# Continuous Data Protection

## PowerVault DL Backup to Disk Appliance

symantec.

# Continuous Data Protection

## Current Situation

The PowerVault DL Backup-to-Disk Appliance – Powered by Symantec Backup Exec offers the industry's only fully integrated backup-to-disk solution with software factory installed. Industry leaders Dell and Symantec have co-developed this offering to give you easier management capabilities of the backup-to-disk environment. It's an ideal way for any IT department to achieve faster, more reliable backups and restores. In addition, the appliance includes continuous data protection capabilities designed to protect systems immediately as they change. .

Today's Windows based organizations face many challenges when it comes to data protection. First, data volumes continue to grow at 40 percent to 60 percent each year, making it increasingly difficult for administrators to back up mission-critical data in acceptable time frames (or within available backup windows). Additionally, instant on-demand data recovery is becoming increasingly vital for business operations. While traditional tape backups have proven effective over the years, their reliability has been questioned, and today's business climate demands faster, more efficient backups and on-demand recovery.

## The Opportunity

Disk-based data protection, specifically continuous data protection, provides the opportunity to address these issues in a revolutionary way. Continuous data protection:

- Eliminates the need for backup windows
- Enables file recovery in seconds
- Allows end users to recover their own data without contacting IT
- Delivers a complete, integrated disk-to-disk-to-tape solution

Continuous data protection allows any organization to manage data growth, improve reliability, and speed up data recovery and it improves overall data protection without weighing down IT in costly high-administration solutions.

## The Solution: PowerVault DL Backup-to-Disk Appliance with Symantec™ Backup Exec Continuous Protection Server

The PowerVault DL Backup-to-Disk Appliance includes Backup Exec Continuous Protection Server (CPS), a complement to Backup Exec for Windows Servers specifically designed for disk. Backup Exec CPS revolutionizes backups by eliminating backup windows, improving backup reliability, and featuring the industry's first Web-based end-user file retrieval. It integrates with Backup Exec for Windows Servers to deliver a complete disk-to-disk-to-tape solution. This solution improves data protection and reduces the administrative complexity associated with traditional data protection practices. Continuous data protection eliminates the need for full, incremental, or differential backups by protecting data immediately and then continuously backing it up to disk. It also decreases the complexity of current methodologies as well as helping reduce the cost of the media used.

Because Windows file server data is continuously protected on disk, it can be recovered quickly and end users can restore their own files without contacting IT which improves service levels without increased IT headcount or administrative cost.

## Understanding Traditional and Continuous Data Protection

As you consider a suitable data protection strategy for your organization, it is important to understand the differences between traditional tape-based, traditional disk-based, and continuous disk-based data protection offerings.

## Traditional Tape Backups

### Key Benefits

Traditionally, tape backups have proven to be an effective and inexpensive means for data protection and recovery. The key benefits of traditional tape backups include:

- Inexpensive medium to store data
- Portable format that can easily be moved offsite
- Familiar to administrators, who know and understand tape backups

### Key Drawbacks

As useful as tape backups are, there are three key challenges with tape. First is reliability. In a Byte and Switch survey [(1)], about one quarter (25.6 percent) of survey respondents said their backups fail at least twice a week because of the failure of the tape cartridges (52.9 percent) and the tape drives (45 percent). The second challenge is complexity. Tape lacks the flexibility and simplicity that many organizations need today in a data protection solution. Last is speed. As data volumes increase, tape backups are taking longer. A few notable drawbacks to tape backups include:

- High impact on production server (backups must occur during off-peak hours)
- Only a limited number of servers backed up at one time

(1) http://storagemagazine.techtarget.com/magPrintFriendly/0,293813,sid35_gci1052905,00.html

Symantec Corporation World Headquarters
20330 Stevens Creek Blvd., Cupertino, CA 95014 USA
+1 (408) 517 8000 / +1 (800) 721 3934
www.symantec.com

- Once-a-day backups—only capture a single point of recovery
- Increasingly complex management (incrementals, differentials, multivendor solutions, and so on)
- Questionable reliability

**Recovery**

The point of protecting data is ensuring that it is recoverable when needed. With tape backups, however, recovery can be a time-consuming, bottlenecked process that makes it difficult to get the right file to the right person at the right time. Key drawbacks to tape recovery include:

- Recovery can be lengthy and cumbersome.
- Only trained administrators can recover data.

**Backup Process**

1. A full backup of each file server is performed at a scheduled time once a week.
2. Incremental backups of each file server are performed daily, during off-peak hours.

**Recovery Process**

1. Users submit a file restore request to administrators.
2. Administrators locate the tape(s); mount it, designate the file from the point of the last backup, and restore to the user.

## Disk-Based Backups

**Key benefits**

Disk-based backups provide several key benefits that are not realized with tape. First, backups are typically faster and more efficient, while recovery time improves significantly. Additionally, disk traditionally provides a more reliable format for data protection. Benefits include:

- Faster, more efficient backups
- More reliable backups
- Faster and easier recovery
- Possibility to back up to tape for long-term archival and offsite storage

**Key drawbacks**

While disk-based backups significantly improve data protection and recovery, they still have some drawbacks:

- Potential impact on production servers (still require a backup window)
- Data backed up to disk, possibly using tape emulation (sequentially, but not continuously)
- Data backed up in backup format—IT administration still needed for restores

**Recovery**

Symantec Corporation World Headquarters
20330 Stevens Creek Blvd., Cupertino, CA 95014 USA
+1 (408) 517 8000 / +1 (800) 721 3934
www.symantec.com

Because the backup resides on disk, it is much faster to restore. There is no need to locate the tape, load it, and then reload the data. It is faster and more efficient.

**Backup Process**

1. A full backup of each file server is performed once a week.
2. Incremental/differential backups of each file server are performed daily, during off-peak hours.
3. Backups can be migrated to tape for long-term data protection or disaster recovery.

**Recovery Process**

1. Users submit a file restore request to administrators.
2. Administrators quickly restore the file from disk at the point of the last backup.

## Continuous Disk-Based Backups

**Key benefits**

Continuous data protection revolutionizes data protection by offering the core benefits of disk-based data protection (faster backups, near-instant restore), while lessening some of the hardships of current backups. Key benefits include:

- Help ensure that data is always protected
- Only captures changed portion of files (block-level changes)
- Simplifies backups—eliminates incrementals, fulls, and so on
- Can back up multiple file servers simultaneously
- Minimizes backup windows for protected systems
- Leverages tape backups for long-term archival and offsite storage
- Files in native format, enabling end-user recovery

**Key Drawbacks**

- May not provide tape-based backup, *which is still needed for long-term data protection or offsite storage*
- May not integrate with the current backup solution

**Recovery**

Instant, flexible, and granular recovery is a central focal point for continuous disk-based protection. CPS significantly reduces IT administration while improving service levels and end-user productivity. End users can find and retrieve files in seconds without contacting IT.

Key benefits include:

- Provides instantaneous recovery
- Enables end users to retrieve their own files
- Enables recovery of files from multiple points in time

**Backup Process**

Symantec Corporation World Headquarters
20330 Stevens Creek Blvd., Cupertino, CA 95014 USA
+1 (408) 517 8000 / +1 (800) 721 3934
www.symantec.com

1. Users save files to file servers (business server).
2. Continuous Protection Agent streams file changes to Backup Exec CPS.
3. Microsoft® Volume Shadow Copy Service (VSS) snapshots provide versioning and granular point-in-time recovery of files.
4. Backup Exec media server provides backup to tape for longer term retention or offsite storage.

**Recovery Process**

1. Administrators or end users can retrieve previous versions of files using simple Web-based recovery.

## Backup Exec Continuous Protection Server Key Benefits

### Eliminates Backup Windows

Symantec Backup Exec offers the Continuous Protection Server to help ensure that your data is always protected and available. As a continuous disk-based data protection solution, CPS notes when a file changes and helps ensure the change is captured and protected. It only captures granular or block-level changes, not the whole file, reducing the impact on network performance. Not only is the most recent data protected, but multiple versions of files are also captured and available for recovery or retrieval through the use of snapshots. Snapshots represent a specific point in time of the CPS backup destination. Snapshots can be created manually or scheduled to occur on a periodic basis within the CPS admin console. Snapshots are retained for a default period of 24 hours unless specified. CPS integrates with Microsoft Volume Shadow Copy Services (VSS). VSS requires a minimum of 300 MB of space before any snapshots have been taken. Additional space requirements depend on the size of the data being protected and the frequency in which the snapshots are occurring. The more frequent the snapshots, the greater the space requirements will be for storing the snapshots.

