Veeam Availability on UCS

Shawn Lieu

Veeam Solutions Architect, vExpert

Contents

The Challenge

With data growing at astounding rates, IT managers are depending more and more on reliable backup and recoverability of their data. High-growth businesses require a complete data protection solution that is reliable, flexible and easy to use. Virtualizing an environment provides increased levels of data Availability, but the need to meet aggressive RPOs and RTOs becomes increasingly difficult.

Traditional backup tools were not created for virtualized environments. That makes it hard for many organizations to take full advantage of their virtualized environment, and many IT managers struggle with:

- Unreliable backups
- Recovery that takes too long
- High costs associated with managing backup data and secondary storage
- Inability to provide reliable and true backups for compliance purposes
- Lost productivity due to management complexity
- The need to scale backup operations for growth

IT managers can meet the challenges of ever-shrinking RPOs and the aggressive RTOs associated with virtualized environments.

The Solution

Veeam® enables *Availability for the Always-On Enterprise*™ with Cisco UCS for combined data management and protection solutions required for 24/7 application Availability.

By combining Cisco UCS and Veeam solutions, customers eliminate data loss and deliver fast data recovery, helping them minimize risk, decrease downtime and easily adapt to business changes to meet the most stringent recovery time and point objectives, or RTPO™.

Veeam Backup & Replication™ unifies backup and replication in a single solution — increasing the value of backup and reinventing data protection for VMware vSphere and Microsoft Hyper-V virtual environments. The Veeam agentless design provides multiple backup options to meet your needs. Features such as source-side deduplication and compression, change block tracking, parallel processing, and automatic load balancing provide the fastest, most efficient backups possible.

Figure 1

The Cisco UCS S3260 Rack Server (Figure 1) is a modular, high-density server ideal for modern data protection. The Cisco UCS S3260 addresses the need for highly scalable computing with high-capacity local storage. Designed for a new class of applications, it is simple to deploy and excellent for backup repositories. Together, Veeam and Cisco UCS S3260 create the perfect staging area for backups — reducing backup ingest bottlenecks and providing faster backups using parallel processing. In addition, Veeam Backup & Replication provides:

- Granular recovery of VMs and files, including Microsoft Exchange and SharePoint application items.
- The ability to automatically verify every backup, every VM, and every replica — every time.
- Self-service recovery of VMs and guest files without direct network connection to the VM, user permissions or the need to deploy costly agents.
- Instant VM Recovery® to recover a failed VM in less than two minutes.
- A choice to back up and recover what you need, where you need it, and when you need it —whether it's on site, on tape or in the cloud. Veeam and Cisco offer the right solution for performance, flexibility and reliability — providing an impressive, modern disaster recovery (DR) solution for your VMware vSphere or Hyper-V environment.

Deployment Recommendations

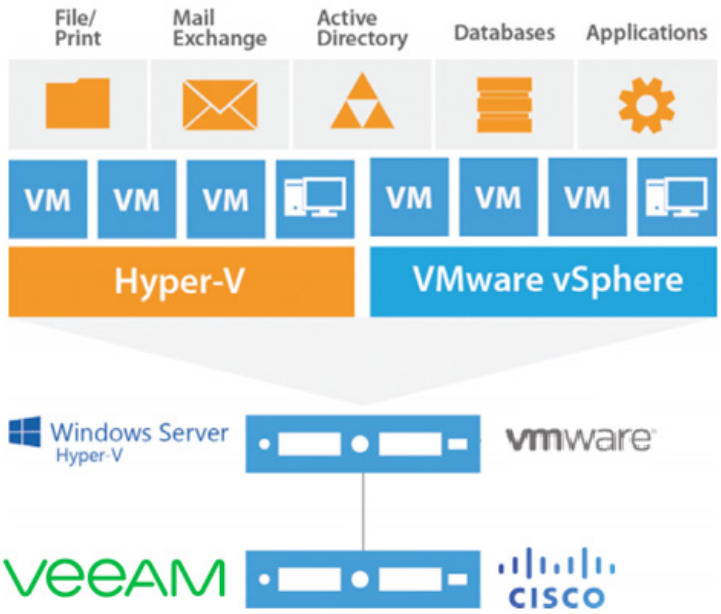

Figure 2

Simplified deployment helps streamline your data protection strategy. With the UCS S3260's combination of compute, memory and high-capacity storage, deployment of Veeam Modern Data Protection can be accomplished on a single UCS S3260 server, as show in Figure 2.

UCS S3260 recommended specifications:

- 2x Intel Xeon processors
- 128GB–256GB RAM
- 2x SSD's for OS (RAID 1)
- 4GB of RAID cache with battery backed write cache
- 64-bit Windows OS (Server 2016 required for ReFS 3.1)

There are a number of different ways to install the Windows OS onto the S3260's SSD, please refer to the S3260 installation guide for details. We recommend you use two SSDs in a RAID1 configuration for the Windows OS. Once Windows is installed, several drivers will need to be installed as well. Drivers can be downloaded here: https://software.cisco.com/download/navigator.html

For environments with existing Fabric Interconnects, UCS Manager can be leveraged. For environments that already have UCS Manager in place, server configuration, network connectivity and storage can all be configured here. In this guide, we will cover CIMC (Cisco Integrated Management Controller) and CLI. Create a UCS S3260 volume for a Veeam backup repository using CIMC. CIMC can be accessed via the web interface or via SSH. Of the two methods covered, select the method you are most comfortable with. Before proceeding with volume creation, determine with recommended RAID selection works best for your environment. There are two recommended RAID options, RAID6 & RAID60 depending on number of drives. See the table (Figure 3) below for additional information on the recommended configurations.

Disk count	RAID layout
14	1x RAID6 (1x 11+2 Disks) 1 Global Hot Spare
28	1x RAID 60 (2x 11+2) 2 Global Hot Spares
56	1x RAID60 (4x 11+2 Disks) 4 Global Hot Spares

Figure 3

CIMC Virtual Drive configuration via web interface

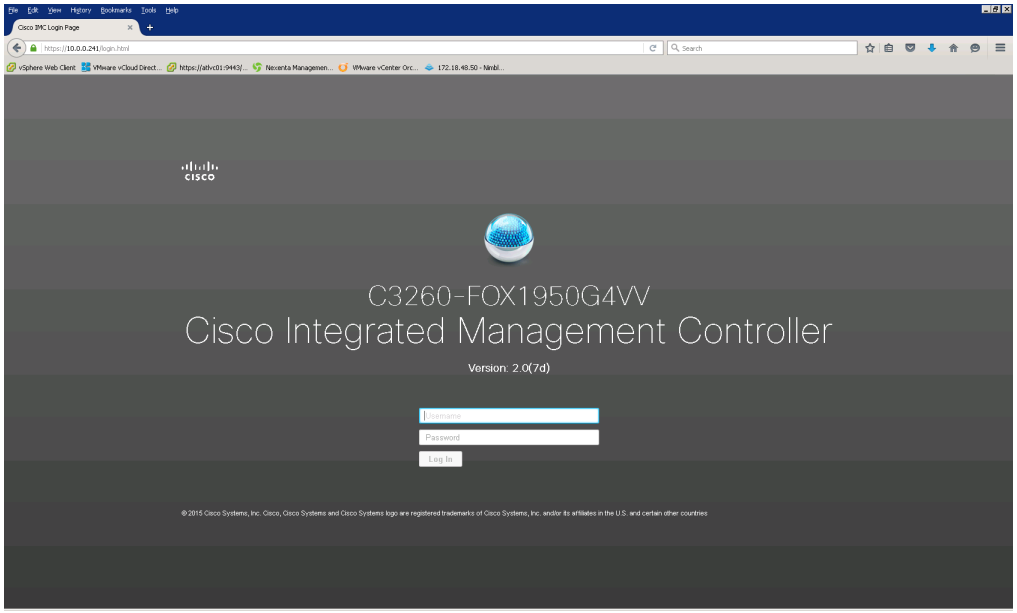

Figure 4

Open a web browser and enter the IP for the CIMC. You will be directed to the login screen where you can enter your credentials for access, see Figure 4.

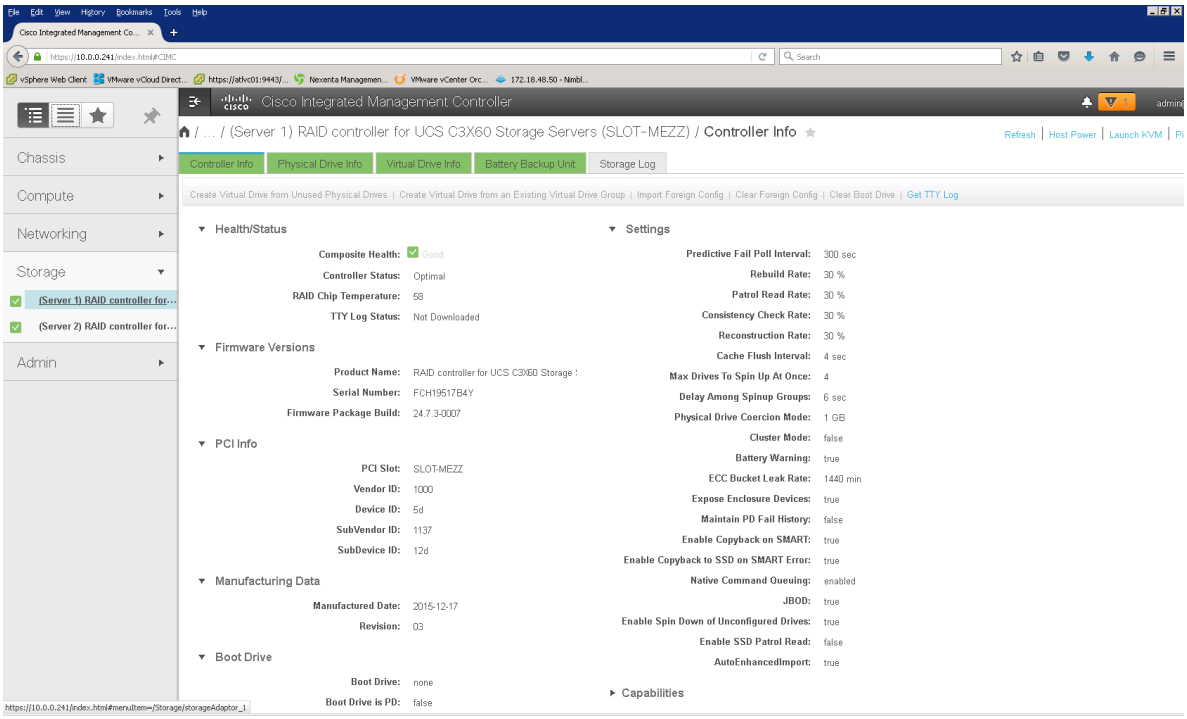

Figure 5

Once logged in, click on the menu options in the top left-hand corner, see Figure 5. Expand the **Storage** menu from the left side pane and select the controller.

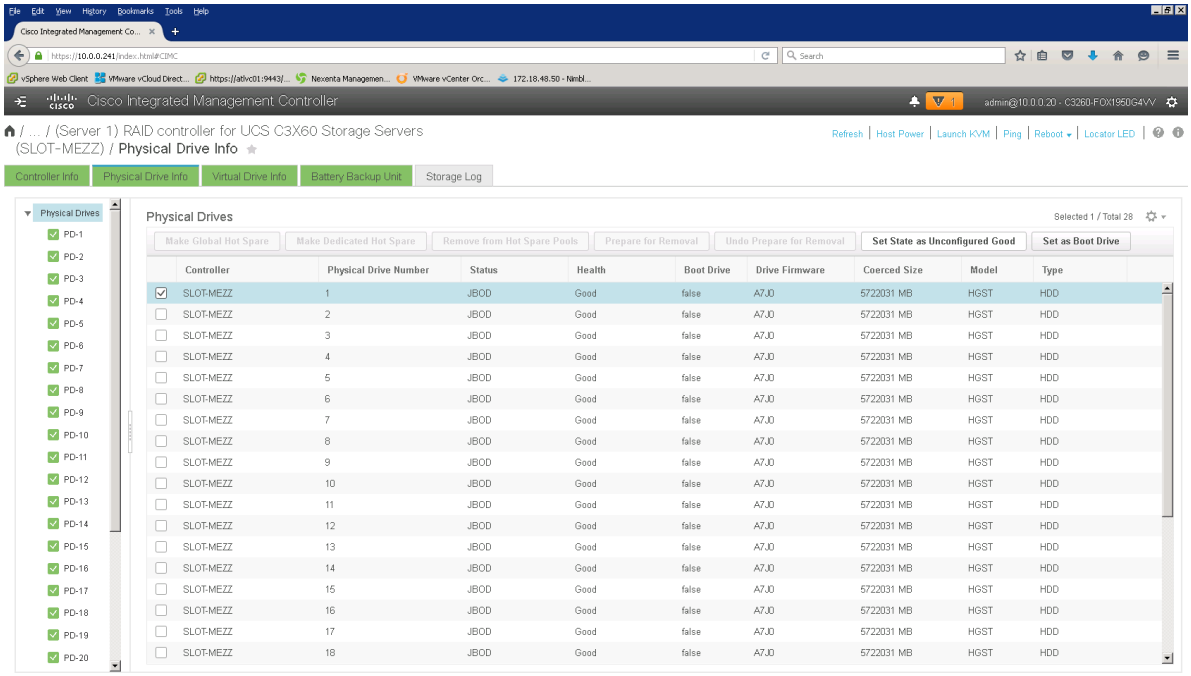

Figure 6

Under the **Physical Drive Info** Tab (Figure 6), select each drive individually and click **Set State as Unconfigured Good**. Repeat this for all physical drives available, then click on the **Controller Info** Tab.

