Configuring Off-host Backups with Backup Exec 2010

Dell PowerVault DL Backup to Disk Appliance and Dell MD3000i Storage Arrays

symantec™

Configuring Off-host Backups

**Current Situation**

Microsoft Exchange Server and SQL Server are mission-critical components in today's business environment. IT administrators need to ensure that access to data and email communications for employees, customers, and partners is maintained 24 hours a day, 7 days a week. The greater reliance on all forms of electronic communication raises the potential of quickly escalating into a business disaster when any event causes mission-critical email and database data to become unavailable.

The PowerVault DL Backup-to-Disk Appliance powered by Symantec Backup Exec coupled with the Backup Exec Advanced Disk-based Backup Option (ADBO) used in conjunction with the snapshotting capabilities of Dell PowerVault MD3000i Storage Arrays are combined to create a comprehensive solution for customers that want quick recovery and off-host backup support for Microsoft Exchange Server 2003, 2007 and 2010 and Microsoft SQL Server 2000, 2005, and 2008. This solution eliminates backup windows, reduces the performance load on application servers, and quickly brings applications back online after data corruption issues. This solution leverages the Volume Shadow Copy Service (VSS) capabilities built into Microsoft Exchange, Microsoft SQL Server, and Microsoft Windows 2008 and the hardware snapshot capabilities of Dell PowerVault MD3000i Storage Arrays.

How does Off-host Backup Work?
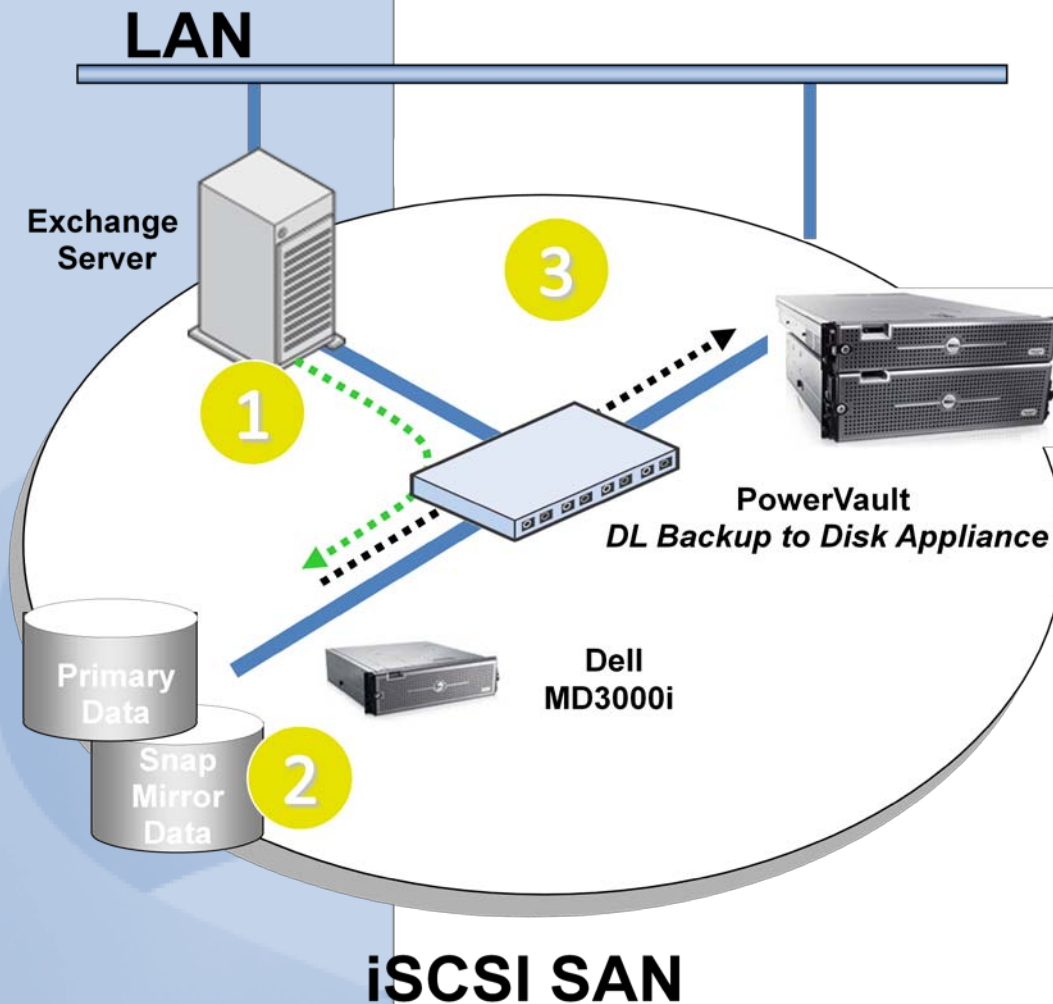
Off-host backup minimizes the impact to the LAN by moving backup data across the SAN during the backup process. An off-host backup is performed on the following manner:

1) The PowerVault DL Backup to Disk Appliance powered by Symantec Backup Exec in conjunction with Backup Exec Remote Agent installed on the protected server (Exchange in this example) prepare the remote server for protection

2) The MD3000i Storage Array creates a snapshot of the protected server's data residing on the array.

3) The snapshot is mounted directly to the Backup Exec media server and the backup data flows directly across the SAN instead of the LAN.

Solution Components

PowerVault DL Backup to Disk Appliance powered by Symantec Backup Exec

Dell has simplified the backup process by offering the only integrated hardware, software and services solution powered by Symantec Backup Exec. The PowerVault DL Backup to Disk Appliance is factory installed with Symantec Backup Exec software and a unique wizard driven set up and management utility. The backup software comes with integrated automated dynamic disk provisioning that configures and sets up the disks for immediate use. Set it up, configure storage, add more disks – it only takes a few clicks.

Advanced Disk-based Backup Option (ADBO)

Enables faster backups and restores through advanced disk-based backup and recovery, including Synthetic and Off-Host backups to perform zero impact backups. Synthetic backups reduce backup windows and network bandwidth requirements and do not impact the original client. New true image restore functionality automatically restores data sets sequentially, simplifying restores. The Off-Host backup feature enables improved backup performance and frees the remote computer by processing the backup operation of the remote computer on a Backup Exec media server instead of on the remote computer or host computer.

Advanced Open File Option

The Symantec Backup Exec for Windows Servers Advanced Open File Option (AOFO) uses advanced open file and image technologies designed to alleviate issues that are sometimes encountered during backup operations, such as protecting open files and managing shortened backup windows.

Agent for Windows Systems

The Remote Agent is a system service that runs on remote Windows servers and workstations. The Remote Agent provides faster backup processing by locally performing tasks that in typical backup technologies that require

extensive network interaction. The Remote Agent processes backup data into a continuous stream that the media server then processes as a single task. This method provides better data transfer rates over traditional technologies, which require multiple requests and acknowledgments between the media server and the remote server.