Backup Exec continuous data protection helps eliminate the ever-shrinking backup window faced by organizations by protecting data whenever a file changes—continuously. This means no more backup window, because IT is not performing the traditional full, incremental, or differential backups of business-critical data on file servers. This simplifies management and reduces costs:

- Protects data immediately and continuously
- No impact on the production business server
- Protects only changed data
- Continuously protects multiple servers simultaneously

Symantec Corporation World Headquarters
20330 Stevens Creek Blvd., Cupertino, CA 95014 USA
+1 (408) 517 8000 / +1 (800) 721 3934
www.symantec.com

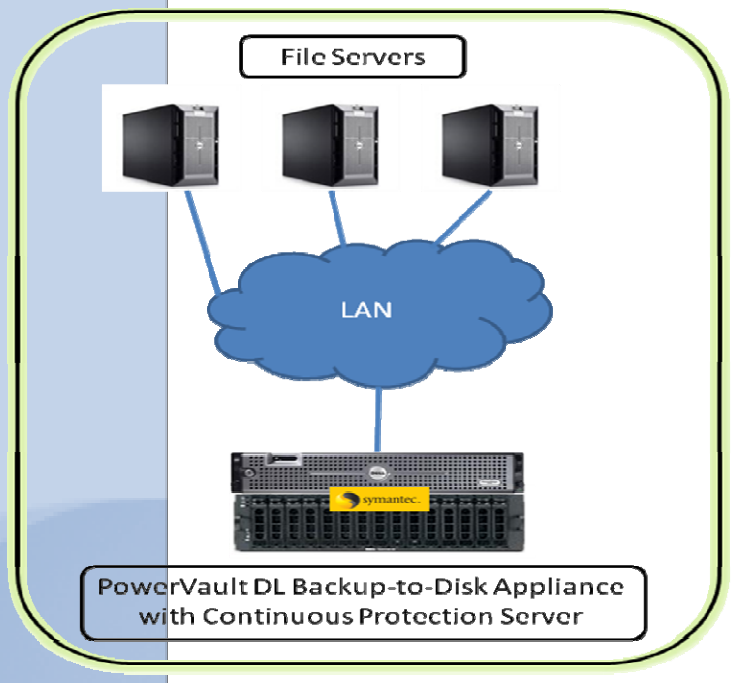


**Figure: Continuous Protection Deployment**

**Delivers Web-Based File Retrieval**

Backup Exec Continuous Protection Server also reduces overall administration costs using Backup Exec Retrieve—a simple Web interface that enables end users to retrieve previous versions of files protected by Continuous Protection Server without contacting IT. Empowering end users to retrieve their own files frees up IT to focus on other business-critical needs of the organization. Retrieving lost, corrupted, or overwritten data is as easy as searching for and downloading a file from the Internet. There is no backup tape to locate or load and no data to restore to find the correct file. Best of all, there is no client software or agents to install on individual desktops and laptops. Users only need a standard Web browser, making data retrieval easier than ever:

- Simple Web search engine–like experience
- For administrators or end users
- No special software needed—only a standard browser
- No special training needed

Symantec Corporation World Headquarters
20330 Stevens Creek Blvd., Cupertino, CA 95014 USA
+1 (408) 517 8000 / +1 (800) 721 3934
www.symantec.com

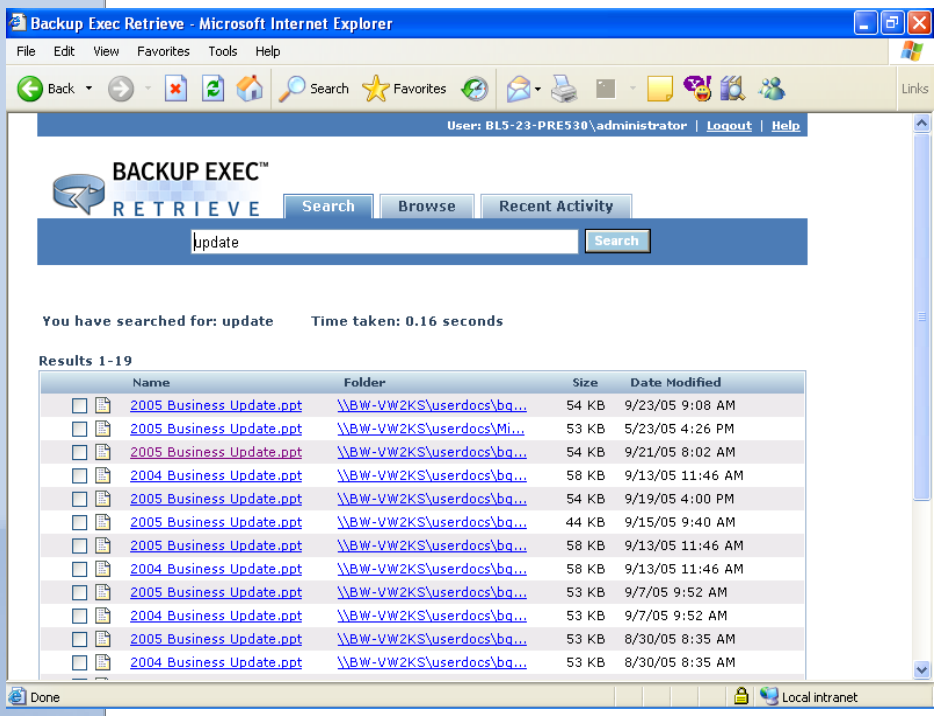


**Figure: Backup Exec Retrieve provides Web Based File Retrieval**

**Provides Comprehensive Protection: Just Add Data**

Built on the tried, trusted, and proven Backup Exec technology, Backup Exec *for Windows Servers* delivers continuous disk-based data protection combined with traditional data protection to provide a comprehensive disk-to-disk-to-tape solution, protecting business-critical files, databases, and applications.

Centralized administration provides scalable management of distributed backup and remote servers. An intuitive interface and wizards simplify data protection and recovery procedures for any level user and any size network. Sophisticated database and groupware agents provide online protection and granular recovery. Even entry-level system recovery is integrated into the Backup Exec solution. Backup Exec delivers a comprehensive disk and tape-based solution:

- Comprehensive disk-to-disk-to-tape data protection
- From applications to file servers to workstations
- Integrated management by means of Backup Exec SmartLink

While productivity and resources continue to be a major focus for organizations of all sizes, the Backup Exec SmartLink integration simplifies management for many tasks—letting IT manage more with less.

Symantec Corporation World Headquarters
20330 Stevens Creek Blvd., Cupertino, CA 95014 USA
+1 (408) 517 8000 / +1 (800) 721 3934
www.symantec.com

## Features/Benefits Highlights

### Provides Continuous Data Protection

Backup Exec provides real-time protection of Windows file servers. The instant that files are changed or created, they are protected by Backup Exec CPS technology. After the first copy of a file is protected, only the changed portion of that file is protected—at the block level—by CPS. This efficient data protection technology reduces the amount of data moving across the network and the amount of data to protect—and recover. Additionally, Backup Exec CPS enables IT and end users to retrieve not only the current version of files, but also previous versions.

### Provides Web-Based File Retrieval

Backup Exec includes Backup Exec Retrieve, a simple Web-based file retrieval that lets users retrieve their own files—without IT intervention. Searching is simple because files are indexed by name and type. No other data protection solution offers this simplicity or functionality. Because it uses a standard Web browser to enable users to retrieve lost, overwritten, or corrupted files, there is no software to install or update on individual workstations. Recovering a file or its previous versions is as easy as clicking a link to download a file from the Internet, including previous versions of files. It is simple to deploy, easy to use, and helps improve service levels without addition administration overhead.

### Provides a Total Solution

Equipped with Backup Exec CPS, Backup Exec combines continuous disk-based data protection with tape-based data protection management, providing comprehensive disk-to-disk-to-tape functionality. Administrators can monitor continuous protection jobs from the Backup Exec administration console.

### Does Not Require Active Directory or SQL

Backup Exec CPS software can run by itself on a stand-alone server or on the same server with Backup Exec *for Windows Servers*. It does not require any other Microsoft servers or components to run and it does not require the protection server to be in the same domain as the file servers it backs up.

### Provides Bandwidth Throttling

Administrators can manage and control network resource use by granting the maximum bandwidth continuous protection can use for either LANs or WANs. This helps administrators, especially those looking to eliminate hardware, media, and administration in remote offices and to centralize data protection, ensure that data is continuously protected with minimal disruption to ongoing business activities.

Symantec Corporation World Headquarters
20330 Stevens Creek Blvd., Cupertino, CA 95014 USA
+1 (408) 517 8000 / +1 (800) 721 3934
www.symantec.com

**Provides Snapshot Management and Grooming**

Backup Exec CPS provides snapshot management which gives administrators increased flexibility and granularity in managing their point-in-time snapshots. Because Backup Exec CPS leverages VSS for snapshots, a maximum of 64 snapshots can be saved on the storage volume. However, CPS is unique, as it enables administrators to define snapshot policies that control the specific periods of time snapshots are retained. Specifically, administrators can decide to hold on to each snapshot for hourly, daily, weekly, and monthly intervals, providing greater flexibility and maximizing the 64 snapshots availability.

**Automatically Recovers from Network Outages**

Backup Exec CPS can automatically recover from a network outage that has interrupted continuous protection. This feature, called *Auto Resume*, is especially useful for WAN connections and remote offices. In the event of a connectivity issue, changes will journal on the protected file server until connectivity with the protection server has been reestablished. Upon reconnecting, the CPS will automatically resume continuous protection, without the need for manual resynchronization and/or administrator intervention.

