Dell EMC SC Series: Veeam Backup & Replication Integration

Abstract

This document provides guidance for integrating and configuring Veeam® Backup & Replication™ data protection solutions with Dell EMC™ SC Series storage.

August 2019

Revisions

Date	Description
August 2019	Initial release

Acknowledgements

Author: Jason Boche

Table of contents

Executive summary

Data protection and recovery are fundamental services that every data center provides. However, achieving effective and timely virtual machine recovery is challenged by workload consolidation through virtualization, increasing rates of data growth, and application and data mobility.

Dell EMC and Veeam have partnered to create a solution that addresses these challenges. This solution leverages the combined power of Veeam® Backup & Replication™ and the performance and scale of Dell EMC™ SC Series storage snapshots. This document provides guidance for integrating and configuring this data-protection solution.

D∅LLEMC

1   Introduction

Virtualization has been and continues to be a transformative technology in the modern data center. Conventional methods of server consolidation used in the past are no longer practical in a virtualize-first era. The benefits of efficiency, mobility, uptime, and cost savings are quickly realized. In the wake of these efforts, new opportunities for data protection and recovery have emerged. In some cases, these solutions have risen out of necessity to keep pace with virtualized data-center trends. In other cases, they are needed to maintain increasingly aggressive service-level agreements tied to data protection and recovery.

Veeam Backup & Replication offers several methods for protecting and recovering virtual machine (VM) and application-specific data in VMware® vSphere® environments. vSphere snapshots are leveraged to allow continuous operation of the VM. At the same time, the Veeam Backup & Replication proxy server streams the quiesced contents of the VM from its vSphere host to a Veeam native backup file. This file resides on storage that is accessible to the backup server. The length of time a VM is in vSphere snapshot mode depends on the amount of time it takes to back it up. When the backup is complete, the vSphere snapshot is closed. For small backup jobs, a VM may be in snapshot mode for a few minutes. For much larger jobs such as a full backup of a large data set, a VM may be in snapshot mode for several hours.

Veeam and Dell EMC have partnered to offer SC Series native snapshot support with Backup & Replication software, providing a scalable and performance-optimized solution with robust features. This offloads the bulk of the snapshot exposure and proxy server backup streaming from the vSphere host to the SC Series array during the backup process. Likewise, shortening the data-protection process by using SC Series snapshots allows for more snapshot frequency and a better Recovery Point Objective (RPO). Lastly, data recovery such as Veeam Instant VM Recovery® alternatively stems directly from SC Series view volumes instead of from backup files on Veeam vPower® NFS.
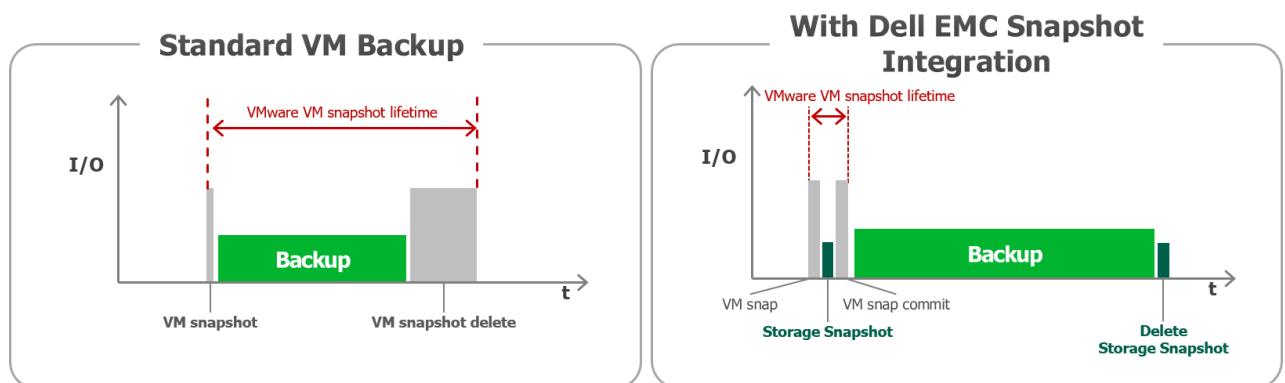

Figure 1   Virtual machine open snapshot lifetime comparison

This document provides a brief introduction to Veeam Backup & Replication with storage integration. For more detailed information, refer to the Veeam Backup & Replication 9.5 Update 4 User Guide for VMware vSphere. Veeam supports Microsoft® Hyper-V® but this paper focuses on VMware vSphere virtualization.

2 Requirements

This section describes the requirements to integrate Veeam Backup & Replication software with SC Series storage.

Backup & Replication requirements:

- Veeam Backup & Replication 9.5 Update 4b or newer is required.
- Backup servers may be physical or virtual.
- The SC Series plug-in is installed only on the backup server.
- The SC Series plug-in is not installed on separate proxy servers.
- iSCSI proxy servers may be virtual or physical.
- Fibre Channel proxy servers must be physical and zoned to the SC Series storage.
- The proxy server must have Fibre Channel or iSCSI fabric connectivity to the SC Series storage.
- VMware vSphere Virtual Volumes™ (vVols) are not supported.
- Physical mode Raw Device Mapping (pRDM) is not supported.
- Veeam-specific features such as Explorer from Storage Snapshot, Backup from Storage Snapshot, Snapshot only jobs, and On-Demand Sandbox for Storage Snapshots require an appropriate level of Veeam licensing covered by Veeam Backup & Replication, Veeam Availability Suite, or Veeam Essentials.

SC Series requirements:

- Dell™ Storage Center OS (SCOS) 7.4 firmware is required.
- An administrator-level account is required on SC Series storage to be used as Veeam credentials. For security and audit best practices, this should be a service account.
- Live Volumes are not supported.
- There are no Dell EMC licensing requirements specific to Veeam integration.

3 SC Series infrastructure setup and configuration

To begin setup, download the Dell EMC SC Series plug-in for Veeam Backup & Replication from the Veeam website. Install the plug-in on the Veeam backup server.
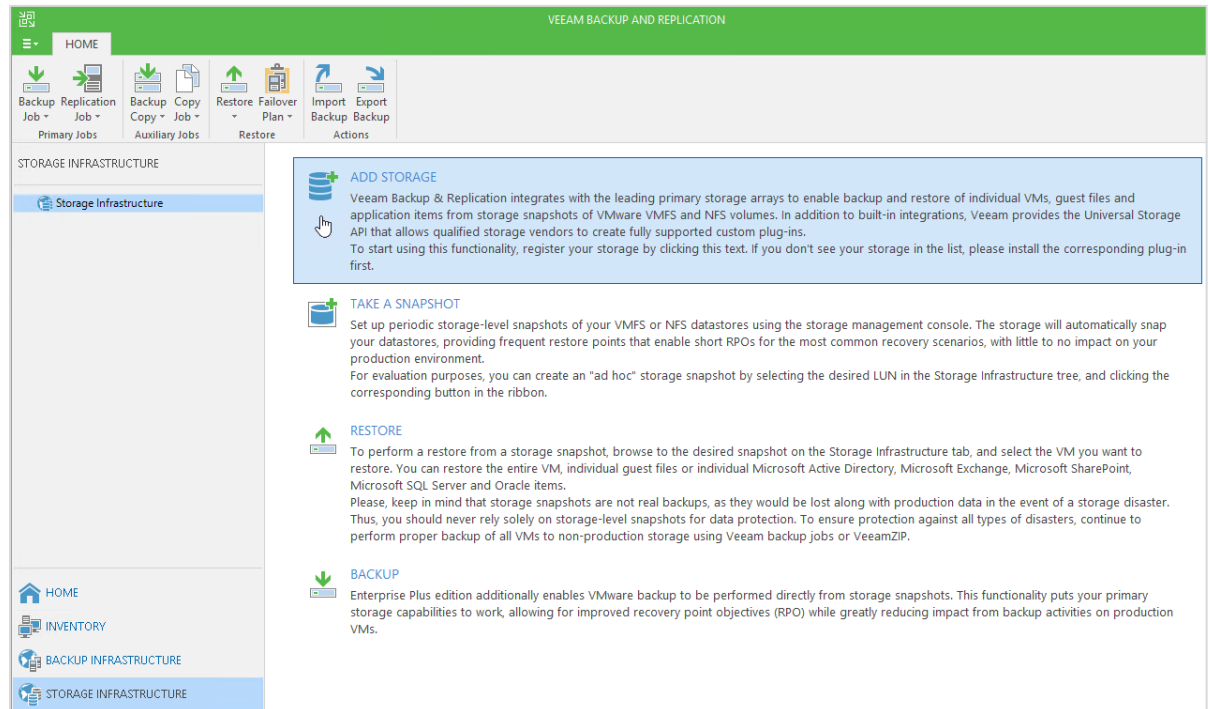
With the plug-in installed, before SC Series storage can be integrated, setup must first take place in Veeam Backup & Replication. Additional configuration is optional and depends on the needs of the environment.

