

StarWind Virtual Tape Library: Configuration Guide for Cloud Storage, VTL Deployed as a Windows Applications using GUI

2024

TECHNICAL PAPERS



Trademarks

“StarWind”, “StarWind Software” and the StarWind and the StarWind Software logos are registered trademarks of StarWind Software. “StarWind LSFS” is a trademark of StarWind Software which may be registered in some jurisdictions. All other trademarks are owned by their respective owners.

Changes

The material in this document is for information only and is subject to change without notice. While reasonable efforts have been made in the preparation of this document to assure its accuracy, StarWind Software assumes no liability resulting from errors or omissions in this document, or from the use of the information contained herein. StarWind Software reserves the right to make changes in the product design without reservation and without notification to its users.

Technical Support and Services

If you have questions about installing or using this software, check this and other documents first - you will find answers to most of your questions on the [Technical Papers](#) webpage or in [StarWind Forum](#). If you need further assistance, please [contact us](#).

About StarWind

StarWind is a pioneer in virtualization and a company that participated in the development of this technology from its earliest days. Now the company is among the leading vendors of software and hardware hyper-converged solutions. The company's core product is the years-proven StarWind Virtual SAN, which allows SMB and ROBO to benefit from cost-efficient hyperconverged IT infrastructure. Having earned a reputation of reliability, StarWind created a hardware product line and is actively tapping into hyperconverged and storage appliances market. In 2016, Gartner named StarWind “Cool Vendor for Compute Platforms” following the success and popularity of StarWind HyperConverged Appliance. StarWind partners with world-known companies: Microsoft, VMware, Veeam, Intel, Dell, Mellanox, Citrix, Western Digital, etc.

Copyright ©2009-2018 StarWind Software Inc.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written consent of StarWind Software.

Annotation

Relevant products

This guide is applicable for StarWind VTL (build version 12767 and later).

Purpose

StarWind Virtual Tape Library (VTL) is a software solution that allows you to emulate physical Tape Libraries while storing data on the hard disk drives. The solution targets companies that want to completely quit using the physical Tape Library, as well as simplify and accelerate the process of data backup and recovery.

This document outlines how to configure a StarWind VTL and includes steps on how to replicate the tapes to the cloud object storage.

Audience

This technical guide is intended for storage and virtualization architects, system administrators, and partners designing virtualized environments using StarWind Virtual Tape Library (VTL).

Expected result

The end result of following this guide will be a fully configured StarWind VTL with replicated tapes to the cloud object storage.

Prerequisites

StarWind VTL system requirements

Prior to installing StarWind Virtual SAN, please make sure that the system meets the requirements, which are available via the following link: <https://www.starwindsoftware.com/system-requirements#virtual-tape-library>

Recommended RAID settings for HDD and SSD disks:
<https://knowledgebase.starwindsoftware.com/guidance/recommended-raid-settings-for-hdd-and-ssd-disks/>

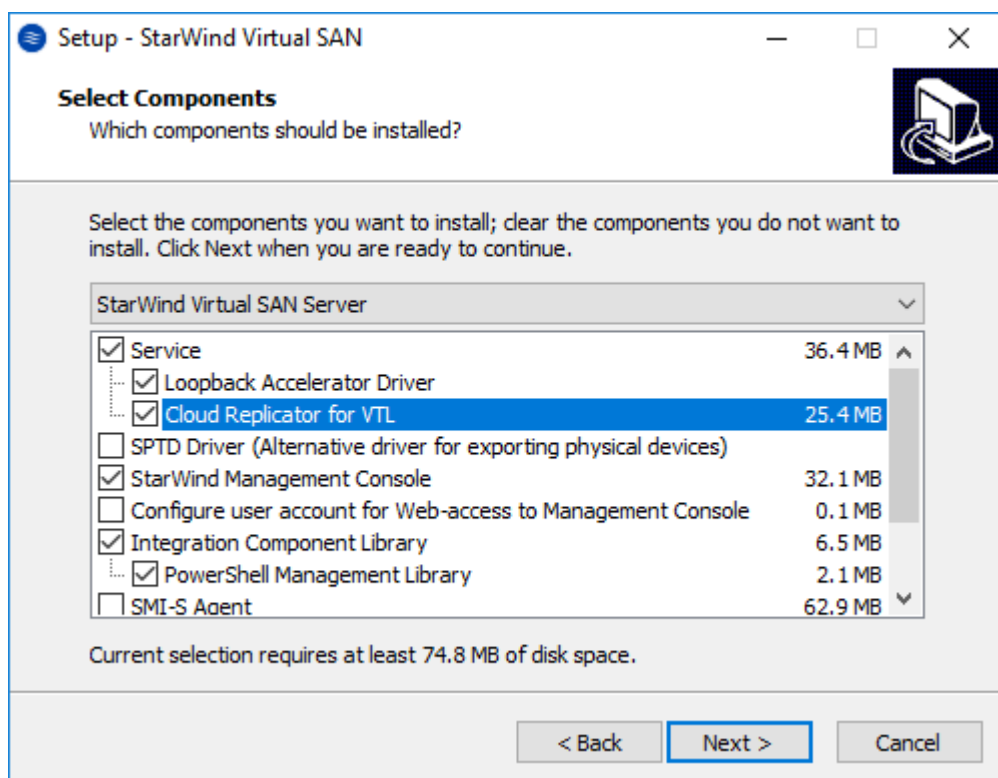
IMPORTANT NOTE: In order to fit the ransomware resiliency, the VTL should be located on the dedicated storage/host which must be isolated from the production environment.

Please read the following document for details:

[Backing up StarWind Virtual SAN Environment: Best Practice.](#)

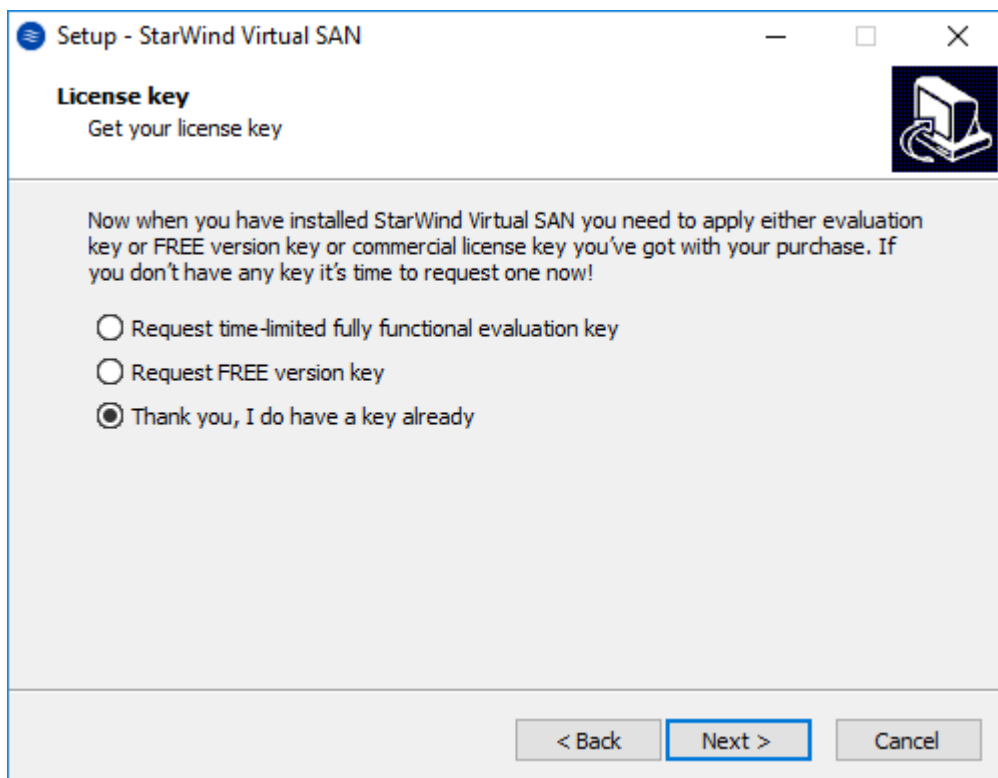
Installing Starwind Vtl

1. Launch the downloaded setup file on the server where StarWind VTL has to be installed.
2. Read and accept the License Agreement.
3. Read carefully the information about new features and improvements.
Note: the text in red indicates warnings for users who are updating existing software installations.
4. Click Browse to modify the installation path if necessary.
5. To install StarWind VTL service along with StarWind Virtual SAN service, enable the checkboxes as in the image below.



6. Specify the Start Menu folder.
7. Enable the checkbox to create a desktop icon.

8. Select the appropriate option to enter the license key.



9. Review the licensing information and click Next to apply the license key.

10. Verify the installation settings and click Install to continue or Back to make any changes.

11. Enable the appropriate checkbox to launch the StarWind Management Console right after the setup wizard is closed.

12. Click Finish to close the wizard.

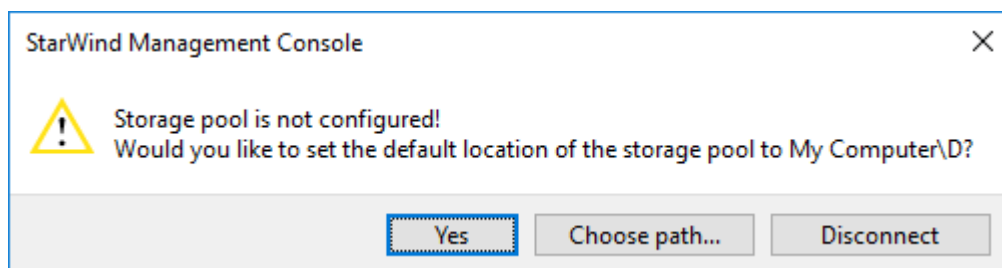
Configuring Virtual Tape Library

1. Launch the StarWind Management Console by double-clicking the StarWind tray icon. NOTE: If StarWind service and Management Console are installed on the same server, the Management Console will automatically add the local StarWind instance to the Console tree after the first launch. Then, the Management Console automatically connects to it using the default credentials. To add remote StarWind servers to the Console, use the Add Server button on the control panel.

2. StarWind Management Console will ask to specify the default storage pool on the

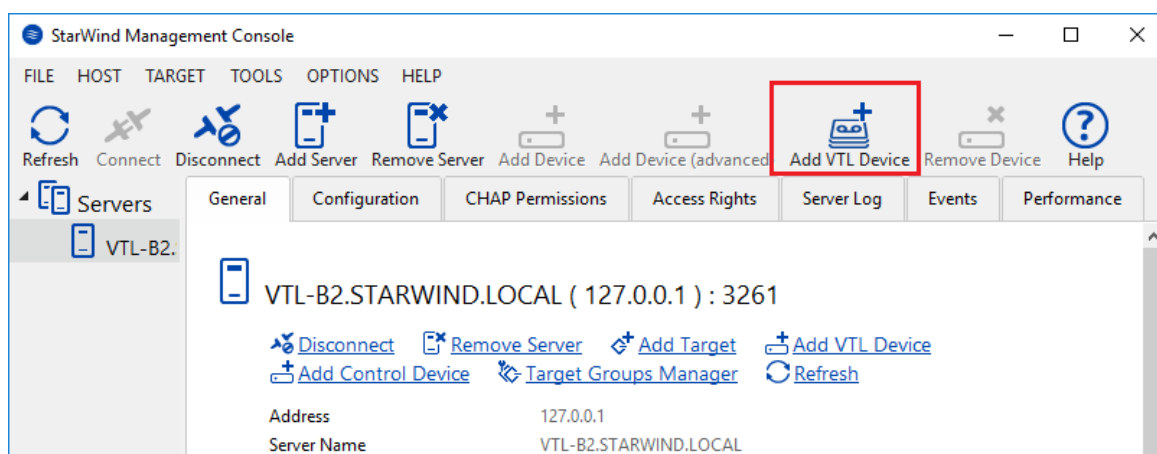
server you are connecting to for the first time. Please, configure the default storage pool to use one of the volumes you have prepared as StarWind storage earlier. All the devices created through the Add Device wizard will be stored on that storage pool by default.

3. Press the Yes button to configure the storage pool. Should you require to change the storage pool destination, press Choose path... and point the browser to the necessary disk.



4. Select the StarWind server where the device needs to be created.

5. Press the Add VTL Device button on the toolbar.



6. Specify the Virtual Tape Library location in the appeared window and click Next.

← Add Device Wizard

Virtual Tape Library Location

☒ Create a New Virtual Tape Library

Name:

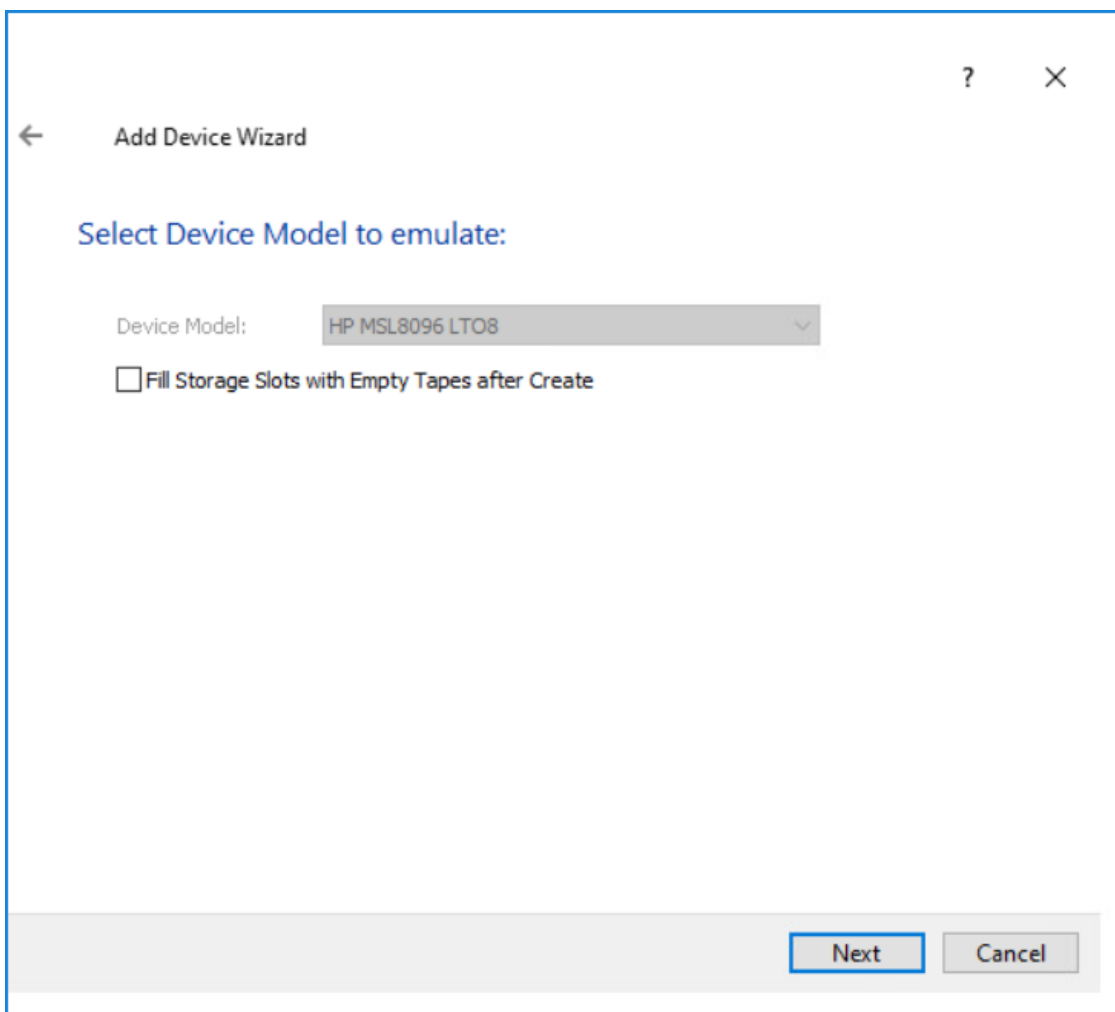
Location:

☐ Use an Existing Virtual Tape Library

Location:

Next Cancel

7. Select the Device Model from a drop-down list. You can also fill all slots in the newly created Tape Library with empty tapes.



8. Provide Target Alias or choose the default one.

← Add Device Wizard

Target Parameters

Choose a Target Attachment Method

Create new Target

Target Alias

VTL

☐ Target Name

iqn.2008-08.com.starwindsoftware:vtl-b2.starwind.local-vtl

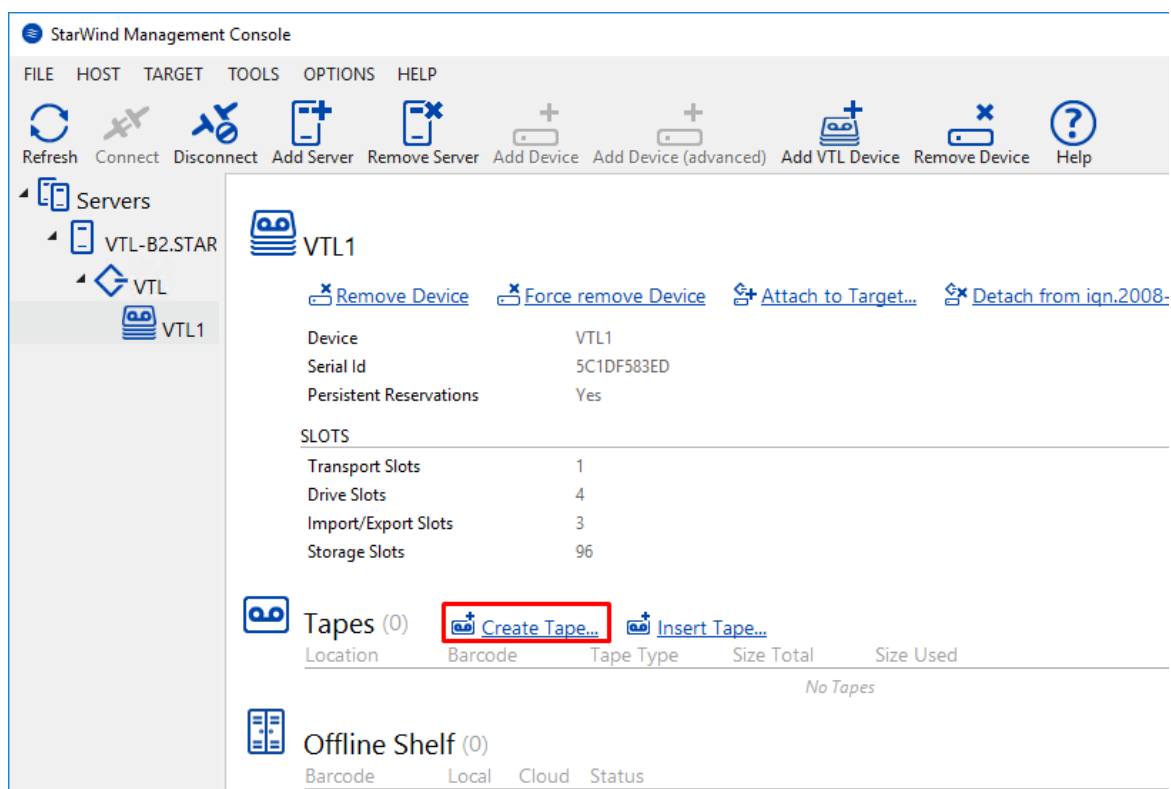
☒ Allow multiple concurrent iSCSI Connections

Next Cancel

9. Press the Create button to start the creation process.

10. Once the device creation is completed, click Close.

11. Once the VTL device is created, the tapes can be added. To do this, select the VTL device and click the Create Tape button located in the Tapes section.



12. The Create Tape wizard will appear. Optionally, select the checkbox and specify the custom path where the tape files must be stored.

13. Specify the Number of Tapes, Tape Type, and other parameters and click the Create button. It's possible to customize the tape parameters.

← Create Tape

Specify Tape Parameters

☐ Custom Barcode

Barcode

Number of Tapes

Tape Type

☐ Custom Tape Size

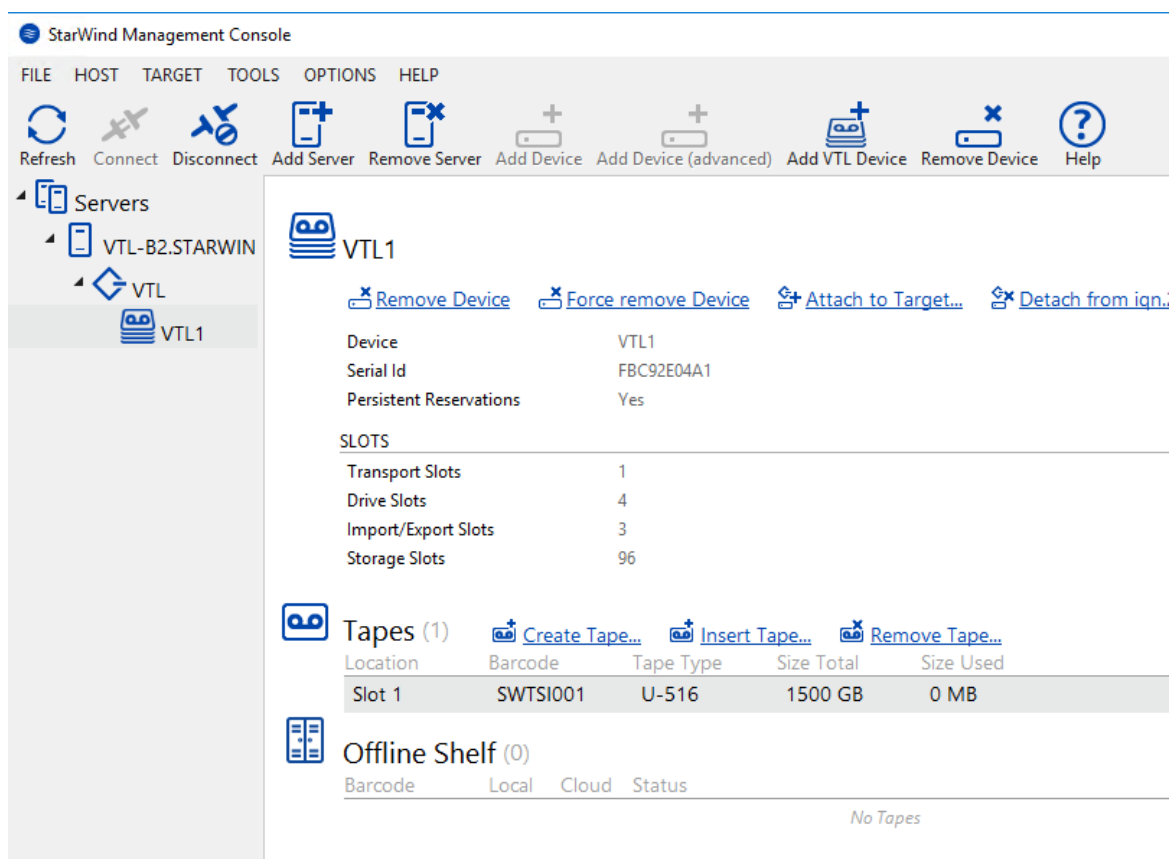
Tape Size GB

☐ Split Into Parts

Part Size GB

Create Cancel

14. The created tape appears in the first slot of the VTL device in the StarWind Management Console.



If required, create new tapes in the same way.

Selecting The Cloud Storage Provider

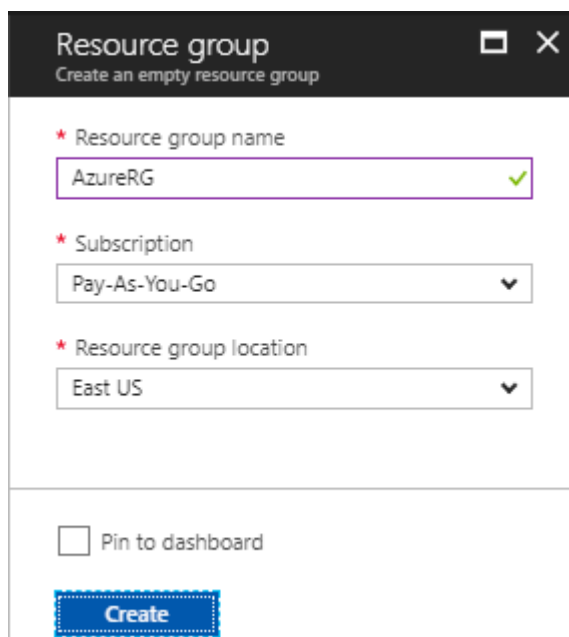
To further proceed with configuring StarWind VTL Cloud Replication, please select the cloud storage provider of your choice:

Microsoft Azure

Getting Cloud Account Credentials in Microsoft Azure Cloud Storage

1. From a browser, navigate to the [Azure portal](#) and sign in with your Azure account.
2. Create a Resource group in the Azure portal. It's a container that collects related resources for an Azure solution, or those resources that ought to be managed as a group. Make sure you have selected the location with minimal network latency.
3. In the portal, click New. In the Search the marketplace field, type "Resource group".

Locate Resource group from the returned list and click it to open the Resource group window. Near the bottom of the Resource group window, click Create.



The screenshot shows a window titled "Resource group" with the subtitle "Create an empty resource group". It contains three required fields, each marked with a red asterisk:

- Resource group name:** A text input field containing "AzureRG" with a green checkmark icon on the right.
- Subscription:** A dropdown menu showing "Pay-As-You-Go" with a downward arrow.
- Resource group location:** A dropdown menu showing "East US" with a downward arrow.

Below these fields is a checkbox labeled "Pin to dashboard" which is currently unchecked. At the bottom of the window is a blue button with the text "Create".

4. Navigate to Resource group and select it. In the top menu, select Add. In the Search the marketplace field, type "Virtual Network". Locate Virtual Network from the returned list and click it to open the Virtual Network window. Use Resource Manager as a deployment model.

Create virtual network

Name

AzureVNet1

✓

Address space ⓘ

10.10.0.0/25

✓

10.10.0.0 - 10.10.0.127 (128 addresses)

Subscription

Pay-As-You-Go

▼

Resource group

☐ Create new
 ☒ Use existing

AzureRG

▼

Location

East US

▼

Subnet

Name

default

Address range ⓘ

10.10.0.0/26

✓

10.10.0.0 - 10.10.0.63 (64 addresses)

☐ Pin to dashboard

Create

Automation options

5. In the Search the marketplace field, type “Storage account”. Locate “Storage account – blob, file, table, queue” from the returned list and click it to open the Storage account window.

6. Select the account type as StorageV2 (general purpose v2).

7. Specify the performance tier: Standard or Premium. Select Replication plan.

8. Specify default Access tier: Hot or Cool. Click here for [more details](#).

Create storage account

The cost of your storage account depends on the usage and the options you choose below.
[Learn more](#)

* Name ⓘ

starwindvtl01

✓

.core.windows.net

Deployment model ⓘ

Resource manager

Classic

Account kind ⓘ

StorageV2 (general purpose v2)

▼

* Location

East US

▼

Replication ⓘ

Read-access geo-redundant storage (RA-...

