Configuration Guide and Best Practices for NetApp and Veeam Backup & Replication 9.5

Stefan Renner
Alliance Systems Engineer

Shawn Lieu
Veeam Solutions Architect, vExpert

1 + 1 = 3
NetApp + Veeam
Better Together

Contents

Introduction

We will cover proper configuration and best practices for leveraging NetApp ONTAP and Veeam® Backup & Replication™ in this whitepaper. Advanced settings and options are available within the GUI and through registry changes. Customizing the deployment of Veeam to suit your environment will result in better performance and lower overhead.

Information on system requirements and limitations

Before you start your implementation, please check the system requirements and limitations when using Veeam in combination with NetApp ONTAP.

To get the latest updates, please follow the links below:

Veeam Backup & Replication v9 requirements and limitations for ONTAP:
https://helpcenter.veeam.com/backup/vsphere/storage_limitations_netapp.html

Veeam Backup & Replication v9 supported ONTAP versions:
https://helpcenter.veeam.com/backup/vsphere/system_requirements.html#storage

Veeam Backup & Replication 9.5 requirements and limitations for ONTAP:
https://helpcenter.veeam.com/docs/backup/vsphere/storage_limitations_netapp.html?ver=95

Veeam Backup & Replication 9.5 supported ONTAP versions:
https://helpcenter.veeam.com/docs/backup/vsphere/system_requirements.html?ver=95#storage

Furthermore, we recommend reviewing the storage integration section at our Help Center page:
https://helpcenter.veeam.com/docs/backup/vsphere/storage_integration.html?ver=95

Preparing the NetApp Storage System

To ensure successful backup, replication and restore from storage snapshots, the administrator must set up the NetApp storage system and backup infrastructure resources to properly interface with the Veeam Backup & Replication console.

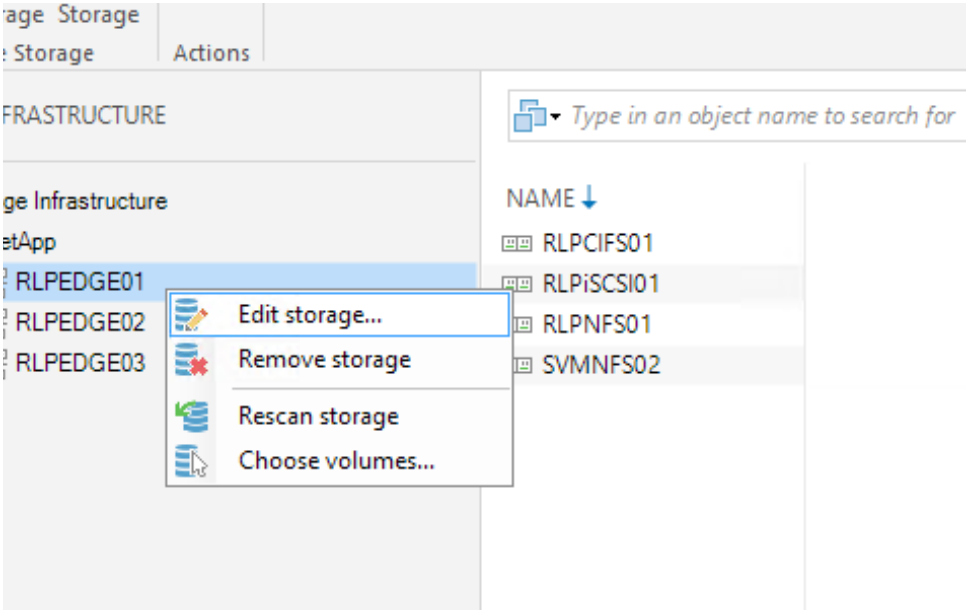
Backup Proxy

For storage rescan and Backup from Storage Snapshots, Veeam Backup & Replication requires that the backup proxy be set up in a specific way:

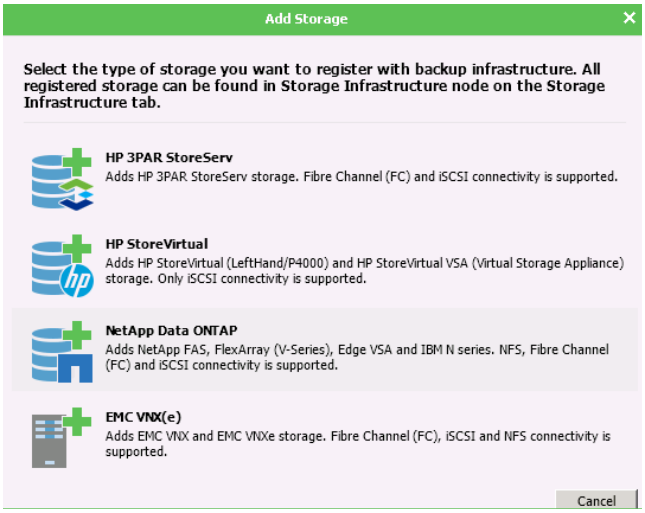
- For a NetApp storage system running ONTAP via NFS and iSCSI protocols, no preparatory actions are required. Veeam Backup & Replication will set up all necessary rules automatically
- For a NetApp system running ONTAP over Fiber Channel, the administrator must manually create an initiator group that will contain a WWN ID of the backup proxy over which backup and replication will be performed. All Fiber Channel devices must be properly installed and the WWN IDs must be properly zoned on the Fiber Channel switch. We recommend creating a separate igroup, and avoid adding the proxy WWPN to the ESXi igroups
- For a secondary NetApp ONTAP system running SnapMirror/SnapVault it is necessary to set up access for the Veeam proxy server as well.

Adding NetApp Storage and preparing for the storage rescan process

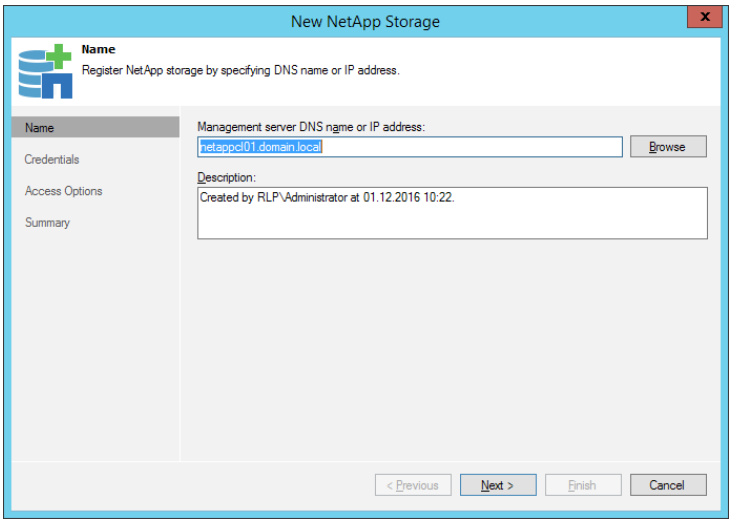
The NetApp storage system must be added to Veeam Backup & Replication, in the **Storage Infrastructure** view.



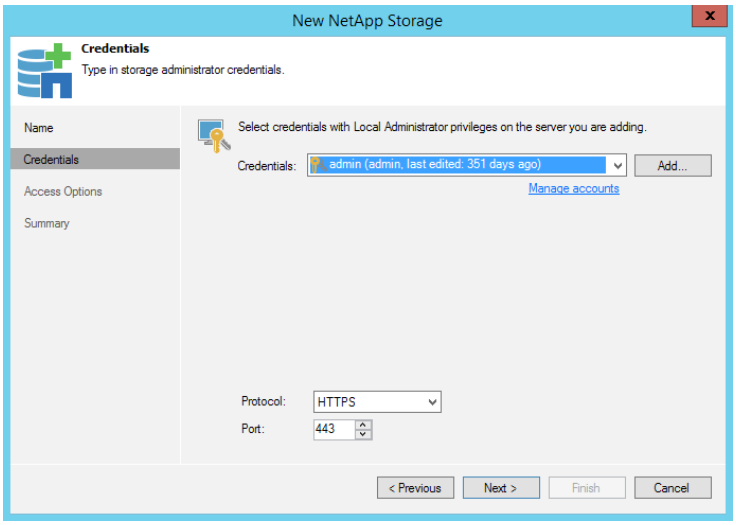
You can add the storage system by clicking **Add Storage** and by selecting **NetApp ONTAP** from the options menu. This will launch the associated wizard.



On the first step of the wizard, you can add the management IP or DNS name of either the cluster or the controller. Click **Next** to proceed.

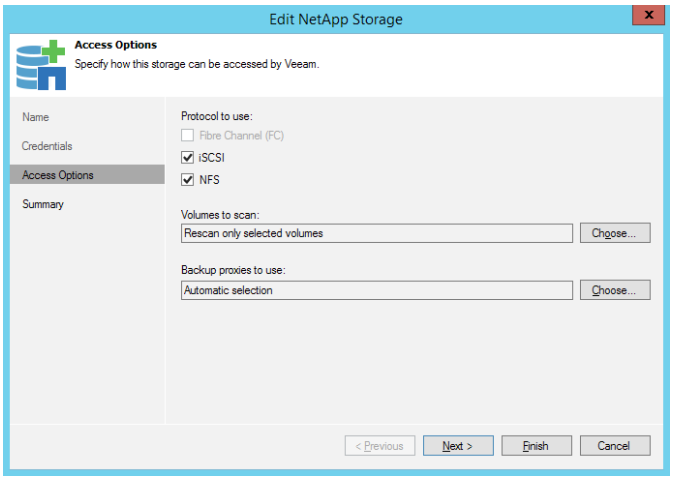


The second step of the wizard is where the necessary credentials must be selected. If credentials are not present, click the **Add** button to add them. You may also change the protocol and port assignments from this screen. Click **Next** to proceed.



After the credentials are verified, you will be presented with **Access Options**. You can define different access settings like the protocol selection, proxy affinity and volumes to scan here. You may find additional details on the list of potential settings on page 24, **NetApp Advanced Option Settings**.

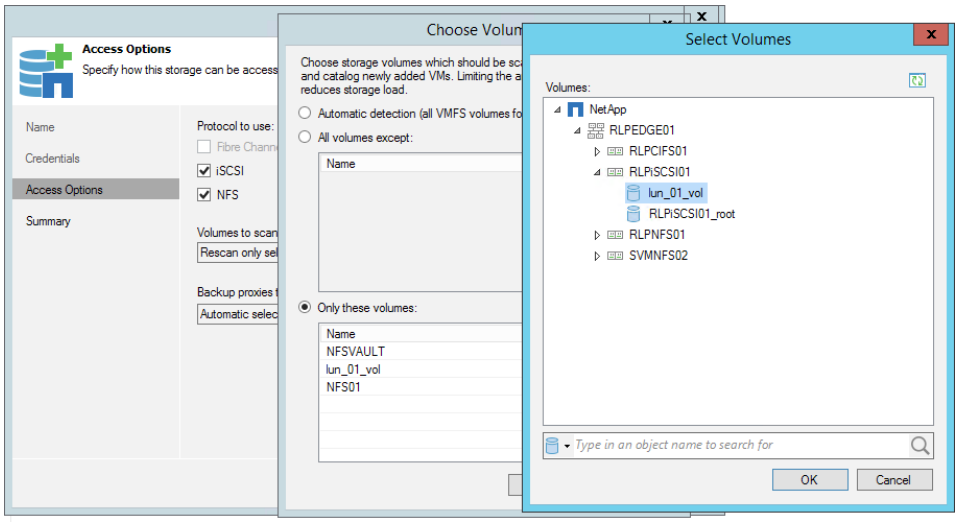
When adding a new cluster, it is **highly recommended** to select all the volumes wish to include by clicking **Volumes to scan from the Veeam console**. Veeam will scan all volumes found on the NetApp controller or cluster by default. To minimize the required overhead and performance on the NetApp controller, you can select only the relevant volumes.



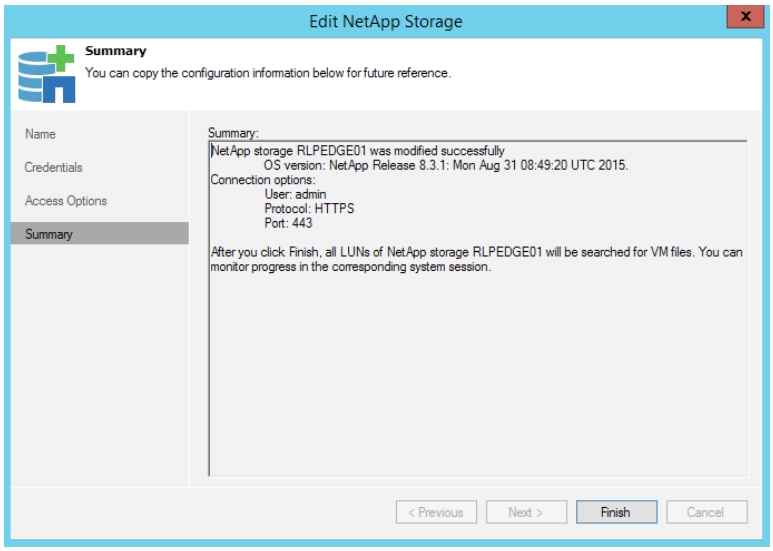
If your controller is already added, you can choose the volumes afterwards in the advanced settings of your NetApp controller in our GUI.

You can choose between the following options in the volumes selection:

- Automatic detection (all VMFS volumes found with initial scan)
- All volumes except
- Only these volumes



Depending on your environment, you can choose the correct option and define the volumes that should be scanned.



On the final step of the wizard, you may verify the connection settings.

After the storage system is added, Veeam Backup & Replication performs its initial scan. Make sure that the following requirements are met to ensure successful storage system scan:

- An administrator account on NetApp is required to add a NetApp storage system
- Network access from the Veeam backup server to the Management interfaces is required
- Licenses for cloning (+SnapVault / SnapMirror) are required. To learn more about licenses and NetApp features that are used in different environments, see Backup and Restore from Storage Snapshots
- SnapVault / SnapMirror relationships must be properly set up
- Fiber Channel: By default, Veeam can rescan storage snapshots by iSCSI. If you want to use Fiber Channel instead, you need to create an initiator group with the backup proxy WWNs on the NetApp storage system. To prioritize FC, you need to set the registry key, "UseiSCSIFirstForSanRescan = 0". For more information, please see page 23, **Advanced options in the registry**
- NFS: An Export/namespace (for primary and secondary) and SnapVault / SnapMirror secondary side must be properly set up (see **NetApp Namespace settings for ONTAP secondary systems**)
- Client permissions, export policies and initiators are updated and created automatically by Veeam Backup & Replication
- SAN / network must be properly configured so that the backup proxy can access the NetApp storage system

Veeam snapshot scanning

Veeam's NetApp integration provides the ability to restore files, items and objects out of NetApp storage snapshots. During a backup job, Veeam refers to vCenter to determine the vm-datastore-volume relation and to identify the VMs associated with a specific NetApp volumes. Veeam then provides you with the option to restore either from a Veeam created or a third-party created NetApp storage snapshot. To determine the snapshot relationship across all VMs, Veeam performs a full scan of the specified NetApp volumes on a regular basis. The scanning process makes sure that our GUI displays the correct VMs so that you may perform restores from all available NetApp storage snapshots.