Note: For the initial storage discovery, Veeam recommends adding vSphere infrastructure before adding the storage infrastructure, but this is not necessary. Veeam needs this to compare the list of virtual machines found within each snapshot.
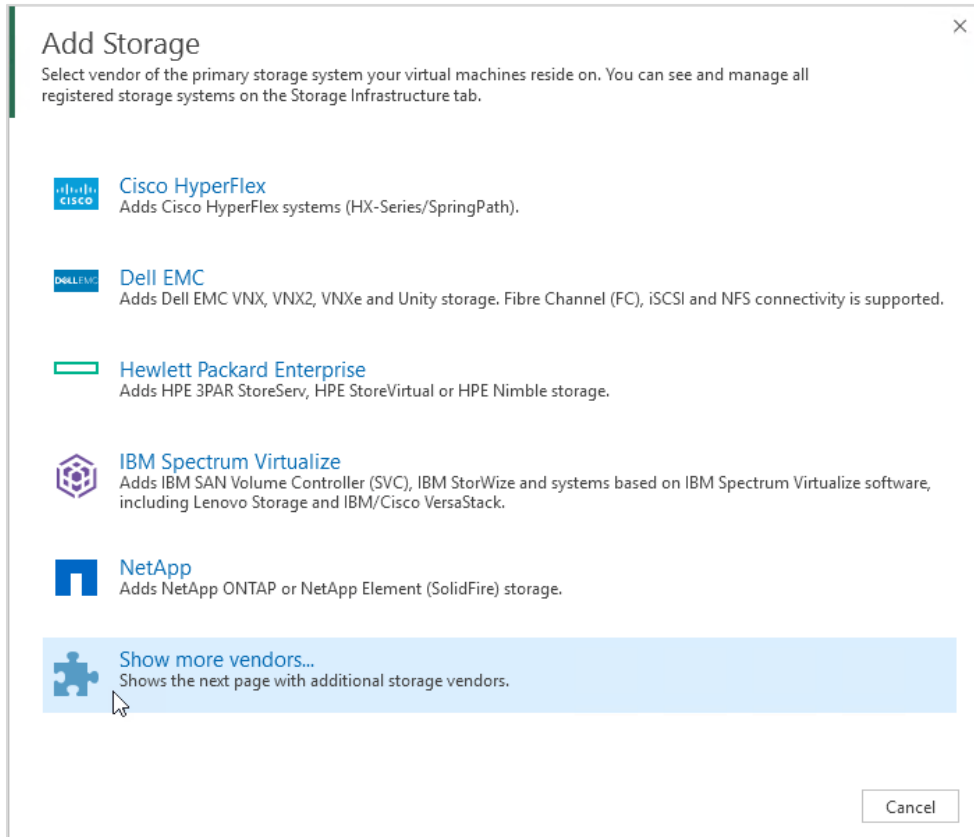
3.1 Adding SC Series to the storage infrastructure

Each SC Series array that will be integrated with Veeam Backup & Replication must be added to the storage infrastructure.
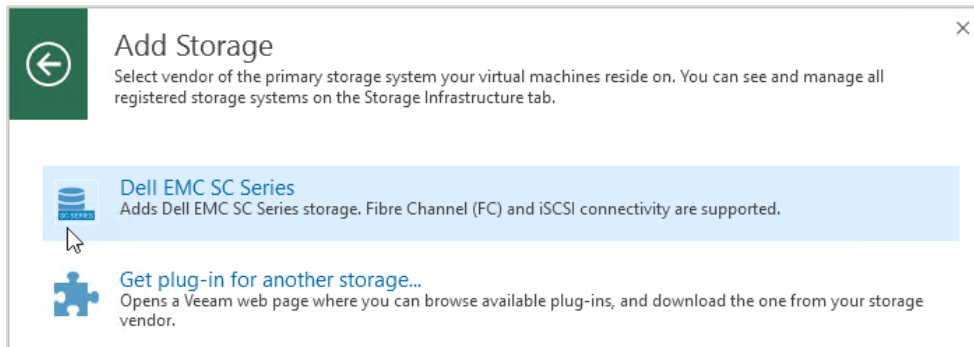
1. In the **Storage Infrastructure** menu, click **Add Storage**.

2. Click **Show more vendors**.

3. Click **Dell EMC SC Series** to select the installed SC Series plug-in.

4. Enter the SC Series management DNS FQDN or IP address.

Note: SC Series storage is added to the Veeam storage infrastructure by each individual storage array. Dell™ Storage Manager (DSM) federated storage management is not involved in Veeam integration.

5. In the **Credentials** drop-down menu, choose or create an administrator-level account that has been created on SC Series storage.

6. Choose the protocol which will be used between the backup proxy server and SC Series storage. In the following example, iSCSI is used. A backup proxy can be automatically selected or specifically named here.
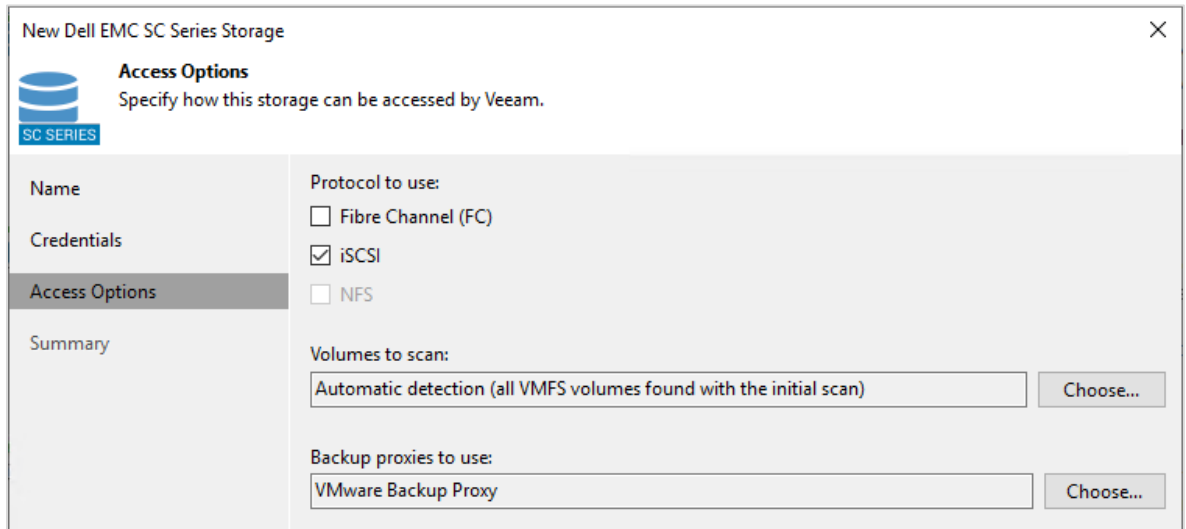
Note: In smaller environments, the backup server and the proxy server often are the same server sharing both roles. In larger environments, there may be separate proxy servers. In addition, **Volumes to scan** may be filtered now or later to speed up the scan process and reduce the number of storage objects visible in Veeam Backup & Replication. Live Volumes will automatically be filtered out because they are not supported.

7. As part of the prior steps and in iSCSI environments, Veeam will automatically create the necessary proxy server object(s) on the SC Series storage with the appropriate iSCSI initiator information. In Fibre Channel environments, the proxy server object(s) must be created manually as well as zoned to the SC Series storage. Proxy server LUN mappings are not required as Veeam handles this automatically.
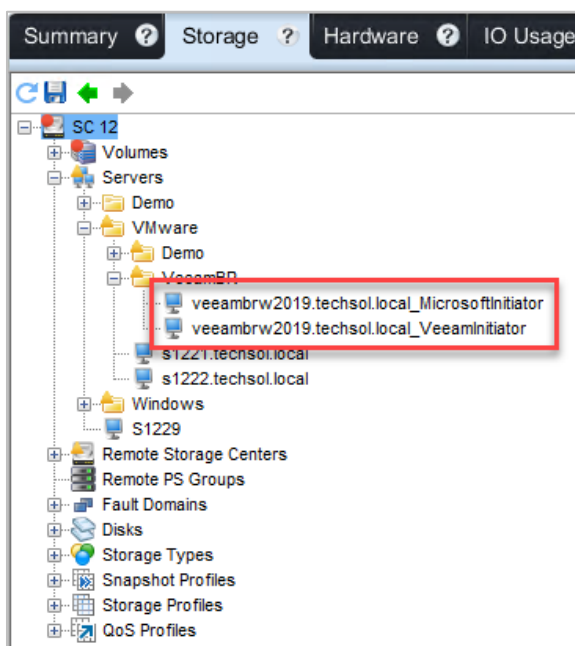
Note: During a Veeam rescan process, a Veeam IQN is used. During Backup from Storage Snapshot process, a Microsoft IQN is used. During a restore process, Veeam will try an ESXi IQN one by one and if necessary create a server object.