▼

Performance ⓘ

Standard

Premium

Access tier (default) ⓘ

Cool

Hot

* Secure transfer required ⓘ

Disabled

Enabled

* Subscription

Pay-As-You-Go

▼

* Resource group

☐ Create new
 ☒ Use existing

AzureRG

▼

Virtual networks

Configure virtual networks ⓘ

Disabled

Enabled

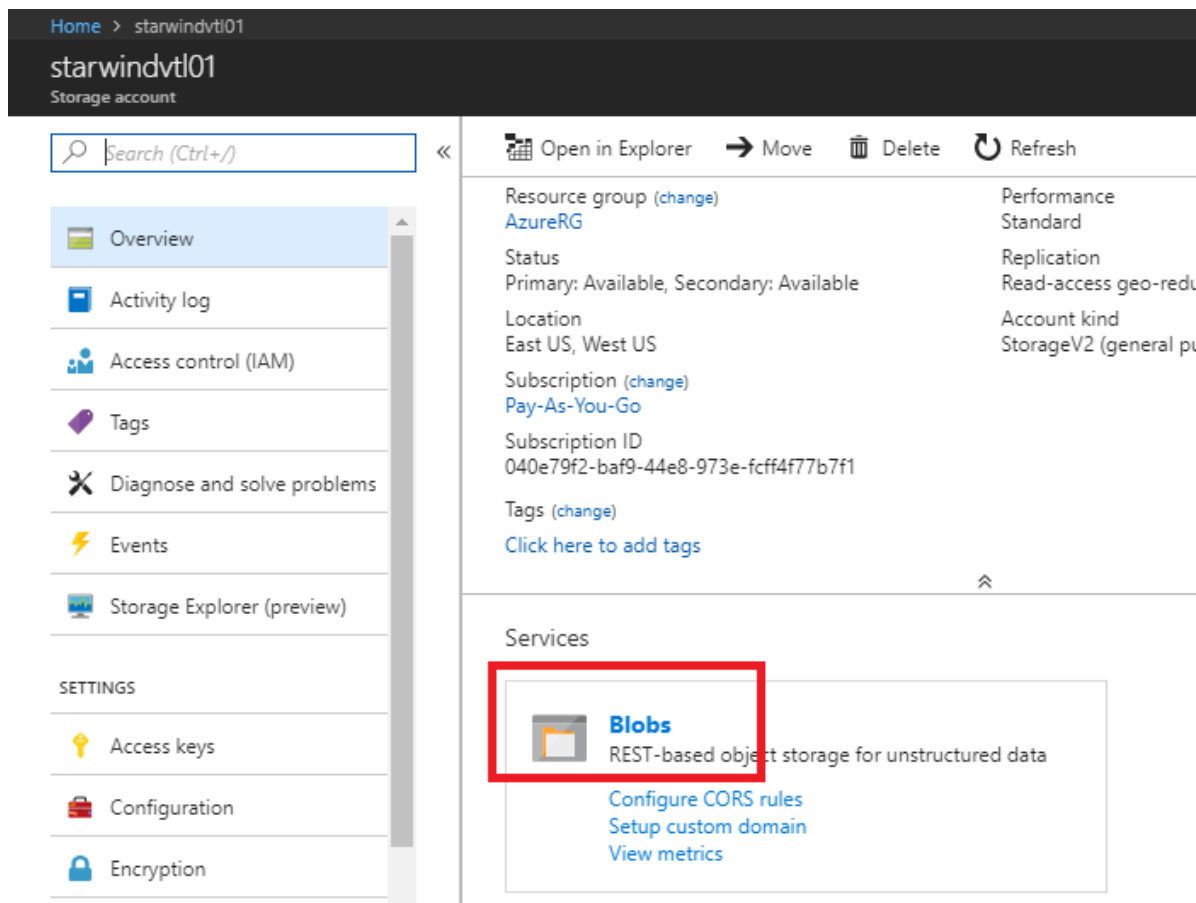
☐ Pin to dashboard

Create

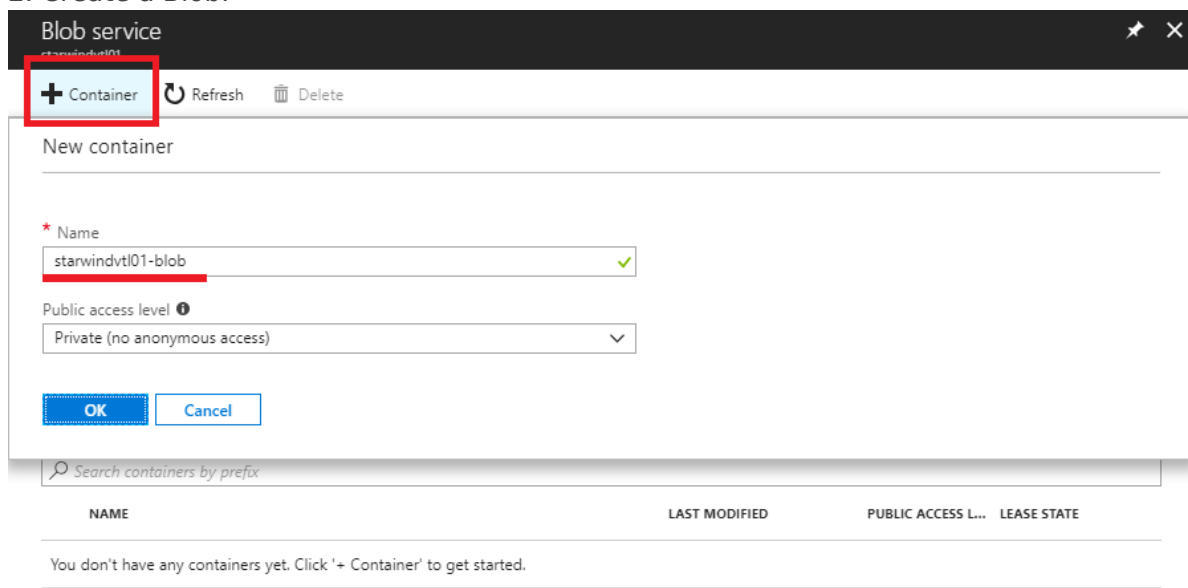
Automation options

Creating Microsoft Azure Blob

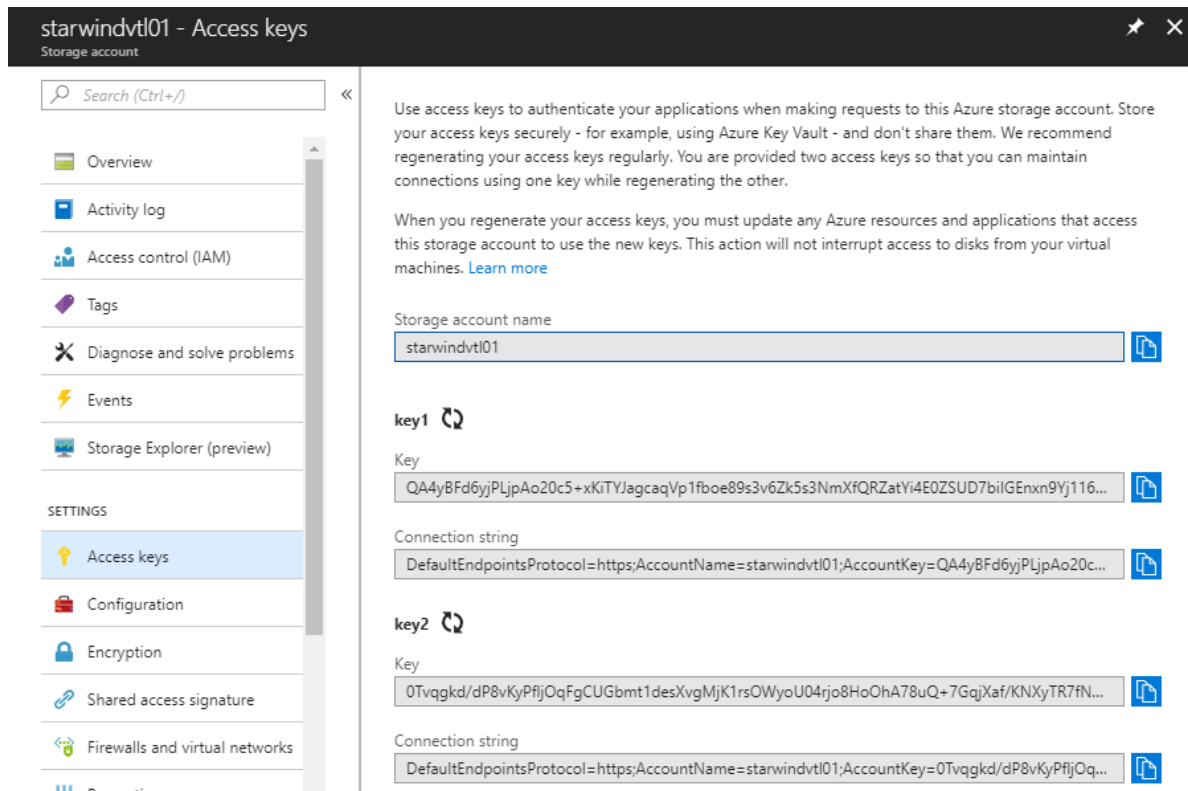
1. Open a storage account. Navigate to Blobs.



2. Create a Blob.



3. Go back to the storage account. Open Access Keys.



4. Click copy key1 or key2 to get access.

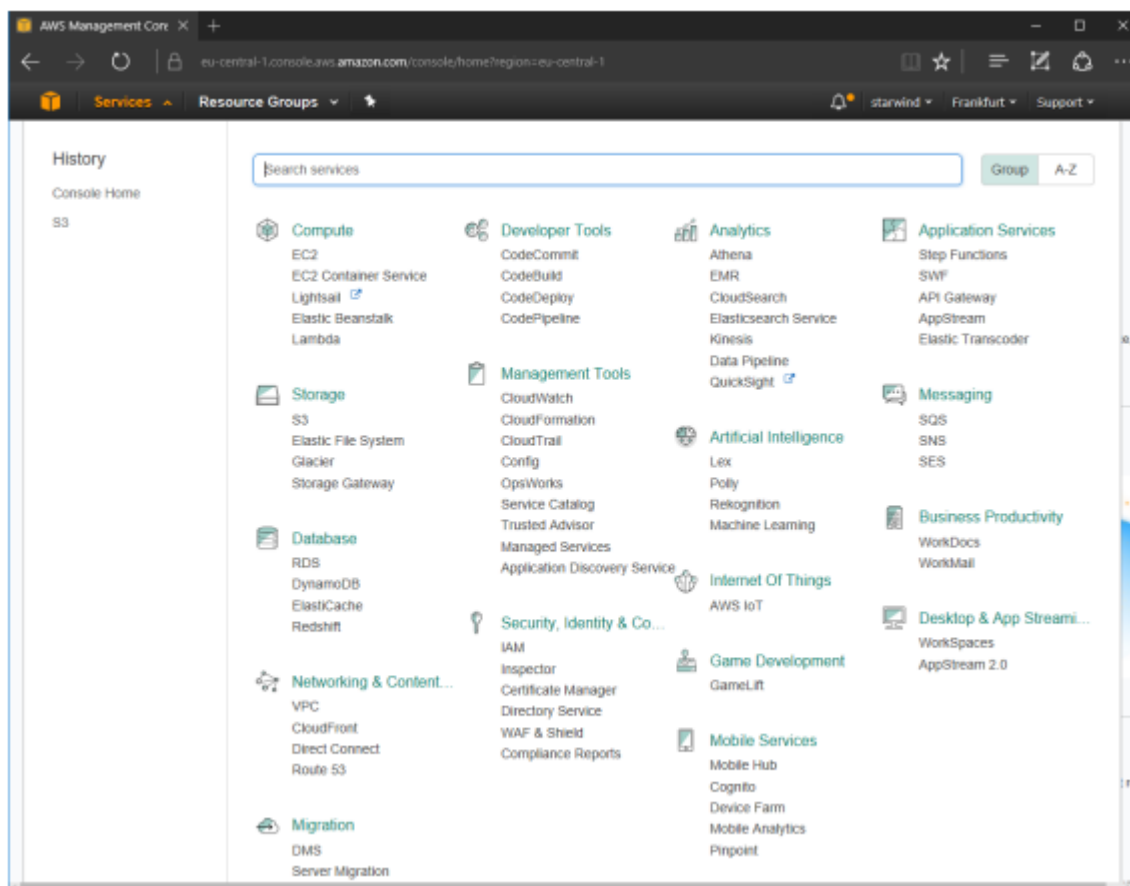
NOTE: When generating a new access key, the old one will no longer work.

5. To proceed with configuring StarWind VTL Cloud Replication, please return to the Configuring Cloud Replication section.

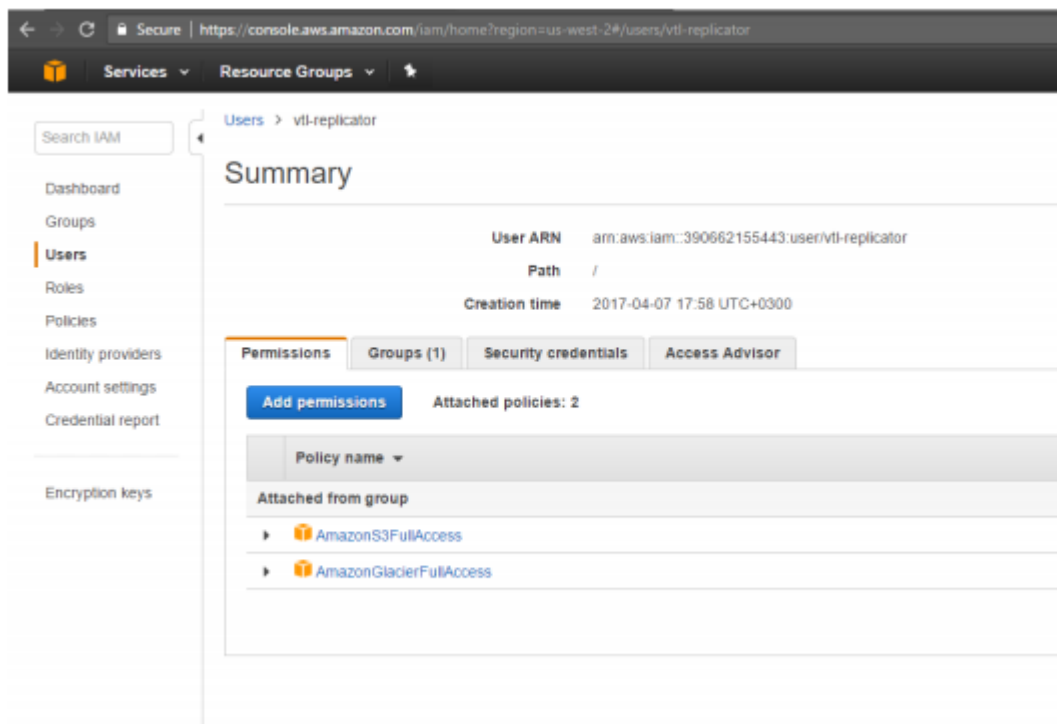
Amazon Web Services (Aws)

Getting Access Key ID and Secret Access Key in AWS

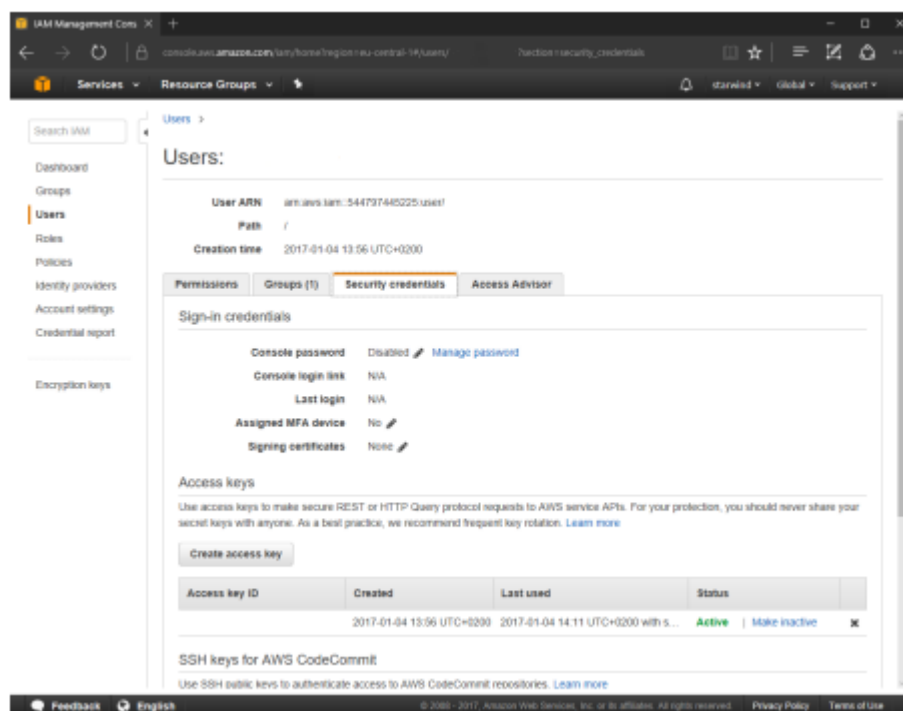
1. To get the Access key ID and Secret access key, launch AWS Management Console.
2. Then click Services -> Security, Identity & Compliance -> IAM.



3. Click Users, select the existing User or create the new one.
4. Make sure to assign necessary Permissions to the corresponding User.



5. In the User's profile, click the Security Credentials and press the Create access key button.



6. Click Show in the Secret access key field.

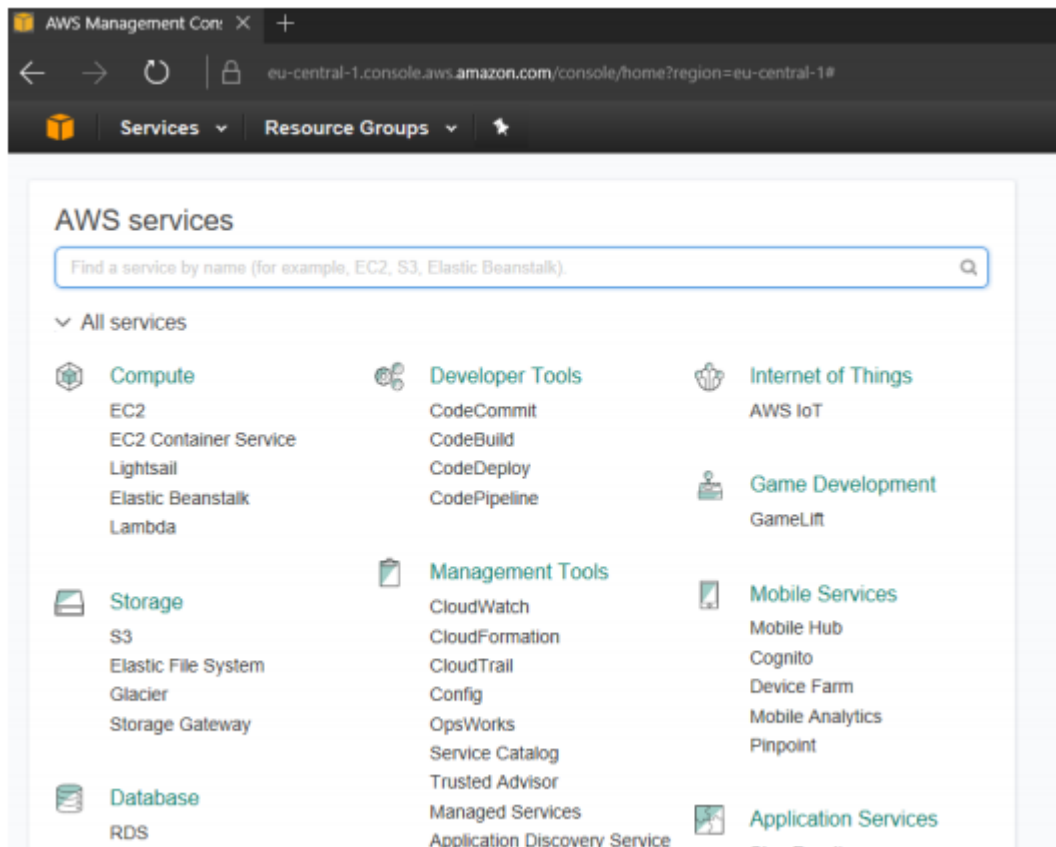
NOTE: Save the Access key ID and Secret access key as this information will be used during the configuration process.

NOTE: In some cases, the user might need to have restricted access to the cloud

resources. Please follow the guide here to change the user's permissions:
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users_change-permissions.html

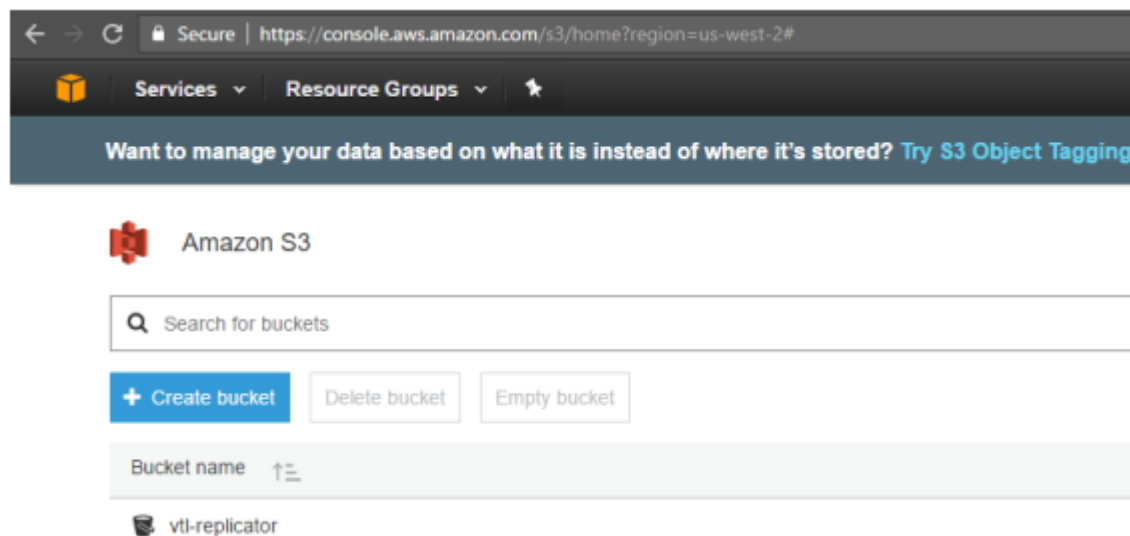
Creating Amazon S3 Bucket

1. To create Amazon S3 bucket, select Storage and S3, and click the Create Bucket button.



3. Enter an appropriate Bucket Name, choose the Region in a drop-down menu and click Create.

4. The newly created bucket will appear in the list.

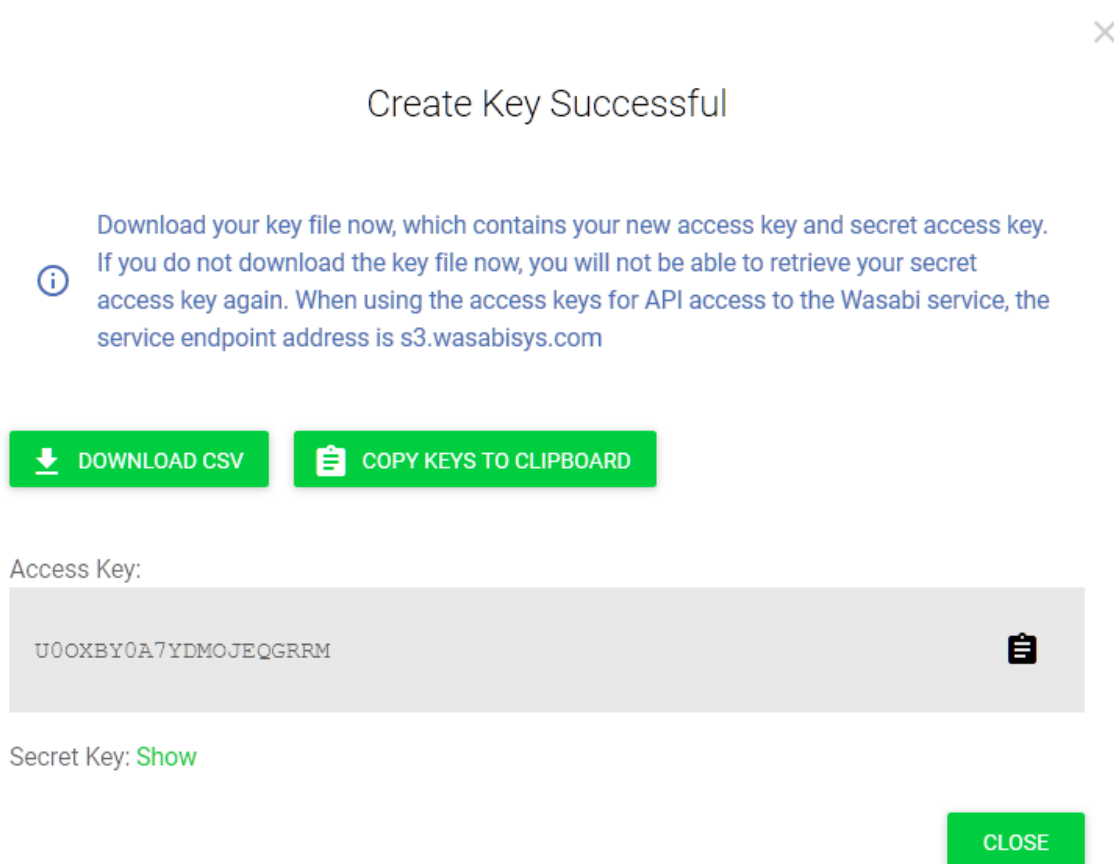


5. To proceed with configuring StarWind VTL Cloud Replication, please return to the Configuring Cloud Replication section.

Wasabi

Getting Account ID and Application Key in Wasabi Cloud Storage

1. Sing up to Wasabi using the following link: <https://wasabi.com/>
2. In the left-side menu of the Wasabi console, go to Access Keys and click on Create New Access Key.



3. Press DOWNLOAD CSV or COPY KEYS TO CLIPBOARD to save the values.



Create Key Successful



Download your key file now, which contains your new access key and secret access key.
If you do not download the key file now, you will not be able to retrieve your secret access key again. When using the access keys for API access to the Wasabi service, the service endpoint address is s3.wasabisys.com



DOWNLOAD CSV



COPY KEYS TO CLIPBOARD

Access Key:

JADK4DN2A5D9UBX00NKX



Secret Key: [Hide](#)

9gUD3MFy31srhzzaEzgnEL1PRScKvFakApoydbef

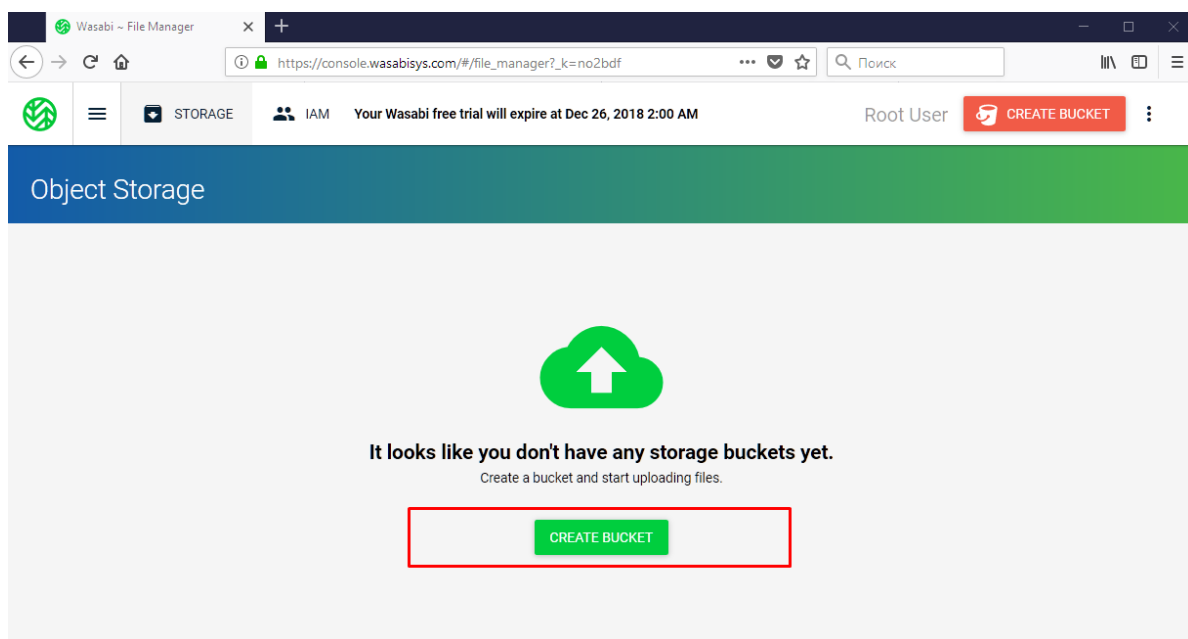


CLOSE

NOTE: Make sure the keys are saved, as it is not possible to view the Secret Key once again after pressing the Close button.