By default, the Veeam server scans the NetApp controller every 10 minutes to determine if any new snapshots were created on the storage volumes. If there are new snapshots or volumes, the Veeam server will mount (in case of FC/iSCSI/FCoE) the LUN or will use NFS to examine the datastore to determine the VMs associated with the newly created snapshots and volumes.

Once you add a NetApp storage system to Veeam Backup & Replication, Veeam performs the following operations:

1. **Performs initial system scan.** Veeam gets specific storage information about cluster members, IP addresses, vFiles, SCVs and IP addresses for iSCSI/NFS and WWN. It also gets a list of volumes and snapshots, LUNs and NFS, and creates a list of all snapshots for each volume, and a list of all LUNs and NFS exports.

2. **Checks if storage volumes are accessible by backup proxies.** Veeam checks what license is available for each protocol. It gets a status of the FC and iSCSI server on the NetApp storage system, gets a list of all initiators for all backup proxies and tests connections to the iSCSI or NFS server from these backup proxies. Veeam also obtains a list of preconfigured Fiber Channel backup proxies on the server.

3. **Looks up for VMware vSphere datastores.** Veeam searches for NetApp exports in all VMware servers added to Veeam Backup & Replication. All VMs found on VMware datastores are "propagated" to storage snapshots. This helps Veeam make up a rough list of VMs on storage snapshots. Veeam presumes that all VMs whose disks are hosted on datastores are also available on corresponding storage snapshots*.

4. **Rescans VMs on datastores.** Veeam verifies the VM list created at the previous step. It exports storage snapshots to backup proxies and rescans the list of VMs. Rescan over NFS or iSCSI is performed remotely. A rescan over Fiber Channel requires LUNs to mount (LUNs are mounted in groups of 10)**.

5. **Deletes orphaned storage snapshots.** Veeam obtains a list of snapshots for each volume, obtains a list of snapshots created by Veeam from the configuration database and builds the snapshot chain. Snapshots without locks are removed from the hierarchy (note that this is applicable to snapshots created with traditional LUN cloning only).

** If a VM is deployed after the snapshot is created, this VM will be displayed as present on the snapshot at this point in time. However, actual data restore will not work.*

*** VMs deployed after the snapshot is created are removed from the list at this step of the rescan operation.*

The following table shows three different scanning workflows:

Adding a new NetApp controller	Creating a new snapshot	Automatic scanning*
1. Collect specific storage information	1. Creating a new snapshot	1. The storage monitor runs in the background
2. List of volumes, snapshots, LUNs and NFS exports	2. List of initiators	2. Detecting new snapshots and volumes
3. Checking licenses, FC and iSCSI server	3. Testing iSCSI, NFS and FC from proxies	3. Scanning every 10 minutes
4. List of initiators	4. Searching NetApp exports in VMware	4. List of initiators
5. Searching NetApp exports in VMware	5. Adding founded VMs from datastore to snapshots	5. Testing iSCSI, NFS and FC from proxies
6. Adding founded VMs from datastore to snapshots	6. Export and scan the Snapshots with proxies	6. Searching NetApp exports in VMware
7. Export and scan the snapshots with proxies	7. Update the Veeam view	7. Adding founded VMs from datastore to snapshots
8. Update the Veeam view		8. Export and scan the founded objects with proxies
		9. Update the Veeam view

**Full system scan is performed every seven days per default*

The performance of a scan of the NetApp controller depends on the protocol used, as well as the completion time of several tasks that are executed on the ONTAP operating system. Therefore, it is recommended to have some performance headroom on the controller. Keep in mind that if your controller is already running on > 90% CPU utilization, the scan will take some time.

The scanning interval of 10 minutes and seven days can be changed with a registry key.

To change the interval please open your registry and browse to "HKEY_LOCAL_MACHINE\SOFTWARE\Veeam\Veeam Backup and Replication\".

You can create the following keys to change the scan behaviors there.

Attention: Keep in mind that every change in your registry should only be performed when it is required. Don't change any other values as this could make your installation or system unusable.

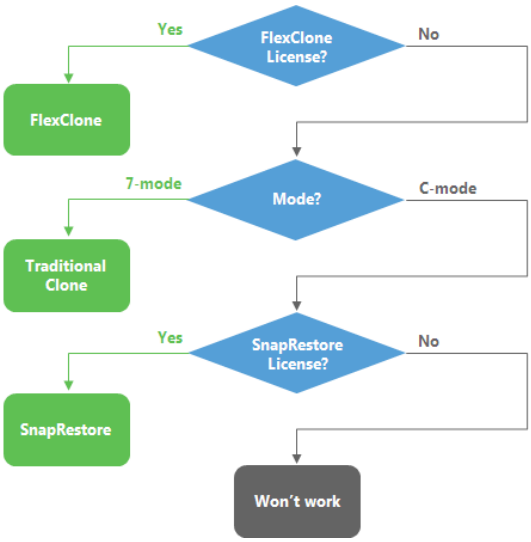
Key	SanMonitorTimeout	SanRescan_Periodically_Days
Type	REG_DWORD	REG_DWORD
Default	600 (seconds)	7 (days)
Description	Defines how frequent we should monitor SAN infrastructure and run incremental rescan in case of new instances.	Defines how frequent we should initiate periodic full rescan after the Veeam Backup service rescans.

Backup and restore workflow for Storage Snapshots

Backup and restore procedures from storage snapshots depend on the type of protocol of the NetApp storage system; Fiber Channel, iSCSI or NFS. They also depend on the license installed on the NetApp storage system and available NetApp features.

Backup: Fiber Channel and iSCSI

To perform backup and replication from storage snapshots, Veeam Backup & Replication verifies what type of license is installed on the NetApp storage system and what features are available.



The table below describes all operations that are performed during VM backup or replication in environments where traditional LUN cloning, SnapRestore or FlexClone features are available.

Feature available/Operation	Traditional Clone	SnapRestore Clone	FlexClone Clone
Perform VSS operations	✓	✓	✓
Create a VMware VM snapshot	✓	✓	✓
Obtain block matrix	✓	✓	✓
Create a NetApp volume snapshot	✓	✓	✓
Create a thin clone of the LUN	✓	✓	✓
Remove VMware VM snapshot	✓	✓	✓
Mount the clone to the backup proxy	✓	✓	✓
Back up VM	✓	✓	✓
Unmount the clone from the backup proxy	✓	✓	✓
Delete the clone of the LUN	✓	✓	
Delete NetApp Volume Snapshot	✓	✓	

Backup: NFS Protocol

Backup and replication from storage snapshots over NFS is architecturally much easier to implement than similar processes configured on NetApp storage systems utilizing Fiber Channel or iSCSI.

1. Veeam instructs NetApp to create a snapshot of the volume on which the VM disks are located
2. NetApp provides read-only access to this snapshot for the backup proxy
3. Veeam reads data directly from the snapshot by sending NFS requests by its own NFS agent

Important! If a VM has existing VMware snapshots, this VM will be skipped from processing. To learn more, see Veeam documentation at http://www.veeam.com/documentation-guides-datasheets.html.

Restore: Fiber Channel and iSCSI

VM data restore from storage snapshots over Fiber Channel, Fiber Channel over Ethernet (FCoE) and iSCSI protocol is performed in the following manner:

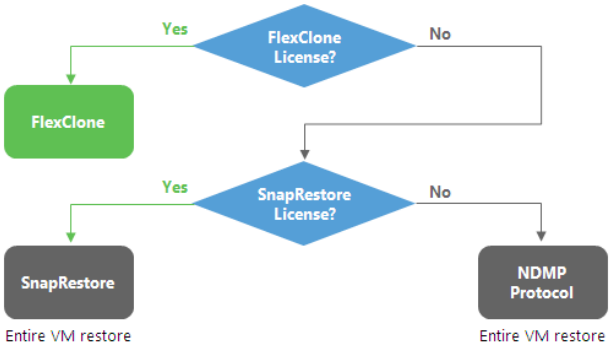
1. Veeam creates a thin clone of the LUN in the snapshot and maps the thin clone to the ESXi host. For snapshot mounting, the backup administrator can select any ESXi host in the backup infrastructure
2. Veeam initiates rescan on the storage adapter on the ESXi host
3. The discovered clone will be re-signatured by the ESXi host
4. A new datastore named "snap-<xxxxxxxx-datastore name>" appears on the ESXi host

A VM (in case of Instant VM recovery) or a proxy appliance to which VM disks are mounted (in case of filelevel restore or application items restore) is registered from this datastore on the ESXi host.

Restore: NFS Protocol, 7-Mode

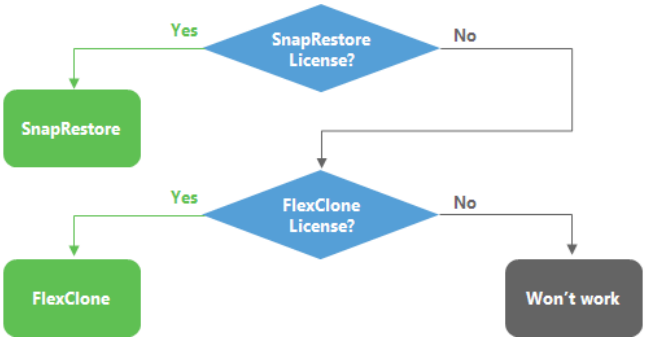
To restore data from storage snapshots, Veeam Backup & Replication verifies what type of license is installed on the NetApp storage system and what features are available.

FlexClone is the only license that enables real, instant data restore for 7-mode (Instant VM Recovery®, file-level and application items restore). If you use SnapRestore or NDMP protocol, Veeam will first restore all data from the storage snapshot, and then start VMs, files or application objects restore jobs.



Restore: NFS Protocol, (ONTAP)

To restore data from storage snapshots, Veeam Backup & Replication verifies what type of license is installed on the NetApp storage system and which features are available.



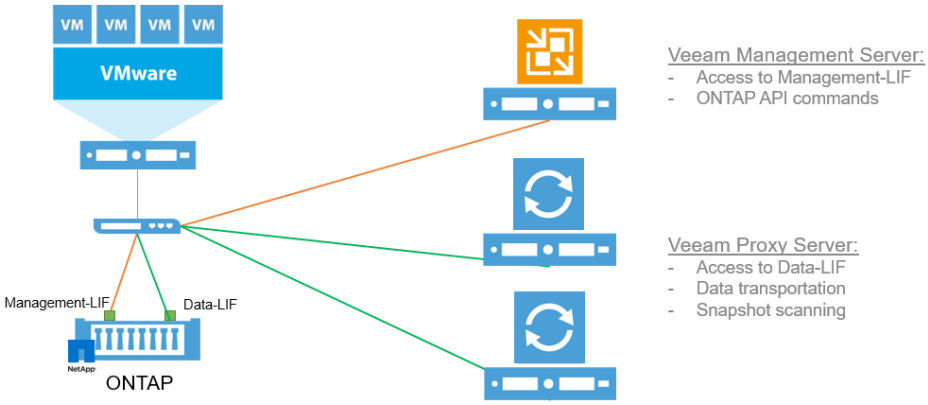
The table below describes all operations that are performed during data restore from storage snapshots in environments where traditional NDMP protocol, SnapRestore or FlexClone features are available.

NDMP protocol	SnapRestore clone	FlexClone clone
Create a Veeam_<vm name>_Restore folder on the volume	Create a Veeam_<vm name>_Restore folder on the volume	Create a thin clone of the volume
Copy data from the snapshot to this folder over NDMP protocol	Copy files from the snapshot to Veeam_ folder using SnapRestore	
Expose /volume/<Veeam_<vm name>_ Restore> to the ESXi host	Expose /volume/<Veeam_<vm name>_ Restore> to the ESXi host	Expose the clone of the volume to the ESXi host
Start a VM (for Instant VM Recovery) or proxy appliance (for file-level or application items restore) on the ESXi host	Start a VM (for Instant VM Recovery) or proxy appliance (for file-level or application items restore) on the ESXi host	Start a VM (for Instant VM Recovery) or proxy appliance (for file-level or application items restore) on the ESXi host
Let the user restore files / migrate the VM	Let the user restore files / migrate the VM	Let the user restore files / migrate the VM
	Dismount /volume/<Veeam_<vm name>_ Restore> from the ESXi host	Dismount the clone of the volume to the ESXi host
	Delete the clones and the folder	Delete the clone of the volume

The ONTAP FlexClone License is highly recommended for any restore and sandbox operation.

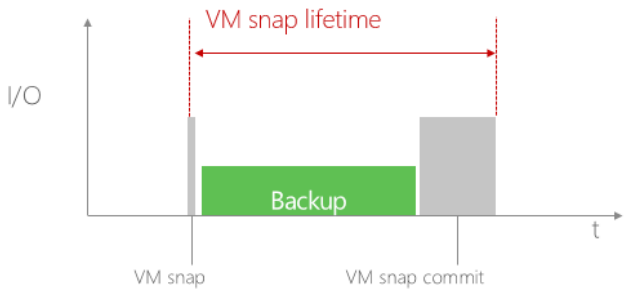
Storage access rules

Veeam is an Enterprise Availability solution that scales by adding multiple proxy servers to initiate data transfer directly out of ONTAP Storage Snapshots. Besides the Proxy role, there is also a Management Role that holds all relevant management information, like scheduler, jobs, etc. Each of these functions require different methods for integrating with ONTAP. While the Management server only needs to access the ONTAP API, the Proxy server needs accessing to the Storage Snapshot data via the data LIFs. The following diagram illustrates the required access path for each Veeam function.



Design and proxy best practices for Backup from Storage Snapshots

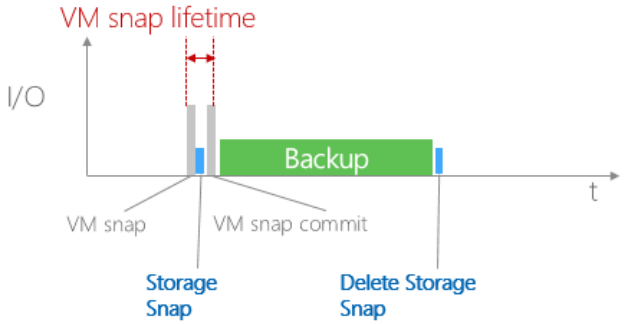
We're getting questions about design best practices for Backup from Storage Snapshots on a regular basis. Backup from Storage Snapshots (BfSS) is a technology which minimizes the amount of overhead placed on your VMware environment during a backup job. If you run a backup without BfSS, the workflow is the following:



- Create VMware snapshot
- Back up the data
- Delete VMware snapshot

During the entire backup process, the VMware snapshot remains open. This results in the consumption of CPU and storage IO resources which could impact VM application performance. This is especially true when the VM snap commits are taking place; administrators will typically see a spike in overhead on the host.