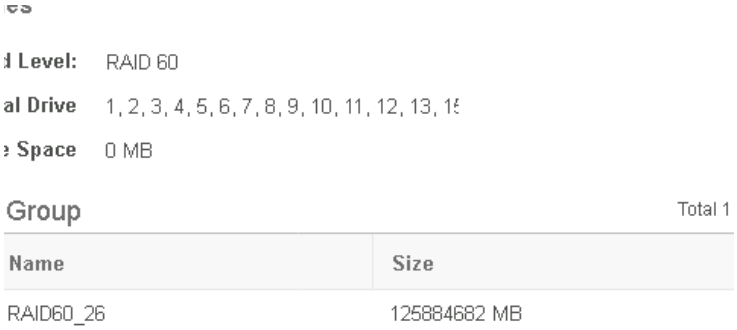

Figure 7

Click **Create Virtual Drive from Unused Physical Drives** and a configuration box will pop up (Figure 7). The selections made here will result in a new Virtual Drive that will be used as a Veeam backup repository.

Let's begin with the following recommended settings (Figure 7) for a Veeam repository:

- RAID Level: 60
- Refer to the table (Figure 3) for drive group recommendations
- Virtual Drive Name: any name you'd like, up to 15 characters
- Access Policy: Read Write
- Read Policy: Always Read Ahead
- Cache Policy: Cached IO
- Disk Cache Policy: Disabled
- Write Policy: Write Back Good BBU
- Strip Size: 512k
- Size: specify the desired Virtual Drive size in MB, GB or TB

Once the recommended settings have been entered, click **Create Virtual Drive**. This will take a few moments. Once complete, you can click on the Virtual Drive Info tab to verify. Select the Virtual Drive Info from the right side pane to verify the newly created Virtual Drive, see Figure 8.

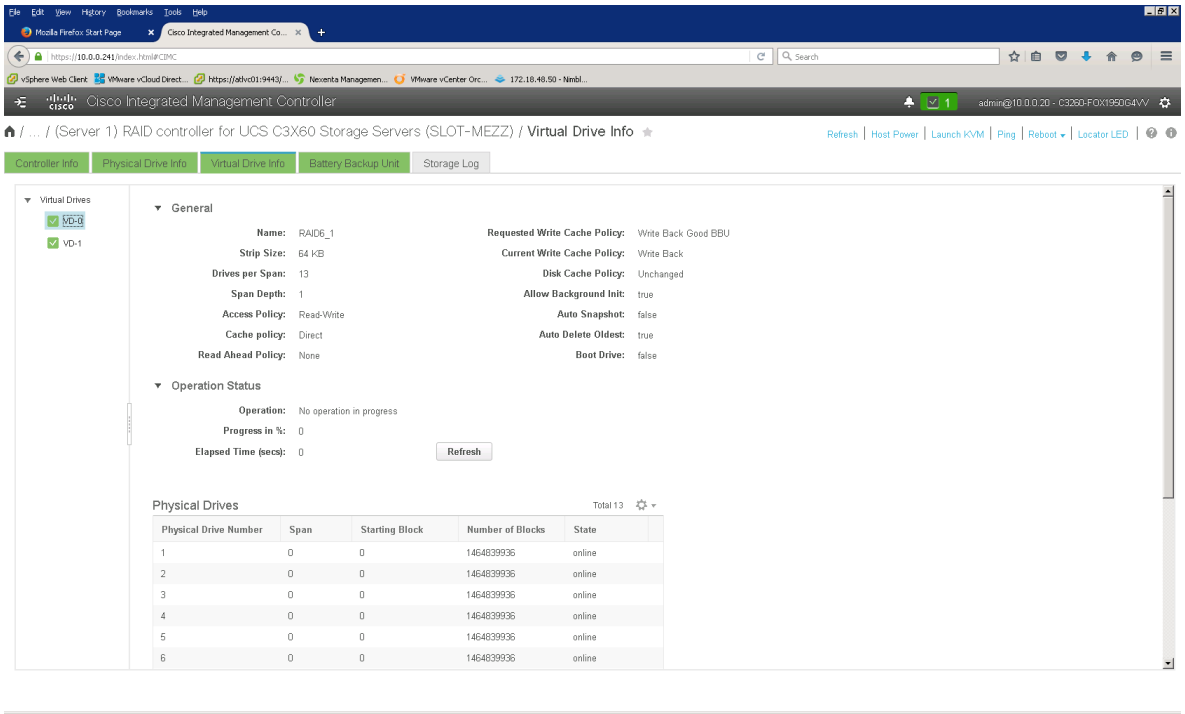

Figure 8

Now that the Virtual Drive is verified, it's time to mount the volume in Windows. If you used the web interface to configure the Virtual Drive, skip past the following section for SSH. Return to the S3260 Windows OS to create the new volume.

Before you create the volume in Windows, you will need to make sure that all necessary vnics are created. Number of vnics required will depend on your environment and what type of backup mode you wish to leverage within Veeam. For best performance, direct storage access is the preferred backup mode. To leverage direct storage access, the Veeam server will need management network as well as storage network access. The vnics required can also be created within CIMC or via SSH. There are other transport modes and other deployment scenarios not covered within this guide, please refer to the Veeam User Guide (link located on page 35).

CIMC Virtual Drive configuration via SSH

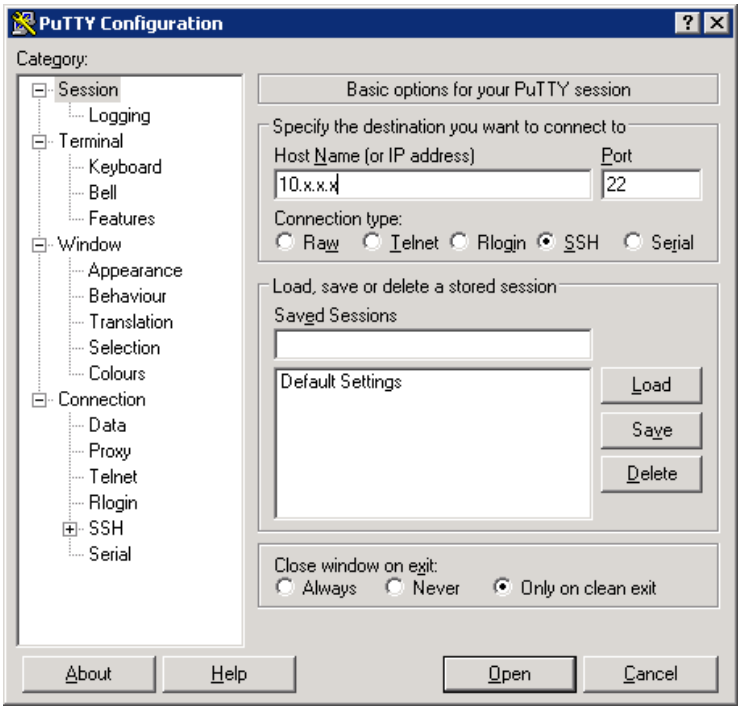

Figure 9

Open a SSH client, PuTTY will be used in this example. To connect to CIMC, enter the IP address and click Open, see Figure 9. PuTTY will connect and prompt you for the login name and password.

After you are logged in, you will be presented with the command prompt. Enter the following commands to configure the Virtual Drive.

1. Server # scope chassis
2. Server/chassis # show server
   Server ID Power Serial Number Product Name PID UUID
   --------- ----- ------------- ------------ ---------- ------------------------------------
   1 on FCH1944J57S UCS C3160 UCSC-C3X60-SVRNB xxxxxxx
3. Server /chassis # scope server 1
4. Server/chassis/server # show storageadapter
   PCI Slot Health Controller Status ROC Temperature Product Name Serial Number Firmware Package Build Product ID Battery Status Cashowche Memory Size Boot Drive Boot Drive is PD
   ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---
   ----
   SLOT-XXXX Good Optimal 58 degrees C RAID controller for UCS C3X60 S... FCH19517B4Y 24.7.3-0007 LSI Logic Optimal 4025 MB none false
5. Server/chassis/server # scope storageadapter SLOT-XXXX
6. Server/chassis/server/storageadapter # show physical-drive
   Physical Drive Number Controller Health Status Boot Drive Manufacturer Model Predictive Failure Count Drive Firmware Coerced Size Type Link Speed
   ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ----- ----------
   1 SLOT-XXXX Good JBOD false HGST HUS726060AL... 0 A7J0 5722031 MB HDD 12.0 Gb/s
   .....etc
7. Server/chassis/server/storageadapter # scope physical-drive X "X is the assigned physical drive number"
8. Server/chassis/server/storageadapter/physical-drive # make-unconfigured-good
   Please confirm that you want to change physical drive X from a JBOD to Unconfigured Good.
   If the drive is subsequently used in a RAID operation, all data on the drive will be lost.
9. Enter 'yes' to confirm -> yes "must type yes to confirm"
10. Server/chassis/server/storageadapter/physical-drive # exit
    Note: The steps highlighted in green must be repeated for every single physical drive available.

11. Server/chassis/server/storageadapter # create-virtual-drive

12. Please enter RAID level
    0, 1, 5, 6, 10, 50, 60 --> 6 "Select your desired RAID setting, 6 or 60 are the recommended selections"

13. Please choose from the following 15 unused physical drives:
    ID Size(MB) Model Interface Type
    1 5722031 HGST SAS HDD
    ....etc

14. Specify physical disks for span 0: "If configuring RAID 60, a minimum of 2 spans are required"
    Enter comma-separated PDs from above list--> 1,2,3,4,5,6,7,8,9,10,11,12,13 "refer to figure 3 for the recommended drive configurations"

15. Please enter Virtual Drive name (15 characters maximum, hit return to skip name)--> VIRTUALDRIVENAME
    "any name you would like up to 15 characters"

16. Please enter Virtual Drive size in MB, GB, or TB
    Example format: 400 GB --> 62942341 MB "Enter the desired drive size in MB, GB or TB"

17. Optional attribute:
    stripsize: defaults to 512k Bytes
    0: 8K Bytes
    1: 16K Bytes
    2: 32K Bytes
    3: 64K Bytes
    4: 128K Bytes
    5: 256K Bytes
    6: 512K Bytes
    7: 1024K Bytes
    Choose number from above options or hit return to pick default--> 3 "recommended"
    stripsize will be set to 512k Bytes (7 and 'strip-size\512k')

18. Disk Cache Policy: defaults to Unchanged
    0: Unchanged
    1: Enabled
    2: Disabled

19. Choose number from above options or hit return to pick default--> 2 "recommended"
    Read Policy: defaults to No Read Ahead
    0: No Read Ahead
    1: Always

20. Choose number from above options or hit return to pick default--> 1 "recommended"

21. IO Policy: defaults to Direct I/O
    0: Direct I/O
    1: Cached I/O

22. Choose number from above options or hit return to pick default--> 1 "recommended"

23. IO Policy: defaults to Direct I/O
    0: Direct I/O
    1: Cached I/O
    Choose number from above options or hit return to pick default--> 1 "recommended"

24. Access Policy: defaults to Read Write
    0: Read Write
    1: Read Only
    2: Blocked
    Choose number from above options or hit return to pick default--> Picking default "recommended"

25. New virtual drive will have the following characteristics:
    - Spans: '[14.15.16.17.18.19.20.21.22.23.24.25.26.27]'
    - RAID level: '6'
    - Name: 'RAID6_2'
    - Size: 62942341 MB
    - stripsize: 512k Bytes
    - Write Policy: Write Back Good BBU
    - IO Policy: Cached I/O

    OK? (y or n)--> y "enter y if the settings are correct or n to reconfigure"
    Note: If you have selected and configured RAID6, repeat the virtual drive creation for the additional RAID6 groups.