**Remote Office Deployment: Continuous Protection Server**

Continuous Protection Server is an ideal solution for protecting remote office environments that are connected over Wide-Area Networks (WAN). A key concern in WAN environments is that WAN links tend to be much slower than Local Area Network connections. Continuous Protection Server helps minimize the impact of the slow connection by only transmitting the block level changes from the remote office back to the central office When planning a remote office data protection strategy it is important to consider the following items:.

- Amount of Protected Data
- Network Bandwidth
- Data Seeding

Symantec Corporation World Headquarters
20330 Stevens Creek Blvd., Cupertino, CA 95014 USA
+1 (408) 517 8000 / +1 (800) 721 3934
www.symantec.com

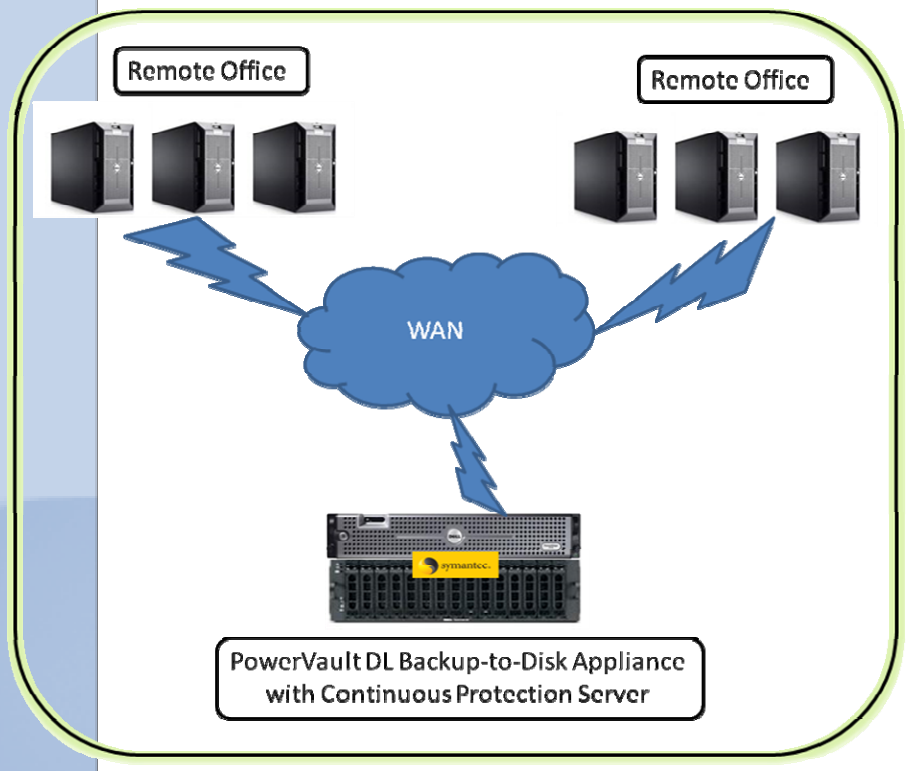


**Figure: Remote Office Deployment**

**Amount of Protected Data**

One of the key factors in sizing your data protection environment using Continuous Protection is determining the amount of data that will be sent over the network from the protected systems to the PowerVault DL Backup-to-Disk Appliance. After the initial data is copied from the protected servers to the appliance, Continuous Protection Server only copies new and changed data from the protected systems. A simple calculation for determining the amount of data to be transmitted is:

Data change rate (GB) per hour + new data rate (GB) per hour = total data/hr

**NOTE:** Continuous Protection Server transmits only the changed data (blocks) except for small files. If a file is smaller than1 MB, then the entire file will be transmitted.

Symantec Corporation World Headquarters
20330 Stevens Creek Blvd., Cupertino, CA 95014 USA
+1 (408) 517 8000 / +1 (800) 721 3934
www.symantec.com

**Network Bandwidth**

Another key factor in sizing your data protection environment using Continuous Protection Server is the available network bandwidth for backup operations. Network bandwidth is dependent on the type of network deployed in the data protection environment. The theoretical maximum network throughput values are as follows:

- 10/100 Ethernet: 1.0 MB/sec – 10 MB/sec
- Gigabit Ethernet (GbE): 100 MB/sec

These rates are theoretical maximums, and actual throughput can be substantially less. A conservative estimate is to assume that the amount of data that can be transferred is 70% of the theoretical maximum. Applying 70% to the theoretical maximums gives the following network performance:

- 10/100 Ethernet: 0.7 MB/sec – 7 MB/sec (42 MB/min – 420 MB/min)
- Gigabit Ethernet (GbE): 70 MB/sec (4.2 GB/min)

It is important to compare the amount of data that can be transmitted over the backup network with the amount of data that is expected to change and be protected over that network. When making this comparison, it is recommended to use the conservative estimate for the maximum amount of network bandwidth available to account for items such as latency and overhead. If the network bandwidth is unable to meet the requirements for the amount of data being protected, additional networks or network interfaces may be required to support the throughput requirements to protect the data.

Symantec Corporation World Headquarters
20330 Stevens Creek Blvd., Cupertino, CA 95014 USA
+1 (408) 517 8000 / +1 (800) 721 3934
www.symantec.com

## Installing Continuous Protection Server on the PowerVault DL Backup to Disk Appliance

**NOTE:** The following steps assume the PowerVault DL Backup to Disk appliance has been setup and configured for operation utilizing the automatic disk provisioning. In addition, the appliance will need to be restarted during this process to complete the installation of CPS.

Backup Exec Continuous Protection Server requires drive letter access when installed on the PowerVault DL Backup to Disk Appliance. As part of normal appliance operations Backup Exec will automatically configure and manage the disks attached to the system. However, drive letters are not assigned to the virtual disks in the system as part of this process. In order to support the installation of Backup Exec Continuous Protection server, at least one drive letter must be available to store the data protected by CPS. A drive letter can be assigned to one or more virtual disks attached to the appliance by performing the following steps:

1. Start the Windows Server Manager and Select **Storage -> Disk Management**. Windows will display all of the disks attached to the system. The Virtual Disks created by Backup Exec are labeled BEVirtualDisk.

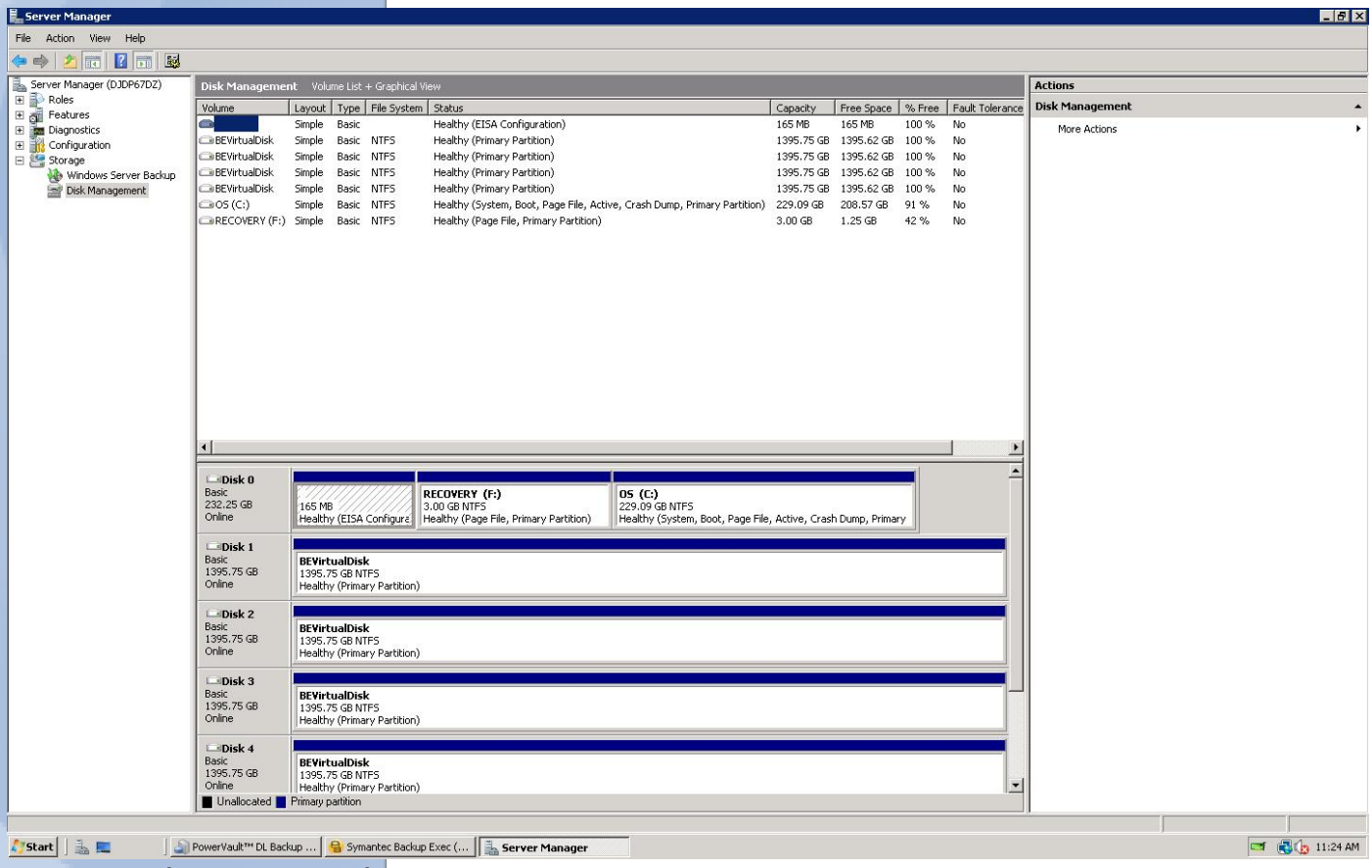


**Figure: Windows Server Disk Management**


Symantec Corporation World Headquarters
20330 Stevens Creek Blvd., Cupertino, CA 95014 USA
+1 (408) 517 8000 / +1 (800) 721 3934
www.symantec.com

2. Determine a virtual disk where the CPS data will be stored. This location is referred to as a CPS Backup Destination from within CPS. Left click on the virtual disk and select **Change Drive Letter and Path** from the popup menu.