Agent for Microsoft Exchange Server

Backup Exec Agent for Exchange provides continuous data protection for Exchange Server and revolutionizes data protection and recovery by eliminating the daily backup window for Exchange backup jobs while still allowing recovery of individual messages, folders and mailboxes – in seconds with patent-pending Granular Recovery Technology. Additionally, administrators don't need to run a mailbox (or MAPI) backup, which significantly reduces the number of backups, time and cost required to protect Exchange. With Granular Recovery Technology, the Exchange Agent can granularly recover from a single full backup, eliminating the need for multiple Exchange backups. Backup Exec Agent for Exchange provides fast, flexible technology that protects vital Exchange Server 2003, 2007 and 2010 data while the application is still online.

Agent for Microsoft SQL Server

Efficiently eliminate the daily backup window for SQL servers and enable recovery of database transactions that were made right up to the time of the hardware or software failure. Additionally, flexible recovery options allow IT administrators to restore SQL databases to destinations other than where they originated, directing a copy of the actual data streams being sent to media by a SQL database to a local directory for later use. The SQL Server 2005 snapshots are integrated into the Backup Exec catalog for a consolidated look at all data copies available for recovery in seconds. This agent provides SQL Server 7.0, SQL Server 2000, SQL Server 2005 and 2008 administrators with granular protection on 32- and 64-bit systems down to the individual database or file group.

symantec.™

DELL

Note: Before continuing with the installation and setup of the DL Backup to Disk Appliance and MD3000i for off-host backups, refer to the Best Practices and Troubleshooting section located at the end of the document.

Dell PowerVault MD3000i Storage Arrays

The PowerVault MD3000i networked storage array leverages the modularity and availability of the PowerVault series to deliver an IP network storage solution that can consolidate up to 16 hosts. By extending the connectivity capability of today's MD3000 controller architecture, Dell is able to bring to market a low cost, easy to use, expandable, and highly available iSCSI SAN storage arrays.

The process for configuring the PowerVault DL Backup to Disk Appliance powered by Symantec Backup Exec for off-host backups includes:

1. Installing the Dell PowerVault MD3000i Storage Software on the PowerVault DL Backup to Disk Appliance.
2. Configuring the PowerVault DL Backup to Disk Appliance for access to the iSCSI array and snapshots that are being protected.
3. Installing the Backup Exec options on the media server and the remote server that is being protected using off-host backups.
4. Configuring and running off-host backup jobs.
5. Configuring and running restores of data, that has been backed up, using the off-host backup methodology

Installing the Dell PowerVault MD3000i Storage Software on the Backup Exec Media Server

This process assumes that the Dell PowerVault MD3000i array is setup and configured and the PowerVault DL Backup to Disk Appliance will be added to an existing installation.

NOTE: Ensure the premium feature license for snapshots is installed. Please contact a Dell sales representative to purchase this feature if it's not already installed.

1. Start the installation of the Dell PowerVault MD3000i Storage Software by selecting **install MD3000i Storage Software.**
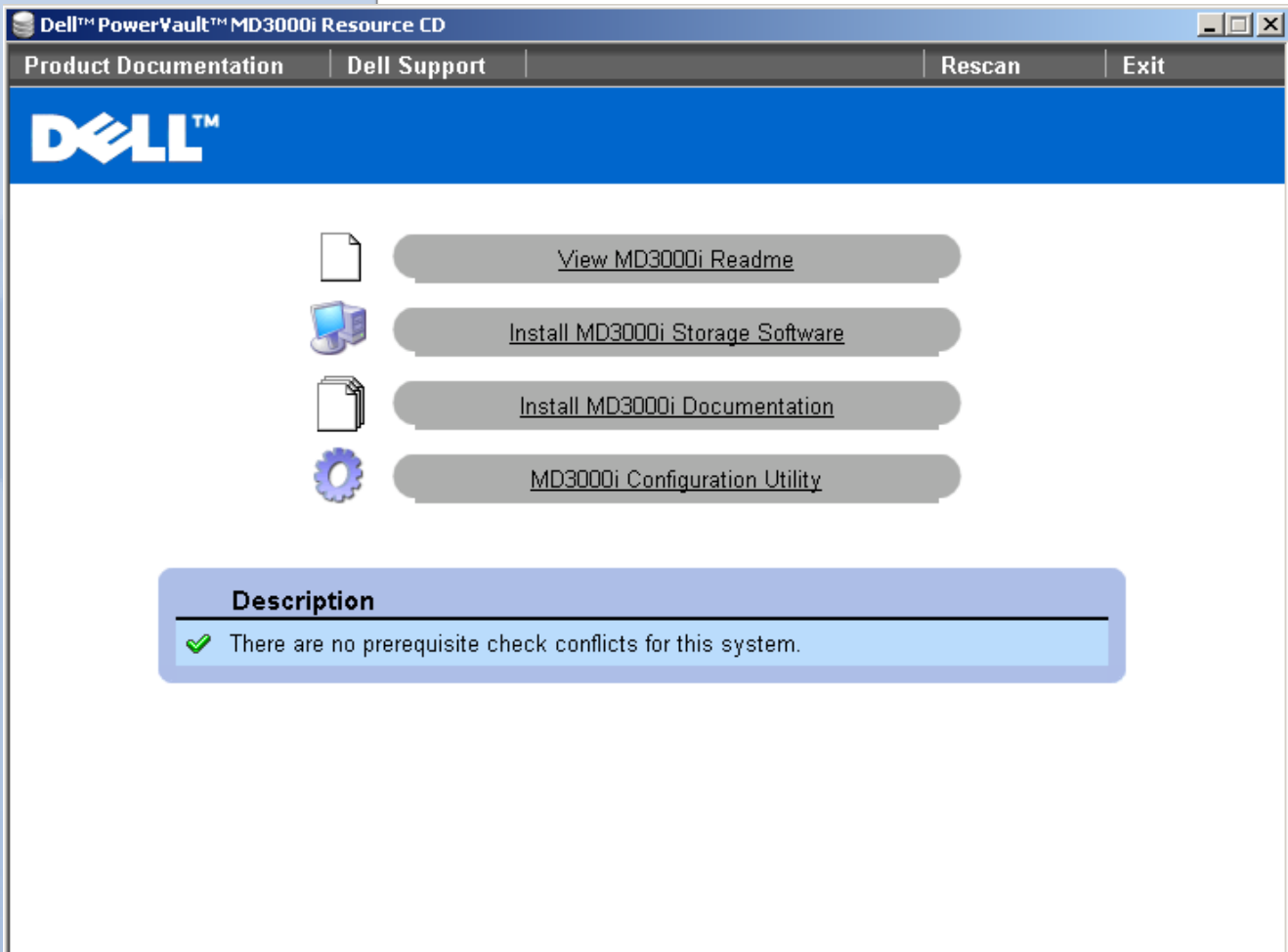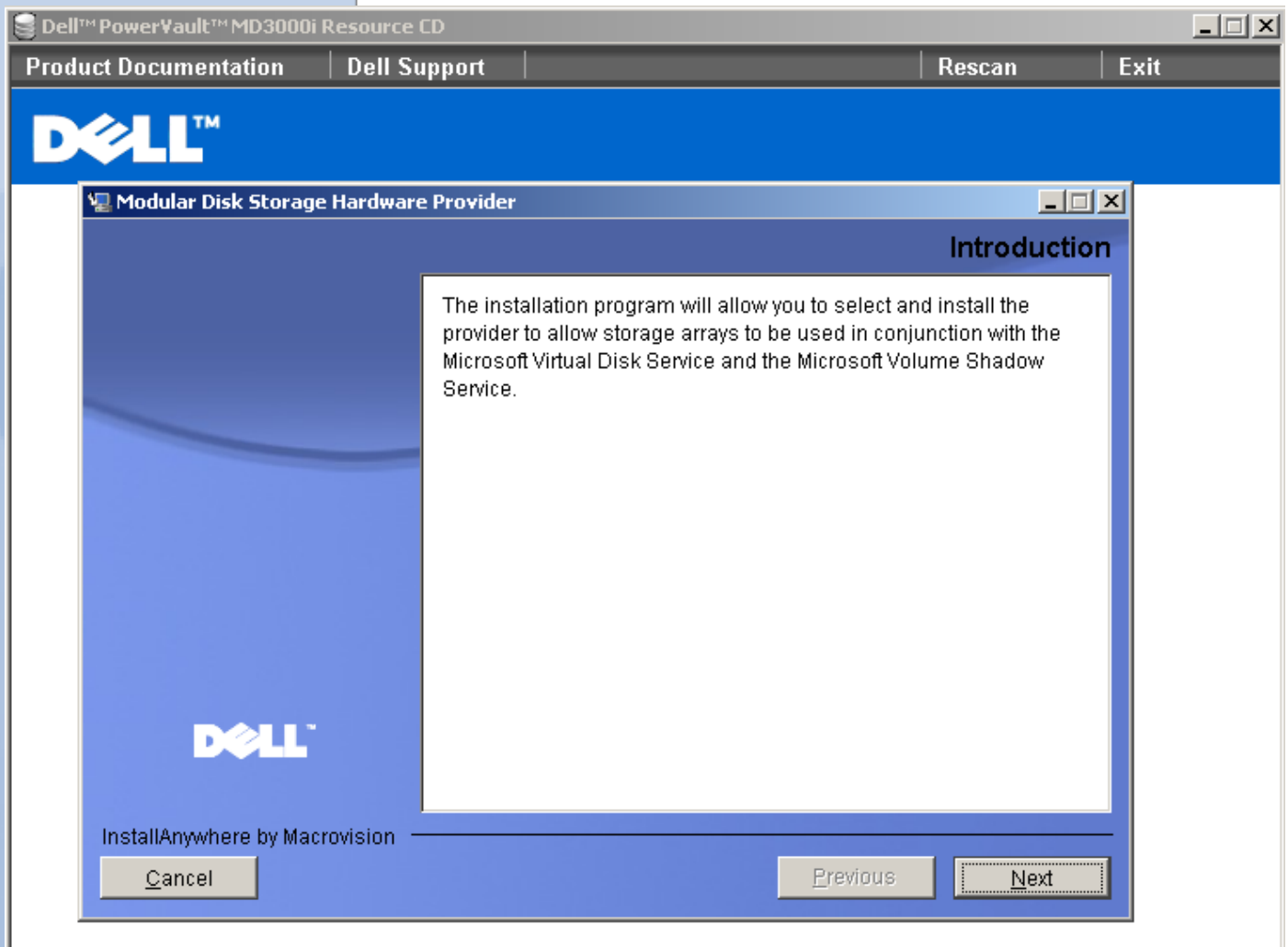