Creating Wasabi Bucket

1. To create the Wasabi bucket, open the Buckets section and click the CREATE BUCKET button.



2. Specify the Bucket Name and click the Create Bucket button.

✕

Create Bucket

1 Bucket Name
2 Set Properties
3 Review

Select Bucket Name

Bucket Name
starwindvtl

Select Region

Region
us-east-1

CREATE BUCKET
CANCEL
NEXT

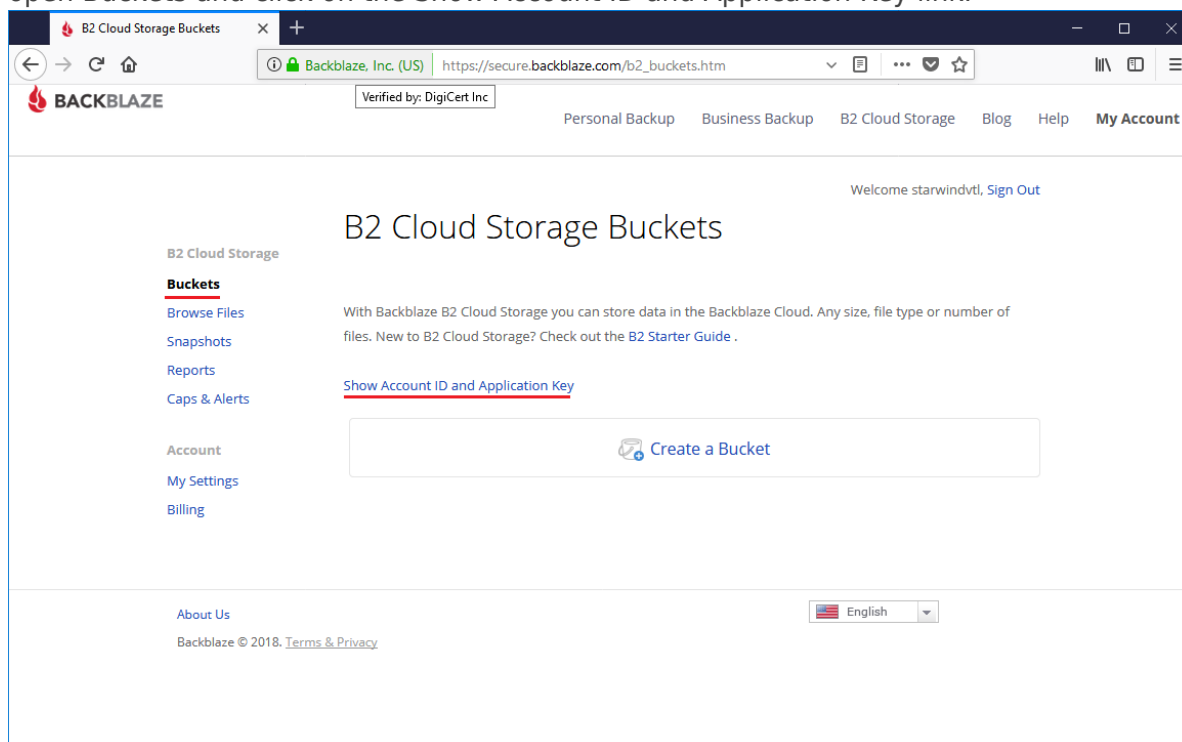
3. To proceed with configuring StarWind VTL Cloud Replication, please navigate to the Configuring Cloud Replication section.

Backblaze B2 Cloud Storage

Getting Account ID and Application Key in Backblaze B2 Cloud Storage

1. Sing up to Backblaze B2 Cloud Storage using the following link: <https://www.backblaze.com/b2/cloud-storage.html>

2. To get the Account ID and Application Key, sing into Backblaze B2 Cloud Storage, open Buckets and click on the Show Account ID and Application Key link.

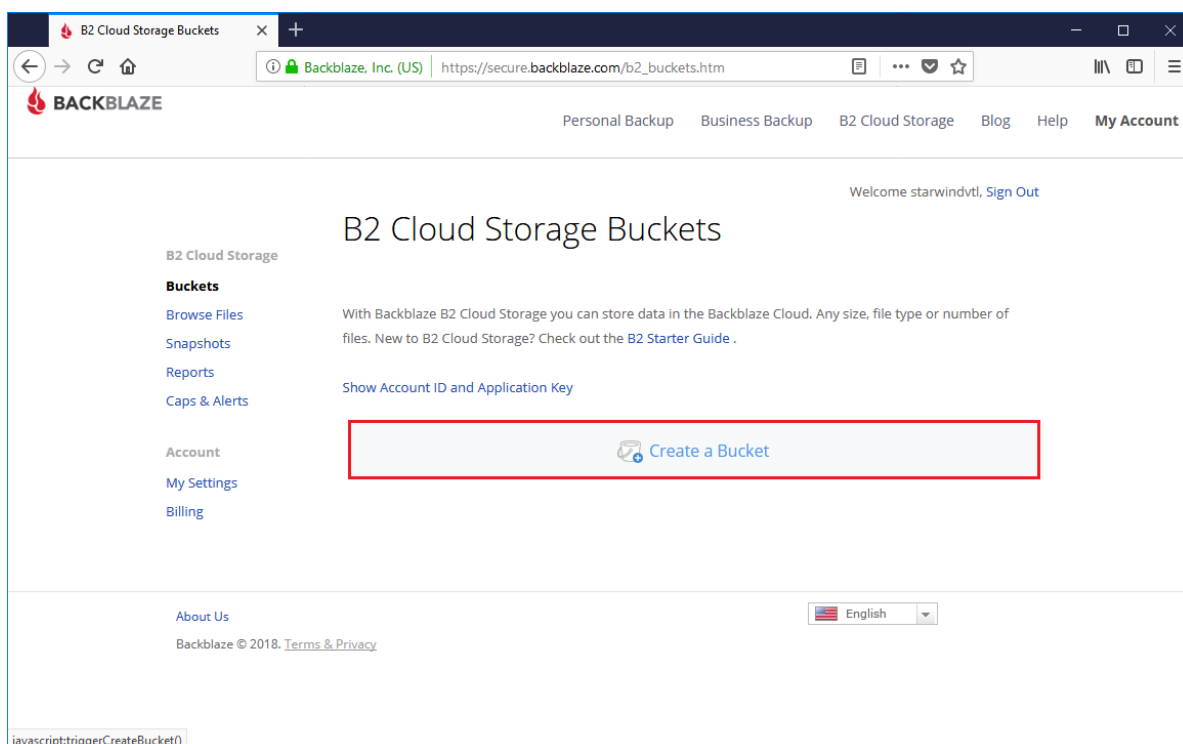


3. Click Create Application Key to get it.

NOTE: When you create a new application key, the old one will no longer work.

Creating Backblaze B2 Cloud Storage Bucket

1. To create the B2 Cloud Storage Bucket, open the Buckets section and click on the Create a Bucket button.



2. Specify a Bucket Unique Name and click on the Create a Bucket button.

×

Create a Bucket

All files must be in a bucket. There are no charges for creating a bucket. Only 100 buckets can be created per account. Each bucket name must be at least 6 characters long.

Bucket Unique Name:

Files in Bucket are: ☒ Private ☐ Public

Create a Bucket

Cancel

3. Once the bucket is created, click on the Lifecycle Settings button to specify the

custom lifecycle rules.

B2 Cloud Storage

Buckets

[Browse Files](#)

[Snapshots](#)

[Reports](#)

[Caps & Alerts](#)

Account

[My Settings](#)

[Billing](#)

B2 Cloud Storage Buckets

With Backblaze B2 Cloud Storage you can store data in the Backblaze Cloud. Any size, file type or number of files. New to B2 Cloud Storage? Check out the [B2 Starter Guide](#).

[Show Account ID and Application Key](#)

 [Create a Bucket](#)



StarWindVTL

[Upload/Download](#)

Created: January 12, 2018
Bucket ID: b7c754dc66a0edbb670c071a
Type: Private
File Lifecycle: Keep all versions
Snapshots: 0
Current Files: 0
Current Size: 0 bytes

[Bucket Settings](#)


[Lifecycle Settings](#)

[CORS Rules](#)

4. In Lifecycle Settings, choose Use custom lifecycle rules, edit rules, and click Update Bucket.

✕

Lifecycle Settings


 You can control how long to keep files in your B2 bucket - [Learn More](#).


☐ Keep all versions of the file (default)

☐ Keep only the last version of the file

☐ Keep prior versions for this number of days:

☒ Use custom lifecycle rules:

 Add Lifecycle Rules

File Path <small>fileNamePrefix</small>	Days Till Hide <small>daysFromUploadingToHiding</small>	Days Till Delete <small>daysFromHidingToDeleting</small>
<div style="display: flex; align-items: center;"> <div style="margin-right: 10px;"></div> <input style="width: 100%;" type="text"/> </div>	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>

Update Bucket

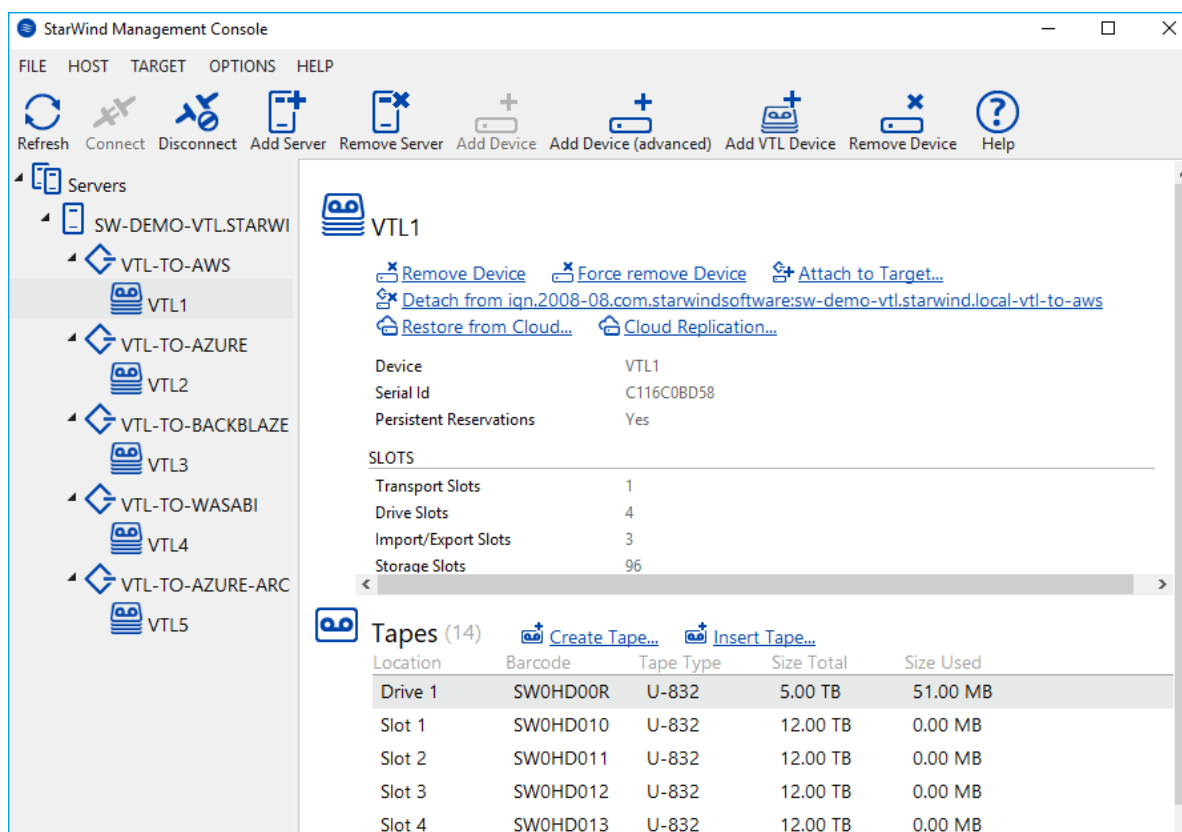
Cancel

Changes take effect in approximately **10 minutes**.

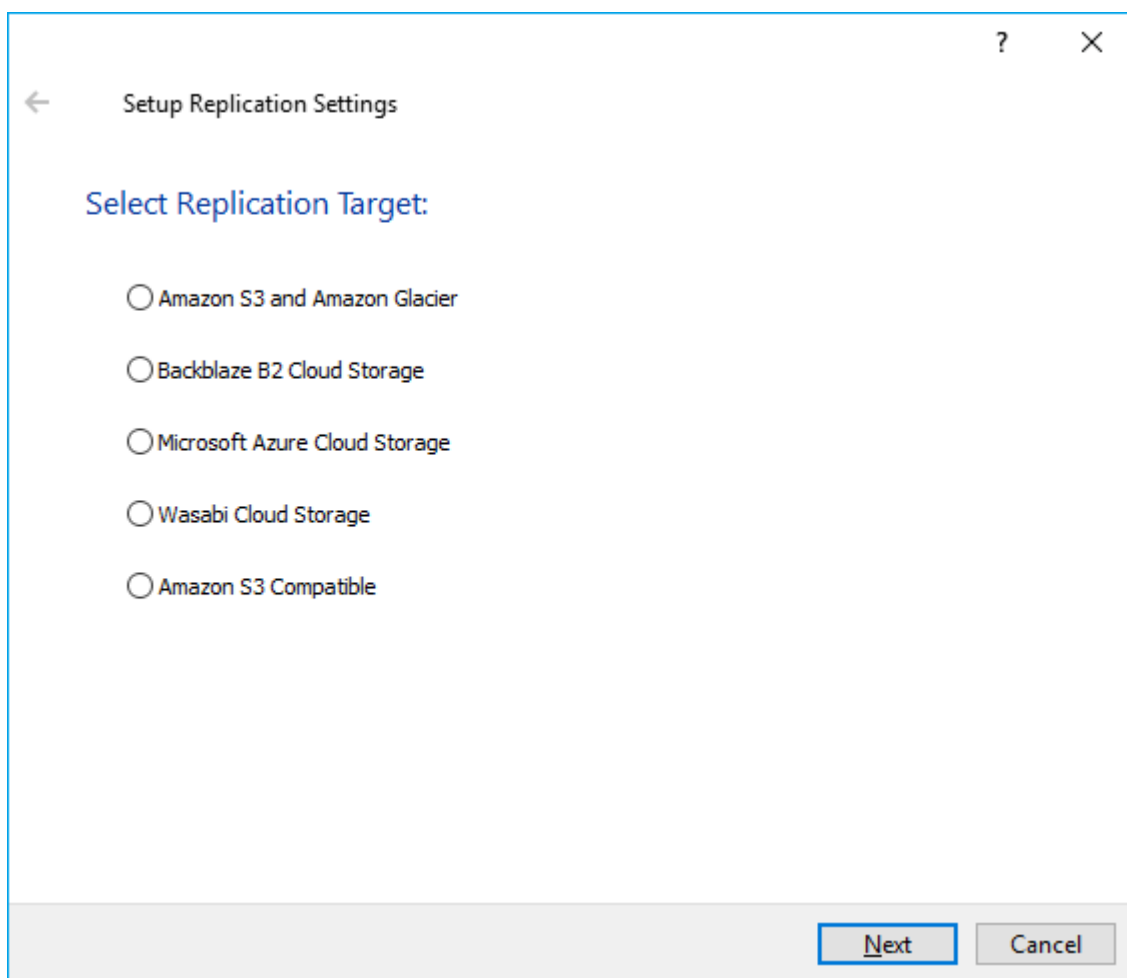
5. To proceed with configuring StarWind VTL Cloud Replication, please navigate to the Configuring Cloud Replication section.

Configuring Cloud Replication

1. To enable the replication between StarWind and cloud storage, navigate to the VTL device and click Cloud Replication.



2. Choose the required cloud storage and click Next.



Amazon S3 And Amazon Glacier

1. In the Replication Settings, specify Access Key ID, Secret Access Key, Bucket and Region obtained and configured previously and press the Next button.

Setup Replication Settings

Specify Credentials for Replication Target Access

Access Key ID: AKIAJB6A6AIFG2MF2LYQ

Secret Access Key: ●●●●●●●●●●●●●●●●●●●●

Bucket: starwind-vtl-demo

Region: US Standard (US East (N. Virginia))

Next Cancel

2. Specify Tape File Retention Settings and click Apply. Optionally, select Create new empty tapes automatically when the existing tape is exported for replication.

Setup Replication Settings

Tape File Retention Settings

Start replication to cloud after the tape removed from drive, days:
Replicate Immediately

☒ Create new empty tapes automatically when existing tape removed from VTL for replication.

Keep local copy after the file has been replicated, days:
Delete Immediately

Keep copy in cloud storage after the file has been replicated, days:
Set Value 14

Keep file in S3 before moving to Glacier, days:
Set Value 14

Apply Cancel

3. The automatic tape replication to the cloud storage is successfully configured according to the retention policy specified above.
IMPORTANT NOTE: Retention settings should be configured according to your corporate RTO and RPO requirements.

Backblaze B2 Cloud Storage

1. In the Replication Settings, specify Key ID, applicationKey, Bucket obtained and configured previously and press the Next button.

Setup Replication Settings

Specify Credentials for Replication Target Access

keyID: 19c4510ace47

applicationKey:

Bucket: SW-VTL-Demo

Next Cancel

2. Specify Tape File Retention Settings and click Apply. Optionally, select Create new empty tapes automatically when the existing tape is exported for replication.

Setup Replication Settings

Tape File Retention Settings

Start replication to cloud after the tape removed from drive, days:
Replicate Immediately

☒ Create new empty tapes automatically when existing tape removed from VTL for replication.

Keep local copy after the file has been replicated, days:
Delete Immediately

Keep copy in cloud storage after the file has been replicated, days:
Never Delete

Apply Cancel

3. The automatic tape replication to the cloud storage is successfully configured according to the retention policy specified above.
IMPORTANT NOTE: Retention settings should be configured according to your corporate RTO and RPO requirements.

Microsoft Azure Cloud Storage

1. In the Replication Settings, specify Storage Account, Key, Container, Region obtained and configured previously and press the Next button.

Setup Replication Settings

Specify Credentials for Replication Target Access

Storage Account: demovtl

Key:

Container: demo-container

Region: Public

Next Cancel

2. Specify Tape File Retention Settings and click Apply. Optionally, select Create new empty tapes automatically when the existing tape is exported for replication.

Setup Replication Settings

Tape File Retention Settings

Start replication to cloud after the tape removed from drive, days:
Replicate Immediately

☒ Create new empty tapes automatically when existing tape removed from VTL for replication.

Keep local copy after the file has been replicated, days:
Delete Immediately

Keep copy in cloud storage after the file has been replicated, days:
Set Value 30

Keep file in Hot access tier before moving to Cool, days:
Set Value 14

Keep file in Cool access tier before moving to Archive, days:
Set Value 14

Apply Cancel

3. The automatic tape replication to the cloud storage is successfully configured according to the retention policy specified above.
IMPORTANT NOTE: Retention settings should be configured according to your corporate RTO and RPO requirements.

Wasabi Cloud Storage

1. In the Replication Settings, specify Access Key, Secret Key, Bucket, Region obtained and configured previously and press the Next button.

Setup Replication Settings

Specify Credentials for Replication Target Access

Access Key: bSTVO1DFHMK5J6I07OLO

Secret Key:

Bucket: demovtl

Region: US Standard (USEast1) ▼

Next Cancel

2. Specify Tape File Retention Settings and click Apply. Optionally, select Create new empty tapes automatically when the existing tape is exported for replication.

Setup Replication Settings

Tape File Retention Settings

Start replication to cloud after the tape removed from drive, days:
Replicate Immediately

☒ Create new empty tapes automatically when existing tape removed from VTL for replication.

Keep local copy after the file has been replicated, days:
Delete Immediately

Keep copy in cloud storage after the file has been replicated, days:
Never Delete

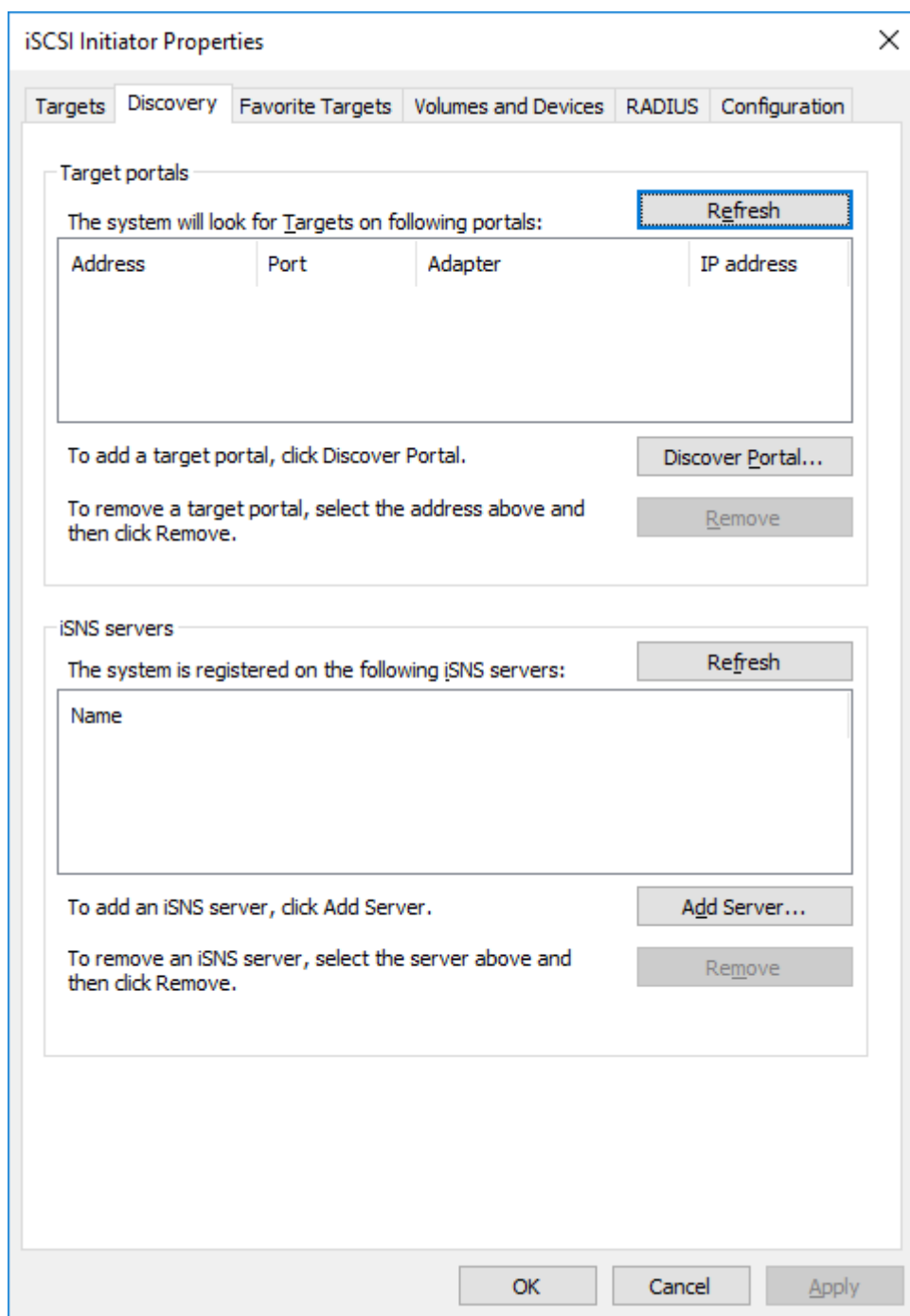
Apply Cancel

3. The automatic tape replication to the cloud storage is successfully configured according to the retention policy specified above.
IMPORTANT NOTE: Retention settings should be configured according to your corporate RTO and RPO requirements.

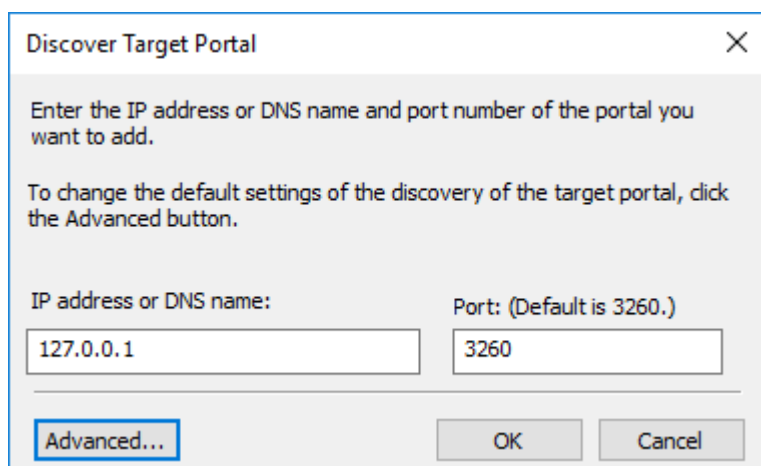
Mounting Vtl On The Backup Host

To pass-through the VTL device to the Windows server with the backup software provider, the corresponding VTL iSCSI target should be mounted first.

1. Open Microsoft iSCSI Initiator, navigate to the Discovery tab, and press the Discover Portal button.



2. Enter the localhost address (127.0.0.1) and press the Advanced button.

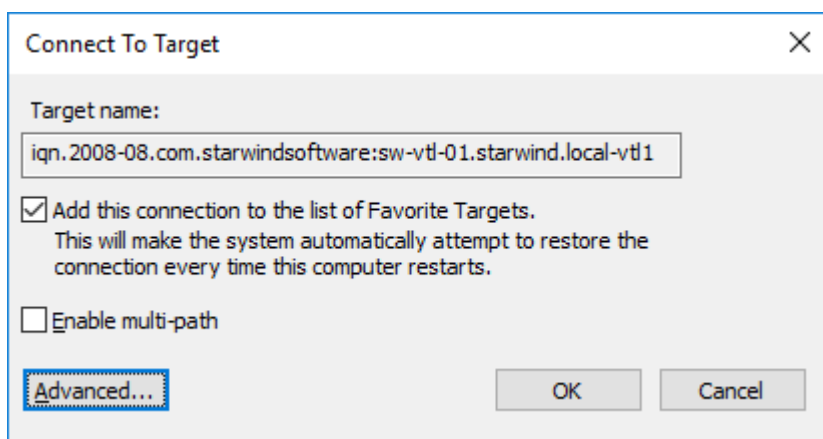


The image shows a 'Discover Target Portal' dialog box with a close button (X) in the top right corner. Inside the dialog, there is instructional text: 'Enter the IP address or DNS name and port number of the portal you want to add.' and 'To change the default settings of the discovery of the target portal, click the Advanced button.' Below this text are two input fields. The first field is labeled 'IP address or DNS name:' and contains the text '127.0.0.1'. The second field is labeled 'Port: (Default is 3260.)' and contains the text '3260'. At the bottom of the dialog, there are three buttons: 'Advanced...' (highlighted with a blue border), 'OK', and 'Cancel'.

3. Select Microsoft iSCSI Initiator from the Local Adapter drop-down list and press OK.

The screenshot shows the 'Advanced Settings' dialog box with the 'IPsec' tab selected. The 'General' tab is also visible. The 'Connect using' section has three dropdown menus: 'Local adapter' set to 'Microsoft iSCSI Initiator', 'Initiator IP' set to 'Default', and 'Target portal IP' set to an empty dropdown. The 'CRC / Checksum' section has two checkboxes: 'Data digest' and 'Header digest', both unchecked. The 'Enable CHAP log on' checkbox is also unchecked. The 'CHAP Log on information' section contains a text box for 'Name' with the value 'iqn.1991-05.com.microsoft:vtl.starwind.local' and an empty 'Target secret' text box. Below this, there are three more checkboxes: 'Perform mutual authentication' (unchecked), 'Use RADIUS to generate user authentication credentials' (unchecked), and 'Use RADIUS to authenticate target credentials' (unchecked). The dialog box has 'OK', 'Cancel', and 'Apply' buttons at the bottom right.

4. The newly added Discovery Portal will appear in the list.
5. Navigate to the Targets tab, find the iSCSI target which corresponds to the StarWind VTL device, and press the Connect button.
6. Leave the Enable Multipath checkbox empty and press the Advanced button.



7. Set Local adapter as Microsoft iSCSI Initiator, specify 127.0.0.1 / 3260 as Target portal IP and double-click the OK button to complete the target connection.

Advanced Settings

General **IPsec**

Connect using

Local adapter: Microsoft iSCSI Initiator

Initiator IP: Default

Target portal IP: 127.0.0.1 / 3260

CRC / Checksum

☐ Data digest ☐ Header digest

☒ Enable CHAP log on

CHAP Log on information

CHAP helps ensure connection security by providing authentication between a target and an initiator.

To use, specify the same name and CHAP secret that was configured on the target for this initiator. The name will default to the Initiator Name of the system unless another name is specified.

Name: iqn.1991-05.com.microsoft:sw-vtl-01.starwind.local

Target secret:

☐ Perform mutual authentication

To use mutual CHAP, either specify an initiator secret on the Configuration page or use RADIUS.

