Connected Backup

Software Version 9.0.7

Upgrading the Data Center

MICRO FOCUS

Document Release Date: December 2022
Software Release Date: December 2022

Legal notices

Copyright notice

© Copyright 2017-2022 Micro Focus or one of its affiliates.

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) are as may be 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.

To check for updated documentation, visit https://www.microfocus.com/documentation/connected-backup/.

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. If you need an account, 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: Upgrade Connected Backup Components

This chapter provides information about how to upgrade Micro Focus Connected Backup components.

How the Upgrade Process Affects Users

The impact that the upgrade process has on end-users depends on the type of Connected configuration in your environment.

- **Stand-alone Data Center**. The upgrade process causes a service outage for your Connected Backup users. Schedule downtime for your users' file backup and retrieve operations.
- **Mirrored Data Center**. When you upgrade your mirrored Data Center, you must upgrade the primary server before you upgrade the secondary server. To avoid downtime for your users, the mirror server that is not being upgraded can be left running.
- **Clustered Data Center**. When you upgrade your clustered Data Center, you must upgrade the Registration Master server on the primary Data Center side before you upgrade the secondary side. To avoid downtime for your users, the mirror side that is not being upgraded can be left running.

Optional Upgrade Assistance

Micro Focus offers Professional Services to help organizations with the Connected Backup upgrade process. The intimate product knowledge of the Professional Services team can shorten

implementation time, minimize cost and complexity, and reduce risk related to the upgrade process.

For more information about scheduling a Professional Services engagement to assist you with your upgrade, including cost, contact your salesperson.

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* guide.

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

Prepare for the Upgrade

This section contains the high-level procedure and related subtasks that you must perform to prepare your environment for the upgrade process.

To prepare for the upgrade

1. Review the guidelines and recommendations for this release.

   For information about these items, see Review Upgrade Guidelines and Recommendations, below.

2. Verify the integrity of the SQL databases on all Data Center servers that host a Registry database.

   For information, see Verify Data Integrity, on page 8.

3. Download the software for this release.

   For information about how to perform this task, see Download the Software , on page 8.

Review Upgrade Guidelines and Recommendations

Before you upgrade to this release, consider the following information:

- Ensure that the servers where the Registry databases reside have the following amounts of free space on them to support the upgrade process:
  - **Transaction log (`Registry.ldf`)**. Free disk space in the amount of 10% of the current size of the Registry transaction log.
  - **Database file (`Registry.mdf`)**. Free disk space in the amount of 10% of the current size of the Registry database file.

    > **CAUTION:** Do not attempt to upgrade your Data Center if you do not have the required amount of free space for the Data Center upgrade.

- Your Data Center server must meet the system requirements for the upgraded Data Center version. For more information about these requirements, refer to the *Connected Backup Release Notes* for this release.
- If you put the databases and transaction logs on RAID 1/RAID 1+0 or SAN volumes that are optimized for transactional databases, you reduce the time required to upgrade and you improve overall system performance.

  When you perform the upgrade, the upgrade program uses the license file already on your Data Center. You do not need to obtain a new license file, unless you change the network interface card (NIC) on the Data Center. You can use the License Request Form available through theMySupport portal to request for a license.
- Adhere to the following deployment requirements:
  - You must install only one instance of the Management API per cluster or stand-alone configuration.
  - You can install the Management API and DataTransfer API on either the same server or different servers. If you support Connected Mobility applications, they require access to only the Management API.

    For example, if you support Connected Mobility access from the Internet and want to secure the DataTransfer API, install the 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 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 and DataTransfer API components support use of certificates to ensure secure communication with other components.

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

Server contents	SSL required?	SSL port requirement	SSL certificate requirement
Management API only	Yes	Any site-specified	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.

Verify Data Integrity

To verify the integrity of the SQL databases in your Connected environment, perform this task on all Data Center servers that host a Registry database.

To verify the integrity of your SQL databases

1. Open the SQL query interface and connect to the Data Center.
2. Run the `DBMaint.sql` script from the `\DataCenter\Scripts` folder.

NOTE: This procedure can take several hours.

3. Check the output for errors. If the output includes errors, do not perform the upgrade. Contact Support.
4. Close the SQL query interface.

Download the Software

Software for Connected Backupback-end components is provided in three packages:

- **`v9.0.7.bdc.english.zip`.** Contains updates to the following Connected Backup components:
  - Data Center
  - Web Services applications:
    - Support Center
    - Account Management Website
    - DataTransfer API
  - PC and Mac Agents
- **v9.0.7.mgmtAPI.zip**. Contains the Management API software.
- Optionally, software for Connected Reporting Services (CRS) is provided in a separate package. For more information on installing CRS, refer to the *Connected Reporting Service*

Installation guide.

To download the software

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

Upgrade Connected Backup

This section provides the high-level procedure that you must perform to install this release. Separate tasks in this chapter provide details about how to perform each step.

Before You Begin

If you are reinstalling this release in an environment that uses SSL certificates for your DataTransfer nodes, determine whether the Common Name (CN) in the certificate is the same as the server's fully qualified domain name (FQDN). If it is not, update each node's URL in the OutflowServices table in the Registry database to use the FQDN. Otherwise, the installation process will fail.

For information, see Update the Data Transfer API URL in the Registry Database, on page 20.

To upgrade Connected Backup

1. If necessary, upgrade your Connected Backup environment to a version that this release supports for direct upgrades.

   For the list of Connected Backup versions from which you can upgrade to this release, refer to the *Connected Backup Release Notes*.