2. Select the language for installation and click **Ok** to continue.
3. Select **Next** to continue.
4. Accept the terms of the license agreement and click **Next** to continue.

5. Verify the installation path and select **Next** to continue.
6. Select **Host** as the installation type and select **Next** to continue.
7. The Pre-Installation Summary screen appears, showing the installation destination, the required disk space, and the available disk space. Select **Install** to continue.
8. When the installation completes, select **Done** to continue.
9. A screen appears asking if you want to restart the system now. Select **No, I will restart the system myself.**
10. The Modular Disk Storage Hardware Provider (VDS/VSS) must be installed. Navigate to the windows\VDS_VSS directory on the installation media. Select the 32-bit or x64 version of the executable. The DL Backup to Disk Appliance uses x64 version.

11. Select **Next** when the introduction screen appears.

12. Select **Next** to acknowledge the copyright statement.
13. Accept the terms of the license agreement and click **Next** to continue.
14. Verify the installation path and select **Next** to continue.
15. The Pre-Installation Summary screen appears, showing the installation destination, the required disk space, and the available disk space. Select **Install** to continue.
16. When the installation completes, select **Done** to continue.
17. Restart the system.

Using the MD Storage Manager to Configure the Media Server for access to the array

1. Launch the MD Storage Manager on the system being used as the management station.
2. Click on the **Configure** tab, then select **Configure Host Access (Manual).**
3. At **Enter host name,** enter the host server to be available to the storage array for virtual disk mapping.
4. In the **Select host type** drop-down menu, select the host type. Click **Next** to continue.
5. If the iSCSI initiator shows up in the list of **known iSCSI initiators,** make sure it is highlighted and click **Add.** Click **Next** to continue. Otherwise, click **New** and enter the **iSCSI initiator name**.