☐ Use RADIUS to generate user authentication credentials

☐ Use RADIUS to authenticate target credentials

OK Cancel Apply

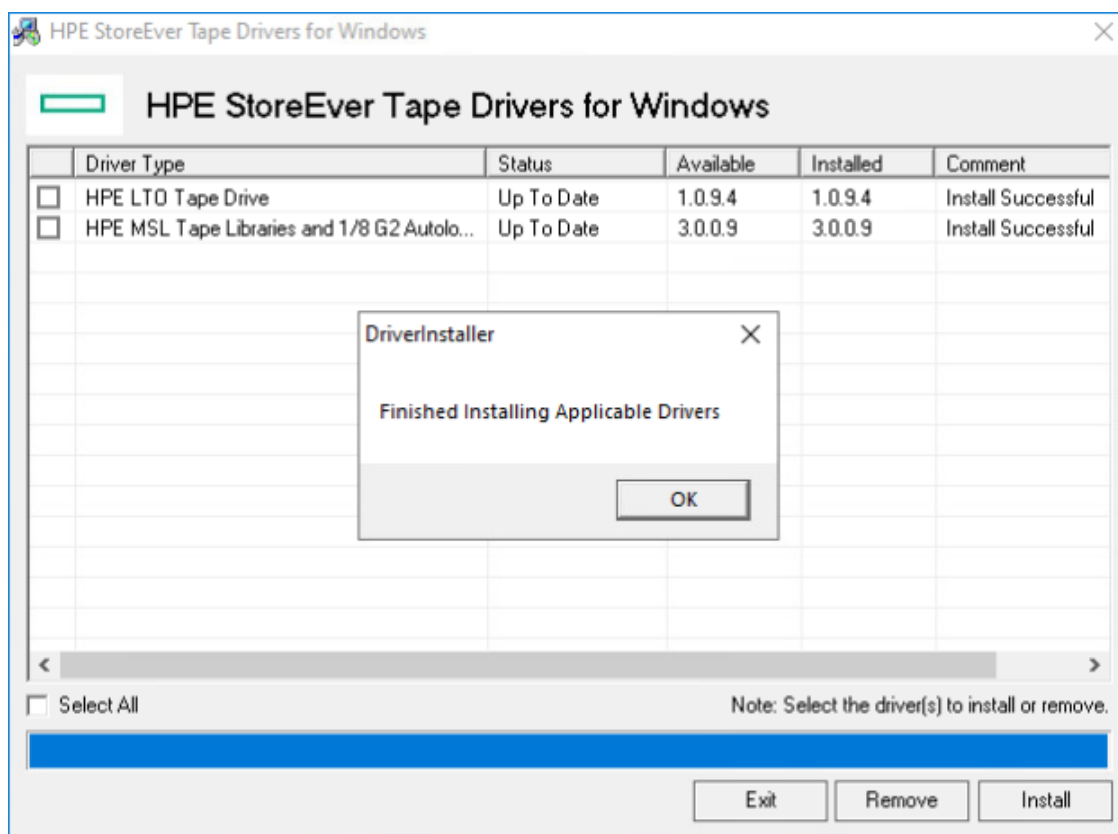
The VTL iSCSI target should be shown as Connected in the list.

Installing tape library drivers

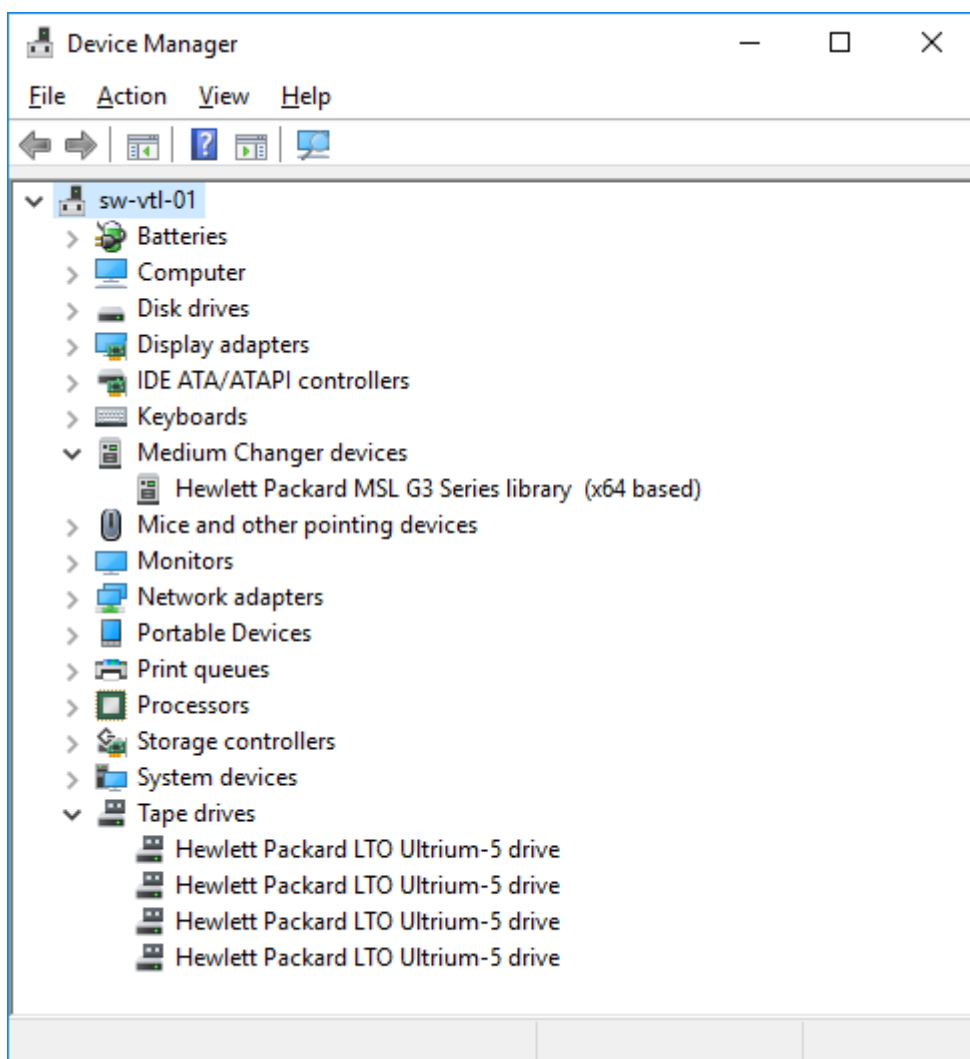
It's recommended to install the latest update driver from HP. The driver for HP MSL8096 can be downloaded here:

[HPE StoreEver Tape Drivers for Microsoft Windows](#). The current version that supports Windows Server 2022 is 4.6.0.0. HP drivers must be installed on the host (localhost in this example) where StarWind VTL device is mounted via iSCSI.

1. Extract the downloaded driver and launch cpqsetup.exe.
2. Choose the Select All checkbox and click Install.



3. Once the drivers are installed, the Medium Changer devices is shown as Hewlett Packard MSL G3 Series library (x64 based).



The tape library is ready to be added to the server with the backup software provider.

Backing Up To Starwind Virtual Tapes

Choose the required backup software provider to add StarWind Virtual Tape Library to:

Microsoft System Center Data Protection Manager

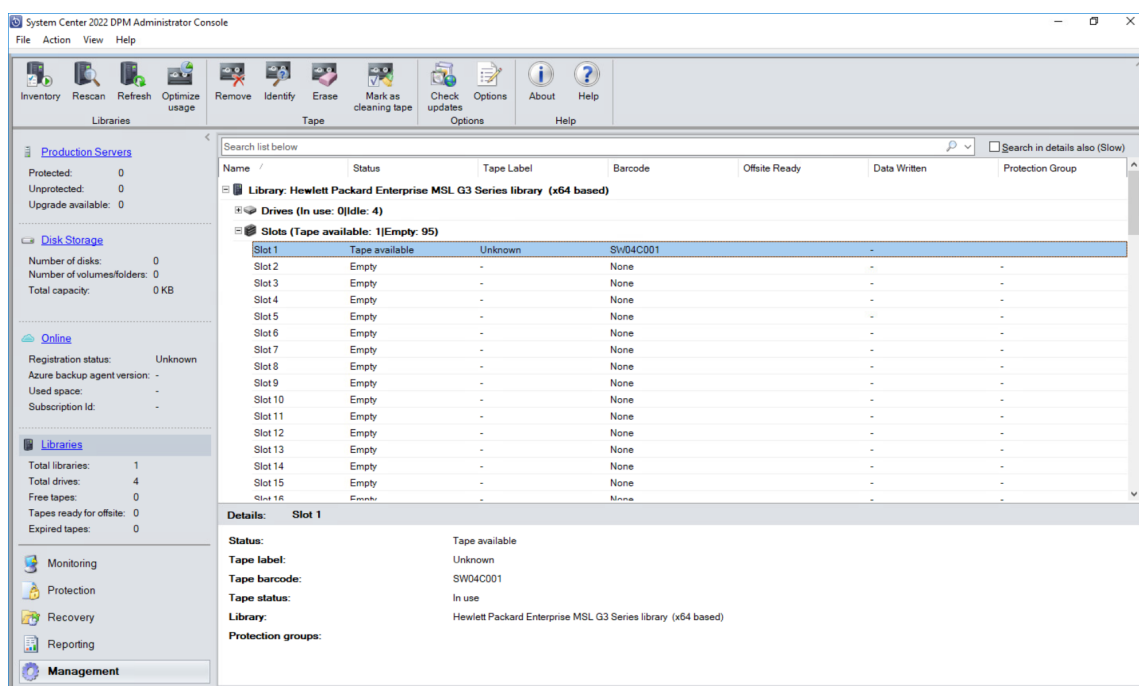
Adding StarWind VTL Device to Microsoft SCDPM

In case of any question regarding Microsoft SCDP deployment, please refer the following link:

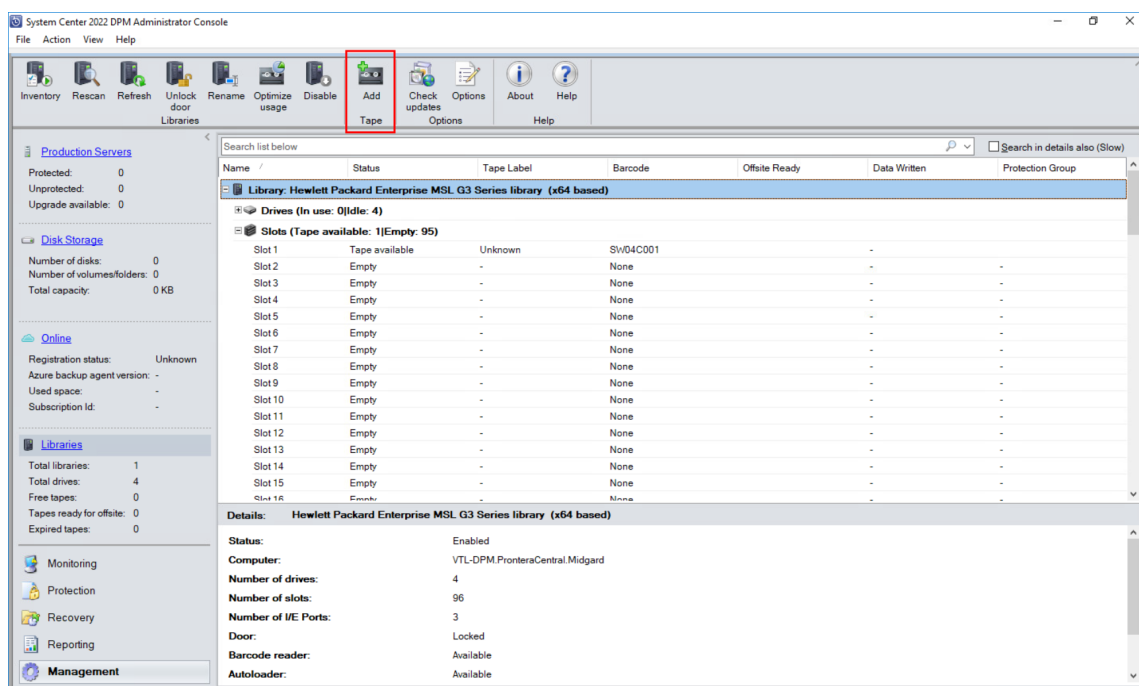
<https://docs.microsoft.com/en-us/system-center/dpm/install-dpm?view=sc-dpm-1807>

1. DPM automatically detects tape devices that are attached to it and they are displayed in the Libraries workspace of the Management view. If the tape isn't displayed, it can be detected manually with the Rescan button.

2. After the rescan, check that the details displayed in Device Manager and in the tape library are the same.

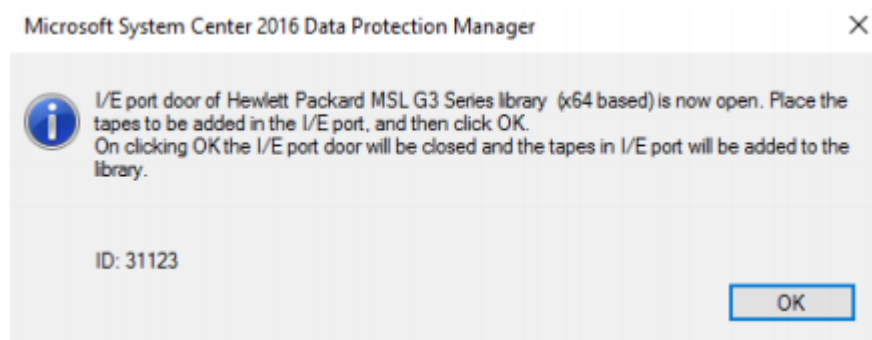


3. To add more tapes, select the tape library in the Libraries workspace of the Management view, and then click Add.



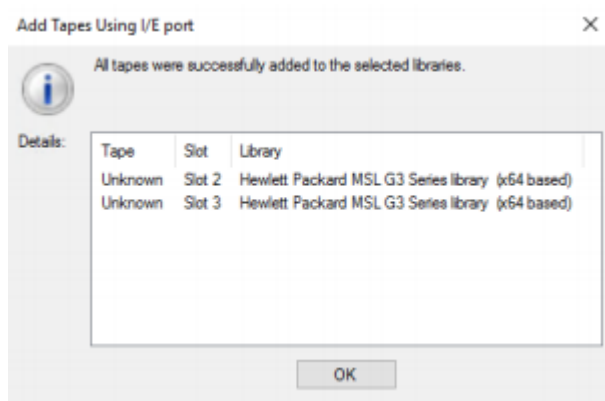
4. The I/E port door named “Hewlett Packard MSL G3 Series library” will be opened, and more tapes can be created using StarWind management console as described in the previous steps.

NOTE: Do not press OK in case more tapes need to be created.

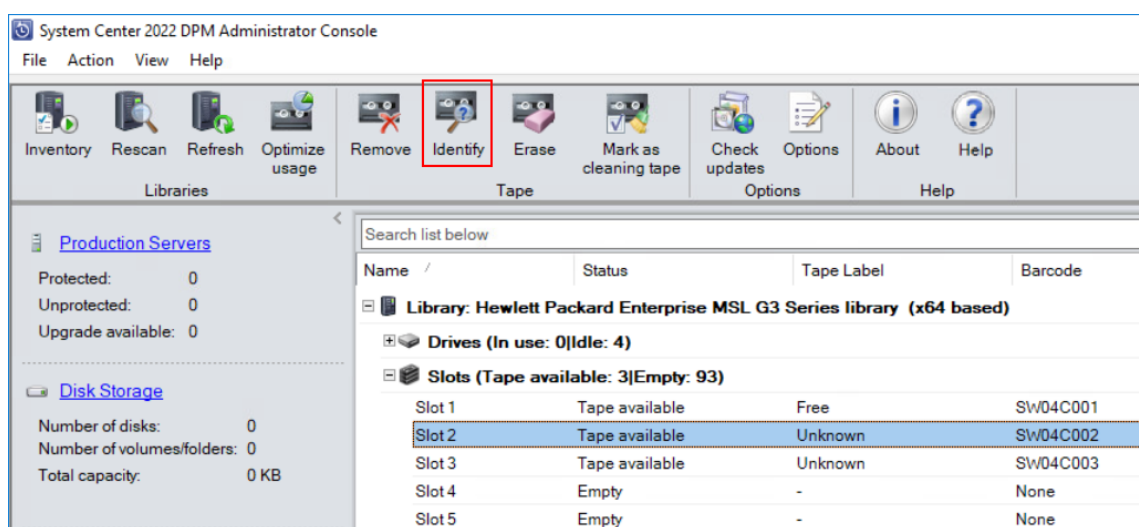


NOTE: While adding/removing tapes to the tape library using the Unlock library door or Add tape, DPM will automatically inventory the library. While adding/removing tapes to the tape library without using Unlock library door or Add tape, the Inventory library action must be used to update the information in DPM Administrator Console.

5. Once the tapes are created using StarWind management console, press OK. DPM will detect the newly added tapes as shown in the screenshot.

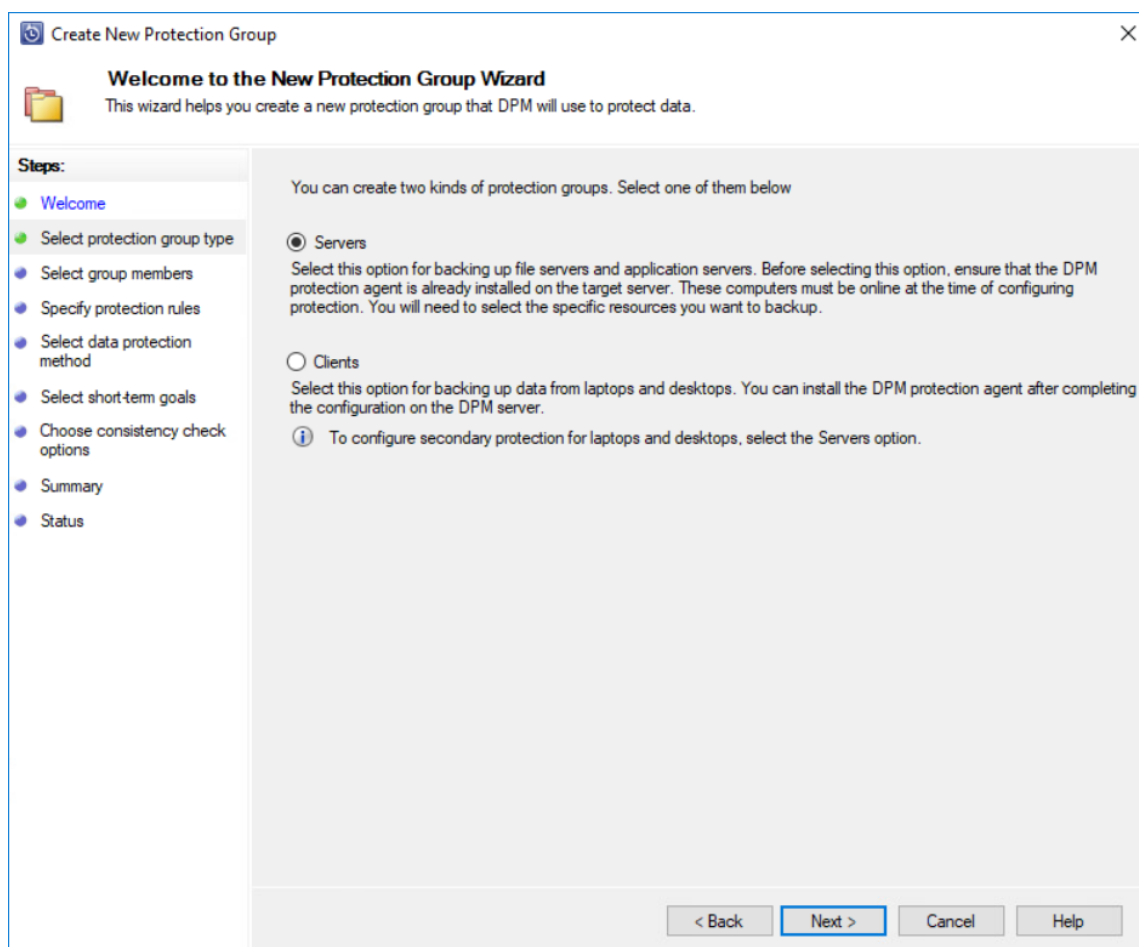


6. Prior to using the newly added tapes, Identify the “Unknown” tapes so they become “Free” and ready to be used.

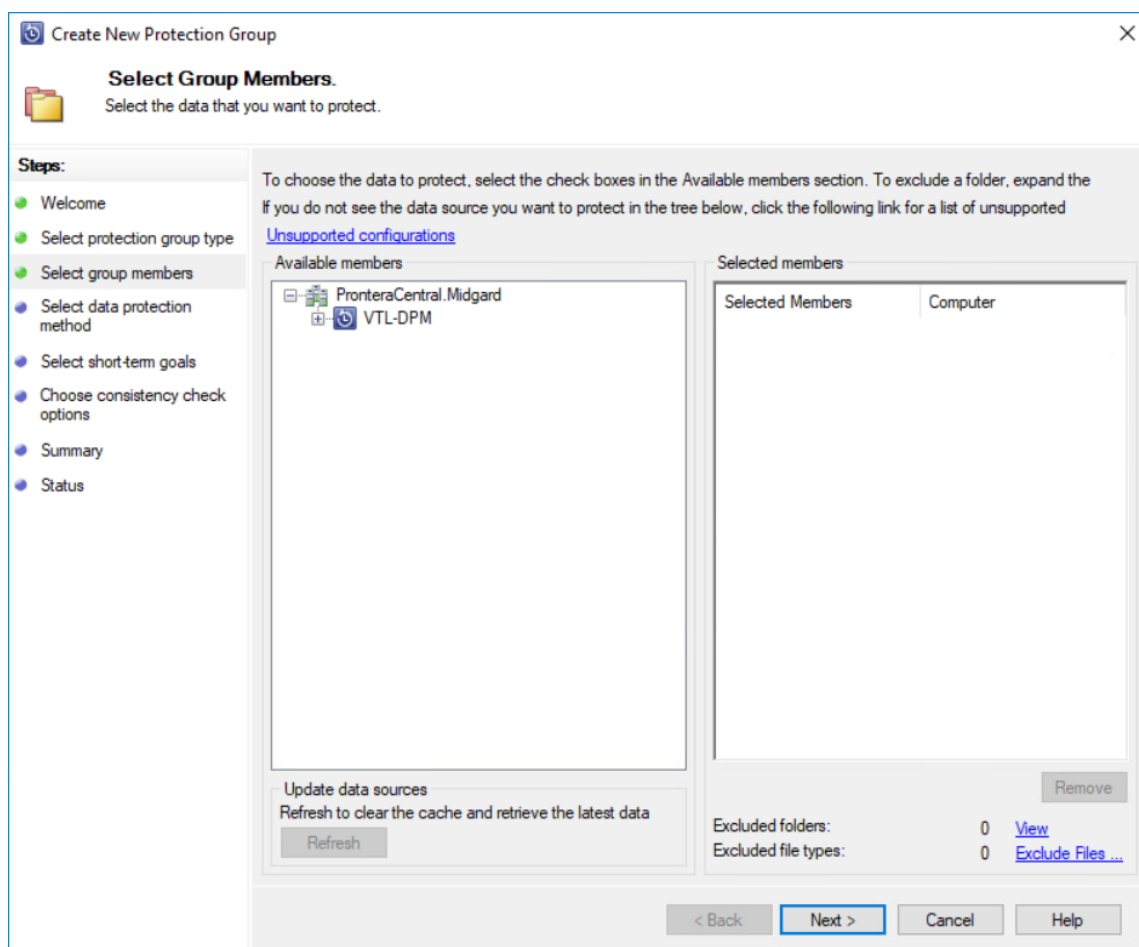


Configuring protection group for DPM

1. Open DPM Management Console in the Protection workspace of the Management view, and then click New+
2. Select the required backup option (Servers / Clients).



3. Choose the data that needs to be protected.



4. In Protection Group Wizard, select the required protection option:

- short-term protection (Disk / Tape)
- long-term protection (Tape)

The screenshot shows the 'Create New Protection Group' wizard in the StarWind interface. The current step is 'Select Data Protection Method'. The wizard has a sidebar with steps: Welcome, Select protection group type, Select group members, Select data protection method (current), Select short-term goals, Choose consistency check options, Summary, and Status. The main area shows the 'Protection group name' as 'Protection Group 1'. Under 'Protection method', it says 'Select your protection method.' There are three options:

- ☒ I want short-term protection using: A dropdown menu shows 'Tape' selected, with 'Disk' and 'Tape' as options.
- ☐ I want online protection. Below it, text says 'Configure online protection from the Management page to enable this option.'
- ☒ I want long-term protection using tape

 At the bottom right, there are buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

5. In Protection Group Wizard, specify the short-term goals.

Create New Protection Group

Specify Short-Term Protection
Specify your short-term recovery goals, which DPM will use to generate your protection plan.

Steps:

- Welcome
- Select protection group type
- Select group members
- Select data protection method
- Specify short-term goals**
- Specify long-term goals
- Select library and tape details
- Summary
- Status

Specify your protection goal on tape.

Retention range: 12 weeks

Frequency of backup: Daily

Backup mode: Only full backup

Backup schedule:
Specify your backup day and time.

Full backup time: 11:00 PM

Full backup days: ☐ Sunday ☒ Monday ☒ Tuesday ☒ Wednesday ☒ Thursday ☒ Friday ☒ Saturday

< Back Next > Cancel Help

6. Specify the required Long-Term Goals.

Create New Protection Group

Select Long-Term Goals

DPM will create a protection plan using your long-term recovery goals.

Steps:

- Welcome
- Select protection group type
- Select group members
- Select data protection method
- Specify short-term goals
- Specify long-term goals
- Select library and tape details
- Summary
- Status

Specify your long-term recovery goals for tape-based protection. All long-term tape-based protection uses full backups.

Recovery goals

The retention range and backup frequency that you select will determine the recovery point schedule.

Click Customize to modify the recovery point schedule or the default tape labels.

Retention range: 3 Years

Frequency of backup: Quarterly

Recovery points: 1 recovery point every 3 month(s) for the last 12 month(s)
1 recovery point every 1 year(s) for the last 3 year(s)

Restore Defaults Customize

Backup schedule

Based on the specified backup frequency, the tape library will perform a full backup to the tapes according to the following schedule

Click the Modify button to choose the backup days in case of daily tape backups.

Quarterly: Day 1, 11:00 PM

Yearly: January 1, 11:00 PM

Modify...

< Back

Next >

Cancel

Help

7. Specify the required Library and Tape Details.

Create New Protection Group

Select Library and Tape Details
Specify details about tape and the library that you would like to use for backup.

Steps:

- Welcome
- Select protection group type
- Select group members
- Select data protection method
- Specify short-term goals
- Specify long-term goals
- Select library and tape details**
- Summary
- Status

Specify details about the library and tape that you want to use for tape backups.

Library details

Library: Hewlett Packard Enterprise MSL G3 Series library (x64 v)

Drives allocated: 4

Copy library: Hewlett Packard Enterprise MSL G3 Series library (x64 v)

☐ Check backup for data integrity (time consuming operation)

Tape options for short-term protection

☒ Compress data

☐ Encrypt data
A valid DPM encryption certificate must be available on this DPM server. For more information click Help.

☐ Do not compress or encrypt data.

Tape options for long-term protection

☒ Compress data

☐ Encrypt data
A valid DPM encryption certificate must be available on this DPM server. For more information click Help.