26. Server/chassis/server/storageadapter # scope physical-drive 28

27. Server/chassis/server/storageadapter/physical-drive # make-global-hot-spare

28. Server/chassis/server/storageadapter/physical-drive #

Creating a new volume in Windows

Once the Virtual Drive has been created, a new volume and drive letter can be assigned in Windows. You will encounter a pop-up asking if the new disk will be MBR or GPT, select GPT. The newly created Virtual Drive will appear in the offline state. As part of the process, bring the drive online, format it and give it a drive letter. This configuration can be completed via the Disk Management interface within Windows (Figure 10).

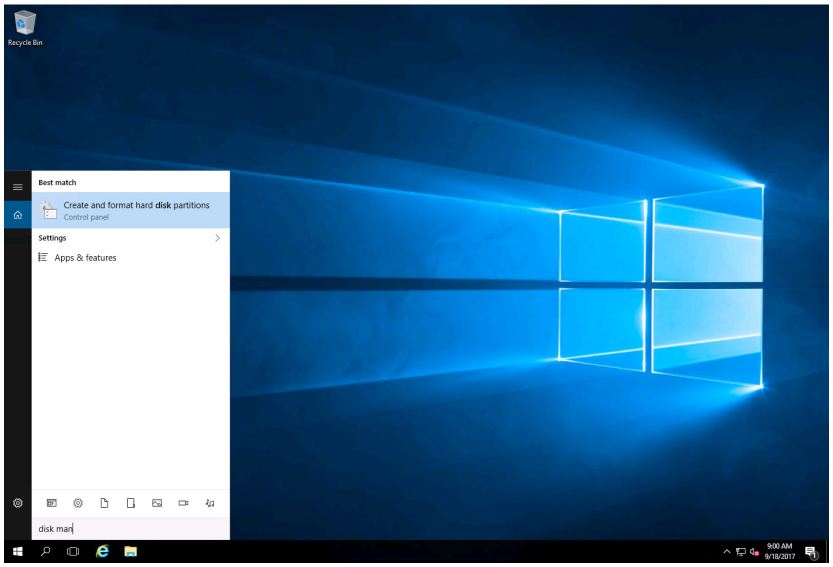

Figure 10

Right click on the new disk and select **Online**. Once online, right click in the space that currently says **Unallocated** (Figure 11). A menu will appear with multiple options, but for this example, New **Simple Volume** will be selected.

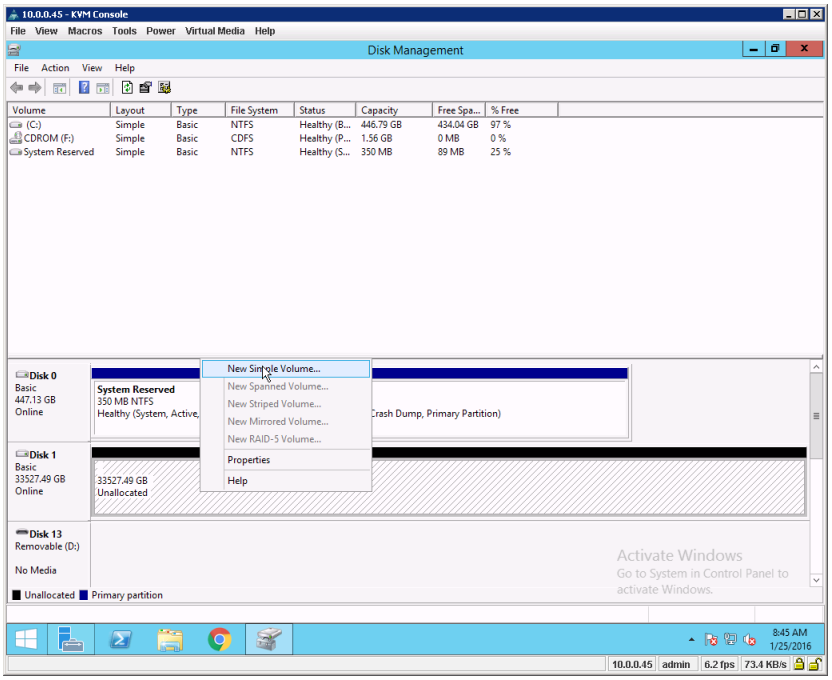

Figure 11

Making this selection will launch the New Simple Volume Wizard (Figure 12). Continue by click **Next**.

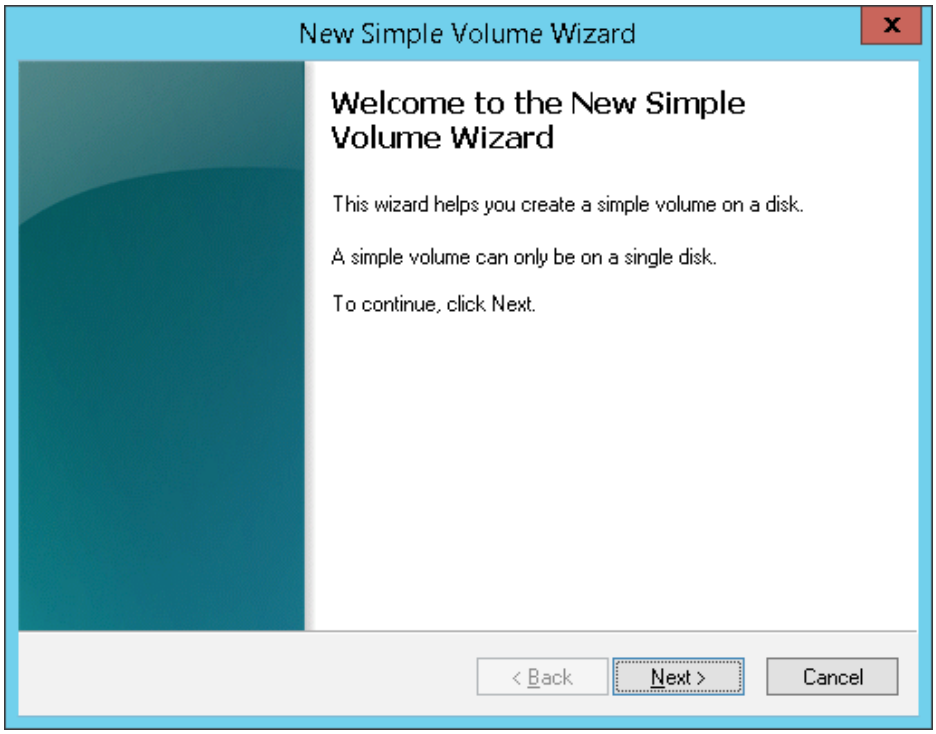

Figure 12

On the next step of the wizard, specify the volume size. Based on the maximum disk space in MB, the new simple volume size in MB should be prepopulated with the same value. Click Next to accept the maximum size and continue (Figure 13).

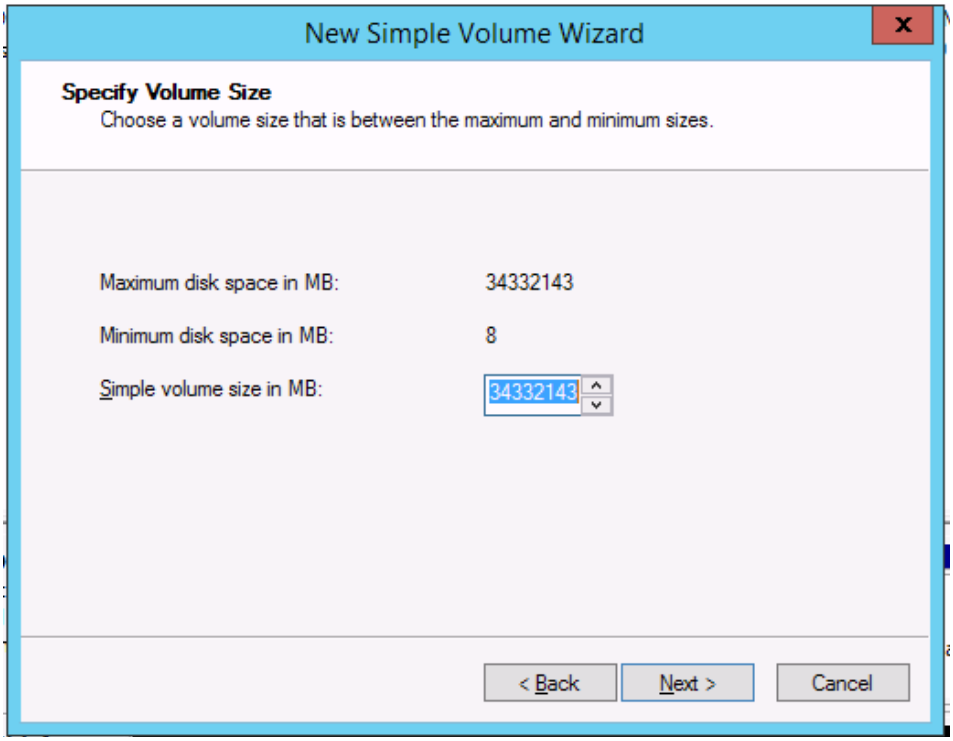

Figure 13

Next, assign a drive letter to the new volume. Once the selection has been made, click **Next** to continue (Figure 14).

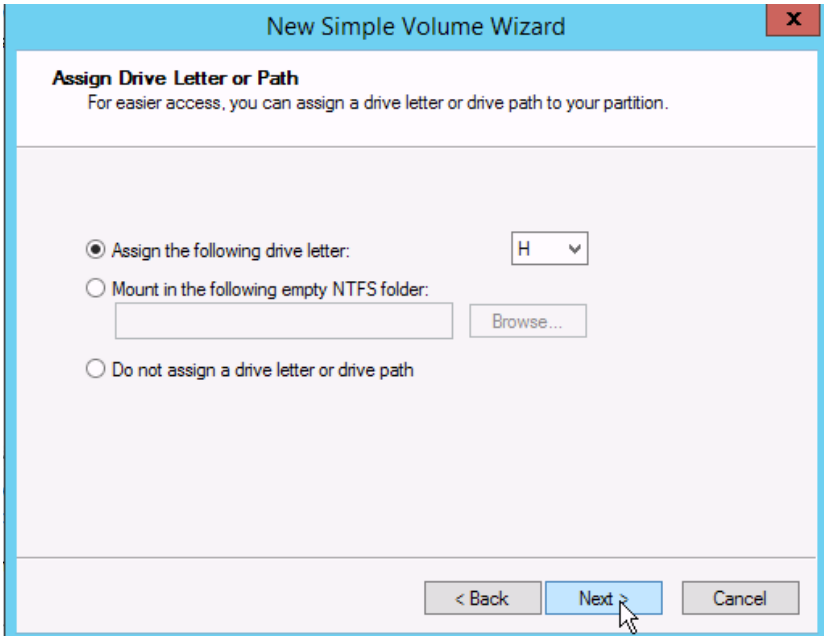

Figure 14

The next screen will have the format and file system options. Select the desired file system (ReFS is recommended), allocation unit size of 64K is recommended, and enter in a volume label. Click **Next** to continue (Figure 15).

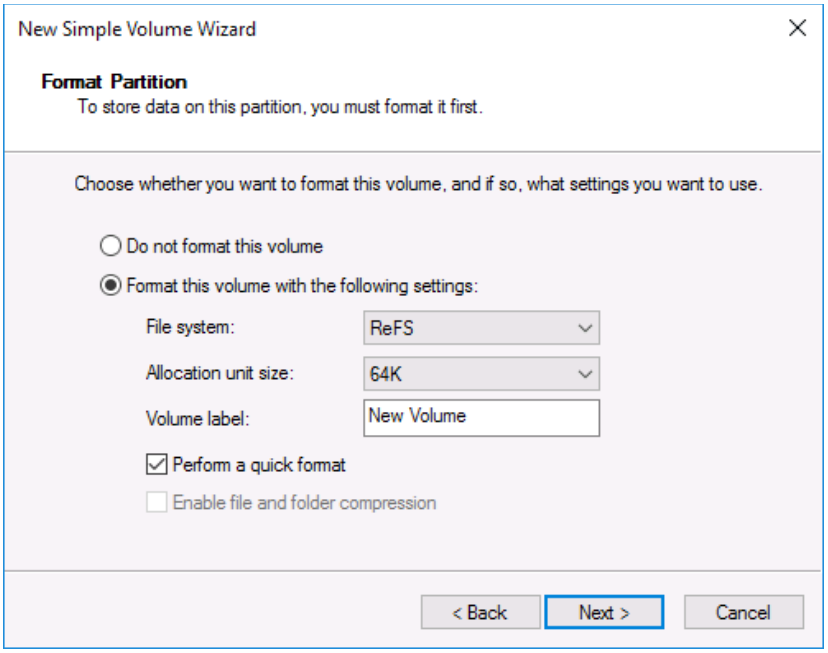

Figure 15

On the final screen, verify the settings are correct and click **Finish** (Figure 16). After a few moments, the new volume will be ready for use.

