Connected Backup

Software Version 9.0.3

Installing the Data Center

Document Release Date: October 2020
Software Release Date: October 2020

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 MySupport portal. Many areas of the portal, including the one for documentation, require you to sign in with a Software Passport. If you need a Passport, you can create one when prompted to sign in.

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: Size your Data Center

This chapter provides information that you can use as a guide to determine the hardware requirements for your Micro Focus Connected Backup Data Center.

- Overview, below
- Size estimates, on the next page
- Network bandwidth requirements, on the next page

Overview

The hardware requirements for your Data Center depend on the following factors:

- Your user population
- Your Agent configuration type
- Your future plans

For example, you have licenses for 5,000 users. However, you might want to deploy hardware that serves 10,000 users in order to scale the Data Center to handle more users in the future.

Use the sizing information in this chapter to determine the hardware requirements for your Data Center.

> **NOTE:**
> The assumptions in this chapter vary with each Agent account type. Also, the assumptions in this chapter are for the long term life cycle of your Data Center hardware.

Assumptions for PC accounts

The information in this chapter assumes the following about PC accounts:

- First backup of each account is 2 GB of compressed data, on average

  This number does not include common files that use SendOnce technology.
- Size per month of compressed backup data per end user is 1 GB
- Number of files in first backup is 1,750,000, on average
- Number of delta files backed up monthly is 7,500 per end user
- Average total account size is 18 GB of compressed data

Assumptions for Mac accounts

The information in this chapter assumes the following about Mac accounts:

- First backup of each account is 4 GB of compressed data, on average

  This number does not include common files that use SendOnce technology.

- Size per month of compressed backup data per end user is 1 GB
- Number of files in first backup is 300,000, on average
- Number of delta files backed up monthly is 75,000 per end user
- Average total account size is 20 GB of compressed data

Size estimates

For information about the minimum size estimates for a Data Center based on the number of PC and Mac accounts or Data Center applications, refer to the *Connected Backup Requirements Matrix* guide*.*

> **NOTE:**
> If you configure a mirrored Data Center, each server must conform to the same minimum guidelines.

For a customized sizing estimate contact your Professional Services representative.

Network bandwidth requirements

When you consider the network load that results when you run your Data Center, focus on the number of Agents you deploy. You must have sufficient network bandwidth available for the Agents to communicate with the Data Center server.

If you have a mirrored configuration for your Data Center, each Agent must have access to both of the servers if the Agent cannot connect to its primary server. The mirrored servers must have access to sufficient network bandwidth to communicate with each other.

For more information about the recommended network requirements, refer to *Connected Backup Requirements Matrix* guide.

Chapter 2: Prepare for installation

This chapter explains how to prepare your server for a Data Center installation.

Overview

Before you install the Data Center, you must complete the following tasks:

- Evaluate the appropriate configuration and licensing for your organization.
- Review Data Center server requirements.
- Review storage solutions requirements.
- Review network requirements.
- Review security requirements for your Data Center.
- Install and configure Microsoft software.
- Prepare the Support Center and Account Management Website server(s) for installation.

The following sections describe these tasks in detail. The procedures for these tasks depend on your Data Center configuration. For example, a standalone Data Center has a different configuration than a mirrored Data Center.

For Data Center hardware and software requirements, refer to *Connected Backup Requirements Matrix* guide.

To make the Data Center installation easier, and to organize your Data Center information, use the worksheets in Data Center management worksheets, on page 53 and Data Center installation worksheets, on page 57.

> **NOTE:**
> The Data Center supports the Account Management Website with MyRoam for Connected Backup Agents. If you use Legacy (7.x) Agents only, ignore all references to the MyRoam application.

Evaluate configuration and license options

Before you install the Data Center, evaluate the deployment options and select the configuration and licensing agreement that is appropriate for your information backup requirements. As part of this process, determine the following options:

- Whether to use a standalone or mirrored Data Center
- Your licensing needs
- Which features you need to deploy
- The sections in this topic explain these considerations.

Determine type of Data Center configuration

As you prepare to deploy the Data Center, decide whether to use a standalone Data Center with one server, or a mirrored Data Center. You also can use a clustered Data Center. Clustered environment can include sets of mirrored servers or standalone servers in one Data Center.

Whether you use a mirrored or standalone Data Center depends on the anticipated size of your Data Center and your hardware. For example, a mirrored configuration requires two of everything that a standalone configuration requires. The benefit of redundant data is server availability during maintenance downtime or in the event of a disaster.

Whichever configuration you select, you need additional servers to function as Web servers for Support Center, and optionally, the Account Management Website with MyRoam, Management API, and DataTransfer API, and Connected Reporting Services Web Console.

Request a license file

You purchase licenses for Agent accounts. You must also license every Data Center. Before you install the Data Center software, you must obtain a permanent license. However, if you do not have a license when you install a Data Center, the Data Center Setup program creates a temporary license that expires in 30 days.

With your Data Center license, you can access optional features, such as EmailOptimizer, that your enterprise has chosen to implement. The license software also tracks the number of licensed users on the Data Center and warns you when your contracted license agreement nears capacity.

You can use the License Request Form available through the MySupport portal to request for a license.

Review Data Center requirements

For information about specific hardware and software requirements for the Data Center, refer to *Connected Backup Requirements Matrix* guide.

Virtualization support

For more information, refer to *Connected Backup Interoperability Matrix* guide.

Recommended hardware for database backups

Standalone Data Centers use the Daily Automatic Procedure and the Weekly Automatic Procedure to back up the SQL databases. For more information, refer to *Administering the Data Center* guide. Whatever backup method you use, back up your SQL databases regularly.

If you run a mirrored or clustered Data Center, the Data Center replicates SQL data between the servers. Therefore, the Weekly Automatic Procedure does not back up the databases. The complete mirroring of the databases on a mirrored Data Center simplifies and expedites recovery from data loss.

Antivirus software and the Data Center

Before you start the Data Center, adjust your antivirus software to exclude the Data Center Customers folder and the Microsoft SQL Server database from antivirus scans. Antivirus software might confuse the compressed and encrypted archives in the Customers folder with virus signatures. Most antivirus software would isolate the archives and, as a result, corrupt them. If the archives are corrupted, the Data Center can not gain access to them and the data is lost.

Archived files that have been infected with a virus do not affect Data Center servers. The nature of the encryption and compression techniques you use during backup inoculates the virus so that it does not affect the servers. Connected Backup software, however, does not protect end users who might recover an infected file. If the Agent backs up a file that is infected, the Agent recovers the file as infected. The only way to accurately detect and remedy infected files is to use antivirus software to scan the Agent client computer.

Review storage solutions requirements

To expand available archive storage, add a secondary storage device to your Data Center. The Data Center supports the Disk (primary) storage.

Disk storage solutions

The Data Center supports the following disk-based solutions for primary storage:

- Network Attached Storage (NAS)
- Storage Attached Network (SAN)
- Direct Attached Storage (DAS)

Network Attached Storage

If the Data Center uses NAS devices for archive storage, follow the instructions from the NAS vendor to install and connect the device to the Data Center servers.

The Data Center uses universal naming convention (UNC) paths and the Microsoft Common Internet File System (CIFS) to address NAS devices. The Data Center installation prompts you for the share name of the NAS device on the Data Center server. To keep track of this information, see Data Center installation worksheets, on page 57.

> **CAUTION:**
> Do not install the SQL Server database files on a NAS device. Microsoft and NAS vendors support this configuration, but they do not support the Data Center.

The Data Center domain account, CNTD_DCServices, must have full permissions on the NAS volume. For more information, see Review security requirements, on the next page.

Storage Attached Network

The Data Center views Storage Attached Network (SAN) as a logical drive. If you use a SAN with your Data Center configuration, during Data Center Setup, select the drive letter associated with the SAN as the Customers volume.

Unlike NAS devices, you can install the SQL database files on a SAN, but it is not required. A SAN does not require that you give permissions to the CNTD_DCServices account because Data Center Setup configures the CNTD_DCServices account to gain access to the Customers folder on the SAN.

> **NOTE:**
> Do not modify these settings unless directed by Professional Services or Support.

Review network requirements

The Agent must be able to communicate with the Data Center. Also, if you run a mirrored configuration, the Data Center servers must be able to communicate with each other. For information on network bandwidth requirements, refer to *Administering the Data Center* guide.

When you set up a mirrored pair, assign a unique IP address, or optionally a DNS name, to each server. Before you install the Data Center software, establish connectivity between the pair of servers.

In addition, configure the following network requirements:

NetBios Over TCP/IP	On the Data Center computer, enable NetBios over TCP/IP. The `HostID.exe` program requires this configuration to verify the Data

	Center server's MAC address against the Data Center license.
Ports	If you protected your domain with a firewall, you must configure the firewall to permit the Agents, Data Center, and Web servers to contact one another. For more information, see Configure your firewall, on page 26.
File and Printer Sharing for Microsoft Networks	Enable the **File and Printer Sharing for Microsoft Networks** property on the network connections that the Data Center uses. If you do not enable this property, some backup and replication components do not work.

> **NOTE:**
> To enable the IPv6 connectivity between the PC Agent and Data Center, you must enter the **DNS Host Name** in the **Agent Connections Network Interface** wizard during the Data Center Installation.

Review security requirements

The Data Center uses Windows authentication and logons to run its services and to connect to SQL Server. The Data Center installation software creates three domain accounts, each with few permissions, to run the Data Center services and components.