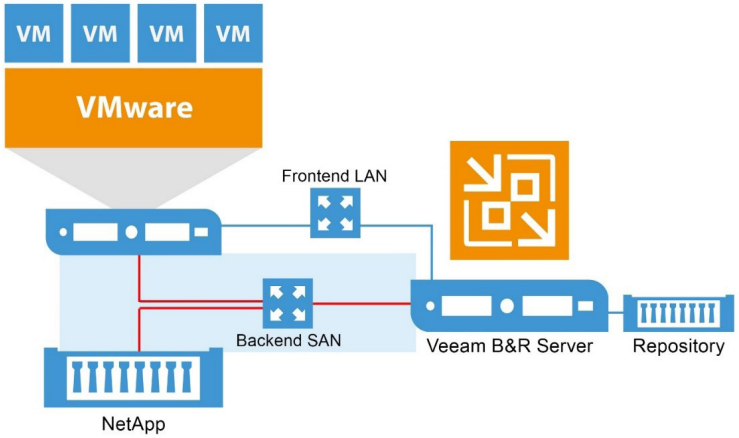
If BfSS is used, however, the process for performing a backup is much more efficient:



- Create VMware snapshots
- Create storage snapshot
- Delete VMware snapshot
- Back up the data
- Delete storage snapshot

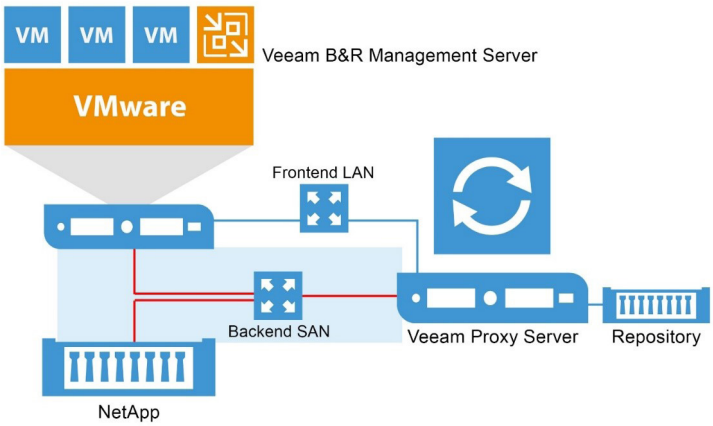
Through this workflow, the VMware snapshot only remains open for a couple of seconds or minutes, compared to the hours it can take when performing backups the standard way. As soon as the VMware snapshot is committed, there is no more load on the VMware environment as we backup directly from the storage snapshot. All of Veeam's additional benefits, like deduplication and compression, parallel processing or CBT are still used when using BfSS. Using BfSS accelerates backups jobs since Veeam backs up directly from storage snapshots.

To leverage BfSS, you need to configure a Veeam proxy server with access to the VMware storage infrastructure. This Veeam proxy can either be the Veeam management server itself or a server with a proxy role managed by a centralized Veeam Backup & Replication server. To use BfSS in the most efficient way, we recommend configuring the proxy server on a physical server with direct access to the storage backend. A design where a single Veeam Backup & Replication server manages all the required backup roles could look like the following:



Make sure that you separate storage and network traffic at the Veeam proxy server. It is not recommended to share the same network interface for both SAN and LAN traffic. Even in an environment where NFS or iSCSI is used, don't share the same Ethernet link for backup and network data as this could result in additional latency on the storage network.

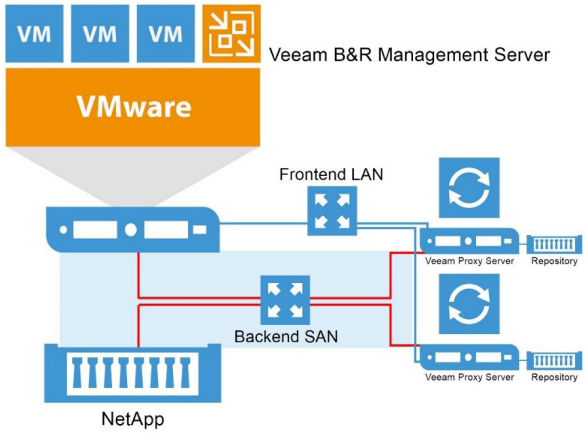
Another design option is to separate the Veeam management server from the Veeam proxy server. In this case, the Veeam management server can be configured as a VM, while the Veeam proxy server, or data mover, is deployed on a physical server:



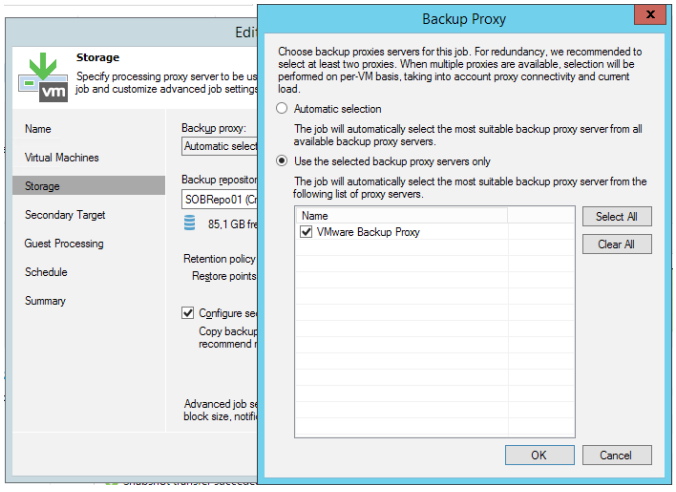
Again, do not share the same interface on the physical server for SAN and LAN traffic.

In this design you can dedicate the physical proxy server for processing backup data by defining the proxy server in the job settings. The settings can be found below.

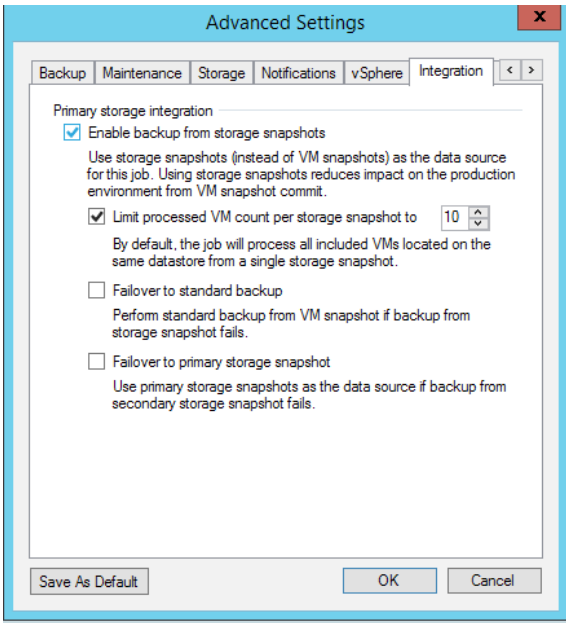
Larger environments can scale by using multiple physical proxy servers coupled with a single, centralized Veeam management server:



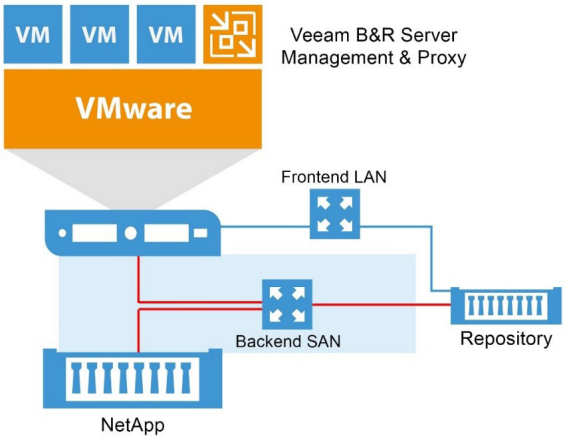
When scaling, you can run multiple jobs simultaneously. To maximize performance, you can define the specific proxy server for each backup job to use by configuring the proxy host directly within the job settings. Go into the job settings and select the proxy within the storage tab.



The job will then use the designated proxy during the next backup event. Make sure that in the advanced options of the job our storage integration is activated.



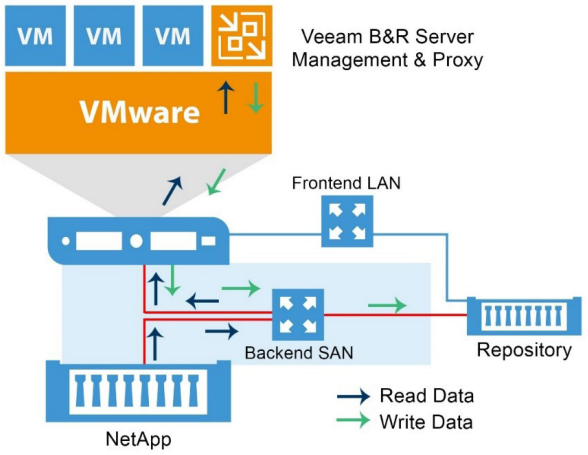
From time to time, users ask if it is possible to use a virtual proxy to perform backups from storage snapshots. We don't recommend this design if your storage backend is based on FC, as it doesn't make sense to map a physical FC interface into your VM. While implementing a virtual BfSS proxy server is supported by Veeam, we recommend you carefully think through all the design implications before doing so. A design utilizing NFS and iSCSI could look like the following:



Let's imagine the following environment:

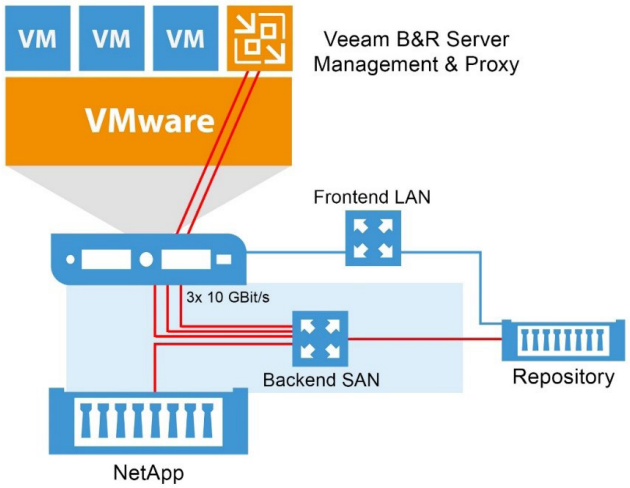
- iSCSI or NFS is the storage protocol
- 10 Gbit/s storage backend network
- The repository is a iSCSI LUN mapped directly into the proxy VM
- The proxy is a virtual machine

In this case, it is very important to understand the data flow before designing, procuring and configuring your server. The data flow would look like the following:



In this design, your data will need to be processed two times through the hypervisor in order for it to be backed up to the storage repository. The data will go from primary storage, through the storage network and the hypervisor into the Veeam Backup & Replication server (read data), and then back from the VM through the hypervisor and the storage network to the repository (write).

As you can see, this is not very efficient. And, from a design perspective, it isn't better than utilizing a physical host. Moreover, in this example, you would need to use at least 3x 10Gbit/s interfaces:



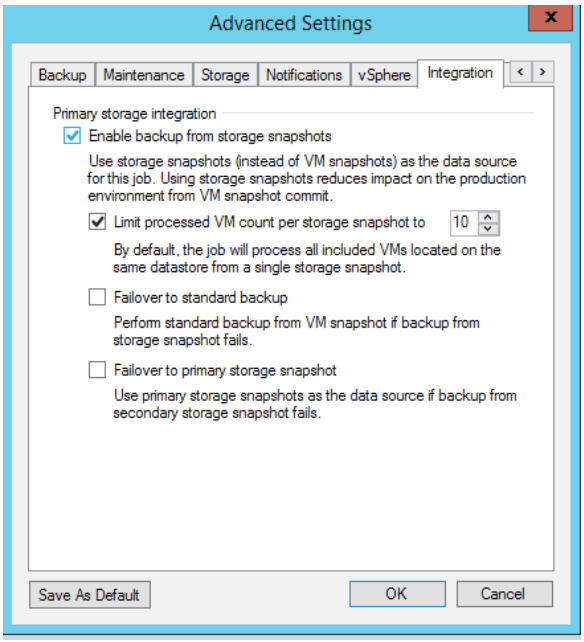
Needed network interfaces on ESXi:

- 1x VMware ESXi to NetApp storage for regular VMware traffic
- 1x Veeam Backup & Replication VM to NetApp storage for reading the BfSS data
- 1x Veeam Backup & Replication VM to Repository for writing the data as well as several more interfaces for LAN connections and multipath capabilities

Again, do not share the same interfaces for read and write data as sharing the interface may result in throttling down the bandwidth by as much as 50%. BfSS is leveraged to maximize backup performance and optimize the way backup data is processed. It is also used to separate backup tasks from the production environment to eliminate overhead on the hypervisor. By using a virtual proxy server, you will not attain the full performance and efficiency benefits of BfSS.

Advanced options for NetApp storage integration

With of Veeam Backup & Replication 9.5, different advanced options for Backup from Storage Snapshots are available:



Enable backup from storage snapshots:

Enable this option to use the feature within the job. The feature is enabled by default.

Limit processed VM count per storage snapshot to:

Enable this option if you have to back up a large amount of VMs within the same datastore. This option allows you to define how many VMs are processed at once. If for example, you have a job with 1,000 VMs and you define 50 as the value, our engine will run 20 times (1000/50=20) to backup all the VMs. In this case, Veeam will create a VMware snapshot of the first 20 VMs, then create a storage snapshot. If enabled, it will also trigger a SnapVault/SnapMirror update, and backup the 20 VMs. After the first 20 are finished, the next 20 VMs will be snapshotted in VMware and so on. With that, the time it takes to get consistent VM snapshots, and the amount of time snapshots remain open, can be dramatically reduced. If you process application-consistent snapshots, keep an eye on the processing time. It can take a while for volume snapshot creation. The recommended VM count is about 30-40.

Failover to standard backup:

Select this if you would like to perform a failback to non-snapshot based backup in the event that BfSS is not working. Best practice is to leave it disabled, otherwise you may not realize there is a problem in your environment.

Failover to primary storage snapshot:

Enable this option if you would like to use the primary snapshot in case there are issues with cloning and/or SnapMirror/ SnapVault operations.

Technical recommendations for NetApp ONTAP and Veeam Backup & Replication setup

It is important to not hit the maximum number of snapshots per NetApp volume with multiple jobs — the hard limit is 255, so never plan more than 250. The following recommendations should be considered:

- If you want to use Veeam NetApp snapshot orchestration, VMware datastore level scope is recommended for jobs
- It is recommended to place only one VMware datastore on a NetApp volume
- If only Veeam snapshot orchestration is used, follow the NetApp recommendations for the datastore size and VM count. But, if Veeam backups are created on top of Veeam NetApp snapshot orchestration, we suggest using not more than 8 TB in a single Veeam full backup file. It is technically possible and supported to grow beyond that

If you use iSCSI/FC to perform Backup from Storage Snapshots, we suggest reducing "PDORemovePeriod" at MPIO/NetApp-DSM to 10 seconds at the Veeam Proxy, to reduce background processing time per Snapshot at scan and backup processing time.

The key can be found at: HKLM\SYSTEM\CurrentControlSet\Services\ONTAPdsm\Parameters.

Key	**PDORemovePeriod**
Default	20 (seconds)
New Value	10 (seconds)
Description	This setting controls the amount of time (in seconds) that the multipath pseudo-LUN will continue to remain in system memory, even after losing all paths to the device. When this timer value is exceeded, pending I/O operations will be failed, and the failure is exposed to the application rather than attempting to continue to recover active paths.

