policy:

```
vprotect vmpolicy -rT 3afcd507-a4f5-484d-8d34-53c73d7a5809 inc policy1
```

- To set 2 schedules (GUIDs are comma-separated) for a policy (first GUID):

```
vprotect vmpolicy -s 3afcd507-a4f5-484d-8d34-53c73d7a5809 391203e3-ad6c-4532-
b69c-78b3a5cf4ef5,e4c1c61d-26db-4e41-87cf-2195d5498cde
```

- To set backup destination (you can use name or GUID) for a policy (first GUID):

```
vprotect vmpolicy -b 3afcd507-a4f5-484d-8d34-53c73d7a5809 ISP
```

Snapshot management policies for VMs

Snapshot management policies module enables CDM for your VMs and manages their retention. Currently it is supported for KVM, Citrix, RHV/oVirt/OLVM platforms.

To manage snapshot policies for VMs in the system use `vprotect vm-snappolicy` sub-command.

VMs are assigned automatically to the policy only if VM has no policy assigned already. If automatic assignment has been turned on for a policy and either name of the VM matches regular expression, or tag detected (Citrix/RHV/oVirt/OLVM)

matches tag defined for the policy, VM is assigned to the policy, and all schedules for a policy will also be automatically invoked for this VM.

Note: only VMs with assigned snapshot management policy can be snapshot from the CLI or UI

```
[root@vprotect ~]# vprotect vm-snappolicy
Required option: [-rR Remove rules from policy, -rT Remove auto-assignment tag, -aC
Set auto-assignment HV clusters, -c Create a new policy, -d Delete a policy, -g Show
details, -l List policies, -L List VMs in the policy, -aM Set auto-assignment mode, -
m Modify policy, -aN Set auto-removal of non-present VMs flag, -p Set policy's backup
task priority (0-100, 50 = default), -aR Add new rule to selected policy, -r List
rules for policy, -aT Add auto-assignment tag, -U Unassign VMs from the policy, -V
Assign VMs to the policy]

usage: vm-snappolicy -aC <GUID > <[HV_CLUSTER_GUID,...,HV_CLUSTER_GUID]> | -aM <GUID>
<DISABLED|ASSIGN_ONLY|ASSIGN_AND_REMOVE> | -aN <GUID> <0|1> | -aR <NAME>
       <POLICY_GUID> <RETENTION_DAYS> <RETENTION_VERSIONS> | -aT <GUID> <inc|exc>
<TAG> | -c <NAME> | -d <GUID> | -g <GUID> | -l | -L <GUID> | -m <GUID>
       <NAME> | -p <GUID> <PRIORITY> | -r <GUID> | -rR <POLICY_GUID>
<RULE_GUID,...,RULE_GUID> | -rT <GUID> <inc|exc> <TAG> | -U <VM_GUID,...,VM_GUID> | -
V
       <GUID> <VM_GUID,...,VM_GUID>
Snapshot policy management
 -aC,--set-auto-assign-hv-clusters <GUID > <[HV_CLUSTER_GUID,...,HV_CLUSTER_GUID]>
Set auto-assignment HV clusters
 -aM,--set-auto-assign-mode <GUID> <DISABLED|ASSIGN_ONLY|ASSIGN_AND_REMOVE>
Set auto-assignment mode
 -aN,--set-auto-remove-non-present <GUID> <0|1>
Set auto-removal of non-present VMs flag
 -aR,--add-rule <NAME> <POLICY_GUID> <RETENTION_DAYS> <RETENTION_VERSIONS>
Add new rule to selected policy
 -aT,--add-auto-assign-tag <GUID> <inc|exc> <TAG>
Add auto-assignment tag
 -c,--create <NAME>
Create a new policy
 -d,--delete <GUID>
Delete a policy
 -g,--details <GUID>
Show details
 -l,--list
List policies
 -L,--list-vms <GUID>
List VMs in the policy
 -m,--modify <GUID> <NAME>
Modify policy
 -p,--set-priority <GUID> <PRIORITY>
Set policy's backup task priority (0-100, 50 = default)
 -r,--list-rules <GUID>
List rules for policy
 -rR,--remove-rules <POLICY_GUID> <RULE_GUID,...,RULE_GUID>
Remove rules from policy
 -rT,--remove-auto-assign-tag <GUID> <inc|exc> <TAG>
Remove auto-assignment tag
 -U,--unassign-vms <VM_GUID,...,VM_GUID>
Unassign VMs from the policy
 -V,--assign-vms <GUID> <VM_GUID,...,VM_GUID>
Assign VMs to the policy
```

Examples

- To list all snapshot policies

```
vprotect vm-snappolicy -l
```

- To show details of the given VM (by GUID)

```
vprotect vm-snappolicy -g 3afcd507-a4f5-484d-8d34-53c73d7a5809
```

- To create a new policy

```
vprotect vm-snappolicy -c "My Policy"
```

- To add `policy1` tag (include) for a policy:

```
vprotect vm-snappolicy -aT 3afcd507-a4f5-484d-8d34-53c73d7a5809 inc policy1
```

- To remove `policy1` tag (include) for a policy:

```
vprotect vm-snappolicy -rT 3afcd507-a4f5-484d-8d34-53c73d7a5809 inc policy1
```

- To set 2 schedules (GUIDs are comma-separated) for a policy (first GUID):

```
vprotect vm-snappolicy -s 3afcd507-a4f5-484d-8d34-53c73d7a5809 391203e3-ad6c-
4532-b69c-78b3a5c
```

Snapshot management policies for storages

To manage snapshot policies for storage in the system used `vprotect storage-snappolicy` sub-command.

Storages are assigned automatically to the policy only if storage has no policy assigned already. If an automatic assignment has been turned on for a policy and the name of the storage matches the regular expression, storage is assigned to the policy, and all schedules for a policy will also be automatically invoked for this storage.

Note: only storage with assigned snapshot management policy can be a snapshot from the CLI or UI

```
[root@vprotect ~]# vprotect storage-snappolicy
Incorrect syntax: Missing required option: [-rR Remove rules from policy, -c Create a
new policy, -d Delete a policy, -g Show details, -l List policies, -aM Set auto-
assignment mode, -L List storages in the policy, -m Modify policy, -aN Set auto-
removal of non-present VMs flag, -aP Set auto-assignment storage pools, -p Set
policy's backup task priority (0-100, 50 = default), -aR Add new rule to selected
policy, -r List rules for policy, -S Assign storages to the policy, -U Unassign
storages from the policy]
```

```
usage: storage-snappolicy -aM <GUID> <DISABLED|ASSIGN_ONLY|ASSIGN_AND_REMOVE> | -aN
<GUID> <0|1> | -aP <GUID > <[STORAGE_POOL_GUID,...,STORAGE_POOL_GUID]> | -aR <NAME>
<POLICY_GUID> <RETENTION_DAYS> <RETENTION_VERSIONS> | -c <NAME> | -d <GUID> | -g
<GUID> | -l | -L <GUID> | -m
       <GUID> <NAME> | -p <GUID> <PRIORITY> | -r <GUID> | -rR <POLICY_GUID>
<RULE_GUID,...,RULE_GUID> | -S <GUID> <STORAGE_GUID,...,STORAGE_GUID> | -U
<STORAGE_GUID,...,STORAGE_GUID>
+Snapshot policy management for storages
 -aM,--set-auto-assign-mode <GUID> <DISABLED|ASSIGN_ONLY|ASSIGN_AND_REMOVE>
Set auto-assignment mode
 -aN,--set-auto-remove-non-present <GUID> <0|1>
Set auto-removal of non-present VMs flag
 -aP,--set-auto-assign-storage-pools <GUID >
<[STORAGE_POOL_GUID,...,STORAGE_POOL_GUID]>   Set auto-assignment storage pools
 -aR,--add-rule <NAME> <POLICY_GUID> <RETENTION_DAYS> <RETENTION_VERSIONS>
Add new rule to selected policy
 -c,--create <NAME>
Create a new policy
 -d,--delete <GUID>
Delete a policy
 -g,--details <GUID>
Show details
 -l,--list
List policies
 -L,--list-storages <GUID>
List storages in the policy
 -m,--modify <GUID> <NAME>
Modify policy
 -p,--set-priority <GUID> <PRIORITY>
Set policy's backup task priority (0-100, 50 = default)
 -r,--list-rules <GUID>
List rules for policy
 -rR,--remove-rules <POLICY_GUID> <RULE_GUID,...,RULE_GUID>
Remove rules from policy
 -S,--assign-storages <GUID> <STORAGE_GUID,...,STORAGE_GUID>
Assign storages to the policy
 -U,--unassign-storages <STORAGE_GUID,...,STORAGE_GUID>
Unassign storages from the policy
```

Examples

To list all snapshot policies

```
vprotect storage-snappolicy -l
```

- To show details of the given snapshot policy (by GUID)

```
vprotect storage-snappolicy -g 3afcd507-a4f5-484d-8d34-53c73d7a5809
```

- To create a new policy

```
vprotect storage-snappolicy -c "My Policy"
```

- To set 2 schedules (GUIDs are comma-separated) for a policy (first GUID):

```
vprotect vm-snappolicy -s 3afcd507-a4f5-484d-8d34-53c73d7a5809 \
 391203e3-ad6c-4532-b69c-78b3a5c
```

Schedules

Schedule management module is used to create schedules associated with VMs or groups of VMs. Each schedule defines days of week and the hour when the backup tasks should be invoked. Each schedule also defines a time window in which the backup process must start. If the task queue is full and the tasks starts after the specified amount of time from the schedule – it will be cancelled and marked as failed.

Note:

- tasks in the queue are run in order from the highest to the lowest priority.
- you can assign multiple schedules if you need backup to be executed at different hours on different days
- remember always to assign schedules to VM or VM group – schedule can be assigned only to a single VM or VM group

To manage schedules in the system used `vprotect sched` sub-command.

```
[root@vprotect ~]# vprotect sched
Incorrect syntax: Missing required option: [-a Set schedule to be active (1) / not
active (0), -c <NAME> <VM_BACKUP | SNAPSHOT | APP_BACKUP> <BACKUP_TYPE> <TIME |
INTERVAL> <START_TIME | INTERVAL_START_HOUR-INTERVAL_END_HOUR> <DURATION |
INTERVAL_FREQUENCY> <everyday | LIST_OF_DAYS_OF_WEEK> <any | FIRST_IN_MONTH |
SECOND_IN_MONTH | THIRD_IN_MONTH | FOURTH_IN_MONTH | LAST_IN_MONTH> <any |
LIST_OF_MONTHS
 Create schedule for VM (backup type: FULL / INCREMENTAL), -d Delete schedule, -g
Show details, -l List schedules, -m <GUID> <NAME> <TYPE> <TIME | INTERVAL>
<START_TIME | INTERVAL_START_HOUR-INTERVAL_END_HOUR> <DURATION | INTERVAL_FREQUENCY>
<everyday | LIST_OF_DAYS_OF_WEEK> <any | FIRST_IN_MONTH | SECOND_IN_MONTH |
THIRD_IN_MONTH | FOURTH_IN_MONTH | LAST_IN_MONTH> <any | LIST_OF_MONTHS
 Modify schedule (backup type: FULL / INCREMENTAL)]

usage: sched -a <arg> | -c <arg> | -d <arg> | -g <arg> | -l | -m <arg>

Schedule management
 -a,--set-active <GUID> <0|1>              Set schedule to be active (1) / not active
(0)
 -c,--create     <NAME> <VM_BACKUP | SNAPSHOT | APP_BACKUP> <BACKUP_TYPE> <TIME |
INTERVAL> <START_TIME | INTERVAL_START_HOUR-INTERVAL_END_HOUR> <DURATION |
                 INTERVAL_FREQUENCY> <everyday | LIST_OF_DAYS_OF_WEEK> <any |
FIRST_IN_MONTH | SECOND_IN_MONTH | THIRD_IN_MONTH | FOURTH_IN_MONTH | LAST_IN_MONTH>
<any | LIST_OF_MONTHS>
                                           Create schedule for VM (backup type: FULL
/ INCREMENTAL)
 -d,--delete <GUID>                        Delete schedule
 -g,--show-details <GUID>                  Show details
 -l,--list                                 List schedules
 -m,--modify <GUID> <NAME> <TYPE> <TIME | INTERVAL> <START_TIME |
INTERVAL_START_HOUR-INTERVAL_END_HOUR> <DURATION | INTERVAL_FREQUENCY> <everyday |
               LIST_OF_DAYS_OF_WEEK> <any | FIRST_IN_MONTH | SECOND_IN_MONTH |
THIRD_IN_MONTH | FOURTH_IN_MONTH | LAST_IN_MONTH> <any | LIST_OF_MONTHS>
```

```
                                                Modify schedule (backup type: FULL /
INCREMENTAL)
```

Examples

- To list all schedules

```
vprotect sched -l
```

- To create a full virtual machine backup schedule with a name Schedule1 executed every day at 05:00 with 60 minutes of time window:

```
vprotect sched -c Schedule1 VM_BACKUP FULL TIME 05:00 60 everyday any any
```

- To create an incremental virtual machine backup schedule with a name Schedule2 executed every Monday, Wednesday and Friday at 17:00 with 90 minutes of time window:

```
vprotect sched -c Schedule2 VM_BACKUP INCREMENTAL TIME 17:00 90 mon,wed,fri any
any
```

Note that days of the week are given as a single comma-separated string of short (3-letter) weekday names

- To disable a schedule with GUID `6651787d-9a55-421d-8158-ead80a70a9cb`:

```
vprotect sched -a 6651787d-9a55-421d-8158-ead80a70a9cb 0
```

VM backup/restore

This module is used to manage the backup and restore processes. It is also used to list backups of a particular VM.

To invoke backup and restore tasks use `vprotect brvm` sub-command.

```
[root@vprotect ~]# vprotect brvm
Required option: [-b Backup (full), -B Backup (full) with task priority (0-100, 50 =
default), -gL Show file details, -F List file systems, -H Restore the backup to the
hypervisor. For KVM mixed volumes please provide storages in form of
BF_GUID=STORAGE_ID with files separated by semicolon, i.e. "BF_GUID=STORAGE_ID;
BF_GUID2=STORAGE_ID2 ...", -i Backup VM (incremental), -I Backup VM (incremental)
with task priority (0-100, 50 = default), -l List backups, -L List backup files, -M
Restore the backup to the hypervisor manager, -r Restore the backup, -T List tasks
related to the backup, -gb Show backup details]

usage: brvm -b <GUID> <BP_GUID | BP_NAME> | -B <GUID> <BP_GUID | BP_NAME> <PRIORITY>
| -F <GUID> | -gb <BACKUP_GUID> | -gL <BACKUP_FILE_GUID> | -H <GUID>
       <HV_GUID | HV_HOST> <STORAGE_ID> | -i <VM_GUID> <BP_GUID | BP_NAME> | -I
<VM_GUID> <BP_GUID | BP_NAME> <PRIORITY> | -l | -L <GUID> | -M <GUID>
       <HVM_GUID | HVM_HOST> <STORAGE_ID> <[CLUSTER_ID]> | -r <GUID> <NODE_GUID |
NODE_NAME> <DIRECTORY> | -T <GUID>
VM backup & restore
```

```
 -b,--backup <GUID> <BP_GUID | BP_NAME>
Backup (full)
 -B,--backup-with-priority <GUID> <BP_GUID | BP_NAME> <PRIORITY>
Backup (full) with task priority (0-100, 50 = default)
 -F,--list-file-systems <GUID>                                          List
file systems
 -gb,--show-backup-details <BACKUP_GUID>                                Show
backup details
 -gsi,--show-backup-status-info <BACKUP_GUID>                           Show
backup status info
 -gL,--show-files-details <BACKUP_FILE_GUID>                            Show
file details
 -H,--restore-to-hv <GUID> <HV_GUID | HV_HOST> <STORAGE_ID>
Restore the backup to the hypervisor. For KVM mixed volumes please provide

storages in form of BF_GUID=STORAGE_ID with files separated by semicolon, i.e.
"BF_GUID=STORAGE_ID; BF_GUID2=STORAGE_ID2 ..."
 -i,--backup-inc <VM_GUID> <BP_GUID | BP_NAME>
Backup VM (incremental)
 -I,--backup-inc-with-priority <VM_GUID> <BP_GUID | BP_NAME> <PRIORITY>
Backup VM (incremental) with task priority (0-100, 50 = default)
 -l,--list                                                              List
backups
 -L,--list-files <GUID>                                                 List
backup files
 -M,--restore-to-hvm <GUID> <HVM_GUID | HVM_HOST> <STORAGE_ID> <[CLUSTER_ID]>
Restore the backup to the hypervisor manager
 -r,--restore <GUID> <NODE_GUID | NODE_NAME> <DIRECTORY>
Restore the backup
 -T,--list-tasks <GUID>                                                 List
tasks related to the backup
```

Examples

- To list all backups and their status:

```
vprotect brvm -l
```

- To show backups of a particular VM:

```
vprotect vm -L 0f36f40c-6427-4035-9f2b-1ead6aca3597
```

- To show files that a specific backup consists of:

```
vprotect brvm -L 4f1c7907-72e9-4797-8470-3f1fbb081751
```

- To show detected file systems in specific backup:

```
vprotect brvm -F 4f1c7907-72e9-4797-8470-3f1fbb081751
```

- To create a full backup of a VM and store it in backup destination set to rule called `MyTSM`

```
vprotect brvm -b 0f36f40c-6427-4035-9f2b-1ead6aca3597 MyTSM
```

- To restore a full backup with given GUID on the current node (`this`) to the `/vprotect_data`

```
vprotect brvm -r 2132182d-e9ab-4478-a1db-48222b0e515b this /vprotect_data
```

- To create an incremental backup (Citrix only) of a VM and store it in backup destination called `MyTSM`

```
vprotect brvm -i 0f36f40c-6427-4035-9f2b-1ead6aca3597 MyTSM
```

- To restore VM backup (first GUID) to the hypervisor (second GUID - Citrix XenServer only) and specific storage

```
vprotect brvm -H 2132182d-e9ab-4478-a1db-48222b0e515b c93140b8-a898-4aff-8eef-
645587ca8289 "Local storage"
```

Storage backup/restore

This module is used to manage the backup and restore process of storage providers.

To invoke backup and restore tasks use `vprotect brst` sub-command.

```
[root@localhost vprotect]# vprotect brst
Incorrect syntax: Missing required option: [-b Backup (full), -B Backup (full) with
task priority (0-100, 50 = default), -r Restore the backup, -S Restore the storage to
the storage provider., -T List tasks related to the backup, -gL Show file details, -i
Backup STORAGE (incremental), -I Backup STORAGE (incremental) with task priority (0-
100, 50 = default), -gb Show backup details, -l List backups, -L List backup files]

usage: brst -b <GUID> <BP_GUID | BP_NAME> | -B <GUID> <BP_GUID | BP_NAME> <PRIORITY>
| -gb <BACKUP_GUID> | -gL <BACKUP_FILE_GUID> | -i <STORAGE_GUID> <BP_GUID | BP_NAME>
| -I <STORAGE_GUID> <BP_GUID | BP_NAME> <PRIORITY> | -l | -L <GUID> | -r <GUID>
<DIRECTORY> | -S <GUID>
       <STORAGE_PROVIDER_GUID | STORAGE_PROVIDER_NAME> <RESTORE_PATH> | -T <GUID>
Storage backup & restore
 -b,--backup <GUID> <BP_GUID | BP_NAME>
Backup (full)
 -B,--backup-with-priority <GUID> <BP_GUID | BP_NAME> <PRIORITY>
Backup (full) with task priority (0-100, 50 = default)
 -gb,--show-backup-details <BACKUP_GUID>
Show backup details
 -gL,--show-files-details <BACKUP_FILE_GUID>
Show file details
 -i,--backup-inc <STORAGE_GUID> <BP_GUID | BP_NAME>
Backup STORAGE (incremental)
 -I,--backup-inc-with-priority <STORAGE_GUID> <BP_GUID | BP_NAME> <PRIORITY>
Backup STORAGE (incremental) with task priority (0-100, 50 = default)
 -l,--list
List backups
```

```
 -L,--list-files <GUID>
List backup files
 -r,--restore <GUID> <DIRECTORY>
Restore the backup
 -S,--restore-to-storage-provider <GUID> <STORAGE_PROVIDER_GUID |
STORAGE_PROVIDER_NAME> <RESTORE_PATH>   Restore the storage to the storage provider.
 -T,--list-tasks <GUID>
List tasks related to the backup
```

Examples

- To list all backups and their status:

```
vprotect brst -l
```

- To show backups of a particular storage:

```
vprotect br -L 0f36f40c-6427-4035-9f2b-1ead6aca3597
```

- To show files that a specific backup consists of:

```
vprotect brst -L 4f1c7907-72e9-4797-8470-3f1fbb081751
```

- To create a full backup of a storage and store it in backup destination called `MyTSM`

```
vprotect brst -b 0f36f40c-6427-4035-9f2b-1ead6aca3597 MyTSM
```

- To restore a full backup with given GUID on the current node (`this`) to the `/vprotect_data`

```
vprotect brst \
-r 2132182d-e9ab-4478-a1db-48222b0e515b this /vprotect_data
```

- To create an incremental backup of a storage and store it in backup destination called `MyTSM`

```
vprotect brst -i 0f36f40c-6427-4035-9f2b-1ead6aca3597 MyTSM
```

Mounted backups

The Mounted backup management module is used to mount and unmounts backups on the given node. This feature is currently supported for RHV/oVirt/OVM VMs. Each mounted backup can be mounted automatically (auto-detection of mount points within a single root or manually with separate mount points for each volume.

To invoke mount/unmount tasks use `vprotect mnt` sub-command.

```
```

```
[root@vprotect ~]# vprotect mnt
Incorrect syntax: Missing required option: [-T List tasks related to the mounted
backup, -u Unmount previously mounted backup, -F List file systems, -l List mounted
backups, -L List mounted files, -mi Mount iSCSI., -m Mount backup according to the
MOUNT_SPECIFICATION, -Li List files for selected backup, that can be mounted using
iSCSI mode.]

usage: mnt -F <GUID> | -l | -L <GUID> | -Li <BACKUP_GUID> | -m <GUID>
<NODE_CONFIG_GUID | NODE_CONFIG_NAME> <auto|manual> <MOUNT_SPECIFICATION> | -mi
<BACKUP_GUID> <NODE_CONFIG_GUID | NODE_CONFIG_NAME>
<ALLOWED_CLIENT,...,ALLOWED_CLIENT> <DISK_GUID,...,DISK_GUID> | -T <GUID> | -u <GUID>
Mounted backup management
 -F,--list-file-systems <GUID>
List file systems
 -l,--list
List mounted backups
 -L,--list-files <GUID>
List mounted files
 -Li,--list-iscsi-mountable-files <BACKUP_GUID>
List files for selected backup, that can be mounted using iSCSI mode.
 -m,--mount <GUID> <NODE_CONFIG_GUID | NODE_CONFIG_NAME> <auto|manual>
<MOUNT_SPECIFICATION>                                          Mount backup
according to the MOUNT_SPECIFICATION
 -mi,--mount-iscsi <BACKUP_GUID> <NODE_CONFIG_GUID | NODE_CONFIG_NAME>
<ALLOWED_CLIENT,...,ALLOWED_CLIENT> <DISK_GUID,...,DISK_GUID>   Mount iSCSI.
 -T,--list-tasks <GUID>
List tasks related to the mounted backup
 -u,--unmount <GUID>
Unmount previously mounted backup
```

Examples

- To list all mounted backups:

```
vprotect mnt -l
```

- To list all mounted files used by mounted backup with GUID `1ac068d3-4848-4c98-b30b-54ce050b6a95` (**note** that this is mounted backup GUID not a backup GUID):

```
vprotect mnt -L 1ac068d3-4848-4c98-b30b-54ce050b6a95
```

- To show detected file systems in specific backup:

```
vprotect mnt -F 1ac068d3-4848-4c98-b30b-54ce050b6a95
```

- To mount all file systems in backup with GUID `2132182d-e9ab-4478-a1db-48222b0e515b` and node config with GUID `3a9d48dc-e48f-11eb-a1ce-005056a6b7e5` to /mnt/myVM/2017-01-01:

```
vprotect mnt -m 2132182d-e9ab-4478-a1db-48222b0e515b 3a9d48dc-e48f-11eb-a1ce-
005056a6b7e5 auto /mnt/myVM/2017-01-01
```

- To mount manually file systems in backup with GUID `2132182d-e9ab-4478-a1db-48222b0e515b` with specifying mount points you need to provide semicolon-separated list where you provide name of the volume=mount point (white space before or after semicolon or equal sign is not allowed)

```
vprotect mnt -m 2132182d-e9ab-4478-a1db-48222b0e515b manual
"/dev/sda1=/mnt/myVM/sda1;/dev/vg_sda/lv_root=/mnt/myVM/lv_root"
```

- To unmount mounted backup with GUID `1ac068d3-4848-4c98-b30b-54ce050b6a95`:

```
vprotect mnt -u 1ac068d3-4848-4c98-b30b-54ce050b6a95
```

Tasks

The Task Management module is used to show and cancel tasks being executed. You can also monitor the progress of the tasks.

Note:

- tasks in the queue are run in the order from the highest to the lowest priority.
- queue is being periodically cleaned, so only the last tasks are being shown

To manage tasks use `vprotect task` sub-command.

```
[root@vprotect ~]# vprotect task
Incorrect syntax: Missing required option: [-Q List queued tasks, -R List running
tasks, -d Delete/cancel task, -F List finished (including failed) tasks, -g Show task
details, -l List tasks (this node only), -L List tasks (all nodes and not assigned to
any node)]

usage: task -d <GUID> | -F | -g <GUID> | -l | -L | -Q | -R
Task management
 -d,--delete <GUID>    Delete/cancel task
 -F,--list-finished    List finished (including failed) tasks
 -g,--details <GUID>   Show task details
 -l,--list             List tasks (this node only)
 -L,--list-all         List tasks (all nodes and not assigned to any node)
 -Q,--list-queued      List queued tasks
 -R,--list-running     List running tasks
```

Examples

- To list tasks assigned to the current node:

```
vprotect task -l
```

- To list all tasks in the system:

```
vprotect task -L
```

- To show task details:

```
vprotect task -g 091d623d-edea-490f-8b3b-da30c09a3f93
```

- To cancel the task with ID `091d623d-edea-490f-8b3b-da30c09a3f93`:

```
vprotect task -d 091d623d-edea-490f-8b3b-da30c09a3f93
```

Note: Some tasks may require to be finished before they are canceled, i.e. export VM from the hypervisor – after cancellation, it may take some time for the task to process cancel request and clean up snapshots, etc. if necessary - backup will be marked as failed.

Project

The Project module is used to view details and set a quota for available projects.

```
[root@localhost vprotect]# vprotect project
Incorrect syntax: Missing required option: [-g Show Project details, -l List
Projects, -sQ Set Project Quota]

usage: project -g <GUID> | -l | -sQ <GUID> <QUOTA_GUID>
Project management
 -g,--details <GUID>                  Show Project details
 -l,--list                            List Projects
 -sQ,--set-quota <GUID> <QUOTA_GUID>  Set Project Quota
```

Examples

- To list all projects:

```
vprotect project -l
```

- To set quota with GUID `6f0bfb3c-24dd-4d12-8a72-997ded2ecc98` to project with GUID `ca707d31-f403-40d5-b160-6ac512457b87`

```
vprotect project -sQ ca707d31-f403-40d5-b160-6ac512457b87 6f0bfb3c-24dd-4d12-
8a72-997ded2ecc98
```

User Management

The User module is used to manage users and their settings. You can add or remove users, change their password or timezone.

```
[root@localhost vprotect]# vprotect user
Incorrect syntax: Missing required option: [-c Create user, -d Delete user, -g Show
```

```
user details, -l List users, -m Update user's property, -sP Update user's password, -
sA Update user's activation state]

usage: user -c <LOGIN> <FIRST_NAME> <LAST_NAME> <TIMEZONE> <LANGUAGE> <ACTIVE> | -d
<GUID> | -g <GUID> | -l | -m <GUID> <PROPERTY_NO.> <VALUE> | -sA <GUID> <ACTIVE> | -
sP <GUID>>
User management
 -c,--create <LOGIN> <FIRST_NAME> <LAST_NAME> <TIMEZONE> <LANGUAGE> <ACTIVE>   Create
user
 -d,--delete <GUID>                                                             Delete
user
 -g,--details <GUID>                                                            Show
user details
 -l,--list                                                                      List
users
 -m,--modify <GUID> <PROPERTY_NO.> <VALUE>                                      Update
user's property
 -sA,--set-active <GUID> <ACTIVE>                                               Update
user's activation state
 -sP,--set-password <GUID>>
```

Examples

- To create a new user

```
vprotect user -c jdoe John Doe UTC EN true
```

- To list all users

```
vprotect user -l
```

```
                GUID                   First Name  Last Name  Active
------------------------------------  ----------  ---------  ------
                                   1  The         Admin      true
259c07ab-5097-4826-8a91-dd281840faf5  John         Doe        true
```

- To set password for the user

```
vprotect user -sP 705490c2-7734-4a56-a563-24471447bf2b
```

Quota

Quota management module is used to manage backup/restore limits for virtual machines in projects.

