



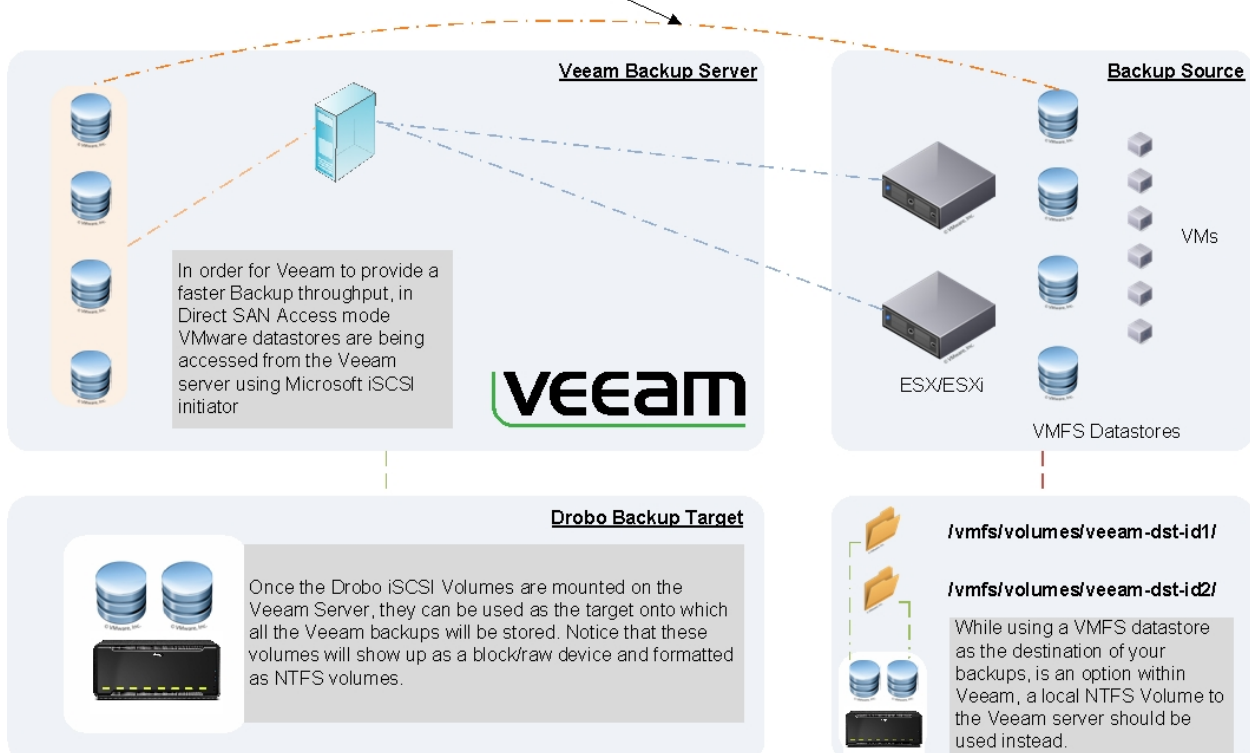
This document shows you how to use a Drobo iSCSI SAN Storage array with Veeam Backup & Replication version 5 in a VMware environment. Veeam provides fast disk-based backup and recovery of virtual machines (VMs), while Drobo provides an ultra-easy-to-use and scalable disk-based storage target. The combined solution provides reliable and affordable disk-based backup storage for your virtualized server environment. With this solution, users have the ability to recover instantly from many different restore points on disk media vs. tape and enjoy faster backups and restores without the hassle of managing catalogs of tapes.



Topics

- Veeam basics
- Creating and mounting a Drobo volume
- Using Microsoft iSCSI Initiator to connect to VMware datastores
- Adding a new vCenter Server
- Creating a new Veeam Backup job
- Restoring virtual machines with Veeam Backup

Direct SAN Access Mode: The Veeam server will use the connected iSCSI volumes to talk to the VMware datastores. This approach provides a much faster backup throughput.





What You Will Need

- Drobo model B800i or B1200i
- Drobo Dashboard management software (most recent version)
- Enterprise-grade 7200RPM SAS or SATA disk drives (recommended)
- Windows Server 2008 R2 (dedicated server recommended)
- Veeam Backup and Replication version 5

Veeam Basics

Veeam has changed the way IT administrators think about recovery time frames and procedures. Backup and replication v5 has greatly simplified the steps needed to perform backups, restores, as well as true 99.99% uptime requirements. As a Windows-based application, Veeam software can be installed on either a guest OS in a virtual environment or on a physical server. The advantage of installing on a physical server is that backup storage can be directly attached and deliver the best throughput—if attaching a tape library to the same physical server is still required in addition to disk-based backup. Further, installing Veeam as a physical server offloads the CPU burden of the backups from the VMware cluster, benefiting compression and deduplication.

Veeam Backup & Replication version 5 provides:

- Instant recovery so that you can start a virtual machine from the backup
- Built in deduplication and compression
- U-AIR—item-level recovery from any virtualized application
- Ability to allow users to restores their own files
- SureBackup—backup recovery verification
- Replication for DR

Backup Modes

Veeam Backup & Replication supports different backup methods depending on the environment. Direct SAN Access is preferred and is featured in this document. Because Veeam takes advantage of VMware Storage APIs, it is the most efficient method. Three transport modes are available:

- *Direct SAN Access.* Supported only for VMs that reside on a block storage device (iSCSI). In Direct SAN Access mode, Veeam runs on a physical server and backs up VM datastores directly without going through the ESX/ESXi host. Direct SAN Access mode also adds failover safety mechanisms. Note that if Direct SAN Access mode becomes unavailable, Veeam fails over to Network mode in order to complete the backup.
- *Virtual Appliance.* In this mode Veeam is installed on a VM and disks from the VMs that are to be backed up are “hot-added” to the Veeam VM. Data is read directly from the storage stack instead of over the network. The advantage of using Virtual Appliance mode is its ability to directly back up VMs on NFS storage.
- *Network* The least efficient mode because the Veeam Backup & Replication server is connected to the ESX/ESXi host over the network using Network Block Device Protocol (NBD) to connect to the VM datastore. This adds additional network traffic and resource usage on the host, which can negatively impact VMs running on the host.



Veeam Hardware Requirements

Veeam recommends dedicating a server to be used solely for Veeam backups. While a VM host can be the backup server, a physical host would tend to outperform a virtual host due to dedicated resources and no virtualization layer. Make the decision based on the amount of data to be backed up and features you might want to use in Veeam (for example, compression and deduplication).

Network Considerations

By default Veeam uses the LAN or primary network interface to communicate with VMware servers and/or the vCenter server. However, based on VMware best practices and general iSCSI SAN best practices, management and messaging traffic should be isolated from the iSCSI/SAN traffic. This of course increases SAN performance and offloads the LAN. Therefore it is strongly recommended that if Veeam is installed on a physical host, two or more interfaces should be dedicated following VMware best practices so that when performing backups, Veeam can take advantage of Direct SAN access mode, allowing for faster backup throughput. For the network, use different VLANs or even different Ethernet switches to isolate traffic and protect service levels.