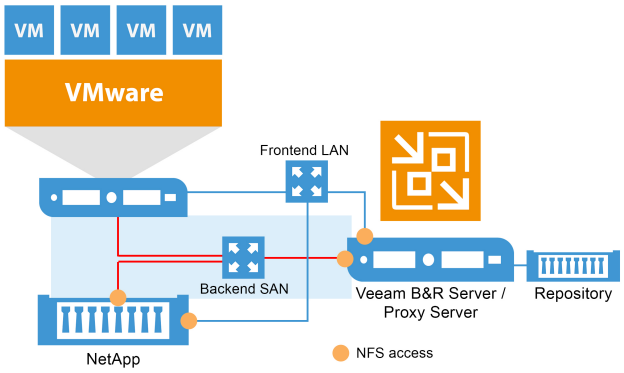
If you use FC for Backup from Storage Snapshots, we recommend to map at least one LUN from each Storage controller to the proxy server after you zoned them in the FC Switches. This helps to avoid longer rescans at OS boot or Snapshot unmapping. It can be sized as a 40MB big thin volume. You do NOT need to enable this volume in disk manager.

Things to consider

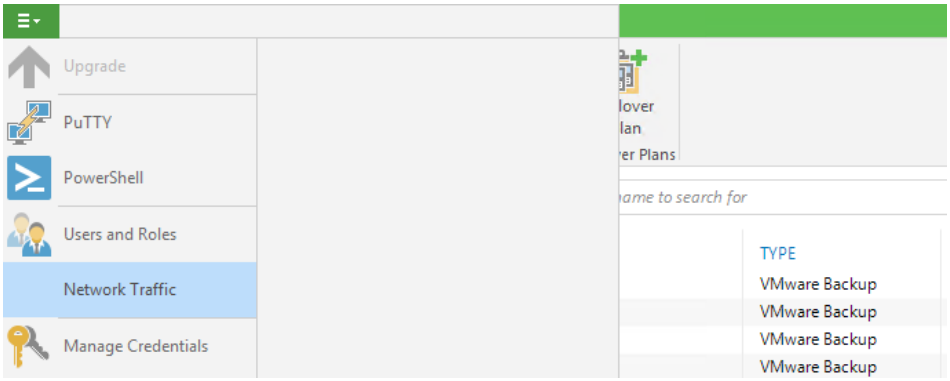
- Only VMs with VMDK disks are supported. You cannot backup your standard NAS shares from the NetApp system with non-VMware data. Veeam Backup & Replication does not perform snapshot orchestration for non-VMware datastore based data.
- To use Veeam Explorer™ for Storage Snapshot, the VMDKs of a VM need to stay on a single volume.
- Infinite volumes are not supported.
- Configurations with VMs stored on a qtree that resides on a non-default vFiler is not supported.
- NDMP tape output is not supported, but you can use Veeam D2D2T backup.
- If you want to use Backup from Storage Snapshots (backup out of NetApp ONTAP) or if you want to use Veeam in-guest processing (consistency) together with VMs on NFS datastores, VMs may not be configured with VMware vSphere snapshots.

Preferred network settings for Backup from Storage Snapshots with NFS

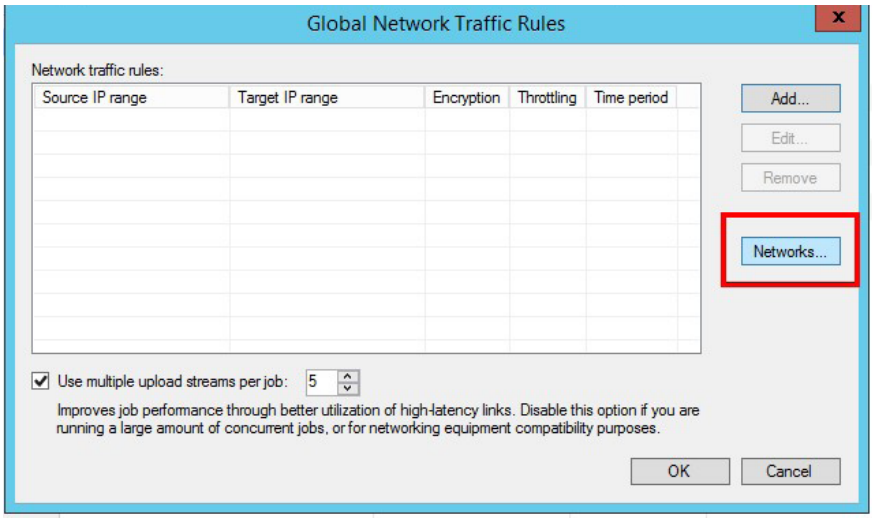
In advanced configurations, there can be multiple ways the Veeam proxy server and the NetApp ONTAP system can access a NFS volume. The following graphic shows a design where two NFS networks are available. One is the storage backend (for VMware) and one is the LAN frontend (for client access).



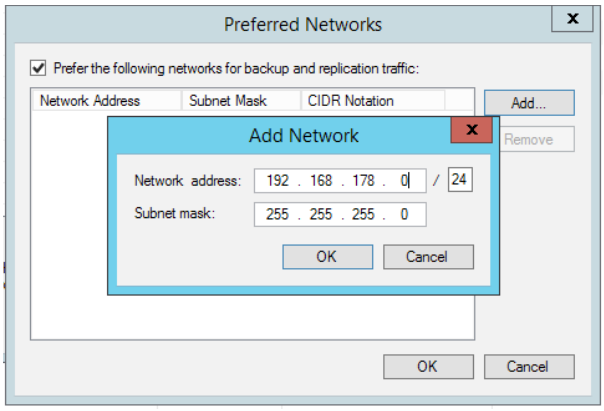
We recommend using the storage backend network for data access. In this configuration, the 1 GBit/s front-end LAN may be used even if there is a 10 GBit/s storage backend. The preferred network settings of the Global Network Traffic Rules dialog can be used to define which network the Veeam proxy should use for data transfer. Therefore, go to **Home — Network Traffic**.



In the dialog go to **Networks**.



Here, you can add the preferred network or even the preferred IP address your NetApp LIFS Veeam should use for NFS or iSCSI data processing. If the network is not available, the engine will failover to the next available network.



A second way to define the preferred IP address in ONTAP is to use the following registry key:

Key	**NetAppOrderedIPList**
Type	String
Value	IP Address of NetApp ONTAP NFS and iSCSI interface
Description	Specify preferred NetApp ONTAP adapters IP addresses for NFS or iSCSI access separated by a semicolon.

Additional advanced options in the registry

With Veeam Backup & Replication, we provide several registry keys to change the behavior when working together with NetApp SAN storage systems.

The keys need to be created in "HKEY_LOCAL_MACHINE\SOFTWARE\Veeam\Veeam Backup and Replication\".

Key	**SanMaxConcurrentCreatingVmSnapshotsPerEsx**
Type	REG_DWORD
Default	10
Description	Defines the amount of snapshots that could be initiated on VMs which belong to the same host. How many VMware snapshots are created at the same time per ESXi host.

Key	**SanMaxConcurrentCreatingVmSnapshotsPerVc**
Type	REG_DWORD
Default	20
Description	Defines the amount of snapshots that could be initiated on VMs which belong to the same vCenter. How many VMware snapshots are created at the same time per vCenter server.

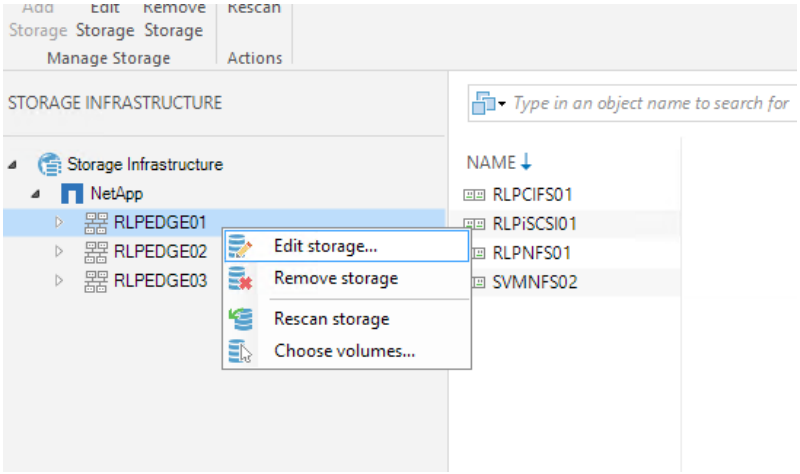
Key	**MaxConcurrentDeletingSnapshotsForCluster**
Type	REG_DWORD
Default	4
Description	Defines the amount of snapshot deletion tasks which can be initiated at once. How many VMware snapshots are deleted at the same time.

Attention: Keep in mind that every change in your registry should only be performed when it is required. Don't change any other values as this could make your installation or system unusable.

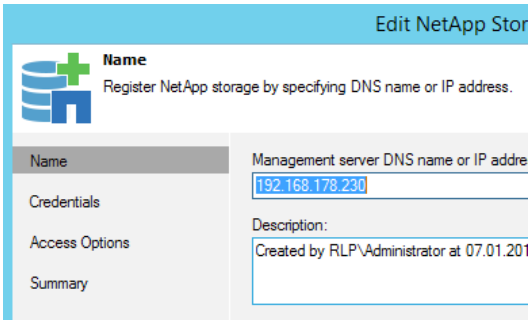
Depending on your environment, it would make sense to change some of the values above. Specifically, the "SanMaxConcurrentCreatingVmSnapshotsPerVc" setting could be modified to control how many VMware snapshots are created at the same time. If you have enough resources available in your data center, this option allows you to finish jobs faster. But, don't forget that changing the values can also cause your VMware environment to run into performance issues, as increasing the number of concurrent snapshots will require more compute and storage resources.

NetApp advanced access options

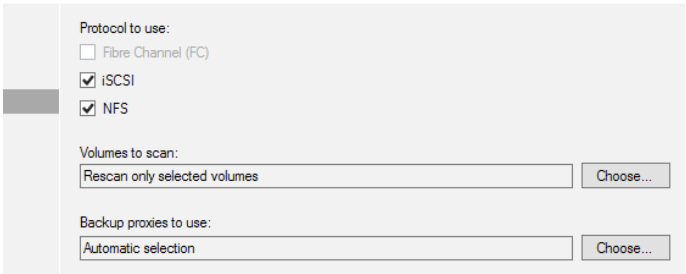
With Veeam Backup & Replication 9.5, the advanced options of a NetApp ONTAP Cluster were redesigned from scratch and received more scalability enhancements. To change the advanced settings, please navigate to the **Storage Infrastructure** tab, select your ONTAP Cluster with a right click and select **Edit Storage**.



In the window, select **Access Options** to see the new advanced settings interface.

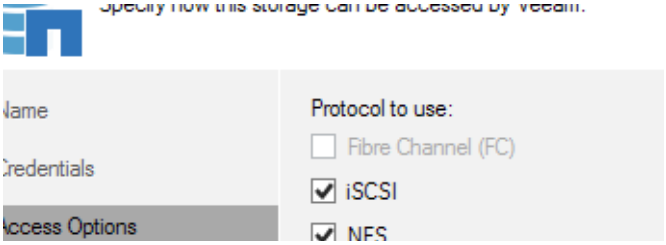


The new tab contains three different advanced options to optimize the storage access and improve the scalability in large installations.



Protocol to use

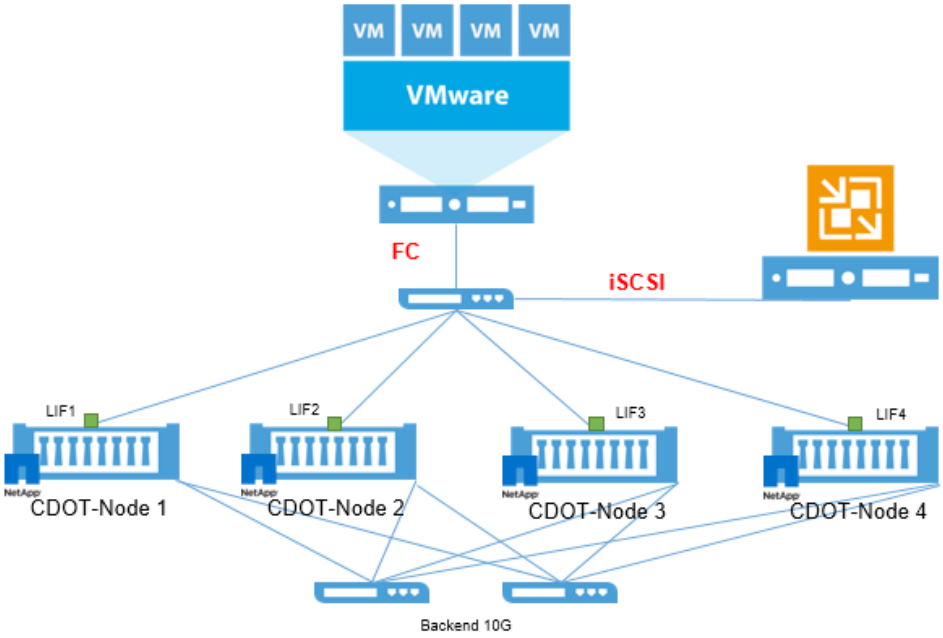
NetApp storage systems are multiprotocol systems. Many controllers in the field have multiple protocols licensed and active. Veeam supports all available protocols (NFS, iSCSI, FC and FCoE) in combination with Backup and Replication. During the discovery, the engine tries first to use iSCSI for mounting the datastore to the Veeam Proxy server, even if FC is configured. If iSCSI is not working FC will then be used.



If you have an environment where both licenses (FC and iSCSI) are enabled and active, you can enforce Veeam Backup & Replication to use the non-default protocol (FC) for backup. To change the behavior, you can now select the protocol Veeam should use for accessing (storage scan, Backup from Storage Snapshots, etc.) the ONTAP system.

With the new protocol selection, you will force our engine to use your desired protocol for accessing your NetApp storage system. This saves some time during the job initialization and can be used to build designs where VMware is using FC to access ONTAP but Veeam uses iSCSI to back the data up.

The image below depicts a dedicated 10GBit/s backup Ethernet as an example.

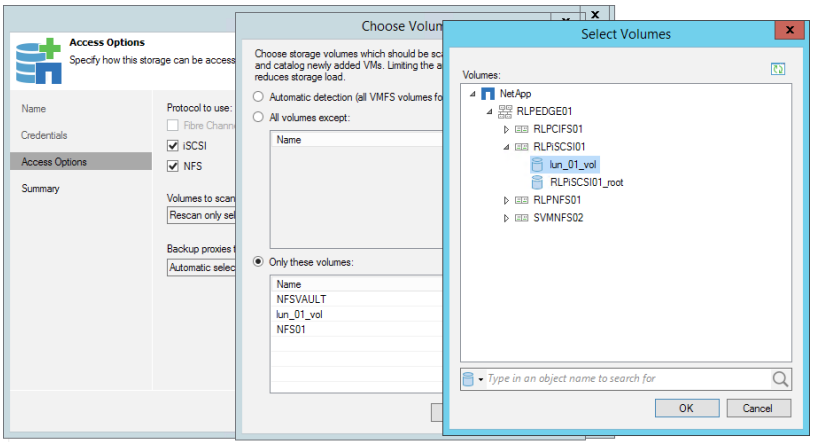


Volumes to scan

Veeam needs to scan the NetApp ONTAP volumes in order to map out the snapshot locations of each VM. If you have a large environment with hundreds of VMs and volumes, a rescan can take a considerable amount of time, especially if Veeam has to rescan snapshots that are not relevant to the search. Therefore, you can use **Volumes to Scan** to select the volumes to be used by Veeam. Please select all volumes that contain VMware VMs here, so that the engine only scans the desired snapshot volumes.