During installation, Data Center Setup creates these accounts as least privilege accounts, and uses the names and passwords that you specify to create these accounts. The permissions assigned to these accounts are specific to their functionality. To change the names of these accounts, be sure to keep track of the new name and password of each account for future use. Choose account names that accurately reflect the purpose of the account. Alternatively, you can accept the default account names created during installation.

Domain accounts

The Data Center installation creates several domain accounts.

Default Account Name	Purpose
CNTD_ DCServices	Used to run BackupServer, PoolServer, DCAlerter, ReplicationServer, IndexServer, Compactor.
CNTD_ WebServices	Used by Connected Web Services applications: • Support Center (32-bit) • Account Management Website (32-bit and 64-bit) • DataTransfer API (64-bit)

Default Account Name	Purpose
	- Management API (64-bit) applications.
CNTD_ DataBundler	Used to run DataBundler. For more information about how to install and invoke DataBundler, refer to *Administering the Data Center* guide.
CRSServices	Used to run Connected Reporting Services ETL jobs. Add the service account running the ETL jobs on Connected Reporting Services to each Connected Backup Registry database server's CRSServices role in SQL Server. Refer to the *Connected Reporting Service Installation* guide for more information.

You can create domain accounts before you run Data Center Setup. However, the accounts must be in the same domain, especially in a mirrored configuration where servers must communicate with each other.

> **IMPORTANT:**
> To log on to the server, use an account that has local administrator privileges and the permission to create domain accounts that can run Data Center Setup. If you do not, the accounts that you created do not have the necessary permissions to start services, authenticate attempts to log on to Support Center and Account Management Website, or run DataBundler.

You can create the domain accounts either manually or automatically. Data Center Setup prompts you to provide a password for each account.

> **CAUTION:**
> The domain accounts that Data Center Setup creates to run the Data Center have few permissions. Do not use these accounts to log on to the Data Center server.

Domain account for SQL Server

To run Microsoft SQL Server, you need a domain account with local administrative privileges that has a strong password. For more information, see Install and configure SQL Server, on page 17.

Group Policy Objects (GPO) considerations

If you use Group Policy Objects (GPO) to harden your server with 64-bit Connected Backup to meet PCI standards, the Data Center Setup application cannot create Windows Scheduled Tasks for the DailyMaint, WeeklyMaint or LDAPSyncher applications during the installation process.

Micro Focus recommends that you disable the GPOs or remove the server from the organizational unit (OU) during the Data Center setup process. This prerequisite ensures that the Data Center Setup application can create Windows Scheduled Tasks for the DailyMaint, WeeklyMaint or LDAPSyncher applications during the installation process, as required.

Enable the TLS protocol

Connected Backup version 9.0.3 supports TLS 1.0 , 1.1, and 1.2 for encrypting traffic. You must enable the same version across all servers.

SSL 2.0 and 3.0 must be disabled across all servers.

> **NOTE:** Ensure that, in a system on which you have installed the AMWS or Support Center, disable any weak and vulnerable cipher having a block size of 64-bits, such as Triple DES. Also disable all RC4 ciphers such as TLS_RSA_WITH_RC4_128_SHA and TLS_RSA_WITH_RC4_128_MD5 and other ciphers such as TLS_RSA_WITH_AES_256_CBC_SHA (0x35), TLS_RSA_WITH_AES_128_CBC_SHA (0x2f), TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014), and TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013).

Install and configure Microsoft Windows

Before you install the operating system or SQL Server, verify that the server meets the Data Center software requirements. For more information about Data Center software requirements, refer to *Connected Backup Requirements Matrix* guide.

When you install the required software, follow the guidelines in the rest of this chapter to prepare your server for a Data Center installation.

Windows Server installation guidelines

When you install Windows Server, use the following guidelines to prepare the Windows server for a Data Center installation:

1. Set the default locale and the current locale of the Windows server to **English (United States)**.

   For more information about how to set the regional settings, refer to Windows Help.

2. When Windows Server Setup prompts you about disk partitions, perform the following tasks:

   - Delete any disk partitions, even if you remove a system partition. However, do not delete any proprietary computer vendor partitions you created for configuration purposes (for example, an EISA partition).

   - Create a boot partition large enough for the operating system, Data Center application, and SQL Server.

     RAID or other redundant storage works best for the boot partition, but not essential.

   For more information about partition sizing, refer to *Connected Backup Requirements Matrix*guide and the Microsoft support Web site.

3. Install Windows in the new partition. Specify NTFS formatting for the system or boot partition.

4. When Windows Server Setup prompts you about the licensing modes, select the license option best suited for your Microsoft Windows purchase.
5. When you choose names for your Data Center server(s), do not use the words “backup” and “update” (and other keywords that Microsoft SQL Server uses) as part of the server name.

   If you use these words in the server name, it causes problems when the Data Center software attempts to perform SQL queries. Also, do not use special characters, such as a hyphen (-), in the server name.
6. When you install Windows Server, select the following options:
   - Typical settings.
   - Add the server to the appropriate domain during the initial Windows Server installation.
   - Install IIS separately after you install the server.

     For more information about how to install IIS, refer to Windows Help.
7. When Windows Server Setup prompts you for the network protocols, ensure that the TCP/IP protocol is selected.
8. If this server hosts any Connected Web Services applications, install IIS.

   For more information about how to prepare your Web server, see Web server preparation, on page 19.

Windows Server configuration guidelines

After you install Windows Server, configure and prepare the server for the Data Center installation:

- Create data partitions.
- Synchronize date and time.
- Verify mirrored servers (for mirrored configurations).
- Verify the connection for remote computers.
- Make emergency repair disks.

Create data partitions

To store your SQL databases and archive files, create data partitions. Use the following best practices partition map as you configure your Data Center server:

Partition	Contents
C:	Operating system, PAGEFILE, applications (including Data Center and SQL Server)
D:	SQL databases (.mdf files)
E:	SQL transaction logs (.ldf files)

Partition	Contents
F:	Database file backups
G: and higher	Archives

Each partition should represent a completely separate hard drive. You can combine partitions, such as placing the SQL databases and transaction logs on the same partition, but this reduces Data Center performance and causes more risk of loss if a hard drive is lost due to disaster.

For more information about how to move the SQL transaction logs to a separate partition after a Data Center installation, contact Support.

If necessary, use the following guidelines to modify the archive partitions:

- The CNTD_DCServices account must have the Change permission. The CNTD_CDMaker account must have the Read permission. The account used to log on to the Data Center must have administrator privileges that grant full permissions to these shares.
- Any accounts with access to the user’s archives, such as those accessed by DataBundler, must be in the same domain.

Synchronize Date and Time Settings

If you run a mirrored Data Center configuration, set the date and time for the mirrored server to be the same as the date and time on the first Data Center server.

If you run a clustered Data Center configuration, set the date and time for each pair of servers to be the same as the date and time as the Registration Master pair of Data Center servers.

All servers in a mirrored or clustered Data Center configuration (regardless of geographic location) must have the same time zone and daylight savings settings.

All servers in a mirrored or clustered Data Center configuration (regardless of geographic location) must run the same time zone and daylight savings rules (DST2007 patch installed or not installed).

You must synchronize the time values, which can be different by a maximum time of 30 seconds. If the time values differ by more than 30 seconds, errors occur.

> **NOTE:**
> To synchronize the time between the two servers, use any time-synchronization tools that run as a service under Windows.

Verify mirrored servers

If you run a mirrored Data Center configuration, verify that each server can write files to its mirror. On each server, map a network drive from the server to its mirror. Map the drive to the mirrored server's data partition, as explained in the section Create data partitions, on the previous page. Ensure you are logged in with a domain account that has local administrator rights on both systems, and then type the following path:

```
\\computer\driveLetter$
```

where `driveLetter` is the drive for the data partition.

Do not select **Reconnect at Login**. This network drive maps the data partition on the mirror to a drive letter on this server. Verify that you can copy files to and from the remote drive from your local drive.

Disconnect the network drive when you finish with the test. Test this process on the mirrors in each pair.

Verify the connection from remote computers

Verify that end-user computers can ping each Data Center server. If you configured your firewalls to prohibit a ping connection from a computer to the Data Center, you can skip this verification.

In a Command Prompt window on a user's computer, use the command `dsping ip` to verify that you can ping each Data Center. For example:

```
dsping 111.111.111.111
```

Verify that a computer you want to use for Help Desk tasks can connect to the Web pages on the Web server(s) for Support Center and the MyRoam application. Using Internet Explorer, open the default page on each server:

```
[http]|[https]://webServerName/supportcenter/default.aspx
```

Create an emergency repair disk

After you install and configure your servers, but before you install the Data Center software, create an emergency repair disk for each Data Center. For more information about how to create an emergency repair disk, refer to Microsoft Windows Help.

Install and configure SQL Server

Microsoft has implemented a processor-based licensing model to simplify licensing SQL Server. For an updated list of processor-based licensing models, search for Multicore Processor Licensing on the Microsoft Web site.

Connected Backup does not support the installation of SQL Server on an SQL Server farm to use with the Data Center. You must install SQL Server locally for use with the Data Center. For information about supported versions of SQL Server, refer to *Connected Backup Requirements Matrix* guide.

To configure SQL Server, follow the installation instructions provided by Microsoft. During the installation, ensure that you meet the following requirements:

- SQL Server must allow Windows authentication. Create a domain account that has local administrator privileges for SQL Server to run. Use the same login account for all SQL Servers in your Data Center.
- The Data Center server supports only the Default instance of SQL Server.
- When specifying the disk drive for the SQL Server installation path, enter the SQL database partition created using the instructions in the section, Create data partitions, on page 15.