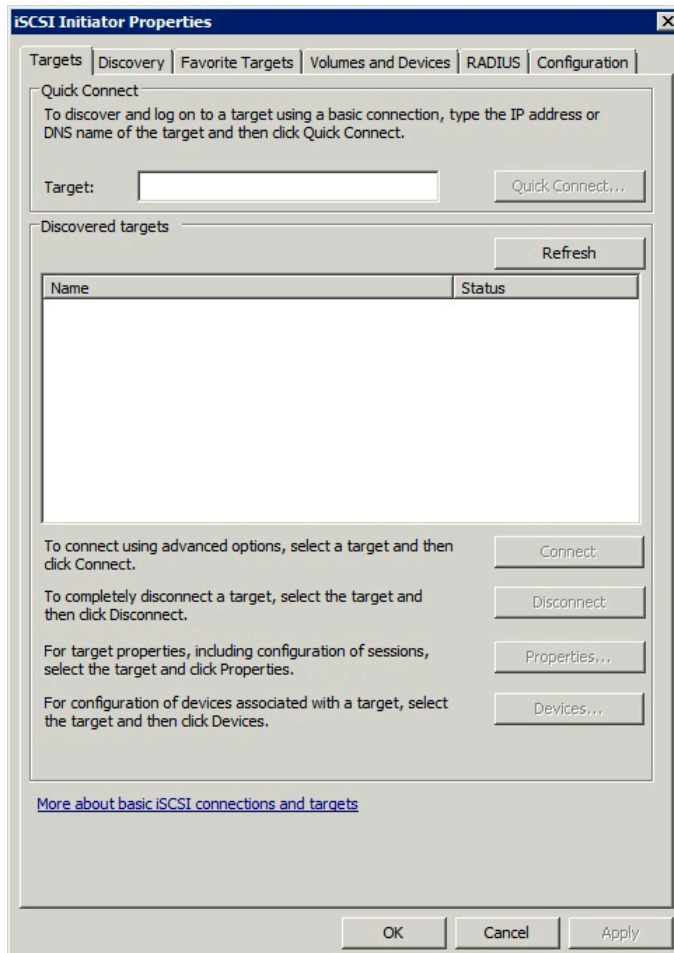


Creating and Mounting a Drobo Volume

Follow the directions in the Drobo Online User Guide to configure the Drobo and create an NTFS volume:
<http://www.drobo.com/support/documentation.php>

STEP 1

In this step, two Drobo volumes are created using Drobo Dashboard. Do NOT install Drobo Dashboard on the Veeam server but on a different host. Once the volume is created, it will be the repository in which Veeam stores its backups.



Mount these volumes using Microsoft iSCSI Initiator on the Veeam server. Once the volumes have been created, using Drobo Dashboard to open Microsoft iSCSI Initiator on the Veeam server: **Start > Administrative Tools > iSCSI Initiator**

If you have not used Microsoft iSCSI Initiator before, you will notice that the list of volumes is empty.

Click the **Discovery** tab.



STEP 2

The screenshot shows the 'iSCSI Initiator Properties' dialog box with the 'Discover Target Portal' tab selected. The dialog has a title bar with a close button. Below the title bar, there's a section for entering the IP address or DNS name and port number. The IP address field contains '172.32.16.53' and the port field contains '3260'. There are buttons for 'Advanced...', 'OK', and 'Cancel'. Below this, there's a section for removing a target portal with a 'Remove' button. At the bottom, there's a section for iSNS servers with a 'Refresh' button, a list box for server names, and buttons for 'Add Server...' and 'Remove'. A link 'More about Discovery and iSNS' is also present. At the very bottom, there are 'OK', 'Cancel', and 'Apply' buttons.

iSCSI Initiator Properties

Discover Target Portal

Enter the IP address or DNS name and port number of the portal you want to add.

To change the default settings of the discovery of the target portal, click the Advanced button.

IP address or DNS name: 172.32.16.53 Port: (Default is 3260.) 3260

Advanced... OK Cancel

To remove a target portal, select the address above and then click Remove. Remove

iSNS servers

The system is registered on the following iSNS servers: Refresh

Name

To add an iSNS server, click Add Server. Add Server...

To remove an iSNS server, select the server above and then click Remove. Remove

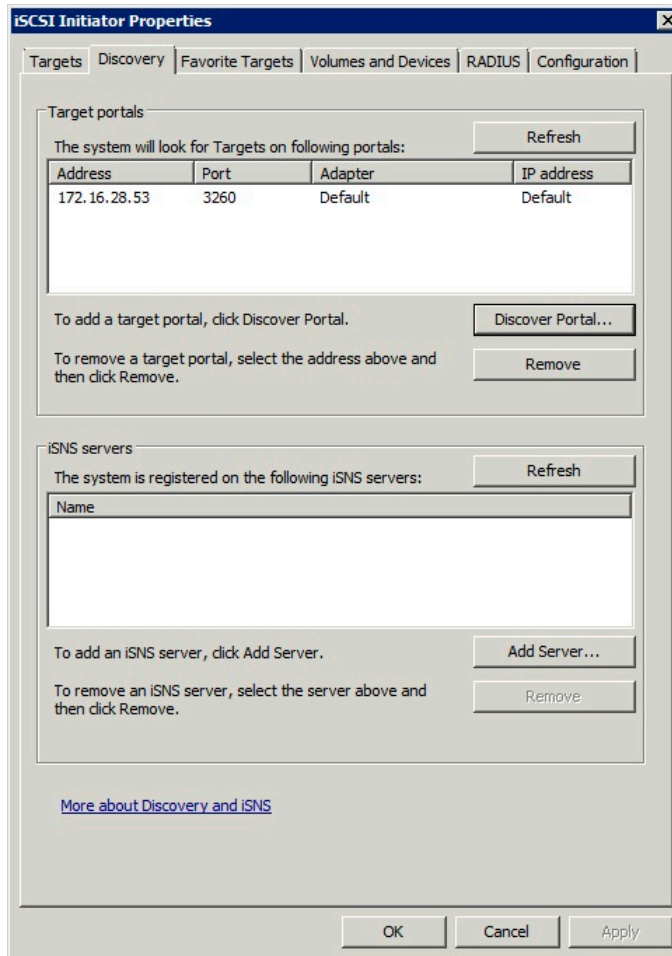
[More about Discovery and iSNS](#)

OK Cancel Apply

Click the **Discover Portal** button, add the IP address of the Drobo, and click **OK**.



