OpenText™ Content Server

Upgrade Guide

The OpenText™ Content Server Upgrade Guide explains how to upgrade Content Server to a new major version and how to apply Content Server Updates.

Upgrading Content Server to a new major version through a "parallel upgrade" is a complex operation that requires preparation and testing. This guide walks you through the process. It starts with your initial research, follows with the preparation of your Source and Target Environments, and culminates in the upgrade of your Content Server database and search index. You can ensure a successful Content Server upgrade by following the steps outlined in this document and by testing your upgrade in advance.

Applying a Content Server Update is a step that you should perform every three months to keep Content Server up to date with the latest features and fixes. The second section of this guide explains how to apply a Content Server Update, either by using Cluster Management or by manually extracting the Update to your Content Server deployment.

LLESCOR160205-IUP-EN-01

OpenText™ Content Server
Upgrade Guide
LLESCOR160205-IUP-EN-01
Rev.: 2018-June-05

This documentation has been created for software version 16.2.5.
It is also valid for subsequent software versions as long as no new document version is shipped with the product or is published at https://knowledge.opentext.com.

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Tel: +1-519-888-7111
Toll Free Canada/USA: 1-800-499-6544 International: +800-4996-5440
Fax: +1-519-888-0677
Support: https://support.opentext.com
For more information, visit https://www.opentext.com

Disclaimer

No Warranties and Limitation of Liability

Every effort has been made to ensure the accuracy of the features and techniques presented in this publication. However, Open Text Corporation and its affiliates accept no responsibility and offer no warranty whether expressed or implied, for the accuracy of this publication.

Table of Contents

Chapter 1

Upgrading Content Server

Upgrading Content Server to its latest major version allows you to benefit from all of the capabilities that Content Server has to offer.

This guide walks you, the Content Server administrator, through the upgrade process. It starts with your initial research, follows with the preparation of your Source and Target Environments, and culminates in the upgrade of your Content Server database and search index. You can ensure a successful Content Server upgrade by following the steps outlined in this document and by testing your upgrade in advance.

This chapter covers the following topics:

- "The Parallel Upgrade Method" on page 5
- "Plan the Content Server Upgrade" on page 7
- "Prepare Content Server in your Source Environment" on page 16
- "Install the New Version of Content Server on the Operating System" on page 30
- "Connect and Upgrade Content Server Components" on page 32
- "Start up Search and Indexing and add Front-End Instances" on page 47

1.1 The Parallel Upgrade Method

To upgrade Content Server, you perform a *parallel upgrade installation*. A parallel upgrade installation allows you to preserve your existing Content Server deployment while you set up your upgraded Content Server installation.

In a parallel upgrade installation, you make copies of key elements from your Content Server environment: your database, External File Store, and Search Index. You install a new instance of the latest version of Content Server. To the extent possible, you set up your new instance to match your existing deployment: using the same directories, network ports, virtual web directory names and so on. You then connect that instance of Content Server to a copy of your production. The database directs you as you install required modules, set up your Admin servers, connect to your Storage Providers, and finally upgrade the database itself.

After your database is upgraded, you connect to OpenText™ Directory Services (OTDS). OTDS manages your Content Server users and groups, and provides other services such as license management.

If necessary, you then make adjustments to your Search and Indexing environment, such as modifying Index Partition paths, to reflect changes in your new environment. Once that's done, you apply a new license to Content Server.

After you perform some additional configuration and testing, your new version of Content Server is ready to use in production. You can start up all of its components, including the full Search and Indexing environment, and make it available to your user community.

Terms Used in this Guide

In this guide, certain terms are used consistently with specific meanings.

Environments

`Source environment` and `Target environment` designate the environments involved in a parallel upgrade.

Source environment
The Content Server system that you are upgrading.

Target environment
The new version of Content Server that you install. During the upgrade, you migrate your data to this environment and eventually bring it into production as your upgraded Content Server environment.

Content Server Instances

You can run a full deployment of Content Server on a single host computer, but a production deployment of Content Server typically includes multiple instances of Content Server that are deployed for varying purposes. This guide refers to two types of Content Server instance: `Admin server` (which can be `Default` or `Additional`) and `Front-End Instance`.

Admin Server
An Admin server runs the Content Server Admin service. It operates the Search and Indexing processes, and runs other background processes including Memcached, Document Conversion Server, and the internal OTDS (which it normally runs only on test servers). It does not necessarily run the Content Server service or provide a GUI. It cannot be managed by Content Server users who do not have the **System administration rights** privilege.

Default (or "primary") Admin server
The `Default Admin server` is the first Admin server that you install. It normally runs both the Content Server service and the Content Server Admin service, and serves to organize the overall Search and Indexing environment. It is also known as the Primary Admin server.

Additional (or "secondary") Admin server
An `Additional Admin server` is any Admin server that you add to your Content Server deployment after you have installed the Default Admin server. Additional Admin servers allow for scaling of the Search and Indexing environment. They typically do not run the Content Server service or provide a GUI. Additional Admin servers are also known as Secondary Admin servers.

Front-End Instance

A Front-End Instance of Content Server runs both Content Server and Content Server Admin services. It makes Content Server's GUI and functionality available to Content Server users.

1.2 Plan the Content Server Upgrade

Before you begin upgrading Content Server, plan the upgrade and review its requirements. The Upgrade Central (https://knowledge.opentext.com/go/UpgradeCS) section of OpenText My Support has numerous resources that supplement the information in this guide and can help you with your planning.

This chapter covers the following topics:

1.2.1 Verifying Platform Requirements

Verify that you have a suitable software environment for upgrading to Content Server.

Obtain Supported Software Components

Content Server can be installed on the following operating systems:

- Microsoft ® Windows®
- Oracle Linux
- Red Hat® Enterprise Linux®

The following database management systems can be used with Content Server:

- Microsoft® SQL Server®
- SAP® HANA
- Oracle® Database
- PostgreSQL

Note: Databases are supported on any operating system supported by the database vendor. You do not have to run the database on the same operating system as Content Server.

The following web servers can be used with Content Server:

- Microsoft Internet Information Services (IIS)
- Oracle® iPlanet Web Server
- Apache® HTTP Server

The following application servers can be used with Content Server:

- Apache® Tomcat™
- IBM® WebSphere®

Review the Content Server Release Notes

To determine the specific versions of operating systems, database management systems, web servers, and other components that are supported for use with Content Server, review the Content Server Release Notes.

Review Module Release Notes

Optional modules may also have particular platform requirements. For more information, see the Release Notes that accompany each optional module.

UTF-8 Compliant Database

To upgrade to Content Server 16.2, you must start with a UTF-8 compliant database running on Content Server 9.7.1, 10.0.x, 10.5.x, or 16.0.x. If your database uses Latin-1 character encoding, you must convert the database to UTF-8 before you can upgrade.

Figure 1-1 illustrates the various upgrade paths to Content Server 16.2.x. The path that you follow depends on your current version of Content Server and whether your database currently uses UTF-8 character encoding.

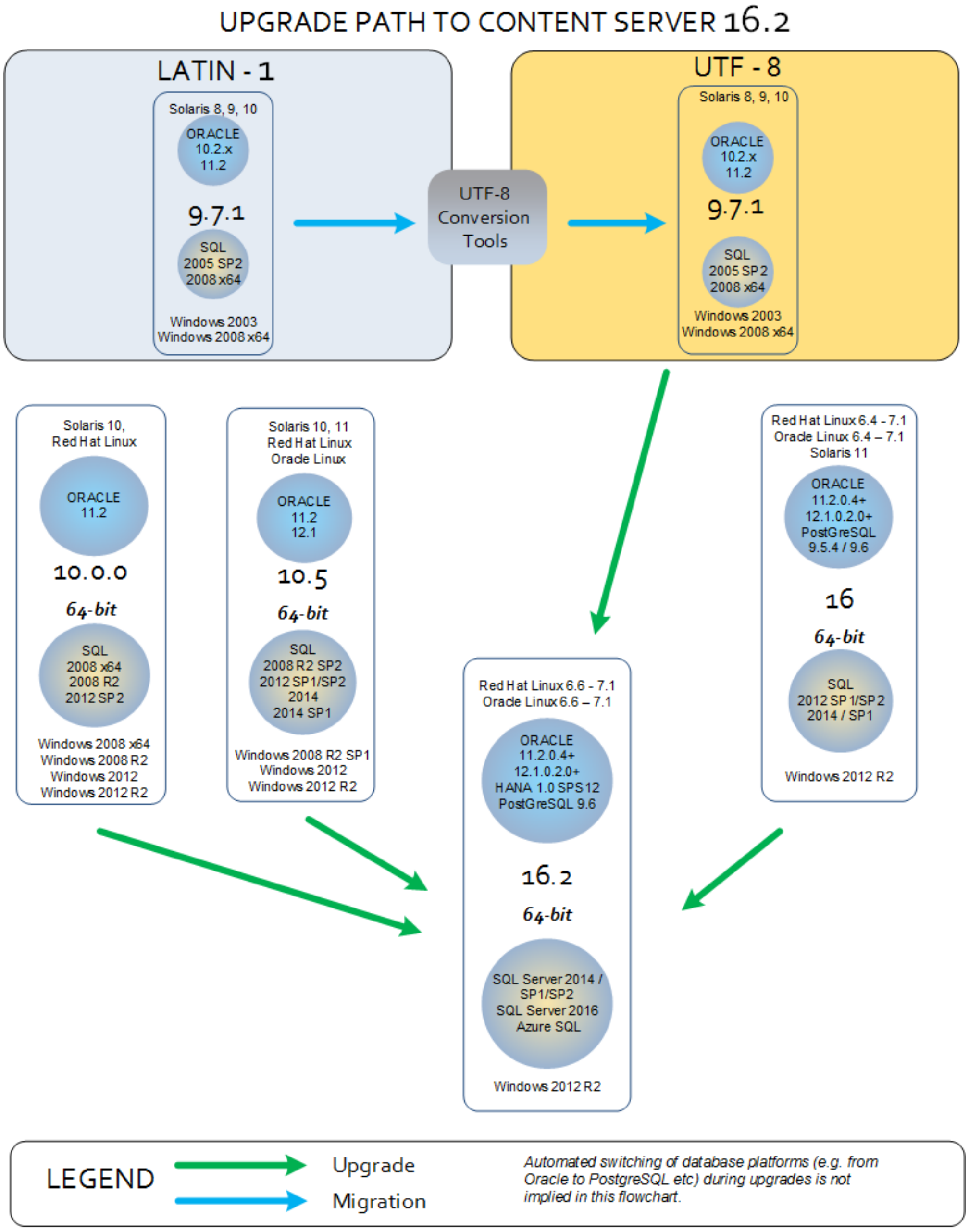

UPGRADE PATH TO CONTENT SERVER 16.2
LATIN - 1
Solaris 8, 9, 10
ORACLE 10.2.x 11.2
9.7.1
SQL 2005 SP2 2008 x64
Windows 2003 Windows 2008 x64
UTF-8 Conversion Tools
UTF - 8
Solaris 8, 9, 10
ORACLE 10.2.x 11.2
9.7.1
SQL 2005 SP2 2008 x64
Windows 2003 Windows 2008 x64
Solaris 10, Red Hat Linux
ORACLE 11.2
10.0.0
64-bit
SQL 2008 x64 2008 R2 2012 SP2
Windows 2008 x64 Windows 2008 R2 Windows 2012 Windows 2012 R2
Solaris 10, 11 Red Hat Linux Oracle Linux
ORACLE 11.2 12.1
10.5
64-bit
SQL 2008 R2 SP2 2012 SP1/SP2 2014 2014 SP1
Windows 2008 R2 SP1 Windows 2012 Windows 2012 R2
Red Hat Linux 6.4 - 7.1 Oracle Linux 6.4 – 7.1 Solaris 11
ORACLE 11.2.0.4+ 12.1.0.2.0+ PostGreSQL 9.5.4 / 9.6
16
64-bit
SQL 2012 SP 1/SP2 2014 / SP1
Windows 2012 R2
Red Hat Linux 6.6 - 7.1 Oracle Linux 6.6 – 7.1
ORACLE 11.2.0.4+ 12.1.0.2.0+ HANA 1.0 SPS 12 PostGreSQL 9.6
16.2
64-bit
SQL Server 2014 / SP1/SP2 SQL Server 2016 Azure SQL
Windows 2012 R2
LEGEND
Upgrade
Migration
Automated switching of database platforms (e.g. from Oracle to PostgreSQL etc) during upgrades is not implied in this flowchart.

Figure 1-1: Flowchart showing the upgrade path to Content Server

Note: For information about converting a database to UTF-8, see the *Livelink ECM – Enterprise Server - UTF-8 Database Conversion Guide (LLESCOR-AUT)* on OpenText My Support: https://knowledge.opentext.com.

1.2.2 Upgrading Optional and Custom Modules

Every deployment of Content Server has its own combination of optional modules, and many organizations deploy custom modules created for their own needs. This section provides information on upgrading optional and custom modules.

Tip: For detailed information on installing, upgrading and uninstalling Content Server, see *OpenText Content Server - Module Installation and Upgrade Guide (LLESCOR-IMO)*.

Optional Modules

Install the latest versions of optional modules when you upgrade Content Server. Module versions released prior to the current Content Server version are typically incompatible with the current Content Server version.

Tip: The *OpenText Content Server Module Matrix* on My Support (https://knowledge.opentext.com) provides a list of module versions that are compatible with various versions of Content Server.

As part of your upgrade planning, verify that compatible versions of optional modules are available in the languages that you need and for the operating system that you use. Investigate how each module is upgraded. All optional modules are not upgraded in the same way.

Module Maintenance and Licenses

In Content Server 10.5 and later, some modules require the application of a license. If you are installing a module that requires a license, obtain a license file by logging onto http://productactivation.opentext.com/ContentServer with the user name and password that was provided to you when you purchased the module.

In addition, if you have purchased optional modules from third parties, ensure that you have adequate licensing for your module upgrade.

Custom Modules

If you have custom modules, be prepared to test and modify them. For more information, contact OpenText Customer Support.

If your organization has made customizations to Content Server that affect the Content Server database schema, make sure you back up the current data before upgrading.

1.2.3 Reviewing Workflows and Other Key Deployment Features

Identify any important features of your Content Server deployment so that you can test them on the upgraded platform. Many organizations have workflows that support mission-critical processes. If yours does, ensure that you identify them and test them.

In addition, you should identify LiveReports, Custom Views, Appearances, and other features that are unique to your Content Server so that you can verify their functionality during your upgrade testing and after you upgrade your production Content Server.

Security and administrative settings may have new default configurations that require you to make adjustments to these items. For example, in Content Server 16.2, the **Open** command is disabled by default. If you have Custom Views that rely on the **Open** command to display graphics, you will need to allow use of the **Open** command or change the behavior of the Custom View (by having it retrieve graphics from the Content Server `support` directory, for example).

