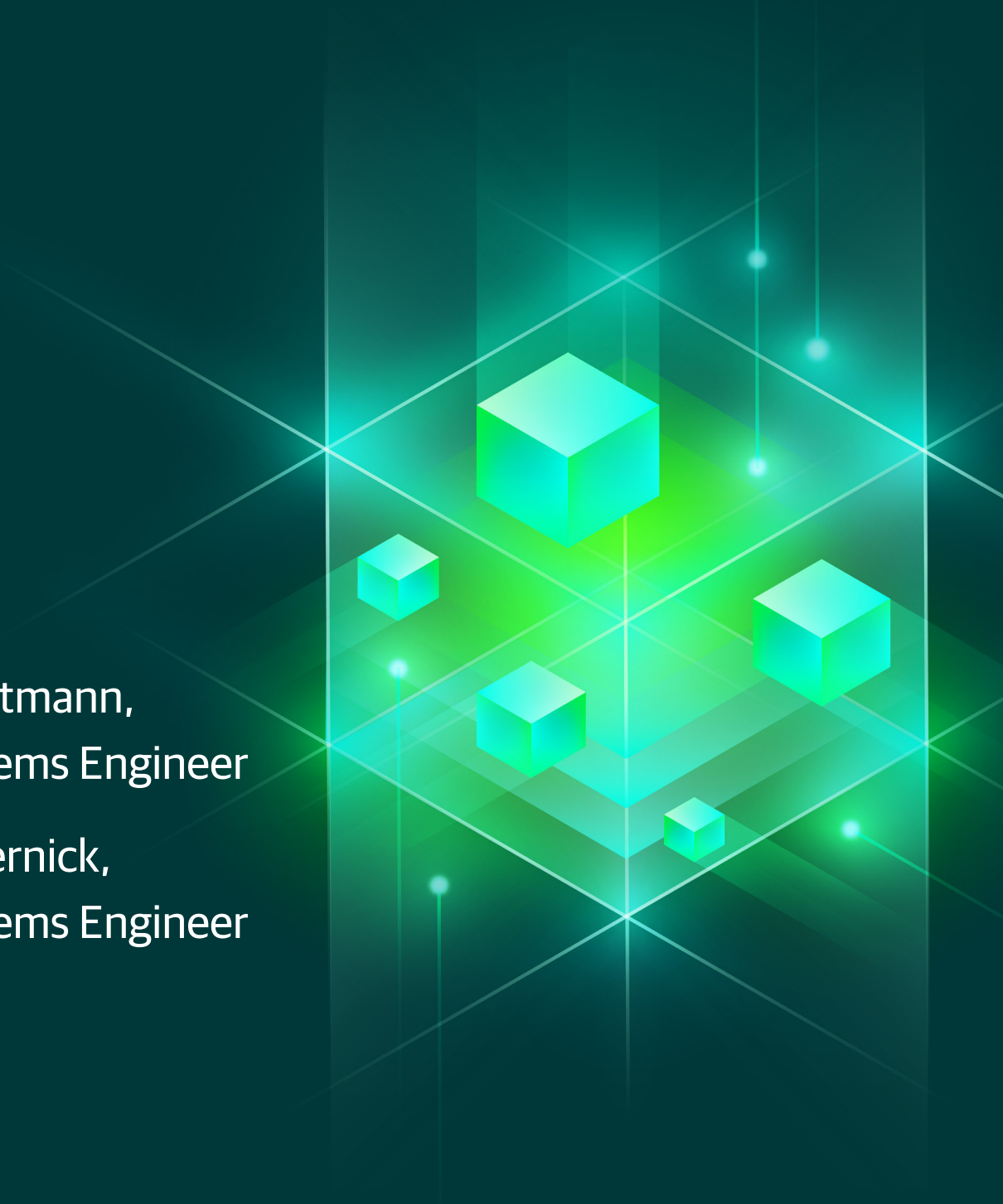
VEEAM

Advanced guide to NAS backup from Storage Snapshots



Marco Horstmann,
Senior Systems Engineer

David Bewernick,
Senior Systems Engineer

Contents

Introduction

In version 10 of Veeam® Availability Suite™ we introduced a new feature called NAS Backup. With this feature we can backup NAS shares from classic Windows or Linux servers as well as NAS storage systems in a very efficient way. In this white paper we will focus on several common NAS storage systems for which we have a high demand from customers to offer data protection.

Disclaimer

The scripts provided in our examples are just that: Examples. All responsibility for the execution and maintenance of these scripts remains the responsibility of the customer and not the creator of these scripts. These scripts are only tested in small lab environments and not on production systems.

The challenges

Backing up a share has several challenges which need to be solved. Some of these challenges can be solved by native product functionality while others require additional logic. Here are two example situations that customers frequently face:

First example: Open files

When a backup is created from a share, all files to protect need to be read from the source. Today fileservers and NAS systems have something that's called opportunistic locking (also called Oplocks). These Oplocks can be used to protect files from being accessed by multiple clients at the same time. While backing up a share that contains several files that have an exclusive lock active, these files will be skipped because Veeam is not able to read their data. After a defined amount of time, the software will perform retries to backup these files with the expectation that a user has closed the files and no Oplocks are present anymore. If the file cannot be backed up within the set time frame and amount of retries, the backup job will finally skip them and finish the job with a warning.

Second example: Consistent state of complete filesystems

The larger the filesystem to protect is, the longer the backup will run. This can add up to an initial backup that takes several hours or maybe even several days.

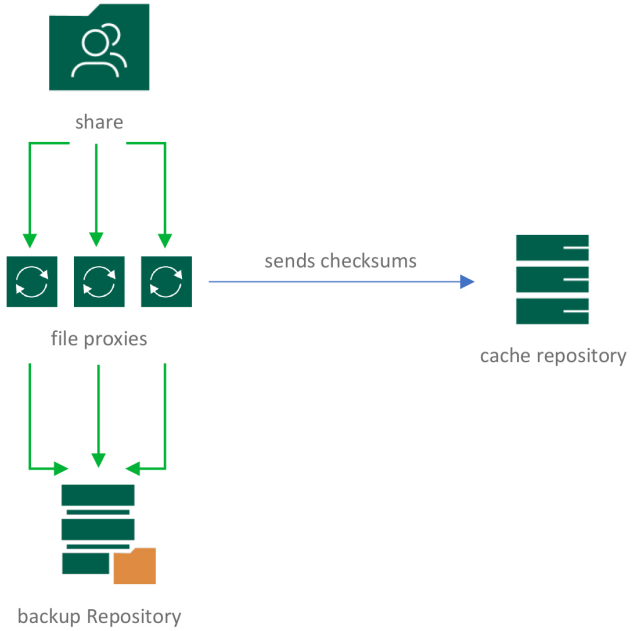
While the backup job is running, files and folders may be changed over the time it takes to complete. This results in no consistent restore point at the start time of the backup. For examples, say the files were backed up between 8 p.m. and 2 a.m. Nobody would know which folder was backed up at which time.

Not only that, files in certain subfolders may have changed during that time and the backup will contain files from various points in time. Say file A was backed up at 8:20 p.m. but was changed at 8:30 p.m. The backup will contain the file version from 8:20 p.m., not the other one. At the same time, say file B was backed up at 11 p.m. and changed at 9 p.m. during the backup. The backup will contain the file version from 9 p.m., not 11 p.m.

Another issue occurs with applications that use file shares for storage and as a database for management or indexing. Both the share and the application should be backed up at the same time for consistency. Because of this, it's important to make sure a specific point in time in the backup shares the same point in time as the protected database to prevent inconsistency.

The solution

With Veeam Backup & Replication™ v10 you can back up NAS shares directly. Both major NAS protocols NFS and CIFS are supported. To back up shares, you first need to deploy several file proxies. We would suggest a minimum of two proxies because in our test labs we've seen that the performance is much better with two proxies vs. one proxy.

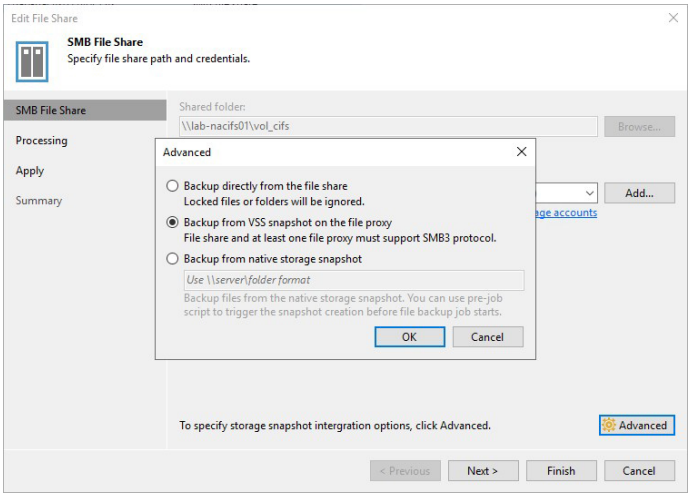


These file proxies will scan all folders of this share and create a CRC tree of files and folders. This CRC tree will then be stored on a cache repository. A cache repository is just a simple backup repository. This repository should reside as close as possible between the file proxies and the file share to minimize the network load. The repository will be used while every job run locates the changed files and folders. After estimating what needs to be backed up, the file proxies will protect those files and folders.

