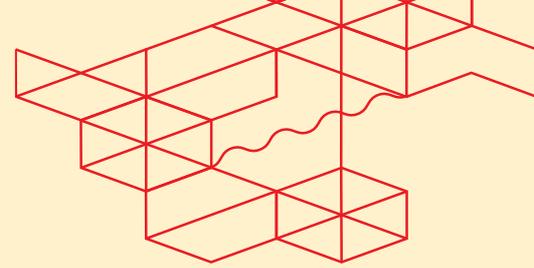


Managed Private Backup - User Guide

Version 1.1, April 2025

Contents

Managed Private Backup - User Guide	1
1. Introduction	2
2. Concepts	3
2.1 Equinix Customer Portal and Managed Solutions Portal	3
2.2 Operational Console	3
2.3 Organization	3
Tenant Admin	4
Tenant Users	4
3. Onboarding	5
4. User Management and SSO	6
4.1 User Management	6
4.2 Login To the Operational Console	6
4.3 Using a Different Identity Source	7
5. Use of the Operational Console	8
5.1 How to connect with the Managed Private Backup?	8
5.2 How to authenticate / log-in to Managed Private Backup	9
5.3 How to give someone else to use the operational console?	10
5.4 How to configure image level protection for MPC?	10
5.5 How to configure image level protection for Colocation (on-premises) environments (VMWare):	11
5.6 How to deploy agent level backups?	17
5.7 How to add paths to the agent backup policy?	38
5.8 How to include targets on the VM backup policy?	40
5.9 How to check if the backup job was finished successfully?	41
5.10 How to troubleshoot why the backup job has failed?	41
5.11 How to check how much data has been protected from one specific Server/instance?	42
5.12 How to run backup on demand?	42
5.13 How to run restore on demand?	43
Other documentations	46
Where to find Service Description?	46
Where to find EMS policy?	46
Where to find official Commvault documentation?	46
How to ask for help	46



1. Introduction

With Managed Private Backup (MPB) you have access to a scalable, secure, and reliable backup platform across the globe. MPB allows you to abstract hardware and software investments and remove the need for hardware lifecycle management and complex daily operations.

To keep it simple, MPB is ordered based on the amount of data you need protected (measured in terabytes). MPB helps you keep costs under control with a baseline commitment and allows you to backup volumes above your committed baseline if needed (overage charges applies).

You may select multiple combinations of retention periods and offsite protection options for each target (based on unique data sets) while maintaining data sovereignty for your workloads.

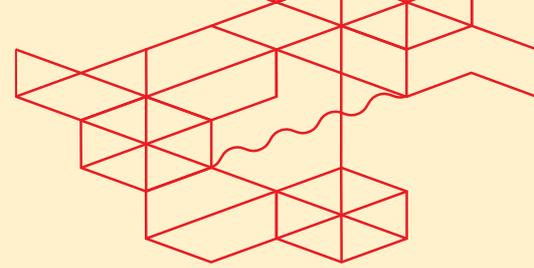
- You could protect up to 10TB of data with 30 days of retention and no offsite protection, plus.
- protect an additional 5TB of data with 5 years of retention and 5 years of offsite protection, plus.
- protect and additional 5TB of data with 10 years of retention and 10 years offsite protection.

Each combination is unique to your requirements.

MPB also provides high security standards and ransomware protection.

- Please note - Server size limitations for MPB are 10TB maximum per Virtual machine

Please refer to [MPB Service Description](#) for a full list of features and information.



2. Concepts

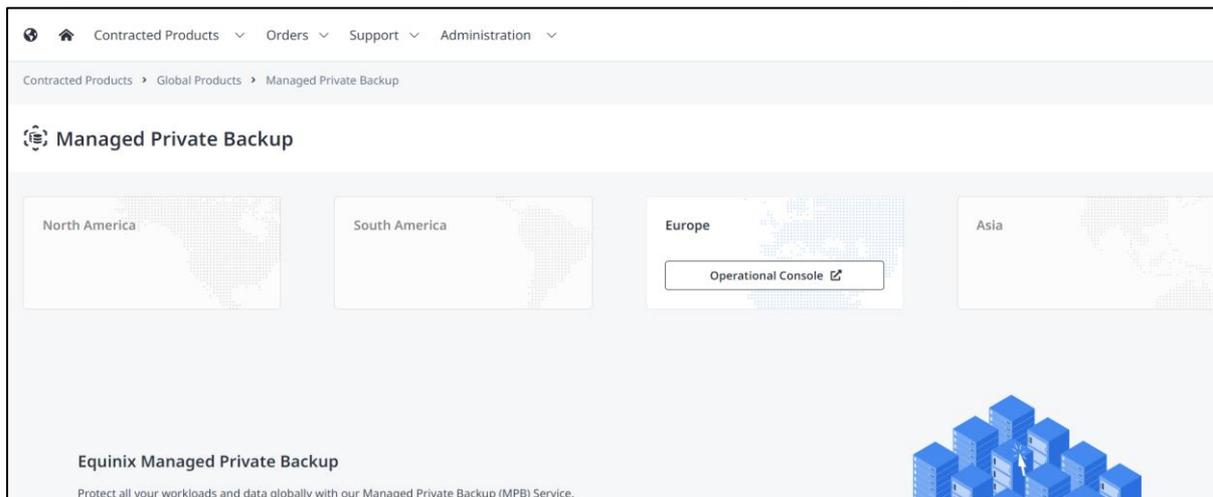
To gain a good understanding of the names and terms used later on in in this document, they will be explained first.

2.1 Equinix Customer Portal and Managed Solutions Portal

The Equinix Customer Portal (ECP) is the portal where the user management for the users who need access to the Operational console is performed. Part of the ECP is the Managed Solutions Portal (MSP) where you can raise tickets, services requests and get insights in the usage of the MPB service. On the ECP you will find the Product page where you can access the Operational Console.

2.2 Operational Console

The Operational Console is the portal where all the tasks for managing your MPB environment can be performed. The Operational Console gives you access to MPB in a certain region, MPB has four Regions, e.g. South America, North America, Europe and Asia. If you have an MPB in a specific region, the Operational Console will be accessible via one of the four buttons on the page.



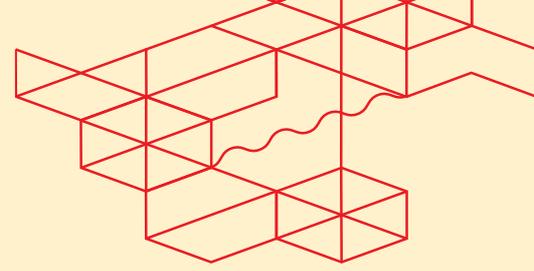
2.3 Organization

An Organization (Org) defines the customer within the Operational Console. The Org can be viewed as a container that groups together all MPB resources like backup volumes and retention settings located within an MPB region.

The name of the Org is needed when logging into the MPB Operational Console. Use the Org name when this quick start guide mentions “<organization name>”.

When Equinix performs the initial deployment for a new MPB customer, the first user that is configured is the customer administrator account. This account is created by Equinix during the onboarding process and is based on the name and email provided by the customer.

The first customer administrator account added is automatically added to the “Tenant Admin” group. Being a member of this group assigns the account all the permissions in the Operational Console.



EMS - Managed Private Backup User Guide – Release 1.1

Tenant Admin

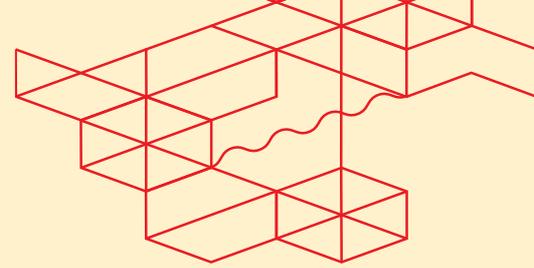
Permissions:

- Access MPB Console
- Create backup routines
- Perform on-demand backups
- Run restores
- Run Reports
- Monitor Alerts, events and Threats
- Create Tags
- Download and install backup agents

Tenant Users

Permissions:

- TBD

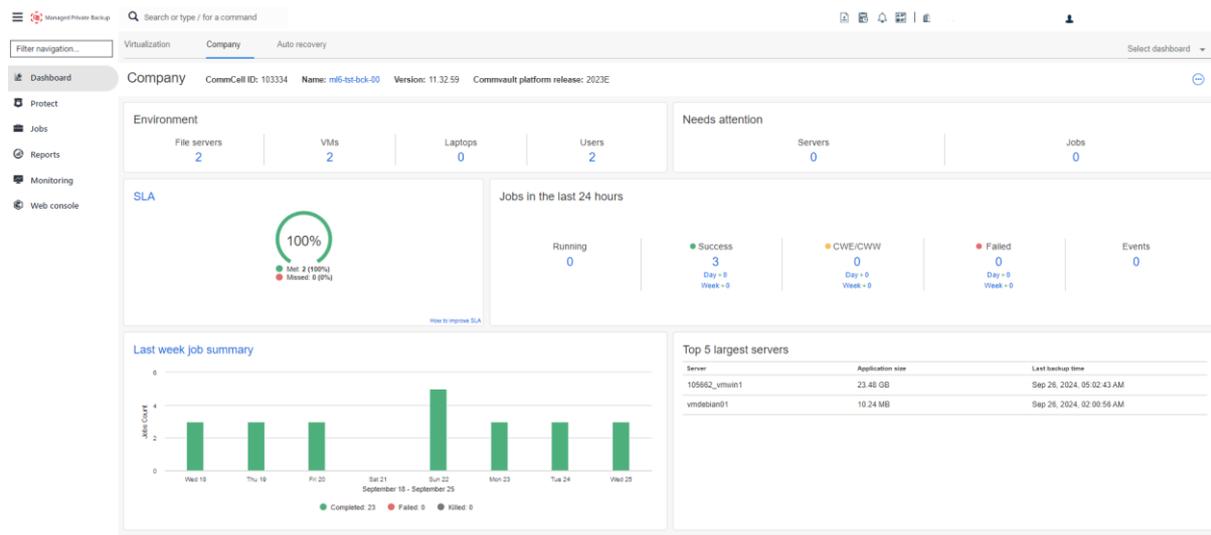


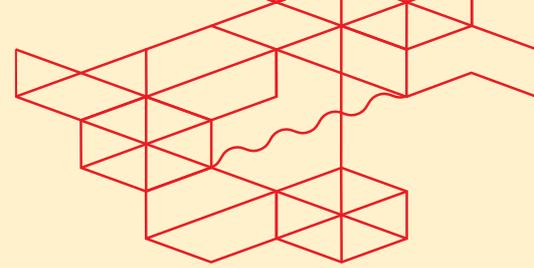
3. Onboarding

During the MPB onboarding process you receive the following information:

- Organization name
- One or more customer accounts with one of the above roles assigned
- The ordered volume of resources that are provisioned by region and by retention rules
- Authentication Code for performing installations

Figure 2: Example of MPB environment after onboarding

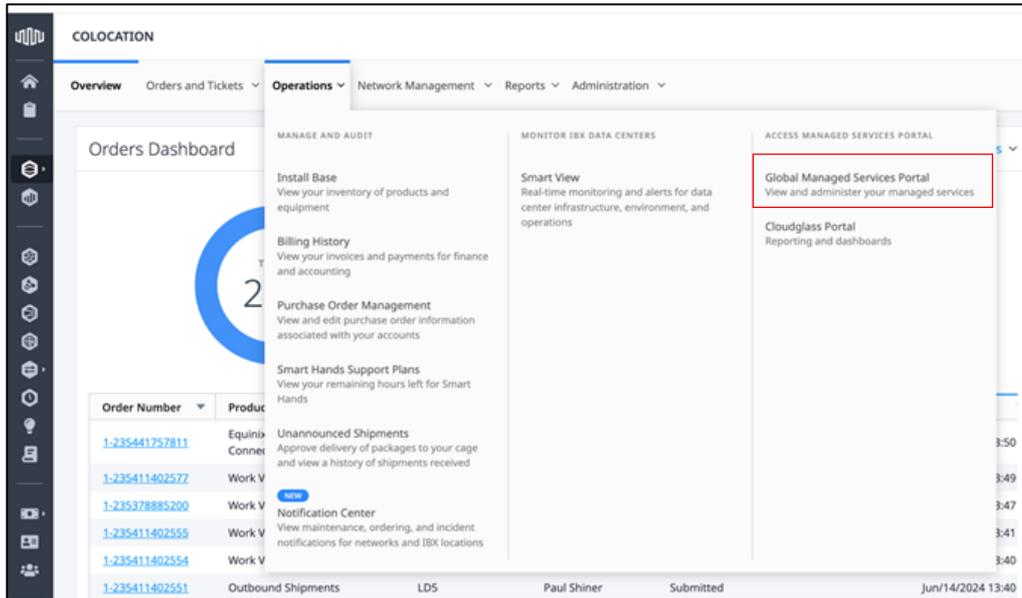




4. User Management and SSO

4.1 User Management

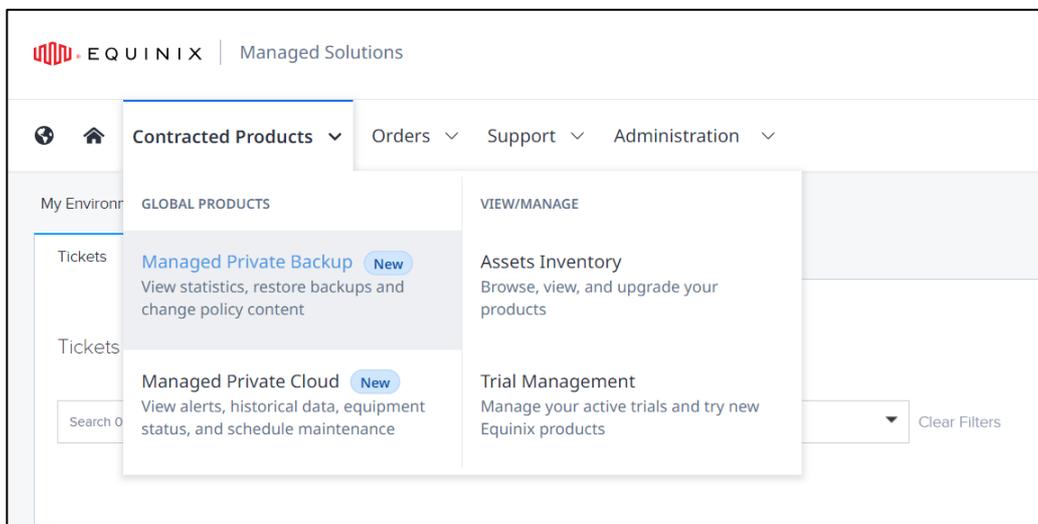
Users of the Operational Console are managed at the ECP, you can find the documentation on User Management and Password management at [the following link](#).

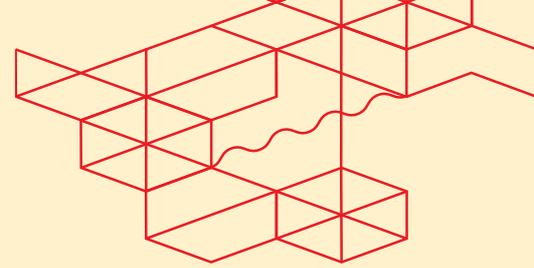


Once the users have been added to the ECP customer can raise a Service Request to assign a MPB Tenant role to the new user. Use the [link](#) to find the user guide for raising a service request in the Managed Solutions Portal.

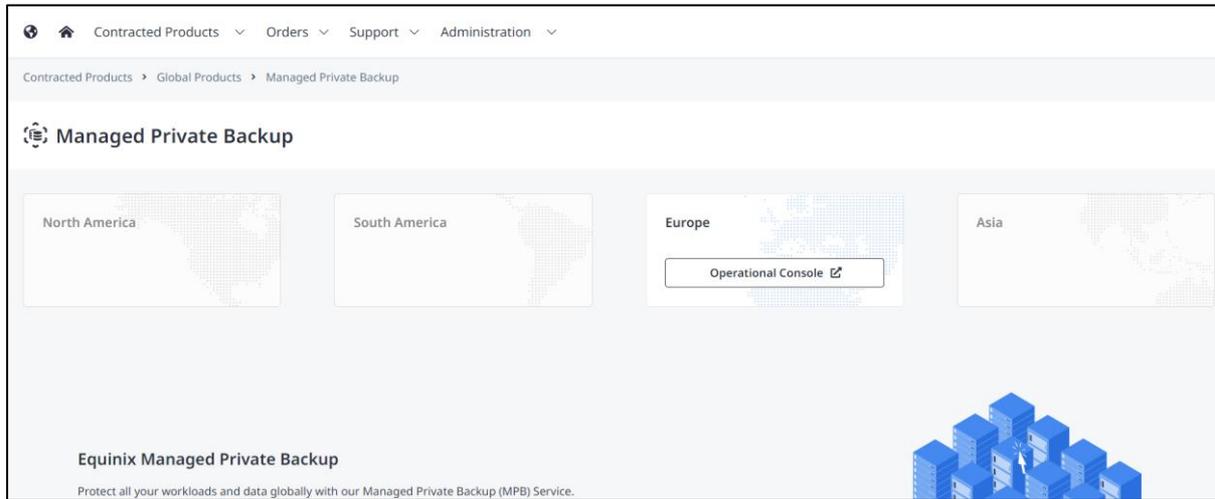
4.2 Login To the Operational Console

When logged into the ECP you navigate to the product page via the Managed Solutions Portal/ Services/ Managed Private Cloud from here you can login to the Operational Console in the region of your choice.





EMS - Managed Private Backup User Guide – Release 1.1



When you access direct from the URL of the Operational Console and click “Sign In”, you will be redirected to ECP where you can enter your ECP credentials.