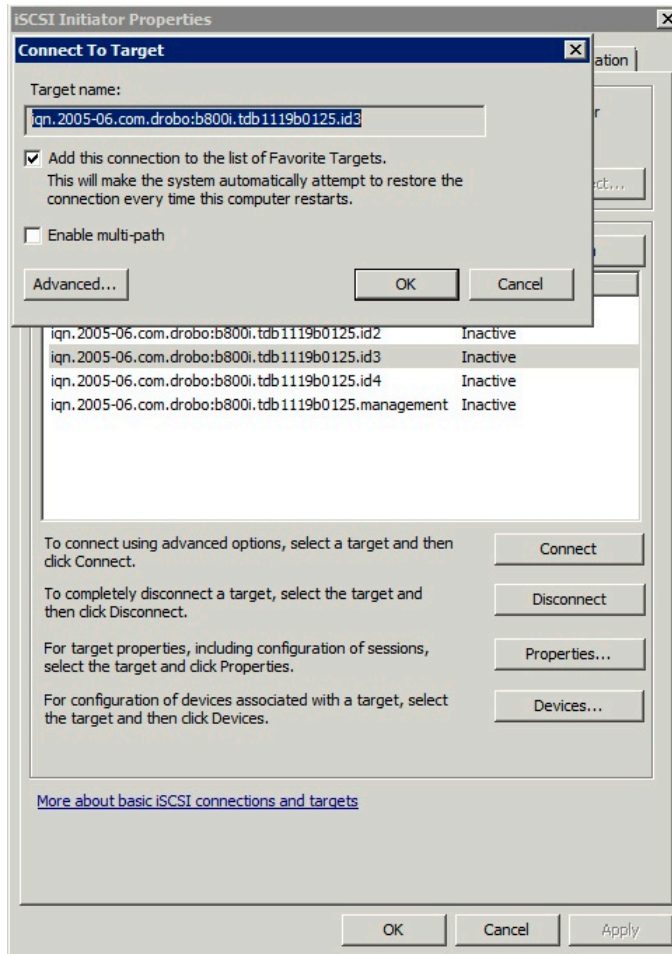
STEP 3



The address is now added in the Target portals list. Click the **Targets** tab.



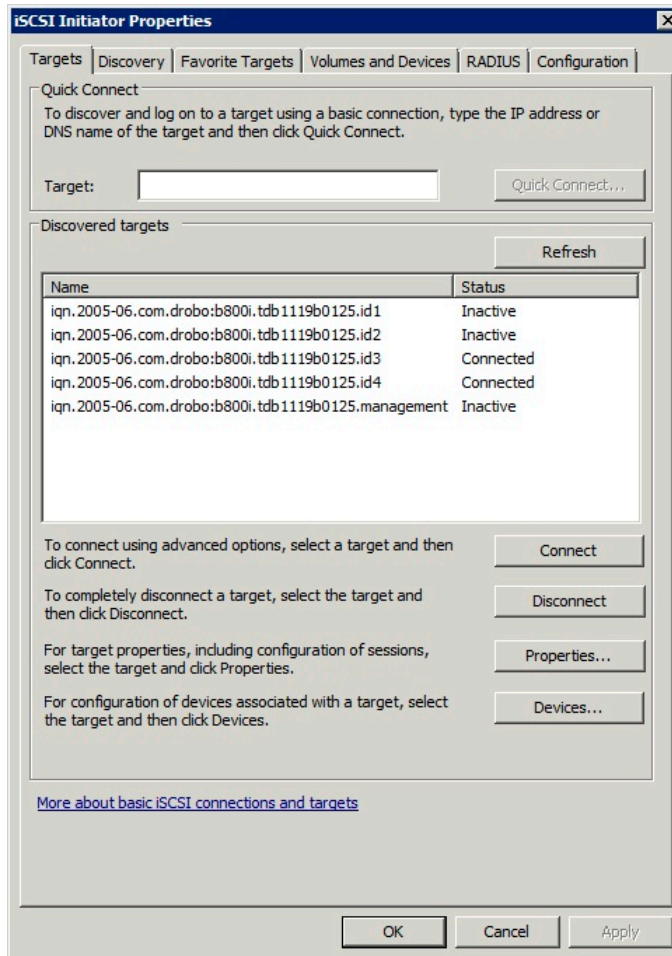
STEP 4



Select the volume you wish to mount, click **Connect**. In the pop-up dialog, and click **OK**.



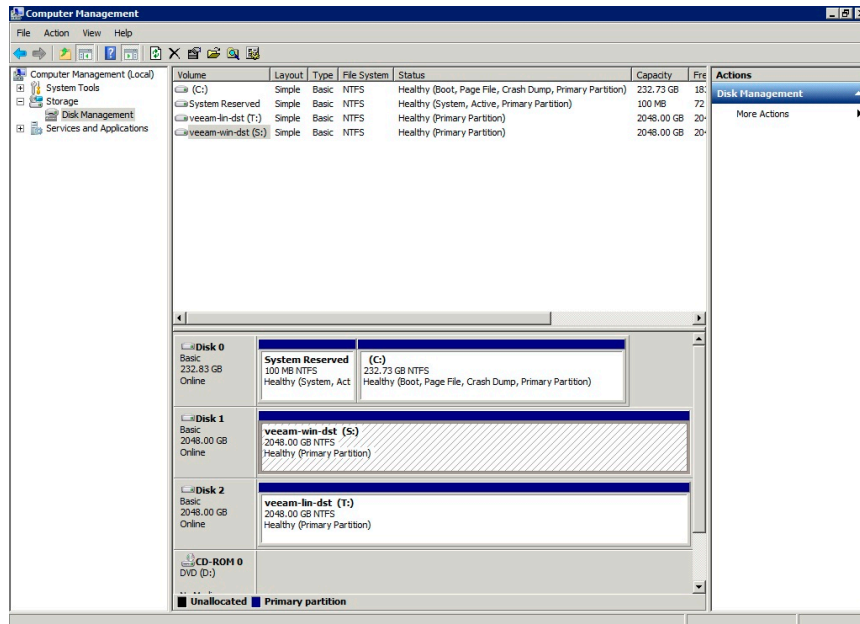
STEP 5



Once you have selected and connected the volumes you want to use, click **OK** to close Microsoft iSCSI Initiator.



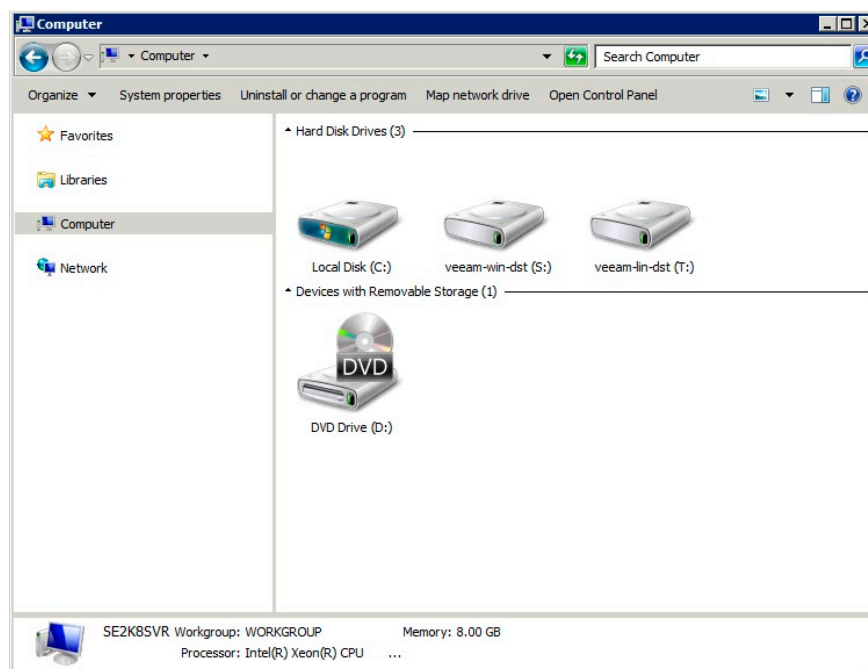
STEP 6



To open Computer Management, choose **Start > Administrative Tools > Computer Management**.