The iSCSI initiator name can be found on the **General tab** of the iSCSI Initiator properties window.
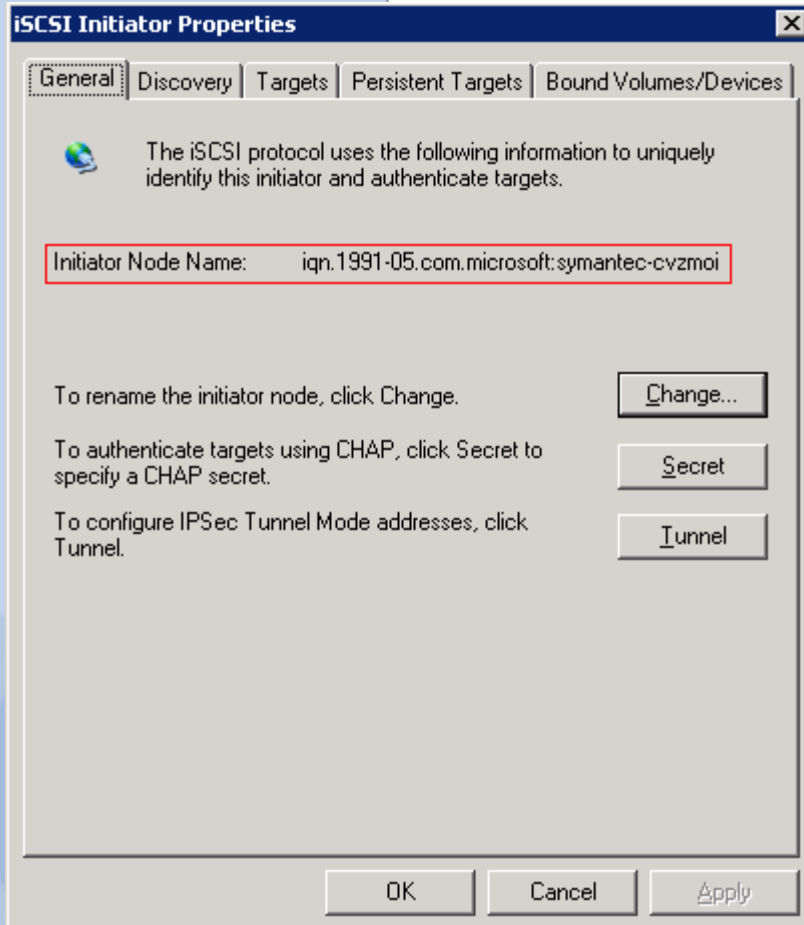
6. Choose whether or not the host server will be part of a host server group that will share access to the same virtual disks as other host servers. The Backup Exec Media Server will need access to the snapshots of the protected server in order to backup those snapshots. Click **Next** to continue.
7. Click **Finish** to complete the setup.

Configure the Media Server for access the array

1. Click on **Start -> Programs -> Microsoft iSCSI Initiator -> Microsoft iSCSI Initiator** or **Start -> Administrative Tools -> iSCSI Initiator.** The iSCSI Initiator properties dialogue box appears.
2. Click on the **Discovery** tab. Click **Add.** Specify the IP address of the MD3000i.
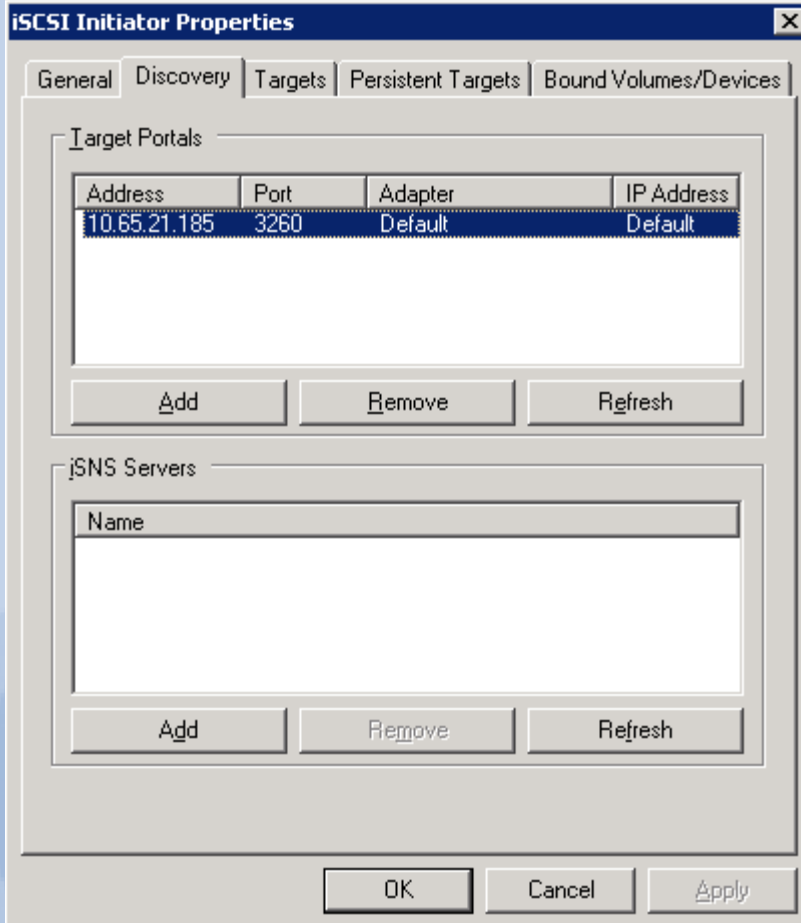
3. Click on **Targets** tab and click **Refresh.** If not already done so, this will populate the iSCSI targets that the media server can access.
4. If the volume requires CHAP credentials, click **Advanced** in the Log On to Target dialog box. Set the **CHAP logon information** check box and specify the CHAP user name and secret. The username must match an access control record for the volume.

Installing and Configuring the Backup Exec Agents and Options for Off-host Backup

NOTE: The following assumes that Backup Exec has been installed on a server.

1. From the Backup Exec UI, Select **Tools** -> **Install Options and License Keys on this Media Server**
2. The Backup Exec License Wizard appears. Enter the license keys for:
   - Advanced Disk-based Backup Option
   - Agent for Windows Systems (if applicable)

- Exchange Agent (if applicable)
- SQL Agent (if applicable)

NOTE: A remote agent is required for each remote system that is being protected.