Sign In

Equinix Portal

Username or Email Address

Password

Sign In

[Reset Password](#)

[Retrieve Your Username](#)

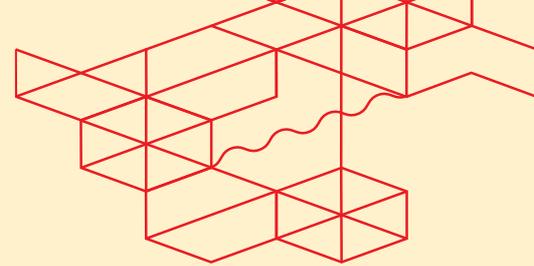
[Sign In Help](#)

or

Sign In with SSO

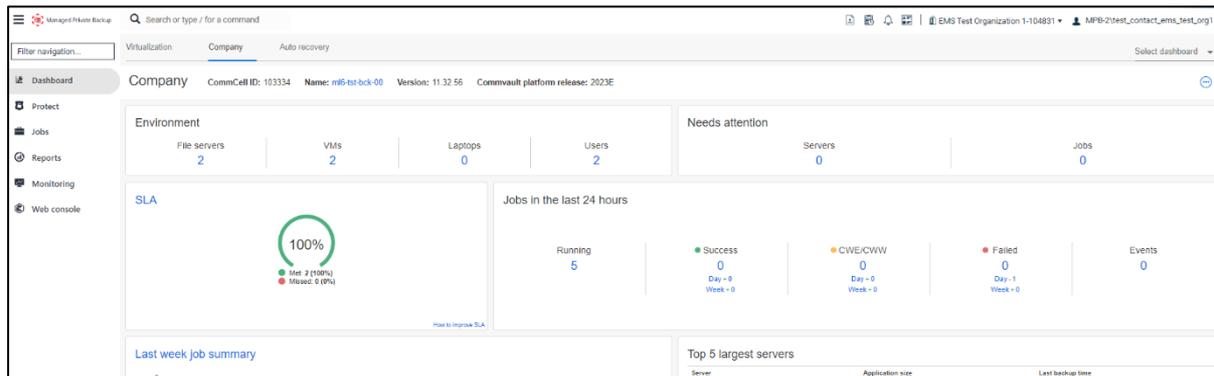
4.3 Using a Different Identity Source

In the ECP you can configure federation to your own identity provider so you can use your company credentials to login to the Operational Console, you can find the instructions about federation at docs.equinix.com



5. Use of the Operational Console

The MPB operational console looks like this:



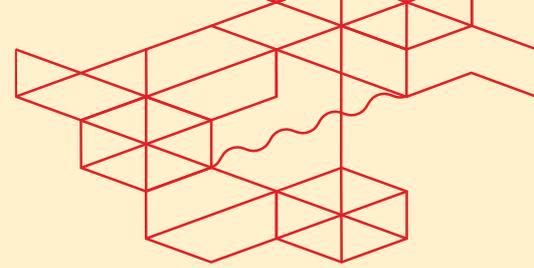
On the left menu, you will find links to:

- **The start dashboard:** where you may find overall up to date information about your backup situation, including how many servers or virtual machines are being protected and the status of the previous backup jobs.
- **Protect:** this is where you may map servers or instances to be protected.
 - **Virtualization:** virtual machines/ instances you may have mapped to protect with image level backup
 - **File Servers:** that you may have mapped to protect with agent-level backups.
 - **Databases:** that you may have mapped to protect with specific database agent technology
- **Jobs:** this is where you will find the current active jobs and the backup history.
- **Reports:** on this section, we provide information generated by the Commvault solution about the reliability of the backup solution in place and its effectiveness.
 - **Please note the SLA demonstrated here is not the current SLA agreed to when subscribing to the MPB Service.**
- **Monitoring:**
 - **Events:** will show you some technical information logs that may help you or your team to troubleshoot
 - **Unusual file activities:** will list some atypical behaviors that may be associated with security threats or ransomware. This is not a replacement of your antivirus or security software but may help you to prevent threats to your protected data.
- **Download center:** here you will find your agent packages to download and install on your servers that need to be protected with agents.

5.1 How to connect with the Managed Private Backup?

Please remember that you need to subscribe to MPB for each location (IBX) where you need to protect data.

If for instance you have ordered Managed Private Cloud in Chicago (CH3) IBX, you will need to order



EMS - Managed Private Backup User Guide – Release 1.1

MPB in CH3 to protect data that resides there. This gives us the ability to help you with governance requirements, such as sovereignty rules.

5.1.1 Image-level Protection

Image level protection allows MPB to connect at the hypervisor layer of our Managed Private Cloud product or a Hypervisor (currently VMWare and Hyper-V, other technologies in the future) and execute snapshot backups. This allows for quicker restores of complete virtual machines for Disaster Recovery purposes.

If you are a MPC customer, all the connectivity needed for image-level protection has already been deployed by the Equinix team at this point.

5.1.2 Agent-level protection

To improve your experience with protection and restore activities, some workloads have specific agents that allow you to execute a more detail-oriented protection.

The available agent-level protection on MPB are:

- **File server agents (Windows, Linux and AIX):** this agent allows you to protect individual folders and files, allowing you to restore more granular information.
- **Database agents:** these agents allow you to protect individual databases and allow you to restore more granular information, such as a table.
 - Microsoft SQL Server agent
 - Oracle Database agent
 - MySQL Database agent
 - PostgreSQL Database agent
 - IBM DB2 Database agent

To be able to connect to individual instances or virtual machines, you need to make sure the following connectivity can be established.

5.1.3 Ports used by MPB to protect your environment

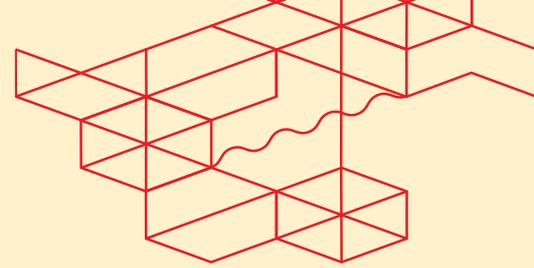
Specific TCP ports should be open from each target (server) to the MPB Service

- TCP 443 (from customer to backup infrastructure – please use the address informed to you during the fulfillment process)
- TCP 8400 to 8499 ports (bi-directional)
- Equinix Fabric connection for colocation customers.

5.2 How to authenticate / log-in to Managed Private Backup

To have access to the Managed Private Backup service, you should use the same credentials used to connect to Equinix Customer Portal. If you or someone of your team does not have access yet to ECP, ask about it with your primary contact with Equinix.

Please do not share your personal credentials with other members of your team. This violates the Acceptable Use Code for Equinix products and creates a lack of control and other security issues for your data.



EMS - Managed Private Backup User Guide – Release 1.1

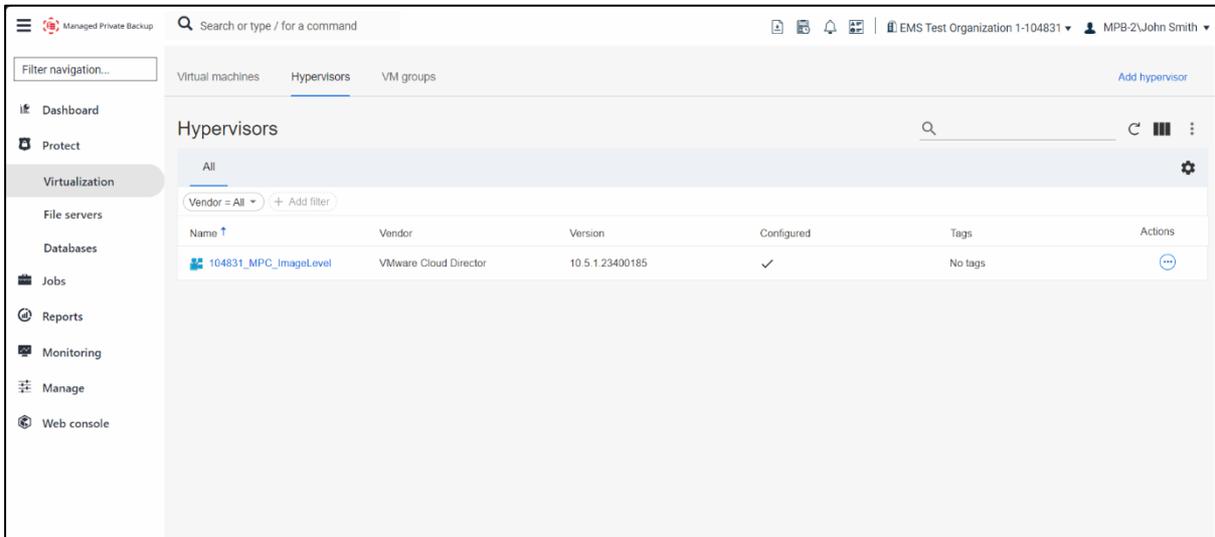
To find the current Operational Console URL address, please use the product page inside the Managed Services Portal. If you opt to save a previously used URL address to your browser bookmark, you may face difficulties to find the service in the future if the URL is changed in the back end.

5.3 How to give someone else to use the operational console?

In you need to give permission to someone else to access the MPB Service, you will need to first, request access for this person to the Equinix Customer Portal and then open a ticket to give this person the appropriate permissions to access the MPB. You will find an option called “Create user in Operational Console” in the service catalog.

5.4 How to configure image level protection for MPC?

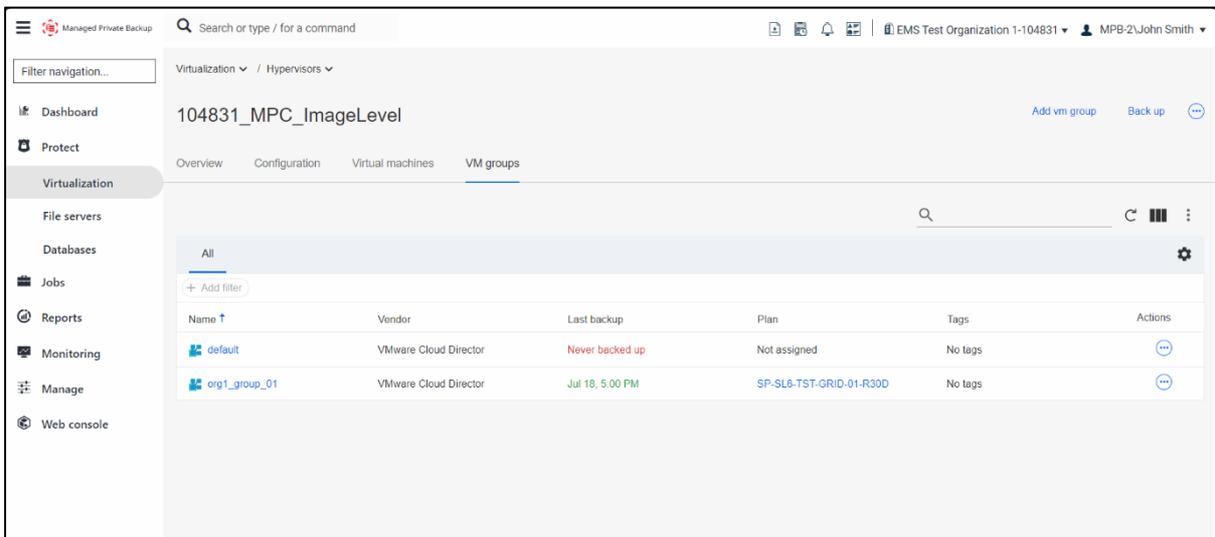
As informed before, all the connectivity required to protect MPC at an image level should already be in place to start with this protection. Once ready, you will find the access pre-configured as this:



The screenshot shows the Equinix Managed Private Backup console interface. The left sidebar contains navigation options: Dashboard, Protect, Virtualization (selected), File servers, Databases, Jobs, Reports, Monitoring, Manage, and Web console. The main content area is titled 'Hypervisors' and shows a table with the following data:

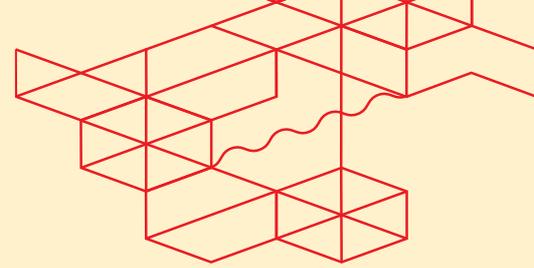
Name	Vendor	Version	Configured	Tags	Actions
104831_MPC_ImageLevel	VMware Cloud Director	10.5.1.23400185	✓	No tags	⋮

Then, you will be able to see your **Virtual Machine Groups** on the VM Groups tab:



The screenshot shows the Equinix Managed Private Backup console interface with the 'VM groups' tab selected. The main content area is titled '104831_MPC_ImageLevel' and shows a table with the following data:

Name	Vendor	Last backup	Plan	Tags	Actions
default	VMware Cloud Director	Never backed up	Not assigned	No tags	⋮
org1_group_01	VMware Cloud Director	Jul 18, 5:00 PM	SP-SL6-TST-GRID-01-R30D	No tags	⋮

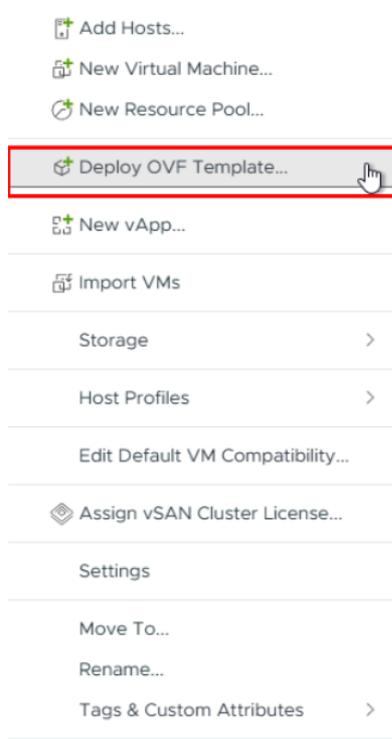


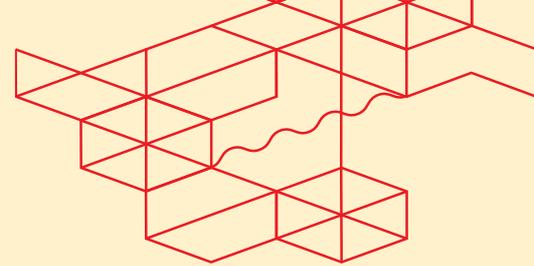
Please note that on this example the org1_group_01 vmgroup has a specific backup policy applied: in this case **30 days of retention without offsite protection**. This entry is also referring to the proxy server. You will receive IP address and FQDN for the proxy server.

5.5 How to configure image level protection for Colocation (on-premises) environments (VMWare):

5.5.1 Install a VSA Commvault on version 11.36

After downloading the .ova from Download center on MPB Console, deploy it on the vCenter:





EMS - Managed Private Backup User Guide – Release 1.1

Right click the vApp where the VM Appliance will be placed, then choose **Deploy OVF Template**

Deploy OVF Template

- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 Select storage
- 6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

⚠ Select a template to deploy. Use multiple selection to select all the files associated with an OVF template (.ovf, .vmdk, etc.)
✕

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

URL

http | https://remoteserver-address/filetodeploy.ovf | .ova

Local file

UPLOAD FILES

No files selected.

CANCEL
NEXT

Select an OVF template from your machine and click **UPLOAD FILES** then **Next**

Deploy OVF Template

- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 Select storage
- 6 Ready to complete

Select a name and folder

Specify a unique name and target location

Virtual machine name: Virtual Appliance Name

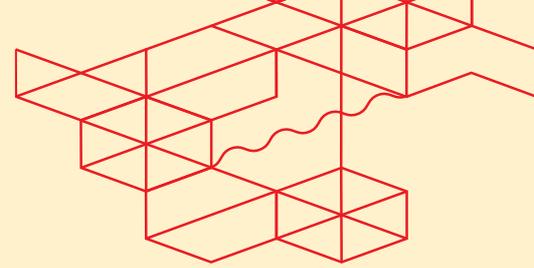
Select a location for the virtual machine.

- ▼ [icon]
- ▼ [icon] Discovers virtual machine
- ▼ [icon] ESX Agents
- ▼ [icon] INFRA
- ▼ [icon] MPB
- ▼ [icon] Backup
- ▼ [icon] Commvault Data
- ▼ [icon] Commvault Mgmt
- ▼ [icon] Commvault Proxy
- ▼ [icon] MPC
- ▼ [icon] MPF

Customize this virtual machine's hardware

CANCEL
BACK
NEXT

Select the Display VM Name and location


EMS - Managed Private Backup User Guide – Release 1.1

Deploy OVF Template

- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 Select storage
- 6 Ready to complete

Select a compute resource

Select the destination compute resource for this operation

- ▼ [Icon] MAINTENANCE
 - [Icon] Cluster Name
 - [Icon] Node A
 - [Icon] Node B
 - [Icon] Node C
 - [Icon] Node D
 - [Icon] Node E
 - [Icon]
 - [Icon]
 - [Icon]
- > [Icon] ESX Agents

Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

Select the Adequate Compute Resource

Deploy OVF Template

- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 Configuration
- 6 Select storage
- 7 Select networks
- 8 Customize template
- 9 Ready to complete

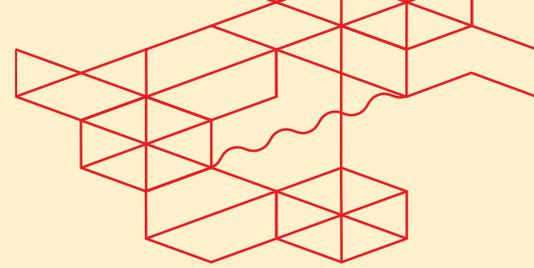
Review details

Verify the template details.

Publisher	No certificate present
Product	Commvault Access Node
Version	2.0.1
Vendor	Commvault
Download size	3.4 GB
Size on disk	4.3 GB (thin provisioned) 337.0 GB (thick provisioned)

CANCEL BACK NEXT

Hit Next



EMS - Managed Private Backup User Guide – Release 1.1

Deploy OVF Template

- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 Configuration
- 6 Select storage
- 7 Select networks
- 8 Customize template
- 9 Ready to complete

Configuration

Select a deployment configuration

- Extra Small 50TB BETB
- Small 100TB BETB
- Medium 150TB BETB
- Large 300TB BETB
- Extra Large 500TB BETB

Description
8 vCPUs, 32 GB memory, 37GB OS disk, 400GB Data Disk 1, 300GB Data Disk 2

5 Items

CANCEL BACK NEXT

Select the resources for the VSA accordingly to your environment BackEnd TB.

