

IBM OpenPages with Watson
Version 8.2.0

Installation and Deployment Guide



Note

Before using this information and the product it supports, read the information in [“Notices” on page 469](#).

Product Information

This document applies to IBM OpenPages with Watson Version 8.2.0 and may also apply to subsequent releases.

Licensed Materials - Property of IBM Corporation.

© Copyright IBM Corporation, 2003, 2023.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

© **Copyright International Business Machines Corporation .**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Chapter 1. Introduction.....	1
Getting started.....	1
Installation locations for IBM OpenPages with Watson.....	2
Changes to the installation process.....	4
Notes for customers upgrading or migrating from 7.3.x.....	7
Special characters in passwords.....	12
Chapter 2. What's new?.....	15
New features in version 8.2.0.4.....	15
New features in version 8.2.0.3.....	15
New features in version 8.2.0.2.....	15
New features in version 8.2.0.1.....	16
New features in version 8.2.0.....	18
New features in version 8.1.0.1.....	20
New features in version 8.1.....	20
New features in version 8.0.0.2.....	22
New features in version 8.0.0.1.....	23
New features in version 7.4.0.....	24
New features in version 7.3.0.2.....	25
New features in version 7.3.0.1.....	25
New features in version 7.3.0.....	26
Chapter 3. OpenPages with Watson overview.....	27
OpenPages with Watson components.....	27
Installation server.....	28
Database server.....	28
Application server.....	28
Reporting server.....	29
Search server.....	29
Server topology and installation configurations.....	29
Clustered environments.....	31
Configure clustered environments.....	31
Chapter 4. Installation prerequisites.....	33
Software prerequisites.....	33
Prerequisite software for all servers.....	33
Prerequisite software for the installation server.....	34
Prerequisite software for the database server.....	34
Prerequisite software for application servers.....	35
Prerequisite software for reporting servers.....	37
Prerequisite software for the search server.....	38
Prerequisite software for OpenPages client computers.....	38
Hardware prerequisites.....	39
VMWare configuration requirements on Windows computers.....	39
Chapter 5. OpenPages installation server and app.....	41
Installation on different operating systems.....	41
Setting up the installation server on Windows.....	41
Setting up the installation server on Linux.....	43
Migrating deployments and installation server users.....	44

Installing agents manually.....	45
Update the installation server and agents.....	47
Updating the installation server.....	47
Updating agents manually.....	48
Logging in to the installation app.....	49
Adding users.....	50
Changing passwords.....	51
Starting the installation server.....	53
Stopping the installation server.....	53
Starting the installation agent manually.....	54
Stopping the installation agent manually.....	54
Changing the port number of the installation server.....	55

Chapter 6. Install IBM OpenPages with Watson..... 57

Installation process overview.....	57
Preparing your system for installation.....	58
Checklist if you are using existing hardware.....	58
Checklist for Windows servers.....	59
Checklist for Linux servers.....	60
Checklist for application servers.....	64
Checklist for the database server (Db2).....	65
Checklist for the database server (Oracle).....	87
Checklist for reporting servers.....	110
Checklist for the search server.....	124
Port assignments	124
Create the database schema objects.....	126
OpenPages database object creation for Db2.....	126
OpenPages database schema creation for Oracle.....	132
Creating a deployment.....	141
Considerations for IBM OpenPages solutions.....	144
Super Administrator.....	144
Configuring the database server (Db2).....	144
Configuring the database server (Oracle).....	146
Configuring application servers.....	149
Configuring reporting servers.....	150
Configuring a search server.....	152
Post installation tasks.....	153
Updating WebSphere Liberty on application servers.....	153
OpenPages with Watson CommandCenter post-installation tasks.....	155
Loading the Cognos dashboard integration after installing.....	158
Configuring OpenPages applications to use a domain account on Windows operating systems.....	159
Configuring file share permissions on Linux operating systems.....	159
Sharing a network OpenPages storage directory on Linux operating systems.....	159
Sharing a network OpenPages storage directory on Windows operating systems.....	161
Updating the location of the openpages - storage directory (Db2).....	161
Updating the location of the openpages - storage directory (Oracle).....	163
Configuring IBM HTTP Server to balance the load on application servers	164
Load balancing the reporting server.....	170
Admin application server tuning.....	175
Database server tuning for Db2 databases.....	176
Database server tuning for Oracle databases.....	178
Enabling LDAP for the OpenPages application.....	178
Disabling LDAP for the OpenPages application.....	180
Accessing OpenPages.....	180
Search server post installation tasks.....	180
Preventing orphan objects.....	187
Verification checklist.....	187

Chapter 7. Migrate to a new version of IBM OpenPages with Watson.....	189
Migration overview.....	189
Migration process overview: Using the database server from your source environment.....	190
Migration process overview: Using new hardware for the database server.....	192
Upgrade prerequisite software	196
Oracle upgrade options and Oracle PDB.....	196
Cognos Analytics upgrade process: 10.2.x to 11.1.....	197
Cognos Analytics upgrade process: 11.0.x to 11.1.x.....	197
Preparing the search server in the source environment.....	198
Backing up your source environment.....	198
Upgrade the OpenPages database.....	199
Migrating a custom encryption keystore.....	200
Migrate files.....	201
Backing up application files.....	201
Restoring application files.....	204
Restore the storage directory in the target environment.....	205
Upgrading application data.....	205
Post migration tasks.....	206
Loading the Cognos dashboard integration after migrating.....	208
Updating search server settings.....	208
Updating URL host pointers for reports.....	209
Verify the list of valid domains and host names for Cognos Analytics.....	210
Upgrading the OpenPages password encryption algorithm to AES encryption.....	211
Updating security rules.....	211
Custom settings in configuration files	212
Search server post migration tasks.....	212
Enable LDAP after migrating.....	213
Enabling a JDBC connection for the OpenPages database (Db2).....	213
Enabling a JDBC connection for the OpenPages database (Oracle).....	213
Updating the reporting schema.....	214
Regenerating the reporting framework.....	214
Deleting Fujitsu workflow reports.....	215
Migration verification tests.....	215
Configure new features.....	217
Rolling back an OpenPages migration.....	218
Chapter 8. Migration task reference for Db2 databases.....	219
Back up the database (Db2).....	219
Dropping the Db2 Text Search index and disabling Db2 Text Search.....	219
Backing up the OpenPages database during a migration to 8.2 (Db2).....	220
Backing up the Cognos database during a migration to 8.2 (Db2).....	221
Restore the OpenPages database in your 8.2 environment (Db2).....	222
Restoring the OpenPages database (Db2).....	223
Restore Db2 Text Search	224
Update the databases for a Db2 11.1.x fix pack.....	224
Restoring the Cognos content store (Db2).....	225
Upgrade the databases (Db2).....	226
Extending database row sizes for the databases (Db2).....	227
Preparing for the database upgrade (Db2).....	227
Running the pre-upgrade DBA script (Db2).....	229
Validating the pre-upgrade DBA step (Db2).....	230
Upgrading the database (Db2).....	231
Running the post-upgrade DBA script (Db2).....	232
Validating the post-upgrade DBA step (Db2).....	233
Updating the location of the openpages - storage directory (Db2).....	234
Update the database connection information (Db2).....	236

Updating the <code>aurora.properties</code> file (Db2).....	236
Updating the data source connection in WebSphere Liberty (Db2).....	237
Updating the Cognos content store information (Db2).....	237
Updating the database connection information for the search server (Db2).....	238
Updating the <code>deploy.properties</code> file.....	238
Updating the connection to the OpenPages database for Cognos (Db2).....	238
Chapter 9. Migration task reference for Oracle databases.....	241
Backing up the OpenPages database during a migration (Oracle).....	241
Backing up the Cognos content store during a migration (Oracle).....	242
Restore the OpenPages database in your 8.2 environment (Oracle).....	243
Preparing to import the OpenPages database (Oracle).....	244
Restoring the OpenPages database schemas (Oracle).....	245
Remap schema and table space names (Oracle).....	248
Restore the Cognos content store in your 8.2 environment (Oracle).....	250
Preparing to import the Cognos content store (Oracle).....	250
Restoring the Cognos content store (Oracle).....	250
Upgrade the OpenPages database (Oracle).....	252
Preparing for the database upgrade (Oracle).....	252
Running the pre-upgrade DBA script (Oracle).....	254
Validating the pre-upgrade DBA step (Oracle).....	255
Upgrading the schema (Oracle).....	256
Running the post-upgrade DBA script (Oracle).....	257
Validating the post-upgrade DBA step (Oracle).....	258
Updating the location of the <code>openpages-storage</code> directory (Oracle).....	258
Update the database connection information (Oracle).....	260
Updating the <code>aurora.properties</code> file (Oracle).....	260
Updating the data source connection in WebSphere Liberty (Oracle).....	261
Updating the Cognos content store information (Oracle).....	261
Updating the database connection information for the search server (Oracle).....	263
Updating the <code>deploy.properties</code> file.....	263
Updating the connection to the OpenPages database for Cognos (Oracle).....	263
Oracle Transparent Data Encryption for migration customers.....	264
Chapter 10. OpenPages solutions post-migration tasks.....	267
Configuring email notifications for questionnaire assessment triggers.....	268
Updating the RCSA Alignment helper in profiles.....	269
Removing the Scenario Analysis triggers.....	269
Updating Scenario Analysis field dependencies.....	270
Loading the timesheet helpers.....	271
Loading the timesheet helpers.....	271
Updating the timesheet helpers.....	273
Disabling the old timesheet entry helper.....	273
Importing the solutions report packages.....	274
Updating MRG.....	275
Updating TPRM.....	276
Loading the sample workflows.....	277
Chapter 11. Fix packs.....	279
Fix pack process overview.....	279
Prepare for a fix pack.....	280
Review new features and fixes.....	280
Back up your existing environment.....	280
Verifying servers before you install a fix pack.....	282
Installation tasks for fix packs.....	282
Update the OpenPages database manually (Db2).....	282
Update the OpenPages database manually (Oracle).....	289

Installing a fix pack.....	295
Postinstallation tasks.....	297
Restoring solutions helpers, images, and other files.....	297
Updating the IBM OpenPages SDI Connector for UCF Common Controls Hub.....	297
Updating IBM Security Directory Integrator for the QRadar connector	298
Configure new features.....	299
Solutions postinstallation tasks.....	300
Regenerating the reporting framework.....	306
Additional tasks for fix packs.....	306
Performing a silent installation of a fix pack.....	306
Rolling back a fix pack.....	307
Chapter 12. Starting and stopping servers.....	309
Starting application servers.....	309
Starting application servers by using Windows services.....	309
Starting all application services by running a script (Windows).....	310
Starting all application servers by running a script (Linux).....	310
Determining application readiness.....	311
Stopping application servers.....	311
Stopping application servers by using Windows services.....	311
Stopping all application servers in Windows by using a script.....	311
Stopping all application servers on Linux by using a script.....	312
Start or stop the global search services.....	312
Starting the global search services by using a script.....	312
Stopping the global search services by using a script.....	313
Starting the global search services on Windows.....	313
Starting the global search services on Linux.....	314
Stopping the global search services.....	315
Start or stop the database services.....	315
Starting and stopping the Oracle database server in a Windows environment.....	315
Starting and stopping the Oracle database server in Linux environments.....	316
Starting and stopping the Cognos services.....	317
Using the IBM Cognos configuration tool to start and stop the IBM Cognos service.....	317
Using the Windows operating system to start and stop the IBM Cognos service.....	317
Using the Linux operating system to start and stop the IBM Cognos service.....	318
Starting and stopping the OpenPages with Watson Framework Model Generator service on Windows.....	318
Starting and stopping the OpenPages with Watson Framework Model Generator service on Linux.....	318
Chapter 13. Single sign-on integration for the OpenPages application server.....	321
Configuring SAML single sign-on.....	321
Disabling SAML single sign-on.....	324
Configuring an error page for SAML single sign-on.....	325
Configuring mixed mode single sign-on (SAML and IBM OpenPages with Watson).....	326
Configuring multiple IDs for a SAML identity provider.....	329
Configuring SPNEGO single sign-on.....	331
Disabling SPNEGO single sign-on.....	336
Configuring single sign-on by using OpenID Connect.....	336
Disabling OpenID Connect single sign-on.....	338
Configuring header-based single sign-on.....	339
Custom header-based SSO library.....	341
Disabling header-based single sign-on.....	343
Setting user passwords to never expire.....	343
Configuring the single sign-on logout destination.....	343
Avoiding server timeouts in single sign-on environments.....	344

Chapter 14. QRadar integration.....	345
Installing IBM Security Directory Integrator for QRadar integration.....	345
Setting up the QRadar SSL certificate.....	346
Importing the assembly line for QRadar.....	347
Configuring the QRadar connector properties file.....	347
Configuring the QRadar connector passwords properties file.....	348
Chapter 15. IBM OpenPages SDI Connector for UCF Common Controls Hub.....	351
Installing IBM Security Directory Integrator for IBM OpenPages SDI Connector for UCF Common Controls Hub.....	351
Installing IBM OpenPages SDI Connector for UCF Common Controls Hub.....	352
Importing the assembly lines for UCF.....	353
Configuring the connection information.....	354
Configuring OpenPages for UCF integration.....	355
Importing business entities.....	356
Updating object type relationships for UCF.....	356
Updating UCF fields.....	357
Update business entities, fields, and field groups.....	358
Chapter 16. Approval app.....	361
Deployment process overview for the approval app.....	361
Pre-upgrade tasks for the approval app.....	362
Preparing for the deployment of the approval app.....	362
Supported data types and field types in the approval app.....	362
Ensuring that you have the fields and field groups required for the approval app profile	363
Updating triggers for the approval app	369
Loading the approval app profile	370
Completing the approval app deployment.....	371
Conditional steps for the approval app.....	371
Upgrade the approval app.....	371
Pre-upgrade tasks for the approval app.....	372
Updating the approval app configuration file.....	372
Upgrading the approval app.....	373
Chapter 17. Loss Event Entry.....	375
Installation process overview for Loss Event Entry.....	375
Pre-installation tasks for Loss Event Entry.....	375
Installation tasks for Loss Event Entry.....	376
Post-installation tasks for Loss Event Entry.....	377
Upgrade process overview for Loss Event Entry.....	378
Upgrading Loss Event Entry.....	379
Updating the Loss Event Entry configuration file.....	380
Migration process overview for Loss Event Entry.....	381
Additional tasks for Loss Event Entry.....	382
Silent installation for Loss Event Entry.....	382
Manual data loading for Loss Event Entry.....	383
Chapter 18. IBM OpenPages Third Party Risk Management.....	387
Installation process overview for IBM OpenPages Third Party Risk Management.....	387
Pre-installation tasks for IBM OpenPages Third Party Risk Management.....	388
Preparing for the installation of IBM OpenPages Third Party Risk Management.....	388
Loading the IBM OpenPages Third Party Risk Management solution.....	389
Configuring menu items for IBM OpenPages Third Party Risk Management.....	390
Completing the IBM OpenPages Third Party Risk Management installation.....	390

Chapter 19. Uninstalling OpenPages with Watson.....	391
Uninstalling OpenPages with Watson.....	391
Appendix A. Silent installations.....	393
Creating a deployment file by using the installation server.....	393
Creating a deployment file manually.....	393
Deployment file properties.....	394
Modifying the migration properties file.....	396
Running the silent installation commands.....	396
Appendix B. Install OpenPages by using Docker.....	399
Installing Docker.....	399
Installing OpenPages on a single server by using Docker.....	401
Installing OpenPages in a distributed environment by using Docker.....	402
Installing only the OpenPages applications by using Docker.....	404
Accessing the applications.....	405
Stopping and starting OpenPages services deployed to Docker and other tasks.....	405
Uninstalling OpenPages from Docker.....	406
Appendix C. Additional tasks.....	407
Adding servers to an OpenPages with Watson deployment.....	407
Adding servers to a deployment (horizontal cluster members).....	407
Adding non-admin application servers to a deployment (vertical cluster members).....	409
Backing up the OpenPages database (Db2).....	410
Backing up the Cognos database (Db2).....	411
Backing up the OpenPages database (Oracle).....	412
Backing up the Cognos content store (Oracle).....	413
Updating host names.....	414
Refreshing an 8.2 environment with data from an 8.1.x or earlier environment	414
Upgrading application data to 8.2.0.x.....	416
Adding solutions to a deployment.....	418
Enabling only the Task Focused UI.....	419
Removing WebSphere Application Server.....	421
Standalone deployments.....	421
Shared-cell deployments.....	421
Appendix D. Troubleshooting problems.....	423
Troubleshooting resources.....	423
Searching knowledge bases.....	424
Getting fixes.....	424
Contacting IBM Support.....	424
Exchanging information with IBM.....	426
Subscribing to Support notifications.....	426
Log files.....	427
Collect log files and diagnostic data.....	428
Order of starting and stopping services	431
Manually creating the reporting table space and user for Oracle databases.....	431
Oracle package dependencies.....	432
Known problems and solutions for global search.....	434
Global search start fails.....	434
Global search setup fails.....	435
Forcing a reset of global search.....	435
Checking for global search setup issues and periodic monitoring.....	437
Encryption of long strings in OpenPages running on Oracle.....	437
Creating the global search index.....	437
Before you contact IBM OpenPages Support.....	438

Installation issues and solutions.....	438
Error: Cannot manage agent without connection information.....	438
Error starting the installation app.....	439
Silent installation hangs.....	439
Validation error: OpenPages connection refused.....	440
Restoring the installation server.....	440
Restoring an installation agent.....	441
Global search fails to validate during upgrade.....	442
Docker containers not starting.....	443
Application URL is missing the domain of the host after a Docker deployment.....	443
Errors while loading data after you upgrade.....	444
Warnings about system views when loading data.....	444
Password confirmation field is empty after you import deployment properties	445
Update to IBM Installation Manager 1.8 is blocked when the data location is the same as the installation location.....	445
SQL0569N Authorization ID <i>user_name</i> does not uniquely identify a user, a group or a role in the system error.....	446
OpenPages with Watson and software that is installed in a directory that contains spaces.....	447
Garbled characters are displayed on the OpenPages with Watson home page when you log in for the first time.....	447
Manually loading the configuration data after a new installation.....	447
Manually loading the configuration data after a migration.....	449
Manually loading the configuration data after a fix pack.....	450
Dropping the OpenPages database for IBM Db2	452
Troubleshooting Oracle schema creation.....	452
Dropping the Cognos content store (Oracle).....	454
Updating the services for multiple Db2 instances.....	455
OP-03620: The Reporting Schema has not been instantiated error.....	455
Issues when importing databases.....	456
Logging in to Cognos Analytics fails.....	456
Cognos content store import fails	457
Updating the Oracle client path on the reporting server	457
Issues when you use IBM Installation Manager on Linux.....	458
Issues with IBM Db2 and Oracle after upgrading to RHEL 7.2.....	458
libdb2. so cannot be loaded.....	458
Data validation errors when installing Loss Event Entry.....	458
Memory validation step fails for an Oracle database.....	459
Configuring the Oracle data pump directory.....	459
CM-CFG-5114: The Cognos service does not start	460
CM-CAM-4005 Unable to authenticate.....	460
Agent does not exist on remote server.....	461
Errors during database server validation (Db2).....	461
Rollback errors during a database upgrade.....	462
Error: Cannot run schema upgrade.....	462
Loading the application and object strings.....	463
One or more required WLP features unavailable.....	463
OpenPages reports are not displayed in IBM Cognos Analytics.....	464
Troubleshooting IBM OpenPages with Watson solutions.....	465
Reporting Framework generation fails with BC error.....	465
Enabling the new timesheet entry helper.....	466
Manually installing IBM OpenPages solutions.....	467
Notices.....	469
Index.....	473

Chapter 1. Introduction

IBM OpenPages® with Watson™ is an integrated governance, risk, and compliance (GRC) platform that enables companies to manage risk and regulatory challenges across the enterprise.

Audience

The *IBM OpenPages with Watson Installation and Deployment Guide* provides instructions for installing the OpenPages with Watson application. The guide also provides instructions for migrating OpenPages with Watson to a new version.

Please read the following important information regarding IBM OpenPages with Watson documentation

IBM® maintains one set of documentation serving both cloud and on-premises IBM OpenPages with Watson deployments. The IBM OpenPages with Watson documentation describes certain features and functions which may not be available on the cloud.

If you have any questions about the functionality available in the product version that you are using, contact IBM OpenPages Support by using the [IBM Support portal](#).

Finding information

To find product documentation on the web, including all translated documentation, access [IBM Documentation](#).

Accessibility features

Accessibility features help users who have a physical disability, such as restricted mobility or limited vision, to use information technology products. OpenPages documentation has accessibility features. PDF documents are supplemental and include no added accessibility features.

Getting started

Use this list to determine your installation path for IBM OpenPages with Watson.

If OpenPages isn't installed yet or you want to do a fresh installation

See the following topics to get started:

- [Chapter 4, “Installation prerequisites,” on page 33](#)
- [Chapter 5, “OpenPages installation server and app,” on page 41](#)
- [Chapter 6, “Install IBM OpenPages with Watson,” on page 57](#)

If your source environment is at version 7.4.x, 8.0.x, or 8.1.x

You can upgrade or migrate to 8.2.

With an *upgrade*, you install version 8.2 on top of your existing deployment. This method is sometimes called an “in-place upgrade.” or an “over-the-top upgrade.”

If you want to do an upgrade, see the following guides:

- *IBM OpenPages with Watson Upgrade Guide for IBM Db2*
- *IBM OpenPages with Watson Upgrade Guide for Oracle*

Or, you can do a *migration upgrade*. With a migration upgrade, you do a fresh installation of 8.2 and then migrate files and data. Use this option, for example, if you want to use new hardware. If you want to do a migration upgrade, see the following topics to get started:

- [Chapter 4, “Installation prerequisites,” on page 33](#)

- [Chapter 5, “OpenPages installation server and app,” on page 41](#)
- [Chapter 7, “Migrate to a new version of IBM OpenPages with Watson,” on page 189](#)

If your source environment is at version 7.3.x

You must migrate to 8.2.

With a migration upgrade, you do a fresh installation of 8.2 and then migrate files and data.

See the following topics to get started:

- [Chapter 4, “Installation prerequisites,” on page 33](#)
- [Chapter 5, “OpenPages installation server and app,” on page 41](#)
- [Chapter 7, “Migrate to a new version of IBM OpenPages with Watson,” on page 189](#)

Fix packs

If your source environment is at 8.2, you can install 8.2 fix packs.

If your source environment is at version 7.2.x or earlier, you must first migrate to 7.3.x or later. You can then migrate to 8.2.

Installation locations for IBM OpenPages with Watson

The installation directory is the location of product artifacts after a package, product, or component is installed. The following table lists the conventions that are used to refer to the installation location of installed components and products:

Important: Directory locations that contain spaces are not supported. IBM OpenPages with Watson or any software that is used by it must not be installed into a directory with spaces. For example, do not install database server, database client, or application server software into the Program Files directory.

If you're using IBM OpenPages for IBM Cloud Pak for Data, see the *IBM OpenPages with Watson Administrator's Guide*.

Table 1. Variable notations for installation directories	
Directory	Description
<installation_server_home>	<p>The directory where the IBM OpenPages with Watson installation server is installed.</p> <p>For example:</p> <ul style="list-style-type: none"> • On Windows: C:\IBM\OPInstall\OP_<version>_Installer • On Linux®: /home/opuser/IBM/OPInstall/OP_<version>_Installer
<agent_home>	<p>The directory where the IBM OpenPages with Watson installation agent is installed on a remote server.</p> <p>For example:</p> <ul style="list-style-type: none"> • On Windows: C:\IBM\OPAgent • On Linux: /home/opuser/IBM/OPAgent

Table 1. Variable notations for installation directories (continued)

Directory	Description
<OP_HOME>	<p>The directory where OpenPages with Watson is installed.</p> <p>For example:</p> <ul style="list-style-type: none"> • On Windows: C:\IBM\OpenPages • On Linux: /opt/opuser/IBM/OpenPages <p>In the installation app, you specify the <OP_HOME> directory in the OP Home Directory field each Application Server card.</p>
<ORACLE_HOME>	<p>The installation location of the Oracle database software.</p> <p>For example:</p> <ul style="list-style-type: none"> • On Windows: <ul style="list-style-type: none"> – C:\app\oracle\product\19.0.0\client_1 (Oracle Admin Client) – C:\oracle\instantclient_19_9 (Oracle Instant Client) – C:\app\oracle\product\19.0.0\dbhome_1 (server) • On Linux: <ul style="list-style-type: none"> – /home/oracle/app/oracle/product/19.0.0/client_1 (Oracle Admin Client) – /home/oracle/instantclient_19_9 (Oracle Instant Client) – /home/oracle/app/oracle/product/19.0.0/dbhome_1 (server)
<DB2_HOME>	<p>The installation location of the IBM Db2® software.</p> <p>For example:</p> <ul style="list-style-type: none"> • On Windows: C:\IBM\SQLLIB • On Linux: /home/db2inst1/sqllib
<WLP_HOME>	<p>The installation location of IBM WebSphere® Liberty.</p> <p>For example:</p> <ul style="list-style-type: none"> • On Windows: <OP_HOME>\wlp • On Linux: <OP_HOME>/wlp
<WLP_USER_HOME>	<p>The location of OpenPages with Watson application files and server configuration files.</p> <p>For example:</p> <ul style="list-style-type: none"> • On Windows: <OP_HOME>\wlp-user • On Linux: <OP_HOME>/wlp-user
<COGNOS_HOME>	<p>The installation location of Cognos® Analytics.</p> <p>For example:</p> <ul style="list-style-type: none"> • On Windows: C:\IBM\cognos\analytics • On Linux: /usr/IBM/cognos/analytics

Table 1. Variable notations for installation directories (continued)

Directory	Description
<JAVA_HOME>	<p>The installation location of IBM SDK, Java™ Technology Edition or Java Runtime Environment (JRE).</p> <p>IBM SDK example on an application server:</p> <ul style="list-style-type: none"> • On Windows: C:\IBM\java_8.0_64 • On Linux: /opt/IBM/java_8.0_64 <p>JRE example on a reporting server where Cognos Analytics is installed:</p> <ul style="list-style-type: none"> • On Windows: C:\IBM\cognos\analytics\jre • On Linux: /usr/IBM/cognos/analytics/jre <p>Note: In Cognos Analytics 11.1.5 and later, the path is:</p> <ul style="list-style-type: none"> • On Windows: C:\IBM\cognos\analytics\ibm-jre\jre • On Linux: /usr/IBM/cognos/analytics/ibm-jre/jre <p>IBM SDK example on a search server:</p> <ul style="list-style-type: none"> • On Windows: C:\IBM\java_8.0_64\ • On Linux: /opt/IBM/java_8.0_64/
<CC_HOME>	<p>The installation location of OpenPages with Watson CommandCenter.</p> <p>For example:</p> <ul style="list-style-type: none"> • On Windows: C:\IBM\OpenPages\CommandCenter • On Linux: /opt/IBM/OpenPages/CommandCenter
<SEARCH_HOME>	<p>The installation location of global search.</p> <p>The <SEARCH_HOME> directory contains the opsearchtools.jar, Apache Solr, and other global search files. The global search indexing directory is also stored in the <SEARCH_HOME> directory.</p> <p>For example:</p> <ul style="list-style-type: none"> • On Windows: C:\IBM\OpenPages\OPSearch • On Linux: /opt/IBM/OpenPages/OPSearch <p>In the installation app, you specify the <SEARCH_HOME> directory in the Search Home Directory field on the Search Server card.</p>

Changes to the installation process

If you installed previous versions of IBM OpenPages with Watson, you will notice many differences. The installation process has changed to make it easier to install and maintain IBM OpenPages with Watson.

IBM OpenPages with Watson now uses IBM WebSphere Liberty. When you install OpenPages, WebSphere Liberty is automatically installed and configured for you.

The following sections describe the main changes to OpenPages on WebSphere Liberty.

Deployment manager

You no longer need to set up a deployment manager for OpenPages.

When you migrate, the installer server updates the `deploy.properties` file automatically. You do not need to edit the file to remove the deployment manager. When you open your deployment in the installation app, review each card, enter passwords, and then continue with the migration.

The admin application server is still *AppServer1*.

Nodes and cells

WebSphere Liberty does not use "nodes" or "cells". Each horizontal cluster member is its own instance of WebSphere Liberty. Vertical cluster members share the same instance of WebSphere Liberty.

If you have a shared cell deployment, you can upgrade or migrate to 8.2, and then do some manual steps to remove OpenPages from the cell.

WebSphere installation user (wasuser)

You no longer need the `wasuser` operating system user account. OpenPages installs WebSphere Liberty with the `opuser` account.

The WebSphere username and password are no longer required by tools and utilities, such as OPBackup.

File locations

Table 2. File locations		
	Pre-8.2	8.2.0 and later
Application server runtime	<code><WAS_HOME></code>	<code><OP_HOME>/wlp</code>
OpenPages application files	<code><OP_Home>/profiles/ <node>/ installedApps/<cell>/op- apps.ear</code>	<code><OP_HOME>/wlp-usr/shared/ apps/op-apps.ear</code>
Server profiles	<code><OP_Home>/profiles/ <node>/ servers/<profile></code> Where <i><profile></i> was configured in the WebSphere Administrative Console	<code><OP_HOME>/wlp-usr/servers</code>
Server logs	<code><OP_Home>/profiles/ <node>/logs/<server></code>	<code><OP_HOME>/wlp- usr/servers/ <server_name>Server<#>/ logs</code>

The WebSphere Liberty documentation uses the placeholder `${server.output.dir}`. In OpenPages, the equivalent directory is `<OP_HOME>/wlp-usr/servers/<server_name>Server<#>`.

For example, `${server.output.dir}/logs` is the `<OP_HOME>/wlp-usr/servers/
<server_name>Server<#>/logs` directory on an OpenPages application server.

Environment variables

OpenPages configures the following environment variables for WebSphere Liberty:

- `<WLP_HOME>`: This directory is where WebSphere Liberty is installed on the application server.
- `<WLP_USER_HOME>`: This directory is where OpenPages application files and server configuration files are stored. The application and configuration files are stored in a separate directory to simplify updates to WebSphere Liberty.

Java

You need to install IBM SDK, Java Technology Edition on each application server before you install OpenPages. You can get the IBM SDK from the OpenPages installation package.

Starting and stopping application servers

You use the following scripts to start and stop application servers: `startAllServers.sh | .cmd` and `stopAllServers.sh | .cmd`. The `stopAllServers.sh | .cmd` script no longer requires a username and password.

The following scripts are no longer used:

- `startManager.sh | .cmd`, `stopManager.sh | .cmd`
- `startNode.sh | .cmd`, `stopNode.sh | .cmd`
- `startServer.sh | .cmd`, `stopServer.sh | .cmd`

For Microsoft Windows, the OpenPages service is now called: `<OpenPages_server_name>Server#`. The following services are no longer used:

- `IBMWAS<version>Service - <OpenPages_dmgr_name>`
- `IBMWAS<version>Service - <OpenPages_node_name>`
- `IBMWAS<version>Service - <OpenPages-node-name>Server<#>`

Application server log files

Application server activity, including server startup, is now logged in the following file: `<OP_HOME>/wlp-user/servers/<server_name>Server<#>/logs/messages.log`.

The `startServer.log` and `SystemOut.log` files are no longer used.

Application server configuration

In previous releases, you used the IBM WebSphere Integrated Solutions Console to configure application server settings. You now use the following files to configure application server properties.

- `<OP_HOME>/wlp-user/servers/<server_name>Server<#>/bootstrap.properties`: This file contains server properties, such as the OpenPages application port number.
- `<OP_HOME>/wlp-user/servers/<server_name>Server<#>/configDropins/overrides/jvm.options`: Use this file to customize the options for the JVM, such as Java heap size.
- `<OP_HOME>/wlp-user/servers/<server_name>Server<#>/configDropins/overrides/op-apps.xml`: Use this file to customize OpenPages, for example to change the context root, configure single sign-on, set up TLS/SSL, and so on.

If you previously customized the `web.xml`, `application.xml`, or settings in the IBM WebSphere Integrated Solutions Console, you need to re-apply the configurations in WebSphere Liberty.

Application server tuning

In previous releases, it was necessary to configure the OpenPages application servers to avoid timeouts, Java heap errors, and other issues. You no longer need to do this task. The application server tuning parameters are set when you install OpenPages. You can adjust the settings if needed, however.

Location for customized JSPs

Previously, customized JSPs were stored in the following locations:

```
<OP_HOME>/profiles/<OpenPages-node-name>/installedApps/  
<OpenPages-cell-name>/op-apps.ear/openpages.war
```



```
<OP_HOME>/profiles/<OpenPages-node-name>/installedApps/  
<OpenPages-cell-name>/op-apps.ear/publishweb.war
```

```
<OP_HOME>/profiles/<OpenPages-node-name>/installedApps/  
<OpenPages-cell-name>/op-apps.ear/sosa.war
```

Now, store your customized JSPs in the following locations:

```
<OP_HOME>/wlp-user/shared/apps/op-apps.ear/openpages.war
```

```
<OP_HOME>/wlp-user/shared/apps/op-apps.ear/publishweb.war
```

```
<OP_HOME>/wlp-user/shared/apps/op-apps.ear/sosa.war
```

Keystore on application servers

The installation process creates a default keystore: `<OP_HOME>/wlp-user/servers/<server_name>Server<#>/resources/security/key.p12`. The initial password of the keystore is the same as the OpenPagesAdministrator password that you set when you install OpenPages. You can change the keystore password. For more information, see the *IBM OpenPages with Watson Administrator's Guide*.

Workflow Server card removed

The **Workflow Server** card is no longer available in the installation app because the functionality to integrate IBM OpenPages with Watson with IBM Business Process Manager was removed.

Other changes

- The J2EE libraries are stored in `<WLP_HOME>/dev/api/spec`.

Notes for customers upgrading or migrating from 7.3.x

If you installed IBM OpenPages with Watson 7.3.x or earlier, you will notice many differences to the installation process. The installation process has changed to make it easier to install and maintain IBM OpenPages with Watson.

Phases of the installation process

The installation process is divided into three phases:

- **Validation:** After you enter the details for your deployment, you validate them. The installation server checks your deployment for any issues that need to be resolved before you continue with the installation. The installation server also installs and starts agents on the remote servers that are in your deployment.
- **Installation:** During this phase, the installation server stages the assets onto the servers in your deployment.
- **Configuration:** During this phase, the installation server sets up and configures the OpenPages components.

You complete each phase before continuing to the next phase.

New installation server component

The installation server replaces the IBM OpenPages Administrative Console. The installation server automates many tasks that were done manually in previous versions. The installation server also provides more validation, more flexibility in configuring your deployment, and improved error logging.

You can install and upgrade multiple environments with a single installation server. You can install the installation server on a separate computer or on a server in an OpenPages environment. In addition, you do not need to install IBM Installation Manager to install the installation server. The installation server includes its own installer.

The installation server provides a web application, called the installation app, which you can use to install and upgrade OpenPages. You can also install and upgrade in silent mode. The installation app replaces the OpenPages Administrative Console user interface.

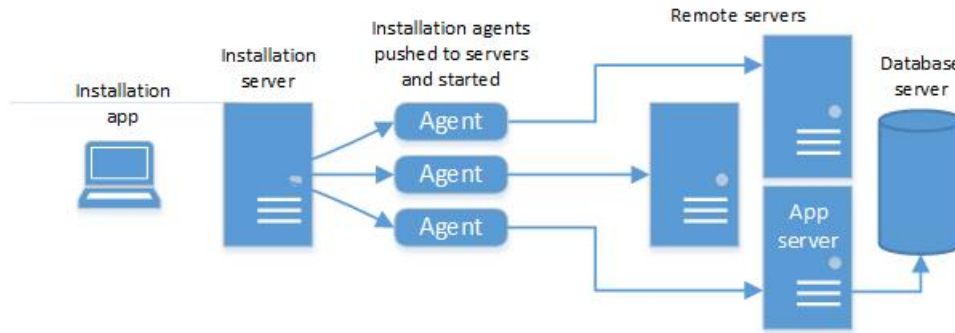


Figure 1. Installation server

Tip: You can log out and close the installation app during the **Install** and **Configure** processes. The processes continue to run. When you log in to the installation app again, the app shows the status of your deployment.

Agents

In previous versions, you needed to install `OPAdminConsoleRemote` on each server in your deployment. Now, the installation server installs the agent software and starts the agents on remote servers automatically. The agent software is not needed on the database server.

To install the agents on remote servers, you must have access to an account on the remote server. The account must have the necessary permissions to install and run software on the remote server.

Or, you can install the agents manually on remote servers.

Ports

In previous versions, default ports were used. Now, you can set custom port numbers for application servers, Cognos Analytics, and other components when you configure your deployment.

Rollback operations

In previous versions, if a failure occurred during an operation, the entire process failed. Now, you can use the **Rollback** option for each server to roll back the operation that caused the error. This feature enables you to resolve issues more quickly and resume the installation from the point of failure.

Migrating files during a migration upgrade

You can choose the files and directories that you want to migrate when you do a migration upgrade of OpenPages.

Redesigned database scripts

The database scripts that are used to install and upgrade the OpenPages database have been redesigned. The redesigned scripts provide the following enhancements:

- The database installation and upgrade scripts incorporate more pre- and post-validation checks than in previous versions.

- The scripts now separate DBA and non-DBA tasks.

When you install the database, you now have the following options:

- You can use the OpenPages installation app to create the database objects. The user who installs OpenPages must provide DBA credentials.
- A database administrator can run the scripts that require DBA privileges, and then another user can use the OpenPages installation app to complete the installation.
- You can create all of the objects required for the database manually before you install OpenPages. A database administrator must run the scripts that require DBA privileges. A schema user can run the other scripts.

When you upgrade the database, a database administrator runs the scripts that require DBA privileges. A user who is not a database administrator can run the scripts that do not require DBA privileges.

- Oracle Transparent Data Encryption is now supported.
- You can use an Oracle pluggable database (PDB) for the OpenPages database.
- You can customize the schema name (Oracle) and table space names (Oracle and IBM Db2) when you create the OpenPages database.
- You no longer need to run the `sysdba-xa-views-wrapper.sql` script. The `sysdba-create-xa-views.sql` and `sysdba-xa-grants.sql` scripts are also no longer used.

Validation

Additional validation is done before you install OpenPages. The installation server validates each server in your deployment before the installation process begins.

The additional validation prevents possible deployment failures caused by configuration issues, unmet prerequisites, and insufficient permissions. The additional validation enables you to identify and resolve issues up-front, which can save you time and effort.

For example, the installation server checks if ports are occupied. If a port is occupied, you can fix the issue before you install OpenPages. In previous versions, the ports were not validated. If a port was occupied, the deployment failed.