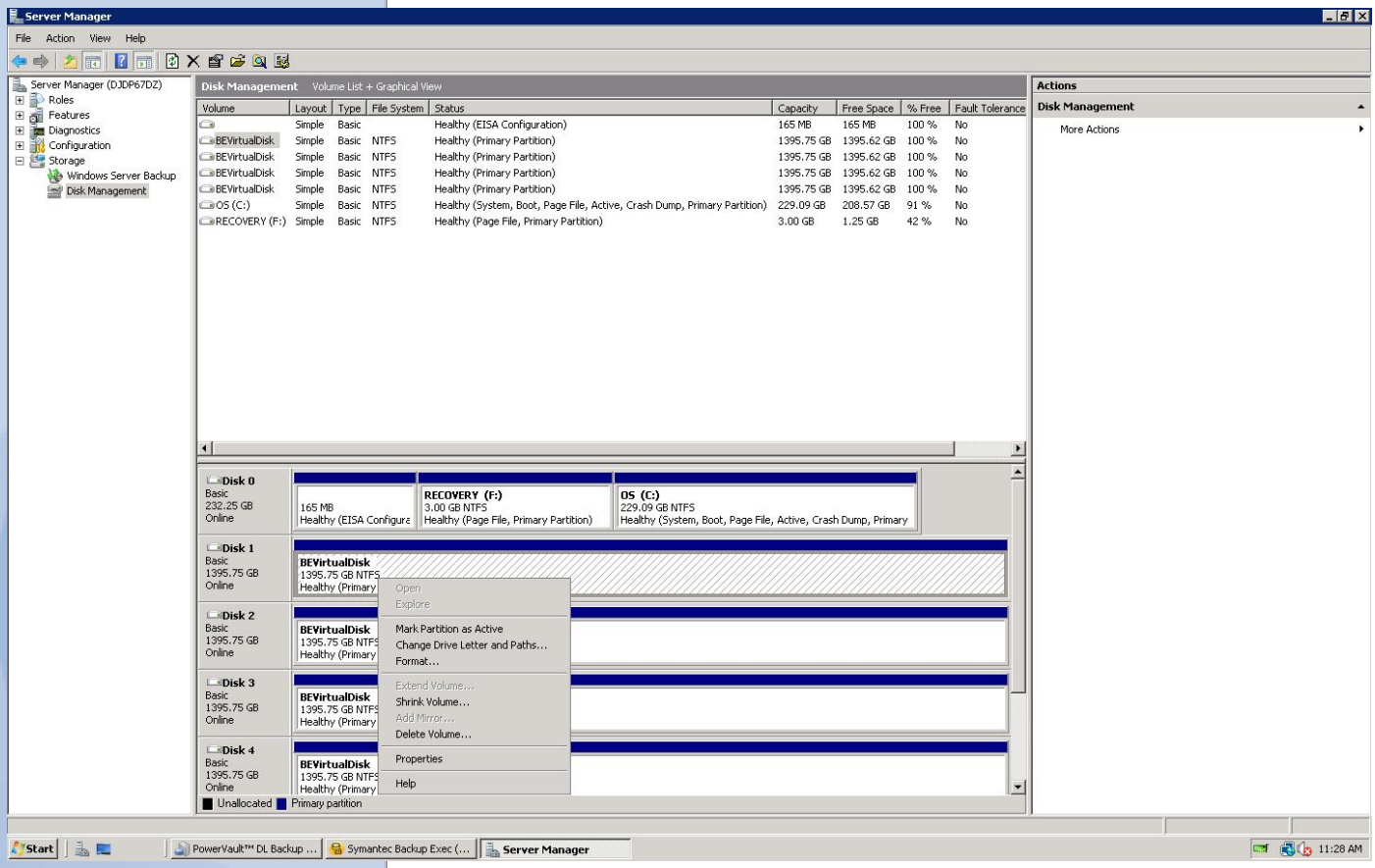


**Figure: Virtual Disks**

3. Click **Add** from the popup menu. Select an available drive letter to assign to the virtual disk. Select **Ok** to continue.


Symantec Corporation World Headquarters
20330 Stevens Creek Blvd., Cupertino, CA 95014 USA
+1 (408) 517 8000 / +1 (800) 721 3934
www.symantec.com

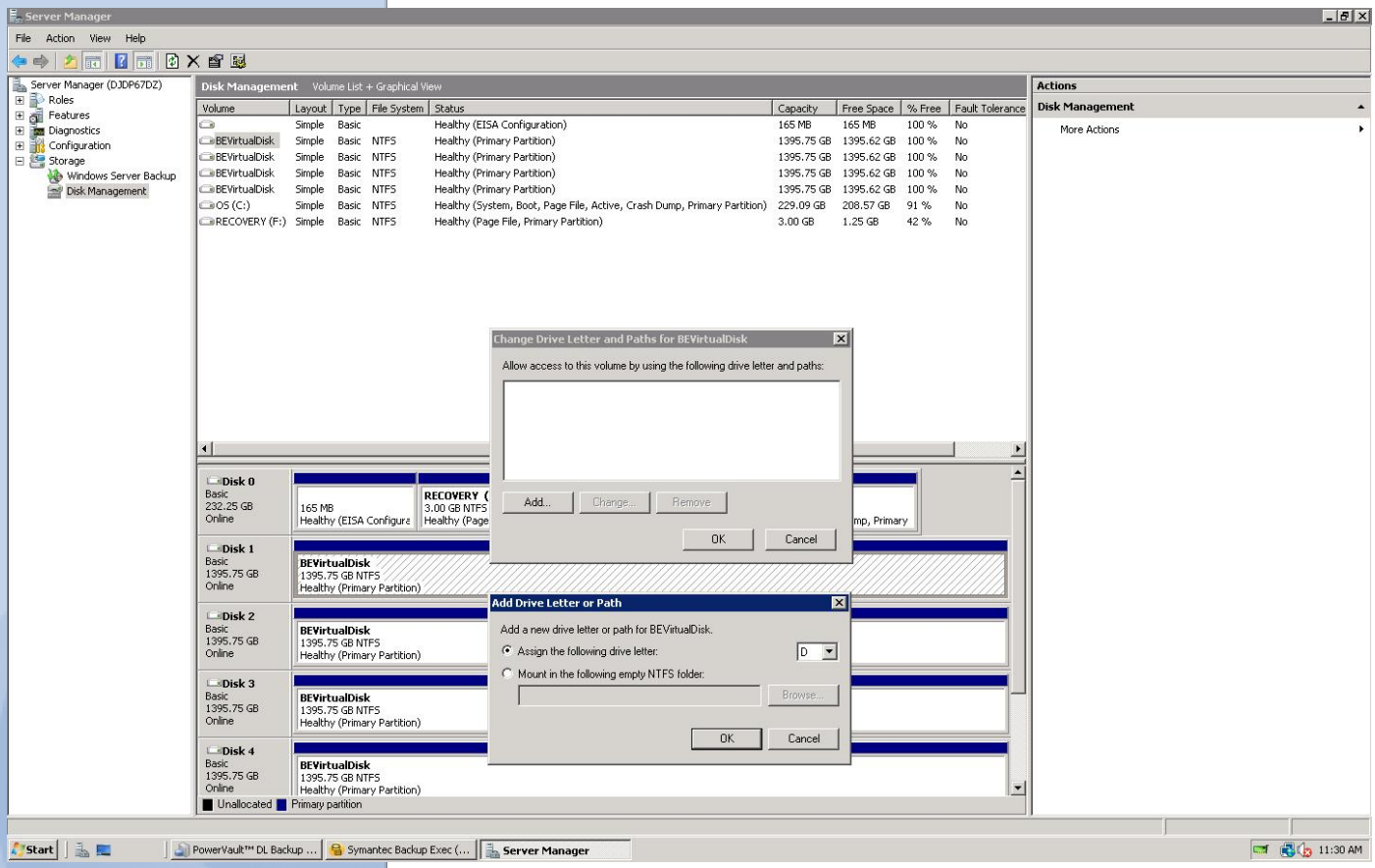


**Figure: Assigning a drive letter to a Virtual Disk**

4. Using Windows Explorer, create a folder on the virtual disk that will store the CPS data. It is not recommended to use the **BEControl** or **BEData** directories on the virtual disk to store the CPS data. These folders contain the Backup Exec configuration information and backup data from Backup Exec defined backups. In this example, the folder **CPS Data** has been manually created to store the CPS data.