Deploy OVF Template

- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 Configuration
- 6 Select storage
- 7 Select networks
- 8 Customize template
- 9 Ready to complete

Select storage

Select the storage for the configuration and disk files

Encrypt this virtual machine (Requires Key Management Server)

Select virtual disk format As defined in the VM storage policy ▾

VM Storage Policy vSAN Default Storage Policy ▾

Disable Storage DRS for this virtual machine

Name	Storage Compatibility	Capacity	Provisioned	Free
Disk Pool	Compatible	62.88 TB	34.95 TB	53.43 TB

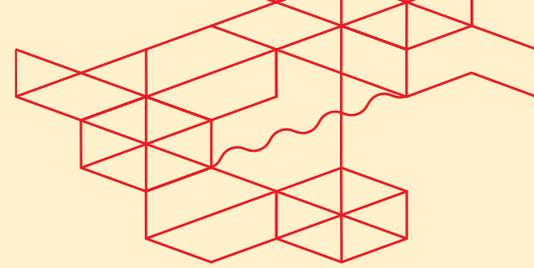
Manage Columns Items per page 10 ▾ 1 item

Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

Select the designated Storage, is important that the policy is configured with thin provisioning



EMS - Managed Private Backup User Guide – Release 1.1

Deploy OVF Template

- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 Configuration
- 6 Select storage
- 7 Select networks
- 8 Customize template
- 9 Ready to complete

Select networks

Select a destination network for each source network.

Source Network	Destination Network
VM Network	VM Network Identifier v
1 item	

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

CANCEL
BACK
NEXT

Select All the networks needed to talk to MPB assets and vCenter Server

Set the disks size, IP address for the Gateway and Client Name

Deploy OVF Template

- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 Configuration
- 6 Select storage
- 7 Select networks
- 8 Customize template
- 9 Ready to complete

Customize template

Customize the deployment properties of this software solution.

ⓘ 1 property has an invalid value x

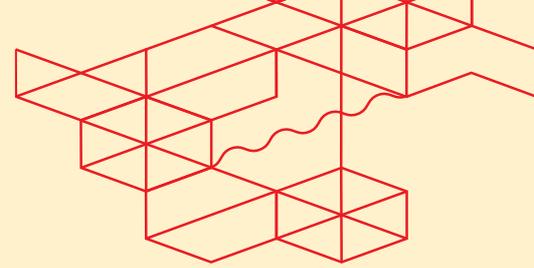
Disk Size Configuration 2 settings

Software installation disk size (GB)	200
Deduplication storage disk size (GB)	100

Client Configuration 5 settings

CS/Network gateway hostname	The CS/network gateway hostname:port IP of the Network Proxy
Auth Code (required)	<input type="text"/>
Client Name (required)	Proxy Display Name
Client Hostname	<input type="text"/>
Client Group name	<input type="text"/>

CANCEL
BACK
NEXT



EMS - Managed Private Backup User Guide – Release 1.1

Choose and IP Address, NetMask, Gateway and DNS for this VSA Proxy

Deploy OVF Template

- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 Configuration
- 6 Select storage
- 7 Select networks
- 8 Customize template
- 9 Ready to complete

Customize template

Client Group name _____

Networking 7 settings

Use DHCP? Please uncheck for static IP address

IP Address (leave default for DHCP) 10.38.22.90

Netmask (leave default for DHCP) 255.255.255.0

Gateway (leave default for DHCP) 10.38.22.1

DNS Search Suffix (leave default for DHCP) Comma separated DNS domain names

Primary DNS Server (leave default for DHCP) 10.37.0.10

Secondary DNS Server (leave default for DHCP) 10.37.0.11

OS Configuration 1 settings

Password for 'root' user (required)

CANCEL
BACK
NEXT

Leave the username blank as the AuthCode will be used.

Deploy OVF Template

- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 Configuration
- 6 Select storage
- 7 Select networks
- 8 Customize template
- 9 Ready to complete

Customize template

Secondary DNS Server (leave default for DHCP) 10.37.0.11

OS Configuration 1 settings

Password for 'root' user (required)

Password 👁

Confirm Password 👁

Advanced Configuration 5 settings

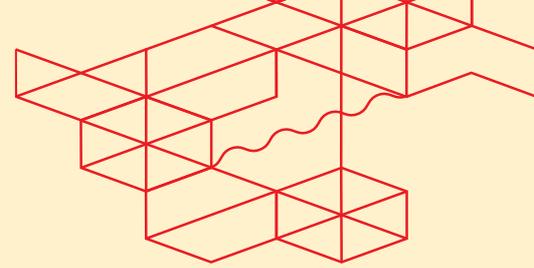
CS Username (leave blank if authcode is being used) admin

CS Password (leave blank if authcode is being used)

Password 👁

Confirm Password 👁

CANCEL
BACK
NEXT



EMS - Managed Private Backup User Guide – Release 1.1

Deploy OVF Template

- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 Configuration
- 6 Select storage
- 7 Select networks
- 8 Customize template**
- 9 Ready to complete

Customize template

Confirm Password

Advanced Configuration 5 settings

CS Username (leave blank if authcode is being used)	<input type="text" value="admin"/>
CS Password (leave blank if authcode is being used)	Password <input type="password" value="....."/>
	Confirm Password <input type="password" value="....."/>
Additional Route Configuration	IP route configuration in the format (0.0.0.0/0,0.0.0.0) <input type="text" value="0.0.0.0/0,0.0.0.0"/>
Linux Timezone	Enter the Linux OS qualified timezone <input type="text"/>
NTP server hostname	<input type="text"/>

CANCEL
BACK
NEXT

Customize with:

- Select the size of the disk, we need to decrease it as much as possible
- Network Gateway Proxy Hostname/IP - IP or FQDN
- Client Name - name that will be displayed on the MPB Console
- IP addresses, network mask, Gateway and DNS (when applicable) according to the region
- Root password for the OS of the Proxy
- Leave Password Blank to use Authcode

After installing it, you'll need to log-in the Proxy Server, and edit the hosts file and configure naming entries as below (address will be provided during onboard session):

```

root@debian:/# cat /etc/hosts
127.0.0.1    localhost
10.21.0.10  debian

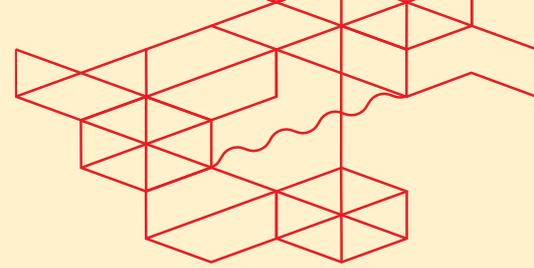
# The following lines are desirable for IPv6 capable hosts
::1        localhost ip6-localhost ip6-loopback
ff02::1    ip6-allnodes
ff02::2    ip6-allrouters
172.16.0.2    sl6-182391296-bng-02.tst-eu.equinixms.com sl6-182391296-bng-02
root@debian:/#
  
```

5.6 How to deploy agent level backups?

In the case where an agent backup is needed, you will need to download and install the agent files on the target file server or database server. To be able to do that, we will provide some detail information during the shadow session. The download is available in the MPB Console, under Download center.

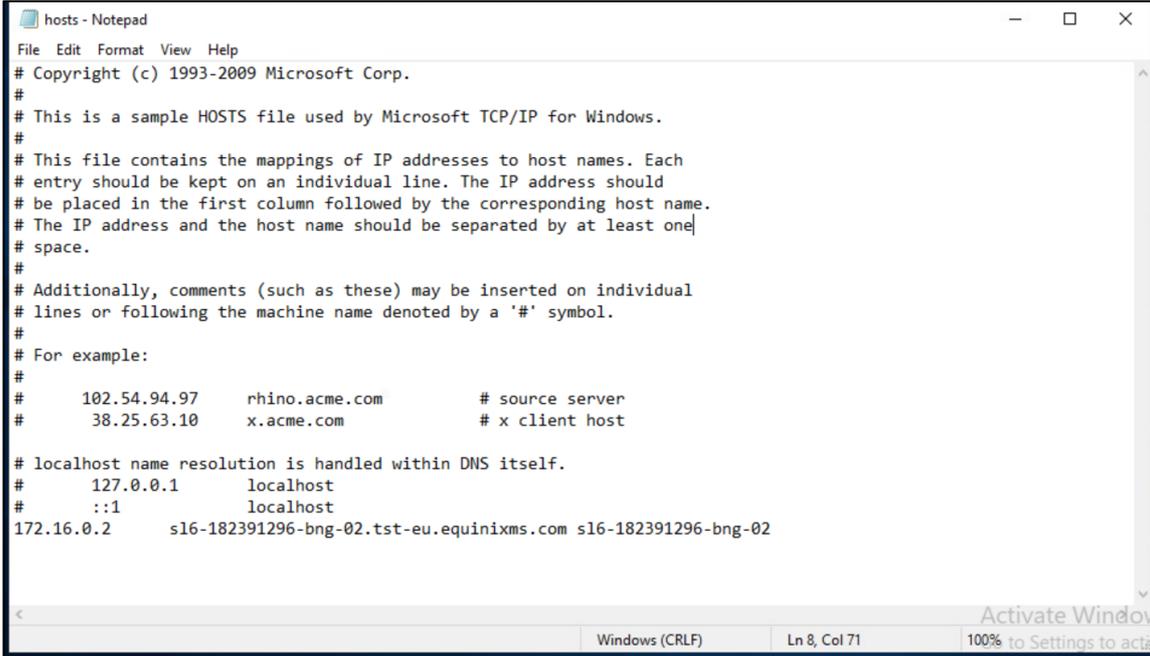
5.6.1 Add naming entries manually

The first step is to go to you server/virtual machine and configure naming entries as below (address will be provided during onboard session):



EMS - Managed Private Backup User Guide – Release 1.1

For Windows Operating System, add entry in HOSTS configuration file:



```

hosts - Notepad
File Edit Format View Help
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com           # source server
#       38.25.63.10      x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1        localhost
#       ::1             localhost
172.16.0.2      s16-182391296-bng-02.tst-eu.equinixms.com s16-182391296-bng-02
    
```

For GNU/Linux/AIX operating system, add entry in /etc/hosts file:

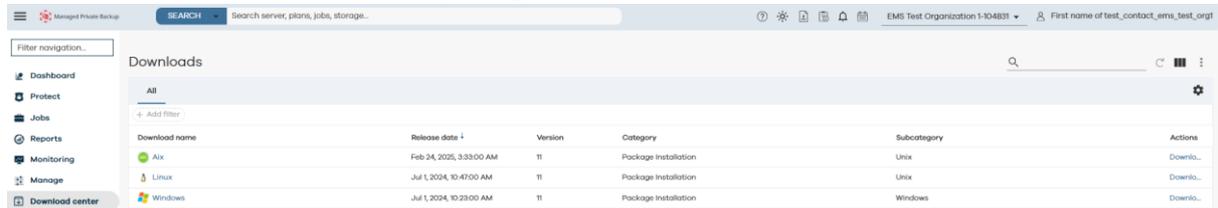
```

root@debian:/# cat /etc/hosts
127.0.0.1      localhost
10.21.0.10    debian

# The following lines are desirable for IPv6 capable hosts
::1          localhost ip6-localhost ip6-loopback
ff02::1     ip6-allnodes
ff02::2     ip6-allrouters
172.16.0.2   s16-182391296-bng-02.tst-eu.equinixms.com s16-182391296-bng-02
root@debian:/#
    
```

5.6.2 Package download

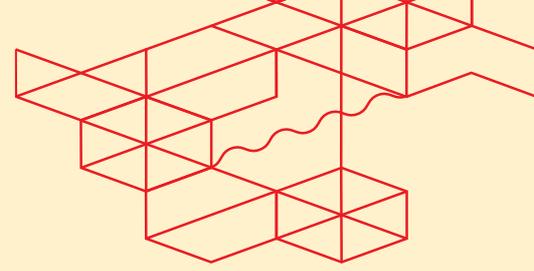
Then you'll be able to download the packages needed from the MPB operational console:



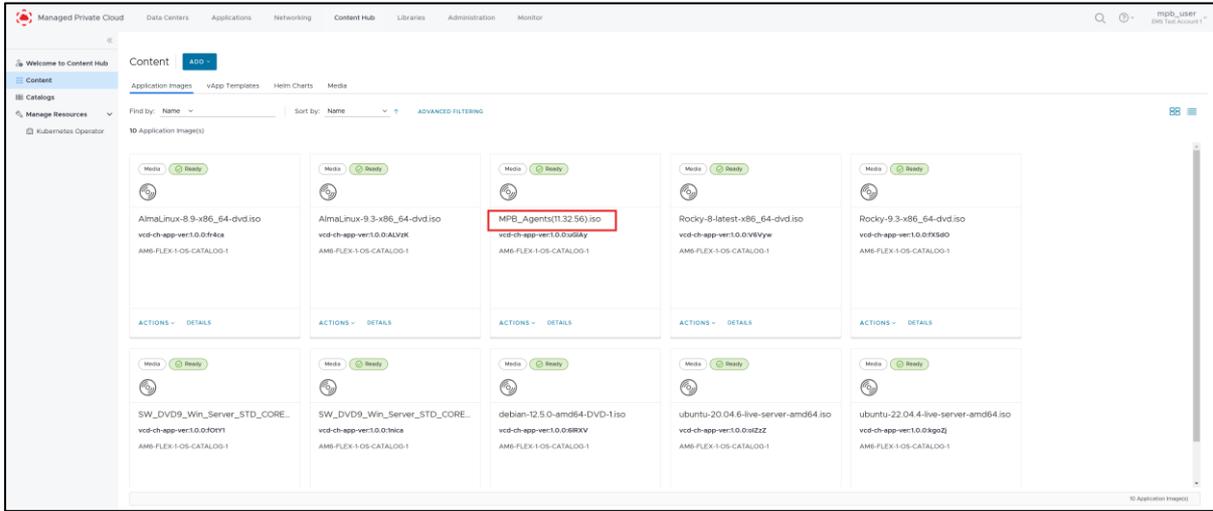
Download name	Release date	Version	Category	Subcategory	Actions
Aix	Feb 24, 2025, 3:33:00 AM	11	Package Installation	Unix	Download
Linux	Jul 1, 2024, 10:47:00 AM	11	Package Installation	Unix	Download
Windows	Jul 1, 2024, 10:23:00 AM	11	Package Installation	Windows	Download

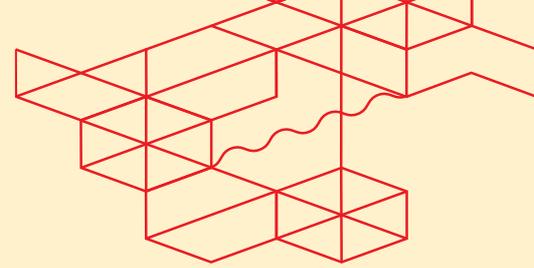
Please download the respective package from this page and execute the installation on your server (you do not need to download all packages, just those you need).

In case you are installing an agent for MPC virtual machines, you may also mount the installation ISO from the VCD content hub as showed below:



EMS - Managed Private Backup User Guide – Release 1.1





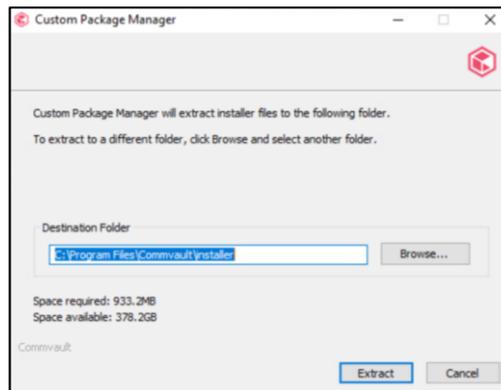
EMS - Managed Private Backup User Guide – Release 1.1

5.6.3 Agent installation steps

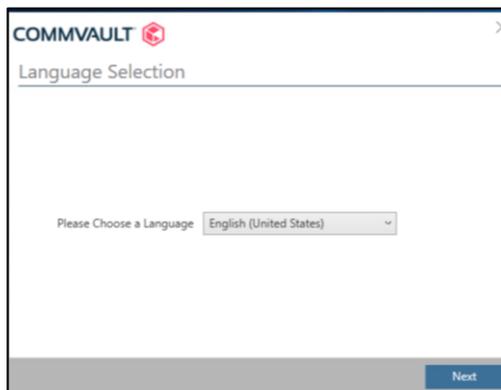
For Windows based systems (File System or MS-SQL Server agent)

Please run the .exe file.

