Veeam and Pure Storage

Integrated Deployment Guide

1 + 1 = 3
Pure Storage + Veeam
Better Together

Contents

Introduction

In this deployment guide, we guide you through the installation of the Veeam® and Pure Storage integrated solution. Starting with Veeam Backup & Replication™ 9.5 update 3, new integrated features are available for Pure Storage systems by installing the Pure Storage Plugin. The integration features are:

- Backup from Storage Snapshots
- Veeam Explorer™ for Storage Snapshots
- Veeam DataLabs™ for Storage Snapshots

This streamlined guide will help with your installation, for more detailed installation instructions, leverage the following guide:

Veeam Backup & Replication User Guide for VMware vSphere

Veeam summary

Veeam Availability Suite™ combines the industry-leading backup, restore and replication capabilities of Veeam Backup & Replication with the advanced monitoring, reporting and capacity-planning functionality of Veeam ONE™. Veeam Availability Suite delivers everything you need to reliably ensure and manage your **VMware vSphere environment**. The Veeam agentless design provides multiple backup options. Features such as source-side deduplication and compression, change block tracking, parallel processing and automatic load balancing provide the fastest, most efficient backups possible.

Pure Storage summary

Pure Storage helps companies push the boundaries of what's possible. Pure's end-to-end data platform — including FlashArray, FlashBlade and a converged offering with Cisco, FlashStack — is powered by innovative software that's cloud-connected for management from anywhere on a mobile device and supported by the Evergreen business model. The company's all-flash-based technology, combined with its customer-friendly business model, drives business and IT transformation with solutions that are effortless, efficient and evergreen. With Pure's industry-leading Satmetrix-certified NPS (net provider score) of 83.7, Pure customers are some of the happiest in the world, and include organizations of all sizes, across an ever-expanding range of industries.

Veeam's Pure Storage integration (vSphere only)

Create fast backups from storage snapshots for quick and efficient item-level recovery; leverage Pure Storage snapshots and replicated snapshots to create a robust, enterprise-level data protection solution. Veeam Backup & Replication lets you leverage Pure Storage snapshots as a part of a comprehensive backup and recovery strategy, where snapshots and image-level backups complement each other. With Veeam Backup & Replication, you can:

- Perform backups from Pure Storage snapshots
- Restore data directly from Pure Storage snapshots

Veeam Backup & Replication pre-installation considerations

The following requirements are necessary for the installation of Veeam:

- Veeam Availability Suite 9.5 Enterprise Plus License Key
- Veeam Availability Suite 9.5 Installation ISO
- Pure Storage Plugin
- Available Windows server with the following:

1. 64-bit OS
2. X86-64-processor with 4 cores minimum
3. Recommended 12 GB RAM plus 2 GB RAM, per concurrent task
4. 2 GB of available disk space for installation

- Available HBA for direct storage fabric connection (10 Gb e/FC) and network connectivity
- Purity, version 4.8 or higher

Install Veeam Backup & Replication 9.5

To install Veeam Backup & Replication 9.5, follow these steps:

1. Log into the available Windows server as a user with Local Administrator privileges.
2. Mount the installation image using disk image emulation software, or burn the iso image to a blank CD/DVD.
3. After you mount or insert the disk with Veeam Backup & Replication setup, **Autorun** will open a splash screen with installation options. If **Autorun** is not available or disabled, run the **Setup.exe** file from the CD/DVD disk. Alternatively, you can right-click the new disk in **My Computer** and select **Execute Veeam Backup & Replication Autorun**, or simply double-click the new disk to launch the splash screen.

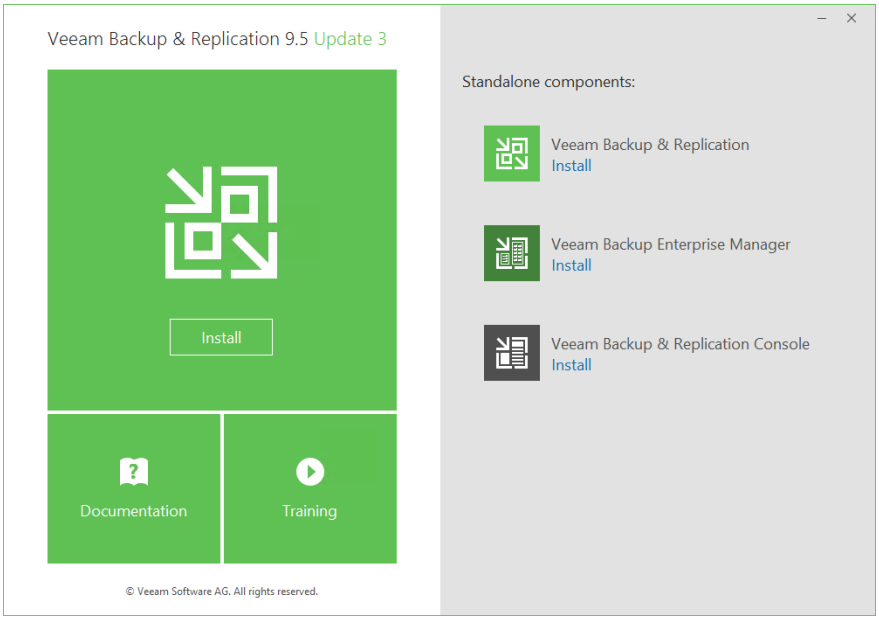

Figure 1: Veeam Backup & Replication installation splash screen

4. Click the **Install** link in the **Veeam Backup & Replication** section of the splash screen.
5. At the **Welcome** step of the wizard, click **Next** to start the installation.
6. To begin the installation, you must accept the license agreement. Read the license agreement, select the **I accept the terms in the license agreement** option and click **Next**.

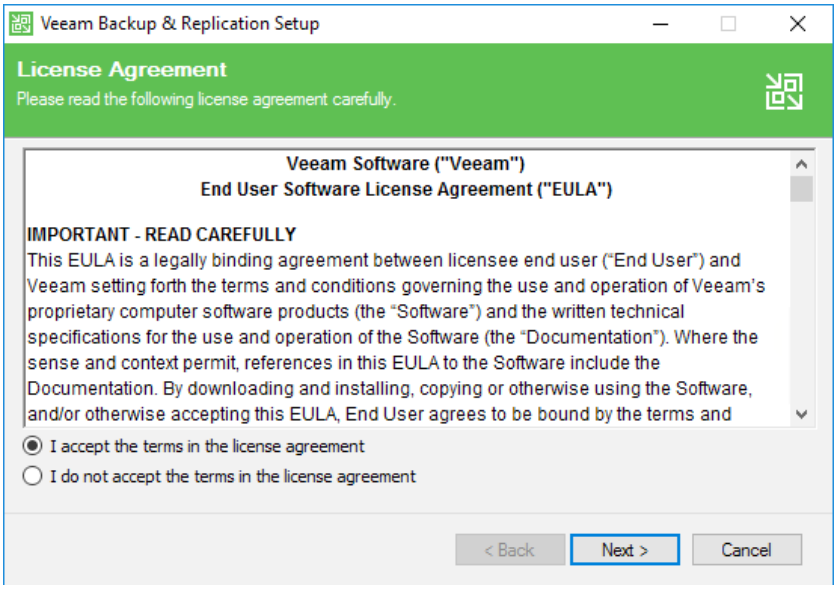

Figure 2: Veeam EULA

7. You can install Veeam Backup & Replication with a trial license that was sent to you after registration or a full purchased license. To install a license, click Browse and select a valid license file for Veeam Backup & Replication.

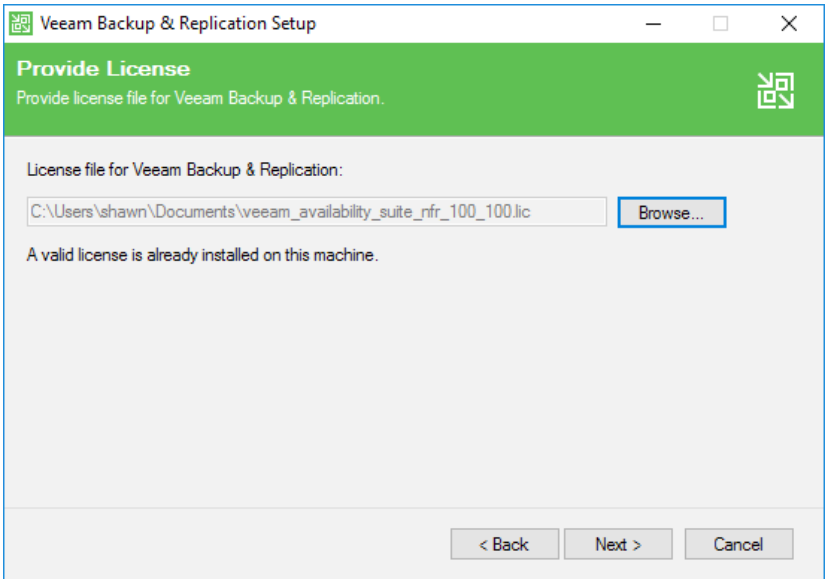

Figure 3: Veeam License File Selection

8. Select the components you want to install. The Veeam Backup & Replication setup includes the following components:

- **Veeam Backup & Replication**
- **Veeam Backup Catalog** responsible for indexing VM guest OS files
- **Veeam Backup & Replication Console**

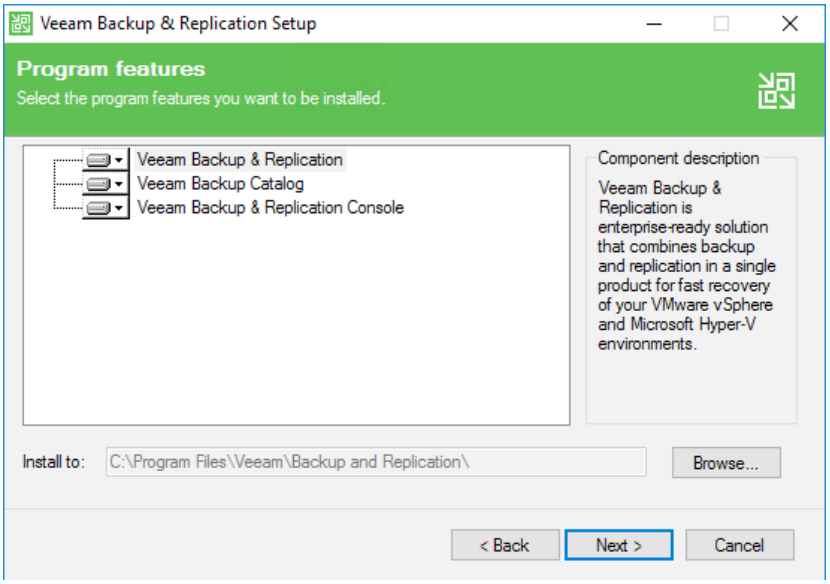

Figure 4: Setup options

9. Before proceeding with the installation, the setup wizard will perform a system configuration check to determine if all prerequisite software is available on the machine. If some of the required software components are missing, the wizard will offer to install missing software automatically.

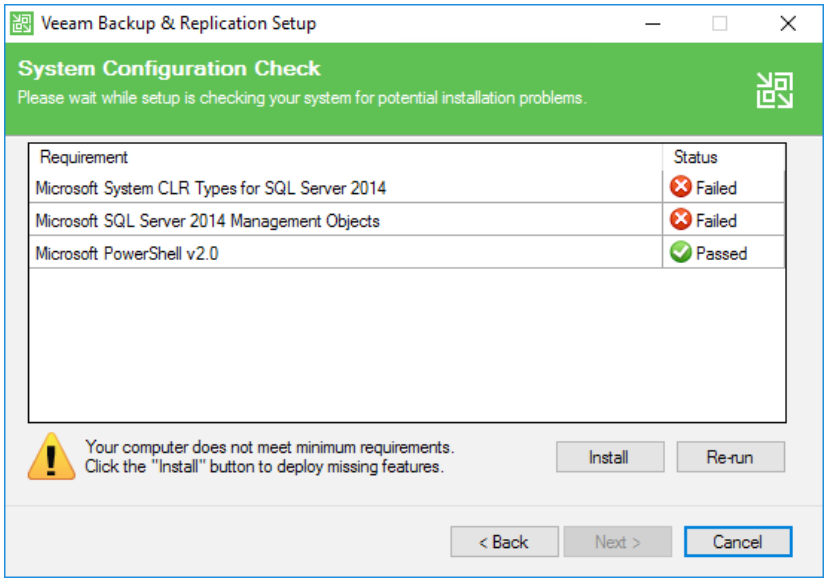

Figure 5: Pre-installation system configuration check

10. Choose to accept the recommended default settings or check the box Let me specify different settings. Checking the box to specify your own settings will enable you to customize your Veeam installation. If you go with the default settings, click **Install** and proceed to the next section. If you chose to specify your own settings, you can check the box to customize the configuration.

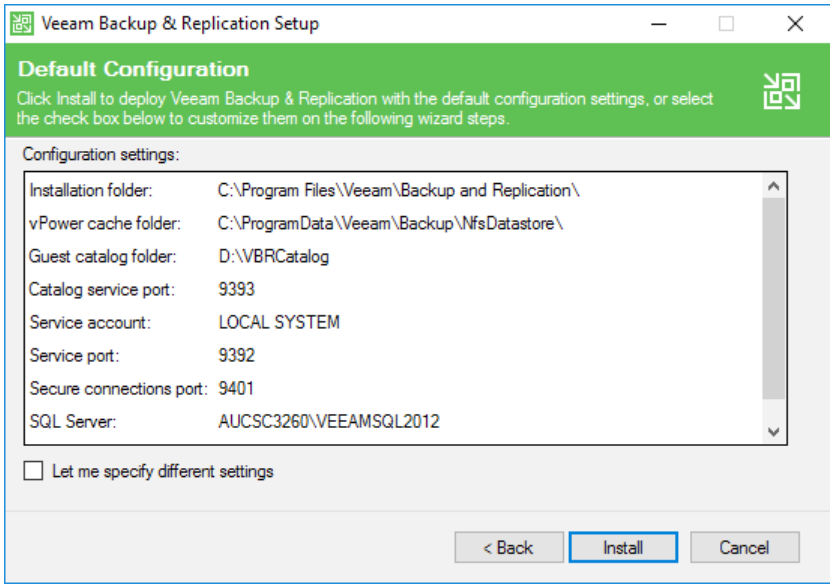

Figure 6: Default configuration

11. You can go back, review and modify previous steps using the **Back** button. If you are sure that all settings are configured correctly, click **Install** to begin the installation. When the installation completes, click **Finish** to exit the setup wizard. You can now start Veeam Backup & Replication.