3. Verify that the licensed options will be installed on the media server and click **Next**.
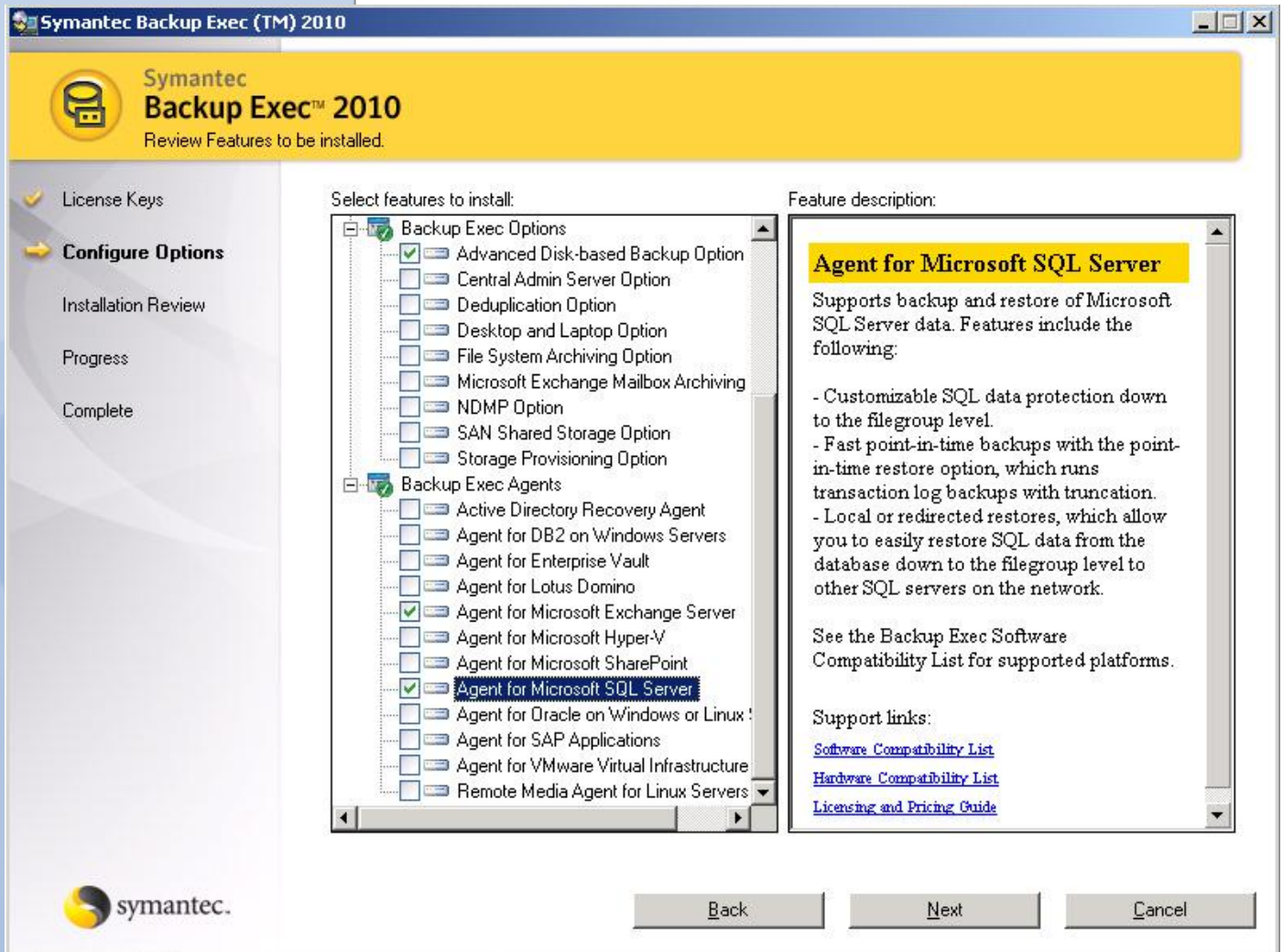
4. A summary of the agents and options to be installed is presented. Click **Install** to continue.
5. Once the installation has completed, click **Finish** to continue.
6. Next, remote agents need to be installed on the systems that are being protected. Select **Tools -> Install Agents and Media Servers on other Servers.** The installation wizard appears. Click **Next** to continue.

7. Right click on Windows Remote Agents and select **Add Remote Computer**. Browse through either *Active Directory Domains **or** Microsoft Windows Network* to browse and find the remote computers to install the agents on. Make sure to select all of the systems that will be protected by Backup Exec.
8. Enter the Username, Password, and Domain information that has administrative rights on the target system and can be used to install the agent. Click **Ok** to continue.
9. Select the *Remote Agent for Windows Systems **and** Advanced Open File Option* and click **Finish** to continue.

Creating Backup Jobs

Now that the remote agents have been installed, Backup jobs can be created and run to protect the remote systems using an off-host backup.

1. Select the **Backup Tab** and select **New Backup Job.** The Backup Job properties screen will appear.
2. Select the remote system and data that is to be protected. If you are protecting a file server, select the files, folders, or volumes. If you are protecting a Microsoft Exchange Database, select the Information Store. If you are protecting a SQL Server, select the SQL instance.

Backup Job Properties

Source
- Selections
- Resource Order
- Resource Credentials
- Priority and Availability
- Selection List Notification

Destination
- Device and Media

Settings
- General
- Advanced
- Network and Security
- Pre/Post Commands
- Advanced Open File
- Advanced Disk-based Backup
- Microsoft SQL
- Microsoft Exchange
- Microsoft SharePoint
- Microsoft Active Directory
- Lotus Domino
- Oracle
- DB2
- NetWare SMS
- Linux, Unix, and Macintosh
- NDMP
- Enterprise Vault
- VMware Virtual Infrastructure
- Microsoft Virtual Server
- Notification

Frequency
- Schedule

Selections

Selection list name:
Backup 00006

Load selections from existing list...

☑ Include subdirectories
☑ Show file details

Selection list description:

Include/Exclude...

View by Resource | View Selection Details

- ☑ All Resources
  - ☐ DJDP67DZ
    - ☐ C:
    - ☐ F:
    - ☐ O:
    - ☐ System State
    - ☐ Microsoft SQL Server "BKUPEXEC"
    - ☐ Utility Partition
    - ☐ Shadow Copy Components
  - ☑ Favorite Resources
    - ☐ Linux/Unix Servers
    - ☐ Macintosh Systems
    - ☑ Windows Systems
      - ☐ DJDP67DZ
      - ☑ DL2000-OH
        - ☐ C:
        - ☑ G:
        - ☐ System State
        - ☐ Utility Partition
        - ☐ Shadow Copy Components
    - ☐ Domains
    - ☐ Oracle Real Application Clusters
    - ☐ NDMP Servers
    - ☐ Microsoft SharePoint Server Farms
    - ☐ User-defined Selections
    - ☐ Enterprise Vault

Name ▲	Size	T
☑ $RECYCLE.BIN		F
☑ System Volume I...		F
☑ Users		F

Run Now | Cancel | Help

3. Next, select the destination for the backup. Select **Device and Media** and then select the destination from the **Device** drop down.
4. Select **General** to name the backup job and specify additional options.
5. Select **Advanced Disk-based Backup** and select the option *Use offhost backup to move backup processing from remote computer to media server.* Under snapshot provider, select **Hardware – Use technology provided by the hardware manufacturer.**