SQL Server installation guidelines

To install SQL Server

1. Start the **Microsoft SQL Server Setup** Wizard. For information about the wizard, see Microsoft SQL Server install documentation.
2. On the **Feature Selection** page, select the following features:
   - **Database Engine Services**.
   - **SQL Server Books Online**. This feature is optional but recommended.
   - **Management Tools - Basic**.
   - **Management Tools - Complete**.

   > **NOTE:** For SQL Server 2016, you will need to install the **Management Tools** (Basic and Complete) separately as the options are not available in the **Feature Selection** page. To do this, navigate back to the Install wizard by selecting **Installation** in the left menu, click the second option, **Install SQL Server Management Tools** to start the installation process.
3. On the **Server Configuration** page, select **Use the same account for all SQL services**. If the account password does not meet security standards, the SQL Server setup application displays the following message:

   ```
   The credentials you provided for the SQL Server Agent service are invalid.
   ```

   Change the password to meet the required security standards. For more information about secure passwords, refer to the SQL Server documentation.
4. Enable **SQL Server Agent**.
5. Ensure that the SQL Server and the SQL Server Agent services run as the same Windows service account.
6. When the installation completes, apply the most recent SQL Server Service Pack.

Prepare servers for Connected Web Services applications

The Data Center software includes four Web-based applications, called Connected Web Service applications.

Account Management Website	Lets you download the PC Agent software and manage account information. If you enable the optional MyRoam application, you can retrieve files over the Internet.

DataTransfer API	Provides the ability to search, view, and retrieve files from Connected Backup accounts at the request of the Management API. This component is a private API.
Management API	Provides the single point of contact between Connected Mobility and the back-end Connected components. It receives all Connected-related requests from the app and forwards them to the appropriate component for processing. It then returns the response. This component is a private API.
Support Center	Lets you administer and manage your accounts.
Connected Reporting Services Web Console	Provides a Web-based application that lets authorized Connected Backup technicians run interactive reports against their Connected Backup Registry databases and manage subscriptions to scheduled CRS reports. For more information on Connected Reporting Services, refer to *Connected Reporting Services Installation Guide* and *Connected Reporting Service Administration Guide*.

NOTE:
If, during Data Center setup, you specify an installation path to the Data Center that contains spaces, the Account Management Website does not open. The following are examples of path names that contain spaces:

```
C:\Program Files\DataCenter
```

```
C:\Progra~1\DataCenter
```

When you specify the path to the Data Center, do not include spaces in the path name. The following is an example of a path name that does not contain spaces:

```
C:\ProgramFiles\DataCenter
```

For more information about how to create Agent configurations, refer to Support Center Help.

Web server preparation

Before you can install Connected Web Services applications, you must configure your Web server properly. Prepare the server in the following order:

Install Microsoft Windows Server

For more information, see Windows Server installation guidelines, on page 14. Verify that the Windows Server installation includes Internet Explorer version 6.0 or later.

Install Internet Information Server

For more information about how to install Internet Information Server (IIS), refer to Windows Help.

The Data Center Setup program installs Support Center and the MyRoam application to the default Web server location that you specify under the following Windows registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots

Before you install the Data Center software, you can change the location of where you want to install Support Center and MyRoam. To do so, use IIS Manager to change your Web server location.

To access Support Center and MyRoam with Anonymous Access rights, IIS installation creates a default user account named IUSER_servername. By default, this account might not have sufficient permissions to gain access to all files.

To grant yourself the correct permissions, complete one of the following tasks:

- Grant the IUSER_*servername* account Full Control permissions to the following folders:

  `\Datacenter`

  `InetPub\wwwroot\SupportCenter`

  `InetPub\wwwroot\MyRoam`

  `Temp` (depending on your operating system, either `WINNT\Temp` or `Windows\Temp`).

- Change the default account (IUSER_*servername*) to the Web Services logon account (CNTD_ WebServices) that you create during Data Center Setup. Give this account Full Control permissions to the `Temp` folder (depending on your operating system, `WINNT\Temp` or `Windows\Temp`).

Enable IIS 6 Compatibility mode

Before installing the Connected Web Services applications, you must configure the IIS 6 Compatibility mode.

To enable IIS 6 compatibility mode for Windows Server 2008

1. Click **Start**, click **Administrative Tools**, and then click **Server Manager**.
2. In Server Manager, expand **Roles**.
3. If **Web Server (IIS)** is not listed as a server role, add the role.
   a. In Server Manager, right-click **Manage Roles**, and then click **Add Roles**.

      The Add Roles Wizard opens.

   b. In the Add Roles Wizard, click **Select Role Services**.
   c. On the Select Role Services page, click **Web Server (IIS)**, and then click **Next**.

      Because of role dependency, **File Server** is selected when you click **Web Server (IIS)**.

4. If **Web Server (IIS)** is listed as a server role, add new role services.
    a. In the Roles window, scroll to the **Web Server (IIS)** section.
    b. In the Web Server (IIS) section, scroll to **Role Services**, and then click **Select Role Services**.

        The Role Services page opens.
5. On the Role Services page, expand **Common HTTP Features**, and then select the following features:
    - **Static Content**
    - **Default Document**
    - **Directory Browsing**
    - **HTTP Errors**
    - **HTTP Redirection**
6. Expand **Application Development**, and then select the following feature:
    - **ASP.NET**

    If you are prompted to add required role services, click **OK**.
7. Expand **Security**, and then select **Windows Authentication**.
8. Expand **Management Tools**, expand **IIS 6 Management Capability**, and then select the following features:
    - **IIS 6 Metabase Compatibility**
    - **IIS 6 WMI Compatibility**
    - **IIS 6 Scripting Tools**
    - **IIS 6 Management Console**
9. Click **Next**, and then click **Install**.

To enable IIS 6 compatibility mode for Windows Server 2012, Windows Server 2016, or Windows Server 2019

1. Click **Start**, click **Administrative Tools**, and then click **Server Manager**.
2. In Server Manager, expand **Roles**.
3. If **Web Server (IIS)** is not listed as a server role, add the role.
    a. In Server Manager, click **Add roles and features**.

        The Add Roles and Features Wizard opens.
    b. In the Add Roles and Features Wizard, click **Role based or feature based installation**.
    c. On the Select server roles page, click **Web Server (IIS)**, and then click **Next**.

Because of the role dependency, the following options are selected:

- **File Server** is selected when you click **Web Server (IIS)**.
- **IIS Management Console** is selected when you click **Management Tools**.

d. Click **Add features**, and then click **Next**.

4. If **Web Server (IIS)** is listed as a server role, add new role services.

   a. In the Roles window, scroll to the **Web Server (IIS)** section.

   b. In the Web Server (IIS) section, scroll to **Roles and Features** section.

   c. From the Tasks drop-down list, choose **Add Roles and Features**.

   The Select server roles page opens.

5. On the Select server roles page, expand **Common HTTP Features**, and then select the following features:

   - Static Content
   - Default Document
   - Directory Browsing
   - HTTP Errors
   - HTTP Redirection

6. Expand **Application Development**, and then select the following features:

   - **ASP.NET 4.7:** For Windows Server 2019
   - **ASP.NET 4.6:** For Windows Server 2016
   - **ASP.NET 4.5** For Windows Server 2012
   - **ASP.NET 3.5** For Windows Server 2012, Windows Server 2016, and Windows Server 2019.

   > **NOTE:**
   > Because of the role dependency, the following extensions are added:
   >
   > - When you select ASP.NET4.7, the ISAPI Filters and .NET Extensibility 4.7 are added.
   > - When you select ASP.NET 4.6, the ISAPI Filters and .NET Extensibility 4.6 are added.
   > - When you select ASP.NET 4.5, the ISAPI Filters and .NET Extensibility 4.5 are added.
   > - When you select ASP.NET 3.5, the ISAPI Filters and .NET Extensibility 3.5 are added.

   If you are prompted to add required role services, click **OK**.

7. Expand **Security**, and then select **Windows Authentication**.

8. Expand **Management Tools**, expand **IIS 6 Management Capability**, and then select the

following features:

- **IIS 6 Metabase Compatibility**
- **IIS 6 WMI Compatibility**
- **IIS 6 Scripting Tools**
- **IIS 6 Management Console**

9. Click **Next**, and then click **Install**.

Disable HTTP Verbs

To prevent providing access to sensitive information, such as authentication data or cookies, contained in the HTTP headers of the request, you must deny the following verbs:

- TRACE
- OPTIONS
- HEAD

To disable HTTP Verbs

1. Open Internet Information Services (IIS) Manager.
2. In the Connections pane, go to the connection, site, application, or directory for which you want to modify your request filtering settings.
3. In the Home pane, double-click Request Filtering.
4. In the Request Filtering pane, click the HTTP verbs tab, and then click Deny Verb... in the Actions pane.
5. In the Deny Verb dialog box, enter the HTTP verb that you wish to block, and then click **OK**.

   For example, to prevent HTTP TRACE requests to your server, you should enter "TRACE" in the dialog box. Similarly, you can follow the above mentioned steps to deny OPTIONS and HEAD verbs.

Enable the TLS protocol

Connected Backup version 9.0.3 supports TLS 1.0 , 1.1, and 1.2 for encrypting traffic. You must enable the same version across all servers.

SSL 2.0 and 3.0 must be disabled across all servers.