3.2 Configuring SC Series storage infrastructure

After adding SC Series to the storage infrastructure, the environment may be tuned.

3.2.1 Volume filtering

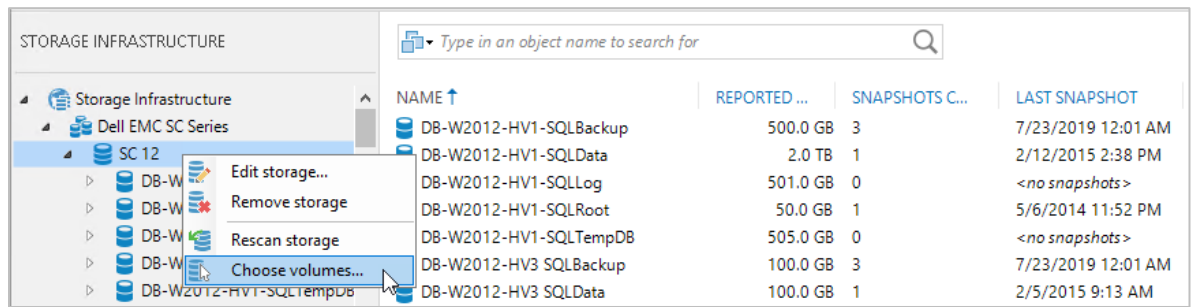With SC Series being shared storage, non-VMware or an overwhelming number of volumes may initially be discovered by Veeam as shown below.

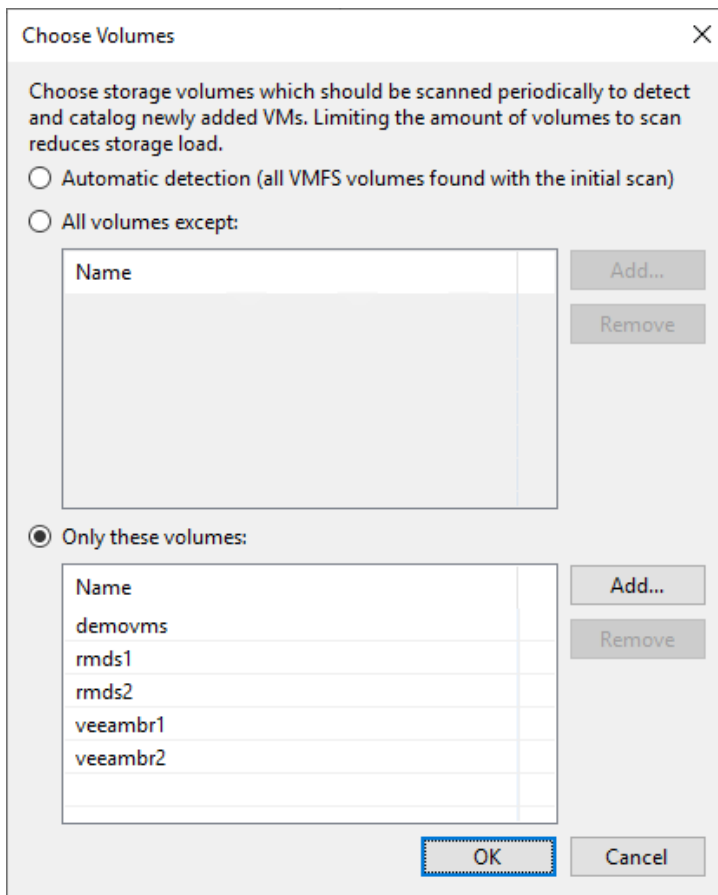1. To filter out the unnecessary volumes, right-click the SC Series storage and click **Choose volumes.** Veeam documentation refers to this process as limiting the rescan scope.

2. Choose the volumes to use exclusively with Veeam Backup & Replication or filter them out.

3. After the next storage discovery, the volume list should reflect the volume filtering preferences. The SC Series arrays and corresponding volumes will be the only volumes available to Veeam storage snapshot integrated data protection and recovery jobs. Storage discoveries and rescans will complete quicker with a lower number of volumes and snapshots to work with.

Note: Up to this point, a Veeam data protection job has not yet been created or run. However, the SC Series volumes and corresponding snapshots found in the discovery process can already be leveraged by Veeam for Instant VM Recovery. Almost any SC Series snapshot, regardless of how it was created, can be used by Veeam to recover VM data as long as the volume is tied to a vSphere infrastructure managed by Veeam.

3.2.2 Proxy server object in Dell Storage Manager

The proxy server initiator is activated on-demand and as needed by Veeam. During periods of downtime, the server object initiator in Dell Storage Manager (DSM) may flag as paths being down along with a red error status. This may generate unnecessary alerts in DSM. This red alert condition can be eliminated by editing the server object and unselecting the two boxes which alert on lost or partial connectivity as shown below.
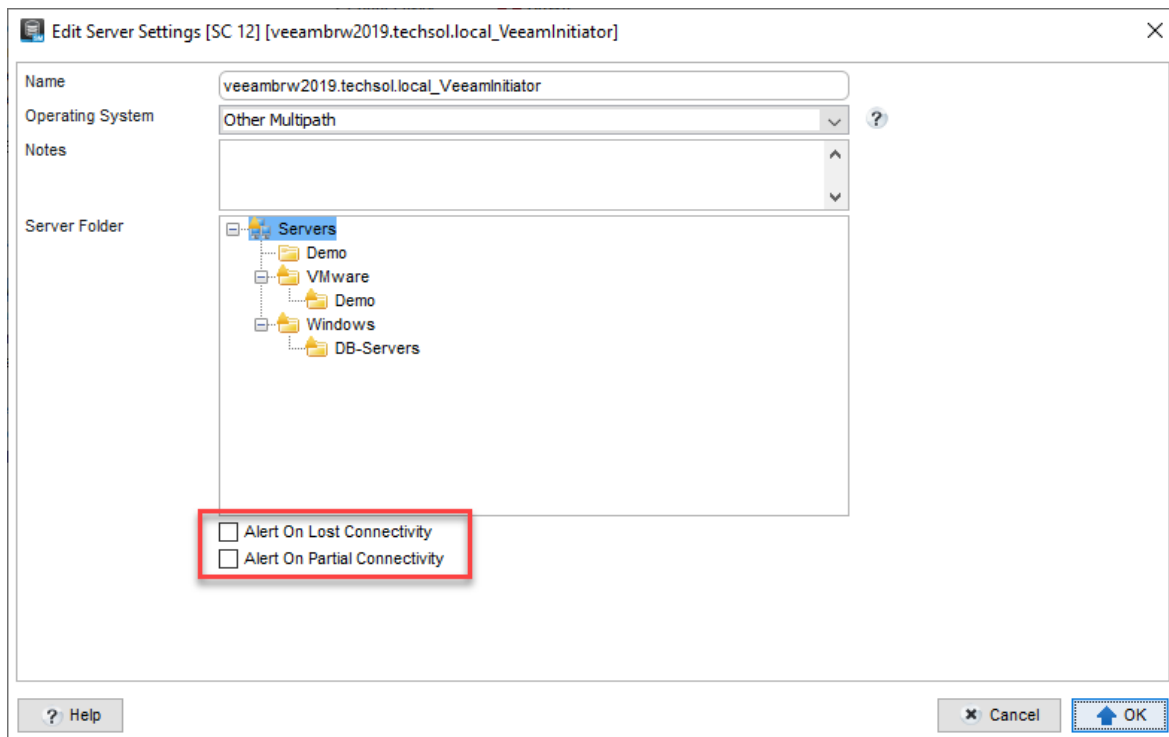
Note: Veeam recommends multipath I/O (MPIO) for proxy servers.

3.2.3 Configuring proxy server transport mode in Veeam

The Veeam Backup & Replication proxy server transport mode defines how the proxy server retrieves virtual machine data for backup repository jobs. Several modes are available:

- Automatic selection: Data retrieval mode selection is automatic. Direct storage access through the Dell EMC SC Series plug-in will be used whenever possible if installed, configured, and available.
- Direct storage access: Direct storage access through the Dell EMC SC Series plug-in will be used.
- Virtual appliance: The proxy server is deployed as a virtual machine. VM virtual disks in scope of the backup job are hot added to the proxy server VM configuration while the backup job runs. VM virtual disks are hot removed after the backup job completes.
- Network: The proxy server retrieves VM data from the vSphere hypervisor through the network using the NBD protocol over the vSphere management network.