In the volumes selection, you can choose between the following options:

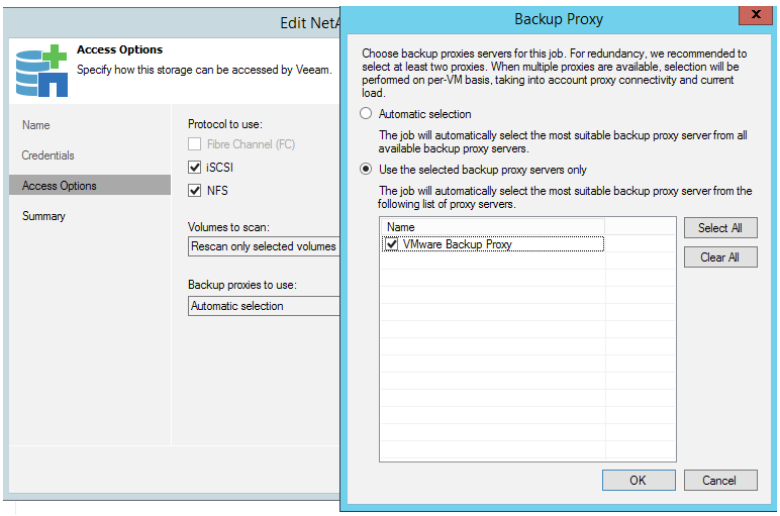
- Automatic detection (all VMFS volumes found with initial scan)
- All volumes except
- Only these volumes



Depending on your environment, you can choose the correct option and define the volumes that should be scanned.

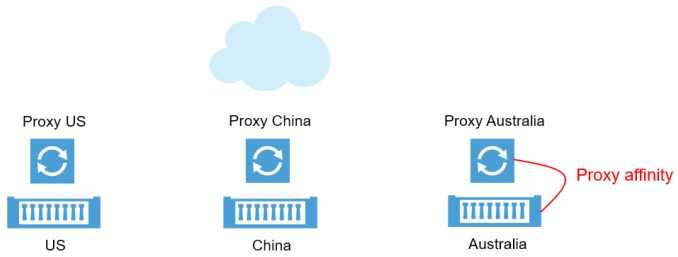
Backup proxy to use

The third advanced setting is **Backup proxy to use**. You can define which Backup proxies are used to access the ONTAP system for scanning and Backup from Storage Snapshots here. You can set proxy affinity rules and force Veeam to only use the selected proxies.

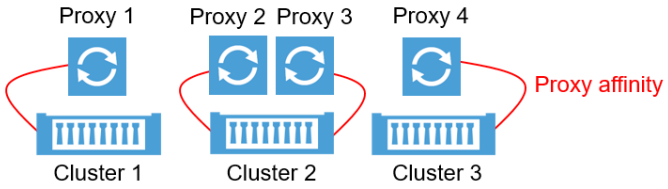


The two main benefits of setting this setting are:

- If you have multiple NetApp ONTAP systems distributed across different locations, you can enforce Veeam to use only the proxy server located near the ONTAP system in question



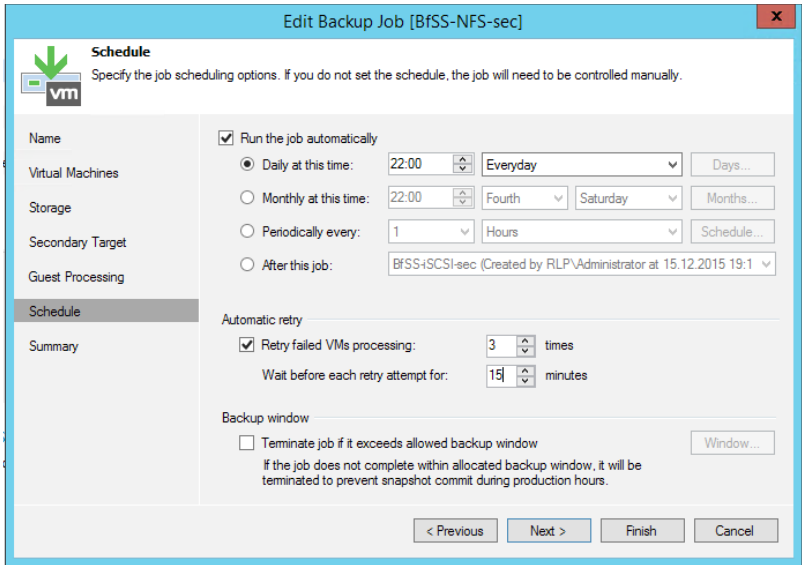
- In larger deployments with multiple ONTAP clusters and proxy servers, you can define which proxy server to use during Veeam backup and restore events, to ensure resource Availability and SLA fulfillment. In this example, we have configured only Proxy 2 and Proxy 3 with access to Cluster 2



Advanced configuration with NetApp MetroCluster installation

The NetApp High Availability solution MetroCluster is fully supported for 7-mode (> ONTAP 8.1) and Veeam Backup & Replication v8 and higher. Failover situations are transparent to Veeam (cluster LIF available) at the (local) cluster. Site failover will stop and terminate any Veeam jobs that may be running (Primary Site Cluster LIF down). Automatic retry (enabled per default) will process all VMs that were not successfully completed during the original job runtime. With this option, you can ensure successful backup completion even during a site failover event. The default retry settings are set to restart the job(s) 3 times with a 10 minute wait period between retries.

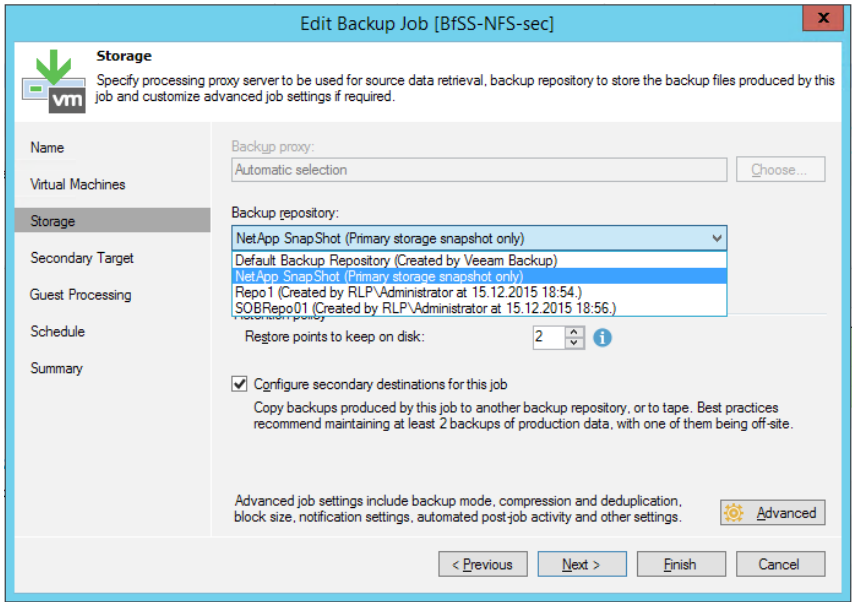
In MetroCluster environments it is recommended to change this value to 15 minutes within the scheduled setting of each job.



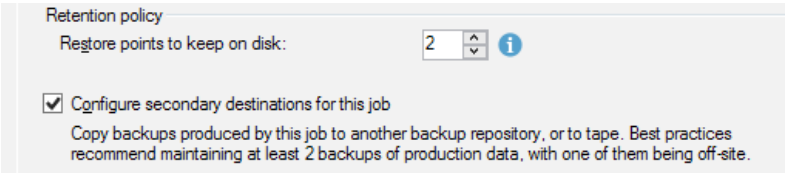
NetApp Snapshot and SnapMirror policy settings for ONTAP

With Veeam Backup & Replication, you can cascade NetApp storage controllers and use the SnapMirror or SnapVault feature to replicate and backup data from your primary to your secondary NetApp system. Within the Backup Job settings, you are able to define where you would like BfSS to occur (Primary or Secondary Array) and also define if it will be a snapshot orchestration only job (no Veeam backup created).

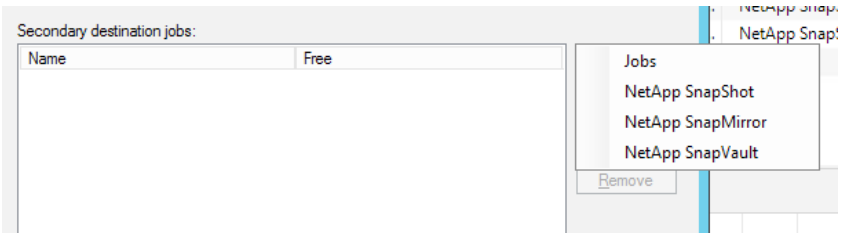
To define whether it will be a BfSS or snapshots only job, you will select under the **Storage** menu, the appropriate **Backup repository**. The automatically created **NetApp Snapshot** repository will designate that this will be a snapshots only job.



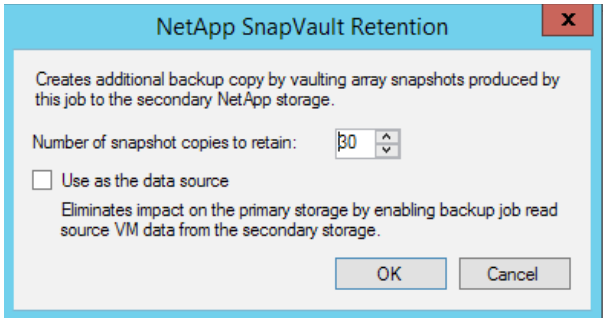
Under the **Storage** menu, you can also select the option **Configure secondary destination for this job** to define secondary NetApp tasks.



The **Secondary target** window, you can add secondary tasks to be executed following the completion of the first job. The available options will change depending on whether it is a snapshots only or BfSS job. For a BfSS job, you will have four options: Jobs, NetApp Snapshot, NetApp SnapMirror and NetApp SnapVault. Select the appropriate secondary target(s) and proceed to the next step. For snapshots only jobs, you will have two secondary target options: NetApp SnapMirror and NetApp SnapVault. Select the appropriate target(s) and proceed to the next step.

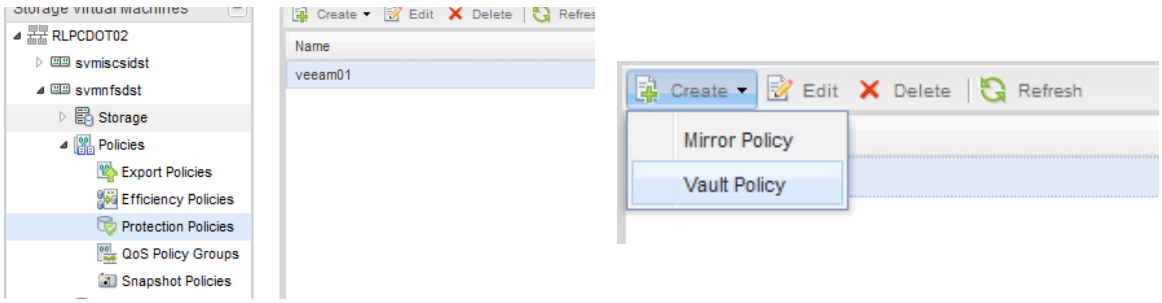


When selecting the option **NetApp SnapVault**, you have to specify how many Snapshots to save on the secondary NetApp volume. For BfSS jobs, you will have an additional option to use the SnapMirror or SnapVault snapshot as the data source for Veeam created backups. This can be specified by simply checking the, **Use as the data source** box. If this box is not checked, BfSS will use the primary storage snapshot as the data source.

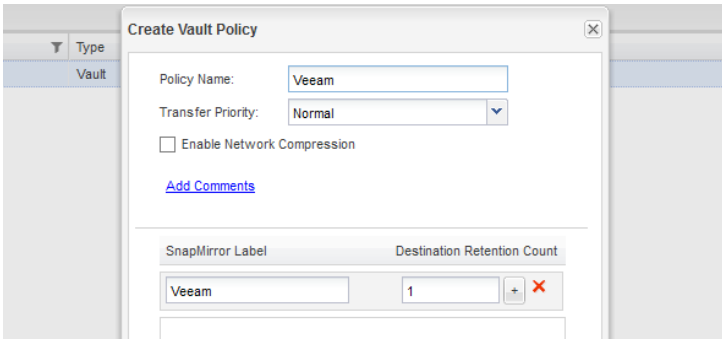


To leverage NetApp SnapMirror and SnapVault with Veeam, the protection relationship and initial transfer needs to be configured on NetApp before the first job is executed. Please refer to NetApp's documentation to see how a relationship is created.

As all the Snapshot handling is performed by Veeam, we recommend you create a specific NetApp SnapMirror policy on the destination controller where the NetApp internal SnapVault Snapshot count is disabled. To create this kind of policy you need to login to your NetApp controller system manager and navigate to **SVM-Policies-Protection Policies**. Create a new policy by clicking **Create — Vault Policy**.



In the next window, please add a policy name (e.g. Veeam) and a **SnapMirror Label** (e.g. Veeam) with a **Destination Retention Count** of one (0 cannot be used). Right after that, click on the plus sign next to the numeral one to add the line into the policy.



By clicking **Create** the new policy will be created and be in effect. Keep in mind, that protection policies are configured at a per SVM setting. You need to create the policy for every SVM separately. Right after your policy is created you can assign the policy to the SnapVault relationship which is used by Veeam.

To create a new relationship, please follow the instructions outlined in NetApp's documentation. During the creation of the relationship, we recommend that you assign the previous SnapVault policy and disable the NetApp internal schedule.

Standard, version flexible and mirror-vault configurations

For years, NetApp has provided two different type of data protection solutions — SnapMirror and SnapVault. SnapMirror is used to mirror the state of the volume to a secondary volume including all Snapshots and can be used as a disaster recovery (DR) solution. SnapVault is used as a data protection (backup) solution based on Snapshots. With SnapVault you can configure a different number of Snapshots across primary and secondary volumes. For example, you can save 10 snapshots on your production volume for instant recovery and store 200 snapshots on your secondary volume for long-term retention purposes.

With ONTAP 8.3, NetApp has extended the data protection relationship (type XDP) support by two more use cases — mirroring and mirror-vault. Mirror-vault can be used to have one data protection relationship for both backup (SnapVault) and DR (SnapMirror). In previous versions, you only had one data protection (type DP) relationship for async-mirror (SnapMirror) and one extended data protection relationship (type XDP) for SnapVault. The table below explains the current modes of data protection policies that are available to configure and their related results. The new flexible version of SnapMirror is part of XDP as well.

