Connected Backup

Software Version 9.0.6

Administering the Data Center

Document Release Date: April 2022
Software Release Date: April 2022

Legal notices

Copyright notice

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Documentation updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

You can check for more recent versions of a document through the https://www.microfocus.com/documentation/connected-backup/.

Additionally, if you subscribe to the appropriate product support service, you will receive new or updated editions of documentation. Contact your Micro Focus sales representative for details.

Support

Visit the MySupport portal to access contact information and details about the products, services, and support that Micro Focus offers.

This portal also provides customer self-solve capabilities. It gives you a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the MySupport portal to:

- Search for knowledge documents of interest
- Access product documentation
- View software vulnerability alerts
- Enter into discussions with other software customers
- Download software patches
- Manage software licenses, downloads, and support contracts
- Submit and track service requests
- Contact customer support
- View information about all services that Support offers

Many areas of the portal require you to sign in with a Software Passport. If you need a Passport, you can create one when prompted to sign in. To learn about the different access levels the portal uses, see the Access Levels descriptions.

Contents

Chapter 1: Data Center services

This chapter provides an overview of the services that the Data Center uses to run Data Center servers.

Services overview

To perform the necessary tasks to run the Data Center server, the Data Center uses the following services:

- BackupServer overview, below — Facilitates data backups and retrievals
- IndexServer overview, on page 11 — Indexes file and archive information to databases
- ReplicationServer overview, on page 11 — Replicates between servers in a mirrored pair configuration
- PoolServer overview, on page 12 —Maintains the shared pool that the SendOnce technology uses
- Compactor overview, on page 13 — Removes old data from the Data Center
- DCAlerter overview, on page 13 —Alerts technicians about Data Center events

> **NOTE:**
> When you administer the Data Center services, do not pause the services. Use only Stop and Start when managing Data Center services. If you pause a service, you cannot view its status in the Data Center Management Console (DCMC).

BackupServer overview

The BackupServer service processes requests from the Agent for data backup and retrieval. BackupServer gathers backed-up data into an archive. The Data Center saves the archive as a file with a `.arc` extension and stores it in the Customer folder. Each file contains file backup data transmitted from a client during a single backup session.

CAUTION:
Do not delete `.arc` files from the Customers directory. Doing so deletes end users' data and renders it unrecoverable.

If the data from a single backup session is large, BackupServer saves information to more than one archive. Each represents a portion of the backup session. Using multiple archives helps to optimize data recovery performance.

When BackupServer receives a request from the Agent to retrieve a file, BackupServer must find the first backup of the file (the base) and all the changes (the deltas) necessary to recreate the specific version of the file requested.

For example, you request to retrieve the third backed-up version of a file:

- BackupServer must retrieve the base (version 1)
- The delta that represents the differences between version 1 and version 2
- The delta that represents the differences between version 2 and version 3

Because you backed up the base and the deltas in different backup sessions, they are in different archives. Typically, BackupServer uses multiple archives to retrieve a file.

In addition to processing requests for data backup and retrieval, BackupServer manages the list of authorized user accounts and registers new accounts. There is one user account for each client.

BackupServer starts automatically with Windows Server. The Data Center Management Console (DCMC) includes a **BackupServer** node. This node lets you view the following information:

- Service status
- Sessions
- Properties

To view and edit status information

1. Select **Start** > **All Programs** > **Data Center** > **Data Center Management Console**.
2. In the left pane, expand the Data Center server name that runs the service.
3. Right-click **BackupServer,** and then select **Properties**.

NOTE:
If you want to enable the IPv6 connectivity between the PC Agent and Data Center, the server connections in the BackupServer properties must be configured with DNS names.

CAUTION:
Make sure to contact Connected Backup support team before you change the default values for the following Backup server session limits:

- Maximum Active Sessions
- Maximum Active Backup Sessions

- Maximum Active First Backup Sessions
- Maximum Active Download Sessions

IndexServer overview

As Agents back up archives to the Data Center server, information about each file in the archive must be stored in the Directory database. After an archive is fully written to the Data Center, the IndexServer writes the information to the Directory database, allowing for faster lookups of file data during retrieves. When the indexing process is finished, the archive is queued for replication to the mirrored server (if you use a mirrored configuration).

If the Data Center is mirrored or part of a non-mirrored cluster, the IndexServer writes information to the database for all archives that have been replicated from the mirrored server.

IndexServer starts automatically with Windows Server. The Data Center Management Console (DCMC) includes an **IndexServer** node that lets you access the following information:

- Service status
- Properties

To view and edit status information

1. Select **Start** > **All Programs** > **Data Center** > **Data Center Management Console**.
2. In the left pane, expand the Data Center server name that runs the service.
3. Right-click **IndexServer,** and then select **Properties**.

ReplicationServer overview

The ReplicationServer service replicates the following content between the servers in a mirrored pair:

- Archives
- Database table rows
- Agent configurations

IMPORTANT:
The ReplicationServer service runs only on Mirrored Data Center configurations, either a mirrored pair or as part of a mirrored cluster.

After the Agent backs up an archive to the Data Center server and indexes the database, the archive goes into a queue to be replicated to the mirror. The ReplicationServer services replicates the archive to the mirror as a whole rather than in portions as the Agent backs it up.

Most, but not all, of the database tables in the schema replicate between the servers in a mirrored pair. When a row in a replicated database table is inserted, deleted, or modified, the database is placed in a queue for replication between the mirrored servers. SQL replication handles the replication process.

ReplicationServer starts automatically with Windows Server. Archives, database entries, and Agent configuration files are replicated continuously when ReplicationServer runs. If you have to pause or stop replication, you can pause or stop the service in the Data Center Management Console (DCMC).

The DCMC includes a **ReplicationServer** node that lets you view the following information:

- Service status
- Properties

To view and edit status information

1. Select **Start** > **All Programs** > **Data Center** > **Data Center Management Console**.
2. In the left pane, expand the Data Center server name that runs the service.
3. Right-click **ReplicationServer,** and then select **Properties**.

PoolServer overview

PoolServer maintains the shared file pool that implements SendOnce technology. SendOnce technology recognizes duplicate files from multiple Agents and stores an identical file for each duplicated file on the Data Center server.

1. BackupServer stores the original contributor's file
2. SendOnce recognizes that a duplicate file is being sent for backup by another Agent
3. PoolServer stores an identical file as the original contributor's file

Using PoolServer reduces the storage space needed on the Data Center, as additional duplicate files backed up to the Data Center reference the PoolServer-saved copy, instead of a copy of each duplicate file being stored. Backing up references to files that were already saved by the PoolServer also reduces the amount of time Agents are connected to the Data Center during backups.

PoolServer also implements the Copy On Reference scheduled process. Copy On Reference cleans the shared file pool of uncommon files. When two Agents back up an identical file (for example, an application file, operating system file, or common organization file), the SendOnce technology places the file in a queue for Copy On Reference. Copy On Reference makes a copy of the file and places it in a special account known as the Pool Account. The Pool Account always uses 999999999 as its account number. Any Agent that backs up the same file references the copy instead of sending another full copy of the file to the server. Also, if any Agent needs to retrieve the file after backing it up, the Agent retrieves the copy from the Pool Account.

Every 14 days by default, the PoolServer removes references to files that no other account has backed up within 14 days. These files are removed to keep the Directory database from growing too large and to keep the performance of the SendOnce operation efficient. You can use DCMC to change the number of days that uncommon files remain in the pool.

> **NOTE:**
> While you can change this value, you should use the default value of 14 days for the SendOnce pool, unless you are directed to change the value by Support.

PoolServer starts automatically with Windows Server.

The Data Center Management Console (DCMC) includes a **PoolServer** node that lets you access the following information:

- Service status
- Properties

To view and edit status information

1. Select **Start** > **All Programs** > **Data Center** > **Data Center Management Console**.
2. In the left pane, expand the Data Center server name that runs the service.
3. Right-click **PoolServer,** and then select **Properties**.

Compactor overview

The Compactor service cleans old data off of the Data Center. Compactor verifies synchronization between mirrored servers, applies expiration rules to backed up data, and deletes expired data. The goal of Compactor is to speed up the Retrieve process and reduce the amount of data stored long term on the Data Center.

For more information about the Compactor process, see Compactor, on page 14.

DCAlerter overview

DCAlerter monitors the Data Center event logs for the event IDs that you specify. When the Data Center logs an event ID that you have specified for notification, DCAlerter sends an e-mail message to the designated individuals.

You can specify your SMTP mail host and an administrator e-mail address for DCAlerter during Data Center Setup. If you do not enter the SMTP mail host information during Data Center Setup, the DCAlerter feature is not active. Data Center Setup installs a default set of events for notifications. You can modify the installed settings using DCMC.

To view status information in the details pane, select **DCAlerter** from the console tree for the server the service runs on.

To view and edit DCAlerter settings

1. Select **Start** > **All Programs** > **Data Center** > **Data Center Management Console**.
2. In the left pane, expand the Data Center server name that runs the service.
3. Right-click **DCAlerter,** and then select **Properties**.

> **NOTE:**
> The DCAlerter service can generate a large amount of email for those individuals configured as recipients. Be sure to carefully configure the event groups to only send those event messages that are necessary to monitor the Data Center.

Chapter 2: Compactor

This chapter describes the Compactor service.

Compactor Service and Data Center configurations

Compactor is a Data Center service that runs continuously based on Data Center activity. Compactor has the following capabilities:

- Reduce the overall storage requirement for the Data Center.
- Improve the performance of Agent file retrieval.
- Free disk space by removing expired data.
- Reduce the size of the databases.
- Improve data integrity.

Compactor configurations

Compactor runs on all Data Center configurations, but runs differently on mirrored configurations than it does on stand-alone or non-mirrored cluster configurations.

Compactor in mirrored Data Centers

In mirrored Data Centers, the Compactor service runs on both servers. However, only one of the servers in the pair controls the workload of the compaction process. This server is called the primary server. If you run a clustered Data Center, there is one primary server for every mirrored pair in the cluster. For example, a clustered Data Center with three mirrored pairs has three primary servers. You can check the status of the primary server(s) in the Compactor view of DCMC.

Administration of Compactor

You can use DCMC to administer Compactor in the following ways:

- Start, stop, or pause the Compactor service.
- Specify startup parameters.

- Monitor Compactor progress for the current session.
- Monitor disk space.
- Monitor Compactor progress for the past 90 days.

For more information on these topics, refer to DCMC Help.

Compactor tasks

The Compactor service removes redundant data from the Data Center. It also removes data that is older than set expiration parameters. To remove data, Compactor performs the following tasks:

1. Selects accounts
2. Synchronizes archives (mirrored Data Center configurations only, either a mirrored pair or as part of a mirrored cluster)
3. Marks files as expired according to rules set during Data Center installation
4. Repackages archives
5. Deletes expired archives and database entries
6. Informs the Agent of changes

Select accounts

For each session, Compactor determines which accounts to work on. Compactor first locks the account from all other processes.

Compactor runs continuously, but you can start the Compactor service manually if you specify an account. You can also run Compactor service on canceled accounts. For more information about how to use switches to start Compactor, refer to the DCMC Help.

Synchronize archives

Compactor then verifies synchronicity between the archives in the account and the database information on the local server, and then between the two servers of a mirrored pair.

If inconsistencies exist (corrupt or missing files), Compactor tries to correct them. If inconsistencies still exist, Compactor marks the files that it cannot retrieve for deletion, and then requests that the Data Center notify the Agent to resend those files.

Mark files as expired

- To expire files, Compactor uses rules that technicians create during Data Center installation. These rules specify the following parameters:
- How long to keep data for cancelled accounts

- How long to keep files deleted from the Agent computer
- How long to keep files excluded from the Agent backup
- How many versions of a file to keep and how long to keep them

For more information about expiration rules, see File Expiration overview, on the next page.

Compactor runs through every version of every file for the selected account. If an expiration rule applies to a file, Compactor marks the file as expired. Expiration settings are immediately applied to your Data Center, but these settings require Compactor to process the account to be fulfilled. Compaction cycles fluctuate with each added variable. These variables might be one or all of the following considerations:

- Number of accounts
- Size of the back up set
- Number of file revisions per account
- Expiration settings

Compactor does not copy archives for accounts that are canceled and ready for compaction. Canceled accounts are processed first.

Repackage archives

After Compactor marks files as expired, it determines which files to delete and which archives to repackage for efficiency.

If a failure to retrieve the archive from storage or disk occurs, Compactor attempts to retrieve the archive from the server's mirror. When Compactor works with files in an archive, it either copies or rebases the file. Rebasing takes the original base of a file (the first backed-up version) and combines it with its deltas (subsequent changes to backed-up files) to create a new base. Compaction deletes the expired base and deltas. When a file has not expired, but it is in an archive with other files that Compactor must rebase or delete, Compactor copies the files to new archives. After the repackaging process, Compactor performs additional data integrity checks on the new archives.

Delete archives and database entries

After Compactor repackages all archives, it deletes the old archives from disk. During this process, Compactor also deletes the appropriate database rows for these files and archives. When this step is complete, the account is unlocked, allowing access to all processes.

Notify the Agent about changes

After Compactor repackages or deletes archives, BackupServer notifies the Agent of the change. The next time the Agent connects to the Data Center server, the Data Center updates the file list with the new information from the compaction process. After Compactor deletes files, the Agent cannot restore the files. Therefore, the Agent must update the list of files available for retrieval. The Agent also resends any files or revisions that are missing from the Data Center that remain on the local computer.

After Compactor migrates all new archives, the process begins again. Compactor checks for available disk cache and selects the next account for compaction.

File Expiration overview

To reuse disk and archive storage space, the Data Center use the expiration process to delete old data.

When technicians set up the Data Center, they specify parameters that define when data is “old” and ready for deletion. The file expiration rules have default settings created by Data Center Setup. You can accept the defaults if you do not know the parameters that you need.

On a disk-only configuration, the file expiration rules keep your Data Center from running out of disk storage. Monitor a disk-only configuration closely in the weeks after startup, and decrease the file expiration rules if disk space fills too quickly. On disk-only configuration, if space is tightly limited, you need more aggressive file expiration rules. Use DCMC to change file the expiration rules.

Expiration rules and default settings

Expiration rules have the following default settings:

- **Canceled**. The minimum number of days after an account is canceled until its backed-up data is deleted. The default number of days until deletion is 60.
- **Deleted**. The minimum number of days that the Data Center retains a file after it has been deleted from the Agent. If a file is backed up and later deleted, you can usually retrieve the file with the Agent. However, if the Data Center expires and compacts the file, you cannot retrieve it. The default value is 90 days for disk-only configuration.
- **Excluded**. The number of days that the Data Center retains a file after the end-user excludes it from the backup list on the Agent. If you back up a file and then later exclude it from the Agent backup list, the next time Compactor runs on the account the file is expired and deleted. For disk-only configuration, the default value is 10 days.
- **RecentVersions and OldVersions**. Used together to specify the number of versions of a retained file. For example, if RecentVersions = 9 (versions) and OldVersions = 30 (days), then old versions of a file are deleted if they are more than 30 days old or there are 9 more recent versions. The most recent backed-up version of a file is not expired using these parameters. The default value for RecentVersions is 10 versions for disk-only configurations. The default value for OldVersions is 45 days for disk-only configurations.

CAUTION:
Micro Focus Connected Backup is a backup and restore application, and is not designed as an archiving application. Do not modify the values of these settings to more than double the default values for the following reasons:

- Storage needs may be greatly increased.
- Data Center performance may be decreased.
- Permanent data loss is possible, due to reduced data integrity checks.

Rule exceptions

Data can remain on the Data Center longer than the expiration rules imply. For example, on January 1, a user deletes a file from his or her computer. The file has been backed up to the Data Center. The user then performs a subsequent backup.

Compactor typically processes disk-only accounts every 30 days. To use the January 1 example from the previous paragraph, the next time Compactor can process the user's account is on February 2nd. If you delete a file, the expiration rule for deleted files is typically 45 days. As Compactor processes this account, Compactor marks the deleted file for deletion from the Data Center. However, the file can remain on the Data Center for more than 90 days after the user deletes it from the his or her computer. This occurs because the expiration rule values and the number of days between Compactor runs for an account are minimum values. Data can remain on the Data Center longer than these values indicate.

Chapter 3: Integrate the Data Center with enterprise directory

This chapter describes how to integrate your Data Center with an enterprise directory.

Enterprise directory overview

In Connected Backup, an enterprise directory is the application you use to manage your directory services requirements. Enterprise directory uses Lightweight Directory Access Protocol Version 3 (LDAPv3), a software protocol that enables you to store personal information for every individual in your organization. This directory of information enables other applications, including Connected Backup, to read information from it for authentication and other purposes.

You can integrate some or all of your Agents with your enterprise directory by mapping a community in Support Center. If you map a community to enterprise directory, all of its subcommunities use enterprise directory as well. It is important to map a community to enterprise directory before you allow Agents to register to the community.

> **NOTE:**
> You administer your enterprise directory and the information it contains separately from Connected Backup. Connected Backup uses information from the enterprise directory, and cannot be used as an enterprise directory.
>
> Administer your enterprise directory based on the application vendor's instructions.

For more information on enterprise directory requirements to work with your Data Center, refer to *Connected Backup Interoperability Matrix* guide.

Enterprise directory uses

You can use Enterprise directory to validate Support Center technicians and optionally, to maintain the personal data of end users. When you integrate Connected Backup with your enterprise directory, you gain the following benefits:

- Support Center technicians can use their enterprise directory passwords for authentication.
- Support Center technicians cannot gain access to Support Center after reassignment or termination.

- Agent accounts can authenticate with the current enterprise directory user account and password. This means that Agent users can use their enterprise directory credentials to register Agents and retrieve data.
- You can perform Account Lifecycle Management, because your accounts are based on your existing enterprise directory accounts.
- The contact information for accounts can be automatically populated and updated. This is useful for account management, reporting, and troubleshooting.

Existing enterprise directory servers

If you have an existing enterprise directory server, use Support Center to map the directory to the Data Center database. For more information about how to map your Data Center to the enterprise directory Data Center, refer to Support Center Help.

Validate Support Center technicians

Use Support Center to map the Data Center or communities to an enterprise directory. When you associate a community with an enterprise directory, Support Center technicians in that community must use their LDAP user ID and password to log on to Support Center.

Enterprise directory management

For enterprise directory-enabled communities, the Data Center synchronizes user information between the enterprise directory server and the Data Center databases. The LDAPSyncher application uses Windows Scheduled Tasks to perform this synchronization process and run daily.