To manage Quotas in the system use `vprotect quota` sub-command.

```
[root@localhost vprotect]# vprotect quota
Incorrect syntax: Missing required option: [-aR Add Rule to Quota, -c Create Quota, -
d Delete Quota, -g Show Quota details, -sN Change Quota name, -l List Quotas, -L List
```

```
Projects for Quota, -eR Edit Rule in Quota, -sA Change Quota active state, -dR Delete
Rule from Quota]

usage: quota -aR <GUID> <RULE_NAME> <TYPE> <ACTIVE> <HARD_LIMIT>
<HARD_LIMIT_TIME_FRAME> <SOFT_LIMIT> <SOFT_LIMIT_TIME_FRAME> | -c <NAME> | -d <GUID>
| -dR <GUID> <RULE_NAME> <TYPE> | -eR <GUID> <RULE_NAME> <TYPE> <ACTIVE>
       <HARD_LIMIT> <HARD_LIMIT_TIME_FRAME> <SOFT_LIMIT> <SOFT_LIMIT_TIME_FRAME> | -g
<GUID> | -l | -L <GUID> | -sA <GUID> <ACTIVE> | -sN <GUID> <NAME>
Quota management
 -aR,--add-rule <GUID> <RULE_NAME> <TYPE> <ACTIVE> <HARD_LIMIT>
<HARD_LIMIT_TIME_FRAME> <SOFT_LIMIT> <SOFT_LIMIT_TIME_FRAME>    Add Rule to Quota
 -c,--create <NAME>
Create Quota
 -d,--delete <GUID>
Delete Quota
 -dR,--delete-rule <GUID> <RULE_NAME> <TYPE>
Delete Rule from Quota
 -eR,--edit-rule <GUID> <RULE_NAME> <TYPE> <ACTIVE> <HARD_LIMIT>
<HARD_LIMIT_TIME_FRAME> <SOFT_LIMIT> <SOFT_LIMIT_TIME_FRAME>   Edit Rule in Quota
 -g,--details <GUID>
Show Quota details
 -l,--list
List Quotas
 -L,--list-projects <GUID>
List Projects for Quota
 -lR,--list-all-rules
List all possible rule names
 -sA,--set-active <GUID> <ACTIVE>
Change Quota active state
 -sN,--set-name <GUID> <NAME>
Change Quota name
```

Examples

- To list all quotas:

```
vprotect quota -l
```

- To list all projects for Quota with GUID `1ac068d3-4848-4c98-b30b-54ce050b6a95`:

```
vprotect quota -L 1ac068d3-4848-4c98-b30b-54ce050b6a95
```

- To list all possible rule names:

```
vprotect quota -lR
```

- To add rule to Quota with GUID `1ac068d3-4848-4c98-b30b-54ce050b6a95`:

```
vprotect quota -aR 1ac068d3-4848-4c98-b30b-54ce050b6a95 NUMBER_OF_BACKUPS TOTAL
true 10 24 5 10
```

RBAC

This module allows listing possible context types and privilege types used in RBAC management.

This module uses `vprotect rbac` sub-command.

```
[root@localhost vprotect]$ vprotect rbac
Incorrect syntax: Missing required option: [-lp List all possible privilege types, -
lc List all possible context types]

usage: rbac -lc | -lp
User management
 -lc,--list-context     List all possible context types
 -lp,--list-privilege   List all possible privilege types
```

Examples

- To list all possible privilege types

  ```
  vprotect rbac -lp
  ```

User Role Management

The User Role management module is used to manage Roles and their privileges.

Note:

- only rules that are created by the user can be deleted.

To manage User Roles in the system use `vprotect role` sub-command.

```
[root@localhost vprotect]$ vprotect role
Incorrect syntax: Missing required option: [-rC Remove context from the role, -aC Add
context to role, -c Create role, -d Delete role, -g Get role details, -lC List
contexts of the role, -l Get role list, -m Modify role name, -rP Remove privilege
from the role, -aP Add privilege to role]

usage: role -aC <GUID> | -aP <GUID> <PRIVILEGE NAME> | -c <NAME> | -d <GUID> | -g
<GUID> | -l | -lC <GUID> | -m <GUID> <NAME> | -rC <GUID> <CONTEXT INSTANCE GUID> | -
rP <GUID> <PRIVILEGE NAME>
+Access management
 -aC,--add-context <GUID>                                Add context to role
 -aP,--add-privilege <GUID> <PRIVILEGE_NAME>             Add privilege to role
 -c,--create <NAME>                                      Create role
 -d,--delete <GUID>                                      Delete role
 -g,--details <GUID>                                     Get role details
 -l,--list                                               Get role list
 -lC,--list-contexts <GUID>                              List contexts of the role
 -m,--modify <GUID> <NAME>                               Modify role name
 -rC,--remove-context <GUID> <CONTEXT_INSTANCE_GUID>     Remove context from the role
 -rP,--remove-privilege <GUID> <PRIVILEGE_NAME>          Remove privilege from the role
```

Examples

- To create a new Role

```
vprotect role -c Tester
```

- To add VE_INSTANCE_READ privilege to a Role with GUID `1ac068d3-4848-4c98-b30b-54ce050b6a95`

```
vprotect role -aP 1ac068d3-4848-4c98-b30b-54ce050b6a95 VE_INSTANCE_READ
```

User Group Management

+User Group management module is used to bind Users with a set of Roles.

Note:

- only groups that are created by the user can be deleted.

To manage User Roles in the system use `vprotect group` sub-command.

```
[root@localhost vprotect]$ vprotect group
Incorrect syntax: Missing required option: [-rR Remove role from the group, -aR Add
role to the group, -c Create group, -rU Remove user from the group, -d Delete group,
-aU Add user to the group, -g Get group details, -l Get group list, -m Modify group
name]

usage: group -aR <GUID> <ROLE GUID> | -aU <GUID> <USER_GUID> | -c <NAME> | -d <GUID>
| -g <GUID> | -l | -m <GUID> <NAME> | -rR <GUID> <ROLE_GUID> | -rU <GUID> <USER_GUID>
AppUser Group management
 -aR,--add-role <GUID> <ROLE GUID>      Add role to the group
 -aU,--add-user <GUID> <USER_GUID>      Add user to the group
 -c,--create <NAME>                     Create group
 -d,--delete <GUID>                     Delete group
 -g,--details <GUID>                    Get group details
 -l,--list                              Get group list
 -m,--modify <GUID> <NAME>              Modify group name
 -rR,--remove-role <GUID> <ROLE_GUID>   Remove role from the group
 -rU,--remove-user <GUID> <USER_GUID>   Remove user from the group
```

Examples

- To add Role with GUID `1ac068d3-4848-4c98-b30b-54ce050b6a95` to Group with GUID `54c57989-9d99-480f-a6da-b4f34b7bd812`

  ```
  vprotect group -aR 54c57989-9d99-480f-a6da-b4f34b7bd812 1ac068d3-4848-4c98-b30b-
  54ce050b6a95
  ```

- To remove User with GUID `91e6bf9c-59c6-4653-9854-e9c920198343` from Group with GUID `54c57989-9d99-480f-a6da-b4f34b7bd812`

  ```
  vprotect group -rU 54c57989-9d99-480f-a6da-b4f34b7bd812 91e6bf9c-59c6-4653-
  9854-e9c920198343
  ```

Application backup/restore

This module is used to manage tge backup and restore process. It is also used to list backups of a particular application.

To invoke backup and restore tasks use `vprotect brapp` sub-command.

```
[root@vprotect ~]# vprotect brapp
Required option: [-b Backup (full), -B Backup (full) with task priority (0-100, 50 =
default), -r Restore the backup, -T List tasks related to the backup, -gL Show file
details, -I Restore and import backup. Enter D as path for DEFAULT source path from
application, -gb Show backup details, -l List backups, -L List backup files]

usage: brapp -b <GUID> <BP_GUID | BP_NAME> | -B <GUID> <BP_GUID | BP_NAME> <PRIORITY>
| -gb <BACKUP_GUID> | -gL <BACKUP_FILE_GUID> | -I <BACKUP_GUID>
       <DST_APP_GUID> <PATH> | -l | -L <GUID> | -r <GUID> <NODE_GUID | NODE_NAME>
<DIRECTORY> | -T <GUID>
Application backup & restore
 -b,--backup <GUID> <BP_GUID | BP_NAME>                              Backup (full)
 -B,--backup-with-priority <GUID> <BP_GUID | BP_NAME> <PRIORITY>   Backup (full) with
task priority (0-100, 50 = default)
 -gb,--show-backup-details <BACKUP_GUID>                             Show backup
details
 -gL,--show-files-details <BACKUP_FILE_GUID>                         Show file details
 -I,--restore-and-import <BACKUP_GUID> <DST_APP_GUID> <PATH>       Restore and import
backup. Enter D as path for DEFAULT source path from application
 -l,--list                                                           List backups
 -L,--list-files <GUID>                                              List backup files
 -r,--restore <GUID> <NODE_GUID | NODE_NAME> <DIRECTORY>           Restore the backup
 -T,--list-tasks <GUID>                                              List tasks related
to the backup
```

Examples

- To list all backups and their status:

```
vprotect brapp -l
```

- To show backups of a particular VM:

```
vprotect app -L 0f36f40c-6427-4035-9f2b-1ead6aca3597
```

- To show files that a specific backup consists of:

```
vprotect brapp -L 4f1c7907-72e9-4797-8470-3f1fbb081751
```

- To create a full backup of a app and store it in backup destination called `MyTSM`

```
vprotect brapp -b 0f36f40c-6427-4035-9f2b-1ead6aca3597 MyTSM
```

- To restore a full backup with given GUID on the current node (`this`) to the `/vprotect_data`

```
vprotect brapp -r 2132182d-e9ab-4478-a1db-48222b0e515b this /vprotect_data
```

- To restore application backup (first GUID) to the other application (assuming it has REMOTE_SSH in Command Execution Configuration - second GUID)

```
vprotect brapp -H 2132182d-e9ab-4478-a1db-48222b0e515b c93140b8-a898-4aff-8eef-
645587ca8289 "Local storage"
```

Applications

The Application management module is used to provide information about apps that have been defined report the status of the last backup of your apps (and all backups for a particular app).

To manage Applications in the system used `vprotect app` sub-command.

```
[root@vprotect ~]# vprotect app
Required option: [-A Assign application backup policy, -dE Delete environment
variable, -c Create a new application, -d Delete an application, -aE Add environment
variable to application, -g Show application details, -xC Set application CMD exec
configuration, -l List applications, -L List backups of the application, -m Modify
application, -sC Set SSH access credentials, -sH Set SSH access host/port, -sK Set
SSH key path, -mE Modify environment variable. Set variable hidden in UI(1) or
visible(0), -lE List environment variables for application, -sN Set application node]

usage: app -A <GUID> <APP_POLICY_GUID> | -aE <APP_GUID> <NAME> <VALUE> | -c <NAME>
<CONFIG_GUID> | -d <GUID> | -dE <GUID> | -g <GUID> | -l | -L <GUID> | -lE
       <APP_GUID> | -m <GUID> <NAME> | -mE <GUID> <APP_GUID> <NAME> <VALUE> <0|1> | -
sC <GUID> <SSH_USER> <SSH_PASS> | -sH <GUID> <SSH_HOST> <SSH_PORT> | -sK
       <GUID> <SSH_KEYPATH> | -sN <GUID> <NODE_GUID> | -xC <GUID>
<APP_CMD_EXEC_CONFIG_GUID>
Application backup management
 -A,--assign-app-policy <GUID> <APP_POLICY_GUID>                    Assign
application backup policy
 -aE,--add-env-variable <APP_GUID> <NAME> <VALUE>                   Add environment
variable to application
 -c,--create <NAME> <CONFIG_GUID>                                   Create a new
application
 -d,--delete <GUID>                                                 Delete an
application
 -dE,--delete-env-variable <GUID>                                   Delete
environment variable
 -g,--details <GUID>                                                Show application
details
 -l,--list                                                          List applications
 -L,--list-backups <GUID>                                           List backups of
the application
 -lE,--list-env-variables <APP_GUID>                                List environment
variables for application
 -m,--modify <GUID> <NAME>                                          Modify
application
```

```
 -mE,--modify-env-variable <GUID> <APP_GUID> <NAME> <VALUE> <0|1>   Modify
environment variable. Set variable hidden in UI(1) or visible(0)
 -sC,--set-ssh-credentials <GUID> <SSH_USER> <SSH_PASS>             Set SSH access
credentials
 -sH,--set-ssh-host <GUID> <SSH_HOST> <SSH_PORT>                   Set SSH access
host/port
 -sK,--set-ssh-key-path <GUID> <SSH_KEYPATH>                       Set SSH key path
 -sN,--set-node <GUID> <NODE_GUID>                                 Set application
node
 -xC,--set-app-cmd-exec-config <GUID> <APP_CMD_EXEC_CONFIG_GUID>   Set application
CMD exec configuration
```

Examples

- To list all Applications

```
vprotect app -l
```

- To show details of the given Application (by GUID)

```
vprotect app -g 0f36f40c-6427-4035-9f2b-1ead6aca3597
```

- To add Application (first GUID) to the given policy (second GUID):

```
vprotect app -A 0f36f40c-6427-4035-9f2b-1ead6aca3597 3afcd507-a4f5-484d-8d34-
53c73d7a5809
```

- To show backup history of a VM with given GUID:

```
vprotect app -L 0f36f40c-6427-4035-9f2b-1ead6aca3597
```

Application backup policies

Application backup policies management module is used to define backup policies for Applications. You can assign different backup priority for a policy when the scheduler invokes backup task. You need first to define the application backup policy and then add Applications to it. The Application can belong only to a single backup policy.

To manage Application policies in the system used `vprotect apppolicy` sub-command.

Note: it is impsortant to assign backup destination for a policy (required for node to know where to store backups)

```
[root@vprotect ~]# vprotect apppolicy
Required option: [-p Set policy's backup task priority (0-100, 50 = default), -rR
Remove rules from policy, -A Assign applications to policy, -aR Add new rule to
selected policy, -r List rules for application backup policy, -c Create application
backup policy, -d Delete a policy, -U Unassign applications from policy, -g Show
details, -l List policies, -m Modify application backup policy]

usage: apppolicy -A <GUID> <APP_GUID,...,APP_GUID> | -aR <NAME> <POLICY_GUID>
```

```
<SCHEDULE_GUID> <BACKUP_DESTINATION_GUID> | -c <NAME> <PRIORITY> | -d <GUID> |
       -g <GUID> | -l | -m <GUID> <NAME> <PRIORITY> | -p <GUID> <PRIORITY> | -r
<GUID> | -rR <POLICY_GUID> <RULE_GUID,...,RULE_GUID> | -U <GUID>
       <APP_GUID,...,APP_GUID>
Application backup policy management
 -A,--assign applications <GUID> <APP_GUID,...,APP_GUID>
Assign applications to policy
 -aR,--add-rule <NAME> <POLICY_GUID> <SCHEDULE_GUID> <BACKUP_DESTINATION_GUID>   Add
new rule to selected policy
 -c,--create <NAME> <PRIORITY>
Create application backup policy
 -d,--delete <GUID>
Delete a policy
 -g,--details <GUID>                                                            Show
details
 -l,--list                                                                      List
policies
 -m,--modify <GUID> <NAME> <PRIORITY>
Modify application backup policy
 -p,--set-priority <GUID> <PRIORITY>                                            Set
policy's backup task priority (0-100, 50 = default)
 -r,--list-rules <GUID>                                                         List
rules for application backup policy
 -rR,--remove-rules <POLICY_GUID> <RULE_GUID,...,RULE_GUID>
Remove rules from policy
 -U,--unassign applications <GUID> <APP_GUID,...,APP_GUID>
Unassign applications from policy
```

Examples

- To list all application backup policies

```
vprotect apppolicy -l
```

- To show details of the given application (by GUID)

```
vprotect apppolicy -g 3afcd507-a4f5-484d-8d34-53c73d7a5809
```

- To create a new policy

```
vprotect apppolicy -c "My Policy" 50
```

- To set backup destination for a policy:

```
Syntax: -aR <NAME> <POLICY_GUID> <SCHEDULE_GUID> <BACKUP_DESTINATION_GUID>
vprotect apppolicy -aR MyPolicyRule d804439e-aeda-4fea-8f79-710dc355d2d1
1076134b-4e29-45ea-8c79-1e8ca216a3b8  9038d316-5d02-4972-913b-4201f4947178
```

Application command execution management

Application command execution management module is used to define command execution for application. You can assign application to command definition or show details of command config. As you can see in the module syntax, you can do much more and we will show such operations in examples.

```
[root@vprotect ~]# vprotect appconf
Required option: [-sS Set source path. Please remember that wildcard paths should be
specified inside double quotes., -A Assign applications to config, -c Create
application command execution config, timeout [min.], -d Delete application command
execution config, -e Set export data to false(0) or true(1), -g Show details, -l List
application command execution configs, -m Modify application command execution
config", -sC Set CMD as semi-colon-separated string, i.e. "cmd;-a;-b", -r Remove
files after export to false(0) or true(1), -sE Set handling for standard error.
Values: DONT_IGNORE, IGNORE_WITH_WARNING, IGNORE_WITHOUT_WARNING, -t Set timeout in
minutes, -U Unassign applications from config, -sI Set ignored command exit codes
e.g. '15, 101-150' or '*']

usage: appconf -A <GUID> <APP_GUID,...,APP_GUID> | -c <NAME> <NODE | REMOTE_SSH>
<FILE | STREAM> <TIMEOUT> | -d <GUID> | -e <GUID> <0|1>
       | -g <GUID> | -l | -m <GUID> <NAME> <NODE | REMOTE_SSH> <FILE | STREAM> | -r
<GUID> <0|1> | -sC <GUID> <CMD_STRING> | -sE <GUID>
       <HANDLING> | -sI <GUID> <IGNORED_EXIT_CODES> | -sS <GUID> <SOURCE_PATH> | -t
<GUID> <TIMEOUT> | -U <GUID> <APP_GUID,...,APP_GUID>
App command execution management
 -A,--assign-applications <GUID> <APP_GUID,...,APP_GUID>            Assign
applications to config
 -c,--create <NAME> <NODE | REMOTE_SSH> <FILE | STREAM> <TIMEOUT>   Create
application command execution config, timeout [min.]
 -d,--delete <GUID>                                                 Delete
application command execution config
 -e,--set-export-data <GUID> <0|1>                                  Set export data
to false(0) or true(1)
 -g,--details <GUID>                                                Show details
 -l,--list                                                          List application
command execution configs
 -m,--modify <GUID> <NAME> <NODE | REMOTE_SSH> <FILE | STREAM>      Modify
application command execution config"
 -r,--remove-after-export <GUID> <0|1>                              Remove files
after export to false(0) or true(1)
 -sC,--set-cmd-arg <GUID> <CMD_STRING>                              Set CMD as semi-
colon-separated string, i.e. "cmd;-a;-b"
 -sE,--set-std-error <GUID> <HANDLING>                              Set handling for
standard error. Values: DONT_IGNORE,

IGNORE_WITH_WARNING, IGNORE_WITHOUT_WARNING
 -sI,--set-ignored-codes <GUID> <IGNORED_EXIT_CODES>                Set ignored
command exit codes e.g. '15, 101-150' or '*'
 -sS,--set-source-path <GUID> <SOURCE_PATH>                         Set source path.
Please remember that wildcard paths should be
                                                                    specified inside
double quotes.
 -t,--timeout <GUID> <TIMEOUT>                                      Set timeout in
minutes
 -U,--unassign-applications <GUID> <APP_GUID,...,APP_GUID>          Unassign
applications from config
```

Examples

- To list all command configs:

```
[root@vprotect ~]# vprotect appconf -l

                GUID                                  Name              CmdExecMethod
Applications  Export data  Remove files after export  Source type
------------------------------------  --------------------------  -------------  ----
--------  -----------  -------------------------  -----------
758112e8-2db6-46b1-8a65-ee7064f4933f  DB2                         Remote SSH     -
true         true                        File
f807b3b1-7909-471f-8224-b8948dfca91f  file-backup                 Remote SSH     -
true         false                       File
8b5e2b3f-3837-4f9d-a52a-fa7e9d0378fe  Kubernetes/OpenShift etcd   Remote SSH     -
true         true                        File
9a6b1277-4388-42c3-8f81-ea4af6b0b27c  mysql                       Remote SSH     -
true         true                        File
785ac097-cd1d-43e3-92c3-ac42d710adb3  MySQL/MariaDB               Remote SSH     -
true         true                        File
49fa4b52-0fda-44db-a692-7ee8ed071b86  MySQL/MariaDB_2             Remote SSH     -
true         true                        File
```

- To see command config details:

```
[root@vprotect ~]# vprotect appconf -g 9a6b1277-4388-42c3-8f81-ea4af6b0b27c
Property                  Value
------------------------  ------------------------------------------------------------
--

GUID                      9a6b1277-4388-42c3-8f81-ea4af6b0b27c
Name                      mysql
CmdArg                    [$VP_MYSQL_SCRIPTPATH/vp_backup_mysql.sh, >>,
$VP_MYSQL_LOGFILE]
Applications              []
Cmd execution method      REMOTE_SSH
Export data               true
Remove files after export  true
Source type               FILE
Source path               $VP_MYSQL_STOREPATH/*
Timeout in minutes        60
Ignored exit codes        -
Standard error handling   DONT_IGNORE
```

Restore Jobs

You can use this small module to list restore job operations and see the details of every task.

```
[root@vprotect ~]# vprotect restorejob
Incorrect syntax: Missing required option: [-g Show restore job details, -l List
restore jobs]

usage: restorejob -g <RESTOREJOB_GUID> | -l
Restore jobs
 -g,--show-restore-job-details <RESTOREJOB_GUID>   Show restore job details
 -l,--list                                         List restore jobs
```

Examples

- To list restore jobs:

```
 [root@vprotect ~]# vprotect restorejob -l

                GUID                      Restore Type     Status
Status info
VM/APP
------------------------------------  ------------------  -------  ------------------
-------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------
------
e9aff98f-e431-467f-b9f9-46b2f86068eb  Restore and mount   Success  Backups of VM:
[PM]Windows_2016 (size: 50 GiB) mounted in: 1m 14s.
-
0dcdfed3-f793-4b9f-8faf-a608396de8e8  Restore             Failed
ExternalAPIException: Failed to create directory: /vprotect_data/import/a2778f74-
dc6c-4a1d-88ea-1f85361f4fbd/VM_01_Apine/2020-06-08__11.50.
-
fd99c9ec-ac25-448c-a973-d654936076b2  Restore             Failed   Backup destination
is not assigned to the node
-
f23c2c8c-2bec-4e8e-9ba9-2c6251434907  Restore and mount   Success  Backups of VM:
alpine (size: 2.3 GiB) mounted in: 1m 31s
a24f15c0-617f-4808-869a-ed346e30a713  Restore and import  Success  Backups of VM:
Alpine-Linux (size: 2 GiB) imported in: 3m 5s.
```

- To see restore job details:

```
[root@vprotect ~]# vprotect restorejob -g e9aff98f-e431-467f-b9f9-46b2f86068eb
Property                        Value
------------------------------  ------------------------------------------------
--------

GUID                            e9aff98f-e431-467f-b9f9-46b2f86068eb
Restore Type                    RESTORE_AND_MOUNT
Status                          SUCCESS
Status info                     Backups of VM: [PM]Windows_2016 (size: 50 GiB)
mounted in: 1m 14s.
VM/APP                          -
Tasks                           0
Backup                          1906e226-2ba6-439a-b723-31efb6e5196a
Destination VM/APP              [PM]Windows_2016 (f2354325-562e-465b-abc4-
c4db51036b80)
Restore Storage ID              -
Restore Cluster ID              -
Restored VM/APP Name            -
Restore Project Name            -
Restore Path                    -
Tenant ID                       -
Base Image                      -
Data Center Name                -
Restored Disk Allocation Format  -
Mounted Backup Mode             AUTO
```

```
Backup Type                          FULL
Node                                 vPro-Local (b46043f2-df06-482c-b4ba-37fc8093022c)
```

Recovery plans policies

The Recovery plans policies module is used to define recovery plans policies and rules for VMs. You can assign different restore priorities for a policy when the scheduler invokes the restore task. You need first to create a new policy and then add new rules to it.

```
[root@vprotect ~]# vprotect recplan
Required option: [-sRrci Set restore cluster id in rule, -sRa Set rule status, -
sRhvmt Set hypervisor manager type in rule, -sRuag Set rule use auto generated name,
-sRrp Set restore path in rule, -sRdc Set data center in rule, -sRn Set node in rule,
-sRrn Set target VM name in rule, -sRtp Set target project in rule, -aR Add new rule
to selected policy, -sRdaf Set disk allocation format in rule, -sRrsi Set restore
storage id in rule, -sRv Add virtual machines to rule, -rR Remove rules from policy,
-c Create a new policy, -d Delete a policy, -sRbs Set backup selection in rule, -g
Show details, -sRovw Set overwrite status in rule, -l List policies, -m Modify
policy, -p Set policy's backup task priority (0-100, 50 = default), -r List rules for
policy, -srBi Set base image in rule, -sRhv Set hypervisor in rule, -sRhvm Set
hypervisor manager in rule, -sRhvt Set hypervisor type in rule]

usage: recplan -aR <NAME> <POLICY_GUID>> | -c <NAME> | -d <GUID> | -g <GUID> | -l | -
m <GUID> <NAME> | -p <GUID> <PRIORITY> | -r <GUID> |
       -rR <POLICY_GUID> <RULE_GUID,...,RULE_GUID> | -sRa <RULE_GUID> <TRUE|FALSE>> |
-srBi <RULE_GUID> <BASE_IMAGE_UUID>> | -sRbs
       <RULE_GUID> <LAST_SUCCESSFUL | ANY>> | -sRdaf <RULE_GUID> <PREALLOCATED |
SPARSE>> | -sRdc <RULE_GUID> <DATA_CENTER_NAME>> | -sRhv
       <RULE_GUID> <HYPERVISOR_GUID>> | -sRhvm <RULE_GUID> <HYPERVISORMANAGER_GUID>>
| -sRhvmt <RULE_GUID> <HYPERVISORMANAGERTYPE>> |
       -sRhvt <RULE_GUID> <HYPERVISORTYPE>> | -sRn <RULE_GUID> <NODE_GUID>> | -sRovw
<RULE_GUID> <TRUE|FALSE>> | -sRrci <RULE_GUID>
       <RESTORE_CLUSTER_ID>> | -sRrn <RULE_GUID> <VM_NAME>> | -sRrp <RULE_GUID>
<PATH>> | -sRrsi <RULE_GUID> <RESTORE_STORAGE_ID>> |
       -sRtp <RULE_GUID> <PROJECT_NAME>> | -sRuag <RULE_GUID> <TRUE|FALSE>> | -sRv
<RULE_GUID> <VM_GUIDS>>
Recovery plan policies
 -aR,--add-rule <NAME> <POLICY_GUID>>                                          Add
new rule to selected policy
 -c,--create <NAME>
Create a new policy
 -d,--delete <GUID>
Delete a policy
 -g,--details <GUID>                                                           Show
details
 -l,--list                                                                     List
policies
 -m,--modify <GUID> <NAME>
Modify policy
 -p,--set-priority <GUID> <PRIORITY>                                           Set
policy's backup task priority (0-100, 50 = default)
 -r,--list-rules <GUID>                                                        List
rules for policy
 -rR,--remove-rules <POLICY_GUID> <RULE_GUID,...,RULE_GUID>
Remove rules from policy
 -sRa,--set-rule-active <RULE_GUID> <TRUE|FALSE>>                              Set
rule status
```

```
 -srBi,--set-rule-base-image <RULE_GUID> <BASE_IMAGE_UUID>>                          Set
base image in rule
 -sRbs,--set-rule-backup-selection <RULE_GUID> <LAST_SUCCESSFUL | ANY>>          Set
backup selection in rule
 -sRdaf,--set-rule-disk-allocation-format <RULE_GUID> <PREALLOCATED | SPARSE>>   Set
disk allocation format in rule
 -sRdc,--set-rule-data-center <RULE_GUID> <DATA_CENTER_NAME>>                    Set
data center in rule
 -sRhv,--set-rule-hv <RULE_GUID> <HYPERVISOR_GUID>>                              Set
hypervisor in rule
 -sRhvm,--set-rule-hvm <RULE_GUID> <HYPERVISORMANAGER_GUID>>                     Set
hypervisor manager in rule
 -sRhvmt,--set-rule-hvm-type <RULE_GUID> <HYPERVISORMANAGERTYPE>>                Set
hypervisor manager type in rule
 -sRhvt,--set-rule-hv-type <RULE_GUID> <HYPERVISORTYPE>>                         Set
hypervisor type in rule
 -sRn,--set-rule-node <RULE_GUID> <NODE_GUID>>                                   Set
node in rule
 -sRovw,--set-rule-overwrite <RULE_GUID> <TRUE|FALSE>>                           Set
overwrite status in rule
 -sRrci,--set-rule-restore-cluster-id <RULE_GUID> <RESTORE_CLUSTER_ID>>          Set
restore cluster id in rule
 -sRrn,--set-rule-restored-name <RULE_GUID> <VM_NAME>>                           Set
target VM name in rule
 -sRrp,--set-rule-restore-path <RULE_GUID> <PATH>>                               Set
restore path in rule
 -sRrsi,--set-rule-restore-storage-id <RULE_GUID> <RESTORE_STORAGE_ID>>          Set
restore storage id in rule
 -sRtp,--set-rule-target-project <RULE_GUID> <PROJECT_NAME>>                     Set
target project in rule
 -sRuag,--set-rule-use-auto-generated-name <RULE_GUID> <TRUE|FALSE>>             Set
rule use auto generated name
 -sRv,--set-rule-vms <RULE_GUID> <VM_GUIDS>>                                     Add
virtual machines to rule
```