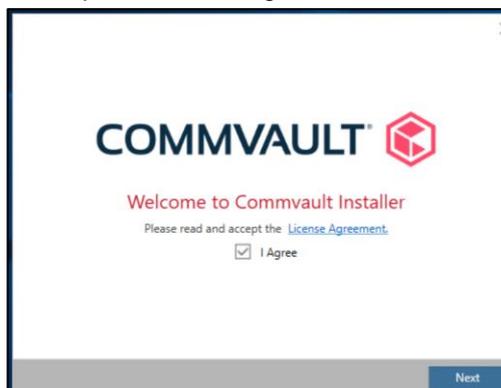
Extract it

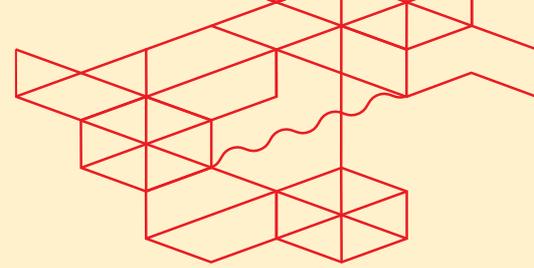


Choose a Language



If you want, please read and accept the license agreement, then select I agree





EMS - Managed Private Backup User Guide – Release 1.1

Select to install the packages on this computer



Choose Advanced selection

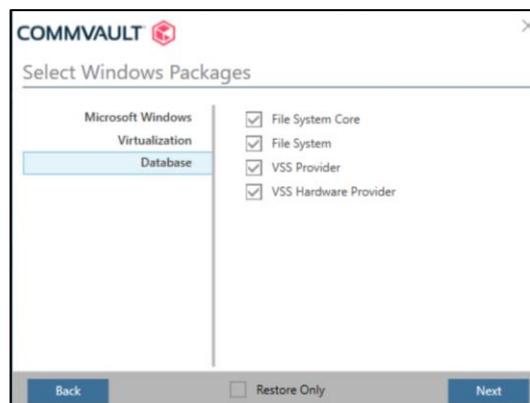


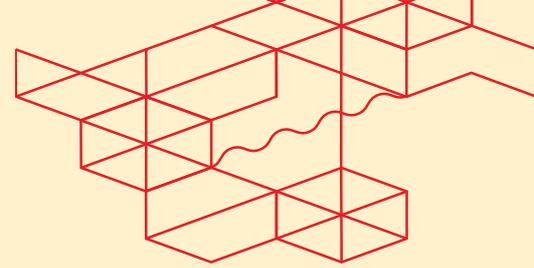
Select the desired packages

File System Core + File System for File System backups

VSS Provider + VSS Hardware Provider + Virtual Server for VSA Proxy or Hyper-V Backups

MS-SQL Server for Databases



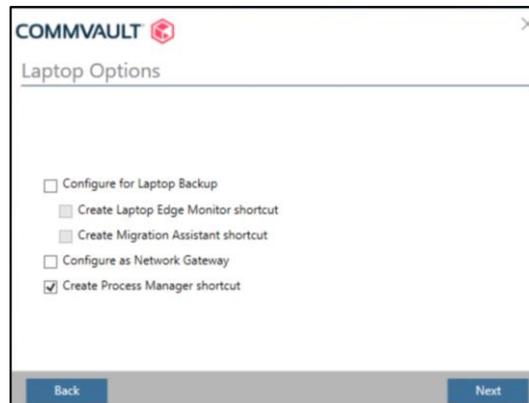


EMS - Managed Private Backup User Guide – Release 1.1

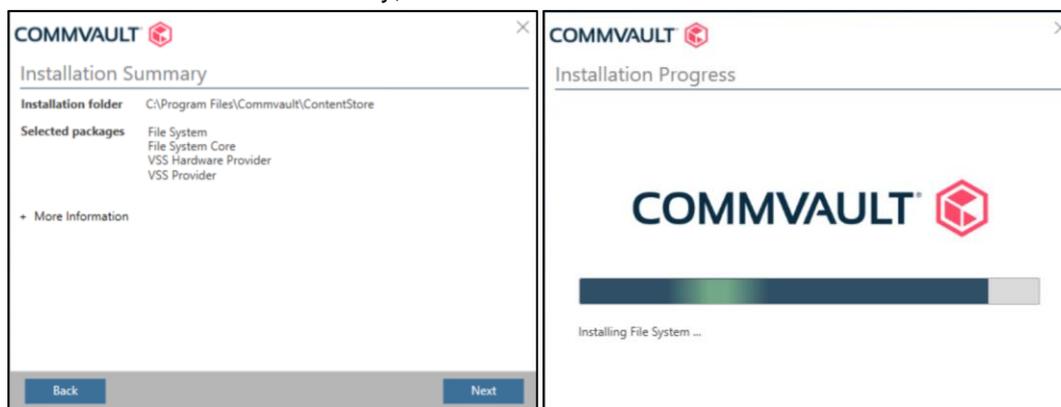
Choose the installation path (default is C:\Program Files\Commvault\ContentStore)

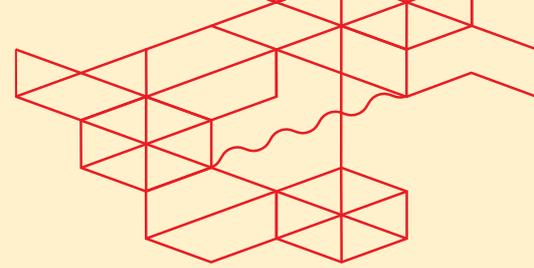


If you are unsure, please, leave those options as default



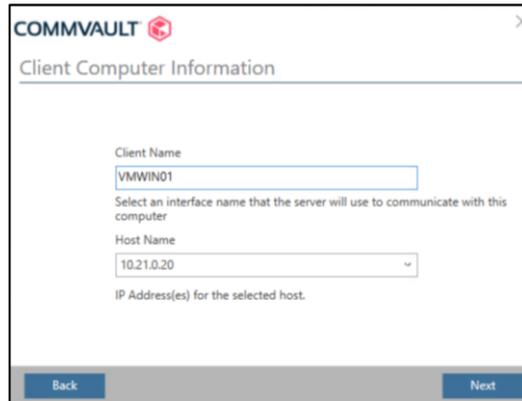
Review the installation Summary, then hit Next



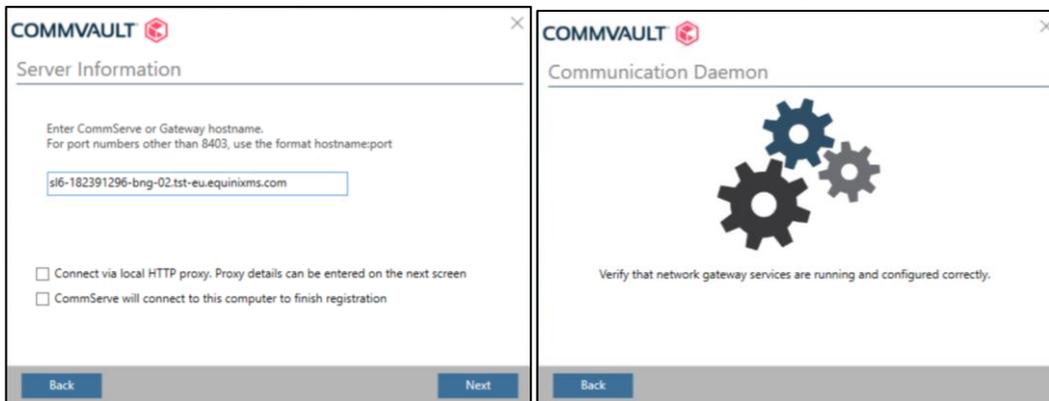


EMS - Managed Private Backup User Guide – Release 1.1

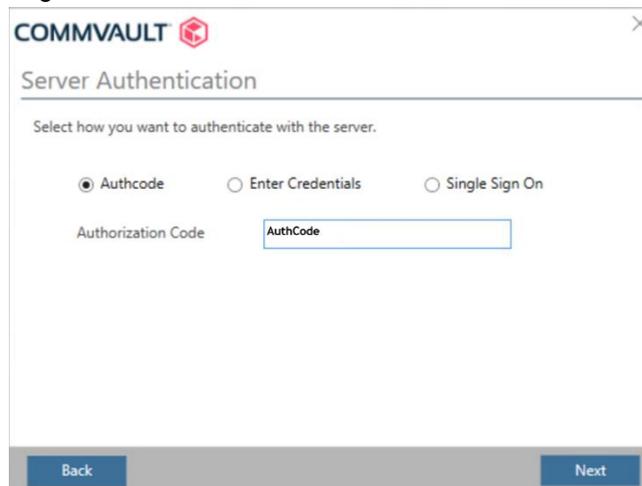
Select the Client Name (which will be displayed on MPB Console) and the IP interface (Host Name) where the backup traffic will transit.

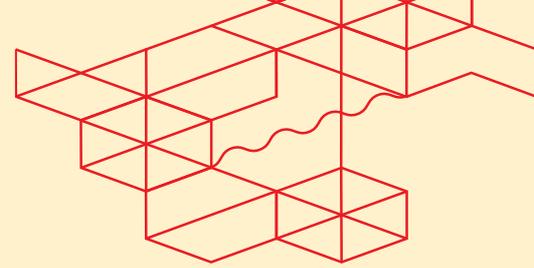


Enter Network Gateway Proxy Address (the same inserted in step 2.6.1)



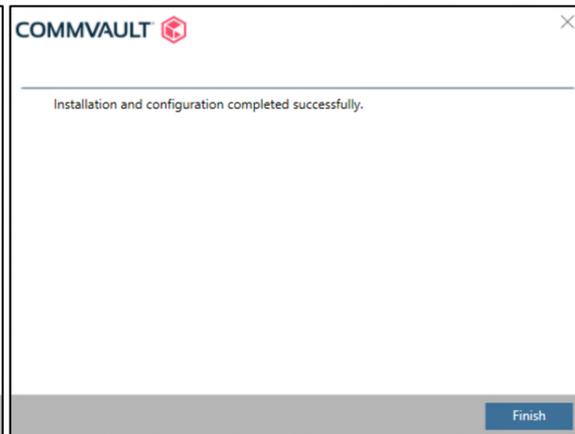
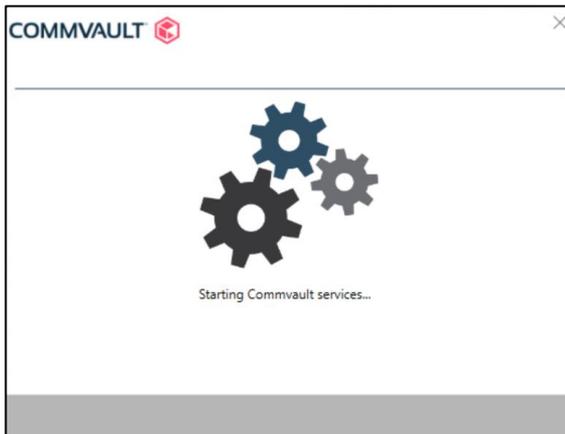
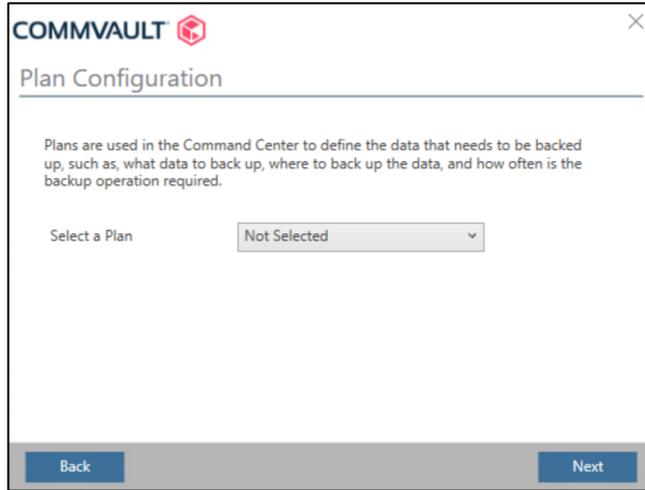
Once the installation begins, you will need AuthCode provided during the shadow session to correctly configure the agent.





EMS - Managed Private Backup User Guide – Release 1.1

You may use this opportunity to choose the protection plan for this virtual machine/server:



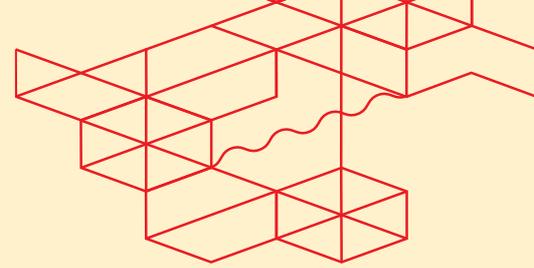
For GNU/Linux/AIX

Extract the .tar file, then, in the extracted folder, run the following command:

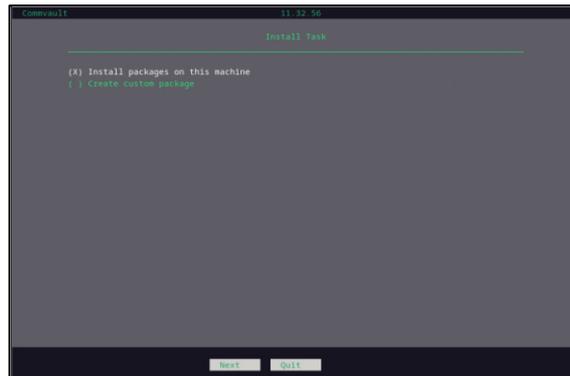
`./cvpkgadd`

```
root@debian:/tmp/Unix# ls
Commvault.app.xml  cvpkgseed  linux-x86  pkgsinmedia.txt  pkg.xml.description  support
cvpkgadd           detect     linux-x8664  pkg.xml          silent_install      version
root@debian:/tmp/Unix# ./cvpkgadd █
```

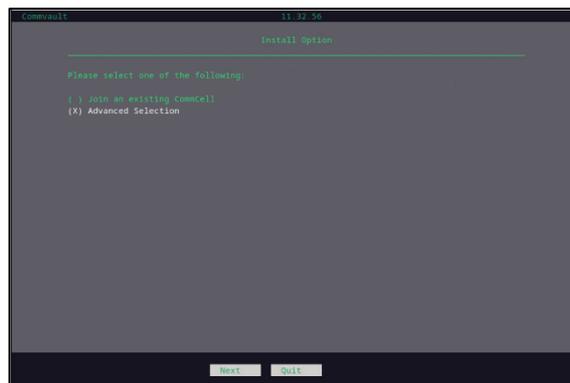




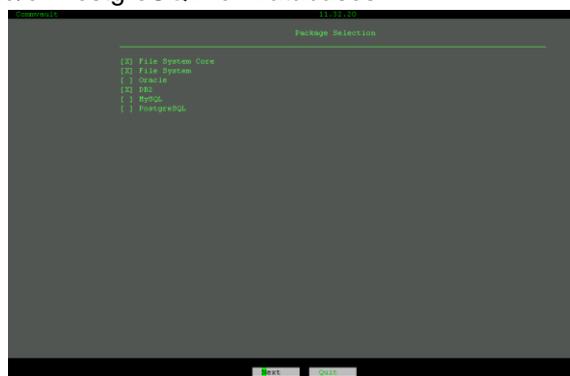
Select packages on this machine

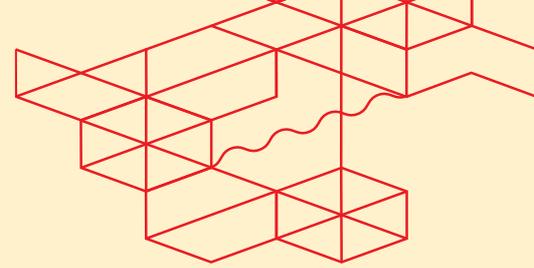


Select Advanced Selection



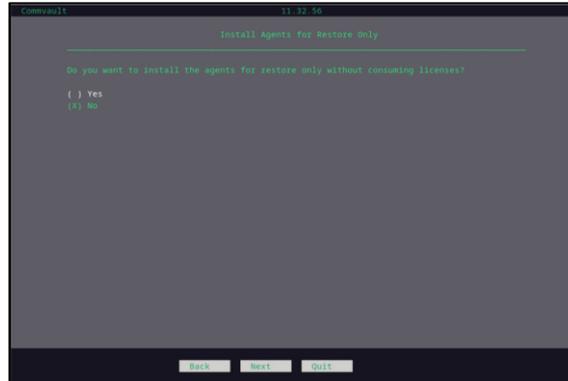
Select the packages that you desire installation
File System Core + File System for File System backups
Virtual Server for VSA Proxy
Oracle, MySQL, DB2 and/or PostgreSQL for Databases





EMS - Managed Private Backup User Guide – Release 1.1

Select No for install agents for restore only (this kind of agent doesn't perform backups).

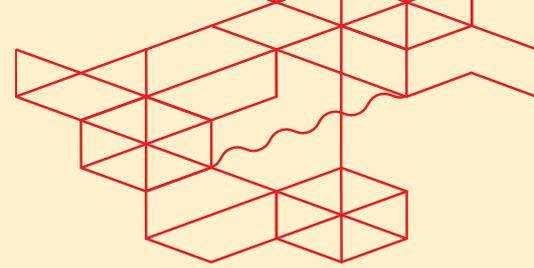


Select the install path (default is `/opt`)



Select the Log Directory (default is `/var/log`)





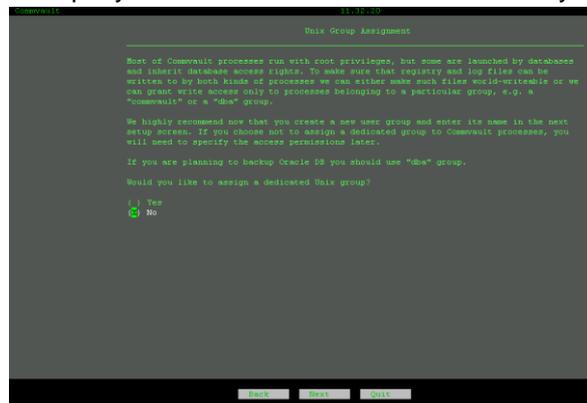
EMS - Managed Private Backup User Guide – Release 1.1

Select no for software for laptop or desktop backups

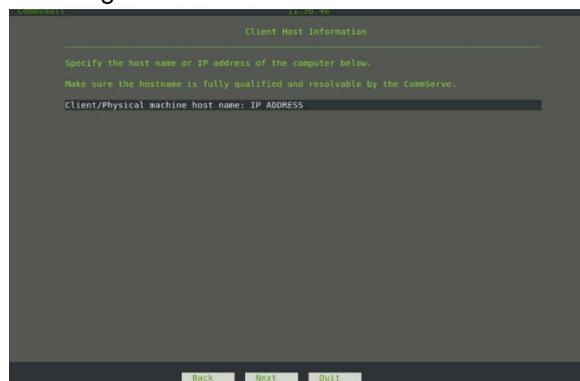


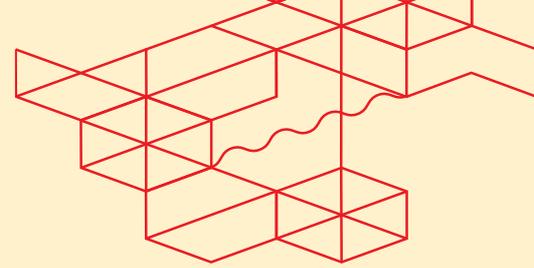
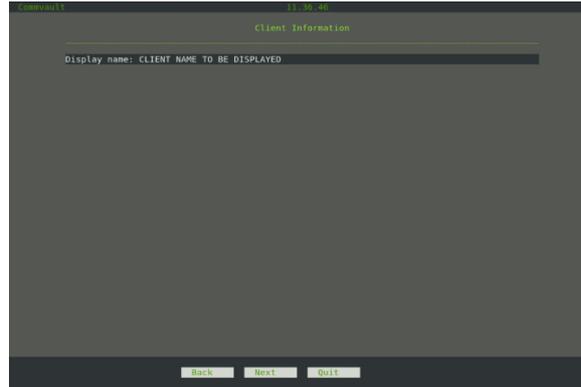
Unix Group Assignment.

Create or assign a Unix Group if you want to. It is recommended mostly in Database Agents.