Relationship Type	Policy Type	Result
DP	async-mirror	Standard SnapMirror
XDP	async-mirror	Version Flexible SnapMirror
XDP	mirror-vault	Mirror and Vault combined
XDP	vault	Standard SnapVault

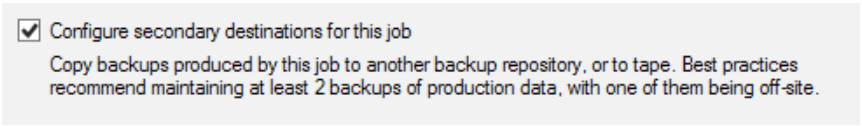
As you can see, NetApp has now integrated two additional types of policies into XDP. Veeam supports all four different types of data protection policies and relation types.

If you want to use any kind of secondary integration, you simply have to select it from within the Veeam job settings.

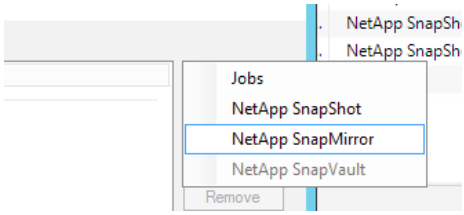
Depending on your SnapMirror policy type, you will need to configure the appropriate option to get the update to a secondary system running ONTAP.

1. Standard SnapMirror relation (async-mirror, DP)

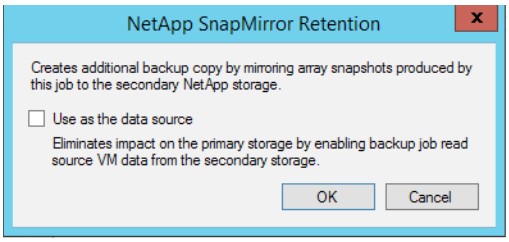
To get a standard SnapMirror relationship configured, you need to choose, **Configure secondary destination for this job** in your Veeam Job under the section labeled **Storage**.



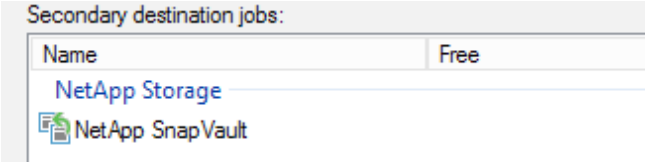
In the next section, labeled **Secondary Target**, you can now add a SnapMirror update by clicking on **Add** and selecting **SnapMirror**.



In the next drop down window simply click **OK** to add SnapMirror secondary target job to your original Veeam Job.

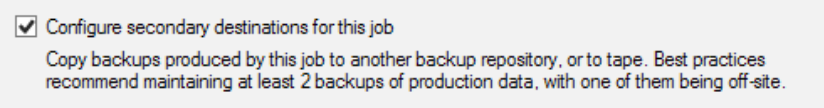


You will see the SnapMirror Job in the GUI.

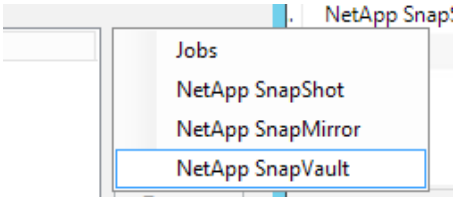


2. Standard SnapVault relation (vault, XDP)

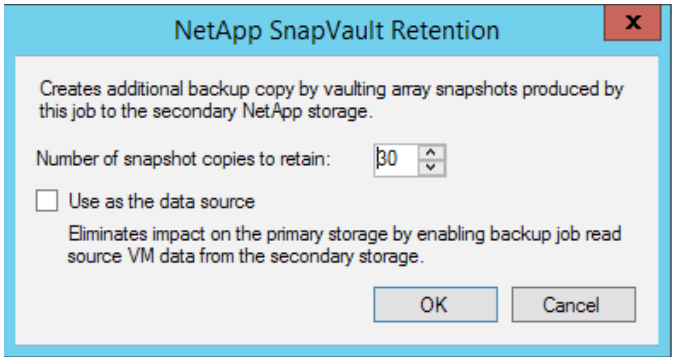
To get a standard SnapVault relationship configured, you need to choose **Configure secondary destination for this job** in your Veeam Job under the section labeled **Storage**.



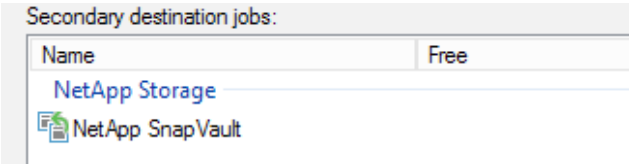
In the next section, labeled **Secondary Target**, you can add a SnapVault update by clicking on **Add** and selecting **SnapVault**.



In the next drop down window, you have to specify the amount of snapshots that should be saved on the secondary window (SnapVault retention). In this example, 30 snapshots will be saved on the secondary volume.

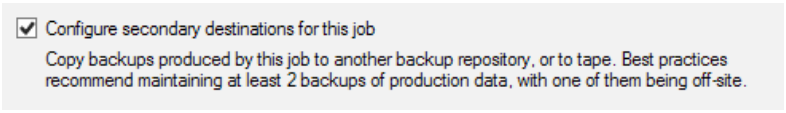


After clicking **OK**, you will see the SnapVault integration appear immediately in the GUI.

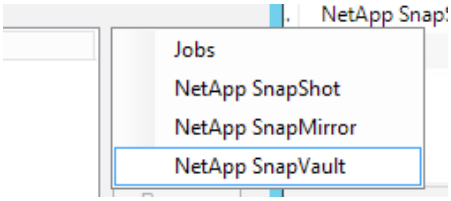


3. Version Flexible SnapMirror (async-mirror, XDP)

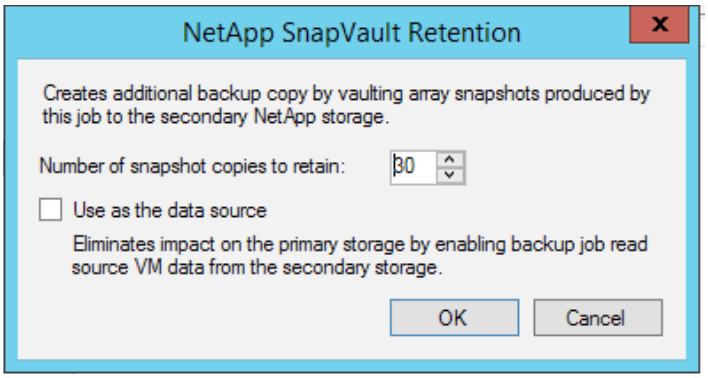
To get a flexible SnapMirror relationship working, you have to choose **Configure secondary destination for this job** in your Veeam job under the section labeled **Storage**.



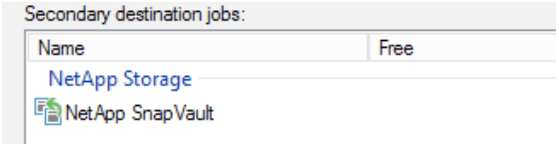
As the flexible SnapMirror type is **XDP,** Veeam recognizes it as a SnapVault relationship. That means that you have to select **NetApp SnapVault** under **Add** in the **Secondary Target window**.



In the next window, you can leave everything on the default settings. Since it is a mirror, the number of snapshot copies for secondary does not have any effect. The number of snapshots that will be saved on the secondary volume depends on the input value keyed into the Job setting **Storage** under **Restore points to keep on disks**.

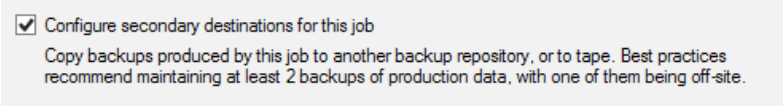


After a click **OK**, you will see the version flexible SnapMirror integration appear immediately in the GUI (shown as NetApp SnapVault).

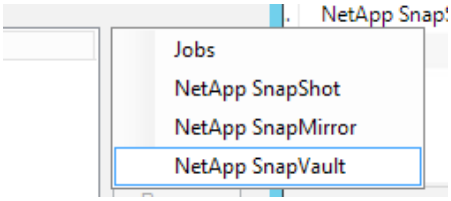


4. Mirror and Vault combined (MirrorAndVault, XDP)

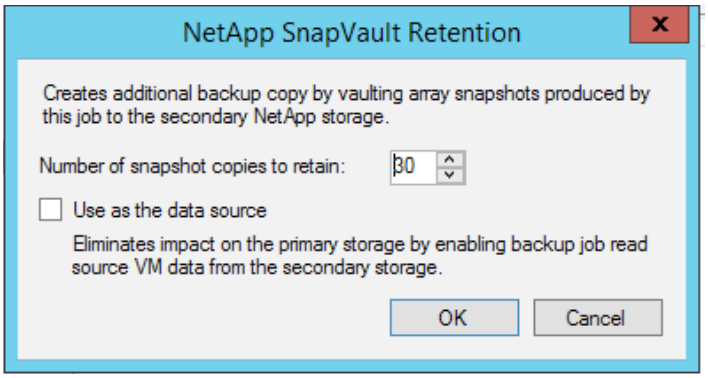
To get a combined SnapMirror/SnapVault (mirror-vault) relationship working, you have to choose **Configure secondary destination for this job** in your Veeam Job under the section labeled **Storage**.



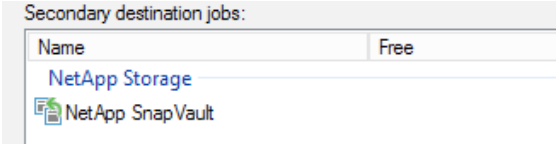
As the mirror-vault relation type is **XDP**, Veeam recognizes it as a SnapVault relationship. That means that you have to select **NetApp SnapVault** under **Add** in the **Secondary Target window**.



In the next window you can specify the number of snapshots that should be retained on the secondary volume. In our example, we are retaining 30 snapshots on the secondary volume.

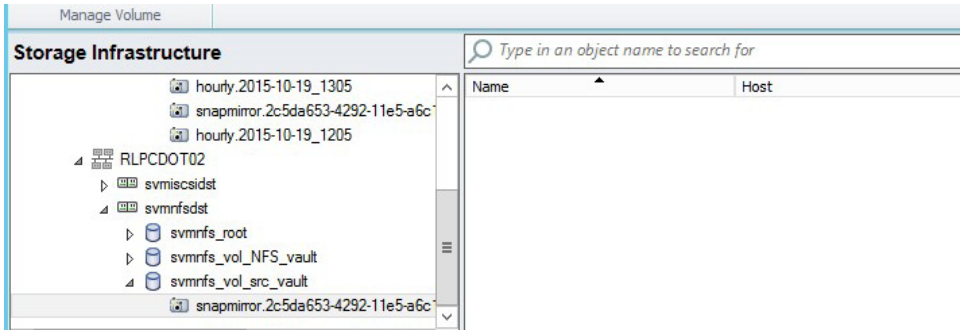


After clicking **OK**, you will see the mirror-vault integration immediately appear in the GUI (shown as NetApp SnapVault).

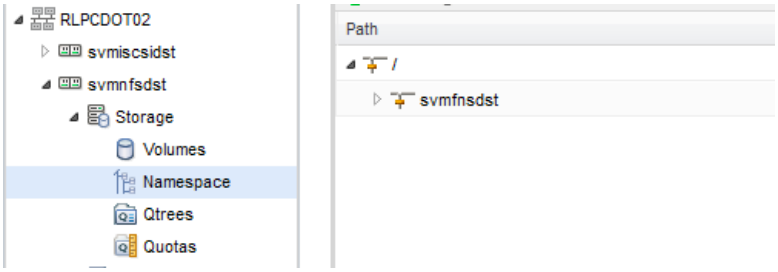


NetApp Namespace settings for ONTAP secondary systems (NFS only)

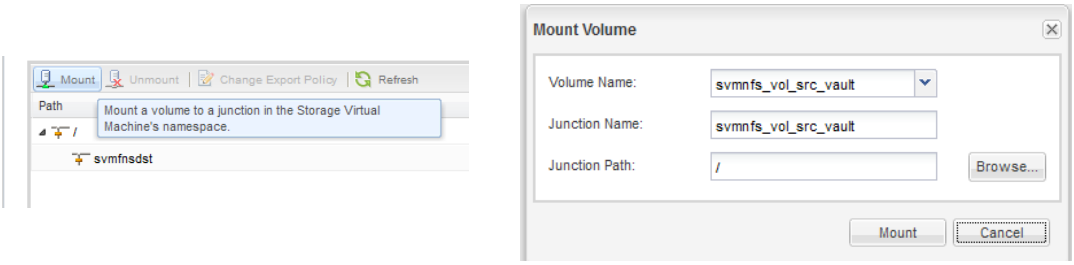
If would you like to leverage the integration between Veeam Backup & Replication and NetApp SnapVault or SnapMirror, it is important to examine the details of how destination volumes are configured. The first step is to configure and initialize the SnapMirror or SnapVault relationships with NetApp management tools upfront. Therefore, please refer to the proper NetApp documentation and keep in mind that you will need to assign the correct policies as described previously in this document. After the relationship is initialized and configured, the NetApp destination volume will be discovered by Veeam after the next scheduled scan task. If you leave the NetApp destination volume with the default settings, you will see the following screen.



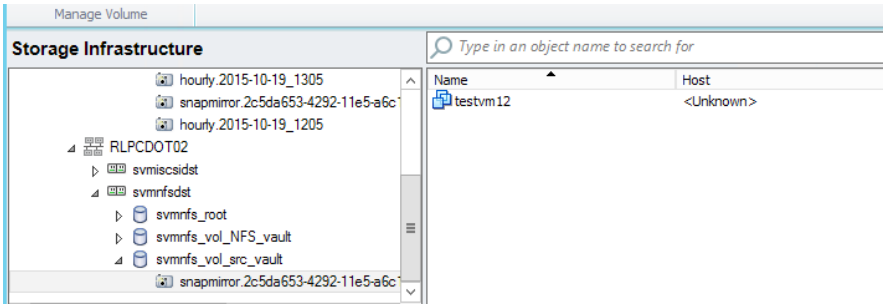
No VM is displayed under the Snapshots and Veeam interface. The problem here is, the Veeam server is not able to access the newly created NetApp volume at the destination site. As a result, Backup from Storage Snapshot will not function well at a secondary site. To access the destination volume for the scan, we need to make sure that the volume is properly configured. By default, the destination volumes are not configured to directly mount on the ONTAP Namespace. Consequently, Veeam is not able to access and scan volume. To mount the volume on to the namespace of the secondary NetApp system, login to your system manager and navigate to the correct storage virtual machine. From there, go to **Storage — Namespace**.



Click on **Mount** and provide a mount path. The following screenshot is an example. Specific values will depend on your design and how your environment is set up.



After you have mounted the destination volume to the local namespace, it will be accessible to the Veeam server. To rescan the system, you can either wait for an automatic rescan or you can manually initiate a rescan of the controller by executing through the Veeam GUI. As soon as the rescan is finished, you will be able to browse the snapshots and see all the VMs assigned to that volume. You may now also use backup from storage snapshot from the secondary NetApp controller.