Some of your LiveReports may no longer function as expected after an upgrade. For example, Content Server 16 and later replaces the Undelete and optional OpenText Recycle Bin module with a built-in core Recycle Bin. Any LiveReports created in Content Server 10.5 or earlier that reference the Undelete Volume or the optional Recycle Bin will not work after you upgrade to Content Server 16.2.

1.2.4 Reviewing Customizations

If your organization has customized Content Server to modify its appearance, enhance its functionality, or resolve issues specific to your organization, determine which customizations you need to implement in your upgraded environment.

1.2.5 Transitioning from LAPI to REST API or Web Services

As announced by OpenText in numerous locations since the release of Content Server 10.5.0, LAPI is not supported in Content Server 16 and later. You should transition any LAPI applications that you use in your Content Server deployment to applications that you use Content Server Web Services or the Content Server REST API.

More information on Content Server Web Services and the Content Server REST API can be found in the Champion Toolkit document **White Paper – Adapting and Integrating ECM** on OpenText My Support (https://knowledge.opentext.com) and on the OpenText Developer Network (http://otdn.opentext.com)

1.2.6 Transitioning to OpenText Directory Services

Content Server 16.2 requires the use of OpenText™ Directory Services 16.2 (OTDS) for user management and authentication. Content Server Directory Services (CSDS) is not supported in Content Server 16 and later.

Tip: Content Server Directory Services is an optional module for Content Server 10.5 and earlier that provides synchronization and authentication features, including the ability to synchronize Content Server users and groups with an external directory.

As part of your deployment plans, you should plan to manage your user base in OpenText™ Directory Services. OpenText™ Directory Services is a single application that you can use to manage creation, synchronization, and authentication of users and groups in all of your OpenText applications.

If you already use OpenText Directory Services, you will transfer user management from Content Server or Content Server Directory Services to your existing deployment. If you do not have an existing deployment, you should plan to implement one.

Once you have installed OTDS, it will assume responsibility for enforcing password policy, including such settings as minimum number of characters and whether symbols and uppercase characters are required. Unlike earlier versions of Content Server, Content Server 16.2 does not enforce password policy itself. It relies on OTDS to do this. You should plan on reviewing the default settings in OTDS to ensure that they are suitable for your Content Server deployment.

For detailed information on OpenText Directory Services, including information on network ports that you must open on your Content Server host computers, see *OpenText Directory Services - Installation and Administration Guide (OTDS-IWC)*.

1.2.7 Verifying Patches

As part of your upgrade preparations, you should ensure that your Source and Target Environments are up to date with the latest patches and Updates.

Tip: Patches for Content Server are version-specific. For example, patches for Content Server 16.0.x are not compatible with Content Server 16.2.x.

Use Cluster Management in your target Content Server environment (and, if possible, in your Source Environment) to ensure that your system has all of the recommended and required patches in place.

Tip: Introduced in Content Server 10.5, Cluster Management simplifies patch management and ensures that patches are applied consistently in a clustered Content Server deployment. For more information on Cluster Management, see *OpenText Content Server Cluster Management - Admin Online Help (LLESPAT-H-AGD)*.

In your Source Environment, you should make sure that you have the latest patches in place for your environment, including your optional, third-party, and custom modules, before you copy your database, file store, and search index. You should also review the patches that you have to determine whether you need similar ones in your Target Environment.

The official patches in your Target Environment do not need to be an exact match of the patches in your Source Environment. The issues resolved by the patches in your source environment no longer exist in the newer version of Content Server. However, if you have created an unofficial patch to customize Content Server, you may need to create and test a similar patch in the target system to enable the same customization. Similarly, if you have third-party or custom modules in your source system, you should review their patches to see whether the issues that they resolve are fixed in the newer versions of these modules in your Target Environment.

Tip: One indicator that a patch applies to a third-party or custom module is that it has a name that deviates from the naming scheme used by official Content Server patches. Official Content Server patches issued by OpenText use the following naming scheme:

- **Content Server 10.5.x**

  `pat10500####`
- **Content Server 16.0.x**

  `pat160000####`
- **Content Server 16.2.x**

  `pat162000####`

Where # represents a digit.

Occasionally, in your Target Environment, it is necessary to have one or more patches in place before you start Content Server for the first time and configure it. This is most likely to occur when you are installing Content Server for integration with other OpenText or third-party products and modules. Check the release notes and installation guides for such products and modules to verify whether this is necessary in your case. If it is necessary to have specific patches in place before you start Content Server for the first time, you cannot use Cluster Management to apply them. Instead, copy the patches manually into the `<Content_Server_home>\patch\` folder before you start the Content Server service. Then complete the application of all available patches by running Cluster Management after you have started Content Server and performed the initial configuration.

You can simplify your analysis of patches in the Source Environment by applying the latest Update for Content Server. Content Server Updates resolve issues that were previously corrected by patches, and allow you to remove patches before you upgrade Content Server.

Tip: For a list of patches that you can remove when you apply an Update to Content Server 16.0.0, consult the Content Server Release Notes and run

Update Analyzer. The Content Server Release Notes contain a section that shows which patches are included in the Update. For information on running Update Analyzer, see “Using Update Analyzer” on page 54.

When you use Cluster Management to apply an Update, superseded patches are removed automatically.

1.2.8 Recreating or Copying the Search Index

There are two ways to upgrade your Search Index during a parallel upgrade:

- Recreate the index by re-indexing all of your Content Server data
- Copy your existing Search Index to the Target Environment

If it is practical in your environment, OpenText recommends that you recreate your index by re-indexing all of your Content Server data. Re-indexing allows you to take full advantage of the improvements in Content Server 16.2, including:

- Smaller index size
- Better performance
- Better accuracy and relevancy of search results
- Fewer search partitions

New index information, such as the information provided in the `OTFileType` feature, and better management of suspicious or erroneous metadata, is generated by the updated Document Conversion Server and the Search Engine only when items are indexed. This new information is not available for items that have already been indexed before you install the upgraded Document Conversion Server and Search Engine, so a migrated index does not contain this information for existing index items. The information is available for items that are indexed after the upgrade.

But creating a new index can be time-consuming and resource-intensive, and it triggers the generation (or regeneration) of all of the thumbnails in your environment, which causes database load to increase for a period of time. If your upgrade testing reveals that re-indexing takes too much time, copying your index may be a better choice. Search indexes from Content Server 10 and later are compatible with Content Server 16.2, and can be migrated to the new system by following the instructions in this guide.

Tip: OpenText provides tools that assist with incremental re-indexing and upgrades to the search index. If you migrate your index, you can still realize the benefits of re-indexing by performing incremental re-indexing and upgrades to the Search Index after your upgrade is complete.

1.2.9 Reviewing New Features and Functionality

Each new version of Content Server provides improvements and introduces new functionality. Take some time to understand the improvements delivered in the new versions before you begin the upgrade process.

When you review your Source Environment, examine optional module functionality that may have become available as part of core functionality in the upgraded version of Content Server. In some cases, you may be able to remove existing modules or customizations.

The following are examples of new or changed functionality in Content Server 16.2:

Access to Content Server Administration pages
Content Server 16.2 does not require you to enter the Web Administrator password to access the Content Server Administration pages. Users with the **Web Admin** usage privilege or one of the Business Administration usage privileges can access the Administration pages without entering a password.

Business Administration roles
Business Administration roles enable users to perform administrative functions without having full access to the Content Server Administration page, allowing you to delegate duties that only system administrators could perform in earlier versions.

Smart View Workflow
Content Server Workflows can now be actioned in the Smart View.

OpenText Directory Services 16.2 Required
Content Server 16.2 requires the use of OpenText Directory Services (OTDS) 16.2 for user synchronization and authentication. In addition, OTDS is now responsible for Content Server license management.

New External System Attributes
New Content Server node attributes exist that can be employed to track the “real-world” attributes of documents and other Content Server items. For example, a digital copy of the book **Les Misérables** could have a **User Identity** attribute of `Victor Hugo` and a **Source Created** attribute of `1862`.

New Default Modules
A number of previously optional modules are installed by default, including OpenText™ Classifications, OpenText™ Attribute Extensions (now supported for use on Smart View), Document Properties Synchronization (now supported on Linux), and all of the modules previously sold separately in the Content Server Extended Collaboration bundle, including Wiki, Blogs, Forums and Communities. The Collaboration modules are all supported on Content Server Smart View.

Tip: This is a brief high-level overview of some of Content Server 16.2’s most important new features. To learn more about the improvements and new features in Content Server 16.2, review the *What’s New* section of the Content

Server Release Notes and module Release Notes, and visit the Upgrade Central section of OpenText My Support.

1.2.10 Review the Content Server Installation Guide

This guide focuses on the steps involved in upgrading Content Server, but the installation of a new version of Content Server during a parallel upgrade is a major step in itself. If you have installed Content Server in the past, you may consider yourself familiar with the overall installation steps, but the installation of each version of Content Server may nonetheless have notable differences. For example, the installation of Content Server 16.2 includes a step where you must decide on whether to implement an internal or external OTDS server.

For detailed information on installing Content Server, refer to *OpenText Content Server - Installation Guide (LLESCOR-IGD)*

1.3 Prepare Content Server in your Source Environment

This section describes how to prepare your source Content Server system for the upgrade, and make copies of the External File Store, database, and Search Index for use in the Target Environment. It covers the following topics:

- "Generate a System Report" on page 16
- "Apply Content Server Updates and Patches" on page 17
- "Disable Global Appearances, Agents and Notifications, and Remove Obsolete Modules" on page 17
- "Prepare and Copy the Search Index" on page 19
- "Verify and Back Up the Database" on page 21
- "Create the Content Server Database in the Target Environment" on page 24
- "Prepare the External File Store" on page 26
- "Migrate Users and Groups" on page 26

1.3.1 Generate a System Report

Content Server system reports (also known as *sysreports*) contain extensive information on your Content Server deployment. You can generate a *Lite System Report* or a *Full System Report*. A Full System Report provides a thorough record of your Source Environment, which can be useful throughout the upgrade process. OpenText recommends that you generate a Full System Report.

To generate a System Report:

1. In the **Server Configuration** section of the **Content Server Administration** page, click **System Report**.

2. On the **Content Server System Report** page, select **Lite System Report** or **Full System Report**, and then click **Generate**.

   Tip: When the System Report is generated, you can view the file by clicking the link on the **Content Server System Report** page. The System Report is stored in the Content Server `logs` folder: *`<Content_Server_home>`*`\logs\sysreport.txt`.

1.3.2 Apply Content Server Updates and Patches

Before you upgrade, make sure your Source Environment is running the latest Update for Content Server and has all available patches. If possible in your Source Environment, use Cluster Management to ensure that your patches are up to date.

Note: See "Installing Content Server Updates" on page 53 for information on installing Content Server Updates.

If you cannot apply the latest Update for Content Server, review the latest Release Notes for your major version of Content Server and note any special procedures that apply to the application of Updates that were issued after your current Update. For example, Updates may require you to remove certain Content Server modules, so you may need to perform similar actions in your Target Environment.

1.3.3 Disable Global Appearances, Agents and Notifications, and Remove Obsolete Modules

Remove or disable items in your Source Environment that are not initially needed in the Target Environment or that could complicate the upgrade unnecessarily.

Important
The steps described in this section temporarily remove functionality from the Source Environment. During a test upgrade, perform the steps *only* in the test environment. When you are ready to start the production upgrade, perform them on the production environment. You should make a full backup of your environment before you perform the following steps so that you can roll back to the original Source Environment if issues occur.

Disable Global Appearances

Disabling Global Appearances simplifies upgrade troubleshooting. If issues arise that involve the graphical user interface, troubleshooting them is easier if Global Appearances are not enabled.

To disable Global Appearances:

1. In the **Appearances Administration** section of the **Content Server Administration** page, click **Open the Appearances Volume**.
2. For each Global Appearance in the Appearance Volume:

a. Open the Global Appearance.

b. Click **Edit Settings** (✎).

c. Select **Disabled**.

d. Click **Submit**.

Disable Agents and Notifications

Disabling Agents and Notifications prevents unnecessary processes from running when you upgrade the database, and stops Content Server from generating unnecessary Notifications.

To disable Agents and Notifications:

1. In the **Notification Administration** section of the **Content Server Administration** page, click **Configure Notification**.
2. In the **Enable Notifications** section of the **Configure Notification** page, click **Disable**, and then click **Submit.**
3. In the **Notification Administration** section of the **Content Server Administration** page, click **Configure Scheduled Activities**.
4. In the **Status** area for each activity, click **Disable**, and then click **Submit**.
5. Restart the Content Server services.

Remove Obsolete Modules

Remove any obsolete modules, modules that you no longer require, and modules that cannot be upgraded, before you copy the database. For more information, see "Reviewing New Features and Functionality" on page 15.

If you do not remove obsolete modules from your source system before you copy the database, you will encounter module errors on the **Install Modules** page and you will not be able to proceed with your upgrade of Content Server. See "Upgrade Content Server Modules" on page 35

Remove Remote Search from Content Server 10.0.0 SP2 Update 9 and earlier

In Update 10 and later for Content Server 10.0.0 SP2, Remote Search is included in the core functionality of Content Server. If your Source Environment has Update 9 or earlier for Content Server 10.0.0 and you have the Remote Search module installed, uninstall the Remote Search module before you copy your Content Server database. Do not remove your remote search processes.

Tip: OpenText recommends that you apply the latest Update before you upgrade your Source Environment. (See "Apply Content Server Updates and Patches" on page 17)

Remove CAP Connector from Content Server 10.0.0

In Content Server 10.0.0, the CAP Connector module is included as an optional module for Content Server. In Content Server 10.5 and later, this module is no longer available. If your Source Environment includes the CAP Connector module, uninstall it before you copy your Content Server database.

1.3.4 Prepare and Copy the Search Index

Prepare the search index for migration, verify it, and then make a copy of it for use in your Target Environment.

Delete Help Data Source Folders

On the **Content Server System** page, delete the **Admin Help Data Source Folder** and the**User Help Data Source Folder**.

You will recreate these data sources on the target system. If the Recycle Bin module is installed, ensure that all references to the Admin Help Data Source Folder and the User Help Data Source Folder are removed from the database by purging these data source folders from the Recycle Bin.

Disable System Object Management Alerts

Disable System Object Management Alerts to prevent undesired messages being sent during the upgrade and migration.

To disable System Object Management Alert emails:

1. In the **Search Administration** section of the **Content Server Administration** page, click **Configure System Object E-mail Delivery**.
2. In the **Recipients and Options** section of the **Configure System Object E-mail Delivery** page, clear the **Active** check box beside all recipients, and then click **Apply**.

Run an Index Verification

Before you copy your index to your Target Environment, verify the integrity of your Search Index.