2. Download and extract the Connected Backup software for this release.

   For more information, see To download the software, above.

3. Upgrade the Data Center.

a. Stop Data Center services.

b. Before you upgrade, back up the SQL databases.

c. For a mirrored or clustered configuration, upgrade the Registration Master and directory databases for the primary Data Center.

d. Back up the SQL databases.

e. Perform the Data Center upgrade.

For information, see Upgrade the Data Center, on the next page.

4. Upgrade the Connected Web Services applications:

- Support Center
- Account Management Website
- DataTransfer API

For information, see Upgrade Web Services Applications, on page 14.

5. For a mirrored or clustered configuration, upgrade the Registry and directory databases for the secondary Data Center.

   For information, see Upgrade the Data Center, below.

6. Install or upgrade the Management API.

   If you have not previously installed the Management API, the upgrade process provides you the option to install it.

   If the Management API is already installed, the installation process provides you the option to reinstall it.

   For information, see Install or Upgrade the Management API, on page 16.

7. On each server that hosts the Management API, configure an SSL certificate.

   This includes servers that host both the Management API and DataTransfer API. For detailed information, see Install the SSL Certificate, on page 19.

8. On each server that hosts only the DataTransfer API, either enable or disable SSL support, as required.

   By default, the DataTransfer API supports SSL. Depending on whether you want the DataTransfer API to support SSL, you must either enable SSL or disable its support for it.

- To enable SSL for the DataTransfer API, configure an SSL certificate as described in Install the SSL Certificate, on page 19.
- To disable DataTransfer API support for SSL, configure the API so that it does not require SSL. For information, see Disable DataTransfer API Support for SSL, on page 21.

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

   Refer to the *Connected Reporting Services Installation* guide for more information.

10. Verify that the application upgrades or installations were successful.

    For information, see Verify the Upgrade, on page 25.

After you have installed and verified the Connected Backup components for this release, you must configure mobile device support for user accounts. Users are unable to access their accounts with the Connected Mobility app until you perform this configuration.

For more information, refer to the *Connected Mobility Administration* guide.

Upgrade the Data Center

This section contains the high-level procedure and related subtasks that you must perform to upgrade the Data Center.

To upgrade the Data Center

1. Stop all Connected services on the Data Center server that hosts the Registry and directory databases.

In a clustered environment, also stop the Connected services of all other directory servers on the same side of the cluster.

For example, when you stop the Connected services on the primary Registration Master server of a cluster, also stop all Connected services on the primary server of each additional server pair.

For information, see Stop Data Center Services, below.

2. If you are upgrading the primary server of a mirrored or clustered configuration, direct the Web services applications to the other Data Center server with a Registry database.

   Before you upgrade the primary server, redirect Connected Web Services applications to the secondary server to prevent a service interruption to them. After you upgrade the applications, redirect them back to the primary server.

   See Redirect Web Services Applications to Another Server, on the next page.

3. Back up the SQL databases.

   See Back Up the SQL Databases, on page 13.

4. Upgrade the Registry server.

   See Perform the Data Center Upgrade, on page 13.

5. Start the Data Center and verify the upgrade.

   See Start the Upgraded Data Center , on page 13.

Stop Data Center Services

Before you upgrade the Registration Master, you must stop the Data Center services that use it.

In a mirrored or clustered environment, to ensure access during the upgrade, Data Center services on the secondary servers should remain running.

To stop the Data Center services

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

Redirect Web Services Applications to Another Server

In a mirrored or clustered environment, Connected Web Services applications are directed to the registration server of either the primary or secondary Data Center. To ensure that access to these applications remains available while you upgrade their Data Center, direct the applications to the other registration server.

You must redirect the following applications: Support Center, Account Management Website, and DataTransfer API (if installed prior to this release).

> **NOTE:** Do not use this task with stand-alone servers because there is no fail-over Data Center server to which the Web Services applications can connect.

To redirect the Web services applications

1. Log on as a user with local administrator privileges to a Data Center server where one or more Connected Web Services applications reside.
2. Open the Windows Registry Editor.
3. If the server hosts the Support Center or Account Management Website application, update the **RegistryConnect** key:
   - On a 64-bit server: **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SupportCenter**

   a. Modify the value of **RegistryConnect** to reflect the server name of the other Data Center in the pair.

      For example, SERVER1 and SERVER2 are in a mirrored pair. To upgrade SERVER1, which hosts the Registry database that the Web Services applications use, change:

      ```
      DRIVER={SQL Server Native Client
      11.0};SERVER=SERVER1;DATABASE=Registry;Trusted_Connection=Yes
      ```

      to

      ```
      DRIVER={SQL Server Native Client
      11.0};SERVER=SERVER2;DATABASE=Registry;Trusted_Connection=Yes
      ```
4. If the server hosts the DataTransfer API, update the **DB_PreferredRegistry** key:

   a. Navigate to **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Outflow**

   b. Modify the value of **DB_PreferredRegistry** to reflect the server name of the other Data Center in the pair.

      For example, SERVER1 and SERVER2 are in a mirrored pair. To upgrade SERVER1, which hosts the Registry database that the Web Services applications use, change `SERVER1` to `SERVER2`.
5. Close the Registry Editor.
6. Log off the server.
7. Repeat this task for each additional server that hosts a Connected Web Services application in your environment.

Back Up the SQL Databases

Back up all Registry and Directory SQL Server databases in your environment so that you can revert to them if the upgrade process fails.