Go to the Disk Management section under Storage. You will now see two additional disks, which are the iSCSI volumes you have just connected to. If the volumes are not mounted, mount them and assign them a drive letter.

STEP 7



A window prompts you to select a folder. In this example, a folder that resides on one of the Drobo volumes is selected.

To learn about Drobo and iSCSI, visit: <http://www.drobo.com/resources/iscsi.php>

NOTE: Veeam requires Microsoft Windows diskpart automount feature to be *disabled* when the backup mode is Direct SAN Access. However, Drobo Dashboard requires that this feature be *enabled*, so that volumes can be created, mounted, and formatted in Drobo Dashboard. Therefore it is recommended that Drobo Dashboard be installed on a host that is not the Veeam server.



Using Microsoft iSCSI Initiator To Connect to VMware Datastores

As discussed previously, Microsoft iSCSI Initiator is used on the host where Veeam is installed to allow Veeam to:

- Connect but NOT mount the ESX/ESXi datastores on which the VMs reside
- Connect but NOT mount the ESX/ESXi datastores to which VMs can be backed up

NOTE: This step is very similar to the previous section, in which Microsoft iSCSI Initiator was used to connect to iSCSI volumes. However, because these volumes are formatted as VMFS, Windows does not show them in My Computer. They do, however, appear as volumes in Disk Management.

There is a potential risk that the VMFS volumes are re-signatured by Windows if you attempt to initialize one of these volumes and or assign it a drive letter. To prevent this from happening, Veeam recommends that the diskpart automount be disabled. This is not applicable if you are using Veeam Backup & Replication version 5, since it will automatically disable automount.

For more information, visit:

<http://www.veeam.com/blog/using-the-iscsi-initiator-within-veeam-backup-replication-in-a-vm.html>



STEP 1

The screenshot shows the 'iSCSI Initiator Properties' dialog box with the 'Configuration' tab selected. The dialog has a title bar with a close button. Below the title bar are tabs: 'Targets', 'Discovery', 'Favorite Targets', 'Volumes and Devices', 'RADIUS', and 'Configuration'. The 'Configuration' tab contains the following text: 'Configuration settings here are global and will affect any future connections made with the initiator.' followed by 'Any existing connections may continue to work, but can fail if the system restarts or the initiator otherwise tries to reconnect to a target.' and 'When connecting to a target, advanced connection features allow specific control of a particular connection.' Below this is a text field for 'Initiator Name:' containing 'iqn.1991-05.com.microsoft:w2k8sr2vdicm.solutions.drobo.com'. To the right of the text field is a 'Change...' button. Below this is a 'To modify the initiator name, click Change.' label. Further down are three buttons: 'CHAP...', 'IPsec...', and 'Report'. To the left of these buttons are labels: 'To set the initiator CHAP secret for use with mutual CHAP, click CHAP.', 'To set up the IPsec tunnel mode addresses for the initiator, click IPsec.', and 'To generate a report of all connected targets and devices on the system, click Report.' At the bottom left is a link 'More about Configuration'. At the bottom right are three buttons: 'OK', 'Cancel', and 'Apply'.

iSCSI Initiator Properties

Targets | Discovery | Favorite Targets | Volumes and Devices | **RADIUS** | Configuration

Configuration settings here are global and will affect any future connections made with the initiator.

Any existing connections may continue to work, but can fail if the system restarts or the initiator otherwise tries to reconnect to a target.

When connecting to a target, advanced connection features allow specific control of a particular connection.

Initiator Name:
iqn.1991-05.com.microsoft:w2k8sr2vdicm.solutions.drobo.com

To modify the initiator name, click Change. Change...

To set the initiator CHAP secret for use with mutual CHAP, click CHAP. CHAP...

To set up the IPsec tunnel mode addresses for the initiator, click IPsec. IPsec...

To generate a report of all connected targets and devices on the system, click Report. Report

[More about Configuration](#)

OK Cancel Apply

To open Microsoft iSCSI Initiator, choose **Start > Administrative Tools > iSCSI Initiator**.



STEP 2

The screenshot shows the 'iSCSI Initiator Properties' dialog box with the 'Discovery' tab selected. The 'Target portals' section contains a table of default portals and buttons to discover or remove them. The 'iSNS servers' section is currently empty with buttons to add or remove servers. A link for 'More about Discovery and iSNS' is at the bottom.

Address	Port	Adapter	IP address
172.16.28.128	3260	Default	Default
169.254.1.0	3260	Default	Default
172.16.28.58	3260	Default	Default
172.16.28.48	3260	Default	Default

In the Discovery tab, click **Discover Portal**.

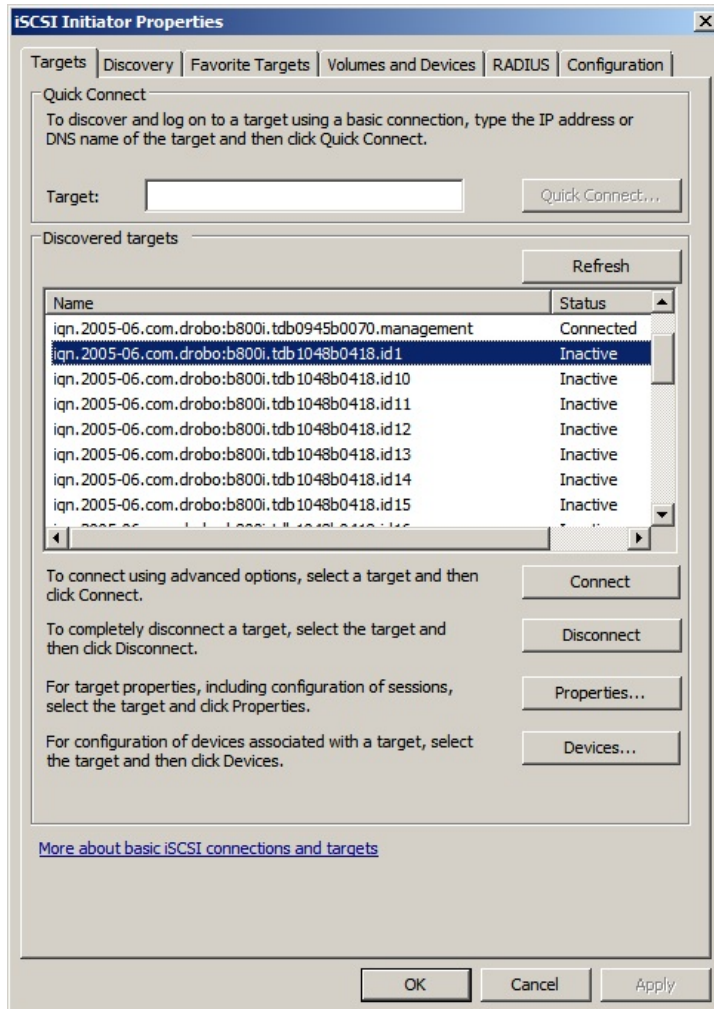
STEP 3

The screenshot shows the 'Discover Target Portal' dialog box. It prompts the user to enter an IP address or DNS name and a port number. The 'IP address or DNS name' field contains '172.16.28.48' and the 'Port' field contains '3260'. There are buttons for 'Advanced...', 'OK', and 'Cancel'.