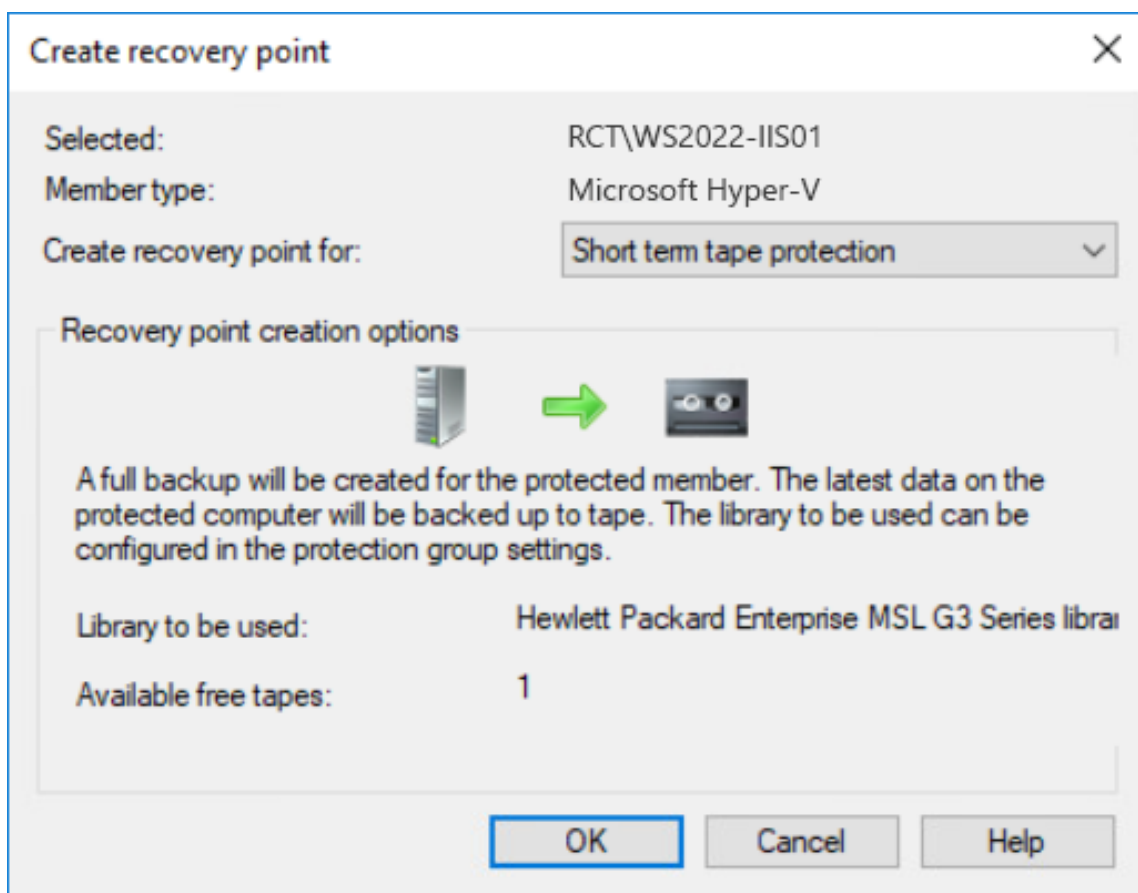
☐ Do not compress or encrypt data.

i You can optimize tape usage for this protection group using 'Optimize Tape Usage' on the Libraries Management page.

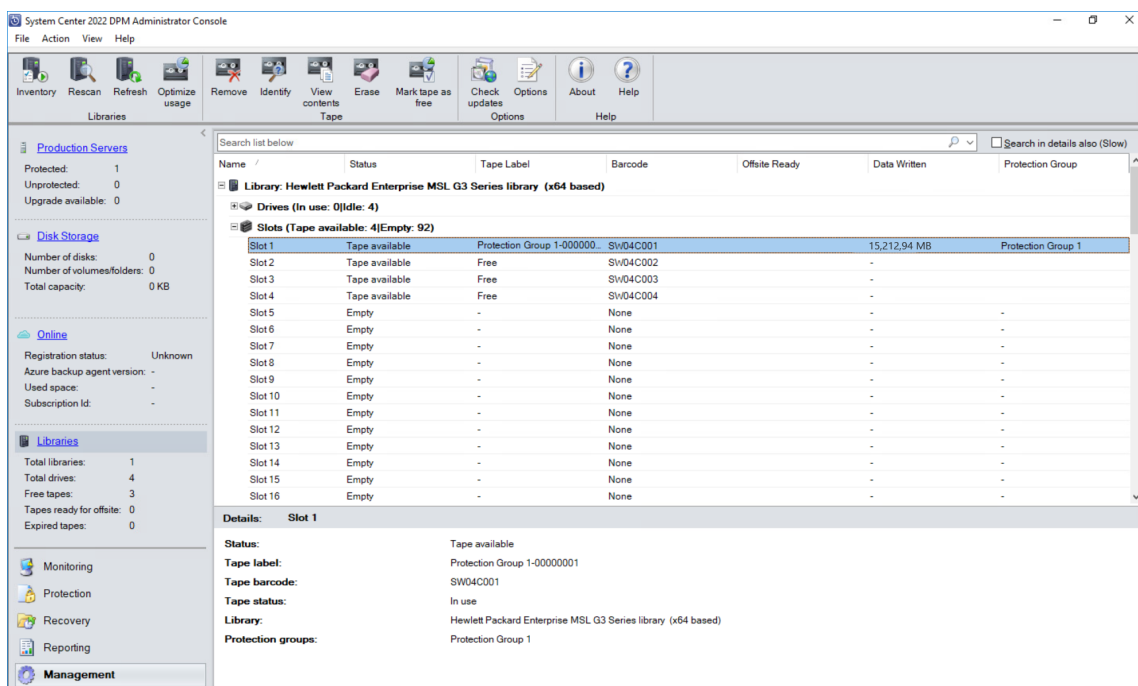
< Back **Next >** Cancel Help

8. Review the Summary and click Create Group.

9. To create a manual recovery point, navigate to the Protection workspace of the Management view, right-click on the protected item and select Create recovery point... Select Short term tape protection or Long term tape protection.

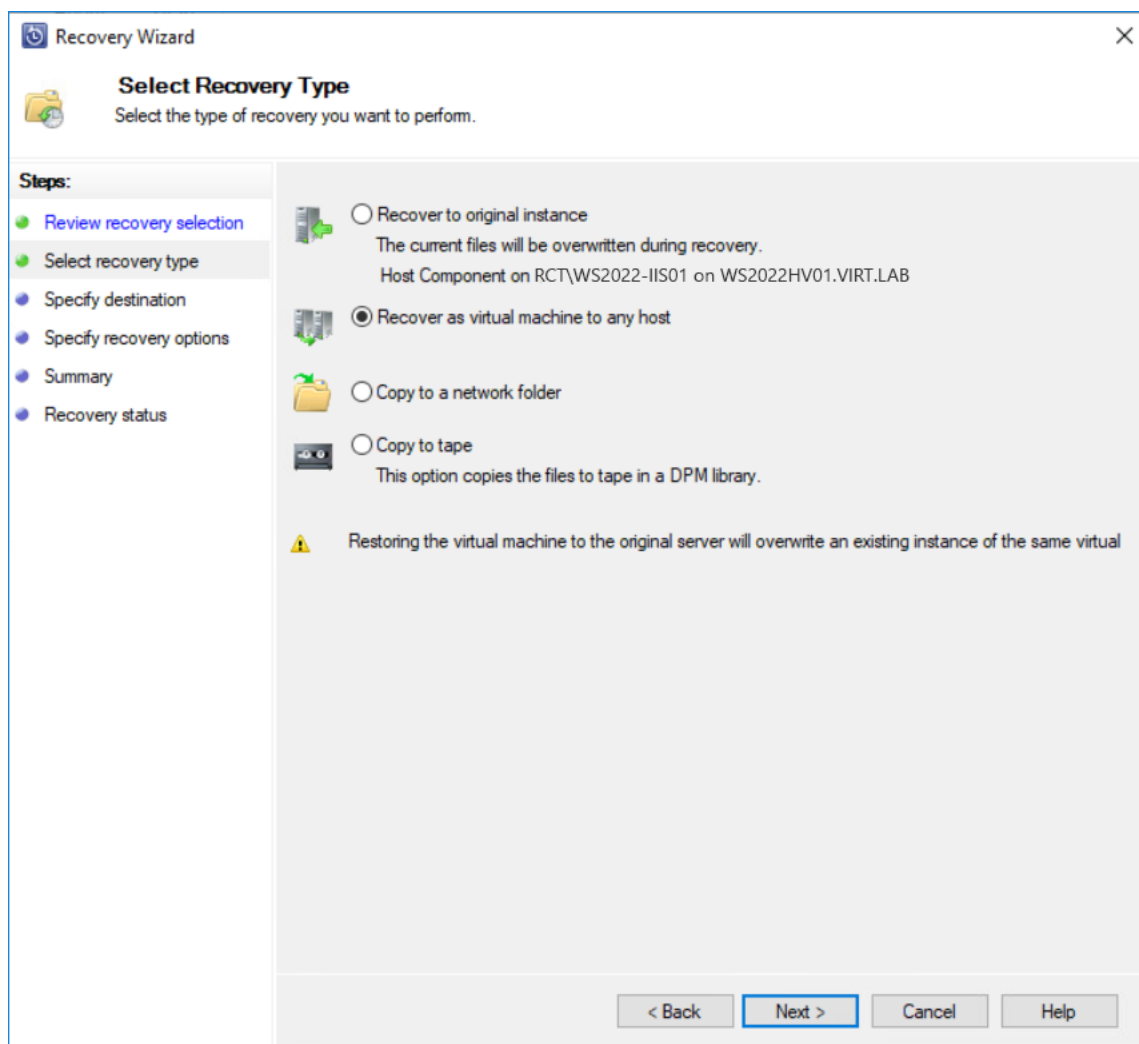


10. Open the Libraries workspace of the Management view, the protection group named "Tape Protection Group 1" is assigned to slot 1.



Restoring data from tape

1. Make sure that the tape library is online and does not report any errors; this can be done by verifying the alerts in the Monitoring view of the DPM console or in the Libraries workspace of the Management view of the DPM console.
2. In the DPM console, go to Recovery and choose the data source to recover.
3. Mark the data source and choose the data and time for the restore. Right-click on the data source and choose Recover... to start the Recovery wizard.
4. In the Review Recovery Selection wizard, review the data source that is chosen for recovery and click on Next to continue.
5. In the Select Recovery Type wizard, choose one of the recovery options:



6. To recover data as a virtual machine, select Recover as virtual machine to any host option.

7. In the Specify Destination wizard, select the location to recover the virtual machine to.

Recovery Wizard

Specify Destination
Specify where you want to recover the virtual machine.

Steps:

- Review recovery selection
- Select recovery type
- Specify destination
- Specify recovery options
- Summary
- Recovery status

Specify where you want to recover the virtual machine.

☐ Destination host uses remote storage.

All the files will be copied inside a folder named WS2022-IIS01_10-11-2023_8.20.39' in the copy destination.

Destination host: WS2022-HV03.VIRT.LAB Browse...

Destination path: D:\VMs

Space required: 14.86 GB

Space available: 640.47 GB

< Back Next > Cancel Help

8. In the Specify Recovery Options wizard, configure specific options for the recovery.
NOTE: Make sure to choose the library that hosts all the tapes that are needed for the recovery.

Recovery Wizard

Specify Recovery Options
Specify the options to apply to the recovery.

Steps:

- Review recovery selection
- Select recovery type
- Specify destination
- Specify recovery options**
- Summary
- Recovery status

Recovery library
All the tapes needed for recovery needs to be present in this library.
Library name: Hewlett Packard Enterprise MSL G3 Series library (x64 basec)

Network bandwidth usage throttling
Status: Disabled [Modify...](#)

SAN Recovery
☐ Enable SAN based recovery using hardware snapshots
Click on Help to learn about the prerequisite steps

Notification
☐ Send an e-mail when this recovery completes
Recipients: Separate e-mail addresses with comma.
Example: Kim@Contoso.com, Terry@Adventure-works.com

< Back Next > Cancel Help

9. In the Summary step, verify the recovery settings, and click Recover to start the process of recovering the virtual machine to a different host.

NOTE: DPM uses a scratch before it sends the data to the selected data source. It is very important that the DPM %systemdrive% server has more than 10 GB of free disk space. DPM supports item-level recovery (ILR), which allows performing a specific recovery of files, folders, volumes, and virtual hard disks from a host-level backup of Hyper-V virtual machines to a network share or a volume on a DPM protected server. However, ILR is not supported when restoring from tapes. Only an entire VM or a single virtual hard disk can be restored.

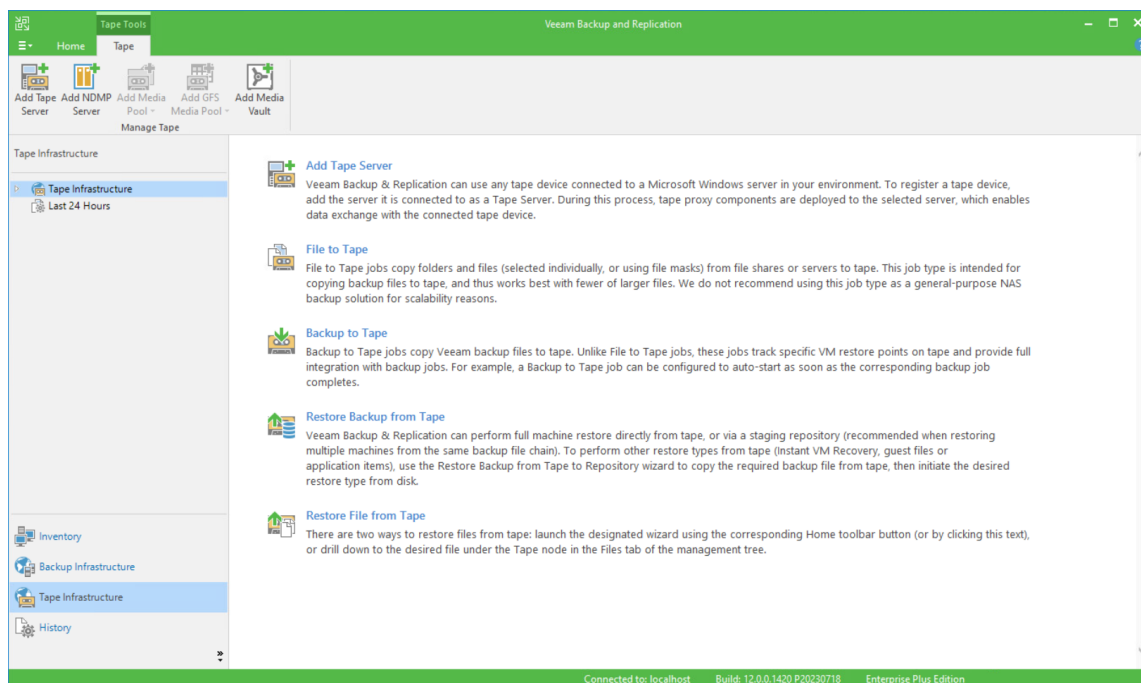
10. To restore files from the cloud storage, please navigate to the Restoring tapes from the cloud storage section.

Veeam Backup & Replication

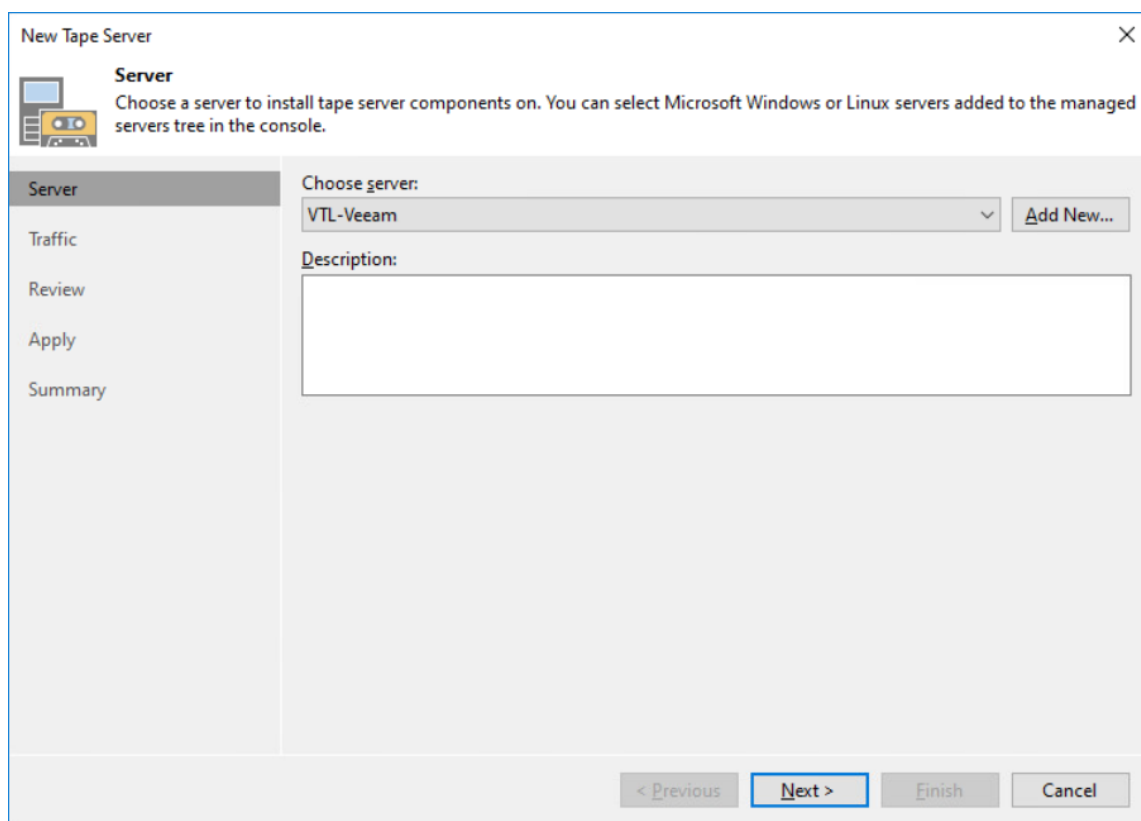
Please refer to the following guide if having any questions about Veeam Backup & Replication deployment:

<https://www.veeam.com/documentation-guides-datasheets.html?ad=menu-resources>

1. Open the Veeam Backup & Replication console. Open the Tape Infrastructure tab.

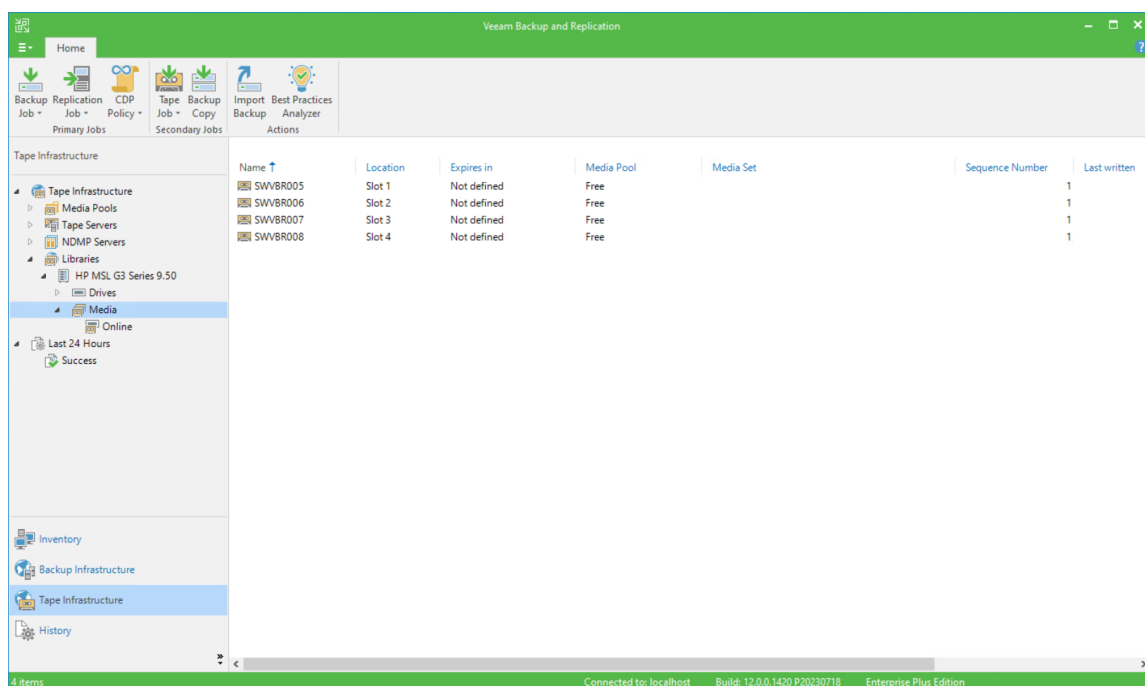


2. Open the Add Tape Server wizard. Choose the local server and press Next.



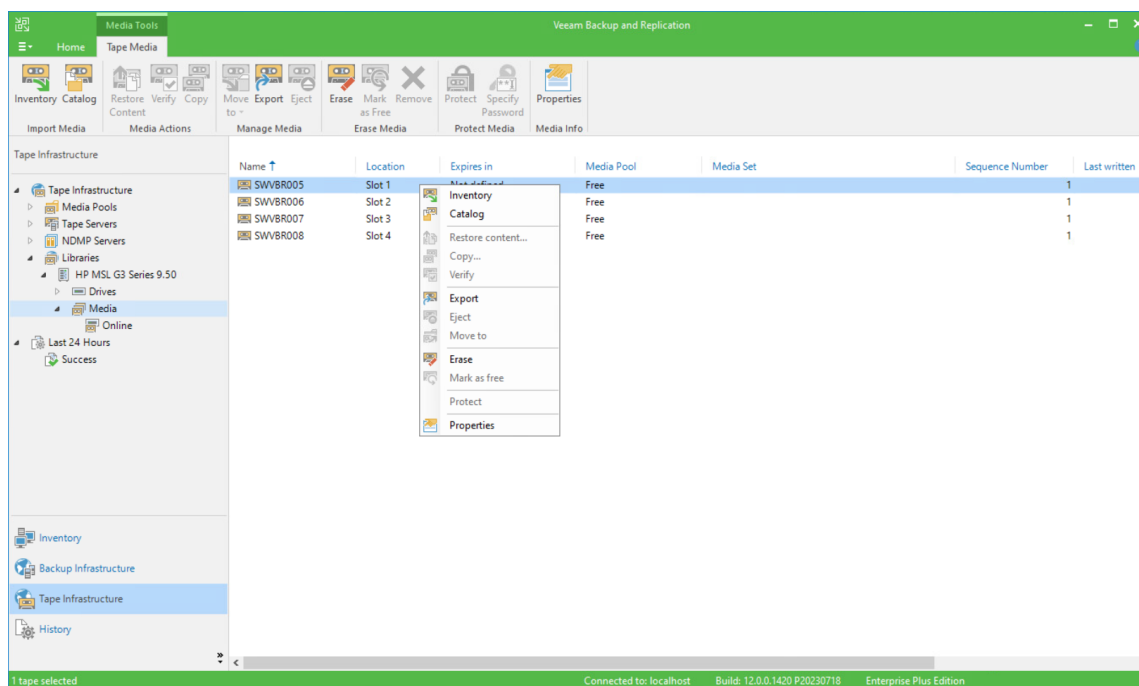
3. Complete the wizard, select Start tape library inventory when I click Finish and press the Finish button.

4. After Tape Inventory job is finished, the newly added tape library device will appear.



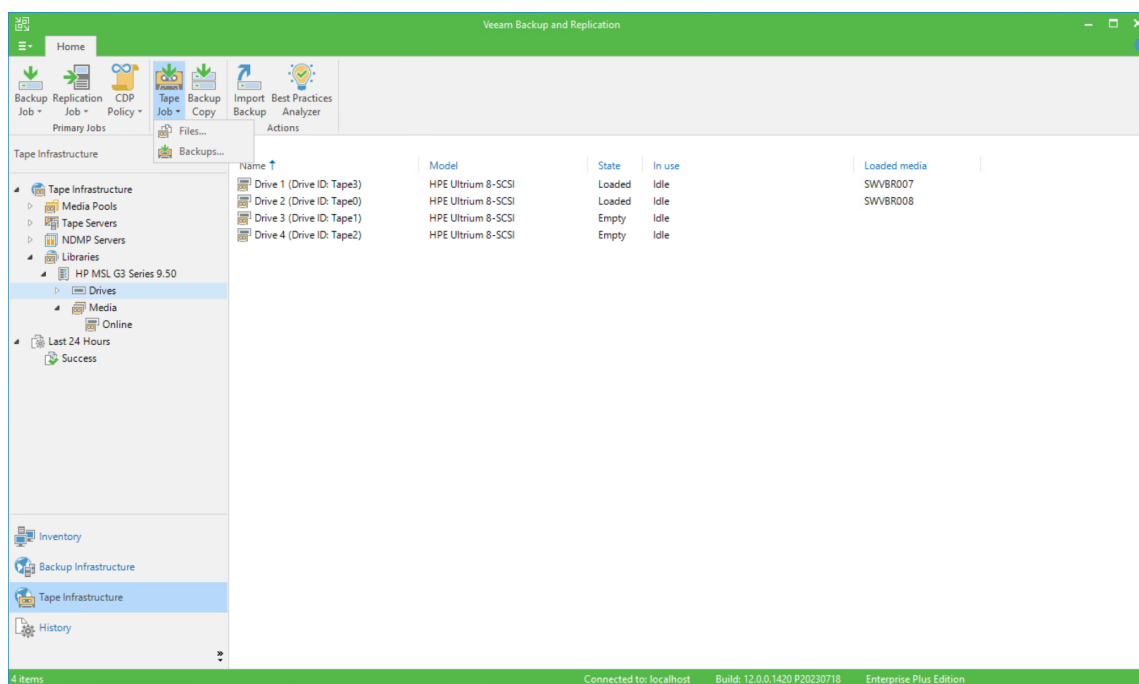
TE: You can also configure Backups to Tape Job. For more details, please refer to the following link: https://helpcenter.veeam.com/docs/backup/vsphere/creating_backup_to_tape_jobs.html?ver=95

5. Before using the new tape, erase it. To erase tapes, click Media and right-click the required tape to erase.

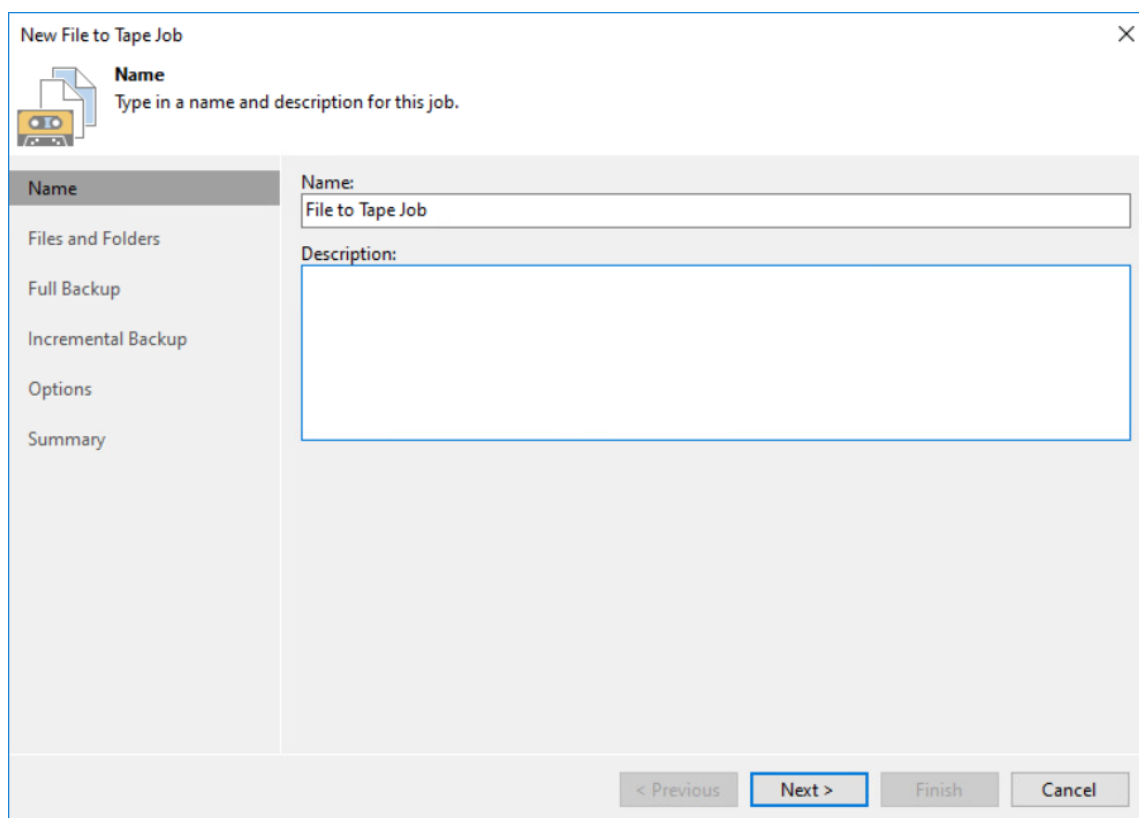


The tape will be loaded into Drive.