The default transport mode is automatic selection. If the proxy server is dedicated to SC Series integration, it may be preferred (but unnecessary) to force the transport mode to direct storage access. To do so, complete the following steps.

1. In the **Backup Infrastructure** menu, right-click the proxy server and click **Properties.**
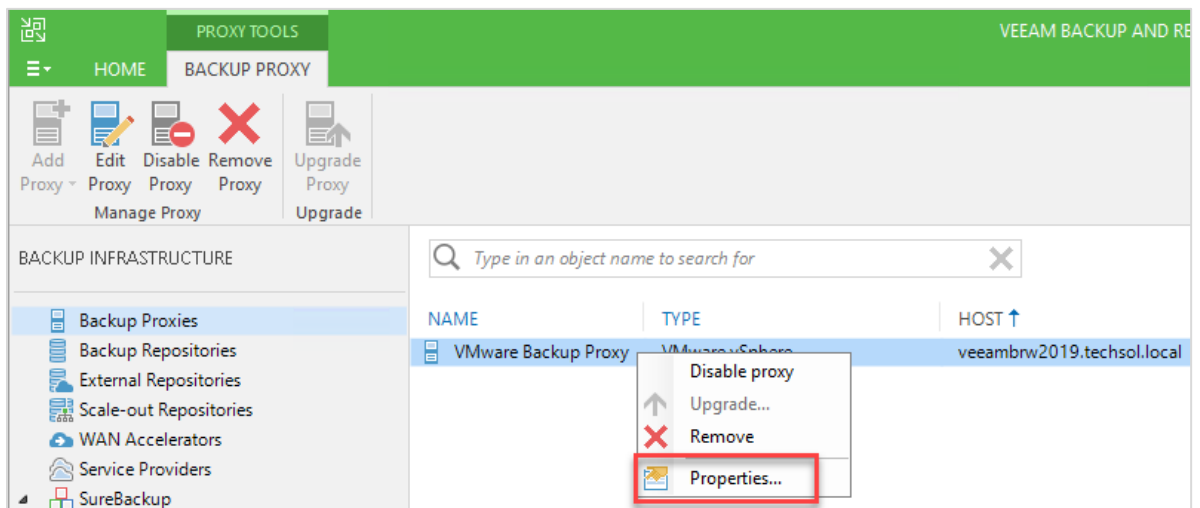
2. Under **Transport mode**, click **Choose**.
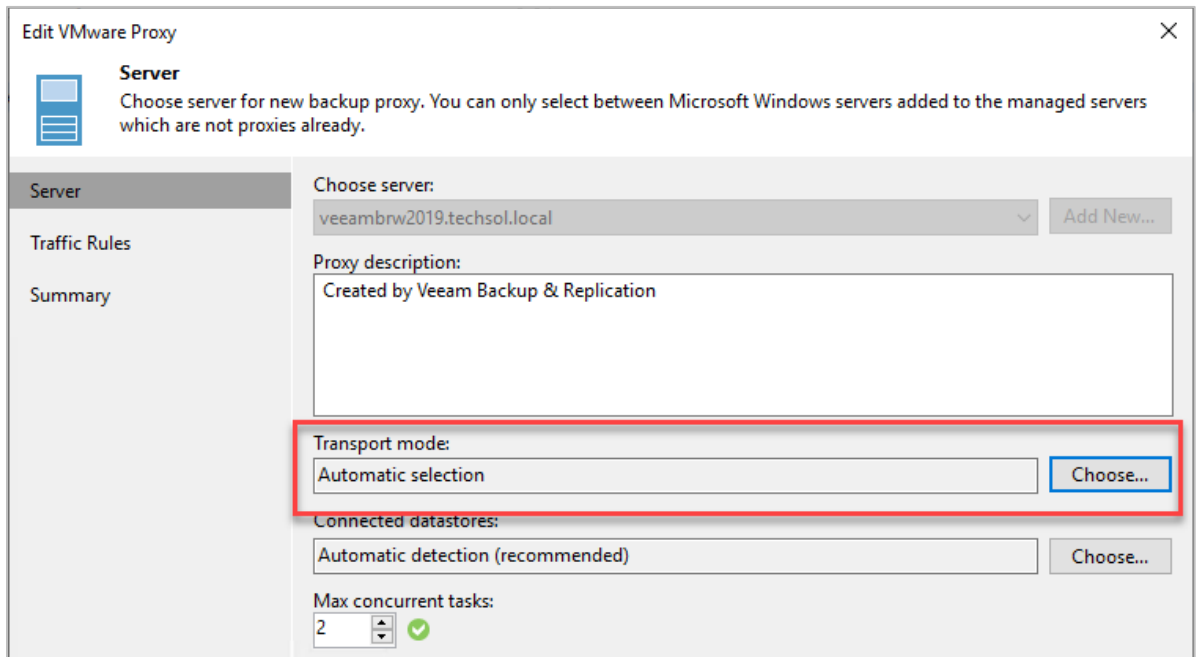
3. Select **Direct storage access**.
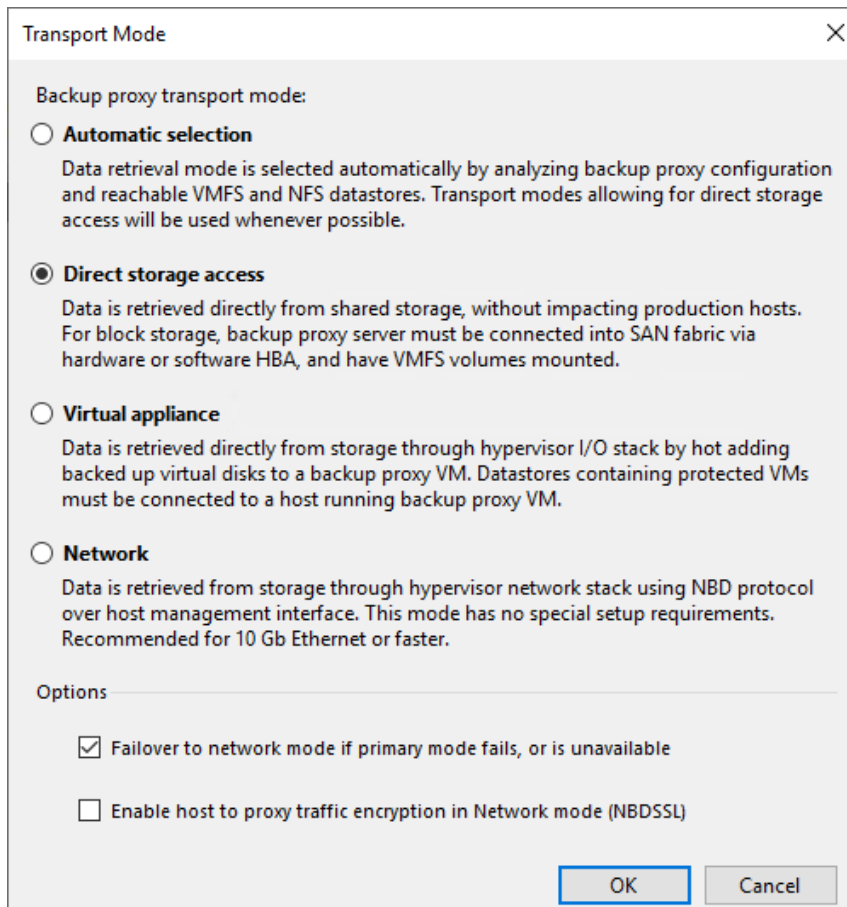
4. Click **Finish**.

Note: The transport mode applies to backup jobs only. For instance, a snapshot takes place and VM data is streamed by the proxy server to a backup repository that is accessible to the backup server. The transport mode does not apply to Dell EMC SC Series snapshot jobs.

4   Backup job creation

Backing up and restoring VM data is where operations staff spend the bulk of their time within Veeam Backup & Replication. These areas are also where the Dell EMC SC Series plug-in integration comes into play. Within the Veeam Backup & Replication user interface, there are many ways in which to create a backup job. The operational process and options for creating backup jobs are well documented by Veeam and are not included in this document. However, with storage integration there are a few underlying differences to point out. They are important to understand because this is where the plug-in yields its benefits.

4.1   Veeam backup repository

If backing up VM data to a native Veeam backup repository, choose this repository in the backup job. Locate the backup repository choice in the **Storage** section of the backup job configuration.

Veeam will create a backup chain in the repository which contains a number of file types such as .VBK, .VIB, .VRB, and .VBM. The effective data retention is controlled by the value of **Restore points to keep on disk** and is built into the backup chain.