For more information on how the engine works, see this manual section: https://helpcenter.veeam.com/docs/backup/vsphere/file_share_support.html.

With this new NAS backup solution, Veeam Backup & Replication allows us to add a share to the inventory. In the advanced settings of the file share you can specify several options, as seen below:

Backup directly from file share



For legacy and basic NAS backup functionalities, this is the option to choose. It works out-of-the-box for any CIFS/SMB or NFS share, but can bring some challenges that we want to solve with this white paper.

The first challenge is open or locked files. If a file cannot be opened or read during the backup process, it will be skipped after a defined number of retries, and a warning will be written to the backup log.

The second challenge is that you have no specific backup point in time for all the files in the share. This is based on the fact that during the time it takes to protect files and folders, objects in the share may get created, modified, deleted after they have been backed up. But, while all that is happening, the protection will still be going on for other areas of the file structure.

Backup from VSS snapshots on the file proxy

This option can be used if your proxies and file share both support SMB 3.0 and your file share is able to process remote VSS requests. This option should work with Windows Server 2012 and later. Because many NAS appliances use things like samba packages or their own SMB implementations, you need to verify this option with the specific vendor to see if they can support this. In our tests, we tried to create VSS snapshots starting with NetApp Clustered Data Ontap version 8.2 and newer. The NetApp system created a Storage Snapshot and at the end of the job run it was successfully removed. All other tested systems, even if they support SMB 3.0, don't have remote VSS support.

If your system supports remote VSS and doesn't replicate to a secondary system that should be used as a data source, this option will give you the easiest out-of-the-box configuration because no additional processing (i.e., scripts) is needed. This white paper is focused on providing a solution for shares that don't have remote VSS support or use vendor-specific replication.

Backup from native storage snapshots

This option is also referenced as "backup from alternative location", because a Storage Snapshot isn't the only solution you can use as source path for the backup job. Maybe your NAS appliance will replicate to another location or system and you want to use the secondary destination to create backups from this.

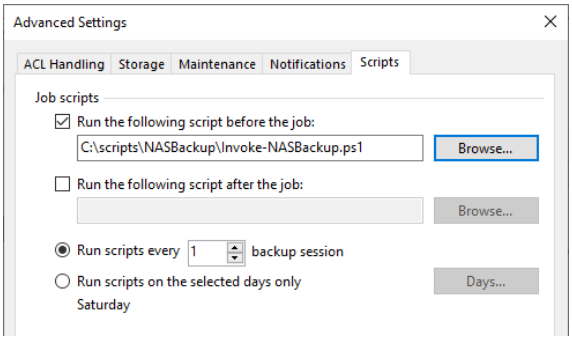
With this function you can back up:

- NAS appliances that support snapshots (both SMB and NFS) but are unable to provide remote VSS support.
- NAS appliances that replicate to a secondary system.

For these scenarios, we created some sample scripts that will show what your solution can look like. Sample scripts can be found at: https://github.com/VeeamHub/powershell .

General scripting advice

Within the file backup job, you're able to add scripts that run before and after the job. You can also specify if this script should be run on every backup session or only on specific days.



To use an alternative path in most storage systems, you will need to create a kind of Storage Snapshot. "Snapshot" is the term most vendors use, so we will use it in this white paper as well. You must check if the vendor will provide a scripting option. Depending on the vendor, we see four major options for creating snapshots:

- PowerShell
- RestFUL API
- SSH commands
- Vendor-specific command line utility

You need to ensure that your script provides error level/code to Veeam Backup & Replication. Veeam Backup & Replication will execute this script and if the error code 0 is returned, and Veeam Backup & Replication will show a successful script execution. Returning error codes other than 0 will create a warning in the job log. In both cases, the job will run until it's done.

To run scripts from a backup job, it's important to know that they will be running in the context of a Veeam Backup & Replication service. In most cases, this will be the SYSTEM user. If PowerShell stores credentials in a file, they are encrypted in the user context in which they are provided. So, credentials that are used to connect to NAS storage systems need to be saved from the correct user account. To be able to save credentials by the SYSTEM user, use the Microsoft Sysinternals tool PSEXEC.

Learn more: https://docs.microsoft.com/en-us/sysinternals/downloads/psexec

To start a PowerShell in the SYSTEM context, the command would be:

PsExec64.exe -i -s powershell.exe -ExecutionPolicy Unrestricted

Now the commands to save a credential set can be performed. Here is an example that stores them in a vendor-nas-system-credentials.xml file:

$credential = Get-Credential

$credential | Export-CliXml -Path "C:\scripts\vendor-nas-system-credentials.xml"

This .xml file can be used as a parameter when calling a script in a backup job. Then, the decryption will be correctly done.

Also, running a PowerShell with PSEXEC can be quite helpful when troubleshooting a script that needs to run with the SYSTEM user.

Examples

NetApp FAS-Series

For this example, we installed Veeam Backup & Replication v10 and installed two NetApp Simulator Ontap version 9.5 simulators. We also created two SVMs for CIFS, each with one volume called "vol_cifs" on primary and "vol_cifs_mirror" on secondary with a SnapMirror relationship between both volumes. A SnapVault relationship would work, too.

Prerequisites

To run something like this, you need to download and install the NetApp PowerShell Toolkit 9.6 on your Veeam Backup & Replication server. After installing this tool kit, you need to restart Veeam Backup & Replication in order to use the new modules.

You can find the NetApp PowerShell Toolkit 9.6 download and documentation here: https://mysupport.netapp.com/tools/info/ECMLP2310788I.html?productID=61926&pcfContentID=ECMLP2310788

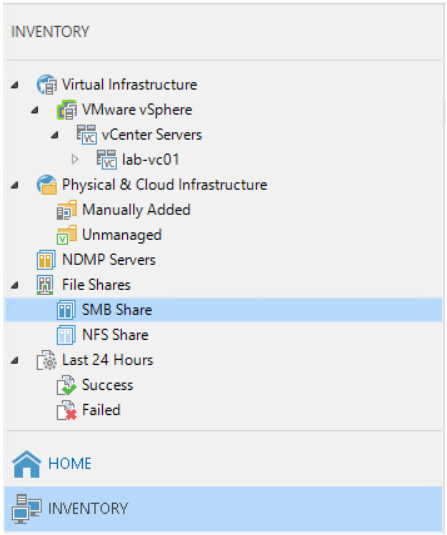
In this example we are using a script that we added to Veeamhub: https://github.com/VeeamHub/powershell/tree/master/BR-NASBackup4NetApp

Overview of snapshots with a NetApp system

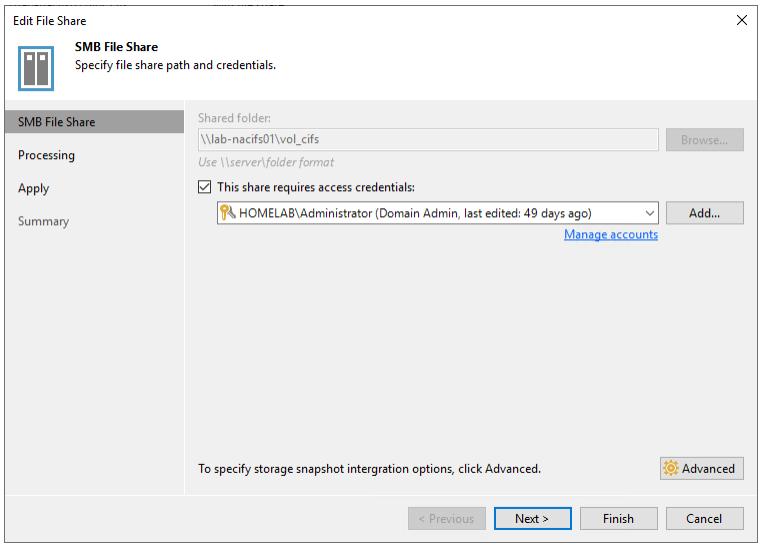
The NetApp FAS series storage systems and the virtual variants of it create snapshots on a volume level and that includes all subfolders. The filesystem WAFL (Write Anywhere File Layout) does have a special hidden folder called ".snapshot". This ".snapshot" folder shows all of the existing snapshots. You can browse this folder and, for example, open an older version of a file or folder. Because ".snapshot" had some issues in the past with Windows-based systems, NetApp shows this ".snapshot" folder as "~snapshot". This decision will influence the path that will be used later when adding shares back up.