Symantec Corporation World Headquarters
20330 Stevens Creek Blvd., Cupertino, CA 95014 USA
+1 (408) 517 8000 / +1 (800) 721 3934
www.symantec.com

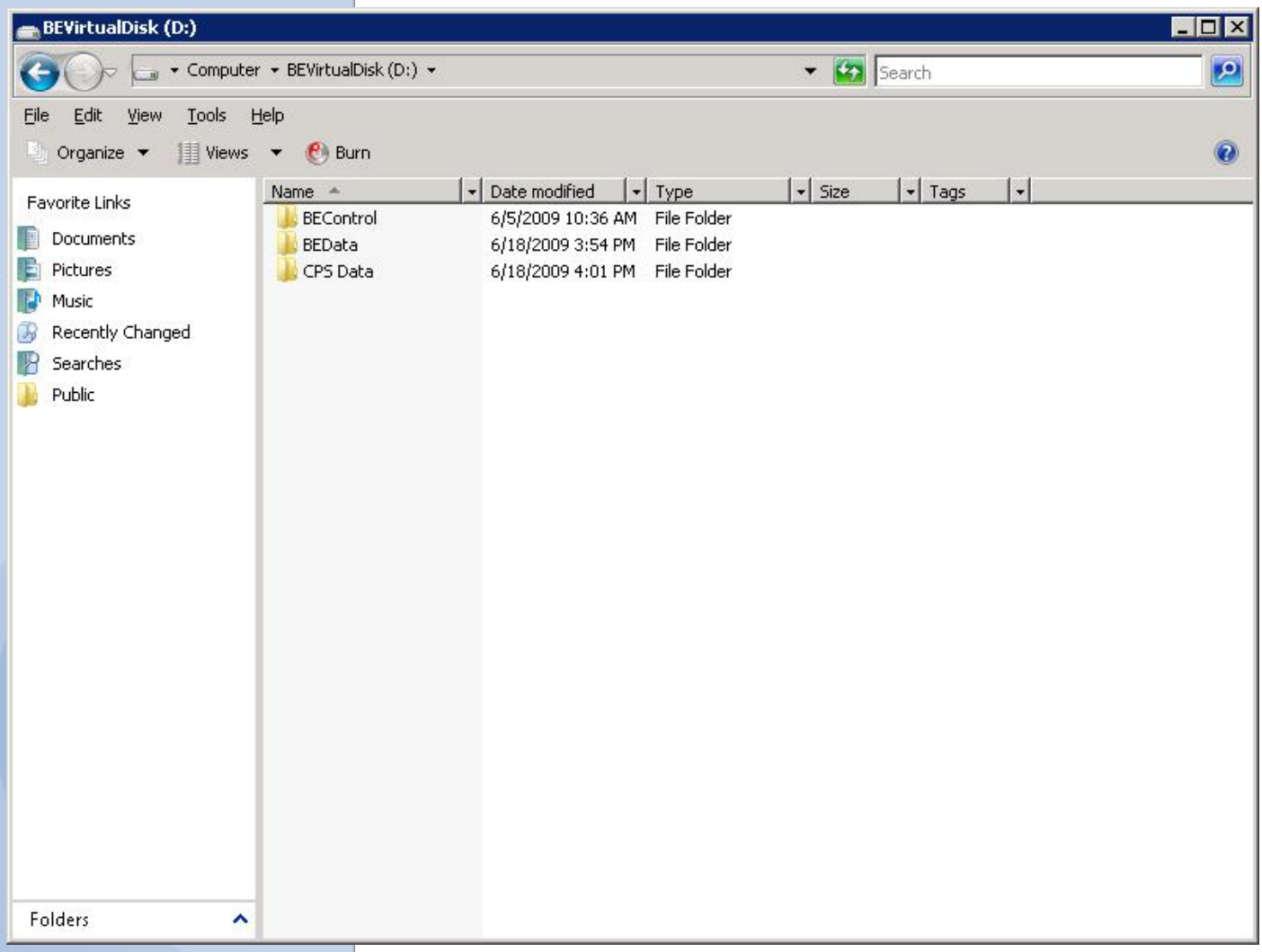


**Figure: View of Backup Exec Virtual Disk from Windows**

5. These steps can be repeated if additional virtual disks will be used as destinations to store CPS data.

The system is now ready for installation of Continuous Protection Server.

1. Locate the Backup Exec Continuous Protection Server media that is included with your PowerVault DL Backup to Disk Appliance. Insert the media into the optical drive of the PowerVault DL Backup to Disk Appliance.
2. The Symantec Backup Exec Continuous Protection Server Browser will appear. Select **Start the Backup Exec Continuous Protection Server Installation.**
3. The Welcome screen appears. Click **Next** to continue.
4. Select *I accept the terms of the license agreement* to accept the license agreement. Click **Next** to continue**.**

Symantec Corporation World Headquarters
20330 Stevens Creek Blvd., Cupertino, CA 95014 USA
+1 (408) 517 8000 / +1 (800) 721 3934
www.symantec.com

5. The Environment Pre Check appears. Correct any items that are flagged with a Red X. Click **Next** to continue**.**
6. Enter the license keys for Continuous Protection Server. The Backup Exec Agent for Windows Systems is used to license Continuous Protection Server. The license keys are included with the PowerVault DL media kit. Click **Next** to continue**.**
7. Select the options to install locally to the PowerVault DL Backup to Disk Appliance. See the screen shot below for the options to install. Click **Next** to continue.

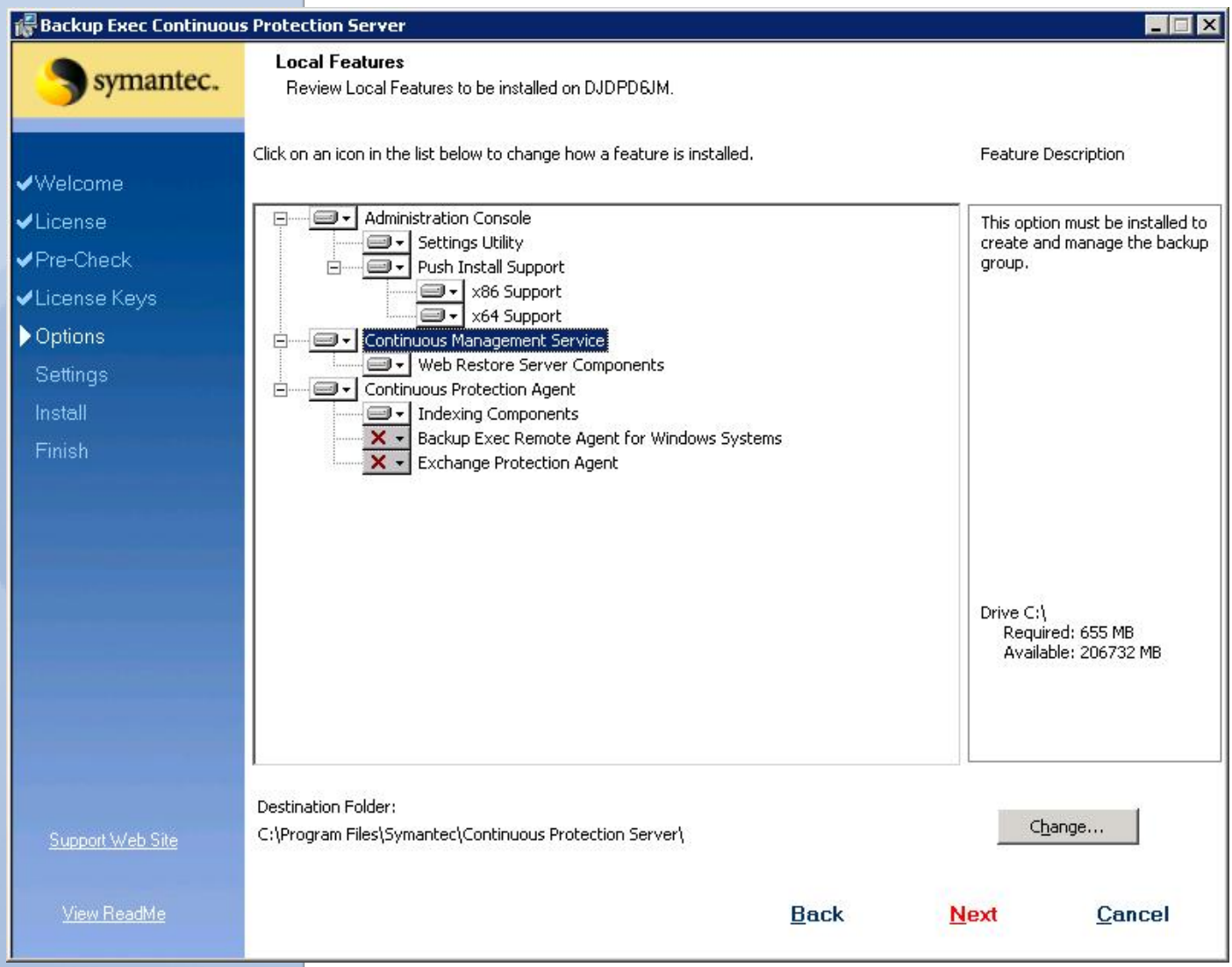


**Figure: CPS Local Install Options**


Symantec Corporation World Headquarters
20330 Stevens Creek Blvd., Cupertino, CA 95014 USA
+1 (408) 517 8000 / +1 (800) 721 3934
www.symantec.com