Note: The following instructions apply to Content Server 10.5 and later. If you are running a different version of Content Server, the exact steps may differ.

To verify the Search Index:

1. In the **Search Administration** section of the **Content Server Administration** page, click **Open the System Object Volume**.
2. Click the Enterprise Data Source Folder **Functions** menu, and then click **Maintenance**.

3. In the **Options** section of the **Content Server Data Source Maintenance** page, click **Configure Search Index Verification**, and then click **OK**.

4. On the **Configure Index Verification** page, enable **Run Once** in the **Mode** section, click the nearest next hour for **At These Hours**, and then click **Update**.

After the verification runs, the report is available in the **Verification Reports** folder on the **Content Server System** page. Resolve any issues highlighted in the report. In particular, ensure that there are no objects missing from the Search Index. If there are, ensure that **Enable Correction** is set on the **Configure Index Verification** page, and that it is configured to resolve the issues identified in the Index Verification Report.

Stop the Search Processes and Copy the Index

Stop the Search and indexing processes and make a copy of the index if you intend to copy your index into the Target Environment. (If you plan on re-indexing your Content Server repository, it is not necessary to make a copy of the index. You will build a new index in the Target Environment.)

> **Important**
>
> If the extractor continues to operate, new items will be added to the index after you make your backup and the indexes in your source and Target Environments will no longer be identical.

To stop the Search Processes and copy the index:

1. Open the **Enterprise Data Flow Manager** page.

   a. In the **Search Administration** section of the **Content Server Administration** page, click **Open the System Object Volume**.

   b. Click **Enterprise Data Source Folder** on the **Content Server System** page.

   c. Click **Enterprise Data Flow Manager** on the **Enterprise Data Source Folder** page

2. On the **Enterprise Data Flow Manager** page, click the Enterprise Extractor Process **Functions** menu, and then click **Stop**.

3. On the **Enterprise Data Flow Manager** page, wait for Content Server to finish indexing the items that are currently in the Data Flow.

4. In the **Interchange Pools** section, verify that all numbers in the **Pending** column are zero, and then stop all of the Search and Indexing processes

   - On the Functions menu of the **Enterprise Dataflow Manager**, click **Suspend**.
   - Return to the **Enterprise Data Source Folder** page, and on the Functions menu of the **Enterprise Search Manager**, click **Stop**.

> **Important**
> When you upgrade your database, the target system will attempt to restore the saved state of the various processes. Your Search and Indexing system should be in an idle state when you upgrade.

5. Stop the Content Server services on the Default Admin Server. Set the services to manual startup.

6. Stop the Content Server Admin service on any Additional Admin servers.

7. Copy the entire `Index` folder from your Source Environment to the location where Content Server will access it in the Target Environment.

8. From each Admin server in your environment, copy the following files from the *`<Content_Server_home>`*`\config\` folder:

   - `LLFieldDefinitions.txt`
   - `LLFieldDefinitions_EL.txt`
   - `otadmin.pwd`

   You will copy these files back into the corresponding *`<Content_Server_home>`*`\config\` folder later when you set up the Additional Admin servers in your Target Environment. See "Install Admin Servers on the Operating System" on page 31.

1.3.5 Verify and Back Up the Database

Upgrading your Content Server database is the crucial step of your overall Content Server upgrade. You can increase the chances of a smooth upgrade by verifying your database using Content Server's built-in tools, and by examining your database to understand whether it has had any modifications since it was first installed.

Once you have verified and examined the database, take a backup for use in your Target Environment.

Verify the Database

Unresolved database issues can cause complications during the database upgrade or prevent the database and its information from successfully upgrading. OpenText recommends that you perform a Level 5 Database Verification and correct any reported database issues before you upgrade.

> **Tip:** Verifying the Content Server database on a large production system can be time-consuming. It may take more than a day for the verification to complete, but it is an important step in ensuring that your upgrade completes successfully. You can shorten the running time of a database verification of level 3 or higher by temporarily adding an index to your Content Server database.
>
> **Oracle, PostgreSQL, SQL Server, and SAP HANA**
>
> ```
> CREATE INDEX dversdata_providerid ON DVersData (ProviderID);
> ```

After the database verification completes, you can drop the index.

Oracle, PostgreSQL, and SAP HANA

```
DROP INDEX dversdata_providerid;
```

SQL Server

```
DROP INDEX dversdata.dversdata_providerid;
```

To verify the database:

1. Start the Content Server services.
2. In the **Database Administration** section of the **Content Server Administration** page, click **Maintain Current Database**.
3. On the **Maintain Current Database** page, click **Verify This Database**.
4. On the **Verify Content Server Database** page, enable a database diagnostic level, and then click **Perform Diagnostic**.

Verify Microsoft SQL Server Isolation Levels

In Content Server 16.0.0 and later, a SQL Server database is required to have the `READ_COMMITTED_SNAPSHOT` isolation level. In previous versions of Content Server, this setting was recommended, but not required.

To determine if your database has enabled the `READ_COMMITTED_SNAPSHOT` isolation level, Open SQL Server Management Studio and run this query: `SELECT is_read_committed_snapshot_on FROM sys.databases WHERE name='<Content_Server_database>'`. If the query returns a `1`, `READ_COMMITTED_SNAPSHOT` is enabled. If it returns a `0`, it is not.

In preparation for your Content Server upgrade, you should enable the `READ_COMMITTED_SNAPSHOT` isolation level in your source database. If the Content Server database in your Source Environment does not have the `READ_COMMITTED_SNAPSHOT` isolation level, the database upgrade will fail and the following message will appear: **A recoverable error has occurred in the upgrade process. The required READ_COMMITTED_SNAPSHOT setting is not set correctly for this database.** See “Connect to your Content Server Database Copy” on page 35.

To set the READ_COMMITTED_SNAPSHOT SQL Server isolation level:

1. Open Microsoft® SQL Server® Management Studio.
2. Verify that no users or processes are accessing the Content Server database.
3. Run the following command:
   - `ALTER DATABASE <DB_Name> SET READ_COMMITTED_SNAPSHOT ON`

Examine the Database

OpenText Database Diff is a tool that compares two database schemas and reports on the differences between them. It is available on OpenText My Support at https://knowledge.opentext.com/go/41602824.

You can use Database Diff to compare the structure of your existing production database in your Source Environment to the structure of an empty database in your Target Environment (after you have installed all the same modules that exist in your Source Environment). Because the empty database is newly installed, this comparison can help you determine whether you have modified your production Content Server database by adding tables, columns, indexes, views or triggers.

If Database Diff reveals that modifications have been made to the database in your Source Environment, you should verify whether the modifications will serve any purpose in the upgraded environment. If they will not, consider rolling them back before the database upgrade. If you decide to retain any database modifications, you should verify that they remain in place after you have successfully upgraded the copy of your source database. Re-apply them if they have not, but only after you have thoroughly verified that Content Server is working as expected.

Other uses for Database Diff during an upgrade include:

- Compare schemas from your production, QA, Dev, and UAT environments.
- Compare the Content Server database schema before and after an upgrade.
- Compare the Content Server database schema before and after installing a module.

Back up the Database

Make a backup of the Content Server database using the tools and procedures supplied by your database vendor. This database backup is what you will upgrade, after you restore it in your Target Environment. Your actual production database in your Source Environment will be unaffected by the upgrade.

> **Important**
> The current state of your Content Server deployment, including the processes that are enabled or disabled, is captured in the Content Server database. Disabling inessential processes before you copy the database helps to ensure that, after you upgrade the database, Content Server does not start any processes before you have prepared the system for them.
>
> When you make a copy of your database for use in your Target Environment, ensure that:
>
> - The latest Update and patches are installed on the source Content Server. For more information, see “Apply Content Server Updates and Patches” on page 17.

- Global Appearances are disabled. For more information, see "Disable Global Appearances, Agents and Notifications, and Remove Obsolete Modules" on page 17
- Agents and Notifications are disabled. For more information, see "Disable Global Appearances, Agents and Notifications, and Remove Obsolete Modules" on page 17
- Obsolete modules are removed. For more information, see "Disable Global Appearances, Agents and Notifications, and Remove Obsolete Modules" on page 17.
- The Admin Help and User Help data sources are deleted. For more information, see "Delete Help Data Source Folders" on page 19.
- System Object Volume alerts are disabled. For more information, see "Disable System Object Management Alerts" on page 19.
- No Search processes are running. For more information, see "Stop the Search Processes and Copy the Index" on page 20.

1.3.6 Create the Content Server Database in the Target Environment

On the database server in your Target Environment, create an empty database and restore the the database backup that you took in "Back up the Database" on page 23.

Create the Target Database in SQL Server

When a Content Server database that is stored in Microsoft SQL Server is migrated from one version of Content Server to another, it is necessary that the database owner has the same SID (Security Identifier) in both the source and target database. For this reason, migrating a Content Server database stored in SQL Server requires special steps.

To migrate a Content Server database that is stored in Microsoft SQL Server:

1. Obtain the SID of the Content Server database user.

   Run the following query against the Content Server database in your Source Environment:

   ```
   SELECT name, sid FROM sysusers WHERE
   name='<Content_Server_database_user>'
   ```

   Example: `SELECT name, sid FROM sysusers WHERE name='cs_dbuser'`

   This query should return output similar to the following:

   ```
   name        sid
   cs_dbuser   0x53CE9AC3AE668A4990C9EA9C09DCC289
   ```

2. Use the information obtained in step 1 to create a Content Server database user with the same SID. Assign this user to the staging database.

On the target database server, run the following query against the Content Server database:

```
sp_addlogin '<login_name>', '<password>', '<database_name>',
'<language>', <sid>
```

Example: `sp_addlogin 'cs_dbuser', 'password', 'staging', 'us_english', 0x53CE9AC3AE668A4990C9EA9C09DCC289`

3. Create a new database with the same name as the database that you backed up in your Source Environment. Assign the user that you created in step 2 as the owner of this database.

4. Restore the backup of your source database to the database that you created in step 3.

You are now ready to connect to this database in Content Server and to upgrade it to the current version of Content Server.

Disable the Oracle Database Recycle Bin

If your Content Server deployment uses Oracle Database, OpenText recommends that you disable the Oracle Recycle Bin before you upgrade your Content Server database. Testing by OpenText has shown that database locking and timeout errors can occur when you upgrade the Content Server database with the Oracle Recycle Bin enabled.

To determine if the Recycle Bin is enabled, log onto Oracle Database as SYSTEM and run the following query:

```
SELECT value FROM v$parameter WHERE Name='recyclebin';
```

If the Recycle Bin is enabled, this query returns output similar to the following:

```
VALUE
-----------------------------------------------------------
ON
```

To disable the Recycle Bin, log onto Oracle Database as SYSDBA and run the following query:

```
ALTER SYSTEM SET recyclebin = OFF;
```

Alternatively, you could use a logon trigger to disable this feature for only the Content Server database user, as follows:

```
create or replace trigger cs_logon_trigger after logon on
<Content_Server_database_user_name>.schema
begin
execute immediate 'ALTER SESSION SET recyclebin = OFF';
end;
/
```

After you successfully upgrade the Content Server database, re-enable the Oracle Recycle Bin.

1.3.7 Prepare the External File Store

To prepare the External File Store, make a copy of it and store it in the location where Content Server will access it in the Target Environment.

The Content Server database stores the location of your External File Store, so your upgraded Content Server will expect to find the External File Store in the same place as it is located in your Source Environment. If you want, however, you can specify a different External File Store location when you perform the initial configuration of your upgraded Content Server installation.

Tip: A Content Server upgrade may modify Categories, Form Templates and other system configuration objects.

OpenText recommends that you use external storage for documents and emails, and internal (database) storage for system configuration objects. If you store system configuration objects using internal storage, you can perform a preliminary test upgrade of the Content Server database without completely replicating your external file store. You still require a connection to the external file store (because the database upgrade verifies the presence of the external file store before it proceeds), but it does not need to contain all of the documents that are in your production file store.

OpenText recommends, however, that you perform at least one test upgrade connected to a complete replica of your external file store before performing your production upgrade. If that is not possible, after the upgrade is complete, you should perform thorough testing in your production environment to identify any differences between your test and production upgrades.

1.3.8 Migrate Users and Groups

Content Server 16.2.0 requires the use of OpenText™ Directory Services 16.2.0 and later to manage its users. In your Target Environment, you can connect to an external OTDS server or an internal OTDS (an instance of OTDS that is embedded in Content Server).

Note: OpenText recommends that you use an external OTDS server for a production deployment of Content Server.

If you already use OTDS 16.2.0 or later in your Source Environment, you do not need to take additional steps to migrate your Content Server users and groups when you upgrade your Target Environment. But if your Source Environment uses an earlier version of OTDS or if it uses an internal OTDS, you should save your Content Server users, groups, and OTDS configuration information so that you can restore this information in your Target Environment.

In your Source Environment, Content Server users and groups are normally stored in one of the following repositories:

Content Server Users and Groups

In a default installation, Content Server 10.5 and earlier stores user and group information internally. If your Source Environment uses Content Server users and groups, you will perform a migration to OpenText Directory Services when you upgrade Content Server. See "Connect OpenText Directory Services" on page 40.

OpenText Content Server Directory Services

Content Server Directory Services is an optional module for Content Server 10.5 and earlier that provides synchronization and authentication features, including the ability to synchronize Content Server users and groups with an external directory. If your Source Environment uses Content Server Directory Services, you will migrate the Content Server Directory Services sync profile to OpenText Directory Services when you upgrade Content Server, and use the migrated sync profile to import your users and groups to OpenText Directory Services.

For more information on migrating Content Server Directory Services to OpenText Directory Services, see section 5.2.8.3 "Migrating users and groups from Content Server 10.5 to Directory Services 16" in *OpenText Directory Services - Installation and Administration Guide (OTDS-IWC)*

External OpenText Directory Services

If you use an external, or standalone, deployment of OpenText Directory Services 16.0.0 or earlier in your Source Environment, you may need to export your users, groups, and OTDS configuration information to one or more files that you will use when you upgrade to OpenText Directory Services 16.2.0 or later. The specific procedure depends on the version of OTDS that is deployed in your Source Environment.

For more information on upgrading OpenText Directory Services, see section 1.2 "Importing data from previous versions of Directory Services" in *OpenText Directory Services - Installation and Administration Guide (OTDS-IWC)*.

Internal OpenText Directory Services

If you use an internal OTDS server in your Source Environment, you will export your users, groups, and OTDS configuration information to an LDIF file. When you upgrade Content Server, you will import the LDIF file to reconstitute your Content Server users, groups, and OTDS configuration data. For information on importing the LDIF file from an internal OTDS, see "Enable an Internal OTDS Server" on page 42.

Tip: The option to create and use an internal OTDS server exists in Content Server 16.0.0 and later.