> **NOTE:** This step can take several hours to complete. If you receive error messages or warnings during the backup, do not continue with the upgrade process. Contact Support.

To back up SQL Databases in a Stand-alone Environment

1. In Control Panel on the Data Center server, open **Scheduled Tasks**.
2. Right-click **WeeklyMaint**, and select **Run**.
3. Close **Scheduled Tasks**.

To back up SQL Databases in a Mirrored or Clustered Environment

1. Open the SQL Server query interface and connect to the Data Center.
2. Run the `database_backup.sql` script from the `\DRProcs` folder in the Data Center installation folder.
3. Close the SQL Server query interface.

Perform the Data Center Upgrade

Use the Data Center Setup application to upgrade the Data Center.

To perform the Data Center upgrade

1. Log on to the Data Center server that contains the Registry database as a user with local administrator privileges.
2. Ensure that the SQL Server service and the SQL Server Agent service run as the same Windows service account.
3. Copy the **v9.0.7.**`bdc.english.zip` package to the local server, and then extract its contents to a temporary location.

   This process extracts the files and folders that the upgrade process requires, including the Data Center Setup application, `setup.exe`.
4. Run the Data Center Setup application.
5. Answer the Setup wizard prompts to perform the upgrade.

   For information about the selections available, refer to Data Center Setup Help.
6. After the upgrade completes, click **Finish**.
7. Log off the server computer.

Start the Upgraded Data Center

After you upgrade the Data Center, you must start the Data Center services.

To start the Data Center services and verify their operation

1. Open the DCMC on the upgraded server.
2. In the left pane, expand the upgraded Data Center server name.
3. Right-click **BackupServer** and then select **Properties**.
4. In the Session Restrictions section, select **Allow Backups** and **Allow Restores**.
5. Click **OK**.
6. In a clustered environment, repeat In the left pane, expand the upgraded Data Center server name., above through Click OK., above for all other directory servers on the same side of the cluster.
7. In a clustered environment, start all Connected services on each directory server that resides on the same side of the cluster as the Registry database that you just upgraded.

   If the DCAlerter is not enabled for your environment, the DCMC displays an error when it tries to start it. You can ignore this error and close it.
8. Close the DCMC.
9. To verify that the upgrade completed successfully, use the DCMC to make sure that the following conditions exist:
   - All Data Center services are running.
   - The DCMC interface shows the correct product version number for the BackupServer service on servers that host the upgraded Registry and Directory databases.
   - The BackupServer service is accepting backups.

Upgrade Web Services Applications

This task provides information about how to upgrade the Connected Web Services applications—Support Center, Account Management Website, and DataTransfer API.

If you have not previously installed the DataTransfer API, the install application provides you the ability to install it.

> **CAUTION:** Before you upgrade the Web Services applications, you must upgrade the Data Center to the new Connected Backup version.

Before You Begin

The Data Center Setup application requires the Connected Web Services domain account to upgrade the 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.

Upgrade Web Services Applications

To upgrade Web Services applications

1. Log on to a Data Center server where one or more Connected Web Services applications reside.

   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 upgrade the Registry database

2. Copy the **v9.0.7.**`bdc.english.zip` package to the local server, and then extract its contents to a temporary location.

   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.

4. Answer the Setup wizard prompts to perform the upgrade.

   For more information about the selections during setup, refer to Data Center Setup Help.

5. In a mirrored or clustered configuration, direct the Web Services applications back to the other Data Center with a Registry database.

   For more information, see Redirect Web Services Applications to Another Server, on page 12.

6. (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.

7. Log off the server computer.

8. Repeat this task for each additional server that hosts a Connected Web Services application.

9. If you are installing a new instance of the DataTransfer API, the wizard displays several installation-specific prompts:

   - In the Data Center Setup - Component Options dialog box, select the **Install the Connected DataTransfer API** check box.
   - 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`**.

- In the DataTransfer API Settings dialog box, browse to select the location that the API uses for temporary storage.
- In the Installation Directory dialog box, browse to select the locations in which to install API-related files.

10. 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

    a. Open the Windows registry editor.

    b. Create a new key at the following registry location:

    HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Connected\SSWS

    c. 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`

      The setting was previously defined in a context parameter in `web.xml`

      ```
      <context-param>
      <param-name>com.connected.ssw.downloadStagingDir</param-name>
      <param-value>C:\temp</param-value>
      </context-param>
      ```

Upgrade the Data Center on Secondary Servers

In a mirrored or clustered environment, upgrade the secondary servers in the Data Center.

1. Redirect the Web Services to the primary servers in the Data Center.

   For more information, see Redirect Web Services Applications to Another Server, on page 12

2. Perform the Data Center upgrade on the secondary servers.

   For more information, see Perform the Data Center Upgrade, on page 13.

Install or Upgrade the Management API

This task provides information about how to install or reinstall 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.

Upgrade of the Management API is performed using the Management API Service installer to reinstall the Management API service. The installer detects that the Management API service is already installed, and prompts for reinstallation.

Before You Begin

The Management API install application prompts for the name of 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. You must know the password to this account before you start the upgrade process.

Before you install or upgrade the Management API, you must do the following if you have not previously done so:

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.

Enable the TLS Protocol

Connected Backup version 9.0.7 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.

To install or upgrade the Management API

1. Log on to the server where you plan to install or upgrade 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 upgrade 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 **`v9.0.7.`**`mgmtAPI.zip` package 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.