8. Enter the name of a new Backup Group. A Backup Group is a logical group of machines protected by CPS. If more than one Backup Group is created, only machines within the same Backup Group will be able to see each other in the CPS Administrative Console. Click **Next** to continue**.**
9. Enter the name and password of Administrator account for the CPS services to use. Click **Next** to continue**.**
10. The network interface used by the Continuous Management Service will need to be specified if multiple network interfaces are detected. Select a network interface to use for the service. Click **Next** to continue**.**
11. Specify the support folder locations for CPS.
    a. System Cache Directory – The directory where CPS can store System State and Shadow Copy Components for backup purposes.
    b. Journal Directory – Contains the dynamic changes that occur during the backup process
    c. Indexing Directory – Holds indexes of the snapshots captured on the CPS server

    Click **Next** to continue**.**
12. The installation summary appears. Verify all selections. Click **Install** to continue.
13. Once the installation is completed the appliance will need to be restarted. Click **Finish** to complete the process and restart the appliance.

Now that CPS has been installed, the following configuration steps must be performed to configure the appliance for CPS backup operations:

1. Installing Continuous Protection Agents on remote systems

   **NOTE:** This step is not required if a Backup Exec Agent for Windows System is already installed on a remote server. An agent must be installed on each remote system being protected by CPS.
2. Creating Backup Destinations – Backup destinations are the locations that contain the CPS backup data
3. Create Backup Jobs – Determine the data that is protected by CPS.
4. Seed the data – Data seeding is the process of creating an initial copy of the backup data outside the Backup Exec Continuous Protection Server framework before any continuous protection jobs have been run. This is not required; however, copying the initial data using this methodology is beneficial in environments where continuous protection jobs are run over slow network connections such as a Wide Area Network (WAN).

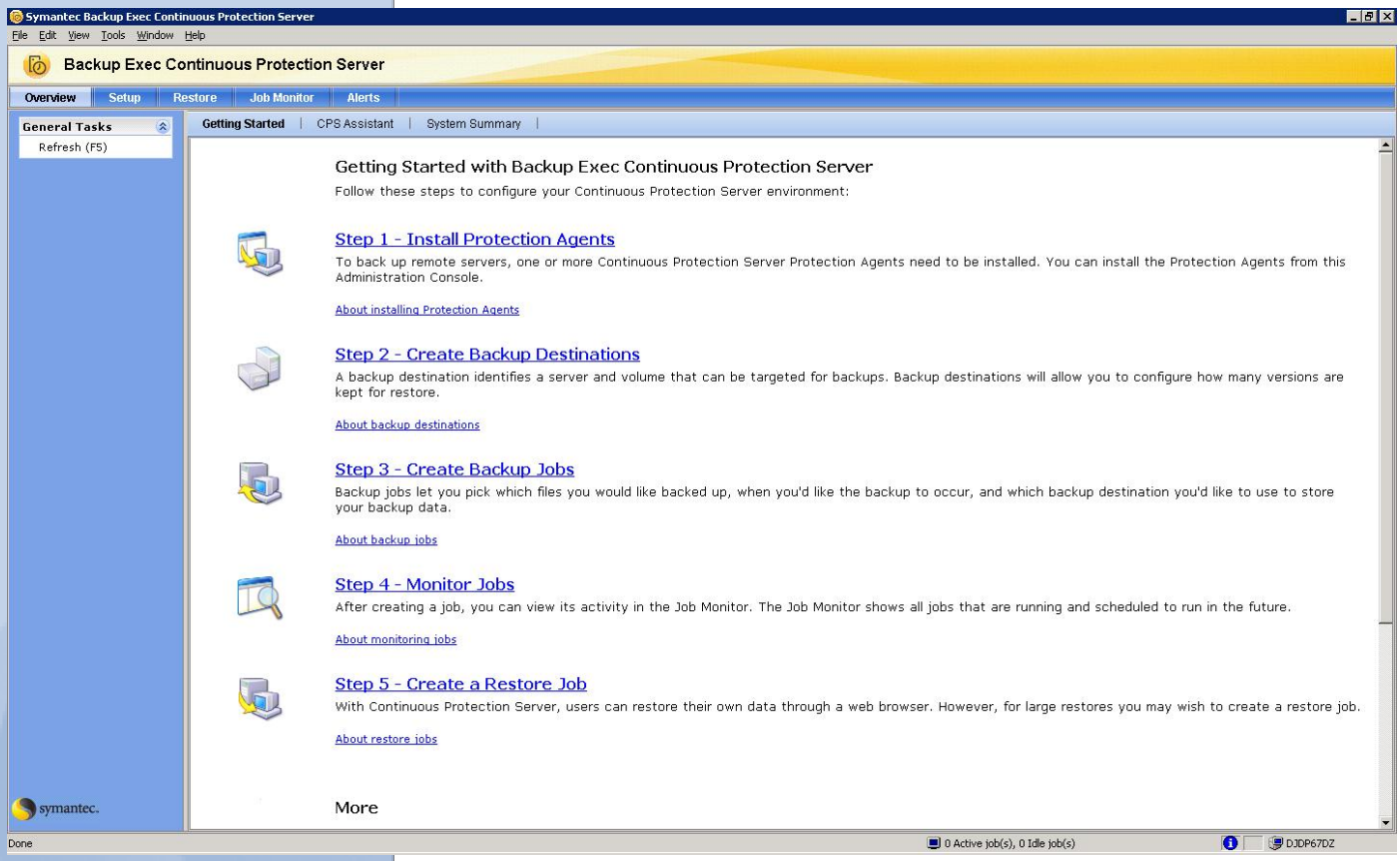


**Figure: Continuous Protection Server Getting Started Screen**

This document is not intended to cover the installation of Continuous Protection Agents. Please refer to the Backup Exec Continuous Protection Server Administrator's Guide for information on installing agents.

Backup destinations must be setup before backup jobs can be configured. From the Getting Started Screen, select **Step 2 – Create Backup Destinations**. The Backup Destination Wizard will appear.

1. Click **Next** to continue.
2. Enter a name and description for the backup destination. This information is used to help uniquely identify the backup destination. Click **Next** to continue.
3. Backup destinations can be stored on systems where the continuous protection agent or management service has been installed. In this example, the destination will be stored on the PowerVault DL Backup to Disk Appliance. Select the computer name in the **Computer** dropdown of the PowerVault DL Backup to Disk Appliance. Click **Next** to continue.
4. Determine the path on the computer where the data will be stored. If a Backup Exec Virtual Disk is being used to store the data, it is recommended that the data be stored in the **CPS Data** (or similar folder) created on the virtual disk in the previous section. Do not store the data in the **BEControl** or **BEData** folders that are present on the Backup Exec Virtual Disk. **Note:** Remember the path as it will be needed later as part of the seeding process.

Symantec Corporation World Headquarters
20330 Stevens Creek Blvd., Cupertino, CA 95014 USA
+1 (408) 517 8000 / +1 (800) 721 3934
www.symantec.com

5. The next step is determining the snapshot schedule for the backup destinations. Snapshots can be created at regular intervals to provide a point in time view of the data in the backup destination. Set a schedule for the snapshots and click **Next** to continue.
6. Retention periods are used to determine how long each snapshot is available before being overwritten. Set a retention schedule for the snapshots and click **Next** to continue.
7. The properties for the backup destination have been specified. Click **Finish** to complete the setup process.

Refer to the Backup Exec Continuous Protection Server Administrator's Guide for information on configuring CPS backup jobs. An example job configuration is provided in the next section in order to illustrate the process of data seeding.

Symantec Corporation World Headquarters
20330 Stevens Creek Blvd., Cupertino, CA 95014 USA
+1 (408) 517 8000 / +1 (800) 721 3934
www.symantec.com

## Data Seeding

Data seeding is the process of creating an initial copy of the backup data outside the Backup Exec Continuous Protection Server framework before any continuous protection jobs have been run. This is not required; however, copying the initial data using this methodology is beneficial in environments where continuous protection jobs are run over slow network connections such as a Wide Area Network (WAN). Data is copied to the Continuous Protection Server outside of the backup network (out of band) eliminating the impact that the initial backup has on the network. Once the data has been copied and placed on the Continuous Protection Server, only data that changes on the protected system is transmitted over the network.