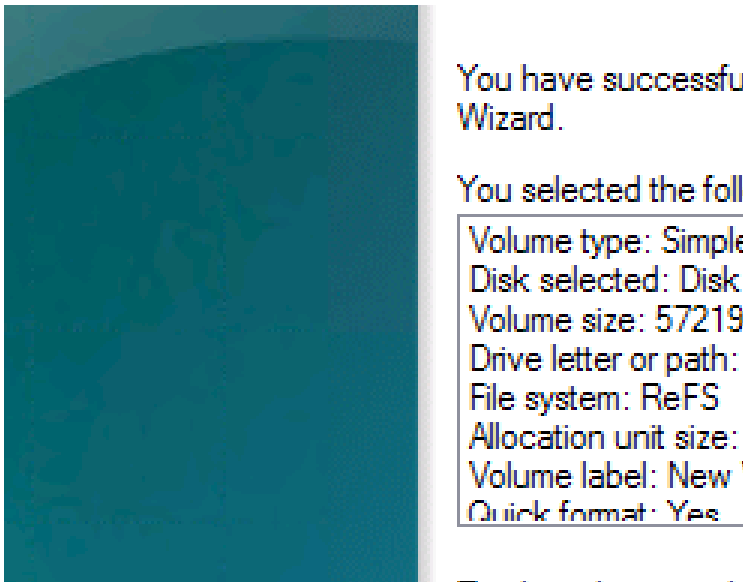

Figure 16

Once the volume has been created and assigned a drive letter, close the **Disk Management** window. The next step is to install Veeam Backup & Replication.

Veeam Backup & Replication installation process

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

1. Log into the S3260 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 screen with installation options (Figure 17). 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.

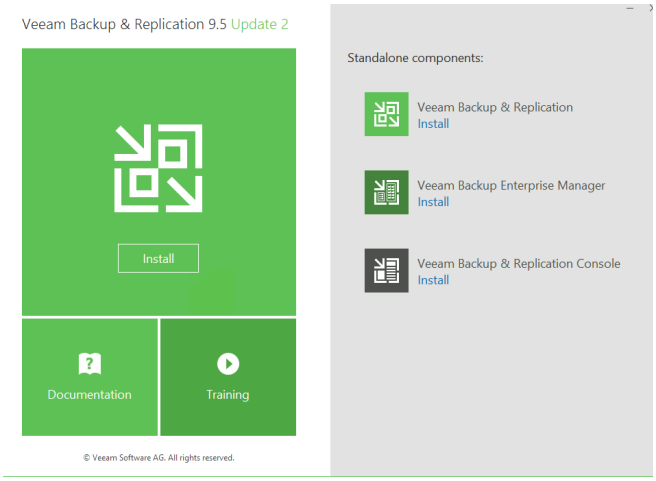

Figure 17

4. Click the **Install** link in the **Veeam Backup & Replication** section of the splash screen.
5. On the **Welcome** step of the wizard, click **Next** to start the installation.
6. To begin the installation, you must accept the license agreement (Figure 18). Read the license agreement, select the **I accept the terms in the license agreement** option and click **Next**.

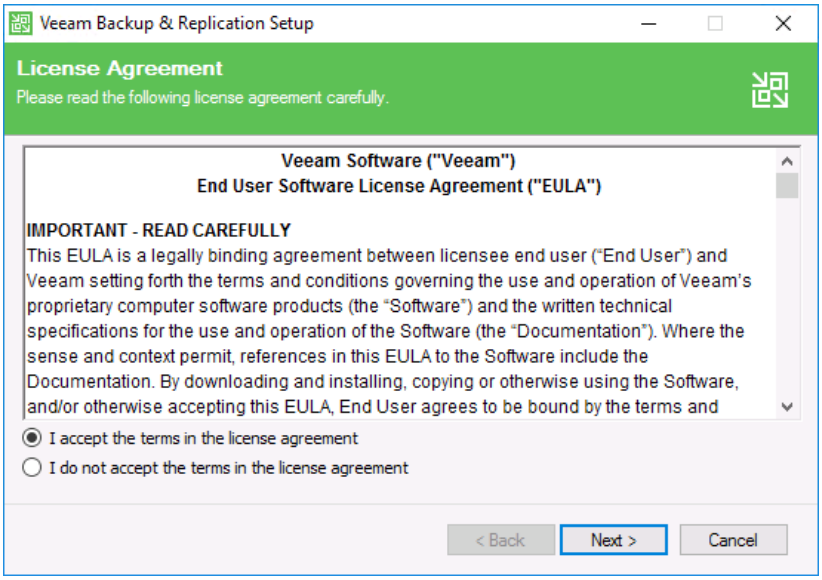

Figure 18

7. You can install Veeam Backup & Replication with a trial license that was sent to you after registration or a purchased full license. To install a license, click **Browse** and select a valid license file for Veeam Backup & Replication (Figure 19).

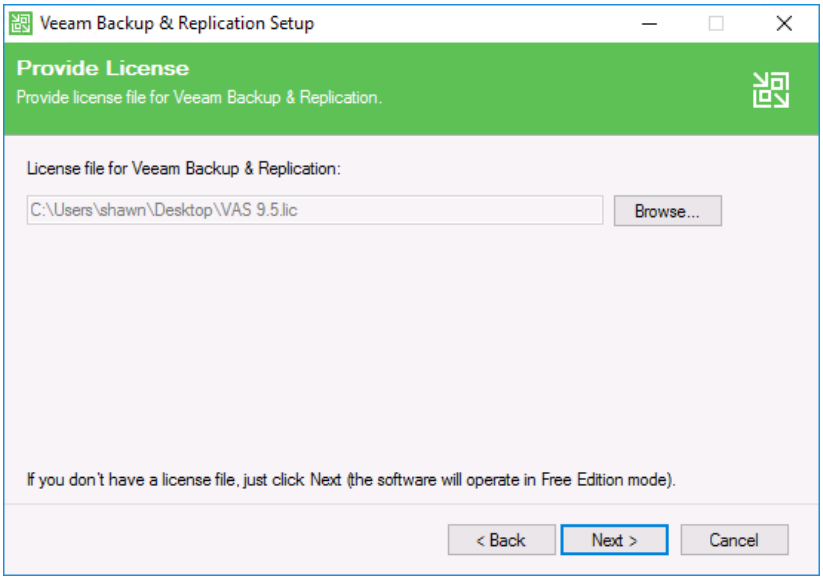

Figure 19

8. Select the components you want to install (Figure 20). The Veeam Backup & Replication setup includes the following components:

- Veeam Backup & Replication
- Veeam Backup catalog
- Veeam Backup & Replication console

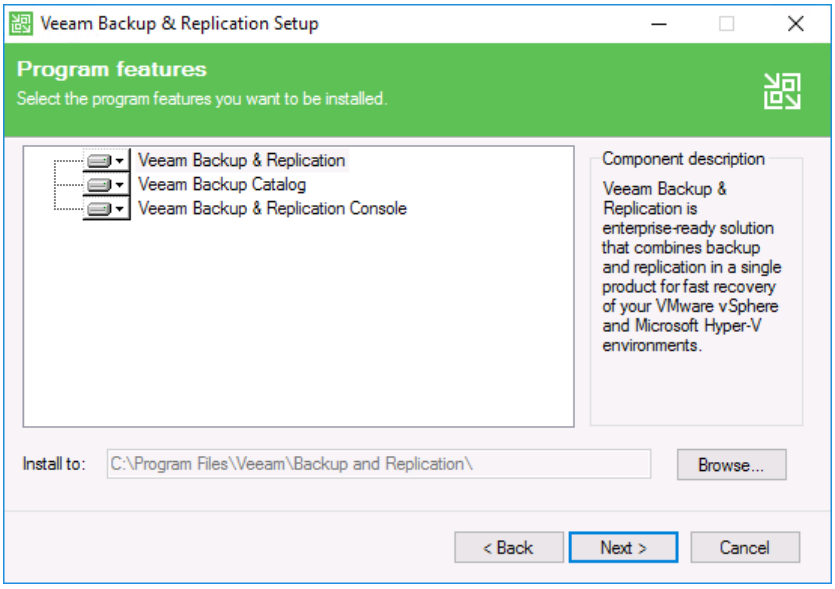

Figure 20

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 you to install missing software automatically (Figure 21).

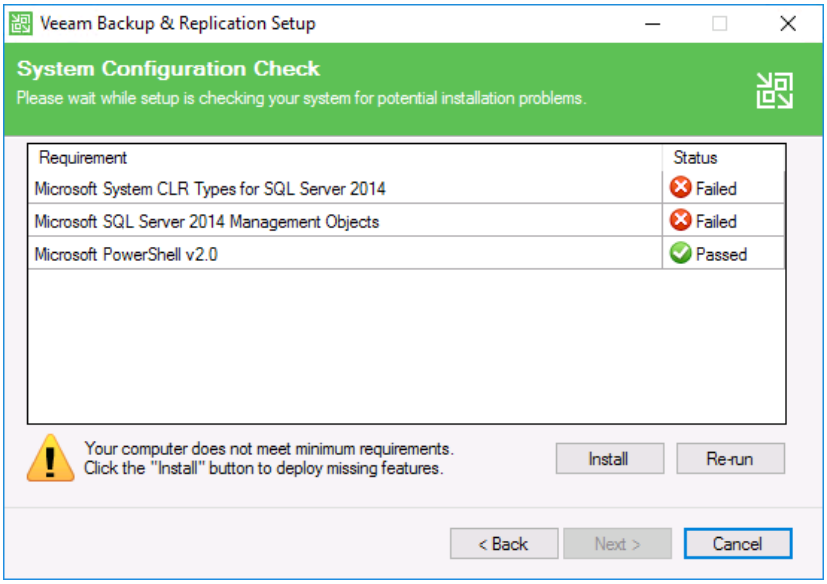

Figure 21

10. At this step, Veeam will list all pre-defined defaults for installation. If you wish to change any of the default directories or port numbers, check the **Let me specify different settings** box (Figure 22).

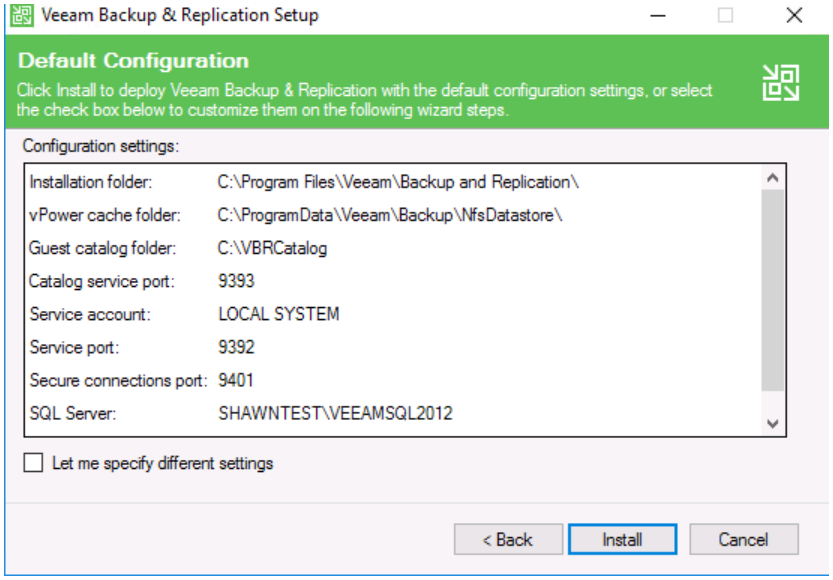

Figure 22

11. When the installation completes, click **Finish** to exit the setup wizard (Figure 23). You can now start Veeam Backup & Replication.

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
- SAN infrastructure to allow for integration with the various storage systems

Adding the Virtual Infrastructure

1. For building your backup infrastructure in a VMware vSphere environment, Veeam Backup & Replication supports the following types of servers (Figure 23):

- VMware server
- Microsoft 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). Note: Free ESXi is not supported.

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

Figure 23

For building your backup infrastructure in a Microsoft Hyper-V environment, Veeam Backup & Replication supports the following types of servers (Figure 24):

- Microsoft Hyper-V server
- Microsoft Windows server
- Linux server
- SMB3 server

You can connect both physical and virtual machines to the Veeam backup server and assign different roles to them. The table below describes which roles can be assigned to the different types of servers added to Veeam Backup & Replication.