Validation messages are displayed on server cards. When you click the card, an error icon is displayed next to the field where the error occurs.

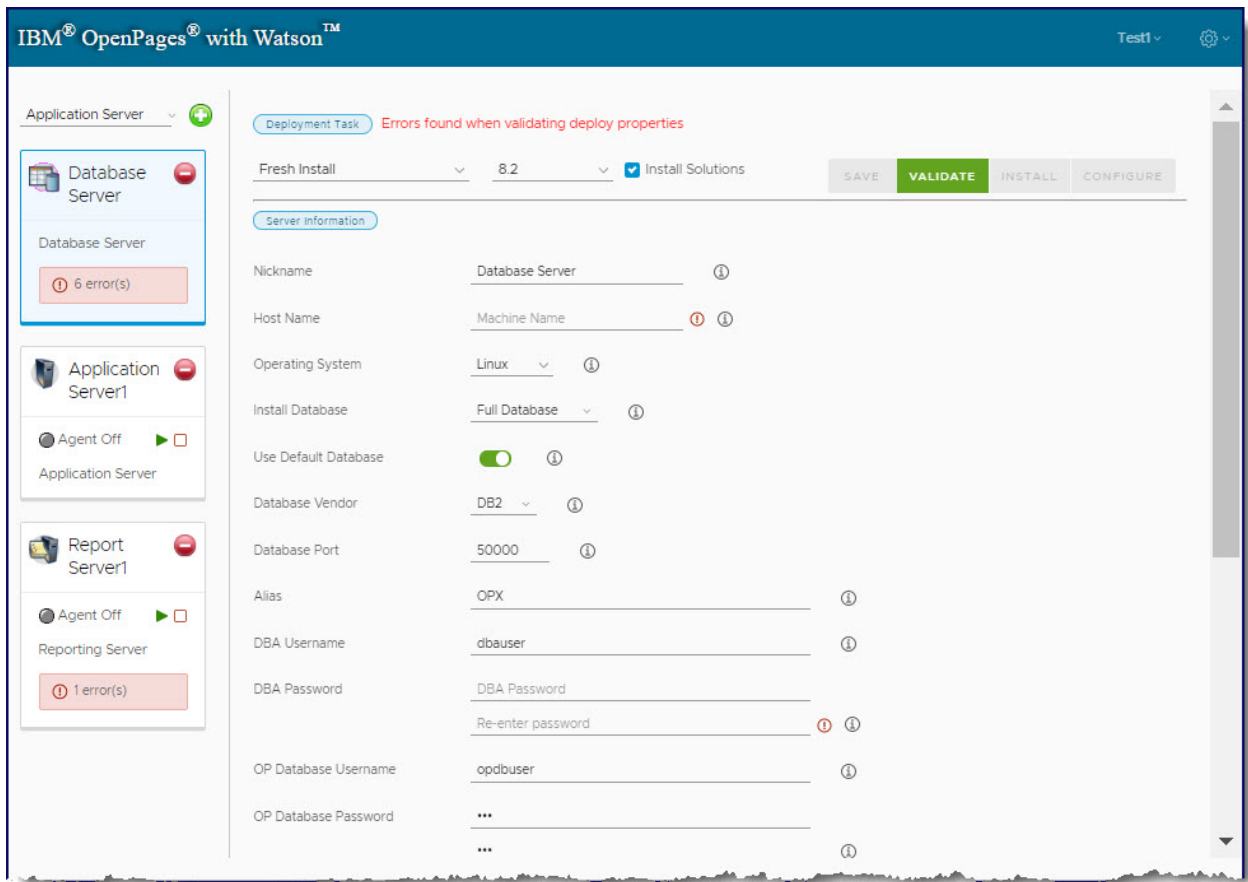


Figure 2. Example of error notifications

Installation progress

You can see the progress of your installation. Each server card shows the name of the process that is currently running. The cards are refreshed every 30 seconds, approximately.

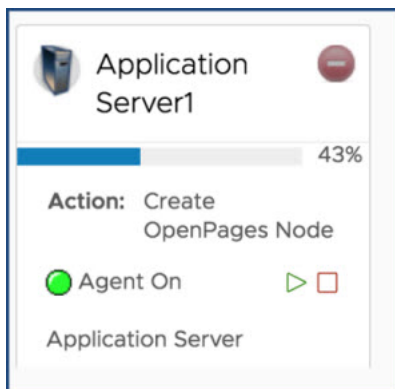


Figure 3. Progress is shown on server cards

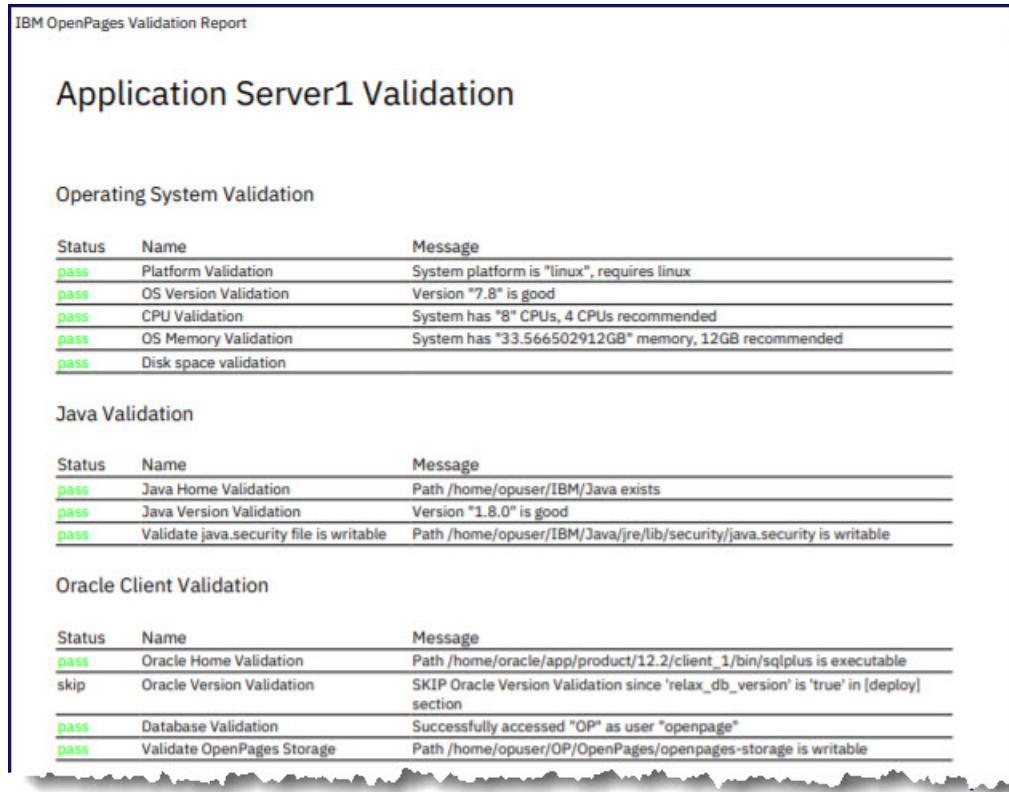
Log files and reports

The installation server provides more logging and exception handling.

- You can validate your deployment before you begin the installation process.
- You can download the validation results in a report to see the details.

- When the installation server encounters an exception, the error is displayed in the user interface. You can download the log file.
- You can view log files for each phase of the installation process as well as for each server in your deployment.

The following image shows an example of a pre-installation validation report. The page about Application Server1 is displayed. No errors were found.



IBM OpenPages Validation Report

Application Server1 Validation

Operating System Validation

Status	Name	Message
pass	Platform Validation	System platform is "linux", requires linux
pass	OS Version Validation	Version "7.8" is good
pass	CPU Validation	System has "8" CPUs, 4 CPUs recommended
pass	OS Memory Validation	System has "33.566502912GB" memory, 12GB recommended
pass	Disk space validation	

Java Validation

Status	Name	Message
pass	Java Home Validation	Path /home/opuser/IBM/Java exists
pass	Java Version Validation	Version "1.8.0" is good
pass	Validate java.security file is writable	Path /home/opuser/IBM/Java/jre/lib/security/java.security is writable

Oracle Client Validation

Status	Name	Message
pass	Oracle Home Validation	Path /home/oracle/app/product/12.2/client_1/bin/sqlplus is executable
skip	Oracle Version Validation	SKIP Oracle Version Validation since 'relax_db_version' is 'true' in [deploy] section
pass	Database Validation	Successfully accessed "OP" as user "openpage"
pass	Validate OpenPages Storage	Path /home/opuser/OP/OpenPages/openpages-storage is writable

Figure 4. Example of a validation report that shows results for an application server

Warnings do not need to be fixed before you install OpenPages.

IBM Java 8 is provided with Cognos Analytics

In previous versions, you needed to install Java on each reporting server in your deployment. Cognos Analytics V11 includes IBM Java 8.

IBM HTTP Server for Cognos Analytics

If you use IBM HTTP Server to load balance the reporting servers, note that the configuration method has changed. See the Cognos Analytics documentation for details.

Oracle database alias

If you use the same Oracle database instance for OpenPages and Cognos, use the same database alias for both OpenPages and Cognos.

When you configure the database connection information, you can choose to use either the SID or the Service Name.

Special characters in passwords

You can use certain special characters in certain passwords.

If you are upgrading or migrating from 8.1.0.1 or earlier, install the 8.2 installation server, complete the upgrade or migration process, and then update passwords to use special characters.

The special characters that you can use in passwords are:

```
. + - [ ] * ~ _ # : ?
```

Note: Spaces are not supported.

You can use these special characters in database user passwords and operating system accounts for database schema owners.

If you use special characters in passwords, you must surround the password in quotation marks. Use the following syntax:

IBM Db2 connection strings

For Db2 databases, when you provide a password in a connection string, use the following syntax:

On Linux, use \ ' around the password. For example:

```
clpplus -nw openpage/\ 'DB~Password\'@host:50000/opx
```

On Windows, use single quotation marks around the password:

```
clpplus -nw openpage/'DB~Password'@host:50000/opx
```

IBM Db2 script parameters in CLPPlus

For Db2 databases, when you provide a password in a script parameter, use the following syntax:

On Linux, use one of the following options:

- Use \ ' around the password. For example:

```
clpplus -nw @sql-wrapper CustomIndexing_Step1_AddTextIndexing_to_DB.sql  
/tmp/log.log c6de0652985e 50000 OPX db2inst1 \ 'DB~Password\' openpage
```

- Use \ " around the password:

```
clpplus -nw @sql-wrapper CustomIndexing_Step1_AddTextIndexing_to_DB.sql  
/tmp/log.log c6de0652985e 50000 OPX db2inst1 \ "DB~Password\" openpage
```

On Windows, use one of the following options:

- Use ' around the password. For example:

```
clpplus -nw @sql-wrapper CustomIndexing_Step1_AddTextIndexing_to_DB.sql  
/tmp/log.log jwinpages.swg.usma.ibm.com 50000 OPX db2admin 'DB~Password' openpage
```

- Use \ " around the password:

```
clpplus -nw @sql-wrapper CustomIndexing_Step1_AddTextIndexing_to_DB.sql  
/tmp/log.log jwinpages.swg.usma.ibm.com 50000 OPX db2admin \ "DB~Password\" openpage
```

Db2 utilities

When you run Db2 utilities, such as db2 connect or db2rbind, do not use quotation marks around passwords.

Oracle connection strings

For Oracle databases, when you provide a password in a connection string, use \ " around the password. For example:

```
sqlplus sys/\ "DB~Password\"@op as sysdba
```

Oracle script parameters in SQL*Plus

For Oracle databases, when you provide a password in a script parameter, use the following syntax:

- On Windows, use double quotation marks around the password.

```
sqlplus /nolog @sql-wrapper.sql
update-storage c:\temp\upd-storage-output.log
op openpages "pass~word" LFS eng11 eng11
Windows c:\OpenPages\openpages-storage
```

- On Linux, use single quotation marks around the password.

```
sqlplus /nolog @sql-wrapper.sql
update-storage /home/op/upd-storage-output.log
op openpages 'pass~word' LFS eng11 end11
Unix /usr/opdata/openpages-storage
```

Installation scripts, tools, and utilities

For tools and utilities that take the password as a parameter, use the following syntax:

- On Windows, use double quotation marks around the password.

```
op-validate-dba-install.bat "DB~Password"
```

- On Linux, use single quotation marks around the password.

```
./op-validate-dba-install.sh 'DB~Password'
```

Passwords in property files

For .env files and .properties files, do not use any quotation marks around passwords.

Chapter 2. What's new?

New and changed features affect the installation and configuration of IBM OpenPages with Watson. Use this information to help you plan your upgrade and deployment strategies and the training requirements for your users.

For information about all new features for this release, see the *IBM OpenPages with Watson New Features Guide*.

For an up-to-date list of environments that are supported by OpenPages with Watson, see the [Supported Environments website](#).

New features in version 8.2.0.4

The new features in IBM OpenPages with Watson version 8.2.0.4 are described in the following sections.

Administration and serviceability enhancements

Table 3. Administration and serviceability enhancements	
For new information about...	See this topic...
Upgrade from Apache Log4j 1 to Apache Log4j 2 and changes to log files	“Configure new features” on page 299

New features in version 8.2.0.3

The new features in IBM OpenPages with Watson version 8.2.0.3 are described in the following sections.

Solutions enhancements

Table 4. Solutions enhancements	
For new information about...	See this topic...
Update to IBM OpenPages Internal Audit Management	“Updating IBM OpenPages Internal Audit Management settings” on page 303

New features in version 8.2.0.2

The new features in IBM OpenPages with Watson version 8.2.0.2 are described in the following sections.

Software versions

For details about supported software, see the [Supported Environments website](#).

Table 5. Changes to supported software versions	
Software	Conformance changes
Linux:	Red Hat Enterprise Linux (RHEL) Server 8 is now supported. If you use Linux 8.x, you also need to upgrade software that is used by IBM OpenPages with Watson, such as Db2, Oracle, and IBM Installation Manager (IIM). Review the Supported Environments website .

Table 5. Changes to supported software versions (continued)

Software	Conformance changes
Microsoft Windows	Microsoft Windows Server 2019 is now supported. If you use Microsoft Windows Server 2019 you also need to upgrade software that is used by IBM OpenPages with Watson, such as Db2, Oracle, and IBM Installation Manager (IIM). Review the Supported Environments website .
Oracle	Oracle Instant Client is now supported for Oracle 19c. For more information, see “Oracle Instant Client” on page 101 .

Solutions enhancements

Table 6. Solutions enhancements

For new information about...	See this topic...
Updating to the new version of IBM OpenPages Financial Controls Management	“Updating IBM OpenPages Financial Controls Management” on page 302
For the following solutions, you can replace computed fields with calculations: <ul style="list-style-type: none">IBM OpenPages Internal Audit ManagementIBM OpenPages IT Governance	“Replacing computed fields with calculations ” on page 304

Administration and serviceability enhancements

Table 7. Administration and serviceability enhancements

For new information about...	See this topic...
Improved logging for SAML, OIDC, and SPNEGO single sign-on	IBM OpenPages with Watson Administrator's Guide
After you install 8.2.0.2, note the following name changes: <ul style="list-style-type: none">bcprov-jdk14-145.jar is now bcprov-jdk15to18-1.68.jarorg.bouncycastle145.jce.provider.BouncyCastleProvider is now org.bouncycastle.jce.provider.BouncyCastleProviderCAMCryptoBC is now BC	

New features in version 8.2.0.1

The new features in IBM OpenPages with Watson version 8.2.0.1 are described in the following sections.

Software versions

For details about supported software, see the [Supported Environments website](#).

Table 8. Changes to supported software versions

Software	Conformance changes
IBM Db2	Enterprise Server Edition 11.5.4.x and later 11.5.4.x releases is now supported. If you are upgrading or migrating to 8.2, complete the upgrade or migration before you upgrade to Db2 11.5.4. Otherwise, you will see errors during the OpenPages database upgrade. Version 11.1.4.4 is the minimum supported version.
IBM Security Directory Integrator	7.2.0.6 is now supported

Solutions enhancements

Table 9. Solutions enhancements

For new information about...	See this topic...
Version 8.2.0.1 introduces updates to IBM OpenPages Regulatory Compliance Management.	If you want to update this solution, contact IBM OpenPages Support.

Administration and serviceability enhancements

Table 10. Administration and serviceability enhancements

For new information about...	See this topic...
New application permissions <ul style="list-style-type: none"> Watson Language Translation Watson Language Translation UI 	“Configure new features” on page 299
The location of the dojo and idx files has changed. The new paths are: <ul style="list-style-type: none"> <OP_HOME>/wlp-usr/shared/apps/op-apps.ear/sosa.war/dojo <OP_HOME>/wlp-usr/shared/apps/op-apps.ear/sosa.war/idx 	
You can configure your deployment to use only the Task Focused UI.	“Enabling only the Task Focused UI” on page 419
You can specify a page to display when an error occurs with SAML single sign-on.	“Configuring an error page for SAML single sign-on” on page 325
The script for cross-track links in reports and drill-through reports has changed. If you have custom reports, update them with the new script.	See the <i>IBM OpenPages with Watson Report Author's Guide</i> .
If you use IBM OpenPages SDI Connector for UCF Common Controls Hub, update it to use IBM Security Directory Integrator 7.2.0.6 and updated assembly lines.	“Updating the IBM OpenPages SDI Connector for UCF Common Controls Hub” on page 297

New features in version 8.2.0

The new features in IBM OpenPages with Watson version 8.2.0 are described in the following sections.

Software versions

For details about supported software, see the [Supported Environments website](#).

Table 11. Changes to supported software versions	
Software	Conformance changes
Linux:	Red Hat Enterprise Linux (RHEL) Server 6.6 is no longer supported.
Microsoft Windows	Microsoft Windows Server 2012 Standard Edition and Microsoft Windows Server 2012 R2 Standard Edition are no longer supported.
AIX®	AIX is no longer supported.
Oracle	Oracle 12.1.0.2 is no longer supported.
IBM Db2	Enterprise Server Edition 11.5.0.x and later 11.5.x.x releases is now supported. Version 11.1.4.4 is the minimum supported version.
IBM SDK, Java Technology Edition	Version 8.0.6.5 and later fix packs is supported.
IBM WebSphere Application Server Network Deployment	IBM OpenPages with Watson now uses IBM WebSphere Liberty. IBM WebSphere Application Server Network Deployment (also called traditional WebSphere) is no longer supported.
IBM WebSphere Liberty	IBM WebSphere Liberty is installed automatically when you install IBM OpenPages with Watson. For more information, see “Changes to the installation process” on page 4 .
IBM Cognos Analytics	11.1.3 is now the minimum supported version. Later 11.1.x continuous releases are also supported.
Web browser support	Microsoft Edge Chromium is now supported by IBM OpenPages with Watson. Note: Current IBM Cognos Analytics 11.1.x versions do not support Microsoft Edge Chromium. For the latest information, see the Supported Software Environments report for Cognos .
IBM Business Process Manager	The integration of IBM Business Process Manager with IBM OpenPages with Watson is no longer supported.

Solutions enhancements

Table 12. Solutions enhancements	
For new information about...	See this topic...
Version 8.2 introduces a new solution, IBM OpenPages Business Continuity Management, which is available in fresh installations only.	IBM OpenPages with Watson Solutions Guide
Version 8.2 introduces significant updates to the following solutions. The updated solutions are available in fresh installations only. <ul style="list-style-type: none"> IBM OpenPages Regulatory Compliance Management 	If you are upgrading or migrating to 8.2 and you want to update these solutions, contact IBM OpenPages Support.
IBM OpenPages Vendor Risk Management is now called IBM OpenPages Third Party Risk Management.	Chapter 18, “IBM OpenPages Third Party Risk Management,” on page 387

Administration and serviceability enhancements

Table 13. Administration and serviceability enhancements	
For new information about...	See this topic...
ObjectManager has changed. <ul style="list-style-type: none"> The ObjectManager.log file is now created in the directory that you specify in the <code><loader-file-path></code> parameter. If the parameter is not specified, the log file is created in the current directory. The <code>-server</code> parameter is ignored because ObjectManager now runs on the server. You can install ObjectManager on a remote computer and run it remotely. 	IBM OpenPages with Watson Administrator's Guide
The search server now uses IBM SDK, Java Technology Edition.	“Getting a copy of the IBM SDK (Linux)” on page 63
New application permissions	“Configure new features” on page 217
For Oracle, when you do a fresh installation or upgrade, the installation server checks the objects that are required by OpenPages with Watson. If public access is missing on an object, the installation process grants access to the openpages database user automatically.	“Oracle package dependencies” on page 432
In mixed-mode SSO, non-SSO users now log in by using the OpenPages login page rather than a pop up.	Chapter 13, “Single sign-on integration for the OpenPages application server,” on page 321
The root folder of the OpenPages installation media has changed to <code>/OP_<version>_Main/</code> .	.
The default protocol that is used by OpenPages for secure connections (SSL/TLS) is now TLSv1.2.	

New features in version 8.1.0.1

The new features in IBM OpenPages with Watson version 8.1.0.1 are described in the following sections.

Software versions

For details about supported software, see the [Supported Environments website](#).

Table 14. Changes to supported software versions	
Software	Conformance changes
Oracle	19c is now supported.

Solutions enhancements

Table 15. Solutions enhancements	
For new information about...	See this topic...
Various updates to solutions	

Administration and serviceability enhancements

Table 16. Administration and serviceability enhancements	
For new information about...	See this topic...
The @ character is no longer supported in database passwords.	“Special characters in passwords” on page 12
OPX has been removed. The new Manage Pages and Templates option on the Settings menu in the Task Focused UI is used to define report pages and page templates.	<i>IBM OpenPages with Watson Administrator's Guide</i>

New features in version 8.1

The new features in IBM OpenPages with Watson version 8.1.0 are described in the following sections.

Software versions

For details about supported software, see the [Supported Environments website](#).

Table 17. Changes to supported software versions	
Software	Conformance changes
Oracle	18c is now supported. Oracle 12.2.0.1 and 12.1.0.2 are also supported.
IBM Db2	11.1.0 (and future 11.1.x.x releases) is now supported.
IBM Java SDK/JRE	Version 8.0.5.26 and later fix packs is supported.
IBM WebSphere Application Server	9.0.0.10 (or a higher fix pack) is now supported. WebSphere 9.0.0.3 is no longer supported.
IBM Cognos Analytics	11.1.1 (and higher 11.1.x continuous releases) is now supported. Cognos 11.0.x is no longer supported.

Table 17. Changes to supported software versions (continued)	
Software	Conformance changes
IBM Security Directory Integrator (SDI) SDI is the new name for IBM Tivoli® Directory Integrator.	7.2.0.3 is now supported. IBM Tivoli Directory Integrator 7.1.1.x is no longer supported.
Web browser support	Safari is now supported for the Task Focused UI only.

Solutions enhancements

Table 18. Solutions enhancements	
For new information about...	See this topic...
For fresh installations, the Timesheet Entry Helper and Timesheet Approval helper are installed and enabled by default. For migrations and in-place upgrades, you can install and enable the timesheet helpers.	For migrations, see "Loading Timesheet Helpers" For in-place upgrades, see the upgrade guides: <ul style="list-style-type: none"> • <i>IBM OpenPages with Watson Upgrade Guide for IBM Db2</i> • <i>IBM OpenPages with Watson Upgrade Guide for Oracle</i>
Version 8.1 introduces significant updates to the following solutions. The updated solutions are available in fresh installations only. <ul style="list-style-type: none"> • IBM OpenPages Model Risk Governance • IBM OpenPages Operational Risk Management • IBM OpenPages Regulatory Compliance Management 	If you are upgrading or migrating to 8.1 and you want to update these solutions, contact IBM OpenPages Support.

Administration and serviceability enhancements

Table 19. Administration and serviceability enhancements	
For new information about...	See this topic...
Oracle Multitenant architecture You can use a pluggable database (PDB).	“Oracle upgrade options and Oracle PDB” on page 196
In-place upgrades	“Getting started” on page 1 <i>IBM OpenPages with Watson Upgrade Guide for IBM Db2</i> <i>IBM OpenPages with Watson Upgrade Guide for Oracle</i>
The installation server service and the installation agent service are now named <code>ibmopenpageswithwatsoninstaller<version>.exe</code>	
You can no longer regenerate the Legacy Reporting Framework. Use the Reporting Framework V6.	Before you install, upgrade, or migrate to 8.1, migrate reports to the Reporting Framework V6. .

Table 19. Administration and serviceability enhancements (continued)	
For new information about...	See this topic...
The following can now be used as base currencies: BYN, MRU, STN, UYW, and VES.	
The database statistics collection script (collect-schema-stats.sql) has been updated.	<p>If you customized the script, back up your changes before you upgrade. For more information, see the upgrade guides:</p> <p><i>IBM OpenPages with Watson Upgrade Guide for IBM Db2</i></p> <p><i>IBM OpenPages with Watson Upgrade Guide for Oracle</i></p> <p>.</p>

New features in version 8.0.0.2

The new features in IBM OpenPages with Watson version 8.0.0.2 are described in the following sections.

Software versions

For details about supported software, see the [Supported Environments website](#).

Table 20. Changes to supported software versions	
Software	Conformance changes
Oracle	12.2.0.1 is now supported.
Microsoft Windows Server	<p>Microsoft Windows Server 2016 is now supported.</p> <ul style="list-style-type: none"> • If you use IBM Db2 and you use Microsoft Windows Server 2016 on the database server, you must use version 11.1.1.1. • If you use Oracle and you use Microsoft Windows Server 2016 on the database server, you must use version 12.2.0.1.
Microsoft Internet Explorer	Although Microsoft Internet Explorer 11 is fully supported only in Native mode, OpenPages 8.0.0.2 includes a capability to assist customers whose IT policies automatically switch users' browsers to Compatibility View mode. This new capability forces the user's OpenPages session to run in Native mode.

Solutions enhancements

Table 21. Solutions enhancements	
For new information about...	See this topic...
You can install new timesheet helpers.	

Administration and serviceability enhancements

Table 22. Administration and serviceability enhancements	
For new information about...	See this topic...
If you install the installation agents manually, you can leave the Local User Name and Local User Password fields empty.	“Installing agents manually” on page 45
You can now use a specific set of special characters in passwords.	“Special characters in passwords” on page 12
It's now easier to see the status of installations. During an installation, the server cards in the installation app display the name of the process that is currently running. The display is updated every 30 seconds, approximately.	“Installation progress” on page 10
You can refresh an upgraded environment. If you upgrade to OpenPages 8.0.x and perform UAT in your new environment for several weeks, you might need to later refresh your upgraded environment with the latest snapshot of your production data.	“Refreshing an 8.2 environment with data from an 8.1.x or earlier environment ” on page 414
Information about how to update host names is now available.	“Updating host names” on page 414

New features in version 8.0.0.1

The new features in IBM OpenPages with Watson version 8.0.0.1 are described in the following sections.

Administration and serviceability enhancements

Table 23. Administration and serviceability enhancements	
For new information about...	See this topic...
The new installation app makes it easier to install IBM OpenPages with Watson fix packs.	
When you enter passwords on server cards, you are now prompted to enter the passwords again to confirm them.	
Additional queries have been added to the log collector output to provide more detailed environment information.	For information about the LogCollector tool, see “Collect log files and diagnostic data” on page 428
The new Trigger Configuration Refresh Utility enables you to refresh the trigger cache. You no longer need to restart servers.	For more information, see Refreshing trigger configurations

New features in version 7.4.0

The new features in IBM OpenPages with Watson version 7.4.0 are described in the following sections.

Software versions

For details about supported software, see the [Supported Environments website](#).

<i>Table 24. Changes to supported software versions</i>	
Software	Conformance changes
Linux	Red Hat Enterprise Linux (RHEL) 6.6 (and higher minor releases and updates) is now supported in addition to RHEL 7.0. RHEL 6.5 is no longer supported.
AIX	AIX 6.1 is no longer supported. AIX 7.1 or higher is supported.
IBM WebSphere Application Server Network Deployment	IBM WebSphere 9.0.0.3 (or higher fix packs) is now supported. IBM WebSphere 8.5.5.x is no longer supported.
IBM DB2®	DB2 ESE 11.1.1.1 (or higher editions/fix packs) is supported in addition to DB2 ESE 11.1.0.0.
Oracle	Oracle 11g is no longer supported. Oracle SE 12.1.0.2 and later fix packs is supported.
IBM Java SDK/JRE	Version 8.0.4.1 and later fix packs is supported. Java 1.7 is no longer supported.
Microsoft Internet Explorer	Internet Explorer 11 in Native mode is supported. Internet Explorer 9 and 10 and Internet Explorer in Compatibility View mode are no longer supported. The Force Internet Explorer Compatibility Mode registry setting has been removed and is disregarded during upgrade. Google Chrome is also supported.
IBM Cognos	11.0.7 Interim Fix 1001 (and higher 11.0.x continuous releases) is now supported. IBM Cognos Business Intelligence 10.2.2.x is no longer supported.
Fujitsu	Fujitsu Interstage BPM is no longer supported.

Administration and serviceability enhancements

For an overview of the changes to the installation process, including the new installation server, see [“Changes to the installation process” on page 4](#).

<i>Table 25. Administration and serviceability enhancements</i>	
For new information about...	See this topic...
The new installation app makes it easier to install IBM OpenPages with Watson.	Chapter 5, “OpenPages installation server and app,” on page 41
The installation process has been redesigned.	Chapter 6, “Install IBM OpenPages with Watson,” on page 57
The upgrade process has been redesigned.	Chapter 7, “Migrate to a new version of IBM OpenPages with Watson,” on page 189
Shared cell deployments	
Oracle Transparent Data Encryption is now supported.	For new installations of IBM OpenPages with Watson, see “Oracle Transparent Data Encryption (TDE) for fresh installations” on page 136 . For upgrades, see “Oracle Transparent Data Encryption for migration customers” on page 264 .
The SQL for security rules has changed.	In certain security rules, the product was improperly extending or restricting access to users when the conditions of the security rule were met by data in past reporting periods, even when the user was interacting with data in the current reporting period. This issue was addressed by a fix to the security rules SQL that had this problem. When the fix is applied, security rule conditions are evaluated against data in the correct reporting period only. See “Updating security rules” on page 211 .

New features in version 7.3.0.2

The new features in IBM OpenPages with Watson, version 7.3.0.2, are described in the following sections.

Integration with IBM Regulatory Compliance Analytics

You can import data from IBM Regulatory Compliance Analytics into IBM OpenPages with Watson. To enable this functionality, you need to do some post-installation tasks.

New features in version 7.3.0.1

The new features in IBM OpenPages with Watson, version 7.3.0.1, are described in the following sections.

OpenPages Third Party Risk Management solution loader

The OpenPages Third Party Risk Management solution loader enables customers who upgraded from a fresh 7.2 installation to version 7.3.0.1 to load the objects, relationships, and profiles to use the OpenPages Third Party Risk Management solution.

If you had a fresh installation of IBM OpenPages with Watson version 7.2 with solutions and then upgraded to version 7.3.0.1 or later, use the solutions loader to install OpenPages Third Party Risk Management. You must have the 7.2 solutions schema in your environment. You must also have licensed OpenPages Third Party Risk Management.

UCF connector integration

Use IBM OpenPages SDI Connector for UCF Common Controls Hub to import data from UCF Common Controls Hub into IBM OpenPages with Watson.

For more information, see [Chapter 15, “IBM OpenPages SDI Connector for UCF Common Controls Hub,” on page 351.](#)

New features in version 7.3.0

New features affect the installation and configuration of IBM OpenPages with Watson.

Collect and view logs

The new LogCollector tool provides a command-line interface that you can use to collect log files and diagnostic data from the IBM OpenPages with Watson environment.

With the LogCollector tool, you can collect log and diagnostic files from the IBM OpenPages with Watson environment and from the IBM OpenPages with Watson database.

For more information, see [“Collect log files and diagnostic data” on page 428.](#)

Administrative Console application interface runs on Linux

You can now run the IBM OpenPages with Watson Administrative Console application interface on Linux systems. For more information, see [“Setting up the installation server on Linux” on page 43.](#)

Software versions

OpenPages with Watson now supports Red Hat Enterprise Linux (RHEL) 7.0 (and higher minor releases and updates). Red Hat Enterprise Linux (RHEL) 6.5 (and higher minor releases and updates) is also supported.

OpenPages with Watson requires new versions of some software. If you are upgrading or migrating, you must update your environment to use these versions:

- IBM WebSphere Application Server 8.5.5.9
- If you are using IBM DB2, version 11.1 is required. IBM DB2 version 10.5 is no longer supported.
- If you are using IBM DB2, IBM Cognos Business Intelligence (BI) version 10.2.2.6 or later is required.

Integration with IBM Business Process Manager

The integration of IBM OpenPages with Watson with IBM Business Process Manager gives you access to an enhanced level of GRC process automation. IBM Business Process Manager is a leading industry process automation system that is both scalable and highly configurable.

Chapter 3. OpenPages with Watson overview

You use IBM OpenPages with Watson to manage risk and regulatory challenges across the enterprise. OpenPages with Watson provides core services and components that span risk and compliance domains. These components include operational risk, policy management, financial controls management, IT governance, internal audit, regulatory compliance management, and model risk governance.

The following diagram shows the architectural components for OpenPages with Watson applications. The platform contains the database and key services such as the security framework and reporting framework, and document management. The solutions are configurations that work with the platform.

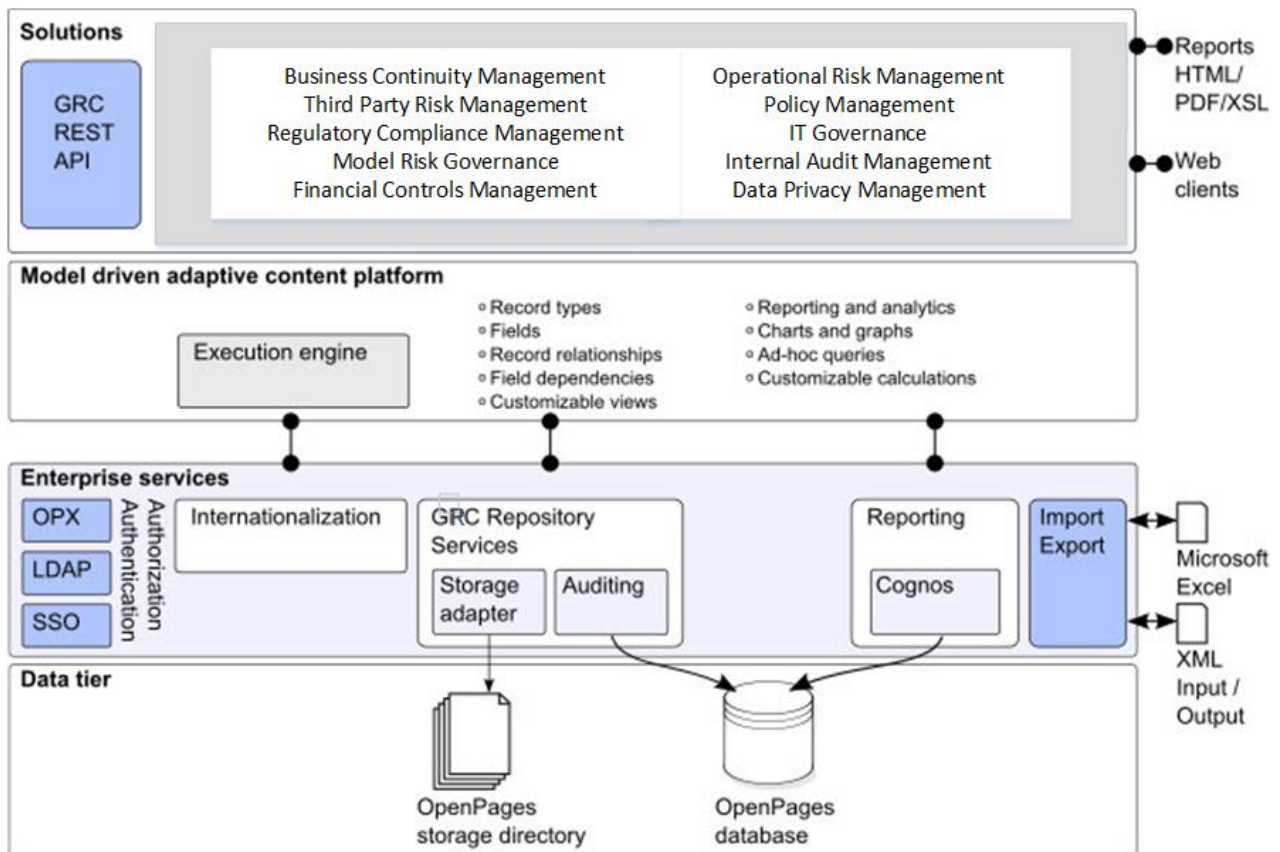


Figure 5. OpenPages with Watson components

OpenPages with Watson components

IBM OpenPages with Watson consists of the following components:

- An installation server, which is used to install IBM OpenPages with Watson.
- A database server for hosting the OpenPages with Watson repository.
- One or more application servers for hosting the OpenPages with Watson application.
- One or more reporting servers for hosting Cognos Analytics and OpenPages with Watson CommandCenter.
- Up to one search server (optional) for hosting the OpenPages with Watson global search component.

After installation, users can access OpenPages with Watson from a separate client computer.

Installation server

The IBM OpenPages with Watson installation server is required to install and upgrade IBM OpenPages with Watson (migration upgrades and in-place upgrades). You can also use it to apply fix packs and interim fixes. The installation server includes a web interface, called the installation app.

The installation server uses installation agents to install components on remote servers, except the database server. The installation server pushes the agent software to the remote servers and starts the agents automatically. For each remote server, you must provide the credentials of a local user who can install and run software on the remote server. Alternatively, you can install the agent software manually.

You can set up the installation server on one of the servers in your OpenPages environment or on a separate computer.

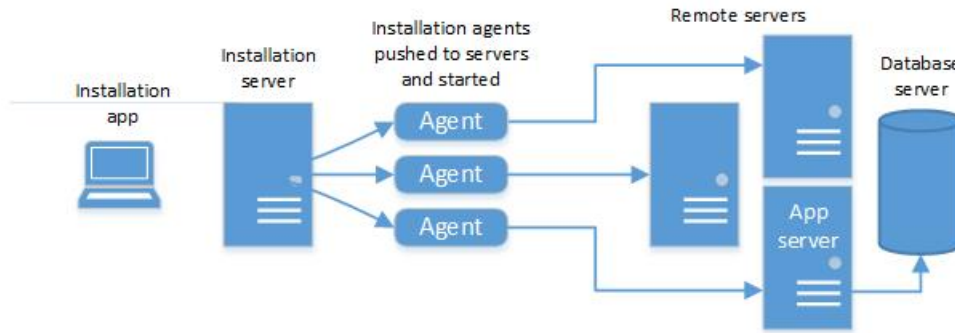


Figure 6. Installation server

Database server

A database server is required to host the IBM OpenPages with Watson repository. The repository is a central source for metadata management, versioned application data, and access control.