   If the Management API is already installed, the Management API Service installer prompts to reinstall or uninstall the Management API service.

   - Select **Reinstall the Management API service** to reinstall the Management API
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 (or `https`). For example: **`https://www.example.com`**.

e. Optionally, in the **SSO Service Prov. Secret** box, 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 computer.

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, below

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, and then skip the remaining steps in this task.

     For information, see Disable DataTransfer API Support for SSL, on page 21.

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 22

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 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 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.

   Connected Backup version 9.0.7 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).

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, below

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.

Install Connected Reporting Services

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.

Refer to the *Connected Reporting Services Installation* guide for more information on system requirements and installation procedures.

Verify the Upgrade

To verify the upgrade of Web Services applications

1. On a computer that does not host the Support Center:
   a. Open a Web browser, and then type the URL for your 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, log on to Support Center and search for a user account.
2. On a computer that does not host the Account Management Website or an Agent:
   a. Open a Web browser, and then type the registration URL of Account Management Website.
   b. Use Account Management Website to register a new account, and then download and install an Agent on that computer.
3. On a computer that does not host an instance of the DataTransfer API:
   a. Open a Web browser, and then type **[http]|[https]://*DataTransferAPIServer***/ose/OutflowServiceExtension.dll/status.

      Where ***DataTransferAPIServer*** is the name of the server where the DataTransfer API resides.
   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. On a computer that does not host an instance of the Management API:
   a. Open a Web browser, and then type **https://*ManagementAPIServer*/ManagementAPI/ManagementService.svc**.

      Where ***ManagementAPIServer*** is the name of the server where the Management API resides.
   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 is complete.

Changing default session timeout for AMWS application

Post upgrade, if you want to change the session timeout to a value different than the default one, perform the following steps:

1. Navigate to `DataCenter\apache-tomcat-9.0.37\webapps\ssws\WEB-INF` folder on the server where AMWS is installed.
2. Open the `web.xml` in a text editor.
3. Locate the `<session-timeout>` parameter in `web.xml` and change its value as per your requirement.

   The following is an example code snippet:

   ```
   <session-config>
   <session-timeout>15</session-timeout>
   </session-config>
   ```
4. Restart the Apache Tomcat dctomcat service.

Chapter 2: Uninstall Components

This chapter contains information about how to uninstall the Management API and DataTransfer API components. Although these components are required to support the Connected Mobility app, you might want to uninstall them from one server, and then reinstall them on a new server.

Uninstall the Management API

This task provides information about how to uninstall the Management API software.

To uninstall the Management API

1. Log on as a user with local administrator privileges to the server where the Management API resides.
2. Copy the `v9.0.7.mgmtAPI.zip` package 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`, which you use to uninstall the software.
3. Right-click the `ManagementAPIServiceInstaller.exe` file, and then select **Run as administrator**.

   The Management API Service Installer starts.
4. Click **Uninstall the Management API service**.

   The uninstall process starts and displays a confirmation prompt.
5. Click **Yes**.

   The application removes the Management API service.
6. If the public-facing name for this server is different than its internal server name, remove the **PublicServerName** registry key that you created for the server.
   a. Open the Windows Registry Editor.
   b. Delete the **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Connected\MAPI** key.
   c. Close the Registry Editor.
7. Log off the server computer.

Uninstall the DataTransfer API

This task provides information about how to uninstall the DataTransfer API software.

To uninstall the DataTransfer API

1. Log on as a user with local administrator privileges to the server where the DataTransfer API resides.
2. In the taskbar, click **Start**, click **Settings**, and then click **Control Panel**.

   Control Panel opens.
3. Double-click **Programs and Features**.

   The Program and Features window opens.
4. Right-click the **Data Center** entry, and then click **Uninstall**.

   A confirmation prompt opens.
5. Click **Yes**.

   The uninstall process runs and removes all DataTransfer API software from the server and all data related to the server from the Registry databases.
6. Log off the server.

Chapter 3: Upgrade Windows Server and SQL Server

This chapter explains how to upgrade your Data Center servers. The available upgrade options are with the following software combinations:

- Windows Server 2012 R2 and SQL Server 2012 SP4
- Windows Server 2012 R2 and SQL Server 2016
- Windows Server 2016 and SQL Server 2016
- Windows Server 2019 and SQL Server 2016 SP2
- Windows Server 2016 and SQL Server 2019
- Windows Server 2019 and SQL Server 2019

The following topics are explained in detail:

Upgrade Requirements

The following requirements apply to the upgrade process for stand-alone, mirrored, and clustered Data Centers:

- synchronize Connected Backup versions

  All servers in your Connected Backup configuration must have version 8.8.1 or later installed before you upgrade any Data Center servers.

- confirm which SQL Server and Windows Server versions Connected Backup supports

  For specific versions of these components and all other requirements of Connected Backup, refer to the *Connected Backup Requirements Matrix* guide.

- complete upgrade in a timely manner

  When upgrading your Data Center configuration to SQL Server, many situations can prevent you from upgrading all servers at the same time, such as unavailable hardware and software or a limited maintenance window.

To address these situations and to minimize service outages to Connected Backup users during the upgrade process, you can run your Data Center configuration with some Data Center servers running on Windows Server with SQL Server 2016 and some continuing to run with the following software combinations:

- Windows Server 2008 R2 and SQL Server 2008 R2 SP3
- Windows Server 2012 R2 and SQL Server 2012 SP4
- Windows Server 2016 and SQL Server 2019
- Windows Server 2019 and SQL Server 2016 SP2
- Windows Server 2019 and SQL Server 2019

However, we recommend that you complete the upgrade of the remaining servers to SQL Server in a timely manner.