Examples

- To create new policy:

```
[root@vprotect ~]# vprotect recplan -c "New Recovery Policy"

                GUID                            Name           Priority  Rules
------------------------------------  --------------------  --------  -----
d76bb990-817d-47ca-ba04-1dbdeffacf2a  New Recovery Policy  50        0
```

- To add new rule to selected policy:

```
[root@vprotect ~]# vprotect recplan -aR Rule1 d76bb990-817d-47ca-ba04-1dbdeffacf2a
Property      Value
------------  -----------------------------------

GUID          d76bb990-817d-47ca-ba04-1dbdeffacf2a
Name          New Recovery Policy
Priority      50
No. of rules  1
```

- To list policies:

```
[root@vprotect ~]# vprotect recplan -l

                GUID                         Name          Priority  Rules
------------------------------------  -------------------  --------  -----
d76bb990-817d-47ca-ba04-1dbdeffacf2a  New Recovery Policy  50        1
```

- To list rules assigned to policy:

```
[root@vprotect ~]# vprotect recplan -r d76bb990-817d-47ca-ba04-1dbdeffacf2a

                GUID                   Name   VMs  Hypervisor Type  Hypervisor Manager
Type  Hypervisor  Hypervisor Manager  Node  Backup Selection  Active  Restore Storage
Id  Restore Cluster Id  Target VM Name  Target Project  Restore Path  Overwrite  Base
Image  Data Center  Disk Allocation Format  Use auto generated name
------------------------------------  -----  ---  ---------------  ------------------
-----  ----------  ------------------  ----  ----------------  ------  --------------
----  ------------------  --------------  --------------  ------------  ---------  --
--------  -----------  ----------------------  ------------------------
6f0cc9ae-5842-4339-aee1-c8d21904317b  Rule1  []   -                -
-           -                   -     Last successful   true    null  null  null
null  null  true       -           -            -                        false
```

- To select the virtual machine you want to restore using a rule :

```
[root@vprotect ~]# vprotect vm -l      # To list virtual machines and their GUID's

[root@vprotect ~]# vprotect recplan -sRv 6f0cc9ae-5842-4339-aee1-c8d21904317b
f2354325-562e-465b-abc4-c4db51036b80

                GUID                         Name          Priority  Rules
------------------------------------  -------------------  --------  -----
d76bb990-817d-47ca-ba04-1dbdeffacf2a  New Recovery Policy  50        1
```

Integration

In this section, we're going to highlight key aspects necessary to integrate 3rd party solutions with Data Protector for Cloud Workloads. We assume a typical scenario, where you want to invoke Data Protector for Cloud Workloads operations on behalf of a user of a self-service portal. We assume that the end-user uses the above-mentioned portal for a subset of administrative actions, and we want to give a user ability to perform basic backup-related operations.

These include:

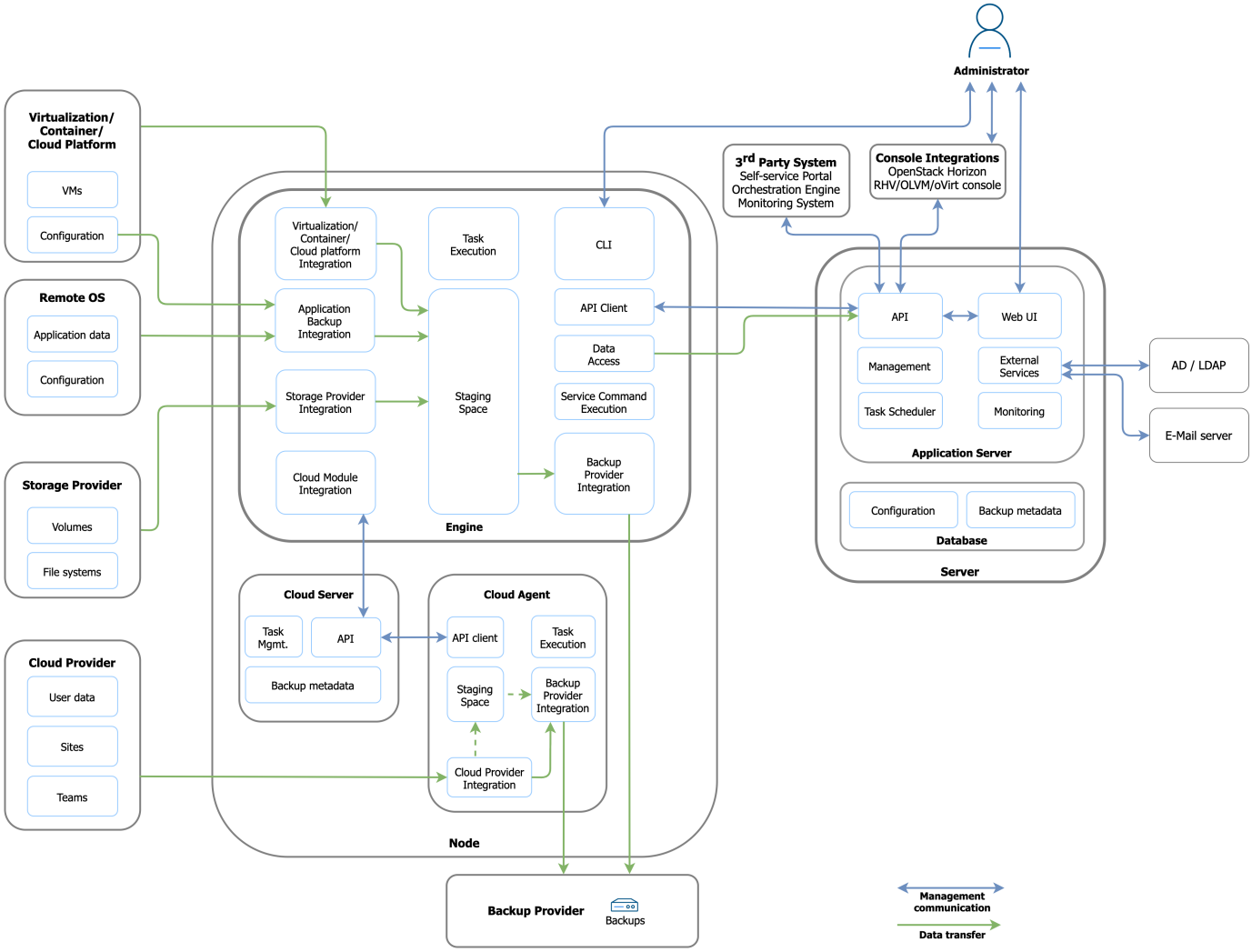
- listing VMs in inventory (including already non-existing)
- getting VM details
- performing backup of a VM on the list
- browse backup history
- restore specified VM
- monitor progress of each operation
- manage policies and schedules

Architecture

The architecture below shows key components, communication, and data flows. All communication between 3rd party systems goes via RESTful API exposed by Data Protector for Cloud Workloads Server. Tasks are being performed by the Node behind the scenes. End-user is going to use only a 3rd party system to invoke and monitor the status of the tasks.

Multi-tenancy and permission handling are on the 3rd-party system side. There is however `tenantID` field in several cases which can be used to assign objects to the tenant on the 3rd-party system side, later to be used in filter criteria.

A 3rd-party system must use a dedicated Data Protector for Cloud Workloads account to perform operations.



Integration steps

Setup

Your system is going to communicate over HTTPS which by default runs on port 8181, but during the setup can optionally be exposed on 443 as well. You need to generate an SSL certificate as described here.

Data Protector for Cloud Workloads can invoke operations only on VMs that exist in its inventory. It is being synced periodically so that it reflects changes in the virtualization platform.

REST API can either be invoked directly or using the generated client for Java. Please contact us to receive the current client version matching your language.

The base URL for API calls is: `https://<DP4CW_server_IP>:PORT/api`. We'll assume that all endpoints are prefixed with the base URL in the rest of this guide. In this guide we'll focus on the integration process, and skip actual requests and responses here and - please check API docs for details.

Quite often in requests or responses, Data Protector for Cloud Workloads requires `NameAndGuid` to refer to other objects. `GUID` is the ID that you can use later to get additional information about i.e. hypervisor or backup. For convenience, we provide `name` to present it on the list views.

When you need to provide `NameAndGuid` in requests, you actually need to pass the object that has just `GUID` provided.

A similar concept applies to enum types - Data Protector for Cloud Workloads uses `EnumNameAndDescription` with `name` as enum name and `description` to show it to the end-user in a more user-friendly way. Anywhere when you are

required to use enums such as type, state, days of the week, etc. you need to use `EnumNameAndDescription` object. In requests, you need to provide just `name`.

Login

When you want to invoke APIs, you need to be authenticated first. Data Protector for Cloud Workloads API exposes an endpoint that you need to send login and password first to the `POST /session/login` endpoint. Save cookies so that you'll be able to invoke the next calls.

If you ever call any end-point without having a valid session, you'll receive 401 Unauthorized responses. You need to re-login then and repeat your request.

In the rest of this guide, we assume that you have a valid session before you call any end-point mentioned.

Listing VMs in inventory (including already non-existing)

If you have a dedicated view of the VMs that are available for restore you need to call: `/virtual-machines`. This will retrieve all VMs visible by Data Protector for Cloud Workloads. `GUID` is the ID that you should refer to when invoking any operation on the VM. `UUID` is the ID that your infrastructure uses to identify objects.

For a multi-tenant environment make sure to filter out VMs on your side according to your ACLs or ownership of the VMs. For OpenStack Data Protector for Cloud Workloads records project ID and allow to use it to filter VMs like this: `/virtual-machines?tenantid={PROJECTID}`

Getting VM details

You may want to show VM details to the end-user. Call `GET /virtual-machines/{guid}`. Some useful information includes assigned policies, protection status or last backup sizes, and timestamps.

Performing backup of a VM on the list

The Backup consists of 2 phases in Data Protector for Cloud Workloads - export and store. End-user will initiate "backup", but your system should create an "export" task. Store task will be created automatically once export succeeds. To create an export task you need to provide the following information by the `POST /tasks/export` endpoint:

- `windowStart` and `windowEnd` - start and end of a time window for an export task - a task will fail if it is not started within this time range; both values provided as UNIX time in milliseconds
- `priority` - 0-100 - higher priority tasks are executed first; 50 by default
- `backupType` - `FULL` or `INCREMENTAL`; note that incremental backups are supported only for some platforms and they require at least one schedule of type incremental assigned to the policy that VM uses; if a snapshot for incremental backup is not found, a full backup will be done instead
- `backupDestination` - provided as `NameAndGuid` - target where the backup is going to be stored
- `protectedEntities` - collection of `NameAndGuid` referring to VMs that you want to backup - Data Protector for Cloud Workloads will create one export task for each referred VM

In the response, you'll receive task details, and you may want to record `GUID` to monitor later its progress or status. A new `backup` entry is going to be created automatically - you may also want to record this number if you want to present its details.

Progress monitoring of each operation

You can show the status and progress of each operation by calling `GET /tasks` (retrieves all tasks) and filtering the results or monitoring a particular task by calling `GET /tasks/{guid}`. There are also several useful query parameters that you can use to retrieve a filtered list:

- `protectedEntity` - GUID of VM that you refer to

- `backup` - GUID of a backup
- `schedule` - GUID of a schedule that invoked this task
- `state` - task state as `EnumNameAndDescription`: `QUEUED`, `RUNNING`, `FINISHED`, `FAILED`, `CANCELLED`
- `type` - task type as `EnumNameAndDescription`: `INDEX`, `EXPORT`, `STORE`, `RESTORE`, `OLD_BACKUPS_REMOVAL`, `OLD_SNAPSHOTS_REMOVAL`, `IMPORT`, `MOUNT`, `UNMOUNT`, `DELETE`, `SNAPSHOT`, `SNAPSHOT_REVERSION`
- `tenantId` - to filter out tasks only belonging to VMs owned by a particular tenantID (currently OpenStack only)

Browsing backup history

You can retrieve backup history including statuses, sizes, and time stats for each backup by calling `GET /backups/?protected-entity={guid}`, where you provide `guid` of your VM.

Restoring specified VM

Similar to backup, restore typically consists of several tasks. If you restore VM to the file system on the node, then it is just one task: `restore`. However, you usually want the user to restore and import VM automatically to the virtualization platform or mount it for file-level restore.

Let's focus on the restore with import case. You need to submit a task to `POST /tasks/restore-and-import` endpoint and provide:

- `backup` - GUID of a backup to be restored
- `hypervisor` or `hypervisorManager` - specify either one or the other - your target HV or HV manager depending on the virtualization platform
- `restoredPeName` - optional name of a restored VM
- `restoreStorageId` - some virtualization platforms require this to select the storage to which VM has to be restored;
- `restoreClusterId` - some virtualization platforms require this to select the cluster to which VM has to be restored;
- `restoreProject` - some virtualization platforms require this to select a project to which VM has to be restored
- `dataCenter` - some virtualization platforms require this to select datacenter to which VM has to be restored; this is a `DataCenterDTO` (currently having only `name` property)

Once the restore task completes, an import task will be created. Monitor tasks to show user current progress.

VM backup policy and schedule management

In order to allow users to have an automatic, scheduled backup you need to create a schedule and policy and make sure that both VMs and schedules are assigned to the policy. A Policy can have multiple schedules. VM can have exactly one backup policy assigned. Schedules are not assigned directly to the schedules - they are actually a part of a Policy Rule. And can be assigned to multiple rules, however in an external system this maybe not be convenient and we recommend using dedicated schedules for each policy. Currently, Data Protector for Cloud Workloads supports one rule per policy, but from API perspective - there is a collection of rules in the policy.

Schedules can be active or not, they have to specify which type of backup needs to be done, and when. Policies specify options to automatically assign VMs based on certain criteria. It is not recommended to expose these criteria to the end-user, as currently multi-tenancy support doesn't cover this case.

When you're exposing schedules and policies you may want to filter only these owned by a particular tenant. When you create/update them you need to provide additional `tenantId` to be able later to use it when listing objects.

Listing schedules

To list schedules and retrieve basic info use `GET /schedules` with optional query param `tenantid`.

Creating schedules

To create a **** schedule use `POST /schedules` endpoint and provide the following information:

- `name` - has to be globally unique, however, you can handle uniqueness on your site or generate names if you don't need to present them to end-user
- `backupType` - `EnumNameAndDescription` - a type of backup to perform: `FULL` or `INCREMENTAL`
- `type` - `EnumNameAndDescription` - for VM backup it is `VM_BACKUP` (other options are `APP_BACKUP` and `SNAPSHOT`); this type must match policy type
- `executionType` - `EnumNameAndDescription` - schedules can be executed at given `TIME` (based on `hour` field) or on `INTERVAL` basis
- `hour` - a time when schedule should be invoked - it is a time offset from UTC midnight in milliseconds, i.e. 3600 means 1:00 am UTC
- `active` - a boolean flag to activate or deactivate the schedule
- `startWindowLength` - used to assign window end to export tasks in milliseconds (which will be set to `hour` + `startWindowLength`)
- `daysOfWeek` - collection of `EnumNameAndDescription` - days of the week `MONDAY`, ..., `SUNDAY` when schedule needs to be run
- `months` - collection of `EnumNameAndDescription` - days of the week `JANUARY`, ..., `DECEMBER` when schedule needs to be run; if empty - only during specified months schedule is executed
- `dayOfWeekOccurrences` - collection of `EnumNameAndDescription` - days of the week occurrences `FIRST_IN_MONTH`, `SECOND_IN_MONTH`, `THIRD_IN_MONTH`, `FOURTH_IN_MONTH`, `LAST_IN_MONTH`, when schedule needs to be run; if empty - only during first, ..., the last occurrence of specified days of week schedule is executed
- `rules` - collection of `NameAndGuid` - policy rules to which assign schedule to
- `interval` - object containing `startHour`, `endHour` (time offset from UTC midnight in milliseconds) and `frequency` (also in milliseconds)
- `tenantId` - string identifying tenant to which assign the schedule - this is used only by 3rd party system to filter out the listing

Getting schedule details

To get schedule details use `GET /schedules/{guid}`.

Updating schedule

To update the schedule use `PUT /schedules/{guid}` endpoint and provide the same information as in the creation request.

Deleting schedule

To delete the schedule use `DELETE /schedules/{guid}`.

Listing VM backup policies

To list policies and retrieve basic info use `GET /policies/vm-backup` with optional query param `tenantid`.

Creating VM backup policy

Policy creation is a 2 step process. It requires creating policy itself and then setting rules set on the policy. This ruleset currently must be a 1 element set.

To create a schedule use `POST /policies/vm-backup` endpoint and provide the following information:

- `name` - has to be globally unique, however, you can handle uniqueness on your site or generate names if you don't need to present them to end-user* `priority` - priority assigned to backup tasks (0-100)
- `autoRemoveNonPresent` - a boolean flag to automatically remove from policy non-existing VMs

- `autoAssignSettings` - object specifying details for VM auto-assignment mechanism - not supported in the multi-tenant environment; you need to set `mode` variable of this object to `DISABLED`
- `vms` - collection of `NameAndGuid` containing GUIDs of VMs to be assigned to the policy
- `tenantId` - string identifying tenant to which assign the policy - this is used only by 3rd party system to filter out the listing

You'll receive details including GUID of a newly created policy. The second step is to create a rule and assign it to the policy. Use `POST /rules/vm-backup` with the following information:

- `name` - we recommend generating it if not used by the user
- `schedules` - collection of `NameAndGuid` you want to be assigned to this policy
- `policy` - `NameAndGuid` of a policy that you want this rule to be assigned to.

Getting VM backup policy details

To get policy details use `GET /policies/vm-backup/{guid}`.

Updating VM backup policy

To update policy use `PUT /policies/vm-backup/{guid}` endpoint and provide the same information as in the creation request. Keep in mind, that you may need to update rules as well. You can either use `DELETE /rules/vm-backup/{guid}` and later `POST /rules/vm-backup` and re-create the policy rule or use `PUT /rules/vm-backup/{guid}` to update specific settings of a specific rule. GUID of a rule can be found in policy details (`rules` field).

Deleting VM backup policy

To delete policy use `DELETE /policies/vm-backup/{guid}`. Policy rules will be removed automatically.

Integration Plugins

Data Protector for Cloud Workloads can also be managed by using external plugins. Currently, there are several available, most of which support a subset of the available options of Data Protector for Cloud Workloads, with more and more functionalities being added with each release. Data Protector for Cloud Workloads currently provides integration for the UI

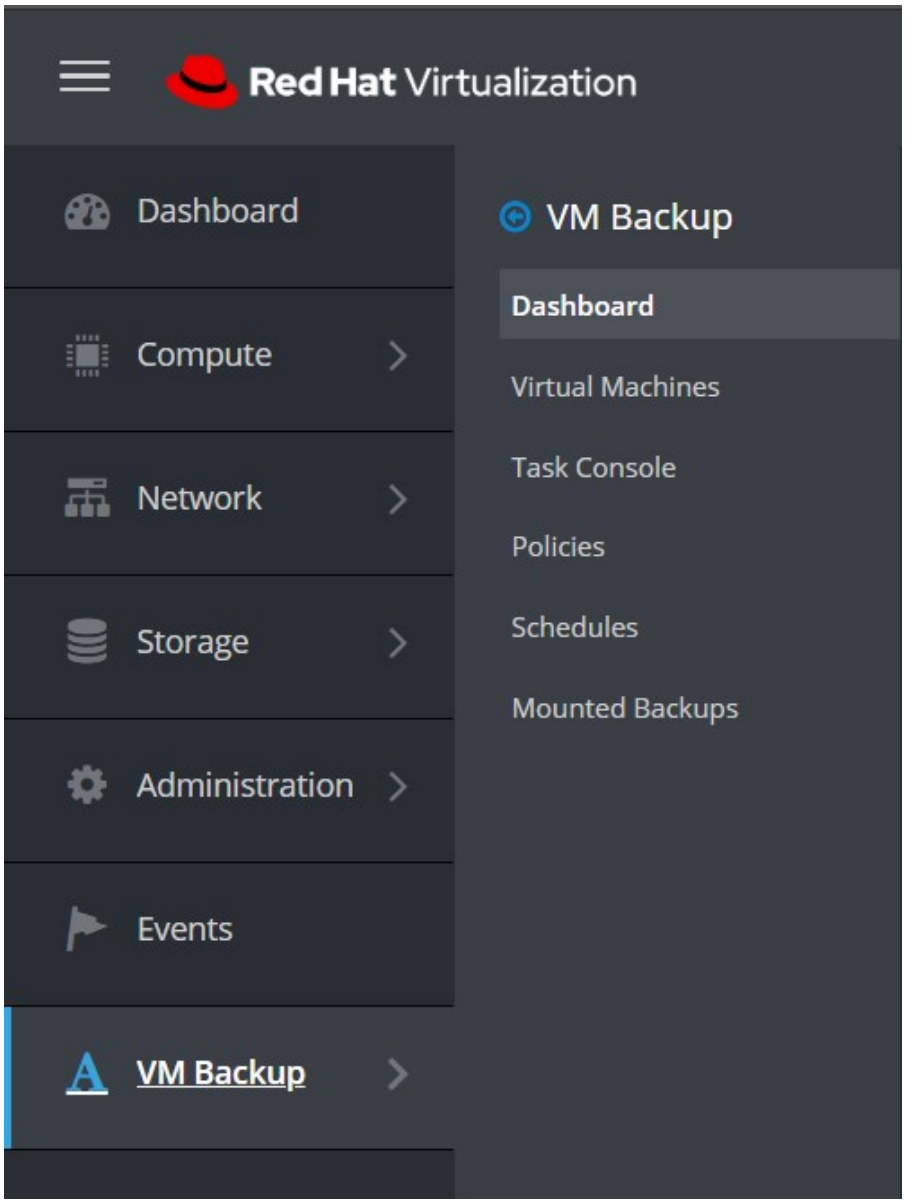
- Red Hat Virtualization
- oVirt
- Oracle Linux Virtualization Manager
- OpenStack Horizon

Red Hat Virtualization UI Plugin

General

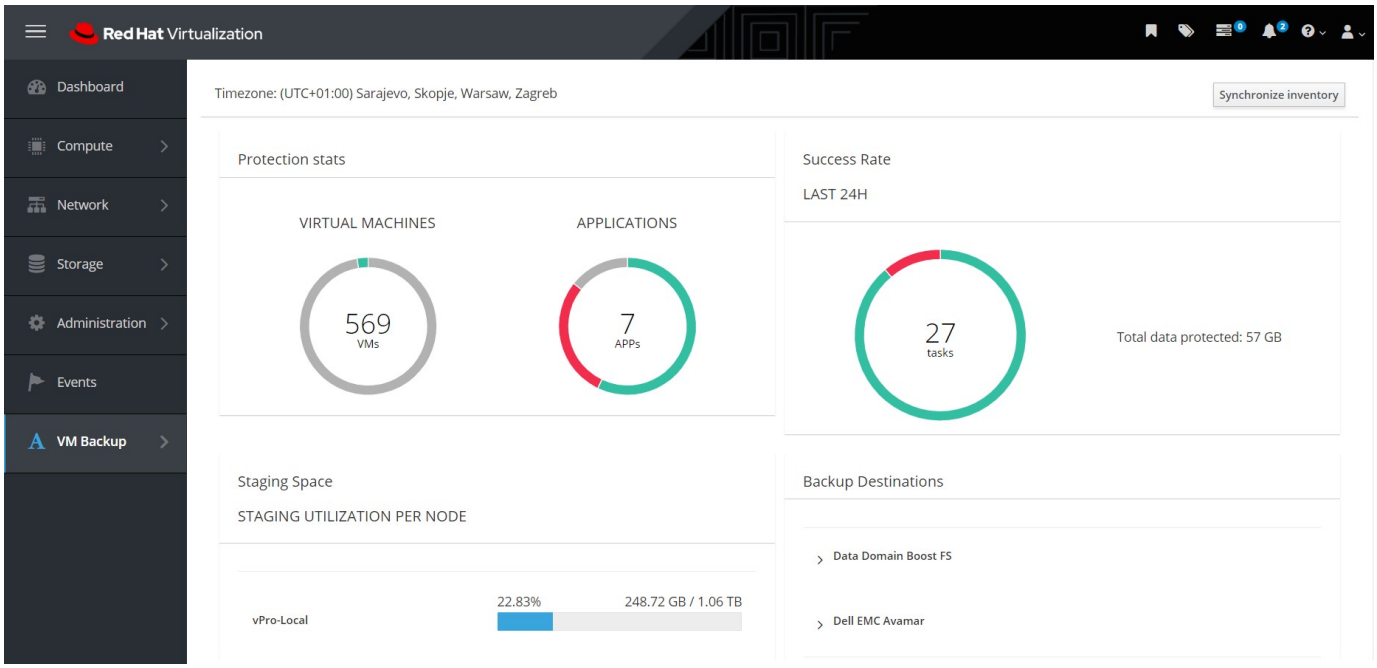
Integration with the Red Hat Virtualization interface allows administrators to perform most of the basic operations without logging into the Data Protector for Cloud Workloads dashboard.

After installation (which is described at the end of this article) you will see a new tab "VM Backups" in the RHV menu.