Adding a file share

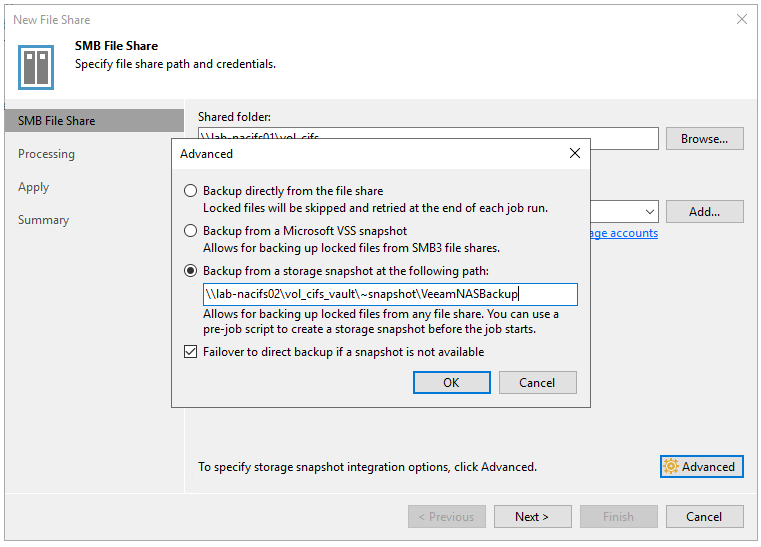
In the INVENTORY pane of Veeam Backup & Replication, you will find a new menu entry called "file shares". Here, you have the option to add SMB file shares, NFS file shares or a managed windows server (i.e., a classic file server), all of which can be used in a file backup job.



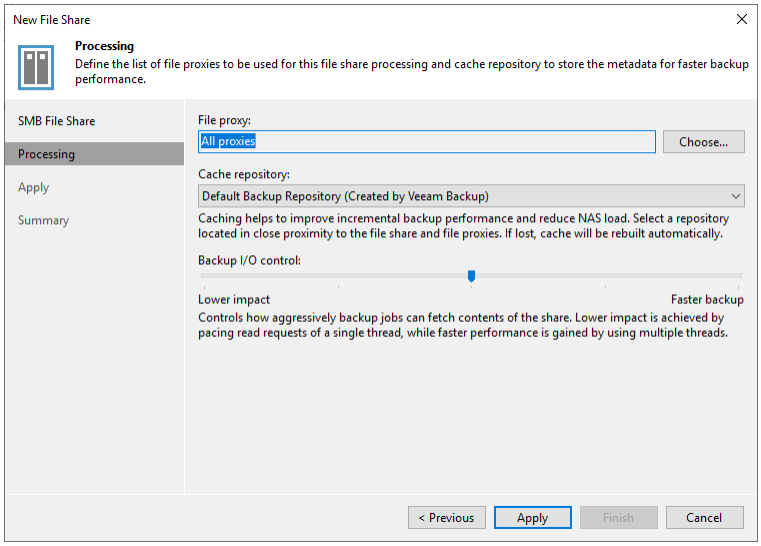
I added the file share \\lab-nacifs01\vol_cifs to Veeam Backup & Replication and configured the advanced option where I told it to use another path as the backup source. This path is a snapshot I've replicated via script from the primary volume to the secondary volume. I will show the script later in this white paper.



Adding the share and setting credentials for accessing this share.

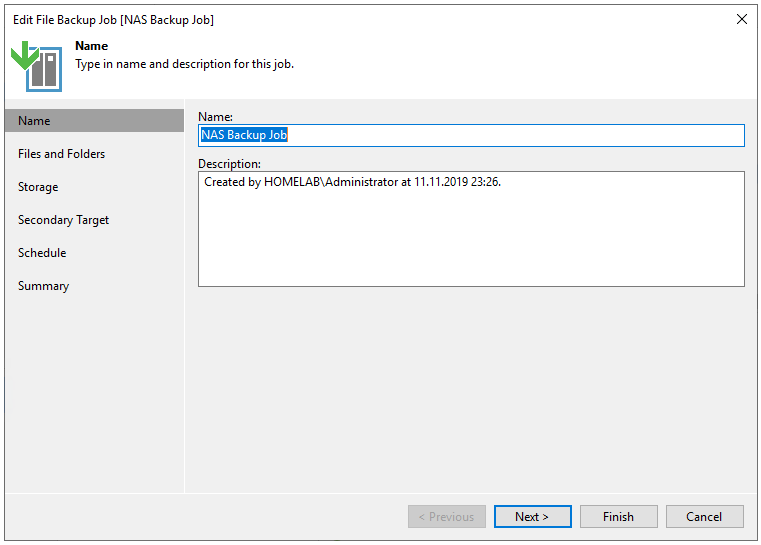


In the advanced settings, you can specify the backup mode. In this example, we want to use the "backup from native storage snapshot" option. In this option, we enter the alternative data path. In this example, we want to use a snapshot, which was created and replicated to the secondary NetApp SVM called "lab-nacifs02".

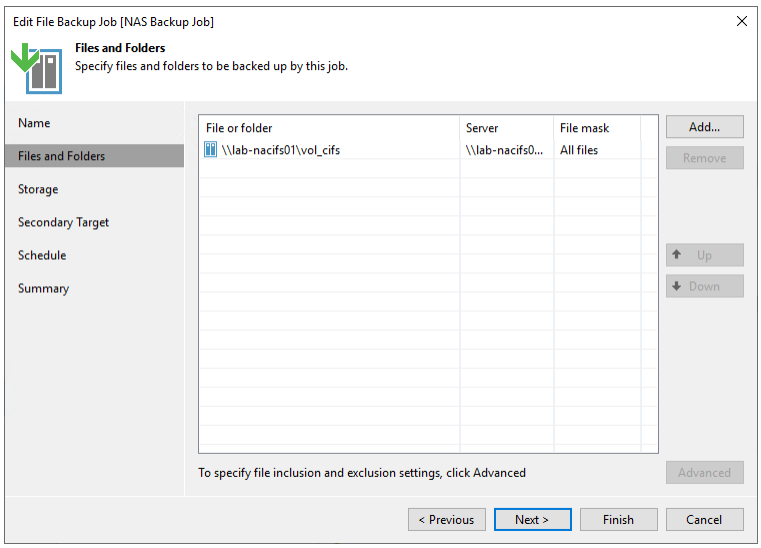


Here, you can set which files and file proxies you want to back up the share and which repository you want to use for caching metadata. On this page, you also can see how many loads Veeam Backup & Replication can back up. Maybe your NAS always has a high IO load and it is a good idea to reduce the additional load for a backup.

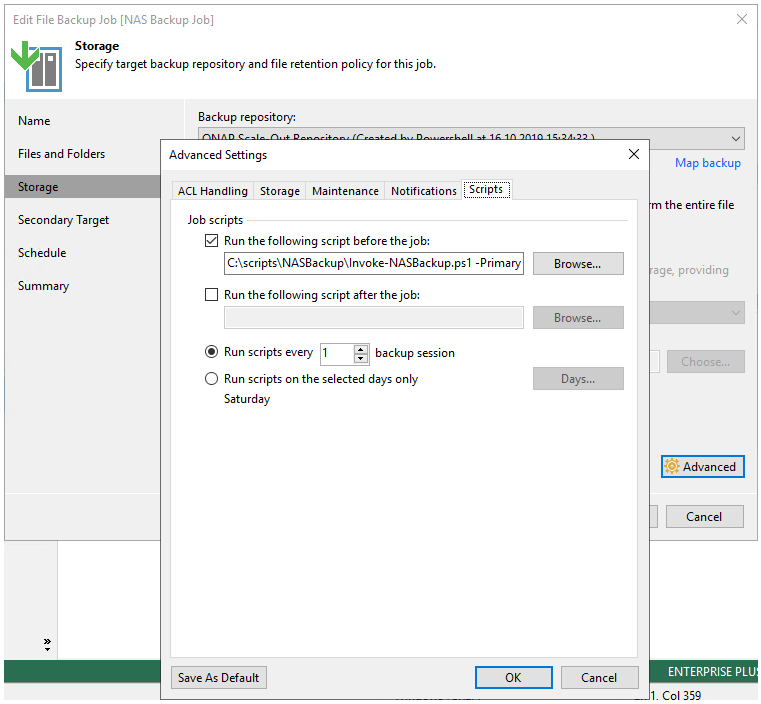
Creating a backup job



After adding the shares to the inventory, we create a new “file backup job” with a name and description and press “next”.



With "add..." you can add one or more shares to this backup job. For each share you can set advanced options like which file extensions should our should not be backed up. When all shares are added, press "next".