Enter the IP address of the array. Shortly thereafter a list of all the volumes that your backup server has access to appears the Targets tab.



STEP 4



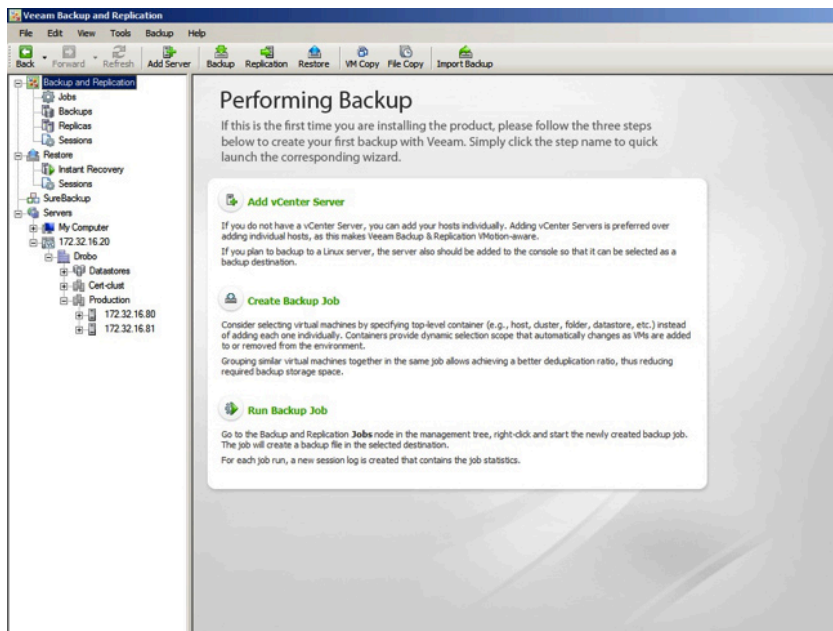
Select each target that you want to mount and click **Connect**.



Adding a New vCenter Server

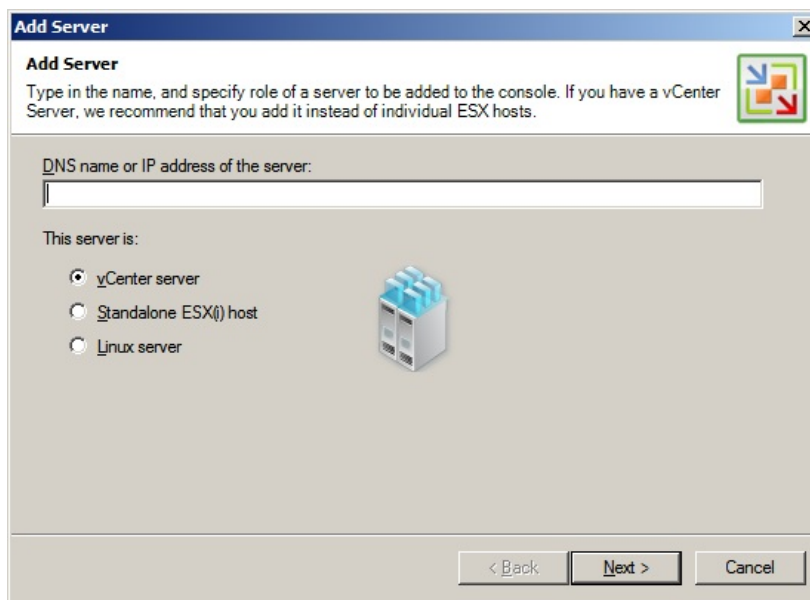
Install Veeam and use the main console to configure and manage backup attributes such as schedules, retention, targets, deduplication, compression, and so on.

STEP 1



Launch Veeam and click **Add vCenter Server**.

STEP 2



Enter the IP address of the server, whether you are adding a vCenter server or a single ESX/ESXi host.



STEP 3

Provide server administrator credentials.

STEP 4

Click **Finish** to complete the Add Server wizard.



Creating a New Veeam Backup Job

STEP 1

New Backup Job

Virtual Machines

Select virtual machines to process via container, or granularly. Container provides dynamic selection that automatically changes as you add new VM into container.

Virtual machines to backup:

Name	Type	Size
------	------	------

Add...
Remove
Exclusions...
Regalculate

Total size:
0.00 KB

< Back Next > Cancel

Click **Create Backup Job** and click **Add**.

STEP 2

New Backup Job

Name and Description

Type in a name and description for this backup job.

Name:
Production Job

Description:
Created by W2K8SR2VDICM\Administrator at 8/5/2011 8:30:50 AM.

< Back Next > Cancel

Enter a name for the backup job. In this example, the name is Production Job.



STEP 3

New Backup Job

Processing Mode
Choose how VM virtual disk images should be retrieved from storage during backup.

☒ **Direct SAN access**
VM data is retrieved using vStorage API directly from SAN. This mode requires that Veeam Backup server is connected directly into SAN fabric, otherwise VM processing will fail.

☐ **Virtual Appliance**
VM data is retrieved from the shared storage through ESX I/O stack. This mode can only be used if Veeam Backup is installed in a VM. Refer to product's documentation for additional requirements.

☐ **Network**
VM data is retrieved using vStorage API through ESX host over LAN using the NBD (Network Block Device) protocol.