> **NOTE:** Ensure that, in a system on which you have installed the AMWS or Support Center, disable any weak and vulnerable cipher having a block size of 64-bits, such as Triple DES. Also disable all RC4 ciphers such as TLS_RSA_WITH_RC4_128_SHA and TLS_RSA_WITH_RC4_128_MD5 and other ciphers such as TLS_RSA_WITH_AES_256_CBC_SHA (0x35), TLS_RSA_WITH_AES_128_CBC_SHA (0x2f), TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014), and TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013).

Configure IIS for MyRoam

Use IIS Manager to verify that you enabled active server pages so that MyRoam will function properly.

To ensure that MyRoam functions properly for Windows Server 2008, or Windows Server 2012

1. Open IIS Manager.
2. Right-click the server name, and then click **Properties**.

   The Properties dialog box opens.
3. Click **MIME Types.**
4. Click **New.**
5. Add the file type `.out` with the MIME type **Application/octet-stream**.
6. To add the new MIME type, click **OK**.
7. Use Services Management to stop the IIS Admin Service and to start the World Wide Web Publishing Service.

To ensure that MyRoam functions properly for Windows Server 2016, or Windows Server 2019

1. Open IIS Manager.
2. Click the server name,
3. In **Features View**, double-click **MIME Types**.
4. In the **Actions** pane, click **Add**.
5. In the **Add MIME Type** dialog box, type a file name extension `.out` in the **File name extension** text box.
6. Type a MIME type **Application/octet-stream** in the **MIME type** text box.
7. Click **OK**.

Ensure the Microsoft Distributed Transaction Coordinator Service Is running

The Microsoft Distributed Transaction Coordinator (MSDTC) service is provided with Microsoft Windows, and enables applications to provide data from several different sources in one transaction. Use the Services Control Panel to make sure the server starts automatically when the server starts, and that it is currently started.

Prepare for integration with Single Sign-on

To support Single Sign-On (SSO) communities and technicians in your Data Center, you must configure a SSO service provider (SP) and identity provider (IdP) and integrate with the Data Center.

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

For more information on configuring SSO in your Data Center, refer to *Administering the Data Center* guide.

Chapter 3: Install Data Center software

This chapter explains how to install and configure the Data Center software on servers that have no a previous Data Center installation. For information about upgrading your Data Center if your server has a previous Data Center version installed, refer to the appropriate Connected Backup guide.

- Install the Data Center software, below
- Verify Data Center installation, on page 30

Install the Data Center software

This chapter explains how to install and configure the Data Center software on servers that do not have a previous Data Center installation.

Do not install the Data Center software until you complete all preinstallation and configuration tasks in Prepare for installation, on page 8. Before you install the Data Center, complete the worksheets listed in the appendixes of this document and have the information available to simplify the installation.

> **CAUTION:**
> Data Center Setup creates a Master Encryption Key (MEK). Store this key in a safe place. You might need the MEK if you reinstall the Data Center software.

Configure your firewall

If your domain or local computer is protected by a firewall or router, you must ensure that the Agents, Data Center, and Web servers can contact one another. This includes configuring Windows Firewall, if it is enabled on the Data Center server.

To configure your firewall, ensure that the following ports are configured for access:

Port	Connection	Description
TCP - port 80	Agent and Web server Agent and Data Center	Used to view Web services, and by Agents to back up and retrieve data to the Data Center
UDP and TCP - port 135	Data Center and Data Center	Used by Windows for server communication
UDP - ports 137 and 138	Data Center and Data Center	Used by Windows for server communication

Port	Connection	Description
TCP - port 139	Data Center and Data Center	Used by Windows for server communication
TCP - port 389	Data Center and LDAP server	Used for LDAP account authentication, without SSL
TCP - port 443	Internal to Web server	IIS to Account Management Website Apache Tomcat Connector
TCP - port 636	Data Center and LDAP server	Used for LDAP account authentication, over SSL
TCP - port 1433	Data Center and Data Center DCMC and Data Center	Used by SQL Server
TCP - port 16384	Agent and Data Center	Used by Agents to back up and retrieve data to the Data Center
TCP - port 16385	Data Center and Data Center	Used to replicate data between mirrored and clustered Data Centers
TCP - port 16386	Internal to Agent	Used to communicate between Agent and Agent Service
TCP - port 16387	Internal to Agent	Used to communicate between Agent and Agent Service (Media Mode SOAP Server)
TCP - port 16388	Internal to Agent	Used to communicate between Agent and Agent Service (background notifier)
TCP - port 16389	Internal to Web server	Used to communicate between IIS and the Tomcat service
TCP - port 16390	Internal to Web server	Used by Account Management Website Tomcat service
TCP - port 16391	Internal to Web server	Account Management Website Tomcat Shutdown Listener
TCP - port 16392	Internal to Agent	Used to communicate between Agent Compound File Analyzer (used by EmailOptimizer) and the Agent Service
TCP - ports	DCMC and	Used to view service status using RPC

Port	Connection	Description
16400 through 16406	Data Center	

Run Data Center setup

Use the Data Center Setup application to install the software.

Before You Begin

Download the appropriate version-specific Connected Backup software package from the MySupport portal to a temporary folder on a server in your environment that is accessible by all other Connected servers.

To install version 8.6.3 and later, also download the Connected Backup Management API package from MySupport portal.

To install the Data Center software

1. Log on to the server as a user with local administrator privileges.
2. In Windows Control Panel, set **Regional Options** to **English, United States** on all Data Center servers.
3. Copy the following package to the local server, and then extract its contents to a temporary location.
   - `v9.0.3.bdc.english.zip`

     This process extracts the files and folders that the installation process requires, including the Data Center Setup application, `setup.exe`.
4. Run the Data Center Setup application.

   Data Center Setup determines whether your system meets the configuration prerequisite requirements.

   If your system does not meet the requirements, Data Center Setup prompts you to correct the configuration. If your system meets the installation prerequisites, continue to follow the installation Setup wizard.
5. Follow the steps in the Setup wizard to install the Data Center.

   For each Data Center environment, you must select one of the following options:
   - To install a Standalone server or the first server in a non-mirrored cluster, select **Standalone Server**.
   - To install primary server in a clustered environment, select one of the following options:

    - **Primary server in a new cluster**: Select this option to install the primary server of the new mirror cluster.
    - **Primary server in an existing cluster**: Select this option to install a new primary server (mirrored cluster) or a new directory server (non-mirrored cluster) in an existing clustered environment.

      In the **Registry Master Server** field, enter the hostname or browse to the computer where the registry database resides.

      Select **Non-Mirrored Directory Server** checkbox to install a directory server in a non-mirrored cluster environment.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.
  - **Secondary Server**: Select this option to install the mirror or secondary server.

  Install the Data Center software and services in the following order:

  a. Primary Server

  b. Secondary Server

  If you install your Data Center in any other order, the setup fails. To correct a failed Data Center setup, you must uninstall the Data Center and begin the installation process again.

  If you have questions about any step, click **Help**.

6. After you install the software on each server in your Data Center, see Verify Data Center installation, on the next page, for a list of items to verify that you installed the software successfully.

Data Center reinstallation

If, under the guidance of Support, you must reinstall the Data Center software, you must understand what reinstallation can and cannot accomplish.

Do not reinstall the Data Center software without the guidance of Support. There are only a few reasons to reinstall the Data Center. Therefore, consult Support to confirm that reinstallation is the best solution.

After you reinstall the Data Center software, the installation affects the software and files in the following way:

- Uses the same version of the Data Center software that currently runs on the Data Center.
- Uses the MEK from the initial Data Center installation to reinstall the Data Center software.
- Has no effect on the SQL databases.
- Has no effect on the archives.
- Has no effect on the Agent configuration files.
- Modifies Windows registry settings pertaining only to Connected Backup software.
- Replaces the Data Center software application files.

- Provides privileges for Windows registry keys, file shares, file directories, and databases. Reinstallation does not take away any privileges.

Verify Data Center installation

To ensure correct Data Center operation, verify the following:

- Proper Data Center software installation
- Proper BackupServer operation
- Proper mirror site replication (mirrored or clustered configuration)

The following sections describe how to complete each of these tasks.

Verify installation of Data Center software

You must verify that you installed the Data Center software properly.

To verify the proper installation of the Data Center software

1. Log on with the same account that you used to install the Data Center software.
2. Use Services in the Windows Control Panel to verify that the following services are in the list and running:
   - Backup Server
   - Compactor
   - Index Server
   - Pool Server
   - Replication Server (if in a mirrored or clustered configuration)
   - MSSQL Server
   - DC Alerter (if used). If you did not configure the SMTP settings during installation, the DC Alerter service is disabled.
3. If the services did not start, restart the server and check the services again in Windows Control Panel Services.

   The services must start when you restart the server.
4. Verify that the services for your Data Center run from the Data Center Management Console (DCMC)**. Click Start > All Programs > Data Center** > **Data Center Management Console**.

   For instructions on how to add a Data Center to DCMC, refer to DCMC Help.
5. In DCMC, expand the **Events** node and click **Application**. Look at the events to see whether BackupServer, DCAlerter, PoolServer, ReplicationServer (if mirrored or clustered), IndexServer, and Compactor have started.

6. Verify that the event log has no warning or error events in it.
7. Verify that the `\Datacenter\setup.log` file, which records every action during the installation of the Data Center software, contains no errors.