6. Navigate to the Home tab, click Tape Job and select Files to run the File to Tape job wizard.



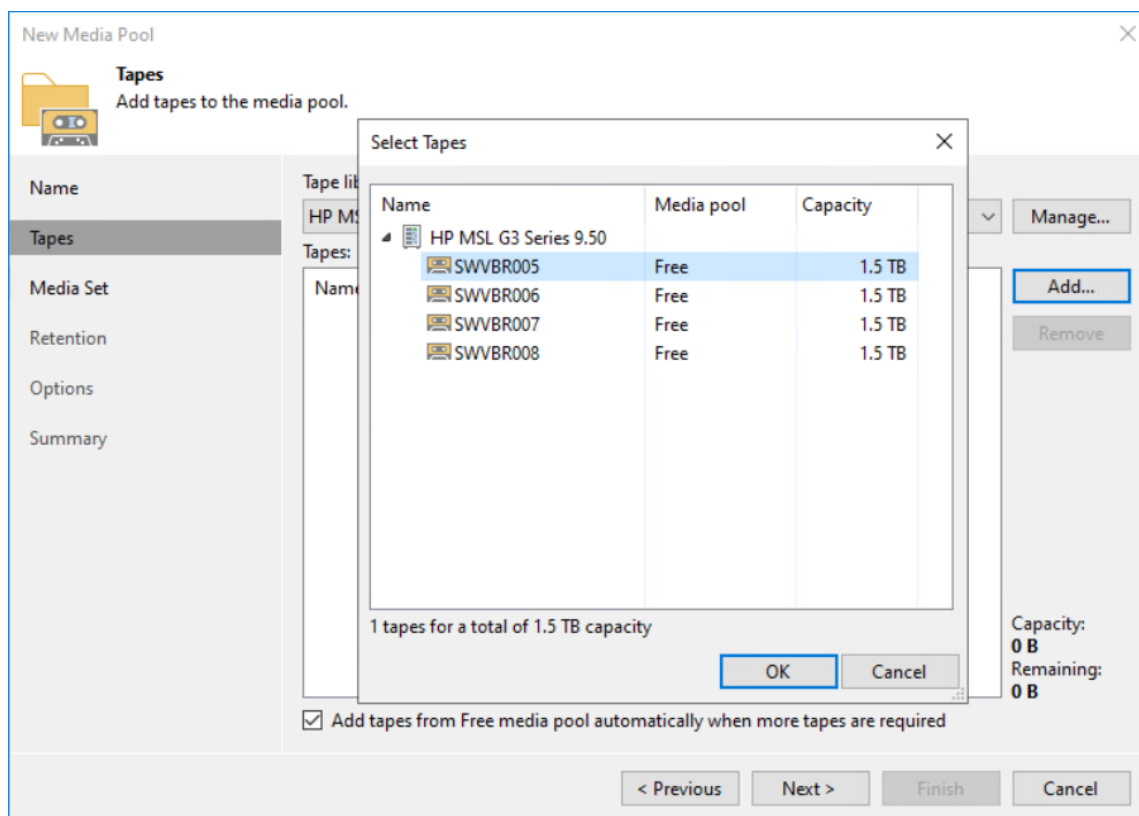
7. Specify the job name and description in the appeared window, and press Next.



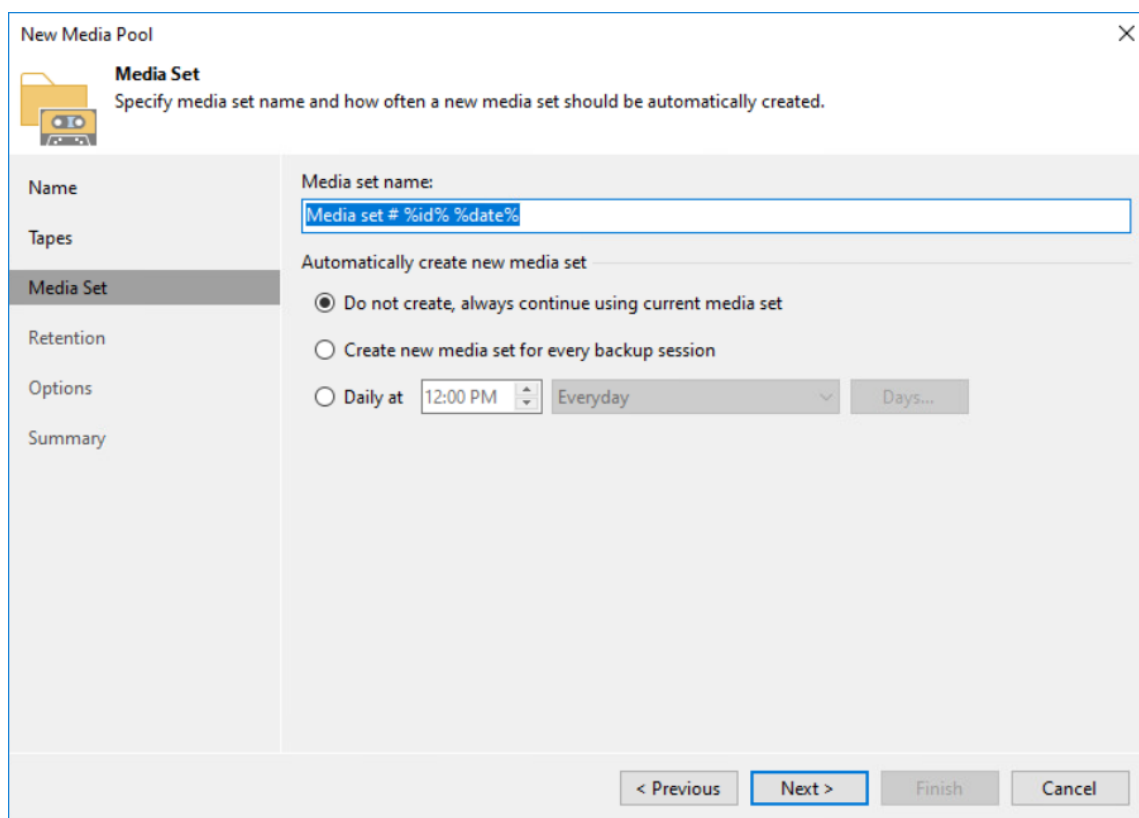
8. Choose files to be backed up and press Next.

10. The New Media Pool wizard will appear. Specify the name and description of the new Media Pool and click Next.

11. Add the existing tape(s) to the Media Pool, click OK and Next to select the tapes.



12. Specify the Media Set name, configure additional settings if necessary, and click Next.



New Media Pool [X]

Media Set
Specify media set name and how often a new media set should be automatically created.

Name
Media set name:
Media set # %id% %date%

Tapes

Media Set

Retention

Options

Summary

Automatically create new media set

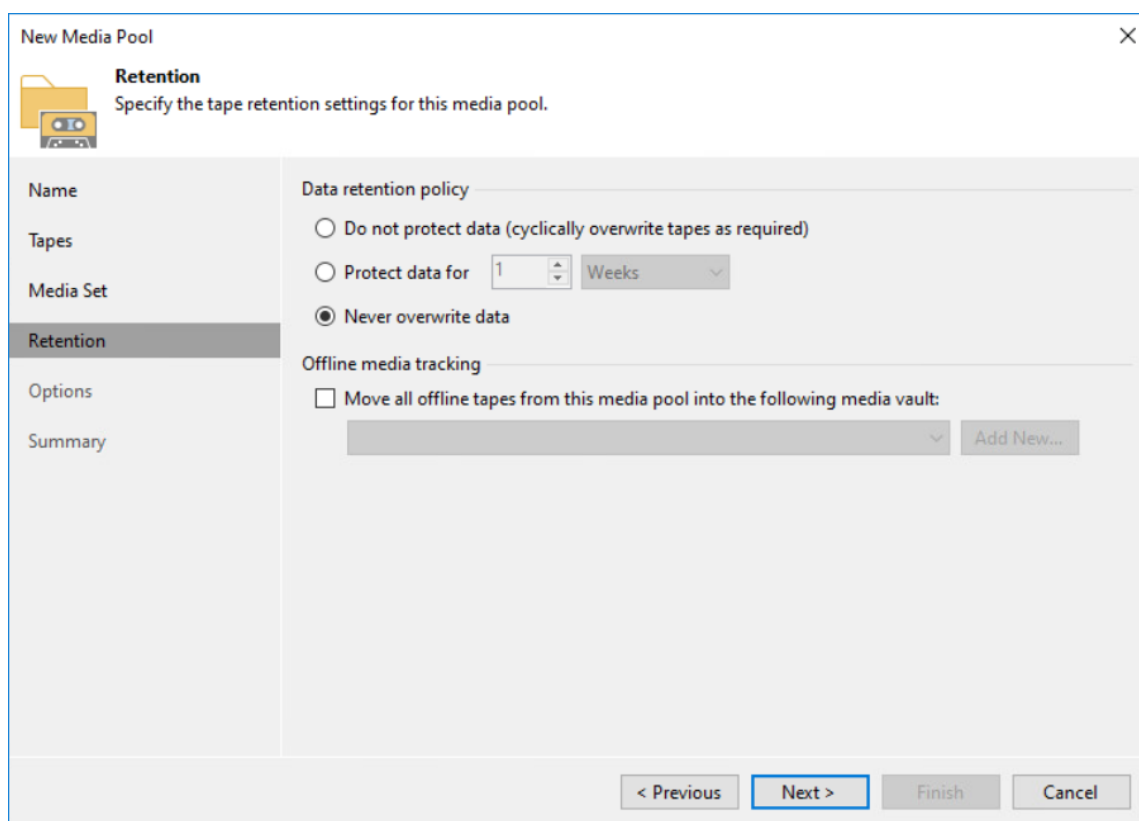
☒ Do not create, always continue using current media set

☐ Create new media set for every backup session

☐ Daily at 12:00 PM Everyday Days...

< Previous Next > Finish Cancel

13. Specify the preferred retention settings if necessary and press Next.



New Media Pool [X]

Retention
Specify the tape retention settings for this media pool.

Name

Tapes

Media Set

Retention

Options

Summary

Data retention policy

☐ Do not protect data (cyclically overwrite tapes as required)

☐ Protect data for 1 Weeks

☒ Never overwrite data

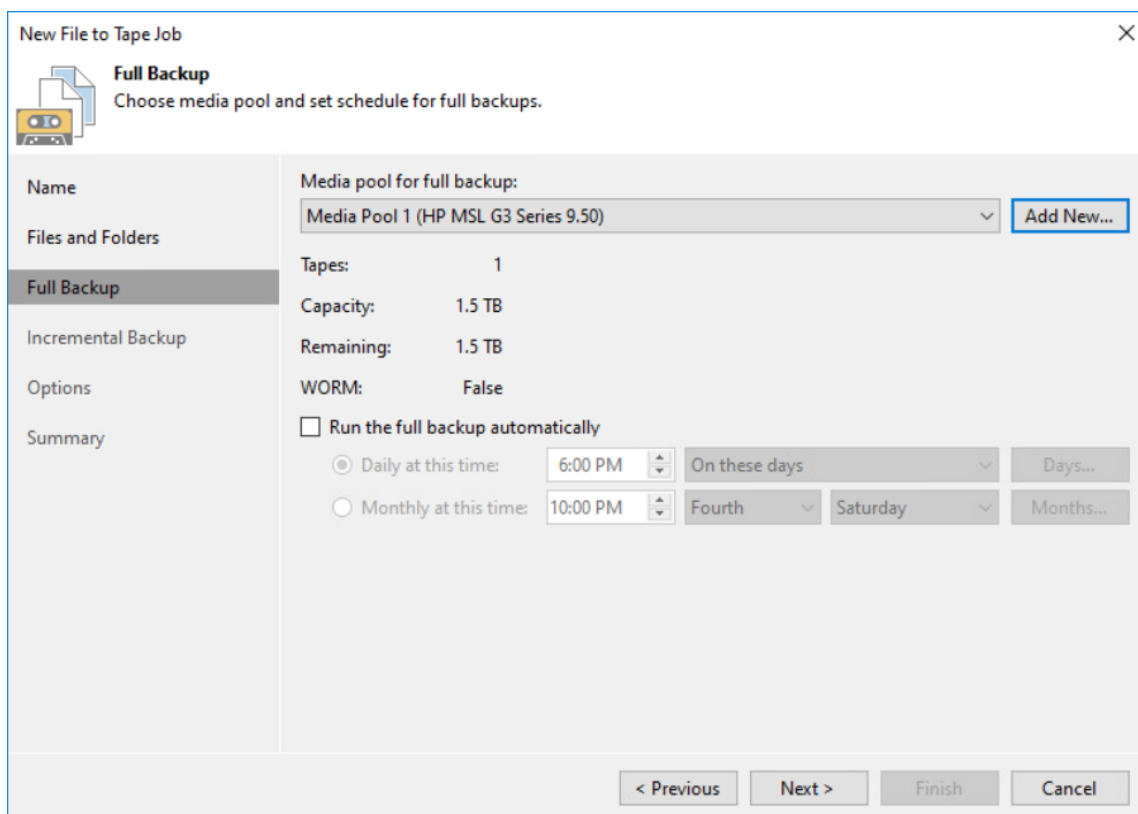
Offline media tracking

☐ Move all offline tapes from this media pool into the following media vault:

[Vault Selection] Add New...

< Previous Next > Finish Cancel

14. Specify the additional options if necessary and click the Apply button.
15. Review the Summary and press Finish.
16. Move back to the New File to Tape Job wizard and press Next to continue.



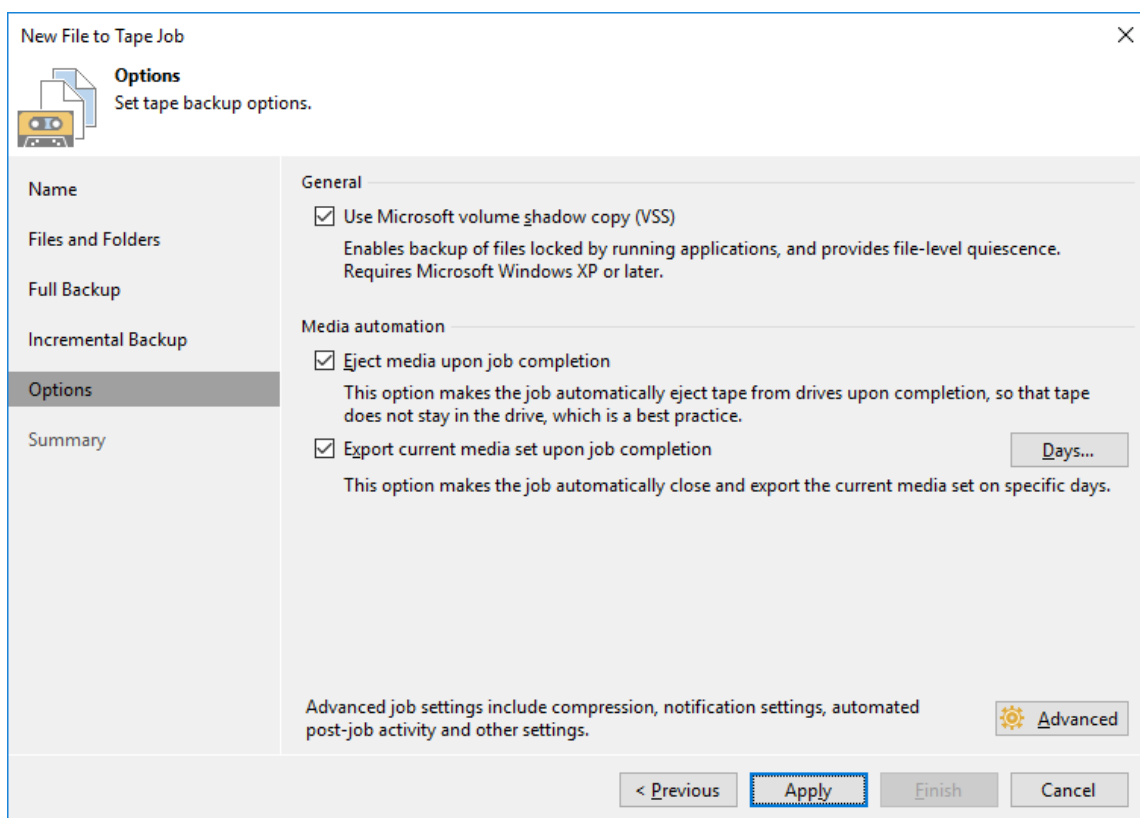
The screenshot shows the 'New File to Tape Job' wizard window. The 'Full Backup' step is selected in the left sidebar. The main area displays configuration options for a full backup. The 'Media pool for full backup' is set to 'Media Pool 1 (HP MSL G3 Series 9.50)'. The 'Tapes' count is 1, 'Capacity' is 1.5 TB, and 'Remaining' is 1.5 TB. The 'WORM' option is set to 'False'. There is an unchecked checkbox for 'Run the full backup automatically'. Below this, there are two scheduling options: 'Daily at this time' (selected) with a time of 6:00 PM and 'On these days' set to 'On these days'; and 'Monthly at this time' with a time of 10:00 PM, 'Fourth' of the month, and 'Saturday'. At the bottom, there are buttons for '< Previous', 'Next >', 'Finish', and 'Cancel'.

17. Configure the Incremental Backup schedule if necessary. Choose the same Media Pool or add the new Media Pool for the incremental backups.

The screenshot shows the 'New File to Tape Job' dialog box with the 'Incremental Backup' tab selected. The dialog has a sidebar on the left with tabs: Name, Files and Folders, Full Backup, Incremental Backup (selected), Options, and Summary. The main area is titled 'Incremental Backup' with the instruction 'Choose media pool and set schedule for incremental backups.' Below this, there is a dropdown menu for 'Media pool for incremental backup:' showing 'Media Pool 1 (HP MSL G3 Series 9.50)' and an 'Add New...' button. To the right of the dropdown are fields for 'Tapes: 1', 'Capacity: 1.5 TB', 'Remaining: 1.5 TB', and 'WORM: False'. Below these is a checkbox 'Run incremental backup automatically' which is unchecked. Under this checkbox are two radio button options: 'Daily at this time:' with a time picker set to '3:00 AM', a day-of-week dropdown set to 'On weekdays', and a 'Days...' button; and 'Monthly at this time:' with a time picker set to '10:00 PM', a day-of-month dropdown set to 'Fourth', a day-of-week dropdown set to 'Saturday', and a 'Months...' button. At the bottom of the dialog are four buttons: '< Previous', 'Next >' (highlighted with a blue border), 'Finish', and 'Cancel'.

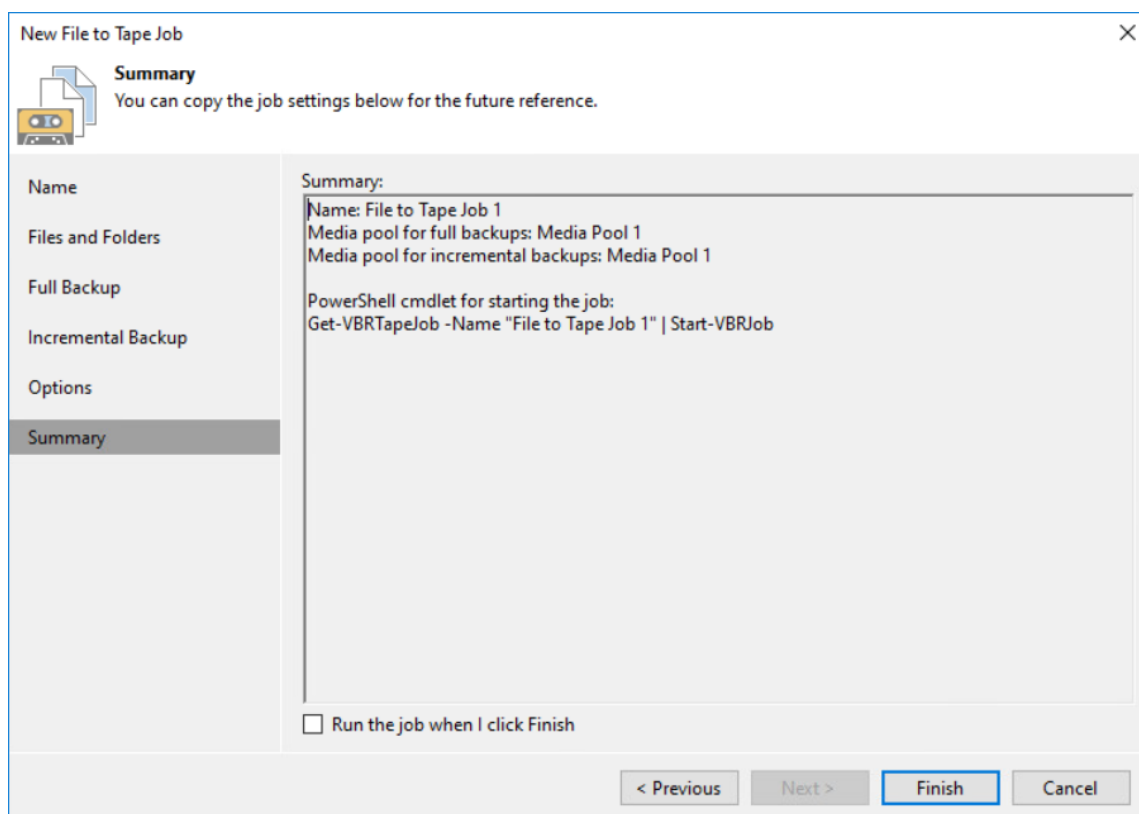
Press Next to proceed.

18. In the Options tab, specify the additional settings and check the Export current media set upon job completion box to allow the automatic tape offload to cloud storage after backup job is completed. It is also recommended to Eject media upon job completion. Click Apply.

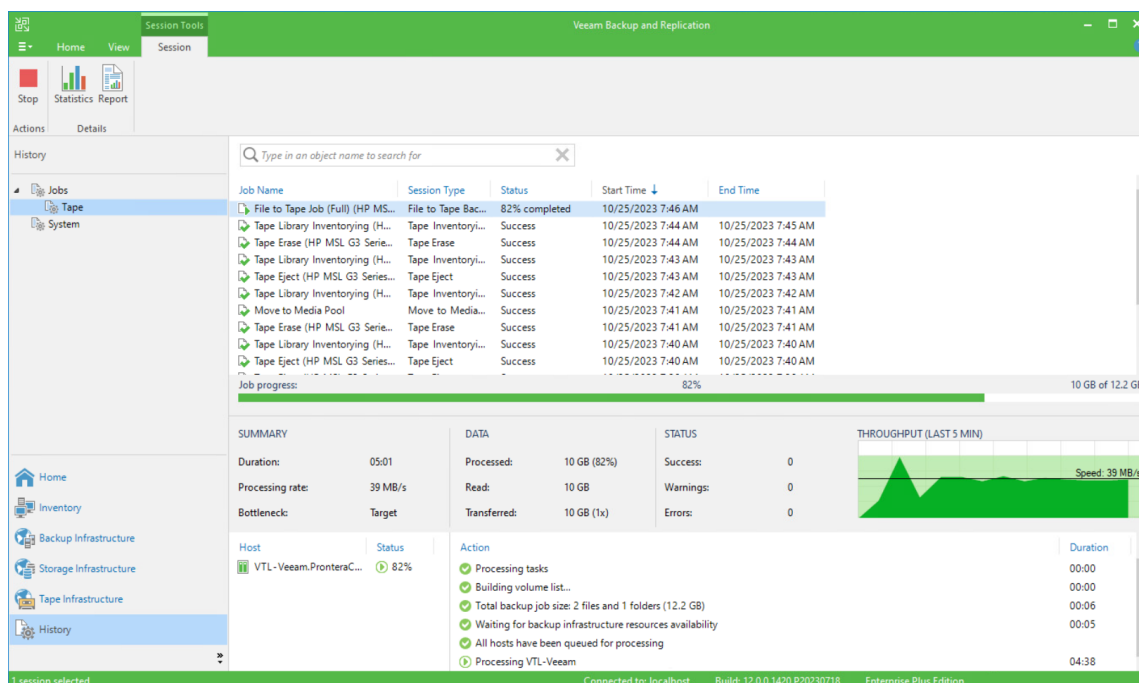


19.

Review the summary, select the Run the job when I click Finish checkbox if the backup job needs to be run right away, and click Finish.

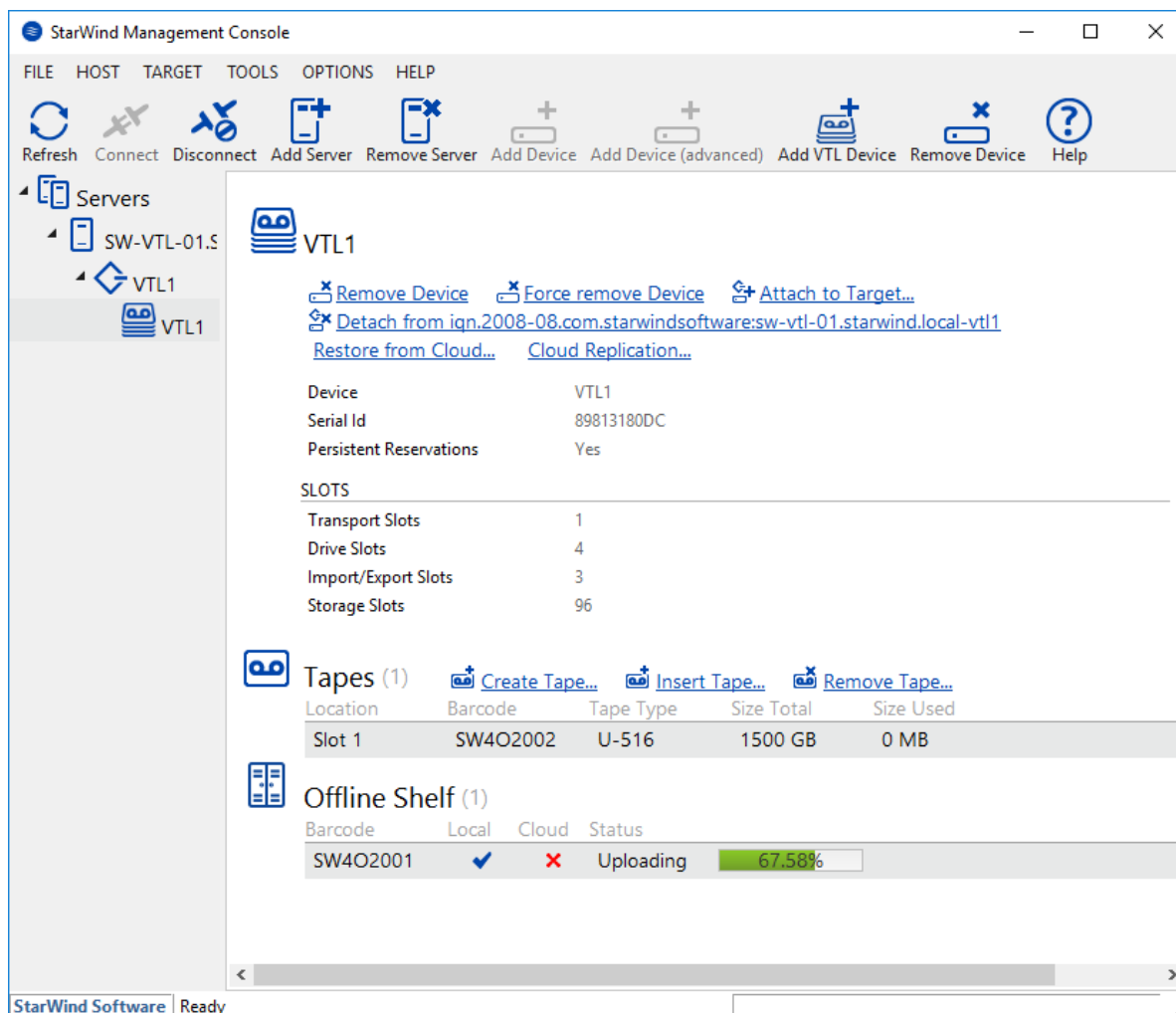


20. The job status and progress can be checked in the History tab.



21. After the job is finished, the tape is automatically ejected, exported, and marked as Offline according to job settings configured above.

20. Since the tape was automatically exported upon job completion and StarWind VTL Replication policy was set to Replicate Immediately, the replication process to the cloud storage has started automatically. The progress can be checked in StarWind Management Console using the Offline Shelf overview.