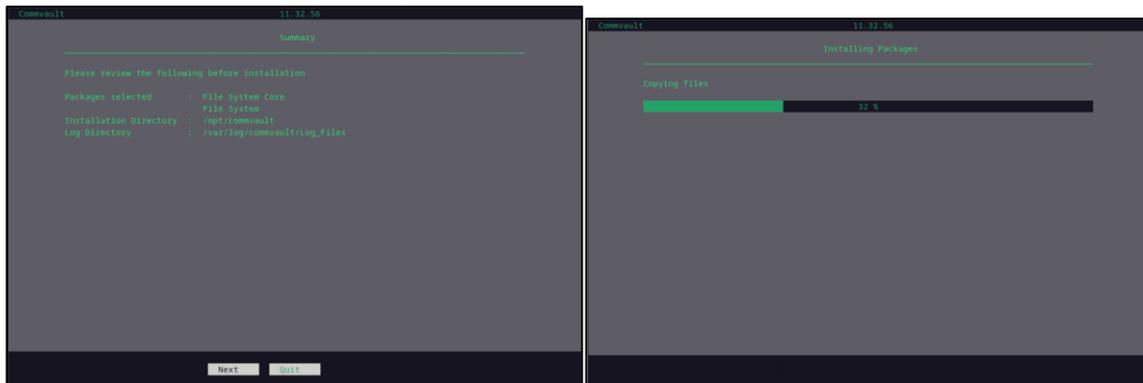


Enter the Agent you are installing IP address.

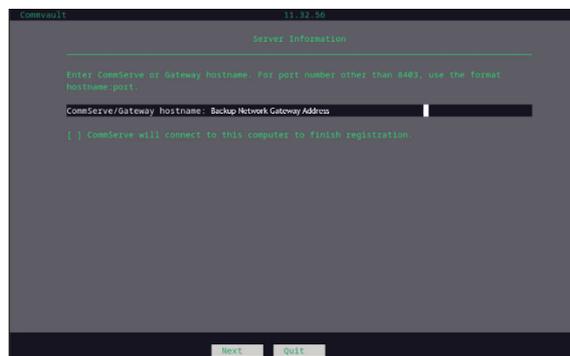


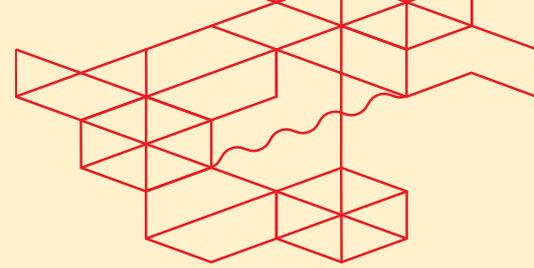

Specify a Client Display name (What will be shown in MPB Console)


***At this point, if your agent is DB2, there are a few additional steps before proceeding, go to topic 2.6.5. If not, ignore this message.**

Review the installation Summary


Enter MPB Network Gateway, provided during onboarding session (the same you entered in step 2.6.1) and leave the option CommServe will connect to this computer to finish registration unchecked.



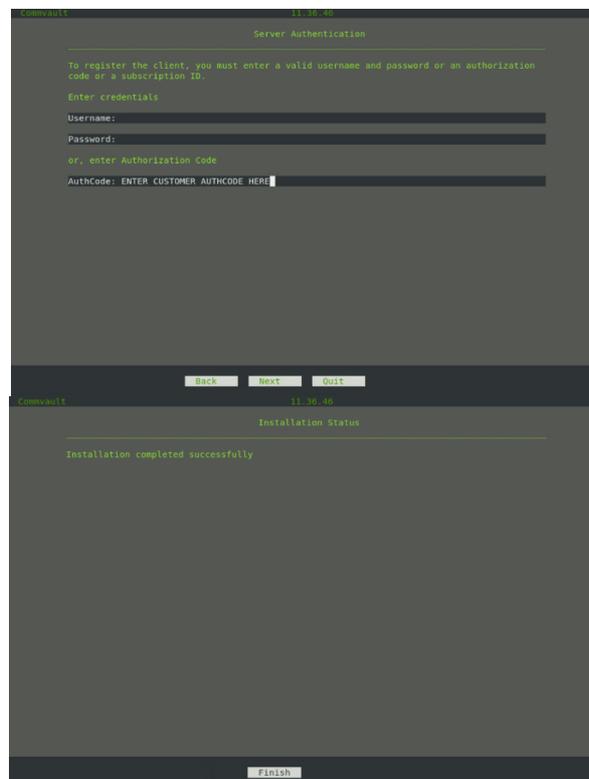


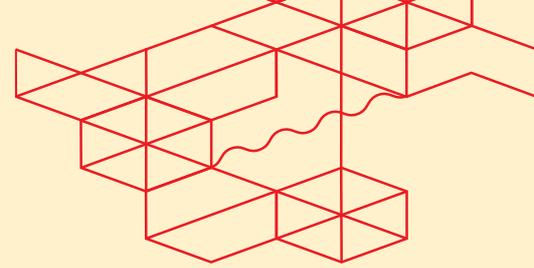
EMS - Managed Private Backup User Guide – Release 1.1

Leave the option of there is a HTTP proxy between customer and server checked as No.



Enter customer Authcode, provided during onboarding. Leave username and password blank.



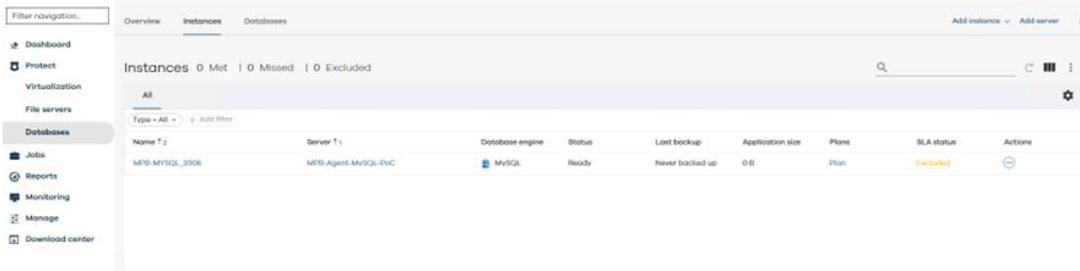


EMS - Managed Private Backup User Guide – Release 1.1

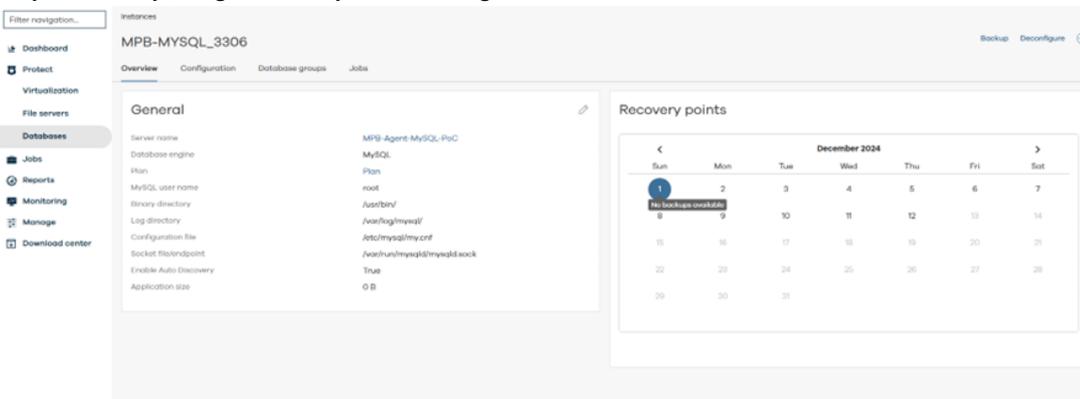
5.6.4 MySQL Agent Installation

Most of the installation steps are similar to installation in 2.6.3.

For MySQL Agent, after installation, go to MPB Console > Protect > Databases



If it's needed, select the Database, in the Overview Tab, select the pencil icon and change the Binary Directory, Log Directory and Configuration File.

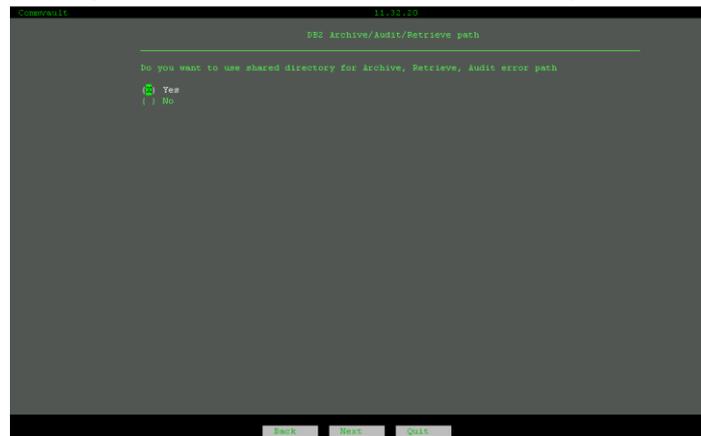


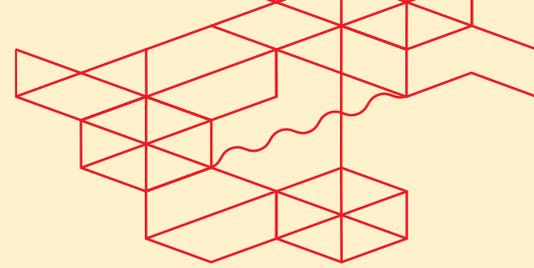
5.6.5 IBM DB2 Agent Installation

For the DB2 Agent, there are a few mid-steps during installation.

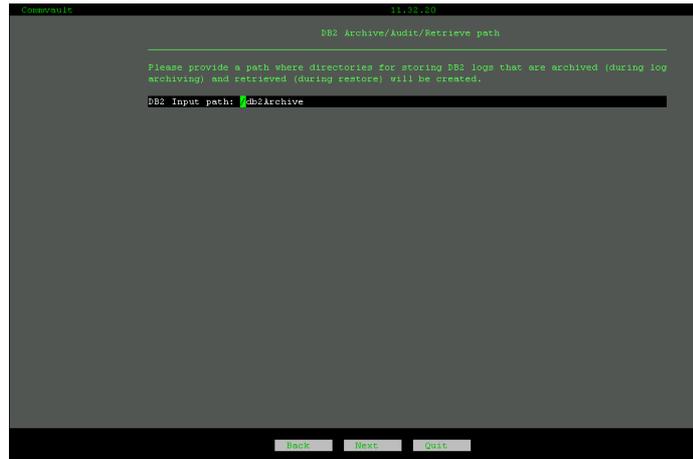
Archive log folder:

Cluster DB2: If the DB2 is configured on a clustered mode you need to select Yes for using shared directory for Archive, Retrieve and Audit error path.

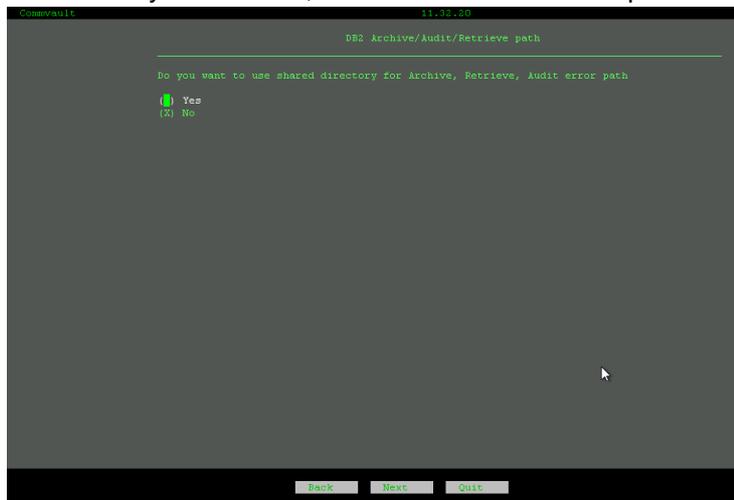




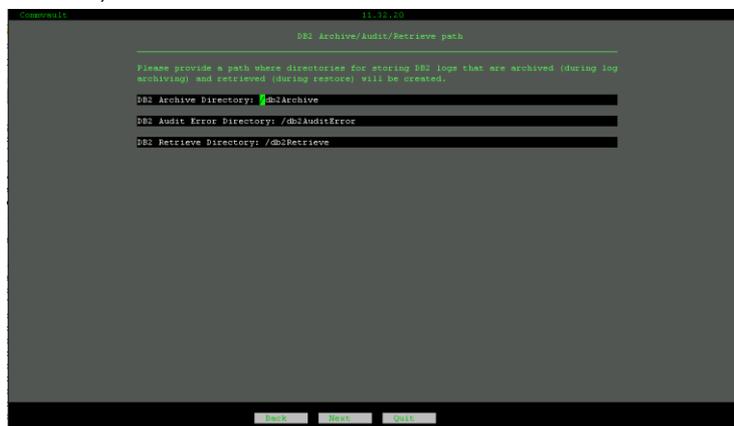
Then, set the DB2 Input path:



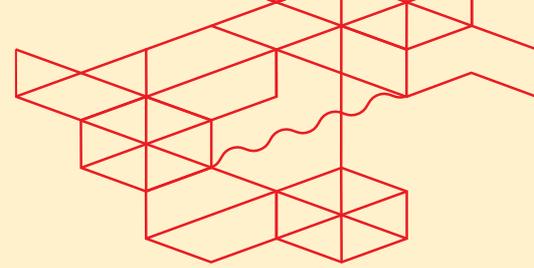
Standalone DB2: If the DB2 is configured on standalone mode you need to select No for using shared directory for Archive, Retrieve and Audit error path.



Set the DB2 Archive, Audit Error and Retrieve directories.

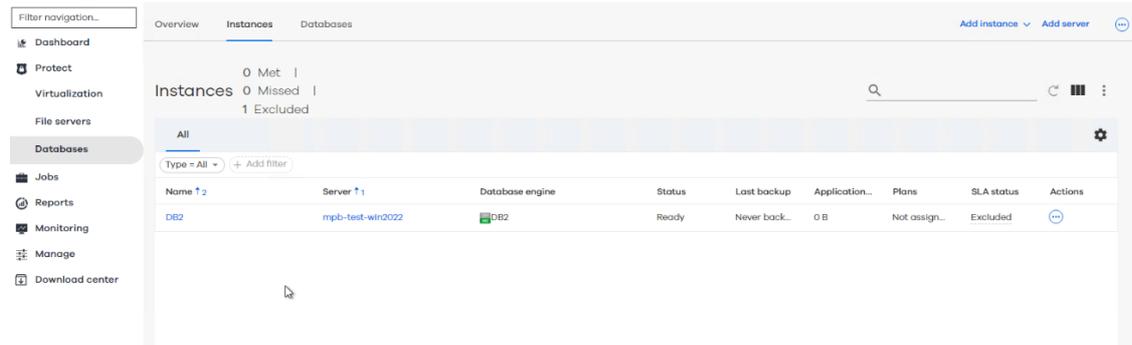


Then proceed with the normal installation like step 2.6.3 described.



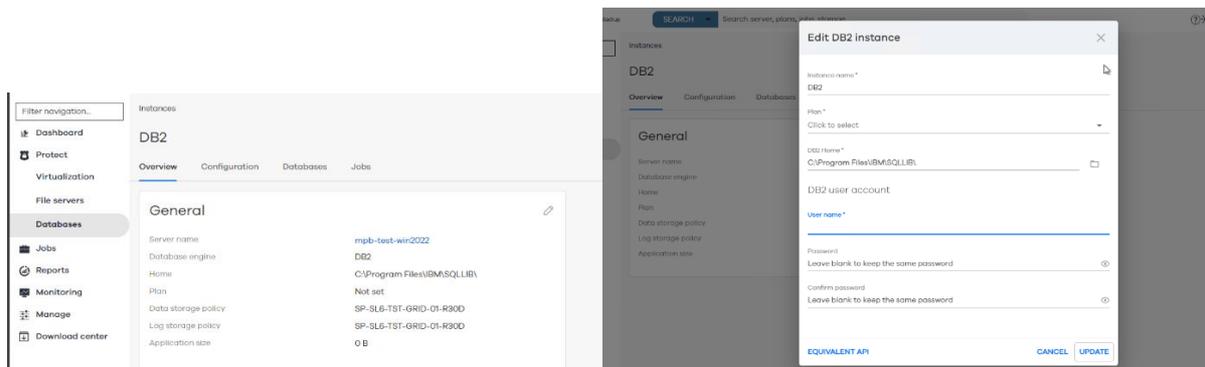
EMS - Managed Private Backup User Guide – Release 1.1

Now, go to MPB Console > Protect > Databases

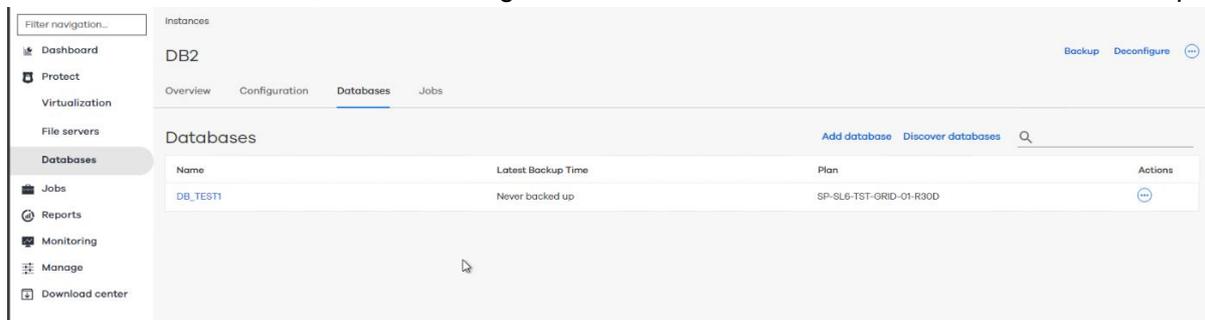


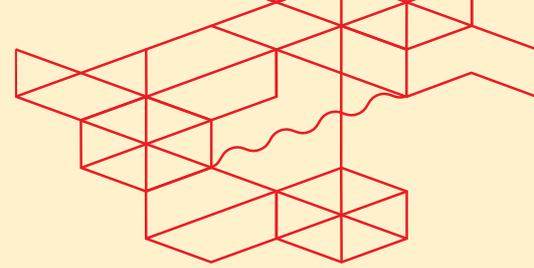
Select the instance, in the Overview tab, click the pencil icon to include:

- The user administrator on the server to execute the backup of the database. This DB2 user must have the following permissions: SYSADM, SYSCTRL, or SYMAINT, and DBADM.
- The plan for the backup execution in this section.
- Information about the DB Home.