   If you have installed a mirrored pair of Data Centers, you can see warnings from the first Data Center that it could not find its mirror. These warnings are typical before and during the time you installed the mirrored pair of Data Centers.

Verify correct BackupServer operation

To verify correct BackupServer operation, connect to the server(s) and use a test account to perform an actual backup and file retrieve.

To install a sample user account onto a client, and then backup and retrieve data

1. Use Internet Explorer to log on to Support Center.
2. In Support Center, create an Agent Setup file. Include rules that select a small number of files to back up.

   For information about how to create an Agent configuration and distribute it to clients, refer to Support Center Help.
3. Use the Agent Setup file on a client computer to install the Agent and register a new account on the Data Center.

   > **CAUTION:**
   > Do not install the Agent software on the Data Center server or Web servers that host Connected Web Services applications (such as Support Center and Account Management Website).
4. Select the Backup Set tab, select a few small files to back up, and then click **Backup Now**.

   The Agent initiates a backup and the backup completes successfully.
5. After the backup completes, retrieve a file, and then complete one of the following tasks:

   a. In a PC Agent, select the **Retrieve** panel. Wait for the files to load. Select a file to retrieve and then click **Retrieve Now**. When the system prompts you, select **Save all files in folder** and type an existing folder name in the **Retrieve Options** dialog box. Click **Retrieve** again.

      A file retrieve is initiated and completes successfully.

   b. In a Mac Agent, select the Retrieve tab, select a file to retrieve and then click **Retrieve**. The Retrieve window opens. You can either choose a new file location, or select the original location of the files to retrieve them to. After you select the location for file retrieval, select **Retrieve**.

      You should see that a file retrieve is initiated and completes successfully.
6. If you are testing a standalone Data Center, use the Windows Add/Remove Programs utility to remove the Agent from the client computer.

If you are testing a mirrored Data Center do not uninstall the Agent. You can use it for other verification tasks.

Verify mirror site replication

Unless you run a standalone Data Center, test your mirrored or clustered Data Center by verifying replication.

To verify mirror site replication

1. Open DCMC and expand your Data Center node in the Console tree.
2. Select the ReplicationServer service.
3. Examine the values of **Archives to replicate** and **Database rows to replicate**.
4. Expand the Data Center node of the other server in the mirrored pair in the Console tree.
5. Select the ReplicationServer service.
6. Examine the values of **Archives to replicate** and **Database rows to replicate**.

If the values are zero, or reduce to zero over time, the Data Center servers are replicating data.

Chapter 4: Install Web Services applications

This chapter explains how to install and configure the Connected Web Services applications on servers that have no previous Connected Backup software on them. For information about upgrading existing Connected Web Services applications, refer to the appropriate Connected Backup upgrade guide.

Review deployment requirements

Before you install Connected Web Services applications, review the following deployment guidelines:

- You must install the Data Center before you install Web Services applications.
- Support Center uses Port 80 to connect to the Data Center unless you use Single Socket Layer (SSL) encryption, which requires Port 443.
- Account Management Website (AMWS) has the following requirements:
  - In a standalone environment, AMWS can reside on its own server or the Data Center server.
  - In a mirrored or clustered environment, AMWS cannot reside on the Data Center server. It can reside on the same server as Support Center.
- Support Center has the following requirements:
  - In a standalone environment, Support Center can reside on its own server or the Data Center server.
  - In a mirrored environment, Support Center should not reside on the Data Center server. It can reside on the same server as AMWS.
  - In a clustered environment, Support Center must not reside on the Data Center server. It can reside on the same server as AMWS.
- Management API and DataTransfer API must reside either on their own servers or on the same

server. Neither component can reside on the Data Center server or any other server that hosts Connected Backup components.

If you support Connected Mobility applications, they require access to only the Management API. Therefore, if you support Connected Mobility access from the Internet and want to secure the DataTransfer API, install Management API and DataTransfer API components on separate servers. If you do not require this level of security, such as in a closed corporate environment, you can install both components on the same server.

- You must install only one instance of the Management API per cluster or standalone configuration.
- You can install multiple instances of the DataTransfer API per cluster to support horizontal scaling. The server that hosts each instance must not host any other Connected component except for possibly the Management API.
- The Management API requires and the DataTransfer API supports use of certificates to ensure secure communication with other components.

  Ensure that you have the required certificates before you install these components. For more information about creating certificates, refer to the Internet Information Services (IIS) Manager online help. The following table summarizes the certificate requirements.

Server contents	SSL required?	SSL port requirement	SSL certificate requirement
Management API only	Yes	443	Third-party trusted Certificate Authority (CA)
DataTransfer API only	No	443 (if SSL supported)	Either: • Third-party trusted CA • Site-specific (self-signed)
Management API and DataTransfer API	Yes	443	Third-party trusted CA

- If you configure the DataTransfer API to use SSL, the Common Name (CN) of the certificate of each node should match the server’s FQDN. Otherwise, the Management API will not be able to contact the node.

  If the CN does not match, after upgrade you must manually update the URL in the OutflowServices table in the Registry database to contain the CN of the server instead of its FQDN. Post-installation steps in this document provide information about how to perform this task.

  > **IMPORTANT:**
  > If you manually change the DataTransfer API URL in the Registry database to use the CN, you must change the value back to the FQDN before you reinstall this release or perform another upgrade. Otherwise, the install process will not work correctly. After you reinstall or upgrade, you must change the URL value to use the CN.

- Connected Backup version 9.0.3 supports TLS 1.0 , 1.1, and 1.2 for encrypting traffic. You must enable the same version across all servers.

SSL 2.0 and 3.0 must be disabled across all servers.

Install Web Services applications

This task provides information about how to install three of the Connected Web Services applications—Support Center, Account Management Website, and DataTransfer API. To install these applications, you use the same Data Center Setup application that you used to install the Data Center.

> **NOTE:**
> The Management API, which is also a Connected Web Services application, has its own installation application. For more information, see Install the Management API, on the next page

Before You Begin

- The Data Center Setup application requires the Connected Web Services domain account to install Connected Web Services applications. This account must be a valid domain account with local administrator privileges on the local server. By default, the name of this account is CNTD_ WebServices. You must know the password to this account before you start the upgrade process.
- Ensure that the Computer Browser service is running. This service maintains a list of computers and the resources located on the network.

To install Web Services applications with the Data Center Setup application

1. Log on to the server where you plan to install a Connected Web Services application.

   You must log on as a local administrator that has SQL Server sysadmin permissions on the Registry databases in your environment. Typically, this account is the same account that you used to install the Registry database.

2. Copy the following package from where you downloaded it to the local server, and then extract its contents to a temporary location.

   - `v9.0.3.bdc.english.zip`

   This process extracts the files and folders that the upgrade process requires, including the Data Center Setup application, `setup.exe`.

3. Run the Data Center Setup application.

   Data Center Setup determines whether your system meets the configuration prerequisite requirements.

   If your system does not meet the requirements, Data Center Setup prompts you to correct the configuration. If your system meets the installation prerequisites, continue to follow the installation Setup wizard.

4. Answer the Setup wizard prompts to install the application.

When you answer the prompts, do the following:

- In the Data Center Setup - Component Options dialog box, select the check box of the application you want to install on the current server.

  > **NOTE:**
  > For standalone environments, be sure to clear the **Data Center** checkbox.

- In the Registry Server Choice dialog box, type or select the host name of the Data Center server where the primary Registry database for the Account Management Website resides.

  Do not type the Fully Qualified Domain Name (FQDN). For example, if the server name is `webserver1.mydomain.com`, only type **`webserver1`**. If you enter the FQDN, the installation completes, but you receive the following error:

  ```
  The program could not be started. Please contact your administrator.
  ```

Answer the remaining prompts with site-specific information. For more information about selections for wizard prompts, refer to Data Center Setup Help.

If you install the Support Center or Account Management Website with the MyRoam application, the Data Center Setup application installs it in your Web server root location (by default, the `/inetpub/wwwroot` folder). If you install the DataTransfer API, the Setup application installs it in the Data Center installation folder, which by default is`/DataCenter`.

The installation process also creates a log file, `\Datacenter\setup.log`, that records every action during installation. Check this file to verify that it contains no errors.

5. (Optional) If the server hosts the DataTransfer API, encrypt the directory in which the API temporarily stores files that it retrieves from user accounts.

   To do so, enable encryption (such as EFS or full disk encryption) on the temporary directory that the DataTransfer API uses when it reconstructs users' files. By default, this directory is `C:\temp`.

   > **NOTE:**
   > If you use EFS, the system encrypts all files that the DataTransfer API writes to the temporary directory.
   >
   > To ensure that the Connected Web Services domain account (by default, CNTD_WebServices) can read these files, you must explicitly give this account the ability to decrypt files in this directory.

   For more information about configuring EFS, refer to the Microsoft EFS documentation.

6. Log off the server computer.
7. Repeat this task for each additional server that hosts a Connected Web Services application.

Install the Management API

This task provides information about how to install the Management API. You can install this component on its own server or one that also hosts an instance of the DataTransfer API. In clustered environments, install only one instance of the Management API per cluster.

Before You Begin

The Management API install application prompts for the credentials to the Connected Web Services domain account. This account must be a valid domain account with local administrator privileges on the local server: By default, the name of this account is CNTD_WebServices.

Before you install the Management API, you must do the following:

1. Add the CNTD_WebServices account to the IIS_IUSRS group, the built-in group used by Internet Information Services (IIS).
2. Give IIS_IUSERS Modify and Write permissions on the `C:\Windows\Microsoft.NET\Framework\v4.0.30319\Temporary ASP.NET Files` directory.

