Cloud Services for Backup Exec

Planning and Deployment Guide

Chapter 1

Introducing Cloud Services for Backup Exec

This chapter includes the following topics:

About Cloud Services for Backup Exec

Cloud Services for Backup Exec is intended for Backup Exec partners who are interested in offering managed backup services to their customers. Cloud Services for Backup Exec works within the partner's datacenter as a "private cloud" configuration.

Managed service providers (MSP) can provide backups over the Internet to a private cloud as an alternative to tape. Backups are encrypted and deduplicated. Additionally, Cloud Services for Backup Exec allows users to perform backups directly to the cloud and restore full or granular information directly from the cloud.

Cloud Services for Backup Exec is also intended for customers with widely distributed networks who are interested in sending and storing duplicate backup copies to disk and tape within a central datacenter location.

The following table further explains some Backup Exec terms that are important to understanding Cloud Services for Backup Exec.

Table 1-1 Backup Exec terms

Term	Definition
Deduplication storage folder	A deduplication storage folder provides integrated deduplication on the Backup Exec media server.
Optimized duplication	A type of duplication that enables deduplicated data to be copied directly from one OpenStorage device to another OpenStorage device from the same vendor.

Granular Recovery Technology (GRT)	A backup option that lets you restore individual items from database backups. A separate backup of the individual items is not required for you to recover one item.

See "Security considerations for Cloud Services for Backup Exec"

See "System requirements for Cloud Services for Backup Exec"

See "Configuring Cloud Services for Backup Exec"

See "About the Cloud Services for Backup Exec configurations"

Security considerations for Cloud Services for Backup Exec

Cloud Services for Backup Exec uses Backup Exec's current job and resource credential model to provide a secure experience. Additionally, Symantec recommends that you use a secure network connection between the customer location and the datacenter using a VPN solution. Various IPsec, SSL layer, and other VPN solutions are available.

You should use VLAN or routing restrictions to keep customer networks isolated from each other when you use any configuration that supports multiple customers.

See "About Cloud Services for Backup Exec"

System requirements for Cloud Services for Backup Exec

The following table lists the minimum system requirements and recommendations for running Cloud Services for Backup Exec:

Table 1-2 System requirements for Cloud Services for Backup Exec

Requirement	Description
Backup Exec media servers	You can configure Cloud Services for Backup Exec in one of three different ways. See "About the Cloud Services for Backup Exec configurations" Any media server in the cloud must include the Backup Exec Deduplication Option. The only requirement for local servers is that they comply with the requirements for Backup Exec 2010. You can find a list of compatible operating systems, platforms, and applications at the following URL: http://entsupport.symantec.com/umi/V-269-1
Deduplication Option license	You must install the Symantec Backup Exec

	Deduplication Option on both the private cloud server and any local media servers. You do not have to create a deduplication storage folder on the local media server. However you must install the Deduplication Option on the local media server to be able to access the shared deduplication storage folder on the server in the cloud. All configurations require a deduplication storage folder on the cloud media server.
Central Admin Server Option license	You must install the Symantec Backup Exec Central Admin Server Option on the local and cloud computers if you use either of the offsite copy configurations.
An active Internet connection	You must have an active Internet connection to transfer data to your private cloud deduplication storage folder.
Virtual private network (VPN)	Symantec recommends that you use a secure network connection between the customer location and the datacenter using a VPN solution. Various IPsec and SSL layer VPN solutions are available.
Domain membership for Cloud Services servers	You should establish domain membership or trust between the private cloud media server and the domain to which any local servers and remote clients belong. You must establish trust between the servers for client-side Granular Recovery Technology (GRT) deduplication and for any Central Admin Server Option (CASO) configurations.

Chapter 2

Configuring Cloud Services for Backup Exec

This chapter includes the following topics:

Configuring Cloud Services for Backup Exec

To configure Cloud Services for Backup Exec, you must complete the following steps.

Table 2-1 How to configure Cloud Services for Backup Exec

Step	Description
Step 1	You must configure the VPN between the private cloud media server instance and any computers running on the local network.
Step 2	You should consider your Backup Exec configuration. You can choose to use a dedicated offsite copy to cloud configuration or direct backup configuration for each customer. See "About the Cloud Services for Backup Exec configurations" You must configure Cloud Services for Backup Exec. See "Setting up the offsite copy to cloud configurations" See "Setting up the direct backup configuration"

Step 4	After you configure the VPN and Backup Exec, you can begin working with Cloud Services for Backup Exec. See "About working with Cloud Services for Backup Exec for the offsite copy configurations" See "About working with Cloud Services for Backup Exec and the direct backup configuration"
Step 5	If you use a VPN gateway with port restrictions, you may need to open port exceptions on both the on-premise and cloud VPN gateways. Port exceptions allow the Backup Exec media server that is located in the cloud to communicate with the on-premise Backup Exec media servers and remote agents. You should also change the CAS Backup Exec SQL port from a dynamically assigned port to a static port. The following Backup Exec support articles list all the port numbers that Backup Exec requires and which ones must be opened: http://www.symantec.com/business/support/index?page=content&id=HOWTO22990#id-SF700155293 http://www.symantec.com/business/support/index?page=content&id=HOWTO22989 http://www.symantec.com/business/support/index?page=content&id=HOWTO23022 The following Backup Exec support article details how to configure the SQL static port: http://www.symantec.com/business/support/index?page=content&id=HOWTO22985

About the Cloud Services for Backup Exec configurations

You can configure Cloud Services for Backup Exec in one of three ways.