On the next dialog window, we again find an "advanced" button. In the advanced dialog we can find a tab called "scripts" where we need to add the pre backup script, which creates and replicates the needed snapshot. In the script examples from prerequisites, you will find an "invoke-NASBackup.ps1" file which can trigger a snapshot for only one share. If multiple shares are on the same volume, you only need to trigger one snapshot. It is usable for all shares on the same volume. This is the main script for creating, replicating and even deleting snapshots. First, it loads the saved credentials to access the source and destination clusters, then it loads the required modules and connects to the NetApp systems. After connecting the NetApp systems, it looks up the volume where the specified share is located and creates a new snapshot and maybe deletes an old existing snapshot.

This script is written for CIFS environments but with some code changes you can use the script for NFS environments, too.

If you want to back up from a SnapVault/SnapMirror destination you need to use the parameters of this script to call the script in the pre-job script settings of the NAS backup job.

```
C:\scripts\NASBackup\Invoke-NASBackup.ps1 -PrimaryCluster “LAB-NA01” -PrimarySVM “LAB-
NACIFS01” -PrimaryShare “vol_cifs” -PrimaryClusterCredentials “C:\scripts\credential_system.
xml”  -UseSecondaryDestination -SecondaryCluster “LAB-NA02” -SecondarySVM “LAB-NACIFS02”
-SecondaryShare “vol_cifs_mirror” -SecondaryCredentials “C:\scripts\credential_system.xml”
```

After changing the script parameters, you can click “OK” and save the changes. Now, you can continue to set up all other job options and at the end, you can start the backup job.

DellEMC² Unity

In this example, we will discuss the option to use a snapshot of a unity storage resource as a source for NAS backup. Since there is no support for remote VSS in the SMB-3 implementation at the time of writing, the solution is to create a snapshot via scripting. The snapshot is created on the file system level and must be with the status shared=yes. This ensures that the snapshot can be presented as a SMB share for backup purposes.

Prerequisites

On a scripting basis, one of the easiest ways is to use PowerShell. As there is no official PowerShell module from DellEMC for Unity systems, we are going to use the community-driven option created by Erwan Quélin. His sources can be found in GitHub and in the PowerShell gallery:

https://github.com/equelin/Unity-Powershell

https://www.powershellgallery.com/packages/Unity-Powershell/0.16.2

Since it is published to the PowerShell gallery, it can easily be downloaded and installed directly within a PowerShell command window with *Install-Module Unity-Powershell*

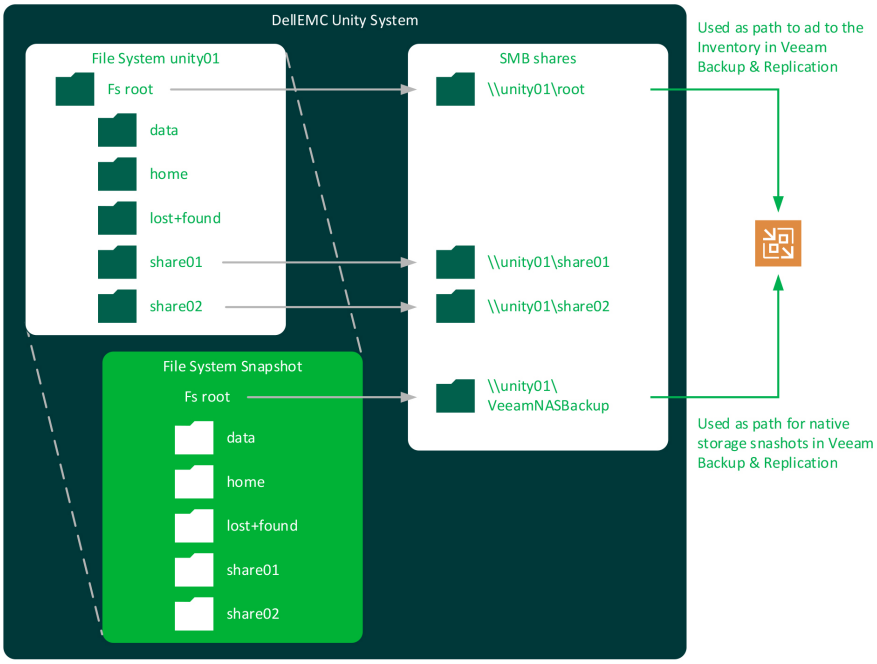
Overview of snapshots with a Unity system

The Unity systems do create snapshots on the file system level and include all the subfolders. The pre-created subfolders are data, home and lost+found. At this point, you have to choose where shared folders are created; either in top root or as subfolders in data and home.

This decision will influence the path that has to be used later when you add the shares you want to back up.

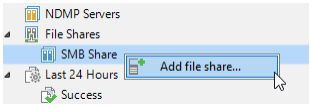
In this example, we have additional folders on the root level that are being used for SMB shares.

To add the root of the file system as an inventory object in Veeam Backup & Replication, we are sharing this root via SMB.

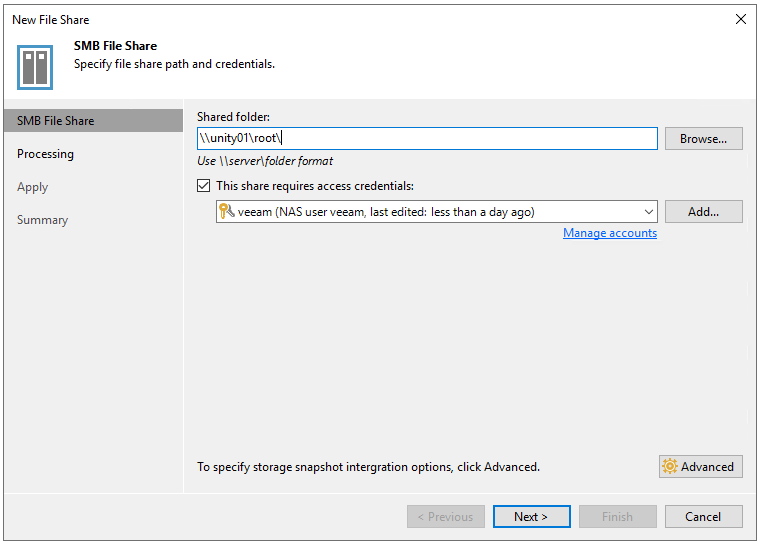


Adding a file share

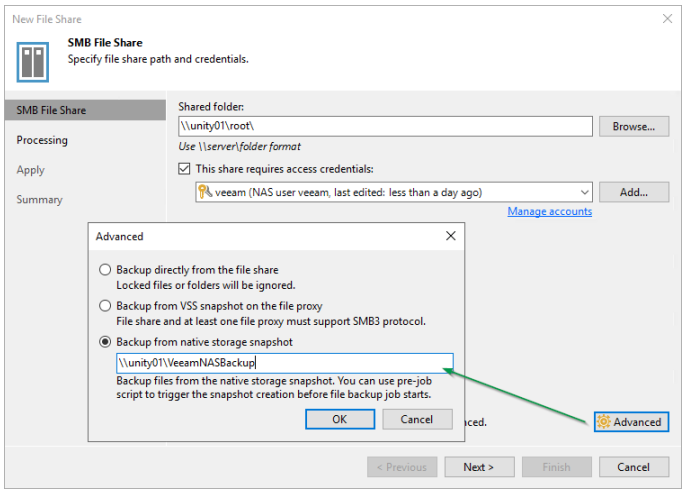
Start by adding amn SMB file share in Veeam Backup & Replication:



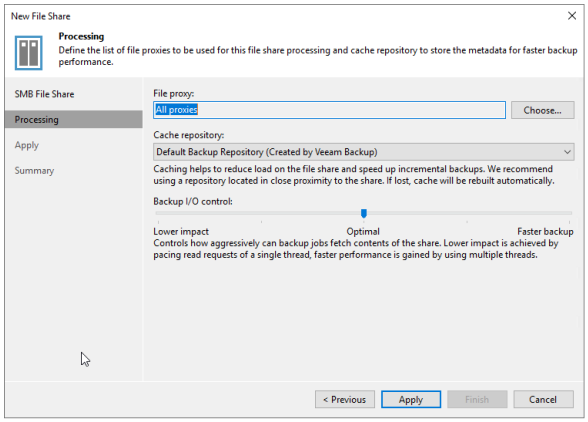
Now we need to provide the UNC path of the root share and credentials:



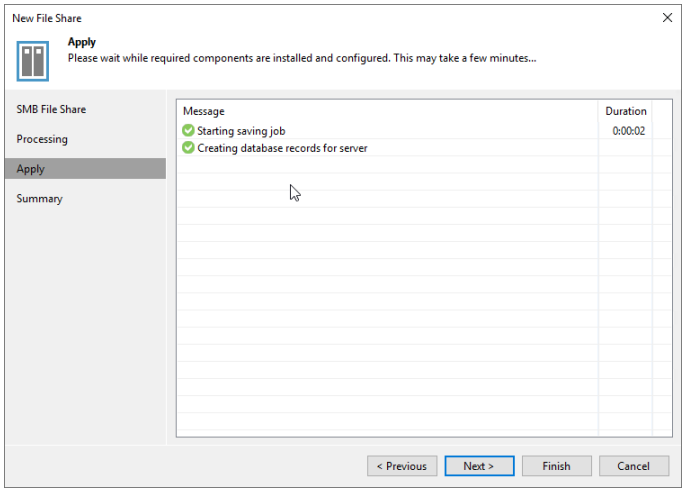
In the next step we open the advanced dialog and provide the path to back up from a native storage snapshot.