Upgrade a Data Center Server to Windows Server

This section describes how to upgrade a Data Center server to the following Window Servers:

- Windows Server 2008 R2 to Windows Server 2012 R2
- Windows Server 2012 R2 to Windows Server 2016

CAUTION: Note the following items about this task:

- The Data Center is out of service while you perform this task.
- To avoid unexpected application behavior, perform the steps of the task in order. You must first upgrade the primary Data Center server and then the secondary Data Center server.
- Certain security settings in the Data Center software are modified during the upgrade. To restore these settings, perform the steps as mentioned in the upgrade task.

All servers in your Connected Backup configuration must have version 8.8.1 or later installed before you upgrade any Data Center servers to Windows Server 2012 R2, and version 8.8.6.1 or later installed for Windows Server 2016.

To upgrade a Data Center server to Windows Server 2012 R2, Windows Server 2016, or Windows Server 2019

1. Use Internet Explorer to log on to Support Center. Verify that the Data Center configuration (including Data Centers and Web servers) is running the Connected Backup version 8.8.1 or later.
2. Upgrade the Data Center server to Windows Server 2012 R2. For details about how to perform this upgrade, refer to Microsoft documentation.
3. After the upgrade completes, use the Services in the Control Panel to verify that the IIS Admin Service and World Wide Web Publishing Service is started. Set the Startup Type to **Automatic**.
4. Verify that the Active Server Pages are enabled in IIS.

5. To restore the Data Center security settings that are modified during the upgrade to Windows Server 2012 R2 or Windows Server 2016, perform the following steps:
   a. Locate the Post2012UpgradeFix folder and the Data Center installer that you have downloaded and copy it to a convenient location on the server. The Post2012UpgradeFix folder contains the following files:
      - Post2012UpgradeFix.vbs
      - SetRegKeyAce.exe.
   b. Start the command prompt as an administrator and run the Post2012UpgradeFix.vbs script.
   c. Click **Yes** in the **Post Windows Server Upgrade Fix** window.
   d. After the script has finished running, click **OK** to close the window.
   e. Use Services in the Control Panel to stop the IIS Admin Service.
   f. Use Services in the Control Panel to start the World Wide Web Publishing Service, and set the startup mode to automatic.

      > **NOTE:** If the Data Center services fail to run after rebooting the system, then you must manually start the Data Center services using the Data Center Management Console as a one-time activity, after you run the script.

6. Use the following steps to verify the upgrade was successful:
   a. Verify that the Application event log has no warning or error events in it.
   b. Use Support Center to view an account's information.
   c. Use Support Center to run a report.
   d. Use Support Center to create an Agent Configuration.
   e. Use the Account Management Website to view account information.

Upgrade Stand-Alone Data Center Servers to SQL Server

This section describes how to upgrade a stand-alone Data Center server to SQL Server 2012 SP4 , SQL Server 2016, or SQL Server 2019.

> **CAUTION:** Note the following items about this task:
> - The Data Center is out of service while you perform this task.
> - To avoid unexpected application behavior, perform the steps of the task in order.

Before You Begin

Ensure the following:

- Your Connected Backup configuration is running the following version:
  - For SQL Server 2012 SP4 Standard or Enterprise (64-bit only)- Connected Backup version 8.8.1 or later

  - For SQL Server 2016 - Connected Backup version 8.8.6 or later.
  - For SQL Server 2019 - Connected Backup version 9.0.4 or later.
- The Data Center server you plan to upgrade is running Windows Server 2012 R2, Windows Server 2016, or Windows Server 2019.

To upgrade a stand-alone Data Center server to SQL Server

1. Prepare the Data Center server for SQL Server upgrade.

   For information, see Prepare for SQL Server Upgrade, on page 34.
2. Upgrade the Data Center server to SQL Server.

   For information, see Upgrade SQL Server, on page 37.
3. Modify the Data Center maintenance scripts and restart the Data Center server.

   For information, see Modify the Data Center Maintenance Scripts , on page 40.
4. Use the Services applet of Control Panel to restart the SQL Server Agent.

Upgrade Mirrored Data Center Servers to SQL Server

This section describes how to upgrade mirrored Data Center servers to SQL Server 2012 SP2 Standard or Enterprise (64-bit only), SQL Server 2016, or SQL Server 2019.

Before You Begin

Ensure the following:

- Your Connected Backup configuration is running the following version:
  - For SQL Server 2012 SP4 - Connected Backup version 8.8.1 or later
  - For SQL Server 2016 - Connected Backup version 8.8.6 or later.
  - For SQL Server 2019 - Connected Backup version 9.0.4 or later.
- The Data Center server you plan to upgrade is running Windows Server 2012 R2, Windows Server 2016, or Windows Server 2019.

> **CAUTION:** To avoid unexpected application behavior, perform the steps of this task in order.

To upgrade mirrored Data Center servers to SQL Server

1. Prepare the primary Data Center server for upgrade.

   For information, see Prepare for SQL Server Upgrade, on page 34.
2. Upgrade the primary Data Center server to SQL Server.