If the enterprise directory server is unavailable, you will see the following behaviors:

- New Agents cannot register.
- Existing Agents cannot retrieve files.
- Technicians cannot log in to Support Center.

If your organization uses Lotus Domino, contact Connected Support for more information and assistance. Support for Lotus Domino requires modifications to the databases in the Data Center integration process.

> **NOTE:**
> Connected Backup supports only LDAPv3. Do not attempt to use enterprise directory applications based on different LDAP variants.

Enterprise directory integration process

> **CAUTION:**
> Read this entire procedure before you integrate and be sure you understand all the requirements and steps.
>
> Complete each set of steps in one phase before you begin the next phase.

Integration includes the following phases:

1. Prepare your IT infrastructure for integration, and gather the information that you need to complete the procedures in this document.

   > **NOTE:**
   > Do not integrate the enterprise directory at the root level of Support Center.

2. Configure your firewall to let the Data Center and Support Center gain access to your enterprise directory.
3. Enable Support Center access.
4. Define the Enterprise Directory Setup Properties in Support Center. This requires you to map Support Center data fields to corresponding enterprise directory data fields.

The following sections explain these phases in detail.

Prepare for enterprise directory integration

The preparation phase requires you to collect information to configure access to your enterprise directory and verify that your infrastructure meets requirements to support integration.

> **NOTE:**
> An LDAP browser helps you identify and locate your enterprise directory accounts and servers. As you prepare process, you can use the LDAP browser to gather information and identify the server(s) that you want to permit Support Center to access. Check if your enterprise directory software includes a browser. If it does not, you can obtain a free LDAP browser from the Internet.

To prepare for integration with enterprise directory

1. Install the Data Center, or upgrade your Data Center to the current version.

   For more information about how to install your Data Center for the first time, refer to *Installing the Data Center* guide.

   For more information about how to upgrade your Data Center, refer to *Upgrading the Data Center* guide.

2. Confirm that your enterprise directory supports LDAPv3, which includes Microsoft Windows Active Directory server.

3. Verify that enterprise directory accounts exist for users to whom you deploy Agents. The users include people use Support Center to manage Connected Backup user accounts, and commonly referred to as Support Center technicians.

   If you plan to use enterprise directory to authenticate Agent registration, this step is critical. Users that do not have enterprise directory accounts cannot authenticate. Therefore, the Agent fails to register.

4. Locate the enterprise directory source server that has access to user accounts to which you plan to deploy Connected Backup Agents. Note the URL for the source server, as you will need it later to grant Support Center access to your enterprise directory.

   For best results, place this server as high as possible in the enterprise directory architecture.

5. Install Secure Socket Layer (SSL) certificates on each enterprise directory server that the Data Center servers and the Support Center server will read.

   SSL prevents unauthorized interception of user credentials.

   For LDAP Enterprise Directory secured via SSL, ensure that the certificates are installed on the Support Center server and any of the following servers that it needs to contact for LDAP authentication and synchronization, including:

   - Enterprise Directory server(s).
   - Data Center server(s).
   - Account Management Website server(s).

6. Create a new enterprise directory account that has read-only permission on the enterprise directory server that you identified in step 4. Remember the user account and password, as you need to enter it in Support Center.

   This account requires read access to all enterprise directory accounts and to your enterprise directory schema. Support Center uses this user account to read information from your enterprise directory during the initial integration, and for every communication from Support Center.

> **CAUTION:**
> Use a password with a minimum of eight characters, and a combination of letters and numbers. Keep in mind that if you change this enterprise directory account password, you must also change it in Support Center.

Configure your firewall

If you protected your Data Center with a firewall, you must configure the firewall to permit the Data Center, Support Center and Registry Master servers access to your enterprise directory servers.

For more information about how to configure your firewall, refer to *Installing the Data Center* guide.

Enable Support Center access

To enable Support Center access, you must provide Support Center the information required to make a connection to your enterprise directory, and mapping the Support Center data fields to your

corresponding enterprise directory data fields.

Data field labels vary from one enterprise directory to another. To determine which fields to map to the Support Center data fields, contact the person who administers your enterprise directory fields.

Define Enterprise Directory Setup Properties

To gain access to your enterprise directory server or servers, Support Center uses the enterprise directory account you created. For more information, see Prepare for enterprise directory integration, on page 21. Support Center connects through your corporate firewall to the enterprise directory and reads account information.

You can enable the Data Center to connect to your enterprise directory to authenticate users who attempt to register Agent accounts and retrieve backed up data. The Data Center also authenticates the technicians who attempt to log on to Support Center to administer your Connected Backup accounts and subcommunities.

To enter the setup properties

1. Log on to Support Center.
2. Locate the subcommunity that you want to integrate with your enterprise directory.

   Your root and subcommunities appear in the navigation tree on the left. You might need to expand your root community node to locate the subcommunity that you want to integrate.
3. To display the **Enterprise Directory Setup** page, on the **Community Status** page, click **Enterprise Directory**.
4. Type the URL of the source server in the **Enterprise Directory Server URL** field.

   The following example shows a valid URL for an Active Directory server.

   LDAP://my.edserver.com/dc=edserver,dc=com

> **NOTE:**
> Connected Backup does not support security groups on an Active Directory server.
>
> The Data Center can connect to a security group, but it cannot authenticate or validate users.

5. To ensure that inbound Support Center connections are secure, select **Use SSL**.
6. In the **Connection Login DN** box, enter the read-only enterprise directory user account ID that you created for Support Center to enable it to connect to your enterprise directory.

   The following example shows an Active Directory account.

   ```
   supportcenter@edserver.com
   ```
7. In the **Connection Password** box, enter the account password.

   The Data Center encrypts and stores the password. Only technicians that have the **Change the Enterprise Directory user** permission have access to the password. For more information, refer to Support Center Help.

8. Select **Verify existence of users through Enterprise Directory** to have Support Center use your enterprise directory to authenticate all users who attempt to register a Connected Backup account.

   > **NOTE:**
   > Connected Backup verifies against only accounts deleted from the enterprise directory. It does not verify against disabled accounts. Connected Backup treats disabled accounts the same as active accounts. If you create an account for a disabled enterprise directory account, you can use Support Center to change the account status to **On Hold** or **Cancelled**.

9. To indicate how you want Data Center to respond to users who fail to authenticate, select one of the following options:
   - **Change the Account Status to On Hold** — if you want to place these accounts on hold temporarily until you can verify independently whether they should be allowed to register.
   - **Change the Account Status to Cancel** — if you want to deny the account registration permanently.
10. Continue to the next section, Map data fields, below, to complete the integration.

> **NOTE:**
> After creating a new sub-community under the Enterprise Directory enabled community, ensure that you manually run the LDAPSyncher utility just once. To do this:
>
> On both the primary and secondary current Registration Master servers, click **Start** > **Control Panel** > **Administrative Tools** > **Tasks Scheduler** > **Task Scheduler Library**> **LDAPSyncher task**>, and then click **Run**.

Map data fields

Support Center also can read user information, such as First Name, Last Name, department or other information from your enterprise directory. To do so, provide Support Center with the name of the corresponding data field in your enterprise directory. For example, you must map the Support Center **Last Name** field to the **SN** (surname) field. By mapping the data fields, you can control which information the Support Center obtains and reads.

Default values for data fields

The following table lists default values for data fields in Mozilla Directory, Novell eDirectory and Microsoft Active Directory. These suggested values might not represent the values in your enterprise directory implementation. For assistance with mapping data fields, consult your enterprise directory administrator.

In the table, an asterisk (*) next to a field indicates a required field, and you must enter the name of your corresponding enterprise directory data field.

Map this Support Center field:	To this Mozilla Directory field:	To this Novell eDirectory field:	To this Microsoft Active Directory field:
User Class *	Inetorgperson	InetOrgPerson	User
LoginID *	Cn	CN	userPrincipalName
UniqueID *	Uid	Uid	objectGUID
First Name	GivenName	Given Name	givenName
Middle Initial	Initials	Initials	initials
Last Name	Sn	Sn	Sn
Address1	Postaladdress	Postal Address	StreetAddress
Address2	Street	Street	Street
City	City	L	City
State	st	ST	st
Zip	Postalcode	PostalCode	Postalcode
Country	Country	Country	c
Telephone	TelephoneNumber	TelephoneNumber	TelephoneNumber
Email *	Mail	Mail	mail
Company	Company	Company	company
Department	departmentNumber	departmentNumber	Department

Map the data fields

To map the data fields

1. In the **Enterprise Directory Setup** page, enter the name of the corresponding enterprise directory data field in each field.

   > **NOTE:**
   > If you do not know which field names to map to the Support Center fields, consult your enterprise directory administrator.

2. Check the spelling, capitalization, and spacing of each field name that you enter.
3. After you map the fields, click **Save**.

Verify successful enterprise directory integration

After you complete the integration procedures, verify that the integration completed successfully and works as expected.

To verify that the enterprise directory integration was successful

1. Create a new technician account in Support Center and verify that you can use that account to log on to Support Center.

   For instructions on how to create technician accounts, refer to *Administering Agents* guide for your operating system.

2. Create a new test Agent configuration in the Support Center community that you integrated with your enterprise directory.

   For more information about how to create an Agent configuration, refer to *Administering Agents* guide for your operating system.

3. Deploy and install that Agent to a user account in the enterprise directory. Verify that you can use the user account in the enterprise directory as credentials to install and register the new Agent.

   For instructions on how to deploy an Agent, refer to *Installing Agents* guide for your operating system.

4. After you install a test Agent, confirm that the account information appears in the Agent. If the account information fields in the Agent are empty, confirm that the fields are populated in the enterprise directory user account.

5. Change a value for a user in a field mapped to the test Agent, and then run LDAPSyncher from the Scheduled Tasks Windows Control Panel. Confirm that the correct values are displayed for the account in Support Center.

Chapter 4: Integrate the Data Center with single sign-on

This chapter describes how to integrate your Data Center with a single sign-on (SSO) service provider.

Single sign-on Service provider overview

Single-sign on (SSO) support lets technicians and users access password-protected Connected Backup functions with their network account credentials, which are defined in a third-party identity provider (IdP). You can configure an existing community to support SSO-enabled accounts under the following conditions:

- You use Connected Backup in a subscription environment.
- You host a Connected Backup environment that is configured to use a single sign-on (SSO) service provider.

For more information on SSO Service Provider (SP) and Identity Provider (IdP) requirements to support your Data Center, refer to *Connected Backup Requirements Matrix* guide.

SSO integration process

> **CAUTION:**
> Read this entire procedure before you integrate and be sure you understand all the requirements and steps.
>
> Complete each set of steps in one phase before you begin the next phase.

Integration includes the following phases:

1. Prepare your IT infrastructure for integration, and gather the information that you need to complete the procedures in this document.
2. Install the SSO service provider software according to its system requirements on the Service Provider (SP) server and the Identity Provider (IdP) server.
3. Configure the contract between the SP and IdP servers. For more information, see Configure the contract, on page 29.

4. Configure the SSO Directory Service on the SP. For more information, see Configure SSO Directory Service, on the next page.
5. Configured the OAuth clients required by Connected applications. For more information, see Configure OAuth clients, on the next page.
6. In Connected Backup Data Center Management Console (DCMC), configure the connections to the SSO service provider and the shared secret. For more information, see Configure DCMC to support SSO, on page 30.
7. In Support Center, enable communities for SSO and create SSO technicians. For more information, see Configure a community for single sign-on support , on page 31.

The following sections explain these phases in detail.

Prepare for SSO integration

The preparation phase requires you to collect information to configure access to your SSO SP and IdP and verify that your infrastructure meets requirements to support integration.

To prepare for integration with SSO

- Install the Data Center, or upgrade your Data Center to the current version.

  For more information about how to install your Data Center for the first time, refer to *Installing the Data Center* guide.

  For more information about how to upgrade your Data Center, refer to *Upgrading the Data Center* guide.

Install the SSO service provider software

Install the SSO Service Provider and Identity Provider software according to its requirements. For more information, refer to your SSO Service Provider (SP) and Identity Provider (IdP) product documentation.

Configure the SP and IdP Connections

Configure the SP and IdP connections according to your security and protocol needs.

If for example, your security policy requires you to use a specific protocol for the SAML bindings, use the SP and IdP Connection interface to set the appropriate SAML bindings for sending and receiving SAML messages.

For example:

- Artifact
- POST
- Redirect
- SOAP

For more information on the SP and IdP connections, refer to your SSO and IdP product documentation.

For more information on SSO Service Provider (SP) and Identity Provider (IdP) requirements to support your Data Center, refer to *Connected Backup Requirements Matrix* guide.

Configure the contract

Configure the contract between the Service Provider (SP) and the Identity Provider (IdP).

The contract needs to meet the following characteristics:

- **Protocol**: SAML 2.0
- **Attribute Contract:** SAML_SUBJECT.

  SAML_SUBJECT must contain the unique identifier, such as a user ID or e-mail address that uniquely identifies a user within the customer domain

For more information, refer to your SSO Service Provider (SP) and Identity Provider (IdP) product documentation.

Configure SSO Directory Service

To support SSO in your Data Center, you must configure the application authentication by activating the SSO Directory Service on the SP.

To activate the SSO Directory Service

1. On the SP server, activate the SSO Directory Service.
2. Enter the name of the specified Id and its Shared Secret.
3. Re-enter the Shared Secret.
4. Take note of the Shared Secret, as you will use it in later steps.

Configure OAuth clients

On the SSO SP Server, configure the listed OAuth clients for use by Connected applications.

- **CB_Web.** Provides implicit grants. No token refresh.
- **CB_App.** Provides authorization code grants. No token refresh.
- **CB_Validation.** Configure for 'Access Token Validation'. This client is used by the applications to validate OAuth tokens.

  A client shared secret is required for this configuration.

  > **NOTE:**
  > The OAuth clients above are required by the Data Center.

> The **CB_Validation** client shared secret is used to configure SSO in the Data Center and during installation of the Management API.

Add redirection URIs for CB_Web OAuth client

To support redirection URIs for Support Center and the Account Management Website, you must add the redirection URIs in the **CB_Web** OAuth client settings.

1. On the SSO SP Server, select the **CB_Web** client from the list of OAuth clients.
2. Add the redirect URI for your Account Management Website.

   For example: `https://<hostname>/ssws/faces/fed_auth_validation.jsp`

   where

   <hostname> is the name of the server that hosts Account Management Website.
3. Add the redirect URIs for your Support Center.
   - `https://<hostname>/supportcenter/fauth.htm`
   - `https://<hostname>/supportcenter/login.asp`

   where

   <hostname> is the name of the server that hosts Support Center.

For more information on configuring OAuth client settings, refer to your SSO SP product documentation.

Add redirection URIs for CB_App OAuth client

To support redirection URIs for Connected application, you must add the redirection URIs in the **CB_App** OAuth client settings.

1. On the SSO SP Server, select the **CB_App** client from the list of OAuth clients.
2. Add the redirect URI `http://localhost:16389`.

For more information on configuring OAuth client settings, refer to your SSO SP product documentation.

Configure DCMC to support SSO

To support SSO in your Data Center, you must configure access in the Data Center Management Console (DCMC).

1. Start the DCMC.
   a. Click **Start > All Programs > Data Center**.
   b. Click **Data Center Management Console**.

The DCMC opens

2. In the SSO Authentication Configuration section, do the following:
   a. In the **SSO Service Provider Base URL** box, type the URL to the SSO service provider that supports your Connected Backup environment.

      For example: https://sso.myDomain.com:9031

   b. In the **SSO Service Provider Secret** box, type the same client secret that you used when you configured the CB_Validation client on your SSO service provider to support Connected Backup.

      The Data Center sends this token with its requests to the SSO service provider so that it can authenticate the requests.

> **NOTE:**
> The client secret to configure SSO in this step must match the **CB_Validation** OAuth client configured in the previous steps.

For more information, refer to the DCMC Help.

Configure a community for single sign-on support

Support Center lets you configure communities for single sign-on support. In an SSO-enabled community, the technicians and users you create map to network accounts defined in the SSO IdP.

To support SSO communities in your Data Center, you must configure SSO communities in Support Center. Each community requires two SSO provider IDs—one for technicians and the other for users. You can use the same ID for both. If the mappings do not exist, Support Center will not save your changes.

The Data Center does not store passwords for SSO-enabled technicians or users. Connected Backup applications delegate the authentication of SSO-enabled accounts to the IdP assigned to the community in which the account resides. The application calls on the IdP to display its browser-based single sign-on page to capture and validate the technician or user account credentials.

To support SSO-enabled accounts with command-line tools that require a password, such as the Retrieve command, you must use non-SSO technicians. These tools do not support SSO-enabled technicians or users due to the browser-based interaction required by the IdP to capture and validate credentials. Conversely, to retrieve files or recover an account through the Agent on behalf of a user with SSO credentials requires an SSO-enabled technician with access to the user account.

If you plan to use command-line tools to support SSO-enabled users, the following describes one way to structure your community hierarchy to ensure that you have technicians that can support these users though command-line utilities or the Agent:

1. Create a non-SSO enabled community that serves as the parent of your community hierarchy. If you host your own Connected Backup environment, you can use the Data Center root community as the parent.

2. Create non-SSO technicians in the parent community. With proper permissions, these technicians can use command-line tools for SSO-enabled users in subcommunities.
3. Create one or more SSO-enabled subcommunities.
4. In each subcommunity, create SSO-enabled technicians and users. SSO-enabled technicians are required to retrieve files or recover an account through the Agent on behalf of SSO-enabled users.

For more information on configuring a community for SSO support, refer to Support Center help.

Verify successful SSO integration

After you complete the integration procedures, verify that the integration completed successfully and works as expected.

To verify that the SSO integration was successful

1. Create a new SSO technician account in Support Center and verify that you can use that account to log on to Support Center using the SSO login page.

   For instructions on how to create technician accounts, refer to *Administering Agents* guide for your operating system.
2. Create a new test Agent configuration in the Support Center community that you integrated with SSO.

   For more information about how to create an Agent configuration, refer to *Administering Agents* guide for your operating system.
3. Verify that the SSO agent user can perform a successful retrieve.
4. Verify that the SSO user is able to register successfully on the Account Management Website by authenticating with the IdP.

Change the SSO shared secret

If you need to change the SSO shared secret at any time after the initial configuration, you must change it in the following locations.