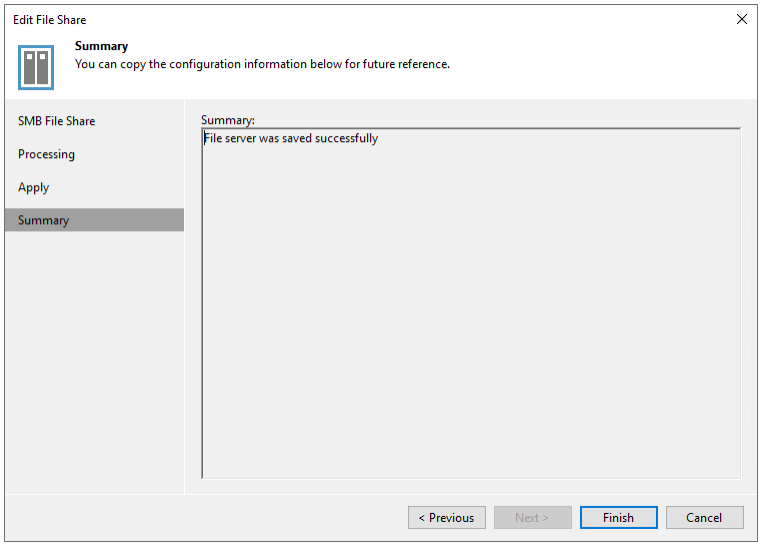


Clicking “OK” and “next” will bring us to the settings for processing options. Here we can define the selection of file proxies, the cache repository and the settings for Backup IO control. Since this is individually related to different setups, we will keep the default values in this scenario.



Continue to apply the settings and finish the wizard:

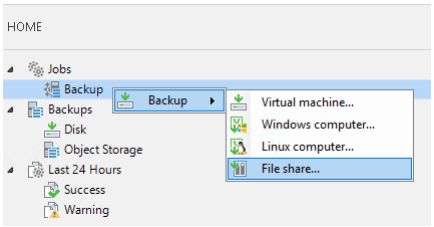




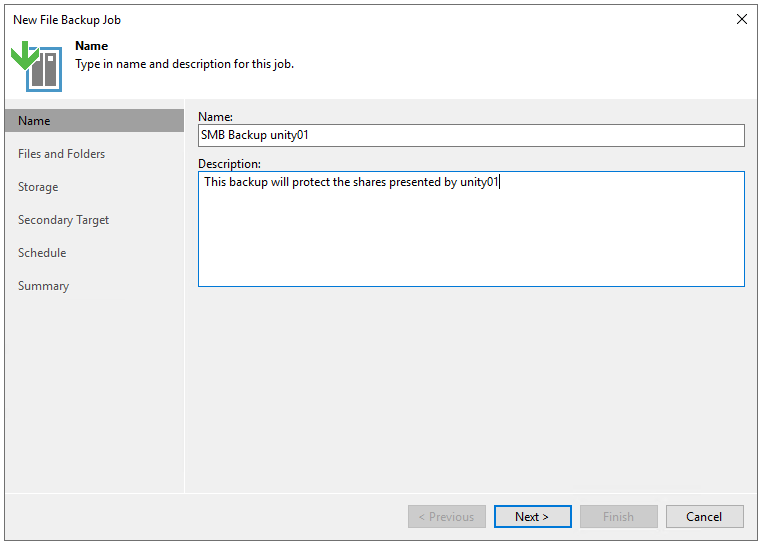
Now we have added the Unity SMB share to the inventory and can proceed with the job creation.

Creating a backup job

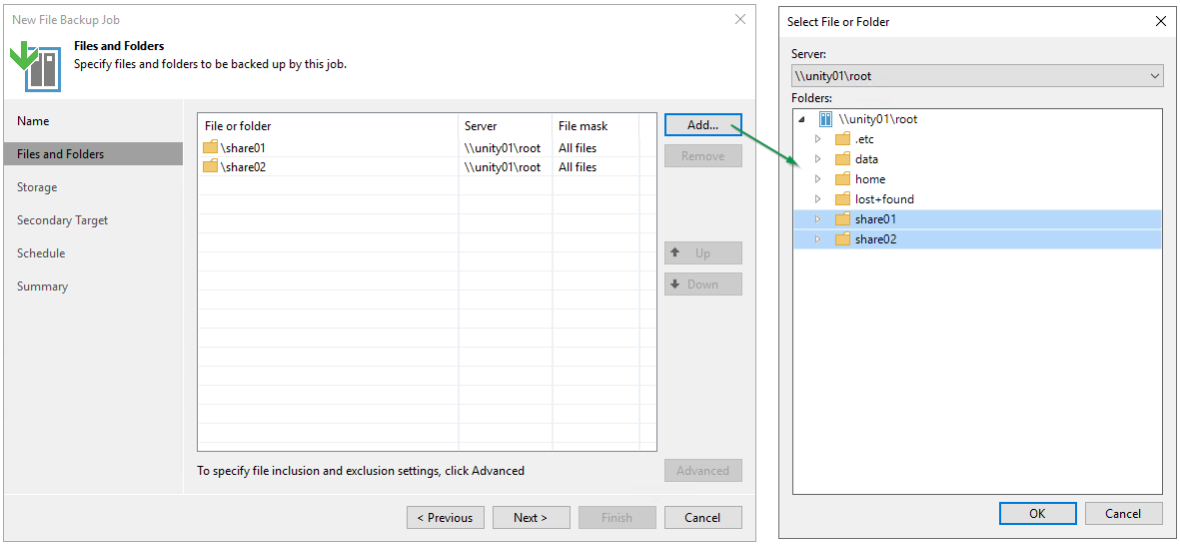
Going to the home section in Veeam Backup & Replication will give us the option to create a new backup for file shares:



Start with providing a name and description for the job:

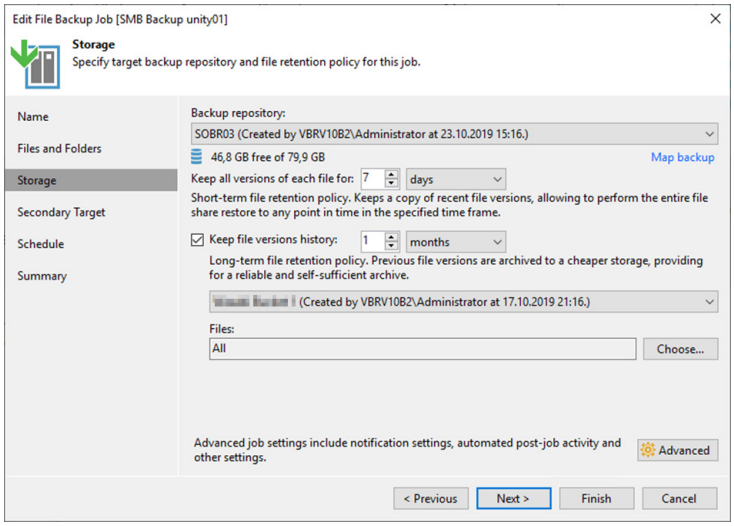


The next step gives us the option to select the server and folders we want to protect:

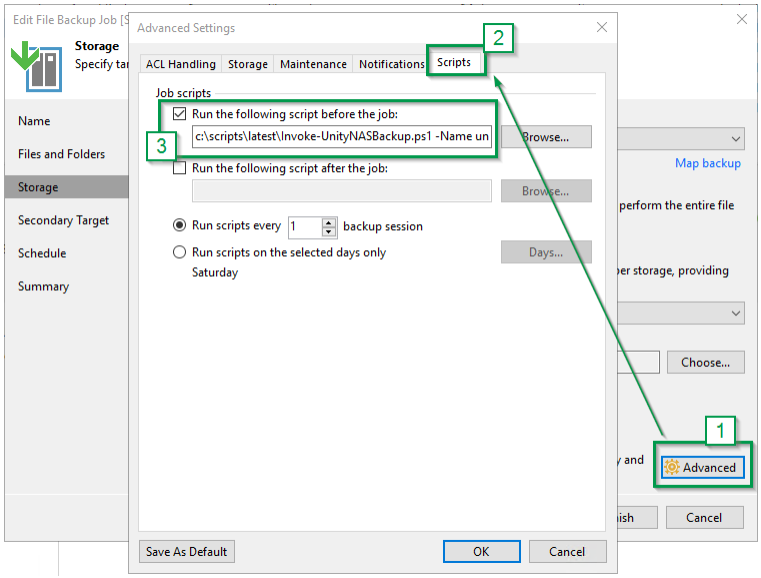


If needed, the advanced option can be used for every added folder to provide specific "include" or "exclude" masks.