12. Install the Pure Plugin. Run the .exe and click **Next** to begin installation.

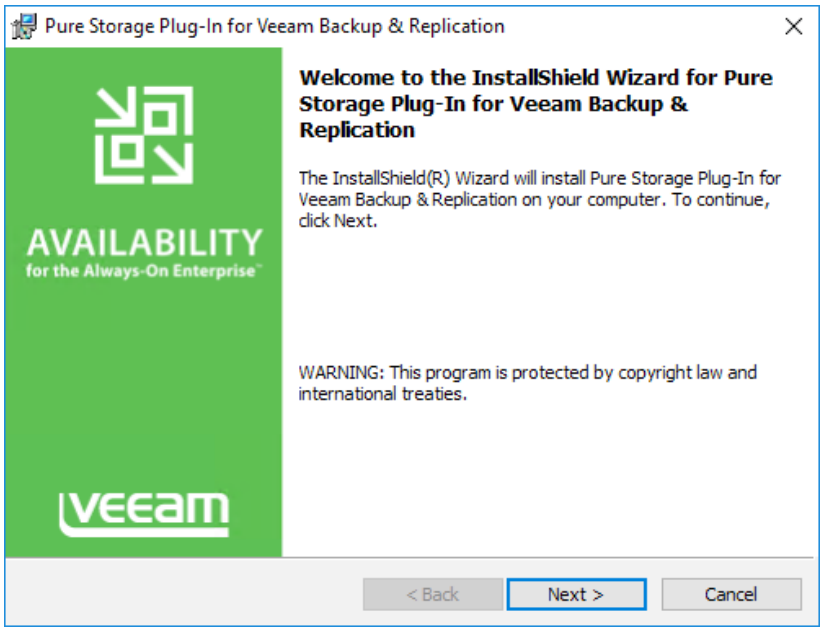

Figure 7: Plugin install wizard

13. Accept the **Terms of Usage** and click **Next** to continue.

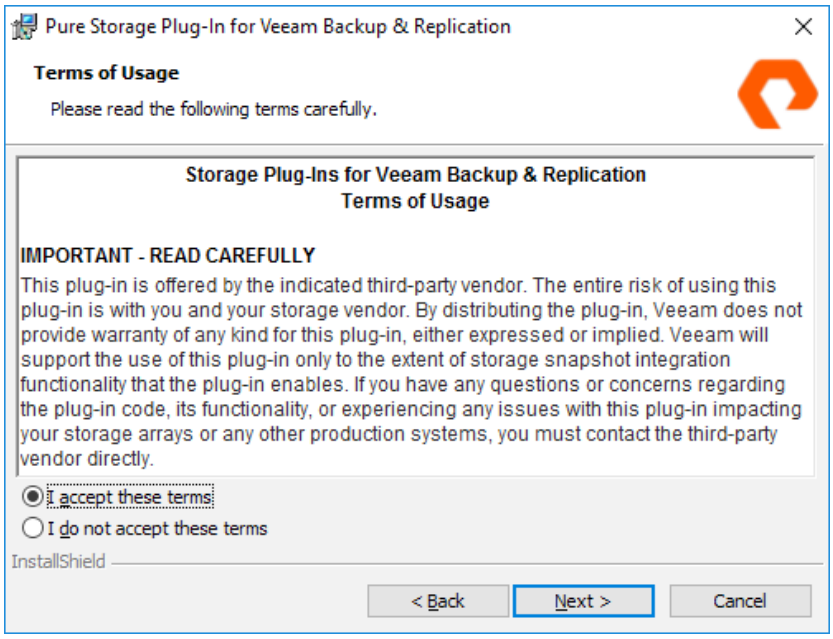

Figure 8: Accept terms

14. Click **Install** to begin the installation process.

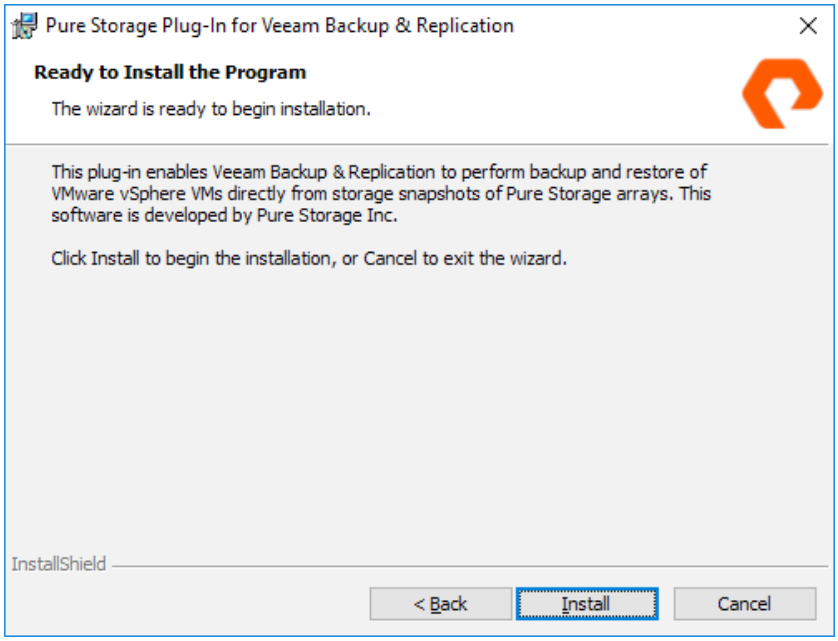

Figure 9: Ready to Install

15. Once the installation complete, click **Finish** and continue to the next section.

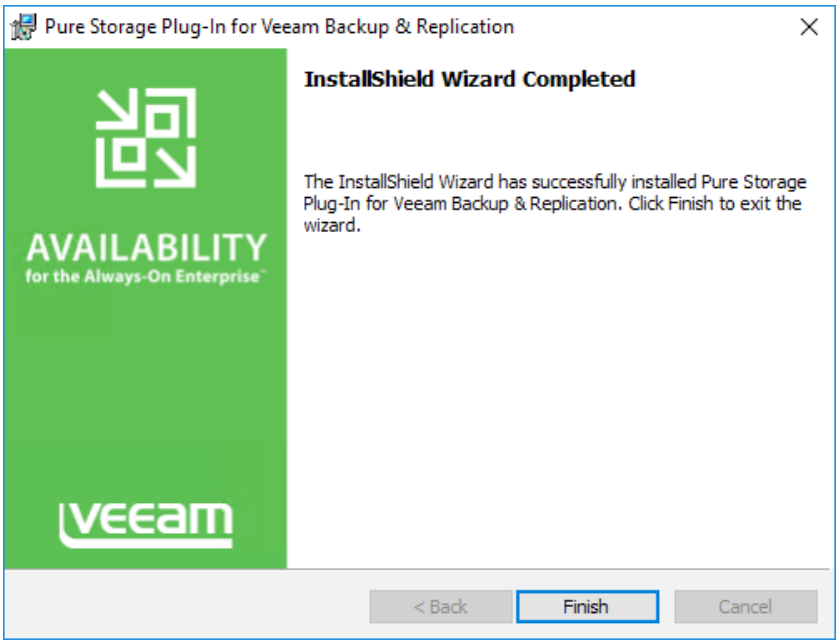

Figure 10: Installation complete

Veeam Backup & Replication configuration

Now that Veeam Backup & Replication is installed, launch the application directly from the desktop icon. Once launched, the following configurations are required:

- Backup Infrastructure including vSphere infrastructure, backup repositories and configuration backups
- Install Pure Storage Plugin
- SAN Infrastructure to allow for integration with the Pure Storage system

Adding the Infrastructure

1. For building your backup infrastructure in a VMware vSphere environment, Veeam Backup & Replication supports the following types of servers:

- VMware Server
- Windows Server
- Linux Server
- vCloud Director

Veeam Backup & Replication allows you to connect both vCenter servers and standalone ESX(i) hosts. If possible, avoid adding ESX(i) hosts, which are part of the vCenter Server hierarchy. Add the corresponding vCenter Server instead. Adding the vCenter Server facilitates management of the backup infrastructure and can be a recommended condition for certain types of operations (such as Quick Migration).

Server Type	Source Host	Target Host	Backup Proxy	Backup Repository
VMware vSphere Server (standalone ESX(i) host or vCenter Server)	●	●	○	○
VMware vCloud Director	●	○	○	○
Microsoft Windows server	○	○	●	●
Linux server	○	○	○	●

Figure 11: Server types

2. To add a VMware server, open the **Backup Infrastructure** view and launch the **Add Server** wizard.

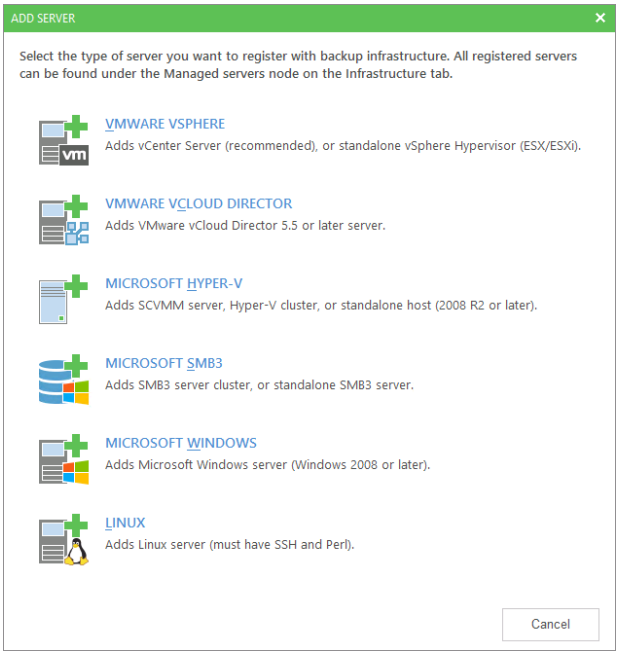

Figure 12: Add Server Wizard

3. Once the **Add Server** wizard is launched, select the first option for VMware vSphere.

4. Enter the DNS name or IP address of the VMware Server. A description can be entered for future reference. The default description will include information about the user who added the server, as well as the date and time when the server is added. When done, click **Next**.

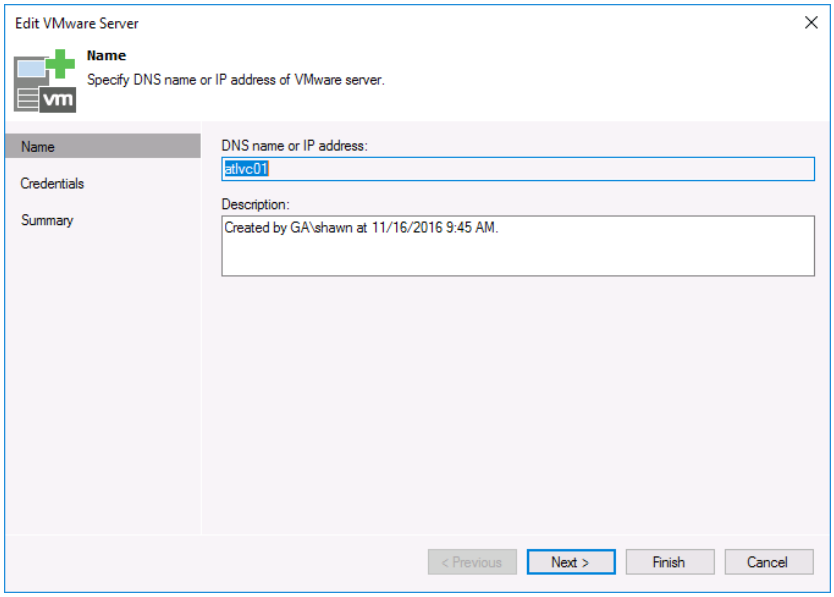

Figure 13: New VMware Server

5. The **Credentials** are next. On this screen, click **Add** to input new credentials. It is recommended that vCenter Admin be used if adding a vCenter Server, and root credentials for standalone ESX(i) hosts. **NOTE:** The username of the account should be provided in the **DOMAIN\USERNAME** format. Click **Next** to proceed.

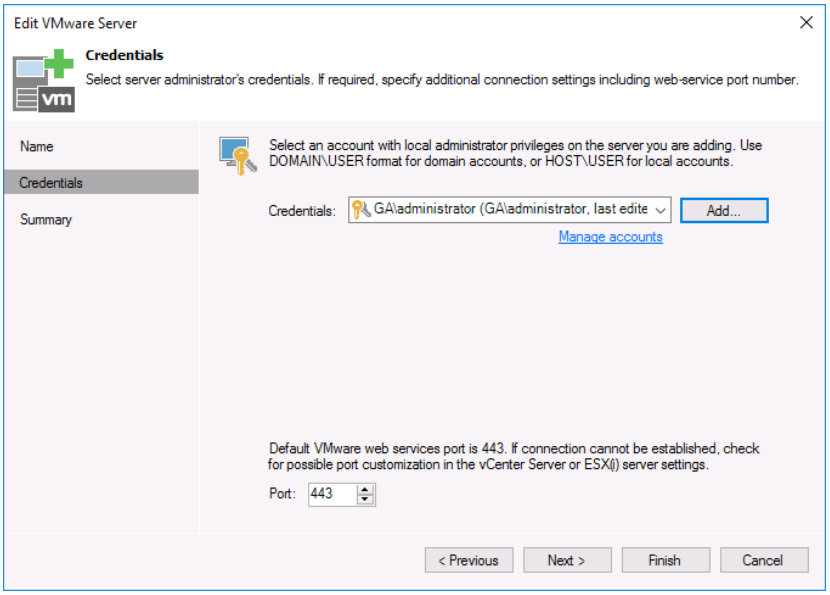

Figure 14: Credentials

6. On the **Summary** screen, review the configuration information and click **Finish** to exit the wizard.
7. You can repeat these steps for any additional VMware servers, Windows servers, Linux servers, or vCloud Director servers you add. **NOTE:** The steps for servers other than VMware are not identical, but they are very similar. At this point, add any Windows or Linux servers you wish to use as a backup repository (backup repositories are the locations where you wish to house your backup files).

Adding additional backup repositories

By default, Veeam automatically creates a local backup repository on the C:\ drive of the Veeam Backup & Replication server. This is not always the best location for your backup files. You can create additional repositories using the steps below.

1. Open the **Backup Infrastructure** view, click on the **Backup Repositories** node in the inventory pane and click **Add Repository** on the ribbon.
2. Specify a name for the repository and provide a description for future reference. By default, the description contains information about the user who created the backup repository, as well as the date and time when the repository was created.
3. Next, choose the type of repository you would like to add, the four options are **Microsoft Windows server**, **Linux server**, **Shared folder** and **Deduplicating storage appliance**.

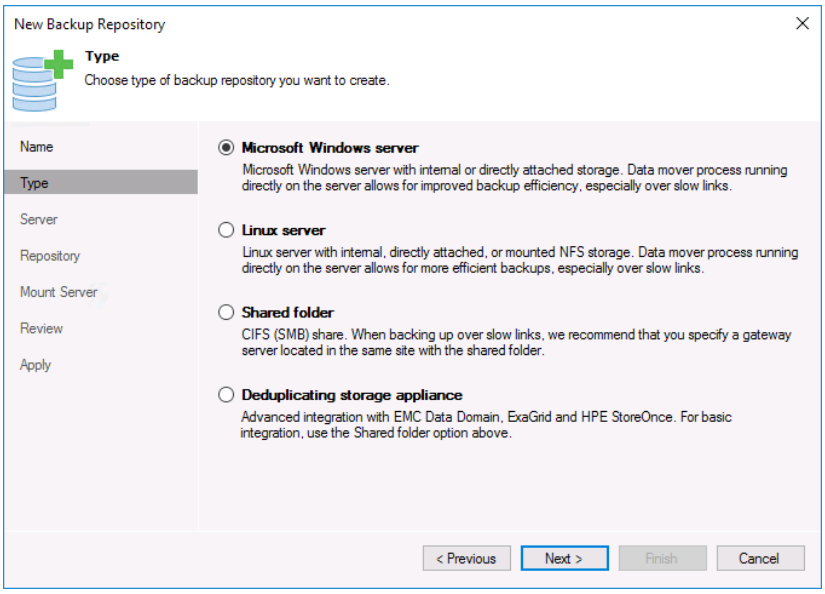

Figure 15: Backup repository types

4. This step depends on the type of backup repository selected. If **Microsoft Windows** server or **Linux server** are selected, follow step 5. If a **Shared folder** is selected, skip to step 6.

5. From the **Repository server** list, select the Windows or Linux server to be used as a backup repository. The **Repository server** list contains only servers that have been added to the **backup infrastructure** beforehand. If a server needs to be added at this point, **Add New** can be selected. Click **Populate** to see a list of the volumes connected to the selected server, their capacity and free space. Click **Next** once the selections are made and skip to step 7.