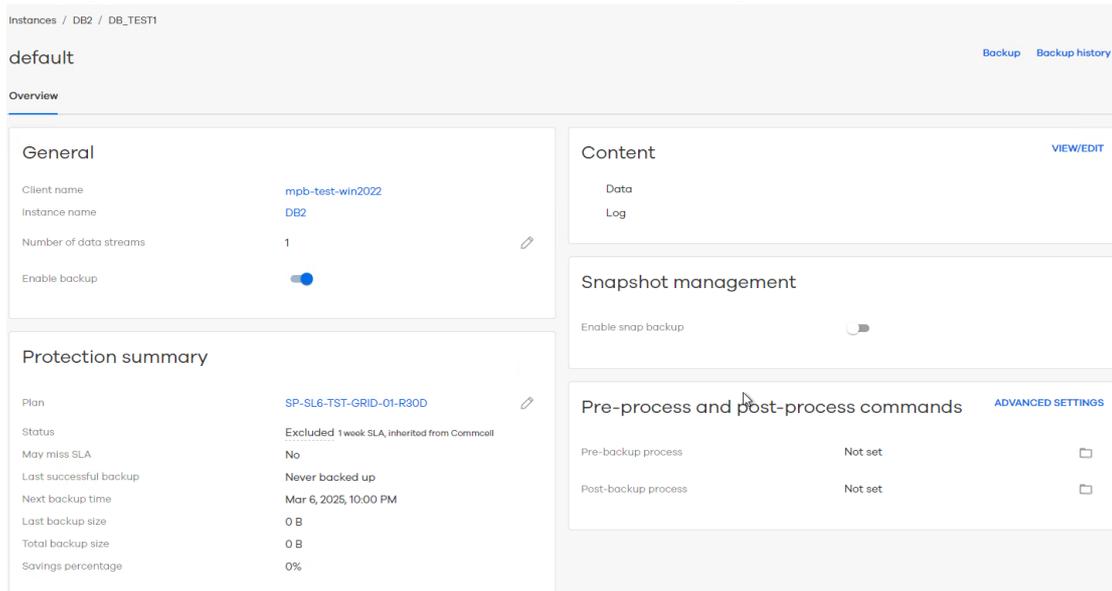
In the Databases tab, we must configure the database for which we want to execute backups:





EMS - Managed Private Backup User Guide – Release 1.1

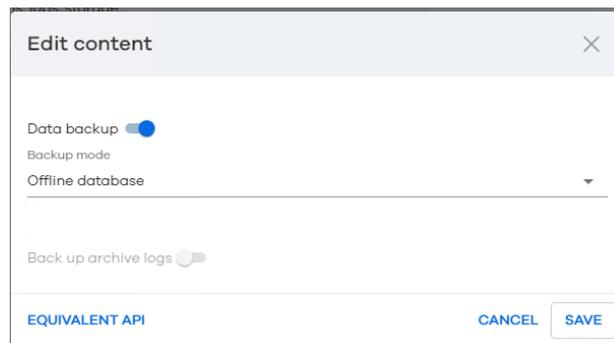
We need to configure the subclient to the backup execution. At this point, we can configure the backup type that we want to execute. To do this, is necessary to edit the content section:



The screenshot shows the configuration page for a subclient named 'default'. The page is divided into several sections:

- General:** Client name (mpb-test-win2022), Instance name (DB2), Number of data streams (1), and Enable backup (checked).
- Protection summary:** Plan (SP-SL6-TST-GRID-01-R30D), Status (Excluded 1 week SLA, inherited from Commcell), May miss SLA (No), Last successful backup (Never backed up), Next backup time (Mar 6, 2025, 10:00 PM), Last backup size (0 B), Total backup size (0 B), and Savings percentage (0%).
- Content:** Includes 'Data' and 'Log' sections, with a 'VIEW/EDIT' link.
- Snapshot management:** Includes 'Enable snap backup' (unchecked).
- Pre-process and post-process commands:** Includes 'Pre-backup process' and 'Post-backup process', both set to 'Not set'.

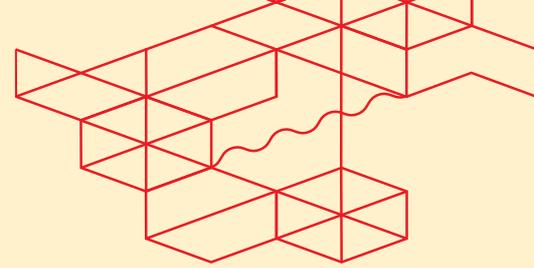
Backup offline. If you need to execute an offline backup of the database, you should configure it as follows.



The 'Edit content' dialog box contains the following configuration options:

- Data backup:** Checked (toggle).
- Backup mode:** Offline database (dropdown menu).
- Back up archive logs:** Unchecked (toggle).

At the bottom of the dialog, there are three buttons: 'EQUIVALENT API', 'CANCEL', and 'SAVE'.



EMS - Managed Private Backup User Guide – Release 1.1

```

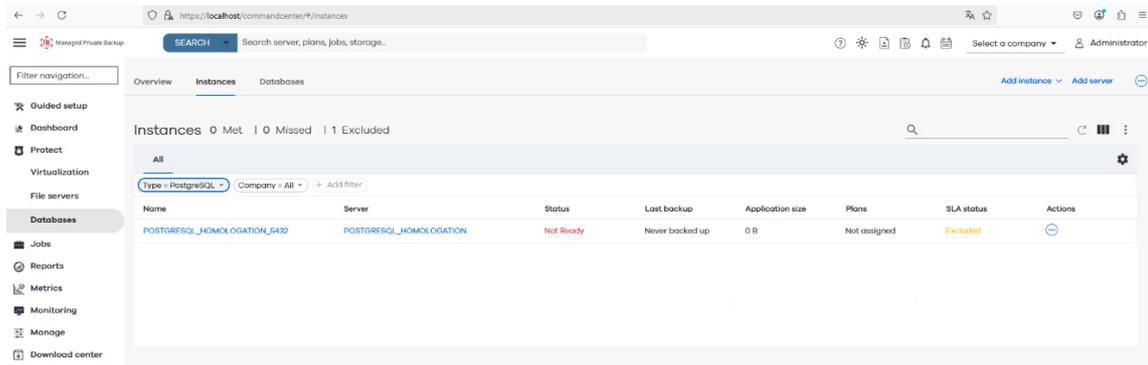
First log archive method          (LOGARCHMETH1) = VENDOR:C:\Program Files\Commvault\ContentStore\Base\DB2Sbt.dll
Archive compression for logarchmeth1 (LOGARCHCOMPR1) = OFF
Options for logarchmeth1          (LOGARCHOPT1) = CvClientName=mpb-test-win2022,CvInstanceName=Instance001
Second log archive method         (LOGARCHMETH2) = OFF
Archive compression for logarchmeth2 (LOGARCHCOMPR2) = OFF
Options for logarchmeth2          (LOGARCHOPT2) =
Failover log archive path         (FAILARCHPATH) =
Number of log archive retries on error (NUMARCHRETRY) = 5
Log archive retry Delay (secs)     (ARCHRETRYDELAY) = 20
Vendor options                     (VENDOROPT) = CvClientName=mpb-test-win2022,CvInstanceName=Instance001
    
```

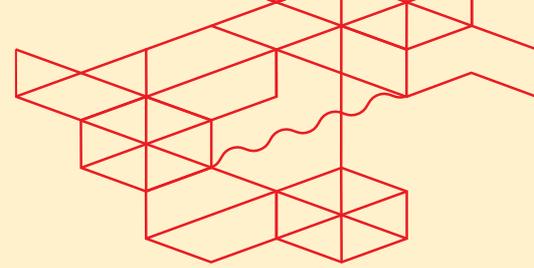
At this point, you can start executing the online backup. However, before that, you need to perform an offline backup of the database.

5.6.6 PostgreSQL Server Installation

Most of the installation steps are similar to installation in 2.6.3.

For PostgreSQL Agent, after installation, go to MPB Console > Protect > Databases > Instances Tab





EMS - Managed Private Backup User Guide – Release 1.1

In the instance Overview, hit the pencil button, we must include:

- **Server Plan**
- **On Connection details, the database user, database password, the Unix username, the maintenance DB, and the port. If those option are correct by default, you can leave it as is..**
- **The plan for the backup execution in this section.**
- **Information about the DB Home.**

Instances

POSTGRESQL_HOMOLOGATION_5432

Overview Configuration Backup sets Jobs

General

Server name	POSTGRESQL_HOMOLOGATION
Database engine	PostgreSQL
PostgreSQL user name	postgres
Plan	Not set
Log storage policy	CV_DEFAULT
Maintenance DB	postgres
Binary directory	/usr/pgsql-17/bin
Library directory	/usr/pgsql-17/lib
Delete archive logs	True
Port	5432
Application size	0 B

Edit PostgreSQL instance

Instance name *
POSTGRESQL_HOMOLOGATION_5432

Plan *
MPB_RJ2-30D#01

Run dump backups with plan-based schedules

Connection details

Database user *
postgres

Password
Leave blank to keep the same password

UNIX user name
postgres

Maintenance DB *
postgres

Port *
5432

• In the PostgreSQL paths, include:

- **Binary directory, Library directory and Archive log directory**

PostgreSQL paths

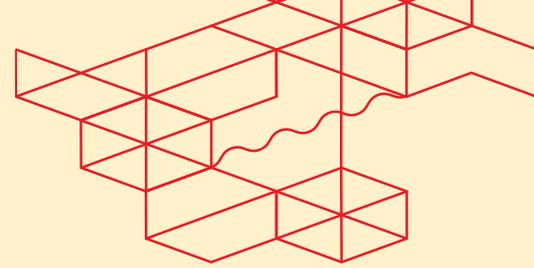
Binary directory
/usr/pgsql-17/bin

Library directory
/usr/pgsql-17/lib

Archive log directory

Delete archive logs

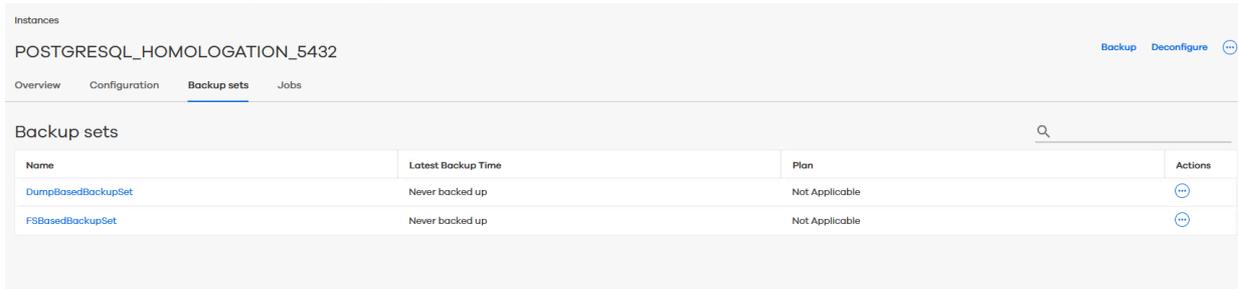
Enable standby backup



EMS - Managed Private Backup User Guide – Release 1.1

In the Backup sets tab, we must configure if it will be a DumpBasedBackupSet or a FSBasedBackupSet:

For FSBasedBackupSet, verify that the archive directory is properly configured, and that archiving is working.



The screenshot shows the 'Backup sets' tab for instance POSTGRESQL_HOMOLOGATION_5432. It displays a table with two backup sets:

Name	Latest Backup Time	Plan	Actions
DumpBasedBackupSet	Never backed up	Not Applicable	⋮
FSBasedBackupSet	Never backed up	Not Applicable	⋮

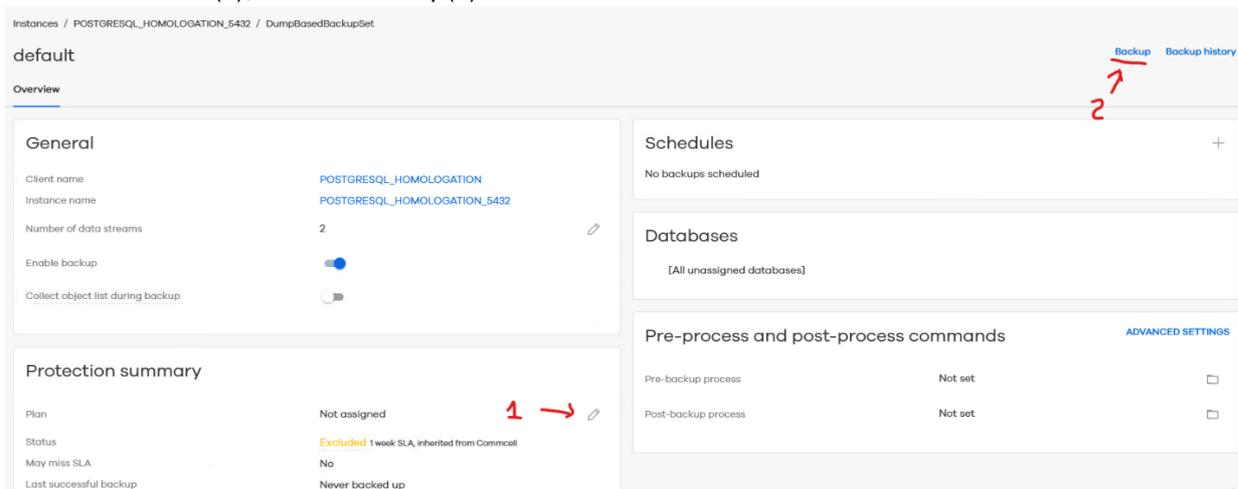
Select the chosen type of backup, then go to Database Groups, hit the desired group:



The screenshot shows the 'Database groups' tab for the selected backup set. It displays a table with one database group:

Name	Latest Backup Time	Plan	Actions
default	Never backed up		⋮

Edit the Plan (1), then hit Backup(2):



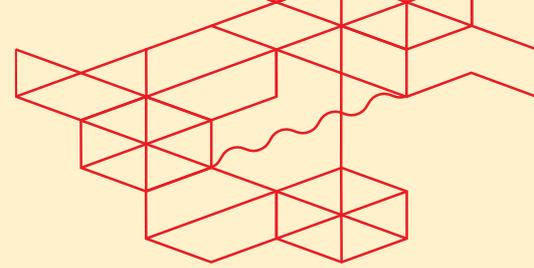
The screenshot shows the configuration page for the 'default' database group. It has several sections:

- General:** Client name (POSTGRESQL_HOMOLOGATION), Instance name (POSTGRESQL_HOMOLOGATION_5432), Number of data streams (2), Enable backup (checked), Collect object list during backup (unchecked).
- Protection summary:** Plan (Not assigned), Status (Excluded 1 week SLA, inherited from Comms), May miss SLA (No), Last successful backup (Never backed up).
- Schedules:** No backups scheduled.
- Databases:** [All unassigned databases]
- Pre-process and post-process commands:** Pre-backup process (Not set), Post-backup process (Not set).

Red annotations: '1' with an arrow points to the 'Plan' field in the Protection summary section. '2' with an arrow points to the 'Backup' button in the top right corner.

If the PostgreSQL pg_hba.conf is set to PEER, it might be needed to adjust the user PostgreSQL Authentication Method:

- peer means it will trust the identity (authenticity) of UNIX user. So not asking for a password.
- md5 means it will always ask for a password, and validate it after hashing with MD5.
- trust means it will never ask for a password, and always trust any connection.



The Database Backup was configured and can be restored:

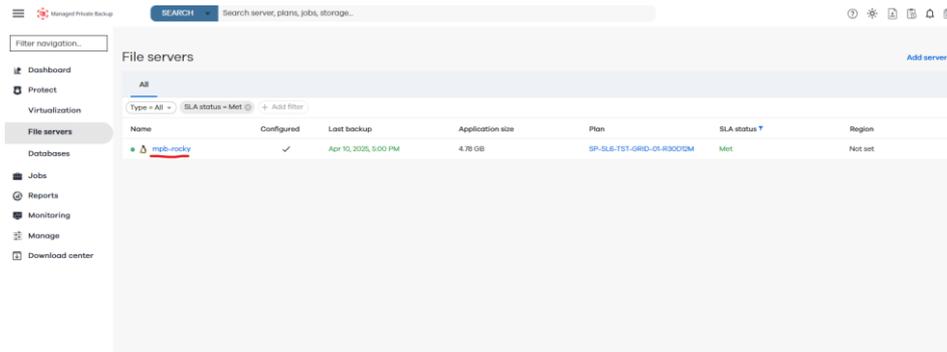
Recovery points DumpBasedBackupSet ▾

March 2025								
<	Sun	Mon	Tue	Wed	Thu	Fri	Sat	>
							1	
	2	3	4	5	6	7	8	
	9	10	11	12	13	14	15	
	16	17	18	19	20	21	22	
	23	24	25	26	27	28	29	
	30	31						

RESTORE

5.7 How to add paths to the agent backup policy?

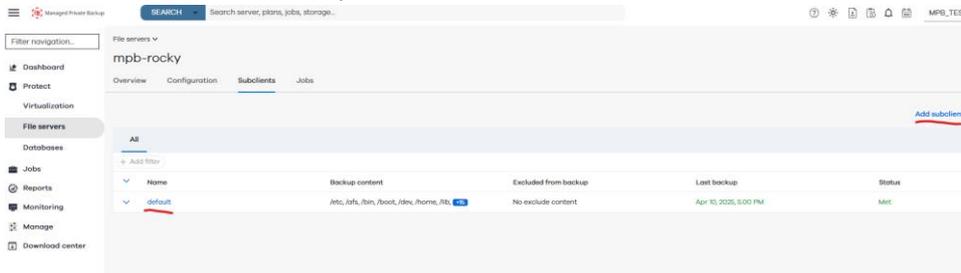
On MPB Console, go to Protect > File Servers, select the desired file server



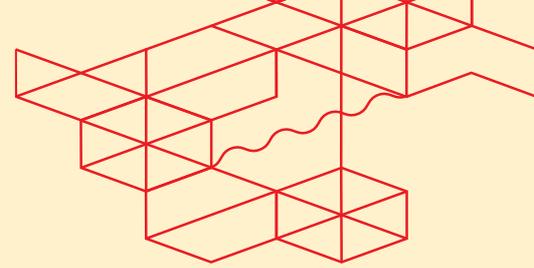
Name	Configured	Last backup	Application size	Plan	SLA status	Region
mpb-rocky	✓	Apr 10, 2025, 5:00 PM	4.78 GB	SP-SLG-TST-GRID-01-R300DM	Met	Not set

Go to Subclients tab, and either select the default subclient or add a new subclient.

Subclients are a way to organize your backup folders files (e.g.: C:, D:, Managers, Analysts). It is needed to have at least one subclient (it will be named default, but can be renamed if wanted).