In the "storage" section we define the backup repositories in which we want to store the backups for short- and long-term retention policies. To offload previous file versions to cheaper storage, enable the long-term option and select your desired repository. This can be object storage as well.



Since we want to back up from a snapshot, we need to add a script that runs at the job start and interacts with the storage. Open the advanced options and go to the "scripts" tab. Here we need to add the script to create a snapshot for the source share and provide some parameters.

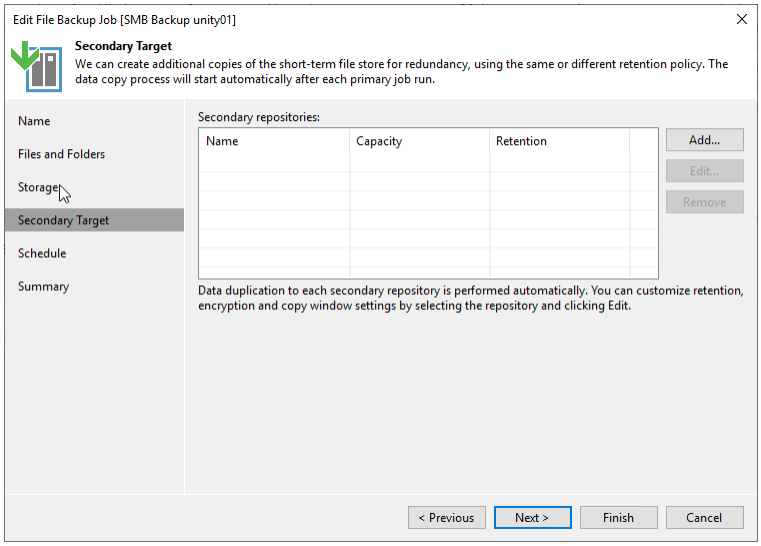


UnityName	With this parameter you specify the Unity DNS name or IP of the management interface.
UnityShare	With this parameter you specify the source SMB share.
UnityCredentialFile	This parameter is the file name of a saved credentials file for authentication.
SnapshotName	With this parameter you can change the default snapshot name “VeeamNASBackup” to your own name.
SnapExpireSeconds	Set the amount seconds after which the snapshot should expire. The default value is 172,800, which is two days.
LogFile	You can set your own path for log files from this script. The default path is the same one Veeam Backup & Replication uses (“C:\ProgramData\Veeam\Backup\UnityNASBackup.log”)

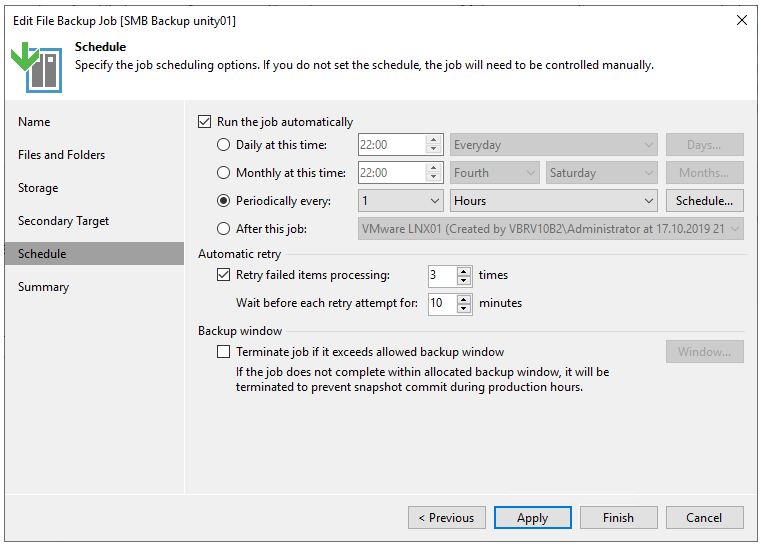
Example

c:\scripts\latest\Invoke-UnityNASBackup.ps1 -Name unityO1mgmt -Share root -CredentialFile C:\Scripts\unity-system-credentials.xml

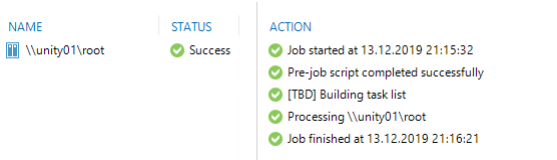
If a second copy of the short-term file store is requested, this option can be found in the “second target” window. We are skipping this here in this particular example setup.



The last page offers options for scheduling the backup job. Customize this to your needs to fulfill recovery time objectives (RTOs) and recovery point objectives (RPOs) and SLA times.



Finally, we can run the job and it should complete successfully with the pre-job script.



DellEMC² Isilon

In this example, we will discuss the option to use a snapshot of an Isilon system as a source for NAS backup. Since there is no support for remote VSS in the SMB-3 implementation at the time of writing, the solution is to create a snapshot via scripting.

Prerequisites

First, please find the PowerShell module from Christopher Banck on github (https://github.com/vchrisb/Isilon-POSH) which actually uses the RestFUL API of the Isilon to manage the system.

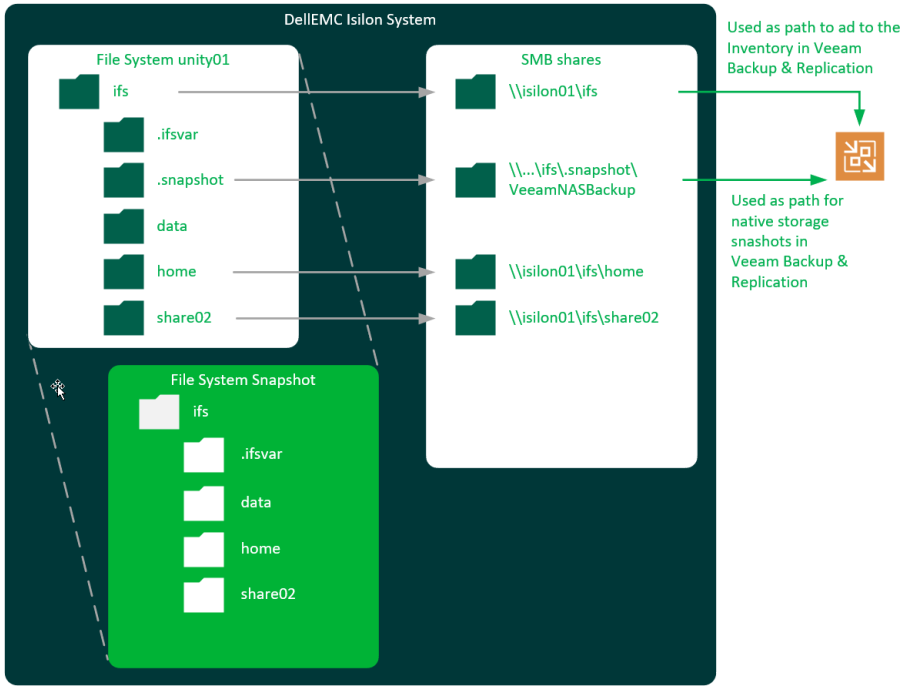
Both of his modules, the IsilonPlatform and SSLValidation, need to be present on the system where you will run the scripts. In most cases this will be:

C:\Program Files\WindowsPowerShell\Modules

The second thing you need to think of is the user account the script runs with. Since this will be triggered by Veeam Backup & Replication, the context most likely will be the system user. To be able to use encrypted credentials in an .xml file, this should be created with PSEXEC to have the decryption right for the system user. Please find instructions to create a credentials .xml file further up in this document.

Overview of snapshots with an Isilon system

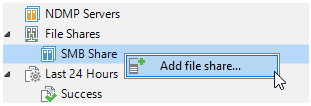
To be able to create snapshots in an Isilon system, the SnapshotIQ function must be activated. The Isilon can create snapshots on a folder-based level. To make things easier in this example, we'll use the root ifs folder to create a snapshot:



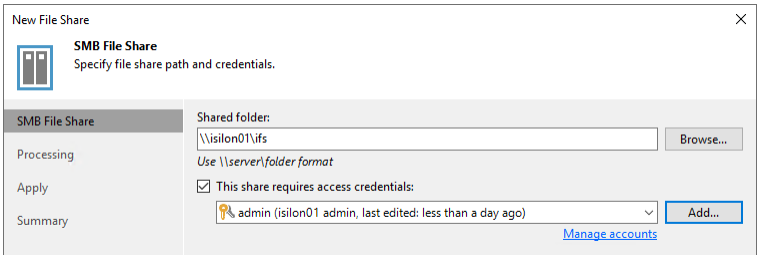
This may not be a best practice for very large systems, but it will give you the option to back up multiple shared folders within one backup job from the same snapshot.