Table 2-2 Specific configurations for Cloud Services for Backup Exec

Configuration type	Details
Offsite copy to cloud managed media server	The offsite copy to cloud managed media server configuration uses a Backup Exec managed media server, central administration server, and domain controller. The configuration provides offsite copy

	capabilities to a managed media server that is located in the private cloud. This configuration requires one managed media server per customer. See "About the offsite copy to cloud managed media server configuration"
Offsite copy to cloud central administration server	The offsite copy to cloud central administration server configuration is similar to the first, except the locations of the central administration server and managed media server are reversed. The configuration provides offsite copy capabilities to a central administration server that is located in the private cloud. This configuration requires one central administration server per customer. See "About the offsite copy to cloud central administration server configuration"
Direct backup	The direct backup configuration uses the Backup Exec Remote Agent instead of the managed media server or central administration server. The configuration provides direct backup capabilities using a Backup Exec media server that is located in the private cloud. This configuration requires one Backup Exec media server per customer. See "About the direct backup configuration"

See "Setting up the offsite copy to cloud configurations"

See "Setting up the direct backup configuration"

About the offsite copy to cloud managed media server configuration

The offsite copy to cloud managed media server configuration involves three computers.

Table 2-4 Offsite copy to cloud managed media server configuration

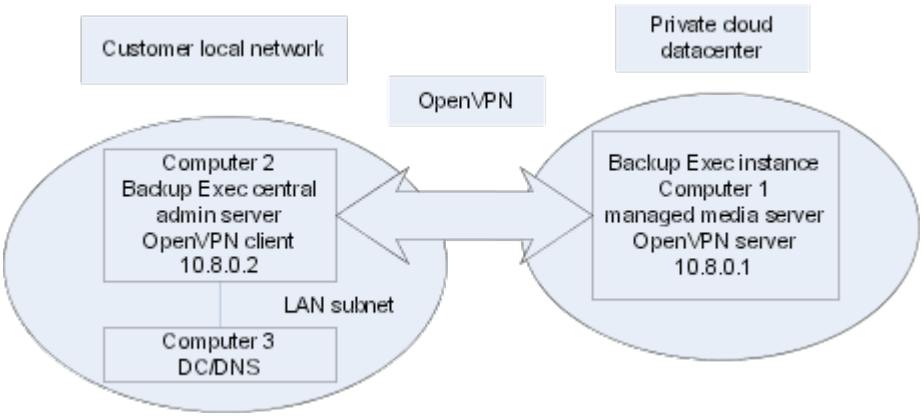
Computer	Role
Computer 1	The first computer (C1) is a Windows 64-bit server that has Backup Exec 2010 R3 installed on it. C1 is configured as a managed media server and it is located in the private cloud.
Computer 2	The second computer (C2) is a Windows 64-bit server that has Backup Exec 2010 R3 installed on it. C2 is a central administration server that is

	located on the local area network.
Computer 3	The third computer (C3) is a domain controller and DNS.

The network connection between the central administration server and the managed media server is not always required to be active. The network connection is only necessary when you run any jobs that involve the managed media server in the private cloud. The network connection does not need to be active for local jobs.

Note: You may use a 32-bit local Backup Exec server for C2 if you do not want to use a local deduplication storage folder.

Figure 2-2 Offsite copy to cloud managed media server



See "About the Cloud Services for Backup Exec configurations"

About the offsite copy to cloud central administration server configuration

The offsite copy to cloud central administration server configuration involves three computers.

Table 2-5 Offsite copy to cloud central administration server configuration

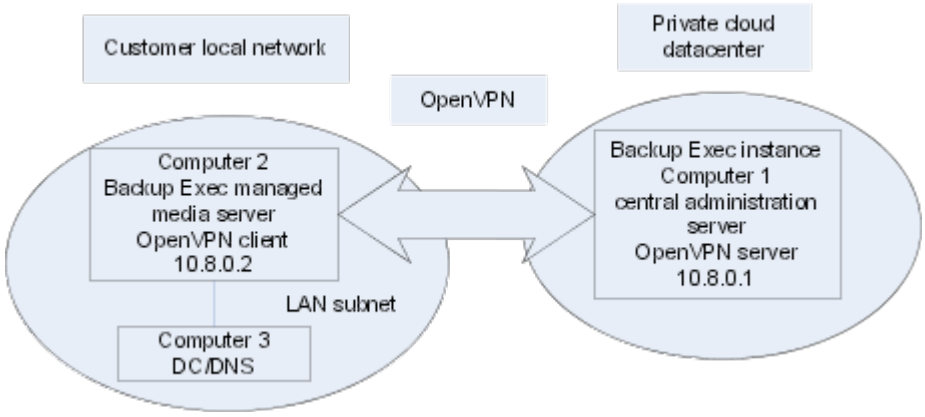
Computer	Role
Computer 1	The first computer (C1) is a Windows 64-bit server that has Backup Exec 2010 R3 installed on it. C1 is configured as a central administration server and it is located in the private cloud.
Computer 2	The second computer (C2) is a Windows 64-bit server that has Backup Exec 2010 R3 installed on it. C2 is a managed media server that is located on the local area network.
Computer 3	The third computer (C3) is a domain controller and

	DNS.

This configuration lets you manage all your Backup Exec jobs within the private cloud's datacenter. It does, however, require that the network connection between the central administration server and the managed media server is active at all times. The network connection must be active even when you run jobs locally.

Note: You can use a 32-bit local Backup Exec media server for C2 if you do not want to use a local deduplication storage folder.

Figure 2-3 Offsite copy to cloud central administration server



See "About the Cloud Services for Backup Exec configurations"

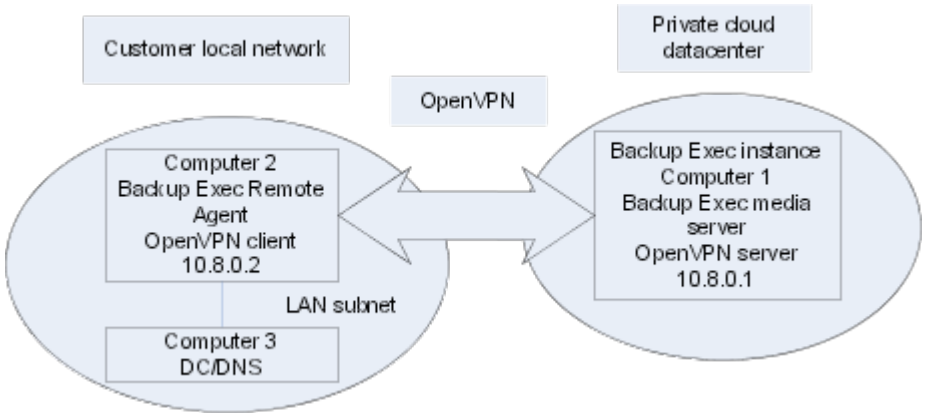
About the direct backup configuration

The direct backup configuration involves a minimum of three computers.