For more information on adding accounts to Local Users and Groups, refer to your Windows documentation

To install the Management API

1. Log on to the server where you plan to install the Management API.

   Use a local administrator account on the same domain as the Connected Web Services domain account. This account must also have SQL Server sysadmin permissions on the Registry databases in your environment. Typically, this account is the same account that you used to install the DataTransfer API.

2. Add the CNTD_WebServices account to the IIS_IUSRS group. For more information on adding accounts to Local Users and Groups, refer to your Windows documentation.

3. Copy the `v`*`9.0.3`*`.mgmtAPI.zip` package from where you downloaded it to the local server, and then extract its contents to a temporary location.

   This process extracts the Management API installation files, including the installation application, `ManagementAPIServiceInstaller.exe`.

4. Right-click the `ManagementAPIServiceInstaller.exe` file, and then select **Run as administrator**.

   The Management API Service Installer starts.

5. In the Service Configuration area, provide the following information:

   a. In the **Domain Name** box, type the name of the domain in which the Connected Web Services account resides.

      Do not type the Fully Qualified Domain Name (FQDN). For example, if the server name is `webserver1.mydomain.com`, type **`webserver1`**.

   b. In the **User Name** box, type the name of the Connected Web Services domain account that the DataTransfer API uses.

      By default, the name of this account is CNTD_WebServices.

   c. In the **Password** box, type the password for the domain account.

d. Optionally, in the **Public Server Name** box, type a base URL common name.

   This creates a registry key named **PublicServerName** at the following registry location:

   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Connected\MAPI with the following String Values:

   - **Name**. **PublicServerName**
   - **Value**. Public name of the server, including the protocol (`https`). For example: **`https://www.example.com`**.

e. Optionally, in the **SSO Service Prov. Secret** field, type the SSO service provider secret to support SSO Authentication.

   The SSO service provider secret is only necessary if the Management API server will support SSO Authentication.

   > **NOTE:**
   > The SSO Service Provider Secret must match the CB_Validation OAuth Client configured for the SSO service provider (SP).
   >
   > For more information, refer to Chapter 5 in *Administering the Data Center* guide.

6. In the **Primary/Stand-alone Server** box, type the host name of the Data Center server where the preferred Registry database for the DataTransfer API resides.

   To verify the connection to the server computer that you typed, click **Test**.

   If you use a clustered or mirrored environment, the application displays the name that it detects for the other Registry database in the **Secondary Server** box.

7. Click **Install**.

   The installation process starts and installs the API in `c:\ManagementSite\ManagementAPI`. If the install process fails, the application writes the error messages to the `InstallLog.log` file, in the local directory.

8. Log off the server.

Configure security settings

By default, the Management API and DataTransfer API components are configured to support SSL communication. The Management API requires SSL so you must install an SSL certificate on each server that hosts that component. However, if you choose not to use SSL for your DataTransfer API components, you must disable SSL support for each one in your configuration.

To configure security settings

1. Install a trusted third-party SSL certificate on the Management API server.

   For more information, see Install the SSL Certificate, on the next page.

2. Perform one of the following, depending on whether you support secure communication between

each DataTransfer API instance and the Management API:

- To support secure communication, install a trusted or self-signed certificate on each separate DataTransfer API server, and then continue with the steps in this task.

  Servers that host both components use the trusted certificate that you previously installed.

- Otherwise, disable SSL support for each instance of the DataTransfer API.

  For information, see Disable DataTransfer API support for SSL, on page 41.

3. If the Data Transfer node uses SSL and its server certificate contains a common name (CN) that is different than the server's FQDN, update the URL for the server in the OutflowServices table of Registry database to contain the CN.

   For information, see Update the Data Transfer API URL in the Registry database, on the next page.

4. To support secure communication Web-based MyRoam sessions and the Data Center, configure the Account Management Website for SSL.

   For information, see Configure the Account Management Website for SSL, on page 42.

Install the SSL Certificate

For a component to support SSL, you must use Internet Information Services (IIS) to install a server certificate on the server where the component resides.

To install an SSL certificate

1. Log on as a user with local administrator privileges to the server where you want to install the certificate.
2. Open **Internet Information Services (IIS) Manager**.
3. In the **Connections** pane, click ***serverName***.

   Where `serverName` is the name of the server computer on which you installed the Management API service.
4. In the **IIS** group, double-click **Server Certificates**.
5. If the list of server certificates does not contain the one that you want to use, install it.
6. In the **Connections** pane, expand the ***serverName*/Sites** node.

   Where `serverName` is the name of the server computer on which you installed the Management API service.
7. Click **Default Web Site**.
8. In the **Actions** pane, click **Bindings**.

   The Site Bindings dialog box opens.
9. In the Site Bindings dialog box, click **Add**.

The Add Site Bindings dialog box opens.

10. In the **Type** list, click **https**.
11. On a server that hosts only the Management API, the **Port** must be set to port 443.

    > **NOTE:**
    > Servers that host the DataTransfer API must use port 443 for SSL connections—regardless of whether the server also hosts the Management API.

12. In the **SSL certificate** list, click the certificate that you want to use, and then click **OK**.

    The Management API requires a certificate from a third-party trusted Certificate Authority (CA). The DataTransfer API supports both third-party and self-signed certificates. If the server hosts both components, install one certificate from a third-party trusted CA.

13. In the Site Bindings dialog box, click **Close**.
14. Exit **Internet Information Services (IIS) Manager**.

Update the Data Transfer API URL in the Registry database

The Registry database contains the URLs that the Management API uses to connect to each DataTransfer API server. By default, these URLs use the Fully Qualified Domain Name (FQDNs) of DataTransfer API servers.

If you configure your DataTransfer nodes to use SSL, the Common Name (CN) of the certificate must match the server’s FQDN. Otherwise, the Management API will not be able to contact the node. If the CN does not match, you must manually update the URL in the OutflowServices table in the Registry database to contain the CN instead of the FQDN.

> **IMPORTANT:**
> If you manually change the DataTransfer API URL in the Registry database to use the CN, you must change the value back to the FQDN before you reinstall or upgrade to this release again. Otherwise, the install process will not work correctly. After upgrade, you must set the value back to the CN.

To update the Data Transfer API URL in the Registry database

1. Stop Internet Information Services (IIS) on all servers that host a Connected Web Services application.

   These applications include: Support Center, Account Management Website, Data Transfer API, and Management API.

2. Log on as an administrator to the Data Center server.
3. Open the SQL query interface and connect to the Registry database.
4. Run one of the following commands, depending on whether you perform this task before or after

upgrade to this release:

- Before upgrade, reset the URL to use the server's FQDN:

  ```
  UPDATE Registry.dbo.OutflowServices
  SET Url='FDQN/ose/OutflowServiceExtension.dll'
  WHERE Url='CN/ose/OutflowServiceExtension.dll'
  ```

- After upgrade, update the URL to use the server's common name:

  ```
  UPDATE Registry.dbo.OutflowServices
  SET Url='CN/ose/OutflowServiceExtension.dll'
  WHERE Url='FDQN/ose/OutflowServiceExtension.dll'
  ```

  Where:

  - **CN**. Common Name used in the DataTransfer API certificate.
  - **FDQN**. Fully qualified domain name of the DataTransfer API server.

5. Close the SQL query interface.
6. Log off of the server.
7. On the mirrored Data Center server, repeat steps Log on as an administrator to the Data Center server., on the previous page through Log off of the server., above.
8. Restart IIS on each server.

Disable DataTransfer API support for SSL

By default, the DataTransfer API is configured to support SSL. Typically, you should use SSL to ensure that Data Center components communicate in a secure manner. However, if you do not implement SSL in your environment, such as in an intranet or non-production lab deployment, you must disable component support for SSL.

To disable DataTransfer API support of SSL

1. Log on as a user with local administrator privileges to the server that hosts the primary Registry database.
2. Open the SQL Server Management Studio, and then log in.
3. To disable SSL support for all instances of the DataTransfer API, run the following SQL statement:

   ```
   UPDATE Registry.dbo.OutflowServices SET secureFlag = 0
   ```

4. To disable SSL support for a single instance of the DataTransfer API:
   a. Run the following SQL statement to determine the server ID for a specific instance of the DataTransfer API:

      ```
      SELECT ServerId, URL FROM Registry.dbo.OutflowServices
      ```

   b. Note the `ServerId` value that corresponds to the DataTransfer node (`URL`) for which you want to disable SSL.

c. Run the following SQL statement to disable SSL:

```
UPDATE Registry.dbo.OutflowServices SET secureFlag = 0 WHERE ServerId = X
```

Where **X** is the `ServerId` value for the DataTransfer node.

5. Exit SQL Server Management Studio.
6. Log off the server.
7. In a clustered environment, repeat this task on the server that hosts the secondary Registry database.

Configure the Account Management Website for SSL

You use Secure Socket Layers (SSL) between Web-based MyRoam sessions and the Data Center to prevent unauthorized interception of user credentials. The following high-level components interact with SSL:

- Microsoft IIS (Internet Information Services) is the primary Web server that uses SSL to communicate securely with users. IIS provides security for applications hosted on the Web server.
- IIS hosts the Apache TomCat service.
- The Apache Tomcat Web server generates the Web pages for Java applications such as the Account Management Website.

> **NOTE:**
> You must modify the configurations for both IIS and Apache Tomcat so they can exchange data.
>
> The IIS service provides security for components hosted on the Web server.