Server Type	Source	Replication Target	Offhost Backup Proxy	Backup Repository
Microsoft Hyper-V Server (standalone Hyper-V host, SCVMM or Hyper-V cluster)	●	●	○	○
Microsoft Windows server	○	○	●	●
Linux server	○	○	○	●
SMB3 server	●	○	○	○

Figure 24

Before you connect a Hyper-V host, cluster or SCVMM, check the following prerequisites:

- File and printer sharing must be enabled in network connection settings of the added Hyper-V host. On every connected Hyper-V host, Veeam Backup & Replication deploys a set of components: *Veeam Installer Service, Veeam Transport Service and Hyper-V Integration Service*. If file and printer sharing is not enabled, Veeam Backup & Replication will fail to install these components.
- [For SCVMM] SCVMM Admin UI must be installed on the Veeam backup server. Otherwise, you will not be able to add SCVMM servers to Veeam Backup & Replication.

2. To add a server, select the desired server type to add, (Figure 25).

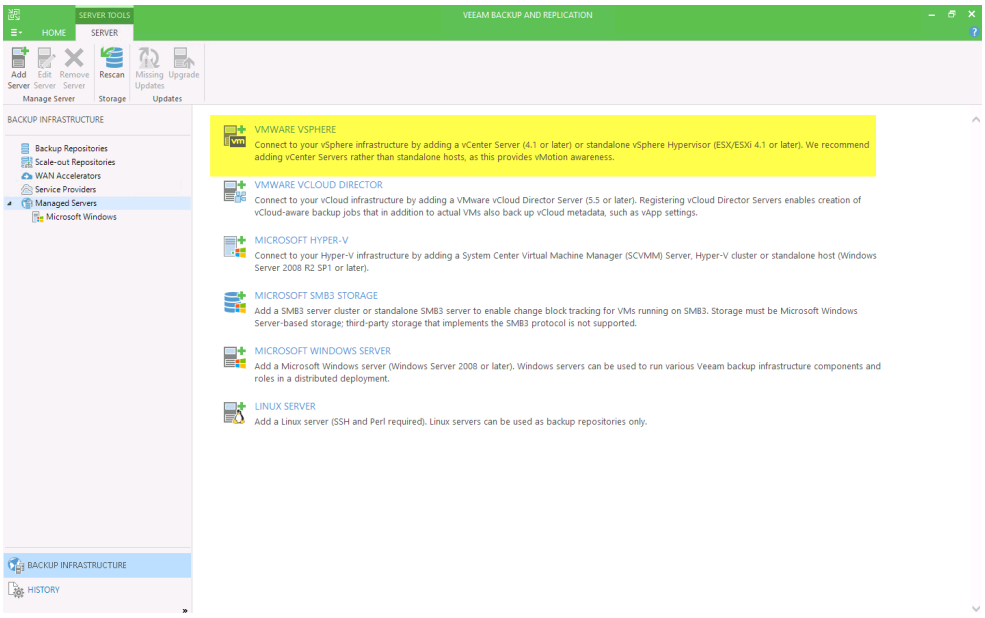

Figure 25

3. Enter the DNS name or IP address the server. A description can be entered for future reference (Figure 26). The default description will include information about the user who added the server, as well as the date and time of when the server was added. When done, click **Next**.

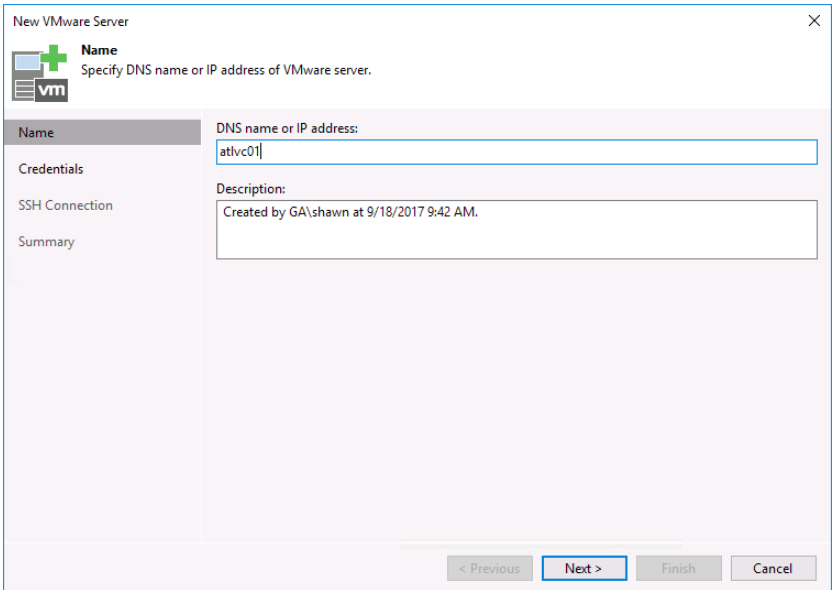

Figure 26

4. For VMware vSphere, skip to step 6. If adding Microsoft Hyper-V, next will be the **Server Type** selection (Figure 27). At this step, select from the three options: Microsoft System Center Virtual Machine Manager (SCVMM), Microsoft Hyper-V cluster or Microsoft Hyper-V server. Once the selection has been made, click **Next** to continue.

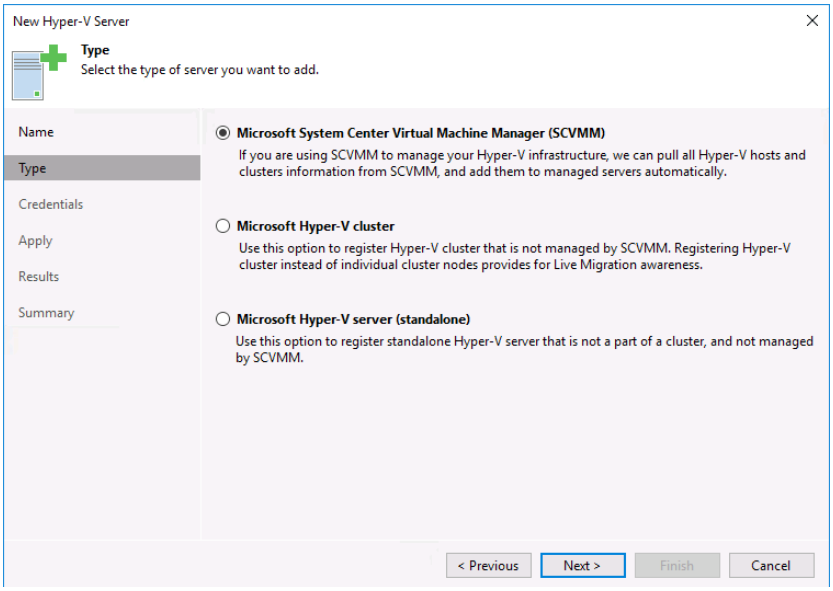

Figure 27

5. Next is the **Credentials**. On this screen click **Add** to input new credentials. For VMware, it is recommended that vCenter Admin be used if adding a vCenter Server and root credentials are needed for standalone ESX(i) hosts. Note: The username of the account should be provided in the DOMAIN\USERNAME format (Figure 28). Click **Next** to proceed.

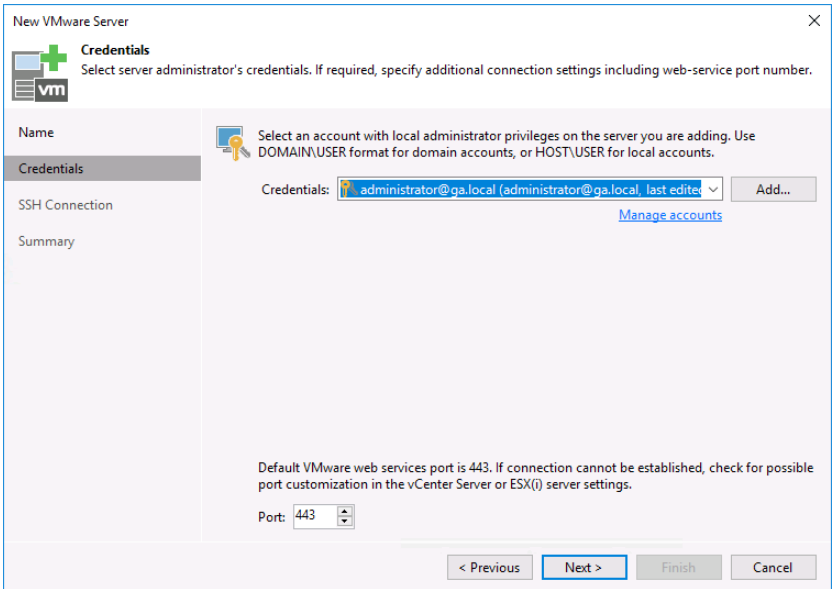

Figure 28

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 servers you need to add. ***Note:*** *The steps for servers other than VMware vSphere or Microsoft Hyper-V are not identical, but 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).*

Creating a new Veeam Backup Repository

By default, Veeam automatically creates a local backup repository (usually on the C:\ drive) of the Veeam Backup & Replication server. We will create a new backup repository so that we are storing backups on our newly created volume. The following steps will outline how to create the backup repository.

1. Select **Backup Infrastructure** from the lower left pane.

2. Right click on **Backup Repositories** and select **Add Backup Repository** (Figure 29).

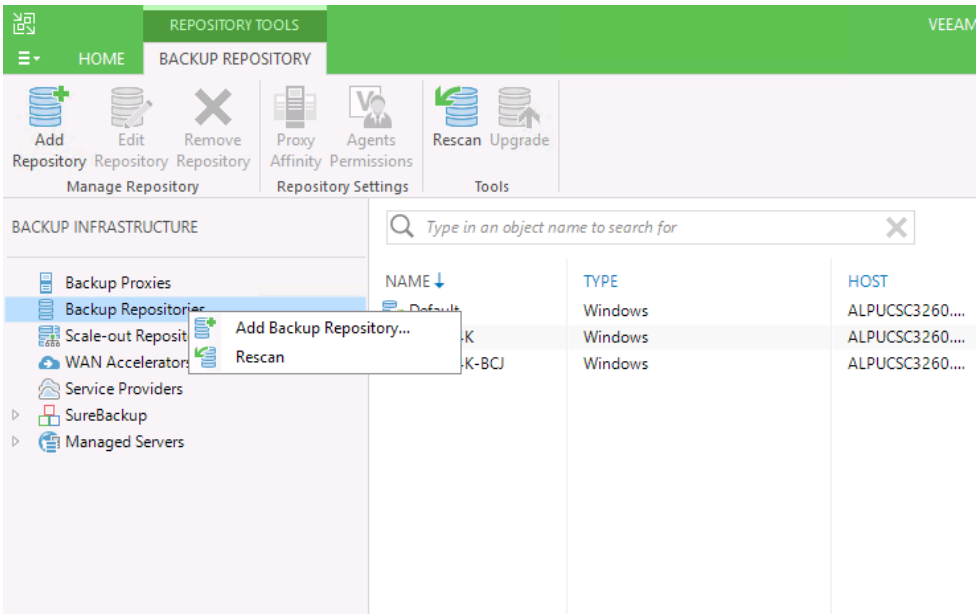

Figure 29

3. The New Backup Repository wizard will launch, the first screen is **Name** (Figure 30). Give the new backup repository a name. The description will be prepopulated, but you can optionally edit this field. Click **Next** to move on to **Type**.

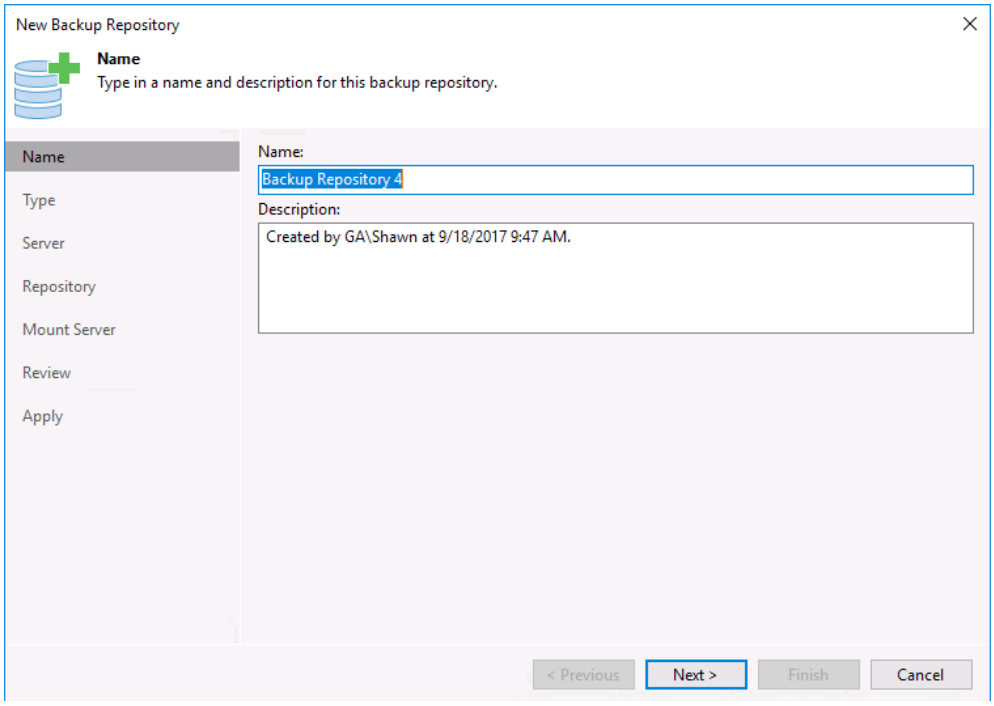

Figure 30

4. On the **Type** screen, there will be multiple options for the repository type. For the S3260, we will select **Microsoft Windows** server and click **Next** to continue to **Server** (Figure 31).