Table 2-6 Direct backup configuration

Computer	Role
Computer 1	The first computer (C1) is the Windows 64-bit server Backup Exec 2010 R3 media server that is located in the private cloud datacenter.
Computer 2	The second computer (C2) is the Windows Remote Agent client that is located on the local area network. You can configure multiple remote agent client computers.
Computer 3	The third computer (C3) is a domain controller and DNS.

Figure 2-4 **Direct backup**



See "About the Cloud Services for Backup Exec configurations"

Setting up the offsite copy to cloud configurations

After you have configured the VPN on the private cloud server, you should configure the Backup Exec media server or servers.

See "Configuring Cloud Services for Backup Exec"

You can select from one of two offsite copy to cloud configurations:

See "About the offsite copy to cloud managed media server configuration"

See "About the offsite copy to cloud central administration server configuration"

Table 2-7 **How to configure the offsite copy to cloud configurations**

Step	Description
Step 1	Install the Backup Exec central administration server. See "Installing the Backup Exec central administration server"
Step 2	Install the Backup Exec managed media server. See "Installing the Backup Exec managed media server"
Step 3	Configure storage devices. See "Setting up storage devices for the offsite copy configurations"
Step 4	Seed the deduplication storage folder with data. See "About seeding the deduplication storage folder for the offsite copy configurations"

Installing the Backup Exec central administration server

You must install Backup Exec for Windows Servers on the computer that serves as the Backup Exec central administration server.

See "Setting up the offsite copy to cloud configurations"

If you use the offsite copy to cloud managed media server configuration, the central administration server is installed on a local office media server (computer 2 or C2). Otherwise, the central administration server is installed as a cloud media server (computer 1 or C1) for the offsite copy to cloud central administration server configuration.

You must add the central administration server to the local domain. Install the Central Admin Server Option (CASO) on the central administration server.

Table 2-8 How to install the Backup Exec central administration server

Step	Description
Step 1	Remove the media server from the workgroup. Add the media server to your local domain by completing the following steps: • Using the Computer Properties dialog box in Windows, add the server to the domain. • Restart the computer when you are prompted to do so.
Step 2	After the server has restarted, log on with the domain account that you want to have administrator rights to your local Backup Exec instance.
Step 3	Use the proper license keys to install Backup Exec 2010 R3. Refer to the Backup Exec Help topic "About installing Backup Exec" for more information: http://www.symantec.com/business/support/index?page=content&id=HOWTO22519&cat=INSTALLING&key=15047&actp=LIST Backup Exec partners can obtain licensing information from the Symantec PartnerNet Web site at the following link: https://partnernet.symantec.com/Partnercontent/Login.jsp
Step 4	Include the Central Admin Server Option (CASO) when you install Backup Exec. Refer to the Backup Exec Help topic "Installing the CASO central administration server" for more information: http://www.symantec.com/business/support/index?page=content&id=HOWTO23024 Install the Deduplication Option when you use the offsite copy to cloud central administration server configurations. Using a local deduplication storage folder on the central administration server is optional for the offsite copy to cloud managed media server configuration.
Step 5	Use domain credentials for the default system logon account when you install Backup Exec.
Step 6	When the installation is complete, set the following registry value to **1** to disable the deduplication storage folder's GRT-to-GRT duplicate copy capability on the media server: dword HKEY LOCAL MACHINE\SOFTWARE\Symantec\Backup Exec for

	Windows\Backup Exec\Engine\Misc\DisablePDI2PDISetCopy This computer is now the central administration server that controls the managed media server across the WAN. For more information about the limitations of offsite copy Granular Recovery Technology (GRT), refer to the following topic: See "Limitations of Granular Recovery Technology with offsite copy"

Installing the Backup Exec managed media server

You must add the managed media server to the local domain.

See "Setting up the offsite copy to cloud configurations"

Note: If you use the offsite copy to cloud managed media server configuration, the managed media server is installed as the cloud media server (computer 1 - C1). Otherwise, the managed media server is installed on a local office media server (computer 2 - C2).

To install the Backup Exec managed media server

1. Remove the media server from the workgroup.
2. Do the following:

   Add the media server to your local domain by completing the following steps:

   - Use the Computer Properties dialog box in Windows to add the server to the domain.
   - Restart the computer when you are prompted to do so.

3. After the server has restarted, log on with the domain account that has administrator rights to your local Backup Exec server.
4. Install Backup Exec 2010 R3 on the server and select the **Managed Media Server** installation option. When Backup Exec prompts you for the central administration server, enter the information for your local Backup Exec central administration server. Additionally, select the Deduplication Option when you use the offsite copy to cloud managed media server configuration. Using a local deduplication storage folder on the managed media server is optional for the offsite copy to cloud central administration server configuration.
5. Select **On the central administration server** for the Device and Media Data Location.
6. At the prompt, specify the same system logon account credentials that you used to install the central administration server.
7. When the installation is complete, on the managed media server, set the following registry value to **1** to disable the deduplication storage folder's GRT-to-GRT duplicate copy capability on the media server:

dword HKEY LOCAL MACHINE\SOFTWARE\Symantec\Backup Exec for Windows\Backup Exec\Engine\Misc\DisablePDI2PDISetCopy

8. Open Backup Exec on the central administration server.
9. On the Media Servers tab, select the managed media server that you installed.
10. Under General Tasks in the task pane, select **Properties**.
11. On the Advanced tab, under Catalog location, do one of the following:

If the managed media server is configured as the cloud media server:	Select **Central administration server (centralized)**.
If the central administration server is configured as the cloud media server:	Select your preferred catalog location from among any of the available catalog location options.