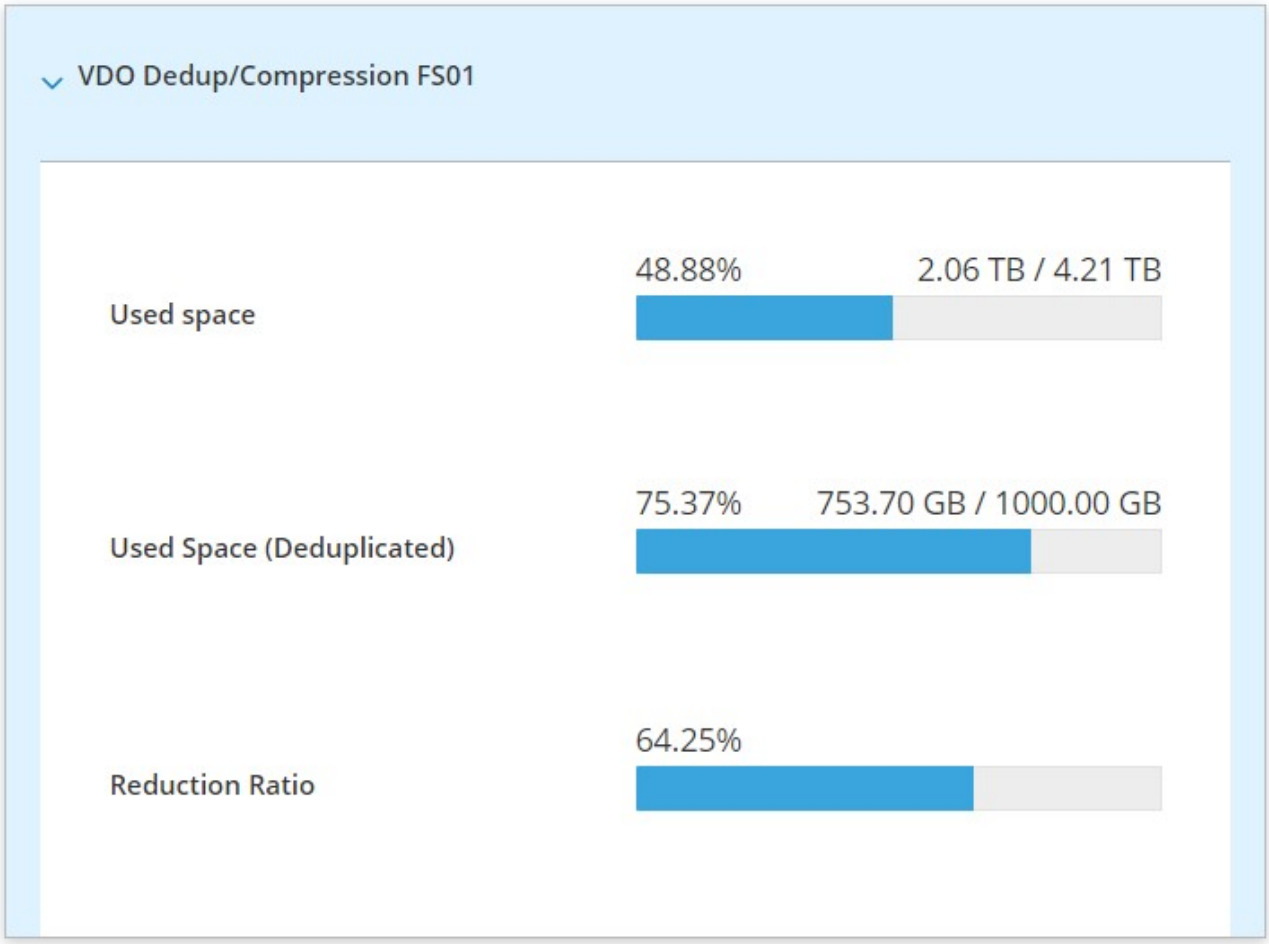


Dashboard

As usual, it contains a short summary of the environment along with a handful of statistics.

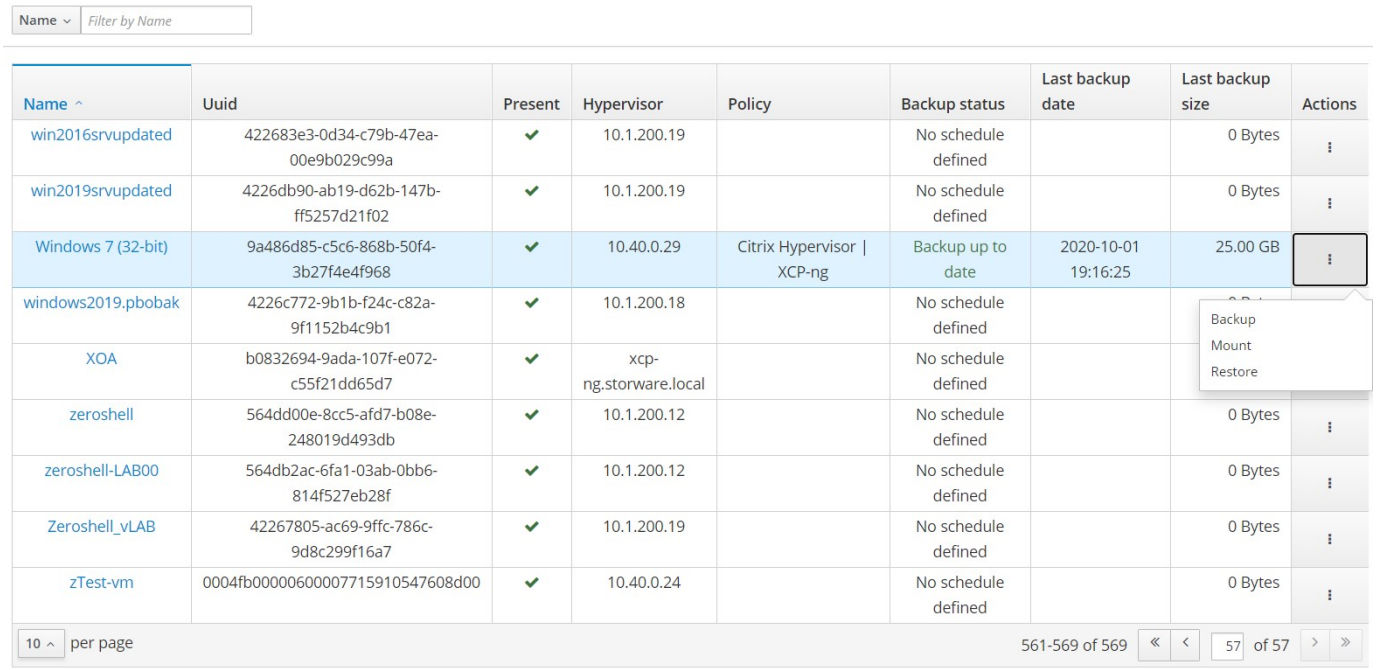


You can also see the data summary of the backup destination.

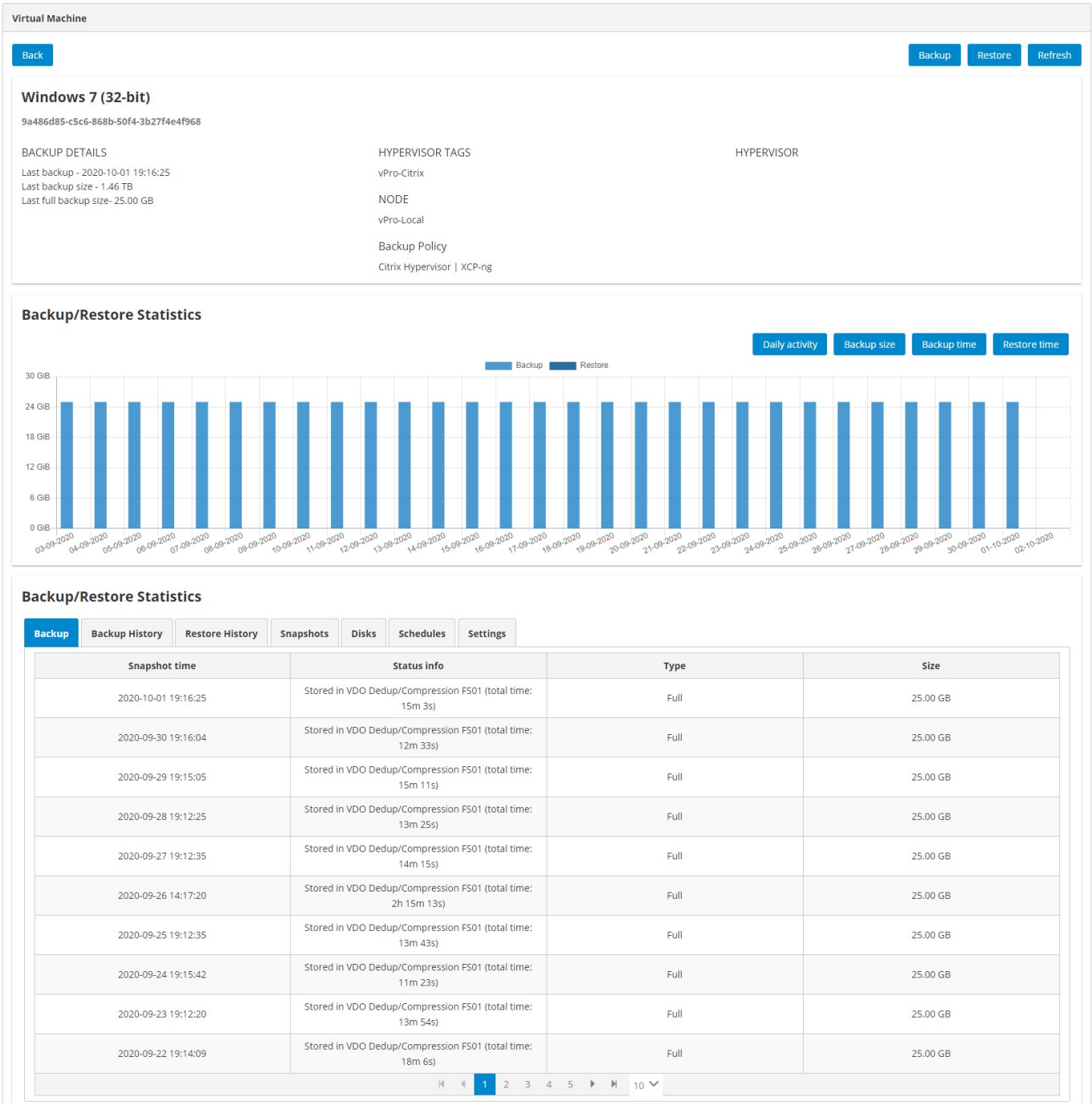


Virtual Machines

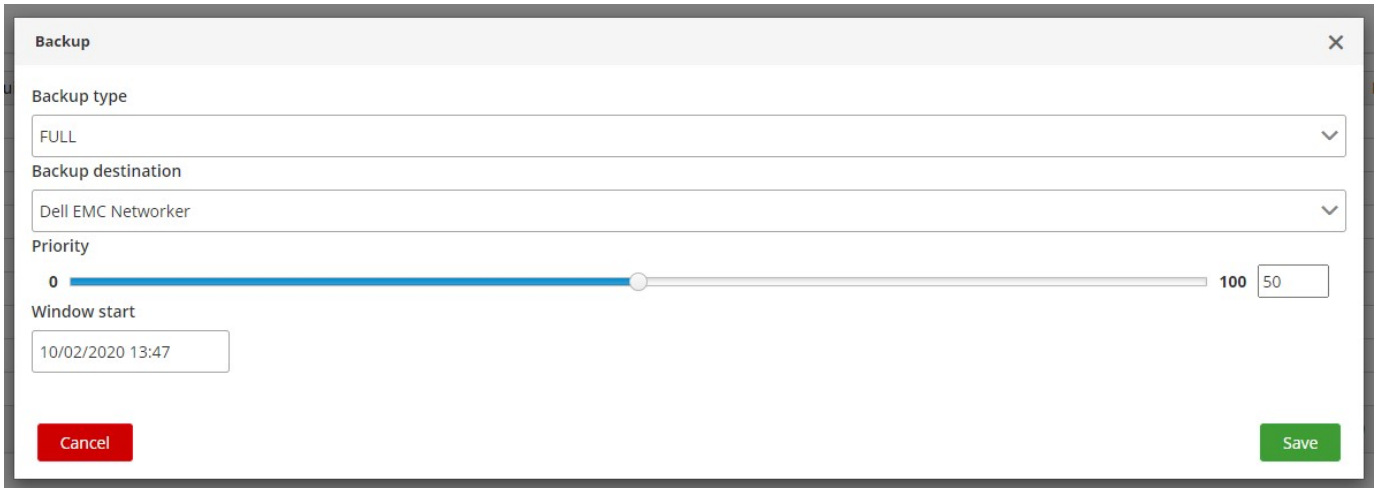
This tab shows all inventoried virtual machines in your RHV environment. In addition, you can also perform a basic backup or restore operations.



But that's not all, you can also go into the details of the virtual machine by clicking on its name:

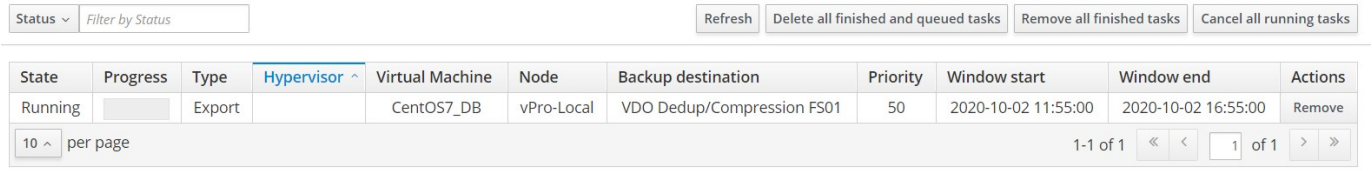


Backup window view:



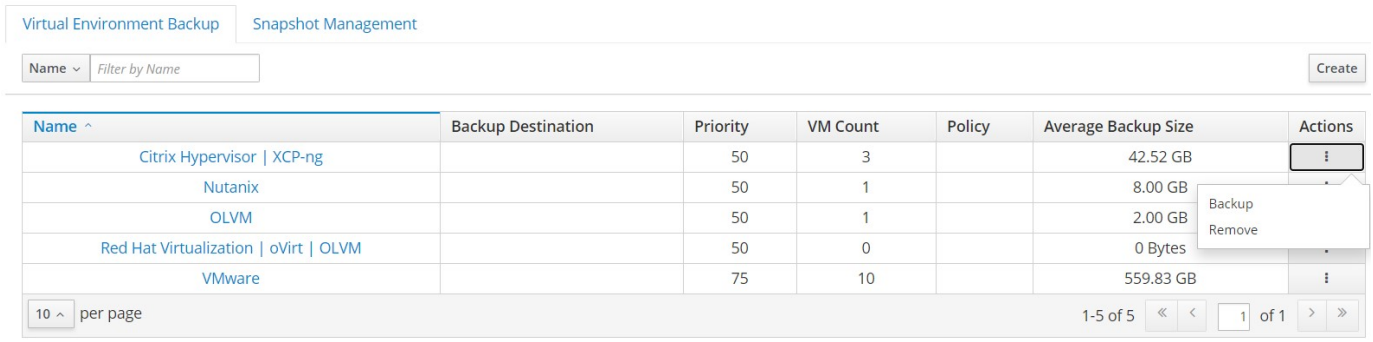
Task console

Basic information about current tasks performed by Data Protector for Cloud Workloads.



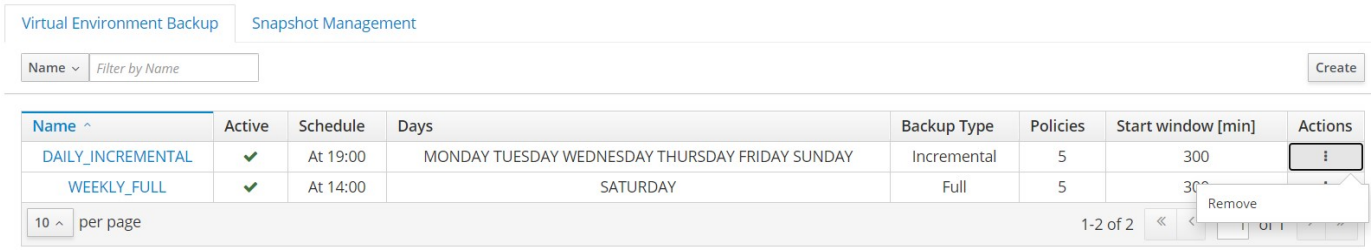
Policies

Allows you to create policies for VM's backups and snapshots. These basically have the same functionalities as Data Protector for Cloud Workloads WebUI.



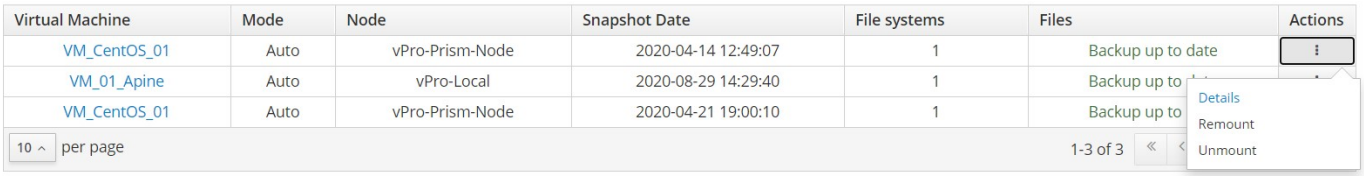
Schedules

As with the policies tab, it allows you to create schedules for the created rules.

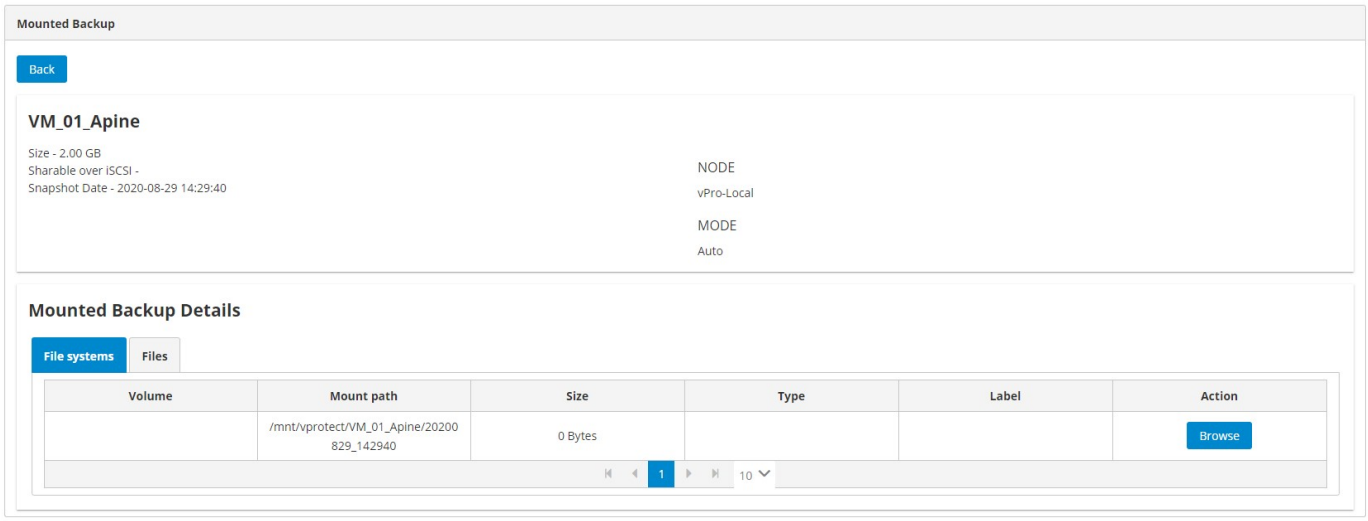


Mounted Backups

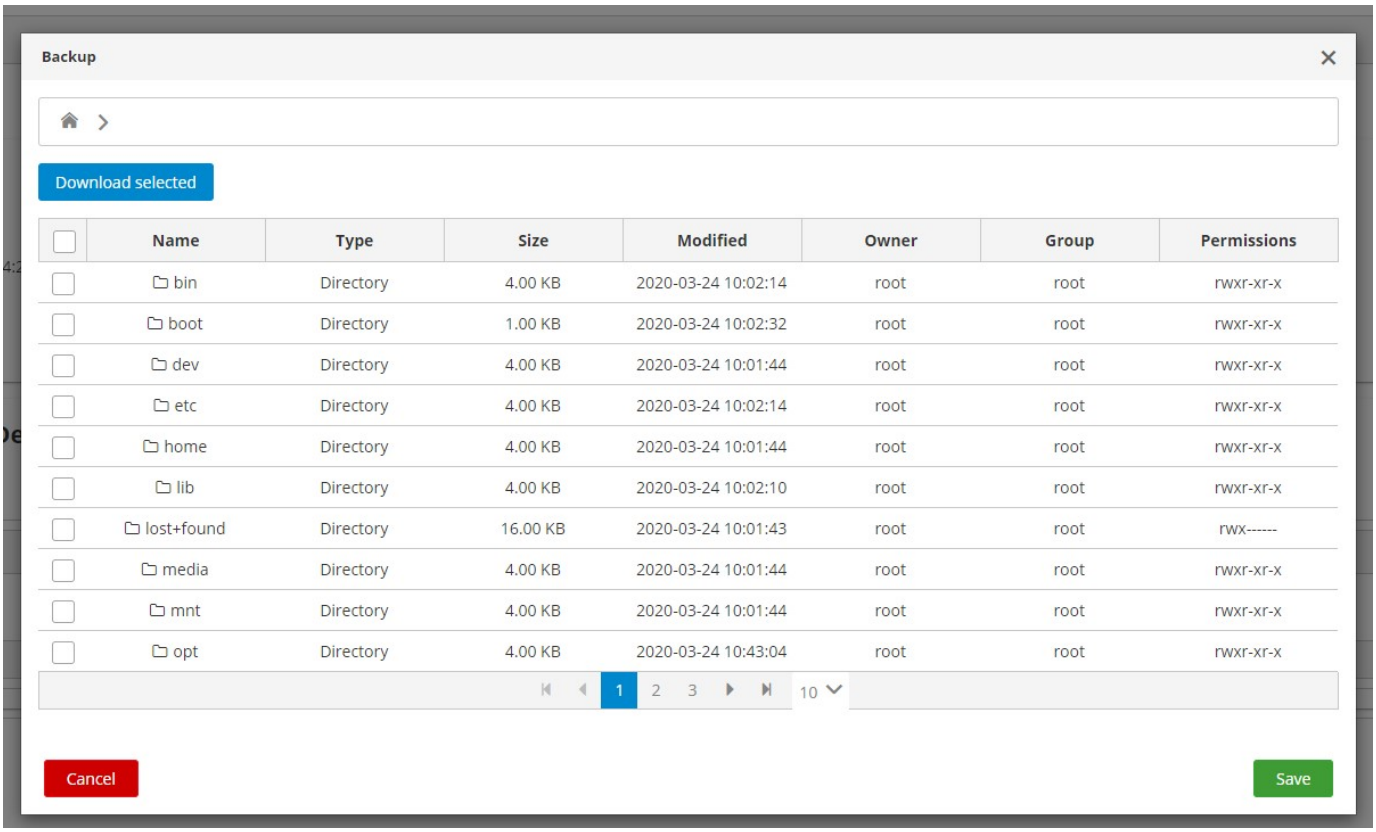
Finally, you can also browse your mounted backups from the RHV dashboard. You only need to enter the backup details using the menu on the right.



From here we can see the basic information about the backup and start browsing the files using the "Browse" button on the right.



Just select a folder or file and then click on the "download selected" button to have the files on your computer.



Installation

1. You can find the add-on in the GitHub repository. Follow the instructions in the README to build or the download plugin. Then extract the provided archive to your RHV manager.
2. In the file `vprotect.json` edit the lines in the config part:
    - `vProtectURL` - the URL to Data Protector for Cloud Workloads API
    - `username` - the name of the administrator in Data Protector for Cloud Workloads
    - `password` - the administrator password in Data Protector for Cloud Workloads

Example:

```
{
   "name": "vprotect",
   "url": "plugin/vprotect/plugin.html",
```

```
    "resourcePath": "vprotect-resources",
    "lazyLoad": false,

    "config": {
        "vProtectURL": "http://10.40.0.55:8080/api",
        "username": "admin",
        "password": "vPr0tect"
     }
  }
```

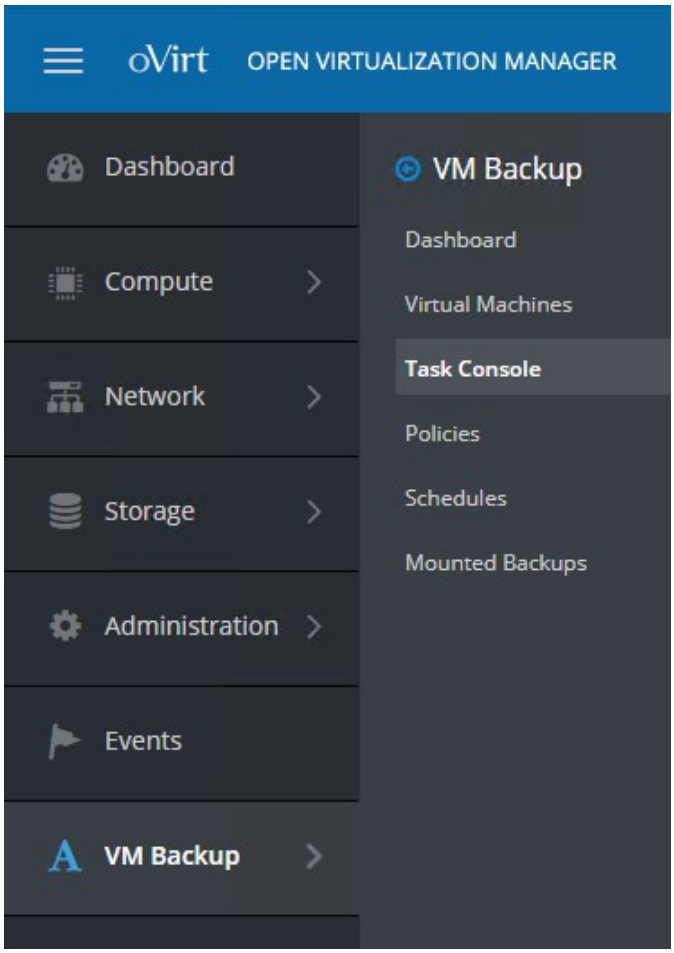
1. Put the `vprotect.json` file and `vprotect-resources` directory in the `/usr/share/ovirt-engine/ui-plugins` directory in the RHV engine.

oVirt UI Plugin

General

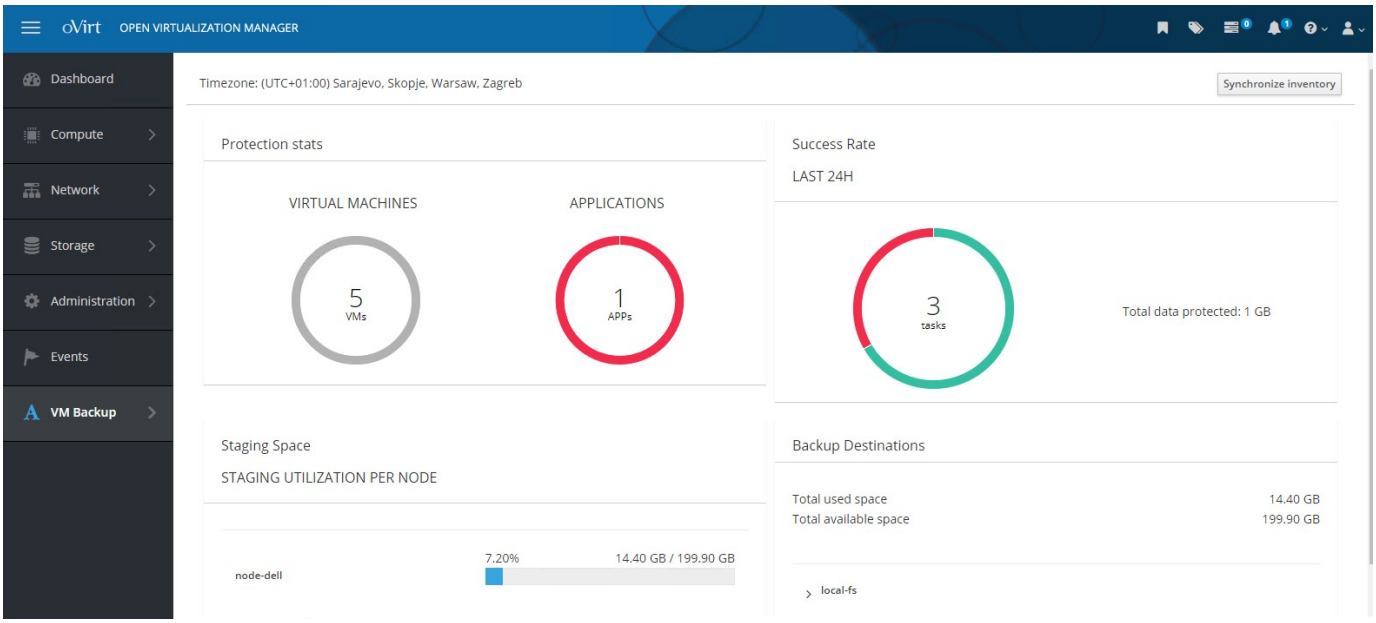
Integration with the oVirt Virtualization interface allows administrators to perform most of the basic operations without logging into the Data Protector for Cloud Workloads dashboard.