Adding a file share

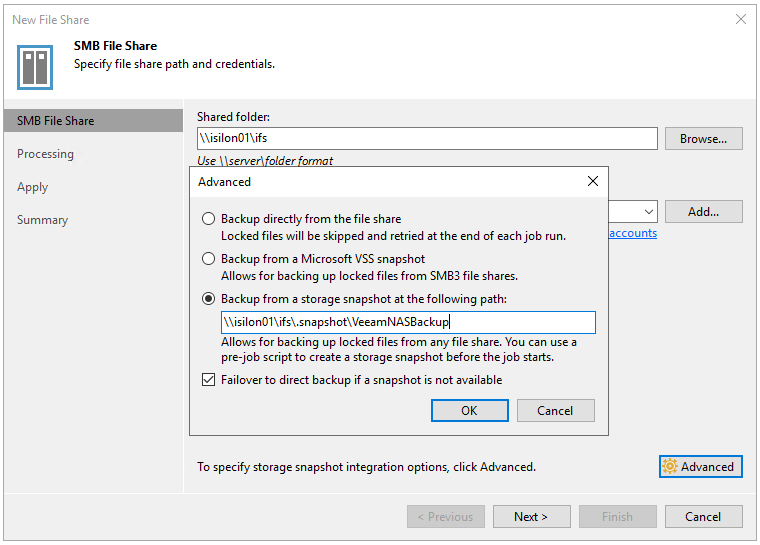
Start by adding a SMB file share in Veeam Backup & Replication:



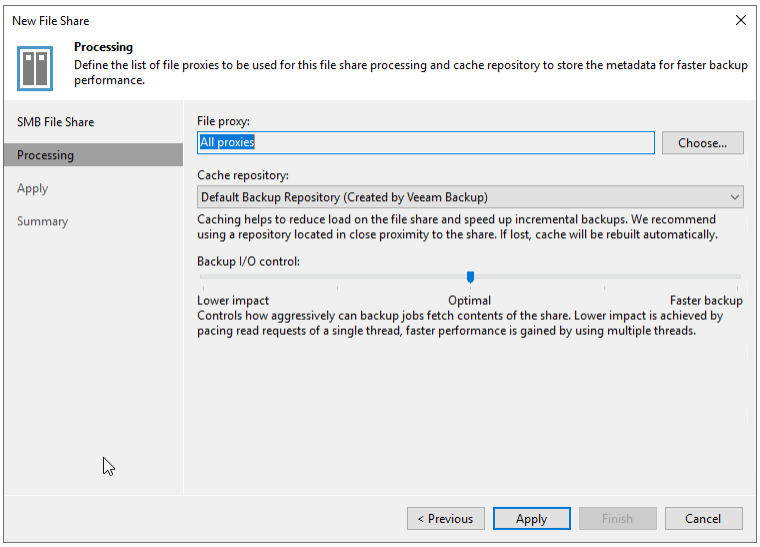
Now we need to provide the UNC path of the root share and credentials:



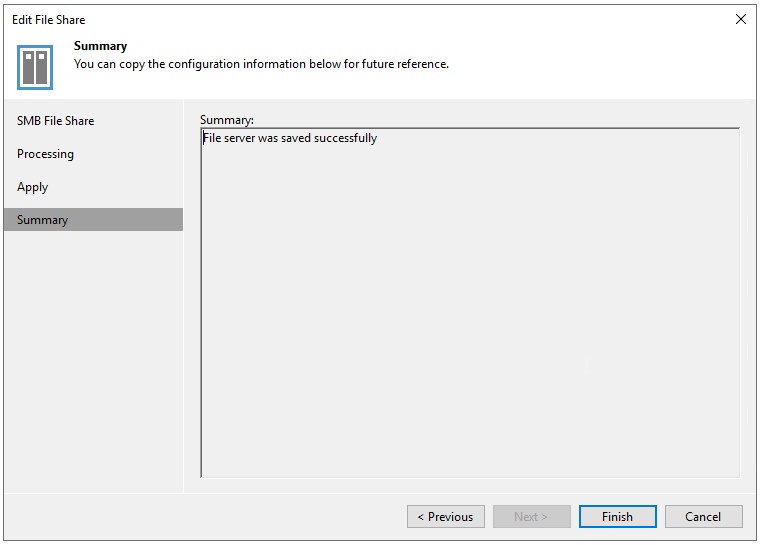
In the next step we open the advanced dialog box and provide the path to back up from native storage snapshots:



Continuing with "OK" and "next" will bring us to the settings for processing options. Here, we can define the selection of file proxies, the cache repository and settings for Backup IO control. Since this is individually related to different setups, we will keep the default values in this scenario.



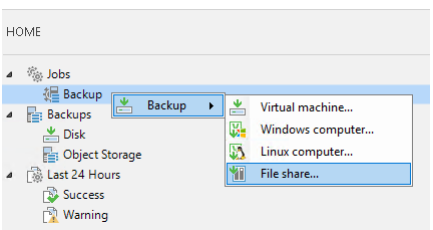
Continue to apply the settings and finish the wizard:



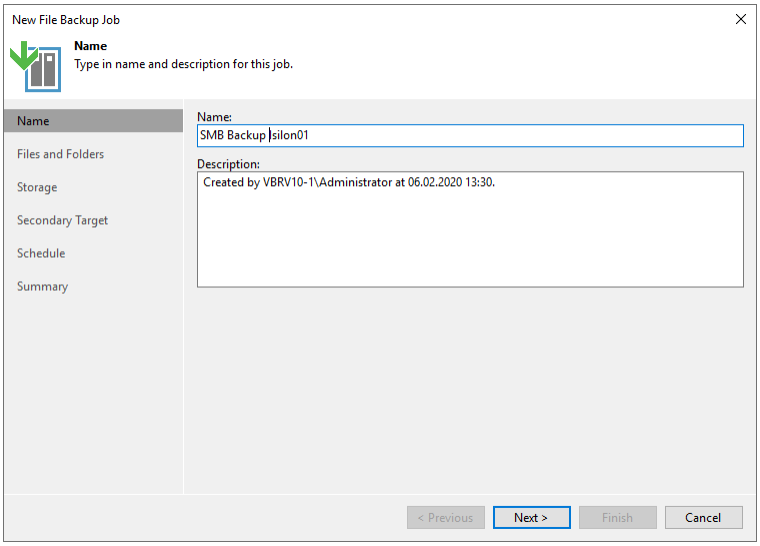
Now we have added the Isilon SMB share to the inventory and can proceed with the job creation.

Creating a backup job

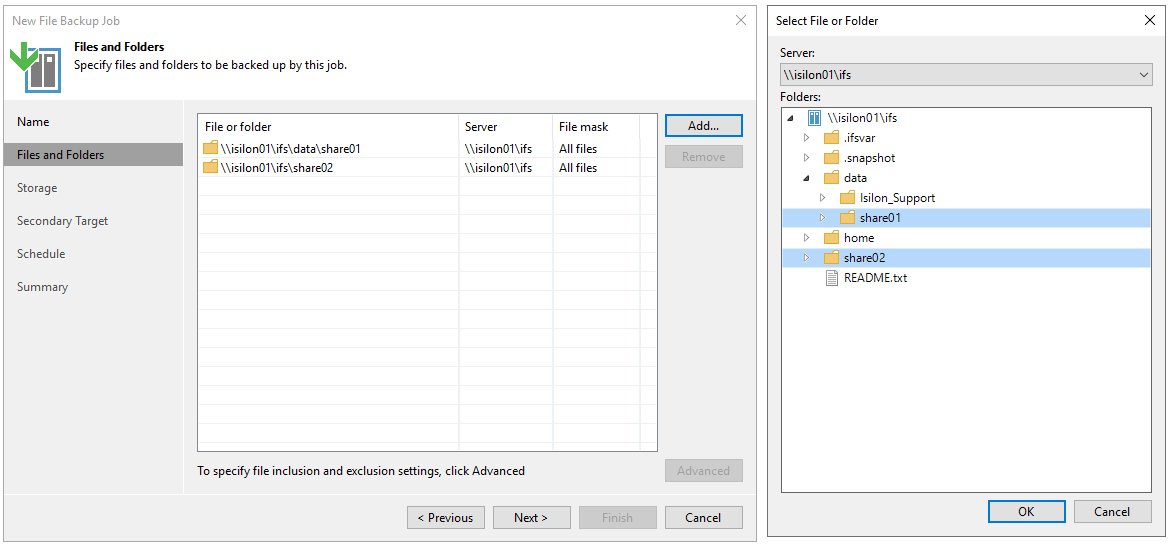
Going to the home section in Veeam Backup & Replication will give us the option to create a new backup for file shares.