12. Click **OK**.
13. On the Media Servers panel, select the media server that is located in the private cloud datacenter.
14. In the task pane, under General Tasks, click **Properties**.
15. On the Advanced tab, select **Private cloud server**.
16.

Setting up storage devices for the offsite copy configurations

Before you can run backup jobs to the private cloud, you must configure storage devices.

See "Setting up the offsite copy to cloud configurations"

Table 2-9 How to set up storage devices for the offsite copy configurations

Step	Description
Step 1	Create new local disk storage devices on computer 2 (C2). You can create a deduplication storage folder, if desired. If you want the at-rest data to be encrypted on your private cloud deduplication storage folder, edit the following file changes on your private cloud Backup Exec instance. Note: The VPN encrypts the data in transit between the local media server and the cloud media server. • Locate and edit the following text file on computer 1 (C1): C:\Program Files\Symantec\Backup Exec\contentrouter.cfg. • Find the line starting with "ServerOptions". • Set the line to `ServerOptions=fast,verify_data_read,noagent_crypt,encrypt` • Save and exit.

Step 2	Create a new deduplication storage folder on your private cloud Backup Exec instance.
Step 3	Refer to the Backup Exec Help topic "Adding a deduplication storage folder" for more information: http://www.symantec.com/business/support/index?page=content&id=HOWTO23351 Symantec recommends that you use a dedicated volume for the deduplication storage folder if possible. Give the deduplication storage folder a unique name to make it easy to differentiate from the local deduplication storage folder, if you created one.
Step 4	Share the new cloud deduplication storage folder with your local Backup Exec computer. Refer to the Backup Exec Help topic "Sharing a deduplication device between multiple media servers" for more information: http://www.symantec.com/docs/HOWTO23348
Step 5	Use the Backup Exec Services Manager to stop and restart all Backup Exec services on the local media server. The process of sharing your cloud deduplication storage folder with your local Backup Exec server is now complete. The private cloud deduplication storage folder should appear and be accessible from both C1 and C2 now.

About seeding the deduplication storage folder for the offsite copy configurations

To avoid long transfer times over the Internet, you can seed your deduplication storage folder in the cloud with the data you need to get started. Seeding your deduplication storage folder is the process of placing any initial configuration files or backup sets in the deduplication storage folder to prepare it for use. Transfer times depend on the amount of data to be copied and backed up to the private cloud Backup Exec instance.

You can seed the initial data using one of two methods, depending on the type of data:

- You can seed the deduplication storage folder with System State operating system backups. Seed the deduplication storage folder by running duplicate backup jobs of System State data of other computers running in the private cloud. Back up System State data for the computers that run the same operating system as the local computers that you want to back up. See "Seeding operating system files for the offsite copy configurations"
- You can send a physical transfer drive that contains backup sets with the relevant data from the local Backup Exec server to the private cloud datacenter. See "About using a transfer drive to seed the deduplication storage folder for the offsite copy configurations"

Seeding operating system files for the offsite copy configurations

To avoid long transfer times over the Internet, you can seed your deduplication storage folder in the cloud with the data you need to get started. One way to seed the deduplication storage folder is to use the System State backup data from other co-located computers.

See "About seeding the deduplication storage folder for the offsite copy configurations"

Table 2-10 How to seed operating system files for the offsite copy configurations

Step	Description
Step 1	Install the Backup Exec Remote Agent for Windows Systems and the Remote Agent for Linux or UNIX Servers on any computers that are co-located in the private cloud. Refer to the Backup Exec Help topic "Push-installing the Remote Agent and Advanced Open File Option to remote computers" for more information: http://www.symantec.com/business/support/index?page=content&id=HOWTO22499 Refer to the Backup Exec Help topic "About installing the Remote Media Agent for Linux Servers" for more information: http://www.symantec.com/business/support/index?page=content&id=HOWTO23502 The computers should be running the same operating system versions as the servers that are to be backed up on the local customer networks.
Step 2	Create and run backup jobs on the private cloud Backup Exec media server. Back up the System State and system volumes of these co-located computers to the private cloud deduplication storage folder.

About using a transfer drive to seed the deduplication storage folder for the offsite copy configurations

To avoid long transfer times over the Internet, you can seed your deduplication storage folder in the cloud with the data you need to get started. One way to seed the deduplication storage folder is to use a physical transfer drive.

See "About seeding the deduplication storage folder for the offsite copy configurations"

Symantec provides a calculator tool that lets you compare the time that is needed to use a transfer drive with the time that is needed to copy data over the Internet. You can find the calculator at the following link:

http://entsupport.symantec.com/umi/V-269-34

To seed your private cloud Backup Exec instance using a transfer drive, complete the following procedure:

See "Seeding the deduplication storage folder using a transfer drive for the offsite copy configurations"

Seeding the deduplication storage folder using a transfer drive for the offsite copy configurations

You can use a physical transfer drive to seed your private cloud Backup Exec deduplication storage folder. Seeding your deduplication storage folder with the files it takes to get started can save you the time of performing a large backup over the Internet.