Configure IIS with SSL

To configure IIS with SSL

1. Install SSL certificates on each enterprise directory server that the Data Center serves and that the Support Center server will access.
2. Configure the Web server to use the SSL certificate for communications between users and the Account Management Website.

   For more information about how to configure your Web server to use SSL for the Account Management Website, see Account Management Website registry settings for SSL communication, on the next page.

Connected Backup does not configure SSL. You must install your SSL certificate on your Windows server. Configuring SSL consists of the following high-level tasks:

- Get a certificate.
- Create an HTTPS site binding.
- Make a request to the site as a test.

For detailed information about how to add SSL certificates to a Web server, refer to Windows Help or the Microsoft Support site.

Account Management Website registry settings for SSL communication

This section describes how to configure the Account Management Website to use SSL to encrypt user communications.

Before You Begin

Ensure that you have added the SSL certificate to the IIS Server.

To enable SSL encryption for the Account Management Website

1. On the Web server, open the Registry Editor, and then navigate to the `Connected` key.

   The key is in the following registry location:

   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Connected
2. Right-click the right pane, and then select **New > Key**.
3. Type `SSWS` as the key name.
4. Right-click the right pane, and then select **New > String Value**.
5. Type `com.connected.ssw.apiServer` as the string value name, and then press `Enter`.
6. Change the value of **`com.connected.ssw.apiServer`** to the full URL of the Account Management Website server, including the `https://` prefix.

   `https://`*`serverName`*`/SSWSAPI/SSWSAPI.dll?Handler=Default`

   Where `serverName` is the name of the server on which you installed the Account Management Website.
7. Click **OK**.
8. Right-click the right pane, and then select **New > String Value**.
9. Type `com.connected.ssw.validateSSL` as the string value name, and then press `Enter`.
10. For the value of **`com.connected.ssw.validateSSL`**, type the appropriate value for your situation:
    - If you use a self-signed SSL certificate for the Account Management WebSite, type `false`, and then press `Enter`.
    - If you use an SSL certificate from an official issuing authority, type `true`, and then press `Enter`.

> **NOTE:**
> - The SSWS registry value you specify overrides a similarly named `ssw` parameter in the `DataCenter\apache-tomcat-9.0.37\webapps\ssws\WEB-INF\web.xml` file.
>
>   If you fail to add the SSWS registry value, misspell its name, or set it to `FALSE`, AMWS uses the value from the `web.xml` file. Therefore, if you encounter unexpected SSL-related behavior, verify the registry value you specified as well as the value defined in the `web.xml` file.

11. Click **OK**.
12. Close the Registry Editor.
13. Open an elevated Command Prompt window, and then type the following commands to stop, and then restart several services:

    ```
    cmd /k "net stop iisadmin & net stop w3svc & net stop dctomcat"
    ```

    ```
    cmd /k "net start iisadmin & net start w3svc & net start dctomcat"
    ```

14. Open the Data Center Management Console (DCMC).
15. Right-click **BackupServer**, select **Properties**, and then select the **General** tab.
16. Type or modify the link to the Account Management Website.

    Ensure that you enter a value that matches the value you enter in Change the value of com.connected.ssw.apiServer to the full URL of the Account Management Website server, including the https:// prefix., on the previous page. For example, `https://serverName`

17. Click **OK**, and then close the DCMC.

The communication between MyRoam sessions and the Data Center is now encrypted.

Enable MyRoam

MyRoam lets users retrieve backed-up files to any computer without the use of the Agent user interface. After users select the files that they want to retrieve, the Data Center creates a .ZIP archive file that contains the selected files. Users download this file and extract it to their computer.

To use the MyRoam application, users must log on to the Account Management Website.

License and permission requirements

To use the MyRoam application, use Support Center to enable it. You can enable the MyRoam feature in your top-level community. You also can enable or disable this feature in individual subcommunities and for Agent configurations.

To enable the MyRoam feature in one or more communities, you must install or enable the following components:

- If you host your own Data Center, you need a license for the MyRoam feature installed on the Data Center server. If your current license file does not include the MyRoam feature, use the License Request Form available through the MySupport portal to request for a license.
- To enable the MyRoam feature in a community, enable the technician permission **Allocate Licenses to Sub-Communities**.
- To enable the MyRoam feature for Agent configurations, enable the technician permission **Modify Agent Configurations**.

MyRoam installation

To install the MyRoam software, run Data Center Setup and select **Install Website with MyRoam**. For procedures that explain how to install software on the Data Center server, see Prepare servers for Connected Web Services applications, on page 18.

Enable the MyRoam feature

To enable the MyRoam feature, you must enable it for each community and each configuration in the community that needs access to this feature.

To enable MyRoam

1. Log on to Support Center using a technician ID that has the **Allocate Licenses to Sub-Communities** and **Modify Agent Configurations** permissions enabled.
2. Select the community where you want to enable the MyRoam feature.
3. On the Community Status page, click **Manage Features**.
4. On the Manage Features page, complete one of the following steps:
   a. Locate the row for the MyRoam feature, and in the Agents column, select **Enabled**.
   b. Locate the row for the MyRoam feature, and in the Agents column, select **Disabled**.
5. Click **Save**.
6. Expand the **PC Configurations** node.
7. Expand the **Website Settings** node, and then select the configuration for which you want to enable the MyRoam feature.
8. Select **Options**.
9. In the Account Management Options section, select **Allow end users to retrieve files using the MyRoam feature**.
10. Click **Finish**.

Install Connected Reporting Services (Optional)

Connected Reporting Services provides a Web-based application that lets authorized Connected Backup technicians run interactive reports against their Connected Backup Registry databases and manage subscriptions to scheduled CRS reports.

Refer to the *Connected Reporting Services Administration Guide* for more information on administering the Connected Reporting Services components.

- Optionally, install Connected Reporting Services databases and Connected Reporting Services Web Console components.

See the *Connected Reporting Services Installation Guide* for more information on system requirements and installation procedures.

Verify Web Services application installation

To verify Web Services application installation, verify the following:

- Required services are running
- Basic operation of Web Services applications

> **TIP:**
> If you cannot gain access to your Connected Web applications during the verification process, verify that network or firewall issues do not block access to the server.
>
> To verify that IIS Admin Service and World Wide Web Publishing Service started, **open Services** on Windows Control Panel.

Verify that required services are running

Use this task to verify that the required services for each Connected Web Services application are running.

To verify that the proper services are running

1. Log on to a server that hosts a new Web Services application with the same account that you used to install the application.
2. Use Services in the Windows Control Panel to verify that the following services are in the list and running:
   - IIS Admin Service
   - World Wide Web Publishing Service
   - Apache Tomcat dctomcat (on the Account Management Website server only)

3. If the services did not start, restart the server and check the services again in Windows Control Panel Services.

   The services must start when you restart the server.

4. Repeat this task on each server where you installed a Connected Web Services application.

Verify basic operation of Web Services applications

Use this task to verify basic operation of Web Services applications.

To verify basic operations of Web Services applications

1. To test Support Center operation, perform the following on a computer that does not host the application:

   a. Open a Web browser, and then type `[http]|[https]://`*serverName*`/supportcenter/`.

      Where *`serverName`* is the name of the server that hosts Support Center.

   b. Verify that the Support Center logon page opens, and that the correct version is visible at the bottom of the page.

   c. To verify that the search function works correctly, use the admin technician ID and password that you created during installation to log on to Support Center, and then search for a user account.

2. To test Account Management Website (AMWS) operation, perform the following on a computer that does not host the application or an Agent:

   a. Open a Web browser, and then type `[http]|[https]://`*serverName*`/ssws/`

      Where *`serverName`* is the name of the server that hosts AMWS.

   b. Verify that the AMWS page opens.

   c. Log on to AMWS and register a new account.

   d. Download and install an Agent on that computer.

   e. To test MyRoam, use the AMWS MyRoam function to retrieve a file.

3. To test DataTransfer API operation, perform the following on a computer that does not host an instance of the API:

   a. Open a Web browser, and then type **`[http]|[https]://`***serverName*`/ose/OutflowServiceExtension.dll/status`.

      Where *`serverName`* is the name of the server that hosts the DataTransfer API.

   b. Verify that you receive a response, in XML format, from the DataTransfer API.

   c. If your environment contains multiple instances of the DataTransfer API, repeat this step to verify each instance.

4. To test Management API operation, perform the following on a computer that does not host an instance of the API:

a. Open a Web browser, and then type `https://`*serverName*/**ManagementAPI/ManagementService.svc**.

   Where *`serverName`* is the name of the server that hosts the Management API.

b. Verify that the ManagementService Service Web page opens and that it contains the following text as the first sentence:

   ```
   You have created a new service.
   ```

The verification process is complete.

Chapter 5: Perform post-installation tasks

This chapter explains how to perform several tasks that you must perform after you install Connected Backup back-end components.

Collect required Data Center disaster recovery files

If your Data Center encounters problems, which include hardware failures or software corruption, you might have to use the disaster recovery procedures in *Connected Backup Disaster Recovery*.

To complete the disaster recovery process successfully, you need certain files from the Data Center. Collect the information and files in the Required Disaster Recovery items section of *Connected Backup Disaster Recovery*, and save them to a secure location in case you need to perform a disaster recovery procedure on your Data Center.

Move the MyRoam scratch folder

When the MyRoam application receives a request to retrieve files, it sends the request to the Data Center server. The Data Center server creates a local `Scratch` folder for each requested download. It uses the `Scratch` folder temporarily to store the rebased files that satisfy the retrieve request.