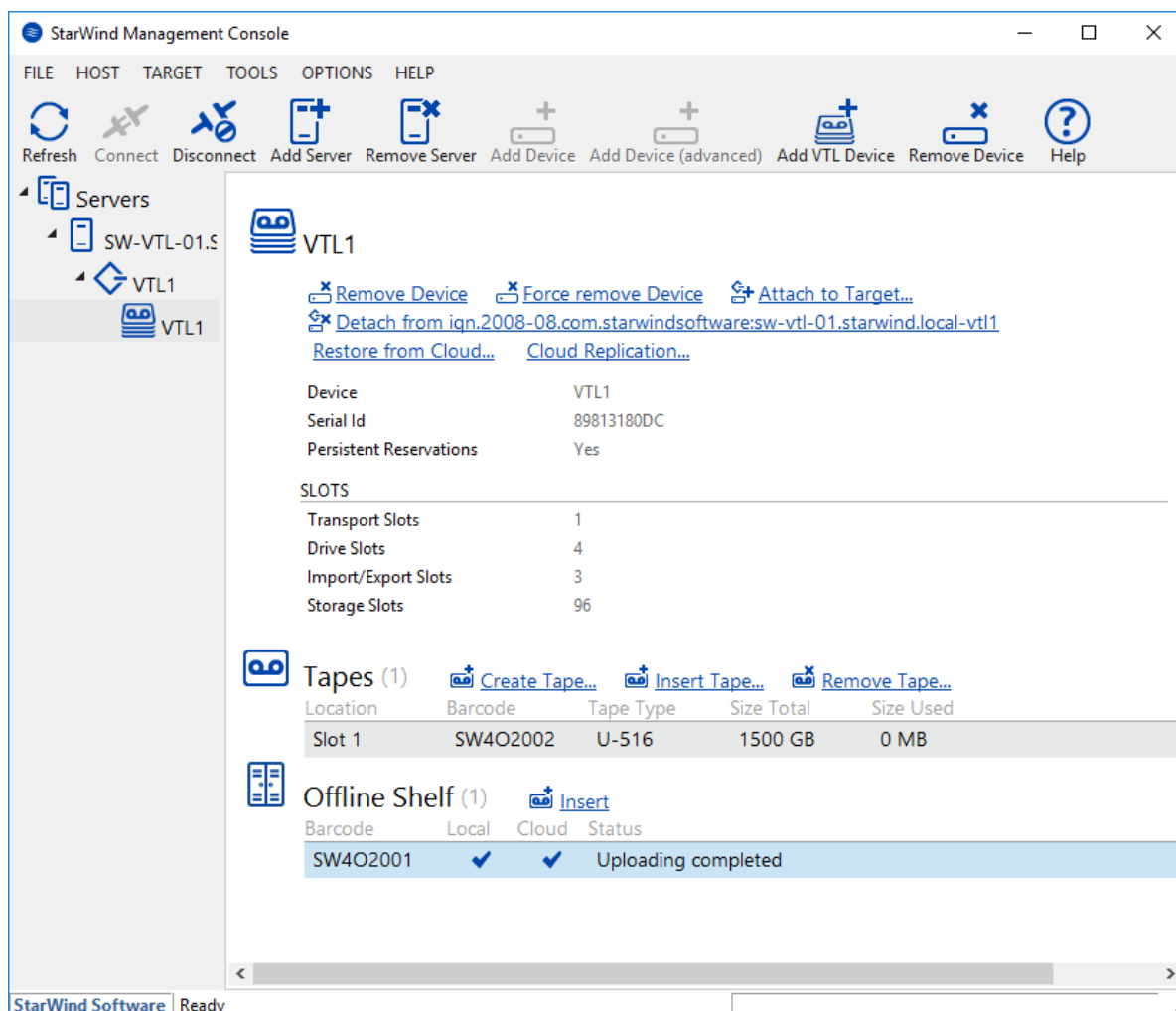


NOTE: In order to automate moving newly created tapes to free media pool in Veeam Backup & Replication, please follow the instructions in [this KB article](#).

NOTE: The tape can be kept in its tape library slot upon backup job completion and offloaded to the cloud storage later. For this purpose, use the disable Export current media set upon job completion and Eject media upon job completion options in File to Tape Job settings using Veeam Backup & Replication Console.

21. After the backup job is finished, in the Veeam B&R console, navigate to Tape Infrastructure -> Libraries -> Media -> Online and choose the tape to upload, right-click it, and press Export. The tape will be automatically offloaded to the cloud storage according to the specified Retention Settings of StarWind VTL.

22. When the tape is successfully uploaded to the cloud, the tape location status in Offline Shelf overview will be marked as Cloud.



23. If the local copy of the tape is not removed after replication, but already moved to Offline Shelf, it can be inserted back into the library by clicking the Insert button.

To restore files from the cloud storage, please navigate to Restoring tapes from the cloud storage section.

Veritas Backup Exec™

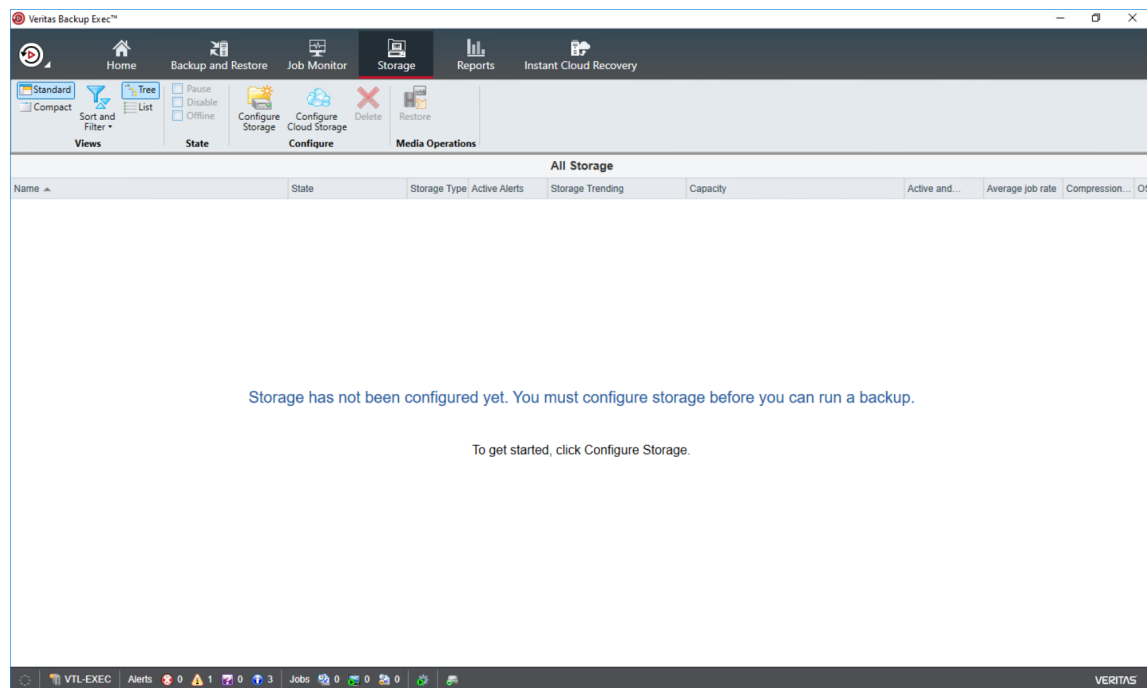
Adding StarWind VTL Device to Veritas Backup Exec™

In case of any question regarding Veritas Backup Exec™ deployment, please refer the

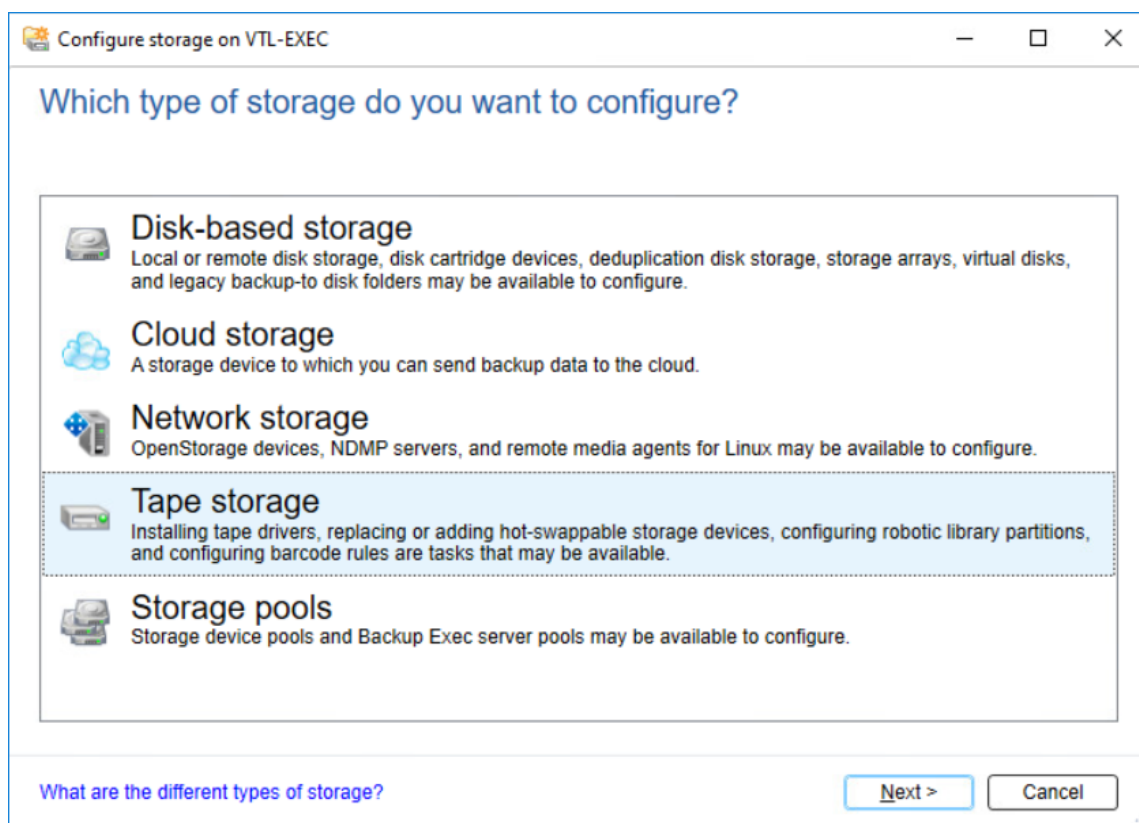
following link:

https://www.veritas.com/content/support/en_US/doc/59226269-99535599-0/v59899992-99535599

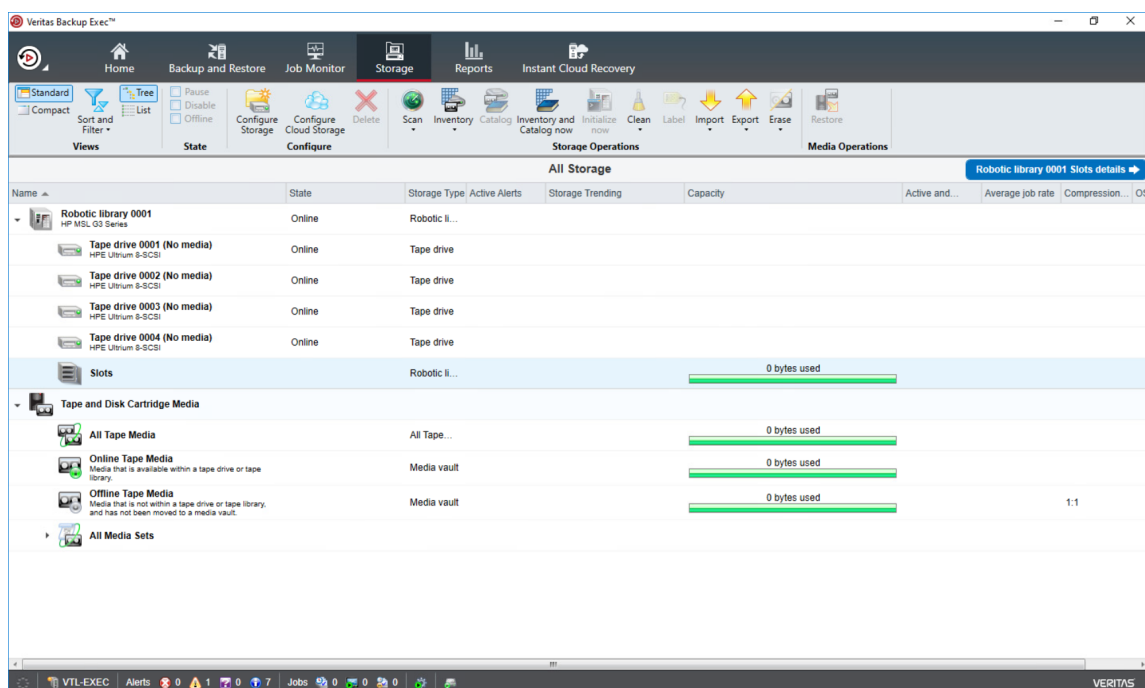
1. In Veritas Backup Exec™ console, click the Storage tab and Configure Storage.



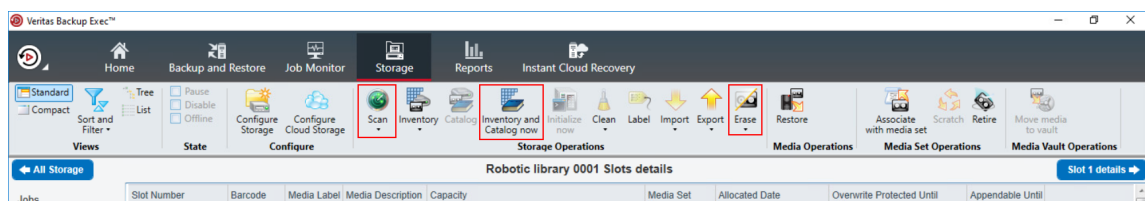
2. In the opened window, select Tape storage and click Next.



3. Select Run the Hot-swappable Device Wizard and click Next.
4. Follow the steps suggested by Hot-Swappable Device Wizard and to complete it.
NOTE: If the tape device has not appeared in the Storage tab, initiate the restart.
5. Double-click Slots to scan, erase, inventory and catalog the tapes.



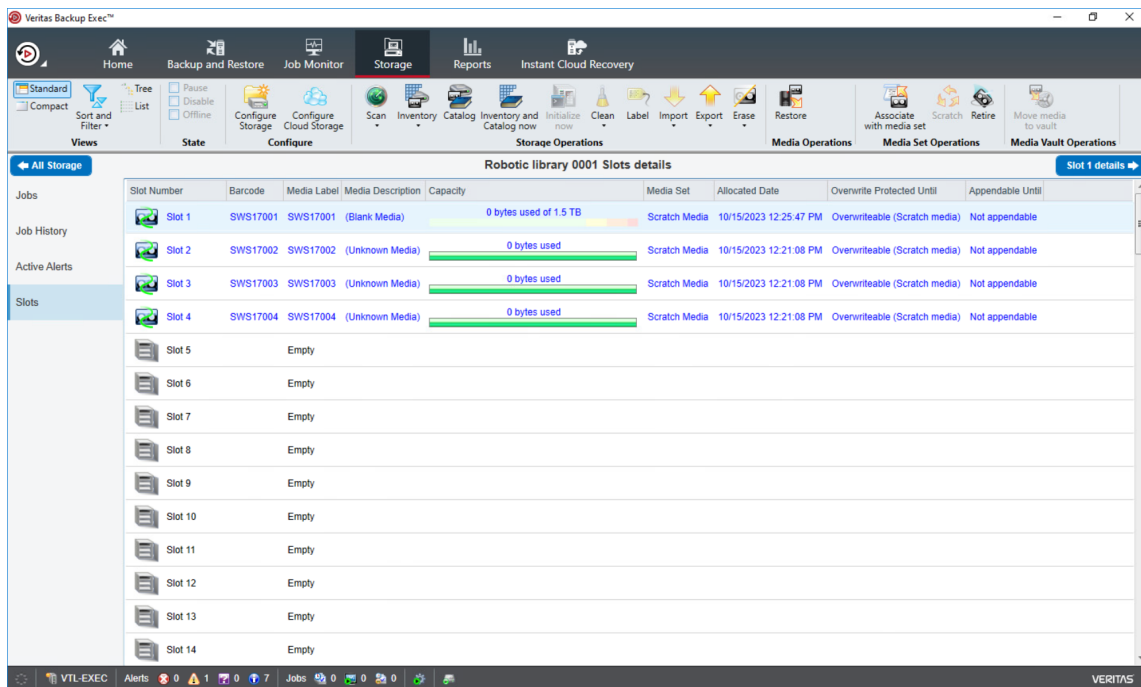
6. Choose the tape and perform the necessary operations.



7. Confirm the data erasure when requested.



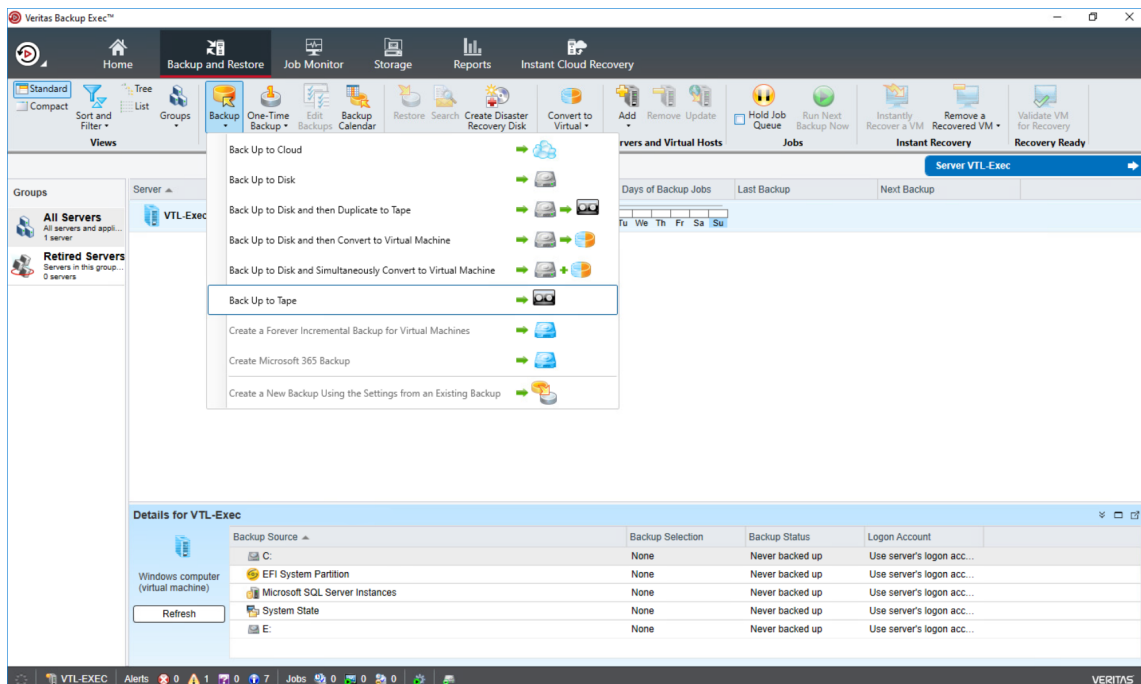
8. The prepared tape should look like in the screenshot below.



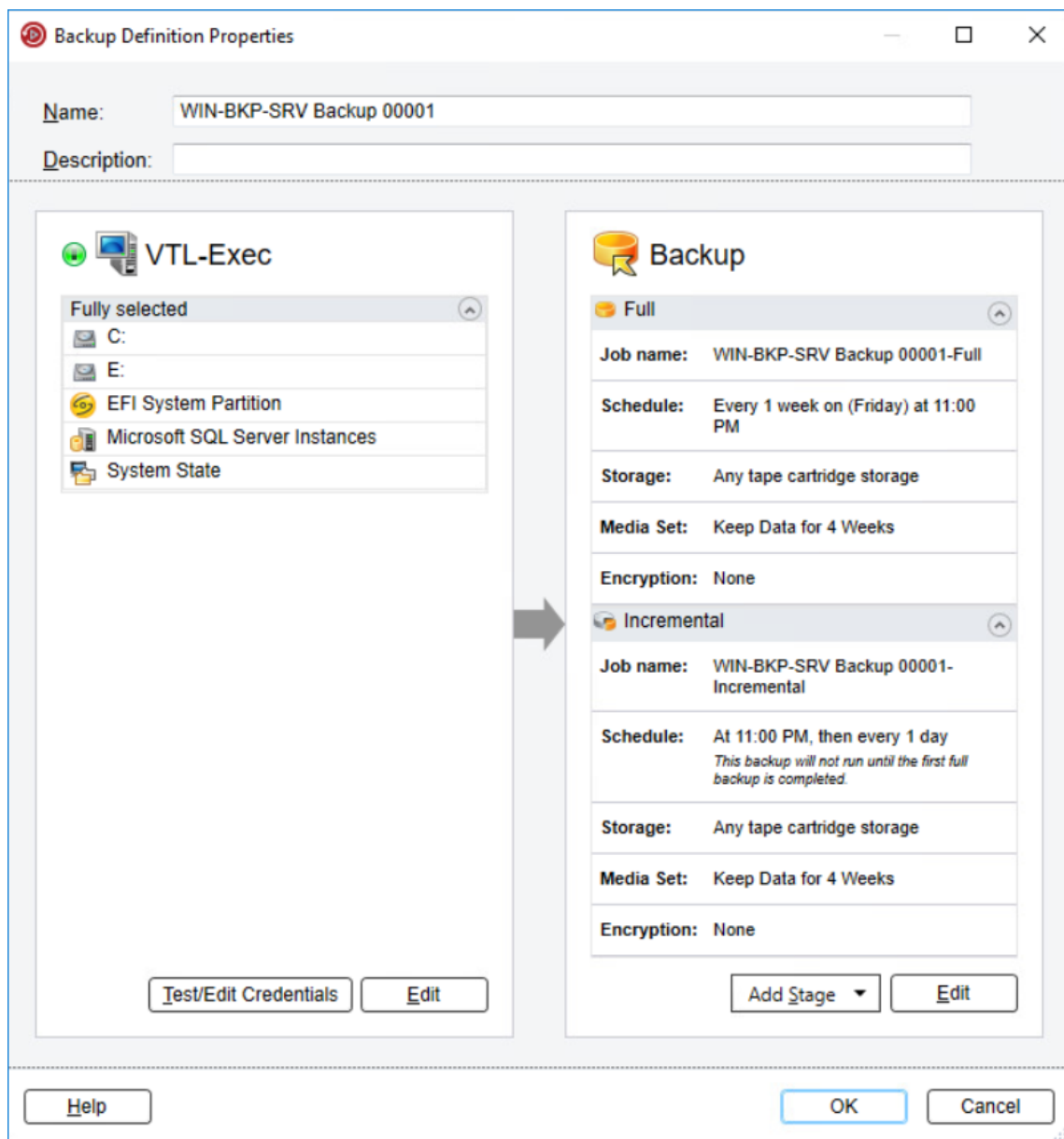
Configuring Backup to Tape job in Veritas Backup Exec™

In this part, the backup/restore process of the folder is shown as an example.

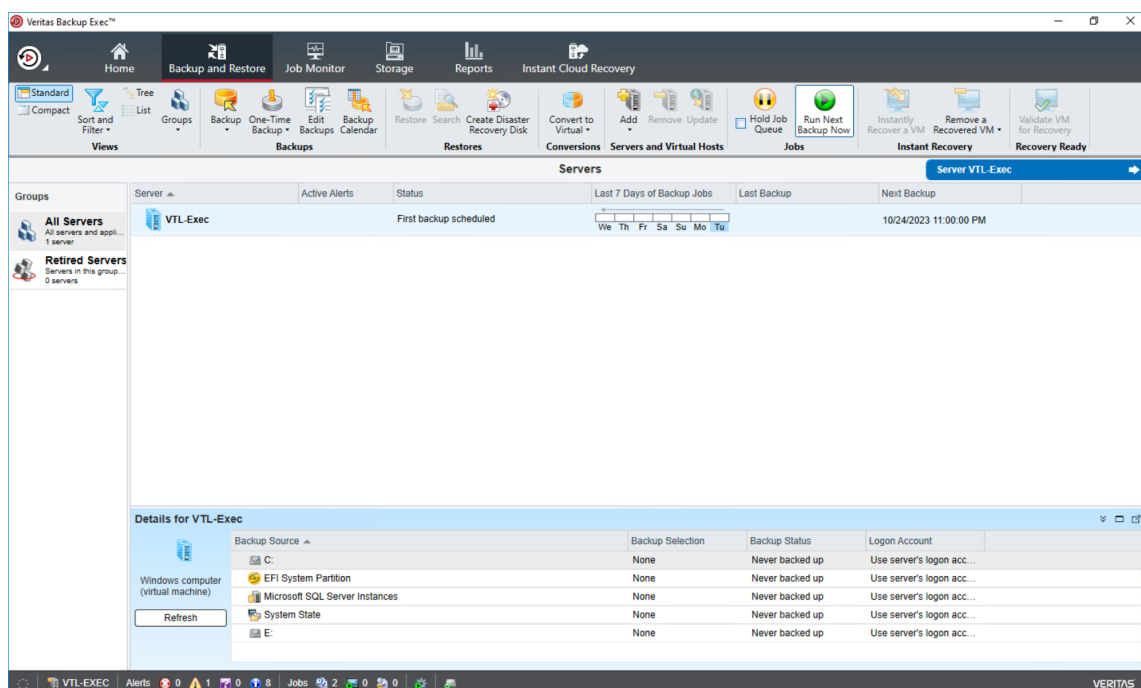
1. In the Backups group, click on the Backup and Restore tab. Click Backup and select Back Up to Tape.



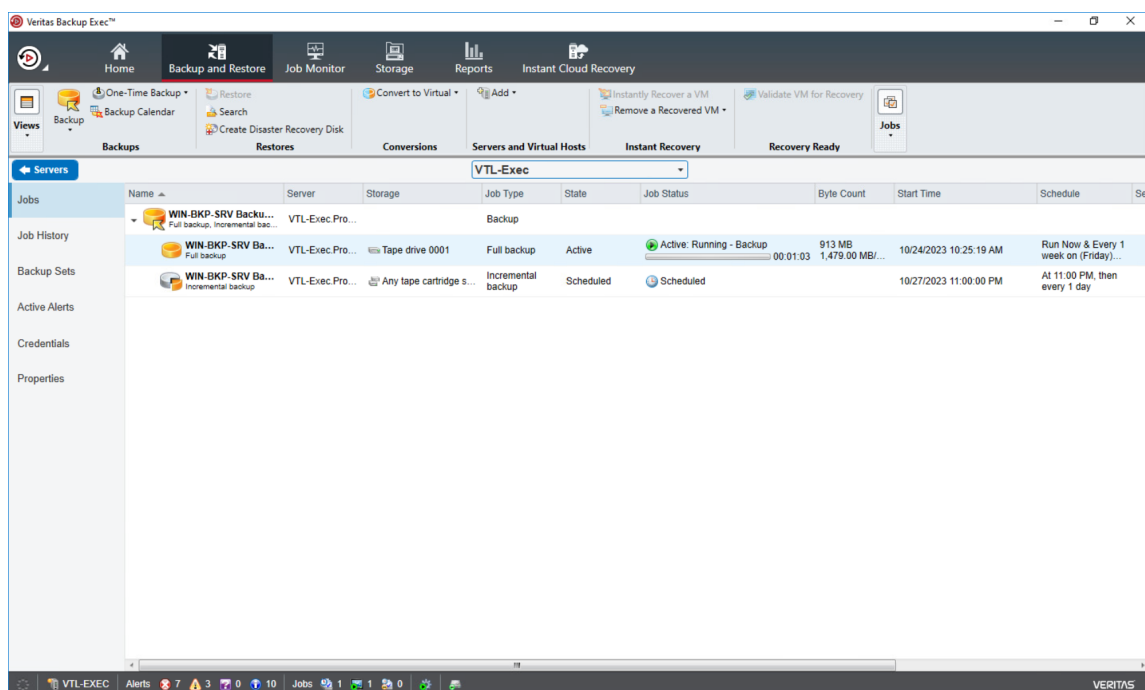
2. Configure the Backup settings and click OK.