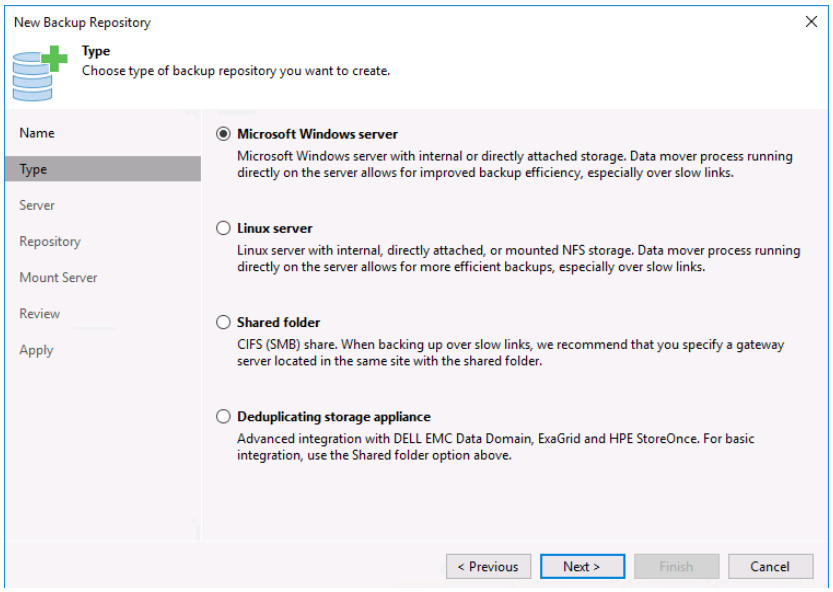

Figure 31

5. Moving on to the **Server** screen, click the **Populate** button for Veeam to detect all volumes on this server. Select the newly created volume and click **Next** to continue to the **Repository** screen (Figure 32).

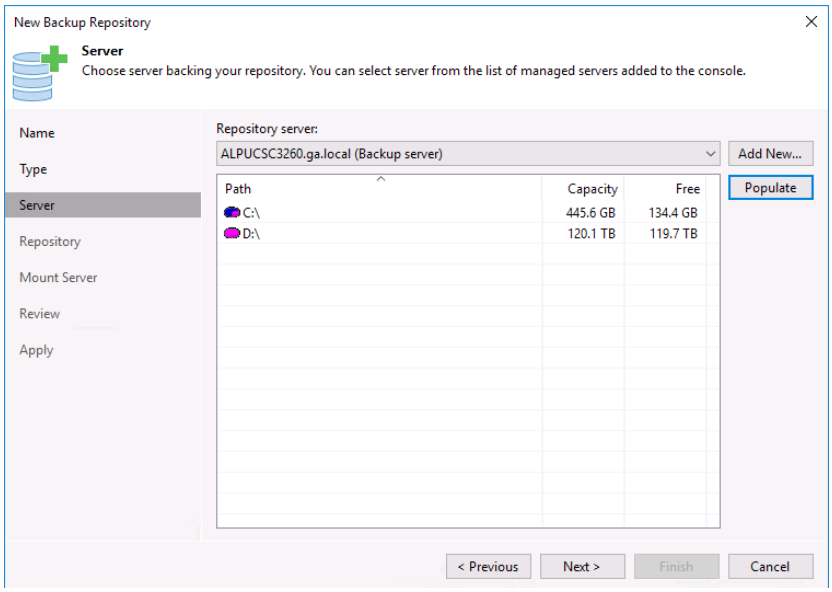

Figure 32

6. The **Repository** (Figure 33) screen is the most important screen in repository creation. First, specify a path on the new volume for which to store backups. Below **Location**, you will find the **Load control** settings. There are two options for load control, you can limit the maximum number of concurrent tasks or you may limit the combined data rate. Maximum concurrent tasks are the usual recommendation here, as the combined data rate can be difficult to determine. To make the determination on the maximum concurrent tasks, there will be some considerations. To avoid confusion, tasks are not jobs. There can be multiple tasks running for a single job if parallel processing is left on (parallel processing is on by default on new installs). The number of available CPU cores will determine the maximum number of concurrent tasks, Veeam will limit one task per available CPU core. Our example box has two physical processors, each with 18 physical cores, so both are capable of 36 concurrent tasks together. We recommend leaving a little headroom so we have limited the number of tasks to 34 in this example. Once the settings have been made, click **Next** to continue.

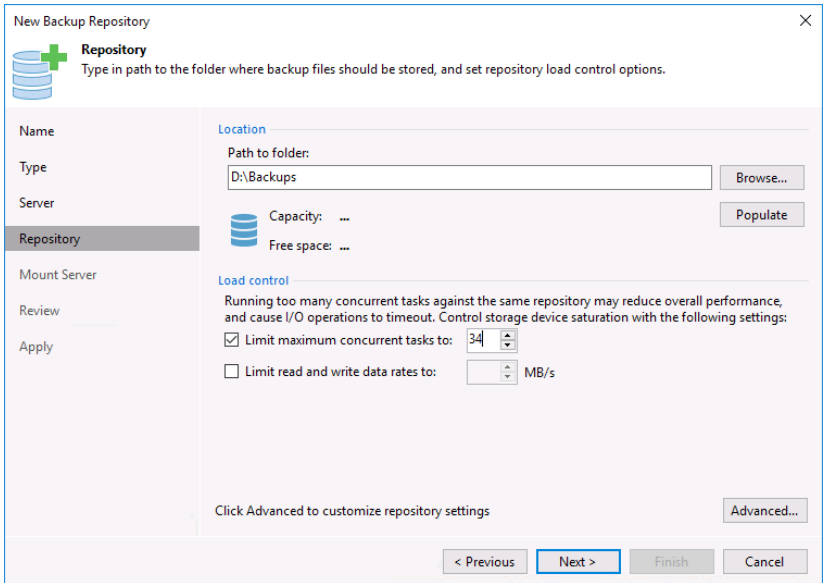

Figure 33

7. Click on the **Advanced** button in the lower right to make additional recommended settings.

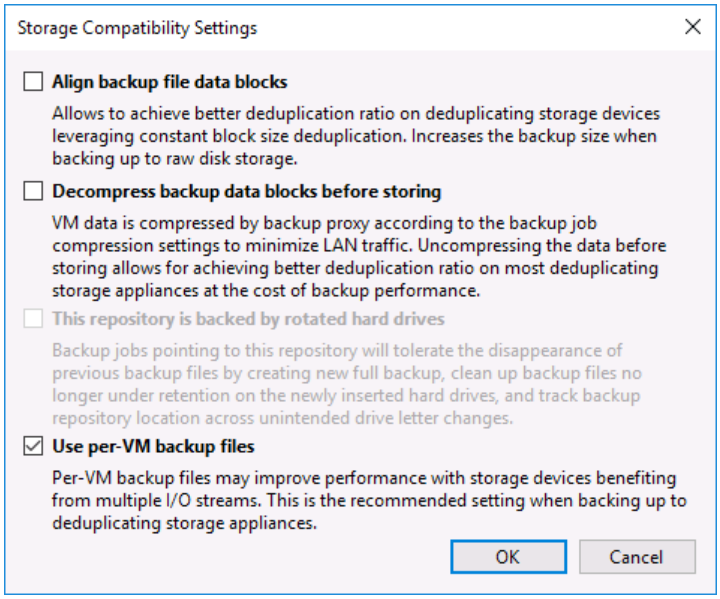

Figure 34

8. Check the **Use per-VM backup files** box, this recommended setting allows Veeam to create a backup file for each VM being backed up (Figure 34).

9. The next screen (Figure 35) is vPower NFS, and no changes need to be made here based on the configuration on the S3260. Click **Next** to proceed to the **Review** screen.

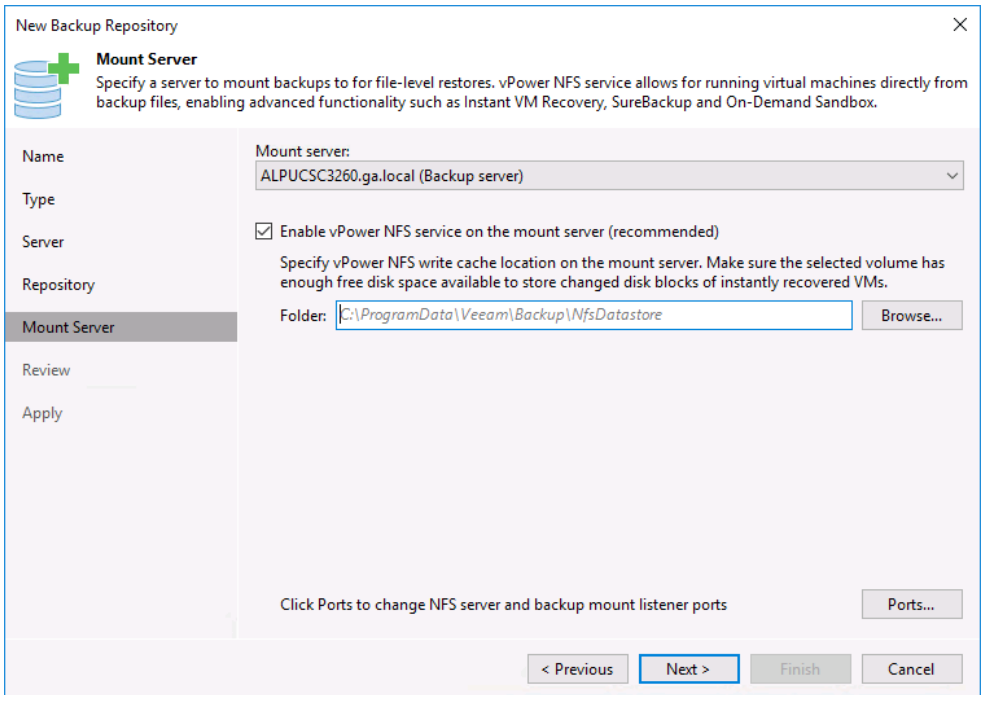

Figure 35

10. On the **Review** screen, verify the desired settings are accurate and click **Next** to continue (Figure 36).

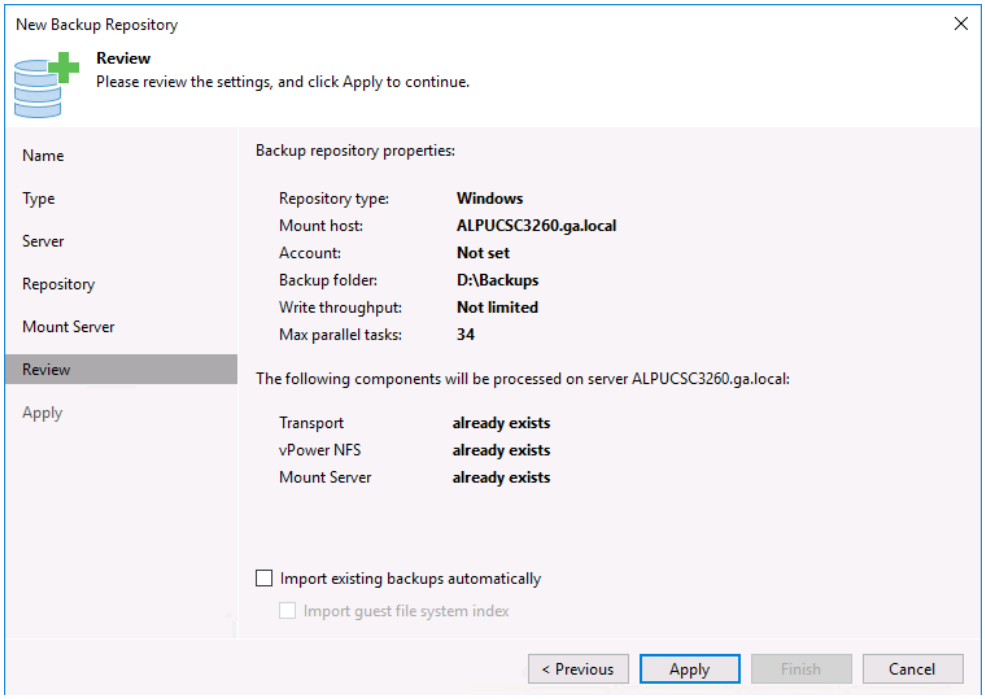

Figure 36

11. Veeam will now apply all the settings and create the new repository, click **Finish** to exit the wizard (Figure 37).