Click Advanced to customize failover and encryption settings. [Advanced](#)

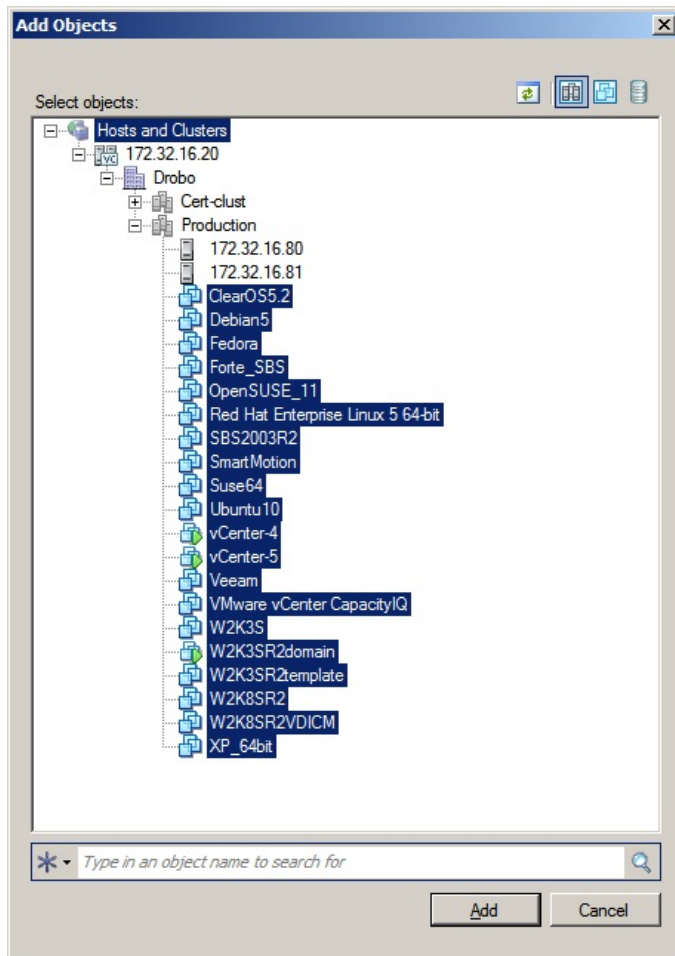
< Back Next > Cancel

Select **Direct SAN access**.

NOTE: Veeam Backup & Replication version 5 fails back to Network mode if SAN mode fails or is not configured correctly on the backup server, which could affect the performance of backups.



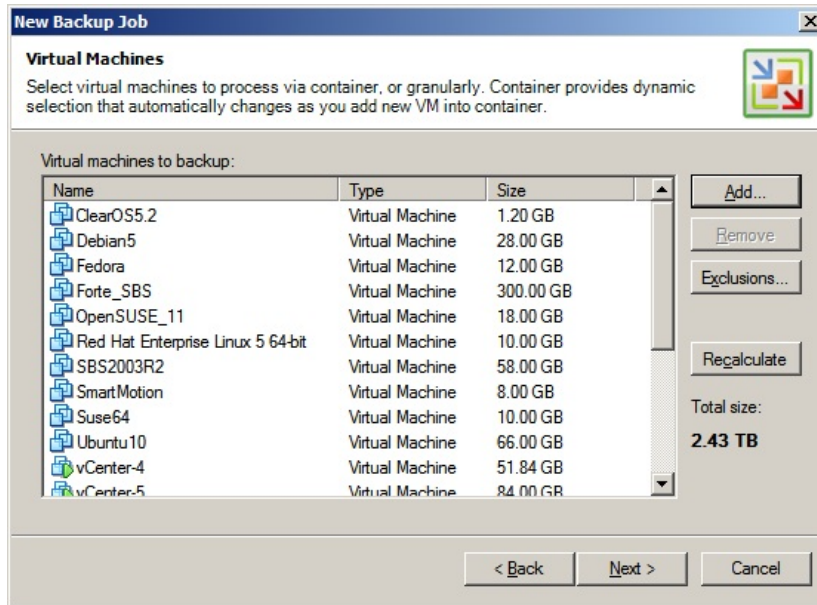
STEP 4



Select the VMs to be backed up.

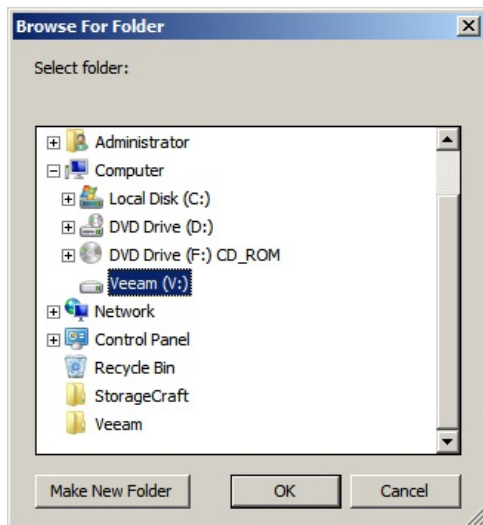


STEP 5



Verify the selected VMs to be backed up and click **Next**.

STEP 6



Select a target on which to store backups.



OPTIONAL FOR STEP 6

New Backup Job

Backup Destination

Specify where to store the backup files produced by this job, and additional job settings. You can only choose backup destination between computers added to the console.

Destination: 172.32.16.70 Host Properties...

Path to folder: Browse... Check Space

File name: Production

Restore points to keep on disk: 14

Deleted VMs retention period: 14 days

To view or edit additional backup job settings, click Advanced.

Advanced...

< Back Next > Cancel

Veeam also allows backups to be stored on a VMFS datastore when leveraging an ESX host, which is not the case for ESXi hosts. With an ESX host, you can opt to select these datastores/volumes as the target. *Note that this configuration may impact performance.*

In this case, the host destination is now an ESX host that holds the VMFS datastores.

Select Folder

Select folder:

- usr
- var
- vmfs
 - devices
 - volumes
 - 4e36b64a-2e67c551-c7f2-180373f0e64b
 - 4e417a0f-be005438-77fd-180373f0e64d
 - 4e417e0c-e704e891-9164-180373f0e64d
 - 4e417e41-25e039e3-3e15-180373f0e64d
 - 4e417eb8-258ab2b7-09e6-180373f0e64d
 - 4e417f02-e0bbfe97-39c2-180373f0d6de
 - 4e417f6e-560c9c4a-2a4e-180373f0d6de
 - 4e418019-dc0899cc-7201-180373f0d6de
 - 4e42e373-d27a2bac-cea0-180373f0e64b
 - 4e444613-c54f0123-d75f-180373f0d6dc
 - 4e44470a-c8500d5a-a6a6-180373f0d6dc
 - datastore1 (1)
 - veeam-dst-id1
 - veeam-dst-id2
 - veeam-src-id2
 - veeam-src-id3

Make New Folder OK Cancel

Click **Browse** to locate the datastore and click **OK**.



STEP 7

New Backup Job

Backup Destination
Specify where to store the backup files produced by this job, and additional job settings. You can only choose backup destination between computers added to the console.

Destination:
This computer or shared folder Host Properties...

Path to folder:
V:\ Browse... Check Space

File name:

Restore points to keep on disk:

Deleted VMs retention period: days

To view or edit additional backup job settings, click **Advanced...**

< Back Next > Cancel

Selecting a VMFS datastore as the destination for backups can have a significant decrease in performance. So in this example, the local disk/iSCSI volume (V:\) is used instead of the default.

Verify that this information is correct and click **Advanced**.

STEP 8

Advanced Settings

Backup | Storage | Notifications | vSphere | Advanced

Backup mode

☐ Reversed incremental
Each incremental run produces full recovery file of the most recent state. Recommended for backup to general purpose disk.