Although Veeam leverages its own backup chain on a backup repository, SC Series snapshots add value and are used in this process. Without storage snapshots, the vSphere snapshot remains open during the duration of the backup which could be several hours or longer. The process is represented in the following points and uses relative times as an example:

1. vSphere snapshot is opened for quiesce and data consistency (5 seconds)
2. VM data to be backed up is streamed to backup repository (hours)
3. vSphere snapshot is closed (depending on size of data, a lengthy time plus risk of corruption)

When storage snapshots are used, the vSphere snapshot is only open for a brief time. In addition, the proxy server accesses the VM data from SC Series storage directly over the Fibre Channel or iSCSI fabric. The same process is represented in the following points and uses relative times as an example:

1. vSphere snapshot is opened for quiesce and data consistency (5 seconds)
2. SC Series snapshot is created (1 second)
3. vSphere snapshot is closed (5 seconds, minimized risk of corruption)
4. SC Series view volume from above snapshot is mapped to proxy server (1 second)
5. VM data to be backed up is streamed from view volume to backup repository (hours)
6. SC Series view volume from above snapshot is unmapped from proxy server (1 second)
7. SC Series view volume from above snapshot is deleted (1 second)
8. SC Series snapshot is expired (1 second)

Note: For this type of backup job, the SC Series snapshot is transient and is expired by Veeam when the backup job completes.

4.2 SC Series snapshot

If backing up VM data to SC Series snapshots, choose the Dell EMC SC Series Snapshot backup repository in the backup job. Locate the backup repository choice in the **Storage** section of the backup job configuration.
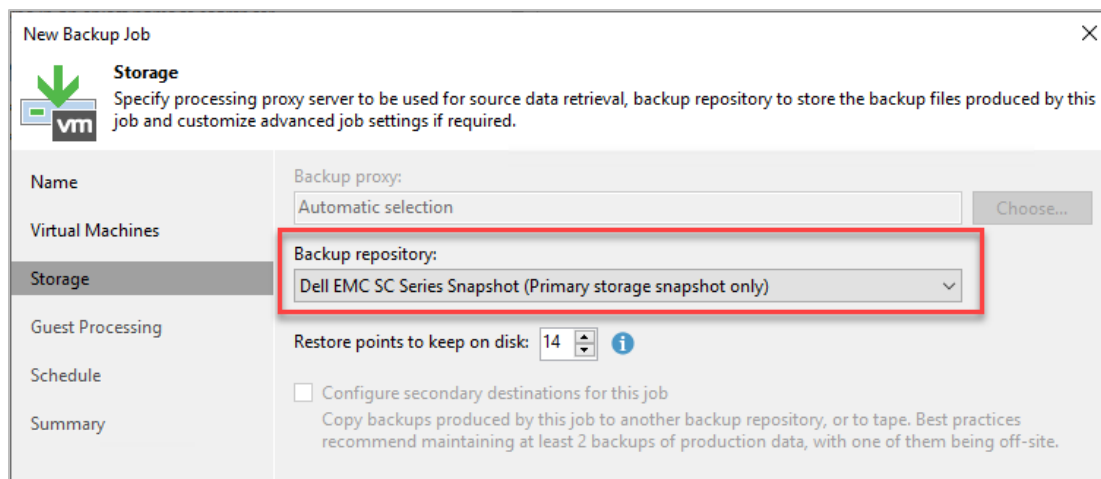
With this type of backup job, Veeam bypasses the use of a backup chain and the VM data is essentially backed up to an SC Series snapshot. The effective data retention is controlled by the value of **Restore points to keep on disk**. In this case, this value is similar to SC Series storage snapshot retention. The storage snapshots are created with no expiration and Veeam will expire the snapshots once the data retention value has been surpassed by a given snapshot. If a backup job is deleted, the unexpired storage snapshots tied to the backup job are orphaned on the array. These will need to be manually cleaned up later or they will remain there forever since they were created with no expiration. This process could be audited and automated through PowerShell since both Veeam and SC Series storage support their own set of operational management cmdlets.

Once again, when storage snapshots are used, the vSphere snapshot is only open for a brief time. However, because VM data is not streamed to a traditional Veeam backup repository, this type of backup timeline is much shorter. This is represented in the following points and uses relative times as an example:

- vSphere snapshot is opened for quiesce and data consistency (5 seconds)
- SC Series snapshot is created (1 second)
- vSphere snapshot is closed (5 seconds, minimized risk of corruption)
- SC Series snapshot is retained for data retention period and eventually expired by Veeam once the data retention value has been surpassed

Note: In this use case, primary storage snapshots are being used as backups. Storage snapshots work well for facilitating day-to-day restore activity. However, in the event of a disaster which impacts the primary SC Series array, the backups and restore points are lost. Consider replicating the Veeam-created snapshots asynchronously or synchronously to a remote site for disaster-recovery purposes.

4.3 Secondary destinations

Another option for backup job creation is the use of a secondary destination. When creating a backup job using a Veeam backup repository, check the box labeled **Configure secondary destinations for this job**. Virtual machines will be backed up to a Veeam backup chain. The storage snapshot used in that job will also be preserved on the array for a specified number of days. This feature creates two backups of production data.
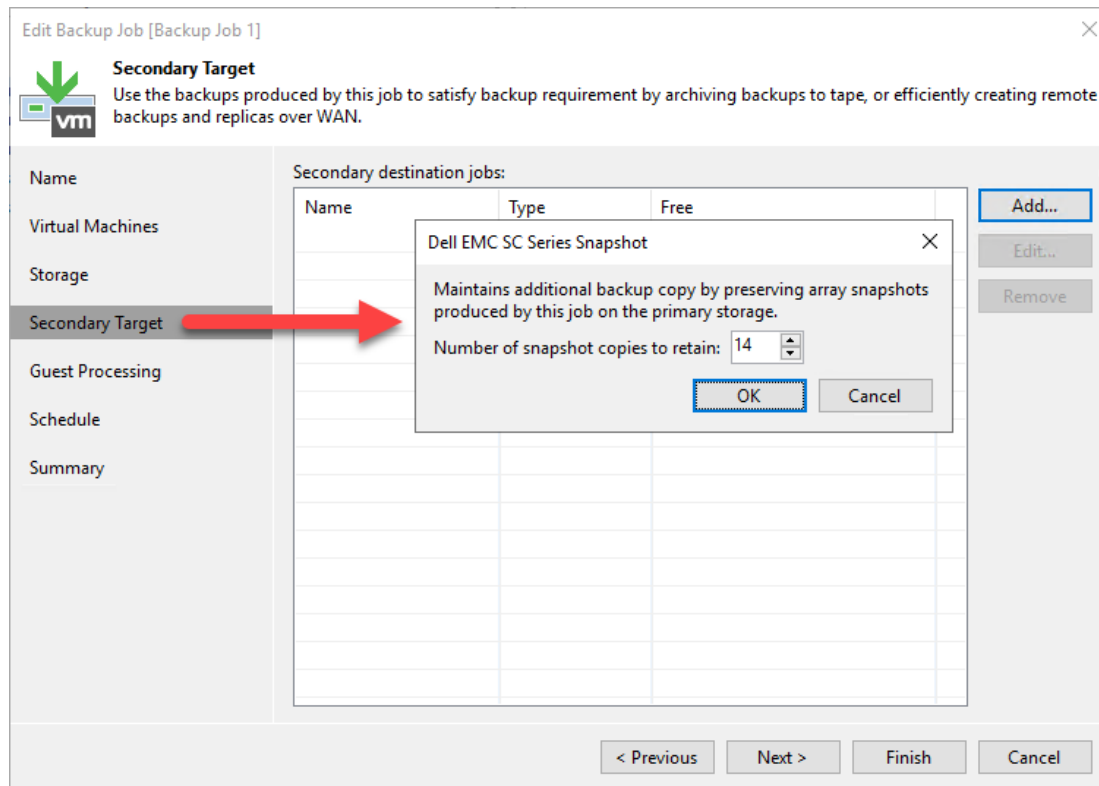
5 Instant VM recovery

Similar to creating backup jobs, the SC Series plug-in integration plays a role in data recovery when recovering from storage snapshots. The key differences between the two methods are the storage protocol and performance of the recovered VM when it is powered on.

5.1 Veeam backup repository

Virtual machine data stored in a Veeam backup chain is recovered with the vPower NFS datastore that is mounted to the recovery vSphere host. With this type of backup job, the added benefits of storage snapshot integration have already been realized in the amount of time a vSphere snapshot remains open during backup. Once the original backup job completed, the associated storage snapshot is expired. There is no SC Series view volume to recover from. Instant VM Recovery from vPower NFS is a proven recovery method. However, the intermediate storage performance of the virtual machine is not designed to match the performance of the original datastore backed by a SAN. vPower NFS is designed to recover a VM quickly to meet an aggressive recovery time objective (RTO). Shortly after, the VM can be migrated using VMware Storage vMotion™ to a more suitable location. This storage location would have services as defined in a service level agreement such as performance profile, data reduction, replication, and encryption.