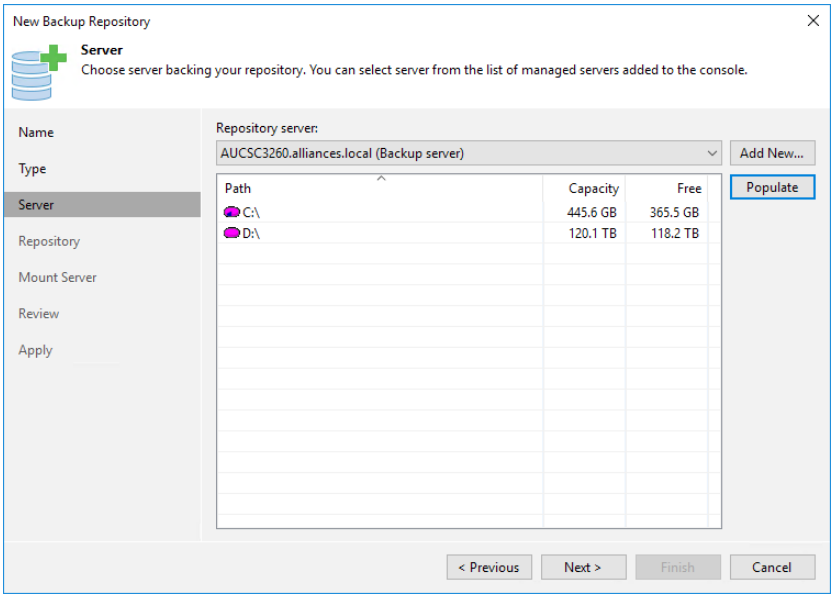

Figure 16: Repository server selection

6. In the **Shared folder** field, specify the UNC path to the shared folder. Select credentials of an account with administrative privileges on the share. Click the **Manage accounts** link at the bottom of the list or click Add on the right to add the necessary credentials. Next, specify the way in which VM data should be written to the shared folder, **Directly from the backup server** or **Through the following Gateway server**. **NOTE:** A Gateway server is highly recommended if this repository is off site. Click **Next** when finished.

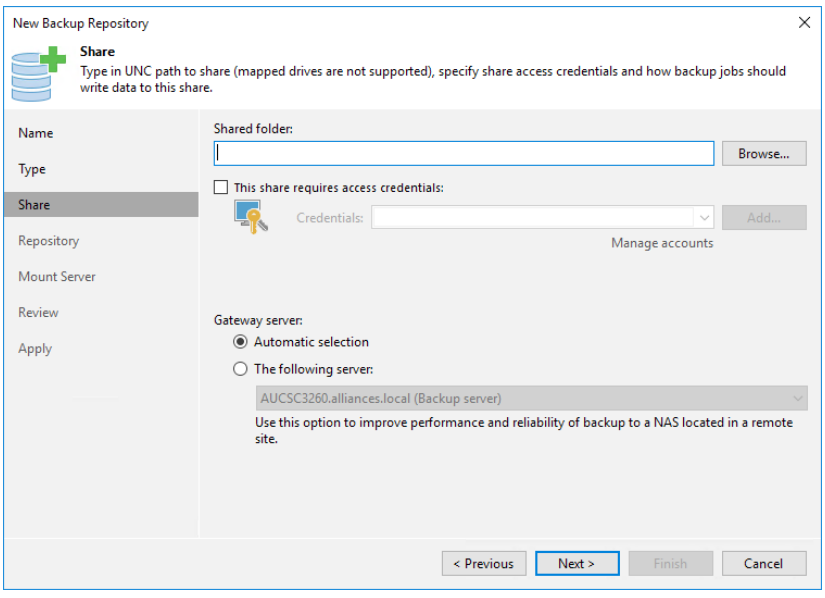

Figure 17: Shared folder configuration

7. In the **Location section**, specify the path to the folder where back-up files should be stored. Click Populate to see the capacity and available free space on the selected partition. In the Load control section, set the necessary values to limit the number of concurrent jobs for the repository. You can also limit the data ingestion rate to restrict the total speed of writing data to the repository disk.

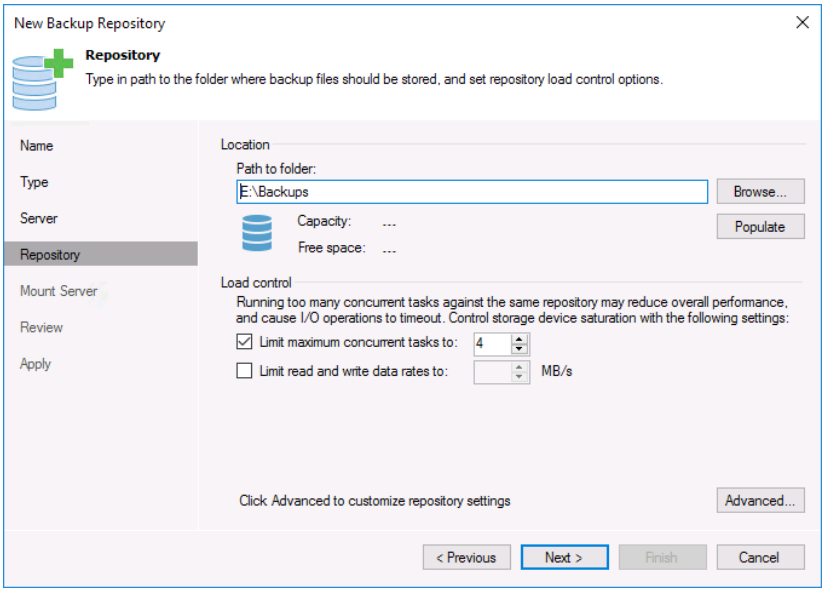

Figure 18: Location and load control configuration

8. If a deduplicating storage appliance or rotated drives will be used, click **Advanced...** to configure additional repository settings. This menu also contains the option to select **Use per-VM backup files**. If these settings are not needed, click **Next** to proceed and skip to step 11.**NOTE:** Follow the Veeam best practices guide for your specific deduplication appliance.

9. For storage systems using a fixed block size, select the **Align backup file data blocks** check box. Veeam will align VM data saved to a backup file to a 4 KB block boundary. This option provides better deduplication across backup files, but can result in a greater amount of unused space on the storage device and a higher level of fragmentation.

10. When compression is enabled for a backup job, VM data is compressed at the source side. However, compressing data prior to writing it to a deduplication storage appliance results in poor deduplication ratios as the number of matching blocks decrease. To overcome this situation, select the **Decompress backup data blocks before storing** check box. If you are using rotating drives for this repository, select **This repository is backed by rotated hard drives**. After your selections are made, click **OK** to accept these settings and then click **Next** to proceed.

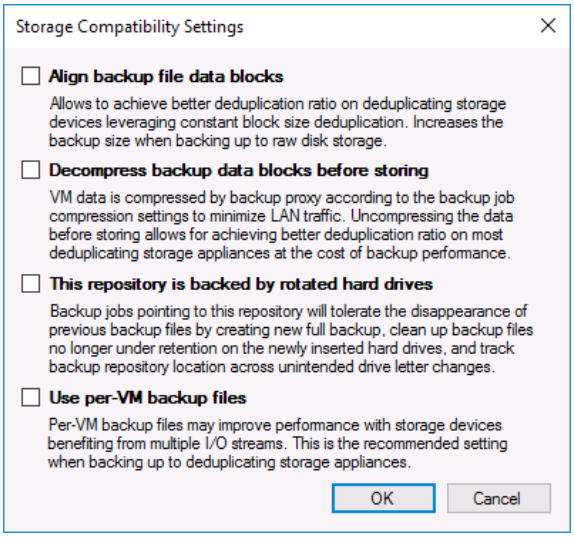

Figure 19:Deduplicating storage compatibility settings

11. Select the **Enable vPower NFS server on the mount server (recommended)** check box to make the repository accessible by the vPower NFS service. You can select any Windows server from the list or choose the **Add Server** option to assign this role to a Windows server not currently added to the console. In the **Folder** field, browse and specify the folder where the instant VM recovery write cache will be stored. This volume should have at least 10 GB of free disk space.

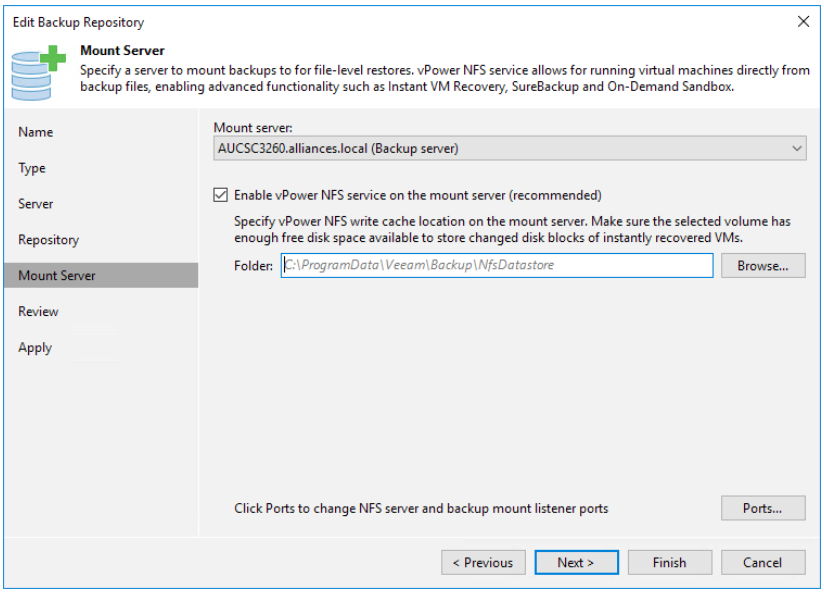

Figure 20: Mount server and vPower NFS configuration

12. To change the default port setting for the vPower NFS and other related components, there are two options listed the bottom right of the screen. Click **Manage** to open the **Network Settings** window and customize network ports for individual components. Click **Ports** to open the **Ports Settings** window and customize the ports for the vPower NFS service. When completed, click **Next** to proceed.

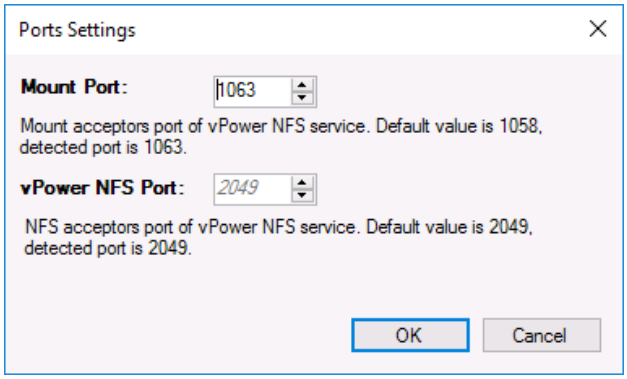

Figure 21: vPower NFS port settings

13. After the wizard checks for existing components, you can review the repository properties and installed components. Click Previous to change any of the properties or click **Next** to proceed and apply these properties.

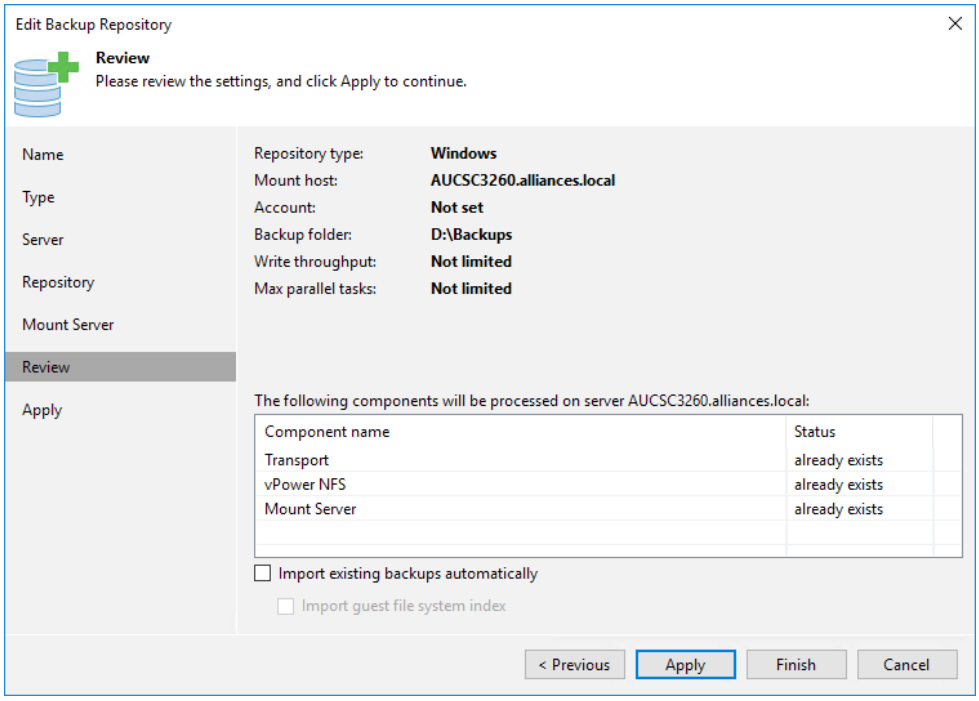

Figure 22: Review repository properties

14. Real time processing results will be displayed in the log. Wait for the required operations to be performed. When the wizard finishes adding the backup repository, you can review the log information. Click **Finish** to exit the wizard.

Configuration backups

Veeam Configuration Backups export the configuration data from the Veeam Backup SQL database and saves the data in a backup file on a repository. If the Veeam backup server fails for some reason, you can re-install the Veeam backup server and then quickly restore its configuration from the backup file. Alternatively, you can apply the configuration of one Veeam backup server to any other Veeam backup server in your backup infrastructure. It is recommended that your regularly create a configuration backup for every Veeam backup server in your backup infrastructure. Periodic configuration backups will reduce the possibility of data loss and minimize administrative overhead if any problem with the backup server(s) occur.

When a configuration backup is performed, Veeam retrieves configuration data for the Veeam backup server from the SQL database. It then writes this data into a set of **.xml files** and archives these **.xml** files to a **.BCO** file.

By default, Veeam is configured to create a configuration backup daily and store it to the default backup repository: the **C:\backup\VeeamConfigBackup\%BackupServer%** folder on the Veeam backup server. However, for security's sake, it is recommended that you store configuration backups on a backup repository ***other*** than the default repository. In this case, the Veeam backup server configuration data will be available for recovery even if the Veeam backup server fails. The following steps outline the scheduling of configuration backups:

1. From the main menu of Veeam Backup & Replication, choose **Configuration Backup**.
2. Make sure that the **Enable configuration backup to the following repository**: check box is selected in the **Export Configuration** window.
3. From the **Backup repository** list, choose the repository to which the configuration backup should be written to. **NOTE:** It is highly recommended that the selected repository NOT reside on the Veeam Backup Server.
4. In the **Schedule** section, click **Configure** and specify the time schedule per when the configuration backup should be created.
5. In the **Retention policy** section, specify the number of configuration backups to keep on the disk.
6. **Encrypt configuration backup** can be also be enabled by checking the box and providing a password to unencrypt the backup.