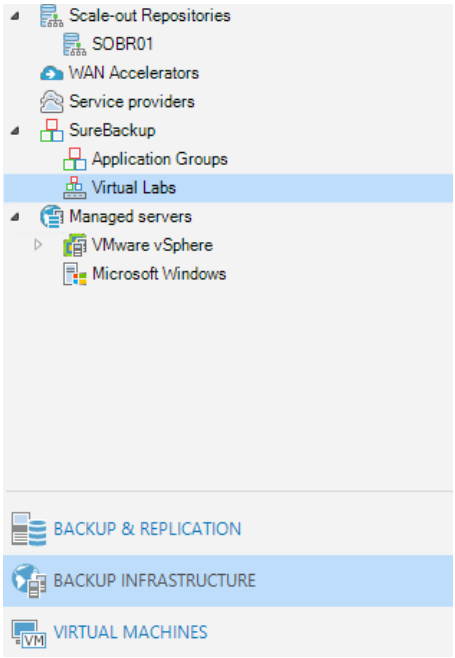


On-Demand Sandbox for Storage Snapshots

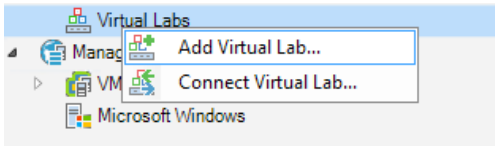
With the release of Veeam Backup & Replication v9, the virtual lab and verified recoverability feature was enhanced by adding the capability to use storage snapshots as the source for running these kind of tasks. In this section, you will see how this needs to be configured and what is important to know.

To use the On-Demand Sandbox™ for Storage Snapshots feature, you need to have a properly configured NetApp integration in place. In addition, all the VMs that you wish to use within the virtual lab need to belong to a volume that on the integrated NetApp system.

The first step is to create a virtual lab. This is an example of a basic virtual lab. For examples of advanced virtual lab configurations, please refer to Veeam's documentation. To create a virtual lab go to **Backup Infrastructure -> SureBackup -> Virtual Lab**.

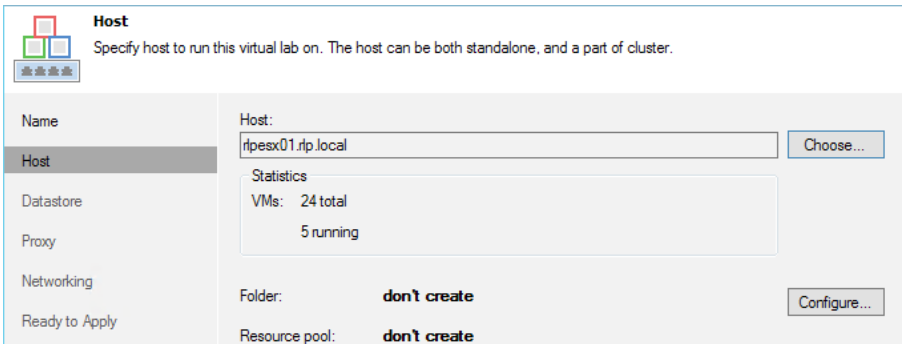


Next, right click on **Virtual Lab** and you will see a context menu where you can choose **Add Virtual Lab**.

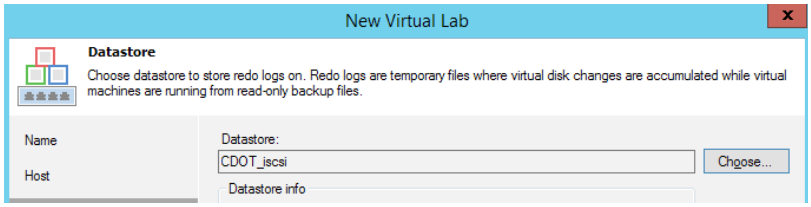


Provide a name for the Virtual Lab and click **Next.**

On the following page, select the host you would like to use for the virtual lab. You can define a specific folder and resource pool as well.



Next, define the datastore where changes are going to be written to. As soon as the virtual lab starts up, you will see a temporary VM folder which is used for the changes within the VM during your tests.

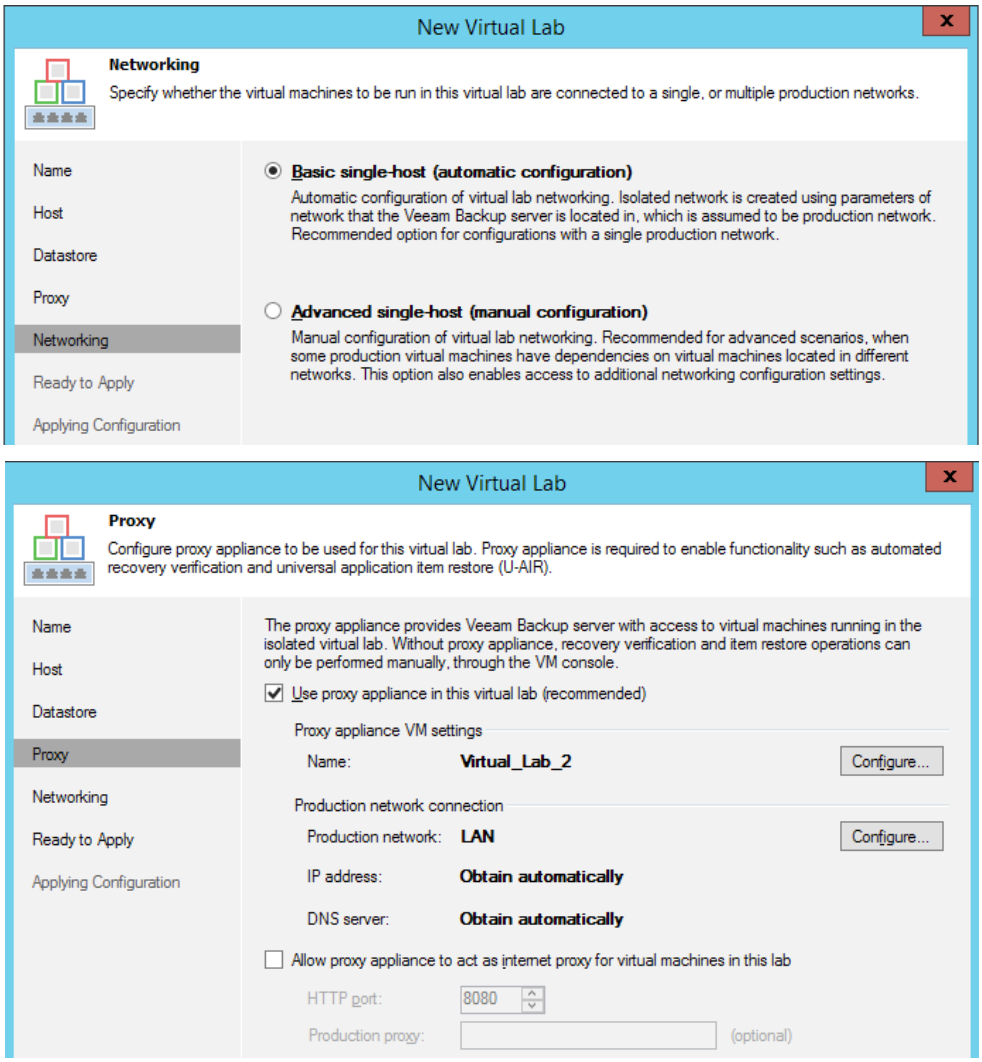


At the Networking step of the wizard, select the type of network settings required for configuring the virtual lab. The virtual lab configuration depends on objects that you plan to verify in the virtual lab.

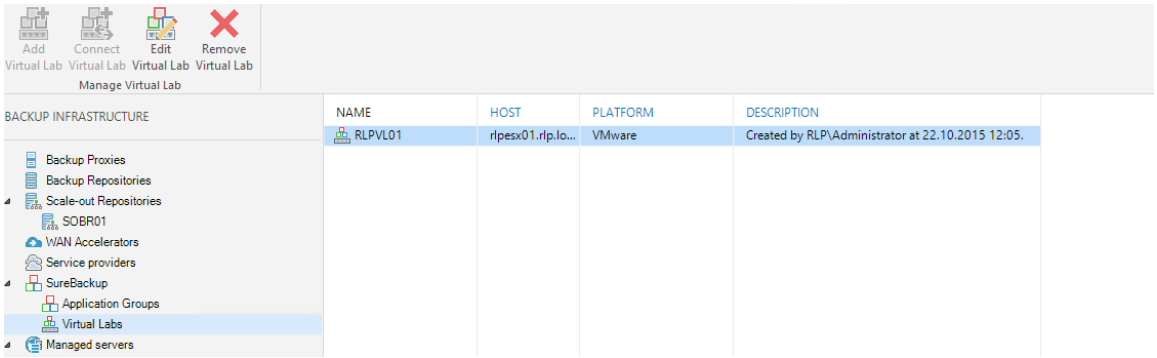
Veeam Backup & Replication offers two networking modes for the virtual lab in which VMs from backups can be verified:

- **Basic single-host.** This networking mode is recommended if all VMs that you plan to verify, VMs from the application group and the backup server, are located on the same production network. In this case, Veeam Backup & Replication will automatically define all networking settings for the virtual lab.
- **Advanced single-host.** This networking mode is recommended if VMs that you plan to verify and/or VMs from the application group are located on different networks. In this case, you will have to manually define settings for isolated networks in the virtual lab.
- You can also verify VM backups in **Advanced Multi-Host virtual labs with DVS**. This scenario can be helpful if you want to test VM backups and replicas in the same virtual lab or want to add verified VM backups and replicas to the same SureBackup® job.

In this example, we are selecting the Basic single-host configuration. In a production deployment, we recommend choosing one of the advanced configurations. For details please have a look at our official documentation (https://helpcenter.veeam.com/backup/vsphere/create_vlab.html).

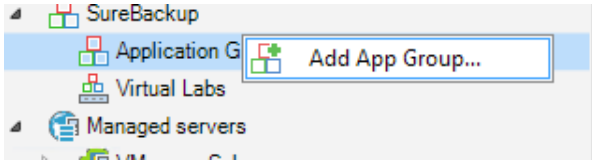


In the next window, you will see a summary of all the settings you defined before. Click on next to start the deployment of the virtual lab within your environment. Depending on the workloads running on our system, this could take several minutes to complete. After the virtual lab is created, you will that lab appear in the GUI.



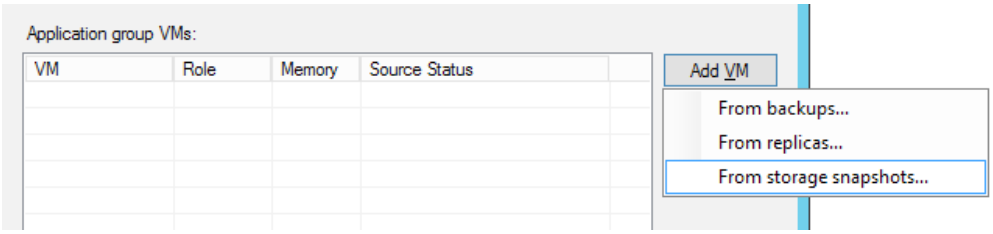
Now that the virtual lab is ready, you can proceed with creating the application group you would like to use with the virtual lab. Go to Backup **Infrastructure — SureBackup — Application Groups**.

Right click on Application Groups. You will see a context menu where you have to select Add App Group.

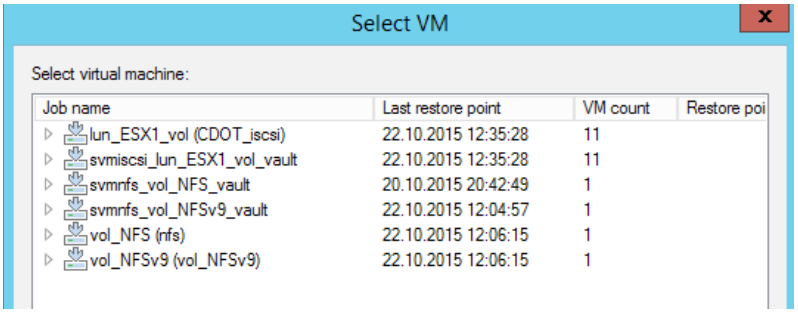


In the first window, define a name and description for the new group and click on **Next**.

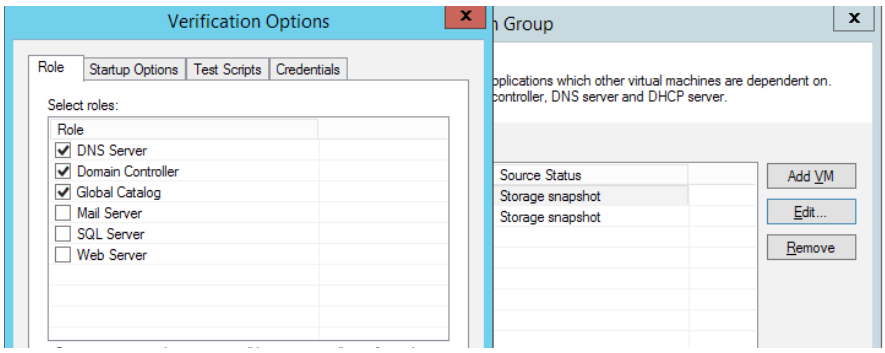
In the next window, you have to define the VMs you want to use within the Application Group. Click on **Add VM** and select, **Storage Snapshot** to use the NetApp Snapshots as a source.



You will now see all the storage snapshots that Veeam has discovered and will able to use for the sandbox. Browse the snapshots and select the VMs you would like to use within your application group.

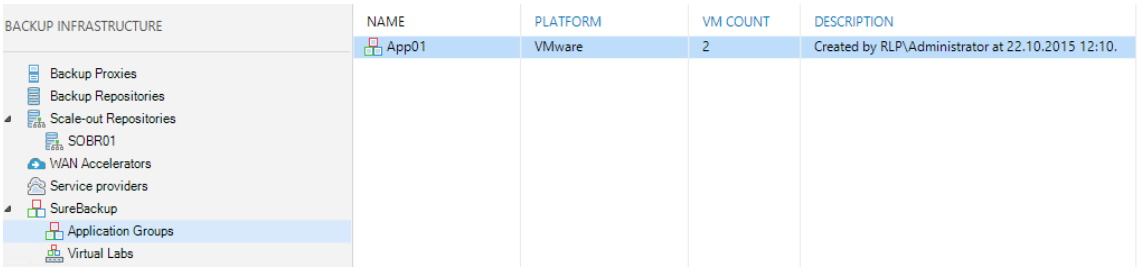


After you have added the VMs to the application group, you can set different options on which verification tasks should be processed within the VM. To do this, select a VM and click **Edit**.