After installation (which is described at the end of this article) you will see a new tab "VM Backups" in the oVirt menu.

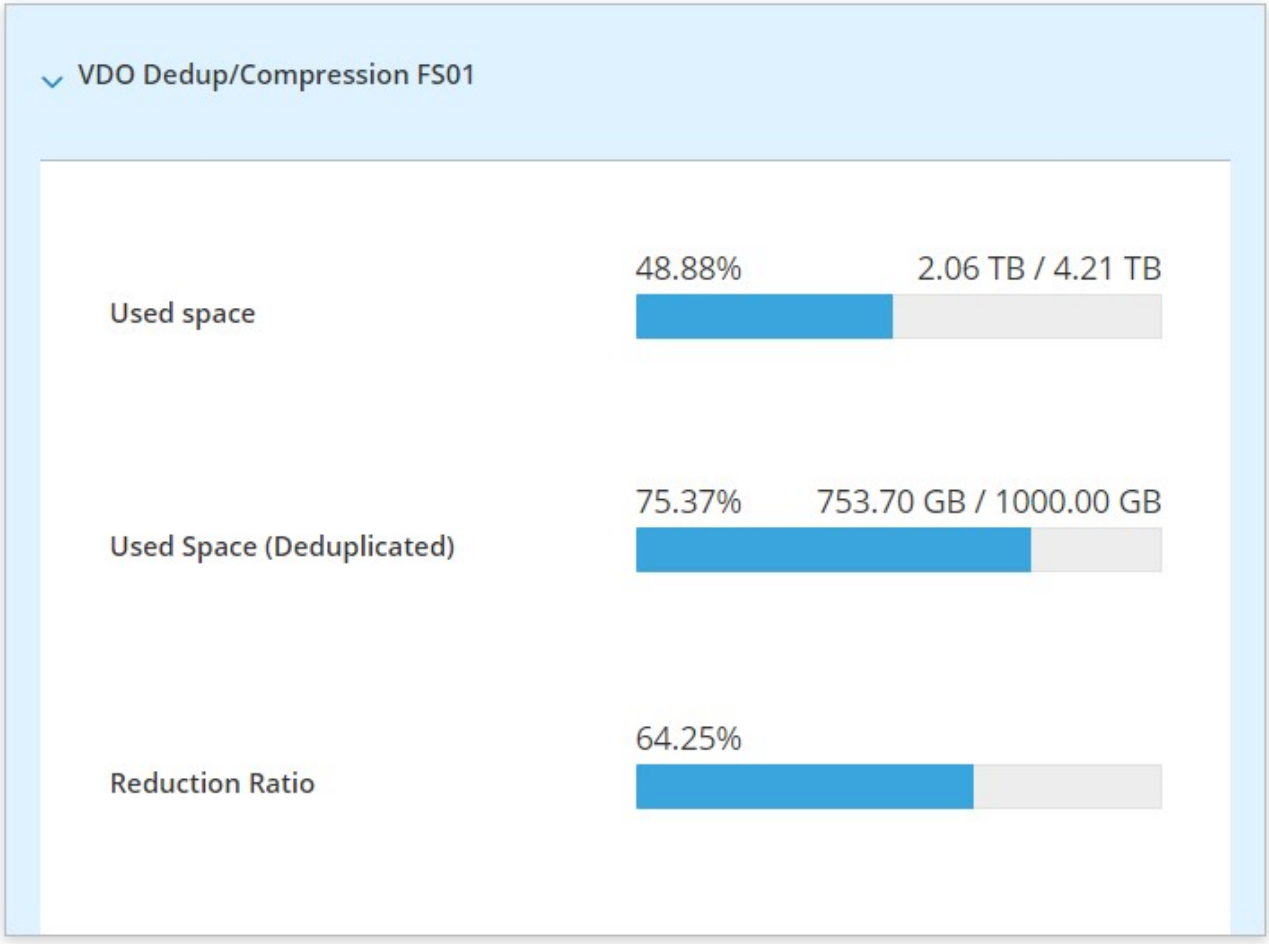


Dashboard

As usual, it contains a short summary of the environment along with a handful of statistics.

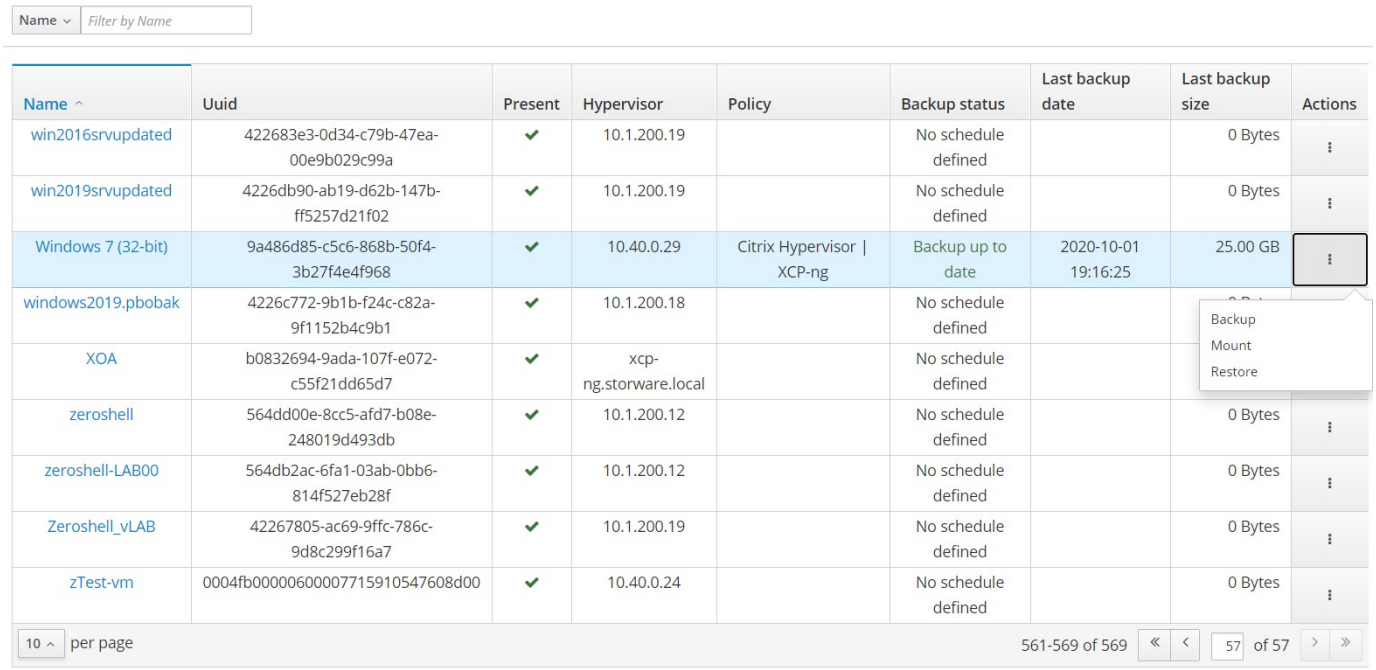


You can also see the data summary of the backup destination.

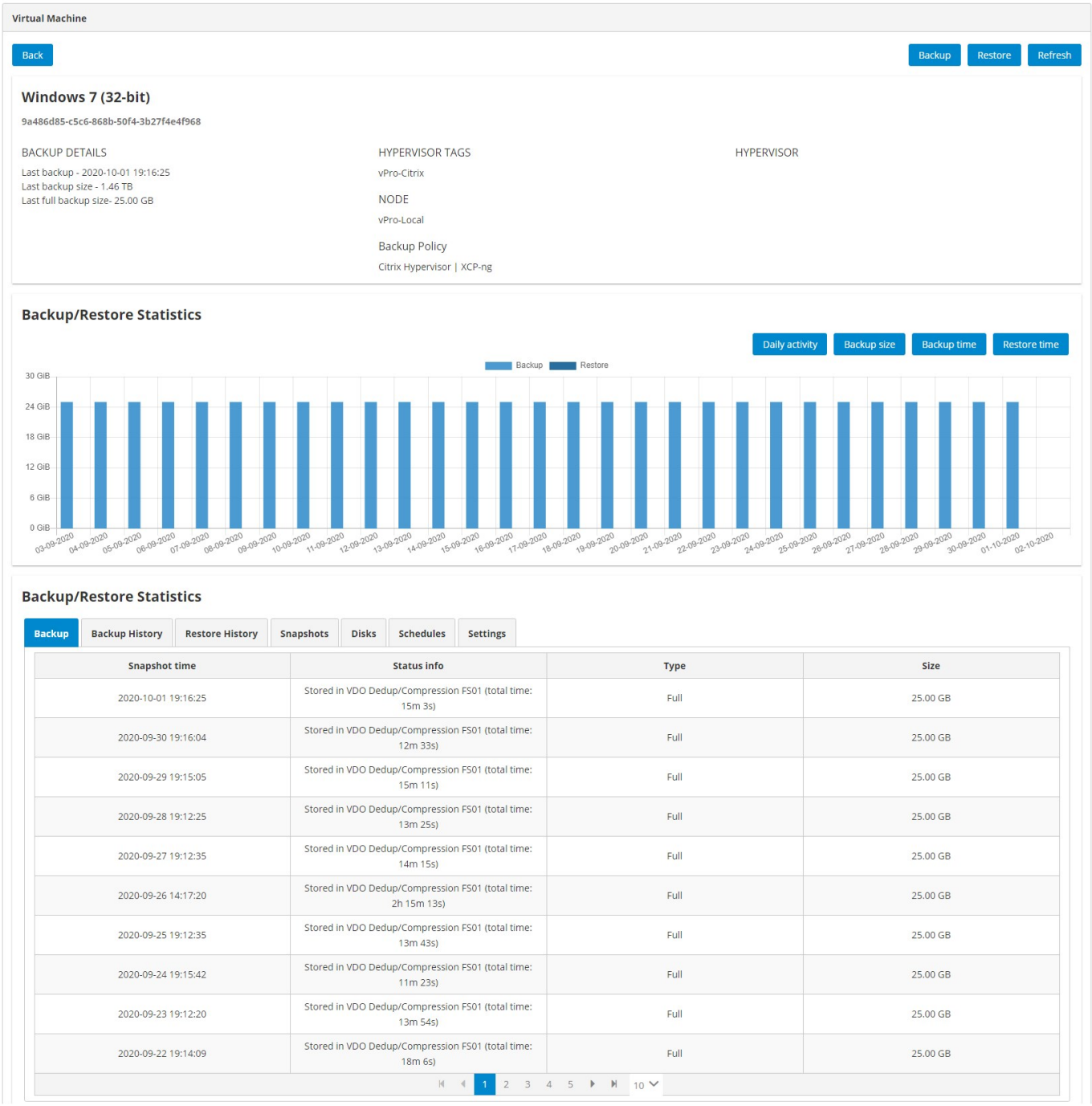


Virtual Machines

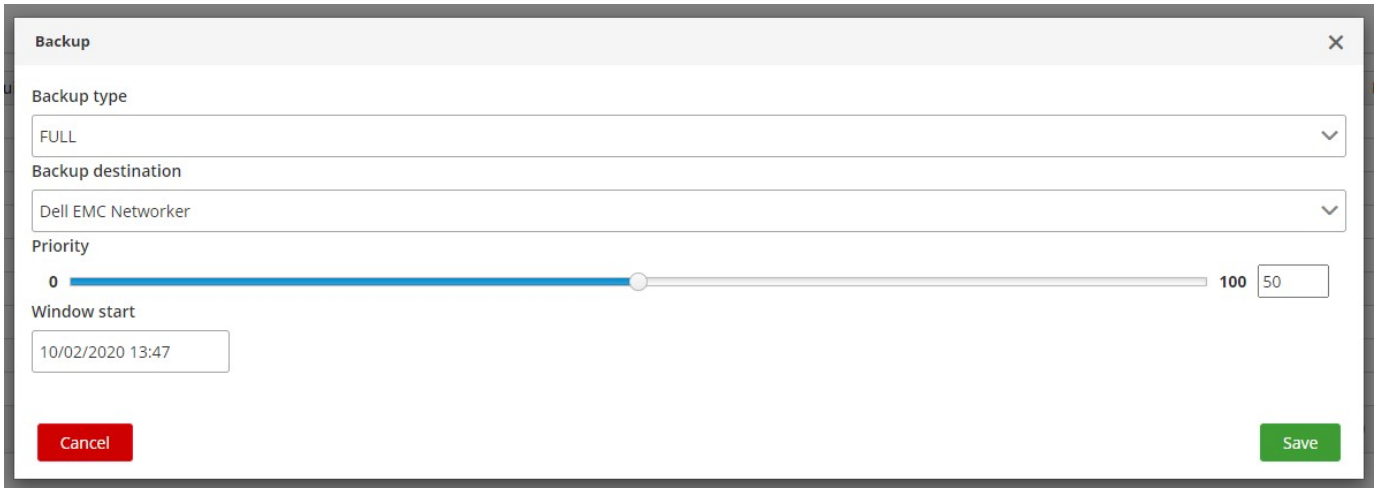
This tab shows all inventoried virtual machines in your oVirt environment. Besides, you can also perform a basic backup or restore operations.



But that's not all, you can also go into the details of the virtual machine by clicking on its name:

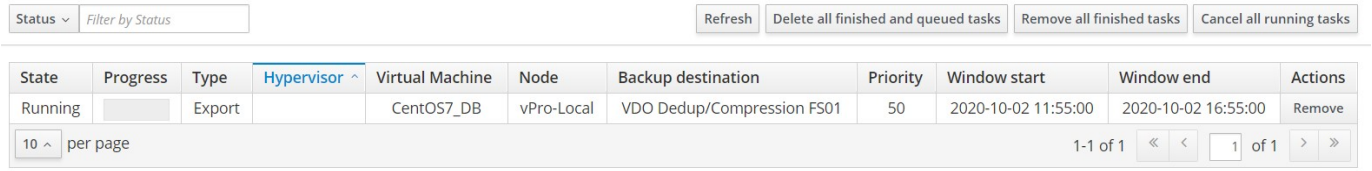


Backup window view:



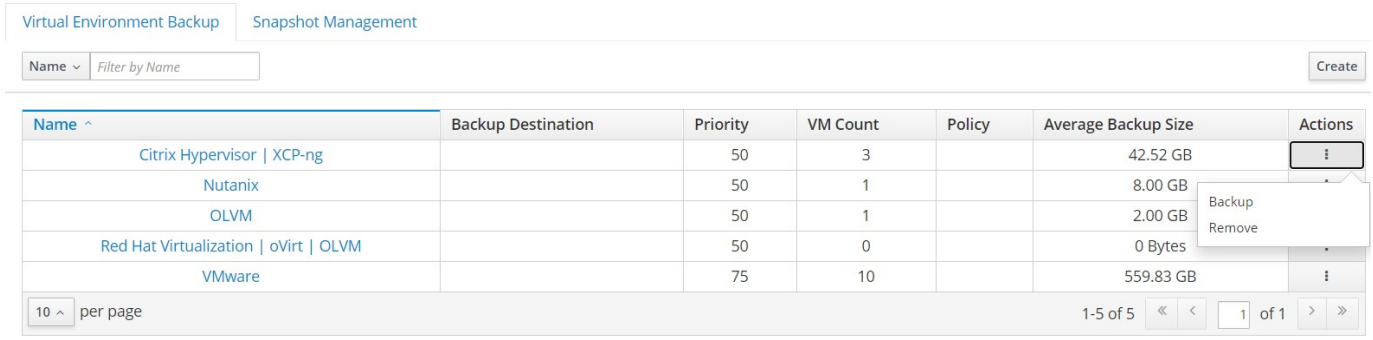
Task console

Basic information about current tasks performed by Data Protector for Cloud Workloads.



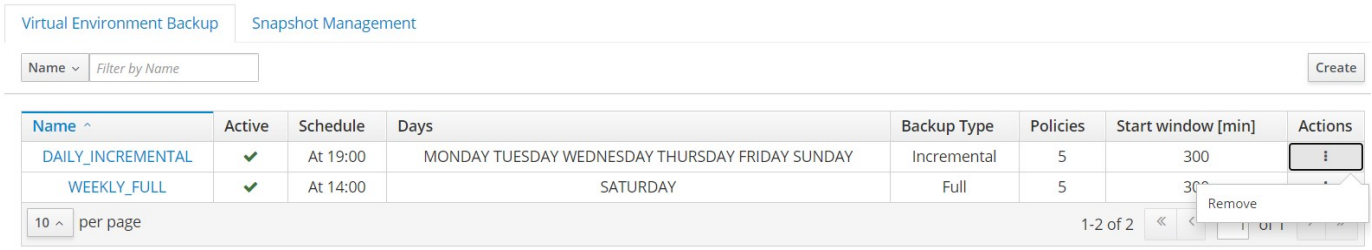
Policies

Allows you to create policies for VM's backups and snapshots. It basically has the same functionalities as Data Protector for Cloud Workloads WebUI.



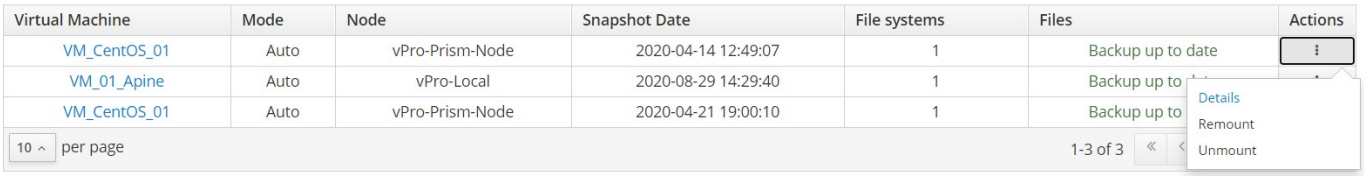
Schedules

As with the policies tab, it allows you to create schedules for the created rules.

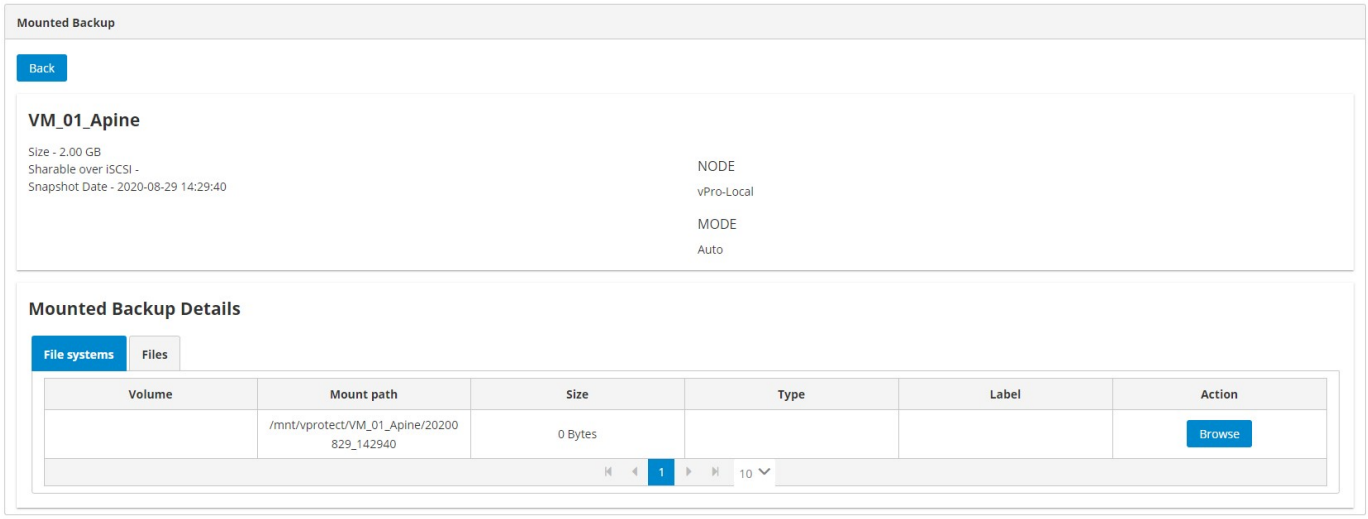


Mounted Backups

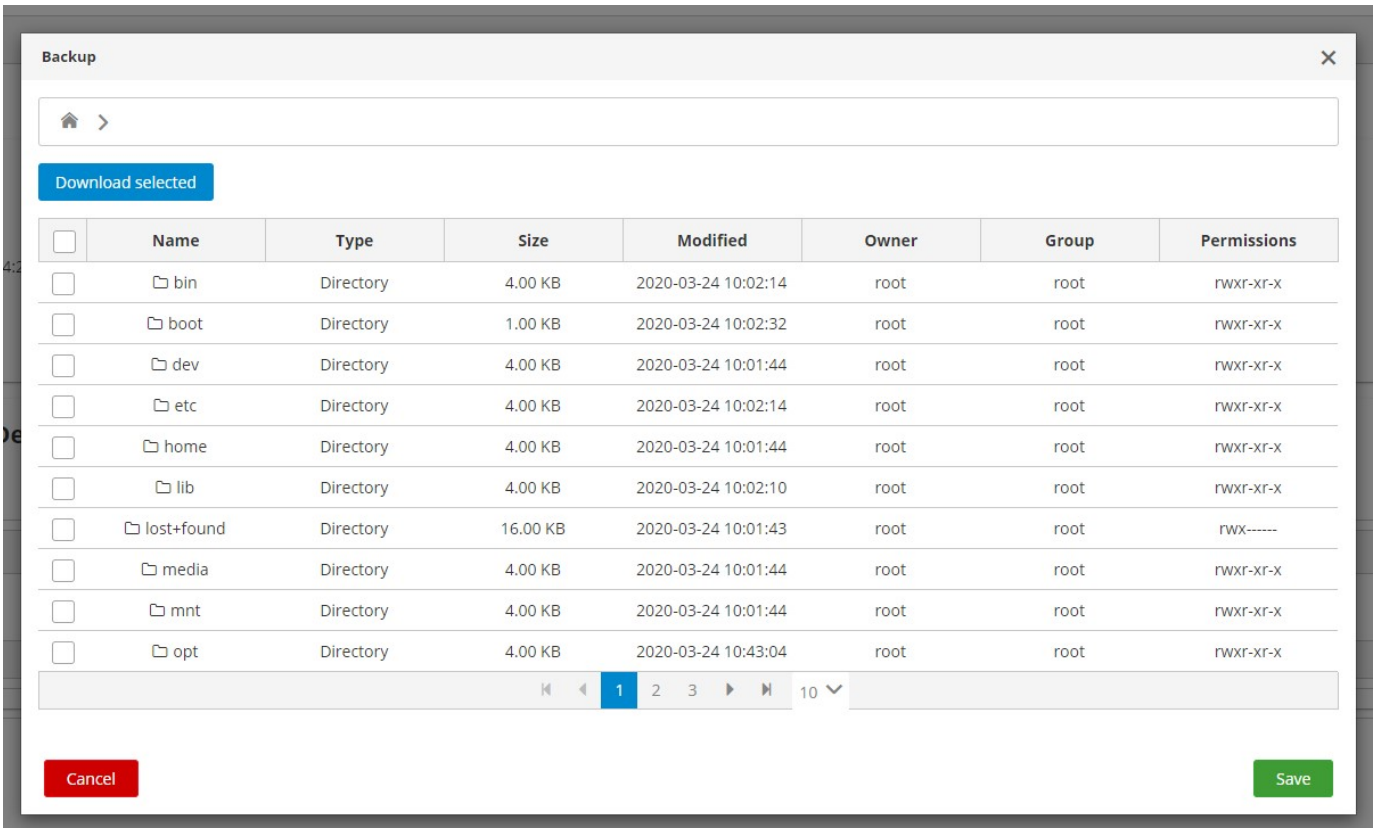
Finally, you can also browse your mounted backups from the oVirt dashboard. You only need to enter the backup details using the menu on the right.



From here we can see the basic information about the backup and start browsing the files using the "Browse" button on the right.



Just select a folder or file and then press the "download selected" button to have the files on your computer.



Installation

1. You can find the add-on in the GitHub repository. Follow the instructions in the README to build or download the plugin. Then extract the provided archive onto your oVirt manager.
2. In the file `vprotect.json` edit these lines in the config part:
    - `vProtectURL` - the URL to Data Protector for Cloud Workloads API
    - `username` - the name of admin in Data Protector for Cloud Workloads
    - `password` - the admin password in Data Protector for Cloud Workloads

Example:

```
    {
       "name": "vprotect",
       "url": "plugin/vprotect/plugin.html",
```

```
    "resourcePath": "vprotect-resources",
    "lazyLoad": false,

    "config": {
        "vProtectURL": "http://10.40.0.55:8080/api",
        "username": "admin",
        "password": "vPr0tect"
     }
  }
```

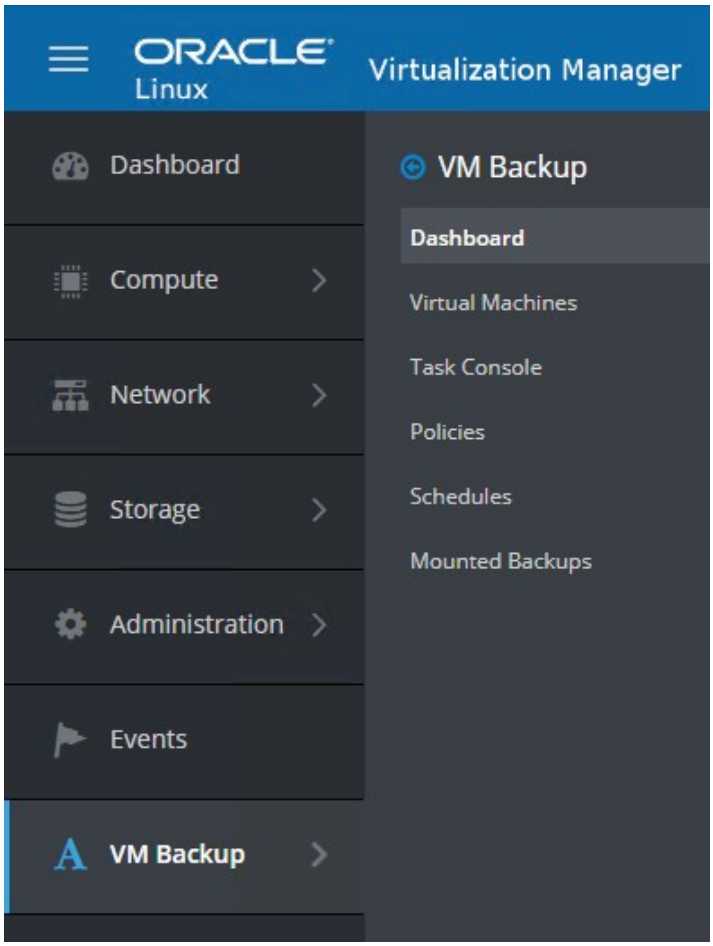
1. Put the `vprotect.json` file and `vprotect-resources` directory in the `/usr/share/ovirt-engine/ui-plugins` directory in the oVirt Engine.