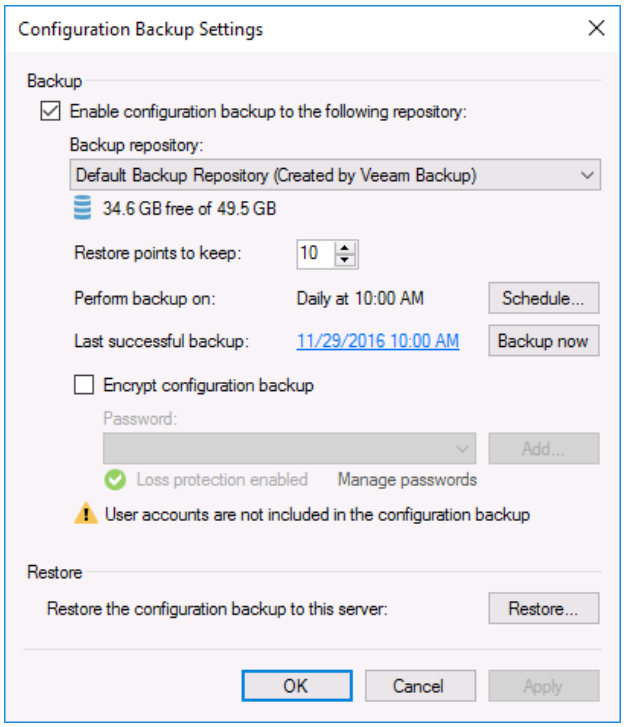

Figure 23: Configuration backup settings

Adding Veeam proxy access to Pure Storage Array

1. For iSCSI, **make sure that the iSCSI service is running on the Veeam Proxy Server**. Once you add the Pure FlashArray(s) into the Veeam Console, Veeam will automatically create the necessary connections. The iSCSI service must be running before you add the FlashArray(s) within the Veeam console.
2. For FC, it is necessary to create these connections manually.
3. Log into the Pure Storage dashboard, select **Storage —> Hosts**

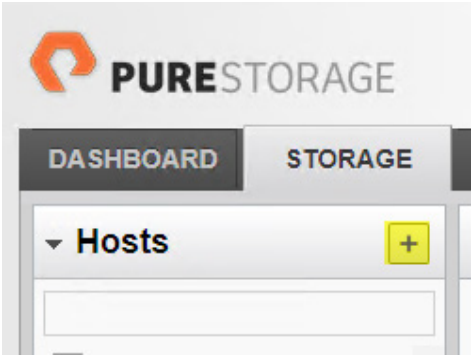

Figure 24: New FC host configuration

4. For an FC host, type the name in the **Name** field and click Create. If more than one host is needed, click the C**reate Multiple**... button.

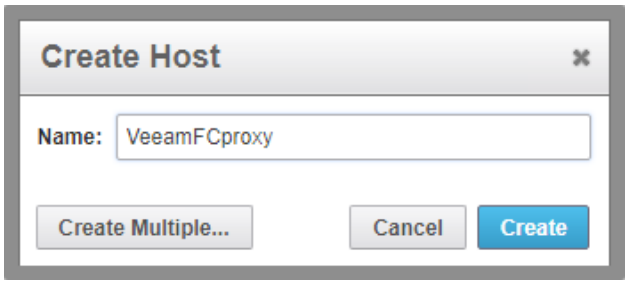

Figure 25: Create host(s)

5. Under the **Host Ports (0)** tab, click the drop-down button below the tab and to the right and select the option: **Configure Fibre Channel WWNs**.

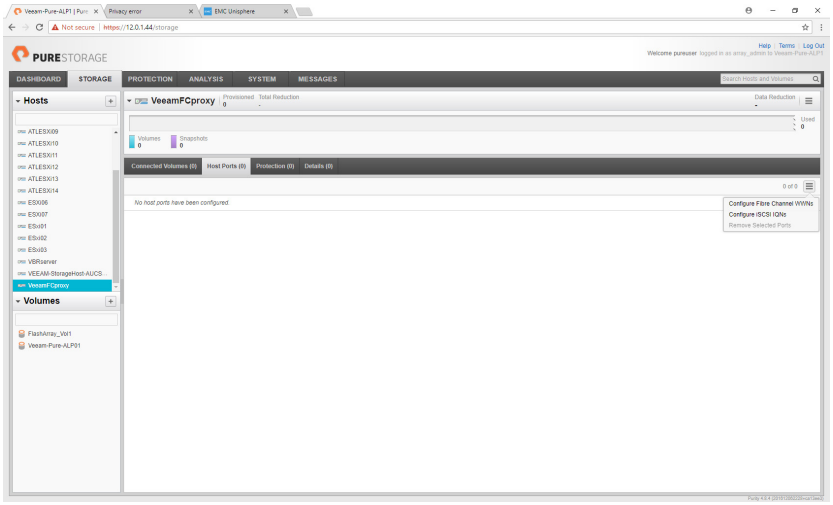

Figure 26: Configure FC WWNs

6. Select **Enter WWNs Manually**.

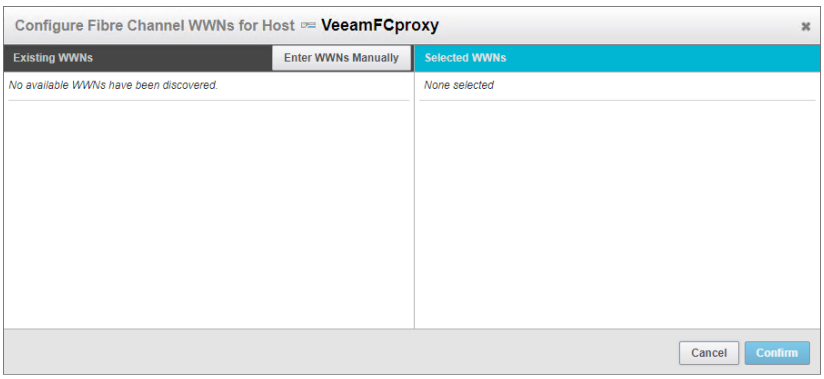

Figure 27: Enter WWNs Manually

7. In the pop-up box, enter the WWN of the proxy server that needs access in the Port **WWNs** field and click **Add**.

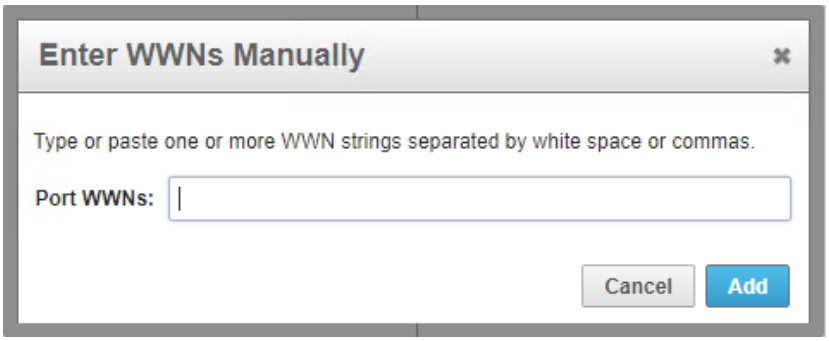

Figure 28: Add WWN

8. Select **Connected Volumes** and click on the menu in the upper right corner.
9. Select the **Connect Volumes** tab.

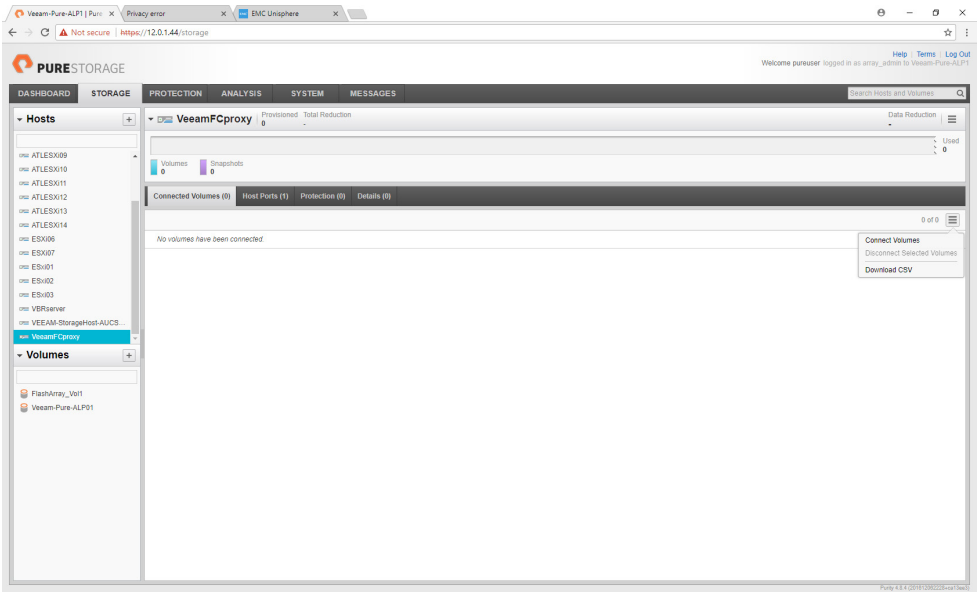

Figure 29: Connect volumes

10. Select from the existing volumes and click Confirm when complete.
11. Repeat all steps above for other Pure Storage arrays in the environment. It is important that Veeam Proxy Servers have access to leverage storage snapshots for backup, restore and sandbox functions.

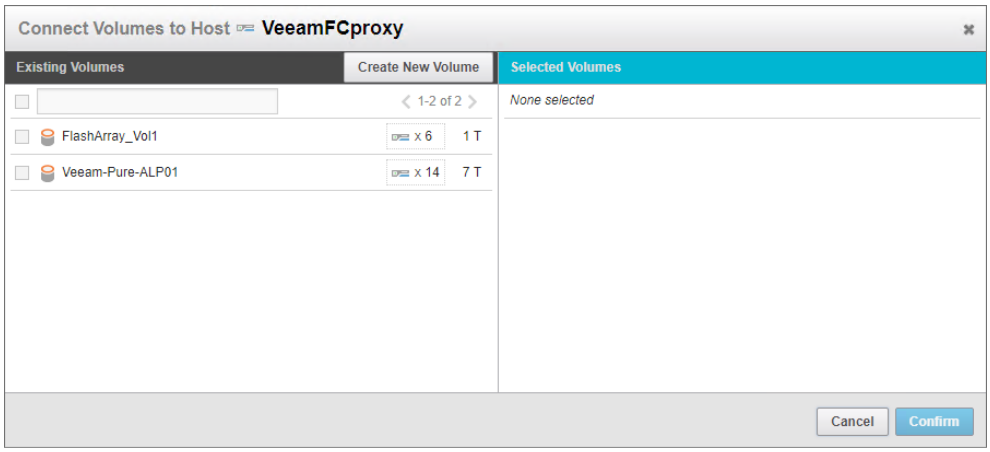

Figure 30:

Adding the SAN Infrastructure

Veeam Backup & Replication lets you leverage Pure Storage snapshots as a part of a comprehensive backup and recovery strategy, where Pure Storage snapshots and image-level backups complement each other. With Veeam Backup & Replication, you can:

- Perform backups from Pure Storage snapshots
- Restore data directly from Pure Storage snapshots
- Perform snapshots-only backups (Snapshot Orchestration)

Before working with Pure Storage snapshots in Veeam Backup & Replication, the backup infrastructure must be properly configured:

1. The Veeam backup server's proxy component is used for re-scanning VMFS on Pure Storage volumes and for performing backup from Pure Storage snapshots. For the proxy component to perform these functions, it must meet the following requirements:

iSCSI protocol

The backup proxy must have a Microsoft iSCSI Software initiator enabled. Backup from storage snapshots requires the Microsoft iSCSI initiator. iSCSI traffic between the backup proxy and storage system must be allowed.

Fiber Channel protocol

The proxy server must have a fiber channel adapter installed and configured, have access to the Pure Storage array through the fiber channel fabric and be zoned to the fiber channel switch. The backup proxy must be registered with a WWN on the Pure Storage array.

2. To start using storage snapshots for backup and restore, the Pure Storage system must be added to Veeam. To do so, open the **SAN Infrastructure** view, click **Add Storage**.

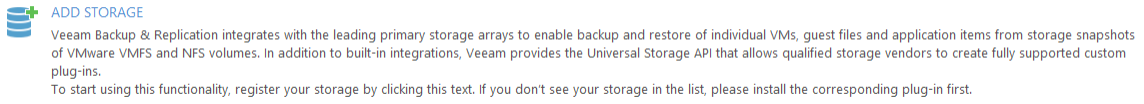

Figure 31: Adding storage

3. From the storage vendors list, select **Pure Storage**.

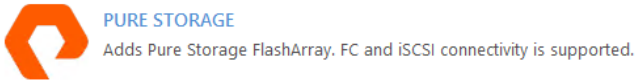

Figure 32: Pure Storage

4. In the **Name** step of the wizard, specify the name and description for the Pure Storage system in the **DNS name or IP address**: field.

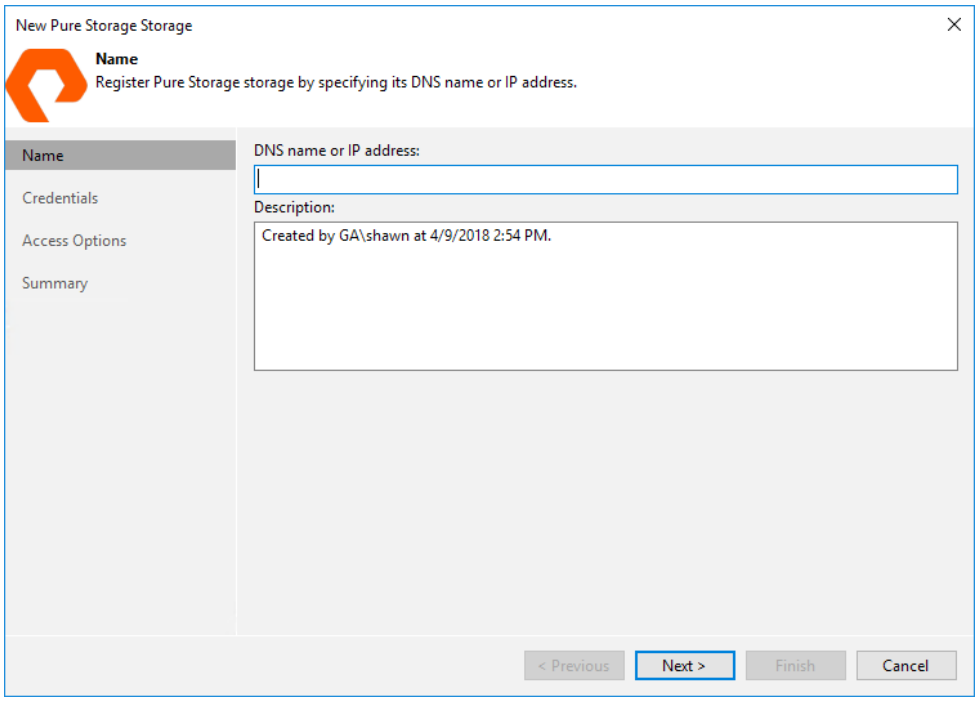

Figure 33: DNS or IP

5. In the Description field, provide a description for future reference. The default description contains information about the user who added the Pure Storage system and the date and time when the storage system was added. Once the description is complete, click **Next**.

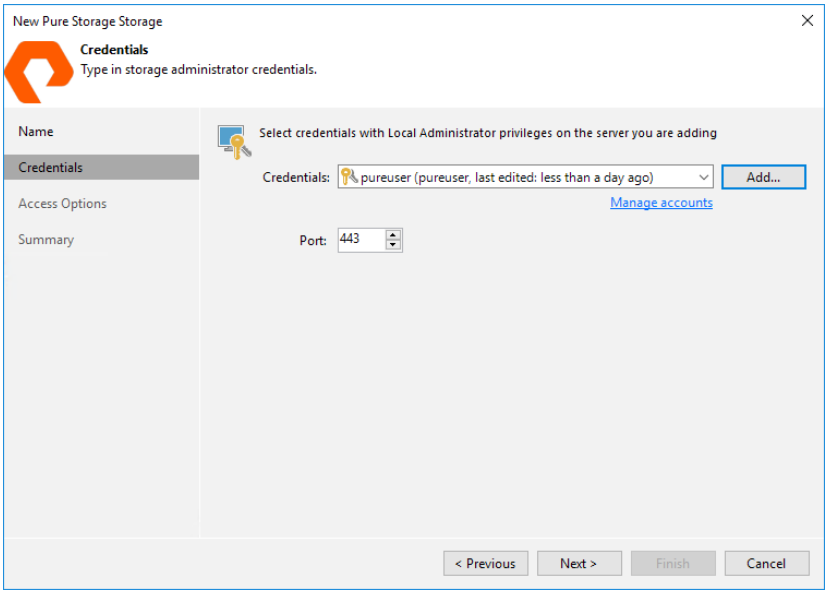

Figure 34: Pure Storage access credentials

6. Next, from the **Credentials** list, select the credentials for the user account to connect to the Pure Storage system. If the necessary credentials are not set up beforehand, click the **Add** button to the right or the **Manage accounts** link below to add the necessary credentials. **NOTE:** The account selected must have administrative privileges on the Pure Storage system.