To install the IBM OpenPages with Watson application, you must create an OpenPages database schema, a set of database users, and table spaces.

You can automatically create and configure these components during the OpenPages installation. Alternatively, you can create them manually before you install OpenPages.

You can use an IBM Db2 database or an Oracle database for the OpenPages repository.

Application server

An application server is required to host the IBM OpenPages with Watson application.

The IBM OpenPages with Watson application server runs the application solutions, and includes the definition and administration of business metadata, UI views, user profiles, and user authorization.

OpenPages with Watson uses IBM WebSphere Liberty. WebSphere Liberty is installed automatically when you install OpenPages with Watson.

You can add horizontal and vertical cluster members for the application server.

The admin application server is the main application server for your deployment. In the installation app, the admin application server is called *AppServer1* by default.

All secondary application servers are known as non-admin application servers.

Reporting server

A reporting server is required to host Cognos Analytics and OpenPages with Watson CommandCenter.

Cognos Analytics

Cognos Analytics provides executive dashboards and reports that are designed to accelerate the review and approval of governance, risk, and compliance management (GRCM) information throughout the enterprise. Business users can browse through complex information easily by clicking dashboard elements to drill down through detailed reports.

Cognos Analytics includes a content store, which is a relational database. The content store contains data, such as report specifications, published models, and the packages that contain them. The content store also contains connection information for data sources.

If you install more than one reporting server with OpenPages with Watson, you only need one IBM Cognos content store database for all servers. The main server is known as the active reporting server, and all secondary servers are known as standby reporting servers.

For more information on active and standby servers, see the *IBM Cognos Analytics Installation and Configuration Guide*.

OpenPages with Watson CommandCenter

OpenPages with Watson CommandCenter provides the integration between OpenPages and Cognos Analytics so that you can create and run reports.

It installs the OpenPages Reporting Framework Generator and the OpenPages security provider, creates the OpenPages data sources, and imports the report packages that are supplied with OpenPages.

Search server

OpenPages with Watson supports a single search server in the enterprise configuration.

The search server is required to host the OpenPages with Watson global search component. Global search is an optional component that you can install so users can search easily for objects across the entire application from the Standard UI.

For best performance, install the search server on a separate computer.

Server topology and installation configurations

Before you install IBM OpenPages with Watson, plan the server topology. The number of computers you use depends on the expected user loads.

A mix of client and server operating systems are supported. For example, you can install OpenPages with Watson application servers on a Windows operating system and install the OpenPages database on Linux operating systems. You can also install the OpenPages application servers on Linux and install the OpenPages database on Windows.

Use the following guidelines to plan your server topology.

Very light loads for proof of concept testing and demos

If you want to install OpenPages to see new features or to develop a proof of concept, you can use Docker to install OpenPages. For more information, see [Appendix B, “Install OpenPages by using Docker,” on page 399](#).

Light loads

For light user loads, you can use one application server, one reporting server, and a database server.

If you are installing a search server, install it on a separate computer.

This topology is typical in a testing or staging environment.

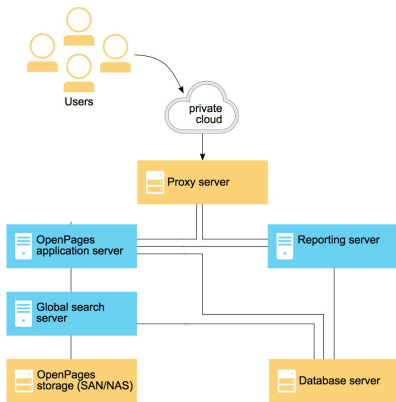


Figure 7. Topology for test environments or light user loads

Moderate to high loads

For moderate to high loads, set up a clustered OpenPages with Watson environment. By adding vertical or horizontal cluster members to the environment, you can increase scalability. Scaling requires that you use a load balancer to distribute the incoming client requests.

You can scale application servers horizontally or vertically by adding cluster members. You can also scale the reporting server by adding horizontal cluster members.

If you are installing a search server, install it on a separate computer.

The following diagram shows an example of using horizontal cluster members for the application server and for the reporting server. A load balancer distributes incoming requests to horizontal cluster members.

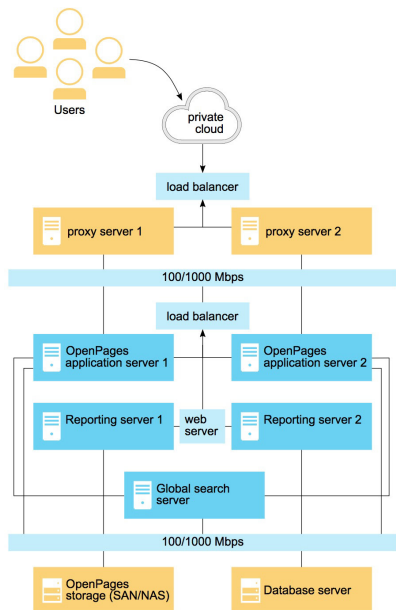


Figure 8. Topology for moderate to high user loads

Clustered environments

A clustered environment consists of multiple IBM OpenPages with Watson application servers (known as cluster members) running simultaneously to provide increased scalability.

You can set up a vertical cluster with multiple cluster members running on a single computer. You can also set up a horizontal cluster with multiple cluster members running on different computers.

When you set up a clustered environment, load balancing is required to distribute incoming client requests across the members. This configuration allows the IBM OpenPages with Watson application to scale as the number of concurrent users increases.

You can also scale the reporting server horizontally by installing additional reporting servers. You must configure additional Cognos dispatchers to ensure that the incoming requests are distributed across multiple servers.

Configure clustered environments

To accommodate increased user loads, you can scale the application servers and reporting servers in your IBM OpenPages with Watson environment.

Scaling application servers

You can scale application servers horizontally or vertically by adding cluster members to the OpenPages environment. A cluster member consists of an instance of the OpenPages application server. Each member runs on a different port.

When you scale, load balancing is required to distribute the incoming requests across the members.

For more information on adding horizontal and vertical cluster members to the OpenPages environment, see [“Adding servers to an OpenPages with Watson deployment” on page 407](#).

Scaling the reporting server

You can scale the reporting server horizontally by installing more reporting servers. You must configure the additional Cognos dispatchers to ensure that the incoming requests are distributed across the multiple servers.

Creating a clustered environment

The process to create a clustered OpenPages environment is summarized here:

1. Install and configure the admin application server, each non-admin application server, and the reporting server as a stand-alone system.

If you are using more than one reporting server, ensure that you stop all standby reporting servers when you install the active reporting server.

2. Configure each system for load balancing.

Set up the load balancer on the OpenPages application server or on an external system.

You can deploy a hardware or software load balancer. The load balancer must support session affinity and port-based URL routing.

Chapter 4. Installation prerequisites

Ensure that you have installed the prerequisite software and hardware before you install IBM OpenPages with Watson.

Software prerequisites

To ensure that your product works properly, apply all minimum required operating system patches, and use only the supported versions of third-party software. Review the prerequisite software before installing IBM OpenPages with Watson.

You can review the supported prerequisite software by using the [Supported Environments website](#).

Prerequisite software for all servers

Before you install IBM OpenPages with Watson, ensure that the prerequisite software is installed on each server in your environment.

The following table lists the third-party software that must be installed on each computer you are using for the database server, all application servers, reporting servers, and the search server.

For more information, see the [Supported Environments website](#).

Table 26. Software prerequisites for all Microsoft Windows servers	
Requirement	Specification
Operating system	Microsoft Windows Server 2016 Standard Edition
Web browser	Google Chrome Microsoft Edge Chromium
File compression utility	For example, WinZip or 7-Zip
PDF reader	For example, Adobe Acrobat Reader

Table 27. Software prerequisites for all Linux computers	
Requirement	Specification
Operating system	Red Hat Enterprise Linux (RHEL) Server 7.x Red Hat Enterprise Linux (RHEL) Server 8.x (supported in 8.2.0.2 and later)
File compression utility	For example, GNU compression utility (gtar)
bash	bash must be installed in /bin/bash.

Note: If you are using Red Hat Enterprise Linux 7.2.x, note the following known issue <https://access.redhat.com/solutions/2062273>. To fix the issue, edit the /etc/systemd/logind.conf file, set RemoveIPC=no, and then restart the corresponding service or reboot.

Prerequisite software for the installation server

The following table provides the software requirements for the installation server.

You can install the installation server on a separate computer or on a computer in your IBM OpenPages with Watson environment, such as the admin application server.

Always use the latest version of the installation server when you install, upgrade, migrate, or apply a fix pack. The latest version is provided in the most recent installation kit or fix pack kit.

After you install the installation server, you can use the OpenPages installation app to create and manage deployments. For more information, see [Chapter 5, “OpenPages installation server and app,”](#) on page 41.

Table 28. Software prerequisites for the installation server computer	
Requirement	Specification
IBM SDK, Java Technology Edition or IBM Runtime Environment for Java 8	IBM SDK, Java Technology Edition Version 8 or IBM Java JRE 8.0_64 Install IBM SDK, Java Technology Edition and set up the system environment variables for Java on the installation server before you install the installation app. See “Getting a copy of the IBM SDK (Windows)” on page 60 or “Getting a copy of the IBM SDK (Linux)” on page 63.
Windows PowerShell	If you are using Microsoft Windows, then Windows PowerShell version 4.0 or later is required.
Additional requirements for Linux servers	If you are using Linux on the installation server or on remote servers, ensure that each Linux server has the following packages: <ul style="list-style-type: none">• psmisc• lsof• iproute The installation server and installation agents need these packages.

Prerequisite software for the database server

You must install the required software on the database server, including any fix packs, patches, or other service updates.

For more information, see the [Supported Environments website](#).

Table 29. Supported database server software

Database server software	Version
IBM Db2	<p>11.5.0.x or later 11.5.x.x releases and 11.1.4.4 or later 11.1.4.x releases</p> <p>Important: Fix pack 8.2.0.1 supports Db2 11.5.4. If you are migrating or upgrading to 8.2, complete the migration or upgrade before you upgrade to Db2 11.5.4. Otherwise, you will see errors during the OpenPages database upgrade.</p> <p>If you use IBM Db2 11.5.0.x, Cognos Analytics 11.1.5 is required.</p> <p>You might also need to install a special build to resolve an issue with Db2. See Some security rule deployments on Db2 can return smaller result sets than expected.</p> <p>If you are installing the database server on a Microsoft Windows operating system, ensure that the C : \ drive contains a minimum of 8 GB of free disk space for temporary files that are created during the installation.</p> <p>If you are installing the database server on a Linux operating system, ensure that the temp directory contains sufficient free disk space for log files that are created during the installation.</p> <p>Note: Use the same version of the Db2 client on your application servers and reporting servers.</p>
Oracle	<p>Oracle Enterprise Edition (EE) 19c (19.3 and later 19.x), 18c (18.3 and later 18.x), and 12.2.0.1</p> <p>Oracle Standard Edition 2 (SE2) 19c (19.x), 18c (18.x), and 12.2.0.1</p> <p>Note: Use the same version of the Oracle client software on your application servers and reporting servers.</p> <p>If you use Oracle 12.2 and you use field level encryption for long string fields, you need to apply an Oracle patch to fix an Oracle issue. See the following technote.</p>

Prerequisite software for application servers

Ensure that you install the prerequisite software on all application servers.

The following table lists the software requirements for application servers.

Table 30. Software prerequisites for application server computers

Requirement	Specification
IBM SDK, Java Technology Edition (IBM SDK)	<p>Version 8</p> <p>IBM SDK is available on the IBM OpenPages with Watson installation media.</p> <p>Install IBM SDK and set up the system environment variables for Java on each application server before you install OpenPages with Watson. See “Getting a copy of the IBM SDK (Windows)” on page 60 or “Getting a copy of the IBM SDK (Linux)” on page 63.</p>
Database client software	<p>IBM Db2 or Oracle database client software.</p> <p>If the database server is on a separate computer, install the database client software on each OpenPages application server in your deployment.</p> <p>Db2</p> <p>Ensure that you use the same version for the database client software and database server software. Apply all required patches, interim fixes, or services to both the database server and the database client software.</p> <p>Oracle</p> <p>You can use the Oracle Admin Client or the Oracle Instant Client (supported in 8.2.0.2 and later).</p> <p>Ensure that you use the same version for the database client software and database server software.</p> <p>If you are using the same computer for the application server and reporting server, you must install the 32-bit version.</p>
IBM Installation Manager (IIM)	<p>1.8.7 or later</p> <p>IIM is used to install IBM HTTP Server, IBM OpenPages Loss Event Entry, and IBM OpenPages SDI Connector for UCF Common Controls Hub.</p>
Additional requirements for Linux servers	<p>Ensure that each Linux server has the following package: <code>psmisc</code></p>

Prerequisite software for reporting servers

The following table provides the software requirements for reporting servers.

Table 31. Software prerequisites for reporting server computers	
Requirement	Specification
Reporting server	<p>Cognos Analytics 11.1.3 or later continuous delivery releases.</p> <p>If you use IBM Db2 11.5, Cognos Analytics 11.1.5 is required.</p> <p>For information about the software prerequisites for Cognos Analytics, see the <i>IBM Cognos Analytics Installation and Configuration Guide</i>.</p> <p>If you are using Linux 7.x, update <code>pam.x86_64</code> and then install <code>pam.i686</code>. For example, run <code>yum install pam.x86_64</code> and then run <code>yum install pam.i686</code>.</p>
Web server	<p>One of the following web servers:</p> <ul style="list-style-type: none">• Apache HTTP Server 2.2.14 or later• IBM HTTP Server 9.0.5 or later• Microsoft IIS 8.0 and later fix packs (Windows only)
Database client software	<p>IBM Db2 or Oracle database client software.</p> <p>If the database server is on a separate computer, install the database client software on each reporting server in your deployment.</p> <p>Db2</p> <p>Ensure that you use the same version for the database client software and database server software. Apply all required patches, interim fixes, or services to both the database server and the database client software.</p> <p>Oracle</p> <p>You can use the Oracle Admin Client or the Oracle Instant Client (supported in 8.2.0.2 and later).</p> <p>Ensure that you use the same version for the database client software and database server software.</p> <p>If you are using the same computer for the application server and reporting server, you must install the 32-bit version.</p>

Prerequisite software for the search server

The following table provides the software requirements for the search server.

The search server must be installed on a different computer from the IBM OpenPages with Watson application server.

Table 32. Software prerequisites for the search server computer	
Requirement	Specification
IBM SDK, Java Technology Edition (IBM SDK)	<p>Version 8</p> <p>The IBM SDK is available on the IBM OpenPages with Watson installation media.</p> <p>Install the IBM SDK and set up the system environment variables for Java on the search server before you install global search. See “Getting a copy of the IBM SDK (Windows)” on page 60 or “Getting a copy of the IBM SDK (Linux)” on page 63.</p>

Prerequisite software for OpenPages client computers

Ensure that prerequisite software is installed on all computers that access IBM OpenPages with Watson.

The following table lists the software requirements for client computers.

Table 33. Software prerequisites for client computers	
Requirement	Specification
Web browser	<p>Google Chrome</p> <p>Apple Safari, for the Task Focused UI only</p> <p>Note: If you use keyboard shortcuts in Safari, enable the following setting: Preferences > Advanced > Press Tab to highlight each item on a webpage.</p> <p>Microsoft Edge Chromium</p>
PDF reader	For example, Adobe Acrobat Reader.
Optional: Microsoft Excel	<p>Microsoft Excel 2010 or 2013.</p> <p>Required for some reporting functions.</p>
Optional: Microsoft Office 2016 or Microsoft 365	Required for users who open and edit Microsoft Office documents directly from OpenPages.
Optional: Microsoft .NET Framework	Required on client computers where IBM Cognos for Microsoft Office products are installed. For more information, see the Cognos documentation.

Hardware prerequisites

To ensure that your product works properly, you must have hardware that is correctly sized for your IBM OpenPages with Watson deployment. Review the hardware prerequisites before installing the deployment.

IBM OpenPages with Watson has recommended and required minimum values per server for disk space and recommended minimum values for CPU and RAM. During the installation process, the actual capacity of the servers in your deployment is checked. A warning is issued if a server does not have the recommended capacity for CPU, RAM, or disk space. An error is issued if a server does not have the required minimum capacity for disk space. Errors must be addressed for the installation process to continue.

For more information, see [OpenPages with Watson Supported Environments](#).

VMWare configuration requirements on Windows computers

The VMWare performance on a virtualized system is comparable to hardware. You can use the hardware guidelines for the database server, application server, reporting server, or search server for sizing VM requirements.

Cloning of IBM OpenPages with Watson application server VMs is not supported.

Chapter 5. OpenPages installation server and app

Use the IBM OpenPages with Watson installation server to install and upgrade (in-place or migration upgrade). You can also use it to apply fix packs and interim fixes. The installation server includes a web interface, called the installation app. The installation app is installed when you install the OpenPages installation server.

You can set up the installation server on one of the servers in your OpenPages environment or on a separate computer.

For example, you can set up the installation server on the admin application server, and then log in to the installation app from your laptop.

Or, you can set up the installation server on your laptop, and log in to the app from your laptop.

Important: If you use Microsoft Windows servers in your deployment, set up the OpenPages installation server on a Windows computer.

The installation server uses installation agents to install components on remote servers. The installation server pushes the agent software to the remote servers and starts the agents automatically. Or, you can install the agent software manually on remote servers, if you prefer.

Installation on different operating systems

You can use different operating systems in your IBM OpenPages with Watson deployment.

If your deployment includes servers that are running on Microsoft Windows, install the IBM OpenPages with Watson installation server on a Windows computer.

For example, if your deployment uses application servers and reporting servers that are running on Linux and a search server that is running on Windows, install the installation server onto a Windows computer.

If all of the servers in your deployment are running on Linux, you can install the IBM OpenPages with Watson installation server on a Linux or Windows computer.

Supported shells for Linux installations

You can run the installation server on the Bourne shell (`/bin/sh`), Bourne Again Shell, (`/bin/bash`), C-Shell (`/bin/csh`), or Korn Shell (`/bin/ksh`).

Setting up the installation server on Windows

You can set up the installation server on a server in your deployment or on a separate computer. Use a computer that can communicate with the servers in your OpenPages environment.

After you set up the installation server, you can use the OpenPages installation app to create and manage deployments.

Note: If you already set up the installation server and you want to update it with a fix pack, see [“Update the installation server and agents”](#) on page 47.

Before you begin

The computer where you set up the installation server must meet the following requirements:

- IBM SDK, Java Technology Edition or Java Runtime Environment (JRE) is installed.
- Java is included in the PATH system environment variable.

You might also want a PDF reader application on the computer. When you install or upgrade OpenPages, you can download validation reports in PDF format.

Procedure

1. Download the OpenPages 8.2 package from Passport Advantage.
2. Log on to the computer as an administrator.
3. If an earlier version of the installation server is running, stop it.
4. Do one of the following steps:
 - Update the antivirus policy on the installation server computer to allow Node .js.
 - Disable antivirus software on the installation server computer. You can re-enable it after you install the installation server.
5. Create a new directory.

If you have more than one version of the installation server on the same host, use a separate directory for each version.

For example, C:\IBM\OPInstall<version>.
6. Locate the installation files.

The files are stored in \OP_<version>_Main\OP_<version>_Installer.
7. Copy the contents of the \OP_<version>_installer directory to the directory that you created.
8. Change directory to
`<installation_server_home>\OP_<version>_installer\install\Windows.`
9. Open a command prompt as an administrator.
10. Run the installation script.

You can use the following optional arguments:

- `/p:<password>` – Sets the password for the initial installation app user, called admin. If you exclude the argument, the `install.bat` script prompts you for the password.
- `/n:<port>` – Sets the port that the installation server runs on when you start it. If you have multiple installation servers that run on the same hardware, ensure that each installation server uses a different port number. Specify an integer in the range 0 - 65535. If you exclude this argument, the default port number (8443) is used.
- `/m:<old_directory>` – Migrates existing deployments and installation server user accounts to the 8.2 installation server. Use this argument if you have 7.4, 8.0.x, or 8.1.x deployments that you want to use with the new installation server. For `<old_directory>`, enter the full path to the 7.4, 8.0.x, or 8.1.x installation server home directory. Alternatively, you can migrate deployments and users after you install the 8.2 installation server. For more information, see [“Migrating deployments and installation server users” on page 44.](#)
- `/s` – Prevents the installation server from starting after the `install.bat` completes. If you exclude this argument, the installation server starts automatically after the `install.bat` script completes.

Syntax:

```
install.bat -acceptLicense [/p:password] [/m:<old_directory>] [/n:<port>] [/s]
```

11. If you did not use the `/p` parameter, type a password and then press Enter.
12. After the installation completes, re-enable the antivirus software on the installation server.

Do this step if you disabled the antivirus software in step [“4” on page 42.](#)
13. Update the installation server to the latest fix pack version.

See [“Update the installation server and agents” on page 47.](#)

Results

The OpenPages installation server is installed.

If you used the `/s` argument, start the installation server. For more information, see the *IBM OpenPages with Watson Installation and Deployment Guide*.

You can now log in. For the user name, type `admin`. For the password, type the password that you set when you ran the `install.bat` script. For more information, see the *IBM OpenPages with Watson Installation and Deployment Guide*.

Note: If you used the `/m` argument but some deployments or users were not migrated, do not run the `install.bat` script again. Instead, repeat the migration without reinstalling. See [“Migrating deployments and installation server users”](#) on page 44.

Setting up the installation server on Linux

You can set up the installation server on a server in your deployment or on a separate computer. Use a computer that can communicate with the servers in your OpenPages environment.

After you set up the installation server, you can use the OpenPages installation app to create and manage deployments.

Important: If you use Windows servers in your deployment, set up the OpenPages installation server on a Windows computer. See [“Setting up the installation server on Windows”](#) on page 41.

Note: If you already set up the installation server and you want to update it with a fix pack, see [“Update the installation server and agents”](#) on page 47.

Before you begin

The computer where you set up the installation server must meet the following requirements:

- IBM SDK, Java Technology Edition or Java Runtime Environment (JRE) is installed.
- Java is included in the `PATH` system environment variable.
- `JAVA_HOME` is set.

You might also want a PDF reader application on the computer. When you install or upgrade OpenPages, you can download validation reports in PDF format.

About this task

This video demonstrates how to set up the installation server. The steps are similar for 8.2: <https://youtu.be/OiyuKjYyPrg>.

Procedure

1. Log on to the computer as an administrator.
2. If an earlier version of the installation server is running, stop it.
3. Do one of the following steps:
 - Update the antivirus policy on the installation server computer to allow `Node.js`.
 - Disable antivirus software on the installation server computer. You can re-enable it after you install the installation server.
4. Create a directory.

If you have more than one version of the installation server on the same host, use a separate directory for each version.

For example, `/home/opuser/IBM/OPInstall<version>`.
5. Locate the installation files.

The files are stored in `/OP_<version>_Main/OP_<version>_Installer`.
6. Copy the contents of the `OP_<version>_Installer` directory to the directory that you created.
7. Change directory to `/home/opuser/IBM/OPInstall/OP_<version>_Installer/install/Linux`.

8. Grant the +rwx permission to the user on the installation server directory, subdirectories, and scripts.
9. Open a shell and run the setup script.

You can use the following optional arguments:

- `-p <password>` – Sets the password for the initial installation app user, called admin. If you exclude the argument, the `install.bat` script prompts you for the password.
- `-n <port>` – Sets the port that the installation server runs on when you start it. If you have multiple installation servers that run on the same hardware, ensure that each installation server uses a different port number. Specify an integer in the range 0 - 65535. If you exclude this argument, the default port number (8443) is used.
- `-m <old_directory>` – Migrates existing deployments and installation server user accounts to the 8.2 installation server. Use this argument if you have 7.4, 8.0.x, or 8.1.x deployments that you want to use with the new installation server. For `<old_directory>`, enter the full path to the 7.4, 8.0.x or 8.1.x installation server home directory. Alternatively, you can migrate deployments and users after you install the 8.2 installation server. For more information, see [“Migrating deployments and installation server users” on page 44](#).
- `-s` – Prevents the installation server from starting after the `install.sh` script completes. If you exclude this argument, the installation server starts automatically after the `install.sh` script completes.

Syntax:

```
./install.sh --acceptLicense [-p password] [-m <old_directory>] [-n <port>] [-s]
```

10. If you did not use the `-p` parameter, type a password and then press Enter.
11. Close the shell window.
12. After the installation completes, re-enable the antivirus software on the installation server.
Do this step if you disabled the antivirus software in step “3” on page 43.
13. Update the installation server to the latest fix pack version.
See [“Update the installation server and agents” on page 47](#).

Results

The OpenPages installation server is installed.

If you used the `-s` argument, start the installation server. For more information, see the *IBM OpenPages with Watson Installation and Deployment Guide*.

You can now log in. For the user name, type admin. For the password, type the password that you set when you ran the `install.sh` script. For more information, see the *IBM OpenPages with Watson Installation and Deployment Guide*.

Note: If you used the `-m` argument but some deployments or users were not migrated, do not run the `install.sh` script again. Instead, repeat the migration without reinstalling. See [“Migrating deployments and installation server users” on page 44](#).

Migrating deployments and installation server users

You can migrate deployments and user accounts from a 7.4.x, 8.0.x, or 8.1.x installation server to the 8.2 IBM OpenPages with Watson installation server.

About this task

Do this task if the following conditions are met:

- You have a 7.4.x, 8.0.x, or 8.1.x installation server (the source installation server).
- You set up the 8.2 installation server (the target installation server).

- When you set up the 8.2 installation server, you did not migrate deployments and user accounts from the source installation server by using the /m (Microsoft Windows) or -m (Linux) argument.

Or, you migrated, but some deployments or user accounts did not get migrated.

When you migrate, keep the following points in mind:

- Deployments and users that already exist in the 8.2 installation server are not migrated.
- User accounts in the source installation server that are missing passwords are not migrated.
- A deployment is not migrated if any validation, installation, or configuration processes are running.

Procedure

1. If the installation app is open, log out and close the browser window.
2. Stop the 7.4.x, 8.0.x, or 8.1.x installation server.

Windows

- Stop the `ibmopenpagesgrcplatforminstaller<version>.exe` (7.4 or 8.0) or `ibmopenpageswithwatsoninstaller<version>.exe` (8.1) service.
- Or, go to the `<installation_server_home>` directory of the installation server that you want to stop. Open a command prompt as an administrator, and then run the following command:

```
npm run stop
```

Linux

- a. Open a shell and go to the `<installation_server_home>` directory of the installation server that you want to stop, for example `/home/opuser/IBM/OPInstall/OP_<version>_Installer`.
- b. Run the following command:

```
npm run stop
```

3. Log on to the computer where you set up the 8.2 installation server.
4. Migrate deployments and user accounts to the 8.2 installation server.
 - a) Open a shell or command window and go to the `<installation_server_home>` directory, for example `/home/opuser/IBM/OPInstall/OP_<version>_Installer`.
 - b) Run the following command:

Replace `<old_directory>` with the full path to the 7.4.x, 8.0.x, or 8.1.x installation server home directory.

```
npm run migration <old_directory>
```

If a deployment or user account is not migrated, fix any issues, and then run the migration again.

Installing agents manually

The installation server can automatically install the agent software on remote servers. But you can install the agent software manually, if you prefer.

Before you begin

The computer where you install the agent software must meet the following requirements:

- IBM SDK, Java Technology Edition or Java Runtime Environment (JRE) is installed.
- Java is included in the PATH system environment variable.

About this task

When you specify the deployment properties for a remote server, you are asked to provide the user name and password of an administrator account on the remote server. The installation server uses these credentials to install the agent software on the remote server. However, your organization might have policies that restrict the use of administrator credentials. In this case, you can install the agent software manually before you install IBM OpenPages with Watson.

The overall process involves the following steps:

1. Install the agent software manually and start the agent on each remote server, except the database server. The agent software is not needed on the database server.
2. In the installation app, enter the deployment properties for the remote servers.
 - Enable the **Remote Deploy** option.
 - Leave the **Local User Name** and **Local User Password** fields empty.
 - In the **Agent Directory** field, type the full path to the directory on the remote server where you installed the agent software. This directory is the `<agent_home>` directory.

Procedure

1. Log on to the remote server as an administrator.
2. Do one of the following steps:
 - Update the antivirus policy on the remote server to allow `Node.js`.
 - Disable antivirus software on the remote server. You can re-enable it after you install the agent software.
3. Create a directory.
For example:
 - Windows: `C:\IBM\OPAgent`
 - Linux: `/home/opuser/IBM/OPAgent`

This directory will be the `<agent_home>` directory for the remote server.
4. Copy the agent installation software to the remote server.
 - a) Locate the following file on the installation server: `<installation_server_home>/op-installer-agent.zip`.
 - b) Copy `op-installer-agent.zip` to the `<agent_home>` directory that you created on the remote server.
 - c) Extract the `op-installer-agent.zip` file into the `<agent_home>` directory.
5. Open a shell or command window. If you are using Windows, open the command window as an administrator.
6. Go to the `<agent_home>/install/<OS>` directory.
7. Run the following script to install the agent software:
 - Windows:

```
install.bat -acceptLicense [/n <port>] [/s]
```

You can use the following optional arguments:

- `/n:<port>` – Sets the port that the installation agent runs on when you start it. Specify an integer in the range 0 - 65535. If you exclude this argument, the default port number (8443) is used.
- `/s` – Prevents the installation agent from starting after the `install.bat` script completes. If you exclude this argument, the installation agent starts automatically after the `install.bat` script completes.

- Linux:

```
chmod 755 install.sh
./install.sh --acceptLicense [-n <port>] [-s]
```

You can use the following optional arguments:

- `-n <port>` – Sets the port that the installation agent runs on when you start it. Specify an integer in the range 0 - 65535. If you exclude this argument, the default port number (8443) is used.
- `-s` – Prevents the installation agent from starting after the `install.sh` script completes. If you exclude this argument, the installation agent starts automatically after the `install.sh` script completes.

8. When the script completes, close the shell or command window.

9. Start the agent.

See [“Starting the installation agent manually” on page 54](#).

10. Update the agent software to the latest fix pack version.

For more information, see [“Update the installation server and agents” on page 47](#).

11. Repeat these steps on each remote server, except the database server.

What to do next

When you enter the server properties in the installation app or in the `deploy.properties` file, do the following steps:

- Enable the **Remote Deploy** option.
- In the **Agent Directory** field, type the full path to the `<agent_home>` directory on the remote server.
- Leave the **Local User Name** and **Local User Password** fields empty.

Ensure that the agents are started before you do any installation tasks. See [“Starting the installation agent manually” on page 54](#).

Update the installation server and agents

Update the installation server to use the latest 8.2.x version.

The latest version of the installation server is provided in the fix pack installation kit.

Do the following tasks:

- Update the installation server.
- If you installed the agent software manually on remote servers, update the agent software on each remote server.

Updating the installation server

Before you install a new version of IBM OpenPages with Watson (a release, fix pack, or interim fix), update the OpenPages installation server to the latest 8.2.x fix pack version.

About this task

This video demonstrates how to update the installation server: <https://youtu.be/FghmmHO5Ug8>.

Procedure

1. Download the latest OpenPages fix pack from Fix Central.
2. Log on to the OpenPages installation server computer as the user who installed the installation server.

Alternatively, you can log in as any user who has full permissions on the installation server directories and who can run Node.js.

3. Locate the `openpages_installer_<version>.zip` file in the fix pack kit.
The file is stored in `/OP_<version>_Main/OP_<version>_Installer`.
4. Copy the file to the `<Installation_server_home>/src/assets/maintenance` directory on the installation server.
5. Stop the installation server if it is running.
6. Update the installation server.
 - a) Open a command prompt as an administrator or open a shell window.
 - b) Go to the `<Installation_server_home>` directory and run the following command:

```
npm run upgrade
```

7. Start the installation server.
8. Verify the update. Log in to the installation app, open any deployment, and click **About** to see the version number.
9. If you installed the agent software manually on the remote servers in your deployment, update the agent software on each remote server.

For more information, see [“Updating agents manually” on page 48](#).

Note: Do not click **Validate** until you have updated the agent software on each remote server.

If the installation server installed the agent software on your remote servers, you do not need to update the agents manually. The installation server updates the agents automatically when you click **Validate**.

Updating agents manually

Use this procedure to update the agent software manually to an 8.2.0.x fix pack version.

About this task

The installation server can automatically update the agent software on remote servers. But you can update the agent software manually, if you prefer.

When you specify the deployment properties for a remote server, you are asked to provide the user name and password of an administrator account on the remote server. The installation server uses these credentials to update the agent software on the remote server. However, your organization might have policies that restrict the use of administrator credentials. In this case, you can update the agent software manually before you install IBM OpenPages with Watson or apply a fix pack.

The overall process involves the following steps:

1. Update the installation server. See [“Updating the installation server” on page 47](#).
2. Update the agent software manually and start the agent on each remote server, except the database server. The agent software is not needed on the database server.
3. In the installation app, enter the deployment properties for the remote servers.
 - Enable the **Remote Deploy** option.
 - You can leave the **Local User Name** and **Local User Password** fields empty.
 - In the **Agent Directory** field, type the full path to the directory on the remote server where the agent software is installed. This directory is the `<agent_home>` directory.
4. Validate your deployment and continue with the installation of OpenPages or the fix pack.

Procedure

1. Log on to the remote server as the user who installed the agent software.

Alternatively, you can log in as any user who has full permissions on the agent directories and who can run `Node.js`.

2. Stop the agent.

For more information, see [“Stopping the installation agent manually” on page 54](#).

3. Copy the installation file to the remote server.

a) Locate the following file in the 8.2.0.x fix pack kit: `openpages_installer_<version>.zip`
The file is stored in `/OP_<version>_Main/OP_<version>_Installer`.

b) Copy `openpages_installer_<version>.zip` to the `<agent_home>/src/assets/maintenance` directory on the installation server.

Do not extract the file.

4. Update the agent software.

On Windows:

- a) Verify that no command prompts or applications, such as Windows Explorer, are accessing the `<agent_home>` directory or its subdirectories.
- b) Open a command prompt as an administrator.
- c) Go to the `<agent_home>` directory
- d) Run the following command.

```
npm run upgrade
```

On Linux:

- a) Open a shell and go to the `<agent_home>` directory.
- b) Run the following command.

```
npm run upgrade
```

When the process completes, the following message is displayed:

```
Installer upgrade is successful...
```

5. Start the agent.

See [“Starting the installation agent manually” on page 54](#).

6. Repeat these steps on each remote server, except the database server.

What to do next

When you fill in the server properties, do the following:

- Enable the **Remote Deploy** option.
- In the **Agent Directory** field, type the full path to the `<agent_home>` directory on the remote server.
- You can leave the **Local User Name** and **Local User Password** fields empty.

Note: If you leave the **Local User Name** and **Local User Password** fields empty, you must start the agents manually. See [“Starting the installation agent manually” on page 54](#).

Logging in to the installation app

Use the installation app to create a new deployment or to work with an existing deployment.

Before you begin

The installation server must be running.

Procedure

1. Open Google Chrome or Microsoft Edge.

2. Go to `https://<host>:<port_number>`.

- Replace `<host>` with the name of the computer where you set up the installation server.
- Replace `<port_number>` with the port number of the installation server. The default port number is 8443.

For example, `https://appserver1.mycompany.com:8443`

If you are running the installation server on your local computer, go to `https://localhost:8443`

3. Enter your credentials.
4. Review and accept the terms and conditions.
5. Click **Login**.

Adding users

You can set up additional user accounts to access the IBM OpenPages with Watson installation app.

About this task

You add users by editing the `<install_server_home>/src/db/jsonDB.json` file.

Create a backup of the `jsonDB.json` file before you begin.

When you save the file and restart the installation server, the passwords in the file are encrypted.

This video demonstrates how to add users and update user passwords:

<https://youtu.be/OQXqUcCf1RE>

Procedure

1. Log out of the IBM OpenPages with Watson installation app.
2. Stop the installation server.
For more information, see [“Stopping the installation server” on page 53](#).
3. Open the `<install_server_home>/src/db/jsonDB.json` file in a text editor.
4. Use the following code as a guide to help you to add user accounts.

```
{
  "token": [],
  "user": [
    {
      "name": "admin",
      "password": "{AES}QiTCrj1RuBgvLvKHm32JoQ==",
      "id": "101",
      "encrypted": true
    },
    {
      "name": "<new_user>",
      "password": "<new_user_password>",
      "id": "102"
    },
    {
      "name": "<new_user>",
      "password": "<new_user_password>",
      "id": "103"
    }
  ]
}
```

Note the following requirements:

- Each user name must be unique.
- Each user account must have a unique ID.

The last block (with ID 103 in this example) does not end with a comma.

5. Save the file and close it.

6. Start the installation server.

Windows

Do one of the following steps:

- Start the `ibmopenpageswithwatsoninstaller<version>.exe` service.
- Go to the `<installation_server_home>` directory. For example `C:\IBM\OPInstall\OP_<version>_Installer`. Right-click the `startup.bat` file and click **Run As Administrator**.

Note: If you do not see the `startup.bat` script, you can also find it and run it from the `<installation_server_home>\install\Windows` directory.

Linux

- a. Open a shell and go to the `<installation_server_home>` directory, for example `/home/opuser/IBM/OPInstall/OP_<version>_Installer`.
- b. Run the following command:

```
./startup.sh
```

Note: If you do not see the `startup.sh` script, you can also find it and run it from the `<installation_server_home>/install/Linux` directory.

Results

The user accounts are added and the passwords in the `jsonDB.json` file are encrypted.

Changing passwords

You can change the passwords of the installation app user accounts.

About this task

You change passwords by editing the `<install_server_home>/src/db/jsonDB.json` file.

Create a backup of the `jsonDB.json` file before you begin.

When you save the file and restart the installation server, the passwords in the file are encrypted.

Procedure

1. Log out of the IBM OpenPages with Watson installation app.
2. Stop the installation server.
For more information, see [“Stopping the installation server” on page 53](#).
3. Open the `<install_server_home>/src/db/jsonDB.json` file in a text editor.
4. Locate the user whose password you want to change, for example `admin2`.

```
{
  "token": [],
  "user": [
    {
      "name": "admin",
      "password": "{AES}QiTCrj1RuBgVlvKHm32JoQ==",
      "id": "101",
      "encrypted": true
    },
    {
      "name": "admin2",
      "password": "{AES}QiTCrj1RuBgVlvKHm32JoQ==",
      "id": "102",
      "encrypted": true
    },
    {
      "name": "admin3",
      "password": "{AES}IAHJQUu_MiqdcX2LtugZcA==",

```

```

        "id": "103",
        "encrypted": true
      }
    ]
  }
}

```

5. Delete the encrypted password and then type a new password.
6. Delete the comma after the id value.
7. Delete the "encrypted": true line.