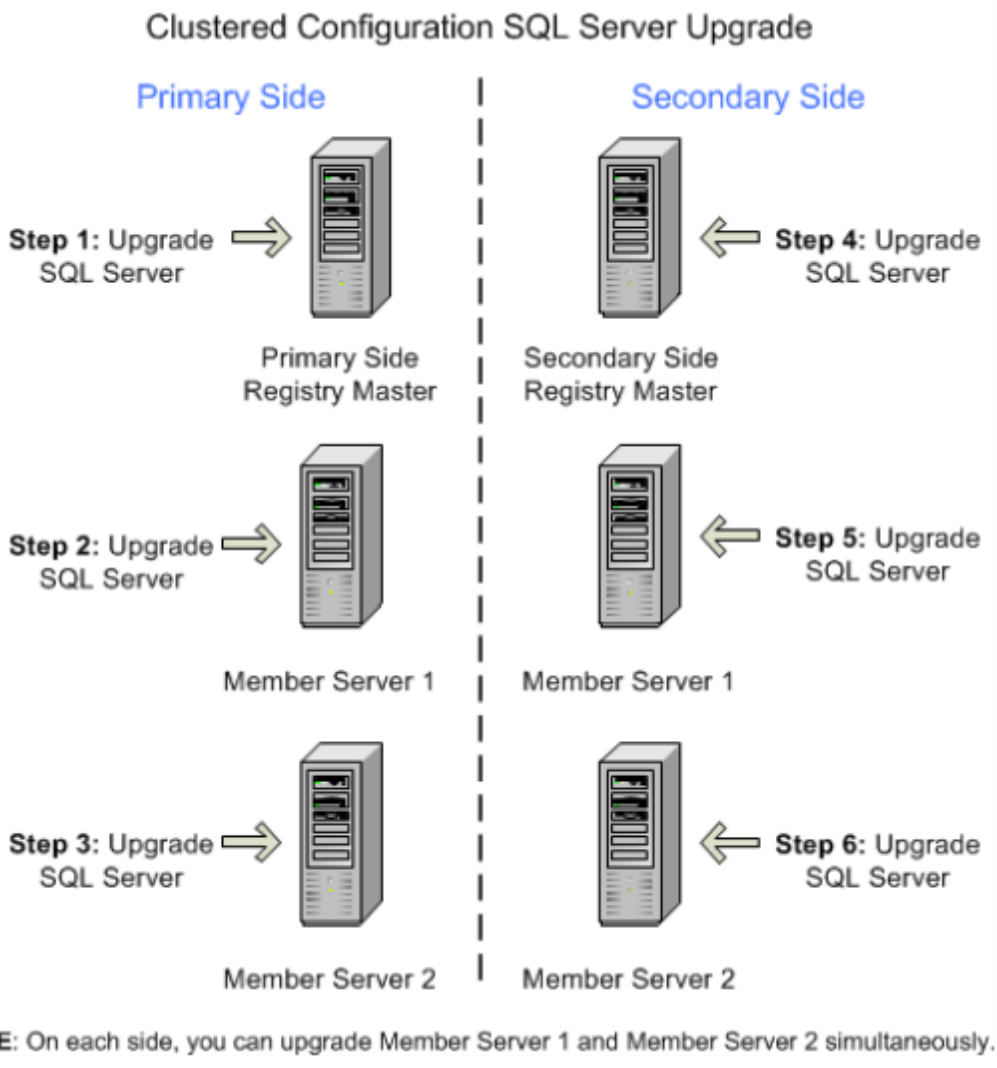
   For information, see Upgrade SQL Server, on page 37.
3. Modify the Data Center maintenance scripts.

For information, see Modify the Data Center Maintenance Scripts , on page 40.

4. Use the Services applet on the Control Panel to restart the SQL Agent on each server you just upgraded.
5. Repeat Prepare the primary Data Center server for upgrade., on the previous pagethrough Use the Services applet on the Control Panel to restart the SQL Agent on each server you just upgraded. , above on the mirrored Data Center server.

Upgrade Clustered Data Center Servers to SQL Server

This section describes how to upgrade clustered Data Center servers to SQL Server 2012 SP4, SQL Server 2016 or SQL Server 2019. The following figure provides an example of the process that you must follow to perform this upgrade.



Before You Begin

Ensure the following:

- Your Connected Backup configuration is running the following version:
  - For SQL Server 2012 SP4 - Connected Backup version 8.8.1 or later
  - For SQL Server 2016 - Connected Backup version 8.8.6 or later.
  - For SQL Server 2019 - Connected Backup version 9.0.4 or later.
- The Data Center server you plan to upgrade is running Windows Server 2012 R2, Windows Server 2016, or Windows Server 2019.

CAUTION: To avoid unexpected application behavior, perform the steps of this task in order.

To upgrade clustered Data Center servers to SQL Server

1. Prepare the Data Center servers on the primary-side cluster for upgrade.

   For information, see Prepare for SQL Server Upgrade, below.
2. Upgrade the primary-side Registry Master server to SQL Server.

   For information, see Upgrade SQL Server, on page 37.
3. Upgrade the remaining primary-side servers to SQL Server.
4. Modify the maintenance scripts on all servers on the primary side of the cluster.

   For information, see Modify the Data Center Maintenance Scripts , on page 40.
5. Use the Services applet on the Control Panel to restart the SQL Server Agent on the servers you just upgraded.
6. Repeat Prepare the Data Center servers on the primary-side cluster for upgrade., above through Use the Services applet on the Control Panel to restart the SQL Server Agent on the servers you just upgraded. , above on the secondary-side cluster to upgrade those servers.
7. Check the application event logs to verify that the Replication Agent jobs start as scheduled.