Backup Job Properties   Comments? _ □ X

Source
  Selections
  Resource Order
  Resource Credentials
  Priority and Availability
  Selection List Notification
Destination
  Device and Media
Settings
  General
  Advanced
  Network and Security
  Pre/Post Commands
  Advanced Open File
  Advanced Disk-based Backup
  Microsoft SQL
  Microsoft Exchange
  Microsoft SharePoint
  Microsoft Active Directory
  Lotus Domino
  Oracle
  DB2
  NetWare SMS
  Linux, Unix, and Macintosh
  NDMP
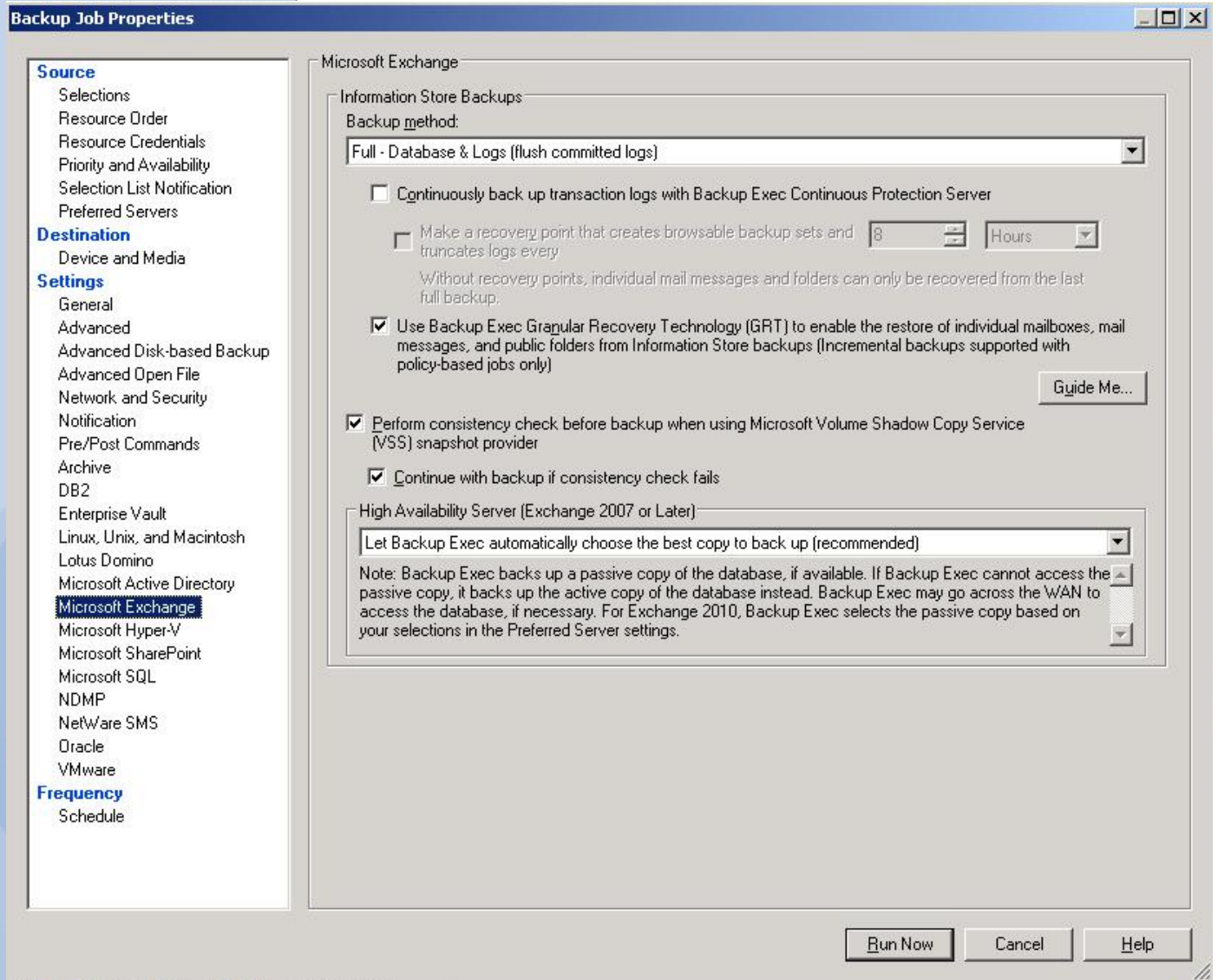 Enterprise Vault
  VMware Virtual Infrastructure
  Microsoft Virtual Server
  Notification
Frequency
  Schedule

Advanced Disk-based Backup

☑ Use offhost backup to move backup processing from remote computer to media server

Snapshot provider: [Hardware - Use technology provided by hardware manufacturer ▼]

Job disposition
  If any of the selected resources do not support offhost backup:
    ⦿ Continue the backup job (offhost backup is not used)
    ○ Fail the backup job (further selections are not backed up after failure occurs)

☐ Process logical volumes for offhost backup one at a time

[Run Now] [Cancel] [Help]

6. Perform this step if this is a backup of Microsoft Exchange. If this is not a backup of Microsoft Exchange, skip to **step 8**. Select **Microsoft Exchange** and verify that the option *Use Backup Exec Granular Recovery Technology (GRT) to enable the restore of individual mailboxes, mail messages, and public folders from Information Store backups*. Continue to **Step 8**.

Backup Job Properties

Microsoft Exchange

Information Store Backups

Backup method:

Full - Database & Logs (flush committed logs)

☐ Continuously back up transaction logs with Backup Exec Continuous Protection Server

☐ Make a recovery point that creates browsable backup sets and truncates logs every [8] [Hours]

Without recovery points, individual mail messages and folders can only be recovered from the last full backup.

☑ Use Backup Exec Granular Recovery Technology (GRT) to enable the restore of individual mailboxes, mail messages, and public folders from Information Store backups (Incremental backups supported with policy-based jobs only)

Guide Me...

☑ Perform consistency check before backup when using Microsoft Volume Shadow Copy Service (VSS) snapshot provider

☑ Continue with backup if consistency check fails

High Availability Server (Exchange 2007 or Later)

Let Backup Exec automatically choose the best copy to back up (recommended)

Note: Backup Exec backs up a passive copy of the database, if available. If Backup Exec cannot access the passive copy, it backs up the active copy of the database instead. Backup Exec may go across the WAN to access the database, if necessary. For Exchange 2010, Backup Exec selects the passive copy based on your selections in the Preferred Server settings.

Source sidebar:
Source
- Selections
- Resource Order
- Resource Credentials
- Priority and Availability
- Selection List Notification
- Preferred Servers

Destination
- Device and Media

Settings
- General
- Advanced
- Advanced Disk-based Backup
- Advanced Open File
- Network and Security
- Notification
- Pre/Post Commands
- Archive
- DB2
- Enterprise Vault
- Linux, Unix, and Macintosh
- Lotus Domino
- Microsoft Active Directory
- Microsoft Exchange
- Microsoft Hyper-V
- Microsoft SharePoint
- Microsoft SQL
- NDMP
- NetWare SMS
- Oracle
- VMware

Frequency
- Schedule

[Run Now] [Cancel] [Help]

7. Perform this step if this is a backup of Microsoft SQL. If this is not a backup of Microsoft SQL, skip to **Step 8.** Select **Microsoft SQL** and specify the backup options for the SQL backup. Continue to **Step 8.**