Start with providing a name and description for the job:

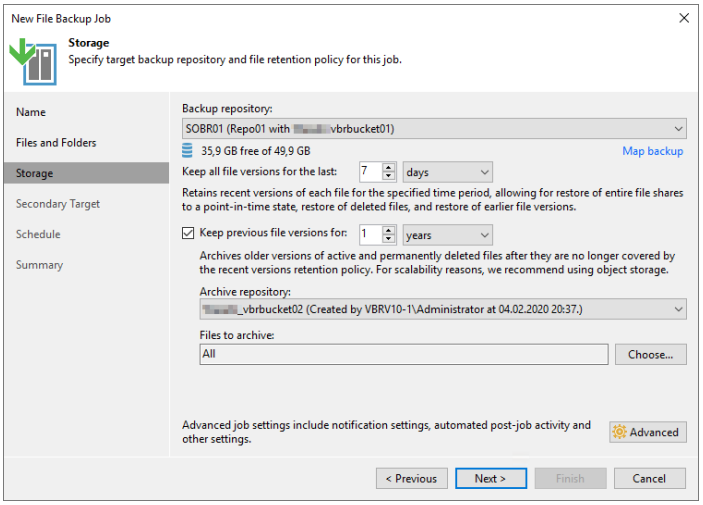


The next step gives us the option to select the server and the folders we wish to protect:

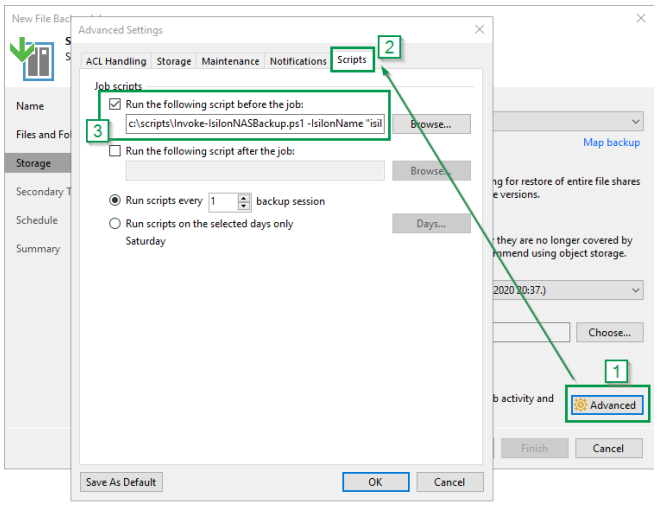


If needed, the advanced option can be used for every added folder to provide specific "include" or "exclude" masks.

In the "storage" section, we define the backup repositories to store the backups for short- and long-term retention policies. To offload previous file versions to cheaper storage, enable the long-term option and select your desired repository. This can be an object storage as well.



Since we want to back up from a snapshot, we need to add a script that runs at the job start and interacts with the storage. Open the advanced options and go to the "scripts" tab. Here we need to add the script to create a snapshot for the source share and provide some parameters.



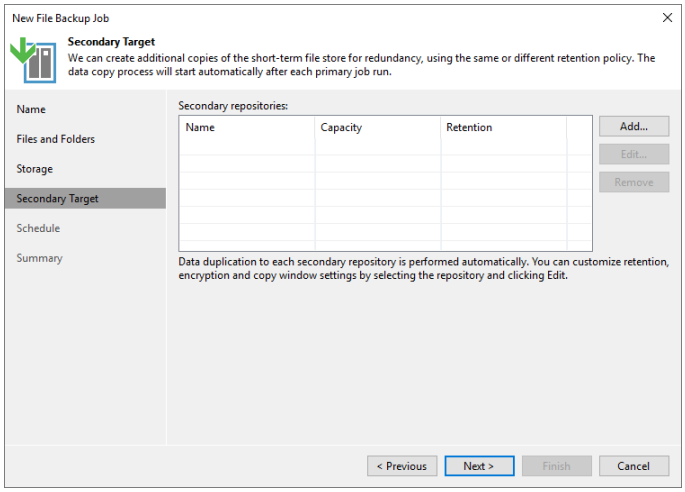
Let´s have a look at the parameter you need to run the script:

IsilonName:	With this parameter you specify the Isilon DNS name or IP.
IsilonCluster:	With this parameter you specify the cluster name of the Isilon system.
IsilonShare:	With this parameter you specify the source SMB share.
IsilonCredentialFile:	This parameter is a file name of a saved credentials file for authentication.
SnapshotName:	With this parameter you can change the default snapshotname „VeeamNASBackup" to your own name [optional].
IsilonSnapExpireDays:	Set the amount of days after which the snapshot should expire. The default value is two days [optional].
LogFile:	You can set your own path for log files from this script. The default path is the same one Veeam Backup & Replication uses by default „C:\ProgramData\Veeam\Backup" [optional].

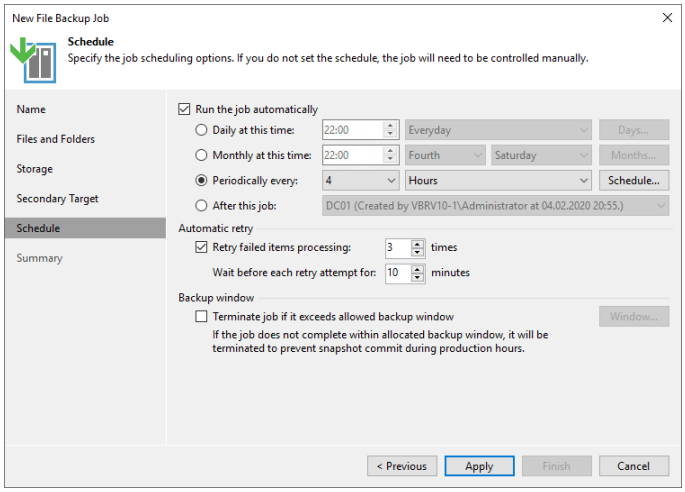
Example

c:\scripts\Invoke-IsilonNASBackup.ps1 -IsilonName "isilon01" -IsilonCluster "isilon01" -IsilonShare "ifs" -IsilonCredentialFile 'C:\Scripts\credential.xml' -IsilonSnapExpireDays "2"

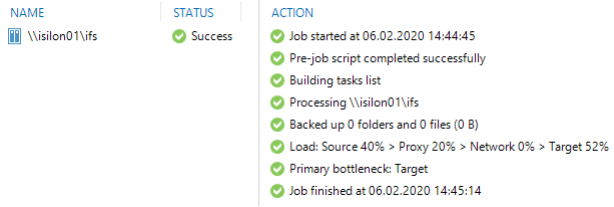
If a second copy of the short-term file store is requested, this option can be found in the following secondary target window. We are skipping this here for the current example setup.



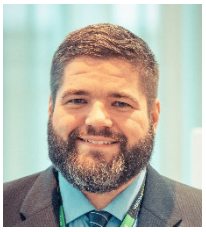
The last page offers the options for scheduling the backup job. Customize this to your needs to fulfill RTOs, RPOs and SLA times.



Finally, we can run the job and it should complete successfully with the pre-job script.



About the authors



Marco Horstmann is a senior systems engineer based near Hanover in northern Germany. He has worked 20 years in the IT industry and has installed many virtualization and storage environments based on products from VMware and NetApp before joining Veeam in 2015.

David Bewernick is a senior system engineer based in northern Germany and he helps customers to find the right Veeam solutions that fit their availability demands. He has more than 17 years of industry experience and focuses primarily on file services, virtualization and storage systems before joining Veeam in 2017.

About Veeam Software

Veeam® is the leader in Backup solutions that deliver Cloud Data Management™. Veeam provides a single platform for modernizing backup, accelerating hybrid cloud and securing your data. With 365,000+ customers worldwide, including 81% of the Fortune 500 and 66% of the Global 2,000, Veeam customer-satisfaction scores are the highest in the industry at 3.5x the average. Veeam's global ecosystem includes 70,000+ partners, including HPE, NetApp, Cisco and Lenovo as exclusive resellers. Headquartered in Baar, Switzerland, Veeam has offices in more than 30 countries. To learn more, visit https://www.veeam.com or follow Veeam on Twitter @veeam

VEEAM

Cloud Data

Backup for what's next

5 Stages of Cloud Data Management — start your journey today!

Learn more: veeam.com