The result is:

```

{
  "token": [],
  "user": [
    {
      "name": "admin",
      "password": "{AES}QiTCrj1RuBgVLvKHm32JoQ==",
      "id": "101",
      "encrypted": true
    },
    {
      "name": "admin2",
      "password": "<new_password>",
      "id": "102"
    },
    {
      "name": "admin3",
      "password": "{AES}IAHJQUu_MiqdcX2LtugZcA==",
      "id": "103",
      "encrypted": true
    }
  ]
}

```

8. Save the file and close it.
9. Start the installation server.

Windows

Do one of the following steps:

- Start the `ibmopenpageswithwatsoninstaller<version>.exe` service.
- Go to the `<installation_server_home>` directory. For example `C:\IBM\OPInstall\OP_<version>_Installer`. Right-click the `startup.bat` file and click **Run As Administrator**.

Note: If you do not see the `startup.bat` script, you can also find it and run it from the `<installation_server_home>\install\Windows` directory.

Linux

- a. Open a shell and go to the `<installation_server_home>` directory, for example `/home/opuser/IBM/OPInstall/OP_<version>_Installer`.
- b. Run the following command:

```
./startup.sh
```

Note: If you do not see the `startup.sh` script, you can also find it and run it from the `<installation_server_home>/install/Linux` directory.

Results

The passwords are changed and they are encrypted in the `jsonDB.json` file.

Starting the installation server

If you stop the IBM OpenPages with Watson installation server you can restart it.

Procedure

1. Log on to the computer where you set up the installation server.
2. Start the installation server.

Windows

Do one of the following steps:

- Start the `ibmopenpageswithwatsoninstaller<version>.exe` service.
- Go to the `<installation_server_home>` directory. For example `C:\IBM\OPInstall\OP_<version>_Installer`. Right-click the `startup.bat` file and click **Run As Administrator**.

Note: If you do not see the `startup.bat` script, you can also find it and run it from the `<installation_server_home>\install\Windows` directory.

Linux

- a. Open a shell and go to the `<installation_server_home>` directory, for example `/home/opuser/IBM/OPInstall/OP_<version>_Installer`.
- b. Run the following command:

```
./startup.sh
```

Note: If you do not see the `startup.sh` script, you can also find it and run it from the `<installation_server_home>/install/Linux` directory.

Results

The installation server is running. You can now log in to the installation app. See [“Logging in to the installation app”](#) on page 49.

Stopping the installation server

You can stop the IBM OpenPages with Watson installation server.

Procedure

1. Log on to the computer where you set up the installation server.
2. Stop the installation server.

On Windows:

- Stop the `ibmopenpageswithwatsoninstaller<version>.exe` service.
- Or, go to the `<installation_server_home>` directory of the installation server that you want to stop. Open a command prompt as an administrator, and then run the following command:

```
npm run stop
```

On Linux:

- a. Open a shell and go to the `<installation_server_home>` directory of the installation server that you want to stop, for example `/home/opuser/IBM/OPInstall/OP_<version>_Installer`.
- b. Run the following command:

```
npm run stop
```

Results

The installation server is stopped. To restart it, see [“Starting the installation server” on page 53](#).

Starting the installation agent manually

You can start the agent on a remote server manually.

About this task

When you specify the deployment properties for a remote server, you are asked to provide the user name and password of an administrator account on the remote server. The installation server uses these credentials to start and stop the agent software on the remote server. If you do not specify login credentials in the deployment properties and you install the agent software manually, you need to start and stop the agent manually. You cannot use the installation app to start or stop the agent.

You might also choose to start and stop agents manually if you prefer to use the command line.

Procedure

1. Log on to the remote server as the user who installed the agent software.

Alternatively, you can log in as any user who has full permissions on the agent directories and who can run `Node.js`.

2. Start the installation agent.

Windows

Do one of the following steps:

- Start the `ibmopenpageswithwatsoninstaller<version>.exe` service.
- Go to the `<agent_home>\install\Windows` directory. Right-click the `startup.bat` file and click **Run As Administrator**.

Linux

- a. Open a shell and go to the `<agent_home>/install/Linux` directory.
- b. Run the following command:

```
./startup.sh
```

Results

The installation agent is running.

Stopping the installation agent manually

You can stop the agent on a remote server manually.

About this task

When you specify the deployment properties for a remote server, you are asked to provide the user name and password of an administrator account on the remote server. The installation server uses these credentials to start and stop the agent software on the remote server. If you do not specify login credentials in the deployment properties and you install the agent software manually, you need to start and stop the agent manually. You cannot use the installation app to start or stop the agent.

You might also choose to start and stop agents manually if you prefer to use the command line.

Procedure

1. Log on to the remote server as the user who installed the agent software.

Alternatively, you can log in as any user who has full permissions on the agent directories and who can run `Node.js`.

2. Stop the installation agent.

- Windows: Stop the `ibmopenpageswithwatsoninstaller<version>.exe` service. Or, open a command prompt as an administrator, go to the `<agent_home>` directory, and run the following command:

```
npm run stop
```

- Linux: Go to the `<agent_home>` directory and run the following command:

```
npm run stop
```

Results

The installation agent is stopped.

Changing the port number of the installation server

You can change the port number of the IBM OpenPages with Watson installation server. This task is optional.

Procedure

1. Log on to the computer where you set up the installation server.
2. If the installation server is running, stop it.

On Windows:

- Stop the `ibmopenpageswithwatsoninstaller<version>.exe` service.
- Or, go to the `<installation_server_home>` directory of the installation server that you want to stop. Open a command prompt as an administrator, and then run the following command:

```
npm run stop
```

On Linux:

- a. Open a shell and go to the `<installation_server_home>` directory of the installation server that you want to stop, for example `/home/opuser/IBM/OPInstall/OP_<version>_Installer`.
- b. Run the following command:

```
npm run stop
```

3. Create a `.env` file to set the port number.

- a) Create a new file and add the following line:

```
INSTALLER_PORT=<port_number>
```

Example:

```
INSTALLER_PORT=9091
```

- b) Save the file in the `<installation_server_home>` directory. Name the file `.env`.

Example: `C:\IBM\OPInstall\OP_<version>_Installer\.env`

4. Start the installation server.

Windows

Do one of the following steps:

- Start the `ibmopenpageswithwatsoninstaller<version>.exe` service.
- Go to the `<installation_server_home>` directory. For example `C:\IBM\OPInstall\OP_<version>_Installer`. Right-click the `startup.bat` file and click **Run As Administrator**.

Note: If you do not see the `startup.bat` script, you can also find it and run it from the `<installation_server_home>\install\Windows` directory.

Linux

- a. Open a shell and go to the `<installation_server_home>` directory, for example `/home/opuser/IBM/OPInstall/OP_<version>_Installer`.
- b. Run the following command:

```
./startup.sh
```

Note: If you do not see the `startup.sh` script, you can also find it and run it from the `<installation_server_home>/install/Linux` directory.

Results

The port number of the installation server is updated. Use the new port number when you log into the installation app: `https://<host>:<port_number>`.

Chapter 6. Install IBM OpenPages with Watson

You can use the installation app to install IBM OpenPages with Watson.

For videos about how to install OpenPages, see the [IBM OpenPages playlist](#) on YouTube.

Installation process overview

Installing OpenPages with Watson requires the following steps.

- Install the OpenPages installation server. See [“Setting up the installation server on Windows”](#) on page 41 or [“Setting up the installation server on Linux”](#) on page 43.
- Update the OpenPages installation server to the latest interim fix or fix pack version. See [“Update the installation server and agents”](#) on page 47.
- Set up the servers that you want to use in your deployment and install the prerequisite software. See [“Preparing your system for installation”](#) on page 58.
- Decide how you want to create the database. You can use the OpenPages installation app to install the database or you can use scripts to do some or all of the database installation steps. If you are using IBM Db2, see [“OpenPages database object creation for Db2”](#) on page 126. If you are using Oracle, see [“OpenPages database schema creation for Oracle”](#) on page 132.
- Install OpenPages. You can use the installation app or you can do a silent installation.

The following tasks are required:

- [“Configuring the database server \(Db2\)”](#) on page 144 or [“Configuring the database server \(Oracle\)”](#) on page 146
- [“Configuring application servers”](#) on page 149
- [“Configuring reporting servers”](#) on page 150

The following task is optional: [“Configuring a search server”](#) on page 152

- Do the post-installation tasks. See [“Post installation tasks”](#) on page 153.

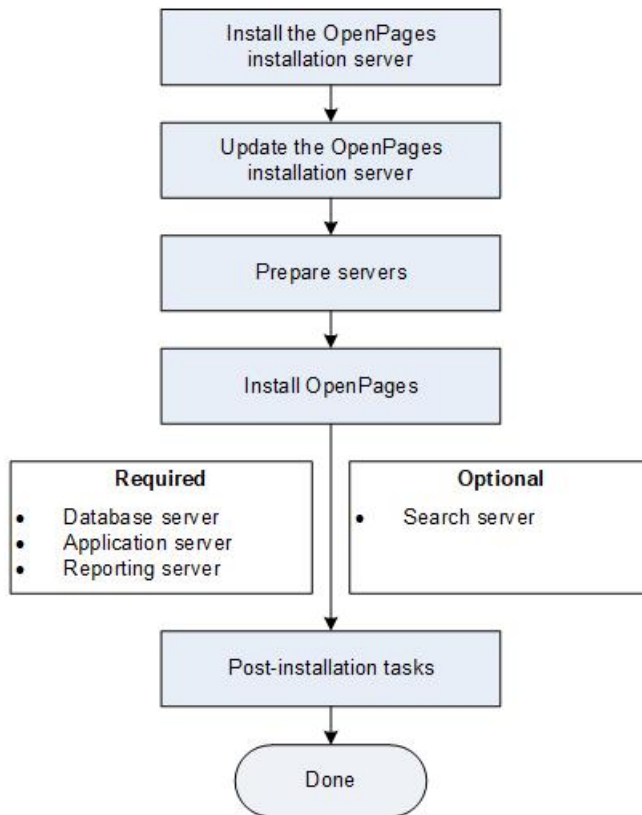


Figure 9. Installation process overview

Preparing your system for installation

Before you install IBM OpenPages with Watson, prepare the servers that you are going to use in your deployment.

Each deployment needs a database server, one or more application servers, and one or more reporting servers. You can also include a search server in your deployment.

Checklist if you are using existing hardware

Do the following steps if you are installing OpenPages on existing hardware where you have an older version of OpenPages installed.

1. Stop all servers (OpenPages application servers, Cognos reporting servers, and global search).
2. Back up the existing OpenPages environment. For more information, see [“Backing up your source environment”](#) on page 198.
3. Use new directory paths for the new installation.
4. If you are using Microsoft Windows:
 - For Cognos Analytics to start, ensure that `<JAVA_HOME>` is set to the location of IBM Java 8 before you start the reporting servers.
 - If Cognos fails to start and the error, `Bad Major Version`, is issued, Cognos did not pick up the change to `<JAVA_HOME>`.

You must set the IBM Java location in the `<JAVA_HOME>` variable in the `<COGNOS_HOME>/bin64/bootstrap_wlp_<OS>.xml` file.

For example, if you want Cognos Analytics to use the IBM SDK, Java Technology Edition that is used by WebSphere, use:

```
<param>-java_home=C:\IBM\java_8.0_64</param>
```

This known issue can occur only on a Windows server where OpenPages and Cognos reside on the same server.

Note: If IBM WebSphere Application Server Network Deployment is installed, you do not need to uninstall it or upgrade it. OpenPages 8.2 includes IBM WebSphere Liberty.

Checklist for Windows servers

Do the following tasks on each Microsoft Windows server before you install IBM OpenPages with Watson:

- Make sure that the clocks are synchronized across the application servers, database server, reporting servers, and the search server.
- Enable Data Execution Prevention (DEP). See [“Enabling Data Execution Prevention for essential Windows programs and services”](#) on page 59.

Do the following additional tasks on all servers except the database server:

- Create the OpenPages installation user and add the user to the power users or admin group. See [“Users and groups for installations on Windows”](#) on page 59.

Do the following steps on all application servers and the search server:

- Install IBM SDK, Java Technology Edition. See [“Getting a copy of the IBM SDK \(Windows\)”](#) on page 60.

Enabling Data Execution Prevention for essential Windows programs and services

By default, Windows Server uses settings that are designed to prevent an application from running unauthorized programs. These settings can interfere with the IBM OpenPages with Watson installation. Configure Data Execution Prevention (DEP) before you start the installation process to prevent any issues.

Procedure

1. Log on to the server.
2. Open the **Control Panel**.
3. Click **System and Security > System > Advanced System Settings**.
4. On the **Advanced** tab, next to the **Performance** heading, click **Settings**.
5. Click the **Data Execution Prevention** tab.
6. Select **Turn on DEP for essential Windows programs and services only**.
7. Click **OK** and then restart your system to enable the change.
8. Repeat these steps for each Windows server in your deployment.

What to do next

When the installation of all software is complete, you can disable the setting.

Users and groups for installations on Windows

To install and configure IBM OpenPages with Watson on a Windows operating system, you must set up an OpenPages installation user that is a member of the power user or administrator group.

In this guide, the OpenPages installation user is called `opuser`.

Important: The password for this user cannot contain spaces or special characters.

Getting a copy of the IBM SDK (Windows)

Before you install OpenPages, install IBM SDK, Java Technology Edition and set up the system environment variables for Java on each application server and the search server. You can also use the steps to install the IBM SDK on the installation server.

About this task

For application servers, the version of the IBM SDK must be the same on each of the servers.

Procedure

1. Locate the IBM SDK on the IBM OpenPages with Watson installation media.

The path is \OP_<version>_Main\IBM_Java\WIN64\java_8.0_64

2. Copy the IBM SDK to the local hard disk of the server.

You can copy the IBM SDK to any directory on the server.

For example, copy the IBM SDK to the root of the C drive under C:\IBM.

3. Set the system environment variables for Java.
 - a) In the Windows search box, type environment variables, and then click **Edit system environment variables**.
 - b) On the **Advanced** tab, click **Environment variables**.
 - c) In the **System Variables** pane, click **New**.
 - d) Type JAVA_HOME in the **Variable name** field.
 - e) Type C:\IBM\java_8.0_64 in the **Variable value** field.
 - f) Click **OK**.
 - g) Under System variables, select the **Path** variable, and then click **Edit**.
 - h) Type %JAVA_HOME%\bin; at the beginning of the list of paths in the **Variable value** field.
 - i) Click **OK**.

Note: Start a new command prompt to see the changes to the environment variables.

4. Verify the version of Java that is on the server.

Run the `java -version` command. The result should be similar to the following sample:

```
java version "1.8.0_241"
Java(TM) SE Runtime Environment (build 8.0.6.5 - pwa6480sr6fp5-20200111_02(SR6 FP5))
IBM J9 VM (build 2.9, JRE 1.8.0 Windows Server 2016 amd64-64-Bit Compressed References
20200108_436782 (JIT enabled, AOT enabled)
OpenJ9 - 7d1059c
OMR - d059105
IBM - c8aee39)
JCL - 20200110_01 based on Oracle jdk8u241-b07
```

If the location of Java changes later, you can update it. For more information, see the following technotes:

- [How to Change the Java Location on an OpenPages Application Server](#)
- [How to Change the Java Location on an OpenPages Global Search Server](#)

Tip: You can also change the location of Java on the reporting server. See [How to Change the Java Location on an OpenPages Reporting Server](#).

Checklist for Linux servers

Do the following tasks on each Linux server before you install IBM OpenPages with Watson:

- Make sure that the clocks are synchronized across the application servers, database server, reporting servers, and the search server.

- Set the file descriptor limit for OpenPages users. For more information, see [“Setting the file descriptor limit for OpenPages with Watson users on Linux”](#) on page 61.

Do the following additional tasks on all application servers (admin and non-admin) and reporting servers (active and standby), and the search server:

- Check the operating system limits that are set on the server. See [“Check operating system limits on Linux”](#) on page 62.

Do the following additional task on all application servers (admin and non-admin) and the search server:

- Create the users and groups for installing OpenPages. See [“Creating the OpenPages installation user \(Linux\)”](#) on page 62
- Create the OpenPages installation directory and give the OpenPages installation user access. See [“Creating the installation directories for Linux”](#) on page 63.
- Install IBM SDK, Java Technology Edition. See [“Getting a copy of the IBM SDK \(Linux\)”](#) on page 63.

Setting the file descriptor limit for OpenPages with Watson users on Linux

You must set the soft and hard limits for the file descriptor and update system files to allocate sufficient resources to the IBM OpenPages with Watson users. You must complete this task on all Linux operating system servers in your environment.

Procedure

1. Log on to the application server as the root user.
2. Verify that the `/etc/pam.d/system-auth` file contains the correct settings by typing the following commands:

```
cat /etc/pam.d/system-auth | grep session | grep pam_unix.so
```

The system response: `session required pam_unix.so`

```
cat /etc/pam.d/system-auth | grep session | grep pam_limits.so
```

The system response: `session required pam_limits.so`

Both commands must return a session line.

3. To determine the current value of the `fs.file-max` property that is set in the `/etc/sysctl.conf` file, type the following command:

```
cat /etc/sysctl.conf | grep fs.file-max
```

- If the `fs.file-max` setting does not exist, add it to the `/etc/sysctl.conf` file by typing the following commands:

```
echo "# Added to increase system open files" >> /etc/sysctl.conf
echo "fs.file-max=500000" >> /etc/sysctl.conf
```

- If the `fs.file-max` setting exists, but it is set to less than 500000, change the `fs.file-max` setting to 500000.

4. Change the file descriptor limits in the `/etc/security/limits.conf` file by adding the following text to the end of the file before the `#End of file` text.

```
* soft nfile 100000
* hard nfile 200000
* soft stack 10240
```

5. To determine the startup limits for the number of processors, type the following command:

```
ls /etc/security/limits.d/90-nproc.conf
```

- If this `90-nproc.conf` file exists, then modify the number of processes to 4096.

- If the file does not exist, add the following lines to the end of the `/etc/security/limits.conf` file:

```
* soft nproc      4096
* hard nproc      5120
```

The soft limit provides a specific limit that can be exceeded, for a short period, up to the system hard limit.

6. Restart the system and then verify the settings that you changed by typing the following command:

```
ulimit -a
```

Check operating system limits on Linux

If your application server, reporting server, or search server is running Red Hat Enterprise Linux, check the operating system limits that are configured on the server.

You can run the `ulimit -a` command to check the limits. Update the limits, if needed, to use the following minimum values:

```
core file size          (blocks, -c) 10485760
data seg size           (kbytes, -d) unlimited
scheduling priority     (-e) 0
file size               (blocks, -f) unlimited
pending signals         (-i) 63407
max locked memory       (kbytes, -l) 65536
max memory size         (kbytes, -m) unlimited
open files              (-n) 100000
pipe size               (512 bytes, -p) 8
POSIX message queues    (bytes, -q) 819200
real-time priority      (-r) 0
stack size              (kbytes, -s) 10240
cpu time                (seconds, -t) unlimited
max user processes      (-u) 127457
virtual memory          (kbytes, -v) unlimited
file locks              (-x) unlimited
```

If you change any values, restart the server.

Creating the OpenPages installation user (Linux)

To install IBM OpenPages with Watson on a Linux operating system, you must create an installation user for OpenPages.

The installation user must have read, write, and execute permissions (775) on the installation files and directories.

For local installations, the OpenPages installation user is the user who runs the OpenPages installation program.

For remote installations, the OpenPages installation user is the user who connects to the remote server.

Before you begin

If you are using an IBM Db2 database, you need to set up additional users and groups. For more information, see [Creating group and user IDs for a Db2 database installation \(Linux and UNIX\)](#) in the IBM Db2 documentation.

Procedure

1. Log on to the application server as `root` and open a shell.
2. To create a group, such as `opgroup`, run the following command:

```
groupadd opgroup
```

3. Create a user, such as `opuser`, and add the user to `opgroup` by running the following command:


```
useradd -m opgroup opuser
```

4. Change the password for the OpenPages installation user by using the following command:

```
passwd opuser
```

5. Grant read, write, and execute permissions to the home directory of the OpenPages installation user.

```
chmod 755 /home/opuser
```

Creating the installation directories for Linux

You must create the installation directories for IBM OpenPages with Watson and change the ownership of these directories to the OpenPages installation user. Do this task if you are installing OpenPages with Watson on a Linux operating system.

Procedure

1. Log on to the application server computer as the root user.
2. If the installation directory for OpenPages does not exist, create it by typing the following command.

Restriction: Ensure that the directory to which you install OpenPages contains only ASCII characters in the path name.

```
mkdir -p <directory>
```

Example:

```
mkdir -p /OpenPages
```

3. Change the ownership of the directory to the OpenPages installation user.

```
chown -R opuser /OpenPages
```

Getting a copy of the IBM SDK (Linux)

Before you install OpenPages, install IBM SDK, Java Technology Edition and set up the system environment variables for Java on each application server and the search server. You can also use the steps to install the IBM SDK on the installation server.

About this task

For application servers, the version of the IBM SDK must be the same on each of the servers.

Procedure

1. Locate the IBM SDK on the IBM OpenPages with Watson installation media.

The path is /OP_<version>_Main/IBM_Java/Linux64/java_8.0_64.

2. Copy the IBM SDK to the local hard disk of the server.

You can copy the IBM SDK to any directory on the server.

For example, copy the IBM SDK to /opt/IBM/.

3. Grant read, write, and execute permissions on Java to the OpenPages installation user (opuser).

Run the following command:

```
chmod -R +x /opt/IBM/java_8.0_64
```

4. Set the system environment variables for Java.

- a) Based on the shell that you are using and the account under which the server will run, edit the .profile or .bashrc file.

- b) Ensure that JAVA_HOME is set to /opt/IBM/java_8.0_64.
- c) Ensure that PATH includes \$JAVA_HOME/bin as the first item.

Note: Start a new shell window to see the changes to the environment variables.

5. Verify the version of Java that is on the server.

Run the `java -version` command. The result should be similar to the following sample:

```
java version "1.8.0_241"
Java(TM) SE Runtime Environment (build 8.0.6.5 - pxa6480sr6fp5-20200111_02(SR6 FP5))
IBM J9 VM (build 2.9, JRE 1.8.0 Linux amd64-64-Bit Compressed References 20200108_436782
(JIT enabled, AOT enabled)
OpenJ9      - 7d1059c
OMR         - d059105
IBM         - c8aee39)
JCL - 20200110_01 based on Oracle jdk8u241-b07
```

If the location of Java changes later, you can update it. For more information, see the following technotes:

- [How to Change the Java Location on an OpenPages Application Server](#)
- [How to Change the Java Location on an OpenPages Global Search Server](#)

Tip: You can also change the location of Java on the reporting server. See [How to Change the Java Location on an OpenPages Reporting Server](#).

Checklist for application servers

Do these tasks on each application server before you install IBM OpenPages with Watson:

- Check that all of the required ports are available. See [“Port assignments ” on page 124](#).
- Install IBM SDK, Java Technology Edition and set the environment variables for Java. See [“Getting a copy of the IBM SDK \(Linux\)” on page 63](#) or [“Getting a copy of the IBM SDK \(Windows\)” on page 60](#).
- Set the DB2_HOME or ORACLE_HOME environment variable.
- If you are using a horizontal cluster for the application servers, do the following tasks:
 - Set up the load balancer.
 - If you are using Microsoft Windows application servers, configure a domain account. See [“Configuring OpenPages applications to use a domain account on Windows operating systems” on page 159](#).
 - If you are using Linux application servers, configure file permissions. See [“Configuring file share permissions on Linux operating systems” on page 159](#).
- If you plan to use IBM HTTP Server, OpenPages Loss Event Entry, or IBM OpenPages SDI Connector for UCF Common Controls Hub, install IBM Installation Manager. See [“Installing IBM Installation Manager” on page 65](#).
- If the database server is on a separate computer:
 - If you are using IBM Db2, see [“Db2 database client installations” on page 85](#).
 - If you are using Oracle, see [“Oracle database client installations” on page 99](#).

Do these additional tasks on the admin application server. (In the installation app, the default name of the admin application server is **AppServer1**. In the `deploy.properties` file, the admin application server is configured in the `[app.server1]` section.):

- Configure the hosts file. See [“Configuring the hosts file” on page 64](#).

Configuring the hosts file

You must ensure that the computer that you use to deploy IBM OpenPages with Watson can connect to each computer on which you install the database server, application servers, reporting servers, and search server. You must also ensure that each server in your deployment can successfully ping and perform a trace route to and from each of the other servers.

Procedure

1. Log on to the admin application server as the admin user.
2. Edit the hosts file:
 - For Linux, go to the /etc directory and open the hosts file in a text editor.
 - For Windows, open the C:\Windows\System32\drivers\etc\hosts file.
3. Add the IP address and name of each OpenPages application server, reporting server, search server, and database server.
4. Save and close the hosts file.
5. Repeat these steps for each OpenPages application server, reporting server, search server, and database server.

Installing IBM Installation Manager

This task is optional. Do this task if you plan to install IBM HTTP Server, IBM OpenPages SDI Connector for UCF Common Controls Hub, or IBM OpenPages Loss Event Entry.

Install IBM Installation Manager on each application server and reporting server.

Ensure that you install the 64-bit version of IBM Installation Manager.

If an older version of IBM Installation Manager is installed, install to a new directory. For more information about this requirement, see [Update to Installation Manager 1.8 is blocked when its data location is within its install location](#).

For more information about IBM Installation Manager, see the [Installation Manager documentation](#).

Procedure

1. Download IBM Installation Manager from [Passport Advantage](#)[®].
2. Run the installation program.
 - Microsoft Windows: Double-click `install.exe`.
 - Linux: Open a terminal window, and then run `./install`.
3. Follow the steps to install IBM Installation Manager.

Checklist for the database server (Db2)

If you use an IBM Db2 database server, do these tasks before you install IBM OpenPages with Watson:

- Check that all of the required ports are available. See [“Port assignments” on page 124](#).
- Install IBM Db2. Include the Db2 Text Search component. See [“IBM Db2 database server installations” on page 66](#).
- Copy the encryption function for OpenPages to the database server. See [“Copying the encryption function for OpenPages to the Db2 server” on page 67](#).
- Set up operating system users and groups (instance owner, DAS user, OP installation user. See [“Operating system user accounts for IBM Db2 databases” on page 83](#).
- Set up the schema owners (the OpenPages database user and the Cognos content store user) See [“Database schema owners” on page 84](#).
- Check that the database user passwords have not expired.
- Prepare a database instance for OpenPages. See [“Preparing the database instances for OpenPages on Db2” on page 81](#).
- Create the OpenPages database. See [“Creating the OpenPages database on IBM Db2” on page 78](#).
- You must create a separate database for Cognos Analytics.

If the database server is on a separate computer, install the database client software on each application server and reporting server. For more information, see [“Db2 database client installations”](#) on page 85.

IBM Db2 database server and client setup for OpenPages with Watson

Before you install OpenPages with Watson, you must complete these tasks if you are installing IBM Db2:

- Install and configure IBM Db2 on the database server.
- Prepare a Db2 database instance for the OpenPages database.
- Create the OpenPages database.
- Install the Db2 database client software on each OpenPages application server and reporting server.
- Verify the connection between the database server and the application and reporting servers.
- Create the OpenPages database objects.

This step is optional. You can use scripts to create some or all of the database objects. Or, you can use the OpenPages installation program to create them.

Restriction: You must use two separate databases - one for the Cognos Analytics content store and one for the IBM OpenPages with Watson database.

IBM Db2 database server installations

You can use an IBM Db2 database for the IBM OpenPages with Watson repository.

Check the specific requirements for your system before you install IBM Db2 products.

For more information about IBM OpenPages with Watson supported software, see [“Software prerequisites”](#) on page 33.

For more information about Db2 system requirements, see the [Db2 for Linux, UNIX, and Windows system requirements](#) web page.

To use Db2 for the OpenPages database, complete the following tasks:

- Install the Db2 database server using a custom installation to include the Db2 Text Search component.

The database server that hosts the OpenPages database must have the required server software installed. Db2 must be installed before you install any required fix packs.

For more information about database server versions, see [“Prerequisite software for the database server”](#) on page 34.

For more information about the Db2 Text Search component, see [“The Db2 Text Search component”](#) on page 67.

Restriction: IBM OpenPages with Watson does not support installation of Db2 software in directories that contain spaces. To use Db2 software that is installed in a directory with spaces, you can enter the short file name convention in the OpenPages installation app. For example, for C:\Program Files\IBM\DB2\SQLLIB, use C:\PROGRA~1\IBM\DB2\SQLLIB.

- Set up the required users and groups. See [“Operating system user accounts for IBM Db2 databases”](#) on page 83.
- Prepare the database instance. See [“Preparing the database instances for OpenPages on Db2”](#) on page 81.
- Create the database. See [“Creating the OpenPages database on IBM Db2”](#) on page 78.

Note: For information about how to upgrade Db2, see [“Upgrading Db2 \(Windows\)”](#) on page 67 or [“Upgrading Db2 \(Linux\)”](#) on page 70.

The Db2 Text Search component

The IBM Db2 Text Search component is required by the IBM OpenPages with Watson installation. When you install the IBM Db2 database server, select the custom installation type and the IBM Db2 Text Search component.

For more information, see [Installing Db2 Accessories Suite for Db2 Text Search](#) in the Db2 documentation.

If the Db2 database server is already installed on the database server computer, use the Db2 setup program to add the Db2 Text Search function to your existing Db2 installation.

To determine whether the Db2 Text Search component is installed, run the **db2ts** command to start or stop the component. If the command fails, the component is not installed. For more information about running the command, see the [Db2 search commands](#) in the Db2 documentation.

Copying the encryption function for OpenPages to the Db2 server

If you are doing a fresh installation or a migration upgrade and using a new computer for the database server, you must manually copy the encryption function for IBM OpenPages with Watson to the IBM Db2 server.

Procedure

1. Go to the `/OP_<version>_Main/OP_<version>_Configuration/Database/DB2/INSTALL_SCRIPTS/bin/<PLATFORM>` directory.
2. Copy the files to the following directories:
 - `<DB2_HOME>/FUNCTION`
 - `<DB2_HOME>/FUNCTION/unfenced`

Upgrade Db2

If you are using IBM Db2, upgrade to a supported version. Version 11.1.4.4 is the minimum supported version for IBM OpenPages with Watson 8.2.

If you are using Db2 11.1.x, apply fix pack 11.1.4.4 or later. For more information, see [Applying fix packs in Db2 database environments](#). You can apply a Db2 11.1.x fix pack before or after you install OpenPages, migrate, or upgrade to 8.2.

You can also upgrade to Db2 11.5. For more information, see [“Upgrading Db2 \(Linux\)”](#) on page 70 or [“Upgrading Db2 \(Windows\)”](#) on page 67.

Important: Fix pack 8.2.0.1 supports Db2 11.5.4. If you are migrating or upgrading to 8.2, complete the migration or upgrade before you apply the Db2 11.5.4 fix pack. Otherwise, you will see errors during the OpenPages database upgrade.

Upgrading Db2 (Windows)

You must upgrade to a supported version of IBM Db2 before you migrate or upgrade to IBM OpenPages with Watson 8.2.

This task provides the basic steps for upgrading IBM Db2. For more information about this process, see the [IBM Db2 documentation](#).

About this task

Important: Fix pack 8.2.0.1 supports Db2 11.5.4. If you are migrating or upgrading to 8.2, complete the migration or upgrade before you apply the Db2 11.5.4 fix pack. Otherwise, you will see errors during the OpenPages database upgrade.

This task uses the following conventions:

- `db2admin`: The OpenPages database instance owner
- `openpage`: The OpenPages database user

- opx: The name of the OpenPages database
- db2inst2: The Cognos database instance owner
- cognosdb: The name of the Cognos content store
- <db_server>: The hostname of the Db2 database server

The steps that you need to do depend on whether you are using your existing database server for OpenPages or using a new database server. If you are using a new database server, you skip the steps about upgrading the database instances and upgrading the databases. Later in the OpenPages migration process, you restore the databases and then upgrade them to the new Db2 version.

Note: When you run Db2 utilities, such as `db2 connect` or `db2rbind`, do not use quotation marks around passwords.

Procedure

1. Stop the following servers:

- Stop all OpenPages application servers.
- Stop the global search services.
- Stop all IBM Cognos services.

2. Check that your system meets the installation prerequisites.

For more information, see [db2prereqcheck - Check installation prerequisites](#).

- a) Go to the directory where you extracted the Db2 installation package.
- b) As the root or sudo user, check the installation requirements.

```
db2prereqcheck -i -v <version>
```

Where <version> is the Db2 version that you want to install.

For example:

```
db2prereqcheck -i -v 11.5.0.0
```

If successful, you see the message DBT3533I The db2prereqcheck utility has confirmed that all installation prerequisites were met.

- c) Review the log file.
- d) As the OpenPages instance owner (for example, db2admin), run the pre-upgrade checks:

```
db2ckupgrade OPX -l c:\tmp\db2ckupgrade.log -u db2admin -p password
```

3. Complete the Db2 pre-upgrade tasks for both the OpenPages database and the Cognos content store. For more information, see [Pre-upgrade tasks for Db2 servers](#).

If you get warnings about the discontinued SYSFUN.ASCII1 function, you can ignore them.

4. Check the value of the application heap size for the Cognos database.

- a) Open the Db2 command line processor (CLP).
- b) Run the following command as the database instance owner. Replace <cognosdb> with the name of your Cognos database.

```
db2 get db cfg for <cognosdb> | findstr APPLHEAPSZ
```

- c) If the value is less than 4096, increase it to a minimum of 4096.

Run the following command as the database instance owner. Replace <cognosdb> with the name of your Cognos database.

```
db2 update db cfg for <cognosdb> using applheapsz 4096
```

5. Drop the Db2 Text Search index and disable Db2 Text Search.

For more information, see [“Dropping the Db2 Text Search index and disabling Db2 Text Search” on page 76](#).

6. Back up the OpenPages database and the Cognos content store.
7. Run the IBM Db2 installation program.

The installation program installs Db2 and upgrades the existing database instances. For more information, see [Upgrading a Db2 server \(Windows\)](#).

- a) Click **Install a Product**.
- b) Click **Work with Existing**.
- c) Select the installation that you use for OpenPages.
- d) Select the **Custom** option.
- e) Expand **Server Support** and select **Db2 Text Search** for installation.
- f) If you do not use Tivoli SA MP, clear the **Tivoli SA MP** check box.
- g) Accept the default settings on each page of the wizard until you are prompted for the **db2admin** credentials.
- h) Enter the domain and password for the db2admin user.
- i) Accept the default settings on the remaining pages of the wizard. Click **Finish**.

When the installation process completes, check the log files.

8. Upgrade your OpenPages database.

For more information, see [Upgrading databases](#).

For example, start the Db2 command line processor (CLP) and run the following commands:

```
set db2instance=db2inst1
db2start
db2 upgrade database opx user db2admin using password
```

9. Upgrade your Cognos content store database.

For more information, see [Upgrading databases](#).

For example, start the Db2 command line processor (CLP) and run the following commands:

```
set db2instance=db2inst2
db2start
db2 upgrade database cognosdb user db2admin using password
```

10. Revalidate objects, rebind packages, and redeploy the Java routines for OpenPages in the OpenPages database.

- a) Start the Db2 command line processor (CLP).
- b) Run the following command:

```
set db2instance=db2inst1
```

- c) Copy the /OP_<version>_Main/OP_<version>_Configuration/Database/DB2/INSTALL_SCRIPTS directory to the database server.
- d) Go to the directory where you copied the INSTALL_SCRIPTS directory, and then revalidate the database objects.

If you are upgrading to 11.5

Run the following commands:

```
db2 connect to OPX user openpage using password
db2 -td@ -f pks_OP_CURRENCY_MGR.sql
db2 -td@ -f pkb_OP_CURRENCY_MGR.sql
clpplus -nw openpage/password@<db_server>:50000/opx @sql-wrapper revalidate.sql
revalidate.log openpage
```

If you are upgrading to 11.1.4.4

Run the following command:

```
clppplus -nw openpage/password@0P:50000/opx  
@sql-wrapper revalidate.sql revalidate.log openpage
```

e) Rebind the packages.

For example:

```
db2rbind opx -l opbind.log all -u db2admin -p password -r any
```

f) Redeploy the Java routines for OpenPages.

For example:

```
manageOPJavaRoutines.bat opx opuser "password" remove opdb2udf.jar
```

```
manageOPJavaRoutines.bat opx opuser "password" install opdb2udf.jar
```

11. Revalidate objects and rebind packages in the Cognos content store.

Note: When you run Db2 commands, such as `db2 connect` or `db2rbind`, do not use quotation marks around passwords.

a) Start the Db2 command line processor (CLP).

b) Run the following command:

```
set db2instance=db2inst2
```

c) Revalidate the database objects.

For example:

```
db2 connect to cognosdb user db2admin using password  
db2 "call sysproc.admin_revalidate_db_objects()"
```

d) Rebind packages in the Cognos database.

For example:

```
db2rbind cognosdb -l cogbind.log -u db2admin -p password
```

12. Optional: Back up the databases.

13. Apply the IBM Db2 license.

a) Extract the quick start activation file for IBM Db2.

b) Start the Db2 command line processor (CLP).

c) Go to the directory where the license file, `db2ese_u.lic`, is stored.

d) Run the following command:

```
db2licm -a db2ese_u.lic
```

14. Start all IBM OpenPages with Watson services.

15. Configure and enable Db2 Text Search, create the index, and schedule a job to synchronize the index.

For more information, see "Utilities for filtering on long string field content in a Db2 database" in the *IBM OpenPages with Watson Administrator's Guide*.

Upgrading Db2 (Linux)

You must upgrade to a supported version of IBM Db2 before you migrate or upgrade to IBM OpenPages with Watson 8.2.

This task provides the basic steps for upgrading IBM Db2. For more information about this process, see the [IBM Db2 documentation](#).

About this task

Important: Fix pack 8.2.0.1 supports Db2 11.5.4. If you are migrating or upgrading to 8.2, complete the migration or upgrade before you apply the Db2 11.5.4 fix pack. Otherwise, you will see errors during the OpenPages database upgrade.

This task uses the following conventions:

- `db2inst1`: The OpenPages database instance owner
- `openpage`: The OpenPages database user
- `opx`: The name of the OpenPages database
- `db2inst2`: The Cognos database instance owner
- `cognosdb`: The name of the Cognos content store
- `<db_server>`: The hostname of the Db2 database server

The steps that you need to do depend on whether you are using your existing database server for OpenPages or using a new database server. If you are using a new database server, you skip the steps about upgrading the database instances and upgrading the databases. Later in the OpenPages migration process, you restore the databases and then upgrade them to the new Db2 version.