8. Click on **Schedule** and specify the scheduling options for the backup. Click **Run Now** to submit the backup job for processing. The backup job status can be monitored from the **Job Status** tab.
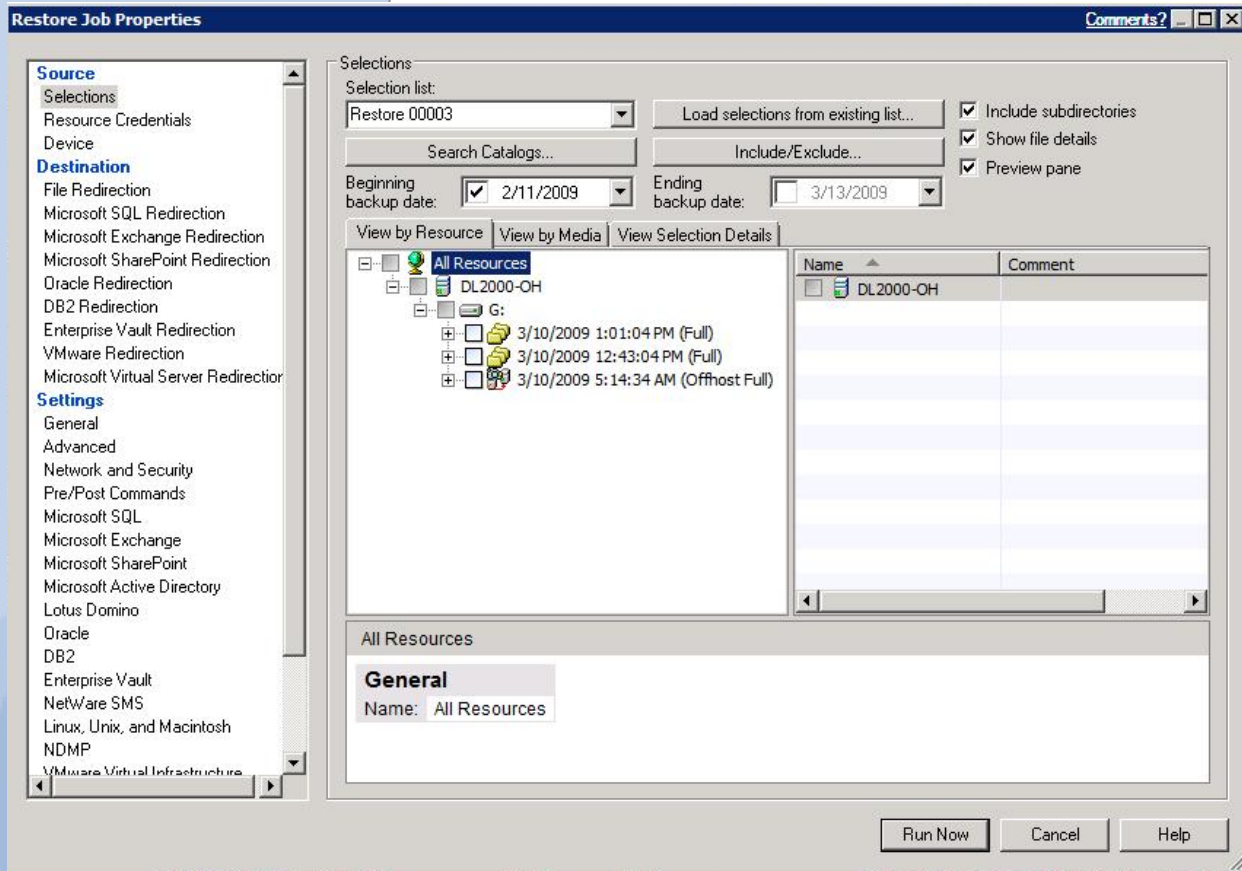
Restoring Data

1. Select the **Restore Tab** and select **New Restore Job.** The Restore Job properties screen will appear.

2. Select the data that is to be restored. If you are restoring data to a file server, individual files and folders or complete volumes can be restored. If you are restoring data to an Exchange server, individual items can be restored such as mailboxes, messages, and public folders and the entire Information Store can be restored. If you are restoring data to a SQL server, select the SQL database for restoration.