5.2 SC Series snapshots

Virtual machine data stored in an SC Series snapshot is recovered with a view volume stemming from the original point-in-time snapshot. When the restore is performed, Veeam orchestrates the process as follows:

1. Create the view volume.
2. Map the view volume to the recovery vSphere host through Fibre Channel or iSCSI.
3. Register the VM .
4. Power on the VM.

The powered-on VM remains running on the view volume until the necessary VM data is recovered or is Storage vMotioned back to its appropriate datastore. At this time, the restore job is terminated and Veeam orchestrates the process of unmounting the view volume from the recovery vSphere host. Finally, the view volume is destroyed. There is a key difference and benefit here: Through the view volume, the powered-on VM inherits the data services of its original volume such as performance profile, data reduction, and encryption. Also, a view volume is more scalable to meet the needs of simultaneous VM recoveries while maintaining these data services.

Another powerful benefit is that through the storage discovery mechanism, Veeam can recover VM data from a variety of SC Series snapshot sources. Storage snapshots created by a volume snapshot profile, DSM, the PowerShell API, Replay Manager, and the vSphere web client plug-in all can be used for Instant VM Recovery. The following example shows an Instant VM Recovery with different SC Series snapshots types to choose from.

1. Under **Storage Snapshots**, drill down to the volume and virtual machine to be recovered. **Choose Instant VM recovery.**
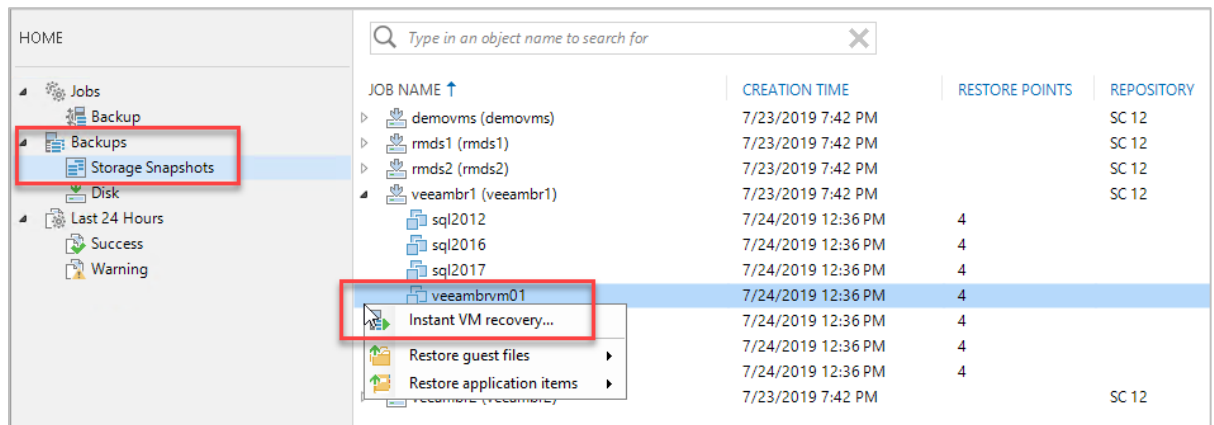

2. Select the storage snapshot to recover from. Note the blend of available snapshot sources.

   – A snapshot from a Veeam Backup & Replication backup job is outlined in green.
   – Snapshots from a volume snapshot profile are outlined in blue.
   – Snapshots from a vSphere web client plug-in are outlined in red.
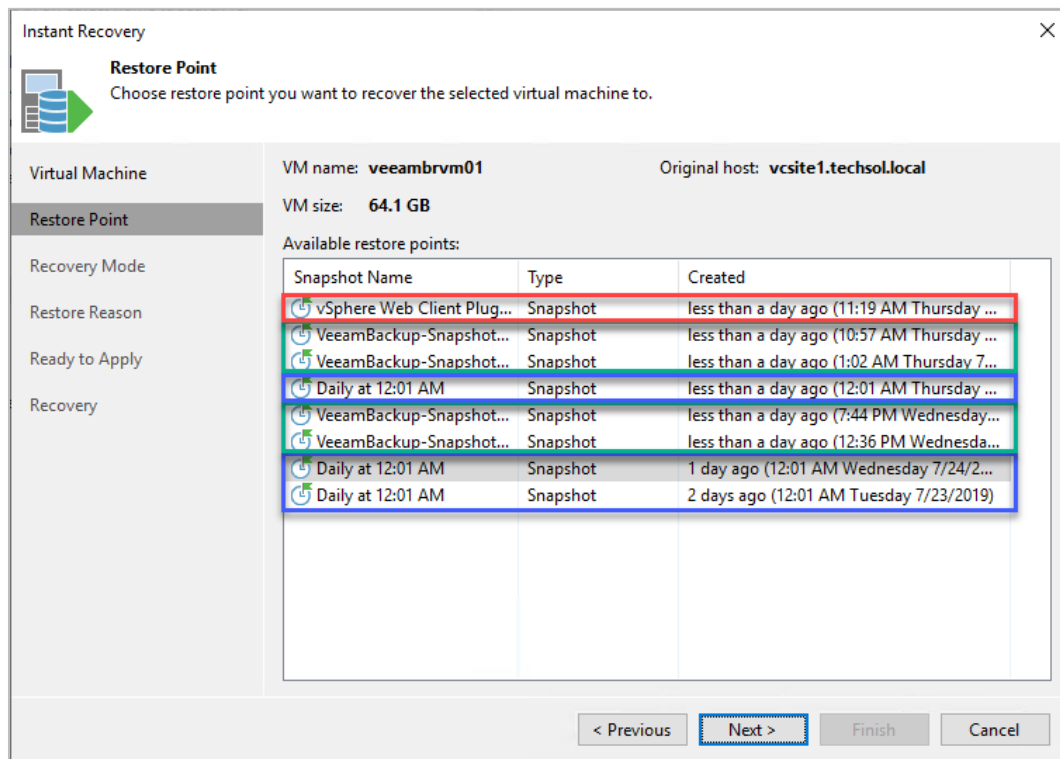

3. The **Recovery Mode** refers to VM inventory name and location but does not initially restore the VM back to the original datastore.

   – **Restore to the original location** powers off and deletes the existing VM prior to the restore.
   – **Restore to a new location** allows for VM recovery while the existing VM persists in parallel.