☒ **Incremental**
Traditional incremental backup with periodic fulls. Recommended for backup to tape, remote site and deduplicating storage appliances.

☒ Enable synthetic fulls (forever-incremental) Days...

Create on: Saturday

☐ Transform previous full backup chains into rollbacks
Allows to keep only one full backup file on disk to save disk space. Increases synthetic full creation time.

Active full backup

☒ Perform active full backups periodically

☐ Monthly on: Months...

☒ Weekly on selected days: Days...

Saturday

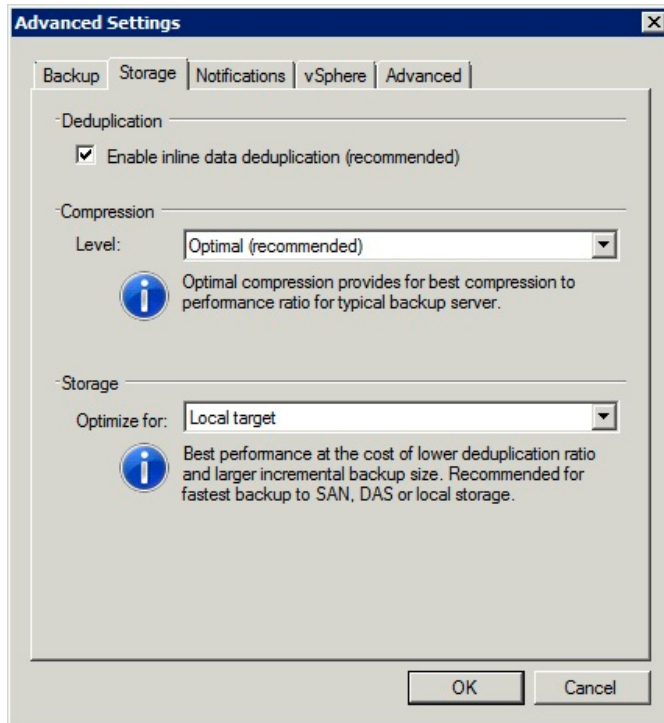
OK Cancel

Select the **Incremental** backup mode.

In addition to incremental backups, active full backups should be performed either weekly or monthly. Select the option that works best in your environment.



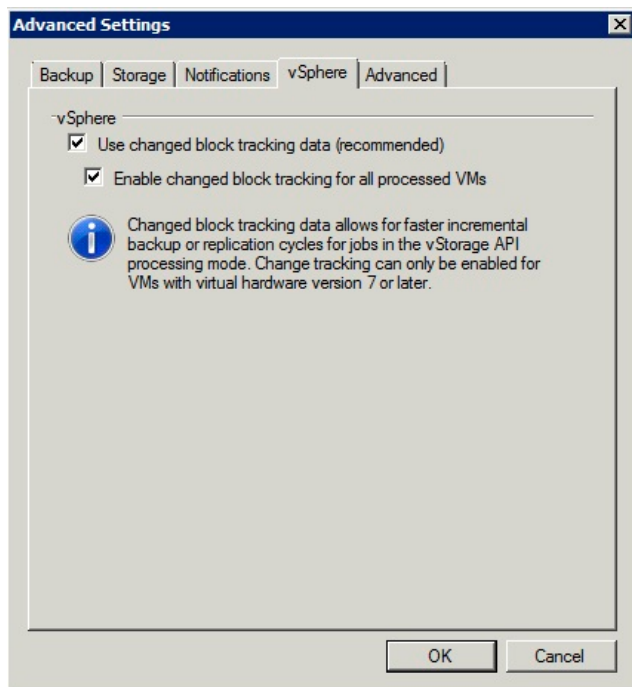
STEP 9



Click the **Storage** tab.

If you wish, enable “Inline data deduplication.” Make sure that compression is set to **Optimal** and that it is optimized for **Local target**.

STEP 10



Click the **vSphere** tab and select “Use changed block tracking data.”



STEP 11

New Backup Job

Guest Processing
Choose additional processing options available for Microsoft Windows guests.

☐ **Enable application-aware image processing**
Quiesces applications inside processed VM using Microsoft VSS to ensure transactionally consistent backup, and configures them to perform required VSS restore step during next VM boot.

☐ **Enable guest file system indexing**
Indexes guest OS files inside processed VM to enable browsing and searching for guest files in backup. Indexing is completely optional, and not required to be able to perform instant file level recovery.

Guest OS credentials
Specify the account with local administrator privileges on all VMs included in this job. Username must be supplied in the DOMAIN\USERNAME format.

Username: Browse...

Password:

Click Advanced to customize processing options for individual VMs. Advanced...

< Back Next > Cancel

Choose additional options for Windows guests.

If you enable either of the additional options, provide a local administrator login.

For more information on application processing and Volume Shadow Copy Services, refer to the Veeam Backup & Replication User Guide at:

<http://www.veeam.com/vmware-esx-backup/resources.html>.

STEP 12

New Backup Job

Job Schedule
Specify the job scheduling options. If you do not set the schedule, the job will need to be controlled manually.

☒ **Run the job automatically**

☒ **Daily at this time:** 6:00 PM everyday Days...

☐ **Monthly at:** 10:00 PM Fourth Saturday Months...

☐ **Periodically every:** 1 Hours Schedule...

☐ **Continuously**

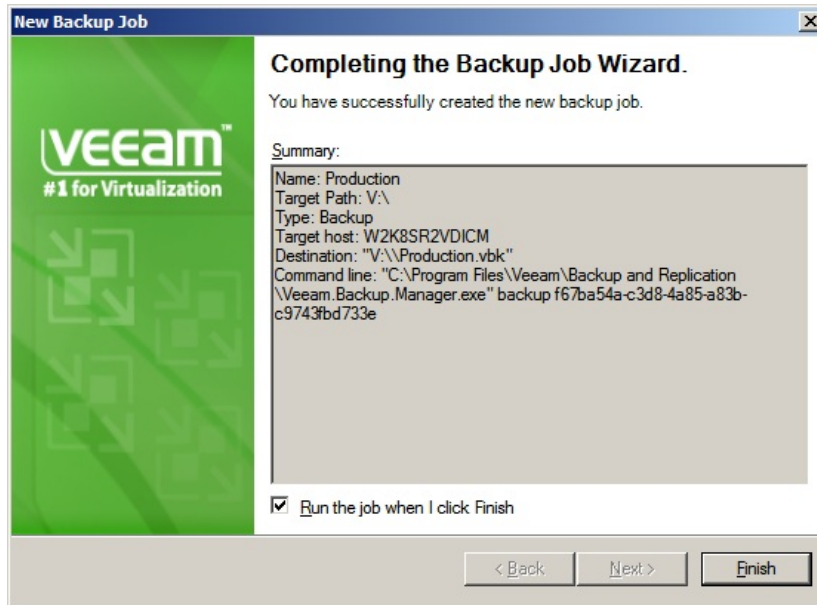
Automatic retry
☒ **Retry failed VMs processing:** 3 times
Wait before each attempt for: 10 minutes