Oracle Linux Virtualization Manager UI Plugin

General

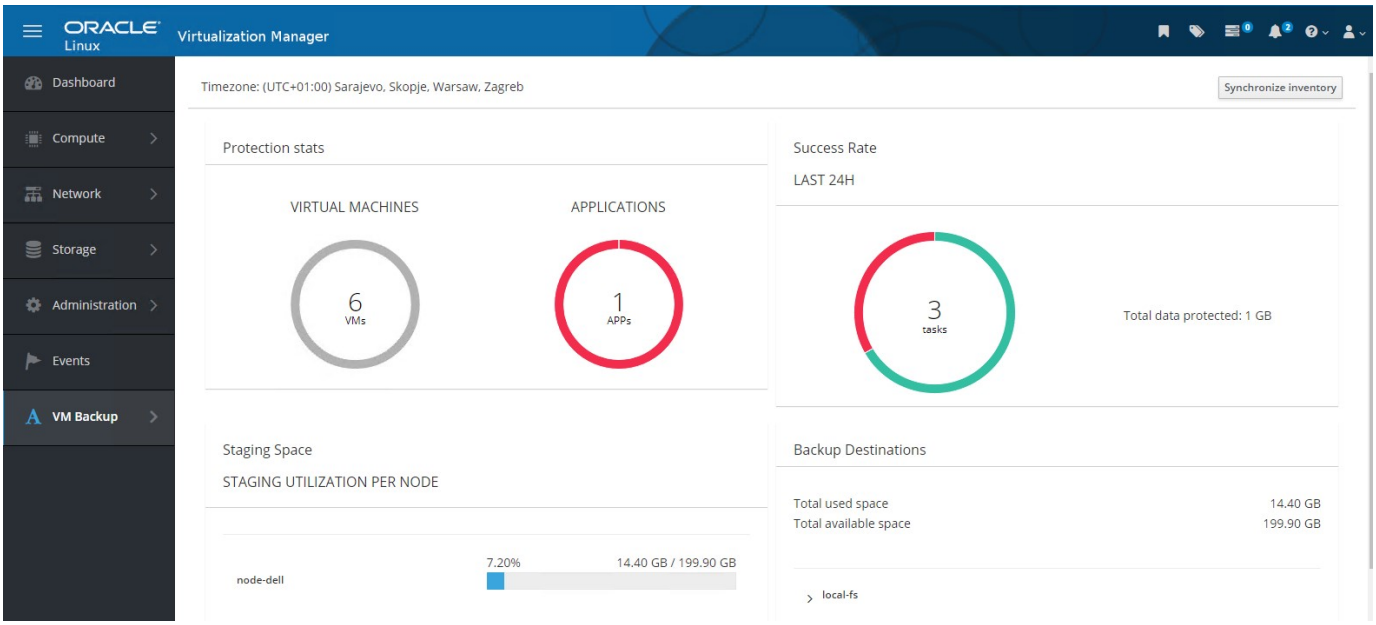
Integration with the OLVM Virtualization interface allows administrators to perform most of the basic operations without logging into the Data Protector for Cloud Workloads dashboard.

After installation (which is described at the end of this article) you will see a new tab "VM Backups" in the OLVM menu.

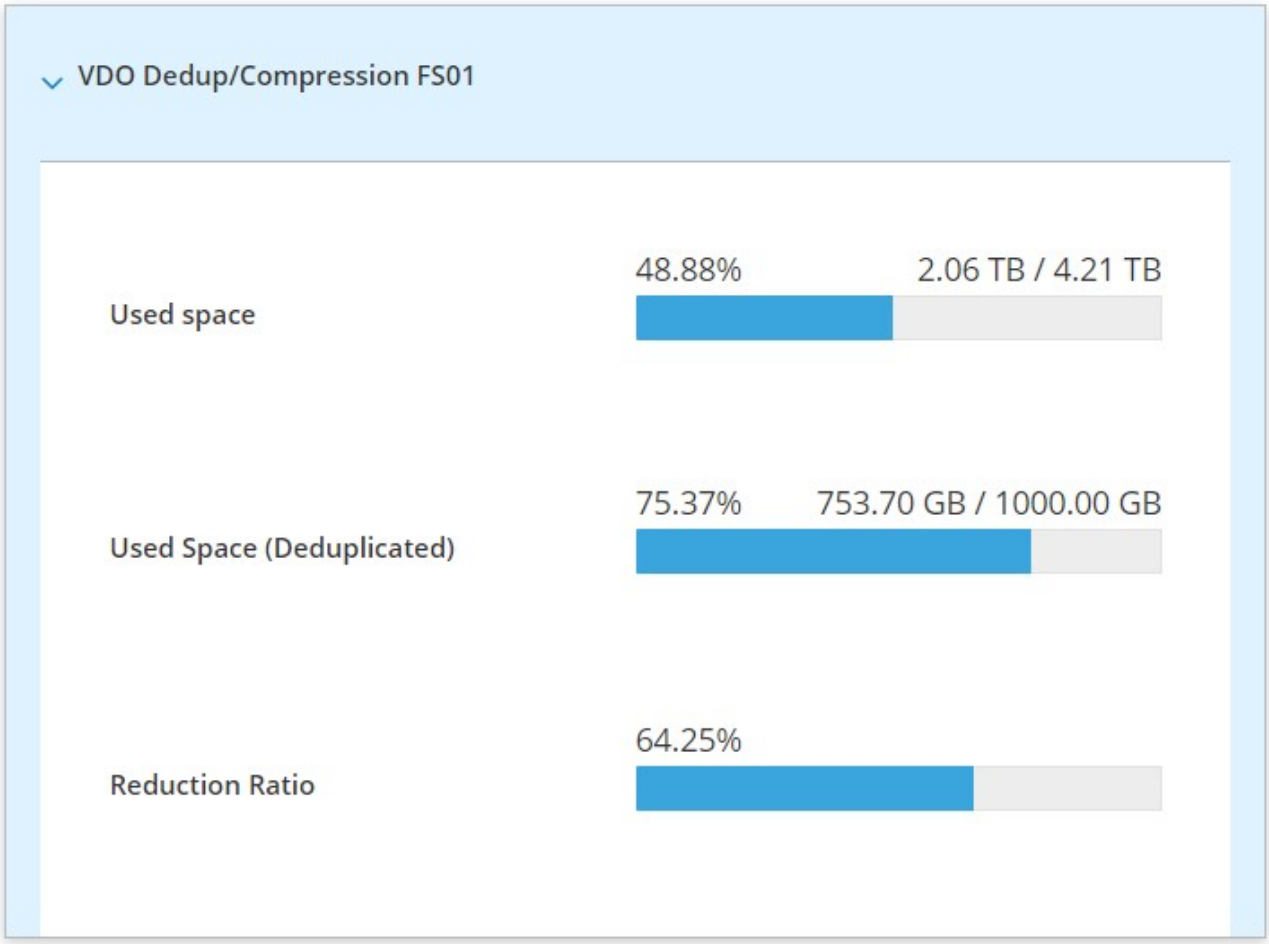


Dashboard

As usual, it contains a short summary of the environment along with a handful of statistics.

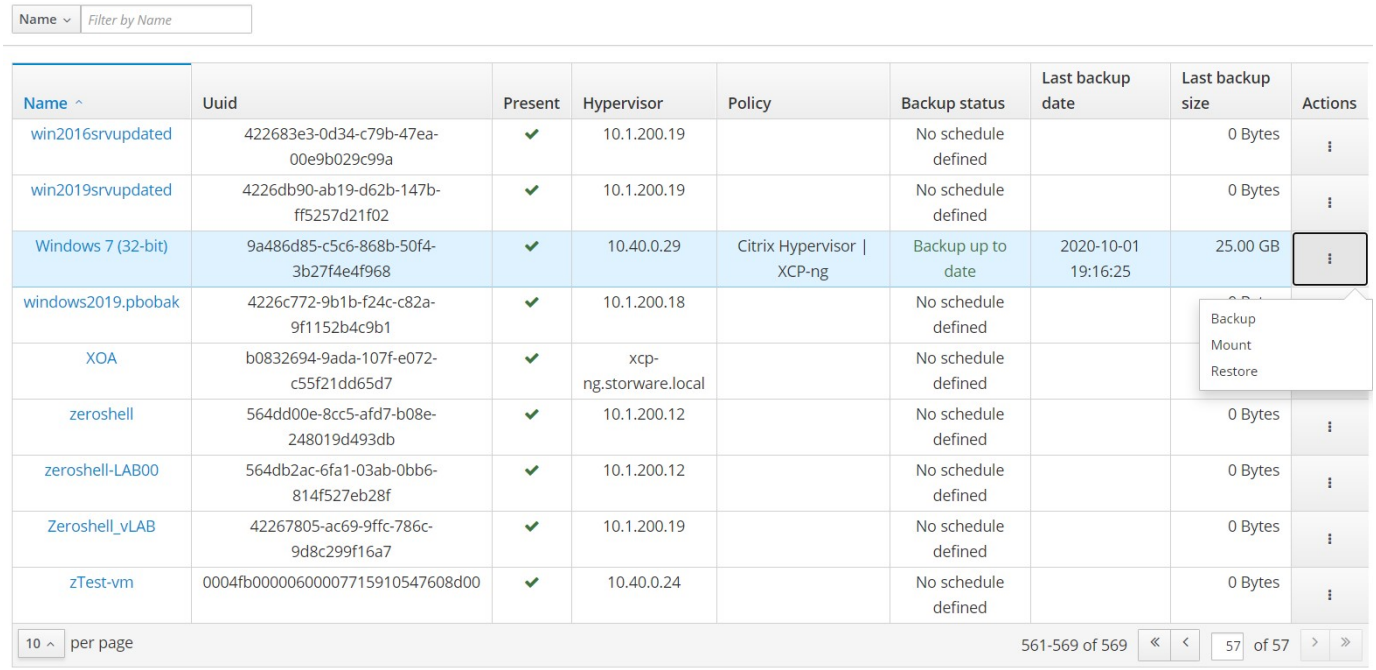


You can also see the data summary of the backup destination.

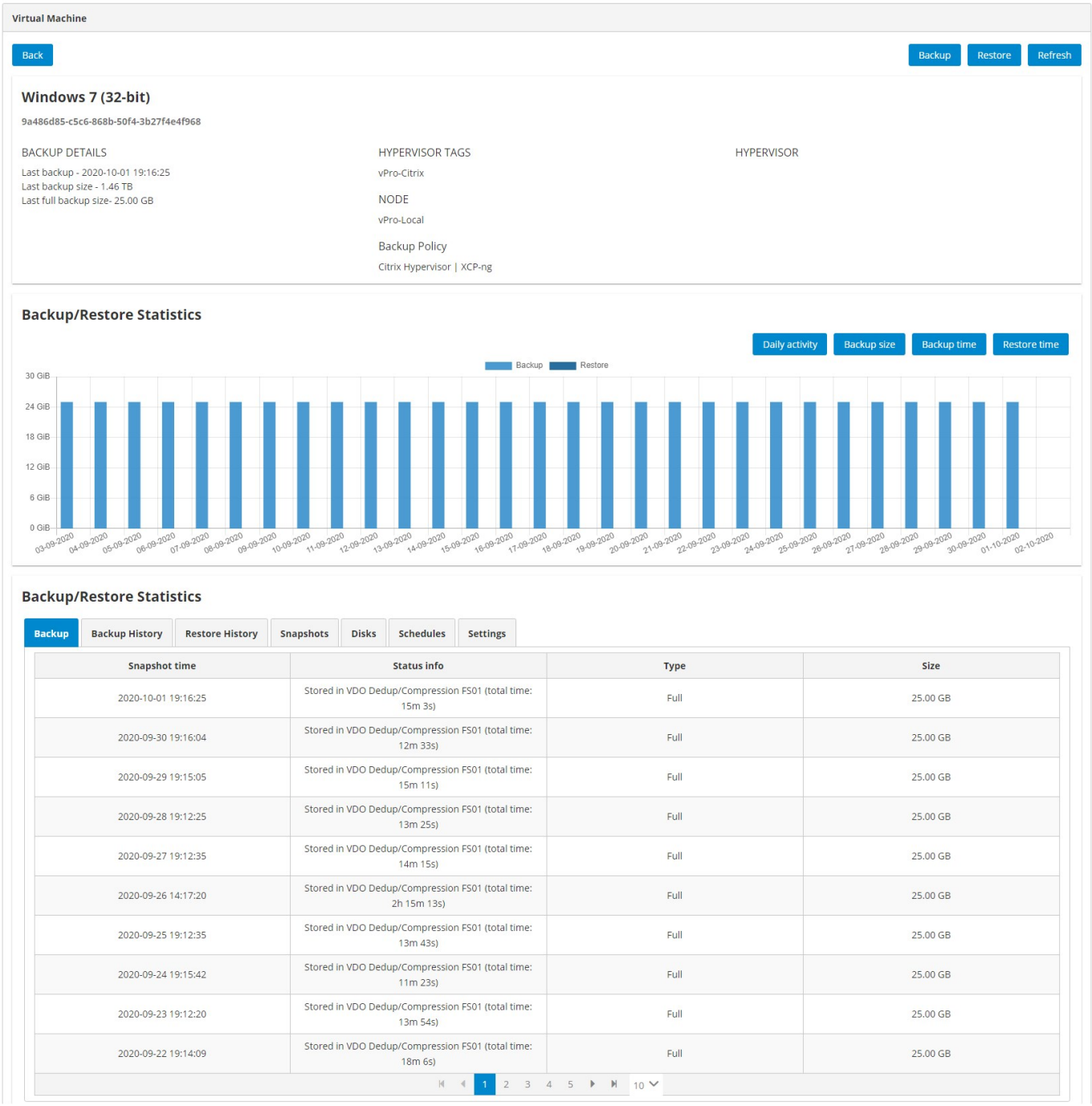


Virtual Machines

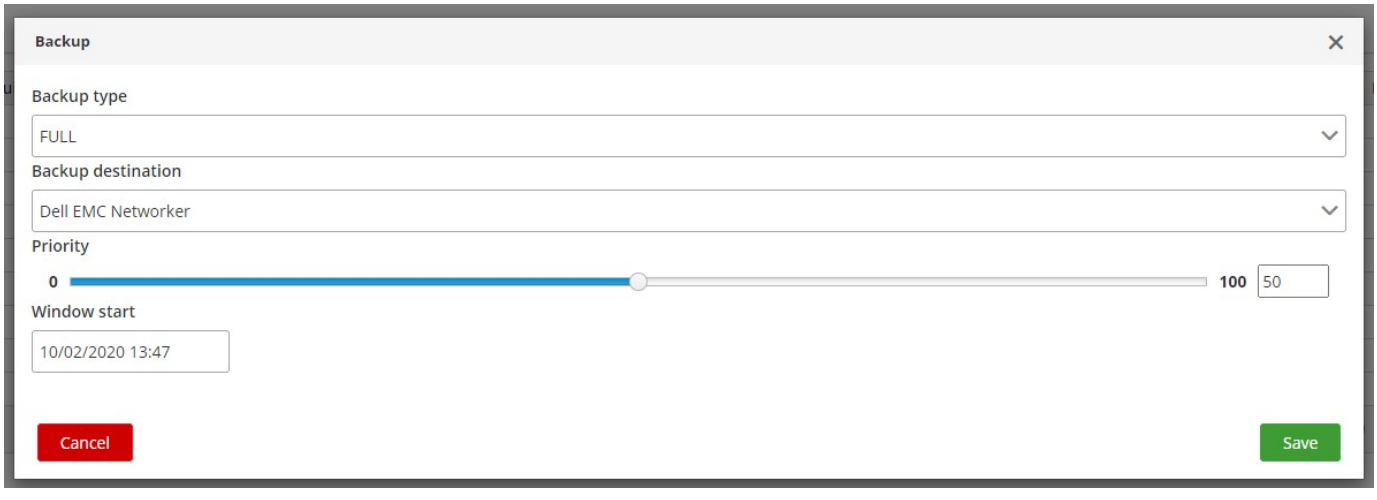
This tab shows all inventoried virtual machines in your OLVM environment. Besides, you can also perform a basic backup or restore operations.



But that's not all, you can also go into the details of the virtual machine by clicking on its name:

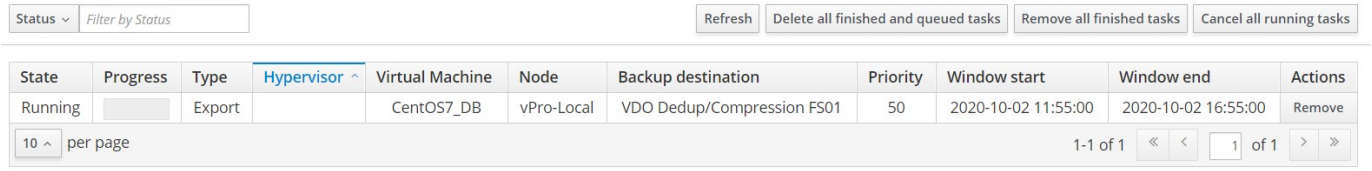


Backup window view:



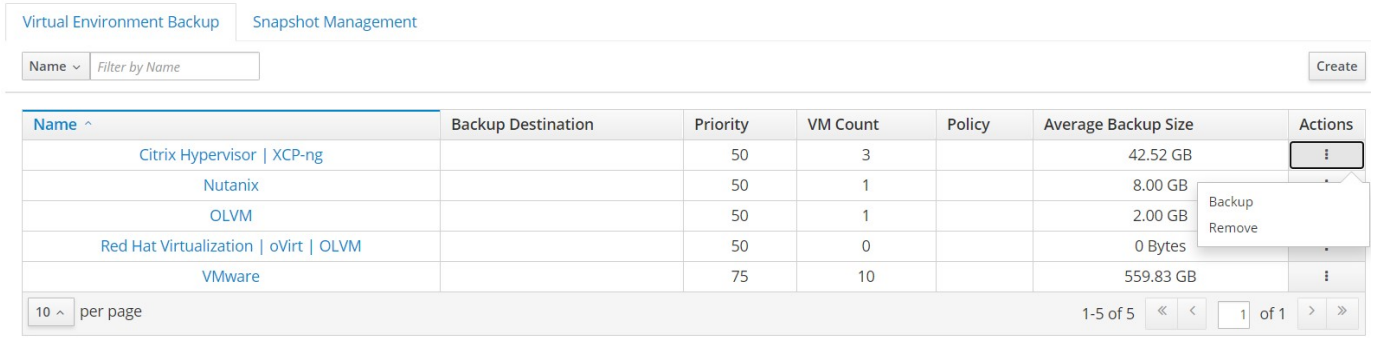
Task console

Basic information about current tasks performed by Data Protector for Cloud Workloads.



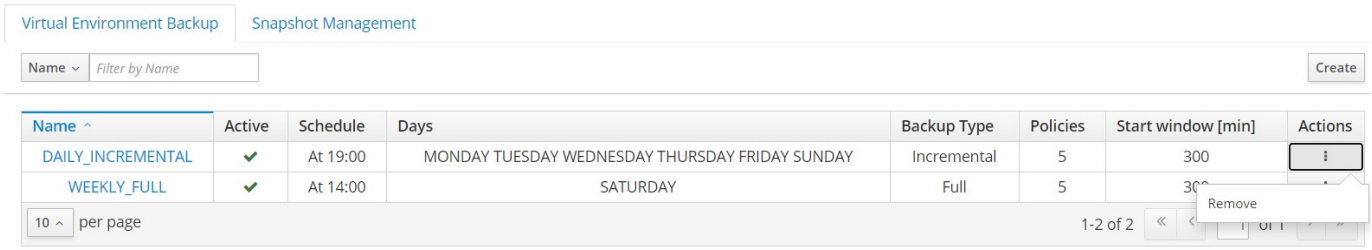
Policies

Allows you to create policies for VM's backups and snapshots. It basically has the same functionalities as Data Protector for Cloud Workloads WebUI.



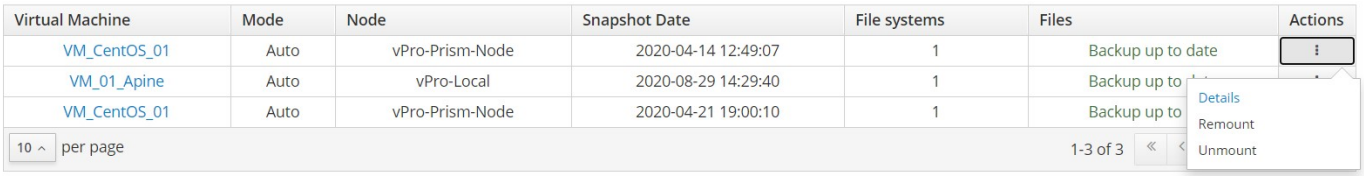
Schedules

As with the policies tab, it allows you to create schedules for the created rules.

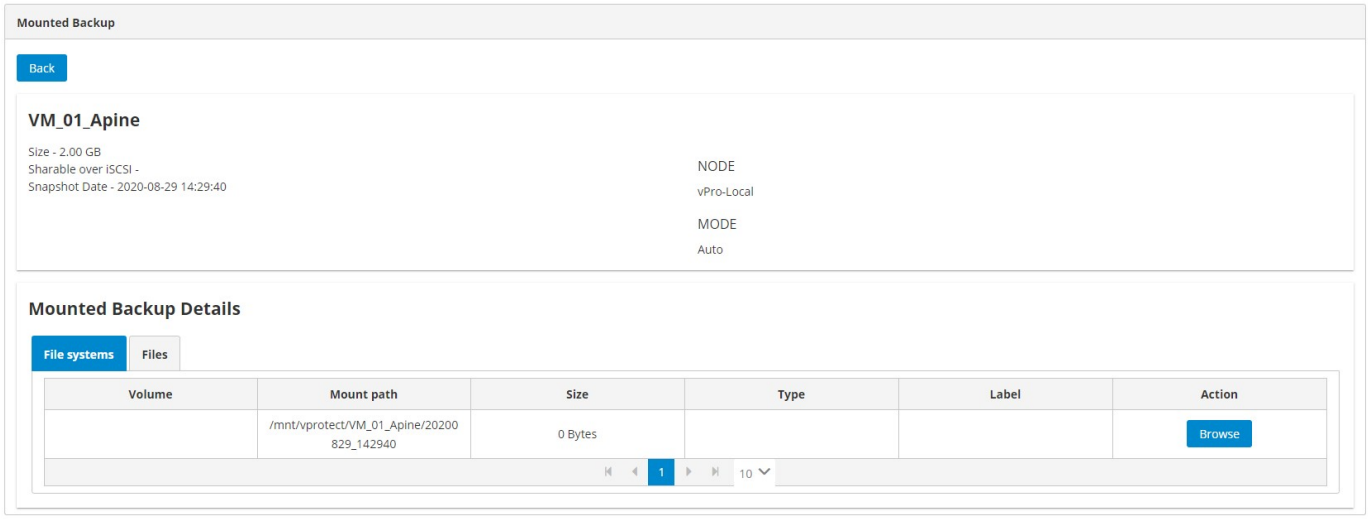


Mounted Backups

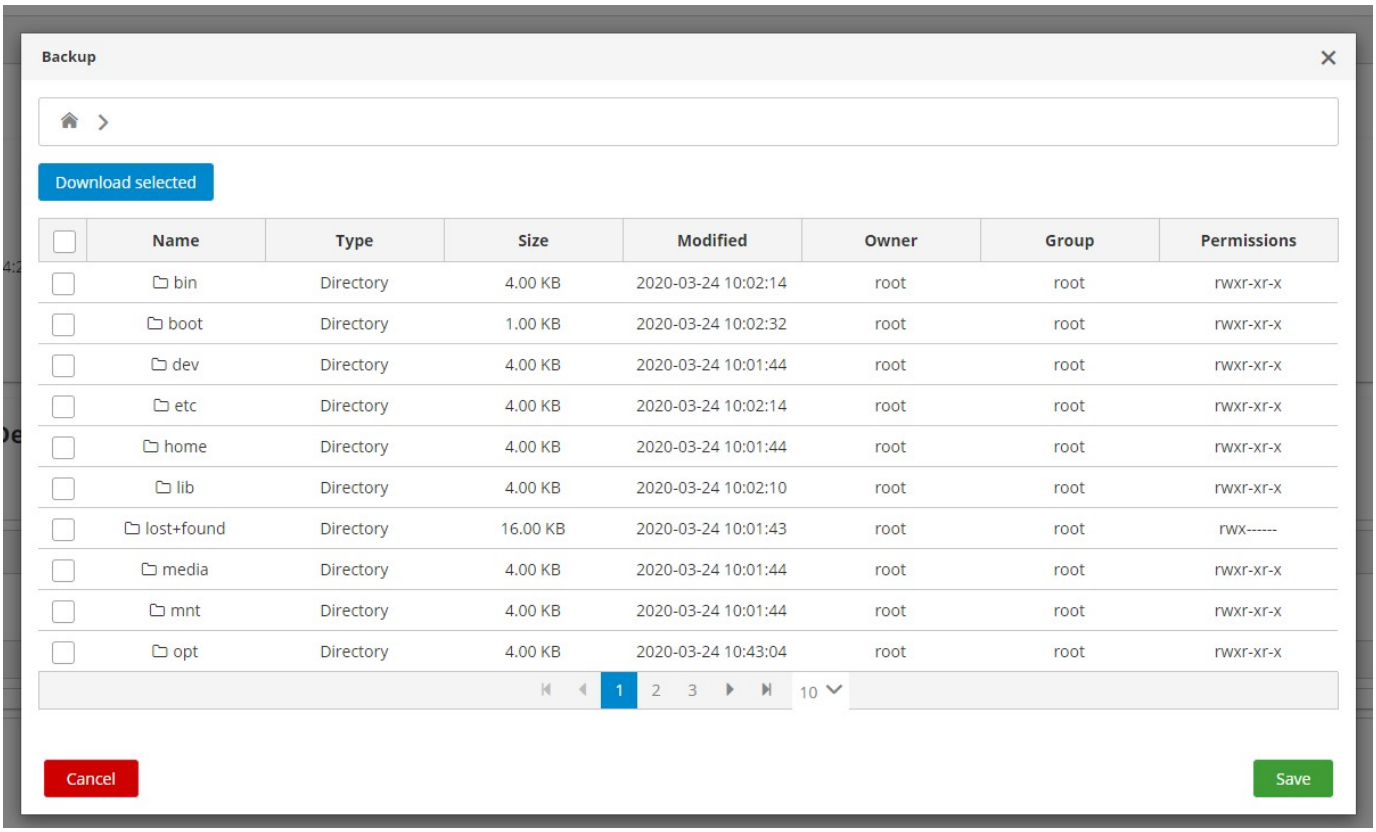
Finally, you can also browse your mounted backups from the OLVM dashboard. You only need to enter the backup details using the menu on the right.



From here we can see the basic information about the backup and start browsing the files using the "Browse" button on the right.



Just select a folder or file and then press the "download selected" button to have the files on your computer.



Installation

1. You can find the add-on in the GitHub repository. Follow the instructions in the README to build or download the plugin. Then extract the provided archive onto your Oracle Linux virtualization manager.
2. In the file `vprotect.json` edit the lines in the config part:
    - `vProtectURL` - the URL to Data Protector for Cloud Workloads API
    - `username` - the name of admin in Data Protector for Cloud Workloads
    - `password` - the admin password in Data Protector for Cloud Workloads

Example:

```
{
   "name": "vprotect",
   "url": "plugin/vprotect/plugin.html",
```

```
    "resourcePath": "vprotect-resources",
    "lazyLoad": false,

    "config": {
        "vProtectURL": "http://10.40.0.55:8080/api",
        "username": "admin",
        "password": "vPr0tect"
     }
  }
```

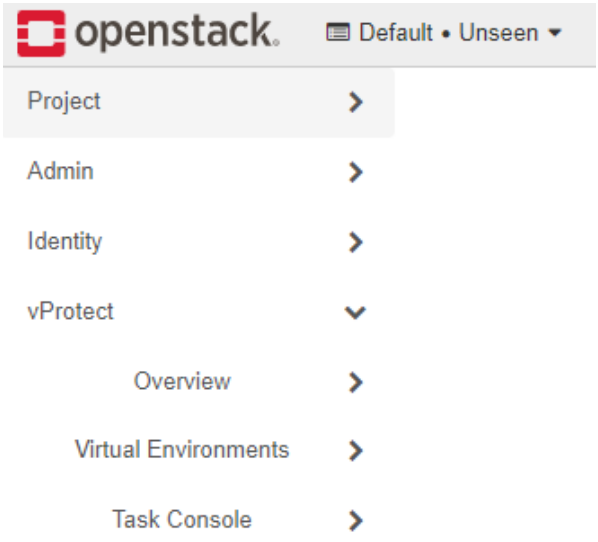
1. Put the `vprotect.json` file and `vprotect-resources` directory in the `/usr/share/ovirt-engine/ui-plugins` directory in the OLVM engine.