Note: When you run Db2 utilities, such as `db2 connect` or `db2rbind`, do not use quotation marks around passwords.

Procedure

1. Stop the following servers:
 - Stop all OpenPages application servers.
 - Stop the global search services.
 - Stop all IBM Cognos services.
2. Mount the IBM Db2 installation media or extract the downloaded installation package onto your file system.
 - a) Log in as the instance owner.
 - b) Create a directory. Do not create it under `/sqllib`.
 - c) Extract the Db2 installation package to the directory that you created.
3. Check that your system meets the installation prerequisites.

For more information, see [db2prereqcheck - Check installation prerequisites](#).

 - a) Go to the directory where you extracted the Db2 installation package.
 - b) As the root or sudo user, check the installation requirements.

```
./db2prereqcheck -i -v <version>
```

Where `<version>` is the Db2 version that you want to install.

For example:

```
./db2prereqcheck -i -v 11.5.0.0
```

If successful, you see the message DBT3533I The `db2prereqcheck` utility has confirmed that all installation prerequisites were met.

- c) Review the log file.
- d) As the OpenPages instance owner (for example, `db2inst1`), run the pre-upgrade checks:

```
./db2ckupgrade OPX -l /tmp/db2ckupgrade.log -u db2inst1 -p password
```

4. Complete the Db2 pre-upgrade tasks for both the OpenPages database and the Cognos database. For more information, see [Pre-upgrade tasks for Db2 servers](#).

If you get warnings about the discontinued SYSFUN.ASCII1 function, you can ignore them.

5. Check the value of the application heap size for the Cognos database.

- a) Run the following command as the database instance owner. Replace *<cognosdb>* with the name of your Cognos database.

```
db2 get db cfg for <cognosdb> | grep -i APPLHEAPSZ
```

- b) If the value is less than 4096, increase it to a minimum of 4096.

Run the following command as the database instance owner. Replace *<cognosdb>* with the name of your Cognos database.

```
db2 update db cfg for <cognosdb> using applheapsz 4096
```

6. Drop the Db2 Text Search index and disable Db2 Text Search.

For more information, see [“Dropping the Db2 Text Search index and disabling Db2 Text Search” on page 76](#).

7. Back up the OpenPages database and the Cognos database.

8. Run the Db2 installation program to upgrade IBM Db2

For more information, see [Upgrading a Db2 server \(Linux and UNIX\)](#).

- a) Log on to the database server as the root user. Go to the directory that you created in step 2. Run the db2setup command.

```
./db2setup
```

- b) Click **Install a Product** and **New Install**.

- c) For the **Product**, choose one of the following:

- If you are upgrading to 11.1.4.4, choose **Workgroup, Enterprise and Advanced Editions**.
- If you are upgrading to 11.5, choose **DB2 Version 11.5 Server Editions**.

- d) Select the **Custom** option.

- e) Do one of the following steps:

If you are moving to a new database server

Check the **Create an instance** checkbox.

For example, if you are migrating to a new version of OpenPages and you want to use a new database server, enable the **Create an instance** option.

If you are using your existing database server

Clear the **Create an instance** checkbox.

For example, if you are upgrading or if you are migrating and you are using your existing database server, clear the checkbox.

- f) Expand **Server Support** and select **Db2 Text Search** for installation.

- g) If you do not use Tivoli SA MP, clear the **Tivoli SA MP** check box.

- h) Accept the default settings on the remaining pages of the wizard.

- i) When the installation process completes, review the log files.

- j) Click **Finish**.

9. If you are upgrading Db2 on your existing database server, upgrade your OpenPages database instance.

Perform this step as the root user. For more information, see the [Db2 documentation](#).

If you are using a new database server, go to step [“14” on page 74](#).

- a) Stop all Db2 11.x databases.

- b) Edit the `/etc/services` file and remove any existing entry for the Db2 text service.

For example, remove db2j_db2inst1 55000/tcp, which is the default entry.

- c) Upgrade the OpenPages database instance.

If you are upgrading to 11.5

Run the db2iupgrade command. For example:

```
cd /opt/ibm/db2/V11.5/instance
./db2iupgrade -u db2fenc1 -j "TEXT_SEARCH,db2j_db2inst1,55000" db2inst1
```

If you are upgrading to 11.1.4.4 from 11.1.x

Run the db2iupdt command. For example:

```
cd /opt/ibm/db2/V11.1/instance
./db2iupdt -u db2fenc1 -j "TEXT_SEARCH,db2j_db2inst1,55000" db2inst1
```

- d) View the log file, for example /tmp/db2iupgrade.log.20620. Verify that the upgrade was successful. Look for the message DBI1070I Program db2iupgrade completed successfully.

- e) Verify the upgrade.

```
cd /opt/ibm/db2/V11.5/bin/
./db2val
```

- f) Check the installation level of the OpenPages database instance.

For more information, see [db2level - Show Db2 service level command](#).

```
db2level
```

Look for a return value that matches the version that you are installing. For example, look for a return value of DB2 v11.5.0.0.

10. Upgrade your Cognos database instance.

Perform this step as the root user

For more information, see the [Db2 documentation](#).

Note: Do this step after the OpenPages database instance upgrade completes successfully.

- a) Upgrade the Cognos database instance.

If you are upgrading to 11.5

Run the db2iupgrade command. For example:

```
cd /opt/ibm/db2/V11.5/instance
./db2iupgrade -u db2fenc1 db2inst2
```

If you are upgrading to 11.1.4.4 from 11.1.x

Run the db2iupdt command. For example:

```
cd /opt/ibm/db2/V11.1/instance
./db2iupdt -u db2fenc1 db2inst2
```

- b) View the log file, for example /tmp/db2iupgrade.log.18463. Verify that the upgrade was successful. Look for the message DBI1070I Program db2iupgrade completed successfully.

- c) Verify the upgrade.

```
cd /opt/ibm/db2/V11.5/bin/
./db2val
```

- d) Check the installation level of the Cognos database instance.

For more information, see [db2level - Show Db2 service level command](#).

```
db2level
```

Look for a return value that matches the version that you are installing. For example, look for a return value of DB2 v11.5.0.0.

11. If you are using Db2 Administration Server (DAS), upgrade the service.

For more information, see [Upgrading the Db2 Administration Server \(DAS\)](#).

For example:

```
cd /opt/ibm/db2/V11.5/instance
./dasmigr
```

The value DBI1070I Program dasmgr completed successfully indicates success.

12. Upgrade your OpenPages database.

Do this step as a user with SYSADM authority.

For more information, see [Upgrading databases](#) in the Db2 documentation.

For example:

```
db2start
db2 upgrade database opx user db2inst1 using password
```

13. Upgrade your Cognos database.

Do this step as a user with SYSADM authority.

For more information, see [Upgrading databases](#) in the Db2 documentation.

For example:

```
db2start
db2 upgrade database cognosdb user db2inst2 using password
```

14. Configure and enable Db2 Text Search, create the index, and schedule a job to synchronize the index.

- a) Start Db2 Text Search.

```
db2ts START FOR TEXT
```

- b) Create the index.

Go to the directory that you created in step 2, go to the TEXT_INDEXING subdirectory, and then run the following command:

```
clpplus -nw @sql-wrapper CustomIndexing_Step1_AddTextIndexing_to_DB.sql
CustomIndexing_Step1_AddTextIndexing_to_DB.log <db_server> 50000 opx db2inst1 'password'
OPENPAGE
```

A warning like the following message is expected and you can ignore it:

```
MESSAGE = <CIE99>CIE0212W Incomplete enablement of the Text Search server.
Reason code = "01"
```

- c) Update the configuration of the text server in the database.

```
cd /home/db2inst1/sqllib/db2tss/bin
TS_AUTH_TOKEN=`configTool printToken | awk 'NR == 2 {print}'`
TS_ENCRYPT_KEY=`configTool printToken | awk 'NR == 4 {print}'`
db2 connect to OPX
db2 select "*" from sysibmts.tsservers | grep $TS_AUTH_TOKEN
if [ $? != 0 ]; then
    echo "*** Registering text search server manually! ***"
    db2 "insert into SYSIBMTS.TSSERVERS (HOST, PORT, TOKEN, key, SERVERTYPE,
SERVERSTATUS)
values ('<db_server>', 55000, '$TS_AUTH_TOKEN', '$TS_ENCRYPT_KEY', 1, 0)"
fi
```

- d) Re-create the text indexes and set up a schedule for refreshing them.

Go to the directory that you created in step 2, go to the TEXT_INDEXING subdirectory, and then run the following command:

```
clpplus -nw @sql-wrapper CustomIndexing_Step2_IndexCreate.sql
CustomIndexing_Step2_IndexCreate.log <db_server> 50000 OPX openpage passwd " '* " '* "
"0,5,10,15,20,25,30,35,40,45,50,55" 1 && \
clpplus -nw @sql-wrapper CustomIndexing_Step3_IndexRefresh.sql
CustomIndexing_Step3_IndexRefresh.log <db_server> 50000 OPX openpage passwd " '* "
" '* " "0,5,10,15,20,25,30,35,40,45,50,55" 1
```

e) Verify that Db2 Text Search is running.

```
db2 "select count(*) from <openpages_database_user>.propertyvals_clob
where contains(CLOB_VALUE, 'RPS') = 1"
```

The expected result is:

```
1
-----
0

1 record(s) selected.
```

15. Revalidate objects, rebind packages, and redeploy the Java routines for OpenPages in the OpenPages database.

Do these steps as the OpenPages database user. In the following examples, the database user is openpage.

- Copy the /OP_<version>_Main/OP_<version>_Configuration/Database/DB2/INSTALL_SCRIPTS directory to the database server.
- Go to the directory where you copied the INSTALL_SCRIPTS directory, and then revalidate the database objects.

If you are upgrading to 11.5

Run the following commands:

```
db2 connect to OPX user openpage using password
db2 -td@ -f pks_OP_CURRENCY_MGR.sql
db2 -td@ -f pkb_OP_CURRENCY_MGR.sql
clpplus -nw openpage/password@<db_server>:50000/opx @sql-wrapper revalidate.sql
revalidate.log openpage
```

If you are upgrading to 11.1.4.4

Run the following command:

```
clpplus -nw openpage/password@OP:50000/opx
@sql-wrapper revalidate.sql revalidate.log openpage
```

c) Rebind the packages.

For example:

```
db2rbind opx -l opbind.log all -u db2inst1 -p password -r any
```

d) Redeploy the Java routines for OpenPages.

For example:

```
./manageOPJavaRoutines.sh opx openpage 'password'
remove /home/db2inst1/sqllib/function/jar/OPENPAGE
./manageOPJavaRoutines.sh OPX openpage 'password'
install /home/opuser/OP/OpenPages/DB2/INSTALL_SCRIPTS/opdb2udf.jar
ls -lrt /home/db2inst1/sqllib/function/jar/OPENPAGE
```

16. Revalidate objects and rebind packages in the Cognos database.

Do these steps as the instance owner for the Cognos database.

a) Revalidate the database objects.

For example:

```
db2 connect to cognosdb user db2inst2 using password
db2 "call sysproc.admin_revalidate_db_objects()"
```

b) Rebind packages in the Cognos database.

For example:

```
db2rbind cognosdb -l cogbind.log -u db2inst2 -p password
```

17. Optional: Back up the databases.

- For the OpenPages database, run the following commands as the instance owner for the OpenPages database:

```
mkdir db2v11bu
cd db2v11bu
db2 backup database opx to .
```

- For the Cognos database, run the following commands as the instance owner for the Cognos database:

```
mkdir db2v11bu
cd db2v11bu
db2 backup database cognosdb to .
```

18. Apply the IBM Db2 license.

For more information, see [db2licm - License management tool command](#).

- a) Get a license for IBM Db2.
- b) Run the db2licm command.

For example:

```
db2licm -a <license_file>
```

Where <license_file> is the full path and file name of the IBM Db2 license.

- c) Verify the license by running the db2licm -l command.

19. Start all IBM OpenPages with Watson services.

Dropping the Db2 Text Search index and disabling Db2 Text Search

If Db2 Text Search is enabled in your source environment, drop the text search indexes, disable the text search service, remove the Db2 administrative task to update the indexes, and disable Db2 Text Search. Do this procedure before you back up the OpenPages database.

Procedure

1. Log on to a system as the OpenPages installation user, for example opuser.

You can use any system with access to CLPPlus that can connect to the database server.

2. Drop the Db2 Text Search index.

- a) Go to the <OP_HOME>/aurora/bin/full-text-index directory.
- b) Open a command or shell window and run the following command:

```
clpplus -nw @sql-wrapper CustomIndexing_Step5_IndexDrop.sql
<LOG_FILE_NAME> <DB2_SERVER_NAME> <DB2_PORT_NUMBER> <DATABASE_NAME>
<OP_DB_USER> <OP_DB_PASSWORD> <FORCE_DROP_INDEX>
```

If the <OP_DB_PASSWORD> contains special characters, surround the password in quotation marks:

- Windows: "password"
- Linux: 'password'

For example

- Windows:

```
clpplus -nw @sql-wrapper CustomIndexing_Step5_IndexDrop.sql  
CustomIndexing_Step5_IndexDrop.log localhost 50000 OPX OPENPAGE "password" Y
```

- Linux:

```
clpplus -nw @sql-wrapper CustomIndexing_Step5_IndexDrop.sql  
CustomIndexing_Step5_IndexDrop.log localhost 50000 OPX OPENPAGE 'password' Y
```

For more information, see "Drop a long string index" in the *IBM OpenPages with Watson Administrator's Guide*.

3. Run the following command to determine if Db2 Text Search is enabled.

```
select * from all_tables where table_schema = 'SYSIBMTS';
```

If the command returns any data, Db2 Text Search is enabled. Continue with the next step to disable Db2 Text Search.

4. Log on to the OpenPages database as the db2inst1 user.

```
db2 connect to opx user opuser using password
```

5. Run the following command to disable Db2 Text Search.

For more information, see [SYSTS_DISABLE procedure - Disable current database for text search](#).

```
db2 "call sysproc.systs_disable('','en_US',?)"
```

Alternatively, use these commands.

```
db2 GRANT SYSTS_ADM TO db2inst1  
db2 grant SYSTS_MGR to db2inst1  
db2 connect reset  
db2ts start for text  
export DB2DBDFT=OPX  
db2ts DISABLE DATABASE FOR TEXT
```

6. Remove the Db2 administrative task to update the indexes

For more information, see the following topic in the Db2 documentation: [Removing a task from the administrative task scheduler](#).

Copy Java routine class files to the Db2 server

If you are using a new instance for the OpenPages database, copy the Java routine class files for IBM OpenPages with Watson to the IBM Db2 server before you create the reporting schema.

Do this task after you upgrade your database server to IBM Db2.

1. Go to the /OP_<version>_Main/OP_<version>_Configuration/Database/DB2/INSTALL_SCRIPTS directory.
2. Copy the following files to the DB2_HOME/FUNCTION directory:
 - opconvert.class
 - regexp.class

For example, on Microsoft Windows operating systems, the <DB2_HOME>\FUNCTION directory is <install_path>\ibm\SQLLIB\FUNCTION.

On Linux operating systems, the default location is /home/<db2_instance_owner>/sqllib/FUNCTION.

Creating the OpenPages database on IBM Db2

IBM OpenPages with Watson requires an OpenPages database. You must create the database before you install IBM OpenPages with Watson.

Procedure

1. Log on to the Db2 database server computer as the Db2 database instance owner.
2. Go to the `/OP_<version>_Main/OP_<version>_Configuration/Database/DB2/INSTALL_SCRIPTS` directory.
3. Verify that you have write permission on the `sql-wrapper.sql` file. If not, switch users or change the permission on the file by using the **chmod** command.
4. Edit the `sql-wrapper.sql` file to ensure that the variables are set correctly for your environment and save the changes.

- On Windows, if required, modify the following properties to suit your environment:

```
define opx_base_currency_iso_code='USD'
define opx_dflt_stor_srv_root='c:\OpenPages\openpages-storage'
define opx_op_admin_name='OpenPagesAdministrator'
define opx_op_admin_pwd='OpenPagesAdministrator'
define sqllib_dir='C:\IBM\SQLLIB'
```

- On Linux, if required, modify the following properties to suit your environment.

```
define opx_base_currency_iso_code='USD'
define opx_dflt_stor_srv_root='opt/openpages-storage/'
define opx_op_admin_name='OpenPagesAdministrator'
define opx_op_admin_pwd='OpenPagesAdministrator'
define sqllib_dir='home/db2inst1/sqllib'
```

5. On Linux, verify that you have execute permission on the `create-opx-db-srv.sh` script.
6. On Windows, start the Db2 command line processor (CLP). Click **Start > IBM Db2 > IBM Db2 Db2COPY1 > Command Line Tools > Db2 Command Window - Administrator**.
7. To create the database for OpenPages, run the `create-opx-db-srv.sh | .bat` script from the command line.

Use the following table to replace the variables in the command-line options with values that are suitable for your environment.

Table 34. Options for the <code>create-opx-db-srv.sh .bat</code> script	
Variable	Description
<code>database_name</code>	The name of the OpenPages database Note: If you are migrating to OpenPages 8.2, use the name from your previous OpenPages environment. Db2 does not support restoring to a database with a different name.
<code>path</code>	The location of the database on the server
<code>catalog_path</code>	The location of the database alias on the local server: <ul style="list-style-type: none">• On Windows operating systems, the <code><catalog_path></code> is the drive letter (C: or E:).• On Linux operating systems, <code><catalog_path></code> is the absolute path (<code>/home/db2inst1</code>).

- On Windows, type the following command:

```
create-opx-db-srv.bat <database_name> <path> <catalog_path>
```

Example: A database named OPX is created. The database and database alias are on the D: drive.

```
create-opx-db-srv.bat OPX D: D:
```

- On Linux, type the following command:

```
./create-opx-db-srv.sh <database_name> <path> <catalog_path>
```

Example: A database named OPX is created. The database and database alias are in the /home/db2inst1 directory.

```
./create-opx-db-srv.sh OPX /home/db2inst1 /home/db2inst1
```

8. If the database server is on a Windows operating system and the OpenPages installation user is not the Db2 database instance owner, run the following script:

```
clpplus -nw <username>/\ '<password>\'@<hostname>: <port>/<database_name>  
@sql-wrapper dba-grant.sql dba-grant.log <instance_owner_username>
```

- <username> is the user name of the OpenPages installation user (the user that is logged in to the system).
- <password> is the password of the OpenPages installation user.
- <instance_owner_username> is the Db2 database instance owner (the user who creates the database instance).

If the OpenPages installation user is the same as the Db2 database instance owner, no action is required.

The script explicitly grants control on the SYSTOOLS schema objects to the Db2 database instance owner.

9. If the database server is on a Windows computer, the OpenPages installation user is not the Db2 database instance owner, and the Db2 database instance owner is not the Db2 administration server (DAS) user, then run the following script:

```
clpplus -nw <username>/\ '<password>\'@<hostname>: <port>/<database-name>  
@sql-wrapper dba-grant.sql dba-grant.log <das_user_name>
```

- <username> is the user name of the OpenPages installation user (the user that is logged in to the system).
- <password> is the password of the OpenPages installation user.
- <das_user_name> is the Db2 Administration server (DAS) user account.

The script explicitly grants control on the SYSTOOLS schema objects to the DAS user.

What to do next

Create the database objects. You can use the OpenPages installation app or you can create the schema by using scripts. See [“OpenPages database object creation for Db2” on page 126](#).

Running the database creation scripts from the OpenPages application server computer

If your IBM OpenPages with Watson application server is not on the same computer as your database server, you can also run the database scripts remotely.

Before you begin

Ensure that your environment meets these prerequisites:

- ___ • The Db2 client software is installed on the application server, see [“Db2 database client installations” on page 85](#)
- ___ • The Db2 database server is running
- ___ • A database instance for the OpenPages database has been created
- ___ • Oracle compatibility mode is enabled
- ___ • You have updated the database manager configuration for the OpenPages database instance
- ___ • You have copied the Java routine class files and encryption files to the Db2 server from the OpenPages installation files.
- ___ • Db2 Text Search is enabled and configured

Procedure

1. Log on to the OpenPages with Watson application server computer as the Db2 administrator.
2. On Windows, start the Db2 command line processor (CLP). Click **Start > IBM Db2 > IBM Db2 Db2COPY1 > Command Line Tools > Db2 Command Window - Administrator**.
3. Go to the /OP_<version>_Main/OP_<version>_Configuration/Database/DB2/INSTALL_SCRIPTS directory.
4. To catalog the node, run the following script:

- Linux:

```
./db2-catalog-node.sh <node_name> <hostname> <port>
```

- Windows:

```
db2-catalog-node.bat <node_name> <hostname> <port>
```

Table 35. Command-line variables for the db2-catalog-node.sh/.bat script

Variable name	Description
<i>node_name</i>	The node name of the database partition server. The node name represents a local nickname that you can set for the computer that contains the database you want to catalog.
<i>hostname</i>	The host name or the IP address of the node where the target database is installed.
<i>port</i>	The port that the database server uses. The default port is 50000.

Example:

- Linux:

```
./db2-catalog-node.sh OPNode op.server.com 50000
```

- Windows:

```
db2-catalog-node.bat OPNode op.server.com 50000
```

5. To create the database for OpenPages, run the create-opx-db-clt script.

Replace the variables with your system values:

- <database_name> is the name of the OpenPages database.

- `<path>` is the location on which to create the database on the server.
- `<catalog_path>` is the location of the database alias on the local computer.
- `<node_name>` is the cataloged node name.
- `<instance_owner_username>` is the user name of the Db2 account that owns the instance on the remote computer.
- `<instance_owner_password>` is the password for the account that owns the database instance.

Use the following syntax:

- Linux:

```
./create-opx-db-clt.sh <database_name> <path> <catalog_path>
```

- Windows:

```
create-opx-db-clt.bat <database_name> <path> <catalog_path> <node_name>  
<instance_owner_username> "<instance_owner_password>"
```

Example: Create a remote database on a Linux system from a Windows-based computer. The Db2 database instance owner on the remote computer is db2admin.

```
create-opx-db-clt.bat OPX C: C: OPNode db2admin "password"
```

Note: Quotation marks are required around a password only if the password contains special characters. See [“Special characters in passwords” on page 12](#).

6. If the database server is on a Windows operating system and the OpenPages installation user is not the Db2 database instance owner, run the following script:

```
clpplus -nw <username>/\'<password>\'@<hostname>: <port>/<database_name>  
@sql-wrapper dba-grant.sql dba-grant.log <instance_owner_username>
```

- `<username>` is the user name of the OpenPages installation user (the user that is logged in to the system).
- `<password>` is the password of the OpenPages installation user.
- `<instance_owner_username>` is the Db2 database instance owner (the user who creates the database instance).

If the OpenPages installation user is the same as the Db2 database instance owner, no action is required.

The script explicitly grants control on the SYSTOOLS schema objects to the Db2 database instance owner.

7. If the database server is on a Windows computer, the OpenPages installation user is not the Db2 database instance owner, and the Db2 database instance owner is not the Db2 administration server (DAS) user, then run the following script:

```
clpplus -nw <username>/\'<password>\'@<hostname>: <port>/<database-name>  
@sql-wrapper dba-grant.sql dba-grant.log <das_user_name>
```

- `<username>` is the user name of the OpenPages installation user (the user that is logged in to the system).
- `<password>` is the password of the OpenPages installation user.
- `<das_user_name>` is the Db2 Administration server (DAS) user account.

The script explicitly grants control on the SYSTOOLS schema objects to the DAS user.

Preparing the database instances for OpenPages on Db2

You must prepare the IBM Db2 database instances that are used for the IBM OpenPages with Watson databases.

Before you begin

For more information about IBM OpenPages with Watson supported software, see [“Software prerequisites”](#) on page 33.

Tip: To verify the current version and service level of IBM Db2, use the **db2level** command.

About this task

To prepare the database instances, you must:

- ___ • Run the `enable-ora-compatibility` script to enable Oracle compatibility mode for the Db2 database instance that is used for the OpenPages schema.
Important: Oracle compatibility mode must not be enabled on the Db2 database instance that is used for the Cognos Analytics content store.
- ___ • Run the `opx-dbm-cfg` script to update the database manager configuration for the OpenPages database instance.
- ___ • Copy the Java routine class files to the Db2 database server installation location from the OpenPages installation files.
- ___ • Enable and configure Db2 Text Search. For more information, see the *IBM OpenPages with Watson Administrator's Guide*.

Procedure

1. Log on to the Db2 database server as the Db2 instance owner.
2. Go to the `/OP_<version>_Main/OP_<version>_Configuration/Database/DB2/INSTALL_SCRIPTS` directory.
3. On Linux, ensure that the Db2 instance owner has execute permission on the scripts in the `INSTALL_SCRIPTS` directory.
 - If the Db2 instance owner owns the directory, type the following command:

```
chmod -R 755 /<path>/INSTALL_SCRIPTS
```
 - If the Db2 instance owner belongs to the same group as the user who owns the directory, type the following command:

```
chmod -R 775 /<path>/INSTALL_SCRIPTS
```
 - If the Db2 instance owner is part of other groups, type the following command:

```
chmod -R 777 /<path>/INSTALL_SCRIPTS
```
4. Edit the `sql-wrapper.sql` file to ensure that the variables are set correctly for your environment and save the changes.

- On Windows, if required, modify the following properties to suit your environment:

```
define opx_base_currency_iso_code='USD'  
define opx_dflt_stor_srv_root='c:\OpenPages\openpages-storage'  
define opx_op_admin_name='OpenPagesAdministrator'  
define opx_op_admin_pwd='OpenPagesAdministrator'  
define sqllib_dir='C:\IBM\SQLLIB'
```

- On Linux, if required, modify the following properties to suit your environment.

```
define opx_base_currency_iso_code='USD'  
define opx_dflt_stor_srv_root='opt/openpages-storage/'  
define opx_op_admin_name='OpenPagesAdministrator'  
define opx_op_admin_pwd='OpenPagesAdministrator'  
define sqllib_dir='home/db2inst1/sqllib'
```

5. Enable Oracle compatibility mode on the OpenPages database instance.

- On Windows, open a command prompt and type `db2cmd` to start the Db2 command line processor (CLP). Then, type `enable-ora-compatibility.bat`.
- On Linux, type `./enable-ora-compatibility.sh`.

Note: If you have multiple instances of the Db2 server, ensure that you choose the DB2COPY of the OpenPages database instance.

Restriction: Db2 compatibility features are enabled at the database instance level and cannot be disabled. Keep the selected compatibility level for the life of the OpenPages database.

To confirm that Oracle compatibility mode is set, type `db2set -all`. Verify that one of the listed profile variables is **DB2_COMPATIBILITY_VECTOR=ORA**.

- Update the database manager configuration for the OpenPages database instance.
 - On Windows, open a command prompt and type `db2cmd` to start the Db2 command line processor (CLP). Then, type `opx-dbm-cfg.bat`.
 - On Linux, type `./opx-dbm-cfg.sh`.
- Copy the Java routine class files for OpenPages to the Db2 server.
 - Go to the `/OP_<version>_Main/OP_<version>_Configuration/Database/DB2/INSTALL_SCRIPTS` directory.
 - Copy the following files to the `<DB2_HOME>/FUNCTION` directory:
 - `opconvert.class`
 - `regexp.class`

For example, on Windows, the `<DB2_HOME>\FUNCTION` directory is `<install_path>\ibm\SQLLIB\FUNCTION`.

On Linux, the default location is `/home/<db2_instance_owner>/sqllib/FUNCTION`.
- Enable and configure text search. For more information, see [Db2 Text Search](#).
- Copy the encryption function for OpenPages to the Db2 server.
 - Go to the `/OP_<version>_Main/OP_<version>_Configuration/Database/DB2/INSTALL_SCRIPTS/bin/<PLATFORM>` directory.
 - Copy the files to the following directories:
 - `<DB2_HOME>/FUNCTION`
 - `<DB2_HOME>/FUNCTION/unfenced`

What to do next

You can create the database instance for OpenPages.

Operating system user accounts for IBM Db2 databases

Operating system user accounts do the procedures that are used to create the IBM OpenPages with Watson database and Cognos Analytics content store.

Restriction: You must use two separate databases - one for the Cognos Analytics content store and one for the IBM OpenPages with Watson database.

Db2 instance owner

This user controls all Db2 processes and owns all file systems and devices that are used by the databases within the database instance.

For Windows operating systems, the default user is `db2admin`.

For Linux operating systems, the default user is `db2inst1`.

The user account for the Db2 instance owner is created as a prerequisite step to installing Db2 software and instance.

Db2 administration server (DAS) user

The user ID for the Db2 administration server user.

For Windows operating systems, the default user is db2admin.

For Linux operating systems, the default user is dasusr1.

Important: To simplify user administration, when you install the Db2 database, ensure that you assign the Db2 instance owner as the DAS user.

OpenPages installation user

This user installs OpenPages with Watson. The user account can create the OpenPages database automatically by using the OpenPages installation app or manually by running scripts.

Restriction: On Windows, if the OpenPages installation user is not the same as the Db2 instance owner, the OpenPages installation user must run the dba-grant.sql script. The script explicitly grants control on SYSTOOLS schema objects to the Db2 database instance owner.

For information about creating the database manually, see [“Creating the OpenPages database on IBM Db2” on page 78](#).

Database schema owners

The following distinct database user accounts must exist before you install OpenPages with Watson and Cognos Analytics:

- OpenPages database user account.
- Cognos Analytics content store user account

On Linux operating systems, the user names for the OpenPages database user account must not be the same as the group name. For example, opuser:opuser is not allowed.

Db2 guidelines for creating users

Important: The user accounts must match the schema names on which they operate.

Follow the [Db2 guidelines for creating user names](#).

For more information about passwords for your Db2 user accounts, see the [IBM Db2 documentation](#).

Users and groups for application servers on Linux that use Db2 databases

To install the Db2 database client and the IBM OpenPages with Watson application, you must create one user and one group.

To install the Db2 database client, create and configure the required user and group as specified in the following table.

Table 36. Required user and group for application servers			
User	Assign to Groups	Permissions	Reason
db2user	The group is assigned during the installation of the Db2 client.	Read, write, execute permission to the Db2 client installation directory.	Required by the Db2 database client installation program.

Table 36. Required user and group for application servers (continued)

User	Assign to Groups	Permissions	Reason
opuser		Read, write, execute permission to the following directories: <ul style="list-style-type: none"> • Db2 database client installation directory. • Java SDK installation directory. • Cognos Analytics installation directory. 	The user account that installs OpenPages.

Db2 database client installations

Install an IBM Db2 database client so that the IBM OpenPages with Watson application servers and reporting servers can connect to the Db2 database server.

Use the following checklist to guide you through the required setup:

- ___ • Install the Db2 client software.

Use the Db2 Setup wizard to install the IBM Data Server Client. For information, see the Db2 documentation:

- [Installing Db2 database servers using the Db2 Setup wizard \(Windows\)](#)
- [Installing Db2 servers using the Db2 Setup wizard \(Linux and UNIX\)](#)

- ___ • Create a Db2 database client instance on the client computer (Linux only).

- ___ • Configure the Db2 client and server connection.

- ___ • Test the connection between the database server and the client.

For information about the installation methods for IBM data server clients in Linux environments, see [Installing IBM data server clients \(Linux and UNIX\)](#) in the Db2 documentation.

Creating and configuring a Db2 client instance in Linux environments

If you are using Linux application servers or reporting servers, create a Db2 client instance on the application server and reporting server computers.

In Windows environments, the client instance is created by default when the client software is installed.

For more information, see [db2icrt - Create instance command](#).

Procedure

1. Log on to the application server computer as a root user.
2. Go to the `<DB2DIR>/instance/` directory.

`<DB2DIR>` is installation location of the Db2 client software. The default installation directory is `/opt/ibm/db2/<version>/instance`.

3. To create an instance for a client, run the following command:

```
db2icrt -s client <instname>
```

The `-s` option is used when you create an instance other than the default instance that is associated with the installed product from which you run the **db2icrt** command.

`<instname>` is the user name of the instance owner.

Example: `db2icrt -s client db2inst2`

The default location of the Db2 instance /home/db2inst2/sqllib.

4. Log on to the reporting server computer as a root user, and repeat steps 2 and 3.

Testing the connection between the Db2 client and server

If the IBM OpenPages with Watson application server is not on the same computer as the database server, test the connection. Ensure that you can connect to the IBM Db2 server from the OpenPages application server computer.

Before you begin

You must have System Administrative (SYSADM) or System Controller (SYSCTRL) authority. Otherwise, ensure that the catalog_noauth option is set to ON. You cannot use root authority when you catalog a node.

Procedure

1. Log on to the OpenPages application server as a Db2 user.
2. If you are using Microsoft Windows, start the Db2 command line processor.

From the command prompt, type db2cmd. Or, click **Start > IBM Db2 > IBM Db2 Db2COPY1 > Command Line Tools > Db2 Command Window - Administrator**.

3. Test the connection from the client to the database.
 - a) To verify that the node was created, issue the following command to list the contents of the node directory:

```
db2 list node directory show detail
```

A list of the nodes that you created is displayed.

```
Node Directory
Number of entries in the directory = 1
Node 1 entry:
Node name           = OPNode_Name
Comment             =
Directory entry type = LDAP
Protocol            = TCPIP
Hostname            = database_server_name
Service name        = 500000
```

- b) To list the database directory, run the following command:

```
db2 list database directory
```

A list of the databases is displayed.

- c) To connect to the remote database from the client, type the following command

```
db2 => connect to <database_alias> user <userid>
```

Example: connect to opdb user opuser

If the connection is successful, a message similar to the following message is displayed:

```
Database Connection Information
Database server = DB2 <version>
SQL authorization ID = opuser
Local database alias = opdb
```


Checklist for the database server (Oracle)

If you use an Oracle database server, do these tasks before you install IBM OpenPages with Watson:

- Check that all of the required ports are available. See [“Port assignments ” on page 124](#).
- If the database server is running on Linux, set up the operating system users and groups for Oracle (oinstall, dba, oracle). See [“Creating users and groups on the Oracle database server for Linux operating systems” on page 87](#).
- Install Oracle and create a database for OpenPages. See [“Oracle Database 18c or 19c installations” on page 88](#) or [“Oracle Database 12.2.0.1 installations” on page 92](#).
- Review the list of Oracle package dependencies.

To function correctly, the OpenPages Oracle packages must have access to some standard Oracle objects. If you are using a standard Oracle deployment, access to these objects is granted by default.

Some environments, however, might restrict the default Oracle access model and remove public access from some of the objects. Review the list of package dependencies to ensure access is granted. See [“Oracle package dependencies” on page 432](#).

- Set environment variables.
 - Windows: See [“Setting the Oracle environment variables for the database server \(Windows\)” on page 96](#).
 - Linux: See [“Setting the Oracle environment variables for the database server \(Linux\)” on page 96](#).

If the database server is on a separate computer, install the database client software on each application server and reporting server. For more information, see [“Oracle database client installations” on page 99](#).

Creating users and groups on the Oracle database server for Linux operating systems

For Linux installations, create and configure the oinstall and dba groups and the oracle user on the server that hosts the Oracle database.

The users and groups must be created and configured by a user with SYSADMIN privileges and access to root.

For more information, see the Oracle documentation.

If you are installing a cluster environment, you must create these users on the cluster administrator server and on each cluster member.

About this task

Use the following table to help you create the required users and user groups for the database server.

Table 37. Required users and groups for Oracle database servers			
User	Assign to Groups	Permissions	Reason
oracle	oinstall; dba oinstall is the primary group for this user.	Read, write, execute permission to the Oracle Admin client installation directory.	Required by Oracle database installation program. Important: The password for this user cannot contain spaces or special characters.

Procedure

1. Log on to the database server as root.
2. Create the groups: oinstall and dba.

- a) Open a Linux shell .
- b) Type the following command:

```
groupadd oinstall
```

This group is the primary group for the oracle user. This group is the inventory group.

Note: The Oracle database requires this name.

- c) Type the following command:

```
groupadd dba
```

Note: The Oracle database requires this name.

3. Create a user that is called oracle, assign the initial login group (oinstall), and add the user to the dba group.

- a) Go to the /usr/sbin/ directory
- b) Type the following command:

```
/usr/sbin/useradd -m -g oinstall -G dba oracle
```

4. Change the password for the oracle user by using the following command:

```
passwd oracle
```

5. At the **New Password** prompt, enter a new password.

Oracle Database 18c or 19c installations

IBM OpenPages with Watson requires a database server. You can use Oracle Database on the database server. After you install Oracle, some configuration is required.

Restriction: Do not install Oracle Database or Oracle Client software into a directory that contains spaces.

Important: The passwords for database users (such as SYSTEM, SYS, DBSNMP, SYSMAN) can contain only the following special characters:

```
. + - [ ] * ~ _ # : ?
```

After installing the Oracle Database software, you must install Oracle Client software on all application servers and reporting servers.

Do the following tasks:

1. If you are installing Oracle on Linux, create the users and groups for Oracle. See [“Creating users and groups on the Oracle database server for Linux operating systems”](#) on page 87.
2. Install or upgrade to Oracle 18c or 19c.
3. Create an Oracle instance for the OpenPages database.
4. Add a local net service name for the OpenPages database.

Installing Oracle 18c or 19c

You can use these steps to set up Oracle 18c or 19c for the OpenPages and Cognos databases.

About this task

The steps in this task are provided to help you understand the overall process. For more information, see the Oracle documentation.

For information about upgrading Oracle, see [“Upgrading Oracle from 12.x to 18c or 19c \(in-place\)”](#) on page 90 or [“Upgrading Oracle from 12.x to 18c or 19c \(migration\)”](#) on page 91.

Procedure

1. Do the Oracle pre-installation steps and check that your system meets the installation prerequisites.

For more information, see:

- Windows: [Oracle Database Installation Checklist](#)
- Linux: [Oracle Database Installation Checklist](#)

2. Download the Oracle installation package for your operating system.

For example:

- Windows: `WINDOWS.X64_180000_db_home.zip`
- Linux: `LINUX.X64_180000_db_home.zip`

3. Create the `ORACLE_HOME` directory.

This directory is where you will install Oracle.

On Linux, for example, you can use the following command:

```
mkdir -p /home/oracle/app/product/18.3
```

4. Extract the Oracle installation package into the `ORACLE_HOME` directory.

The Oracle installer does not allow you to install to a different directory.

For example, on Linux, run the following commands:

```
cd /home/oracle/app/product/18.3
unzip /tmp/LINUX.X64_180000_db_home.zip
```

5. Start the Oracle installation program.

- Windows: Open a command prompt as an administrator, and then run `setup.exe`.
- Linux: Run `./runInstaller`.