See "About using a transfer drive to seed the deduplication storage folder for the offsite copy configurations"

To seed your deduplication storage folder using a transfer drive for the offsite copy configurations

1. Create a removable backup-to-disk folder on a removable drive on the local media server, which is computer 2 (C2). Refer to the Backup Exec Help topic "Creating a backup to disk folder by setting properties" for more information:
   http://www.symantec.com/business/support/index?page=content&id=HOWTO22746
2. Make sure that you select **Software** in the Encryption type field on the Network and Security pane. You must create or select an encryption key for software encryption. Refer to the Backup Exec Help topic "Duplicating backed up data" for more information:
   http://www.symantec.com/business/support/index?page=content&id=HOWTO23014

Copy a backup set to the backup-to-disk folder using one of the following methods:

- Create a duplicate backup job from the latest full backups of the data that you want to use to seed your private cloud deduplication storage folder. Use the local deduplication storage folder as the source and the backup-to-disk folder that you created as the destination.
- For any applications that are capable of Symantec's Granular Recovery Technology (GRT), create a full backup to the backup-to-disk folder. Do not select GRT for any specific GRT-capable applications that you want to back up. Refer to the following topic for more information about the limitations of offsite copy to GRT. See "Limitations of Granular Recovery Technology with offsite copy"

3. Run the job you created in the previous step.
4. Ship the removable disk to the private cloud datacenter.
5. Attach the removable disk to the private cloud Backup Exec media server.
6. Create a removable backup-to-disk folder on the attached removable drive using the backup-to-disk folder that you originally created on the drive.
7. Create and run a Backup Exec inventory job on the removable backup-to-disk folder. For more information, refer to "Inventorying media in a drive" in the Backup Exec Administrator's Guide.
8. Create and run a Backup Exec catalog job on the media in the removable backup-to-disk folder. Refer to the Backup Exec Help topic "Creating a new catalog" for more information:
   http://www.symantec.com/business/support/index?page=content&id=HOWTO22297
9. Perform a duplicate backup job using the files in the backup-to-disk folder as the source content. Use the cloud deduplication storage folder as the destination.
10. When the duplicate backup job is complete, you can use Backup Exec to retire and delete the files in the backup-to-disk folder. Use a disk utility to wipe the removable drive clean. When you have successfully seeded your private cloud deduplication storage folder, you have completed the configuration process. You can proceed to the following topic to begin working in Backup Exec: See "About working with Cloud Services for Backup Exec for the offsite copy configurations"

Setting up the direct backup configuration

You should configure the Backup Exec media server or servers.

See "Configuring Cloud Services for Backup Exec"

The direct backup configuration involves a minimum of three computers.

See "About the direct backup configuration"

Table 2-11 How to configure the direct backup configuration

Step	Description
Step 1	Configure the private cloud deduplication storage folder. See "Configuring the private cloud deduplication storage folder for the direct backup configuration"
Step 2	Seed the private cloud deduplication storage folder with data. See "About seeding the deduplication storage folder for the direct backup configuration"

Configuring the private cloud deduplication storage folder for the direct backup configuration

You must add the private cloud Backup Exec computer to the local domain. You also must create the Backup Exec backup-to-disk and deduplication storage folder devices on the private cloud instance.

See "Setting up the direct backup configuration"

Table 2-12 How to configure the private cloud Backup Exec instance deduplication storage folder

Step	Description
Step 1	Add C1 to your local domain by completing the following steps: • Using the Computer Properties dialog box in Windows, add C1 to the local domain. • Restart the computer when you are prompted to do so.
Step 2	Log onto C1 using the domain account that has administrator rights to your local server.
Step 3	Install Backup Exec 2010 R3 on C1 and specify a domain account system logon.
Step 4	On C1, in Backup Exec, create a new deduplication storage folder. If you want the at-rest data to be encrypted on your private cloud deduplication storage folder, edit the following file changes on your private cloud Backup Exec instance.

	Note: The VPN encrypts the data in transit between the local media server and the cloud media server. • Locate and edit the following text file on computer 1 (C1): C:\Program Files\Symantec\Backup Exec\contentrouter.cfg • Find the line starting with "ServerOptions". • Set the line to `ServerOptions=fast,verify_data_read,noagent_crypt,encrypt` • Save and exit. Refer to the Backup Exec Help topic "Adding a deduplication storage folder" for more information: http://www.symantec.com/business/support/index?page=content&id=HOWTO23351

About seeding the deduplication storage folder for the direct backup configuration

To avoid long transfer times over the Internet, you can seed your deduplication storage folder in the cloud with the data that you need to get started. Seeding your deduplication storage folder is the process of placing any initial configuration files or backup sets in the deduplication storage folder to prepare it for use. Transfer times depend on the amount of data to be copied and backed up to the private cloud Backup Exec instance.

You can seed the initial data using one of two methods, depending on the type of data that you want to seed:

- You can seed the deduplication storage folder with System State operating system backups. Seed the deduplication storage folder by running duplicate backup jobs of System State data of other computers running in the private cloud. Back up System State data for the computers that run the same operating system as the local computers that you want to back up. See "Seeding operating system files for the direct backup configuration"
- You can send a physical transfer drive that contains backup sets with the relevant data from the local Backup Exec media server to the private cloud datacenter. See "Seeding the deduplication storage folder using a transfer drive for the direct backup configuration"

Seeding operating system files for the direct backup configuration

To avoid long transfer times over the Internet, you can seed your deduplication storage folder in the cloud with the data that you need to get started. One way to seed the deduplication storage folder is to use the System State backup data from other co-located computers.

See "About seeding the deduplication storage folder for the direct backup configuration"

Table 2-13 How to seed operating system files for the direct backup configuration

Step	Description
Step 1	Install the Backup Exec Remote Agent for Windows

	Systems on any computers that you intend to back up on the local customer networks. Refer to the Backup Exec Help topic "Push-installing the Remote Agent and Adavanced Open File Option to remote computers" for more information: http://www.symantec.com/business/support/index?page=content&id=HOWTO22499 The computers that you use to seed the data should run the same operating system versions as the computers that are to be backed up.
Step 2	Create and run backup jobs on the private cloud Backup Exec media server. Back up the System State and system volumes of these co-located computers to the private cloud deduplication storage folder.

Seeding the deduplication storage folder using a transfer drive for the direct backup configuration

You can use a physical transfer drive to seed your private cloud Backup Exec deduplication storage folder. Seeding your deduplication storage folder with the files it takes to get started can save you the time of performing a large backup over the Internet.