In either case below, a view volume is used for the recovery. In this example, the restore is redirected to an alternate View volume.
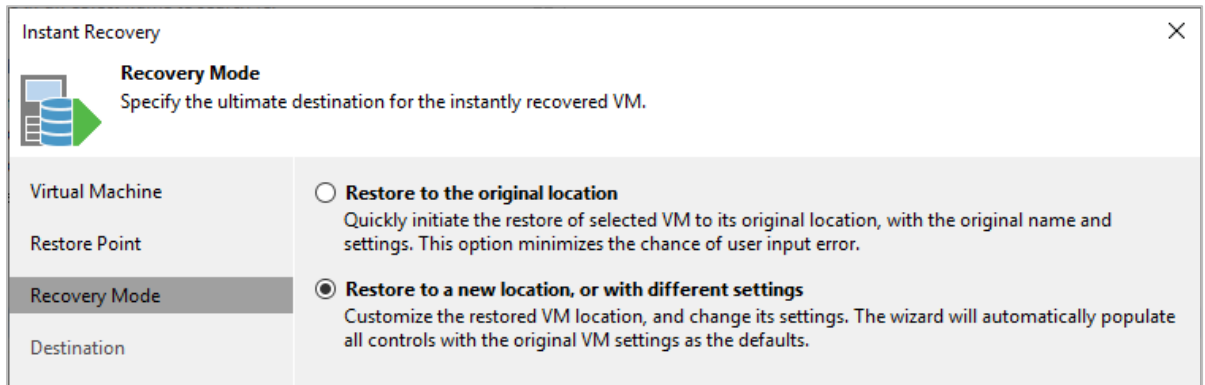
4. Provide the restored VM name, inventory location, and resource pool before completing the Instant VM Recovery workflow steps.
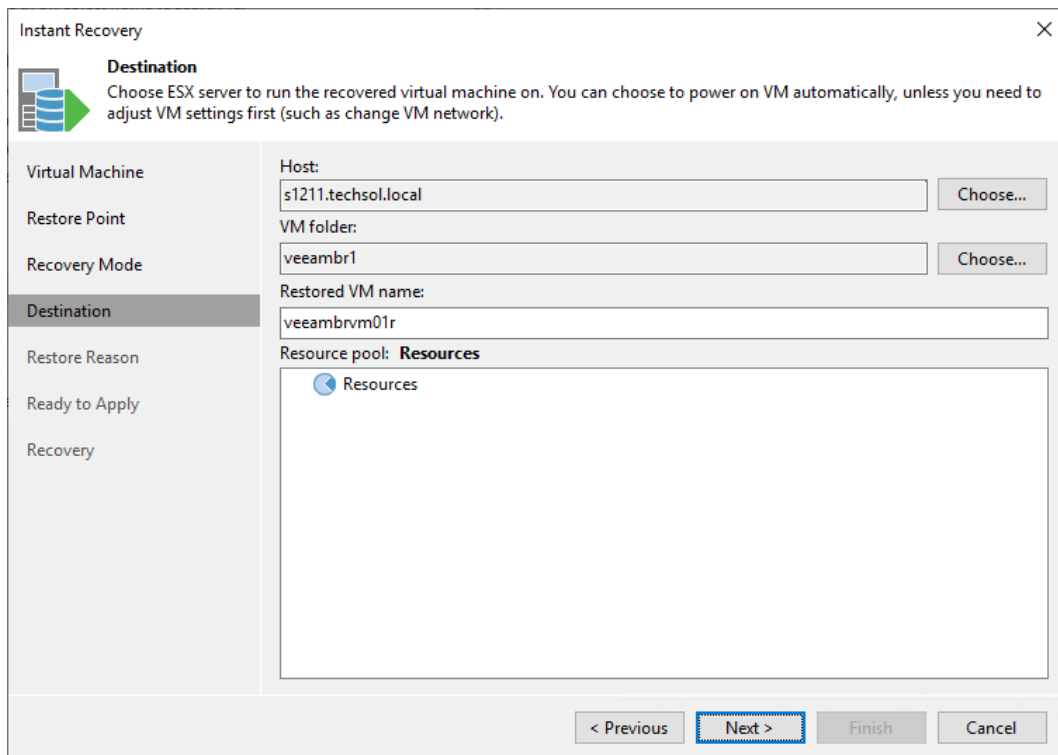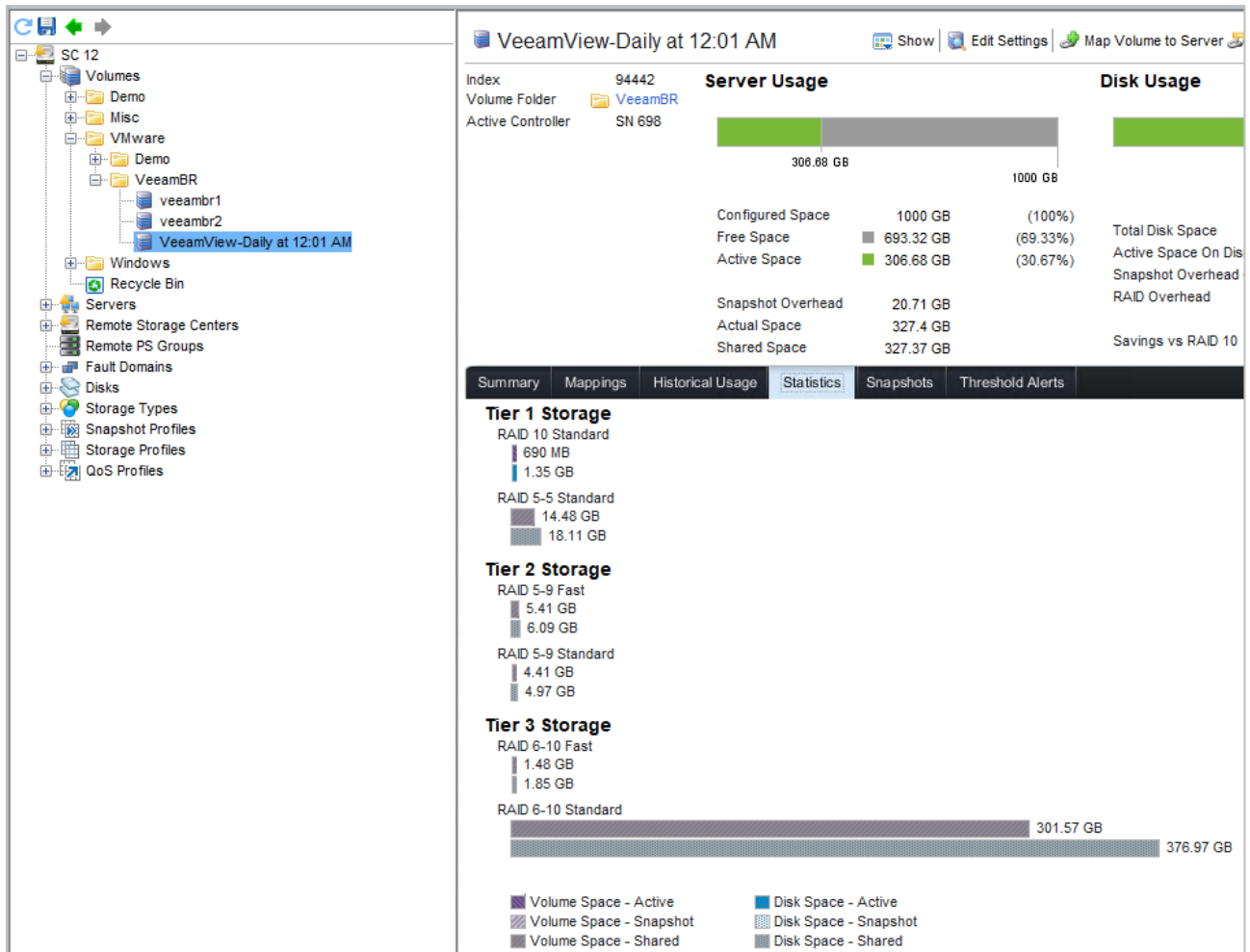
The recovery View volume can be seen in DSM as mapped to the recovery vSphere host.

The **Statistics** tab reveals that the recovery view volume has access to all available tiers and RAID types in the SC Series page pool. The access is defined in the storage profile attached to the volume. This is where view volumes achieve performance and scale beyond vPower NFS. However, restoring from a very old snapshot likely means that frozen storage pages have data progressed down to tier 3 spinning media. While write I/O is almost always ingested into tier 1 RAID 10, read I/O from tier 3 is not as fast as if it was in tier 1 or tier 2. This performance degradation is only temporary, and the next step in the recovery process is to migrate the VM back to its original datastore. This is where all pages would be ingested back into tier 1. This migration can be carried out with a Storage vMotion, or by Veeam through the **Migrate to Production** feature. This feature which will be presented after Instant VM Recovery powers on the VM.

The recovered virtual machine can be seen in the vSphere client. Note its associated datastore **snap-xxx**. This is the transient SC Series view volume discussed above.
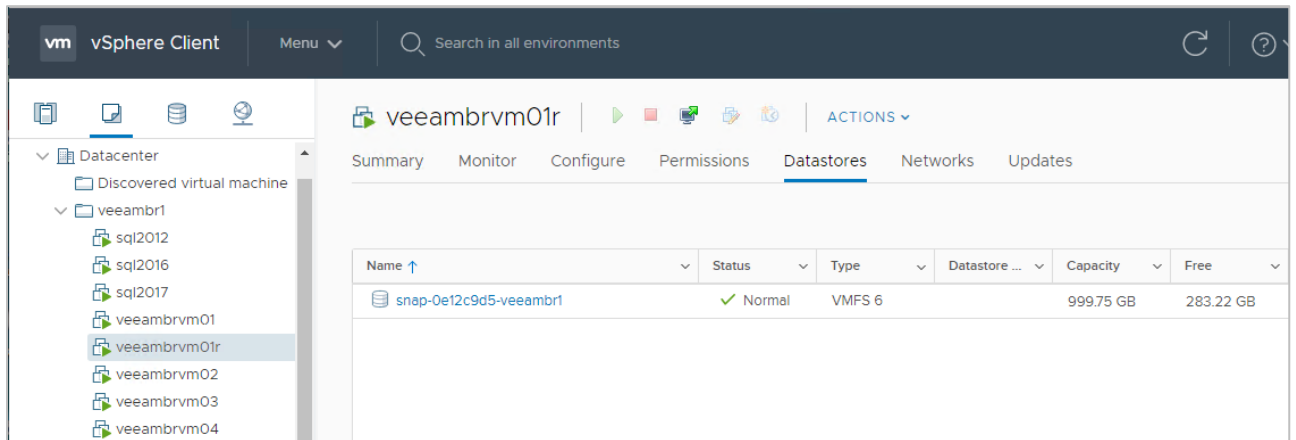
After the VM data has been recovered, use the **Stop Publishing** feature to clean up. If the recovery VM is still registered on the view volume, it will be powered off and unregistered. The view volume will then be unmounted and deleted.

6   Miscellaneous operations

Outside of daily backup and restore operations, there are a few storage-snapshot-related processes that are discussed in this section. It is unlikely these will be used frequently but discussing them helps correlate the task's interaction with SC Series storage.