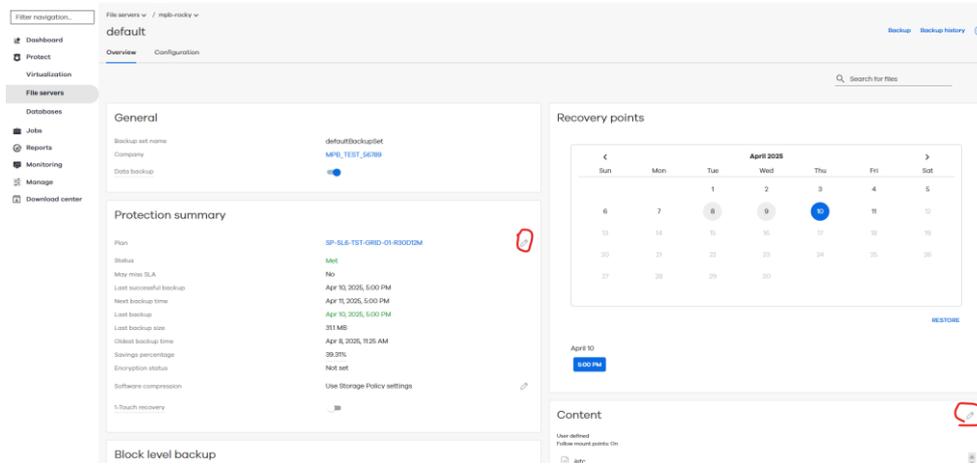


Name	Backup content	Excluded from backup	Last backup	Status
default	/etc, /etc, /bin, /boot, /dev, /home, /lib, /lib64	No exclude content	Apr 10, 2025, 5:00 PM	Met

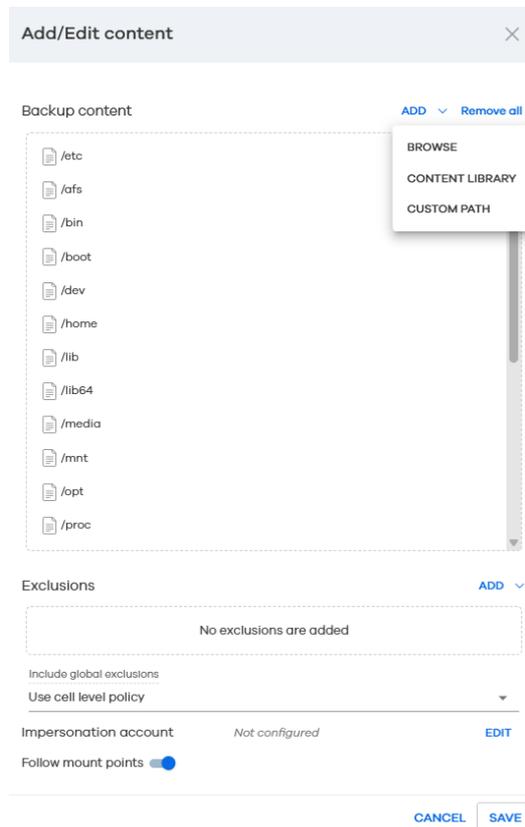


EMS - Managed Private Backup User Guide – Release 1.1

Edit the Plan according to what retention and location is desired, then, edit the Content



Click in ADD to browse for the files, to select a content library or manually insert the paths. It's also possible to select exclusions for the files.



Add/Edit content

Backup content ADD Remove all

- /etc
- /afs
- /bin
- /boot
- /dev
- /home
- /lib
- /lib64
- /media
- /mnt
- /opt
- /proc

BROWSE

- CONTENT LIBRARY
- CUSTOM PATH

Exclusions ADD

No exclusions are added

Include global exclusions

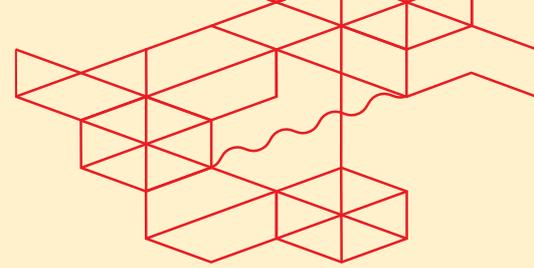
Use cell level policy

Impersonation account *Not configured* EDIT

Follow mount points

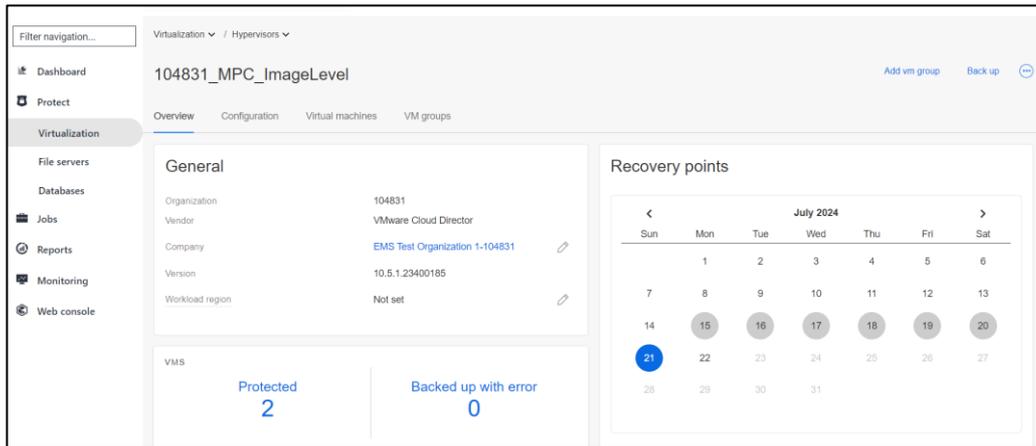
CANCEL SAVE

Hit Save.

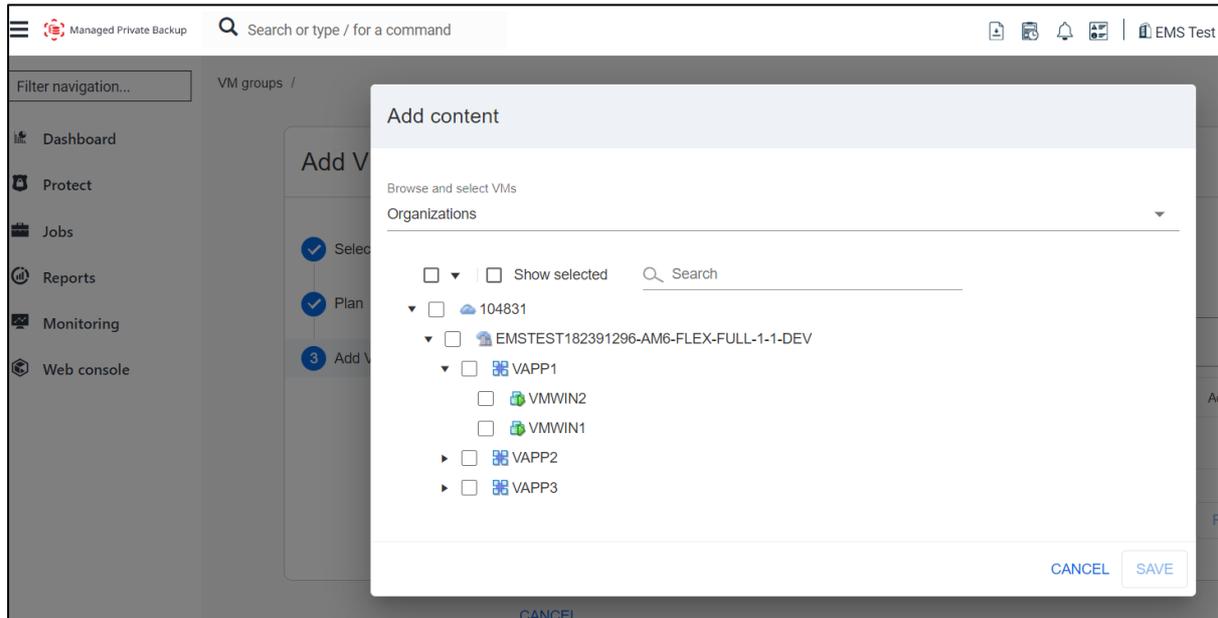


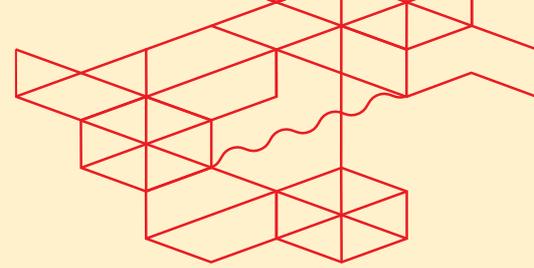
5.8 How to include targets on the VM backup policy?

To include virtual machines to image level backups, please go to Virtualization, select the Hypervisor tab and select your desired Hypervisor (MPC, VMWare or Hyper-V). You will see the screen like the one below where you may explore and select the virtual machines to protect:



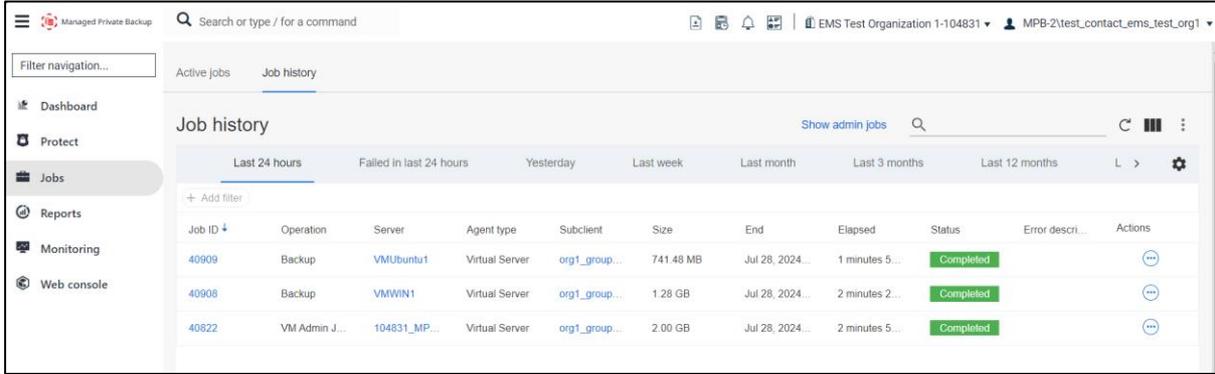
Use the option **“add rule”** to configure a rule to automatically protect any virtual machine on the MPC or the **“content”** to specify manually which data should be protected.





5.9 How to check if the backup job was finished successfully?

To check the execution of the backup jobs, please go to the Jobs section on the left menu and then click on Job history:

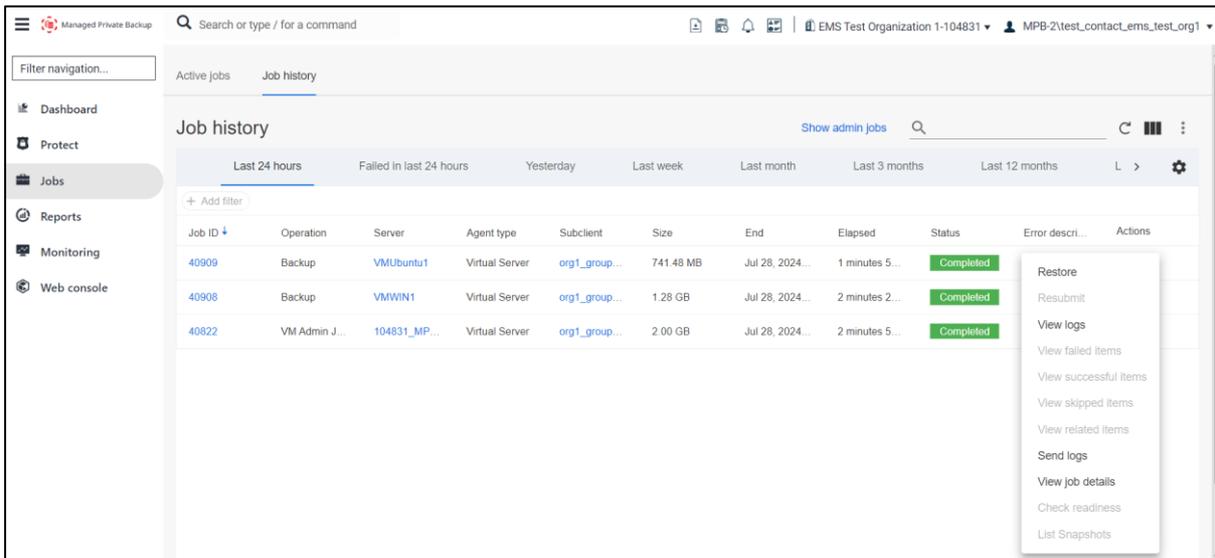


Job ID	Operation	Server	Agent type	Subclient	Size	End	Elapsed	Status	Error descri...	Actions
40909	Backup	VMUbuntu1	Virtual Server	org1_group...	741.48 MB	Jul 28, 2024...	1 minutes 5...	Completed		
40908	Backup	VMWIN1	Virtual Server	org1_group...	1.28 GB	Jul 28, 2024...	2 minutes 2...	Completed		
40822	VM Admin J...	104831_MP...	Virtual Server	org1_group...	2.00 GB	Jul 28, 2024...	2 minutes 5...	Completed		

If you have multiple jobs, please use the next tab Failed in last 24 hours for the most direct view.

5.10 How to troubleshoot why the backup job has failed?

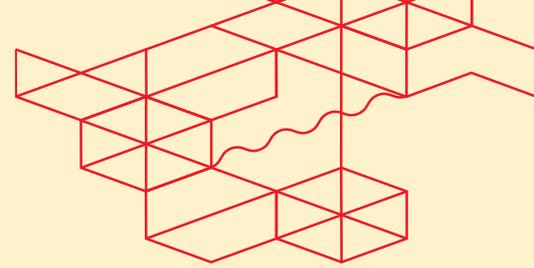
If some of your jobs have failed, you may find the cause of the problem by accessing the job log on the actions column.



Job ID	Operation	Server	Agent type	Subclient	Size	End	Elapsed	Status	Error descri...	Actions
40909	Backup	VMUbuntu1	Virtual Server	org1_group...	741.48 MB	Jul 28, 2024...	1 minutes 5...	Completed		<ul style="list-style-type: none"> Restore Resubmit View logs <ul style="list-style-type: none"> View failed items View successful items View skipped items View related items Send logs View job details Check readiness List Snapshots
40908	Backup	VMWIN1	Virtual Server	org1_group...	1.28 GB	Jul 28, 2024...	2 minutes 2...	Completed		
40822	VM Admin J...	104831_MP...	Virtual Server	org1_group...	2.00 GB	Jul 28, 2024...	2 minutes 5...	Completed		

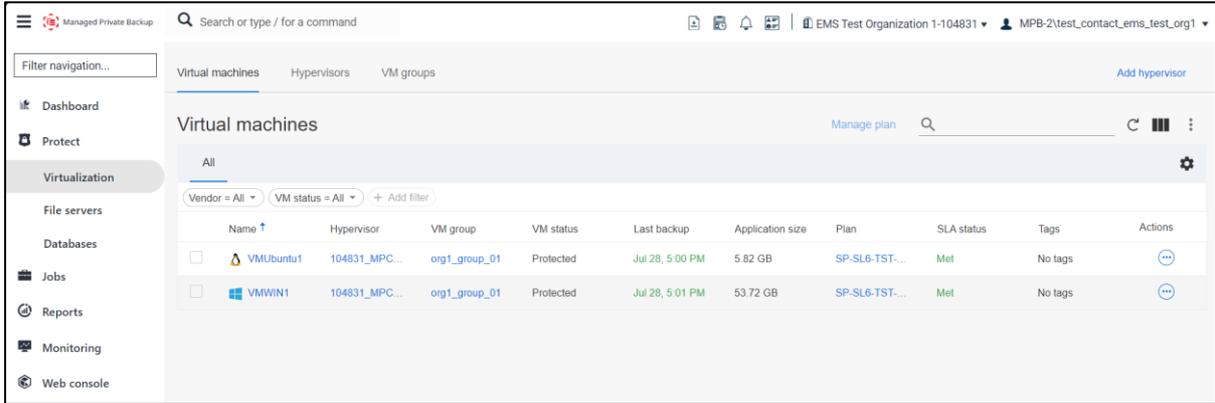
Please note, if you find the backup job has been failing due to an Equinix platform reason, you may raise a ticket anytime.

In the Job details item, you may have an overall view of all detailed process, including which targets were protected and the specific attempts made by MPB to protect the workload.



5.11 How to check how much data has been protected from one specific Server/instance?

To check how much front-end data has been protect by MPB by specific server/virtual machine, you may see the column application size on this page:

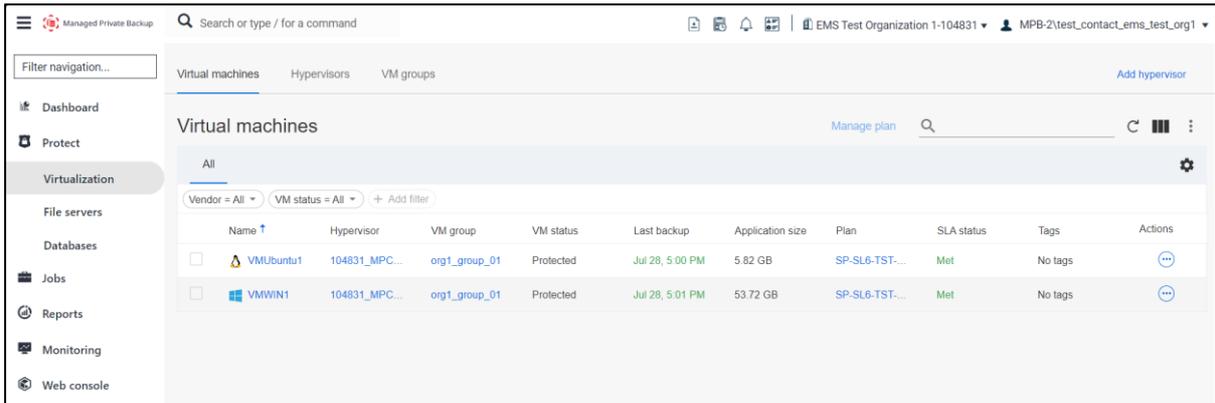


Name	Hypervisor	VM group	VM status	Last backup	Application size	Plan	SLA status	Tags	Actions
VMUbuntu1	104831_MPC...	org1_group_01	Protected	Jul 28, 5:00 PM	5.82 GB	SP-SL6-TST...	Met	No tags	⋮
VMWIN1	104831_MPC...	org1_group_01	Protected	Jul 28, 5:01 PM	53.72 GB	SP-SL6-TST...	Met	No tags	⋮

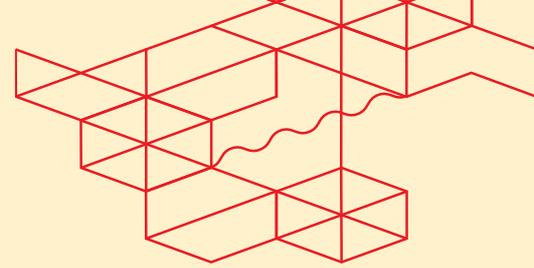
To follow up on your global usage of the product, please open a request ticket. A new report will be available soon.