1. On the SSO SP, configure the SSO Directory Service to use the new shared secret.
2. On the SSO SP, configure the OAuth **CB_Validation** to use the new shared secret.
3. In the Data Center Management Console (DCMC), use the new shared secret in the **SSO Service Provider Secret** box.
4. Reset IIS on the Support Center server.
5. Log in to Support Center to verify the changes.

Chapter 5: Maintain the Data Center configuration

This chapter describes how to update or troubleshoot your Data Center configuration.

Convert a stand-alone Data Center to a mirror

This section describes how add a server to a stand-alone Data Center to create the mirrored Data Center configuration.

Use the following terms and concepts when adding a mirrored server to your stand-alone Data Center.

Server A	Represents the original stand-alone Data Center server
Server B	Represents the server that you add to your new mirrored Data Center configuration

CAUTION:
This procedures in this section include steps that use SQL Management Studio to manually change the SQL databases. Manual changes to SQL databases can cause damage if you perform them incorrectly. Do not change the SQL database except as described in this procedure.

To change a stand-alone Data Center into a mirrored Data Center, use the following procedure:

Before you begin

- Read the entire procedure.
- Only use this procedure with stand-alone Data Center configurations.

  Adding servers to your Data Center configuration requires new licenses for all Data Centers in the configuration. You can use the License Request Form available through the MySupport portal to request for a license.
- The Data Center conversion requires that the Data Center is unavailable to users for backups and retrieves during the conversion process. Schedule an appropriate Data Center conversion time and educate your users regarding backup and retrieve availability.
- Verify that all required software is installed and configured on Server B. Ensure that Server B meets the hardware and software requirements in *Connected Backup Requirements Matrix*.
- Determine the Data Center service account and password information for the Data Center. This information is used during the Data Center install and reinstall processes and must be the same for all Data Center servers.
- Add Server B to the domain that contains Server A. All Data Centers must reside in the same domain.
- Download the Data Center installation file from the MySupport portal . You must install the exact version of the Data Center software on Server B as the version that is installed on Server A.
- Ensure you are logged in to the new servers using an account with local administrator permissions.
- On Server A, use Notepad to edit `\DataCenter\DRProcs\AddingMirrorInsertInfo.sql`. Modify the file to include the following information from Server B:
  - server name
  - DNS name
  - replication IP address
  - backup IP address
- On Server A, run the following SQL scripts in the `\DataCenter\DRProcs` folder:
  - `AddingMirrorInsertInfo.sql`
  - `delete_tables.sql`

Reinstall the Data Center software on Server A

To reinstall the Connected Backup Data Center software on Server A

1. Ensure you have a secure copy of the Connected registry keys for Server A. For more information on how to back up needed files and information for a Data Center, including the Connected registry key, refer to the Required Disaster Recovery items section of *Connected Backup Disaster Recovery* guide.

2. On Server A, using the Data Center Management Console (DCMC), stop the Data Center services on Server A.
3. If Support Center and the Account Management Website are installed on a server other than Server A, stop these services. Open the **Services Control Panel** on the Web services server and stop the IIS Admin and Apache Tomcat (only visible if the Account Management Website is installed) services.
4. On Server A, reinstall the Connected Backup Data Center software as the **Primary server in a new cluster**.
5. After installation completes, ensure that all Data Center services are started except Compactor. If Compactor is started, stop the service using the DCMC.
6. On Server A, open the SQL Server Management Studio.
7. To determine the Primary and Secondary server ID values, run the following script:

```
DECLARE @ServerID tinyint
SELECT @ServerID = max(ServerID) FROM Registry.dbo.Server
UPDATE Registry.dbo.Server
SET SecondaryServerID = @ServerID
WHERE ServerType = 1
AND IsRegistrationMaster = 1 AND IsPrimary = 1
SELECT ServerID ‘Primary Server ID’, SecondaryServerID ‘Secondary Server ID’
FROM Registry.dbo.Server
WHERE ServerType = 1
AND IsRegistrationMaster = 1 AND IsPrimary = 1
```

8. Record the Primary server and Secondary server ID values. You need these values later in the procedure.
9. Close the SQL Server Management Studio.
10. On Server A, using the DCMC, check the event log for errors.

Install the Data Center software on Server B

To install the Connected Backup Data Center software on Server B

1. Copy the Connected\ Keys registry key `.REG` file from Server A to Server B, and then on Server B, double-click the `.reg` file. The `.reg` file recreates the Connected registry key on Server B.

   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Connected\Keys
2. If the MEK and PMEK keys and values are not visible to you, right-click**...\Connected\Keys** and then select **Permissions**. Change the permissions for the logged-on user to **Read**. To close the window, click **OK.**
3. Copy the following scripts from server A (available in DataCenter\scripts) to server B:
   - Replication_Registry_SP.sql
   - Replication_Directory_SP.sql

You must run the above scripts on server B in the following scenarios:

- When the Data Center installation directory on server B is same as that on server A.
- When the Data Center installation directory is different on server B, ensure that you replace the installation directory in both the scripts before running them on server B.

4. On Server B, install the Connected Backup Data Center software. At the prompt, specify the following information:
   - It is a mirrored configuration.
   - You are installing the second server.
   - Server A is the primary.
5. Complete the Connected Backup Data Center installation. The Data Center services automatically start.
6. On Server B, using the DCMC, stop all Data Center services on Server B.
7. On Server B, open the SQL Server Management Studio.
8. Complete one of the following steps:
   - If your Data Center servers are configured with a single archive storage volume, run the following script on Server B to determine the **VolumeID** number:

     ```
     SELECT ID FROM Directory.dbo.Volumes
     WHERE ServerID = <server_id>
     ```

     where

     `<server_id>` is the server ID for Server B. This number was obtained by step 7 in Reinstall the Data Center software on Server A, on page 34.

     After you obtain the *<server_id>* using the previous script, run the following SQL script:

     ```
     UPDATE Directory.dbo.ArchiveSet
     SET VolumeID = x
     ```

     where

     `x` is the `VolumeID` number from the previous script.
   - If your Data Center servers are configured with multiple archive storage volumes, use SQL Server Management Studio on Server B to run the following SQL script:

     ```
     UPDATE Directory.dbo.ArchiveSet
     SET VolumeID = -1
     ```
9. Close the SQL Server Management Studio.
10. Copy the `\DataCenter\Configuration$` folder from Server A to the same folder location on Server B.

Attach the SQL databases to Server B

To copy the SQL databases from Server A to Server B

1. On Server A, using the DCMC, stop all Data Center services on Server A.
2. On Server A and Server B, using the Services Control Panel, stop the SQL Server and the SQL Server Agent services.
3. Copy the following files from Server A to Server B:
   - `Directory.ldf`
   - `Directory.mdf`
   - `Registry.ldf`
   - `Registry.mdf`

   These files are in a designated SQL database volume and folder, as selected in Data Center Setup.
4. On Server A and Server B, using the Services Control Panel, restart the SQL Server and the SQL Server Agent services.
5. On Server B, open the SQL Server Management Studio.
6. In the Object Explorer, expand the server name, and then right-click **Databases**.
7. Click **Attach**.
8. Click **Add**, and then navigate to the location of Registry database files from step 3. Select the `Registry.mdf` file, and then click **OK**.

   Repeat the process for the Directory database.
9. Click **OK** to close the Attach Databases dialog box.
10. To configure the Registry database
    a. Right-click **Registry**, and then select **Tasks > Backup**. The Backup Database window opens.
    b. From the left pane, select **Options**.
    c. Under the Reliability section, select the **Verify backup when finished** check box, and then click **OK**.
    d. From the left pane, click **General**, and then set the **Backup Type** to **Full.**
    e. Click **OK**.
    f. The Destination section indicates the location where you initially installed the SQL Server software. To accept the default location, click **OK**.

       Optionally, to change the destination, click **Delete**, and then click **Add** to create a new location. Browse to a **Selected Path**, and enter a **File Name** in the corresponding fields.
11. Repeat step 10 for the Directory database.

12. On Server B, execute the SQL script `\<installation software folder>\DRProcs\SQLMirror_recover_cleanup.sql`

    where

    `\<installation software folder>` is the software installation folder.

13. On Server A, open the SQL Server Management Studio.
14. To verify that you successfully restored the databases on Server B, run the following script on Server A and Server B:

    ```
    SELECT COUNT(*) FROM Registry.dbo.Customer
    SELECT COUNT(*) FROM Registry.dbo.Community
    SELECT COUNT(*) FROM Directory.dbo.ArchiveSet
    SELECT COUNT(*) FROM Directory.dbo.Symlink
    ```

    Matching results on both servers indicate that you successfully restored the databases. If the results do not match, contact Support.

15. On Server A and Server B, close the SQL Server Management Studio.
16. On Server A, using DCMC, ensure that all the Data Center services are started except Compactor.

Copy archives

To copy the archives from Server A to Server B

1. On Server B, open the DCMC.
2. Expand Server B, right-click **BackupServer**, and then click **Properties**.
3. In the **BackupServer** tab, clear the **Allow Backups** and **Allow Restores** check boxes, and then click **OK**.
4. Start BackupServer on Server B.
5. Close the DCMC.
6. On Server B, start DataCopier. The DataCopier application is in the Data Center installation folder.
7. In the DataCopier - Select Action window, select **Add or rebuild a mirror server**, and then click **Next**.
8. Click **Add Server**.
9. Type the name of the new mirror server in the Add Server dialog box, and then click **OK**.
10. Click **Next**.

    The DataCopier - Summary window opens.

11. Click **Next**.

DataCopier copies the archives from Server A to Server B. The **Copying** window provides the status of the operation.

12. When the operation completes, click **Show Log** to verify that all archives were copied.

> **NOTE:**
> If you experience problems when you copy the archives, do not continue to the next step. Contact Support.

13. Close the DataCopier application.

Prepare Server B for connections

To turn on backups and restores on Server B

1. On Server B, open the DCMC.
2. Expand Server B, right-click **BackupServer**, and then click **Properties**.
3. In the **BackupServer** tab, select the **Allow Backups** and **Allow Restores** check boxes, and then click **OK**.
4. Use DCMC to verify that all Data Center services start for both servers. Start any services that are currently stopped.
5. Close the DCMC.
6. On the server hosting the Support Center and Account Management Website, restart the IIS Admin and Apache Tomcat services.

The Data Center is now a mirrored Data Center configuration.

Convert a mirrored Data Center to a stand-alone

This section explains how to convert a mirrored Data Center to a stand-alone configuration. When implementing the procedure, the user communities are preserved, while it decommissions Server B.

Do not use this procedure on a clustered Data Center.

> **CAUTION:**
> The results of this procedure are irreversible. Before you perform this procedure, contact Support.

This section uses the following terms and concepts as you convert your Data Center.

Server A	The server to remain in operation. For best practice, select the primary Data Center (the first server installed) as the server that you want to designate as the stand-alone server.
Server B	The server to be decommissioned.

If you must keep the secondary server of the mirrored pair as the remaining Data Center server, complete the Configure the secondary server as the primary server, on page 52before you perform this procedure.

Before you begin

- Read the entire procedure.
- Verify that the mirrored Data Center is fully operational and replicates properly.
- Obtain administrative logon access to the Data Center server.
- You must use the same version of the Data Center software installed on the servers before you convert to a stand-alone configuration.
- Notify users that the Data Center will be unavailable during the procedure.
- Record the Server ID and Data Center software version for Server A. To get this information, open DCMC and then select the BackupServer node.
- To perform a full database backup on Server A. To do so, open the `DataCenter\DRProcs` folder, and then run the following scripts:
  - `database_backup.sql`
  - `weeklymaint.sql`

  Do not overwrite the full database backup performed before you convert your Data Center.

  > **NOTE:**
  > To use the databases, Server A must have the Support Center service installed, or point to an independent Support Center server.

- Save the Connected registry **Keys** key. To save the **Keys** key, complete the following steps:
  1. Open the Windows Registry Editor
  2. Select `HKEY_LOCAL_MACHINE\SOFTWARE\Connected\Keys`**.** Ensure that you can see the MEK and PMEK values in the right pane. If you cannot, right-click the **Keys** key and then select **Permissions**. Verify that your `Keys` key permissions are set to **Full Control.** Then, re-examine the **Keys** key.

     > **NOTE:**
     > If you cannot see the MEK and PMEK values for the **HKEY_LOCAL_MACHINE\SOFTWARE\Connected\Keys** key, you cannot complete this procedure. For assistance with completing this task, contact Support.

  3. Right-click the **Keys** key and then select **Export**.
  4. Save the exported file to any folder on the old server.
  5. Copy this file to the replacement server and restore it.
  6. Stop all Data Center services on the old server, and then stop the Replication service on the mirror.

Convert your mirrored Data Center

> **NOTE:**
> This procedure requires that you use SQL Server Management Studio to change the SQL databases. Copy and paste the script content. Do not perform any SQL database changes other than those in this procedure.

To convert a mirrored Data Center to a stand-alone configuration

1. On Server A, use Data Center Management Console (DCMC) to verify that ReplicationServer starts.
2. On Server B, use DCMC to verify that ReplicationServer starts.
3. Use DCMC to perform the following tasks on both Server A and Server B:
   a. Pause BackupServer.
   b. Stop Compactor.
   c. Verify that no backups are in progress.

      If a backup is in progress, wait until the backup completes and then stop BackupServer on both servers.
4. Use DCMC to verify that the replication from Server B to Server A completes with no archive sets on Server B queued for replication, and no database table entries need to be replicated.

   Wait for replication to complete. Depending on the number of backups in progress at the time you paused BackupServer, this might take several minutes.
5. Use DCMC to stop all Data Center services on both servers.
6. Open SQL Server Management Studio and then open the `DataCenter\DRProcs` folder and run the following scripts on Server B:
   - `Uninstall_SQLMirror_Directory.sql`
   - `Uninstall_SQLMirror_Distribution.sql`

     If an error occurs in any SQL script, contact Corporate Support before you proceed with the next step.
7. Open SQL Server Management Studio and run the following scripts on Server A:
   - `Uninstall_SQLMirror_Directory.sql`
   - `Uninstall_SQLMirror_Distribution.sql`
   - `FixupStandaloneServer.sql`
8. Open SQL Server Management Studio and run the following scripts on Server B:
   - `Uninstall_SQLMirror_Directory.sql`
   - `Uninstall_SQLMirror_Distribution.sql`

> **NOTE:**
> When you run the `Uninstall_SQLMirror_Directory.sql` or the `Uninstall_SQLMirror_Distribution.sql` scripts, you might encounter some warnings. These can safely be ignored. However, if an error occurs in any SQL script, contact Corporate Support before you proceed with the rest of the procedure.

9. Remove Server B from the network to ensure that Agents cannot back up to that server. If you reconnect Server B to your network, it must have a new IP address and a new DNS name. This ensures that Server B does not attempt to reconnect for its previous use.

Configure your stand-alone Data Center

To configure you stand-alone Data Center

1. On Server A, run Data Center Setup to configure the server as a stand-alone Data Center. To do so, select **Reinstall the Data Center software**.To reinstall the Data Center software, you must meet the following conditions:
   - Use the same version of the Data Center software currently installed.
   - Use the original Server ID used for this server.
   - Install the Data Center software in the same order as you initially installed it. For example, if you configured your Data Center to use secondary tape sets during the initial installation, you must indicate the same during this installation. Select stand-alone instead of mirrored.
2. After Data Center Setup completes, restart all Data Center servers including the Web server and DataBundler server.
3. Open SQL Server Management Studio and then open the `DataCenter\DRProcs` folder and run the `DropSQLMirrorTables.sql` script on Server A.

   This step removes all tables that contain information replicated from the old mirrored server. Run this script when you are confident that the procedure has been a success.
4. Perform a backup of the SQL databases by running `weeklymaint.sql`. You can find this task in Windows Scheduler. Do not overwrite the full database backup you performed before you began this procedure.

Verifications

To verify that you can perform the following Connected Backup services on the new server:

1. Use an Agent to verify backup and retrieve files to the new stand-alone Data Center.
2. Log on Support Center and verify its usability.
3. Log on to the Account Management Website, and then verify that you can retrieve a file.

4. Create a DVD using the DataBundler application, if used.
5. Use DCMC to verify that all Data Center services started.

Add server pairs to a mirrored environment

This section describes how to add an additional pair of mirrored server to a mirrored data center environment, either a mirrored pair or a mirrored cluster. Adding a second server pair to an existing mirrored Data Center configuration converts the Data Center to a clustered configuration.

In a cluster, the original mirrored Data Center servers are the Registration Master servers. All other mirrored servers in the cluster are referred to as directory servers.

Use the following terms and concepts when adding servers to your Data Center.

Server A	Represents the new primary-side directory server
Server B	Represents the new secondary-side directory server

Before you begin

- Read the entire procedure.
- Use this procedure only with mirrored or clustered Data Center configurations.
- Adding servers to your Data Center configuration requires new licenses for all Data Centers in the configuration. You can use the License Request Form available through the MySupport portal to request for a license.
- Verify that all required software is installed and configured on the new server pair. Ensure that the new server pair meets the hardware and software requirements in *Connected Backup Requirements Matrix*.
- Determine the Data Center service account and password information for the Data Center. This information is used during the Data Center install and reinstall processes and must be the same for all Data Center servers.
- Add the new servers to the domain that contains the existing Data Center. All Data Centers must reside in the same domain.
- Download the Data Center installation file from the MySupport portal. You must install the exact version of the Data Center software on the new server pair as the version that is installed on the existing Data Center.
- Log in to the new servers using an account with local administrator permissions.

Add a new primary directory Data Center server

To add a new primary directory Data Center server

1. On one of the mirrored servers or one of the Registration Master servers if a cluster already exists, open the SQL Server Management Studio.
2. To determine the name of the primary Registration Master server, run the following script.

   ```
   SELECT ServerName FROM Registry.dbo.Server
   WHERE IsRegistrationMaster = 1 AND IsPrimary = 1
   ```

   Record the server name for the server. You need this value later in this procedure.
3. Close the SQL Server Management Studio.
4. On Server A, install the Connected Backup Data Center software as the primary server in an existing cluster.
5. To select the primary Registration Master server for the existing Data Center click the **[...]** button. Select the primary Data Center server that matches the result of the query in step 2. If you type the Data Center information rather than navigate to it, type the computer name, and not the DNS name or IP address, of the server.
6. In the Data Center Setup - Server Group window, use the number provided or type a unique number to control where new accounts and communities are created on the Data Center.
   - If you use the default value of zero (0), Connected Backup creates new accounts on any of the Data Center servers in the cluster.
   - If you use a different, unique value, the accounts for communities created after the Data Center install are stored on the newly added directory servers. Pre-existing communities do not register new accounts or back up to the new servers.
7. Complete the Connected Backup Data Center installation. The Data Center services automatically start.
8. On Server A, using the Data Center Management Console (DCMC), check the event log for errors.