By default, the `Scratch` folder is in the Data Center installation folder (typically, `C:\datacenter)`. You might want to change the location of this folder to a drive that has a significant amount of available disk space, especially if you expect to have many or large MyRoam requests.

To change the location of the Scratch folder

1. In the location of your choice, create a new folder, named `Scratch`.
2. Delete or rename the original `Scratch` folder.
3. Open the Windows registry editor, and then change the value of the **`BackupDataCenter`** registry key to include the new location.

The key is in the following registry location:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Connected\BackupDataCenter

4. Restart the BackupServer service.

Change the Account Management Website download staging directory in Tomcat

To change the temporary storage location, `dlscratch` that Account Management Website uses in Tomcat as the download staging directory, it is necessary to add a registry key.

To change the location of the dlscratch folder

1. Open the Windows registry editor.
2. Create a new key at the following registry location:

   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Connected\SSWS
3. Create a new string value under this key, with the following string values:
   - **Name**. `com.connected.ssw.dowloadStagingDir`
   - **Value**. The new scratch location. For example: `E:\Scratch`

Configure DCAlerter

DCAlerter uses e-mail to notify designated individuals when specific events occur on the Data Center. Data Center Setup activates this feature if you specify your SMTP mail host and an administrator e-mail address during installation. If you did not enter the SMTP mail host information during Data Center setup, the DCAlerter feature is not activated. Data Center Setup installs a default set of events for notifications.

To modify the installed settings, use DCMC. For more information about how to modify the installed settings, refer to DCMC Help.

> **NOTE:**
> When you configure the DCAlerter service, verify that the anti-virus software on the server is not blocking the alerts that DCAlerter sends.

Communities and Enterprise Directory integration

In addition to the basic Data Center configuration tasks, you must create communities and technician IDs in Support Center. You may also want to integrate the Data Center with an enterprise directory.

For information about how to create communities and technician IDs, refer to *Administering Agents* guide for your operating system and Support Center Help.

For information about how to integrate the Data Center with an enterprise directory, refer to *Administering the Data Center* guide.

Manage digital certificates in Support Center

In Support Center, you can use the Manage Digital Certificate page to import and remove available digital certificates. A digital certificate is a digital signature that Windows Operating Systems use to indicate that the software that you download is secure, and that a Certificate Authority (CA) has issued the software.

> **NOTE:**
> Creating a Digital Certificate on a Mac computer is not supported for this release.

For an Agent Installation package to function and sign with a Digital Certificate, Support Center must allow HTTP traffic to sites that can verify the time stamp for the Digital Certificate.

For information about how to use the Manage Digital Certificate page and the permissions to use this page, refer to Support Center Help.

Move SQL Transaction Logs to another partition

To move SQL database transaction log (.LDF) files to a new location on the same disk volume or to a new volume, use the following procedure.

> **NOTE:**
> This procedure requires you to stop the Connected Backup services on the Data Center, which prevents your users from backing up or retrieving files.

This procedure works for any database (Directory or Registry) that the Data Center uses. Complete the procedure for each Connected Backup database on the Data Center before you move the next database transaction log.

To move SQL transaction logs to another partition

1. Use Data Center Management Console (DCMC) to stop Connected services on the Data Center.
2. Open the SQL Server Management Studio, and then select the server that has the transaction log to move.
3. Click **Connect**.
4. In the Object Explorer, expand **Databases**, and then right-click the database associated with the transaction log.
5. On the **Properties** menu, click **Tasks > Detach**.
6. Select the **Drop Connections** check box.
7. Click **OK**.

8. After you detach the database, move the .LDF file for the database to its new location.
9. In the SQL Server Management Studio, in the Object Explorer, right-click **Databases**, and then click **Attach**.
10. In the Attach Databases dialog box, to select a database, click **Add**.
11. In the Locate Database Files dialog box, navigate to the location of the database, and then select the appropriate .MDF file.
12. To accept the database selection, click **OK**.
13. If the location of the database transaction log (.LDF) file is in a different folder, click the browse **...** button in the database details section for the .LDF file for the database, and then select the appropriate .LDF file.
14. Click **OK**.
15. After you move the databases to their new locations, use the DCMC to restart the Connected services.

IIS Server Hardening Recommendations

The following are the server hardening recommendations to hide unwanted response or version headers.

X-AspNet-Version

To hide the X-AspNet-Version, perform the following steps:

1. Open the IIS Manager on the affected Windows server OS.
2. Navigate to **<*Server*> > Sites > Default Web Site > SupportCenter**.
3. In the right pane, scroll down to **Management** and double click to open the **Configuration Editor**.
4. Click the **Section** drop down and expand the **system.web**, and then select the **httpRuntime**.
5. Set the **enableVersionHeader** parameter to **False**.
6. Save the configuration.

X-Powered-By: ASP.NET

To hide the X-Powered-By: ASP.NET, perform the following steps:

1. Open the IIS Manager on the affected Windows server OS.
2. Navigate to **<*Server*> > Sites > Default Web Site > SupportCenter**.
3. In the right pane, go to **IIS** and double click to open the **HTTP Response Headers**.
4. Click on **X-Powered-By: ASP.NET** and click **Remove**.

Appendix A: Data Center management worksheets

This appendix provides worksheets to help you manage your Data Center.

- Software versions, below
- Data Center server information, on page 55

Software versions

Use the worksheets in this section to track information about your Data Center and Agents. Update the information after you upgrade the software, operating system, SQL Server, and hardware.

Data Center versions

Use the following table to track the version of the Connected Backup Data Center software that runs on your Data Center. Update the table after you install new Data Centers or update existing ones.

Server	Version	Installation date

Microsoft Windows versions

Use the following table to keep track of the Windows version that runs on the Data Center servers. Update the table after you install service packs.

Server	Version/update number	Installation date

Server	Version/update number	Installation date

Microsoft SQL Server versions

Use the following table to keep track of the version of the SQL Server that runs on the Data Center servers. Update the table after you install service packs.

Server	Version/update number	Installation date

Agent versions

Use the following table to track the version and type of the Agent deployed to each community on the Data Center. Update the table after you install new Agents or update existing ones.

Type (PC or Mac)	Community	Version	Deployment date

Data Center server information

Use the worksheets in this section to track information about your Data Center server.

Server names and IP addresses

Use the following table to track Data Center server names, IP addresses, and configuration types.

Server name	IP address	Primary/ secondary	Registration master

Licensing information

Use the following table to track the number of licenses, host IDs, and licensed features on each Data Center server.

Server name	Host ID	Number of licenses	Features

Server name	Host ID	Number of licenses	Features

Appendix B: Data Center installation worksheets

This appendix contains worksheets that you can use to record information that you need when you install the Data Center server software.

- Data Center installation worksheets, below

Data Center installation worksheets

Use the Data Center installation worksheets to record information when you install the Data Center server software.

Server names and IP addresses

Use the following table to track Server names and IP addresses that you assign to the Data Center server(s).

Server name	Server DNS name	IP adress

Logical Drive Information

Use the following table to track the drive letter and purpose for each disk drive on each Data Center server:

Drive	Contents	Size (GB)	RAID level

Drive	Contents	Size (GB)	RAID level

SQL Server Logon

Use the following table to track the Logon names and passwords (a domain account with local administrator privileges) necessary to run Microsoft SQL Server on the Data Center server(s):

Server name	User ID	Password saved?
		Saved □
		Saved □
		Saved □
		Saved □
		Saved □
		Saved □

Domain name

Name of the Windows domain where you add the Data Center server(s). You must use an account and password that has administrator privileges in this domain. You use this account to set up the server(s).

Domain:__________________________

Domain Account

Domain account that has local administrative rights to the Data Center server(s). The account should be unprivileged except on the server(s). Setup creates these accounts during installation, or you can create them.

Data Center (CNTD_DCServices, by default)**:**

Domain Account:____________________ Password Saved □

Support Center and MyRoam (CNTD_WebServices, by default)**:**

Domain Account:____________________ Password Saved □

DataBundler (CNTD_DataBundler by default)**:**

Domain Account:____________________ Password Saved □

E-mail settings

E-mail host and address information for the DCAlerter service:

SMTP Mail Host:____

Administrator E-mail Address:____

Alert Sender E-mail Address:____

Support Center administrative password

The password that you assign to the Support Center Admin Technician ID belongs to the first Technician ID that you authorize to use Support Center. It is not a Windows account name.

Support Center Admin Password Saved □

Master Encryption Key (MEK)

Encryption key that the Data Center software generates to encrypt all other encryption keys on the Data Center. Use the MEK that Data Center generates randomly by Data Center Setup or create your own. The MEK must be at least eight characters but no more than 99 characters.

MEK Saved □

NAS Storage

Network Attached Storage (NAS)

Share for the NAS: ______________________________________

Share for the NAS: ______________________________________

Share for the NAS: ______________________________________

Share for the NAS: ______________________________________

Expiration parameters

Expiration parameters, which the Data Center software prompts you for during installation. Accept the defaults if you are not sure.

Expiration Parameter	Default Value	Chosen Value
Canceled	60 days	

Expiration Parameter	Default Value	Chosen Value
Deleted	90 days disk only	
Excluded	0 (zero) days disk only	
Recent Versions	10 versions disk only	
Old Versions	45 days disk only	

Index

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 Installing the Data Center (Micro Focus Connected Backup 9.0.3)

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!