5.12 How to run backup on demand?

To start a manual backup job, you just need to find your server / virtual machine on the Protect tab.

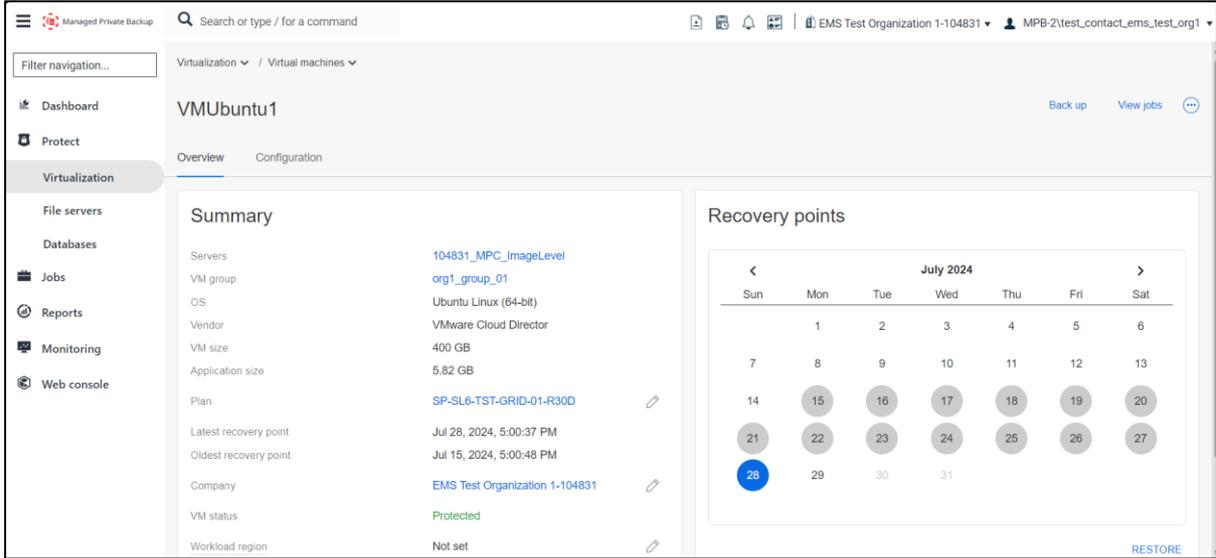


Name	Hypervisor	VM group	VM status	Last backup	Application size	Plan	SLA status	Tags	Actions
VMUbuntu1	104831_MPC...	org1_group_01	Protected	Jul 28, 5:00 PM	5.82 GB	SP-SL6-TST...	Met	No tags	⋮
VMWIN1	104831_MPC...	org1_group_01	Protected	Jul 28, 5:01 PM	53.72 GB	SP-SL6-TST...	Met	No tags	⋮



EMS - Managed Private Backup User Guide – Release 1.1

Click on the server's name you want to protect, then select Backup on the right upper corner:



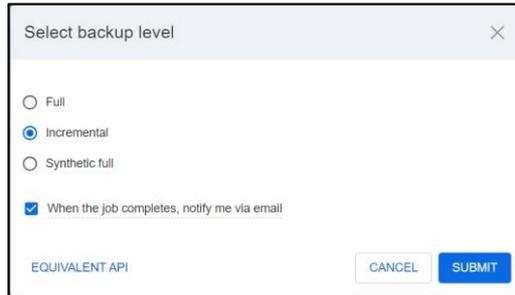
The screenshot shows the 'VMUubuntu1' configuration page. The left sidebar contains navigation options like Dashboard, Protect, Virtualization, File servers, Databases, Jobs, Reports, Monitoring, and Web console. The main content area is divided into 'Summary' and 'Recovery points'.

Summary:

- Servers: 104831_MPC_ImageLevel
- VM group: org1_group_01
- OS: Ubuntu Linux (64-bit)
- Vendor: VMware Cloud Director
- VM size: 400 GB
- Application size: 5.82 GB
- Plan: SP-SL6-TST-GRID-01-R30D
- Latest recovery point: Jul 28, 2024, 5:00:37 PM
- Oldest recovery point: Jul 15, 2024, 5:00:48 PM
- Company: EMS Test Organization 1-104831
- VM status: Protected
- Workload region: Not set

Recovery points: A calendar for July 2024 is shown, with the 28th selected. A 'RESTORE' button is visible at the bottom right of the calendar.

Then select the appropriate backup type and press submit:



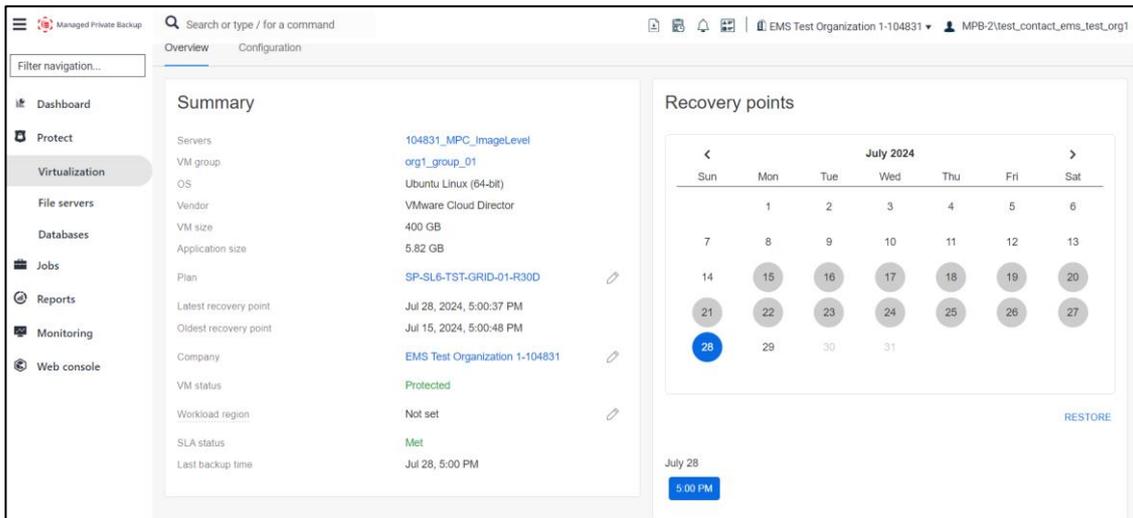
The 'Select backup level' dialog box contains the following options:

- Full
- Incremental
- Synthetic full
- When the job completes, notify me via email
- EQUIVALENT API

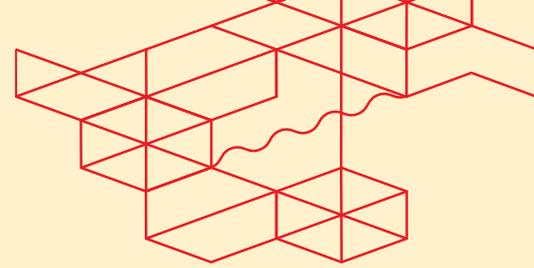
Buttons: CANCEL, SUBMIT

5.13 How to run restore on demand?

On the same page, you will find the latest recovery points available to be restored:



This screenshot is identical to the previous one, but it highlights the '5:00 PM' button located below the 'Recovery points' calendar, indicating the time of the latest recovery point.

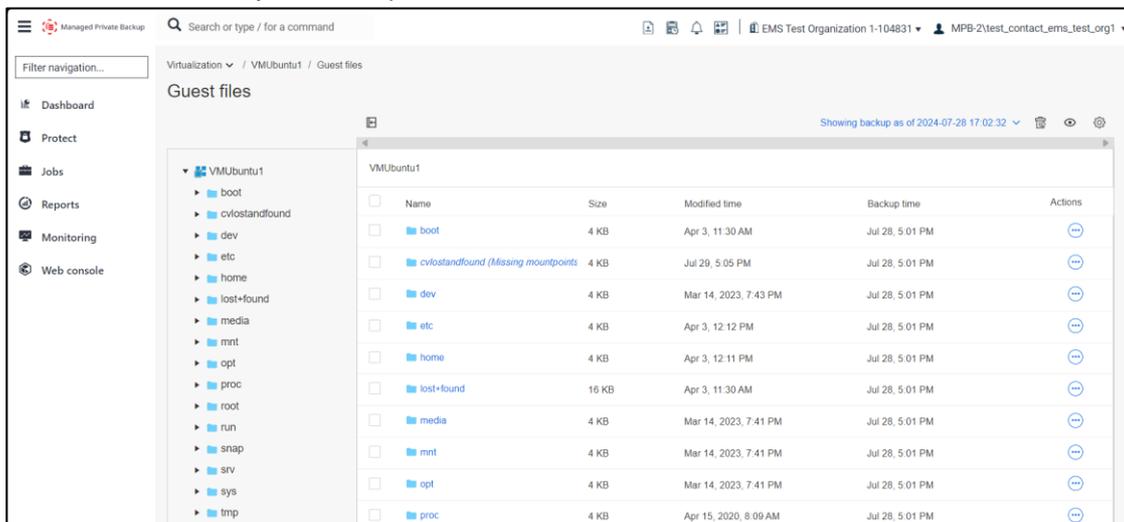


EMS - Managed Private Backup User Guide – Release 1.1

Once you have selected the date, it will show the available restore point that day. Click restore to start the procedure. You will then be presented a choice of recovering some files or the virtual machine completely:



If you select Guest files, you will be presented a list of files to choose from:



Just select the destination desired for the file and click Submit .

If you opt to restore the full virtual machine, you can choose to overwrite the virtual machine or restore as a new virtual machine. Restore Guest Files does not always work within the Commvault environment. If it fails, please select an alternative restore method. You need the connectivity layer and an Agent installed on the destination server to complete restores.

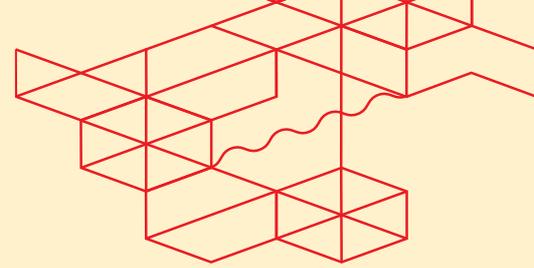
OBS: Guest Files limitations:

If your goal is to restore guest files, it is highly recommended that you use a File System Agent, because its restore will be quicker and more assertive, and since there is a list of limitations on the Guest File restore, and, it is a shared environment, we can't guarantee all requirements for this to work can be met to all customers.

What are the limitations for file level restores?

Consider the following before doing a file level restore:

- The Image Level on Unix /DataAgent can perform a File Level Restore only when the operating systems and their versions on the Client computer and the MediaAgent are same. If the operating systems of the Client computer and the MediaAgent are different, the File Level Restore job will go into pending state with the error message - Please check the log files for this job for more details.



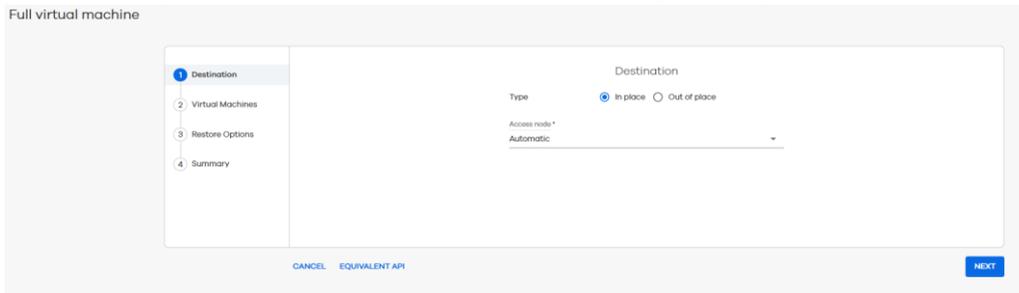
EMS - Managed Private Backup User Guide – Release 1.1

- For a Windows MediaAgent, the Index Cache folder must reside on an NTFS partition.
- If metadata was not collected during a backup, a File Level restore cannot be performed. This might result from having selected the **Skip Metatile Creation** option in the Advanced Backup Options screen, or as a result of failure to collect metadata during the backup, in which case the system generated an Event Message warning of the failure.
- Do not restore:
 - hidden objects
 - system files
 - recycler files
- Image Browse is not supported. A no-image browse operation returns the most recent version of the data that existed back to the most recent full backup, rather than returning an image of the specified entity (i.e., file system/directory). To perform a File Level Restore of an entity to a point in time, you will need to Browse back in time, to the point in time you want to restore.
- If the cluster size (allocation unit) on the disk that you backed up was less than 1024 bytes, a file level restore job will not complete successfully.

Full Virtual Machine Restore

Select the option Full virtual machine, select if it will be restored In place (same location/name as it was backed up, or Out of place, where it will be asked Destination questions)

Full virtual machine



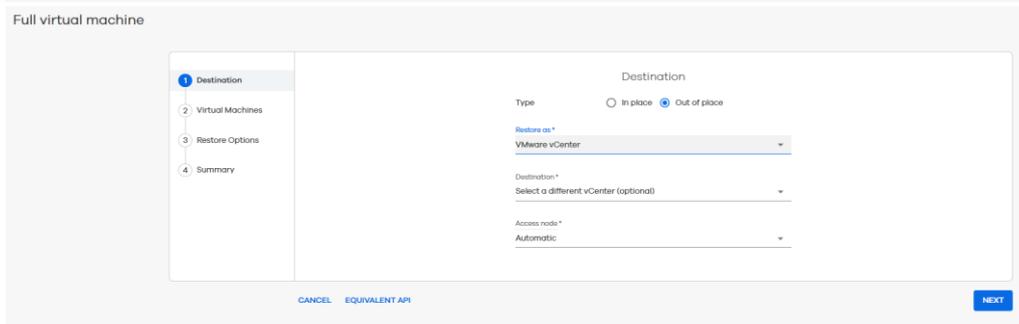
Destination

Type In place Out of place

Access node*
Automatic

CANCEL EQUIVALENT API NEXT

Full virtual machine



Destination

Type In place Out of place

Restore as*
VMware vCenter

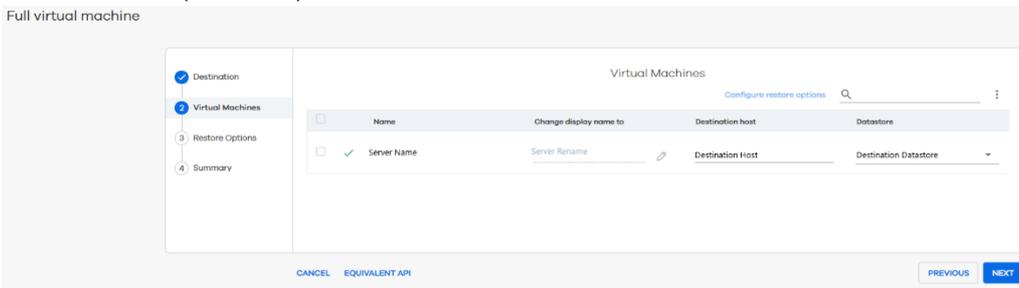
Destination*
Select a different vCenter (optional)

Access node*
Automatic

CANCEL EQUIVALENT API NEXT

Select the New Name (if want to), the Destination Host and Datastore

Full virtual machine

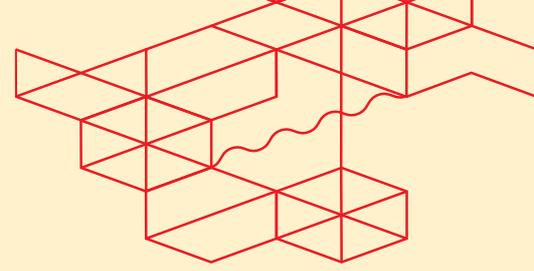


Virtual Machines

Configure restore options

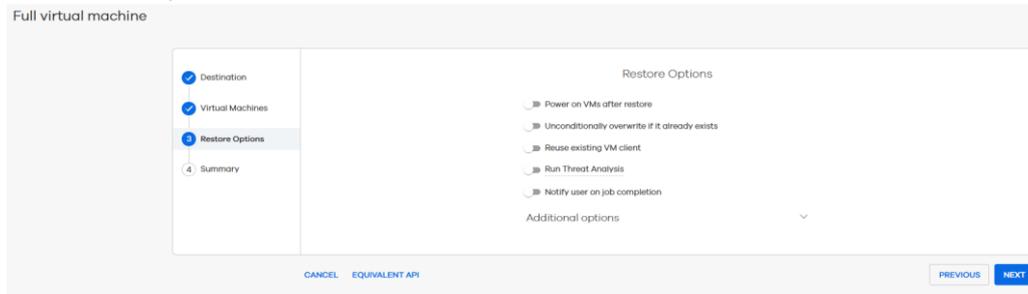
Name	Change display name to	Destination host	Datastore
<input checked="" type="checkbox"/> Server Name	Server Rename	Destination Host	Destination Datastore

CANCEL EQUIVALENT API PREVIOUS NEXT



EMS - Managed Private Backup User Guide – Release 1.1

Select the Restore Options



Review it, and submit

Other documentations

Where to find Service Description?

You will find the most up to date service description on docs.equinix.com website.

Where to find EMS policy?

You will find it on [our website](#).

Where to find official Commvault documentation?

You will find it on <http://documentation.commvault.com/>

How to ask for help

Please make sure to open a ticket every time you need help. This is your guarantee that the right team has received your request and will work on that under the expected SLAs.