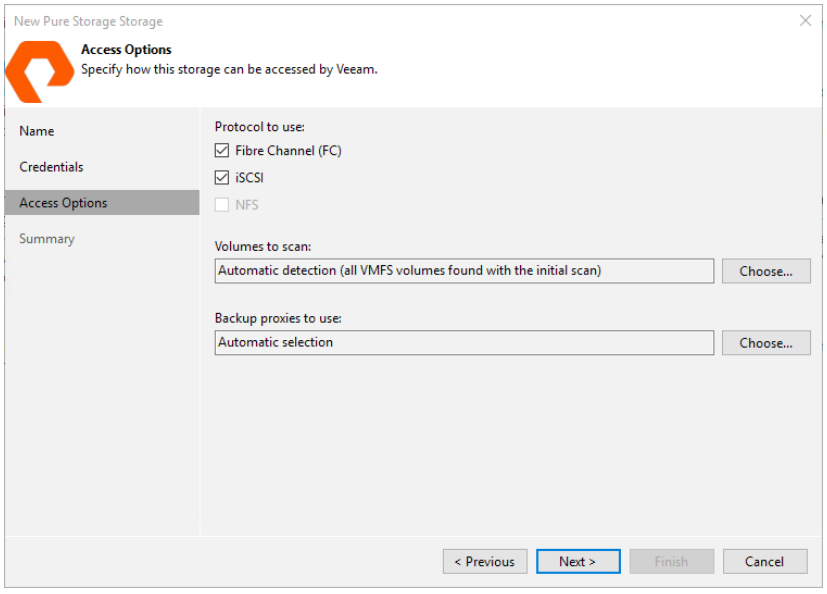

Figure 35: Access options

7. From the **Protocol to use** list, check the type of protocol over which Veeam will back up data from the Pure Storage system.

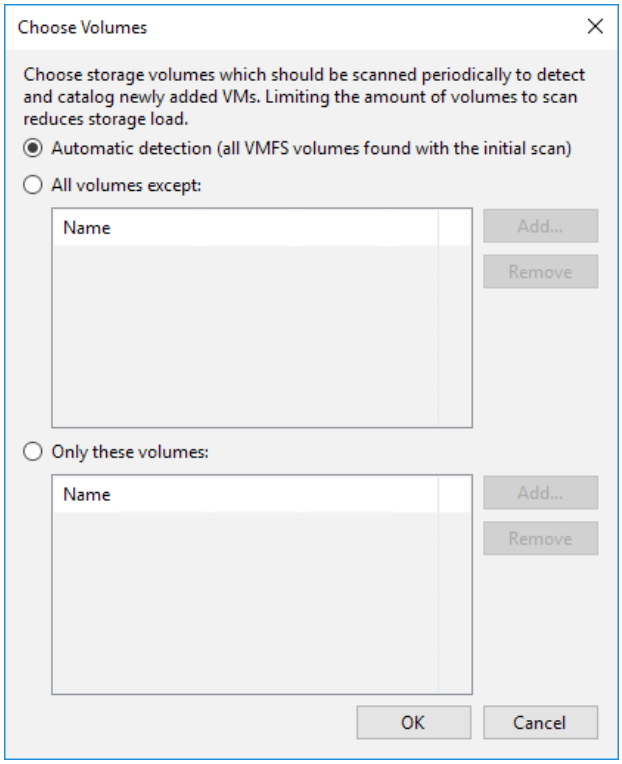

Figure 36: Choose volumes

8. The **Volumes to scan** option allows for customization of the volumes Veeam will scan for VMs and existing snapshots. It is highly recommended this selection be made if you have volumes that contain non-VM data.

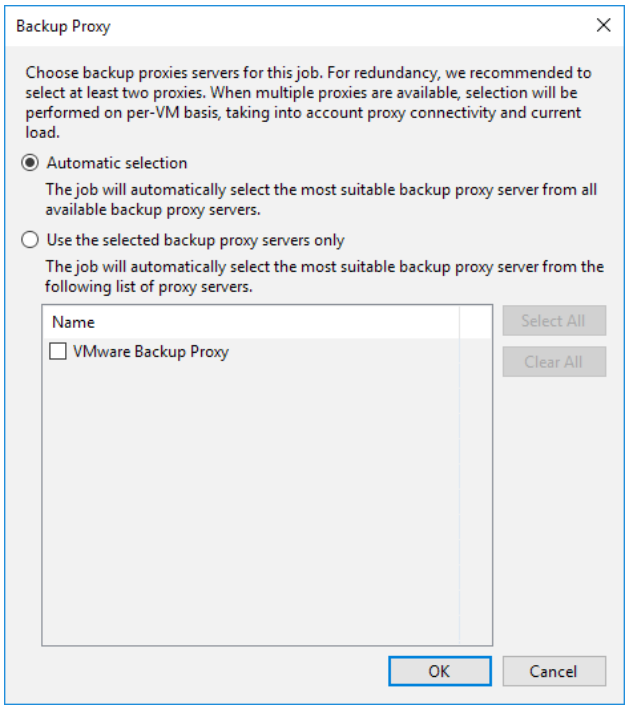

Figure 37: Backup proxy selection

9. The **Backup Proxy** selection can also be important if you have multiple locations and multiple Pure Storage arrays to manage. Proxies can be assigned to specific Pure Storage arrays to keep volume rescans and other management operations local to the storage.

10. Review the summary information and click **Finish**. After you click **Finish**, Veeam will perform the Pure Storage discovery operation; it will rescan the storage LUNs and locate VM files on them.

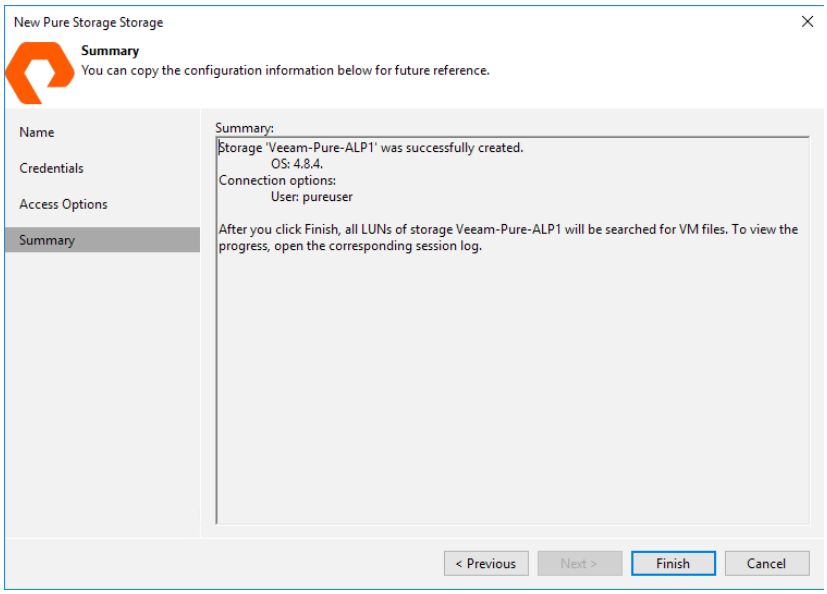

Figure 38: New Pure Storage

11. The details of the rescan process are displayed in the **System** window. This window can be closed and a review of the rescan details can be accessed later in the **History** view of Veeam Backup & Replication. Click **Close** once the discovery is completed.

12. Storage rescans will be performed automatically. Veeam will discover new volumes and snapshots or remove deleted volumes and snapshots from the storage system hierarchy. If necessary, a storage rescan can also be initiated manually.

13. To perform a manual, rescan of the storage system, follow these 4 steps:

a. Open the **SAN Infrastructure** view.

b. In the inventory pane, expand a tree of the storage system to rescan.

c. Select the necessary node in the storage system hierarchy: storage system, volume and so on.

d. Click **Rescan** on the ribbon. Alternatively, you can right-click the necessary node in the hierarchy and select **Rescan**.

Creating and deleting Pure Storage snapshots

Creating and deleting storage snapshots can be performed from the Veeam Backup & Replication interface. Create/delete snapshot operations do not differ from create/delete snapshot operations performed via the Pure Storage dashboard, and any snapshots created manually will be crash-consistent.

Creating a volume snapshot:

1. Open the SAN Infrastructure view.
2. In the inventory pane, expand a tree of the necessary storage system.
3. Right-click the necessary volume and select Create Snapshot.
4. In the New SAN Snapshot window, specify a name for the created snapshot and provide a snapshot description.

Deleting a volume snapshot:

1. Open the SAN Infrastructure view.
2. In the inventory pane, expand a tree of the necessary storage system.
3. Right-click the necessary snapshot and select **Delete Snapshot**.

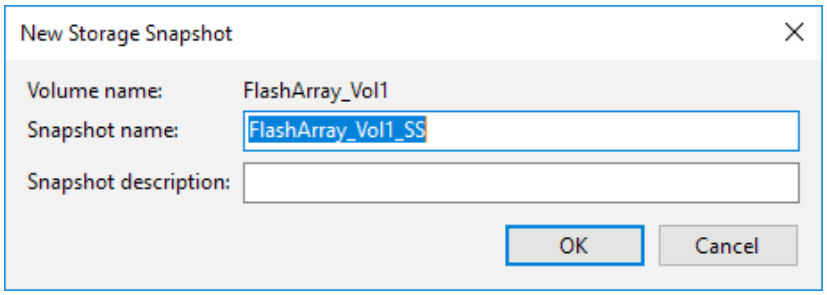

Figure 39: Manual snapshot creation

Performing backup from Pure Storage snapshots

Backup jobs can be configured to use Veeam Backup from Storage Snapshot technology, which leverages Pure Storage system snapshots for backup operations. Instead of reading data from VMware VM snapshots, Veeam reads data from storage snapshots, which speeds up backup operations and improves recovery point objectives (RPOs). Veeam is also able to orchestrate snapshots between Pure Storage arrays without taking a backup. Combining snapshot orchestration along with backups can offer more aggressive RPOs.

Backup from Storage Snapshots: Backup job creation

1. To create a backup from storage snapshots job, select **Backup & Replication** under the **Home** tab. Click on the **Backup Job** button to begin.
2. The **New Backup Job** wizard will pop up. Start by giving the job a Name. Below the job name is the Description box. By default, this box will be populated with the user who created the job along with a date and time stamp. Optionally, additional text can be added. Click Next to move on.

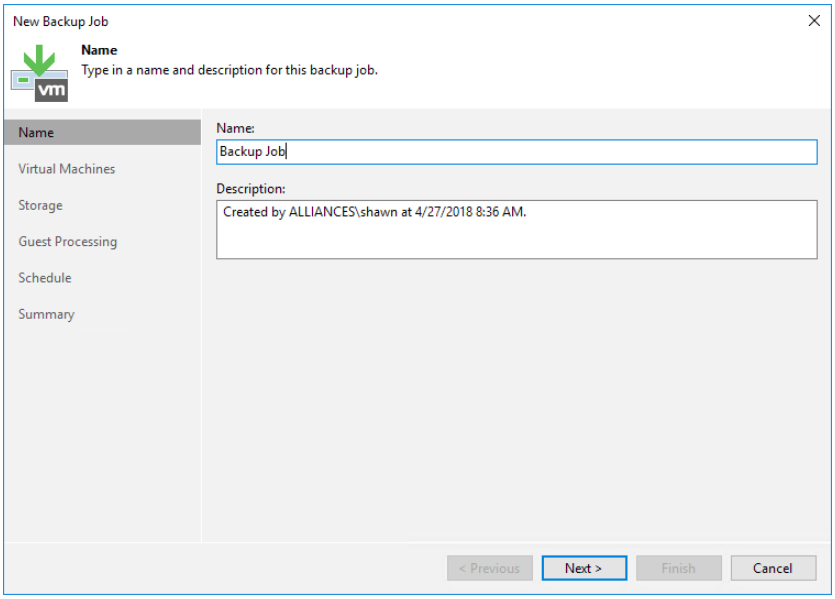

Figure 40: New backup job wizard

3. The next step is to add virtual machines to the job. Start by clicking **Add**. The **Add Objects** window will open. There are multiple options for adding virtual machines into the backup job. Virtual machines can be selected individually or an entire container can be selected. Some of the options are entire hosts, clusters, datastores, folders and VM tags. Since this job will be leveraging volume snapshots on the Pure Storage array, a recommendation is based on the datastore. Click **Add** to add the virtual machines and then **Next** to move on.

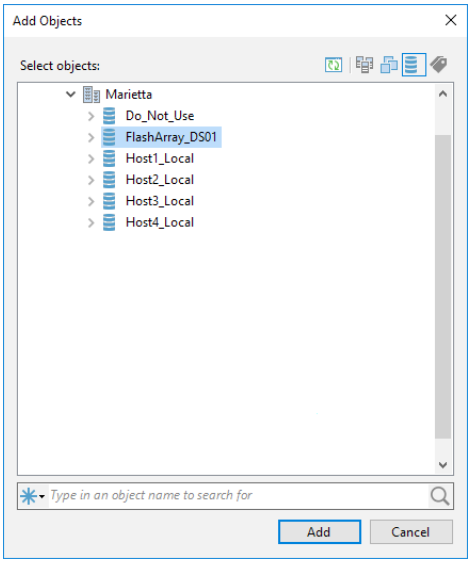

Figure 41: Add virtual machines

4. **Storage** options will allow you to select a specific proxy to leverage for the backup, but by default the **Backup proxy** will be selected automatically. **Backup repository** can be selected by clicking on the drop-down button for the location where the newly created backup files will be stored. **Retention policy** will allow for specifying the desired number of restore points to retain. There is also an option to **Configure secondary destinations for this job**, if this option is selected, a new menu will be available for selecting the secondary destination. Secondary destinations can include a backup copy job, tape job or a secondary Pure Storage array (for replicated snapshots). Click the **Advanced** button in the lower right-hand corner to see where the integration settings for the job are located. Keep in mind that if you wish to perform backups from snapshots located on the secondary array, the **Configure secondary destinations for this jo**b box needs to be checked and the **Backup repository** should be located local to the secondary array. Click **Next** to continue.

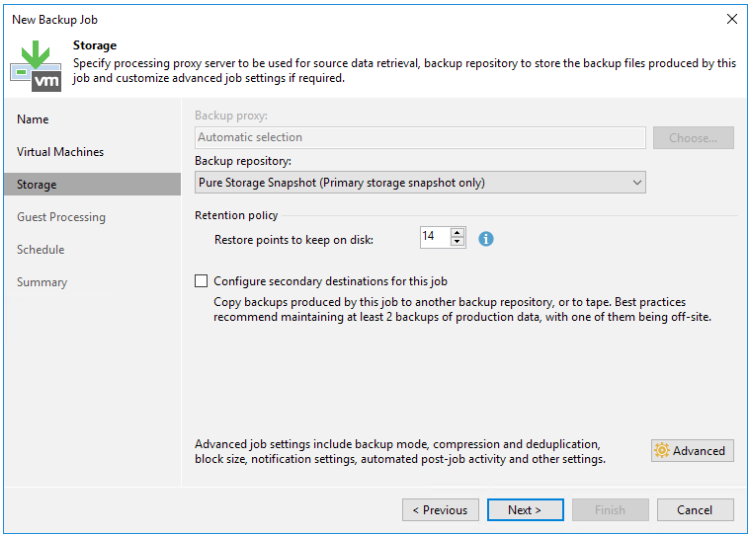

Figure 42: Storage Menu Options

5. Click on the **Integration** tab once the **Advanced** setting window is available. On the **Integration** tab, the **Enable backup from storage snapshots** box should already be checked by default. If it is not checked, check it. Other options include being able to limit the number of process VMs per storage snapshot and failover options for the job. There are many other tabs available that change different aspects of the backup job. For this guide, the other tabs will not be covered. Please refer to the Veeam user guide for details on other tabs. Click **OK** and click **Next** back at the Storage menu to proceed.