Exporting Users and Groups from an Internal OTDS

This section contains instructions on exporting users, groups, and configuration data from your internal OTDS to an LDIF file. When you upgrade Content Server, you will use this file to restore your OTDS data to an internal OTDS that you create in Content Server 16.2. Store this file along with your other important Content Server upgrade files.

The procedure varies according to the version of Content Server that you are upgrading:

- For Content Server 16.0.1 or earlier, follow the steps in "Exporting Users and Groups from an Internal OTDS in Content Server 16.0.1 and earlier" on page 29.
- For later versions of Content Server 16, follow the steps in "Exporting Users and Groups from an Internal OTDS in Content Server 16.0.2 and later" on page 28.

Note: These steps are not necessary (or available) if your Source Environment uses Content Server users and groups, Content Server Directory Services, or a standalone installation of OpenText Directory Services. They are necessary only if your Source Environment uses an internal OTDS. The use of an internal OTDS is available only in Content Server 16.0.0 and later.

Exporting Users and Groups from an Internal OTDS in Content Server 16.0.2 and later

Complete the following steps to export users and groups from an internal OTDS in Content Server 16.0.2 and later.

To export users and groups from an Internal OTDS in Content Server 16.0.2 and later

1. Open the **Deselect Content Server Database** page.

   On the Content Server Administration page, click **Change Current Database**.

   Tip: You can export your OTDS data without actually changing your current Content Server database.

2. On the **Deselect Content Server Database** page, click **Export OTDS data**.
3. On the **OTDS Data Export** page, enable **Export OTDS data**. In the **LDIF data file** box, enter the path where you want the LDIF file to be saved on the Content Server host computer. Click **Continue**.
4. The **OTDS Data Export Status** page appears, and shows the message `OTDS data export has completed successfully`. The LDIF file is saved at the path that you specified in the previous step.

Exporting Users and Groups from an Internal OTDS in Content Server 16.0.1 and earlier

Complete the following steps to export users and groups from an internal OTDS in Content Server 16.0.1 and earlier.

To export users and groups from an Internal OTDS in Content Server 16.0.1 and earlier

1. Log on as an administrator to the Content Server computer that runs your internal OTDS. Open an administrator command window.
2. Reset the OpenDJ Directory Manager password that your internal OTDS installation set for you at installation:

   a. Stop the Content Server services.

   b. Change directory to the internal OTDS installation path: `<Content_Server_home>\module\otdsintegration_16_0_0\otds\install\`

   c. Type the following command:

   ```
   java -jar otds-deploy.jar -resetpassword <new_password>
   ```

   d. Restart the Content Server services.
3. Use the `export-ldif` executable to generate an `otds-16.0.0.ldif` file. This is an `LDIF` export of the entire OpenDJ user database.

   The `export-ldif` executable is found:

   - on Windows, in the `<Content_Server_home>\module\otdsintegration_16_0_0\otds\opendj\bat\` directory.
   - on Linux, in the `<Content_Server_home>/module/otdsintegration_16_0_0/otds/opendj/bin/` directory.

   Open a command window while logged in as an administrator and type the following command:

   ```
   export-ldif "--ldifFile" "otds-16.0.0.ldif" "--backendID"
   "userRoot" "--appendToLDIF" "--hostName" "localhost" "--port" "4444"
   "--bindDN" "cn=Directory Manager" "--bindPassword"
   "<bind_Password>" "--trustAll" "--noPropertiesFile"
   ```

   Note: The *<bind_Password>* is the password that you reset in Step 2.
4. Store the `otds-16.0.0.ldif` file along with your other important Content Server upgrade files.

1.4 Install the New Version of Content Server on the Operating System

Now that you have prepared Content Server in your Source Environment, you are ready to install the new version of Content Server in your Target Environment, and upgrade a copy of the Content Server database from your Source Environment. To simplify your upgrade, it is advantageous to install and configure this target instance so that it is the same as your Source Environment in the following ways:

- The installation folder is on the same drive and has the same name.
- It uses the same network ports.
- The External File Store and `Index` folders have the same names as they do in the Source Environment and are located in the same place relative to the installation folder.

> **Tip:** If you need to change network ports or modify the location of your External File Store and `Index` folders, you can adjust for this and other changes when you run the Content Server installer, or during the initial configuration of Content Server. See "Connect Storage Providers" on page 37, "Connect Admin Servers" on page 36, and "Configure and Migrate the Search System" on page 44.

If your Source Environment has multiple Admin servers and Front-End Instances, the first instance that you configure is your Default Admin server, but before you do that, you need to install every Admin Server in your Target Environment.

That is because, to complete the configuration of your Default Admin server, you must connect to an Additional Admin server for every Additional Admin server that is specified in your Content Server database. In other words, for every Additional Admin server that exists in your Source Environment, you will need to connect to an Additional Admin server in your Target Environment. Run the operating system installation of Content Server on the computers that will host your Additional Admin servers and then start up (only) the Content Server Admin service on these computers. Do this before you configure your Default Admin server, so you can connect to them during its intial setup.

After you complete the creation and configuration of your Search environment, you will install your front-end Content Server instances. (See "Add Front-End Content Server Instances" on page 48.)

This section covers the following topics:

- "Install Admin Servers on the Operating System" on page 31

1.4.1 Install Admin Servers on the Operating System

Run the Content Server installer on every computer that will host an Additional Admin server. Copy the `LLFieldDefinitions.txt`,`LLFieldDefinitions_EL.txt`, and `otadmin.pwd` files that you copied from the corresponding Additional Admin server in your Source Environment to the *<Content_Server_home>*`\config\` folder . (See "Stop the Search Processes and Copy the Index" on page 20.) Start up the Content Server Admin service only.

Note: For detailed information about installing Content Server, see *OpenText Content Server - Installation Guide (LLESCOR-IGD)* and review the Content Server Release Notes.

Perform the following steps on the computer that will become your Default Admin server.

To install Content Server

1. On a new computer in the Target Environment, install the operating system. Install and test a database client. Disable virus-scanning on selected folders. Install and configure a web server.

2. Install Content Server. If possible, install it in the same folder as in your Source Environment, set the support directory mapping to the same name as your Source Environment, and use the same values for **Service Port**, **Admin Port**, and **Cluster Agent Port**. (If that is not possible, configure them to use an available port and make the necessary adjustments on the **Admin Server Configuration** page when you configure your first Content Server instance.)

   When the installation completes, do not start the services.

3. Copy the `LLFieldDefinitions.txt`,`LLFieldDefinitions_EL.txt`, and `otadmin.pwd` files that you copied from the corresponding Additional Admin server in your Source Environment to the *<Content_Server_home>*`\config\` folder . (See "Stop the Search Processes and Copy the Index" on page 20.)

4. Set up your virtual directories in your web server if the installer did not do it automatically, and complete the configuration of your web server for use with Content Server.

   Tip: Web server configuration is performed automatically by the installation program for Microsoft Internet Information Services and Apache Tomcat.

5. Create a Content Server operating system user and configure the Content Server services to run as that user.

1.5 Connect and Upgrade Content Server Components

At this point, you have run the operating system installation of Content Server on a host in the Target Environment for each Admin server that exists in your Source Environment. You have copied your `Index` directory tree and the External File Store to their locations in the Target Environment. A copy of the database from your Source Environment is available on the database server that you will use in the Target Environment.

You are now ready to start the first instance of Content Server (your Default Admin server), configure it, and upgrade the Content Server database.

Note: During the entire upgrade procedure described in this section, do not run the Content Server Cluster Agent. Leave this service off on all Content Server instances until the upgrade is complete.

This section follows the order of your initial configuration of Content Server. It covers the following topics:

- "Modify the opentext.ini File" on page 32
- "Configure Server Parameters" on page 34
- "Connect to your Content Server Database Copy" on page 35
- "Upgrade Content Server Modules" on page 35
- "Connect Admin Servers" on page 36
- "Connect Storage Providers" on page 37
- "Upgrade the Content Server Database" on page 37
- "Configure Modules" on page 40
- "Connect OpenText Directory Services" on page 40
- "Configure and Migrate the Search System" on page 44
- "License Content Server and Modules" on page 46

1.5.1 Modify the opentext.ini File

When you apply an Update or upgrade Content Server, some of the settings that reside in the `opentext.ini` file may be moved to the Content Server database. After an `opentext.ini` setting is moved to the database, it is configurable from the Content Server Administration pages.

In some cases, for the migration of settings to work correctly, the settings must appear in the opentext.ini file before the database upgrade, so that Content Server can read the settings' values and migrate them to the database. As a way of verifying the success of your upgrade, you can identify any settings that exist in the source opentext.ini file that do not appear in the target opentext.ini file. Determine if these settings are available on the Administration pages in your upgraded environment. Pay special attention to any settings that you have moved from their default values.

If you are upgrading from Content Server 10.5 or later and you have applied the latest Update to your Source Environment before your upgrade, there should be few settings that require your attention. If you are upgrading from an earlier version of Content Server, however, you may need to do some research to determine whether a given opentext.ini setting in your Source Environment needs to be added to the opentext.ini file in your Target Environment, or set in the Content Server Administration pages.

The Content Server release notes contain information on settings that have been migrated from the opentext.ini and other similar configuration files. You can also review the contents of your *<Content_Server_home>*/config/config_reference file for examples of upgraded configuration files.

Be sure to note any changes you make to the opentext.ini file. In an environment that has multiple instances of Content Server, you will need to modify the opentext.ini file on each instance in your cluster.

Disable Agents in the opentext.ini File

Open the opentext.ini file, and edit it so that non-essential agents do not run.

Tips

- You will re-enable these agents before you make your upgraded Content Server deployment available to your user base. See "Perform Post-Upgrade Checks and Basic Testing" on page 50.
- You previously disabled Notifications using the Content Server user interface, so you will need to re-enable it there too when you bring Content Server online. See "Disable Agents and Notifications" on page 18.

To disable agents in the opentext.ini file:

1. Stop the Content Server services.
2. Open the opentext.ini file.
3. Edit the [loader] section, so that only load=sockserv is not commented out.

   Example: If the [loader] section of the opentext.ini file has this appearance:

   ```
   [loader]
   load=sockserv;agents;notify;wfagent;wrscheduleagent;wrcollectiona
   gent
   ```

```
load_relagent=relagent
load_distributedagent=distributedagent
load_daagent=daagent
load_verify=verifyAgent
```

Change it so that it has the following appearance:

```
[loader]
load=sockserv
#;agents;notify;wfagent;wrscheduleagent;wrcollectionagent
#load_relagent=relagent
#load_distributedagent=distributedagent
#load_daagent=daagent
#load_verify=verifyAgent
```

4. Save and close the `opentext.ini` file.

1.5.2 Configure Server Parameters

Start up the Content Server and Content Server Admin services on the computer where you just ran the operating system installation of Content Server. Do not start the Content Server Cluster Agent service at this time.

Enter the Content Server Administration page URL, using the URL extension `?func=admin.index`. Because this is the first time that you are opening this page, you are redirected to the **Configure Server Parameters** page.

Enter appropriate settings on the **Configure Server Parameters** page. At a minimum, you must enter a **Web Administrator Password**.

Leave **Enable Logging During Installation** selected. If an issue occurs during the upgrade, OpenText Customer Support can analyze the log files to determine the root cause of the issue.

If you have determined that Content Server should run with a different number of threads than the default number (8), set the desired thread levels in the **Number of Threads** box on the **Configure Server Parameters** administration page. If you are unsure what value to assign, leave the default values in place.

When you have entered values for any of the settings that you want to configure at this time, click **Save Changes**.

When the **Select Default Metadata Language** page appears, select a default metadata language, and then click **Continue**.

1.5.3 Connect to your Content Server Database Copy

In your Target Environment, you have ensured that a copy of the database from your Source Environment is available on your database server and a copy of your External File Store is available on the file system.

> **Important**
>
> Content Server must have a connection to its Storage Providers during the database upgrade so that it can read information on system configuration objects (for example, Categories and Form Templates) and, if necessary, modify them.

Connect to the Database Copy

Connect to the copy of the Source Environment database, and start the Content Server database upgrade.

To upgrade the database from the Source Environment:

1. On the **Database Administration** page, click **Select Existing Database**.
2. On the following pages, select the appropriate database server type, and enter the connection information for the copy of the Content Server database from your Source Environment.
3. On the **Content Server Administrator User Log-in** page, enter the password for the Admin user, and then click **Log-in**.

1.5.4 Upgrade Content Server Modules

After you have connected to a copy of the database from your Source Environment and logged onto Content Server as the Content Server Admin user, the **Install Modules** page appears.

The **Install Modules** page identifies modules that you must install before you can proceed with your Content Server upgrade. Review and correct the errors that appear in the **Module Errors** section. You must resolve every module error before you can continue with the upgrade.

Modules that appear with an error type of **Missing software** represent modules that are installed in your Source Environment. Your database copy has information about such modules and each one must be installed before you can proceed beyond this page. Once you have installed every missing module, Content Server advances you to the **Admin Server Configuration** page.

If your upgrade plan includes the installation of new Content Server modules that do not exist in your Source Environment, you can add them now or after you complete the initial configuration of the upgraded system. To add new modules to your Content Server Target Environment, use your browser's **Back** button to return to the **Install Modules** page. For information on installing optional modules, see *OpenText Content Server - Module Installation and Upgrade Guide (LLESCOR-IMO)*.

1.5.5 Connect Admin Servers

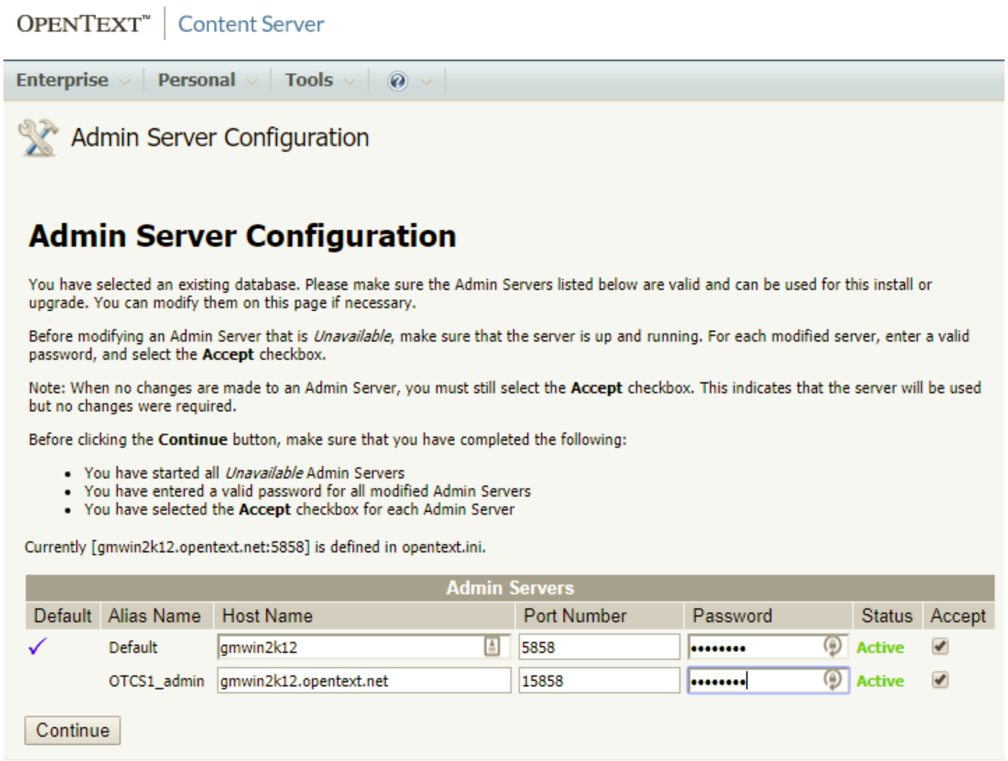
The **Admin Server Configuration** page displays the **Host Name** and **Port Number** of the Admin servers in your Source Environment. You need to change these values for the Additional Admin servers in your Target Environment.