The following example illustrates seeding three folders **dell, Documents and Settings,** and **SRD** on the C Drive from a protected server, "DL2KW2K3".

- This process assumes the CPS backup destination has been configured. In addition, data will be seeded on a per volume and per system basis meaning that separate backup and restore jobs will need to be created for each system and each volume within that system (C, D, E, etc.) that is being protected by CPS.

Backup jobs must be created before the seeding process is stated. From the Getting Started Screen, select **Step 3 – Create Backup Jobs**. The Backup Job Wizard will appear.

1. Click **Next** to continue.
2. Specify a Backup job name and description. Click **Next** to continue.
3. Select a backup destination from the drop down list. Click **Next** to continue.
4. Select the data that will be protected by this backup job. In this example, the folders **dell, Documents and Settings,** and **SRD** are selected. Click **Next** to continue.
5. Read the pop up that appears. Click **Next** to continue.
6. Specify when the backup job runs from the following options:
    a. Whenever a file changes
    b. According to a schedule
    c. Initiate a backup job manual

    Initially, set this option to **Initiate a backup job manually** when seeding the data.

    Click **Next** to continue.
7. Click **Finish** to complete the wizard.

Symantec Corporation World Headquarters
20330 Stevens Creek Blvd., Cupertino, CA 95014 USA
+1 (408) 517 8000 / +1 (800) 721 3934
www.symantec.com

Next, Backup Exec will be used to copy the data for the source system to the backup destination as part of the seeding process. Navigate to the Backup Exec U/I to for the next steps.

1. Select **New Backup Job** from Backup Exec.
2. Select the data on the remote system that is being protected by CPS backup job created in the previous set of steps. In this example, the folders **dell, Documents and Settings,** and **SRD** are being protected. Using the **Selections** tab, select these folders for the backup job.

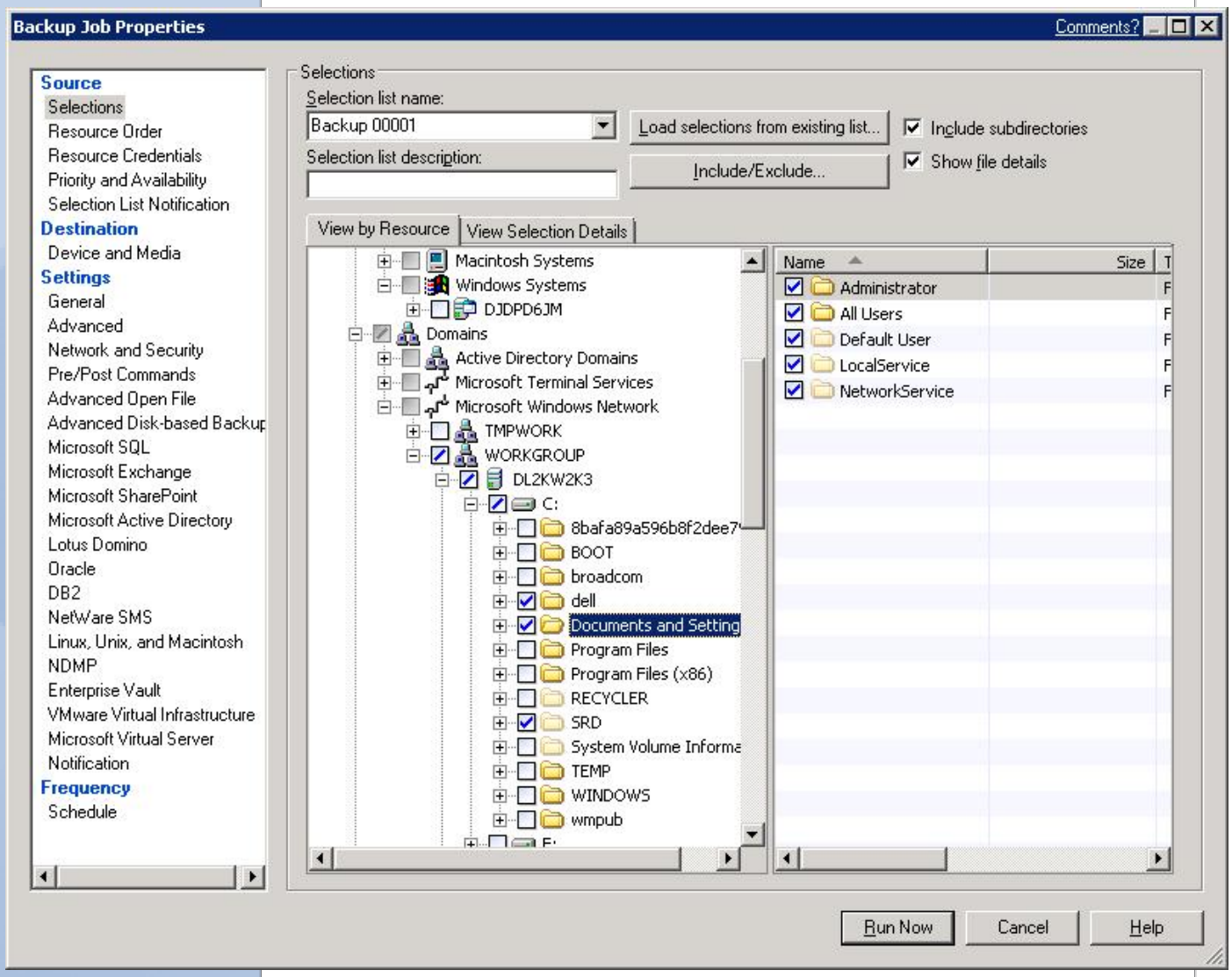


**Figure: Backup Exec Backup Selections**

3. From the **Device and Media** tab, select a target device for this backup.


Symantec Corporation World Headquarters
20330 Stevens Creek Blvd., Cupertino, CA 95014 USA
+1 (408) 517 8000 / +1 (800) 721 3934
www.symantec.com

4. Click **Run Now** to run the backup. A pop up may appear indicating that the job has been submitted. If the pop up appears, click **Ok** to continue.
5. Navigate to the Backup Exec **Job Monitor** tab and wait for the backup job to complete.
6. Once the backup job has completed, select **New Restore Job** from Backup Exec. The Restore Job Wizard appears.
7. Select the data that is to be restored as part of the seeding process. In this example, the folders **dell, Documents and Settings,** and **SRD** need to be restored. Using the **Selections** tab, select these folders for the restore job.