OpenStack UI Plugin

Overview

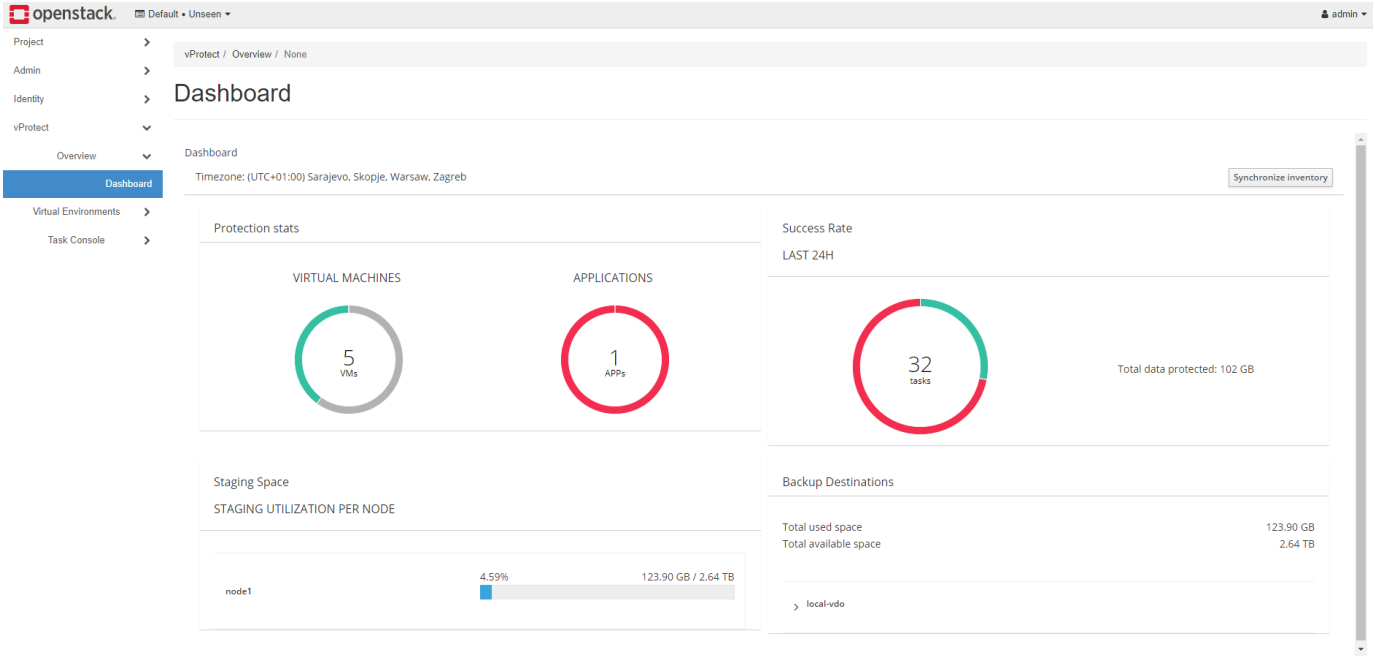
Integration with the Openstack interface is our second plugin alongside the oVirt/RHV virtualization family. Thanks to it, you can perform most of the basic operations without logging into the Data Protector for Cloud Workloads dashboard.

After installation (which is described at the end of this article) you will see a new tab "vProtect" in the OpenStack menu. This consists of several sub-tabs that allow you to perform basic actions such as backup, restore or create a new schedule.



Dashboard

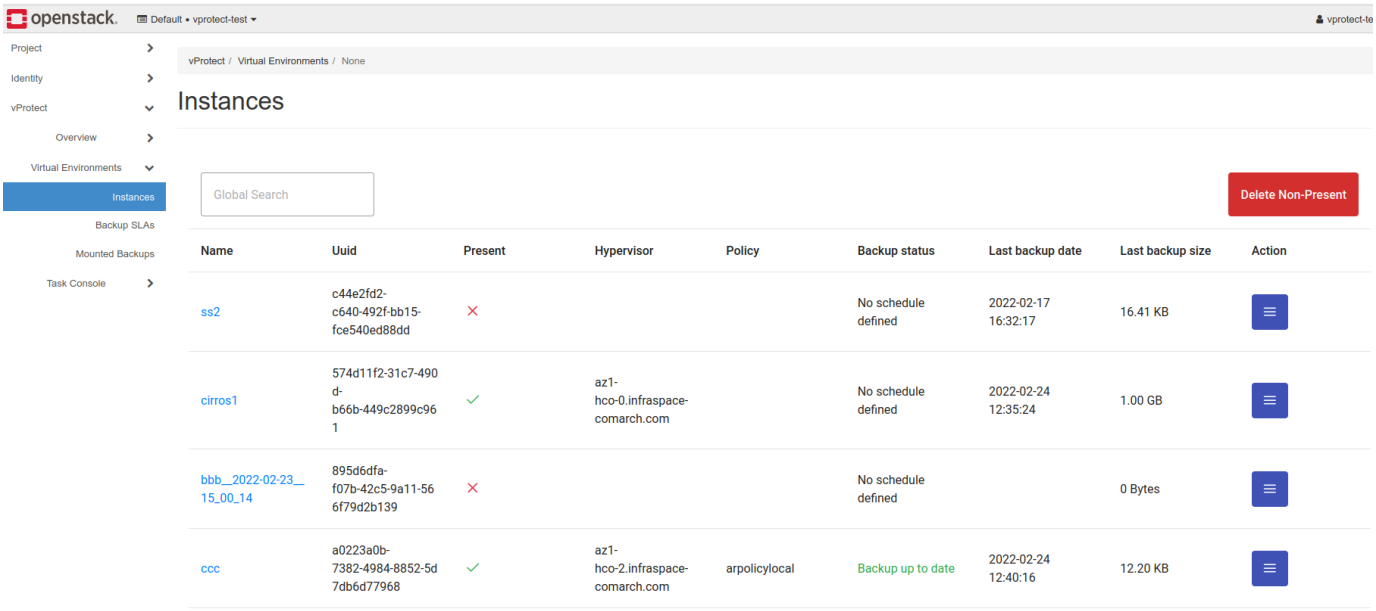
Divided into a few sections, it makes it possible to view and set the most vital options related to management, monitoring, and reporting.



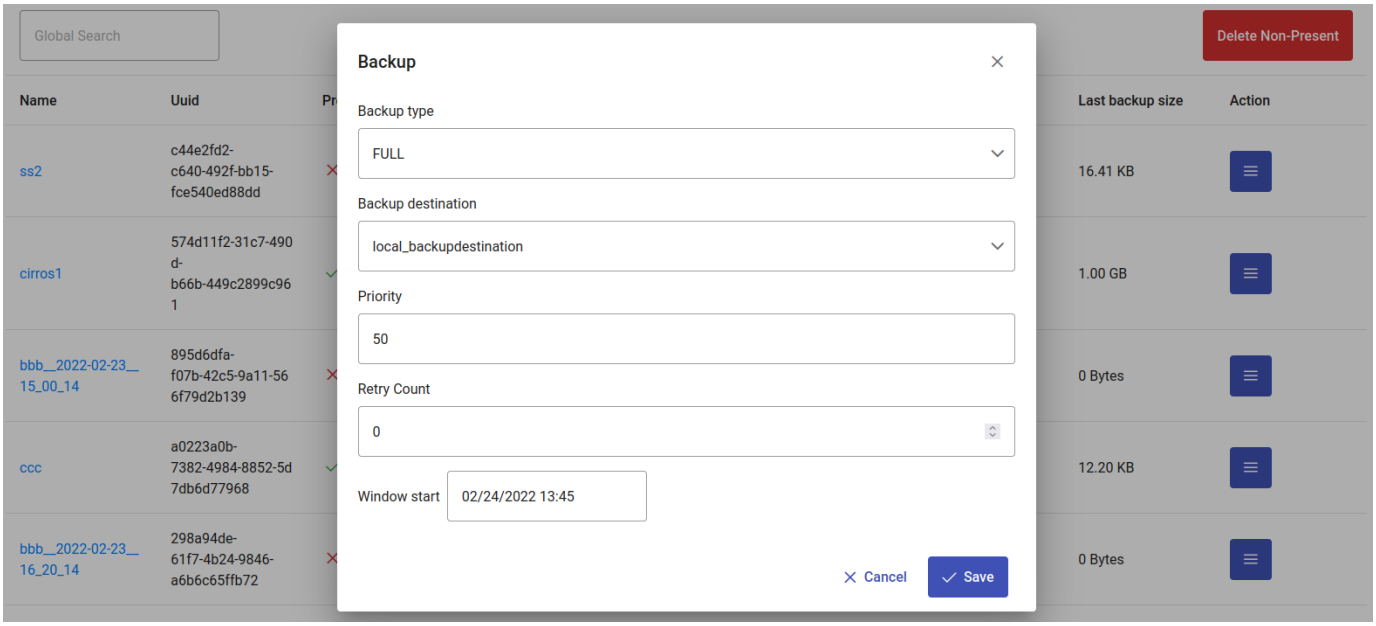
Virtual Environments

Instances

This tab shows all inventoried instances in your OpenStack environment.

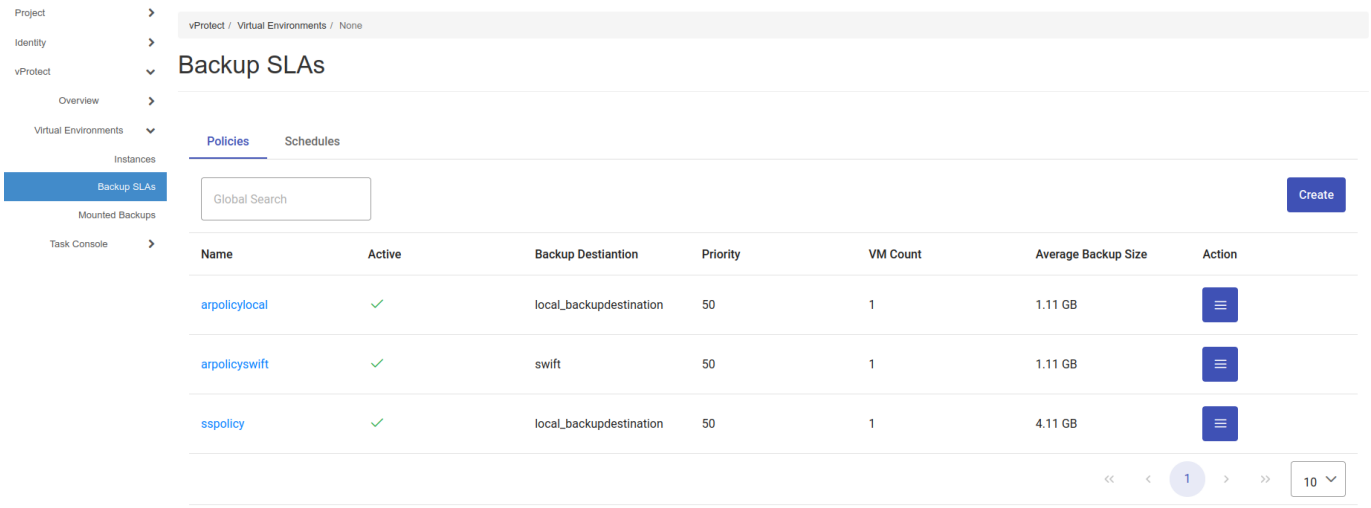


Besides, you can also perform basic backup operations.

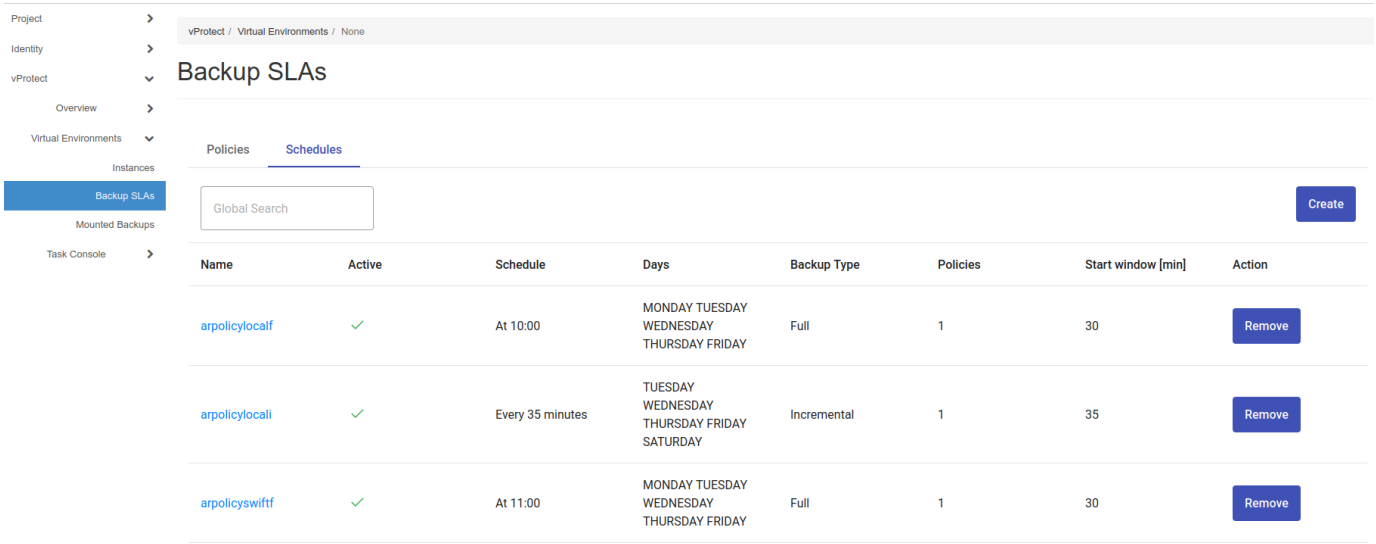


Backup SLAs

Our plugin also allows you to create or manage backup policies

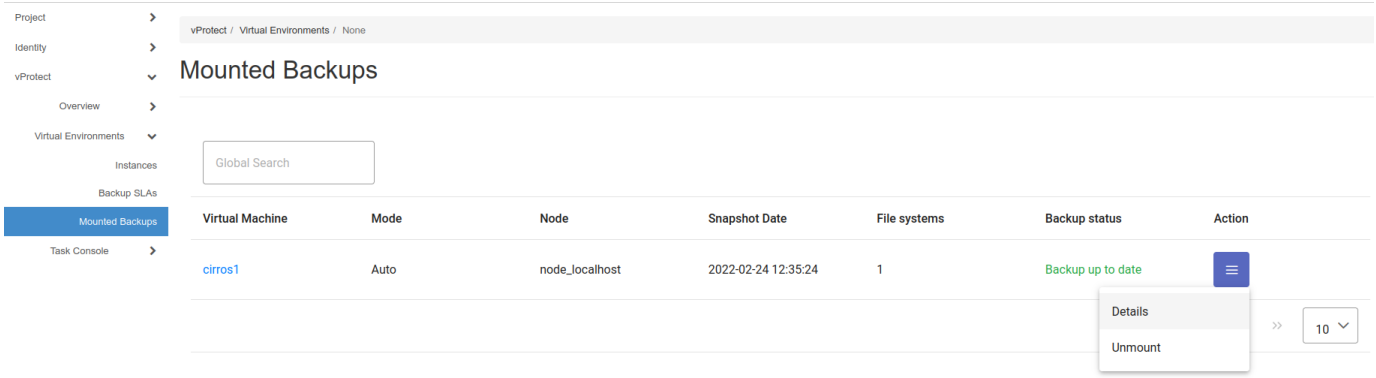


and schedules.

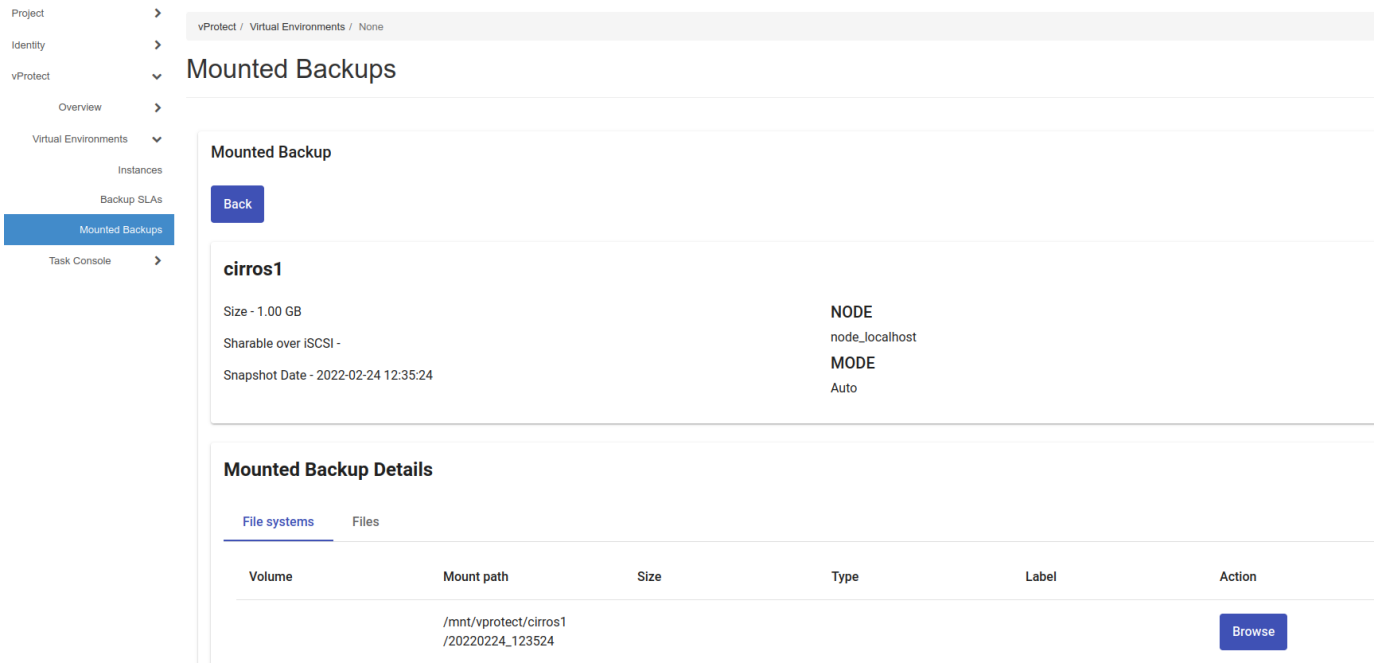


Mounted Backups

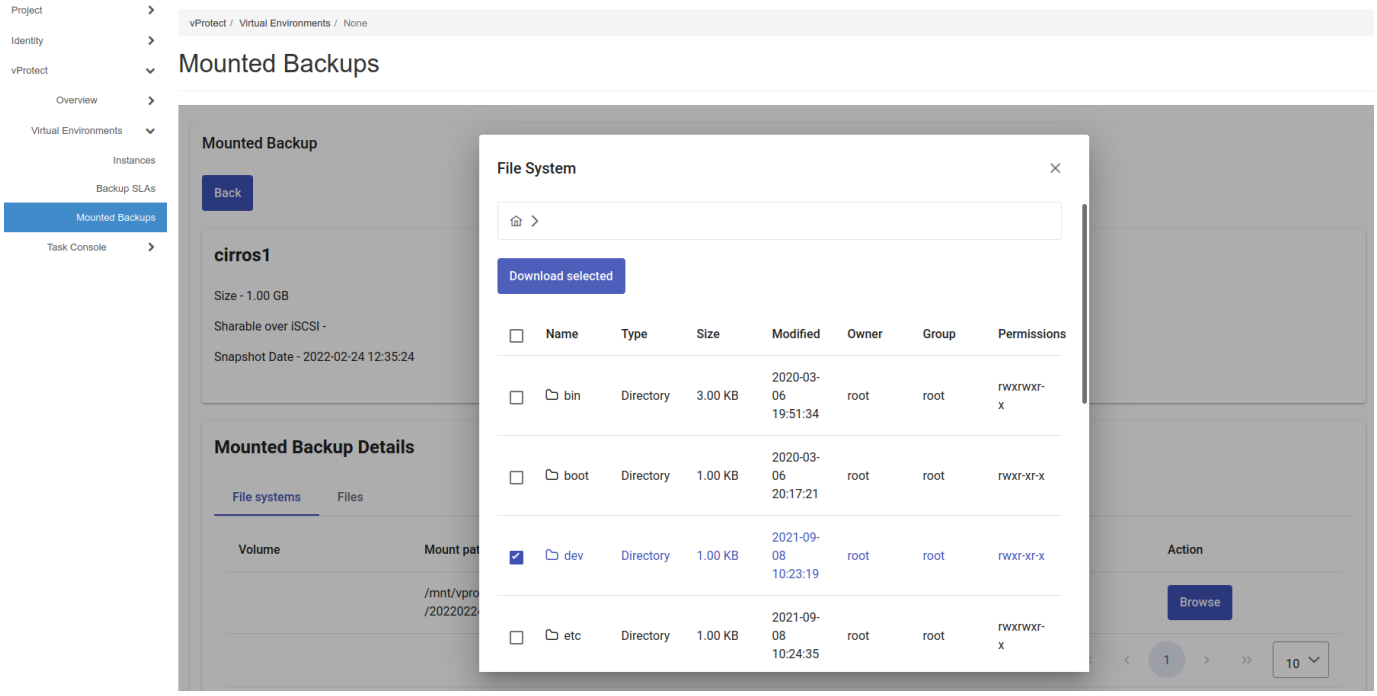
Finally, you can also browse your mounted backups from the OpenStack dashboard. You only need to enter the backup details using the menu on the right.



From here we can see the basic information about the backup and start browsing the files using the "Browse" button on the right.

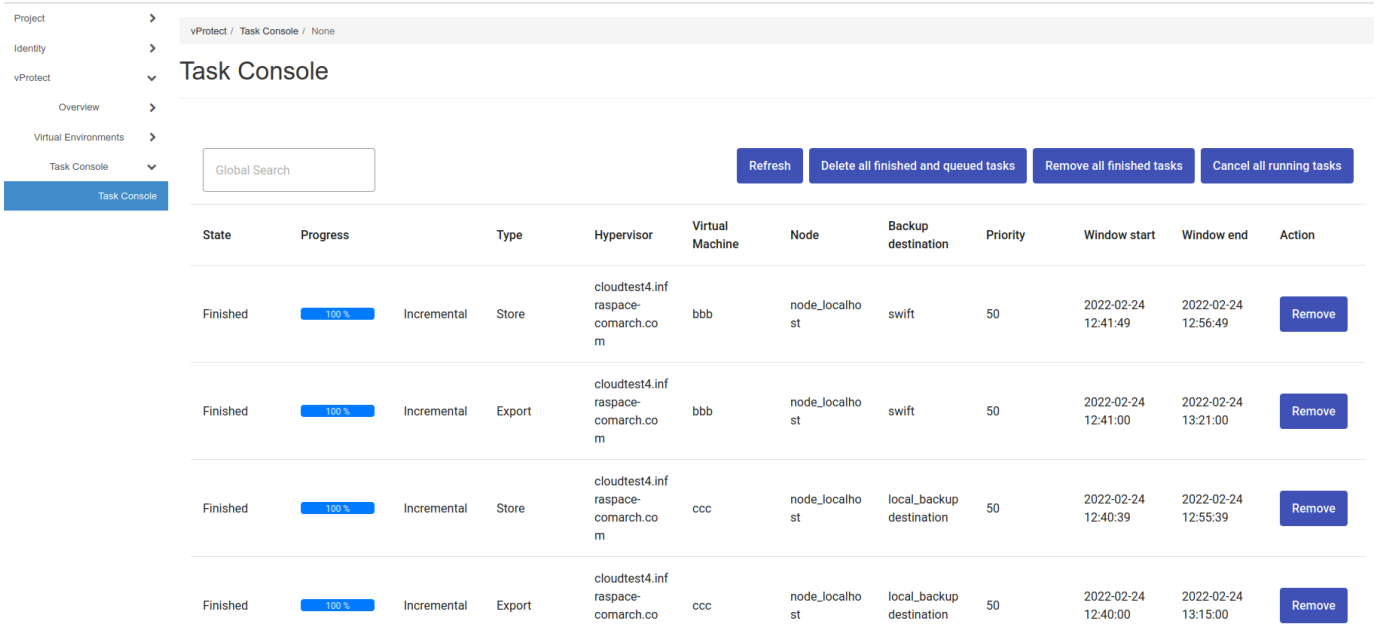


Just select a folder or file and then click on the "download selected" button to have the files on your computer.



Tasks Console

Basic information about current tasks performed by Data Protector for Cloud Workloads.



OpenStack general integration setup

You can find the add-on in the GitHub repository. Extract the provided archive onto your Horizon host and execute `python install.py DP-for-Cloud-Workloads_API_URL USER PASSWORD`

Example: `python install.py http://localhost:8080/api admin vprotect`.

> **Note:** you need to restart your Horizon HTTP server after this

The above-mentioned script will copy the plug-in files to the following folders:

- `/usr/share/openstack-dashboard/openstack_dashboard/dashboards/vprotect` - plugin files
- `/usr/share/openstack-dashboard/openstack_dashboard/enabled` - file to enable the plugin

In order to **uninstall** it, remove the `vprotect` subfolder and `enabled/_50_vprotect.py` file and restart your Horizon HTTP server.

Integrate Data Protector for Cloud Workloads dashboard plugin to OpenStack (LXC)

Requirements:

- git, python3-yaml packages
- internet connection

1. Check the name of the horizon container:

```
lxc-ls -f | grep horizon

example:

[root@aio1 ~]# lxc-ls -f | grep horizon  aio1_horizon_container-b2daccaa RUNNING
1 onboot, openstack 10.255.255.213, 172.29.239.229 - false
```

2. Enter horizon container:

```
[root@aio1 ~]# lxc-attach aio1_horizon_container-b2daccaa
```

3. Install requirements packages:

```
root@aio1-horizon-container-b2daccaa:~# apt install python3-yaml git -y
```

4. Clone from github installations files:

```
root@aio1-horizon-container-b2daccaa:~# git clone
https://github.com/Storware/openstack-horizon-ui-vprotect-extensions
```

5. Change owner of the plugin directory to horizon:horizon

```
root@aio1-horizon-container-b2daccaa:~# chown -R horizon:horizon openstack-
horizon-ui-vprotect-extensions
```

6. Enter plugin directory:

```
root@aio1-horizon-container-b2daccaa:~# cd openstack-horizon-ui-vprotect-
extensions
```

7. Optionally you can ping Data Protector for Cloud Workloads Server by ping

```
root@aio1-horizon-container-b2daccaa:~# ping DP-for-Cloud-Workloads-server-IP-
ADDRESS
```

8. Next, install the plugin

```
root@aio1-horizon-container-b2daccaa:~# python3 install.py http://server-
ip:8080/api admin_user admin_password
```

When the installation process is completed, plugin files should be placed in /usr/share/openstack-dashboard/openstack_dashboard directory. If your path to the dashboard directory is different, create symbolic links from plugin install directories to non-standard directories.

Example:

```
root@aio1-horizon-container-b2daccaa:~# ln -s /usr/share/openstack-
dashboard/openstack_dashboard/dashboards/vprotect /openstack/venvs/horizon-
23.1.0.dev65/lib/python3.8/dist-packages/openstack_dashboard/dashboards/

root@aio1-horizon-container-b2daccaa:~#  ln -s /usr/share/openstack-
dashboard/static/vprotect /openstack/venvs/horizon-
23.1.0.dev65/lib/python3.8/dist-packages/static/

root@aio1-horizon-container-b2daccaa:~#  ln -s /usr/share/openstack-
dashboard/openstack_dashboard/enabled/_50_vprotect.py /openstack/venvs/horizon-
23.1.0.dev42/lib/python3.8/dist-packages/openstack_dashboard/enabled/
```

9. Edit /etc/apache2/sites-available/openstack-dashboard.conf file:

    - Add alias for static files

```
Alias /dashboard/static /openstack/venvs/horizon-
23.1.0.dev65/lib/python3.8/dist-packages/static/
```

    - Directory tag informs you, where dashboards directories should be placed.
    - Second Directory tag informs where static directory from plugin should be placed.