Tip: You previously installed Content Server on the computers that you identified for this role, and started the Content Server Admin service on each of them. (See “Install Admin Servers on the Operating System” on page 31.)

For each Admin server, ensure that the **Host Name** and **Port Number** boxes contain the correct values for your Target Environment. If an Admin server **Status** is **Connect failed**, make sure that it is running and that you have entered the correct Admin server password.

Content Server stores the Admin server password in its database and in the `otadmin.pwd` file that you copied into the *<Content_Server_home>*`\config\` folder earlier. If you see the message **You have entered an incorrect password**, ensure that you are using the correct password from your Source Environment and that you have copied the correct `otadmin.pwd` file into the *<Content_Server_home>*`\config\` folder

Ensure that, for each Admin server, the **Status** is **Active** and the **Accept** check box is selected.



Admin Server Configuration

You have selected an existing database. Please make sure the Admin Servers listed below are valid and can be used for this install or upgrade. You can modify them on this page if necessary.

Before modifying an Admin Server that is *Unavailable*, make sure that the server is up and running. For each modified server, enter a valid password, and select the **Accept** checkbox.

Note: When no changes are made to an Admin Server, you must still select the **Accept** checkbox. This indicates that the server will be used but no changes were required.

Before clicking the **Continue** button, make sure that you have completed the following:

- You have started all *Unavailable* Admin Servers
- You have entered a valid password for all modified Admin Servers
- You have selected the **Accept** checkbox for each Admin Server

Currently [gmwin2k12.opentext.net:5858] is defined in opentext.ini.

Admin Servers

Default	Alias Name	Host Name	Port Number	Password	Status	Accept
✓	Default	gmwin2k12	5858	••••••••	Active	☑
	OTCS1_admin	gmwin2k12.opentext.net	15858	••••••••	Active	☑

When you have verified the configuration of each Admin server, click **Continue**.

1.5.6 Connect Storage Providers

When the **Configure Storage Providers** page appears, review the Storage Providers that appear and ensure that their configuration is correct. If the **Provider Configuration** is not correct, click **Edit** and enter the correct values.

If you want to add additional Storage Providers, you can add Enterprise Archive or External Document Storage now. You can also add Storage Providers later after you have completed your upgrade.

Once you have verified that your Storage Providers are correct, click **Continue** to proceed with your Content Server upgrade.

If the **Content Server Administrator User Log-in** page appears, enter the password for the Admin user, and then click **Log-in**.

1.5.7 Upgrade the Content Server Database

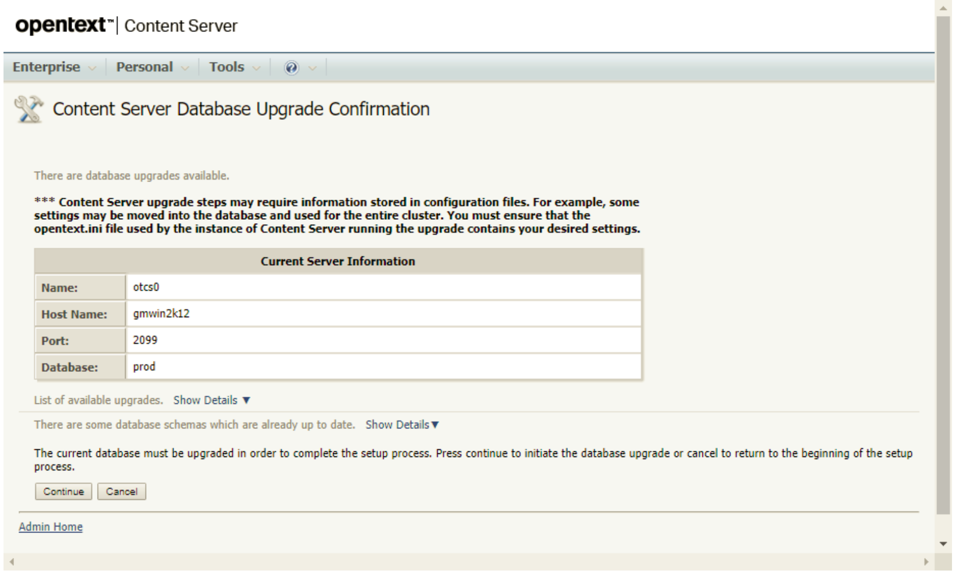
At this point in the upgrade, you have:

- installed all required modules on the operating system and in Content Server
- connected to every required Admin server
- connected to every required Storage Provider

You are now ready to upgrade your copy of the Content Server database from your Source Environment.

Upgrading the Content Server Database

1. On the **Content Server Database Upgrade Confirmation** page, click **Continue**.



Content Server Database Upgrade Confirmation

There are database upgrades available.

***** Content Server upgrade steps may require information stored in configuration files. For example, some settings may be moved into the database and used for the entire cluster. You must ensure that the opentext.ini file used by the instance of Content Server running the upgrade contains your desired settings.**

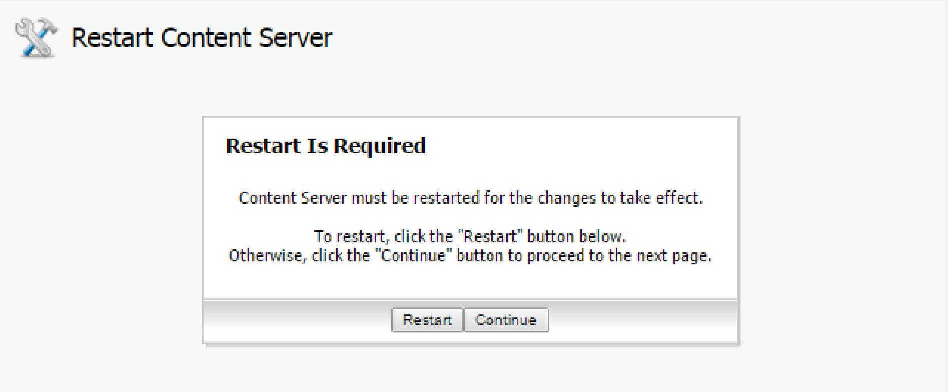
Current Server Information	
Name:	otcs0
Host Name:	gmwin2k12
Port:	2099
Database:	prod

List of available upgrades. Show Details ▼

There are some database schemas which are already up to date. Show Details ▼

The current database must be upgraded in order to complete the setup process. Press continue to initiate the database upgrade or cancel to return to the beginning of the setup process.

2. When the **Restart Content Server** page appears, click **Restart** to restart Content Server automatically (or click **Continue** if you prefer to restart Content Server using the operating system.)



Restart Content Server

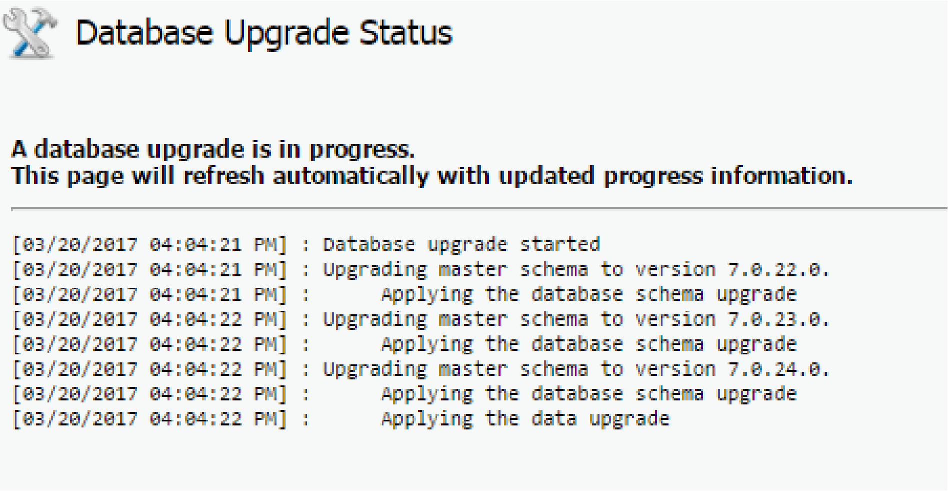
Restart Is Required

Content Server must be restarted for the changes to take effect.

To restart, click the "Restart" button below.
Otherwise, click the "Continue" button to proceed to the next page.

3. When the **Restart Successful** message appears, click **Continue**. The **Database Upgrade Status** page appears.

4. On the **Database Upgrade Status** page, a series of messages indicate the progress of your database upgrade.



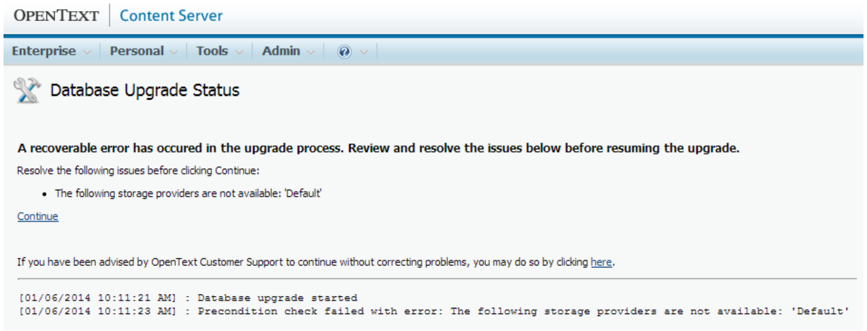
Database Upgrade Status

A database upgrade is in progress.
This page will refresh automatically with updated progress information.

```
[03/20/2017 04:04:21 PM] : Database upgrade started
[03/20/2017 04:04:21 PM] : Upgrading master schema to version 7.0.22.0.
[03/20/2017 04:04:21 PM] :      Applying the database schema upgrade
[03/20/2017 04:04:22 PM] : Upgrading master schema to version 7.0.23.0.
[03/20/2017 04:04:22 PM] :      Applying the database schema upgrade
[03/20/2017 04:04:22 PM] : Upgrading master schema to version 7.0.24.0.
[03/20/2017 04:04:22 PM] :      Applying the database schema upgrade
[03/20/2017 04:04:22 PM] :      Applying the data upgrade
```

! **Important**

If Content Server indicates that a recoverable error has occurred in the upgrade process, correct the issue and then click **Continue**.



Database Upgrade Status

A recoverable error has occured in the upgrade process. Review and resolve the issues below before resuming the upgrade.

Resolve the following issues before clicking Continue:

- The following storage providers are not available: 'Default'

Continue

If you have been advised by OpenText Customer Support to continue without correcting problems, you may do so by clicking here.

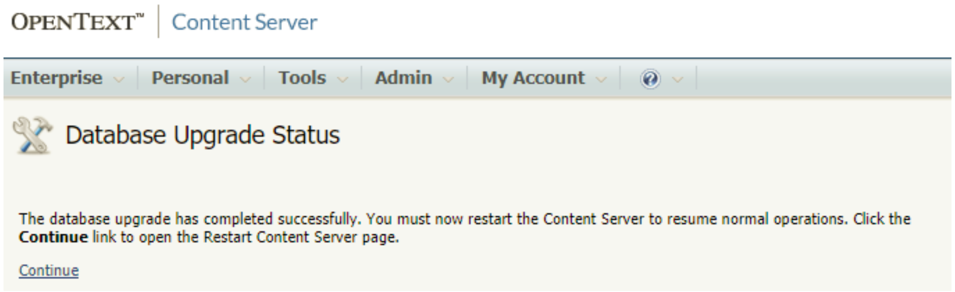
```
[01/06/2014 10:11:21 AM] : Database upgrade started
[01/06/2014 10:11:23 AM] : Precondition check failed with error: The following storage providers are not available: 'Default'
```

On the bottom of the **Database Upgrade Status** page, verify that the message `The database upgrade completed with no errors` appears. If the database upgrade completes successfully, and no errors are present, click **Continue**.

Important

Review the text on the page carefully. Occasionally the **Database Upgrade Status** page may display the message `The database upgrade has completed successfully` when the page also displays messages indicating the occurrence of errors that were not sufficient to halt the database upgrade.

If any errors appear, do not attempt to continue the upgrade or restart the upgrade where it left off. Contact OpenText Customer Support.



Database Upgrade Status

The database upgrade has completed successfully. You must now restart the Content Server to resume normal operations. Click the **Continue** link to open the Restart Content Server page.

Continue

5. The **Restart Content Server** page appears and Content Server is automatically restarted.

6. The **Database Upgrade Status** page appears again. Click **Continue**.

The database migration is now complete. You are now ready to continue with the overall upgrade of Content Server. Click **Continue**.

1.5.8 Configure Modules

Now that you have upgraded the Content Server database, Content Server needs to configure the modules that you installed earlier. (See “Upgrade Content Server Modules” on page 35.) The **Configure Modules** page appears. Click **Continue** and observe that the configuration of each upgraded module completes successfully.

Note: If errors occur on this page, you cannot proceed with the upgrade of Content Server. Contact OpenText Customer Support or the third-party module provider.

When the **Restart Content Server** page appears, click **Restart** to restart Content Server automatically (or click **Continue** if you prefer to restart Content Server using the operating system.)

When the **Restart Successful** message appears, click **Continue**.

1.5.9 Connect OpenText Directory Services

The **Configure OTDS Integration Settings** page appears.

Content Server uses OpenText Directory Services to manage its users. You can choose to use an internal instance of OTDS that is embedded in Content Server, or connect to an external OTDS server. OpenText recommends that you use an external OTDS server for a production deployment of Content Server.

Note: It is possible to use an internal instance of OTDS upon initial installation and later to migrate to using an external OTDS server. For more information, refer to the OTDS documentation.