< Back Create Cancel

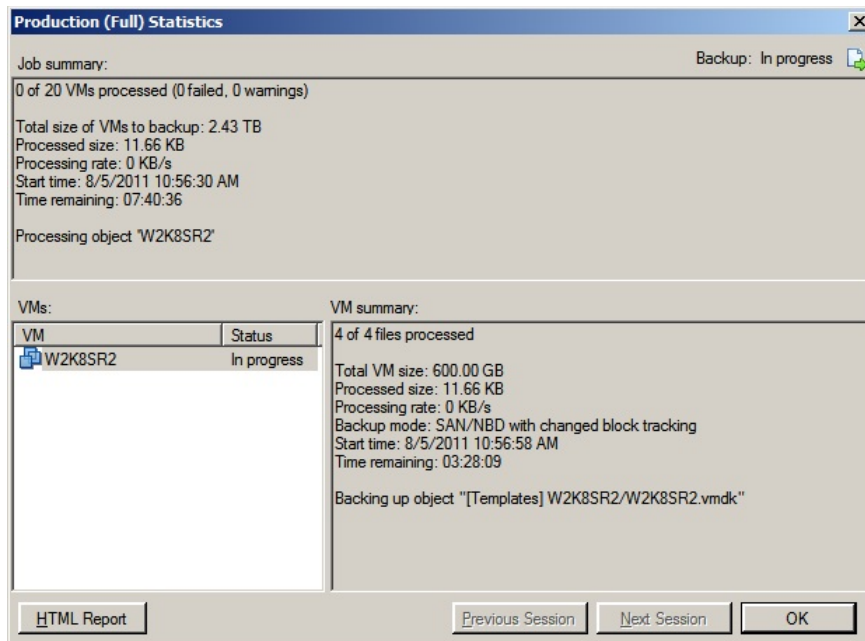
Specify scheduling options.



STEP 13



Click **Finish** to complete the Backup Job wizard.

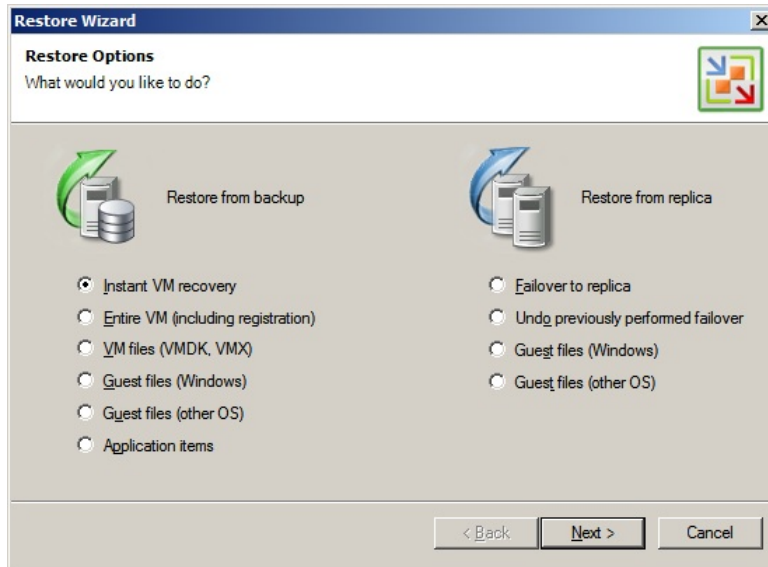


This is an example of real-time statistics for a backup job in progress.



Restoring Virtual Machines with Veeam Backup

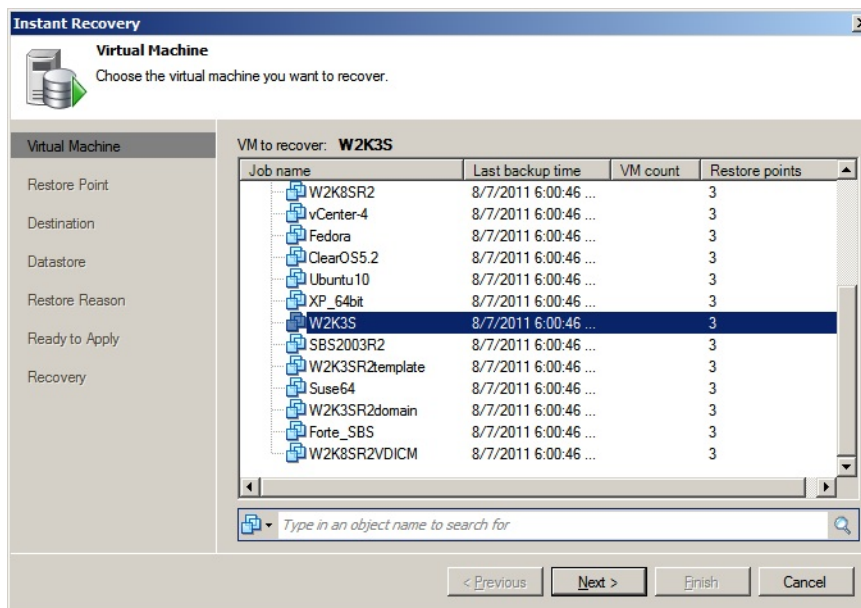
STEP 1



Select the **Restore from Backup** option in the Veeam main console. A wizard guides you through the configuration.

In this example "Instant VM recovery" was selected as a restore point.

STEP 2



Chose the VM you want to restore.



STEP 3

Instant Recovery

Restore Point
Choose restore point you want to recover the selected virtual machine to.

Virtual Machine
Restore Point
Destination
Datastore
Restore Reason
Ready to Apply
Recovery

VM name: **W2K3S** Original host: **f3ef1405-c28a-41d7-901f-**
VM size: **88.00 GB**

Available restore points:

Date	Type
8/7/2011 Sunday 6:11:36 PM	Increment
8/6/2011 Saturday 6:10:40 PM	Full
8/5/2011 Friday 11:10:25 PM	Full

< Previous Next > Finish Cancel

Choose a restore point.

STEP 4

Instant Recovery

Destination
Choose ESX server to run the recovered virtual machine on. You can choose to power on VM automatically, unless you need to adjust VM settings first (such as change VM network).

Virtual Machine
Restore Point
Destination
Datastore
Restore Reason
Ready to Apply
Recovery

Host: 172.32.16.81 Choose...
Restored VM name: W2K3S
Resource pool: Resources

☒ Resources

☐ Connect VM to network
☐ Power on VM automatically

< Previous Next > Finish Cancel

Choose which vSphere server to restore to.

Drobo • 2460 North First Street, Suite 100, San Jose, CA • www.drobo.com • 1.866.97.DROBO

Copyright 2011 Drobo, Inc. Data Robotics, Drobo, DroboElite, DroboPro, BeyondRAID, and Smart Volumes are trademarks of Drobo, Inc., which may be registered in some jurisdictions. All other trademarks used are owned by their respective owners.

All rights reserved. Specifications subject to change without notice. • HT-0044-01 • October 2011