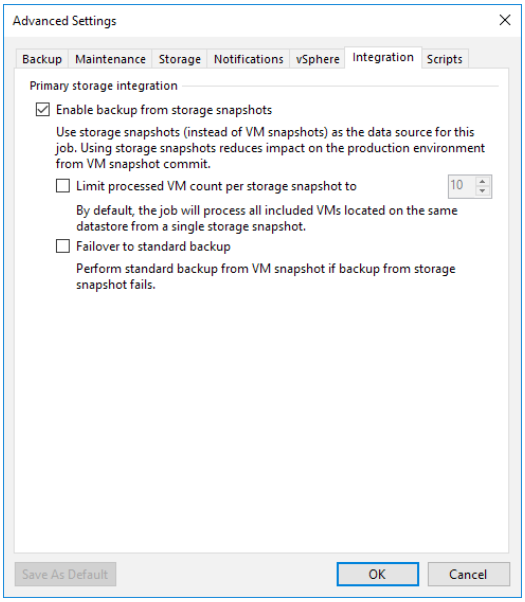

Figure 43: Integrations tab

6. If the secondary target option was checked, the next step includes the **Secondary Target** options. Click **Add** on the right side of the window and a selection box will open. Here, you have the option to retain the storage snapshot and apply a specified retention policy. **Jobs** will allow you to add a backup copy job or tape job. Pure Storage Snapshot will allow you to set retention for the snapshot on the primary **Pure Storage array.** By default, once Veeam completes the backup, it will remove the storage snapshot. This option needs to be selected if Pure Storage snapshot retention is desired on the primary array. Click **OK** and then click **Next** to continue.

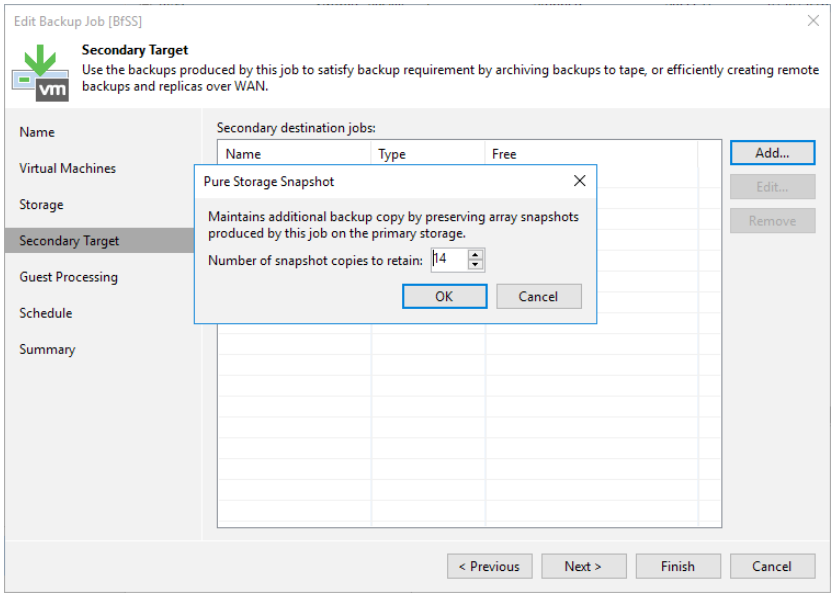

Figure 44: Secondary target selection

7. **Guest Processing** is the next step in the backup job wizard. This is a very important step if application consistency is desired for both the snapshot and backup files. To enable this, check the **Enable application-aware image processing** box. This option will require **Guest OS credentials**. Click **Add** next to the Guest OS credentials to add a new set of credentials or choose credentials from the drop-down box. There is also an **Applications** button. The **enable application-aware processing** button opens a new window where you can select a VM or object you are backing up and **Edit** the way it is processed. Editing a VM or object will open the **Processing settings** window with multiple tabs. These tabs include **General, SQL, Oracle, File Exclusions** and **Scripts**. If you would like more detail on these options, please refer to the Veeam user guide. Under **Guest Processing**, there is also an option to **Enable guest file system indexing**. Enabling this option will allow Veeam to create a searchable catalog of the guest files. It will also enable features such as 1-click restores. To leverage the catalog, the optional **Veeam Backup Enterprise Manager** should be installed. File system indexing will also require **Guest OS credentials**. There is also an Indexing button next to the setting that allows for customization of the indexing Veeam will perform. The last setting in this section is the Guest interaction proxy. By default, Veeam will select an appropriate proxy to perform this interaction, but you can explicitly select the desired proxy or number of proxies. There is also a **Test Now** button near the bottom, which allows you to test the settings prior to running the back-up job. Testing the settings prior to running the job can help prevent job failures due to incorrect or insufficient credentials. When finished with these settings, click **Next** to proceed.

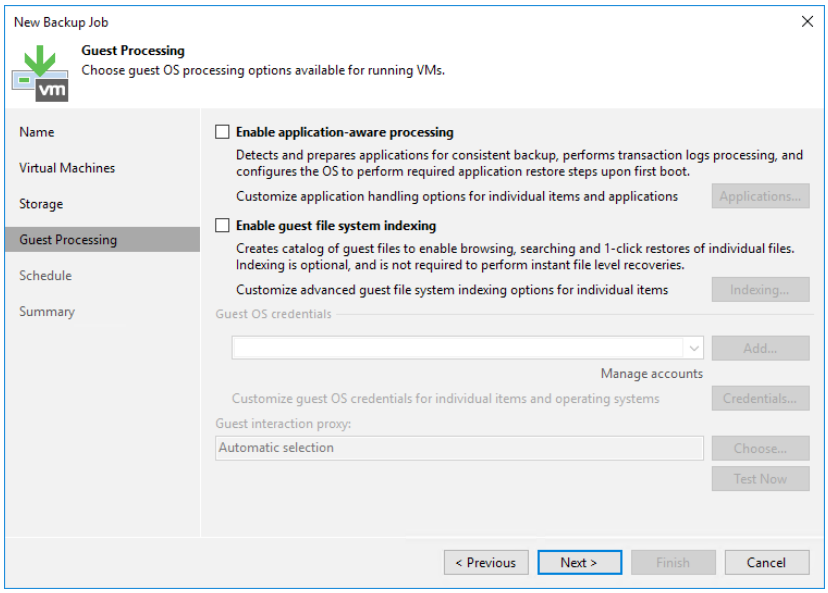

Figure 45: Guest processing and indexing options

8. Next up is the **Schedule**, which is where you can specify when and how often the newly created backup job will run. There are many options to accommodate your business needs. **Automatic retry** allows for setting the number of times to retry a failed attempt to backup a VM and how long Veeam should wait in between retry attempts. **Backup window** is optional and will allow for termination of a job if it runs outside of a specified window. Click **Next** when complete.
9. The final screen on the backup job wizard will display a **Summary** of all the job settings configured throughout the wizard. If these settings are all acceptable, click **Finish** to exit the wizard.

Snapshot orchestration job configuration

1. The snapshot orchestration job is the exact same Backup Job wizard leveraged above. This section will only identify the differences when creating the backup job to perform snapshot orchestration. Please refer to the section above if more information is needed on specific parts of the back-up job creation.
2. Leveraging the **Backup Job** wizard to perform snapshot orchestration on Pure Storage arrays can be done within a single job. To accomplish this, create a new backup job, add VMs or objects into the job and once you get to the Storage options, it will differ slightly. Since the Pure **Storage** is already added into the **Veeam storage infrastructure**, Veeam will automatically create a repository called **Pure Storage Snapshot**. To let Veeam know that this is a snapshot orchestration job, select the **Pure Storage Snapshot (Primary storage snapshot only)** option from the **Backup repository** drop down. Set the desired **Retention** and click **Next** to continue.

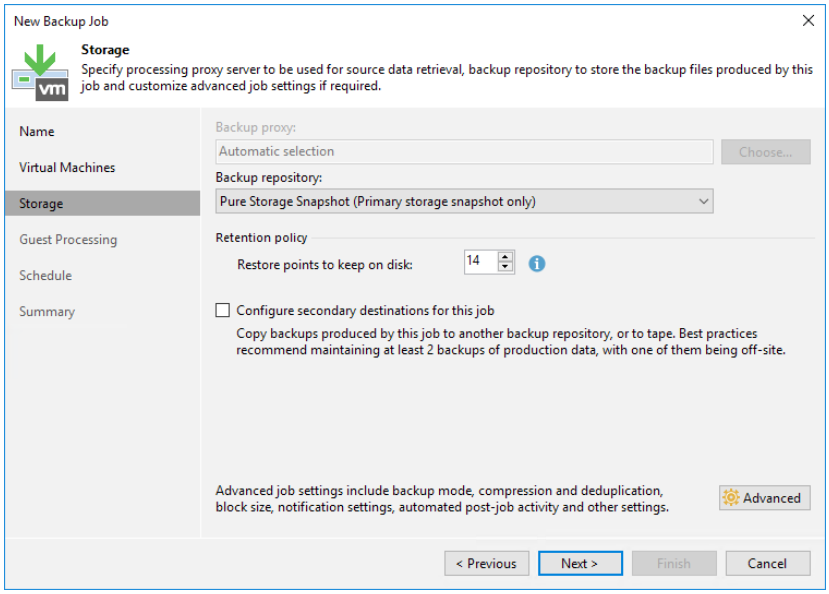

Figure 46: Pure Storage Snapshot Repository

3. **Guest Processing** is identical to the standard backup job, minus the guest file indexing option. Veeam only offers guest file indexing for backups. Enable **application-aware image processing** if an application consistent snapshot is desired. If not, Veeam will simply orchestrate crash-consistent snapshots.
4. **Scheduling** options are identical to the standard backup job. Once the schedule is set, click **Finish**.

Restoring VM data from Pure Storage snapshots

VM data can be restored directly from Pure Storage snapshots if important data is accidently lost or corrupted. The restore process is like a restore from image-level backups of VMs. Veeam Backup & Replication offers the following restore options for Pure Storage snapshots:

- Instant VM Recovery®
- Restoring VM guest OS files (Windows, Linux and others)
- Restoring application items (Exchange, Active Directory, SQL, SharePoint and Oracle)

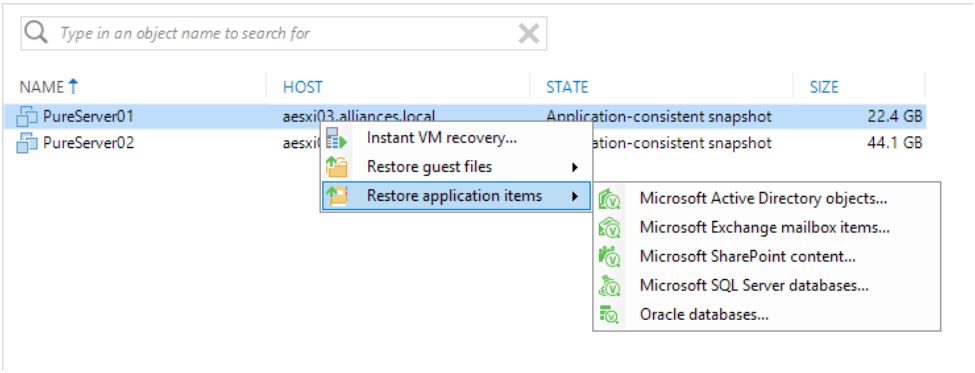

Figure 47: Veeam Explorer for Storage Snapshots

Note: Snapshots created by Pure protection groups are not visible to Veeam. Therefore, the Veeam Explorer for Storage Snapshots will not be able to restore VM data from protection group snapshots.

Prior to performing restoration, the following requirements must be met:

For Pure Storage systems working over iSCSI, make sure that the ESX(i) host selected for storage snapshot mounting has the following:

- Access to the Pure Storage system over an iSCSI connection.
- The host is added to the list of servers having access to storage snapshots from which VM data is to be restored. An initiator group must be created on the Pure Storage system. The initiator group must contain an IQN of the ESX(i) host to which the storage snapshot will be mounted.

For Pure Storage systems working over Fiber Channel, make sure that the ESX(i) host selected for storage snapshot mounting has the following:

- Access to the Pure Storage system over a Fiber Channel connection.
- The host is added to the list of servers having access to storage snapshots from which VM data is to be restored. An initiator group must be created on the Pure Storage system. The initiator group must contain a WWN of the ESX(i) host to which the storage snapshot will be mounted.

Configuring Veeam DataLabs For Storage Snapshots

Veeam DataLabs is a great way to leverage snapshots for testing. Veeam DataLabs consist of three different components: **Application Group, Virtual Lab and SureBackup Job**.

1. To begin, let's start with the Application Group. From the lower left pane, select **Backup Infrastructure**. Under **Backup Infrastructure**, select **SureBackup**.

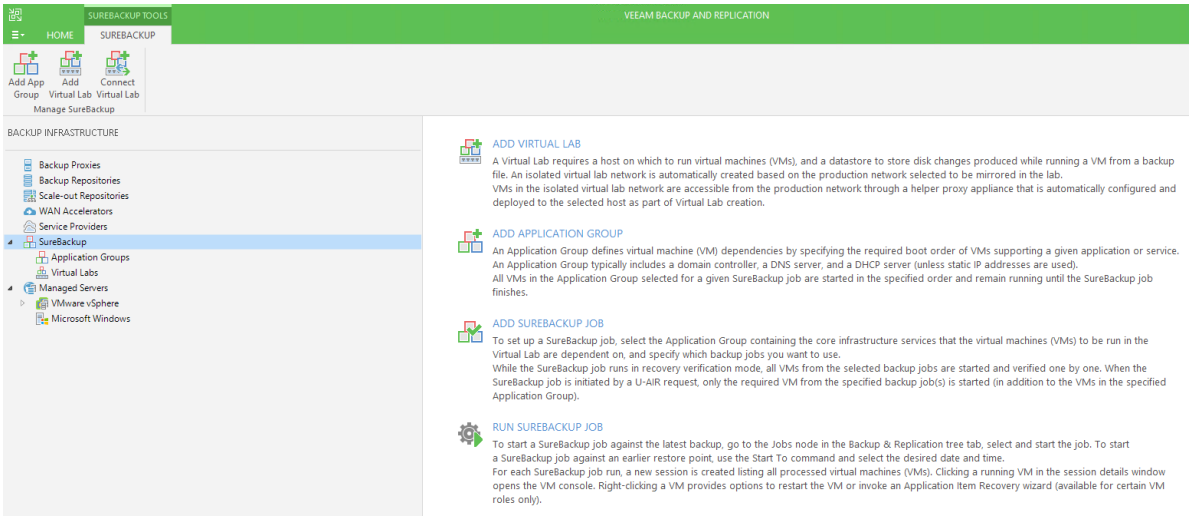

Figure 48: Backup Infrastructure, SureBackup

2. From here, you can select **Add App Group** from the top menu or **Add Application Group** from the right window. This will launch the **New Application Group** wizard. Begin by giving the group a **Name**, the Description box will be automatically populated with the creator, date and time. Additional text can be added as needed. Click **Next** to continue.