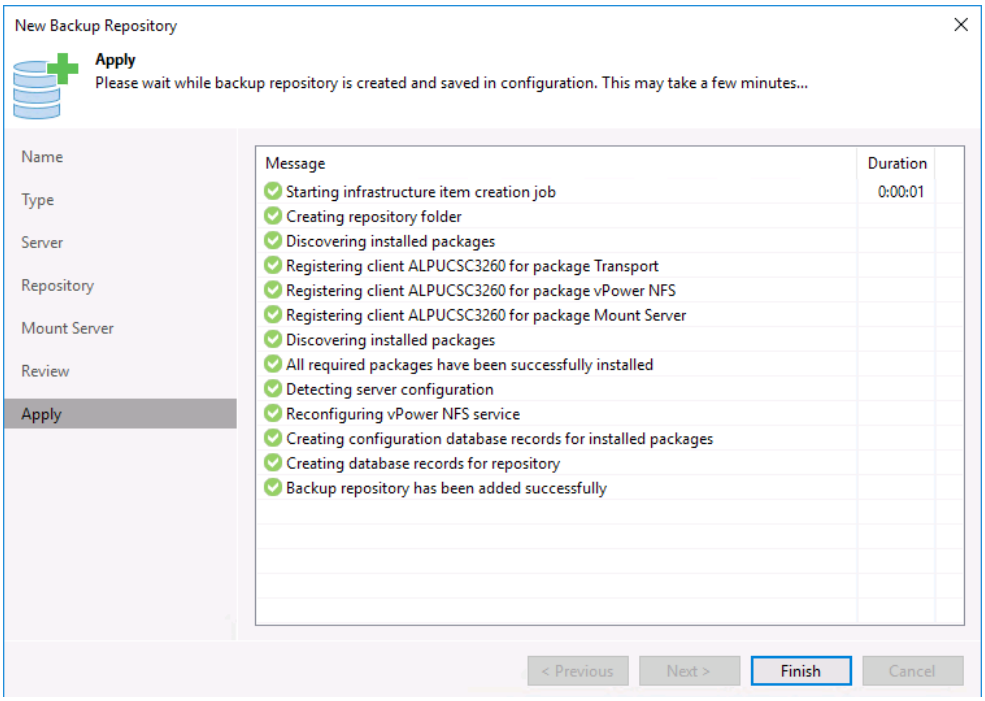

Figure 37

Veeam Backup Proxies

For VMware vSphere:

By default, for VMware there is already a VMware Backup Proxy present. This is the current server running Veeam Backup & Replication. Verify the VMware Backup Proxy settings by selecting **Backup Infrastructure—>Backup Proxies** and then right-clicking on the existing Backup Proxy and selecting **Properties** (Figure 38).

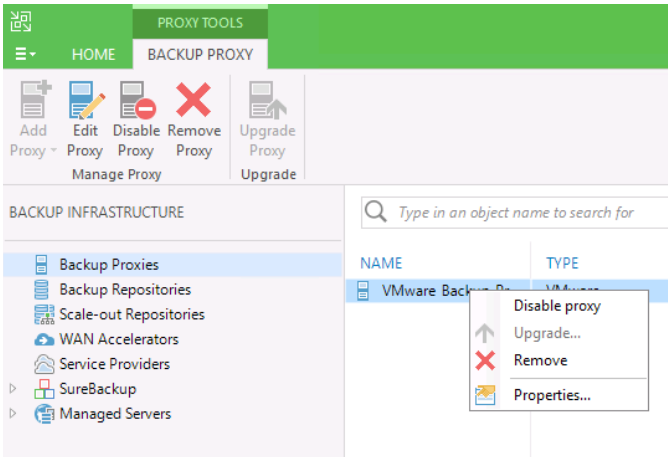

Figure 38

The **Edit VMware Proxy** settings will pop up (Figure 39). Ensure that the maximum concurrent tasks are as expected. Referencing the example we used earlier with the backup repositories, the server has two physical processors with 18 physical cores each. This results in a maximum of 36 concurrent tasks. For this guide, we will leave a little room for overhead and set the maximum number of concurrent tasks to 34.

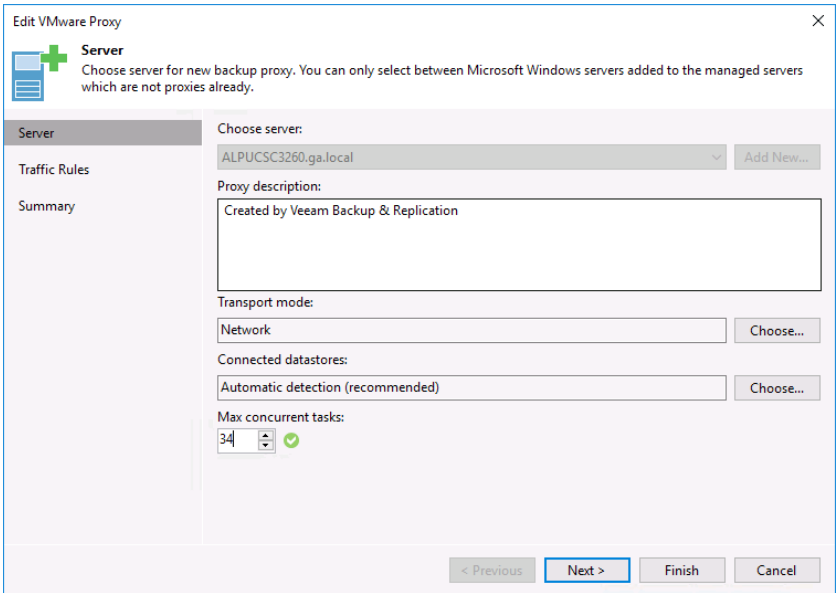

Figure 39

Additional Veeam Backup Proxies can be added to scale the Veeam backup infrastructure for any size environment. Additional S3260s can be used as Veeam Backup Proxies / Backup Repositories by installing a 64-bit Windows operating system (see pre-requisites on page 3). By adding additional S3260s to the backup infrastructure you can scale the backup solution linearly. Each unit provides not only additional backup storage space, but also compute and memory resources. Each S3260 can have up to 60 NL-SAS HDDs for additional backup storage. Backup Proxies can be added, as needed, to scale the backup infrastructure to suite any size environment. To add additional Veeam Backup Proxies, perform the steps below:

For Microsoft Hyper-V:

By default, the Hyper-V hosts are leveraged as On-Host Backup Proxies. To configure the S3260 as an Off-Host Backup proxy, the following pre-requisites must be met:

- Must be running the same version of Windows as the Hyper-V Hosts. The off-host proxy role can only be assigned to Windows Server 2008 R2, Server 2012, Server 2012 R2 and Server 2016.
- The Hyper-V role must be enabled on the off-host proxy.
- The source Hyper-V host and off-host backup proxy must be connected via a SAN configuration to the shared storage that supports VSS hardware providers.
- To create and manage volume shadow copies on the shared storage, you must install and properly configure a VSS hardware provider that supports transportable shadow copies. The VSS hardware provider must be installed on the off-host proxy and Hyper-V host. The VSS hardware provider is typically distributed as a part of client components supplied by the storage vendor.
- If you plan to perform off-host backup for a Hyper-V cluster with CSV, you must deploy an off-host backup proxy on a host that is not a part of a Hyper-V cluster. If the off-host backup proxy is deployed on a node of a Hyper-V cluster, the cluster will fail during VM data processing.

1. Select **Backup Infrastructure** from the lower left pane (Figure 40).
2. Right click on **Backup Proxies** and select **Add VMware Backup Proxy** or **Add Hyper-V Off-Host Backup Proxy**.

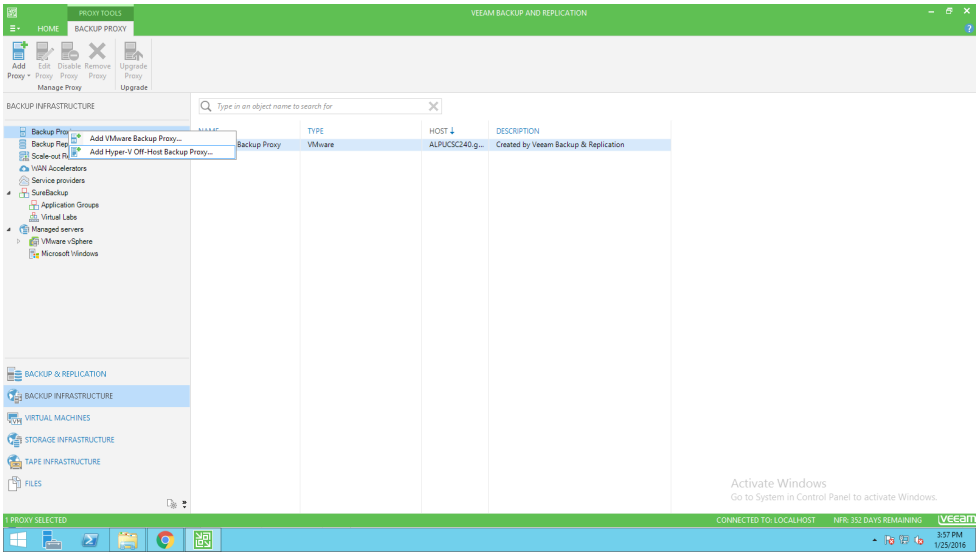

Figure 40

3. From the **Choose server** list, select a Microsoft Windows server to which you want to assign the off-host backup proxy role (Figure 41). If the server is not added to Veeam Backup & Replication yet, you can click **Add New** to open the **New Windows Server** wizard. If the server is already added to Veeam Backup & Replication, skip to step 8.

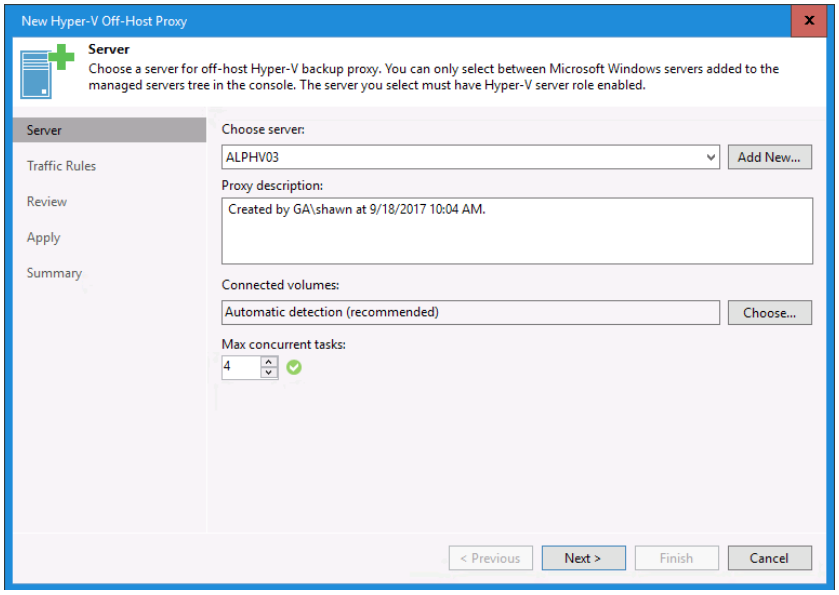

Figure 41

4. In the **New Windows Server** box enter a full DNS or IP address for the Microsoft Windows Server (Figure 42). You can also provide a description for future reference, by default the description contains information about the user who added the server, and the date and time of when the server was added. Click **Next** when complete.