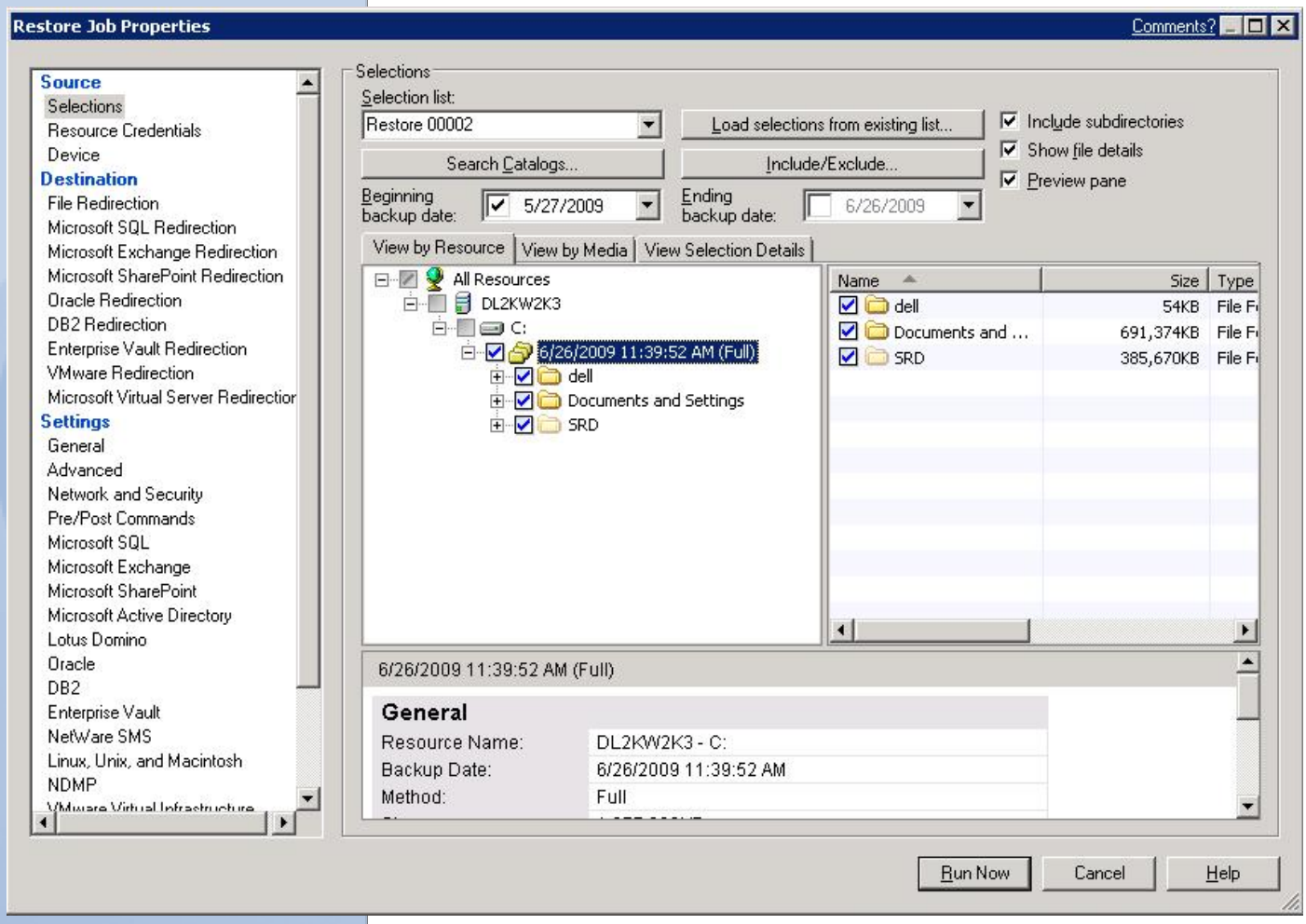


**Figure: Backup Exec Restore Selection**

8. From the **File Redirection** tab, select the checkbox for **Redirect file sets.** In the **Restore to path:** box enter the path to the CPS Backup Destination specified earlier in this document. In this example, the CPS Backup


Symantec Corporation World Headquarters
20330 Stevens Creek Blvd., Cupertino, CA 95014 USA
+1 (408) 517 8000 / +1 (800) 721 3934

Destination path is **CPS Data.** Append the source system name to the path. The source system name is the name of the system that is being protected by CPS. In this example, the source system name is **DL2KW2K3.** Append the drive letter of the source data from the source system to the path. In this example, the drive letter is **C** since the data being protected by CPS resides on the **C** drive on the system **DL2KW2K3.** The **Restore to path:** should read **\CPS Data\DL2KW2K3\C**.

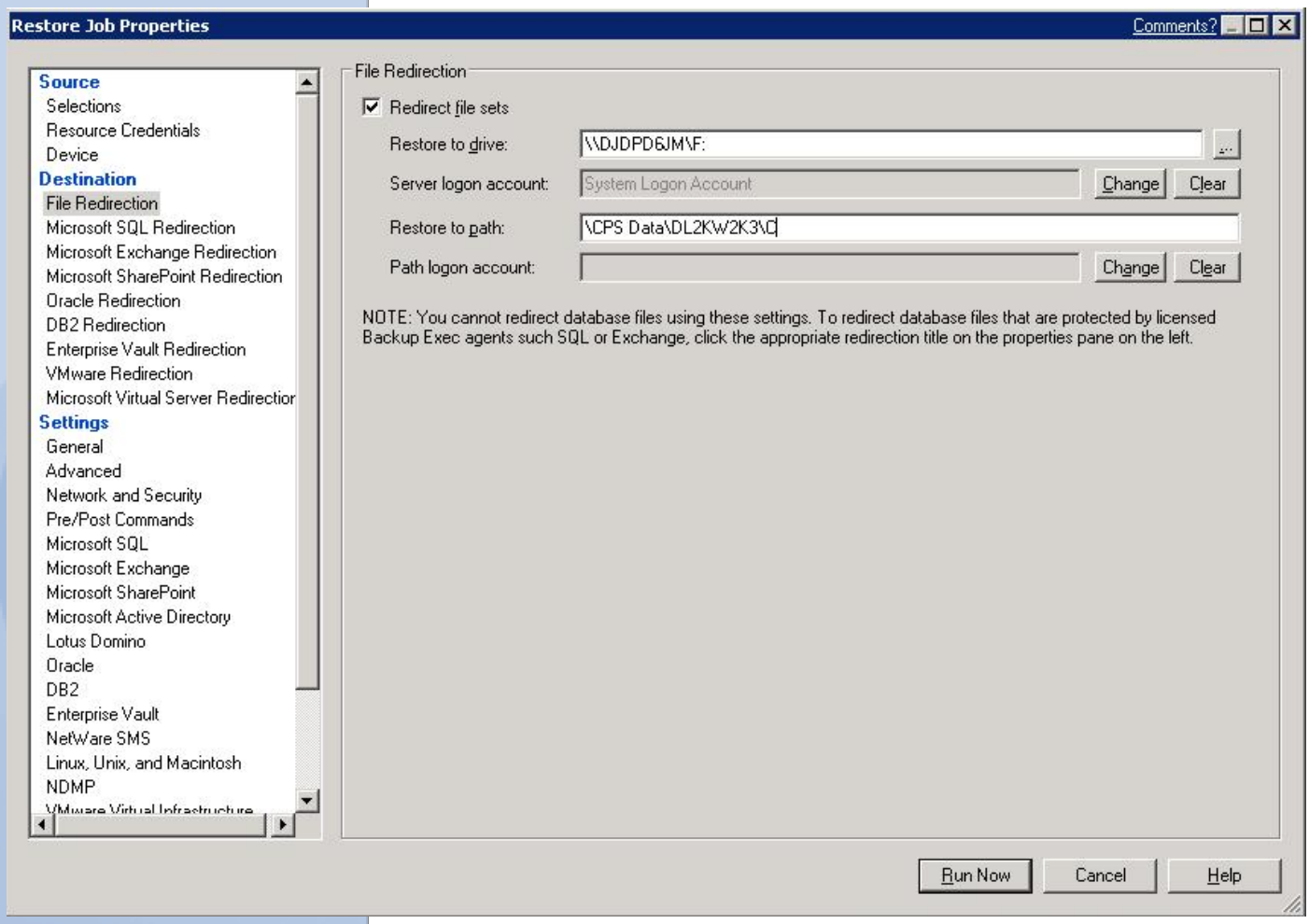


**Figure: File Redirection Restore**

9. Click **Run Now** to run the restore. A new window appears that details the selections for the restore job. Click **Ok** to continue.
10. A pop up may appear indicating that the job has been submitted. If the pop up appears, click **Ok** to continue.
11. Navigate to the Backup Exec **Job Monitor** tab and wait for the restore job to complete.


Symantec Corporation World Headquarters
20330 Stevens Creek Blvd., Cupertino, CA 95014 USA
+1 (408) 517 8000 / +1 (800) 721 3934
www.symantec.com

Repeat this process for each volume and system that is being protected by CPS.

Now that the data has been seeded to the CPS Backup Destination, the CPS Backup Jobs must be started so that data will automatically be protected.

1. From the Continuous Protection Server U/I, select the **Setup** tab. Select the **Backup Jobs** folder. Right click on each backup job and select **Properties.**
2. On the **Schedule** tab, change the **Run backups** setting to either **Whenever a file changes** or **According to a schedule**. Click **Ok** to continue.

## Important Information

The above configuration steps will locate backup data from both Backup Exec and Continuous Protection Server on the same volume(s) in the PowerVault DL Backup to Disk Appliance. However, there are situations where dedicated storage may be desired for CPS. These include:

- Isolating the CPS I/O from your backup to disk I/O to achieve maximum performance
- The folder size created by the automatic disk provisioning is insufficient to hold the CPS data

In these situations, CPS can be installed on a system other than the PowerVault DL Backup to Disk Appliance or an Advanced Disk Configuration can be used with the PowerVault DL Backup to Disk appliance to dedicate storage to CPS. Refer to the Backup Exec Continuous Protection Server for installing CPS on another system. In situations where storage is dedicated on the appliance for CPS, Backup Exec's automatic disk provisioning must be disabled and the disks are manually configured to provide the additional disk storage for CPS.

Please refer to "Configuring the Storage Array Manually" in the Dell PowerVault DL Backup to Disk Appliance Powered by Symantec Backup Exec documentation located at support.dell.com/manuals.

## Summary

While traditional tape backups have been the predominant method for data protection and recovery to date, demands for faster, more reliable, and more efficient backups and on-demand recovery have never been greater. To help organizations adapt to escalating data growth and advancing business requirements, the PowerVault DL Backup-to-Disk Appliance with the Backup Exec Continuous Protection Server, a revolutionary disk-based component that ensures that critical business data is always protected and available by using disk as the primary medium for data protection and recovery. Traditional tape backups and infrastructure can be leveraged to provide secondary data protection for longer term retention and offsite storage. By providing continuous data protection, Backup Exec CPS helps eliminate backup windows and provides instantaneous recovery by including the Web-based file retrieval: Backup Exec Retrieve. Backup Exec Retrieve integrates with Backup Exec to provide a complete disk-to-disk-to-tape solution from a single source.

Symantec Corporation World Headquarters
20330 Stevens Creek Blvd., Cupertino, CA 95014 USA
+1 (408) 517 8000 / +1 (800) 721 3934
www.symantec.com