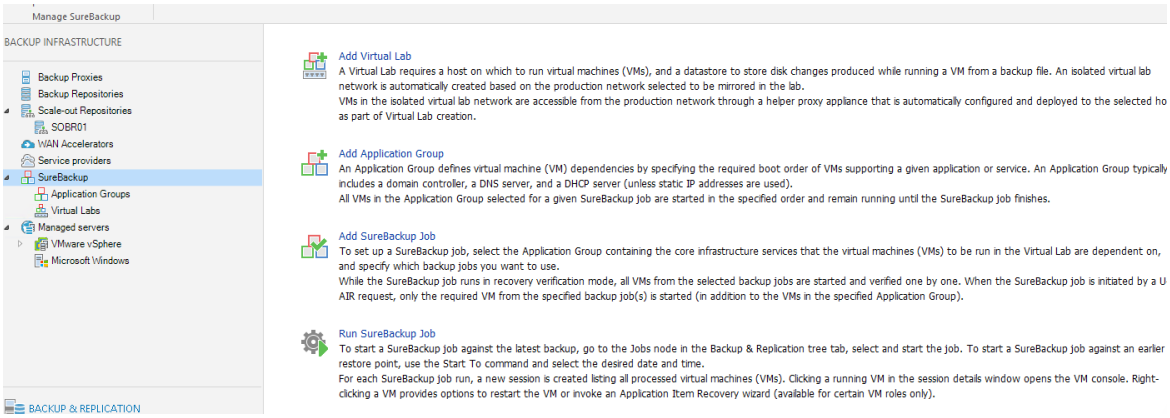


Please refer to our documentation about the detailed setting you can choose within the verification options. If you don't wish to run any verification jobs, just leave the default configuration settings in place. By clicking **Next**, you will have a summary of the previously selected options.

After you have finished the creation of the application group, you will see the group within the GUI.

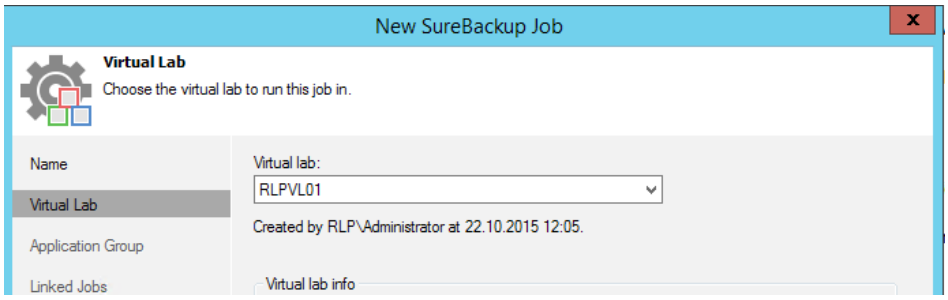


Now that the virtual lab and Application group are created, you are ready to boot up the virtual lab. Click on **SureBackup**.

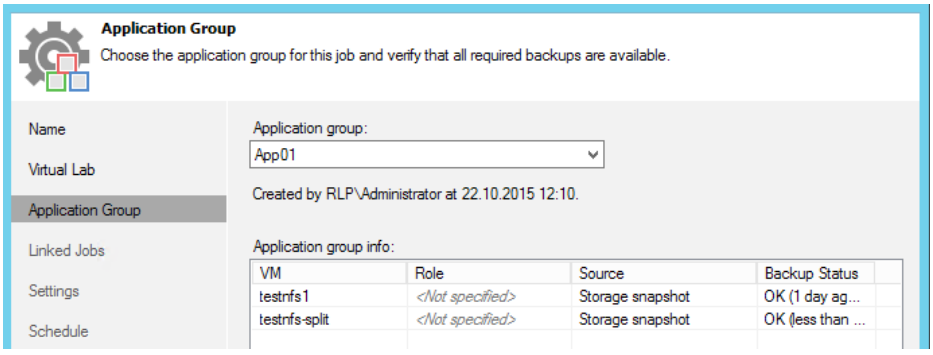


Select **Add SureBackup Job** to create a new task.

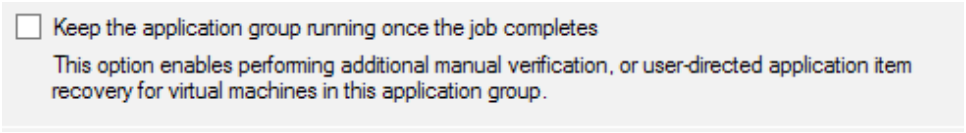
Define a name in the first step and select the virtual lab you would like to use in the second step.



Now select the Application Group you would like to link to this job to.



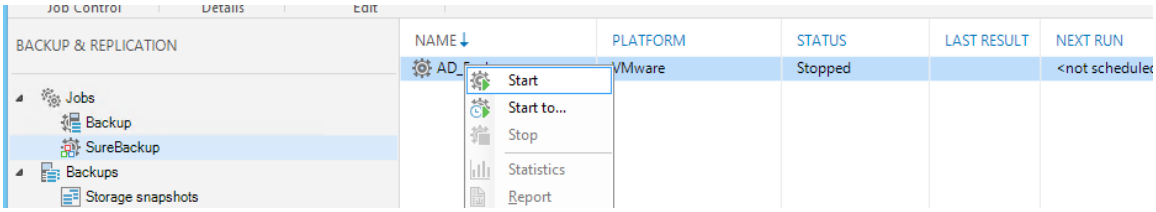
If you would like to keep the lab running, select the following option after the tests are finished:



All the following steps are optional and can be used if required. At the end, you can create a scheduler if you would like to run the job on a regular basis.

At the summary page, click **Finish** to complete the configuration.

Now your SureBackup Job, based on NetApp Snapshots, is configured and ready to use. You can find the job under **Backup & Replication — Jobs — SureBackup**. Select the Job and click **Start** to run it.



Granular ONTAP permission for Veeam Backup & Replication

NetApp ONTAP in both 7-Mode and ONTAP, gives you the option to define users with limited access rights within ONTAP. Through this option you can ensure that external applications, like Veeam, are only able to execute the necessary commands and API requests. In the following section, you can find the minimum required level of access to get the Veeam storage integration for NetApp working. You will also find the commands to be executed to create the relevant objects on your NetApp system.

Granular permissions for 7-mode ONTAP

For NetApp's running in 7-mode, Veeam requires the following minimum access rights within ONTAP:

```
login-http-admin
api-system-*
api-license-*
api-volume-*
api-net-*
api-options-*
api-vfiler-*
api-qtree-*
api-nfs-*
api-snapshot-*
api-lun-*
api-iscsi-*
api-feature-*
```

```
api-registry-*
cli-options
api-fcp-*
api-file-*
api-igroup-*
api-clone-*
api-snapvault-*
api-snapmirror-*
api-cf-*
```

In 7-mode you have to create a role which defines the access rights and assign the role to a group. Finally, a user needs to be created and mapped to the group. In the following CLI example, we show you how you can create these required objects.

Please check the current NetApp documentation (NetApp System Administration Guide) for your ONTAP version for the latest CLI commands.

1. Create the role

The following command creates the role **Veeam**, including all the required access rights on ONTAP and a comment **Veeam role**.

```
useradmin role add Veeam -c "Veeam role" -a login-http-admin,apisystem-*,
api-license-*,api-volume-*,api-net-*,api-options-*,apivfiler-*,
api-qtree-*,api-nfs-*,api-snapshot-*,api-lun-*,api-iscsi-
*,api-feature-*,api-registry-*,cli-options,api-fcp-*,api-file-*,apiigroup-*,
api-clone-*,api-snapvault-*,api-snapmirror-*,api-cf-*
```

With the next command, you can check that the role **Veeam** was created successfully and is configured with all the required access rights.

```
useradmin role list Veeam
```

2. Create the group

After the role is created, you may create the group. In this example, the group is called **Veeam** with the comment **Veeam Backup Group** and the role, **Veeam**, assigned to it.

```
useradmin group add Veeam -c "Veeam Backup Group" -r Veeam
```

With the group list command, you can verify if the group was created successfully and if the role is assigned.

```
useradmin group list Veeam
```

3. Create the user

Now that role and group are ready, you may create the backup user while the NetApp system is added to the Veeam interface. Please replace the <user_name> with the name you desire. It will be assigned to the group Veeam with the comment **Veeam Backup User**.

```
useradmin user add <user_name> -c "Veeam Backup User" -g Veeam
```

Granular Permissions for ONTAP

For NetApp' systems running in ONTAP mode, Veeam requires the following access rights:

```
DEFAULT readonly
cluster readonly
fcp readonly
file readonly
igroup readonly
iscsi readonly
network readonly
node readonly
security readonly
security login readonly
set readonly
snapmirror all
system readonly
version readonly
qtree readonly
lun all
nfs all
snapshot all
volume all
vserver all
```

In CDOT you have to create a role which defines the access rights and assign the role to a user. In the following CLI example, we show you how you to create the required objects.

Please check the current NetApp documentation (NetApp System Administration Guide for Cluster Administrators) for your ONTAP version for the latest CLI commands.

1. Create the role

The following commands are creating the role **Veeam**, including all the required access rights in ONTAP. Please replace <cluster_name> with the name of your cluster.

```
security login role create -vserver <cluster_name> -role Veeam
-cmddirname "DEFAULT" -access readonly
security login role create -vserver <cluster_name> -role Veeam
-cmddirname "cluster" -access readonly
security login role create -vserver <cluster_name> -role Veeam
-cmddirname "fcp" -access readonly
security login role create -vserver <cluster_name> -role Veeam
-cmddirname "file" -access readonly
security login role create -vserver <cluster_name> -role Veeam
-cmddirname "igroup" -access readonly
```

```
security login role create -vserver <cluster_name> -role Veeam
-cmddirname "iscsi" -access readonly
security login role create -vserver <cluster_name> -role Veeam
-cmddirname "network" -access readonly
security login role create -vserver <cluster_name> -role Veeam
-cmddirname "node" -access readonly
security login role create -vserver <cluster_name> -role Veeam
-cmddirname "security" -access readonly
security login role create -vserver <cluster_name> -role Veeam
-cmddirname "security login" -access readonly
security login role create -vserver <cluster_name> -role Veeam
-cmddirname "set" -access readonly
security login role create -vserver <cluster_name> -role Veeam
-cmddirname "snapmirror" -access all
security login role create -vserver <cluster_name> -role Veeam
-cmddirname "system" -access readonly
security login role create -vserver <cluster_name> -role Veeam
-cmddirname "version" -access readonly
security login role create -vserver <cluster_name> -role Veeam
-cmddirname "qtree" -access readonly
security login role create -vserver <cluster_name> -role Veeam
-cmddirname "lun" -access all
security login role create -vserver <cluster_name> -role Veeam
-cmddirname "nfs" -access all
security login role create -vserver <cluster_name> -role Veeam
-cmddirname "snapshot" -access all
security login role create -vserver <cluster_name> -role Veeam
-cmddirname "volume" -access all
security login role create -vserver <cluster_name> -role Veeam
-cmddirname "vserver" -access all
```

With the next command you can check if the role Veeam was created successfully and shows all the required access rights.

```
security login role show -vserver <cluster_name> -role Veeam
```

2. Create the user

Now that role and group are ready, you may create the backup user while the NetApp system is added to the Veeam interface. Please replace the <user_name> with the name you wish to use. It will be assigned to the role **Veeam**. Please replace <cluster_name> with the name of your cluster. You will have to define the password after executing the command.

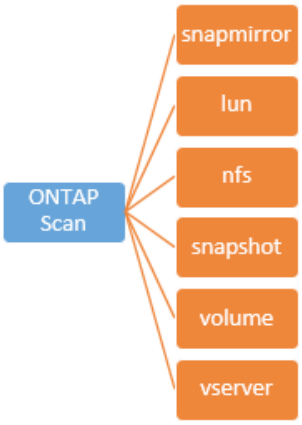
```
security login create -vserver <cluster_name> -user-or-group-name

<user_name> -application ontapi -authmethod password -role Veeam
```

Explanation of granular permissions

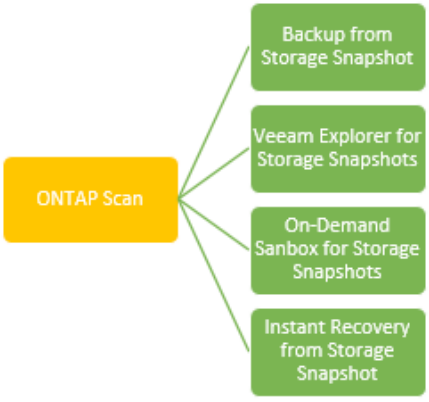
To run jobs with NetApp integration, the ONTAP system has to be added into the Veeam Backup & Replication engine. The engine performs an ONTAP scan on a regular basis to determine all the information needed for features like Veeam Explorer for Storage Snapshots or Backup from Storage Snapshots. The scan determines details like LIF/Interface configuration, exports/igroups and the relation between VMware datastores and NetApp volumes. Most of this information can be obtained by using the ONTAP API calls using read-only permission, however, some of this information can only be obtained through full access privileges.

For example, to perform a rescan of a volume, the right to work with the volume needs to be given. Same for a LUN. Another example is Backup from Storage Snapshot. To successfully perform a BfSS with NFS from a secondary ONTAP system, the Veeam engine has to work with different APIs like **SnapMirror, Volume, Snapshot** and **NFS**.

These permissions are required to ensure that during a Veeam job the correct volumes are mounted by using the correct exports/igroups and NetApp interfaces to the selected proxy server.



This means that all features and technologies within the Veeam engine are dependent on the information obtained through an ONTAP scan. The displayed granular permission privileges are mandatory to perform the required scans and API requests for Veeam's NetApp integration.

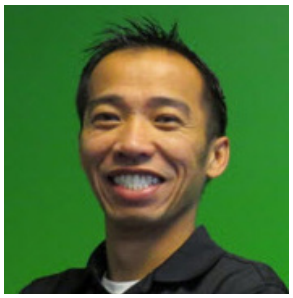


About the Author

Stefan Renner

With more than 11 years of IT-Experience in designing and implementing enterprise data centers, he is the responsible Alliance Systems Engineer for Cisco at Veeam Software. He is a virtualization and data protection IT professional with a lot of experience in the Cisco UCS portfolio, he holds various certifications and is named as a Cisco Champion. Before joining Veeam, he worked as IT-Consultant with a strong focus on NetApp, Cisco, VMware and data protection in projects all over EMEA.

Twitter: @rennerstefan



Shawn Lieu

Shawn is a virtualization and data protection IT professional with over 17 years of industry related experience. He is a Solutions Architect that works with the Global Alliances Team. Shawn is also the co-host of Whiteboard Fridays, a live tech and virtualization show. Shawn lives in Atlanta, Georgia USA.

Twitter: @shawnlieu

About Veeam Software

Veeam® recognizes the new challenges companies across the globe face in enabling the Always-On Business™, a business that must operate 24.7.365. To address this, Veeam has pioneered a new market of Availability for the Always-On Enterprise™ by helping organizations meet recovery time and point objectives (RTPO™) of < 15 minutes for all applications and data, through a fundamentally new kind of solution that delivers high-speed recovery, data loss avoidance, verified protection, leveraged data and complete visibility. Veeam Availability Suite™, which includes Veeam Backup & Replication™, leverages virtualization, storage, and cloud technologies that enable the modern data center to help organizations save time, mitigate risks, and dramatically reduce capital and operational costs.

Founded in 2006, Veeam currently has 47,000 ProPartners and more than 242,000 customers worldwide. Veeam's global headquarters are located in Baar, Switzerland, and the company has offices throughout the world. To learn more, visit http://www.veeam.com.

AVAILABILITY for the Always-On Enterprise™

VEEAM

Veeam makes the Fortune 500 Available. 24.7.365

To enable its **Digital Transformation,** 70% of the Fortune 500 rely on Veeam to ensure Availability of all data and applications. **24.7.365**