3. Select **General** to name the backup job and specify additional options.

4. Perform this step if this is a restore of Microsoft Exchange Data. If this is not a restore of Microsoft Exchange data, skip to **Step 6.** Select **Microsoft Exchange** to verify the restore options for the Exchange data. Continue to **Step 6.**
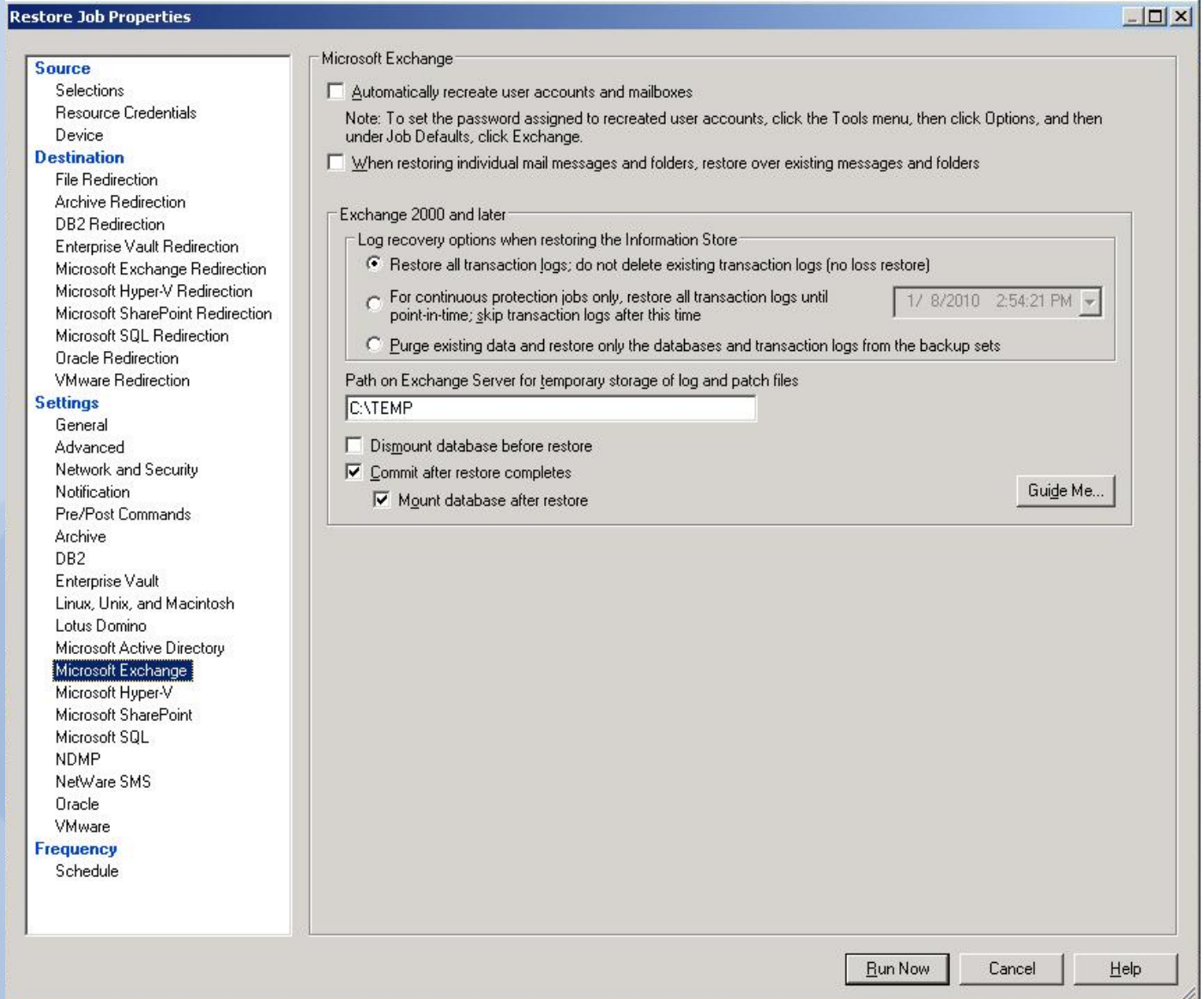
5. Perform this step if this is a restore of Microsoft SQL. If this is not a restore of Microsoft SQL, skip to **Step 6.** Select **Microsoft SQL** to verify the restore options for the SQL data. Continue to **Step 6**.
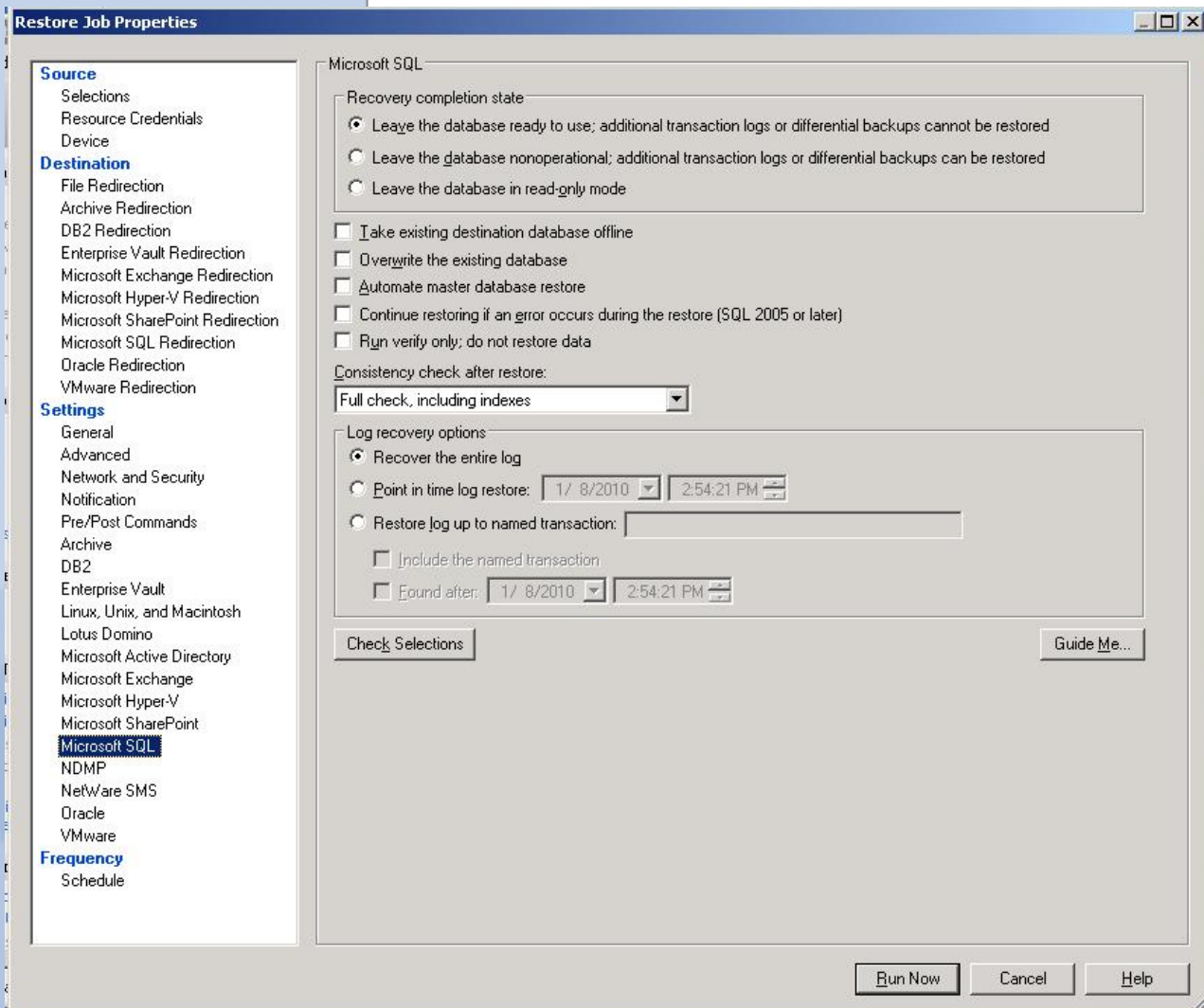
6. Click on **Schedule** and specify the scheduling options for the restore. Click **Run Now** to submit the restore job for processing. The restore job status can be monitored from the **Job Status** tab.

Conclusion

Creating snapshots for off-host backup requires minimal overhead and does not interfere with normal system operations. As a result, administrators can schedule snapshots frequently, minimizing potential data loss during a disaster. Off-host backups are a particularly good solution for organizations with stringent high availability requirements and large amounts of data.

Best Practices and Troubleshooting

- The off-hosts clients must be using Windows Server 2008 to perform off-hosts backups with the DL Backup to Disk Appliance.
- The Backup Exec Hardware Compatibility List contains the list of the supported software and hardware certified with this solution. (http://support.Veritas.com/menu_ddProduct_BEWNT_view_CL.htm). Check the HCL to verify that all components are certified and supported.
- When performing backups of SQL or Exchange databases, all volumes must be able to be snapped concurrently or else the backup operation will fail.
- For off-host backup to work, all volumes must reside on disks that are shared between the remote computer and the Backup Exec media server. It is the backup administrator's responsibility to confirm this. If the volumes are not shared, the import operation will fail, and you may need to clean up the snapshots and resynchronize the volumes manually.
- The provider used for snapshot must be installed on both the media server as well as on the remote computer. If the provider is not installed on the media server, the import operation will fail, and you may need to clean up the snapshots and resynchronize the volumes manually.
- All volumes selected for backup must be transportable to the media server. If Microsoft SQL or Exchange, or other database applications are selected for backup, make sure that the databases and log files reside on transportable volumes.
- In addition to being transportable, all volumes selected for backup must be snappable by the same provider. It is the backup administrator's responsibility to ensure that all volumes in a backup job are supported by the same VSS provider.
- Log files created by the provider or by its supporting application during normal snapshot operation should not reside on any of the volumes being snapped. This prevents VSS from flushing the write buffers, and the snapshot will time-out. Change the log path to another volume.
- Make sure the provider service is running and make sure Microsoft Windows "Volume Shadow Copy" service has not been disabled.
- Make sure the machine-level credentials used for the job are the same on both the media server and the remote computer. Incorrect credentials will cause snapshots or the backup to fail.
- If a backup job is configured in a CASO environment, you must target the job to media servers on which the selected VSS provider is installed rather than allowing the job to be delegated by the central administration server. Otherwise, the job could be delegated to a media server that does not have off-host capability.