SQL Server Upgrade Tasks

This section provides the details and procedures that you need to upgrade the SQL Server.

Prepare for SQL Server Upgrade

Before you upgrade the SQL Server, first prepare the Data Center Server for upgrade.

To prepare a server for SQL Server upgrade

1. Verify the integrity of your data.

   For information, see Verify Data Integrity, on the next page
2. Exit any of the following applications that are running on the server:

- Account Management Website
- Data Center Management Console
- Event Viewer
- Support Center

3. Back up the SQL databases, if needed.

   See Back Up the SQL Databases, below.

4. For a server in a mirrored or clustered environment, redirect the Web Service applications to another server.

   For information, see Redirect Web Services Applications, on the next page.

5. Stop all Data Center services.

   For information, see Stop Data Center Services, on page 37

General Preparation Tasks

This section provides the details and procedures that you need to prepare for a Data Center server upgrade to SQL Server.

Verify Data Integrity

Use this task to verify the integrity of your data on the server you plan to upgrade the SQL Server.

To verify the integrity of your data

1. Open SQL Server Management Studio, and then connect to the Data Center.
2. Run the `DBMaint.sql` script from the `\DataCenter\Scripts` folder.

   > **NOTE:** This procedure can take several hours.

3. Check the output for errors. If the output includes errors, contact Support and do not perform the upgrade.
4. Close SQL Server Management Studio.

Back Up the SQL Databases

To ensure that you have a current copy of your data should you need it in the unlikely event that the upgrade process causes data corruption, back up any Registry Master, system databases, and Directory SQL databases that reside on the server you plan to upgrade. Ensure that you have the base backups before starting an upgrade for all the systems and user databases.

> **NOTE:** This step can take several hours to complete. If you receive error messages or warnings during the backup, do not continue the upgrade process. Contact Support.

To backup the SQL databases for a stand-alone Data Center

1. On the Data Center server, open **Control Panel** > **Administrative Tools** > **Task Scheduler**.
2. Locate the Connected Backup **WeeklyMaint** task, right-click it, and then select **Run**.
3. Close **Task Scheduler**.

To backup the SQL databases for a mirrored or clustered Data Center

> **NOTE:** Mirrored Data Center servers have both a Directory and Registry database. Clustered Data Center servers can have both a Directory and Registry database (non-dedicated Registration Master), just a Registry database (dedicated Registration Master), or just a Directory database (directory server).

1. Open the SQL Server query interface and connect to the Data Center.
2. Run the `database_backup.sql` script from the `\DRProcs` folder in the Data Center installation folder.
3. Close the SQL Server query interface.

Redirect Web Services Applications

The Web server uses the Registry database on a Data Center server in a mirrored or clustered configuration for the Support Center and the Account Management Website. In clustered Data Centers, the Registry database is on the Registration Master servers. To avoid a service interruption for your users during the SQL Server upgrade process, direct the Web server to the other Data Center in the pair during the upgrade.

To redirect the Web services applications to another Data Center server

1. Open the Windows Registry Editor.
2. Navigate to **HKEY_LOCAL_MACHINE\SOFTWARE\Connected\WoW6432Node\SupportCenter**.
3. Modify the value of **RegistryConnect** to reflect the server name of the other Data Center in the pair.

   For example, if SERVER1 and SERVER2 are in a mirrored pair, and SERVER1 is being upgraded and is also the server the Web server uses, change:

   ```
   DRIVER={SQL Server Native Client 11.0};SERVER=SERVER1;DATABASE=Registry;
   Trusted_Connection=Yes
   ```

   to

   ```
   DRIVER={SQL Server Native Client 11.0};SERVER=SERVER2;DATABASE=Registry;
   Trusted_Connection=Yes
   ```
4. Close the Registry Editor.

Stop Data Center Services

Use this task to stop all Data Center services on the Data Center server before you upgrade the SQL Server.

To stop the Connected Backup Data Center services

1. Open the Data Center Management Console (DCMC).
2. In the left pane, expand the Data Center server name you are upgrading.
3. Right-click **BackupServer**, and then select **Properties**.
4. In the Session Restrictions section, deselect **Allow Backups** and **Allow Restores**.
5. Click **OK**.
6. After the number of current sessions goes to zero or stays at a consistently low number, stop all Connected Backupservices.
7. Close the DCMC.
8. Use the Services applet of Control Panel to stop the SQL Server Agent on the Data Center server.

Upgrade SQL Server

This section describes how to upgrade the SQL Server. Connected Backup supports only the following software combinations:

- Windows Server 2008 R2 and SQL Server 2008 R2 SP3
- Windows Server 2012 R2 and SQL Server 2012 SP4
- Windows Server 2012 R2 and SQL Server 2016
- Windows Server 2016 and SQL Server 2016
- Windows Server 2016 and SQL Server 2019
- Windows Server 2019 and SQL Server 2016 SP2
- Windows Server 2019 and SQL Server 2019

You may upgrade the SQL Server based on your needs.

To upgrade the SQL Server

1. Start the Microsoft SQL Server Setup Wizard. For information about the wizard, refer to Microsoft SQL Server upgrade documentation.
2. On the **Components to Install** page, select the following options:
   - **SQL Server Database Services**
   - **Workstation components, Books Online and development tools**

     > **NOTE:** Ensure that only these two options are selected.

3. On the **Feature Selections** page, select only the following features:
   - **Database Engine Services**.
   - **Management Tools - Basic**.
   - **Management Tools - Complete**.