See "About seeding the deduplication storage folder for the direct backup configuration"

Table 2-14 How to seed the deduplication storage folder using a transfer drive for the direct backup configuration

Step	Description
Step 1	Attach a removable drive to the Backup Exec Remote Agent computer (C2).
Step 2	Copy the seed files from C2 to the removable drive.
Step 3	Encrypt the files on the disk using any 3rd party encryption tool.
Step 4	Ship the transfer drive to the private cloud datacenter.
Step 5	Connect the transfer drive to computer 1 (C1).
Step 6	Temporarily unencrypt the data on the transfer drive by using the same tool that was used to encrypt the data.
Step 7	Create and run a backup job that backs up the unencrypted files. Use the deduplication storage folder in the cloud as the destination. Refer to the Backup Exec Help topic "Restoring data by setting job properties" for more information: http://www.symantec.com/business/support/index?page=content&id=HOWTO23121
Step 8	When the backup job is complete, you can delete the copied source files. Use a disk utility to wipe the removable drive clean.

When you have successfully seeded your private cloud deduplication storage folder, you have completed the configuration process.

You can proceed to the following topic to begin working with Backup Exec.

See "About working with Cloud Services for Backup Exec and the direct backup configuration"

Chapter 3

Working with Cloud Services for Backup Exec

This chapter includes the following topics:

About working with Cloud Services for Backup Exec for the offsite copy configurations

Cloud Services for Backup Exec lets you manage backup jobs and policies using the Central Admin Server Option (CASO) and the Deduplication Option.

You may choose to start and stop the private cloud Backup Exec instance VPN link connection manually when you run jobs. Or you may choose to have the VPN link connected and the instance running permanently. Symantec provides a helpful calculator tool that lets you estimate the time that is involved in copying data over the Internet. The cloud backup time calculator can be useful for planning your cloud backup strategy. You can use the calculator to determine if your system resources are adequate for backing up the customers' data within an allotted backup window. The time estimates can help you decide how much data you can reasonably support and how much time you should dedicate to cloud backups.

You can find the calculator at the following link:

http://entsupport.symantec.com/umi/V-269-34

See "Creating duplicate copy policies for the offsite copy configurations"

See "About restoring data from the private cloud using the offsite copy configurations"

See "Restoring data from the private cloud using the offsite copy configurations"

See "Restoring data from the private cloud with a transfer drive using the offsite copy configurations"

Creating duplicate copy policies for the offsite copy configurations

You can copy back up data to your private cloud Backup Exec instance by creating a duplicate copy policy. The policy resides on the central administration server. The policy backs up data to the local deduplication storage folder and then copies those backup sets to the private cloud deduplication storage folder. A third template in the policy verifies that the set was copied to the deduplication storage folder using the cloud media server.

To create duplicate copy policies for the offsite copy configurations

1. On the central administration server, open Backup Exec.
2. On the navigation bar, click **Job Setup**.
3. In the task pane, under Selection Lists Tasks, select **New backup selection list**.
4. Select the resources that you want to back up from the backup selections pane.
5. In the Properties pane, under Destination, click **Device**.
6. Check **Restrict backup of the selection list to devices on the following media server or media servers in a pool**.
7. Select the local media server that is the destination of your local backup jobs.
8. Complete any other remaining options as necessary to create the backup selection list for your policy. Refer to the Backup Exec Help topic "Creating selection lists" for more information: http://www.symantec.com/business/support/index?page=content&id=HOWTO22687
9. On the navigation bar, click **Job Setup**.
10. In the task pane, under Policy Tasks, click **New policy**.
11. Enter a policy name and description.
12. Click **New Template**.
13. On the Template Selection dialog box, select **Backup Template**, and then click **OK**.
14. In the Properties pane, under Destination, click **Device and media**.
15. In the Device field, select your local deduplication storage folder.
16. In the Properties pane, under Settings, click **General**.
17. In the Template name field, enter a name for the template.
18. In the Backup set description field, enter a description for the backup set.
19. Configure any additional job settings for the backup job.
20. In the Properties pane, under Frequency, click **Schedule**.
21. Configure the schedule for when you want the job to run. Refer to the Backup Exec Help topic "Scheduling jobs" for more information: http://www.symantec.com/business/support/index?page=content&id=HOWTO22633

22. When you are finished configuring the backup template, click **OK**.
23. On the New Policy dialog box, click **New Template** again.
24. On the Template Selection dialog box, select **Duplicate Backup Sets Template**, and then click **OK**.
25. Select the backup template that you created in the preceding steps.
26. In the Properties pane, under Destination, click **Device and Media**.
27. In the Device field, select the deduplication storage folder on the cloud-based media server.
28. Select **Use media server deduplication**.

Note: Do not change any other fields on the Device and Media dialog box.

29. In the Properties pane, under Advanced, clear the **Verify after job completes** option. Use a separate verify template to verify the job rather than verifying the job as part of the duplicate template. A separate template lets you avoid reading the entire set data over the WAN.
30. In the Properties pane, under Frequency, click **Schedule**.
31. Configure the schedule for when you want the job to run.
32. Click **OK**.
33. On the New Policy dialog box, click **New Template** again.
34. On the Template Selection dialog box, select **Verify Backup Sets Template**, and then click **OK**.
35. Select the duplicate template that you created in the preceding steps.
36. In the Properties pane, under Frequency, click **Schedule**.
37. Configure the schedule for when you want the job to run.

Note: You can add additional duplicate backup set templates to the policy if you want to configure send additional copies to tape or a remote location, for example.

38. Click **OK**.
39. Create a backup job using the policy and the selection list that you created. Refer to the Backup Exec Help topic "About creating jobs using policies and selection lists" for more information: http://www.symantec.com/business/support/index?page=content&id=HOWTO22927 The duplicate backup job now runs according to the schedule you configured in the policy.

About restoring data from the private cloud using the offsite copy configurations

After you have backed up data to the private cloud Backup Exec instance, you can restore it at any time. Restoring data from a private cloud Backup Exec deduplication storage folder is very similar to restoring data normally in Backup Exec.