Add a new secondary directory Data Center server

To install the Data Center software on the second cluster of servers

1. On Server B, install the Connected Backup Data Center software as a secondary server.
2. To select the primary Data Center server, click the [...] button and select Server A. If you enter the Data Center information rather than navigate to it, type the computer name, and not the DNS name or IP address, of the server.
3. Complete the Connected Backup Data Center installation. The Data Center services

automatically start.

4. On Server B, using the DCMC, check the event log for errors.

The Data Center now has an additional pair of directory servers for use.

Prepare servers for a non-mirrored cluster Data Center

This section describes how to create a Registry Master Server for a Non-Mirrored Cluster Data Center and add a subsequent Directory Server in the cluster. In this configuration, the Data Center Servers are installed individually instead of in pairs.

Use the following terms and concepts when adding servers to your Non-Mirrored Cluster Data Center

Server A	Represents the Registry Master Server
Server B	Represents the Directory Server that you add to your existing Non-Mirrored Cluster Data Center

Before you begin

- Read the entire procedure.
- Use this procedure only with Non-Mirrored Cluster Data Center configurations.
- Adding servers to your Non-Mirrored Cluster Data Center configuration requires new license for the Data Center in the configuration. You can use the License Request Form available through the MySupport portal to request for a license.
- Verify that all required software is installed and configured on the new server. Ensure that the new server meets the hardware and software requirements in *Connected Backup Requirements Matrix*.
- Determine the Data Center service account and password information for the Data Center. This information is used during the Data Center install and reinstall processes.
- Ensure that the first server to be installed must be a Stand-alone server (Registry Master Server) for a non-mirrored cluster, and this server must be a single instance in the Non-Mirrored Clustered configuration.
- For the subsequent Directory Server installations, ensure the following:
  - Web services (AMWS, Support Center) should not be installed on the same servers as the Data Center services (for performance reasons).
  - Ensure that you select **Primary server in an existing cluster** option, and then select **Non-Mirrored Directory Server** checkbox in the **Server Configuration Window.**
  - The Number of Users value in the Database Size dialog must be same as the number of users who will be directly assigned to a Directory Server.
  - Ensure that you use the same Windows service account for all the subsequent installations.

- Ensure that you note the Server ID. The default value is 1 as each subsequent server installation must have its own unique Server ID.

- Download the Data Center installation file from the MySupport portal. You must install the exact version of the Data Center software on the new Directory Server as the version that is installed on the existing Non-Mirrored Cluster Data Center.
- Log in to the new servers using an account with local administrator permissions.

Create a Registry Master server for a non-mirrored cluster Data Center

To create a Registry Master Server:

1. On Server A, you must install the Connected Backup Data Center as a Stand-alone server.
2. In the **Data Center Setup - Server ID** dialog box, create a unique server ID numbers for the server.

   The ID number must be different from any other server ID numbers used in the cluster. Valid numbers for this field are between 1 and 98. Record the server ID you chose for the server. You need the value later in the procedure.
3. In the **Data Center Setup - Database Size** window, specify the estimated number of users you expect to backup data to your Data Center.
4. When prompted, the Customer Volume can be set up in any available location on the server.
5. Complete the Connected Backup Data Center installation.

Add a Directory server to the non-mirrored cluster

To add a Directory server to the non-mirrored cluster:

1. On Server B, you must install the Data Center software as a **Primary server in an existing cluster**.
2. To select the Registry Master Server, click the [...] button and select Server A. If you enter the Data Center information rather than navigate to it, type the computer name, and not the DNS name or IP address, of the server.
3. Select the **Non-Mirrored Directory Server** checkbox.
4. You must ensure that this server is the first directory server added to the cluster or, all existing directory servers in the cluster are non-mirrored.
5. Complete the Connected Backup Data Center installation. The Data Center services automatically start.
6. On Server B, using the Data Center Management Console (DCMC), check the event log for

errors.

7. Repeat steps 1 through 4 to optionally add directory servers to the Non-Mirrored Cluster.

Create Registration Master servers for a mirrored cluster

This section describes how to set up dedicated Registration Master servers for your mirrored clustered Data Center. In the course of these procedures, you are required to move the Registry database from the two servers where the database currently reside on, to the two new servers designated for the Registration Masters.

Before you begin

- Read the entire procedure.
- Only use this procedure with clustered Data Center configurations.
- Adding servers to your Data Center configuration requires new licenses for all Data Centers in the configuration.You can use the License Request Form available through the MySupport portal to request for a license.
- Verify that all required software is installed and configured on the new server pair. Ensure that the new server pair meets the hardware and software requirements in *Connected Backup Requirements Matrix*.
- Determine the Data Center service account and password information for the Data Center. This information is used during the Data Center install and reinstall processes and must be the same for all Data Center servers.
- Add the new servers to the domain that contains the existing Data Center. All Data Centers must reside in the same domain.
- Download the Data Center installation file from the MySupport portal. You must install the exact version of the Data Center software on the new server pair as the version that is installed on the existing Data Center.
- Log in to the new servers using an account with local administrator permissions.

> **NOTE:**
> During the time that this procedure is completed, a service outage is required for the Data Center.

Install the new Registration Master servers

Install the Data Center software on the new mirrored servers that you designate as the Registration Master servers.

To install the Registration Master servers

1. On the one of the new Registration Master servers, install the Connected Backup Data Center as the primary server in a new cluster.

   > **NOTE:**
   > Set up the new Registration Master servers on a new cluster, not on an existing cluster.

2. In the **Data Center Setup - Server ID** dialog box, create a unique server ID numbers for the server.

   The ID number must be different from any other server ID numbers used in the cluster. Valid numbers for this field are between 1 and 98. Record the server ID you chose for the server. You need the value later in the procedure.

3. In the Data Center Setup - Database Size window, type the number 10.
4. When prompted, the Customer Volume can be set up in any available location on the server.
5. Complete the Connected Backup Data Center installation.
6. Using the Data Center Management Console (DCMC), stop all Data Center services on the new Registration Master server.
7. Repeats steps 1 through 6, but in step 1, install the Connected Backup Data Center as a secondary server on the remaining new Registration Master server.

Prepare the mirrored cluster

To prepare the mirrored cluster

1. Using the Data Center Management Console (DCMC), stop ReplicationServer and Compactor on all servers in the cluster.
2. On the Support Center server, use Windows Registry Editor to view the **RegistryConnect** value. The key is in the following registry location:

   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Connected\SupportCenter

   The `SERVER=` value must equal the Secondary Registration Master server name. If it does not equal the Secondary Registration Master server name, change the value.

   > **CAUTION:**
   > Failure to change the SERVER value to the secondary Registration Master server results in a Support Center service outage.

3. If you change the Windows registry, use Control Panel Services to stop the **IIS Admin** service, and then start the **World Wide Web Publishing** service on the Support Center servers.
4. If you use DataBundler, stop all DataBundler applications.
5. To determine the primary side of the Data Center cluster, open the SQL Server Management

Studio on one of the Data Centers servers that contains a Registry database, and run the following script.

```
SELECT ServerName FROM Registry.dbo.Server
WHERE IsRegistrationMaster = 1 AND IsPrimary = 1
```

6. On the each of the Data Center servers that contain a Registry database (the current Registration Master servers), open the SQL Server Management Studio and run the following script.

```
UPDATE Registry.dbo.Server
SET IsRegistrationMaster = 0
WHERE IsRegistrationMaster = 1
```

Point one side of the cluster to a Registration Master server

When you change the server configuration for your entire Data Center, perform the procedure first on the primary side of the Data Center, and then on the secondary side of the Data Center. This ensures that one side of your Data Center can accept backups when the other side is receiving maintenance.

1. Pick one side of the cluster to configure the new Registration Master for use. The remaining instructions in this section refer to the side of the cluster that you choose in this step.
2. Make sure you have a secure copy of the Connected registry keys for the current Registration Master server. For more information on how to back up needed files and information for a Data Center, including the Connected registry key, refer to the Required Disaster Recovery items section of *Connected Backup Disaster Recovery* guide.
3. Using the DCMC, stop all Data Center services for all servers on the chosen side of the cluster.
4. On the Data Center server that contains the Registry database (current Registration Master server), open the SQL Server Management Studio.
5. To link the new Registration Master server to this Data Center, run the following script.

   ```
   EXEC Master..sp_addlinkedserver '<new_server>', N'SQL Server'
   ```

   where

   `<new_server>` is the server name for the new Registration Master server for the chosen side of the cluster.

6. To insert the Server and ServerInterface table information for the new Registration Master server into the Registry database, run the following scripts:

   - ```
     INSERT INTO <old_server>.Registry.dbo.Server
     (ServerID, ServerName, TotalCust, ServerGroup, SecondaryServerID,
     IsRegistrationMaster, IsPrimary, ServerType)
     SELECT ServerID, ServerName, TotalCust, ServerGroup, SecondaryServerID,
     IsRegistrationMaster, IsPrimary, ServerType
     FROM <new_server>.Registry.dbo.Server
     ```

     where
     ```

<old_server> is the server name of the original Registration Master server.

<new_server> is the server name of the new Registration Master server.

- INSERT INTO *<old_server>*.Registry.dbo.ServerInterface
  (ServerID, DNSName, IPAddress, Port, Services, CDate)
  SELECT ServerID, DNSName, IPAddress, Port, Services, CDate
  FROM *<new_server>*.Registry.dbo.ServerInterface

  where

  <old_server> is the server name of the original Registration Master server.

  <new_server> is the server name of the new Registration Master server.

7. To verify the integrity of the Registry database later in this procedure, run the following script:

   ```
   SELECT COUNT(*) FROM Registry.dbo.Customer
   ```

   You need this value later in the procedure.

8. Navigate to the current Registration Master server, and then expand the **Databases** folder.
9. Right-click **Registry**, and then click **Tasks > Detach**. The Detach window opens.
10. Select **Drop Connections**
11. Click **OK**.
12. Close the SQL Server Management Studio.
13. On the current Registration Master server, using the Services Control Panel, stop the SQL Server and the SQL Server Agent services.
14. On the new Registration Master server, using the Services Control Panel, stop the SQL Server and the SQL Server Agent services.
15. Copy the following files from the current Registration Master server to the new Registration Master server:

    - Registry.ldf
    - Registry.mdf

      These files are in a designated SQL database volume and folder, as selected in Data Center Setup. If prompted, confirm that you want to overwrite the original files in the folder.

16. On the new Registration Master server, using the Services Control Panel, restart the SQL Server and the SQL Server Agent services.
17. On the new Registration Master server, open the SQL Server Management Studio.
18. To configure the new Registration Master server to exclusively handle account registration duties and not to store Connected Backup account data, run the following script.

    ```
    UPDATE Registry.dbo.Server
    SET ServerGroup = 99
    WHERE ServerID = X
    ```

    where

X is the ServerID for the new Registration Master server.

19. On each Data Center server in the chosen cluster, using the Registry Editor, change the **Master** value to the new Registration Master server name. The key is in the following registry location:

    HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Connected\BackupServer

20. Copy the Connected registry key `.reg` file from the current Registration Master server to the new Registration Master server.
21. On the new Registration Master server, double-click the `.reg` file. The `.reg` file recreates the Master Encryption Key (MEK) and Pool Master Encryption Key (PMEK) registry keys on the new Registration Master server.
22. On the current Registration Master server, using Registry Editor, delete the **Keys** key. The key is in the following registry location:

    HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Connected

23. On each Data Center server in the chosen cluster, using the Services Control Panel, restart the SQL Server and SQL Server Agent services.
24. On each Data Center server in the chosen cluster, using SQL Server Management Studio, run the following script:

    EXEC Master..sp_setnetname 'RegistryMaster', '*<new_server>*'

    where

    `<new_server>` is the server name of the new Registration Master server.

    > **NOTE:**
    > When you run this script, you might receive the following warning:
    >
    > ```
    > Warning: A linked server that refers to the originating server is not a
    > supported scenario. If you wish to use a four-part name to reference a
    > local table, please use the actual server name rather then an alias.
    > ```
    >
    > You can safely ignore this warning.

25. Copy the following files from the Data Center installation folder of the current Registration Master server to the Data Center installation folder of the new Registration Master server:
    - `privatekey.pem`
    - `certificate.pem`
26. Copy the `\DataCenter\Configuration$` folder from the current Registration Master server to the same folder location on the new Registration Master server.
27. Use DCMC to restart the Data Center services on each Data Center server in the chosen cluster, excepting the ReplicationServer and Compactor services.
28. After you successfully restart the Data Center services, run the following script on the new Registration Master server:

    ```
    SELECT COUNT(*) FROM Registry.dbo.Customer
    ```

Compare these results with those found in step 8. The values must be equal.

29. On the Support Center server, using Registry Editor, navigate to **RegistryConnect**, and change the value of **SERVER** to the server name of the new Registration Master server. The key is in the following registry location:

    HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Connected\SupportCenter

    > **NOTE:**
    > This step is required only for the primary side of the cluster, and is skipped for the secondary side.

30. On the Support Center server, using the Services Control Panel, stop the **IIS Admin** service, and then start the **World Wide Web Publishing** service.
31. Log on to Support Center to verify that Support Center can connect to the Registry database. If you cannot connect to Support Center, contact Support.
32. Using the DCMC, check the event log for errors.

    After you complete each task on the Primary Data Center side, repeat each task in the order they are presented for the Secondary Data Center side.

    > **NOTE:** When you perform maintenance on one side of the cluster, be sure that your Support Center points to the opposite side.

Final steps

1. Use DCMC to start all Data Center services on all Data Centers in the cluster.
2. On both the primary and secondary current Registration Master servers, click **Start > All Programs > Accessories > System Tools > Scheduled Tasks**, and then delete the LDAPsyncher task.
3. Close the Scheduled Tasks window.

A new Registration Master server pair has been incorporated for use into the clustered Data Center.

Configure the secondary server as the primary server

Use the following procedure to make the secondary server the primary server on the Data Center. For example, you install the Data Center on Server A first, which makes it the primary Data Center server. You then install the software on Server B, which makes it the secondary Data Center server.

To make Server B the primary Data Center server

1. Save and export the following the **Compactor** Windows registry key from the primary server. The key is in the following registry location:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Connected\Compactor

2. Import the saved Compactor registry key from step 1 on the secondary server.
3. Delete the **Compactor** registry key on the primary server.
4. Stop all Data Center services on both servers by using DCMC.
5. Use SQL Server Management Studio to run the following command:

   ```
   SELECT * FROM Registry.dbo.Server
   ```

   The command displays the ServerID values for the mirrored servers, which you need to use in step 6.
6. Use SQL Server Management Studio to run the following commands.

   ```
   UPDATE Registry.dbo.Server
   SET IsPrimary = 1 WHERE ServerID = X
   ```

   ```
   UPDATE Registry.dbo.Server
   SET IsPrimary = 0 WHERE ServerID = Y
   ```

   where

   - *X* with the ServerID of the new primary server.
   - *Y* with the ServerID of the old primary server.
7. Use DCMC to stop and restart ReplicationServer on both servers.

   > **NOTE:**
   > If you run a clustered Data Center, use DCMC to stop and restart ReplicationServer on both Registration Master servers.
8. Move the LDAP Syncher scheduled task to the new primary server.

   If you run a clustered Data Center and the servers that you are modifying are the Registration Masters, move the LDAPSyncher scheduled task to the new primary server.

Swap primary and secondary Data Center assignments

If one of a mirrored pair of Data Centers is not running, in most cases users for whom it is the primary Data Center will automatically connect to the mirror that is still up. For example, if Data Center A is not running, and a user has Data Center A for his primary Data Center, he will connect automatically to Data Center B as long as A is down. In practice, this “bounce” feature sometimes fails.

Occasionally, it is necessary to ask the Agent to swap temporarily the precedence of Data Centers, that is, to try to connect to its secondary Data Center first.

> **NOTE:**
> Only use this procedure with mirrored or clustered Data Center configurations.

To change the primary server for a particular account

1. Open a Web browser and log in to Support Center.
2. Search for the account that requires a primary server change, and then click on the account number.
3. On the Account Summary page for the account, click **Primary Server**.
4. Select the server that will be the new primary server for the account, and then click **Save**.
5. Close the Web browser.

Assign Data Center servers and communities based on geography

You can have a Mirrored Data Center configurations, either a mirrored pair or as part of a mirrored cluster where the servers are geographically distant. In this case, you can configure the servers so that the Agent registers, and then consequently, attempts to connect to the local Data Center server first.

For example, you have one Data Center server in California and the mirrored server in New York. You can set up the Data Center so that all end users in New York use the New York server as their primary Data Center server. In addition, end users in California use the California server as their primary server. An end-user's primary Data Center server is the server that the Agent attempts to connect to first. If the primary Data Center server is not available, the Agent attempts to connect to the mirrored server. Because it is a mirror, all data must eventually go to both servers.

Before you begin

Ensure that you have local administrator logon privileges to access the Data Center servers.

To assign Data Center servers and communities based on geography

1. Open Microsoft SQL Server Management Studio and then run the following query:

   ```
   USE Registry

   SELECT * FROM Server
   ```

   The results of the preceding query show an entry for each server. You assign a ServerID number for each server with a Server Group number. The number for both servers is 0, which is the default configuration for mirrored servers.

2. To assign each Data Center server to its own Server Group, run the following query:

   ```
   UPDATE Server

   SET ServerGroup = ServerID

   WHERE ServerType = 1
   ```

3. To verify the update ran properly, run the following query:

   ```
   USE Registry