6. Use the installation wizard to install Oracle.

Use the defaults, except for the following options:

- On the **Select Installation Option** page, select **Create and configure a single database instance**.
- On the **System Class** page, select **Server class**.
- On the **Install Type** page, select **Typical install**.
- On the **Typical Installation** page, enter the values that are appropriate for your environment.

For example, if you want to use Oracle Pluggable Database (PDB), you can use the following values:

- For the **Global Database Name**, type `OPCDB`.
- Select **Create as Container Database**.
- For the **Pluggable database name**, type `OP`.

Or, if you are not using Oracle Pluggable Database, you can use the following values:

- For the **Global Database Name**, type `OP`.
- Clear the **Create as Container Database** check box.
- For the character set, use `AMERICAN_AMERICA.AL32UTF8`.
- On the **Prerequisite Checks** page, fix any issues. If issues are marked **fixable**, click **Fix & Check Again**. Fix any other issues manually.
- For Linux only:
 - Install all recommended packages. For example:

```
yum install -y nfs-utils smartmontools compat-libstdc++-33-3.2.3
```

- If the maximum stack size is an issue, log in as root and edit the `/etc/security/limits.conf` file. Add these lines:

```
* soft stack 10240
* hard stack 10240
```

Log back in as `oracle` and re-run the installer.

- If swap size is an issue, run the following command as the root user to increase the swap size:

```
dd if=/dev/zero of=/swapfile count=8096 bs=1MiB
mkswap /swapfile
chmod 600 /swapfile
swapon /swapfile
```

Where `count` is the amount in megabytes by which to increase the swap size.

When the errors are fixed, you can continue with the installation.

- Run the `root.sh` script as instructed.

Upgrading Oracle from 12.x to 18c or 19c (in-place)

You can upgrade Oracle to version 18c (18.x) or 19c (19.x). Use these steps if you want to upgrade Oracle by installing on top of your existing Oracle deployment (in-place upgrade).

About this task

This topic provides an overview of the upgrade process. For more information, see the [Oracle installation and upgrade guides](#).

Talk to your Oracle database administrator (DBA) before you begin this procedure.

Note: If you use special characters in database passwords, before you upgrade, ensure that your database passwords do not contain the `@` character.

Procedure

1. Do the Oracle pre-upgrade steps and check that your system meets the installation prerequisites.
For more information, see the [Oracle Database Upgrade Guide](#).

2. Stop all OpenPages application servers (admin and non-admin), all reporting servers (active and standby), and the search server.

For more information, see the *IBM OpenPages with Watson Installation and Deployment Guide*.

3. Back up the OpenPages and Cognos databases by using the `OPBackup` and `OPCCBackup` utilities.

For more information, see:

- [“Backing up the OpenPages database \(Oracle\)” on page 412](#)
- [“Backing up the Cognos content store \(Oracle\)” on page 413](#)

4. Install the new version of Oracle.

For more information, see the *IBM OpenPages with Watson Installation and Deployment Guide* and the Oracle documentation.

5. Go to the `ORACLE_HOME` directory, and then start the **Database Upgrade Assistant**.

- Windows: Click **Start > Oracle <HOME_NAME> > Configuration and Migration Tools > Database Upgrade Assistant**.
- Linux: Run `dbua` from the `<ORACLE_HOME/bin` directory. For example:

```
cd /home/oracle/app/product/19.0/bin/
./dbua
```

6. Upgrade the databases.

Confirm the options with your Oracle database administrator. Typically, the default values can be used, with the following exceptions:

- a) Select the OpenPages database and the Cognos database. Type the sysdba credentials. Click **Next**.
Check the list of required and recommended actions. Resolve any issues.
 - b) On the **Select Upgrade Options** tab, use the default options.
 - c) On the **Select Recovery Options** tab, use the options that are recommended by your Oracle database administrator.
To skip backups completely, select **I have my own backup and restore strategy**.
 - d) On the **Configure Network** and **Configure Management** tabs, use the default options.
 - e) Review the **Summary** page. Verify that **Target Oracle Home** and **Source Oracle Home** are correct. Verify the other values on the **Summary** page, and then click **Next**.
7. Do the Oracle post upgrade steps.
For more information, see [Post-Upgrade Tasks for Oracle Database](#)
8. Do the following steps on all application servers and all reporting servers:
- a) Install the new version of the Oracle Client software.
Use the same version as the Oracle Database software.
 - b) Update the <ORACLE_HOME> environment variable to point to the upgraded Oracle installation.
 - c) Copy the following files from your prior Oracle Client installation to the upgraded Oracle Client installation:
 - sqlnet.ora (if it exists)
 - tnsnames.oraVerify that the HOST parameter in the tnsnames.ora file is set to the host name of your upgraded Oracle server.
9. Do the following steps on the active reporting server:
- a) Log on to the active reporting server as a user with administrative privileges.
 - b) Stop the IBMOpenPagesFrameworkModelGenerator service.
 - c) Go to the <CC_HOME>/framework/conf directory.
 - d) Open the framework.properties file in a text editor. Ensure that the oracle.client.path property contains the location of the new Oracle Client bin directory.
 - e) Save and close the file.
 - f) Restart the IBMOpenPagesFrameworkModelGenerator service.
10. Start all OpenPages application servers (admin and non-admin), all reporting servers (active and standby), and the search server.

For more information, see the *IBM OpenPages with Watson Installation and Deployment Guide*.

Upgrading Oracle from 12.x to 18c or 19c (migration)

You can install Oracle 18c (18.x) or 19c (19.x) on new hardware and then migrate the OpenPages and Cognos databases.

About this task

If you want to upgrade Oracle in-place, see [“Upgrading Oracle from 12.x to 18c or 19c \(in-place\)”](#) on page 90.

Note: If you use special characters in database passwords, before you upgrade, ensure that your database passwords do not contain the @ character.

Procedure

1. Do the Oracle pre-upgrade steps and check that your system meets the installation prerequisites.
For more information, see the [Oracle Database Upgrade Guide](#).
2. Install the new version of Oracle.
For more information, see the *IBM OpenPages with Watson Installation and Deployment Guide* and the Oracle documentation.
3. Stop all OpenPages application servers (admin and non-admin), all reporting servers (active and standby), and the search server.
For more information, see the *IBM OpenPages with Watson Installation and Deployment Guide*.
4. Back up the OpenPages and Cognos databases by using the OPBackup and OPCCBackup utilities.
For more information, see:
 - [“Backing up the OpenPages database \(Oracle\)” on page 412](#)
 - [“Backing up the Cognos content store \(Oracle\)” on page 413](#)
5. Restore the OpenPages and Cognos databases by using the OPRestore and OPCCRestore utilities.
6. Do the following steps on all application servers and all reporting servers:
 - a) Install the new version of the Oracle Client software.
Use the same version as the Oracle Database software.
 - b) Update the <ORACLE_HOME> environment variable to point to the upgraded Oracle installation.
 - c) Copy the following files from your prior Oracle Client installation to the upgraded Oracle Client installation:
 - sqlnet.ora (if it exists)
 - tnsnames.oraVerify that the HOST parameter in the tnsnames.ora file is set to the host name of your upgraded Oracle server.
7. Do the following steps on the active reporting server:
 - a) Log on to the active reporting server as a user with administrative privileges.
 - b) Stop the IBMOpenPagesFrameworkModelGenerator service.
 - c) Go to the <CC_HOME>/framework/conf directory.
 - d) Open the framework.properties file in a text editor. Ensure that the oracle.client.path property contains the location of the new Oracle Client bin directory.
 - e) Save and close the file.
 - f) Restart the IBMOpenPagesFrameworkModelGenerator service.
8. Start all OpenPages application servers (admin and non-admin), all reporting servers (active and standby), and the search server.

Oracle Database 12.2.0.1 installations

IBM OpenPages with Watson requires a database server. You can use Oracle Database on the database server. After you install Oracle, some configuration is required.

Restriction: Do not install Oracle database server or Oracle client software into a directory that contains spaces.

Important: The passwords for database users (such as SYSTEM, SYS, DBSNMP, SYSMAN) can contain only the following special characters:

. + - [] * ~ _ # : ?

After installing the Oracle Database software, you must install Oracle Client software on all application servers and reporting servers.

Do the following tasks:

1. If you are installing Oracle on Linux, create the users and groups for Oracle. See [“Creating users and groups on the Oracle database server for Linux operating systems” on page 87](#).
2. Install or upgrade Oracle.
3. Add an Oracle listener for the OpenPages database.
4. Create an Oracle instance for the OpenPages database.
5. Add a local net service name for the OpenPages database.

Upgrading Oracle from 12.1.x to 12.2.0.1

If you are using Oracle 12.1.x, you must upgrade. You can upgrade to version 12.2.0.1.

About this task

The following steps provide an overview of the upgrade process. For details, see the [Oracle installation and upgrade guides](#).

Consult with your Oracle database administrator (DBA) before you begin this procedure.

Procedure

1. Do the pre-upgrade steps.
 - a) If any OpenPages components are running, stop them.
For more information, see [Chapter 12, “Starting and stopping servers,” on page 309](#).
 - b) Back up the OpenPages and Cognos databases by using the OPBackup and OPCCBackup utilities.
 - c) Verify that your environment meets the system prerequisites for Oracle 12.2.0.
For more information, see the [Oracle documentation](#).
 - d) Log in to the database server as the Oracle installation user.
 - e) Empty the Oracle recycle bin by running the following commands:

```
$ sqlplus / as sysdba
SQL> purge recyclebin;
```
 - f) Update the Oracle path in the environment variables on the Oracle server.
For example:
 - On Microsoft Windows, if Oracle 12.1.0.2 is installed in C:\app\product\12.1.0\dbhome_1, change the path to C:\app\product\12.2.0\dbhome_1
 - On Linux, if Oracle 12.1.0.2 is installed in /home/oracle/app/oracle/product/12.1/dbhome_1, change the path to /home/oracle/app/oracle/product/12.2/dbhome_1
2. Upgrade the Oracle database server to version 12.2.0.1.
 - a) Download the Oracle 12.2.0.1 installation package and extract the files.
For example:
 - Windows: V839963-01 for Oracle server 12.2.0.1 Windows 64 bit
 - Linux: V839960-01 for Oracle server 12.2.0.1 Linux x86-64
 - b) Start the Oracle installation program.
 - Windows: Run setup.exe.
 - Linux: Run the runInstaller script.
 - c) Use the installation wizard to install Oracle 12.2.0.

Accept the default options on all pages, except for the options described in the following steps.

Windows

- On the **Select Installation Option** page, select **Upgrade an existing database**.
- On the **Oracle Home User** page, select **Use Windows Built-in Account**.
- On the **Specify Installation Location** page, ensure the **Oracle base** and **Software location** show the same path that you specified in the environment variables.

Linux

- On the **Select Installation Option** page, select **Upgrade an existing database**.
- On the **Specify Installation Location** page, ensure the **Oracle base** and **Software location** show the same path that you specified in the environment variables.
- If errors are shown on the **Perform Prerequisite Checks** page, do the following steps:
 - i) Select **Fix & Check Again**, and follow the instructions.
 - ii) If the maximum stack size is an issue, log in as `root` and edit the `/etc/security/limits.conf` file. Add these lines:

```
* soft stack 10240
* hard stack 10240
```

Log back in as `oracle` and re-run the installer.

- iii) If swap size is an issue, run the following command as a root user to increase the swap size:

```
dd if=/dev/zero of=/tmp/swap1 bs=1M count=512
mkswap /tmp/swap1
swapon /tmp/swap1
```

Where `count` is the size to increase.

When the errors are fixed, you can continue with the installation.

- Run the `root.sh` script as instructed.

For more information about installing Oracle, see the Oracle documentation.

3. Upgrade the databases to 12.2.0.1.

The **Database Upgrade Assistant** starts automatically. Confirm the options with your Oracle database administrator. Typically, the default values can be used, with the following exceptions:

- a) Select the OpenPages database and the Cognos database. Type the `sysdba` credentials. Click **Next**.

If any errors are shown, click **Fix & Check Again** and follow any instructions.

- b) On the **Select Recovery Options**, use the options that are recommended by your Oracle DBA. If you are not sure which options to use, ask your Oracle DBA for help. The options that you need depend on the business requirements and backup procedures at your organization.
- c) Review the **Summary** page. Verify that **Target Oracle Home** and **Source Oracle Home** are correct. Verify the other values on the **Summary** page, and then click **Next**.

4. Click **Finish**.

5. Copy the following files from your Oracle 12.1 server to your 12.2 server:

- `listener.ora`
- `sqlnet.ora`
- `tnsnames.ora`

Verify that the `HOST` parameter in the `tnsnames.ora` file is set to the host name of your Oracle 12.2 server.

6. Open the `listener.ora` file and update the `ORACLE_HOME` parameter. Type the path to the `ORACLE_HOME` directory on your 12.2 server.

7. Do the following steps on all application servers and reporting servers:

- a) Install the Oracle Client 12.2 software.
- b) Update the `<ORACLE_HOME>` environment variable to point to the Oracle 12.2 installation.
- c) Copy the following files from your 12.1 Oracle client installation to the 12.2 client installation:
 - `sqlnet.ora` (if it exists)
 - `tnsnames.ora`

Verify that the `HOST` parameter in the `tnsnames.ora` file is set to the host name of your Oracle 12.2 server.

Results

The Oracle Database and Oracle Client software is upgraded.

When you set up the application servers, reporting servers and the search server, you must update the JDBC database driver files on each of them.

Adding an Oracle listener for the OpenPages with Watson database

You must manually add an Oracle database listener for the IBM OpenPages with Watson database.

Procedure

1. Log on to your database server as a user with administrative privileges.
2. Start the Net Configuration Assistant.
 - a) Open a Command Prompt window as a user with Administrative privileges.
 - b) Go to the `<ORACLE_HOME>/bin` directory.
 - c) To start the Net Configuration Assistant, type the following command: `netca`.
3. Accept the default options on all pages, except for the pages described here. For full information, see the Oracle documentation.
 - a) On the **Listener Configuration, Listener Name** page, ensure the listener name that you specify is unique in the current Oracle Home
 - b) On the **TCP/IP Protocol** page, choose a port.

Creating a database instance for the OpenPages database

You must create an Oracle database instance for OpenPages with Watson to use.

Note: OpenPages with Watson supports PDB databases only with Oracle 12.2 or later.

Procedure

1. Log on to your Oracle database server as a user with administrative privileges.
2. Start the Database Configuration Assistant.
 - a) Open a command prompt window as a user with administrative privileges.
 - b) Go to the `<ORACLE_HOME>/bin` directory.
 - c) To start the Database Configuration Assistant, type the following command: `dbca`.
3. Accept the default options on all pages, except for the pages described here. For full information, see the Oracle documentation.
4. On the **Initialization Parameters** page, change the following settings.
 - a) On the **Memory** tab, click **Custom** and then set the following options:
 - **Memory Management** to Automatic Shared Memory Management.
 - **SGA Size** field to 1024.
 - **PGA Size** field to 768.

b) On the **Sizing** tab, set the following options:

- **Block Size** to 8192.
- **Processes** to 250.

c) On the **Character Sets** tab, select **Use Unicode (AL32UTF8)** and set the **National Character Set** option to **AL16UTF16 - Unicode UTF-16 Universal character set**.

You must create your database with the AL32UTF8 character set.

Add a local net service name for the OpenPages with Watson database

The database client uses a net service name to connect to the IBM OpenPages with Watson repository.

You must add a net service name, with the appropriate host, port, and service name details, for each server in the OpenPages with Watson deployment.

For more information on creating a net service name, see the Oracle documentation.

Setting the Oracle environment variables for the database server (Windows)

After you install the Oracle database server software, you must set the Oracle environment variables on the OpenPages database server computer.

Procedure

1. Log on to the database server as a user with administrative privileges.
2. In the Windows search box, type `environment variables`, and then click **Edit system environment variables**.
3. On the **Advanced** tab, click **Environment variables**.
4. In the **System Variables** pane, click **New**.
5. Add the `ORACLE_HOME` variable, then click **OK**.

`ORACLE_HOME` is the installation location or top-level directory structure for the database installation.

For example: `ORACLE_HOME=C:\app\Administrator\product\19.0.0\dbhome_1`

6. In the **System Variables** pane, select the `PATH` variable.
7. Verify that `%ORACLE_HOME%\bin` is included in the `PATH` variable.

If `%ORACLE_HOME%\bin` is not listed, click **Edit**, add `%ORACLE_HOME%\bin` to the start of the `PATH` variable, and then click **OK**.

By default, the `PATH` variable includes the path `%ORACLE_HOME%\bin` after you install the Oracle database server software.

8. Click **OK**.

Setting the Oracle environment variables for the database server (Linux)

After you install the Oracle database server software, you must set the Oracle environment variables on the OpenPages database server computer.

About this task

The following table lists the environment variables required for Linux operating systems.

Table 38. Oracle environment variables (Linux)	
Environment variables	Description
ORACLE_SID	Specifies the database service name. Restriction: The SID is case-sensitive in Linux environments.

Table 38. Oracle environment variables (Linux) (continued)

Environment variables	Description
ORACLE_HOME	Specifies the installation location or top-level directory structure for the database installation.
NLS_LANG	Specifies the database character set that is configured during the database installation. The default value is AMERICAN_AMERICA.AL32UTF8 Note: To display non-English characters for Japanese locales, set the variable to the following value: NLS_LANG=JAPANESE_JAPAN.JA16SJISTILDE
TNS_ADMIN	Specifies the location of the tnsnames.ora file. The default location is the <ORACLE_HOME>/network/admin directory.

Procedure

1. Log on to the database server as a user with administrative privileges.
2. Open the user profile, and set the ORACLE_SID, NLS_LANG, ORACLE_HOME, and TNS_ADMIN variables.

Important: Use the syntax and delimiters that are appropriate for the shell that you are using.

For example:

```
export ORACLE_SID=OP
export NLS_LANG=AMERICAN_AMERICA.AL32UTF8
export ORACLE_HOME=/home/oracle/app/oracle/product/19.0.0/dbhome_1
export TNS_ADMIN=$ORACLE_HOME/network/admin
```

3. Append the location of ORACLE_HOME/bin to the PATH environment variable.

For example:

```
export PATH=$ORACLE_HOME/bin:$PATH
```

4. Refresh the profile.

For example, open a shell and run the following command:

```
. /home/oracle/.bash_profile
```

Increasing the Oracle connection limit

In clustered environments, you must increase the number of users who can connect to the database instance.

Procedure

1. Log on to the database server as a user with administrative privileges.
2. To start the Oracle Enterprise Manager Database Express console, open a web browser and type `https://<oracle_server_name>:<oracle_port>/em`
3. Log on to the Oracle Enterprise Manager Database Express console by using the following syntax:
`sys/\ "<password>"@sysdba.`
 - a) For the **User Name**, enter sys.
 - b) Enter the password for the sys user.
 - c) From the **Connect As** list, select **SYSDBA**.
4. On the home page, click the **Server** tab.

5. Under **Database Configuration**, click **Initialization Parameters**.
6. On the **Initialization Parameters** page, click the **SPFile** tab.
7. Locate the **Processes** parameter.

If necessary, use the search function by entering Processes in the **Name** field and then clicking **Go**.

8. Enter a value in the **Processes** field.

In a clustered environment, for best performance allocate sufficient processes for each IBM OpenPages with Watson application instance and each corresponding Cognos instance.

For a two-node OpenPages with Watson environment, use the following settings:

OpenPages

Configure 75 processes for each OpenPages instance.

CommandCenter

Configure 80 processes for each OpenPages CommandCenter instance.

Database processing usage

Configure 60 processes for database connection processing and background processes.

By default, this setting is 250 processes and 280 sessions for a two-node OpenPages environment. If you have two or more application servers, increase the number of processes.

9. Click **Apply**.

You are prompted to restart the server.

10. To restart the server, select **Immediate**.

Starting and stopping the Oracle database server in a Windows environment

Use Windows services to start or stop the Oracle database instance.

Procedure

1. Log on to the database server as a user with administrative privileges.
2. Click **Start > Windows Administrative Tools > Services**.
3. Start the Oracle database listener service, which connects the user to the Oracle database instance.

To start the Oracle database instance, right-click the service name (OracleService<SID>) and select **Start**.

Testing the connections to the database server and the OpenPages database (Oracle)

Test whether the SQL*Net connect string can connect to the database listener by using the TNSPING utility in the <ORACLE_HOME>/bin directory. The TNSPING utility tests whether the listener is available. It does not test whether the databases behind the listener are working.

To test that the IBM OpenPages with Watson database is created, use SQL*Plus to log on to the OpenPages Oracle database schema.

Procedure

1. To test whether you can log on to Oracle Enterprise Manager, the web-based interface that is used to administer an Oracle database, type the following command:

```
https://<oracle_server_name>:<oracle_port>/em
```

2. To test whether a SQL*Net connect string can connect to the listener, type the following command:

```
tnsping <database_instance_name>
```

The utility requests acknowledgment that the service name is valid and that the listener is configured to handle requests for that service name.

If the configuration is correct, a message is displayed that shows the return time.

If the configuration is not correct, the utility returns an error message. Ensure that you use the correct service name and that the listener is started on the server computer.

3. To test that the OpenPages database is created, type the following command:

```
sqlplus <username>/\"<password>\"@<service_name>
```

For example, `sqlplus system/\"password\"@op`

The system connects you to an Oracle database instance.

4. To exit SQL*Plus, type `exit`.

Oracle database client installations

You install the Oracle database client on each IBM OpenPages with Watson application server and reporting server. The client software enables a server to connect to the Oracle database server remotely.

If the Oracle database server is installed on the same computer as the application server, the Oracle client software is not required.

You can use the Oracle Admin Client or the Oracle Instant Client (supported in 8.2.0.2 or later for Oracle 19c). The Oracle client software must be at the same version as your Oracle database server.

If you are using Linux, do the following tasks:

- [“Creating the user and group for application servers that use Oracle \(Linux\)” on page 99](#)
- Install the database client software

For information on installing the Oracle Admin Client software, see [“Oracle Admin Client” on page 108](#).

For information on installing the Oracle Instant Client software, see [“Oracle Instant Client” on page 101](#).

If you are using Windows, do the following tasks:

- Install the database client software

For information on installing the Oracle Admin Client software, see [“Oracle Admin Client” on page 108](#).

For information on installing the Oracle Instant Client software, see [“Oracle Instant Client” on page 101](#).

Creating the user and group for application servers that use Oracle (Linux)

To install the Oracle client and the IBM OpenPages with Watson application, you must create one user and one group.

About this task

To install the Oracle Admin client, create and configure the `oinstall` group and the `oracle` user on the server that hosts the OpenPages application.

Table 39. Required users and groups for application servers (Linux)			
User	Assign to Groups	Permissions	Reason
oracle	oinstall The primary group for the oracle user.	Read, write, execute permission to the Oracle Admin client installation directory.	Required by Oracle Admin client installation program. For information on creating standard Oracle users and user groups, see the Oracle documentation.

Table 39. Required users and groups for application servers (Linux) (continued)

User	Assign to Groups	Permissions	Reason
opuser	oinstall	<p>Read, write, execute permission to the following directories:</p> <ul style="list-style-type: none"> • <OP_HOME>/tmp directory. • Oracle Admin client installation directory and <ORACLE_HOME> directory. • Java SDK installation directory. • Cognos Analytics installation directory. <p>User must include <ORACLE_HOME>/bin in the path to run SQL*Plus commands.</p>	Required by the OpenPages installation.

Procedure

1. Log on to the application server as the root user and open a shell.
2. To create a group called oinstall, enter the following command:

```
groupadd oinstall
```

Restriction: The Oracle Admin Client installer requires that this group is named oinstall.

3. To create the oracle user and assign the user to the oinstall group, go to the /usr/sbin/ directory and enter the following command:

```
/usr/sbin/useradd -m -g oinstall oracle
```

Restriction: The Oracle Admin Client installer requires that this user is named oracle.

4. Use the following command to change the password for the oracle user:

```
passwd oracle
```

5. Enter a new password at the **New Password** prompt.
6. To install the OpenPages application, opuser must exist.

If this user does not already exist, create the user:

```
useradd -m -g oinstall <name>
```

If the user already exists, assign it to the oinstall group:

- a. Obtain the groups to which opuser belongs by using the `id opuser` command.
- b. Add the oinstall group to its supplementary groups:

```
usermod -G group1,group2,...,oinstall opuser
```

Example:

Run the command `id opuser`.

The output from the command window shows that `opuser` is assigned to the groups `opgroup` and `staff`:

```
uid=210(opuser) gid=206(opgroup) groups=1(staff)
```

Run the command `usermod -G staff,oinstall opuser`

Run the command `id opuser` to verify whether `opuser` has been assigned to the `oinstall` group successfully.

The output from the command window shows that `opuser` is assigned to the groups `staff` and `oinstall`:

7. If you created a new `opuser` in the previous step, change the password by using the following command:

```
passwd <name>
```

Restriction: The password cannot contain spaces or special characters.

8. At the **New Password** prompt, enter a new password.
9. Grant read, write, and execute permissions for `opuser` to the `ORACLE_HOME` directory. Run the following command by using `SQL*Plus`:

```
chmod -R 775 /home/oracle
```

10. Grant read, write and execute permissions for `opuser` to the Java SDK installation directory and the Cognos Analytics installation directory.

Oracle Instant Client

If you are using Oracle 19c, you can use the Oracle Instant Client (32-bit).

The steps that you need to do depend on your current version of IBM OpenPages with Watson and your installation path.

Fresh installations of 8.2.x

If you are doing a fresh installation of OpenPages 8.2, do the following steps:

1. Update the installation server to 8.2.0.2 or later.
2. When you install OpenPages, use the Oracle Instant Client. For information about installing Oracle Instant Client, see:
 - [“Installing the Oracle Instant Client \(Linux\)” on page 103](#)
 - [“Installing the Oracle Instant Client \(Windows\)” on page 104](#)
3. Verify that the environment variables are set. See [“Environment variables for Oracle Instant Client” on page 107](#).
4. Install Fix Pack 8.2.0.2 or later.

Your deployment temporarily uses a configuration that is not supported for end users. Do not allow end users to log in to OpenPages until you install Fix Pack 8.2.0.2 or later. Oracle Instant Client is not supported in earlier versions of OpenPages.

Migrating to 8.2.x

If you are upgrading to 8.2.x, do the following steps:

1. Update the installation server to 8.2.0.2 or later.
2. When you install OpenPages 8.2.0.0, use the Oracle Instant Client. For information about installing Oracle Instant Client, see:
 - [“Installing the Oracle Instant Client \(Linux\)” on page 103](#)
 - [“Installing the Oracle Instant Client \(Windows\)” on page 104](#)
3. Verify that the environment variables are set. See [“Environment variables for Oracle Instant Client” on page 107](#).

4. Upgrade the OpenPages database.
5. Continue with the migration to 8.2.
6. Install Fix Pack 8.2.0.2 or later.

Your deployment temporarily uses a configuration that is not supported for end users. Do not allow end users to log in to OpenPages until you install Fix Pack 8.2.0.2 or later. Oracle Instant Client is not supported in earlier versions of OpenPages.

Upgrading to 8.2.x

If you are upgrading to 8.2.x, do the following steps:

1. Update the installation server to 8.2.0.2 or later.
2. Install the Oracle Instant Client and update your configuration to use the Oracle Instant Client.

For more information, see:

- [“Installing the Oracle Instant Client \(Linux\)” on page 103](#)
 - [“Installing the Oracle Instant Client \(Windows\)” on page 104](#)
3. Verify that the environment variables are set. See [“Environment variables for Oracle Instant Client” on page 107](#).
 4. Open the `deploy.properties` file in a text editor. For each application server and reporting server, update the `db_client_directory` property to point to the Oracle Instant Client.
 5. Continue with the upgrade to 8.2.
 6. Install Fix Pack 8.2.0.2 or later.

Your deployment temporarily uses a configuration that is not supported for end users. Do not allow end users to log in to OpenPages until you install Fix Pack 8.2.0.2 or later. Oracle Instant Client is not supported in earlier versions of OpenPages.

Updating from 8.2.0.x to 8.2.0.2 or later

If you are already using 8.2.0.0 or 8.2.0.1, do the following steps:

1. Update the installation server to 8.2.0.2 or later.
2. Install the Oracle Instant Client and update your configuration to use it.

For more information, see:

- [“Installing the Oracle Instant Client \(Linux\)” on page 103](#)
 - [“Installing the Oracle Instant Client \(Windows\)” on page 104](#)
3. Verify that the environment variables are set. See [“Environment variables for Oracle Instant Client” on page 107](#).
 4. In the installation app, open your deployment and update application server cards and reporting server cards to point to the Oracle Instant Client. Click **Validate**.
 5. Install Fix Pack 8.2.0.2 or later.

Your deployment temporarily uses a configuration that is not supported for end users. Do not allow end users to log in to OpenPages until you install Fix Pack 8.2.0.2 or later. Oracle Instant Client is not supported in earlier versions of OpenPages.

After 8.2.0.2 or later is installed

If you are using 8.2.0.2 or later, you can switch to the Oracle Instant Client at any time.

1. Install the Oracle Instant Client and update your configuration to use it.

For more information, see:

- [“Installing the Oracle Instant Client \(Linux\)” on page 103](#)
 - [“Installing the Oracle Instant Client \(Windows\)” on page 104](#)
2. Verify that the environment variables are set. See [“Environment variables for Oracle Instant Client” on page 107](#).

3. In the installation app, open your deployment and update application server cards and reporting server cards to point to the Oracle Instant Client. Click **Validate**.

Installing the Oracle Instant Client (Linux)

You can use the Oracle Instant Client. Fix pack 8.2.0.2 adds support for the Oracle Instant Client.

Before you begin

Review the following topic to verify the requirements based on your installation path: [“Oracle Instant Client” on page 101](#).

Ensure that the required users and groups are created. See [“Creating the user and group for application servers that use Oracle \(Linux\)” on page 99](#).

The libaio package is required. For more information, see the Oracle documentation.

Procedure

1. Log on to the application server.
2. Download the 64-bit Instant Client Basic Package, SQL*Plus Package, and the Tools Package. For example:

- instantclient-basic-linux.64-19.9.0.0.0dbru.zip
- instantclient-sqlplus-linux.64-19.9.0.0.0dbru.zip
- instantclient-tools-linux.64-19.9.0.0.0dbru.zip

3. As the oracle user, create a new directory for the Oracle client home directory, ORACLE_HOME. For example:

```
mkdir /home/oracle
```

The following steps use /home/oracle. If you are using a different path, replace /home/oracle with your directory.

4. Copy the Instant Client package files into the directory that you created in step 3, and then expand the files.

```
cd /home/oracle
unzip instantclient-basic-linux.x64-19.9.0.0.0dbru.zip
unzip instantclient-sqlplus-linux.x64-19.9.0.0.0dbru.zip
unzip instantclient-tools-linux.x64-19.9.0.0.0dbru.zip
```

You now have a /home/oracle/instantclient_19_9 directory.

5. Copy the sqlplus and ojdbc8.jar files to the correct locations by running the following commands:

```
mkdir -p /home/oracle/instantclient_19_9/bin
cp /home/oracle/instantclient_19_9/sqlplus /home/oracle/instantclient_19_9/bin
mkdir -p /home/oracle/instantclient_19_9/jdbc/lib
cp /home/oracle/instantclient_19_9/ojdbc8.jar /home/oracle/instantclient_19_9/jdbc/lib
```

6. As opuser, set the following environment variables in the current shell and in the login profile.

```
ORACLE_BASE=/home/oracle/instantclient_19_9/
ORACLE_HOME=/home/oracle/instantclient_19_9/
LD_LIBRARY_PATH=$ORACLE_HOME
JAVA_HOME=<path_to_java_home>
PATH=$PATH:$ORACLE_HOME:$ORACLE_HOME/bin:$JAVA_HOME/bin
export ORACLE_BASE ORACLE_HOME PATH LD_LIBRARY_PATH JAVA_HOME
```

Important: Use the syntax and delimiters that are appropriate for the shell that you are using.

7. Create a /network/admin directory.

```
mkdir -p /home/oracle/instantclient_19_9/network/admin
```

8. Copy the `tnsnames.ora` file from the database server, update it, and then test the database connection.

For more information, see [“Testing the connection to the OpenPages database from the Oracle database client” on page 110.](#)

Create an `sqlnet.ora` file, if needed.

9. Update property files with the new Oracle client directory, `/home/oracle/instantclient_19_9/`.

For more information, see [“Update database client paths in property files” on page 105.](#)

Note: If you are doing a fresh installation of OpenPages, skip this step.

10. Repeat these steps on each application server.
11. Repeat these steps on each reporting server, with the following differences:
 - In step 2, use the 32-bit client packages.
 - In step 6, set the environment variables by using the steps in [“Setting database environment variables for the reporting server on Linux operating systems” on page 122.](#)
 - After step 9, restart the Reporting Framework Generator service. See [“Starting and stopping the OpenPages with Watson Framework Model Generator service on Linux” on page 318.](#)

What to do next

See the following topic to determine your next task: [“Oracle Instant Client” on page 101.](#)

Installing the Oracle Instant Client (Windows)

You use the Oracle Instant Client. Fix pack 8.2.0.2 adds support for the Oracle Instant Client.

Before you begin

Review the following topic to verify the requirements based on your installation path: [“Oracle Instant Client” on page 101.](#)

Download and install the Visual Studio Redistributable from Microsoft. For example, Oracle Instant Client 19 requires the Visual Studio 2017 Redistributable. For more information, see the Oracle documentation.

Procedure

1. Log on to the application server as an administrator.
2. Download the 64-bit Instant Client Basic Package, SQL*Plus Package, and the Tools Package.
For example:
 - `instantclient-basic-windows.x64-19.9.0.0.0dbru.zip`
 - `instantclient-sqlplus-windows.x64-19.9.0.0.0dbru.zip`
 - `instantclient-tools-windows.x64-19.9.0.0.0dbru.zip`
3. Create a new directory for the Oracle client home directory, `ORACLE_HOME`.
For example:

```
C:\oracle\
```

The following steps use `C:\oracle\`. If you are using a different path, replace `C:\oracle\` with your directory.

4. Expand the Instant Client packages into the same directory under `C:\oracle\`.
You now have a `C:\oracle\instantclient_19_9` directory.
5. In `C:\oracle\instantclient_19_9`, create a `\bin` directory.
You now have:

```
C:\oracle\instantclient_19_9\bin
```

6. Copy the contents of C:\oracle\instantclient_19_9 to C:\oracle\instantclient_19_9\bin.
Ensure that you copy the files. Do not cut and paste them.
7. In C:\oracle\instantclient_19_9, create a \jdbc\lib directory.
You now have:

```
C:\oracle\instantclient_19_9\jdbc\lib
```

8. Copy C:\oracle\instantclient_19_9\ojdbc8.jar to the C:\oracle\instantclient_19_9\jdbc\lib directory.
9. Set the following environment variables:

```
ORACLE_BASE=C:\oracle\instantclient_19_9
ORACLE_HOME=C:\oracle\instantclient_19_9
JAVA_HOME=<path_to_java_home>
```

Append the following directory to the PATH environment variable:

```
C:\oracle\instantclient_19_9\bin
```

10. In the C:\oracle\instantclient_19_9 directory, create a \network\admin directory.
You now have

```
C:\oracle\instantclient_19_9\network\admin
```

11. Copy the tnsnames.ora file from the database server, update it, and then test the database connection.
For more information, see [“Testing the connection to the OpenPages database from the Oracle database client”](#) on page 110.
12. Update property files with the new Oracle client directory, C:\oracle\instantclient_19_9.
For more information, see [“Update database client paths in property files”](#) on page 105.
Note: If you are doing a fresh installation of OpenPages, skip this step.
13. Repeat these steps on each application server.
14. Repeat these steps on each reporting server, with the following differences:
 - In step 2, use the 32-bit client packages.
 - In step 9, set the environment variables by using the steps in [“Setting database environment variables for reporting servers on Windows operating systems”](#) on page 123.
 - After step 12, restart the Reporting Framework Generator service. See [“Starting and stopping the OpenPages with Watson Framework Model Generator service on Windows”](#) on page 318.

What to do next

See the following topic to determine your next task: [“Oracle Instant Client”](#) on page 101.

Update database client paths in property files

If you change the Oracle client software from the Admin Client to the Instant Client, you need to update the database client paths in property files.

Application servers

Update the following files:

<OP_HOME>/aurora/bin/op-backup-restore.env

Set ORACLE_SQLPLUS to the location of the sqlplus command.

Examples:

- ORACLE_SQLPLUS=/home/oracle/instantclient_19_9/sqlplus

- ORACLE_SQLPLUS=C:/oracle/instantclient_19_9/sqlplus.exe

<OP_HOME>/aurora/bin/op-backup-restore-env.sh|cmd

- Set ORACLE_HOME.

Examples:

- ORACLE_HOME=/home/oracle/instantclient_19_9
- ORACLE_HOME=C:/oracle/instantclient_19_9

- For Linux, change the Oracle home portion of PATH to the new location. For example, replace

```
PATH=$JAVA_HOME/bin:$ANT_HOME/bin:/home/oracle/app/product/19.3/client_1/bin:$OP_HOME/aurora/bin:$PATH; export PATH
```

With

```
PATH=$JAVA_HOME/bin:$ANT_HOME/bin:/home/oracle/instantclient_19_9:$OP_HOME/aurora/bin:$PATH; export PATH
```

Reporting servers

Update the following files:

<COGNOS_HOME>/bin/BmtScriptPlayer.sh (Linux only)

- Set ORACLE_HOME.

Example:

```
export ORACLE_HOME=/home/oracle/instantclient_19_9
```

- Change the Oracle home portion of LD_LIBRARY_PATH to the new location.

For example, replace

```
export LD_LIBRARY_PATH=/home/opuser/IBM/cognos/analytics/bin:/home/opuser/IBM/cognos/analytics:/home/oracle/app/product/19.3/client_1/lib
```

With:

```
export LD_LIBRARY_PATH=/home/opuser/IBM/cognos/analytics/bin:/home/opuser/IBM/cognos/analytics:/home/oracle/instantclient_19_9
```

- Set TNS_ADMIN to the <Oracle_Home>/network/admin directory.

Example:

```
export TNS_ADMIN=/home/oracle/instantclient_19_9/network/admin
```

<CC_HOME>/framework/conf/framework.properties

Before you edit this file, stop the Reporting Framework Generator service. Restart the service after you complete these updates.

- Set oracle.client.path to the Oracle home directory.

For example:

```
oracle.client.path = /home/oracle/instantclient_19_9
```

Or,

```
oracle.client.path = C:/oracle/instantclient_19_9
```

<CC_Home>/tools/bin/op-cc-backup-restore.env

- Set ORACLE_SQLPLUS to the location of the sqlplus command.