6.1   Storage discovery and rescan

The Storage Discovery and Rescan processes keep Veeam up to date with the following information:

- SC Series volumes that Veeam can manage
- SC Series snapshots on those volumes
- Virtual machines frozen in each snapshot

With this information, Veeam knows what virtual machines can be recovered from a point in time. The Veeam Storage Monitor process runs in the background and automatically rescans storage at 10-minute intervals. A manual rescan can also be run against an entire SC Series array or a single volume.

From the **Storage Infrastructure** menu, right-click an SC Series array or a volume and click **Rescan storage**.
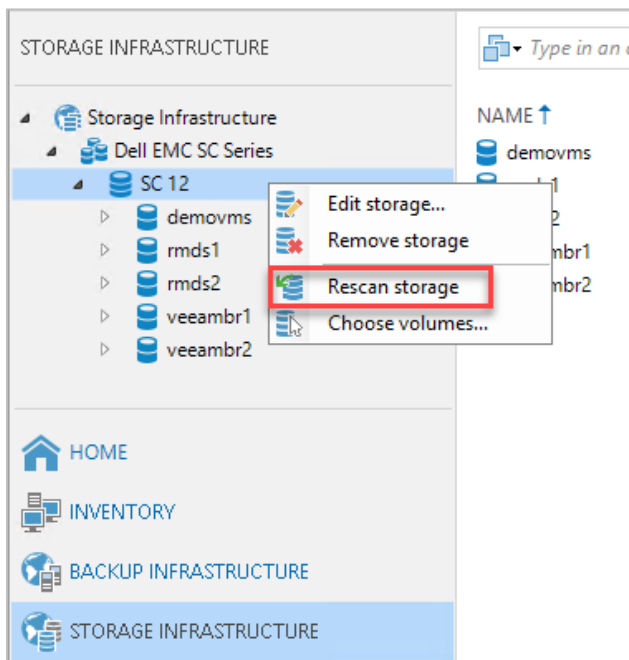
As mentioned above, the rescan process evaluates every snapshot on a volume. The amount of time it takes to rescan a volume is fairly linear with the number of snapshots on a volume. In the example below, note the time required to scan the volume on the left with 9 snapshots and the volume on the right with 73 snapshots.

There are a variety of reasons to manage and limit the number of snapshots a volume has, and Veeam Backup & Replication is an addition reason. As an alternative, the earlier section on volume filtering provides a method to eliminate volumes completely from the rescan process. Veeam documentation refers to this process as limiting the rescan scope. One example takes another look at the two volumes above. If the right-hand volume is not used by Veeam Backup & Replication, 12-minute rescans performed every 10 minutes can be eliminated by filtering out that volume.

Note: In environments where both iSCSI and Fibre Channel storage fabrics are available, iSCSI will be preferred for the scan process as it is faster.

For large environments, two Windows registry entries on the Veeam backup server can be used to tune the automatic rescan interval frequency.

Path: HKEY_LOCAL_MACHINE\SOFTWARE\Veeam\Veeam Backup and Replication
Key: SanMonitorTimeout
Type: REG_DWORD
Default value: 600 (seconds)
Description: Defines incremental rescan interval in seconds

Path: HKEY_LOCAL_MACHINE\SOFTWARE\Veeam\Veeam Backup and Replication
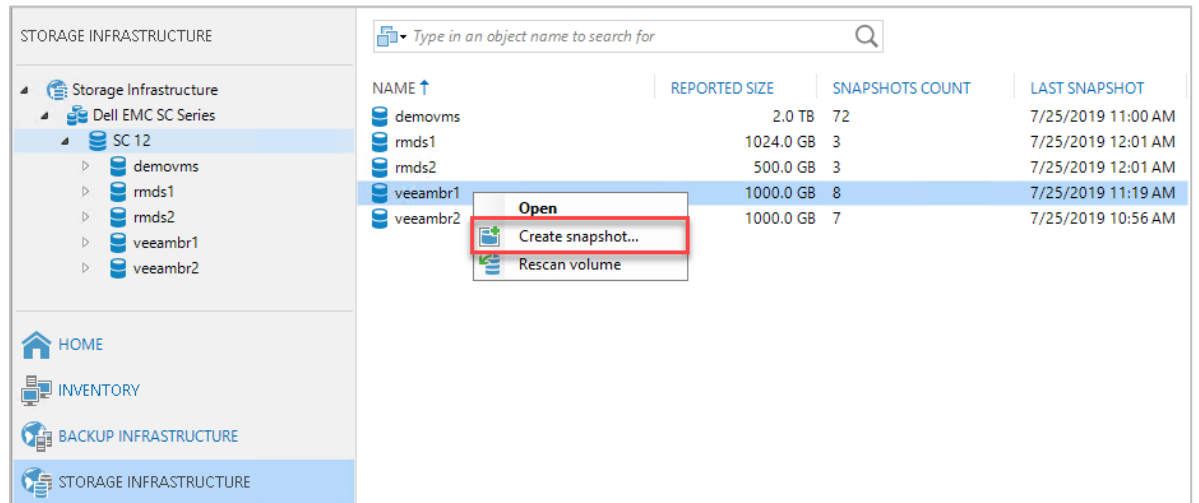Key: SanRescan_Periodically_Days
Type: REG_DWORD
Default value: 7 (days)
Description: Defines periodic full rescan interval in days

6.2   Creating manual snapshots

An SC Series storage snapshot with unlimited expiration can be created manually from the **Storage Infrastructure** menu within Veeam.

1. Right-click a volume and choose **Create snapshot.**

2. Provide the **Snapshot name**. This name will be visible in the snapshot description field of the volume attributes and would be seen in DSM, for example. The Snapshot description field within Veeam is not used with SC Series storage.
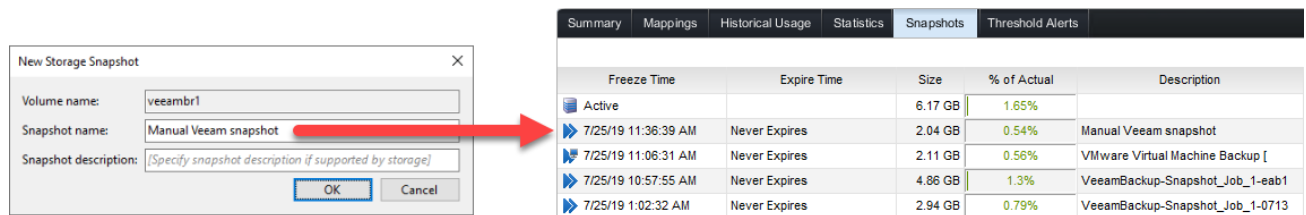
After the snapshot is created, Veeam Backup & Replication will rescan the volume and discover virtual machines that can be recovered from the snapshot.

Note: Veeam Backup & Replication creates snapshots on SC Series storage with no expiration. Remember to expire the snapshot when it is no longer needed.

6.3   Deleting manual snapshots

Any SC Series storage snapshot, even those snapshots that were not created within Veeam, can be manually deleted from the **Storage Infrastructure** menu within Veeam.

Right-click a volume and choose **Delete snapshot.** This marks the snapshot for expiration.

6.4   Orphaned snapshots

As mentioned throughout this document, Veeam Backup & Replication creates SC Series snapshots with no expiration. There are opportunities for snapshots to be created with no follow-up mechanism to expire them. These are referred to as orphaned snapshots. There are a few examples of how snapshots can become orphaned:

- A Veeam backup job is deleted, leaving behind all associated snapshots still within the job's retention policy.
- A manual storage snapshot is created within Veeam and no follow-up step is performed to expire the snapshot when it is no longer needed.

The effective raw storage capacity lost due to an orphaned snapshot depends on the amount of data frozen in the snapshot. Also, a deleted backup job likely orphans many snapshots (14 by default) for each volume it provided data protection for, with each snapshot tying up raw storage.

The best practice is to eliminate orphaned snapshots, which could involve several approaches. Most of these involve documenting operational policies and then following the policy with discipline. The following include simple examples using the scenarios above.

- When a Veeam backup job is deleted, expire its associated snapshots since they fall outside of the job's retention policy. They could take days, weeks, or even months to complete, depending on the backup job interval.
- Implement a weekly PowerShell script that enumerates SC Series volumes and returns volumes with snapshots that have no expiration. Question all results.

7 Conclusion

Veeam Backup & Replication is a powerful data protection and recovery tool for VMware virtual data centers. The Dell EMC SC Series storage integration plug-in adds value to the solution by providing array-based snapshot support at scale.

DELLEMC

A Technical support and resources

Dell.com/support is focused on meeting customer needs with proven services and support.

Storage technical documents and videos provide expertise that helps to ensure customer success on Dell EMC storage platforms.

DELLEMC