   SELECT * FROM Server
   ```

4. Use Support Center to create new communities. After you create the community, be sure to assign the community to the appropriate Data Center server. If communities exist, update each one to point to one Data Center server or the other. To perform this task, complete the following steps:

   a. Use SQL Server Management Studio to run the following script. Record the CommunityID for each community:

      ```
      USE Registry

      SELECT * FROM Community
      ```

      The results from the preceding script display a list of each community that you assigned to a ServerGroup number. The ServerGroup number for each community is 0.

   b. To update each community to the new ServerGroup number, run the following script:

      ```
      USE Registry

      UPDATE Community

      SET ServerGroup = X

      WHERE CommunityId = Y
      ```

      Where

      – *X* is the ServerGroup number that corresponds to the appropriate Data Center server.

      – *Y* is the CommunityID number that corresponds to the appropriate community.

   c. To update each active account to use the appropriate server, run the following script for each community on the Data Center:

      ```
      USE Registry

      UPDATE Customer

      SET AssignedServerId = X

      WHERE OfferId = Y
      ```

      Where

      – *X* is the ServerID number that corresponds to the appropriate Data Center server. To view the ServerID numbers for each server, run the `Select * from Server` query.

      – *Y* is the CommunityID number that corresponds to the appropriate community.

Replace a Data Center server with new hardware

To replace a Data Center of any configuration type with new hardware, refer to the appropriate chapter of the *Data Center Disaster Recovery* guide because both planned and unplanned server replacements

use the same process.

- To replace hardware in a stand-alone Data Center, refer to the “Recovering a Standalone Data Center” chapter.
- To replace hardware in mirrored Data Centers, refer to the “Recovery of a Mirrored Data Center” chapter. In this chapter, use the “Recover One Data Center Server of a Mirrored Pair” topic for each server in the mirror that you want to move to new hardware.
- For clustered Data Centers, refer to the “Recovering a Clustered Data Center” chapter. In this chapter, use the “Recover a Clustered Data Center Server” topic for each server in the cluster that you want to move to new hardware.

Chapter 6: Data Center management tools

This chapter describes the tools that you can install on Data Centers and use to manage Data Centers. It also explains how to install the tools.

Management tools overview

The Connected Backup software includes the following management tools:

Tool	Description of service
Data Center Management Console (DCMC)	Enables you to perform a variety of tasks necessary to monitor and control Data Center operations. The DCMC is a snap-in for the Microsoft Management Console (MMC). For more information, see Manage the Data Center with DCMC, on page 62. This tool is included in the Data Center Toolkit.
CancelHoldAccounts	Enables you to cancel or place an account on hold when you are using Single Sign On (SSO) in your Data Center. CancelHoldAccounts uses SSO CommunityIDs and FedAuth User IDs to identify accounts of interest. For more information, see The CancelHoldAccounts utility, on page 68. This tool is included in the Data Center Toolkit.
DC Message Logger	Enables the Data Center Management Console to read remote event logs. This tool is included in the Data Center Toolkit.
Host ID	Determines the host ID (ethernet host address) of a server. This utility runs on the Data Center; you cannot use it from a remote location.
Disk Status	Displays disk space allocation for files used by the Data Center. This tool is included in the Data Center Toolkit.
DC Status	Provides detailed statistics about each Data Center server's uptime and current status.
dsping	Helps to diagnose connectivity problems. It is similar to the standard ping command, but uses the Data Center protocol rather than the ICMP protocol used by regular ping. This tool is included in the Data Center Toolkit.

Tool	Description of service
dsping80	Helps to diagnose connectivity problems. Similar to dsping, but also uses the Data Center security certificate to test connectivity between Agents and the Data Center.
Dump	Displays the contents of archives and helps to verify the archive integrity. This utility runs on the Data Center; you cannot use it from a remote location.
DCDiag	Gathers current information about the Data Center server that you can send to Support.
Tdate Converter	Converts tdates to conventional date format or conventional dates to tdates. A tdate is the date of backup transmission of a file stored on the Data Center. The Data Center software refers to the date as a 10-digit number of seconds since January 1st, 1970 12:00:00 AM GMT. This tool is included in the Data Center Toolkit.
DataCopier	Copies data from one Data Center server's disk to another. This utility runs on the Data Center; you cannot use it from a remote location.
DataBundler	Creates an image of an Agent account that includes backed-up files from a specific date. You can burn the account image onto a DVD. You can configure DataBundler to create account images when it receives requests, or you can build images manually. When DataBundler builds an account image, it includes a copy of the Agent application. Use the Agent user interface to retrieve files from the account image. For more information, refer to DataBundler Help.
Data Center Toolkit	The Data Center Toolkit includes tools that you can use to monitor and manage the Data Center remotely. You can install the Data Center Toolkit on any number of computers. The computers on which you install the Data Center Toolkit must have access to the Data Center server(s).

Install DataBundler

Data Center Setup does not install DataBundler on the Data Center server. You must install it separately.

DataBundler requirements

To run DataBundler, your computer must meet the following requirements:

- Windows Server operating system that supports Connected Backup. For a list of supported versions, refer to *Connected Backup Requirements Matrix* guide.

- Hard disk space on one volume that is at least twice the size of the largest account (minimum of 6 GB).
- Full connectivity to the Data Center server(s).
- The DataBundler client must be in the same domain as the Data Center server(s) and must have high-speed LAN access to the server(s).
- SQL Server Client Networking Utility that supports Connected Backup. For a list of supported versions, refer to *Connected Backup Requirements Matrix* guide.
- DVD -burning hardware and software. While you burn a DVD, do not use the DataBundler client for any other purpose. Dedicate the client solely to the creation of DVDs. If you expect to burn a large number of DVDs, install DataBundler on more than one computer. Each computer that has DataBundler can burn only one DVD at a time.

> **NOTE:**
> Because of performance issues, do not install DataBundler on the same computer as a Data Center.

Prepare to install DataBundler

Before you install DataBundler, create the user account CNTD_DataBundler on the computer where you plan to install the DataBundler application and add it to the Administrator Users group. With Administrator User privileges, you can successfully burn DVDs.

> **NOTE:**
> If you upgrade your Data Center from an earlier version, you can continue to use the CNTD_CDMaker user account on the computer where you installed the DataBundler application.

Install DataBundler

To install DataBundler

1. Do one of the following:
   - If you want to use DataBundler to create images for 6.x Agents, install version 6.x of the CDMaker software first.

     Do not remove the CD Maker software.
   - If you do not want to use DataBundler to create images for 6.x Agents, continue to the next step.
2. Log on to the computer as an administrator.
3. Close applications that are open.

   If you switch user IDs on the same computer, the first user's open applications do not close automatically.

4. Copy the DataBundler folder from where you installed the Data Center software to a convenient location on the local computer.
5. In the DataBundler folder, double-click `setup.exe`.
6. Follow the instructions in the setup program to install DataBundler.
7. When DataBundler prompts you for the location of where to install the program, specify the location of the large disk volume on which you want Data Bundler to create the account images.

   The setup program creates a share for the folder, so that all members of the domain can have access to it.

Requirements for using DataBundler

Before you use DataBundler application, complete the following tasks:

- Be sure that DataBundler has write access to its installation directory.
- When you start the DataBundler application, use the user account that you specified for the application when you installed the Data Center (CNTD_DataBundler or CNTD_CDMaker)
- Be sure that the DataBundler user account belongs to the Administrators User group.

  > **NOTE:**
  > CNTD_CDMaker is only used on a 7.x or earlier Data Center.

- When you specify the location for the media images, use a UNC (Universal Naming Convention) path to a directory to which DataBundler has access. If you specify a path on the local computer, you must provide write permissions for that directory. If you specify a path on a remote computer, use a shared directory and provide the write privileges. For more information about how to use DataBundler, refer to DataBundler Help.

Install the Data Center toolkit

The Data Center Toolkit lets you use some of the utilities that are included in the Data Center Setup to maintain the Data Center remotely from a computer other than the Data Center server. For example, you can use the Data Center Toolkit to monitor the BackupServer status remotely.

Data Center toolkit requirements

The Data Center Toolkit has the following requirements:

- You must install the Data Center Toolkit on a computer that does not host the Data Center software, but is in the same domain as the Data Center server(s).
- You must install the Data Center Toolkit only on computers with Windows operating systems that use the English locale.
- The computer on which you install the Data Center Toolkit must have access to the Data Center

server(s).

- The computer on which you install the Data Center Toolkit must be in the same domain as the Data Center server(s).

Install the toolkit

You can install the Data Center Toolkit on any number of computers.

> **NOTE:**
> You must install the Data Center Toolkit on a computer that does not host the Data Center software.

To install the Data Center toolkit

1. Navigate to the folder where you downloaded and extracted the contents of the Data Center software installation package
2. In the Toolkit folder, double-click `setup.exe`,and then follow the installation prompts.

Run the Data Center toolkit

The Data Center Toolkit contains the following tools:

- Data Center Management Console (DCMC)
- DC Message Logger
- Disk Status
- Tdate Converter
- dsping
- CancelHoldAccounts

To run a Data Center toolkit

- Click **Start > All Programs > Data Center Toolkit**.

Chapter 7: Manage the Data Center with DCMC

This chapter explains the Data Center Management Console (DCMC). It also describes how to use the DCMC to monitor and control Data Center operations, and manage Connected Backup services.

DCMC overview

The Data Center Management Console (DCMC) is a snap-in for the Microsoft Management Console (MMC). Together with the MMC, the DCMC provides a user interface that you can use to monitor and control Data Center operations and manage the following services:

- BackupServer
- PoolServer
- ReplicationServer
- IndexServer
- Compactor

For more information, refer to the DCMC Help.

> **NOTE:**
> To work with the DCMC, you must be familiar with the Microsoft Management Console (MMC).

The following table describes the tasks that you can perform with the DCMC.

Task	Description
Start, pause, and stop the Data Center services.	Starts, pauses, and stops Data Center services. Also shows icons in the DCMC console tree and information in the details pane to indicate whether Data Center services are running or stopped. For more information about the DCMC interface, see DCMC user interface, on page 64.
View and modify properties for each Data Center service.	Shows the default properties and properties that you selected during Data Center setup. Also lets you can change these properties. Contact Corporate Support for guidance before you make changes.
Monitor multiple	Shows the status of mirrored or clustered servers simultaneously.

Task	Description
Data Center servers simultaneously.	
View event logs and run the Windows Event Viewer.	Shows the event logs for Data Center operations so you can diagnose Data Center problems. You also can run the Windows Event Viewer for a Data Center.

DCMC Access Requirements

To use DCMC, log on to the Data Center server or a remote computer that has the Data Center Toolkit. To use DCMC, you must have access to the following components:

- Local administrator privileges for the following computers:
  - Local computer
  - Data Center servers
  - The **Connected** Windows registry key. The key is in the following registry location:

    HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Connected
- Service Control Manager

  The Service Control Manager lets you start, stop, and query services.
- The disk volumes that are attached to each computer

  By default, Data Center Setup sets these device shares to allow access only to administrators who have privileges in the domain. You can change this setting to allow access to other administrators.
- Event Log on each computer
- SQL Server on the selected server

  You must be able to perform the following tasks on SQL tables:
  - Read queries
  - Inserts
  - Updates
  - Deletes
  - Stored procedure calls

    The Data Center Setup procedure grants access to the Domain Administrators group, but you can extend these permissions to other administrators not part of the group.
- Domain access

  The DCMC computer must be in the same domain as the Data Center server.

Start DCMC

You can run the DCMC on a Data Center server. Alternatively, if your remote computer hosts the Data Center Toolkit, you can run the DCMC remotely.

To start the DCMC, from a Data Center server

1. Click **Start > All Programs > Data Center**.
2. Click **Data Center Management Console**.

To start the DCMC from a remote computer that hosts the Data Center Toolkit

1. Click **Start > All Programs** > **Data Center Toolkit**.
2. Click **Data Center Management Console**.

If your Data Center does not appear in the DCMC console tree, add it. For more information, refer to the DCMC Help.

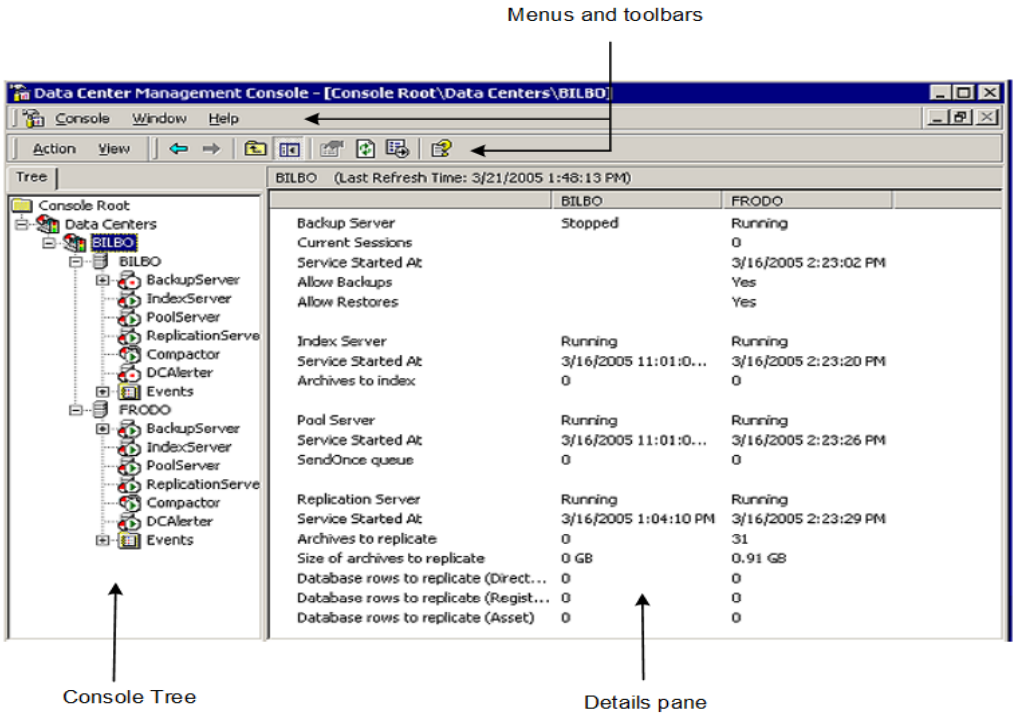
DCMC user interface

The DCMC supports and enhances the standard MMC functions and interface elements. Together with the MMC, the DCMC provides a user interface that lets you manage the Data Center components.

The DCMC interface includes the following elements:

Console tree (left pane)	Displays DCMC icons to make visualizing DCMC components easy
Details pane (right pane)	Provides information based on your selection in the console tree
Menus and toolbars (including shortcut menus)	Displays DCMC commands

The following figure shows the DCMC interface:



Console tree

The console tree uses icons to represent each Data Center component. These icons are organized hierarchically in the following manner:

- Servers appear under the Data Center to which they belong.
- Services and components appear under the server with which they are associated.

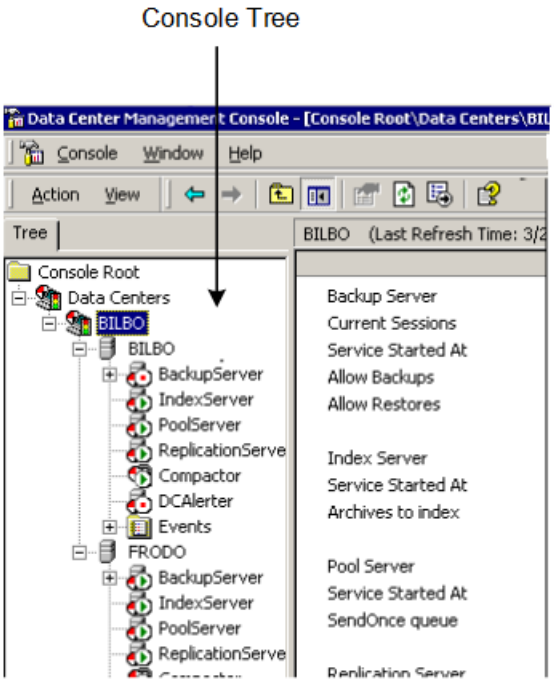
If a service or component contains subcomponents, a plus sign (+) appears to the left of the component icon. To view subcomponents, complete one of the following tasks:

- Click **+**
- Double-click the component name

Icons indicate whether the service or component is running or stopped in the following ways:

- **Running** — green right pointing arrow inside of a circle
- **Stopped** — red square inside of a circle

The following figure shows the DCMC console tree.



Details pane

The DCMC details pane displays information about the item that you select in the console tree. For example, if you select a Data Center in the console tree, the details pane displays the status and other information about the services that run on the Data Center servers.

You can set the DCMC to refresh the view of the details pane at set intervals. By default, the DCMC service refreshes the view every five minutes. You also can manually refresh the view of the details pane.

Menus and toolbars

You can gain access to the DCMC functions and properties through toolbars and menus. The DCMC menus contain the console commands and other DCMC functions.

Menus

DCMC has the following menu types:

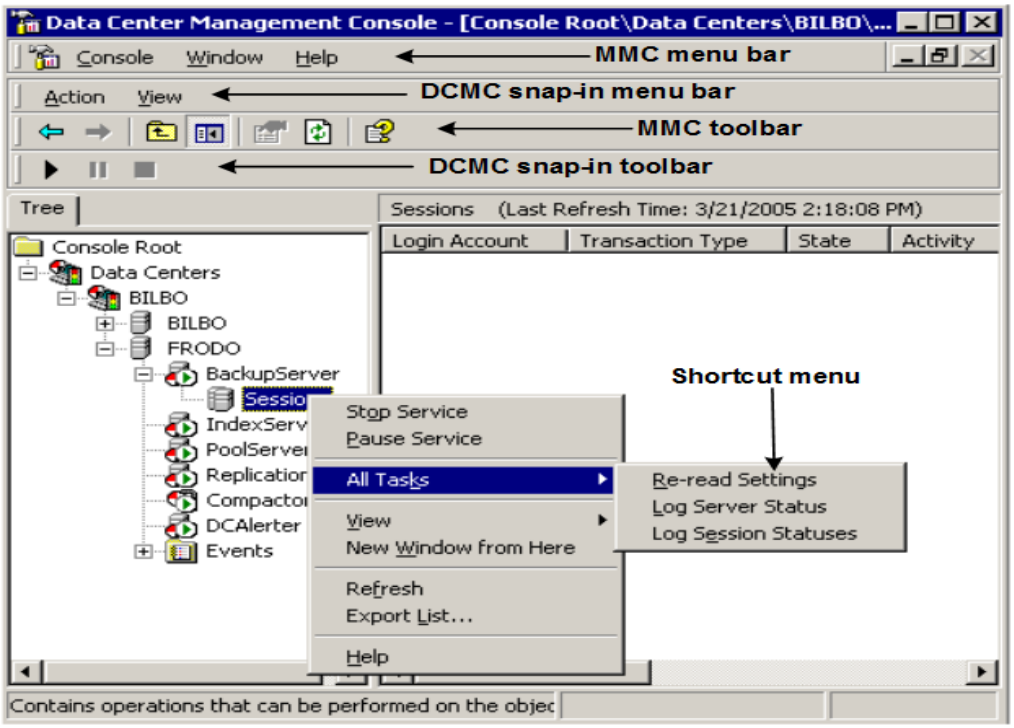
Menu	Description
Microsoft Management Console (MMC) menu bar	Includes the Console, Window, and Help menus. These menus are standard to MMC.

Menu	Description
DCMC snap-in menu bar	Includes the Action and View menus. These menus provide access to DCMC functions and display options for the console tree and details pane.
Shortcut menu	Appears when you right-click items in the console tree and details pane. With a shortcut menu, you can modify the properties for the selected item or run a command relevant to the selected item.

Toolbars

The DCMC contains snap-in tool bars to augment the MMC toolbar. Together, the tool bars provide access to the console functions and DCMC commands. If you do not use the tool bars, you can gain access to the functions and commands through menus. The DCMC also has a description bar, which displays the name of the current view, including the time the view was last refreshed.

The following figure shows the DCMC menus and toolbars:



Chapter 8: The CancelHoldAccounts utility

This chapter explains the CancelHoldAccounts utility for use with Single Sign On (SSO) communities in your Data Center.

CancelHoldAccounts overview

The CancelHoldAccounts utility allows Single Sign On (SSO) community technicians to log in and operated within their communities and also allows root technicians to operate across all SSO communities to cancel or hold accounts.

The CancelHoldAccounts command line utility is included as part of the Data Center installation and separately available in the Data Center Toolkit.

CancelHoldAccounts access requirements

To run the CancelHoldAccounts tools from the DataCenter, log in to a DataCenter host as an administrator and navigate to the DataCenter installation directory.

To run the CancelHoldAccounts tool from any other host, install the Data Center Toolkit as an administrator, and navigate to the directory where it is installed. For more information on installing the Data Center Toolkit, see Install the Data Center toolkit, on page 60.

- Microsoft .NET Framework Version 3.5 or higher

  The CancelHoldAccounts computer must have Microsoft .Net Framework 3.5 or higher installed.

To use CancelHoldAccounts, you must have access to the following components:

- Your Connected Data Center must be licensed for Web Services API.

Assumptions

The CancelHoldAccounts uses SSO community IDs and user IDs to identify accounts to operate upon.

Command syntax

The CancelHoldAccounts utility uses the following syntax.