For example:

```
ORACLE_SQLPLUS=/home/oracle/instantclient_19_9/sqlplus
```

Or,

```
ORACLE_SQLPLUS=C:/oracle/instantclient_19_9/sqlplus.exe
```

<CC_Home>/tools/bin/op-cc-backup-restore-env.sh|cmd

- Set ORACLE_HOME.

For example:

```
ORACLE_HOME=/home/oracle/instantclient_19_9
```

Or,

```
ORACLE_HOME=C:/oracle/instantclient_19_9
```

- Change the Oracle home portion of PATH to the new location.

For Linux, replace:

```
PATH=$JAVA_HOME/bin:$ANT_HOME/bin:/home/oracle/app/product/19.3/client_1/bin:$PATH;  
export PATH
```

With

```
PATH=$JAVA_HOME/bin:$ANT_HOME/bin:/home/oracle/instantclient_19_9:$PATH; export PATH
```

For Windows replace:

```
set PATH=.;%JAVA_HOME%/bin;%ANT_HOME%/bin;C:/oracle/product/19.3.0.0/client_1/bin;
```

With

```
set PATH=.;%JAVA_HOME%/bin;%ANT_HOME%/bin;C:/oracle/instantclient_19_9;
```

Environment variables for Oracle Instant Client

On each application server and reporting server, you need to set environment variables for the Oracle Instant Client.

Application servers

Linux

Verify that the following environment variables are set in the current shell and in the login profile:

```
ORACLE_BASE=/home/oracle/instantclient_19_9  
ORACLE_HOME=/home/oracle/instantclient_19_9  
LD_LIBRARY_PATH=$ORACLE_HOME  
JAVA_HOME=<path_to_java_home>  
PATH=$PATH:$ORACLE_HOME:$ORACLE_HOME/bin:$JAVA_HOME/bin
```

Windows

Verify that the following environment variables are set:

```
ORACLE_BASE=C:\oracle\instantclient_19_9  
ORACLE_HOME=C:\oracle\instantclient_19_9  
JAVA_HOME=<path_to_java_home>
```

Verify that the PATH environment variable includes the <ORACLE_HOME>\bin directory. For example: C:\oracle\instantclient_19_9\bin.

Reporting servers

These examples show the Oracle client, Java, and Path environment variables that you need to verify when you install the Instant Client. When you install Cognos, you need to set additional environment variables.. For more information, see:

- [“Setting database environment variables for the reporting server on Linux operating systems” on page 122](#)
- [“Setting database environment variables for reporting servers on Windows operating systems ” on page 123](#)

Linux

Verify that the following environment variables are set in the current shell and in the login profile:

```
ORACLE_HOME=/home/oracle/instantclient_19_9
TNS_ADMIN=/home/oracle/instantclient_19_9/network/admin
JAVA_HOME=<path_to_java_home>
PATH=$PATH:$ORACLE_HOME:$ORACLE_HOME/bin:$JAVA_HOME/bin
```

Windows

Verify that the following environment variables are set:

```
ORACLE_HOME=C:\oracle\instantclient_19_9
TNS_ADMIN=C:\oracle\instantclient_19_9\network\admin
JAVA_HOME=<path_to_java_home>
```

Verify that the PATH environment variable includes the <ORACLE_HOME>\bin directory. For example: C:\oracle\instantclient_19_9\bin.

Oracle Admin Client

You can use the Oracle Admin Client.

Install the Oracle Admin Client on all application servers and reporting server. For information about installing Oracle Admin Client, see the Oracle documentation.

If you are installing IBM OpenPages with Watson on a single server, you need to do some additional steps. See [“Configuring IBM OpenPages with Watson to work on a single computer with an Oracle database” on page 109](#).

Setting the ORACLE_HOME environment variable on the OpenPages application servers (Linux)

Set up the ORACLE_HOME environment variable to point to the directory where the Oracle database client software is installed. Set the variable on the admin application server and each non-admin application server.

Procedure

1. Log on to the application server. Log on as a non-root user, such as the opuser user that you created for the IBM OpenPages with Watson installation.
2. Open the user profile.

For example:

```
/home/<user>/ .bash_profile
```

Where <user> is the person who logs in to the operating system and creates the OpenPages installation, for example opuser.

3. Set the ORACLE_HOME environment variable to point to the Oracle Admin Client installation directory.

Important: Use the syntax and delimiters that are appropriate for the shell that you are using.

For example:

```
export ORACLE_HOME=/home/oracle/app/oracle/product/19.0.0/client_1
```

4. Append the location of ORACLE_HOME/bin to the PATH environment variable.

For example:

```
export PATH=$ORACLE_HOME/bin:$PATH
```

5. Refresh the profile.

For example:

```
. /home/opuser/.bash_profile
```

Setting the ORACLE_HOME environment variable on the OpenPages application servers (Windows)

Set up the ORACLE_HOME environment variable to point to the directory where the Oracle database client software is installed. Set the variable on the admin application server and each non-admin application server.

Procedure

1. Log on to the application server as a user with administrative privileges and full access to the local server drives..
2. In the Windows search box, type `environment variables`, and then click **Edit system environment variables**.
3. On the **Advanced** tab, click **Environment variables**.
4. In the **System Variables** pane, click **New**.
5. Add the ORACLE_HOME variable, then click **OK**.

For example: ORACLE_HOME=C:\app\Administrator\product\19.0.0\client_1

6. In the **System Variables** pane, select the PATH variable.
7. Verify that %ORACLE_HOME%\bin is included in the PATH variable.

If %ORACLE_HOME%\bin is not listed, click **Edit**, add %ORACLE_HOME%\bin to the start of the PATH variable, and then click **OK**.

By default, the PATH variable includes the path %ORACLE_HOME%\bin after you install the Oracle database server software.

Configuring IBM OpenPages with Watson to work on a single computer with an Oracle database

For test and development environments, you can install IBM OpenPages with Watson, the Oracle database, the 32-bit Oracle client software, and Cognos Analytics on a single computer. However, some configuration is required.

About this task

You can install IBM OpenPages with Watson on a single computer for pre-deployment testing or proof of concept demonstrations. For single computer installations, ensure that the correct Oracle client software is used by each software component.

If you install IBM OpenPages with Watson on a single server, you must install two versions of the Oracle client software. Both the 32-bit and 64-bit versions are required. The OpenPages application requires the 64-bit Oracle client and the Cognos Analytics software requires the 32-bit Oracle client software.

When you install IBM OpenPages with Watson, use the 64-bit client. After the installation is complete, do the steps in this task to set up the 32-bit Oracle client for Cognos Analytics.

Procedure

1. Log on to the Cognos server as a user with administrative privileges.
2. Ensure that the ORACLE_HOME environment variable points to the 32-bit Oracle client software.

3. Edit the PATH variable to add %ORACLE_HOME%\bin.
4. If set, remove the TNS_ADMIN variable.
5. From the command line, go to the <CC_HOME>/framework/conf directory.
6. Open the framework.properties file in a text editor and ensure that the **oracle.client.path** property contains the location of the 32-bit Oracle client bin directory.
7. Save and close the file.

Note: If the server is Windows, ensure that the PATH system environment variable contains the path to the Oracle server and not the Oracle client to avoid issues that can occur on server restarts.

8. Restart the IBMOpenPagesFrameworkModelGenerator service.

Testing the connection to the OpenPages database from the Oracle database client

Test whether the SQL*Net connect string can connect to the IBM OpenPages with Watson database on the Oracle database server from the Oracle database client.

Procedure

1. Copy the file <ORACLE_HOME>/network/admin/tnsnames.ora from the Oracle database server operating system to the <ORACLE_HOME>/network/admin Oracle database client directory on the application server or reporting server.

Ensure that the OpenPages installation user has read, write and execute permissions on the tnsnames.ora file in the Oracle database client operating system.

2. Log on to the application server or reporting server as an OpenPages installation user.
3. Edit the file <ORACLE_HOME>/network/admin/tnsnames.ora, and update the Host value to the host name or IP address of the Oracle database server.
4. To test the connection to the OpenPages database on the database server, type the following command:

```
sqlplus <username>/\"<password>\"@<service_name>
```

For example, sqlplus system/\"password\"@op

The system connects you to an Oracle database instance.

5. To exit SQL*Plus, type exit.

Checklist for reporting servers

Do the following tasks on each reporting server (active and standby) before you install IBM OpenPages with Watson:

- Check that all of the required ports are available. See [“Port assignments” on page 124](#).
- If you are using Linux, give the OpenPages installation user (opuser) read, write, and execute permissions to the following directories:
 - Java SDK or JRE installation directory
 - Cognos Analytics installation directory
- If you are using a horizontal cluster for the reporting servers, set up the load balancer.
- If the database server is on a separate computer, install the database client software (32-bit version) on each reporting server and test the connection.
 - If you are using IBM Db2, see [“Db2 database client installations” on page 85](#).
 - If you are using Oracle, see [“Oracle database client installations” on page 99](#).
- Install and configure a web server. See [“Web server configuration options for Cognos Analytics” on page 115](#).
- If you are using Linux, ensure that you have the 32-bit and 64-bit libraries required by Cognos.

- Install Cognos Analytics, 32-bit version. See [“Installing Cognos Analytics”](#) on page 112.
 - Optional: Include the Cognos Framework Manager when you install Cognos Analytics.
- Copy the JDBC driver to the reporting servers.
- Configure the connection to the content store.
 - If you are using IBM Db2, see [“Configuring a connection to the content store \(Db2\)”](#) on page 117.
 - If you are using Oracle, see [“Configuring a connection to the content store \(Oracle\)”](#) on page 118.
- Start Cognos services. See [“Saving your settings and starting the IBM Cognos services”](#) on page 120.
- Prepare the server for IBM OpenPages CommandCenter.
 - If you are using IBM Db2 for the Cognos database, enable a connection between CommandCenter and the database server. See [“Enabling the connection to a Db2 database from the OpenPages CommandCenter computer”](#) on page 121.
 - If you are using Oracle for the Cognos database, do the following tasks:
 - Set environment variables for CommandCenter on each reporting server.
 - Test the connection to the OpenPages database on the database server.

Installing IBM Installation Manager

This task is optional. Do this task if you plan to install IBM HTTP Server, IBM OpenPages SDI Connector for UCF Common Controls Hub, or IBM OpenPages Loss Event Entry.

Install IBM Installation Manager on each application server and reporting server.

Ensure that you install the 64-bit version of IBM Installation Manager.

If an older version of IBM Installation Manager is installed, install to a new directory. For more information about this requirement, see [Update to Installation Manager 1.8 is blocked when its data location is within its install location](#).

For more information about IBM Installation Manager, see the [Installation Manager documentation](#).

Procedure

1. Download IBM Installation Manager from [Passport Advantage](#).
2. Run the installation program.
 - Microsoft Windows: Double-click `install.exe`.
 - Linux: Open a terminal window, and then run `./install`.
3. Follow the steps to install IBM Installation Manager.

Cognos Analytics installations

Cognos Analytics and OpenPages CommandCenter must be installed on the reporting server.

For more information about IBM OpenPages with Watson supported software, see [“Software prerequisites”](#) on page 33.

Reporting server distribution options

For light user loads, with fewer than 50 concurrent users, Cognos Analytics and OpenPages CommandCenter can be installed on the same computer as the OpenPages application server.

For heavier user loads, install Cognos Analytics and CommandCenter on a different computer than the OpenPages application servers. OpenPages with Watson operates at peak performance when the database server, application server, and the reporting server are installed on separate computers.

Requirements for installing Cognos Analytics in a Linux environment

Cognos Analytics requires specific Linux packages.

For more information, see the [Software Product Compatibility Report](#) for Cognos Analytics.

Requirements for running multiple instances of Cognos Analytics on the same computer

If you want to install multiple instances of Cognos Analytics on the same computer, you must change the configuration to ensure that the instances do not share port numbers or other resources. For more information, see [Configuration settings that are the same for multiple versions on the same server](#) in the IBM Cognos documentation.

Database server requirements for OpenPages with Watson and Cognos Analytics

If you are using an IBM Db2 database server, you must use two separate databases - one for the IBM Cognos content store, and a second one for the IBM OpenPages with Watson database.

If you are using an Oracle database server, for best performance, use separate databases for the content store and the IBM OpenPages with Watson database.

Installing Cognos Analytics

Before you install IBM OpenPages with Watson components, ensure that Cognos Analytics is installed and running on your reporting server computer.

For more information, see the *IBM Cognos Analytics Installation and Configuration Guide* in IBM Documentation.

Before you begin

Review the following notes:

Java

In previous versions, you needed to install Java from the IBM OpenPages with Watson installation media. This step is no longer required. IBM Runtime Environment for Java is provided with Cognos Analytics.

On all operating systems, if the Cognos Analytics installation program does not find Java 8 in the PATH environment variable, the installer automatically points to the Java that is provided with Cognos Analytics. In version 11.1.5 and later the location is `<COGNOS_HOME>/ibm-jre/jre`.

Important: If you want to use your own Java, ensure that it meets the Java requirements for Cognos. For more information, see the [Cognos documentation](#).

Oracle

Verify that the database client software is at the same version as the Oracle database server software. For example, if you are using Oracle 12.2 on the database server, use the Oracle 12.2 client on the reporting servers.

Restriction: Do not install the database client software into a directory with spaces.

If you use Oracle and the OpenPages database is installed on a separate computer than the Cognos Analytics server, ensure that a 32-bit database client is installed on the Cognos Analytics server.

If you are using an Oracle database on the same computer as Cognos Analytics, you must update your environment variables so that the IBM Cognos service uses the 32-bit Oracle libraries, and the Oracle server uses the 64-bit libraries.

IBM Db2

If you are using IBM Db2, install the 64-bit database client, which also includes the 32-bit client software.

Linux

Ensure that the dependent 32-bit and 64-bit libraries are installed.

To create the user variables for the IBM Cognos service, do the following tasks:

- Create a user variable that is named ORACLE_HOME and set its value to the 32-bit Oracle Admin client home.

For example, on Microsoft Windows operating systems, set the ORACLE_HOME user variable to C:\oracle\product\19.0.0\client_1.

- Create a user variable that is named PATH, or append to an existing one, and include the 32-bit Oracle Admin client home.

For example, on Windows, set the PATH user variable to %ORACLE_HOME%\bin;%PATH%.

- Add <ORACLE_HOME>/lib to the system libraries variable.

Linux: Update the LD_LIBRARY_PATH environment variable: LD_LIBRARY_PATH=\$ORACLE_HOME/lib:\$LD_LIBRARY_PATH

The 64-bit IBM Db2 database installation includes libraries for both 32-bit and 64-bit systems. Add the path to the Db2 32-bit server libraries.

- Linux: Update the LD_LIBRARY_PATH environment variable LD_LIBRARY_PATH=\$DB2DIR/lib32:\$LD_LIBRARY_PATH

Procedure

1. Optional: If you have an earlier version of Cognos, back up the content store.
2. Ensure that a web server is installed.

For more information, see [“Prerequisite software for reporting servers” on page 37](#).

3. On the reporting server, install Cognos Analytics.

- a) Install Cognos Analytics.

Restriction: Install Cognos Analytics into a directory that contains only ASCII characters in the path name. Do not install Cognos Analytics into a directory that contains spaces.

For information about installing Cognos Analytics, see the following topics in the Cognos documentation:

- [Installing server components on Windows operating systems](#)
- [Installing on UNIX or Linux operating systems](#)

- b) Install Framework Manager.

Framework Manager is not required in production environments. Framework Manager is the modeling tool for creating and managing business-related metadata.

Restriction: If you need Framework Manager in your development environment, you must install the 64-bit IBM Cognos server and the 32-bit Framework Manager to different directories. The default installation locations for 32 and 64-bit IBM Cognos components are different. For more information about installing Framework Manager, see [IBM Cognos Framework Manager](#) in the IBM Cognos documentation.

4. Copy the JDBC database driver to the <COGNOS_HOME>/drivers directory.
 - If the content store is an Oracle 12.2.0.1, 18c, or 19c database, copy the ojdbc8.jar file from the Oracle installation, <ORACLE_HOME>/jdbc/lib.
 - If the content store is a Db2 database, copy the db2jcc4.jar and db2jcc_license_cu.jar files from the IBM Db2 installation, <DB2_HOME>/sql11ib/java.
5. Append the <COGNOS_HOME>/bin64 directory to the library path environment variable.
 - On Linux operating systems, update the LD_LIBRARY_PATH environment variable.

Example: export LD_LIBRARY_PATH=/opt/ibm/cognos/analytics/
bin64:\$LD_LIBRARY_PATH

6. Append the <COGNOS_HOME>/bin64 directory to the PATH environment variable.

Example: export LD_LIBRARY_PATH=\$LD_LIBRARY_PATH:/opt/ibm/cognos/analytics/
bin64

7. Verify that JAVA_HOME is set in the system environment variables.

Set JAVA_HOME to <COGNOS_HOME>/ibm-jre/jre/bin

Do this step on each reporting server in your deployment (active and standby).

If the reporting server is installed on the same computer as the application server, you can skip this step.

8. If you are using an Oracle database on the same computer as Cognos Analytics, update the IBM Cognos service settings to the user account for which you created the user variables for the 32-bit Oracle libraries.
 - a) Click **Start > Windows Administrative Tools > Services**.
 - b) Right-click the IBM Cognos service, select **Properties**, and click the **Log On** tab.
 - c) Select **This Account**, and select the user account for which you created the user variables for the 32-bit Oracle libraries.

Upgrading Cognos

Upgrade to a supported version of Cognos Analytics.

About this task

If you are using Cognos 11.0.x or 11.1.x, you can upgrade Cognos in-place.

After you upgrade Cognos, copy the bcprov-jdk15to18-1.68.jar file that is provided with IBM OpenPages with Watson to the Java location that is used by the IBM Cognos server, and then register the BouncyCastleProvider in the JRE master security provider file, java.security.

Note the following recent name changes:

- bcprov-jdk14-145.jar is bcprov-jdk15to18-1.68.jar in 8.2.0.2 or later
- org.bouncycastle145.jce.provider.BouncyCastleProvider is org.bouncycastle.jce.provider.BouncyCastleProvider in 8.2.0.2 or later
- CAMCryptoBC is BC in 8.2.0.2 or later

Procedure

1. Log on to the reporting server as a user with administrative privileges.
2. Stop all Cognos services.
3. Upgrade Cognos Analytics. See [Upgrading your current version of Cognos Analytics 11](#).
4. Locate the bcprov-jdk15to18-1.68.jar file.

The file is available on each application server in the <OP_HOME>/temp/jre/lib/ext/ directory.

5. If the Cognos software is using the JRE that is installed with Cognos, do the following steps:

- a) Copy the bcprov-jdk15to18-1.68.jar file to the <COGNOS_HOME>/analytics/jre/lib/ext directory.

Note: If you are using Cognos Analytics 11.1.5 or later, copy the file to <COGNOS_HOME>/analytics/ibm-jre/lib/ext.

- b) Register the BouncyCastleProvider in the JRE master security provider file, if it is not already registered.

To register the provider, add the following line to the `java.security` file that is stored in the `<COGNOS_HOME>/analytics/jre/lib/security` directory.

```
security.provider.<#>=
    org.bouncycastle.jce.provider.BouncyCastleProvider
```

Note: If you are using Cognos Analytics 11.1.5 or later, the `java.security` file is in the `<COGNOS_HOME>/analytics/ibm-jre/lib/security` directory.

Where: The number sign, `<#>`, is one increment above the last number in the list. For example, `security.provider.9`.

6. If the Cognos software is using the JRE that is installed with IBM SDK, Java Technology Edition, do the following steps:

- a) Copy the `bcprov-jdk15to18-1.68.jar` file to the `<JAVA_HOME>/lib/ext` directory.
- b) Register the `BouncyCastleProvider` in the JRE master security provider file, if it is not already registered.

To register the provider, add the following line to the `java.security` file that is stored in the `<JAVA_HOME>/lib/security` directory.

```
security.provider.<#>=
    org.bouncycastle.jce.provider.BouncyCastleProvider
```

Where: The number sign, `<#>`, is one increment above the last number in the list. For example, `security.provider.9`.

7. If the Cognos software is using a JRE that is installed in another location on the reporting server, do the following steps:

Replace `<JAVA_LOCATION>` with the directory where the JRE is installed.

- a) Copy the `bcprov-jdk15to18-1.68.jar` file to the `<JAVA_LOCATION>/lib/ext` directory.
- b) Register the `BouncyCastleProvider` in the JRE master security provider file, if it is not already registered.

To register the provider, add the following line to the `java.security` file that is stored in the `<JAVA_LOCATION>/lib/security` directory.

```
security.provider.<#>=org.bouncycastle.jce.provider.BouncyCastleProvider
```

Where: The number sign, `<#>`, is one increment above the last number in the list. For example, `security.provider.9`.

8. Restart the reporting servers.
9. If you upgraded to 11.1.5 or later and you are using the JRE that is installed with Cognos, you need to update the Java location.

In Cognos Analytics 11.1.5 and later, the path is:

- On Windows: `C:\IBM\cognos\analytics\ibm-jre\jre`
- On Linux: `/usr/IBM/cognos/analytics/ibm-jre/jre`

For more information, see [How to Change the Java Location on an OpenPages Reporting Server](#).

10. If you upgraded to 11.1.5 or later and you are using the JRE that is installed with Cognos, re-import the OpenPages SSL certificates into the Cognos JRE.

For more information, see the *IBM OpenPages with Watson Administrator's Guide*.

Web server configuration options for Cognos Analytics

You must configure your web server before users can connect to the Cognos Analytics portal.

For more information, see the following topics in the Cognos Analytics documentation:

- [Configure Cognos Analytics with your web server](#)

- [Configure Apache HTTP Server or IBM HTTP Server](#)

The configuration for these web servers has changed in IBM Cognos Analytics V11.1 and later. See the following topic for an example of the configuration: [“Configuring Apache Web Server or IBM HTTP Server” on page 116](#)

- [Configuring IIS in Cognos Analytics](#)

If you are using Microsoft Internet Information Services (IIS) on Windows, see the following [technote](#) for information about how to use a script to do the configuration.

Consider the following guidelines:

- Use compiled gateways for production systems

For production systems, you can improve performance by changing the gateway from the default CGI gateway.

- Use CGI gateways

You can use the CGI gateway on IBM HTTP Server, Apache Web Server, or Microsoft Internet Information Services (IIS) Server. Cognos Analytics is configured to use the CGI gateway by default.

- Configure WebDAV to view and browse images

To view and browse images in the Cognos Analytics, configure Web Distributed Authoring and Versioning (WebDAV) on your web server. Report authors can browse for images to include in reports in a way that is similar to browsing a file system.

Configuring Apache Web Server or IBM HTTP Server

You must configure the Cognos Analytics gateway on your web server.

Procedure

1. Log on to the web server as a user with administrative privileges.
2. From the command prompt, go to the `<Webserver_installation>/conf/` directory.
3. Make a backup copy of the `httpd.conf` file and rename the file to: `httpd.conf.original`.
4. Open the `httpd.conf` file in a text editor.
5. Configure the virtual directories by adding the following lines to the end of the `httpd.conf` file.

For example, on Linux:

```
LoadModule headers_module modules/mod_headers.so
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_http_module modules/mod_proxy_http.so

<Location /ibmcognos/bi>
RequestHeader set X-BI-PATH /ibmcognos/bi/v1
ProxyPass http://op-server.com:9300/bi
ProxyPassReverse http://op-server.com:9300/bi
ProxyPassReverseCookieDomain . ibm.com
</Location>

ScriptAlias /ibmcognos/cgi-bin /home/opuser/IBM/cognos/analytics/cgi-bin
<Directory /home/opuser/IBM/cognos/analytics/cgi-bin>
AllowOverride FileInfo
Options FollowSymLinks
Require all granted
</Directory>

Alias /ibmcognos/help /home/opuser/IBM/cognos/analytics/webcontent/documentation
<Directory /home/opuser/IBM/cognos/analytics/webcontent/documentation>
AllowOverride FileInfo
Options FollowSymLinks
Require all granted
</Directory>

Alias /ibmcognos /home/opuser/IBM/cognos/analytics/webcontent
<Directory /home/opuser/IBM/cognos/analytics/webcontent>
AllowOverride FileInfo
Options FollowSymLinks
```

```
Require all granted
</Directory>
```

Note: Ensure that you define the `/ibmcognos/cgi-bin` alias before the `/ibmcognos` alias.

6. Save and close the file.
7. Restart the web server.

Configuring a connection to the content store (Db2)

After you install Cognos Analytics, configure a connection to the content store database.

Important: The content store database must be in a separate database instance than the IBM OpenPages with Watson database. Oracle compatibility mode must not be enabled for the IBM Db2 database instance that is used for the content store.

Before you begin

Ensure that you copied the following files from the `<DB2_HOME>/sqlllib/java` directory to the `<COGNOS_HOME>/drivers` directory:

- `db2jcc4.jar`
- `db2jcc_license_cu.jar`

Procedure

1. Log on to the reporting server as a user with administrator privileges.

Note: For Windows installations, the user must belong to the DB2ADMINS group. For Linux installations, the user must belong to the db2iadm group.

2. Start Cognos Configuration.

- On Windows computers, click **Start > IBM Cognos Analytics > IBM Cognos Configuration**.
- On Linux, go to the `<COGNOS_HOME>/bin64` directory, type `./cogconfig.sh`, and press Enter.

3. In Cognos Configuration, configure the database connection to the content store.

a) In the **Explorer** pane, under **Data Access > Content Manager**, click **Content Store**.

b) In the **Database server and port number** field, enter the name of the computer and the port number on which Db2 is running.

`localhost:50000` is the default setting. 50000 is the default port number that is used by Db2. Replace `localhost` with the Db2 server name. If you are using a different port number, replace the default port with the port that you are using.

c) Click the **Value** field next to the **User ID and password** property, click the edit icon, and type the appropriate values for the Cognos user that you created for the content store database, and click **OK**.

d) In the **Properties** window, for the **Database name** property, type the name for your content store database.

Restriction: Do not use a name longer than eight characters and use only letters, numbers, underscores, and hyphens in the name.

4. Right-click **Content Store**, and click **Generate DDL**.

5. In the message box, click **Details** to record the location of the DDL file that is generated.

The `createDb.sql` file is created in the `<COGNOS_HOME>/configuration/schemas/content/db2` directory.

6. To save your settings in Cognos Configuration, click **File > Save**.

7. To run the script that creates the database, log in to the database server as a user who has permissions to create a database.

a) For Windows installations, at the command prompt, type `db2cmd`.

- b) From the command line, type `db2 -tvf createDb.sql`.
- c) On Windows computers, close the CLP.
8. In Cognos Configuration, in the **Explorer** pane, right-click the content store database connection and click **Test**.

Configuring a connection to the content store (Oracle)

After you install Cognos Analytics, configure a connection to the content store database.

Before you begin

Ensure that you copied the JDBC driver file from the `<ORACLE_HOME>/jdbc/lib` directory on the database server to the `<COGNOS_HOME>/drivers` directory on the reporting server.

- If you are using Oracle 12.2.0.1, 18c, or 19c, copy `ojdbc8.jar`

Procedure

1. Log on to the reporting server computer where Cognos Analytics is installed.
2. Go to the `<OP_version>_Main/<OP_version>_Configuration/Database/ORACLE/COGNOS` directory.
3. Log on to the Oracle database as SYS using the following command:

```
sqlplus <sys>/\"<password>\"@<SID> as sysdba
```

For example:

```
sqlplus sys/\"mypassword\"@OP as sysdba
```

4. At the SQL*Plus prompt, run the following command to create the user and password for the content store database:

```
@cognosdbcreate.sql <cognos_user> <cognos_password>  
                  <oracle_data_home> <tablespace_name> <log_file>
```

Table 40. Parameter descriptions for the `cognosdbcreate.sql` script for Oracle databases

Script parameters	Description
<code>cognos_user</code>	Specifies the new user name for the content store database
<code>cognos_password</code>	Specifies the password for the <code>cognos_user</code>
<code>oracle_data_home</code>	Specifies the location of the Oracle data home directory for the content store database instance. On Windows operating systems: <code><ORACLE_BASE>\oradata\<SID></code>
<code>tablespace_name</code>	Specifies the name of the exported table space.
<code>log_file</code>	Specifies the file name and location of the log file to create.

For example:

```
@cognosdbcreate.sql cognos mypassword /home/oracle/app/oracle/oradata/<SID>  
cognos_ts cognosdbcreate.log
```

5. Exit SQL*Plus.
6. Start Cognos Configuration.

- On Windows computers, click **Start > IBM Cognos Analytics > IBM Cognos Configuration**.
 - On Linux, go to the <COGNOS_HOME>/bin64 directory, type `./cogconfig.sh`, and press Enter.
7. In Cognos Configuration, configure the database connection to the content store.
- a) In the **Explorer** pane, under **Data Access > Content Manager**, right-click **IBM Cognos Content Store > Delete**.
 - b) Right-click **Content Manager > New Resource > Database**.
 - c) In the **New Database** window, for the **Name** field, enter a descriptive name for the connection.
Note: The name is not required to match the database identifier.
 - d) For the **Type**, select **Oracle Database (Advanced)** for Oracle PDB or RAC databases, or **Oracle Database** for non-PDB or non-RAC databases.
 - e) Click **OK**.
 - f) In the **Explorer** panel, select the new connection, and in the **Properties** panel, use the following tables to enter the property settings.

Table 41. Content store property settings for Oracle databases

Property name	Property value
Database server and port number	The name of the database server and the listener port that is used for the database instance.
User ID and password	Click the value field and then click the pencil icon. In the Value - User ID and password field, enter the appropriate values for the user and password for the content store database you created in step 4.
SID	Enter the SID for the database instance.

Table 42. Content store property settings for Oracle database (Advanced) (Oracle PDB or RAC databases)

Property name	Property value
Database server and port number	The name of the database server and the listener port that is used for the database instance.
User ID and password	Click the Value field and then click the pencil icon. In the Value - User ID and password field, enter the appropriate values for the content store database you created in step 4.

Table 42. Content store property settings for Oracle database (Advanced) (Oracle PDB or RAC databases) (continued)

Property name	Property value
Database specifier	<p>Enter a database specifier string in the following format with no carriage returns:</p> <ul style="list-style-type: none"> Oracle PDB databases <pre>//<server>/<service_name></pre> <p>For example, //corpserv1:1522/PDB1</p> Oracle RAC databases <pre>(description=(address=(host=<server_name>)(protocol=tcp)(port=<port>)(connect_data(service_name=<service_name>)))</pre>

- Click **File > Save**.
- To test that the database connection to the content store database is successful, in the **Explorer** pane, right-click the content store database connection and click **Test**.

Saving your settings and starting the IBM Cognos services

You must save your configuration settings and start the IBM Cognos services.

Procedure

- Start Cognos Configuration.
 - On Windows computers, click **Start > IBM Cognos Analytics > IBM Cognos Configuration**.
 - On Linux, go to the <COGNOS_HOME>/bin64 directory, type `./cogconfig.sh`, and press Enter.
- Under **Local Configuration > Environment > IBM Cognos services** ensure that the service name is **IBM Cognos**, the default value.

Important: On Microsoft Windows operating systems, IBM OpenPages with Watson requires IBM Cognos as the service name.
- Under **Local Configuration > Environment** verify that the following settings are using the default port number, 9300:.

- Gateway settings > Gateway URI**
- Dispatcher settingsExternal dispatcher URI**
- Dispatcher settingsInternal dispatcher URI**
- Other URI settingsDispatcher URI for external applications**
- Other URI settingsContent Manager URIs**

Important: Changing the default port number also changes the IBM Cognos service name.

- Click **File > Save** to save your configuration settings.

You must save the configuration settings, even if you have not changed any of the values.

- Click **Actions > Start**.

It might take a few minutes for the IBM Cognos service to start.

If you receive a warning during the **Testing the mail server connection** process, click **OK** and **Continue** to continue starting the services. A mail server connection is not required.



Warning: If you chose to upgrade your content store database by creating a backup and restoring it, you are prompted to upgrade your reports. Do not select the option to upgrade your

reporting content. Upgrade your reports later by using the New Report Upgrade wizard in IBM Cognos Administration.

Enabling the connection to a Db2 database from the OpenPages CommandCenter computer

Cataloging a TCP/IP node adds an entry to the Data Server Client node directory that describes the remote node. This entry specifies the chosen alias, the host name or IP address, and the service name (or the port number) that the client uses to access the remote host.

Before a client application can access a remote database, the database must be cataloged on the client. When you create a database, the database is automatically cataloged on the server with a database alias. The database alias is the same as the database name, unless a different database alias is specified.

Important: If the application server and database server are on the same computer, you can ensure that the Cognos installation user has access to the IBM OpenPages with Watson data source by cataloging the OpenPages repository node and database.

Before you begin

Ensure that IBM Db2 client software is installed on the reporting server.

Procedure

1. Log on to the reporting server with a valid Db2 user ID.
2. If you are using Microsoft Windows, start the Db2 command line processor.

From the command prompt, type `db2cmd`. Or, click **Start > IBM Db2 > IBM Db2 Db2COPY1 > Command Line Tools > Db2 Command Window - Administrator**.

3. Catalog the node by entering the following commands in the command line processor:

```
db2 catalog tcpip node <node_name> remote <hostname/ip_address>  
server <service_name/port_number>  
db2 terminate
```

Example:

```
db2 catalog tcpip node OPNODE remote mycomputer.domain.com server 50000  
db2 terminate
```

4. Catalog the database by entering the following commands in the command line processor:

```
db2 catalog database <database_name> as <database_alias> at node <node_name>  
[ authentication <auth_value> ]
```

Example:

```
db2 catalog database OPX at node OPNODE authentication server  
db2 terminate
```

5. To list the node directory, type the following command:

```
db2 list node directory show detail
```

6. To list the database directory, type the following command:

```
db2 list database directory
```

Setting database environment variables for the reporting server on Linux operating systems

If you use an Oracle database for the IBM OpenPages with Watson repository, you must set some system environment variables on the reporting server.

Procedure

1. Log on to the reporting server as an OpenPages installation user with administrative privileges.
2. To determine the version of Java that is in the PATH variable, run the following command:

```
java -version
```

If you get the following error, Java is not in the PATH variable.

Command not found

3. Set the following environment variables.

Table 43. Environment variable settings on the reporting server (Linux)	
Environment variable	Example settings
JAVA_HOME	Specifies the installation location of your Java Runtime Environment (JRE). For example /usr/IBM/cognos/analytics/ibm-jre/jre
COGNOS_HOME	Specifies the installation location of Cognos Analytics. For example /usr/IBM/cognos/analytics

4. Append JAVA_HOME to the PATH variable.

Example: PATH=\$JAVA_HOME/bin:\$PATH

5. If you use Oracle for the OpenPages database, set the following environment variables.

Table 44. Oracle database environment variable settings on the reporting server (Linux)	
Environment variable	Example settings
ORACLE_HOME	For example: <ul style="list-style-type: none">• Admin Client: /home/oracle/app/oracle/product/<Oracle_version>/client_1• Instant Client: /home/oracle/instantclient_19_9 If you installed the OpenPages application and Cognos on the same server, enter the location of the 32-bit client.
TNS_ADMIN	Specifies the location of the tnsnames.ora file. The default location is \$ORACLE_HOME/network/admin
NLS_LANG	Specifies the database character set configured during the database installation. By default, set to AMERICAN_AMERICA.AL32UTF8 Important: To display non-English characters for Japanese locales, set NLS_LANG=JAPANESE_JAPAN.JA16SJISTILDE

6. Append ORACLE_HOME/bin to the PATH variable.

Example: PATH=\$ORACLE_HOME/bin:\$PATH

7. Refresh the profile.

Setting database environment variables for reporting servers on Windows operating systems

You must set some system environment variables on the reporting server.

Procedure

1. Log on to the reporting server as a user with administrative privileges.
2. Set the following environment variables in the user profile.

Table 45. Environment variable settings on the reporting server (Windows)	
Environment variable	Setting
JAVA_HOME	Specifies the installation location of your Java Runtime Environment (JRE).
COGNOS_HOME	Specifies the location of the Cognos Analytics directory. C:\IBM\cognos\analytics

3. Append JAVA_HOME to the PATH environment variable.

Example: Add %JAVA_HOME%\bin to the PATH environment variable.

4. If you are using an Oracle database for the OpenPages database, set the following environment variables.

Table 46. Oracle environment variable settings on the reporting server (Windows)	
Environment variable	Setting
ORACLE_HOME	The default location is a subdirectory of ORACLE_BASE. For example: <ul style="list-style-type: none">• Admin Client: C:\app\product\<Oracle_version>\client_1• Instant Client: C:\oracle\instantclient_19_9 If you installed the OpenPages application and Cognos Analytics on the same server, enter the location of the 32-bit client.
TNS_ADMIN	Specifies the location of the tnsnames.ora file. The default location is <ORACLE_HOME>\network\admin
NLS_LANG	Specifies the database character set configured during the database installation. The default value is AMERICAN_AMERICA.AL32UTF8 Note: To display non-English characters for Japanese locales, set the NLS_LANG property: NLS_LANG=JAPANESE_JAPAN.JA16SJISTILDE

5. Append ORACLE_HOME\bin to the PATH environment variable.

Example: Add %ORACLE_HOME%\bin to the PATH environment variable.

Testing the connection to the OpenPages database from the Oracle database client

Test whether the SQL*Net connect string can connect to the IBM OpenPages with Watson database on the Oracle database server from the Oracle database client.

Procedure

1. Copy the file `<ORACLE_HOME>/network/admin/tnsnames.ora` from the Oracle database server operating system to the `<ORACLE_HOME>/network/admin` Oracle database client directory on the application server or reporting server.

Ensure that the OpenPages installation user has read, write and execute permissions on the `tnsnames.ora` file in the Oracle database client operating system.

2. Log on to the application server or reporting server as an OpenPages installation user.
3. Edit the file `<ORACLE_HOME>/network/admin/tnsnames.ora`, and update the Host value to the host name or IP address of the Oracle database server.
4. To test the connection to the OpenPages database on the database server, type the following command:

```
sqlplus <username>/\"<password>\"@<service_name>
```

For example, `sqlplus system/\"password\"@op`

The system connects you to an Oracle database instance.

5. To exit SQL*Plus, type `exit`.

Checklist for the search server

If you want to use global search, you need a search server. Do the following tasks on the search server before you install IBM OpenPages with Watson:

- Check that all of the required ports are available. See [“Port assignments” on page 124](#).
- Install IBM SDK, Java Technology Edition and set the environment variables for Java. See [“Getting a copy of the IBM SDK \(Linux\)” on page 63](#) or [“Getting a copy of the IBM SDK \(Windows\)” on page 60](#).

Port assignments

Both dedicated ports and ports that are dynamically assigned for each installation are used for the IBM OpenPages with Watson installation. These default ports can be changed after installation.