Enable an External OTDS Server

For a production deployment of Content Server, OpenText recommends that you connect to an external OTDS Server for user management.

To connect to an external OTDS Server, you need two pieces of information:

- The address of the OTDS Server.
- The ID of the Resource that has been set up in OTDS for use with Content Server.

Tip: The Resource Identifier is available in OpenText Directory Services in the Properties of the Resource.

In addition, if you use a proxy or have a containerized environment, you have the option of providing an explicit OTDS login URL.

For more information on OpenText Directory Services, see *OpenText Directory Services - Installation and Administration Guide (OTDS-IWC).*

To enable an external OTDS Server

1. On the **Configure OTDS Integration Settings** page, select **External OTDS Server** in the **Server Type** menu.
2. In the **Server URL** box, enter the host name (or IP address) and port of your OTDS server. For example, enter `http://MyOtdsServer.corp.com:8080/`.
3. In the **Resource ID** box, enter the Resource Identifier of the OTDS Resource that has been set up for use with Content Server. For example, enter `dba563af-b01d-4f88-bc42-2493c97dbc87`.
4. Optional To explicitly set an OTDS URL to which users should be redirected, enable **Set OTDS login URL**, and then enter the OTDS URL in the **Login URL** box. For example, enter `https://servername.domain.com` or `https://servername.domain.com:8443`.
5. Click **Continue**.
6. The **User and group migration** page appears. In the **OTDS Partition** box, enter a name or accept the default, **Content Server members**. This is the partition that stores users and groups created in Content Server or migrated from the Content Server database.
7. Enable any migration options that apply. Your choices on this page depend on how users and groups are managed in your Source Environment. See “Migrate Users and Groups” on page 26.

   Migration

   Enable **Migrate users and groups from the Content Server database** if the database that you upgraded contains internal users and groups or if it uses Content Server Directory Services, and you are using OTDS for this first time. Do not enable it if the deployment of Content Server that you are upgrading already uses OTDS.

   After you enable **Migrate users and groups from the Content Server database**, additional options become available.

   Migrate internal users and groups

   Enable this option to migrate internal users and groups. All existing users and groups in OTDS contained in the **OTDS Partition** will be replaced with users and groups in the current database.

   Migrate (Tempo) external users and groups

   Enable this option to migrate external (Tempo) users and groups. All existing users and groups in OTDS contained in the **OTDS Partition** will be replaced with users and groups in the current database.

   Content Server Directory Services users and groups

   Any Content Server Directory Services synchronization sources that Content Server detects appear on this page. Enable this option to migrate Content Server Directory Services users and groups.

> **Note:** The migration function does not directly migrate CSDS users and groups. It migrates the CSDS sync profile into OTDS. You can use the sync profile to import users and groups into OTDS

Import
This option is used to import users and groups from an internal OTDS server to a new internal OTDS server. Do not enable this option if you are connecting to an external OTDS server.

Click **Continue**.

8. The **Migration Status** page appears. when `The migration has completed successfully` appears, click **Continue**.

After you successfully connect to the OTDS Server, the **Configure and Migrate the Search System** page appears. Proceed to "Configure and Migrate the Search System" on page 44 to continue the initial configuration of your upgraded Content Server deployment.

Enable an Internal OTDS Server

An internal OTDS server is suitable for a test deployment of Content Server or for a limited production deployment. For production deployments of Content Server, OpenText recommends that you use an external OTDS server.

The internal OTDS server uses a Jetty web and servlet server that is built into Content Server. By default, the internal OTDS server uses a self-signed certificate for HTTPS communications, but you can configure it to use a different certificate by entering appropriate values in the **Java Key Store** settings in the **HTTPS Configuration** section. For more information on configuring Jetty to use a specific certificate, refer to the Jetty documentation.

> **Tip:** Documentation for Jetty, which is a third-party software component, is available on the public Internet. For example, for information on creating a Java keystore, see http://www.eclipse.org/jetty/documentation/current/configuring-ssl.html.

To enable an internal OTDS Server

1. On the **Configure OTDS Integration Settings** page, select **Internal OTDS Server** in the **Server Type** menu.

2. Enter available ports in the boxes in the **OTDS Parameters** and **Jetty Parameters** sections. You can accept the default ports or specify different ones. Click **Check port** to verify that the specified ports are not in use.

3. Optional To configure the internal OTDS Server to use a security certificate of your choice, rather than the default self-signed certificate, enter Java key store parameters in the **HTTPS Configuration** section.

4. Optional To explicitly set an OTDS URL to which users should be redirected, enable **Set OTDS login URL**, and then enter the OTDS URL in the **Login URL** box. For example, enter `https://servername.domain.com` or `https://servername.domain.com:8443`.

   Tip: You many need to enter an explicit OTDS URL if you use a proxy or have a containerized environment.

5. Click **Continue**.

6. The **OTDS Deployment Status** page appears. Click **Show Details** to view log information that shows the progress of the deployment. When the `OTDS deployment has completed successfully` message appears, click **Continue**.

7. The **User and group migration** page appears. In the **OTDS Partition** box, enter a name or accept the default, **Content Server members**. This is the partition that stores users and groups created in Content Server or migrated from the Content Server database.

8. Enable any migration options that apply. Your choices on this page depend on how users and groups are managed in your Source Environment. See "Migrate Users and Groups" on page 26.

   Migration

   Enable **Migrate users and groups from the Content Server database** if the database that you upgraded contains internal users and groups or if it uses Content Server Directory Services.

   After you enable **Migrate users and groups from the Content Server database**, additional options become available.

   Migrate internal users and groups

   Enable this option to migrate internal users and groups.

   Migrate (Tempo) external users and groups

   Enable this option to migrate external (Tempo) users and groups.

   Content Server Directory Services users and groups

   Any Content Server Directory Services synchronization sources that Content Server detects appear on this page. Enable this option to migrate Content Server Directory Services users and groups.

   Note: The migration function does not directly migrate CSDS users and groups. It migrates the CSDS sync profile into OTDS. You can use the sync profile to import users and groups into OTDS

Import

If the Content Server database that you have upgraded is from a Content Server deployment that uses an internal OTDS, enable **Import OTDS data** to import an `LDIF` file containing the users and groups associated with this database. For more information, see section 1.5 "Your Directory Services installation and Content Server" in *OpenText Directory Services Integration Administration - OpenText Content Server (LLESDSI-H-AGD)*.

Click **Continue**.

9. The **Migration Status** or **OTDS Data Import Status** page appears. When a message indicates that the migration or data import has completed successfully, click **Continue**.

After the migration completes, the **Configure and Migrate the Search System** page appears. Proceed to "Configure and Migrate the Search System" on page 44 to continue the initial configuration of Content Server.

1.5.10 Configure and Migrate the Search System

At this point in the upgrade, you have connected and upgraded a copy of your production database in the Target Environment and you have connected to OTDS and migrated your users and groups. It is time to migrate your search infrastructure to the Target Environment.

The first step is to adjust any search paths and DCS settings to reflect differences between your Source and Target Environments.

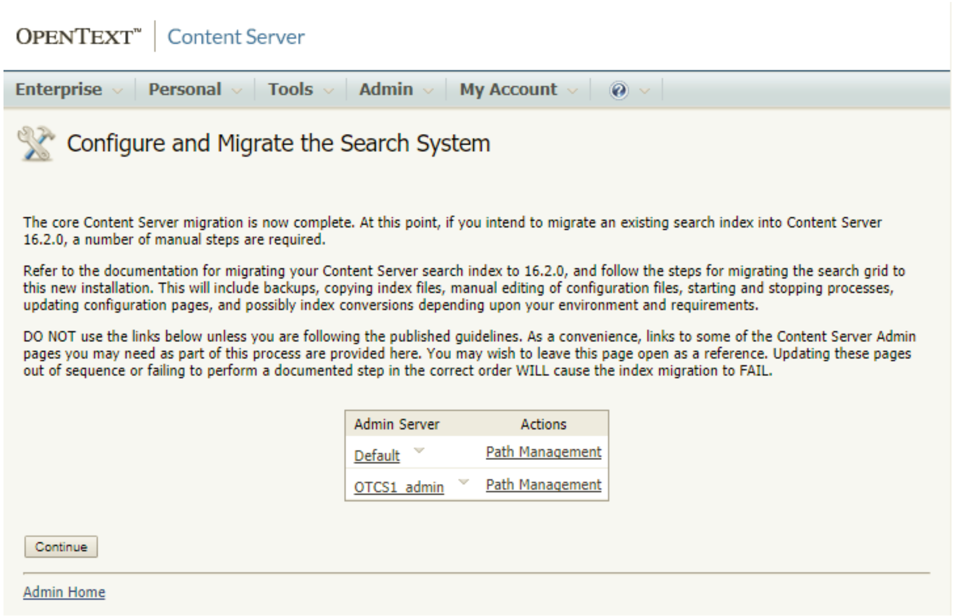
Tip: If you have configured your Target Environment with the same search paths and DCS settings that are used in your Source Environment, you do not need to perform this step.

Important

At this point, the Search and Indexing processes are stopped. (See "Stop the Search Processes and Copy the Index" on page 20.) Do not start the Search processes now. You will start them up later. (See "Resynchronize Admin Servers and Start Search and Indexing Processes" on page 47.)

To connect the Search Index from the Source Environment:

1. On the **Configure and Migrate the Search System** page, open a browser tab or window for each link under **Admin Server** and **Actions**.



Configure and Migrate the Search System

The core Content Server migration is now complete. At this point, if you intend to migrate an existing search index into Content Server 16.2.0, a number of manual steps are required.

Refer to the documentation for migrating your Content Server search index to 16.2.0, and follow the steps for migrating the search grid to this new installation. This will include backups, copying index files, manual editing of configuration files, starting and stopping processes, updating configuration pages, and possibly index conversions depending upon your environment and requirements.

DO NOT use the links below unless you are following the published guidelines. As a convenience, links to some of the Content Server Admin pages you may need as part of this process are provided here. You may wish to leave this page open as a reference. Updating these pages out of sequence or failing to perform a documented step in the correct order WILL cause the index migration to FAIL.

Admin Server	Actions
Default	Path Management
OTCS1_admin	Path Management

2. On each **Admin Server:<*server_name*>** page, verify that the expected processes appear and that they are not running, and then click **Update**.

3. On each **Admin Server Path Management** page:

    a. Make any required adjustments to the values for Partition Location Manager Paths, and then click **Update Partition Location Manager Paths**.

    b. Make any required adjustments to the values for Process Paths, and then click **Update Process Paths**.

    Tip: If necessary, you can return to this page later. To access the **Admin Server Path Management** page after your initial configuration of Content Server, click **Path Management** on the **Functions** menu of any Admin Server.

4. When you have finished configuring your Admin Servers, close the additional browser tabs or windows that you opened, and then click **Continue** on the **Configure and Migrate the Search System** page.

1.5.11 License Content Server and Modules

On the **License Setup** page, apply any required licenses for your Content Server installation.

When you upgrade to a new major version of Content Server, you must obtain a new Content Server license file. Until you apply the license for your new version of Content Server, the **Licensed Version** will appear as the version of Content Server that you are upgrading (for example, `10.5.x` or `16.0.0` and the **Status** will appear as `Invalid Version`.

If you do not have a license, you can continue to use Content Server in administrative mode, but only users with the `System administration rights` privilege will be able to log onto Content Server. To make Content Server available to regular users after you complete your upgrade, apply a Content Server license using OpenText Directory Services. You will no longer be able to apply a license using the Content Server **License Setup** administration page. For information on OpenText Directory Services, see *OpenText Directory Services - Installation and Administration Guide (OTDS-IWC)*.

For information on licensing Content Server and Content Server modules, refer to *OpenText Content Server Admin Online Help - Content Server Administration (LLESWBA-H-AGD)*(under **Server Configuration** in the online Help) or *OpenText Content Server - Installation Guide (LLESCOR-IGD)*.

After you have applied all of your Content Server licenses, click **Continue**. The **Congratulations** page appears, informing you that you have successfully set up Content Server and the database.

1.5.12 Run Cluster Management to Ensure All Patches Are Applied

Run Cluster Management to update the patches on every Content Server instance in your environment.

Apply Updates and Patch your content server up to date

1. Start the Content Server Cluster Agent.
2. If necessary, apply the latest Update for Content Server. (For most Updates, a new Content Server installer is released that installs Content Server and the Update in a single installation, so you have probably already applied the latest Update.) For more information, see “Installing Content Server Updates“ on page 53.
3. Use Cluster Management to ensure that your deployment of Content Server has all of the patches that are appropriate for it. For information on Cluster Management, see *OpenText Content Server Cluster Management - Admin Online Help (LLESPAT-H-AGD)*.

OpenText Content Server Cluster Management manages the application of Content Server patches, Updates and Language Packs, on a single instance of Content Server and throughout a Content Server cluster. Cluster Management automatically handles patch dependencies and removes superseded patches when a newer or more complete version of a patch is applied.

You should run Cluster Management whenever you make changes to your Content Server deployment. Cluster Management checks whether patches are available for your version of Content Server and the modules that are installed on it. If any patches are available, it automatically downloads and installs them to every instance of Content Server running in your Content Server deployment.

For information on configuring and using Cluster Management, refer to *OpenText Content Server Cluster Management - Admin Online Help (LLESPAT-H-AGD)*. You can access this Help topic by clicking **Help for this Page** on the **Cluster Management** administration page.

1.6 Start up Search and Indexing and add Front-End Instances

At this point in the upgrade, you have installed of your Admin servers. You have performed the initial configuration of your Default Admin server, which included upgrading your Content Server database, connecting your Storage Providers, connecting to OpenText Directory Services, and connecting every Additional Admin server in your search and indexing environment. Your search index is in place.

However, you have not applied any changes that you made on the **Configure and Migrate the Search System** page ("Configure and Migrate the Search System" on page 44), and you have not yet added any Front-End Instances.

Begin by resynchronizing your Admin servers and starting up the Search and Indexing processes.

1.6.1 Resynchronize Admin Servers and Start Search and Indexing Processes

Resynchronizing the Admin servers applies the changes that you made in "Configure and Migrate the Search System" on page 44. Perform the following steps on your Default Admin server.

To resynchronize the Admin Servers:

1. In the **Search Administration** section of the **Content Server Administration** page, click **Open the System Object Volume**. Confirm that the search and indexing processes are idle.
2. On the **Functions** menu of each Admin server, click **Resynchronize**.
3. Once each Admin server is successfully resynchronized, start the Search and Indexing processes.

1.6.2 Verify the Migrated Search Index

The Search Index is now up and running. Run an index verification to confirm that there are no issues.

For instructions on running an index verification, see "Run an Index Verification" on page 19.

1.6.3 Recreate Data Sources

Recreate the Admin and User Help data sources.