See "Restoring data from the private cloud using the offsite copy configurations"

It may be more efficient to restore a large amount of data from a Backup Exec private cloud instance using a physical transfer drive. You can use the transfer drive to transfer the data to the local Backup Exec media server. Then use the local media server to run the restore job.

See "Restoring data from the private cloud with a transfer drive using the offsite copy configurations"

Restoring data from the private cloud using the offsite copy configurations

You can restore data from the private cloud Backup Exec instance to the local Backup Exec client computers.

See "About restoring data from the private cloud using the offsite copy configurations"

To restore data from the private cloud using the offsite copy configurations

1. Ensure that the server that you restore contains the network route command that allows it to communicate with computer 1 (C1) as described in the following procedure: See "Configuring local network routing"
2. Open Backup Exec on the central administration server.
3. On the navigation bar, click the arrow next to Restore.
4. Browse the backup set that you want to restore. Select that set and any other necessary job options, and then submit the job. Refer to the Backup Exec Help topic "Restoring data by setting job properties" for more information:

Note: The Media Location column in the Restore job details panel lists the storage devices on which particular backup sets and media are located. It may be useful to reference this information when you determine from which media server location you want to restore data.

Restoring data from the private cloud with a transfer drive using the offsite copy configurations

You can copy data from the private cloud Backup Exec instance to the local Backup Exec media server using a transfer drive. Using a transfer drive can be useful if you want to restore a large amount of data at one time. A large restore job can affect your system resources, depending on the amount of available bandwidth and time to complete the job.

See "About restoring data from the private cloud using the offsite copy configurations"

To restore data from the private cloud using a transfer drive and the offsite copy configurations

1. Create a removable backup-to-disk folder on a removable drive on computer 1 (C1), the private cloud Backup Exec instance. Refer to the Backup Exec Help topic "Creating a backup-to-disk folder by setting job properties" for more information:
   http://www.symantec.com/business/support/index?page=content&id=HOWTO22746
2. Create a duplicate backup job for the backup sets that you want to restore from the cloud-based deduplication storage folder. Select the backup-to-disk folder that you created as the destination storage device. Make sure that you select **Software** in the Encryption type field on the Network and Security pane. You must create or select an encryption key for software encryption. Refer to the Backup Exec Help topic "Duplicating backed up data" for more information:
   http://www.symantec.com/business/support/?page=content&id=HOWTO23014

3. After the job is complete, ship the transfer drive to the local office.
4. After the removable drive arrives, connect the drive to the local media server.
5. Create a backup-to-disk folder on computer 2 (C2) using the removable drive folder as the path.
6. Create and run Backup Exec inventory and catalog jobs on the media in the backup-to-disk folder. For more information, refer to "Inventorying media in a drive" in the Backup Exec Administrator's Guide. Refer to the Backup Exec Help topic "Creating a new catalog" for more information: http://www.symantec.com/business/support/index?page=content&id=HOWTO22297
7. Create a job to restore the data from the new backup-to-disk folder to the appropriate destination.
8. Erase the data from the transfer drive.

Restoring data from a managed media server in the event of a central administration server failure

If a hardware failure or other disaster affects your central administration server, it makes it impossible for your managed media server to run backup or restore jobs. You can recover the central administration server by configuring a replacement computer and reinstalling the Backup Exec central administration server. You can also, however, convert a managed media server to a standalone media server to restore the central administration server.

To convert a managed media server to a standalone media server to restore the central administration server

1. On the managed media server, note the names and directory paths of any local backup-to-disk folders. The backup-to-disk properties are located on the Devices tab.
2. If the managed media server has its own deduplication storage folder, note the folder's name, path, logon account, and password properties. The deduplication storage folder's properties are located on the Devices tab.
3. Open the Add or Remove Programs dialog from the Windows control panel.
4. Select the **Change** option for Symantec Backup Exec.
5. When you reach the Configure Options panel, deselect the **Managed Media Server** and **SAN Shared Storage Option** features. When the installation is complete, the computer is no longer a managed media server. It is now a standalone media server.
6. Open Backup Exec and select the Devices tab.
7. Recreate any local backup-to-disk folders by adding new backup-to-disk folders using the same names and paths that you noted in step 1.
8. Recreate any deduplication storage folders by adding new deduplication storage folders using the same information that you noted in step 2.

Note: It might take much longer to recreate an existing folder than it would to create a new folder. The amount of time depends on how many backup sets the folder contained.

---

9. Create and run a Backup Exec inventory job on each storage device that you recreated. For more information, refer to "Inventorying media in a drive" in the Backup Exec Administrator's Guide.
10. Create and run a Backup Exec catalog job on each media file that the inventory job discovered. Refer to the Backup Exec Help topic "Creating a new catalog" for more information: http://www.symantec.com/business/support/index?page=content&id=HOWTO22297 You can now use the

standalone media server to restore any backup sets that were stored on the media server's storage devices. Once the central administration server has been recovered, you may convert it back into a managed media server using the Backup Exec change installation dialog again. Select the managed media server feature to reconfigure the computer as a managed media server.

About working with Cloud Services for Backup Exec and the direct backup configuration

Cloud Services for Backup Exec lets you manage backup jobs and policies with client-side deduplication for the direct backup configuration.

Symantec provides a helpful calculator tool that lets you estimate the time that is involved in copying data over the Internet. The cloud backup time calculator can be useful for planning your cloud backup strategy. You can use the calculator to determine if your system resources are adequate for backing up the customers' data within an allotted backup window. The time estimates can help you decide how much data you can reasonably support and how much time you should dedicate to cloud backups.