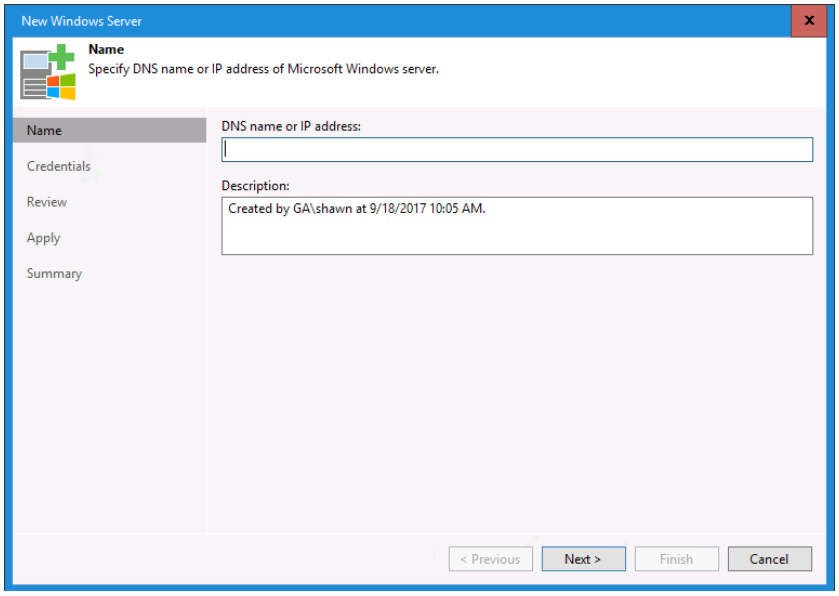

Figure 42

5. Next is the **Credentials** step of the wizard. Specify credentials for the newly added Windows Server (Figure 43). Veeam will used the provided credentials to deploy the following components:

- Veeam Installer service
- Veeam Transport service

To customize network ports used by Veeam Backup & Replication components, click **Ports**. By default, Veeam Backup & Replication components use the following ports:

- Veeam Installer service: port 6160
- Veeam Transport service: port 6162

If necessary, adjust port numbers as required.

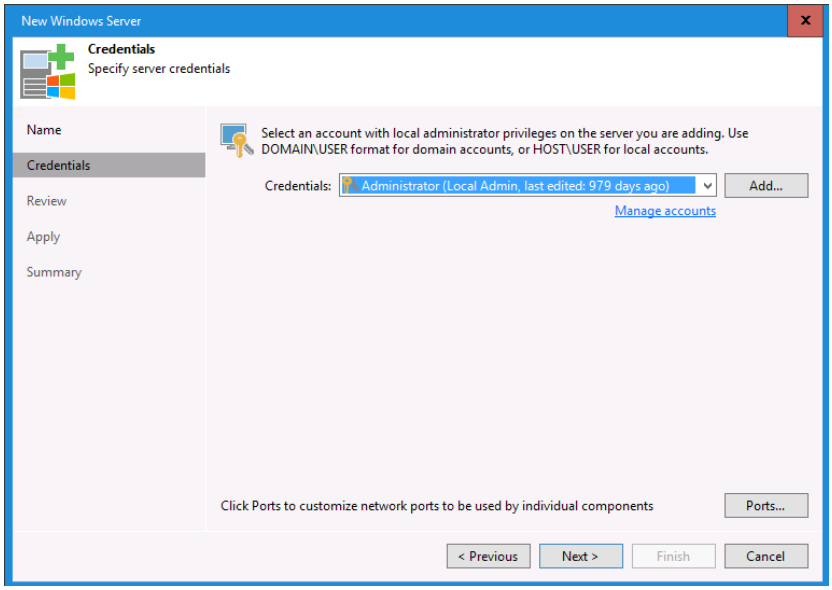

Figure 43

6. At the **Review** step of the wizard, review what Veeam Backup & Replication components are already installed on the server and what components will be installed. Click **Next** to add the Microsoft Windows Server to Veeam Backup & Replication.
7. At the **Apply** step of the wizard, complete the procedure for adding Microsoft Windows server. Review the details for the added Windows Server, click **Next** to proceed and finally click **Finish** to exit the wizard.
8. Back on the New Hyper-V Off-Host Proxy window (Figure 44), you can verify and edit the following:

- In the **Proxy description** field, provide a description for future reference. The default description contains information about the user who added the backup proxy, and the date and time of when the proxy was added.
- In the **Connected volumes** field, specify from which volumes the backup proxy should be able to retrieve VM data. By default, Veeam Backup & Replication automatically detects all volumes accessible by the backup proxy.
- You can set up the list of volumes manually, for example, if you want a backup proxy to work with specific volumes. Click **Choose** on the right of the **Connected datastores** field, choose **Manual selection** and add datastores from which the backup proxy should retrieve VM data.
- In the **Max concurrent tasks** field, specify the number of tasks that the backup proxy must handle in parallel. If this value is exceeded, the backup proxy will not start a new task until one of current tasks is finished. The recommended number of concurrent tasks is calculated automatically based on available resources. Veeam backup proxies with multi-core CPUs can handle more concurrent tasks. For example, for a four-core CPU, it is recommended to specify maximum two concurrent tasks, for an eight-core CPU — six concurrent tasks. When defining the number of concurrent tasks, keep in mind network traffic throughput in your virtual infrastructure.

When ready, click **Next** to proceed.

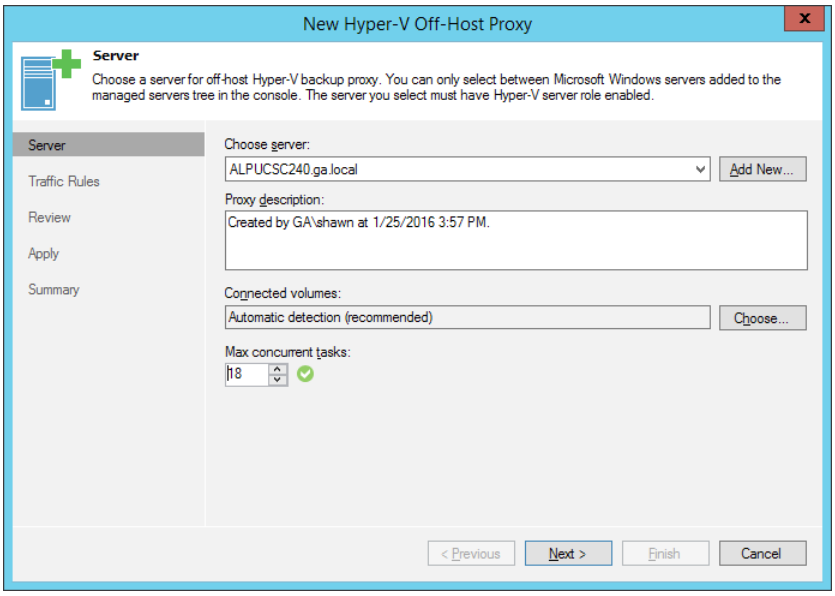

Figure 44

9. At the **Traffic** step of the wizard, configure throttling rules to limit the outbound traffic rate for the backup proxy (Figure 45). Throttling rules can help you manage bandwidth usage and minimize the impact of data protection and DR tasks on network performance. Click **Next** when ready to proceed.

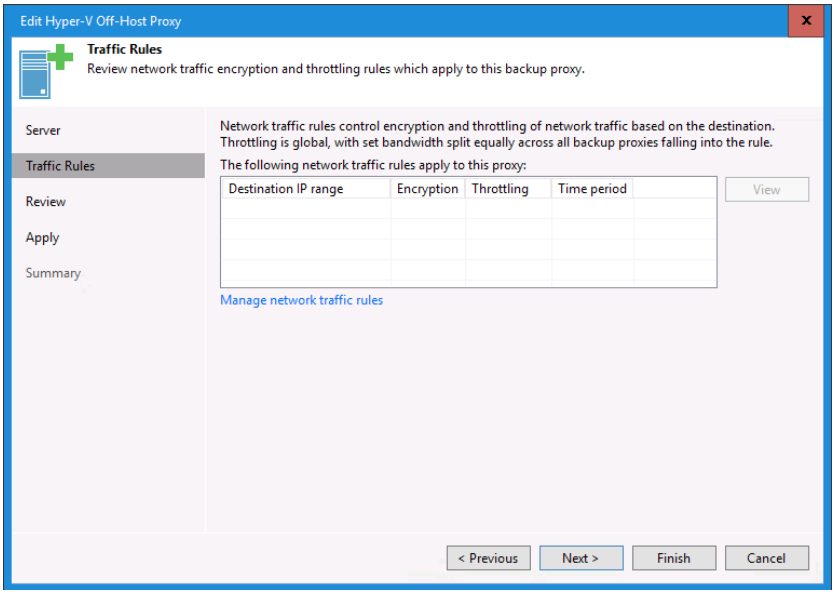

Figure 45

10. At the **Review** step of the wizard, review what Veeam Backup & Replication components are already installed on the backup proxy and what components will be installed (Figure 46). Click **Next** to add the new backup proxy.

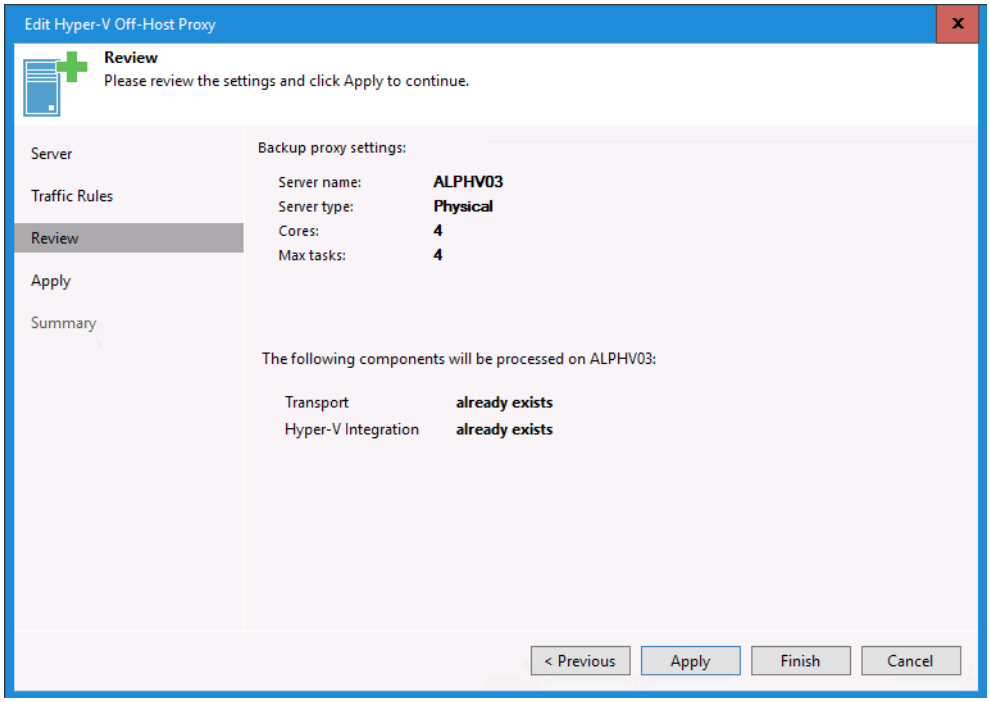

Figure 46

11. At the Apply step of the wizard, complete the procedure of backup proxy configuration. Review the details for the added backup proxy. Click Next and then Finish to exit the wizard.

Now that Veeam Backup & Replication is configured, backup jobs and many other jobs may be configured to use the newly available volume. Additional S3260's configured as a Veeam Backup Proxy / Backup Repository can deployed off site for additional protection or archival of your backups. Veeam backup copy jobs can be leveraged to move backup data to these off-site locations. If further installation or operational detail is needed, refer to the Veeam Backup & Replication user guides for more detail. You can find the Veeam user's guide below:

User Guide for VMware vSphere

User Guide for Microsoft Hyper-V

About the Authors

Stefan Renner

With 11 years of IT-Experience in designing and implementing Enterprise Datacenters, he is the responsible Alliance Systems Engineer for NetApp and Cisco at Veeam Software. Before joining Veeam he worked 7 years as IT-Consultant with a strong focus on NetApp, Cisco, VMware and Data Protection in projects all over EMEA. Stefan lives near Nuremberg in Germany.

Twitter: @rennerstefan

Shawn Lieu

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

Twitter: @shawnlieu

About Veeam Software

Veeam® recognizes the new challenges companies across the globe face in enabling Intelligent Data Management for the Hyper-Available Enterprise™, where business that must operate 24.7.365. To address this, Veeam has pioneered a new market of Availability for the 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 more than 294,000 customers worldwide, and adds an average of 4,000 new customers each month. 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.

Intelligent Data Management

fuels the ***Fortune 500***

VEEAM

Intelligent Data Management
for the Hyper-Available Enterprise