Note: When you prepared the Source Environment for migration, you deleted the Admin and User Help data sources. (For more information, see "Delete Help Data Source Folders" on page 19.)

Perform the following steps for both of the Help data sources.

To recreate the Help data sources:

1. In the **Search Administration** section of the **Content Server Administration** page, click **Open the System Object Volume**.
2. Click **Add New Item**, and then click **Admin Help Data Source** or **User Help Data Source**.

   Tip: To create the data source outside of the Content Server application folder, change the default location of the Base Directory to a subfolder of your `Index` folder, or another location of your choice.

3. Click **Create New Processes**.

If you deleted any other data sources (for example, Spiders or Directory Walkers) before backing up your index and database, recreate those data sources now.

1.6.4 Add Front-End Content Server Instances

Your Target Environment has only Admin servers at this point. Add any Front-End Content Server instances that are required.

For information on installing additional instances of Content Server, see *OpenText Content Server - Installation Guide (LLESCOR-IGD)*.

Cloning Content Server Installations

To set up a Front-End instance, you can re-do the steps that you performed in "Install the New Version of Content Server on the Operating System" on page 30 and "Connect and Upgrade Content Server Components" on page 32. Because the database is already upgraded at this point, and it contains good information for your Storage Providers, Search and Indexing environment, and OTDS, the installation should be straightforward. However, the following procedure provides a convenient method of adding additional Content Server instances. You can use this method to set up Front-End Instances of Content Server.

To clone a Content Server instance

1. Run the Content Server installer to install Content Server on the operating system. Run the installer for all of your optional modules so that configuration information is written to the Windows registry or elsewhere.
2. Stop the Content Server services.
3. Copy the entire *`<Content_Server_home>`* folder structure from your first complete Content Server installation to the new installation, so that the new installation already has any Updates, patches, and customizations that you applied to first Content Server installation.

   Important
   Do not copy the `Index` folder to the cloned Content Server installation, even if it is a subfolder of the *`<Content_Server_home>`* folder.

At this point, you have your application file structure in place, but you need to modify a few configurations that currently refer to the source instance of Content Server, not the cloned instance, before you start your cloned instance of Content Server.

To prepare your cloned instance to connect to the staging database

1. Modify the `opentext.ini` file so it refers correctly to your cloned instance of Content Server.

   Note: Because you copied the `opentext.ini` file from your Default Admin Server installation, some entries specifically reflect the name and IP address of the Default Admin Server. Change these entries to point to your cloned instance of Content Server.

   a. Back up the `opentext.ini` file.
   b. In the `[general]` section, edit the `Server=` entry. Set its value to the fully qualified domain name of your cloned instance of Content Server.
   c. In the `[security]` section, modify the `CGIHosts=` entry. Set its value to the IP address of your cloned instance of Content Server. Alternatively, leave its value empty to allow this instance to accept connections from any IP address.
2. To remove database connection information and ensure that agents do not run at startup, open the `opentext.ini` file, and then do the following:

   a. In the `[general]` section, delete the entire `dftconnection=` line.
   b. In the `[scheduleactivity]` section, set all the values to `=0`.
   c. In the `[loader]` section, ensure that only `sockserv` and `javaserver` are enabled.

Tip: The `[loader]` section should already have only `sockserv` and `javaserver` enabled because you configured your source instance in this manner in "Disable Agents in the opentext.ini File" on page 33.

d. Delete the `[dbconnection:`*`<database_name>`*`]` section.

3. Delete the following files from the *`<Content_Server_home>`*`/config/` folder.

   a. Delete the following Search configuration files:

      - `search.ini`
      - `otadmin.cfg`
      - `otadmin.cfg.old`
      - `otadmin.pid`
      - `otadmin.pid.old`

      Important
      Do not delete the `otadmin.pwd` file. It allows the cloned Content Server instance to log on to the Default Admin Server.

   b. Delete the Admin Server signature files. Signature files have the following format:

      - `ADMINSERVERNAME209X7278888740X0dcsServer.ini`
      - `query_ADMINSERVERNAMEX2099X727888740X2768.in`
      - `ADMINSERVERNAME209X7278888740X2768.dw`

1.6.5 Perform Post-Upgrade Checks and Basic Testing

You have successfully upgraded Content Server. Now it is time to perform some post-upgrade checks and undo some settings that were in place in your during your upgrade. The following is a basic checklist.

- Change the Admin server password.
- Re-enable System Object Volume Alerts if you disabled them earlier.
- Implement any Search customizations that exist in your Source Environment.
- Return logging levels to normal operating levels.
- Enable Agents and Notifications, both in the `opentext.ini` file (see "Disable Agents in the opentext.ini File" on page 33) and in the Content Server interface (see "Disable Agents and Notifications" on page 18).
- Activate the Facets Sidebar. If the Facets Sidebar does not appear on the Enterprise Workspace, open the **Content Server Administration** page. In the Server Configuration section, click **Configure Presentation**. On the **Configure Presentation** page, click **Configure Sidebar**. Select the **Enable Sidebar** check box and activate any sidebar panels that you want your users to be able to view, and then click **Save Changes**.

- Perform basic testing. For example:
  - Open the Enterprise Workspace and check that it has the same content as your Source Environment.
  - Perform a search, and enable **Hit Highlighting** on one of the search results.
  - Test drag-and-drop functions.
- Enable Global Appearances
- If you have modified menus and buttons or other Content Server GUI features in your Source Environment, verify that they are working as expected in your upgraded environment.

  Note: If you upgrade a Content Server environment that includes modifications to the **More** Functions menu item, the **More** Functions menu item might not appear at all for users in the upgraded environment. This is most likely to happen to users who access Content Server in a language other than English. To resolve this problem, open the **Configure Functions Menu** administration page and, without making any changes to your Functions menu configuration, click **Save Changes**.
- Review your Content Server audit settings. The new Content Server version may have new auditing events that you wish to enable.
- Test your LiveReports to verify that they still function as expected.

  Note: If your Content Server deployment uses an Oracle database and the upgrade converts a `varchar(4000)` or similar column type to a `CLOB`, LiveReports that use `ORDER BY`, `UNION`, `GROUP BY`, or any other method of sorting or mass-comparison on the `CLOB` converted from the former `varchar(4000)` require type conversion using `DBMS_LOB.SUBSTR()`.

1.6.6 Bring the Upgraded Environment Online

Now that you have verified that your Target Environment is functioning as expected, bring it online and open it up to your Content Server users. Reconfigure your Domain Name Server to point to your Target Environment.

Note: OpenText recommends that you transfer the domain name of the Source Environment to the Target Environment when you bring the Target Environment into production. If you do not, some links may not function correctly in the upgraded environment. Content Server notifications, for example, contain fully qualified addresses, and Content Server users may create links using your deployment's fully qualified domain name. These links will fail if the domain portion of the Content Server URL changes.

Renaming a Content Server Computer

After you have installed and configured Content Server, OpenText recommends that you do not change the host name of a computer that runs Content Server. Renaming a Content Server computer is a complex operation that affects multiple Content Server components. If you must rename a Content Server computer, OpenText recommends that you obtain assistance from OpenText Professional Services before you proceed.

Chapter 2

Installing Content Server Updates

Content Server Updates deliver performance enhancements, resolve product issues, improve application security and usability, and implement new features for Content Server and the Content Server Search Engine. Content Server Updates are released approximately every three months.

A Content Server Update includes the following individual components:

- A Content Server Update file
- Documentation for the Update
- Patches to be installed in conjunction with the Update files.

Content Server Updates are cumulative. Each Content Server Update contains the changes that were delivered in previous Updates. You need only apply the latest Content Server Update to benefit from all of the fixes and enhancements delivered through Updates. OpenText recommends you apply the latest Update when it becomes available.

Updating the Content Server Java Runtime Environment

After you apply an Update, OpenText recommends that you update your Content Server Java Runtime Environment (JRE) to the latest supported version of JRE 8. For instructions, see "Updating the Content Server Java Runtime Environment" on page 64.

2.1 Applying Content Server Updates

To apply Updates to Content Server, you can use OpenText Content Server Cluster Management. Cluster Management manages the application of Content Server patches, Updates and Language Packs, on a single instance of Content Server and throughout a Content Server cluster. Cluster Management automatically handles patch dependencies and removes superseded patches when a newer or more complete version of a patch is applied.

Cluster Management is designed with clusters in mind. You can use it to apply an Update to multiple instances of Cluster ManagementContent Server in a single operation, but it can also be used to update a standalone installation of Content Server.

Cluster Management Update Analysis allows you to preview the effects that a Content Server Update will have on your system so that you can remove obsolete patches and make appropriate backups before applying an Update.

Using Cluster Management to manage patches, Updates and Language Packs in a Content Server cluster involves three main operations:

1. **Download**

   You use Cluster Management to download patches, Updates and Language Packs to your Cluster Management Master System.
2. **Stage**

   Cluster Management stages downloaded items in the Content Server database, so the items are available to every instance in your Content Server cluster.
3. **Deploy**

   You use Cluster Management to install staged items to every instance in your Content Server cluster.

If Cluster Management is unable to automatically update your entire Content Server cluster, it rolls back the changes that it is making. If you ever need to manually roll back the application of a patch, Update or Language Pack, Cluster Management provides features and information that facilitate the rollback operation.

For information on Cluster Management, see *OpenText Content Server Cluster Management - Admin Online Help (LLESPAT-H-AGD)*.

Note: This chapter explains how to apply an Update to Content Server using Cluster Management. You can also use OpenText™ System Center Manager to apply Content Server Updates. System Center Manager installs, configures, patches, and updates multiple OpenText software applications. For more information, see *OpenText System Center Manager - Installation and Configuration Guide (SYSCM-IGD)*.

2.1.1 Using Update Analyzer

Update Analyzer is a utility included in Content Server Cluster Management that gives you insight into the changes that an Update will make to your system. You can use Update Analyzer to determine whether any files in your Content Server deployment require special attention and to identify patches that you can remove before you apply the Content Server Update.

Running Update Analyzer

To generate an Update Analyzer report:

1. In the **Server Configuration** section of the **Content Server Administration** page, click **Cluster Management**.

2. On the **Cluster Management** page, click **Update Analysis**.

   The **Update Analysis** page opens. It displays your **Current Update (Master)** at the top of the page.

3. In the **Destination Update** menu, select the Update whose effects you wish to analyze.

4. In the **Agents** section of the page, expand any Host of interest and enable one or more Content Server instances.
5. Click **Start Analysis**, and then click **Yes** on the **Analysis Confirmation** dialog box.

   The Update Analysis commences. The **Analysis Status** updates as the analysis progresses.
6. When the **Analysis Complete** dialog box appears, click **OK**.

To view the Update Analysis report, expand the Host and Instance whose report you wish to view, and then click **View Report**.

Interpreting the Update Analysis Delta Report

The **Update Analysis Delta Report** provides information on the files that will be replaced by the Content Server Update indicated in the **Overview** section of the report.

The **Summary** section of the report provides general information on your Content Server system. It also lists patches that you should remove before you apply the Content Server Update.

Tip: You can run Update Analyzer at any time to check whether you have deprecated patches deployed on your Content Server system.

In the **Update Analysis Delta Report**, each file is categorized as `NEW`, `VERIFIED`, or `DIFFERENT`.

NEW

`NEW` files are files that the Update will add to Content Server. They do not currently exist in your Content Server installation.

VERIFIED

`VERIFIED` files are files that the Update will replace and that have a hash value that matches one in the Manifest. This indicates that the file has the content that the Update expects it to have. The file has not been modified since it was originally installed.

DIFFERENT

`DIFFERENT` files are files that the Update will replace, but whose hash value does not match one in the Manifest. This indicates that the file is not the same as when it was first installed. It may have been customized by the System Administrator, a third-party integration, or a patch not listed in the Manifest. OpenText recommends that you make a backup of `DIFFERENT` files before you apply the Update.

Update Analyzer also provides a list of patches that you should remove from Content Server before you apply the Update.

! **Important**

The list provided by the Update Analyzer is as complete as possible, but you should also review the list of patches to be removed that appears in the Content Server Release Notes. If additional removable patches are identified after the release of the Update, the Release Notes will include patches that are not listed in the Content Server Update Delta Report.

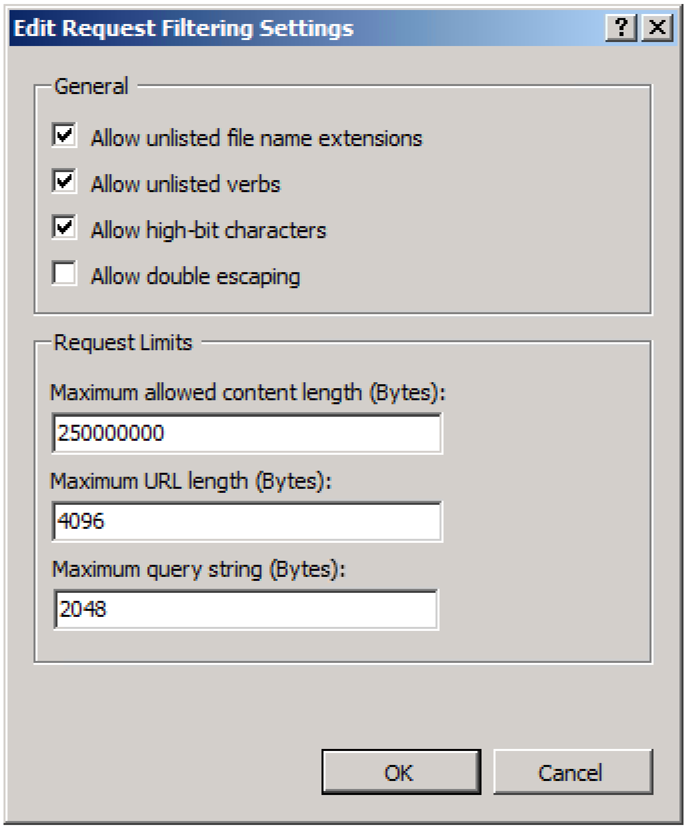
2.1.2 Backing Up Content Server

Content Server Updates overwrite files and may make irreversible changes to your Content Server database. Before you apply the Update, make a full backup of your Content Server installation, including the Search Index, database, External File Store, and the *<Content_Server_home>* folder on each Content Server instance in your environment.

2.1.3 Setting Microsoft IIS Request Filtering to Permit Staging of an Update

`Maximum allowed content length (Bytes)` is a **Request Filtering** setting in Microsoft Internet Information Services that restricts the size of files that can be uploaded to or downloaded from Content Server. If you use Microsoft Internet Information Services with Content Server, OpenText recommends that you configure the `Maximum allowed content length (Bytes)` setting to a value that is higher than the size of the Content Server Update so that you can stage a Content Server Update by dragging it onto **Staged** view of the **Manage Updates** page.