Example: configuration file should look like this:

```
# Ansible managed

# If horizon is being served via SSL from this web server,
# then we must redirect HTTP requests to HTTPS.

# If horizon is being served via SSL via a load balancer, we
# need to listen via HTTP on this web server. If SSL is not
# enabled, then the same applies.
<VirtualHost 172.29.239.229:80>
ServerName aio1-horizon-container-b2daccaa.openstack.local
LogLevel info
ErrorLog syslog:daemon
CustomLog "|/usr/bin/env logger -p daemon.info -t apache2" "%h %l %u \"%r\" %>s
%b \"%{Referer}i\" \"%{User-agent}i\""
Options +FollowSymLinks
RequestHeader set X-Forwarded-Proto "https"

WSGIScriptAlias / /openstack/venvs/horizon-23.1.0.dev65/lib/python3.8/dist-
packages/openstack_dashboard/wsgi.py
WSGIDaemonProcess horizon user=horizon group=horizon processes=1 threads=1
python-path=/openstack/venvs/horizon-23.1.0.dev65/lib/python3.8/site-packages

WSGIProcessGroup horizon
WSGIApplicationGroup %{GLOBAL}

<Directory /openstack/venvs/horizon-23.1.0.dev65/lib/python3.8/dist-
packages/openstack_dashboard>
<Files wsgi.py >
<IfVersion < 2.4>
Order allow,deny
Allow from all
</IfVersion>
<IfVersion >= 2.4>
Require all granted
</IfVersion>
</Files>
</Directory>

Alias /static /openstack/venvs/horizon-23.1.0.dev65/lib/python3.8/dist-
packages/static/
Alias /dashboard/static /openstack/venvs/horizon-
23.1.0.dev65/lib/python3.8/dist-packages/static/
```

```
<Directory /openstack/venvs/horizon-23.1.0.dev65/lib/python3.8/dist-
packages/static/>
Options -FollowSymlinks
<IfVersion < 2.4>
AllowOverride None
Order allow,deny
Allow from all
</IfVersion>
<IfVersion >= 2.4>
Require all granted
</IfVersion>
</Directory>
</VirtualHost>
Edit /openstack/venvs/horizon-23.1.0.dev65/lib/python3.8/dist-
packages/openstack_dashboard/urls.py and add in urlPatterns following line
url(r'^dashboard/', horizon.base._wrapped_include(horizon.urls))
```

Your urls.py should looks like:

```
"""
URL patterns for the OpenStack Dashboard.
"""

from django.conf import settings
from django.conf.urls import include
from django.conf.urls.static import static
from django.conf.urls import url
from django.contrib.staticfiles.urls import staticfiles_urlpatterns
from django.views import defaults

import horizon
import horizon.base
from horizon.browsers import views as browsers_views
from horizon.decorators import require_auth

from openstack_dashboard.api import rest
from openstack_dashboard import views

urlpatterns = [
url(r'^$', views.splash, name='splash'),
url(r'^api/', include(rest.urls)),
url(r'^header/', views.ExtensibleHeaderView.as_view()),
url(r'', horizon.base._wrapped_include(horizon.urls)),
**url(r'^dashboard/', horizon.base._wrapped_include(horizon.urls)),**
]

# add URL for ngdetails
```

10. Restart httpd service

```
/etc/init.d/apache2 restart
```

11. After refreshing the dashboard site, you should see Data Protector for Cloud Workloads tab in the Openstack menu.

Troubleshooting

Data Protector for Cloud Workloads log directory path is `/opt/vprotect/logs` - this is the first place to check for the root cause of errors. All log files are also accessible from `Logs` sections in web UI.

The CLI interface records messages in `vprotect_client.log` files under the subdirectory with the same name as the node. In the same directory you can also find the `vprotect_daemon.log` files, which contain all engine related messages.

The web UI has several directories where it stores log files:

- `appserver` which has all messages coming from the application server - which hosts web UI and API
- `api` which has all messages related to - the core Data Protector for Cloud Workloads Server application
- `cloudagent` which has all messages from Cloud Agent
- `cloudserver` which has all messages from Cloud core part

To verify if services are running, you can use:

- `systemctl status vprotect-server` for the server
- `systemctl status vprotect-node` for the node, or `vprotect status`

If you don't find the root cause of the problem here, you can switch Data Protector for Cloud Workloads to DEBUG mode, and recreate the task to generate logs in DEBUG mode.

How to enable Data Protector for Cloud Workloads DEBUG mode

Quite often support will ask for debug logs for more in-depth troubleshooting. In order to do that please follow the steps below.

Data Protector for Cloud Workloads Node

1. Edit `/opt/vprotect/log4j2-node.xml` change `INFO` to `DEBUG` in `<Property name="logLevel">...</Property>` tag
2. Restart Data Protector for Cloud Workloads-node service:

```
systemctl restart vprotect-node
```

3. Proceed with operations that need to be logged.
4. Then collect logs from `/opt/vprotect/logs/<NODE_NAME>` directory.

Data Protector for Cloud Workloads Server

1. Edit `/opt/vprotect/log4j2-server.xml` change `INFO` to `DEBUG` in `<Root level="...">` tag
2. Restart Data Protector for Cloud Workloads-server service:

```
systemctl restart vprotect-server
```

3. Proceed with the operations that need to be logged.
4. Then collect the logs from `/opt/vprotect/logs/api` and the `/opt/vprotect/logs/appserver` directories.

Data Protector for Cloud Workloads Cloud Agent

1. Edit `/opt/vprotect/cloudagent/AgentConfig.json` file (on the node system) and add below line to the “logs” section:

```
"level": "DEBUG"
```

2. The file should look like that, after the changes:

```
{
"agent": {
        "logs":{
                "path": "../logs/cloudagent",
                "level": "DEBUG"
        }
},
"server": {
    "address": "localhost:8383",
}
}
```

3. Restart Data Protector for Cloud Workloads-node service:

```
systemctl restart vprotect-node
```

4. Proceed with operations that need to be logged.
5. Then collect logs from `/opt/vprotect/logs/cloudagent` directory.

Collecting logs

Using the Web UI

General logs

1. Go to the `Logs` section (top bar)
2. You'll see directories for `api`, `appserver` , `cloudserver` , `cloudagent` and one directory for each node (same as their names)
3. To download all logs - click the button `Download all logs` which will generate an archive containing all logs
4. To download a specific file - browse to the directory and click the name of the log

> **Note:** By downloading logs from WebUI you can also download logs for Data Protector for Cloud Workloads Cloud server and node.

Backup-related logs

1. Go to the VM details and `backup history` tab.
2. Click on the second icon on the right of the backup you want to collect logs for.
3. The downloaded file is `vprotect_daemon.log` filtered, so it should contain only entries related to the tasks of backup/restore operations related to this backup.

Directly from the operating system

Data Protector for Cloud Workloads Node

Log files are stored in this folder: `/opt/vprotect/logs/<node_name>`:

- `vprotect_client.log` - stores CLI-related messages
- `vprotect_daemon.log` - stores Data Protector for Cloud Workloads Node engine related message

Data Protector for Cloud Workloads Server

Log files are stored in:

- `/opt/vprotect/logs/appserver` - application server (hosting Data Protector for Cloud Workloads Server) messages
- `/opt/vprotect/logs/api` - Data Protector for Cloud Workloads Server application logs

External log targets

Data Protector for Cloud Workloads uses log4j2 for logging both in the Node and Server. This module allows you to write to external log targets. All supported appenders are described here: https://logging.apache.org/log4j/2.x/manual/appenders.html.

Below, you can find information on how to set Syslog as a target for Data Protector for Cloud Workloads Server and Node.

1. To support Syslogs, make sure you have `rsyslog` a package - if not you can install it like this:

```
sudo yum -y install rsyslog
```

2. In `/etc/rsyslog.conf` file:
    - uncomment these lines to enable UDP socket transport:

```
#module(load="imudp") # needs to be done just once
#input(type="imudp" port="514")
```

    - add this line under `#### GLOBAL DIRECTIVES ####` section to support newline characters:

```
$EscapeControlCharactersOnReceive off
```

3. Open 514 port for UDP connection

```
firewall-cmd --permanent --add-port=514/udp
firewall-cmd --reload
```

4. Enable rsyslog service

```
systemctl enable --now rsyslog
```

5. To use Syslog's with Data Protector for Cloud Workloads Server add in `log4j2-server.xml` file:
    - in `Appenders` section add Syslog appender:

```
<Socket name="Syslog" host="localhost" port="514" protocol="UDP">
<PatternLayout
pattern="$${hostName} vprotect-server: %level [%t] %c{1}.%M:%L
%n[$${ctx:task:-}] %msg%n%n"/>
</Socket>
```

    - in `Loggers` add reference to Syslog appender in `Root` section:

```
<AppenderRef ref="Syslog"/>
```

6. Restart Data Protector for Cloud Workloads Server service:

```
systemctl restart vprotect-server
```

Example of log4j2-server.xml after modifications:

```
<?xml version="1.0" encoding="UTF-8"?>
<Configuration status="WARN">
    <Properties>
        <Property name="baseDir">/opt/vprotect/logs/api</Property>
    </Properties>
    <Appenders>
        <Console name="Console" target="SYSTEM_OUT">
            <PatternLayout pattern="%d{yyyy-MM-dd HH:mm:ss} %-5p [%t] %c{1}.%M:%L -
%msg%n"/>
        </Console>

        <RollingFile name="RollingFile" filename="${baseDir}/api.log"
                     filepattern="${baseDir}/api.log_%d{yyyy-MM-dd--
HH.mm.ss}.log.zip" fileOwner="vprotect"
                     fileGroup="vprotect" filePermissions="rw-rw----">
            <PatternLayout pattern="[%d{yyyy-MM-dd HH:mm:ss}] %-5p [%t] %X
%c{1}.%M:%L%n%msg%n%n"/>
            <Policies>
                <SizeBasedTriggeringPolicy size="2 MB" />
            </Policies>
            <DefaultRolloverStrategy max="20">
                <Delete basePath="${baseDir}" maxDepth="1">
                    <IfFileName glob="api.log_*.log.zip"/>
                    <IfAccumulatedFileCount exceeds="20"/>
                </Delete>
            </DefaultRolloverStrategy>
        </RollingFile>

        <Socket name="Syslog" host="localhost" port="514" protocol="UDP">
            <PatternLayout pattern="$${hostName} vprotect-server: %level [%t]
%c{1}.%M:%L %n[$${ctx:task:-}] %msg%n%n"/>
        </Socket>
    </Appenders>
    <Loggers>
    <Root level="DEBUG">
            <AppenderRef ref="RollingFile" />
            <AppenderRef ref="Syslog" />
        </Root>
    </Loggers>
</Configuration>
```

1. To use Syslog's with Data Protector for Cloud Workloads Node add in `log4j2-node.xml` file:

    - in `Appenders` section add Syslog appender:

```
```

```
<Socket name="Syslog" host="localhost" port="514" protocol="UDP">
<PatternLayout
pattern="$${hostName} vprotect-node: %level [%t] %c{1}.%M:%L
%n[$${ctx:task:-}] %msg%n%n"/>
</Socket>
```

- in `Loggers` add reference to Syslog appender in `Root` section:

```
<AppenderRef ref="Syslog"/>
```

2. Restart Data Protector for Cloud Workloads Node service:

```
systemctl restart vprotect-node
```

Example of log4j2-node.xml after modifications:

```
<?xml version="1.0" encoding="UTF-8"?>
<Configuration status="WARN">
    <Properties>
        <Property name="logLevel">DEBUG</Property>
        <Property name="baseDir">/opt/vprotect/logs/$${sys:node:-null}</Property>
        <Property name="vmwareBaseDir">/opt/vprotect/logs/vmware</Property>
        <Property name="daemonLogFileName">vprotect_daemon.log</Property>
        <Property name="clientLogFileName">vprotect_client.log</Property>
        <Property name="vmwareLogFileName">vprotect_vmware.log</Property>
    </Properties>
    <Appenders>
        <Routing name="Routing">
            <Routes pattern="$${sys:port}">
                <Route key="$${sys:port}">
                    <RollingFile name="CLI"
filename="${baseDir}/${clientLogFileName}"
                                 filepattern="${baseDir}/${clientLogFileName}.%i">
                        <PatternLayout pattern="[%d{yyyy-MM-dd HH:mm:ss}] %level [%t]
%c{1}.%M:%L %n%msg%n%n"/>
                        <Policies>
                            <SizeBasedTriggeringPolicy size="8 MB"/>
                        </Policies>
                        <DefaultRolloverStrategy max="50">
                            <Delete basePath="${baseDir}" maxDepth="1">
                                <IfFileName glob="${clientLogFileName}.*"/>
                                <IfAccumulatedFileCount exceeds="50"/>
                            </Delete>
                        </DefaultRolloverStrategy>
                    </RollingFile>
                </Route>
                <Route>
                    <RollingFile name="Engine"
filename="${baseDir}/${daemonLogFileName}"
                                 filepattern="${baseDir}/${daemonLogFileName}.%i">
                        <PatternLayout pattern="[%d{yyyy-MM-dd HH:mm:ss.SSS}] %level
[%t] %c{1}.%M:%L %n[$${ctx:task:-}] %msg%n%n"/>
                        <Policies>
```

```
                            <SizeBasedTriggeringPolicy size="8 MB"/>
                        </Policies>
                        <DefaultRolloverStrategy max="50">
                            <Delete basePath="${baseDir}" maxDepth="1">
                                <IfFileName glob="${daemonLogFileName}.*"/>
                                <IfAccumulatedFileCount exceeds="50"/>
                            </Delete>
                        </DefaultRolloverStrategy>
                    </RollingFile>
                </Route>
            </Routes>
        </Routing>

        <Console name="StdOut" target="SYSTEM_OUT">
            <PatternLayout pattern="%msg%n"/>
        </Console>

        <RollingFile name="VMware" filename="${vmwareBaseDir}/${vmwareLogFileName}"
                     filepattern="${vmwareBaseDir}/${vmwareLogFileName}.%i"
fileGroup="vprotect" fileOwner="vprotect"
                     filePermissions="rw-rw-rw-">
            <PatternLayout pattern="[%d{yyyy-MM-dd HH:mm:ss}] %level [%t] %c{1}.%M:%L
%n%msg%n%n"/>
            <Policies>
                <SizeBasedTriggeringPolicy size="8 MB"/>
            </Policies>
            <DefaultRolloverStrategy max="50">
                <Delete basePath="${vmwareBaseDir}" maxDepth="1">
                    <IfFileName glob="${vmwareLogFileName}.*"/>
                    <IfAccumulatedFileCount exceeds="50"/>
                </Delete>
            </DefaultRolloverStrategy>
        </RollingFile>

    <Socket name="Syslog" host="localhost" port="514" protocol="UDP">
            <PatternLayout pattern="$${hostName} vprotect-node: %level [%t]
%c{1}.%M:%L %n[$${ctx:task:-}] %msg%n%n"/>
    </Socket>
    </Appenders>
    <Loggers>
        <Root level="${logLevel}">
            <AppenderRef ref="Routing"/>
            <AppenderRef ref="Syslog"/>
        </Root>
        <Logger name="StdOut" additivity="false">
            <AppenderRef ref="StdOut"/>
        </Logger>
        <Logger name="VMware" level="${logLevel}" additivity="false">
            <AppenderRef ref="VMware"/>
        </Logger>
    </Loggers>
</Configuration>
```

> **Note**: If you want to use Syslogs in both Data Protector for Cloud Workloads Server and Node you need to use two different udp ports and specify them in /etc/rsyslog.conf

Disaster Recovery

Internal Database Protection

Data Protector for Cloud Workloads stores all of the metadata in the local database. It is **highly recommended** to set up periodic DB backup on Data Protector for Cloud Workloads Server. Check Initial configuration for more information.

In case you need to restore Data Protector for Cloud Workloads DB:

- if you have a working Data Protector for Cloud Workloads - you can use it to restore this file to the specified location and then restore it as described in the Disaster recovery section
- if you don't have working Data Protector for Cloud Workloads - you can try to use the last copy of the database (it is left by default in `/tmp/vprotect_db.sql.gz` on the server host.
- if it is not there and you don't have Data Protector for Cloud Workloads working - you may need to use external tools such as S3 browser or just browse through your file system backup destination directories to find and download this file and later restore it as described in the Disaster recovery section.

Once you have your backup you can restore DB with the following command:

```
gunzip < PATH_TO_GZIPPED_BACKUP | mysql -u root -pDBPASSWORD vprotect
```

In case of a complete loss of the Data Protector for Cloud Workloads Server:

1. Reinstall Data Protector for Cloud Workloads Server
    - if you lost your license file please contact support
2. Before starting Data Protector for Cloud Workloads Server - restore the database
    - you can also restore it later (i.e. if you want to reinstall it with Ansible or all-in-one option), but remember to shutdown server first, then restore DB and start the server again
3. Replace all backup provider-specific files (install any binaries specific for required backup destinations)
4. Start Data Protector for Cloud Workloads Server service
5. Install Data Protector for Cloud Workloads Nodes
6. Make sure the staging path on each node is correct and available
7. Re-register and start nodes

At this point, Data Protector for Cloud Workloads should be ready to continue operation.

Known software issues and limitations

Issue ID	Product feature	Description	Workaround
0001	Task cancellation	Task cancellation process will not be reflected in immediate task failure - task state will be changed to cancelled and only when the engine checks its state again will it initiate the cancellation operation - some platforms may even require data transfer to be completed first	Allow the task to cancel and fail gracefully - this will allow Data Protector for Cloud Workloads to clean up temporary artifacts. If you click again, the task will be forced to be removed from the queue and artifacts such as snapshots will be removed as part of the daily snapshot cleanup job. In general, avoid forced removal of tasks.
0002	Storage usage statistics	Storage statistics are updated after each backup or the clean old backups job - this data may not be up-to-date all the time	To have current storage usage updated you can invoke the Clean Old backups job from the Backup Destinations tab
0003	Pre/post access storage command execution	Complete command cannot be provided as a single string. Commands need to have their arguments provided as separate entries (by clicking on the **Add command arg** button). Commands are directly executed using OS-level calls so shell operators are not supported directly.	To use shell-specific operators/commands etc., execute commands with 3 command arguments `/bin/bash`, `-c`, `your command-with-all-arguments-and-shell-operators`
0004	Tasks stuck in the queue in Queued state	Tasks will usually be executed according to the limits set on the node and only if node is running and has available space on the staging	Verify that the node has available space in the staging space path - there should be a warning message in `vprotect_daemon.log`
0005	OpenStack backup using disk attachment	OpenStack with disk-attachment backup strategy (cinder) - 3.9.2 only supports Ceph RBD as a storage backend	N/A
0006	KVM stand-alone - disk formats	VMs being backed up must have virtual disks as QCOW2/RAW files or LVM volumes	N/A
0007	KVM stand-alone - snapshots	Snapshots on KVM hypervisors are made using libvirt (QCOW2/RAW files) or LVM snapshots and are created per volume basis; this operation may not be atomic if multiple drives are used	Make sure the data is in the VM (especially that file systems reside on as few disks as possible to lower the risks of data inconsistency) or try to use pre-post remote command execution to quiesce application before snapshot is done
0008	KVM standalone incremental backup on QCOW2	Incremental backups will be performed only on running VMs. libvirt doesn't allow blockcommit on a power-down VM so snapshot wouldn't be removed.	Full backup will be performed instead

Issue ID	Product feature	Description	Workaround
0009	Backup providers path	The backup provider's paths must be mounted and available ahead - you should provide the path just to the mount point, without any protocol specification	Mount remote file systems first and make sure these are available all the time - in Data Protector for Cloud Workloads configuration please provide just the locally available mount point
0010	Backups marked as Success (removed)	When backup completes or when the clean old backups job is performed, Data Protector for Cloud Workloads marks non-present backups as removed (if any of the files that were part of the backup are not present). This may also happen if your storage was temporarily not available.	Make sure storage and all of the files are available and run the Clean Old Backups job - this job also attempts again to sync files present in the backup provider with the database - if all files for a particular backup are found again (and all previous backups that this particular backup depends on are also present) it will again have Success status
0011	Hypervisor storage usage statistics	Restore may fail due to insufficient storage space in the Hypervisor Storage used as a target because of usage information that is not up to date. Usage statistics are updated only with inventory synchronization job	Run the Inventory Synchronization job again on your hypervisor (or manager) to update storage statistics and try to restore again.
0012	RHV - SSH transfer rate drops after some time	The SSH transfer rate may drop in some environments when used intensively over a longer time.	If possible, and when the network used for transfers is trusted, please use the netcat option to transfer files outside of the SSH channel
0013	Node tasks limits	The number of concurrent tasks are configured in Node Configuration -> Tasks section. These limits apply to all nodes that use this particular configuration. Currently there is no global setting to limit the number of tasks for all of the nodes in the environment.	To limit the number of tasks globally, reduce the numbers in individual node configurations.
0014	Hypervisor-specific settings in Node Configuration	All of the configuration parameters in Hypervisors tab in Node Configuration are applied to all nodes with this configuration - regardless of which hypervisor it is attached to. This implies that Proxmox settings such as compression will have to be the same on all hypervisors handled by nodes with the same configuration assigned and will have to be the same on all of these hypervisors.	To use these settings with different values for some hypervisors you need to assign separate nodes and define separate node configurations. Ultimately, assign separate nodes for these hypervisors.
0015	Inventory synchronization - duplicated UUID	In some cases, it may happen that the same storage was previously detected with a different setup and remained in the database.	Remove the unused hypervisor storage and try to invoke inventory synchronization again.

Issue ID	Product feature	Description	Workaround
0016	Estimated backup size of policy	The estimated backup size of a policy is computed based only on known backup sizes and extrapolated to the rest of the VMs in the group. This implies that estimation will use average backup size and multiply it by the number of all VMs in the group. Even though disk sizes are known it is not always the same as the size of the backups (especially considering compression or the fact that some strategies require chains of backup deltas to be exported)	Wait for a longer period of time, and once more backups are completed this estimation will be closer to the real value.
0017	Citrix Hypervisor/ xcp-ng - transfers	Transfer NIC is not used in incremental backups when the CBT strategy is invoked - Citrix/xcp-ng may require NBD to be exposed by the master - so Data Protector for Cloud Workloads has to read from the address provided by the CBT mechanism in order to connect to the NBD device. Also, in some cases, data can only be transferred from the master host (especially when it is powered down)	Allow network traffic between all hypervisors and corresponding nodes in the same pool, as sometimes actual transfer may occur from the master host instead of the one which hosts the VM.
0018	RHV - SSH Transfer permissions on the hypervisor	SSH Transfer for RHV usually requires root permissions on the hypervisor in order to activate/deactivate LVM volumes for the backup	You may try with a different backup strategy such as Disk-attachment or Disk Image Transfer
0019	RHV - SSH Transfer - hypervisor access	Data Protector for Cloud Workloads using SSH Transfer for RHV environments needs to be able to access all hypervisors in the cluster - as it may happen that the created disk is available only on a subset of them and needs to be transferred or recovered only by using this specific hypervisor	Allow network traffic and provide valid credentials to access all hypervisors in the cluster over SSH.
0020	Nutanix VG support	Data Protector for Cloud Workloads 3.9.2 only supports volumes residing on the storage containers - VGs are not supported yet	N/A
0021	Nutanix Prism Element/Central connectivity	Data Protector for Cloud Workloads is able to perform backups by using APIs provided by Prism Element only - Prism Central doesn't offer a backup API	Connect to your Prism elements by specifying separate Hypervisor Managers in Data Protector for Cloud Workloads (not by pointing to the Prism Central)
0022	Nutanix backup consistency for intensively used VMs	Intensive workload on the VM may affect backup consistency when using crash consistent backup	If you need higher consistency, install Nutanix Guest Tools inside your VM and enable application consistent snapshots in the VM details in Data Protector for Cloud Workloads

Issue ID	Product feature	Description	Workaround
0023	iSCSI shares for RAW backups	RAW backups allow Data Protector for Cloud Workloads to share them over iSCSI. If backups are in other formats (such as QCOW2), these cannot currently be shared over iSCSI	Use automatic mount instead or restore a backup and mount them using external tools such as qemu-nbd for QCOW2 files
0024	Backup and snapshot policies assignment	Only 1 backup and 1 snapshot management policy can be assigned to a given VM	If you need a dedicated setting for a single VM, you need to create a separate policy for that VM
0025	1 schedule per rule	Currently, each schedule can only be assigned to a single rule within the same policy.	If you need to execute two rules at the same time, you need to create separate schedules and assign them to these rules
0026	Staging space	The staging space is an integral part of a node - this allows to mix backup strategies, especially based on the export storage domain/repository approach with other methods and file system scanning for future file-level restores. It needs to be available at all times and the `vprotect` user needs to be able to write to all subdirectories.	To save space and boost backup time (direct writes to the backup destination) you can, however, mount staging and your PowerProtect DD in the same directory - `/vprotect_data`. Please remember to point the backup destination path to a subdirectory of this mount point, such as `/vprotect_data/backups` - still on the same FS, but the paths must be different.
0027	Node OS-level permissions	At the OS level, Data Protector for Cloud Workloads requires significant permissions to be able to manipulate disks, scan for file systems, mount them, expose resources over iSCSI, operate on block devices (NBD/iSCSI/RBD) and more. These unfortunately require multiple sudo entries and that SELinux is disabled at the same moment.	If some features are not required at the same moment - including NBD/iSCSI/NFS related - you may reduce the number of entries in `/etc/sudoers.d/01-vprotect_node` You also can try to enable SELinux, but later you need to track SELinux errors and add appropriate permissions when some of the functionality is blocked
0028	Proxmox VE	CBT backup strategy	Qcow2 virtual machines are required to use the new Proxmox VE backup strategy - Change block tracking (CBT)
0029	Proxmox VE	CBT backup strategy	At the moment, we do not support the "Dirty Bitmaps" function, therefore we require the last snapshot to be left for incremental backups.

Issue ID	Product feature	Description	Workaround
0030	Storage Providers and node assignment	Data Protector for Cloud Workloads supports only one node assigned to the Storage Provider, which means that backup of significantly big volumes from bigger storage providers, i.e. Ceph RBD etc. will require a high performing node and cannot be scaled out by adding nodes	Install multiple Data Protector for Cloud Workloads Server+Node environments and protect the non-overlapping set of volumes with each Data Protector for Cloud Workloads instance.
0031	RHV - Restore with SPARSE disk allocation format	Restore to RHV using the SPARSE disk allocation format is not supported if backup files are in RAW format and the destination storage domain type is in either Fibre Channel or iSCSI. If such configuration is detected, then the disk allocation format is automatically switched to PREALLOCATED	You can use other backup strategies that use QCOW2 files instead of RAW (like disk image transfer). Alternatively, you can select a different storage domain of a type that supports SPARSE disks with RAW files
0032	Microsoft 365 - Restore of site which has been deleted from Bin	If the site has been deleted from the Bin, only site logic can be restored. Links added in the deleted site are not restored	Restore site or subsites to recover it's logic. Next, download data (site content) manually and upload it to SharePoint Online. Begin download from second level of SharePoint protected data (list/pages/document libary)
0033	Microsoft 365 - Restore 1:1 teams chat	Links shared in chat are not working after restore.	You can still download shared files by copying the link address and pasting it in the different web browser tab.

Glossary

- **Backup Destination** - backup provider or storage space holding backups on Data Protector for Cloud Workloads Node where backup files are copied to from **Staging Space** - default and the only currently supported is PowerProtect DD via Boost FS
- **Backup SLAs** - are responsible for the automation of backups of Virtual Environments or Storage instances. Backup SLA consists of the **policy** and **schedule**.
- **Cluster** - corresponds to server pools/clusters/availability zones that have been detected during inventory synchronization of **Hypervisors**
- **Hypervisors** - a list of hypervisors automatically discovered during inventory synchronization of **Hypervisor Manager** or manually added to Data Protector for Cloud Workloads
- **Hypervisor Managers** - a list of hypervisors managers added to Data Protector for Cloud Workloads.
- **Instances** - a list of currently known virtual machines/storage.
- **Inventory synchronization** - a task that index the contents of **Hypervisor Manager**, **Storage Provider,** or **Hypervisor** (if it's not managed by Hypervisor Manager)
- **Mounted backups** - a list of backups which has been mounted by Data Protector for Cloud Workloads and can be browsed.
- **Node** - machine or VM with installed Data Protector for Cloud Workloads Node, its main job is to execute a backup, restore, and mounting tasks. It should have access to the **backup destination** and **staging space**.
- **Node Configuration** - contains settings for nodes to describe their behavior during tasks execution such as maximum numbers of simultaneous backup tasks, timeouts, or **backup destinations** which can be used by nodes. One node configuration can be attached to many **nodes**.
- **Policy** - allow you to group virtual machines or storage instances. Each policy can have multiple **schedules** assigned.
- **Recovery Plans** - are used to automate the DR process, so that Data Protector for Cloud Workloads executes multiple restore operations to the target environment with preconfigured settings.
- **Schedule** - allow you to invoke specific policies periodically. This allows you to back up multiple VMs or storage instances automatically.
- **Snapshot SLAs** - are responsible for the automation of creating snapshots of Virtual Environments or storage instances. Backup SLA consists of the **policy** and **schedule**. The Instance has to be assigned to the **snapshot policy** in order to execute snapshot on demand.
- **Staging Space** - temporary space for backup files mounted on a Data Protector for Cloud Workloads Node; default and recommended configuration is shared space on a PowerProtect DD via Boost FS.
- **Storage** - corresponds to datastores/storage repositories/storage domains that have been detected during inventory synchronization of **Hypervisors**.
- **Storage Provider** - software storage platform that provides storage instances.