   > **NOTE:** For SQL Server 2016 and SQL Server 2019, you will need to install/upgrade 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 **Install SQL Server Management Tools** to start the installation process.

4. On the **Instance Configuration** page, click **Default instance**.
5. When the wizard prompts you to select a feature, select **Database Services**, and then verify that the installation path it displays refers to your current SQL Server installation.
6. When the wizard prompts you for the Instance root directory, either browse to or enter the path to the current version of the SQL Server, and then click **OK**.
7. To verify the data consistency on the server, in SQL Server Management Studio, run the following commands in the below mentioned order:
   a.
```
USE Master

GO

DBCC CHECKDB

GO

USE Model

GO

DBCC CHECKDB

GO

USE Msdb

GO

DBCC CHECKDB

GO

USE Directory

GO

DBCC CHECKDB

GO
```
   b.
```
IF EXISTS (SELECT TOP 1 1 FROM sys.databases WHERE name = 'Registry')

BEGIN
```

```
USE Registry
GO
DBCC CHECKDB
END
```

Check the output for errors. If the output includes errors, contact Support.

8. Update the statistics on the server. To do so, in SQL Server Management Studio, run the following commands in the below mentioned order:
   a.
```
USE Master
GO
sp_updatestats
GO
USE Model
GO
sp_updatestats
GO
USE Msdb
GO
sp_updatestats
GO
USE Directory
GO
sp_updatestats
GO
```
   b.
```
IF EXISTS (SELECT TOP 1 1 FROM sys.databases WHERE name = 'Registry')
BEGIN
USE Registry
EXEC sp_updatestats
END
```

   Check the output for errors. If the output includes errors, contact Support.

9. After the upgrade completes, use DCMC to start the Backup Server and Index Server on the updated server.

Modify the Data Center Maintenance Scripts

After you upgrade the SQL Server, modify the SQL scripts that the system uses to perform maintenance.

To modify the Data Center maintenance scripts

1. Use a text editor to open the `DailyMaint.cmd` file.

   By default, Data Center maintenance scripts resides in the `DataCenter` folder.

2. Locate the following text in the file:

   `\Drive:\Program Files\Microsoft SQL Server\100\Tools\BINN\OSQL.EXE`

   and then, do the following:

   - For SQL Server 2012 SP4 —Replace the located text with the following line:

     `\Drive:\Program Files\Microsoft SQL Server\110\Tools\BINN\OSQL.EXE`

   - For SQL Server 2016—Replace the located text with the following line:

     `\Drive:\Program Files\Microsoft SQL Server\130\Tools\BINN\OSQL.EXE`

   - For SQL Server 2019—Replace the located text with the following line:

     `\Drive:\Program Files\Microsoft SQL Server\150\Tools\BINN\OSQL.EXE`

3. Use a text editor to open the `WeeklyMaint.cmd` file.
4. Locate the following text in the file:

   `Drive:\Program Files\Microsoft SQL Server\100\Tools\BINN\OSQL.EXE`

   and then, do the following:

   - For SQL Server 2012 SP4 — Replace the located text with the following line:

     `Drive:\Program Files\Microsoft SQL Server\110\Tools\BINN\OSQL.EXE`

   - For SQL Server 2016—Replace the located text with the following line:

     `Drive:\Program Files\Microsoft SQL Server\130\Tools\BINN\OSQL.EXE`

   - For SQL Server 2019—Replace the located text with the following line:

     `\Drive:\Program Files\Microsoft SQL Server\150\Tools\BINN\OSQL.EXE`

5. Restart the Data Center server.

General Post-Upgrade Tasks

This section provides the details and procedures that you need to perform after the SQL Server upgrade.

Start Data Center Services

After upgrading the SQL Server, restart the required Data Center services.

To start the Data Center services on the server and verify their operation

1. Open DCMC on the upgraded server.
2. In the left pane, expand the migrated Data Center server name.
3. Right-click **BackupServer**, and then select **Properties**.
4. In the Session Restrictions section, select **Allow Backups** and **Allow Restores**.
5. Click **OK**, and then close DCMC.
6. To verify a successful startup, use DCMC to make sure that the following conditions exist:
   - All Data Center services are running.
   - The BackupServer service is accepting backups.

Redirect Web Services Applications After SQL Server Upgrade

> **NOTE:** Do not use this task with stand-alone servers, as there is no fail-over Data Center server for the Web server to connect to for Support Center and Account Management Website access.

To redirect the Web services applications to an upgraded Data Center server

1. Open the Windows Registry Editor.
2. Navigate to **HKEY_LOCAL_MACHINE\SOFTWARE\WoW6432Node\Connected\SupportCenter**.
3. Modify the value of `RegistryConnect` to reflect the server name of the other Data Center in the pair.

   For example, if SERVER1 and SERVER2 are in a mirrored pair, and SERVER1 was upgraded and is also the server the Web server uses, change:

   ```
   DRIVER={SQL Server Native Client 11.0};SERVER=SERVER2;DATABASE=Registry;
   Trusted_Connection=Yes
   ```

   to

   ```
   DRIVER={SQL Server Native Client 11.0};SERVER=SERVER1;DATABASE=Registry;
   Trusted_Connection=Yes
   ```
4. Close the Registry Editor.
5. Open a Command Prompt window, and then type the following command to restart Internet Information Server (IIS):

   ```
   iisreset
   ```
6. Close the Command Prompt window.

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 Micro Focus Connected Backup 9.0.7 Upgrading the Data Center

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!