If you have not modified the default value set by the Content Server installer, no action is required. By default, the installer for Content Server 16.2.0 and later sets the value of `Maximum allowed content length (Bytes)` to 2,147,483,648 Bytes. This value is large enough for Cluster Management to enable drag and drop of Content Server Updates.



General

☑ Allow unlisted file name extensions

☑ Allow unlisted verbs

☑ Allow high-bit characters

□ Allow double escaping

Request Limits

Maximum allowed content length (Bytes): 250000000

Maximum URL length (Bytes): 4096

Maximum query string (Bytes): 2048

2.1.4 Installing Content Server Updates Using Cluster Management

OpenText recommends that you apply Updates first in a test environment. After you update the test environment successfully, update your production environment.

When you deploy an Update, Cluster Management validates prerequisites, shuts down every instance in the cluster, and then automatically extracts the files in the Update and copies them to the appropriate Content Server folders, overwriting existing files as necessary. Cluster Management then restarts the master instance and every Admin server in your Content Server cluster. If necessary, it upgrades the database. It then restarts every instance in the cluster.

If you have a multilingual Content Server deployment, Cluster Management automatically deploys staged Language Packs for any languages that you have installed in your Content Server deployment.

If Cluster Management encounters an unrecoverable error at any stage of the deployment, it informs you that it is unable to complete the deployment and allows you to roll back any software changes that it has already made.

Important
Cluster Management rolls back software changes that are made to the Content Server application folder. It does not roll back changes to the Content Server database, file store, or search index. If Cluster Management is unable to complete a deployment that makes changes to one of these items, you must restore a Content Server backup set.

Downloading the Update and Language Packs

The Cluster Management **Manage Updates** page displays any Content Server Updates that are available on OpenText My Support (https:\\knowledge.opentext.com). If an Update is available, you can use Cluster Management to download and stage it.

Obtaining Update Language Packs

Automatically
If you have a multilingual deployment of Content Server and you have enabled Cluster Management to automatically download patches, Updates and Language Packs, Cluster Management downloads Language Packs for the Update for each language that you have in your Content Server deployment.

Manually
If you have a multilingual deployment of Content Server and you have not enabled Cluster Management to automatically download patches, Updates and Language Packs, Cluster Management does not download and stage the Language Packs for the Update. You must log onto OpenText My Support, download any Language Packs that you require, and then place them in the Patch Staging Folder.

To download and stage an Update:

1. Open the **Manage Updates** page.

   a. In the **Server Configuration** section of the **Content Server Administration** page, click **Cluster Management**.

   b. On the **Cluster Management** page, click **Manage Updates**.

2. Use Cluster Management to download the Update, using the automatic or manual method.

   - **Automatic**

     In the **Available** view, enable the Update that you wish to apply, and then click **Download**.

     Note: If no check boxes appear to the left of the items in the **Available** view, automatic downloads are not enabled in your Cluster Management settings, and you must use the manual method.

Cluster Management automatically downloads the Update (and Update Language Packs, if applicable) and stages it in the Content Server database, so that it is ready to be installed.

- **Manual**

  1. Open the **Available** view of the **Manage Updates** page.
  2. In the **Action** column of the Update that you wish to apply, click **Download**.
  3. If your Content Server installation uses languages other than English, download Language Packs for the Update from the **Content Server Core Downloads** page of OpenText My Support (https://knowledge.opentext.com/go/4040153)
  4. When the Update has finished downloading, move it (and any Language Packs that you have downloaded) to your Patch Staging Folder. You can do this in a file system utility (for example, Windows Explorer) by moving it to the folder manually, or in Cluster Management by dragging it onto the **Staged** view of the **Manage Updates** page.

  .

> **Tip:** For more information on the various ways of downloading and staging Updates and patches using **Cluster Management**, see *OpenText Content Server Cluster Management - Admin Online Help (LLESPAT-H-AGD)*.

The Update show now be visible in the **Staged** view of the **Manage Updates** page.

Installing the Content Server Update

Once the Update is visible in the **Staged** view of the **Manage Updates** page, it is ready to be installed.

To install the Content Server Update:

1. Open the **Manage Updates** page.

   a. In the **Server Configuration** section of the **Content Server Administration** page, click **Cluster Management**.

   b. On the **Cluster Management** page, click **Manage Updates**.

2. In the **Staged** view of the **Manage Updates** page, enable the Update that you want to install. If the Update includes required patches, enable the patches too. Click **Deploy**.

   > **Tip:** Cluster Management automatically marks deprecated patches for removal.

3. Review the information in the **Confirm Deployment Package** dialog box and then click **OK**.

4. The **Deployment Status** dialog box appears and indicates the progress of the deployment. Upon successful completion of the deployment, the **Deployment**

Complete dialog box appears. Click **OK** to return to the **Deployment Status** dialog box.

> **Note:** If Cluster Management reports that it has encountered an unrecoverable error, see *OpenText Content Server Cluster Management - Admin Online Help (LLESPAT-H-AGD)*.

5. Review the information in the **Deployment Status** dialog box, and then click **OK** to return to the **Manage Updates** page.

Using Cluster Management to Apply New Patches

After Cluster Management has deployed an Update, new patches may be available for Content Server or Content Server modules. Open the Cluster Management **Manage Updates** page and look at the **Available** view to determine if there are any new patches that you should download, stage and install.

For more information on Cluster Management, see *OpenText Content Server Cluster Management - Admin Online Help (LLESPAT-H-AGD)*.

Handling the Optional Core Module Files in the staging Folder

A default installation of Content Server includes modules (sometimes called "optional core modules") that are available by default, but are not installed automatically. If you have not installed an optional core module, its folder resides in the *<Content_Server_home>*`\staging\` folder. After you install an optional core module, its folder resides in the *<Content_Server_home>*`\module\` folder.

Content Server Updates may include improvements for optional core modules. When it does, the Update places folders for these modules in the *<Content_Server_home>*`\staging\` folder.

Compare the contents of the `staging` and `module` folders to determine whether:

- there is no matching module in the `module` folder
- there is a matching module in the `module` folder, and it has the same version number
- there is a matching module in the `module` folder, and it has a higher version number
- there is a matching module in the `module` folder, and it has a lower version number

Based on the results of your comparison, take one of the actions described in this section:

> **Note:** In a clustered installation, perform the action on every instance in the Content Server cluster.

No Corresponding Module in the module Folder

If a module exists in the `staging` folder, but no corresponding module exists in the `module` folder, no action is required.

You have not installed the module, but you may decide to install it at a later date. Leave the module folder in the `staging` folder, so the updates will be available if you install the module later.

Corresponding Module in the module Folder with the Same Version Number

To handle modules in the staging folder that have the same version number as corresponding modules in the module folder:

1. Move the `module` folder from the *`<Content_Server_home>`*`\staging\` folder to the *`<Content_Server_home>`*`\module\` folder, overwriting the contents.
2. Take the following actions with the `adminhelp`, `help` and `support` subfolders of the module you moved in step 1:

   a. Move the `adminhelp` and `help` folders from the `module` folder into the *`<Content_Server_home>`*`\support\` folder.

   b. Move the files in the `support` folder into the *`<Content_Server_home>`*`\support\` folder.

Corresponding Module in the module Folder with a Higher Version Number

Delete the module in the *`<Content_Server_home>`*`\staging\` folder. You have a newer version of the module, so the module improvements in the Update do not apply to your version of the module.

Corresponding Module in the module Folder with a Lower Version Number

Leave the module in the *`<Content_Server_home>`*`\staging\` folder. You have an older version of the module, so the module improvements in the Update do not apply to your version of the module. If you upgrade to the version of the module that the Update modifies, the module updates will already be in place.

Installing Upgraded Core Optional Modules

If the Update includes upgrades to core optional modules, use the Content Server **Install Modules** administration page to upgrade any of the core optional modules that you have previously installed.

Note: In a clustered installation, perform this step on every instance in the Content Server cluster.

Reviewing Changes to Content Server Configuration Files

Some features of Content Server and the Search Engine are managed through configuration files, such as the `opentext.ini` file. In some Updates, OpenText resolves software issues or improves Content Server by adding or modifying settings in its configuration files. Sometimes, however, directly modifying configuration files could affect customizations that you may have made in your Content Server environment.

In such cases, the Update places reference copies of the modified configuration files in the `config_reference` subfolder of the *`<Content_Server_home>`*`\config\` folder. The **Configuration File Changes** section of the Content Server Release Notes explains how these files differ from your existing configuration files.

OpenText recommends that you review the Release Notes and the contents of the files in the `config_reference` folder to see if the configuration file changes would be appropriate in your environment. If so, you should apply these changes in the corresponding configuration files that are located in your *`<Content_Server_home>`*`\config\` folder.

Tip: If you are applying an Update to a new installation of Content Server, OpenText recommends that you copy the files from the `config_reference` folder to the `config` folder in all cases.

Updating Perspective Manager in a Clustered Deployment of Content Server

Perspective Manager allows you to customize the Content Server Smart View user interface to create workspaces tailored to specific user roles. In Content Server 16.2.1 and earlier, it is deployed as a CS Application, but in Content Server 16.2.2 and later, it is deployed as a Content Server module. If you are upgrading from Content Server 16.2.0 or 16.2.1, you may need to remove certain folders from your Content Server application folder to complete the update of Perspective Manager.

Perform the following steps if:

- you are applying Update 16.2.2 or later to a clustered deployment of Content Server 16.2.0 or 16.2.1, and
- when you installed Content Server 16.2.0 or 16.2.1, you followed the instructions in the Content Server Installation Guide on **Setting up Perspective Manager in a Clustered Deployment of Content Server**

You can verify that the steps are necessary by opening the **Applications Management** administration page, which is found in the **Content Server Applications Administration** section of the Content Server Administration page. If **OTPERSPECTIVEMGR** appears with a status of `Not installed properly. Move application folder back to staging and install again`, perform the following steps.

To complete the update of Perspective Manager in a clustered Content Server deployment:

1. Remove the folder named OTPERSPECTIVEMGR from the `...\<Content_Server_home>\csapplications\` folder from each instance of Content Server in the cluster.
2. Remove the folder named OTPERSPECTIVEMGR from the `...\<Content_Server_home>\support\csapplications\` folder from each instance of Content Server in the cluster.

Rebuilding User Help and Admin Help

Content Server Updates often make additions to the Content Server Help pages. Complete the following steps to rebuild your User Help and Administrator Help.

To rebuild the Content Server Help pages:

1. In the **Search Administration** section of the **Content Server Administration** page, click **Open the System Object Volume**.
2. On the **Content Server System** page, delete the **Admin Help Data Source Folder**.
3. On the **Content Server System** page, delete the **Help Data Source Folder**.
4. Create the Admin Help Data Source.
   a. Click **Add Item**, and then click **Admin Help Data Source**.
   b. On the **Create New Admin Help Data Source** page, ensure that all the settings are correct, and then click **Create Processes**.
   c. On the **Status** page, verify that the **All processes have been created successfully** message appears, and then click **Continue**.
5. Create the User Help Data Source
   a. Click **Add Item**, and then click **User Help Data Source**.
   b. On the **Create New User Help Data Source** page, ensure all the settings are correct, and then click **Create Processes**.
   c. On the **Status** page, verify that the **All processes have been created successfully** message appears, and then click **Continue**.

2.2 Updating the Content Server Java Runtime Environment

Content Server ships with a base version of JRE 8. With many Updates, a newer supported Content Server JRE 8 file is made available on OpenText My Support.

The Content Server JRE is not automatically updated when you apply an Update to an existing Content Server installation. You can continue to use your existing version of JRE 8 with a new Update, but OpenText recommends that you update JRE 8 when you apply an Update.

Be sure to use the JRE 8 file that is posted on OpenText My Support. Do not use a JRE that you have obtained from the Internet.

Important
In a clustered Content Server environment, you must run the same JRE on every instance. Ensure that every instance of Content Server has the same JRE version in its `<Content_Server_home>/jre/bin/` folder.

To update the Content Server JRE:

Perform the following steps after you have applied an Update as described in “Applying Content Server Updates” on page 53.

1. Open the **Content Server JRE 8** subfolder of the **Content Server Update** page on My Support, and download the copy of the `Content_Server_Java_Runtime_Environment_8U##_<OS>` ZIP or TAR file that is appropriate for your Content Server operating system (where `##` is the version number of the Content Server JRE and *<OS>* represents your operating system).

2. Stop the Content Server service, Content Server Admin service, and Cluster Agent service on every Content Server instance in your environment.

3. On each Content Server instance in your environment:

   a. Rename the existing `<Content_Server_home>\jre\` folder to `jre_bak` or something similar. Make a note of the permissions applied to this folder.

   b. Extract the contents of the `Content_Server_Java_Runtime_Environment_8U##_<OS>` ZIP or TAR file to the `<Content_Server_home>` folder. Verify that the permissions on the new `<Content_Server_home>\jre\` folder are the same as those that you noted in step 3a above.

   c. Start the Content Server service, Content Server Admin service, and Cluster Agent service.

Chapter 3

Appendix A – Content Server Upgrade Checklist

This Appendix contains a checklist that you can use to verify that you have recorded user names and passwords, retained configuration files, and kept other important information required for your upgrade of Content Server.

3.1 Content Server Upgrade Checklist

Table 3-1: Server Landscape

Item	Comment
Content Server Admin Servers	List each Admin server, including, Admin Server password, ports used, index partitions, installation folder, etc.
Content Server Front-end Servers	List each Front-end server, including ports used and installation folder
Content Server Special-purpose Servers	List any special-purpose Content Server instances (for example, Workflow Agent server), including ports used and installation folder.
Database server	
Web server	
Other servers	For example, Tomcat to support Liquid Office
External File Store	Note the path.
Content Server Search Index	Note the path.

Table 3-2: Database

Item	Comment
Database	Copy database for upgrade testing and to upgrade.
Content Server database user	Name and password. If you use SQL Server, SID of Content Server database user.

Table 3-3: Content Server User Names and Passwords

Item	Comment
Admin User	Probably not needed. You set a new Admin password in the new environment anyway.

Table 3-4: Content Server Information

Item	Comment
`opentext.ini` file	From each instance
Number of threads	From each instance. Note if you intend to change the number of threads used by Content Server
System Report	From each instance
Search Index Verification report	
Index plan	Migrate or recreate?
Modules	List all non-core modules used. Note whether modules are optional, third-party, or custom.
Hotfixes	List any hotfixes that will need to be recreated in the upgraded system
Workflows and Other Key Deployment Features	List key workflows, LiveReports, Custom Views, Appearances and other important features of your Content Server deployment, so that you can test them during and after your upgrade.
Customizations	List any customizations that you have applied to Content Server to change its appearance or functionality.
Configuration files	`LLFieldDefinitions.txt` and `LLFieldDefinitions_EL.txt`.