You can find the calculator at the following link:

http://entsupport.symantec.com/umi/V-269-34

See "Enabling remote agent sharing and client-side deduplication for the direct backup configuration"

See "Creating backup jobs for the direct backup configuration"

See "Restoring data from the private cloud with a transfer drive using the direct backup configuration"

Enabling remote agent sharing and client-side deduplication for the direct backup configuration

Before you can create and run direct backup jobs to the private cloud Backup Exec instance, you must enable remote agent sharing and client-side deduplication. You must complete the following procedure for any remote servers from which you want to run direct backup jobs to the private cloud media server.

To enable remote agent sharing and client-side deduplication for the direct backup configuration

1. In Backup Exec, on the navigation bar, click **Devices**.
2. In the task pane, under Device Tasks, click **Configure devices assistant**.
3. On the Configure Devices Assistant dialog box, click **Remote Agent Deduplication**.
4. On the General tab, in the Server field, enter the name of computer 1 (C1).
5. On the Sharing tab, select computer 2 (C2) and C1.

Note: You must stop and restart Backup Exec services on both C1 and C2.

After you have enabled remote agent sharing and client-side deduplication, you can create and run direct backup jobs.

See "Creating backup jobs for the direct backup configuration"

Creating backup jobs for the direct backup configuration

After you have configured the VPN and enabled any additional computers for remote agent sharing and client-side deduplication, you can create and run direct backup jobs.

See "Enabling remote agent sharing and client-side deduplication for the direct backup configuration"

Use the following procedure to back up data directly to the private cloud Backup Exec instance.

To create backup jobs for the direct backup configuration

1. On computer 1 (C1), open Backup Exec.
2. On the navigation bar, click the arrow next to **Backup**.
3. From the backup selections pane, select the data that you want to back up from computer 2 (C2).
4. In the Properties pane, under Destination, click **Device and Media**.
5. In the Device field, select the private cloud deduplication storage folder.
6. Ensure that the **Use client-side deduplication** field is selected.
7. In the Properties pane, under Settings, click **General**.
8.

Complete the following fields with any relevant information:

- Job name
- Backup set description

9. Configure any other necessary job options: Refer to the Backup Exec Help topic "Creating a backup job by setting properties" for more information: http://www.symantec.com/business/support/index?page=content&id=HOWTO31077
10. Do one of the following:

To run the backup job now:	Click **Run Now**.
To schedule the backup job for later:	In the Properties pane, under Frequency, click **Schedule**.

Restoring data from the private cloud with a transfer drive using the direct backup configuration

You can create a normal restore job to restore data from the private cloud Backup Exec instance to the local client. However, if you want to restore a large amount of data at one time, it may make sense to use a physical transfer drive. The time it takes to transfer a large amount of data depends on the amount of available bandwidth and the time to complete the job.

To restore data from the private cloud with a transfer drive using the direct backup configuration

1. Create and run a redirected restore job on computer 1 (C1) to restore the files to a folder on a removable disk drive.
2. After the job has completed, encrypt the files on the disk using any 3rd party encryption tool.
3. Ship the removable drive to the local office.
4. When the removable drive arrives, unencrypt the files using the same tool that you used to encrypt them.
5. Transfer the unencrypted files to their proper destination on computer 2 (C2).
6. Erase or wipe the files from the transfer drive completely to ensure that the data is permanently removed.

Backup Exec deduplication storage folder requirements

The Backup Exec deduplication storage folder requirements apply to all private cloud configurations. If you reach the share limit on a particular cloud media server, you must add additional cloud media servers.

Refer to the Backup Exec Help topic "About deduplication storage folders" for more information:

http://www.symantec.com/business/support/index?page=content&id=HOWTO23352

Limitations of WAN latency

If your network has high levels of network latency, it can adversely affect the performance of your initial direct cloud backup job. Latency can also affect some duplicate backup jobs that transfer data between the local office and the private cloud media server. You may experience performance issues even if you seeded the deduplication storage folder with a transfer drive, although you always improve performance by seeding folders. During the initial backup job, Backup Exec identifies and caches information about data segments, which provides more efficient performance for subsequent jobs.

Note: High latency values can be considered any average round-trip latency of over 30 milliseconds. The higher the latency, the more Backup Exec's performance is affected.

This limitation does not apply to duplicate backup jobs that are not GRT-enabled, when both the source device and target device are deduplication storage folders.

The following are limitations to using Cloud Services for Backup Exec in high latency environments:

- Duplicate backup jobs that use a source device other than a deduplication storage folder and a private cloud deduplication folder as the destination experience performance issues. Avoid these performance issues by using a deduplication storage folder as local source storage device.
- You may find that using the direct back up to cloud configuration is not suitable for backing up large amounts of data.
- If you delete and recreate policies for the same resources, Backup Exec must cache the data fingerprints all over again. So you may experience the same performance issues as with the initial direct cloud backup job.

Limitations of Granular Recovery Technology with offsite copy

The following are limitations to using Backup Exec's Granular Recovery Technology (GRT) option with the offsite copy configuration:

- Local GRT backup sets that you copy to the private cloud deduplication storage folder are copied as an MTF tape format for more efficient transport. Granular restore of these sets is possible, but it requires staging the set on the cloud media server during granular restore job execution. This limitation does not exist for direct backup of GRT sets to the cloud deduplication storage folder.
- Copying duplicate GRT-enabled sets from local tape devices directly to a cloud deduplication storage folder is not recommended and can result in excessive job run times.
- Backing up GRT-enabled sets directly to the cloud media server may cause reduced performance times in high latency environments. You may experience reduced performance even after the initial backup. If performance continues to be a problem, you may want to disable GRT for direct backups.

Limitations of SAN Shared Storage Option

The following are limitations to using Backup Exec's SAN Shared Storage Option (SSO):

- If you use the offsite copy configuration, you should not configure cloud media servers and local media servers as members of the same SSO SAN. If cloud media servers and local media servers are members of the same SAN, jobs may be incorrectly delegated to media servers.

Limitations of device pools

You should not combine storage devices that are attached to cloud media servers and storage devices that are attached to local media servers in the same device pool. Combining those devices in the same device pool can cause jobs to be incorrectly delegated to media servers.

1. .