```
CancelHoldAccounts.exe
        -endpoint=<URL|host>
        -techid=<id>
        -password=<password>
        -techcommunity=<community-name>
        -cancel | -hold
        -communityid=<community>
        -userid=<user> | @<userfile>
```

Parameter	Short	Default value	Description

`-endpoint=<URL|host>`	`-e`	localhost	URL of the Web Services API endpoint.
			If `-endpoint` is specified, it must appear before any user IDs.
			The full path is
			`https://<supportcentermachine>/AdminAPI/AdminAPI.dll?Handler=Default`
			where `<supportcentermachine>` is the machine where the Web Services API and Support Center is installed.
			For example:
			`-endpoint=https://sc.example.com/AdminAPI/AdminAPI.dll?Handler=Default`
			where
			`https://sc.example.com` is the Support Center server.
			The URL of the Web Services API endpoint must use https://.

`<id>`	`-tid`	none	**(Required)** A valid Technician ID.
`-password=<pwd>`	`-pw`	none	**(Required)** The password associated with the selected Technician ID.
`-techcommunity=`	`-tc`	“” The default -1	Technician login community

Parameter	Short	Default value	Description
<community-name>		community	
-cancel | -hold		none	Specifies the operation to perform. -cancel and -hold are keywords; you must enter either -cancel or -hold, but not both. -cancel Cancels subsequent user account accounts, until another action appears. -hold Puts user account on hold, until another action appears.
-communityid= *<number>*	-cid	none	**(Required)** The community in which subsequent user IDs are looked up. The -communityid parameter can appear only once.
-justification= *"text"*	-j	"CancelHoldAccounts"	The justification message that is logged in Support Center after this utility is run. The -justification parameter is optional, but can only appear once.
statuscode= *<number>*	-sc	0	Status code logged in Support Center after this utility is run. The -statuscode parameter is optional, but can only appear once.
-userid= *<id> | @<file>*	-id	none	Specify the user ids to cancel or put on hold. -user=<id> Indicates the user(s) whose accounts will be cancelled or put on hold. @<file> Indicates the path to a text file containing a list of users whose accounts will be cancelled or put on hold. You must enter either -userid=<id> or @<file>, but not both.

CancelHoldAccounts Command Usage Notes

Consider the following factors when preparing to run the CancelHoldAccounts utility:

- Most parameters in the CancelHoldAccounts utility have shorthand equivalents. See the table above for the parameters, and the examples below.
- For the `-endpoint` parameter for the Web Services API URL, https:// is required.
- For the `-endpoint` parameter, the path after the machine name defaults to `/AdminAPI/AdminAPI.dll?Handler=Default` and the protocol defaults to https://.

  The shortest form of the -endpoint parameter you can use is -endpoint=*<supportcentermachine>*.

  For example:

  `-endpoint=https://sc.example.com/`
- The parameter `-techcommunityid` is the technician's login community.
- If no `-techcommunity` parameter is present, then this is root technician.
- The `-communityid` parameter is required and must appear only once.
- Either `-cancel` or `-hold` is required.
- The text file for use with the `@<file>` parameter must contain one user ID per line.
- User ID parameters must be "quoted" if they contain special characters to the command line parser. User IDs inside a `@<file>` text file do not need to be quoted.

Run the CancelHoldAccounts utility

Run the CancelHoldAccounts utility to cancel or put SSO user accounts on hold.

To run the CancelHoldAccounts utility

1. Log in as an administrator to the computer where you installed the Data Center Toolkit.
2. Navigate to the folder where you installed the Data Center Toolkit.
3. At a command prompt, enter the command with the parameters in order.

   For example:

   CancelHoldAccounts -endpoint=<*URL*> -techid=<*id*> -password=<*password*> -techcommunity=<*community-name*> -cancel | -hold -communityid=<*community*> -userid=<*user*> | @<*userfile*>
4. Press **ENTER**.

   The utility runs.

   When the utility succeeds, the command line returns a success message.

CancelHoldAccounts command syntax examples

The CancelHoldAccounts utility can be run with several combinations of parameters to perform the necessary operations. Below are examples of common scenarios.

Cancel Accounts

The following CancelHoldAccounts command example performs the following actions:

- Attaches to the Web Services API running on localhost, because the `-endpoint` parameter was not specified.
- Logs in as technician Admin with its password into the root community.
- Cancels all accounts in community 3 associated with the users JamesZ and SonaliM.

  CancelHoldAccounts -techid=Admin -password=myPassword -cancel -communityid=3 -userid=JamesZ -userid=SonaliM

  The command example results in the following output:

  ```
  User JamesZ account 101000892 set to status Cancelled

  User SonaliM account 101001288 set to status Cancelled

  User SonaliM account 101001369 set to status Cancelled
  ```

Use shorthand parameters

The following example uses the shorthand versions of each parameter and is equivalent to the previous example.

CancelHoldAccounts -tid=Admin -pw=myPassword -cancel -cid=3 -id=JamesZ -id=SonaliM

The command example results in the following output:

```
User JamesZ account 101000892 set to status Cancelled

User SonaliM account 101001288 set to status Cancelled

User SonaliM account 101001369 set to status Cancelled
```

Hold accounts

The following CancelHoldAccounts command example performs the following actions:

- Attaches to the Web Services API running on localhost, because the `-endpoint` parameter was not specified.
- Logs in as technician Admin with its password into the root community.
- Puts on hold all accounts in community 3 associated with the users JamesZ and SonaliM.

  CancelHoldAccounts -techid=Admin -password=myPassword -hold -communityid=3 -userid=JamesZ

  The command example results in the following output:

```
User JamesZ account 101000892 set to status On Hold
User SonaliM account 101001288 set to status On Hold
```

CancelHoldAccounts with a file of UserIDs

The following example uses a file containing a list of user IDs to cancel instead of individual user IDs.

`CancelHoldAccounts -tid=Admin -pw=myPassword -cancel -cid=3 @users.txt`

where the `users.txt` file contains

```
JamesZ
SonaliM
```

> **NOTE:**
> The text file for use with the `@<file>` parameter must contain one user ID per line.
>
> User ID parameters must be "quoted" if they contain special characters to the command line parser. User IDs inside a `@<file>` text file do not need to be quoted.

Incorrect parameters

If the CancelHoldAccounts utility encounters failures, it logs errors messages to the standard output.

The following CancelHoldAccounts command example contains an incorrect parameter for the -password parameter.

CancelHoldAccounts -techid=Admin -password=myWrongPassword -cancel -communityid=3 -userid=JamesZ

The command example results in the following error output:

```
SOAP exception logging in technician: Unable to authenticate technician. Either
the Technician ID or password is incorrect, or there is more than one technician
with submitted credentials.
```

Error messages

CancelHoldAccounts utility error messages are written to the standard error stream.

CancelHoldAccounts error messages

The following error messages are generated by the CancelHoldAccounts utility.

Error	Description	Corrective Action
`0`	All accounts were handled	

Error	Description	Corrective Action
	successfully.	
1	Missing or invalid parameters.	Check for missing required parameters. If parameters contain spaces or other special characters, the value must be quoted.

Web services API error codes

The following error codes are generated by the Connected Backup Web Services API when the CancelHoldAccounts utility runs and encounters an error.

Error code	Description	Corrective action
1000	Time-out issue from database.	
1001	Access denied, technician does not have “Scripting” permission in Support Center.	The technician must have "Scripting" permission in Support Center.
1014	Access denied, technician does not have access to the selected resource.	The technician must have the "Change the Status of Accounts" permission in Support Center.
1015	The specified community does not exist.	Check Support Center to verify the community ID.
1016	The specified account cannot be found.	
1030	Unable to authenticate the technician.	Verify that you input the correct technician ID and password.
1031	The technician’s password has expired.	

Chapter 9: Data Center logging

This chapter explains how the Data Center logs information.

Event logs

The Data Center provides a standard way for multiple Data Center components to report events. It also provides a way to categorize events according to levels of priority.

The following table describes the Event logs:

Log	Description
DCMaint event log	Contains entries about events that pertain to the Data Center application, and are specifically designated to the DCMaint event log. You can use this event log to monitor the Data Center services. You can view the DCMaint from DCMC or the Windows Event Viewer on the Data Center server. Because the messages in the DCMaint log are detailed, this log is useful for troubleshooting. Added by the Data Center Setup application. **NOTE:** The user account provisioning (add, change, and delete) is now logged into DCMaint. The following changes done by technician are included: • **For communities**: ◦ Changes associated with community, for example, adding/ moving/ renaming a community, updating/removing bandwidth throttling , updating/removing branding , registration status changes, digital licensing changes etc. • **For accounts**: ◦ Changes associated with accounts, for example, updating account configuration, account status, password, contact information etc.
Application event log	Contains event entries that notify the user of an occurrence detected by the operating system or the applications that run on the Data Center server. An event includes the following information: Type of event Date and time that the event occurred

Log	Description
	The computer on which the event occurred Event ID Event category The source of the event You can use the Application event log to troubleshoot and monitor the performance and behavior of the Data Center server and the Data Center application. Standard Windows log file.
Data Center component trace log file	Trace log files provide a deeper level of detail that helps Support diagnose problems. Support uses trace logs to assist users with problems. Trace logs do not come with a standard Data Center configuration. To enable this level of log files, contact Support.

Event messages hierarchy

The Data Center generates event messages in the following order:

- The Application event log contains only event messages specifically designated for the Application event log.
- The DCMaint event log contains event messages specifically designated for the DCMaint event log **and** repeats the event messages that are designated for the Application event log.
- If trace flags are turned on for a Data Center component, the trace log file for the component contains the following messages:
  - Event messages specifically designated for the trace log
  - Event messages designated for the DCMaint event log for that component
  - Event messages designated for the Application event log for that component

Maintain the event logs

This section explains how to maintain the following types of event logs:

- Application event logs
- DCMaint logs

Maintain the application event log

If the addition of an event causes the Application event log to exceed its limit (for example, 50 MB), and if the properties of the Application event log are set to not overwrite events, the Data Center backs up the Application event log file. The Data Center then clears the event log, and adds an informational

message to the log. The message indicates that the event log was backed up and cleared because of space limitations.

The string value **LogFileDir** under the **BackupDataCenter** key in the Windows registry specifies the location to which the Agent backs up the Application event log file. The key is in the following registry location:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Connected\BackupDataCenter

The Data Center names the file according to the following format:

```
NTApp TimeStamp.evt
```

For example, `NTApp 2003-10-01 092345.evt`.

> **NOTE:**
> To backup and clear the Application log, the Data Center must send the message that causes the log to exceed its limit.
>
> For example, if a different server component, such as SQL Server, fills the log, the Data Center does not save the log. You must save and clear the log manually.

Maintain the DCMaint log

If the DCMaint log becomes full, and if the properties of the DCMaint event log are set to not overwrite events, the Data Center backs up the log file and clears the log. The system generates an informational message in the DCMaint event log. The message indicates that the DCMaint event log was backed up and cleared because of space limitations. You can save the log because only the Data Center software writes to the DCMaint event log.

The Data Center performs other maintenance of the DCMaint log upon initialization such as a comparison of the event log size and age to the Windows registry values **MaxSize** and **LogFileTime**. The Data Center also backs up and clears the log if either value exceeds the defined limits.

The string value **LogFileDir** under the **BackupDataCenter** key on the Windows registry specifies the location to which the Agent backs up the DCMaint event log file. The key is in the following registry location:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Connected\BackupDataCenter

The Data Center names the file according to the following format:

```
DCMaint TimeStamp.evt
```

For example, `DCMaint 2003-10-01 092345.evt`.

Data Center protocol session log

The Data Center Protocol Session log (DataCenter.log) records messages that the Data Center sends and receives during backups. Corporate Support and Data Center technicians can use this log and the Agent Protocol Session log to troubleshoot problems that might occur when the Data Center and the Agent communicate during backups. For example, if a problem occurs during backup, the Data Center technician can view both the Agent Protocol Session log and the Data Center Protocol Session log to

determine if the Data Center received all messages sent by the Agent, and the reverse. You can view the Data Center Protocol Session log in a standard text editor such as Notepad.

The Data Center technician can use the Backup Server Properties table on the Data Center Management Console (DCMC) to turn on the Data Center Protocol Session log for specific accounts on a backup server, and to specify the following information:

- Location of the log file
- Level of logging
- Maximum log file size
- Number of log files to keep.

Enable the Data Center protocol session log

The Data Center session log can be configured by the DCMC technician for the following options:

- **Info**. Standard level of logging, captures more information, not for troubleshooting, more for maintenance.
- **Debug**. Detailed level of logging, captures only error messages, troubleshooting.

Data Center protocol log maintenance

The Data Center records session information in one log file unless you specify a different number of log files to keep.

For example, if you specify three log files with a maximum of 8 MB, the Data Center logs information according to the following rules:

- The Data Center stores session information in the DataCenter.log files until the size of the file reaches 8 MB.
- The Data Center renames the log file to `DataCenter.log.1`, and then creates a new `DataCenter.log` file and records the most recent events to the new file.
- When the new `Data.Center.log` files reaches 8 MB, the Data Center renames `DataCenter.log.1` to `Data Center.log.2`, and then renames the `DataCenter.log` to `DataCenter.log.1`. It then creates a new `DataCenter.log` file and records the most recent events to this file. The files are in the location that you specify with the newest log listed first:
  - `DataCenter.log`
  - `DataCenter.log.1`
  - `DataCenter.log.2`

When all three logs are full, the following actions occur:

- The Data Center deletes `DataCenter.log.2`.
- Then, the Data Center renames `DataCenter.log.1` to `DataCenter.log.2`.

- Then, the Data Center renames `DataCenter.log` to `DataCenter.log.1` and then creates a new `DataCenter.log` file.

If a problem occurs during backup, the technician can view both Protocol Session logs to determine whether the Data Center received all messages that the Agent sent.

The DCMC technician specifies the directory for the Data Center Protocol Session log. By default, the Data Center Protocol log is on the Backup Server Properties tab on the DCMC. The string value **LogFileDir** under the **AccountLogging** key in the Windows registry specifies the location to which the Agent backs up the protocol session log file. The key is in the following registry location:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Connected\AccountLogging

> **NOTE:**
> Protocol Session logging is optional. By default, the Protocol Session log is disabled for every account.

Chapter 10: Performance monitoring for Data Center services

This chapter describes performance monitoring for Data Center services.

Overview

Performance monitoring for Data Center services measures the real-time performance of the Connected Backup Data Center.

Counters that work with Microsoft Windows Performance Monitor enable performance monitoring. Counters exist or the following Data Center services:

- BackupServer
- Compactor
- ReplicationServer
- IndexServer
- PoolServer

> **NOTE:**
> This chapter describes only the BackupServer counters. For information about other counters, contact Support.

Evaluate current Data Center capacity

You should monitor your Data Center capacity during the initial phases of deployment, as well as on a regularly recurring basis.

As you deploy the Agent to more computers, you might need to change your original hardware and software configuration. For example, more backup data from an increase in accounts might require you to add more storage space on your server(s).

Check Data Center capacity more frequently for aggressive deployments than for a slow deployments.

To determine when to check capacity, use time intervals based on milestones in your deployment. For example, check capacity when you reach 50%, 60%, 75%, and 90% of your installed projected capacity.

Perform system checks monthly to assess the following hardware and software requirements:

- CPU
- RAM
- SQL database disk partitions

CPU

For best performance, refer to the *Connected Backup Requirements Matrix* guide to determine the appropriate processor for your Data Center servers. If the server overuses the CPU, add additional processors or upgrade the existing processors to improve performance. For more information about Data Center sizing requirements, refer to *Installing the Data Center* guide.

Although CPU usage as a potential bottleneck to Data Center performance is easy to detect, it is difficult to address without a complete hardware upgrade. Certain processes (particularly compaction), however, can use a large amount of CPU resources. During these peak periods, measure CPU use.

To evaluate your server's CPU, use the System Monitor feature of the Windows Performance Monitor to determine averages during peak activity for the following metrics:

- Average CPU utilization: Processor\ % Processor Time > 80% indicates heavy CPU use.

  Generally, a healthy CPU has peaks and valleys of use, with many of the peaks at 100%. Therefore, average processor activity during peak times indicates a better reflection of true performance than the peaks themselves. The average CPU use should be less than 85%.

- System processor queue length: System\ Processor Queue Length > 2 per CPU indicates that CPUs are overwhelmed and are queuing up requests.

  Generally, there should be no more than the number of processors x 2 as an average queue.

RAM

For best performance, refer to the *Connected Backup Requirements Matrix* guide to determine the appropriate amount of RAM for your Data Center servers. To determine whether RAM limits system performance, use the System Monitor feature of your Windows Performance utility to determine averages during peak activity for the following metrics:

- Number of times Windows goes to disk: Memory\Pages/sec > 0 indicates that Windows goes to disk frequently, using disk I/O and CPU resources.

  If you keep this value close to zero, you reduce performance problems incurred if you move to disk. To resolve this issue, add more RAM to your system.

- Number of times per second that Windows has read from the paging file: Memory\Page Reads/sec > 5 indicates that you might need to add more RAM to resolve a bottleneck in your system.

SQL database disk partitions

Check the database disk partition weekly. Also, include this check in your regular assessments to evaluate factors that affect Data Center capacity. For more information, see Check for available disk space, on page 94.

BackupServer counters

The following table describes the BackupServer counters:

Counter name	Counter object name	Description
Backup Server Total Sessions	BACKUPSERVER_ TOTALSESSIONS	Total number of sessions running
Backup Server Sessions Since Startup	BACKUPSERVER_ SSESSIONSSINCESTARTUP	Total number of sessions that have run since startup of the BackupServer service
Backup Server 8.x Sessions	BACKUPSERVER_8X_ SESSIONS	Number of sessions running for 8.x Agents
Backup Server 7.x Sessions	BACKUPSERVER_7X_ SESSIONS	Number of sessions running for 7.x Agents
Backup Server Retrieve Sessions	BACKUPSERVER_ RETRIEVES	Number of retrieval sessions running for all Agents
Backup Server 8.x Retrieve Sessions	BACKUPSERVER_8X_ RETRIEVES	Number of retrieval sessions running for 8.x Agents
Backup Server 7.x Retrieve Sessions	BACKUPSERVER_7X_ RETRIEVES	Number of retrieval sessions running for 7.x Agents
Backup Server First Backup Sessions	BACKUPSERVER_ FIRSTBACKUPS	Number of first backup sessions running for all Agents
Backup Server 8.x First Backup Sessions	BACKUPSERVER_8X_ FIRSTBACKUPS	Number of first backup sessions currently running for 8.x Agents
Backup Server 7.x First Backup Sessions	BACKUPSERVER_7X_ FIRSTBACKUPS	Number of first backup sessions running for 7.x Agents
Backup Server Backup Sessions	BACKUPSERVER_ TOTALBACKUPS	Number of backup sessions running for all Agents
Backup Server 8.x Backup Sessions	BACKUPSERVER_8X_ TOTALBACKUPS	Number of backup sessions running for 8.x Agents

Counter name	Counter object name	Description
Backup Server 7.x Backup Sessions	BACKUPSERVER_7X_ TOTALBACKUPS	Number of backup sessions running for 7.x Agents

Reinstall and remove counters

You can reinstall counters without reinstalling the Data Center.

> **CAUTION:**
> Before you install the performance monitoring counters, use Microsoft Tools to back up the Windows registry. For information about Microsoft Tools, refer to the Microsoft documentation Web site.

To install the counters, you need administrator privileges for the following registry keys:

- **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\009**
- **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services**<*service_name*>

  where

  <service_name> is the name of the service that corresponds with the counter.

If you do not have privileges to modify these registry keys, the installation of the Data Center succeeds, but the installation of the counters fails. For more information, see Troubleshoot, on the next page.

For information about what to do if installation of one or more counters fails, see Troubleshoot, on the next page.

To reinstall or remove counters, use the following programs:

- BackupServerPrfInstaller
- CompactorPrfInstaller
- ReplicationServerPrfInstaller
- IndexServerPrfInstaller
- PoolServerPrfInstaller

Each set of counters has its own program. The programs are in the DataCenter installation folder.

Install counters

To install counters

1. On the Data Center computer, open a command line, and then enter the following command:

   counter_program install

   where

   counter_program is the installation program for the counters that you want to install.

   Example:

   ```
   BackupServerPrfInstaller install
   ```

2. Restart the corresponding Data Center service.

   For example, if you installed the BackupServer counters, restart the BackupServer service

3. Enable the counter.

   For more information, see Reinstall and remove counters, on the previous page.

Remove counters

To remove counters

1. On the Data Center computer, open a command line, and then enter the following command:

   counter_program uninstall

   where

   counter_program is the installation program for the counters that you want to install.

   Example:

   ```
   backupServerPrfInstaller uninstall
   ```

2. Restart the corresponding Data Center service.

   For example, if you installed the BackupServer counters, restart the BackupServer service.

Troubleshoot

This section explains how to resolve the following problems:

- Installation of the counters fails
- The counters work incorrectly

Installation of the counters fails

To install the counters, you need administrator privileges for the following registry keys:

- **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\009**
- **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services**<*service_name*>

  where

  <service_name> is the name of the service that corresponds with the counter.

If you do not have privileges to modify these registry keys, the installation of the Data Center succeeds, but the installation of the counters fails. If the installation of one or more counters fails, the Data Center installation program logs errors to the Data Center Setup log. This log is in `\Datacenter\Setup`. The following error is an example:

```
[2009-08-24 10:11:37 Info (10665)] Running program
'f:\datacenter\PoolServerPrfInstaller.exe' with arguments '-install'

Error: ERROR in CPrfData::InstallPrfData.OpenSubKey failed to open HKEY_LOCAL_
MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib. Failed with error
code: 5
```

If you receive this error, reinstall the counters, but do not install the Data Center. For information, see Reinstall and remove counters, on page 83.

Counters work incorrectly

If counters do not work correctly, they log errors that describe the problem to the DCMaint log. If a set of counters does not work correctly, remove it, and then reinstall it. For instructions, see Reinstall and remove counters, on page 83.

Chapter 11: Daily maintenance

This chapter describes the maintenance tasks that you must perform each day to ensure that the Data Center runs optimally. Because there are tasks to perform throughout the day, this chapter categorizes tasks by those to perform at the start of the day, and those to perform at the end of the day.

For a checklist that you can use to keep track of daily maintenance tasks, see Maintenance checklists, on page 105.

Tasks to complete at the start of every day

At the start of every day, complete the following tasks:

- Verify the Daily Automatic Procedure results.
- Verify personal backups.
- Verify the disk status and whether there is unknown disk space.

Verify the daily automatic procedure results

The Data Center contains a daily maintenance script, `dailymaint.sql`, that runs at 12:00 p.m. every day except Sunday. This script executes the following tasks:

- Backs up the SQL transaction logs for the Directory database and Registry database. These backups happen only for stand-alone Data Centers.
- Calculates statistics on database size, account data totals, and archive storage device totals. An archive storage device is a component that stores data (for example, a SAN device).

> **NOTE:**
> If you run a mirrored Data Center configurations, either a mirrored pair or as part of a mirrored cluster, the Data Center replicates the SQL databases between the servers. Therefore, the Daily Automatic Procedure does not back up the SQL Database. In a mirrored environment, if a data loss occurs, you can restore a database from its mirror.

The `dailymaint.sql` script writes the results of the tasks it performs to two log files in the Data Center folder:

`dailymaint.out`	Contains the results for only the previous day.
`sqldump.log`	Contains an ongoing history of the Daily Automatic Procedure results.

To review the results of the daily automatic procedure

1. In the `\DataCenter` folder, open `dailymaint.out` or `sqldump.log`.
2. Review the output file for errors that might have occurred while the maintenance script was running.

   If the script runs successfully, the output file indicates the following information:

   - The Directory database and Registry database transaction logs have been backed up at the time that you specified. These backups happen only for stand-alone Data Centers.
3. To view the Application event log, open the Data Center Management Console (DCMC), expanding the **Events** node, and click **Application**.
4. Verify that no errors occurred during the daily SQL transaction logs backup.
5. If problems appear in the log files or in the Application event log, contact Support.

> **NOTE:**
> If you run a large stand-alone Data Center, you can schedule the dailymaint.sql script to run more than one time per day. If you run the script more than once a day, you reduce the risk of data loss and decrease the time required to recover a failed system.

Verify personal backups

Verify that user's personal backups complete successfully. To perform this task, you can use the Agent on any computer that backs up to your Data Center.

To verify personal backups on Mac Agents

1. Open the Agent.
2. Click the History tab and select the most recent session logs.
3. To display the log for the selected sessions, click **View Details**.
4. Verify that each session started and completed successfully.
5. Look for errors and indications of problems with the connection.

   Although these types of problems might occur occasionally, they might not indicate a persistent problem.

To verify personal backups on PC Agents

1. Open the Agent.
2. Click the date link next to **Last Backup** on the **Back Up Panel**.
3. Verify that each session started and completed successfully.
4. Look for errors and indications of problems with the connection.

Although these types of problems might occur occasionally, they might not indicate a persistent problem.

Check backup disk status and unknown disk space

Use the Disk Status tool to check the status of the backup disk.

To check disk status

1. Open the Disk Status tool and enter your Data Center name in the Server box.
2. Click **Update**.

   The Disk Status tool displays information about the status of the disk.
3. Verify that all indicators are between normal parameters (in the appropriate colored indicator).
4. Check the unknown disk space.

   The Disk Status tool displays unknown disk space in red. Files not related to the Data Center use the unknown disk space.
5. To generate a text file that lists files on the customer data volume that are unrelated to the Data Center, click **Display**.

   The text file contains columns that list the file name and the file size in bytes.
6. Move or delete these files to allow more space for the Data Center files.

Tasks to complete at the start and end of every day

Perform the following general tasks at every start and end of every day:

- Verify that services are running.
- Examine the Windows event log.
- Verify that Support Center and MyRoam are running.
- Check Copy on Reference and replication.

Verify that the services on the Data Center server are running

To verify that the services are running

1. Open DCMC and expand your Data Center node in the Console tree.
2. Do one of the following:

- If you do not see your Data Center in the Console tree

  a. Right-click **Data Centers**, and then click **Add a Data Center**.

  b. In the **Data Centers** window, select the appropriate configuration for your Data Center, and then type the Data Center or server name (whichever required, based on your configuration selection).

- If you see your Data Center in the Console tree, continue to the next step.

3. To view the status of the services, in the Console tree, click the name of the Data Center server.

   The Console tree displays the following services:

   - BackupServer
   - DCAlerter
   - ReplicationServer
   - IndexServer
   - PoolServer
   - Compactor

4. To restart a service that has stopped

   a. In the left pane, expand the Data Center server name that runs the service.

   b. Right-click the service.

      A dialog box opens.

   c. Click **Start Service**.

If your request to start the service fails, the Data Center sends a message to the Application event log.

To verify the status of the Compactor service

1. Expand the **Events** node.
2. To view event messages, click **DCMaint**.
3. Look for messages with Compactor under the **Source** column.
4. Do one of the following:

- If the Data Center writes warning or error messages to the log file, examine the Compactor log in the Log Files folder and the compaction date appended to the file name.
- If the Data Center does not write warning or error messages to the log, for details on logging and trace logs, see Manage the Data Center with DCMC, on page 62.

Examine the Windows event log

To examine the Windows event log for warning messages or error messages

1. Open the DCMC.
2. In the left pane, expand the Data Center server name.
3. Expand the **Events** node, and click **Application**.
4. Look for warnings and errors in the log window and review them to determine what actions you must take. For more information about how to respond to error messages, contact Support.

Verify that Support Center and MyRoam Are running

To verify that Support Center and MyRoam are running

> **NOTE:**
> The steps to verify MyRoam apply only if your enterprise uses MyRoam for PC Agents.

1. To verify that the IIS Admin Service and the WWW Publishing Service run, open the Services Control Panel and verify that the status is **Started**.
2. To verify that Support Center is running, log on to Support Center from a remote computer and perform a quick lookup of an account.

   The default URL for Support Center has the following syntax:

   ```
   http|https://<servername>/supportcenter
   ```

   where *servername* is the name of the Web server that hosts Support Center
3. To verify that MyRoam is running, log on to the Account Management Website from a remote computer and retrieve one or more files.

Check Copy on Reference and Replication

Copy on Reference is the process that makes copies of files that multiple users have backed up with SendOnce. Replication is the process that, in a mirrored environment, copies files from a Data Center server to it's mirror. To check Copy on Reference and replication, you must check values in DCMC against previously noted values. Therefore, keep a record of values so that you have a data history to which you can refer.

DCMC obtains the values from SQL tables in your database, which under normal circumstances, are typically empty. Because these tables are empty or nearly empty, the values in DCMC should be relatively small.

Check Copy on Reference

To check Copy on Reference

1. Open the DCMC.
2. In the left pane, expand the Data Center server name.
3. Click **PoolServer**.
4. Review and note the values for SendOnce Queue and SendOnce Status.
5. If the SendOnce Queue does not display zero, press F5 to refresh the window.

   If Copy on Reference is working, the value decreases after a few minutes. The SendOnce Queue is processed every 20 minutes by the PoolServer service.

Check replication

You must check replication on each mirrored pair of servers in the Data Center, and on both of the servers that compose a mirrored pair.

To check replication

1. Open DCMC.
2. In the left pane, expand the Data Center server name that runs the service.
3. Click the **ReplicationServer** node.
4. Review and notice the values for Database rows to replicate and Archives to replicate.
5. If the values do not equal zero, press F5 to refresh the window.
6. If replication is working, the values decrease after a few minutes.

Chapter 12: Weekly maintenance

This chapter describes the maintenance tasks that you must perform each week to ensure that the Data Center runs optimally.

For a checklist that you can use to keep track of weekly maintenance tasks, see Weekly maintenance checklist, on page 106.

Verify the results of the weekly automatic procedure

To verify the results of the Weekly Automatic Procedure

- Review the results of the weekly maintenance scripts.
- Review the Application event log.

The following sections explain how to perform these tasks.

Review the weekly maintenance scripts

The Data Center has a weekly maintenance script that runs at 12:00 p.m. every Sunday. This script carries out the following tasks:

- Performs a full backup of the SQL databases on a stand-alone Data Center.
- Collects Data Center statistics.
- Clears the transaction log on a stand-alone Data Center so that the log does not grow continuously.

> **NOTE:**
> If you run a mirrored or clustered Data Center, the SQL databases replicate the data between the servers. Therefore, the Weekly Automatic Procedure does not back up the databases.

The `weeklymaintdisk.sql` script performs the database backup to disk.

> **NOTE:**
> A weekly, full database backup to a disk can use as much disk space as the actual database. If you perform a backup to a disk, use another utility to copy the backup files to a different

> medium. Do not let a new full backup overwrite a previous full backup in case the new backup fails.
>
> Do not back up your SQL databases to the same disk partition as the original SQL databases. If you experience problems with the disk partition, you might lose the databases and the backups.

The Data Center software records the results of the weekly maintenance script to the `weeklymaint.out` file and `sqldump.log` file in the Data Center folder. The files have the following differences:

- The `weeklymaint.out` file contains only the results for the previous week.
- The `sqldump.log` file contains the results for ongoing history.

These files reside in the default `\DataCenter` folder.

Review the `weeklymaint.out` and `sqldump.log` files to verify the following information:

- Whether the database backup succeeded without errors
- Whether the Master, Model, MSDB, Directory and Registry databases have been backed up at the time specified, if you run a stand-alone Data Center
- If you run a stand-alone Data Center, whether the Directory and Registry database transaction logs were backed up at the time specified
- Whether the start and end times written at the start and end of the output file are consistent with the actual start and end times of the backups

Review the application event log

If an output file reports problems with the database backup, review the Application event log for messages that pertain to the backup.

To view the Application event log

1. Open the DCMC.
2. In the left pane, expand the Data Center server name.
3. Expand the **Events** node, and click **Application**.

   The Application windows displays a list of events.

> **NOTE:**
> If you run a large stand-alone Data Center, you can schedule the `weeklymaint.sql` script to run more often. If you increase the frequency, you can reduce the risk of data loss and decrease the time required to recover a failed system.

Weekly backup tasks

Weekly maintenance includes backing up files and folders required for a successful disaster recovery for your Data Center.

For more information about the files and information to back up for your Data Center, refer to Required Disaster Recovery Items in *Data Center Disaster Recovery* guide.

Check for available disk space

Each week, check the available disk space on the following volumes to ensure that the disk has sufficient capacity:

- Customers folder
- SQL database
- SQL database backup

Check the Customers folder

The Customers folder contains the end-user data. If you run a disk-only configuration, you can monitor the available disk space on the Customers volumes with Windows Explorer, or the Disk Status tool. For information about the Disk Status tool, see Check backup disk status and unknown disk space, on page 88.

Check the SQL database

The SQL database grows throughout the life of the Data Center.

To track the size of the SQL database

1. Open Microsoft SQL Server Management Studio.
2. In the **Object Explorer** pane, expand your Data Center server.

   A list of folders is displayed under your Data Center server.
3. Expand the **Databases** folder, then right click **Directory**, and then click **Properties**.

   The **Database Properties** window opens. Locate the Data Center Size information.
4. Under the **Select a Page** pane, select **Files**.
5. To view the path of your `.mdf` and `.ldf` files, scroll to the **Path** column. Make note of this path.
6. Open Windows Explorer, and then select **My Computer**.
7. Follow the path that you noted in step five.
8. Record the size of your `.mdf` files and `.ldf` files for weekly tracking purposes.

9. Calculate how much the used disk space grew since the previous week to determine how much disk space the databases needs for the next three months.

> **CAUTION:**
> Do not back up your SQL databases to the same disk partition as the original SQL databases. If you experience problems with the disk partition for any reason, you might lose the databases and the backups.

Check the SQL database backup

If you run a stand-alone Data Center, monitor the SQL database backup volume for available disk space weekly. Also, move the SQL backups from the disk to other media. Doing so lets you have multiple backups to restore from should a disaster occur.

Perform weekly general tasks

Perform the following general tasks weekly:

- Check system time synchronization.
- Check for updates.

Check system time synchronization

If you run a mirrored Data Center configurations, either a mirrored pair or as part of a mirrored cluster, the two servers that comprise a mirrored pair should run within 30 seconds of each other. Check the time on each server and correct discrepancies.

To check the system time

1. Open the Microsoft SQL Server Management Studio.
2. Open a connection to each mirrored server in the same window.
3. For each server, run `select getdate()`.

> **NOTE:**
> Perform this time check after you add hardware to your server(s) and after changes in standard or daylight savings time.

Check for updates

You can upgrade the Data Center, the Agent, or both. A service release includes all updates released since the last major release or service release.To check for recent software updates, visit the MySupport portal.

Chapter 13: Monthly maintenance

This chapter describes maintenance tasks that you must perform each month to ensure that the Data Center runs optimally.

For a checklist that you can use to keep track of monthly maintenance tasks, see Monthly maintenance checklist, on page 106.

Perform database maintenance

The Data Center contains a monthly maintenance script (`dbmaint.sql`) that runs the DBCC utility (`dbcc checkdb` query). The DBCC utility comes with SQL Server. The DBCC utility checks each Data Center database for the following conditions:

- Logical and physical consistency in the database
- Correctly linked indexes and data pages in tables
- Data and index pages that are consistent with corresponding extent structures
- Correctly ordered indexes, consistent pointers, reasonable data information on each page, and reasonable page offsets

When you run the monthly maintenance script, you must perform tasks that are specific to your Data Center configuration. For this reason, the Data Center Setup program does not add the monthly script to the Windows Scheduler as it does for the daily and weekly scripts, which run on a schedule. You must run the monthly maintenance script manually.

The monthly maintenance script file (`dbmaint.sql`**)**, is in the Data Center folder. To run the script, use SQL Server Management Studio.

> **NOTE:**
> Before you run the script, read the remainder of this section for important guidelines and instructions particular to your Data Center environment.

Considerations for stand-alone Data Centers

To perform maintenance on a stand-alone Data Center, you must stop the BackupServer service. Users cannot backup or retrieve files during maintenance.

The procedures contain references to *Server 1* and *Server 2*. When you follow the procedures, *Server 1* represents your Data Center server. Ignore references in the procedures to *Server 2*.

Considerations for Mirrored Data Centers

To prevent a service outage, continue to run one server in the mirrored pair while you perform maintenance on the other server. When you finish maintenance on the first server, repeat the maintenance tasks for the mirror server.

The procedures contain references to *Server 1* and *Server 2*. When you follow the procedures, consider *Server 1* and *Server 2* as the names of your Data Center servers according to the following conventions:

- *Server 1* represents the server that you shut down for maintenance.
- *Server 2* represents the server that you continue to run.

Considerations for clustered Data Centers

For the purpose of database maintenance, consider each mirrored server pair in a clustered Data Center as a separate Data Center. In other words, perform maintenance on one Data Center in the cluster (one mirrored pair), then perform maintenance again for the next Data Center in the cluster (the next mirrored pair). To save time, perform maintenance on all Data Centers in the cluster sequentially. For example, perform maintenance tasks in sequential order on one side of the cluster (such as the primary side), and then on the mirrored side.

Perform monthly database maintenance

Database maintenance comprises the following tasks:

1. Prepare the mirrored server (for mirrored and clustered Data Centers).
2. Stop all Connected Backup services.
3. Run maintenance SQL scripts.
4. Restart all Connected Backup services.

The following sections explain how to perform these tasks.

> **NOTE:**
> Perform the tasks in the order in which they appear.
>
> This process can take hours on larger Data Centers.

Step 1: Prepare the mirrored server

This procedure applies only to Data Centers that use mirrored or clustered environments.

To prepare the mirrored server

1. Open DCMC.
2. From the console tree, select *Server 2*.
3. Verify that services for *Server 2* are running.

   For more information about how to verify that services are running, seeVerify that the services on the Data Center server are running, on page 88.

Step 2: Stop the server

To stop the server for maintenance

1. Open the Data Center Management Console (DCMC).
2. In the left pane, expand *Server 1*.
3. Right-click **BackupServer**, and then select Properties.
4. In the Session Restrictions section, deselect the Allow Backups and Allow Restores check boxes.
5. Click **OK**.
6. After the number of current sessions goes to zero or stays at a consistently low number, stop all Data Center services.
7. Close the DCMC.

Step 3: Run maintenance SQL scripts

To run maintenance SQL scripts

1. Verify that the Compactor service is stopped. If it is still running, stop the process or wait until the process finishes.
2. Open Microsoft SQL Server Management Studio and connect to *Server 1*.
3. Open the SQL script `weeklymaintdisk.sql`.
4. The script file is in the Data Center folder, default location `\DataCenter`.
5. To run the SQL script, click **Execute**.
6. The system backs up the SQL databases. For more information, seeVerify the results of the weekly automatic procedure, on page 92.
7. After the SQL script finishes, run the SQL script `dbmaint.sql`.

   The script is in the Data Center folder, default location `\DataCenter`. The SQL script can take minutes or hours to complete, depending on the size of your databases.

Step 4: Restart the server

To restart the server

> **NOTE:**
> Do not restart the server until after the SQL `dbmaint.sql` script finishes.

1. To restart the services for *Server 1*
   a. Open DCMC.
   b. Expand *Server 1* in the console tree.
   c. Right-click each service, and select **Start** Service.
2. To verify that Agents can connect to *Server 1*
   a. Right-click **BackupServer**, select **All Tasks**, and click **Log Session Statuses**.
   b. Expand the **Events** node, and click **Application**.
3. To verify that backups or retrievals are in progress
   a. Use the Disk Status tool to check the available free space on the database volume. If the free space on the volume is 10 GB or less, contact Support. Do not continue until you complete this step successfully.
   b. Repeat all steps for *Server 2*.

Perform account maintenance

Abandoned accounts can clutter the Data Center and use space in the databases and archive storage. They also use up seats in the Data Center license.

To minimize clutter on the Data Center, look for the following types of accounts:

- Unowned accounts
- Unsupported Agent versions
- Duplicate accounts
- Inactive accounts
- Heavy hitters
- Invalid accounts

Unowned accounts

An account is unowned when the Data Center cannot determine ownership. You can create an unknown account if you fail to enter a name, e-mail address, telephone number, or other information during the Agent Setup and registration process.

If you can locate missing account information, enter the information on Support Center. Otherwise, cancel the account.

In time, Compactor removes unowned accounts from the Data Center.

Unsupported Agent versions

An unsupported Agent version is an account that runs a version of the Agent software that your organization no longer supports. Your organization might discontinue support for an Agent version for several reasons:

- To reduce support costs and Help Desk calls
- Because Connected Backup no longer supports the Agent version
- Because the version has known issues

When you identify accounts that use unsupported versions of the Agent, upgrade the version for those accounts. To do so, use the upgrade method that your organization employs.

Duplicate accounts

A duplicate account is an unused account because two accounts exist on the same Agent computer. Users might accidentally create a new account during the account recovery process instead of recovering an existing account. Users also might create duplicate accounts if they are unaware of the account recovery process, or if an error occurred during the recovery process that forces the user to create a new account.

You cannot use an automated method to identify duplicate accounts.

To identify duplicate accounts

1. Find multiple accounts registered for the same e-mail address or name.

   To find accounts with the same e-mail address on the Data Center, run the Last Backup report in Support Center, and then sort the results by computer name to identify the duplicate accounts.
2. Determine whether the accounts that you identified in step 1 have the same computer name.
3. Verify that the last backup activity for one account ends, and that a new account registers shortly thereafter.
4. Verify that the new account you determined in step 3 has current backup activity and that the other account does not.

Inactive accounts

An inactive account is one that has had no recorded activity over an extended period of time. An account can become inactive for the following reasons:

- Attrition
- Duplicate account
- Inactive backup schedule
- Agent removed from the computer

For best results, select an account inactivity threshold time frame. For example, if an account has not performed a backup in the past 90 days, the account is inactive. The policy created should be published for end users and Help Desk representatives and should also accommodate end users on extended absence.

Heavy hitters

The following Support Center reports examine the amount of data that each account backs up to the Data Center:

- Heavy Hitters
- Heavy Hitters Cumulative

The reports appear in the Support Center under the **Reports** node. For information about how to run and view the reports, refer to Support Center Help.

Regularly backups of large amounts of data indicate that an account backs up unnecessary data. Large backups put stress on the Data Center server, and the SQL databases.

Each organization must determine what constitutes heavy use and how to manage heavy hitters. Take steps to reduce or eliminate the load that heavy hitters put on the Data Center. Use the results from the heavy hitters reports to decide whether to exclude data from backups or to contact account owners about inordinately large backups.

Invalid accounts

An invalid account is an unstable account. Unstable accounts can occur from a failed registrations. The failure can be from a network error or another failure that did not let the system register. Invalid accounts are rare.

Verify current firmware

Occasionally, hardware manufacturers release firmware fixes and updates for issues. Check with the manufacturer of each hardware component in your Data Center for firmware updates that apply to your equipment.

Check software licensing

You initially purchased a set number of licenses for the Data Center. You can update the Data Center license for the following reasons:

- You want to deploy the Agent to additional computers.
- You want to deploy a new Agent type.
- The network interface card (NIC) on the Data Center changed.
- You installed an additional NIC.
- The license now controls access to some features.

Every server in a mirrored Data Center configurations, either a mirrored pair or as part of a mirrored cluster must have the same license. Therefore, every server must be licensed for the same features and the same number of end-user accounts.

Deploy Agents to additional accounts

If you plan to deploy the Agent to more computers, consider when you want to add more licenses.

To check for the number of available licenses

1. Open the DCMC.
2. Expand the Data Center in the Console tree and expand the primary Data Center server.
3. Expand the **Events** node, and then click **Application**.
4. Find the message that has a **License Manager** source. Event ID 9507 displays the number of seats and features that you or your has company purchased.
5. In Support Center, create a report that displays the number of active accounts.

For more information about how to request a new license, see Maintain the event logs, on the next page.

Add new NICs on the Data Center

You create each license for a Data Center server based on the HostID of the network interface card (NIC). You need a new license if the Host ID on the server changes (you install a new NIC).

To determine the new HostID associated with the new card

1. Open a command prompt window.
2. Change the directory to the Data Center folder. By default, this folder is `\DataCenter`.
3. Type hostid and press Enter.

   The following example shows a system output:

```
The HostID for the current machine is:

0050dad5a9e6
```

> **NOTE:** Provide NetBios over TCP/IP on the Data Center servers. The `HostID.exe` program requires this configuration to verify the Data Center server's MAC address correctly against the Data Center license.

For more information about how to request your new license, see to Maintain the event logs, below.

Determining HostIDs for additional NICs

Each license applies to a specific Data Center server. The association between the license and the server is based on the HostID of the server's network interface card (NIC). You can install a maximum of four NICs on your Data Center server. If your Data Center server uses multiple NICs, the license file must be aware of each NIC.

To determine the HostID of a NIC

1. Open a command prompt window.
2. Change the directory to the Data Center folder. By default this directory is `\DataCenter`.
3. Type hostid and press Enter.

   The following is an example of the system output:

   ```
   The HostID for the current machine is:

   0050dad5a9e6

   0026fal7b9r5

   0123kel8a6w2

   0475der9n3y5
   ```
4. Record the Host IDs in the table in *Installing the Data Center*.

For more information about how to request a new license, see Maintain the event logs, below.

Change the features offered to end-users

If your organization adds or removes features, request a new license to activate or deactivate features. You can use the License Request Form available through the MySupport portal to request for a license.

For more information about how to obtain a new license, refer to *Installing the Data Center* guide.

Maintain the event logs

Windows event logs record software, hardware, and system information. They provide valuable diagnostic information in case of system failure. Track your event logs to help diagnose problems in

case of system failure.

The Data Center saves and clears the Application log only if the Data Center is the application that fills the log. If a different application, such as SQL Server, fills the log, the Data Center does not save and clear it. Therefore, save and clear the Application log manually. The Data Center never saves and clears the System and Security logs.

Store at least three months of event logs. Over time, these logs might become full. Save and clear the current Application and System logs. When the Data Center detects a full DCMaint, the Data Center saves the log to the Log Files folder and clears the log.

For best performance, use *Connected Backup Requirements Matrix* to determine the appropriate log size for your Data Center servers.

You use the Microsoft Windows Event Viewer to access the event logs on the Data Center. You can also use the Event Viewer for the following actions:

- Saving event logs.
- Clearing event logs.
- Preventing the contents of the event logs from being overwritten.
- Increasing the size of the event logs.

For more information about the Event Viewer, refer to Microsoft Windows Event Viewer Help.

Verify records

To ensure that Data Center records remain current

- Examine the daily and weekly scheduled maintenance records to ensure that you performed and recorded the maintenance.
- Compile the system use records, such as the number of end-user accounts, backups, and retrievals, and publish them.
- Examine the service availability records, and compile and publish service availability statistics on a rolling twelve-month basis.
- Examine hardware maintenance records, system software upgrade records, and records of procedure that you performed on the Data Center procedures to verify that you or your staff keeps these records up-to-date.
- Examine the training records of Data Center operators to ensure that you properly train your staff.
- Verify that your vendor support contracts are current.
- When the Data Center server certificate expires after two years, replace the certificate with one that has an expiration date of five years into the future. To do so, run the Certificate Renewer utility. For more information, contact Support.

Chapter 14: Maintenance checklists

This appendix contains checklists that you can use when you perform Data Center maintenance tasks.

- Daily maintenance checklist, below
- Weekly maintenance checklist, on the next page
- Monthly maintenance checklist, on the next page

Daily maintenance checklist

This section contains a checklist of tasks to perform each day. An **M** indicates a task to complete at the start of the day, and an **A** indicates a task to complete at the end of the day. You must perform some of the tasks at both times of the day. Each step in the checklist provides a page reference in case you need detailed information for that step.

√	Morning/Afternoon	Task	Page
	M	Verify the results of the daily automatic procedure.	Verify the daily automatic procedure results, on page 86
	M	Check disk status and unknown disk space using DCMC.	Check backup disk status and unknown disk space, on page 88
	M, A	Verify that services are running using DCMC.	Verify that the services on the Data Center server are running, on page 88
	M, A	Examine the event log through DCMC for any warnings or errors that might need attention.	Examine the Windows event log, on page 90
	M	Verify personal backups by reviewing Agent logs for recent backups.	Verify that Support Center and MyRoam Are running, on page 90
	M, A	Verify that Support Center and Account Management Website are running.	Verify that Support Center and MyRoam Are running, on page 90
	M, A	Check Copy On Reference and replication using DCMC.	Check Copy on Reference and Replication, on page 90

Weekly maintenance checklist

This section contains a checklist of tasks to perform each week. Each step in the checklist also includes a page reference in case you need detailed information for that step.

√	Task	Page
	Verify the results of the weekly automatic procedure by reviewing the weeklymaint.out file with a text editor.	Verify the results of the weekly automatic procedure, on page 92
	Back up required Data Center files and information.	Weekly backup tasks, on page 94
	Check for available disk space.	Check for available disk space, on page 94
	For mirrored or clustered Data Centers: Check time synchronization between mirrored servers. Time on both servers should be within 30 seconds of each other.	Check system time synchronization, on page 95
	Visit the Micro Focus Software Support Online to check for software updates.	Check for updates, on page 95

Monthly maintenance checklist

This section contains a checklist of tasks to perform each month. Each step in the checklist also includes a page reference in case you need detailed information for that step.

√	Task	Page
	Run the database maintenance script, `dbmaint.sql`.	Perform database maintenance, on page 96
	Run Account Management SQL scripts.	Perform account maintenance, on page 99
	Verify firmware is current with manufacturer's specifications.	Verify current firmware, on page 101
	Check your software licensing by checking the License Manager event in the Application event log and comparing it to the number of accounts reported in Support Center.	Check software licensing, on page 102
	Use Windows Event Viewer to save and clear the event log.	Maintain the event

√	Task	Page
		logs, on page 103
	Verify that record keeping is up-to-date.	Verify records , on page 104

Chapter 15: Managing the SSL/TLS protocols

This chapter provides information on how to enable and disable secure communications protocols (SSL and TLS).

Deprecation of TLS 1.0

TLS 1.0 is no longer considered to be a secure version of the TLS protocol, so many corporate compliance standards require it to be disabled and a more secure version, such as TLS 1.1 or later, be used.

> **DEPRECATED:**
> TLS 1.0 has been deprecated and its official “end of life” is June 30, 2018

Secure communication for web services

Secure web communication protocols provide a way to authenticate clients and servers on the web and to protect the confidentiality of communication between clients and servers.

Support Center, Account Management Website (AMWS), and MyRoam web sites use HTTP communication with the Data Center for secure communication.

Microsoft Secure Channel (Schannel) is a security package that facilitates the use of SSL and/or TLS encryption. Schannel uses **Windows Registry settings** to enable and disable SSL/TLS communication over HTTP. You can optionally enable and disable the following protocols:

- PCT 1.0
- SSL 2.0
- SSL 3.0
- TLS 1.0
- TLS 1.1
- TLS 1.2

To ensure secure communication for Connected Backup web applications, perform the following:

• Disable PCT 1.0, SSL 2.0, and SSL 3.0 .

• Enable TLS 1.1 and TLS 1.2.

• (Recommended) Disable TLS 1.0.

Secure communication between Agent and Data Center

The secure communication between Connected Agents and the Data Center are handled using TCP. The Schannel security provider keys, described above, do not have any effect on TCP.

As of Connected Backup 8.6.3.10 and 8.8.7, the two components negotiate the highest level of communication supported by both the Agent and the Data Center. The Data Center supports TCP communication using the following protocols:

• TLS 1.0

• TLS 1.1

• TLS 1.2

The Backup Server (and other Data Center components) disable communication using SSL 2.0 and SSL 3.0.

Disable TLS 1.0

You can disable the use of TLS 1.0 for communication between the Agent and Data Center through a **Windows registry** key. To disable TLS 1.0, the **EnableTLSv10** key must be added to the **Windows Registry** and set to **zero**. Otherwise, TLS 1.0 is not disabled. The Data Center installation process does not add this key so the Data Center administrator must add it manually.

> **NOTE:**
> To disable TLS 1.0 for a mirrored pair or clustered environment, the administrator must add this key to each Data Center in the environment.

To disable TLS 1.0 communication, do the following:

1. Open Windows Registry Editor.
2. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Connected\BackupServer` registry key.
3. Create a new **DWORD** value with the name **EnableTLSv10** and set the value data to **0** .
4. Close the Registry Editor.
5. Restart the Data Center services using DCMC.

> **IMPORTANT:**
> Connected Agents prior to versions 8.6.3.10 and 8.8.7 are hard coded to use TLS 1.0. If you have any such Agents deployed in your environment, disabling TLS 1.0 will prevent those Agents from communicating with the Data Center. As a result, those Agents will no longer backup or restore data.

Index

S

T

U

V

Send documentation feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Administering the Data Center (Micro Focus Connected Backup 9.0.6)

Add your feedback to the email and click **Send**.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to swpdl.ConnectedBackup.DocFeedback@microfocus.com.

We appreciate your feedback!