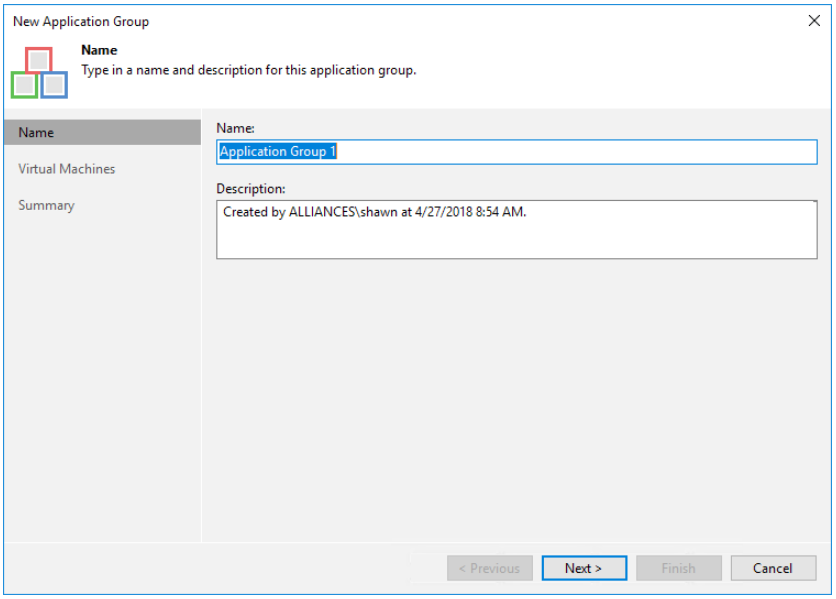

Figure 49: New application group wizard

3. The next step is to add VMs that you would like to bring online in the Veeam DataLabs. Click **Add VM** and select **From storage snapshots**.

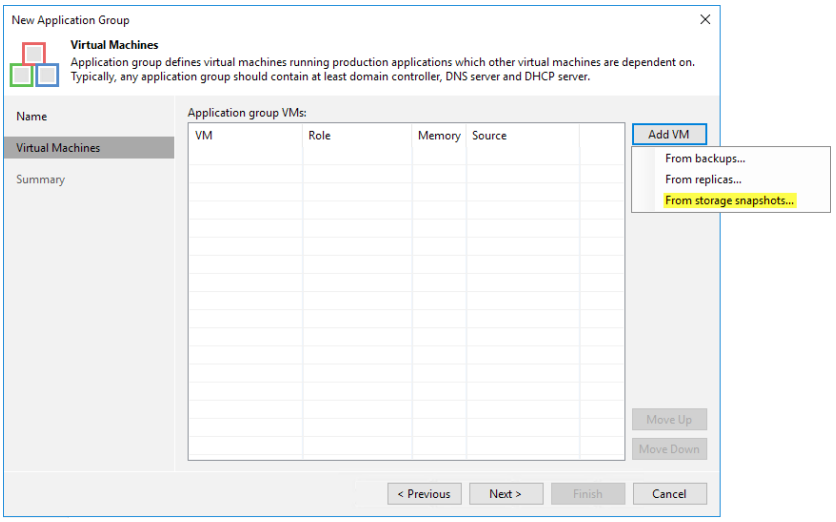

Figure 50: Adding VMs to an application group

4. A new window will pop up to allow you to select VMs available on storage snapshots. Keep in mind that you can make multiple selections by holding Ctrl while making your selections. Click **Add** once your selections are made. Keep in mind that VMs listed under the **Application** group VMs will power on one at a time in the order they appear on the list. As this is a completely isolated environment, please make sure that any necessary dependencies are met. VMs can be rearranged on the list by clicking the **Move Up** or **Move Down** button as needed. Once the list is complete, click **Next** to get to the **Summary**, and then click **Finish**.

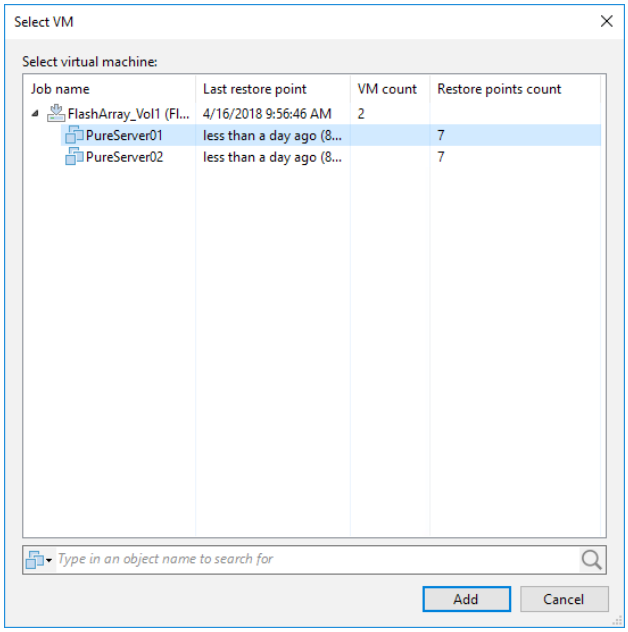

Figure 51: Selecting application group VMs

5. Back at the Veeam console, click **Add Virtual Lab** at either the top menu or right window. This guide will cover a basic configuration for the virtual lab. For more details on how the virtual lab works and advanced configurations, refer to the Veeam user guide. At the **New Virtual Lab** wizard, fill in the **Name** for the virtual lab. The **Description** box will be automatically populated with the creator, date and time. Additional text can be added as needed. Click **Next** to continue.

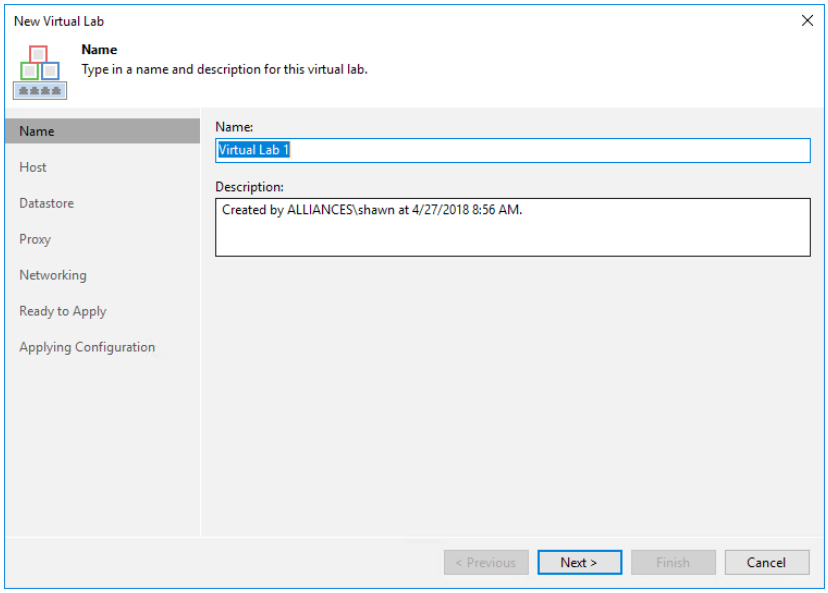

Figure 52: New virtual lab wizard

6. On the **Host** menu, select a host to run the virtual lab on by click **Choose.** While the VMs will be running off storage snapshots, they will require compute and memory resources from the host to run. Keep this in mind when making a host selection. Click on the host where you'd like the virtual lab to run and click **OK**. The **Folder and Resource pool** will be populated with the virtual lab name provided previously. You can change this by clicking **Configure**. Once complete, click **Next**.

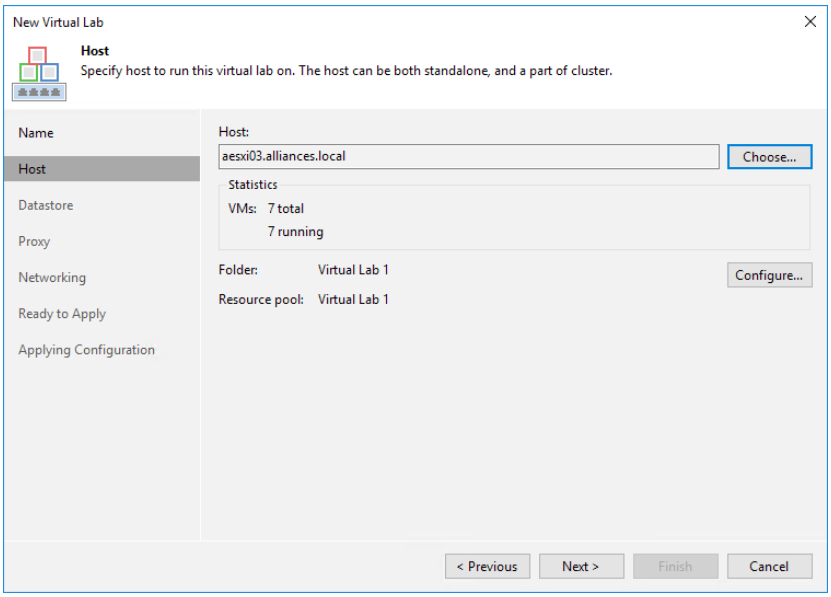

Figure 53: Host selection

7. Next select a **Datastore** to store redo logs on by clicking the **Choose** button. After selecting, click **OK** and then click **Next**.

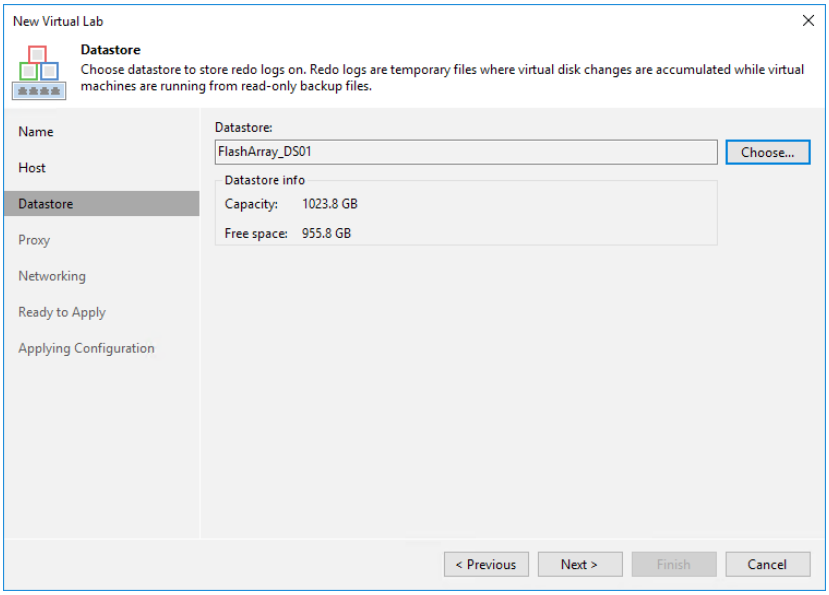

Figure 54: Datastore selection

8. The proxy appliance is an important component of the virtual lab. It acts as a gateway that provides access from the backup server to the VMs in the virtual lab. It is recommended to select the **Use proxy appliance in this virtual lab** check box. Click **Configure** to edit the name of the Proxy appliance, if desired. **Production network connection** is where you will select an appropriate production network in which the proxy appliance will be created. Click **Configure** to select the **Production network** and configure the **IP address** and **DNS server**. The **Production network** selected should be reachable by the backup server.

9. By default, VMs in the virtual lab work in this isolated environment and do not have access to the Internet. If you want to let VMs in the virtual lab access the Internet, select the **Allow proxy appliance to act as internet proxy for virtual machines in this lab** check box. In the **Port** field, specify a port for HTTP traffic. By default, port 8080 is used. In the **Production proxy** field, you can optionally specify an IP address or a fully qualified domain name of an Internet-facing proxy server that VMs must use to access the Internet. Click **Next** to proceed.

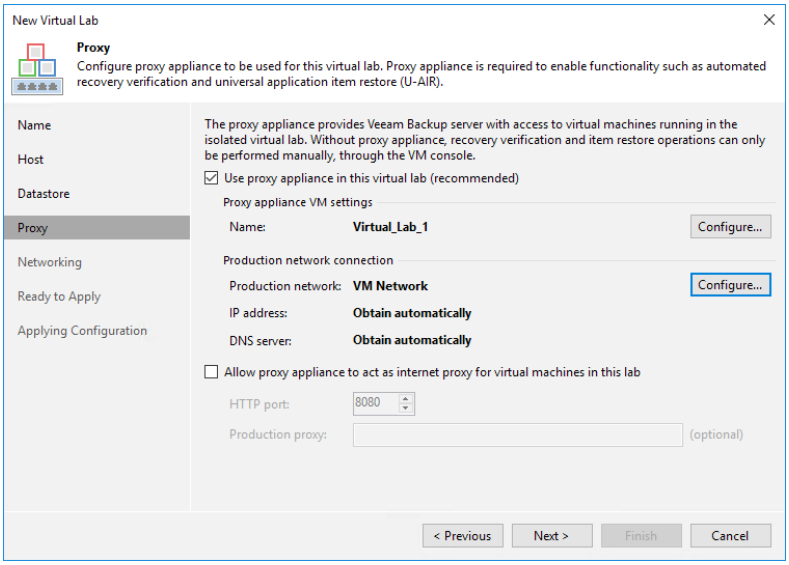

Figure 55: Proxy appliance configuration

10. The next selection will be **Networking**. While there are three options, for the purposes of this guide, the **Advanced single-host (manual configuration)** will be covered. Please read the descriptions under each option and if one of the other options is desired, you may refer to the Veeam user guide for more details. Select A**dvanced single-host (manual configuration)** and click **Next** to continue.

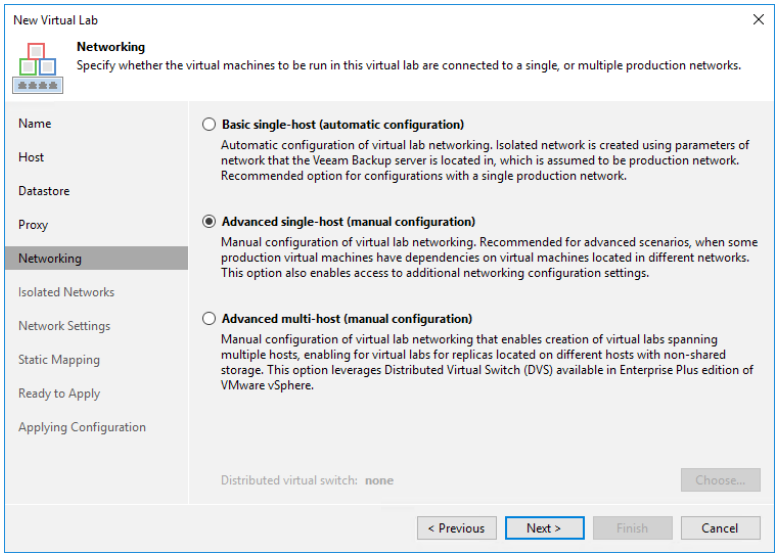

Figure 56: Networking selection

11. In the **Isolated Networks** step, configure isolated networks that the VM from the application group will be connected, Map these networks to production networks where the original VMs are located. The suggested **Network Mapping** should be correct based on the previous selection in step 10. You may **Edit** if necessary. Several production networks can be mapped to isolated networks by clicking **Add**. Click **Next** once verified.