3. Once the job is configured, click the appropriate button to start it.



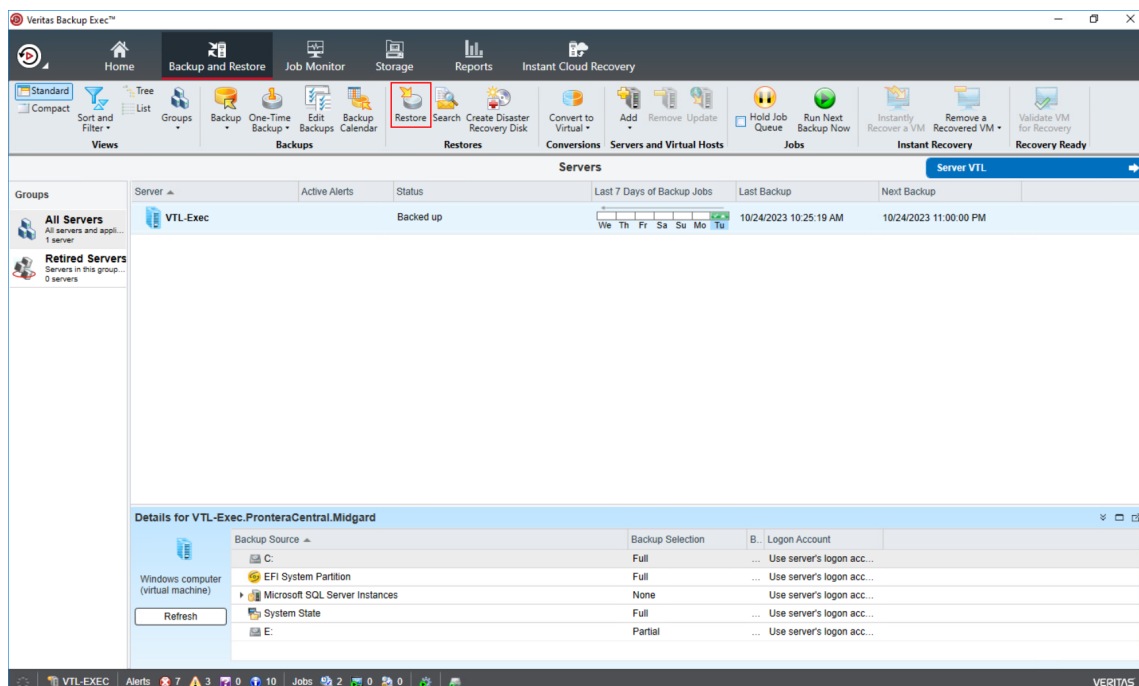
4. When the backup process starts, the progress is shown in the Status section. Double-click on the server to see the details.



5. To check the amount of the occupied storage space, navigate to the Capacity section.

Restore data from Veritas Backup Exec™

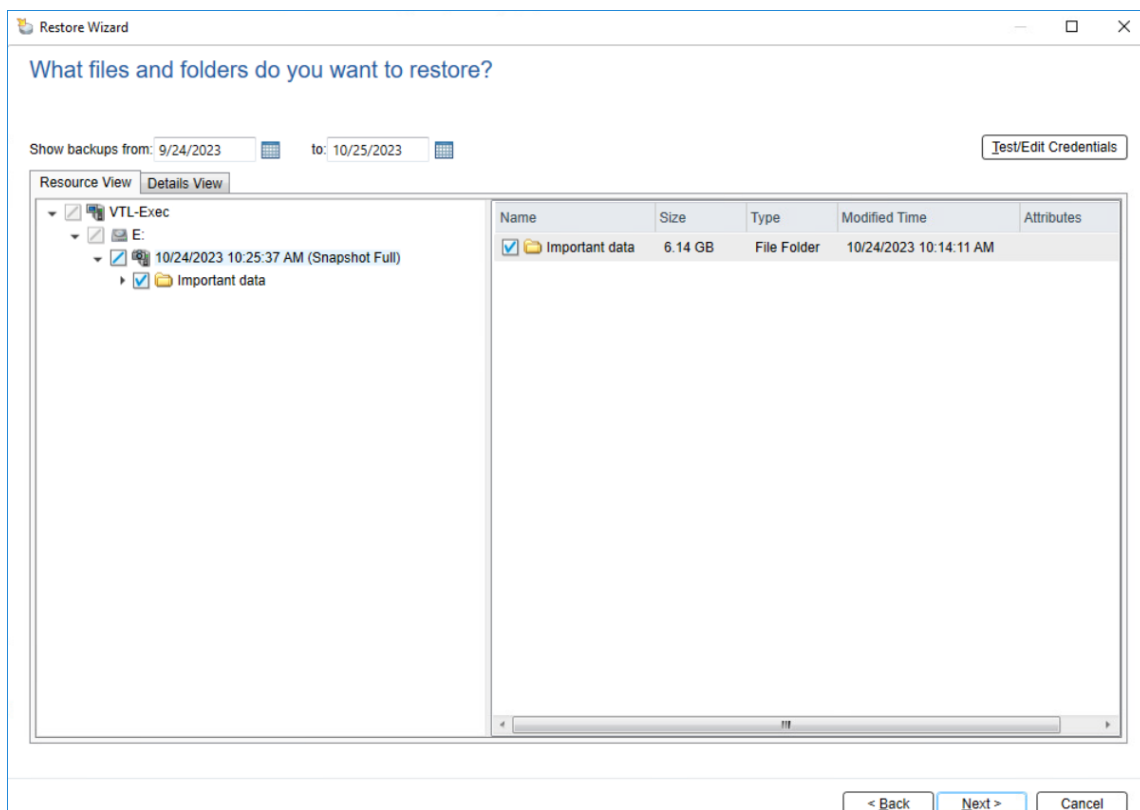
1. To restore data, click Restore in the Backup and Restore tab.



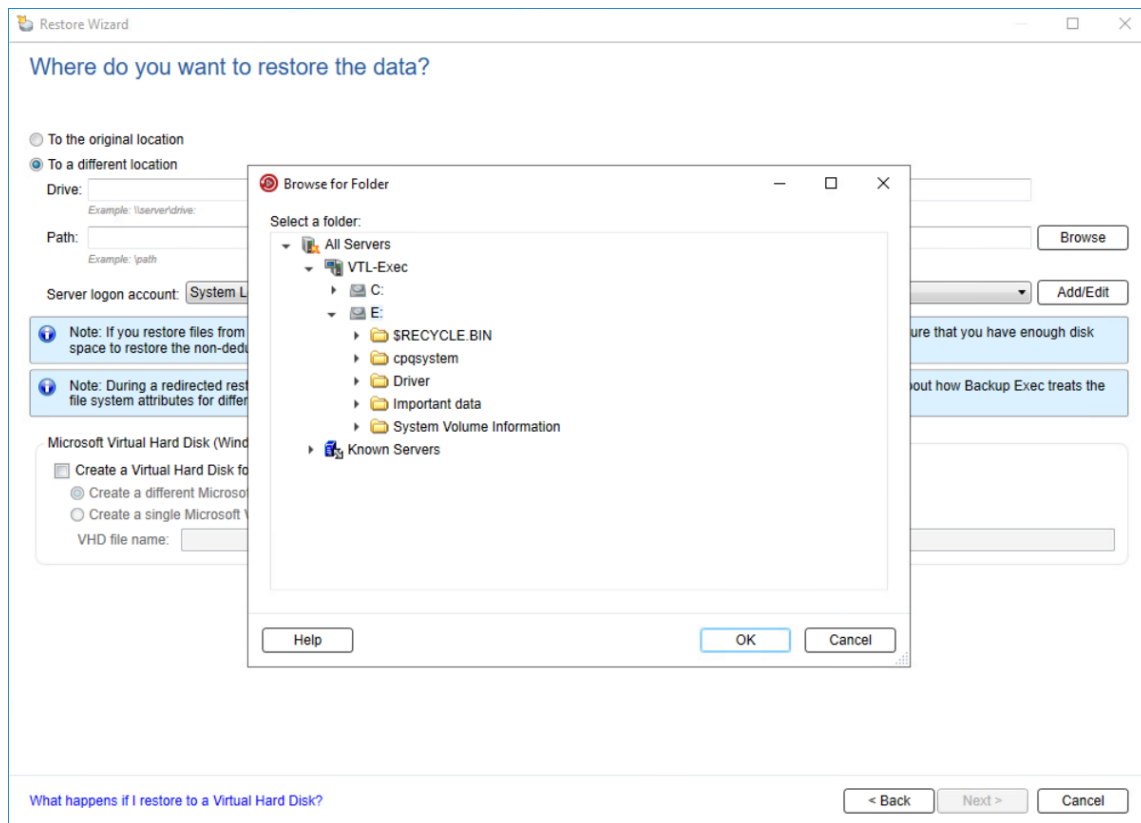
2. Select the type of data to restore.

3. Select the appropriate restore option.

4. Select files and folders to restore.



5. In the Browse for Folder window, specify the destination folder for the restored data and click OK. Then click Next.



6. Confirm the restore location and click Next.

Restore Wizard

Where do you want to restore the data?

☐ To the original location

☒ To a different location

Drive: \\VTL-Exec\I:
Example: \\server\drive

Path: \ Browse
Example: /path

Server logon account: System Logon Account Add/Edit

Note: If you restore files from a volume that has Windows deduplication, Backup Exec places the files on the disk as non-deduplicated. Ensure that you have enough disk space to restore the non-deduplicated data before you run a restore job. For more information see: [TECH204775](#)

Note: During a redirected restore, you may not be able to restore some file system attributes from the original data. For more information about how Backup Exec treats the file system attributes for different types of file systems, see: [TECH205960](#)

Microsoft Virtual Hard Disk (Windows Server 2008 R2 or later)

☒ Create a Virtual Hard Disk for redirected data

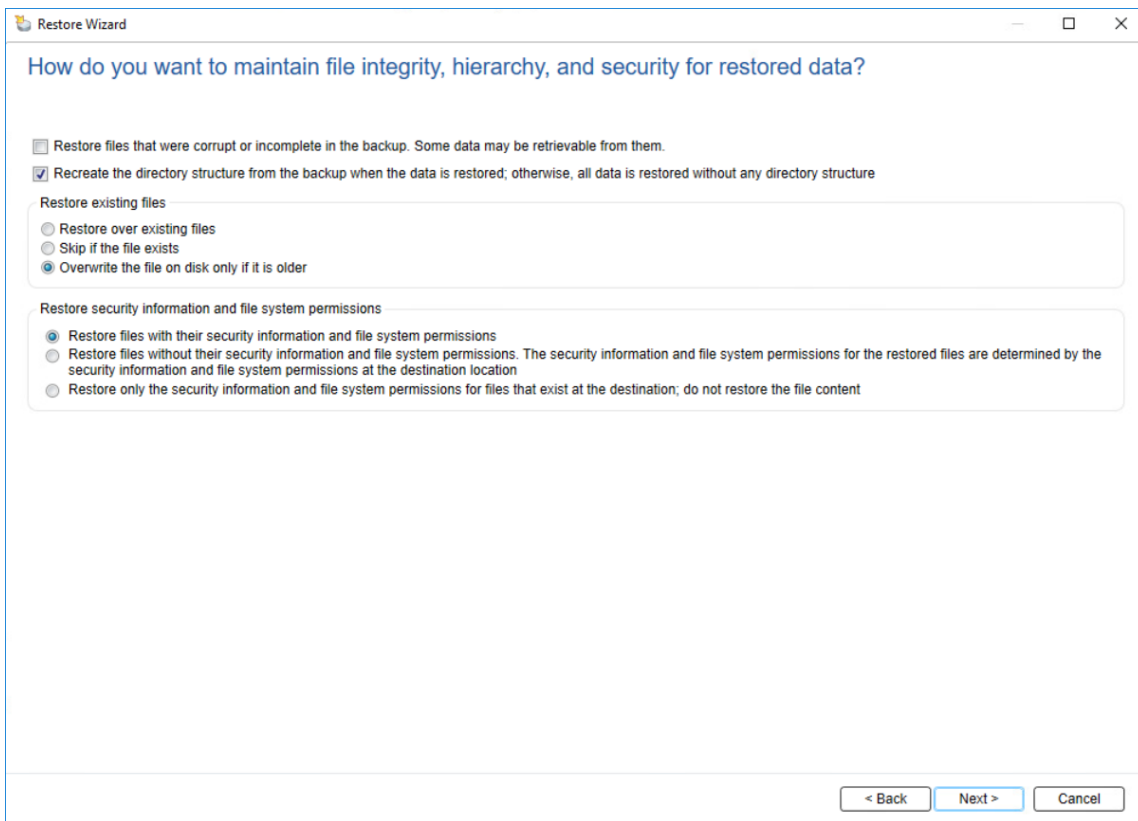
☒ Create a different Microsoft Virtual Hard Disk for each backup set that is restored

☐ Create a single Microsoft Virtual Hard Disk that contains the merged files and folders from all redirected backup sets

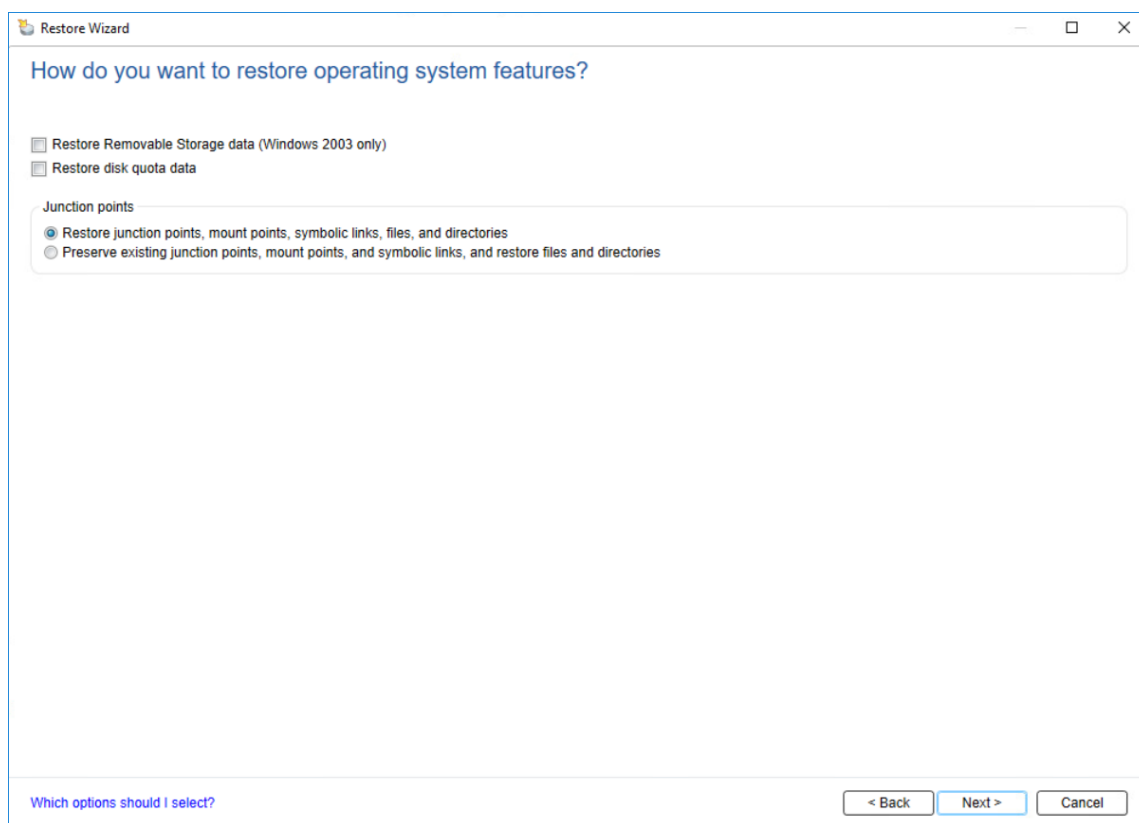
VHD file name:

[What happens if I restore to a Virtual Hard Disk?](#) < Back Next > Cancel

7. Select the settings for file integrity, hierarchy, and security for the restored data.



8. Select options for restoring operating system features.



9. Specify additional tasks to perform before and/or after a restore.

Restore Wizard

What additional tasks do you want to perform before and/or after a restore?

☐ Run a command before and/or after the restore

Type a command to run before the restore runs:

Type a command to run after the restore runs:

☐ Let Backup Exec check the exit codes of the commands to determine if the commands completed successfully

☒ Run job only if pre-command is successful

☒ Run post-command only if pre-command is successful

☒ Run post-command even if job fails

Cancel command if not complete within minutes

Run these commands:

☐ On this Backup Exec server

☒ On each server restored to

Notification

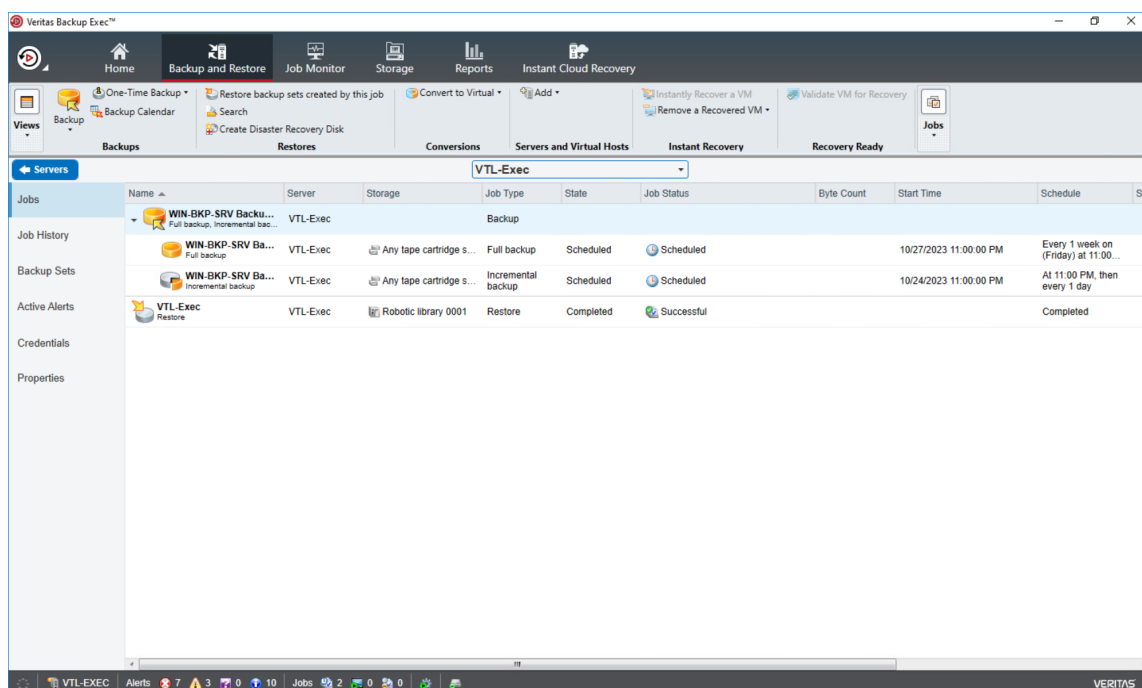
Select each recipient to notify when the job completes.

Recipient Name	Recipient Type

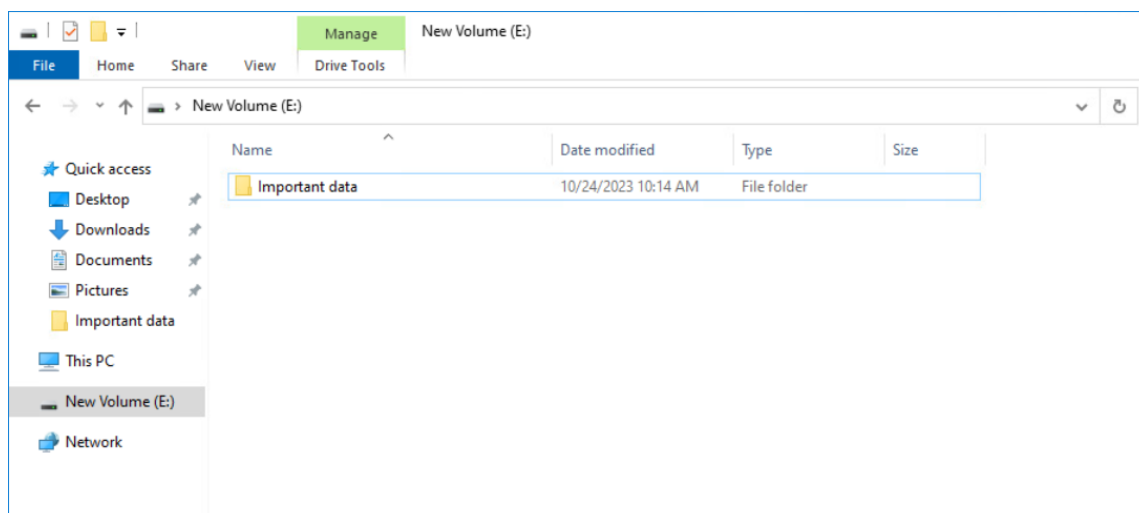
☐ Include the job log in email notifications

Which options should I select for the additional tasks?

10. Specify the restore job Name, Storage, and Schedule.
11. Double-check the summary and complete the restore job by clicking Finish.
12. To check the job progress, navigate to the Backup and Restore tab.
13. To see the restoring details, double-click on the server.



14. The restored files can be found in the specified folder.

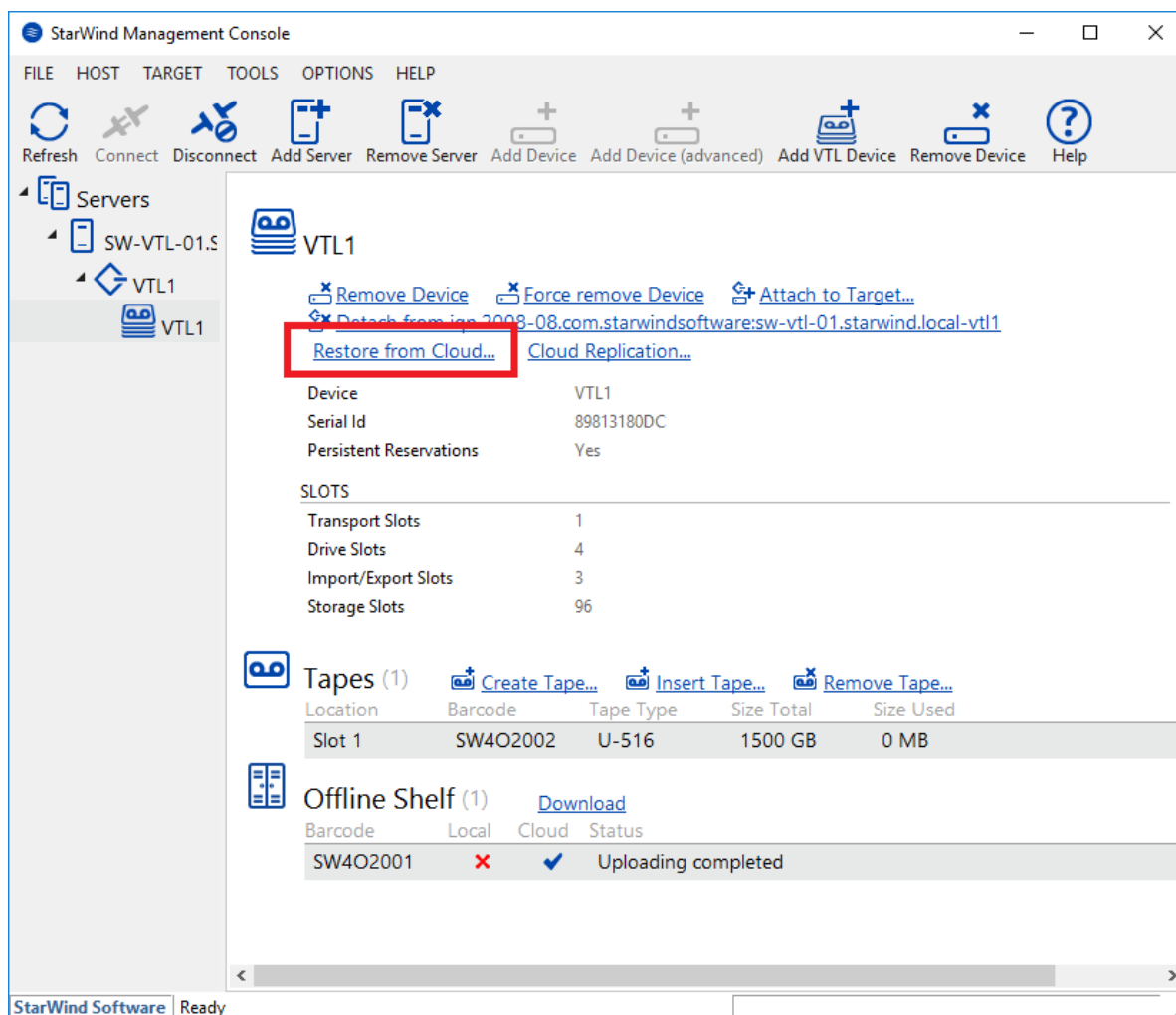


To restore files from the cloud storage, please navigate to Restoring tapes from the cloud storage section.

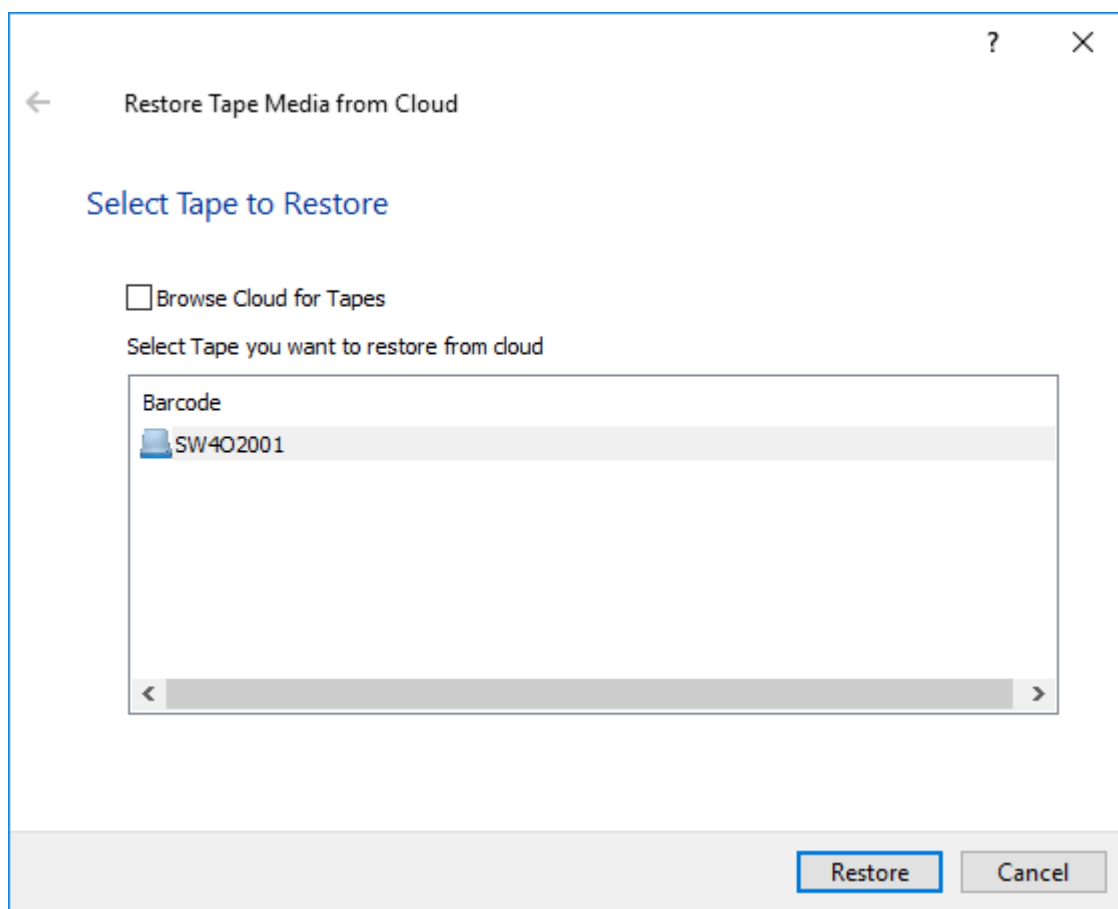
Restoring Tapes From Cloud Storage

After the time specified in StarWind VTL Retention Settings, the local copy of the tape will be deleted, but the tape can be restored from the cloud. In this case, information about the tape is located in the local database.

1. To restore the tape from the Cloud, open StarWind Management Console and choose the VTL device.
2. Click on the Restore from Cloud... option.



3. Identify the tape using its barcode. Click on the tape and press Restore.










4. The download progress can be checked in the Offline Shelf overview. When the download is completed, the tape location status in Offline Shelf overview will be marked as Local and Cloud.

Conclusion

Following this guide, a StarWind VTL was deployed and tapes replication was configured to the cloud object storage.

Contacts

US Headquarters	EMEA and APAC
 +1 617 829 44 95	 +44 2037 691 857 (United Kingdom)
 +1 617 507 58 45	 +49 800 100 68 26 (Germany)
 +1 866 790 26 46	 +34 629 03 07 17 (Spain and Portugal)
	 +33 788 60 30 06 (France)

Customer Support Portal: <https://www.starwind.com/support>

Support Forum: <https://www.starwind.com/forums>

Sales: sales@starwind.com

General Information: info@starwind.com



StarWind Software, Inc. 100 Cummings Center Suite 224-C Beverly MA 01915, USA
www.starwind.com ©2024, StarWind Software Inc. All rights reserved.