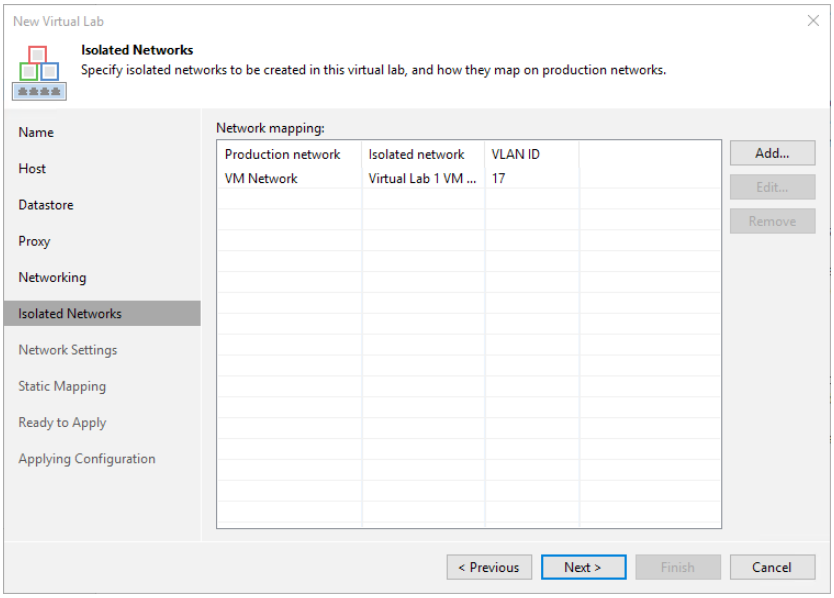

Figure 57: Isolated networks mapping

12. The next step of the wizard will have a virtual NIC already created. Select the **vNIC** by clicking on it, and then click **Edit**. Verify the **vNIC Connection Settings** in the new window, ensuring that the IP address listed is the gateway IP in the corresponding production network. Also, check the masquerade IP address to ensure that it does not match any network within your production environment. DHCP is optional and can be enabled. When complete, click **OK**. If more than one production network was mapped in the previous step, click **Add** to create a vNIC for that network as well. If more than one vNIC is created, the check box **Route network traffic between vNICs** is available. Check the box if desired and click **Next** to proceed.

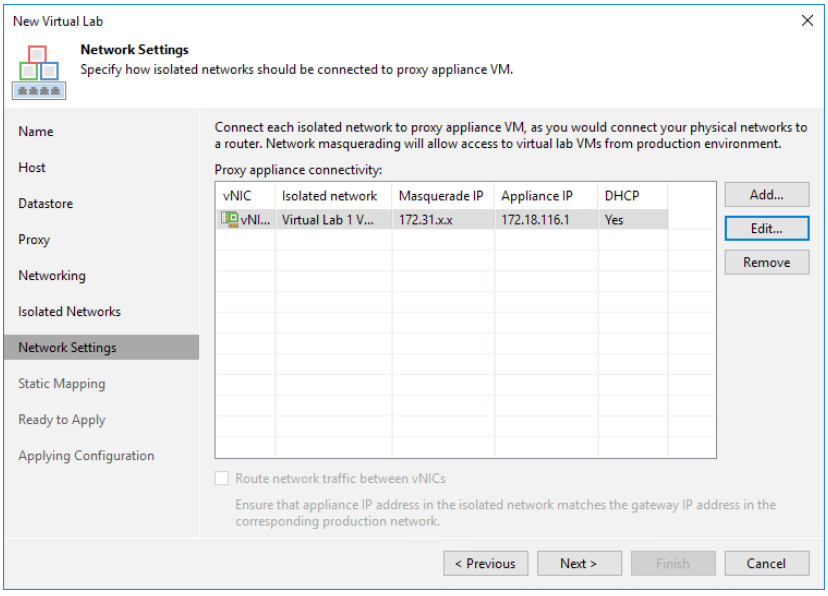

Figure 58: vNIC configuration

13. **Static Mapping** is an optional step that allows you to specify static IP address mapping rules to make VMs in the virtual lab accessible from any machine in the production network. Click **Next**.

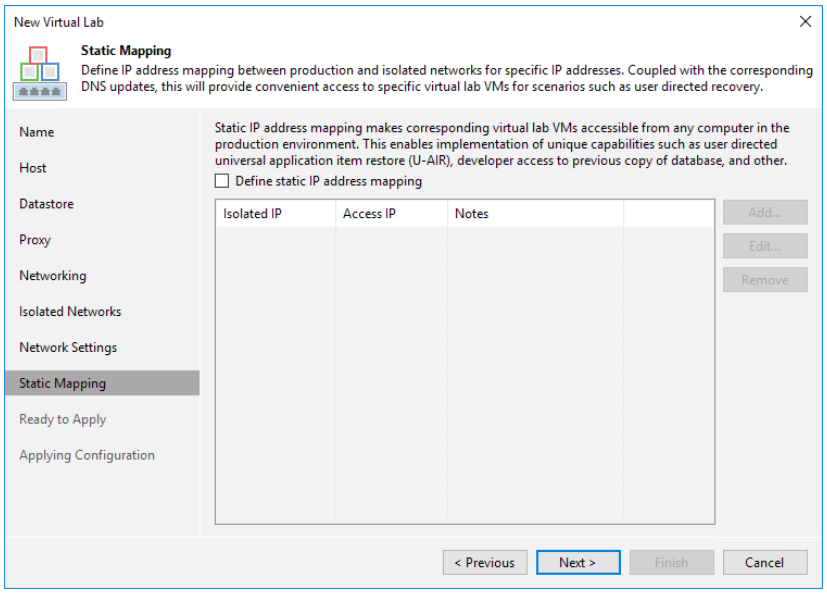

Figure 59: Static IP mapping

14. The **Ready to Apply** step of the wizard shows a summary screen with all the virtual lab parameters configured throughout the wizard. Once the settings have been verified and are satisfactory, click **Next** to begin the creation.
15. Veeam will begin deploying the virtual lab to the designated host. Once it is completed, click Finish to exit the wizard.
16. Now that the **Application Group** and **Virtual Lab** has been completed, the final component is the **SureBackup Job**. Click Add **SureBackup Job** from the right window to launch the wizard.
17. The first step of the wizard allows you to specify a **Name** for the job, the Description box will be automatically populated with the creator, date and time. Additional text can be added as needed. Click **Next** to continue.

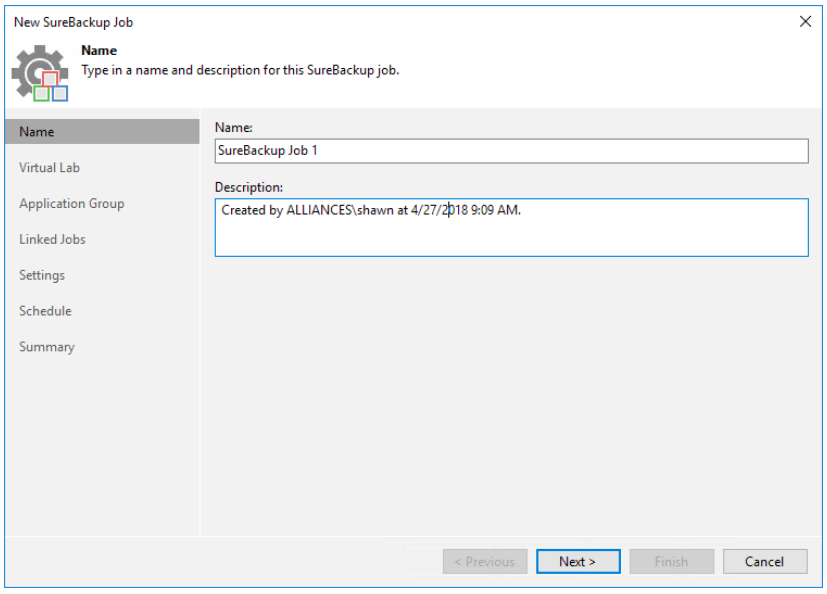

Figure 60: New SureBackup Job wizard

18. The **Virtual Lab** step of the wizard allows you to select the virtual lab you wish to associate to the job. Select the appropriate virtual lab from the dropdown list. Click **Next.**

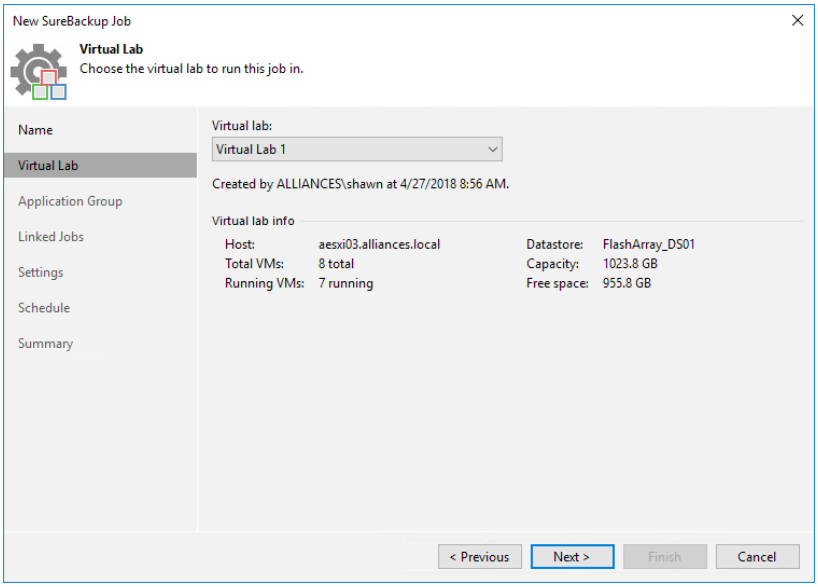

Figure 61: Virtual Lab selection

19. The **Application Group** step will have a drop-down list as well, allowing you to select an application group to associate with the job. Since this job will be leveraged as **Veeam DataLab**s, make sure to check the box **Keep the application group running after the job completes**. Click **Next** to continue.

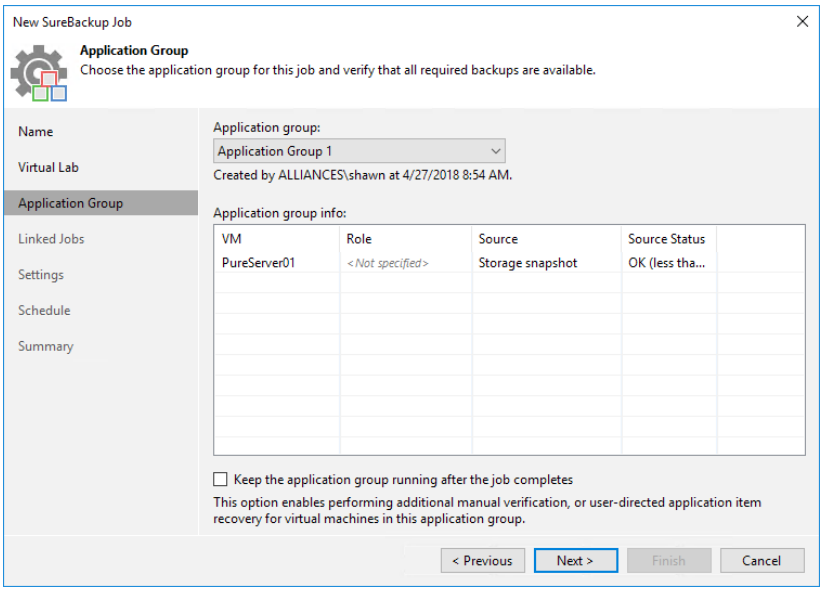

Figure 62: Application group selection

20. The **Linked Jobs** step of the wizard is intended for recovery verification of backups, since we are leveraging this job for Veeam DataLabs, we will skip this step. Click **Next** to proceed.

21. **Settings** will allow you to configure SNMP traps and email notifications for the job. The backup file integrity check is intended to enhance recovery verification for backups so we can skip this option. Click **Next**.

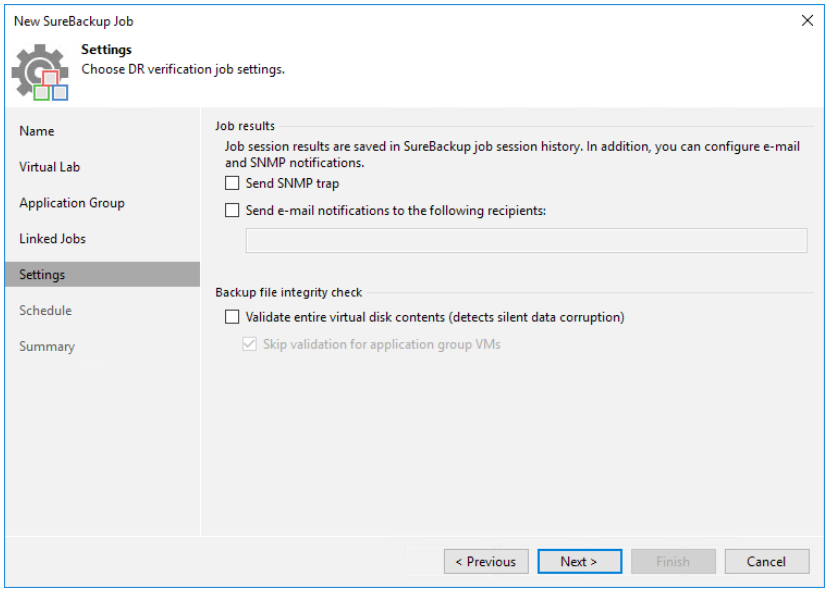

Figure 63:Settings

22. At the **Schedule** settings, you can specify a schedule for the job. Alternatively, you can execute the job manually as needed in the future. Specify a schedule if desired, Click **Save** when complete.

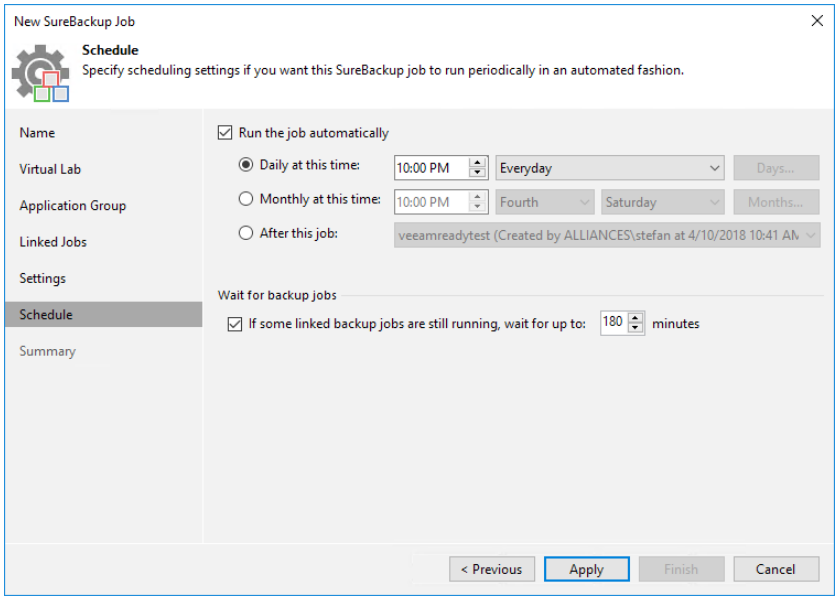

Figure 64: Scheduling

23. The SureBackup Job will be created, and the final step will give you a confirmation. In this step, you can also check the box **Run the job when I click Finish** if you wish to test Veeam DataLabs. Click Finish to exit the wizard.

24. That completes Veeam DataLabs creation. You can execute the SureBackup job at any time by right-clicking on the job name and selecting **Start**.

Summary

Now that Veeam and Pure Storage are both configured, the integrated capabilities will allow for a comprehensive data protection solution. Leverage the power of storage snapshots along with Veeam backups to improve RPOs. And with the recovery capabilities direct from a snapshot or backup, enhance recovery time objectives (RTOs). There are many more capabilities are available and additional options, which are not covered in this guide. Please refer to the guides listed in the **Introduction** to take full advantage of solution.

About the Author

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 55,000 ProPartners and more than 294,000 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**