You can change some port settings during the installation. You can also change the default port settings after installation. For information about changing the ports after installation, see the *IBM OpenPages with Watson Administrator's Guide*.

Default ports

The following table lists the default ports.

Table 47. Default fixed port assignments	
Description	Ports
OpenPages installation server	8443
OpenPages installation agent	8443
OpenPages database instance (Oracle)	1521
OpenPages database instance (IBM Db2)	50000
OpenPages application URL	10108
OpenPages application URL (SSL)	10111

Table 47. Default fixed port assignments (continued)	
Description	Ports
Cognos Analytics gateway (as configured for your web server)	80
Framework Generator port	8080
Cognos Analytics dispatcher URI	9300
Search server (used for indexing and searching OpenPages data)	8983
Search server (used to administer global search)	8985

Files containing port numbers

After installation, you can view the OpenPages application port assignments in the following file on each application server: `<OP_HOME>/wlp-user/servers/<server_name>Server<#>/bootstrap.properties`.

The following tables list property files on the OpenPages admin application server that contain port numbers for other components.

Table 48. Files that contain port numbers		
Port	File name	Parameter Name
Application server ports	<code><OP_HOME>/wlp-user/servers/<server_name>Server<#>/bootstrap.properties</code>	<code>op.http.port</code> <code>op.https.port</code> if you are using SSL
Oracle database instance port	<code><ORACLE_HOME>/NETWORK/ADMIN/tnsnames.ora</code>	N/A
Framework Generator port	<code><OP_HOME>/aurora/conf/aurora.properties</code>	<code>cognos.framework.refresh.servlet</code>
Cognos Analytics server port	<code><OP_HOME>/aurora/conf/aurora.properties</code>	<code>cognos.server</code>
Cognos Analytics Dispatcher URI	<code><OP_HOME>/aurora/conf/aurora.properties</code>	<code>cognos.computation.server</code>

Dynamically assigned ports

Port numbers for IBM OpenPages with Watson servers that are not listed, are assigned dynamically during the installation.

For application servers, when you add a horizontal cluster member, you specify a port number on the application server card in the installation app. The next 20 port numbers are reserved for each vertical cluster member.

Create the database schema objects

Before you install IBM OpenPages with Watson, decide how you want to create the OpenPages database.

OpenPages database object creation for Db2

Before you install IBM OpenPages with Watson, decide how you want to create the OpenPages database objects.

You have the following options:

- You can use the OpenPages installation program to create the database objects. If you choose this option, you need to provide DBA credentials when you install OpenPages.
- You can ask a database administrator to do the steps that require DBA privileges, and then use the OpenPages installation program to complete the database setup. Use this option if your organization's security policies require the separation of DBA and non-DBA tasks. Also, use this option if your database administrator wants to customize the table space names, the schema name, or make other customizations.
- You can create all of the objects required for the database manually by using scripts. Use this option if you want to customize the table space names or if you want to run custom scripts.

The initial install of a Db2 database always assumes LFS for the OpenPages storage type. If you want to use UNC, you must first install with LFS and then use the update storage script to change to UNC.

Preparing the files for your database administrator

Your database administrator needs a set of scripts to create the database objects. You need to prepare the files and send them to your DBA with instructions on how to run the scripts.

Do this procedure if your organization's security policies require the separation of DBA and non-DBA tasks.

About this task

The `sql-wrapper.sql` file contains information that is used by the database scripts. You need to enter the values for your environment, such as the name of the database instance for OpenPages.

When you install OpenPages, use the same values that you set in the `sql-wrapper.sql` file.

Procedure

1. Log on to the Db2 database server computer as a user with administrative privileges.
2. Go to the `/OP_<version>_Main/OP_<version>_Configuration/Database/DB2/INSTALL_SCRIPTS` directory.
3. Verify that you have write permission on the `sql-wrapper.sql` file. If not, change the permission on the file by using the **chmod** command.
4. Edit the `sql-wrapper.sql` file.

Restriction: Change only the parameters that are described in this step.

These parameters are used by the scripts that your DBA will run.

Table 49. Parameters in the <code>sql-wrapper.sql</code> file for Db2 databases	
Property	Description
<code>opx_db2_instance_owner</code>	<p>The database instance owner for OpenPages.</p> <p>The user you specify must have both DBADM and SECADM privileges</p> <p>If your database administrator is going to run the DBA scripts for you, then you can leave this value empty when you run the non-DBA scripts.</p>
<code>opx_db2_server_name</code>	The database server name
<code>opx_db2_port_number</code>	The database port number, for example 50000
<code>opx_db2_db_name</code>	The name of the OpenPages database.
<code>opx_db_owner</code>	The schema owner of the OpenPages database.
<code>opx_dflt_stor_srv_root</code>	<p>The path to the OpenPages storage directory.</p> <p>Example:</p> <pre>define opx_dflt_stor_srv_root='/home/ opuser/OP/OpenPages/openpages-storage'</pre>
<code>opx_op_admin_name</code>	The OpenPages administrator user name
<code>opx_op_admin_pwd</code>	The OpenPages administrator password

5. If your database administrator is going to run the scripts that require DBA privileges, prepare the files for your database administrator.
 - a) Go to the `/OP_<version>_Main/OP_<version>_Configuration/Database/DB2/INSTALL_SCRIPTS` directory.
 - b) Open the `op-dba-install-file-list.txt` file.
 - c) Send your DBA the `sql-wrapper.sql` file that you updated along with the files listed in the `op-dba-install-file-list.txt` file.
 - d) Send your DBA the instructions to run the DBA scripts: [“Running the steps that require DBA privileges” on page 127](#)

Running the steps that require DBA privileges

You can run a script to do the database object creation steps that require DBA privileges. Do this procedure if you do not want to enter DBA credentials when you install OpenPages or if your organization's security policies require the separation of DBA and non-DBA tasks.

Before you begin

- The Db2 database server is running
- A database instance for the OpenPages database is created
- The `sql-wrapper.sql` is configured for your environment

About this task

Run the following script: `op-database-dba-install.sh | .bat`. The script uses the parameters in the `sql-wrapper.sql` file.

The `op-database-dba-install.sh | .bat` calls the following scripts:

- `op-database-dba-install.sql`: Runs the DBA steps. This script calls the other scripts in this list.

- `create-opx-tablespaces.sql`: Creates the OpenPages table spaces.
- `dba-grant.sql`: Grants privileges to the DBA user.
- `create-opx-schema-owner.sql`: Creates the OpenPages schema owner and grants the user access to the OpenPages table spaces.
- `no-op.sql`: This script is empty. Edit this script if you want to run any custom scripts at the end of the DBA setup process. See [“Custom table space names” on page 129](#).

You can do the following configurations:

- You can specify custom names for table spaces
- You can specify a custom SQL script to run

Procedure

1. Log on to the Db2 database server as the Db2 database administrator (DBA).
2. Locate the scripts that are required.

If you are a database administrator, get the scripts from your OpenPages team.

Or, you can get the scripts from the `/OP_<version>_Main/OP_<version>_Configuration/Database/DB2/INSTALL_SCRIPTS` directory.

3. Verify that you have execute permission on the scripts.
4. Open the `sql-wrapper.sql` file. Verify that the values are suitable for your environment.

The user that you specify for the `opx_db2_instance_owner` parameter must have both DBADM and SECADM privileges.

If you want to customize the table space names, see [“Custom table space names” on page 129](#).

Note: Do not modify the parameters in the section that is used only for upgrades.

5. If you are using Microsoft Windows, start the Db2 command line processor.

From the command prompt, type `db2cmd`. Or, click **Start > IBM Db2 > IBM Db2 Db2COPY1 > Command Line Tools > Db2 Command Window - Administrator**.

6. Run the `op-database-dba-install.sh | .bat` script from the command line.

- On Linux:

```
./op-database-dba-install.sh '<dba_password>'
```

- On Windows:

```
op-database-dba-install.bat "<dba_password>"
```

Note: Quotation marks are required around a password only if the password contains special characters. See [“Special characters in passwords” on page 12](#).

7. Verify that the return code is 0, indicating success.

You can also check the log file, `op-dba-install-<timestamp>.log`.

What to do next

You can use the OpenPages installation program to complete the database setup. Or you can complete the database setup manually by using scripts.

Custom table space names

You can customize the table spaces in the OpenPages database. These procedures are intended for database administrators.

To customize the table space names, edit the following properties in the `sql-wrapper.sql` file:

```
define opx_dflt_data_ts='AURORA'  
define opx_dflt_indx_ts='INDX'  
define opx_dflt_temp_data_ts='AURORA_NL'  
define opx_dflt_temp_indx_ts='AURORA_NLI'  
define opx_dflt_dedi_temp_ts='AURORA_TEMP'  
define opx_dflt_snp_ts='AURORA_SNP'  
define opx_dflt_clob_data_ts='AURORA_CLOB_DATA'  
define opx_dflt_domain_indx_ts='AURORA_DOMAIN_INDX'
```

Give the new table space names to the user who will install OpenPages. The table space names must be provided during the installation process.

Preparing to run the non-DBA database scripts

Edit the `sql-wrapper.sql` file to specify the values for your environment.

This procedure is optional. Instead of running scripts, you can complete the database setup when you install OpenPages.

About this task

The `sql-wrapper.sql` file contains information that is used by the database scripts. You need to enter the values for your environment, such as the name of the database instance for OpenPages.

When you install OpenPages, use the same values that you set in the `sql-wrapper.sql` file.

Procedure

1. Log on to the Db2 database server computer as the Db2 database administrator (DBA).
2. Go to the `/OP_<version>_Main/OP_<version>_Configuration/Database/DB2/INSTALL_SCRIPTS` directory.
3. Verify that you have write permission on the `sql-wrapper.sql` file. If not, change the permission on the file by using the **chmod** command.
4. Edit the `sql-wrapper.sql` file to ensure that the variables are set correctly for your environment.

Edit the following parameters, if needed:

Table 50. Parameters in the <code>sql-wrapper.sql</code> file for Db2 databases	
Property	Description
<code>opx_db2_instance_owner</code>	The database instance owner for OpenPages.
<code>opx_db2_server_name</code>	The database server name
<code>opx_db2_port_number</code>	The database port number, for example 50000
<code>opx_db2_db_name</code>	The name of the OpenPages database.
<code>opx_db_owner</code>	The schema owner of the OpenPages database.
<code>opx_dflt_stor_srv_root</code>	The path to the OpenPages storage directory. Example: <pre>define opx_dflt_stor_srv_root='/home/ opuser/OP/OpenPages/openpages-storage'</pre>
<code>opx_op_admin_name</code>	The OpenPages administrator user name

Table 50. Parameters in the <code>sql-wrapper.sql</code> file for Db2 databases (continued)	
Property	Description
<code>opx_op_admin_pwd</code>	The OpenPages administrator password
<code>opx_base_currency_iso_code</code>	<p>The base currency</p> <p>For example, if you use Euros as your base currency, change the default ISO currency code from USD to EUR.</p> <pre>define opx_base_currency_iso_code='EUR'</pre>

5. If you want to load custom data during the database setup process, see [“Loading custom data \(Db2 and Oracle\)”](#) on page 130.

Loading custom data (Db2 and Oracle)

If you want to load custom data during the database setup process, edit the `sql-wrapper.sql` file to specify the scripts to run.

About this task

You can use the `custom_environment_script` and `custom_data_load_script` parameters to configure a custom scripts.

Use the `custom_environment_script` parameter to set environment values. The script that you specify is called each time that the `sql-wrapper.sql` script is called.

Use the `custom_data_load_script` parameter to load custom data. The script that you specify is called by the `op-database-product-install.sh | .bat` script. The custom data load is done as the last step in the `op-database-product-install.sh | .bat` script.

Procedure

1. Open the `sql-wrapper.sql` file.
2. If you are using IBM Db2, verify that the `sqllib_dir` path is correct. If you are running the custom scripts from a computer other than the database server, update the path.
3. Edit the following parameters:

```
define custom_environment_script=no-op.sql
define custom_data_load_script=no-op.sql
```

Replace `no-op.sql` with the script that you want to run.

4. Place your custom scripts in the same directory as the `sql-wrapper.sql` file.

Running the steps that do not require DBA privileges

You can complete the database setup manually by using scripts. Do this procedure after a database administrator has run the DBA scripts.

This procedure is optional. Instead of running scripts, you can complete the database setup when you install OpenPages.

Before you begin

Ensure that the following conditions are met:

- The Db2 database server is running.
- A database instance for the OpenPages database is created.
- The database setup steps that require DBA privileges are complete.

- The `sql-wrapper.sql` file is configured for your environment.

About this task

You need to run the following scripts:

- `op-validate-dba-install.sh | .bat`: Validates that the DBA steps completed successfully.
- `op-database-product-install.sh | .bat`: Performs the database creation tasks that do not require DBA privileges.
- `op-validate-product-install.sh | .bat`: Validates that the database setup steps completed successfully.

These scripts use the parameters that are specified in the `sql-wrapper.sql` script.

Procedure

1. Log on to the Db2 database server computer as the Db2 database administrator (DBA).
2. Go to the `/OP_<version>_Main/OP_<version>_Configuration/Database/DB2/INSTALL_SCRIPTS` directory.
3. Verify that you have execute permission on the scripts in the `INSTALL_SCRIPTS` directory.
4. If you are using Microsoft Windows, start the Db2 command line processor.

From the command prompt, type `db2cmd`. Or, click **Start > IBM Db2 > IBM Db2 Db2COPY1 > Command Line Tools > Db2 Command Window - Administrator**.

5. Run the `op-validate-dba-install.sh | .bat` script from the command line.
The script verifies that the DBA setup steps are complete.

- On Linux:

```
./op-validate-dba-install.sh '<opuser_password>'
```

- On Windows:

```
op-validate-dba-install.bat "<opuser_password>"
```

Replace `<opuser_password>` with the password of the OpenPages database user.

Note: Quotation marks are required around a password only if the password contains special characters. See [“Special characters in passwords” on page 12](#).

6. Verify that the return code is 0, indicating success.
7. Run the `op-database-product-install.sh | .bat` script from the command line.

- On Linux:

```
./op-database-product-install.sh '<opuser_password>'
```

- On Windows:

```
op-database-product-install.bat "<opuser_password>"
```

Replace `<opuser_password>` with the password of the OpenPages database user.

Note: Quotation marks are required around a password only if the password contains special characters. See [“Special characters in passwords” on page 12](#).

8. Verify that the return code is 0, indicating success.

You can also view the log file, `op-database-product-install-<timestamp>.log`.

9. Run the `op-validate-product-install.sh | .bat` script from the command line.
The script verifies that the setup steps are complete.

- On Linux:

```
./op-validate-product-install.sh '<opuser_password>'
```

- On Windows:

```
op-validate-product-install.bat "<opuser_password>"
```

Replace *<opuser_password>* with the password of the OpenPages database user.

Note: Quotation marks are required around a password only if the password contains special characters. See “Special characters in passwords” on page 12.

10. Verify that the return code is 0, indicating success.

You can also view the log file, `validate-product-install-<timestamp>.log`.

11. Remove the passwords from the `sql-wrapper.sql` file for security purposes.

OpenPages database schema creation for Oracle

Before you install IBM OpenPages with Watson, decide how you want to create the OpenPages database.

You have the following options:

- You can use the OpenPages installation program to create the database schema. If you choose this option, you need to provide DBA credentials when you install OpenPages.
- You can ask a database administrator to do the steps that require DBA privileges, and then use the OpenPages installation program to complete the database setup. Use this option if your organization's security policies require the separation of DBA and non-DBA tasks. Also, use this option if your database administrator wants to customize the table space names, the schema name, or make other customizations.
- You can create all of the objects required for the database manually by using scripts. Use this option if you want to do any of the following configurations:
 - Customize the table space names or the schema name
 - Customize the table space data file locations
 - Use Oracle Transparent Data Encryption (TDE)
 - Run custom scripts

The initial install of an Oracle database always assumes LFS for the OpenPages storage type. If you want to use UNC, you must first install with LFS and then use the update storage script to change to UNC.

This video demonstrates how to create the database schema by using scripts. The video shows 7.4 but the steps are similar for 8.2.

<https://youtu.be/hDRT-oW8j7U>

Preparing the files for your database administrator

Your database administrator needs a set of scripts to create the database schema. You need to prepare the files and send them to your DBA with instructions on how to run the scripts.

Do this procedure if your organization's security policies require the separation of DBA and non-DBA tasks.

About this task

The `sql-wrapper.sql` file contains information that is used by the database scripts. You need to enter the values for your environment, such as the name of the database instance for OpenPages.

When you install OpenPages, use the same values that you set in the `sql-wrapper.sql` file.

Procedure

1. Log on to the Oracle database server computer as a user with administrative privileges.
2. Go to the `/OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/INSTALL_SCRIPTS` directory.
3. Verify that you have write permission on the `sql-wrapper.sql` file. If not, change the permission on the file by using the **chmod** command.
4. Edit the `sql-wrapper.sql` file.

Restriction: Change only the parameters that are described in this step.

These parameters are used by the scripts that your DBA will run.

Table 51. Parameters in the <code>sql-wrapper.sql</code> file for Oracle databases	
Property	Description
<code>opx_datafile_storage_dir</code>	Defines the physical locations of the datafiles that are associated with the tablespaces that are created. This should be set to a value that is appropriate for your environment
<code>opx_dflt_sid</code>	The TNS alias of the Oracle database for OpenPages.
<code>opx_db_owner</code>	The database owner, also the name of the schema
<code>opx_op_admin_name</code>	The OpenPages administrator user name
<code>opx_op_admin_pwd</code>	The OpenPages administrator password
<code>opx_dflt_stor_srv_root</code>	The path to the OpenPages storage directory. Example: <pre>define opx_dflt_stor_srv_root='/home/ opuser/ OP/OpenPages/openpages-storage'</pre>

5. If your database administrator is going to run the scripts that require DBA privileges, prepare the files for your database administrator.
 - a) Go to the `/OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/INSTALL_SCRIPTS` directory.
 - b) Open the `op-dba-install-file-list.txt` file.
 - c) Send your DBA the `sql-wrapper.sql` file that you updated along with the files listed in the `op-dba-install-file-list.txt` file.
 - d) Send your DBA the instructions to run the DBA scripts: [“Running the steps that require DBA privileges” on page 133](#)

Running the steps that require DBA privileges

You can run a script to do the database schema creation steps that require DBA privileges. Do this procedure if you do not want to enter DBA credentials when you install OpenPages or if your organization's security policies require the separation of DBA and non-DBA tasks.

Before you begin

- The Oracle database server is running
- A database instance for the OpenPages database is created
- The `sql-wrapper.sql` file is configured for your environment

About this task

Run the following script: `op-database-dba-install.sh|.bat`. The script uses the properties that are defined in the `sql-wrapper.sql` file.

The `op-database-dba-install.sh|.bat` calls the following scripts:

- `op-database-dba-install.sql`: Runs the DBA steps. This script calls the other scripts that are in this list.
- `create-opx-directory.sql`: Sets the location of the data pump directory to use for OpenPages.
- `create-opx-tablespaces.sql`: Creates the OpenPages table spaces. Edit this file to enable Oracle TDE or to customize the table space data file names and locations.
- `create-opx-schema-owner.sql`: Creates the OpenPages schema owner and grants the user access to the OpenPages table spaces.
- `uniform-grants.sql`: Grants privileges to the schema owner.
- `install-oracle-text.sql`: Enables Oracle Text Search.
- `no-op.sql`: This script is empty. Edit this script if you want to run any custom scripts at the end of the DBA setup process.

You can do the following configurations:

- You can specify a custom name for the OpenPages schema
- You can specify custom names for the table spaces
- You can specify custom data file names and locations for the table spaces
- You can enable or disable Oracle Text
- You can specify a custom SQL script to run

Procedure

1. Log on to the Oracle database server computer as the Oracle database administrator (DBA).
2. Locate the scripts that are required.

If you are a database administrator, get the scripts from your OpenPages team.

Or, you can get the scripts from the `/OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/INSTALL_SCRIPTS` directory.

3. Verify that you have execute permission on the scripts.
4. Open the `sql-wrapper.sql` file. Verify that the values are suitable for your environment.
 - Enter the DBA user name in the `opx_oracle_dba_user` parameter. The user that you specify must have SYSDBA privileges.

For example:

```
define opx_oracle_dba_user='SYS'
```

- If you want to customize the table space names, see [“Table space names and other customizations” on page 135](#).
- If you want to use custom locations for the table space data files, see [“Customize table space data file locations” on page 135](#).
- If you use Oracle Automatic Storage Management (ASM), see [“Changing the database script when you use Oracle ASM” on page 136](#).
- If you want to use Oracle TDE, see [“Oracle Transparent Data Encryption \(TDE\) for fresh installations” on page 136](#).

Note: Do not modify the parameters in the section that is used only for upgrades.

5. Run the `op-database-dba-install.sh|.bat` script from the command line.

- On Windows:

```
op-database-dba-install.bat "<dba_password>" "<op_schema_owner_password>"
```

- On Linux:

```
./op-database-dba-install.sh '<dba_password>' '<op_schema_owner_password>'
```

Note: Quotation marks are required around a password only if the password contains special characters. See [“Special characters in passwords” on page 12](#).

6. Verify that the return code is 0, indicating success.

You can also check the log file, `op-database-dba-install-<timestamp>.log`.

What to do next

You can use the OpenPages installation program to complete the database setup. Or you can complete the database setup manually by using scripts.

Table space names and other customizations

You can customize the table spaces in the OpenPages database. These procedures are intended for database administrators.

To customize the table space names, edit the following properties in the `sql-wrapper.sql` file:

```
define opx_dflt_data_ts='AURORA'
define opx_dflt_indx_ts='INDX'
define opx_dflt_temp_data_ts='AURORA_NL'
define opx_dflt_temp_indx_ts='AURORA_NLI'
define opx_dflt_dedi_temp_ts='AURORA_TEMP'
define opx_dflt_snp_ts='AURORA_SNP'
define opx_dflt_clob_data_ts='AURORA_CLOB_DATA'
define opx_dflt_domain_indx_ts='AURORA_DOMAIN_INDX'
```

Give the new table space names to the user who will install OpenPages. The table space names must be provided during the installation process.

Note: If you complete both the DBA and non-DBA setup steps by using scripts, the table space names do not need to be provided when you install the OpenPages.

You can also customize the data file path for each table space. See [“Customize table space data file locations” on page 135](#).

Customize table space data file locations

You can customize the data file location of the OpenPages table spaces.

Procedure

1. Log on to the Oracle database server as the user who installed Oracle.
2. Go to the `/OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/INSTALL_SCRIPTS` directory.
3. Open the `create-opx-tablespaces.sql` script in a text editor.
4. Replace the `&&3` parameter with the full path to the data file.

For example, suppose that you want to customize the location of the `opx_dflt_data_ts` data file:

```
SELECT lower('&opx_dflt_data_ts') lcase_name FROM dual;
create tablespace &opx_dflt_data_ts datafile '&&3/&v_lcase_name..dbf'
size 512 M reuse autoextend on next 128 M maxsize 1024 M &&encrypt_var;
```

Replace &&3 with the full path:

```
SELECT lower('&&opx_dflt_data_ts') lcase_name FROM dual;
create tablespace &&opx_dflt_data_ts datafile '/u01/oradata/OP/&v_lcase_name..dbf'
size 512 M reuse autoextend on next 128 M maxsize 1024 M &&encrypt_var;
```

Note: Do not modify the &v_lcase_name..dbf parameter. The table space name is read from the sql-wrapper.sql file.

Changing the database script when you use Oracle ASM

If you use Oracle Automatic Storage Management (ASM), you must modify some scripted values. You must update the create-opx-tablespaces.sql script before you run the op-database-dba-install.sh|.bat script.

Procedure

1. Log on to the Oracle database server as the user who installed Oracle.
2. Go to the /OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/INSTALL_SCRIPTS directory.
3. Open the create-opx-tablespaces.sql script in a text editor.
4. As appropriate for your environment, replace the '&&3/&v_lcase_name..dbf' parameter with the name of a disk group.

For example, if you want to use a disk group called DATA to store the opx_dflt_data_ts table space, use the following syntax:

```
create tablespace &&opx_dflt_data_ts datafile '+DATA' size 512 M
reuse autoextend on next 128 M maxsize 1024 M &&encrypt_var;
```

5. Save and close the file.

Oracle Transparent Data Encryption (TDE) for fresh installations

You can use Oracle Transparent Data Encryption (TDE) to encrypt the OpenPages and Cognos table spaces in the OpenPages database.

This task is optional.

Note: This task is for new installations only. If you are upgrading, see [“Oracle Transparent Data Encryption for migration customers” on page 264](#).

IBM OpenPages with Watson supports the ability to implement TDE, but TDE is an Oracle feature. You need to be familiar with data encryption of Oracle databases and you need to configure and maintain TDE. If you have questions about TDE, refer to the Oracle documentation.

Restriction: OpenPages supports Oracle TDE only for table spaces. Column-based TDE is not supported.

To implement Oracle TDE, you need to complete two main tasks:

1. Configure a key store. Do this step before you install Cognos and OpenPages.

Your database administrator needs to create a key store. The steps and requirements for key stores are determined by Oracle. IBM is not responsible for the configuration or maintenance of the key store.

Note: A table space can be encrypted only when it is initially created. You cannot alter an existing table space to enable encryption.

2. Encrypt the Cognos and OpenPages table spaces that support encryption.

To install OpenPages with Oracle TDE, you need to do some manual configuration tasks. Review and ensure that you understand these manual steps before you install OpenPages with Oracle TDE.

Note: Oracle does not support encryption on system, undo, or temporary table spaces.

For more information about TDE, refer to the Oracle documentation, such as the [Oracle Database Advance Security Guide](https://docs.oracle.com/database/121/ASOAG/toc.htm) (<https://docs.oracle.com/database/121/ASOAG/toc.htm>).

Prerequisites and process overview

Ensure that your environment meets the prerequisites for Oracle TDE and review the configuration process.

Ensure that your environment meets the following prerequisites:

1. The Oracle database that you are going to use for OpenPages is already created.
2. IBM OpenPages with Watson is not installed.
3. Cognos Analytics is not installed.
4. The Oracle instance is open and accepting connections.
5. The database compatibility parameter is set to your version of Oracle:
 - For Oracle 12.2.0.1, use 12.2.0
 - For Oracle 18c, use 18.0.0
 - For Oracle 19c, use 19.0.0

Complete the following process to configure TDE:

1. Configure a software key store. Refer to the [Oracle documentation](#).
2. Encrypt the OpenPages table spaces that support encryption:
 - a. Verify the value of the database compatible parameter.
 - b. Enable Oracle TDE for Cognos table space.
 - c. Enable Oracle TDE for OpenPages table spaces.
 - d. Create the Cognos database user and table space.
 - e. Run the DBA step of the OpenPages database installation.
 - f. Verify that the table spaces are encrypted.
 - g. Complete the installation of OpenPages and Cognos

Encrypting OpenPages and Cognos table spaces

You can encrypt the OpenPages and Cognos table spaces by using Oracle TDE.

About this task

Do this procedure after you set up the key store and before you install IBM OpenPages with Watson and Cognos Analytics.

Procedure

1. Log on to the OpenPages database instance as the instance owner.
2. Start SQL*Plus.
3. Verify that the database COMPATIBLE parameter is set to the version of Oracle that you are using.

```
select value from GV$SYSTEM_PARAMETER where name = 'compatible';
```

- For Oracle 12.2.0.1, use 12.2.0
 - For Oracle 18c, use 18.0.0
 - For Oracle 19c, use 19.0.0
4. To encrypt the Cognos table spaces, modify the `cognosdbcreate.sql` file.

The `cognosdbcreate.sql` file is located in the following directory: `OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/COGNOS`

- a) Open the `cognosdbcreate.sql` file in a text editor.
- b) Locate the Oracle Transparent Data Encryption section.
- c) Comment out the `define encrypt_var= ' ' line.`

d) Uncomment the line for the encryption algorithm that you are using for the table spaces.

For example, if you are using AES128:

```
--define encrypt_var=''
--define encrypt_var='ENCRYPTION USING ''3DES168'' DEFAULT STORAGE(ENCRYPT)'
define encrypt_var='ENCRYPTION USING ''AES128'' DEFAULT STORAGE(ENCRYPT)'
--define encrypt_var='ENCRYPTION USING ''AES192'' DEFAULT STORAGE(ENCRYPT)'
--define encrypt_var='ENCRYPTION USING ''AES256'' DEFAULT STORAGE(ENCRYPT)'
```

5. To encrypt the OpenPages table spaces, modify the `create-opx-tablespaces.sql` file.

The `create-opx-tablespaces.sql` file is located in the following directory: `OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/INSTALL_SCRIPTS`

- Open the `create-opx-tablespaces.sql` file in a text editor.
- Locate the Oracle Transparent Data Encryption section.
- Comment out the `define encrypt_var=''` line.
- Uncomment the line for the encryption algorithm that you are using for the table spaces.

For example, if you are using AES128:

```
--define encrypt_var=''
--define encrypt_var='ENCRYPTION USING ''3DES168'' DEFAULT STORAGE(ENCRYPT)'
define encrypt_var='ENCRYPTION USING ''AES128'' DEFAULT STORAGE(ENCRYPT)'
--define encrypt_var='ENCRYPTION USING ''AES192'' DEFAULT STORAGE(ENCRYPT)'
--define encrypt_var='ENCRYPTION USING ''AES256'' DEFAULT STORAGE(ENCRYPT)'
```

6. Run the `op-database-dba-install.sh/bat` script.

For more information, see [“Running the steps that require DBA privileges” on page 133.](#)

7. Install Cognos Analytics.

For more information, see [“Installing Cognos Analytics” on page 112.](#)

8. Run the `cognosdbcreate.sql` script.

For more information, see [“Configuring a connection to the content store \(Oracle\)” on page 118.](#)

9. Install IBM OpenPages with Watson.

10. Verify that the table spaces are encrypted.

Log in to the OpenPages database as a DBA user and run the following command:

```
select tablespace_name, encrypted, status from dba_tablespaces;
```

Verify that the output is similar to the following text:

TABSPACE_NAME	ENC	STATUS
SYSTEM	NO	ONLINE
SYSAUX	NO	ONLINE
UNDOTBS1	NO	ONLINE
TEMP	NO	ONLINE
USERS	NO	ONLINE
AURORA	YES	ONLINE
INDX	YES	ONLINE
AURORA_SNP	YES	ONLINE
AURORA_TEMP	NO	ONLINE
AURORA_NL	YES	ONLINE
AURORA_NLI	YES	ONLINE
AURORA_CLOB_DATA	YES	ONLINE
AURORA_DOMAIN_INDX	YES	ONLINE
COGNOS	YES	ONLINE

14 rows selected.

Preparing to run the non-DBA database scripts

Edit the `sql-wrapper.sql` file to specify the values for your environment.

This procedure is optional. Instead of running scripts, you can complete the database setup when you install OpenPages.

About this task

The `sql-wrapper.sql` file contains information that is used by the database scripts. You need to enter the values for your environment, such as the name of the database instance for OpenPages.

When you install OpenPages, use the same values that you set in the `sql-wrapper.sql` file.

Procedure

1. Log on to the Oracle database server computer as the Oracle database administrator (DBA).
2. Go to the `/OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/INSTALL_SCRIPTS` directory.
3. Verify that you have write permission on the `sql-wrapper.sql` file. If not, change the permission on the file by using the **chmod** command.
4. Edit the `sql-wrapper.sql` file to ensure that the variables are set correctly for your environment.

Table 52. Parameters in the <code>sql-wrapper.sql</code> file for Oracle databases	
Property	Description
<code>opx_dflt_sid</code>	The TNS alias of the Oracle database for OpenPages.
<code>opx_db_owner</code>	The database owner, also the name of the schema
<code>opx_op_admin_name</code>	The OpenPages administrator user name
<code>opx_op_admin_pwd</code>	The OpenPages administrator password
<code>opx_base_currency_iso_code</code>	<div>The base currency</div> <div>For example, if you use Euros as your base currency, change the default ISO currency code from USD to EUR.</div> <div><pre>define opx_base_currency_iso_code='EUR'</pre></div>
<code>opx_dflt_stor_srv_root</code>	<div>The path to the OpenPages storage directory.</div> <div>Example:</div> <div><pre>define opx_dflt_stor_srv_root='/home/opuser/OP/OpenPages/openpages-storage'</pre></div>

5. To enable or disable Oracle Text, modify the `flag_install_oracle_text` property.

For example, to enable Oracle Text, type Y.

```
define flag_install_oracle_text='Y'
```

6. If you want to load custom data during the database setup process, see [“Loading custom data \(Db2 and Oracle\)” on page 130](#).

Loading custom data (Db2 and Oracle)

If you want to load custom data during the database setup process, edit the `sql-wrapper.sql` file to specify the scripts to run.

About this task

You can use the `custom_environment_script` and `custom_data_load_script` parameters to configure a custom scripts.

Use the `custom_environment_script` parameter to set environment values. The script that you specify is called each time that the `sql-wrapper.sql` script is called.

Use the `custom_data_load_script` parameter to load custom data. The script that you specify is called by the `op-database-product-install.sh|.bat` script. The custom data load is done as the last step in the `op-database-product-install.sh|.bat` script.

Procedure

1. Open the `sql-wrapper.sql` file.
2. If you are using IBM Db2, verify that the `sqllib_dir` path is correct. If you are running the custom scripts from a computer other than the database server, update the path.
3. Edit the following parameters:

```
define custom_environment_script=no-op.sql
define custom_data_load_script=no-op.sql
```

Replace `no-op.sql` with the script that you want to run.

4. Place your custom scripts in the same directory as the `sql-wrapper.sql` file.

Running the steps that do not require DBA privileges

You can complete the database setup manually by using scripts. Do this procedure after the DBA steps are complete.

This procedure is optional. Instead of running scripts, you can complete the database setup when you install OpenPages.

Before you begin

- The Oracle database server is running
- A database instance for the OpenPages database is created
- The database setup steps that require DBA privileges are complete
- The `sql-wrapper.sql` file is configured for your environment

About this task

You need to run three scripts:

- `op-validate-dba-install.sh|.bat`: Validates that the DBA steps completed successfully
- `op-database-product-install.sh|.bat`: Performs the database creation tasks that do not require DBA privileges
- `op-validate-product-install.sh|.bat`: Validates that the steps completed successfully

Procedure

1. Log on to the Oracle database server as the OpenPages application user, `opuser`.
2. Go to the `/OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/INSTALL_SCRIPTS` directory.

3. Verify that you have execute permission on the files in the `INSTALL_SCRIPTS` directory. If not, change the permission on the file by using the **chmod** command.
4. Verify that the DBA portion of the database setup completed successfully.

- On Windows: Open a command prompt by using the **Run as administrator** option. Run the following script:

```
op-validate-dba-install.bat "<op_schema_owner_password>"
```

- On Linux: Run the following script:

```
./op-validate-dba-install.sh '<op_schema_owner_password>'
```

Note: Quotation marks are required around a password only if the password contains special characters. See [“Special characters in passwords” on page 12](#).

You can view the log file: `op-validate-dba-install-<timestamp>.log`.

5. Run the following script to set up the Oracle database instance.

- On Windows: Open a command prompt by using the **Run as administrator** option. Run the following script:

```
op-database-product-install.bat "<op_schema_owner_password>"
```

- On Linux: Run the following script:

```
./op-database-product-install.sh '<op_schema_owner_password>'
```

Note: Quotation marks are required around a password only if the password contains special characters. See [“Special characters in passwords” on page 12](#).

The `op-database-product-install.sh | .bat` script performs the installation steps that do not require DBA privileges.

6. Run the following scripts to verify the product installation on the Oracle database instance.

- On Windows: Open a command prompt by using the **Run as administrator** option. Run the following script:

```
op-validate-product-install.bat "<op_schema_owner_password>"
```

- On Linux: Run the following script:

```
./op-validate-product-install.sh '<op_schema_owner_password>'
```

Note: Quotation marks are required around a password only if the password contains special characters. See [“Special characters in passwords” on page 12](#).

The `op-validate-product-install.sh | .bat` script verifies that the installation steps completed successfully.

7. Remove the passwords from the `sql-wrapper.sql` file for security purposes.

Creating a deployment

Create a deployment to install IBM OpenPages with Watson. You can create a deployment from scratch or you can import deployment properties from a file.

If you are migrating, you create a new deployment as part of the migration process. For more information, see [Chapter 7, “Migrate to a new version of IBM OpenPages with Watson,” on page 189](#).

Before you begin

- Before you create a deployment, plan your server topology and prepare each server for the installation.

- Ensure that the installation server is updated to the latest version. For more information, see [“Updating the installation server”](#) on page 47. The latest version of the installation server is available in the latest OpenPages fix pack kit.
- Ensure that the installation server can communicate with all of the servers in your deployment.
- On each remote server in your deployment, do one of the following steps:
 - Update the antivirus policy on the remote server to allow Node.js.
 - Disable antivirus software on the remote server. You can re-enable it after you complete the installation of IBM OpenPages with Watson.

About this task

Tip: You can save your work at any time and return to your deployment later to complete the installation.

Procedure

1. Log in to the IBM OpenPages with Watson installation app.

See [“Logging in to the installation app”](#) on page 49.

2. Create a deployment.

You can create a deployment from scratch or you can load values from an existing deployment.

- To create a deployment from scratch, click **Create New**. Type a name for the deployment, and then click **Create**.

Note: The deployment name is used to create directories. Do not use spaces or special characters in the deployment name.

Create New		Create new deployment
Deployment Name	TestDeployment	
	CREATE	
> Choose Existing	Choose Existing Deployment	
> Import/Upload	Import or upload a deployment	

Click **Create New**
Type a name
Click **Create**

Figure 10. Create a new deployment

- To load values from a deployment, click **Import/Upload**. Type a name for the new deployment. Drag a `deploy.properties` file onto the window or click **Browse** to select a file. Click **Upload**.

Note: If you are migrating from 7.3, you can use a `topology.xml` file from your previous version of IBM OpenPages with Watson.

> Import/Upload		Import or upload a deployment
Deployment Name	TestDeployment	
Properties File	Drop properties file here	
	BROWSE FOR FILE	
	deploy.properties	
	Remove file	
	IMPORT	

Click **Import/Upload**
Type a name
Select a file
Click **Import**

Figure 11. Import deployment properties

3. Choose **Fresh install**.

4. Optional: If you want to install IBM OpenPages solutions, see [“Considerations for IBM OpenPages solutions”](#) on page 144.
5. Set up the database server.
See [“Configuring the database server \(Db2\)”](#) on page 144 or [“Configuring the database server \(Oracle\)”](#) on page 146.
6. Set up one or more application servers.
See [“Configuring application servers”](#) on page 149.
7. Set up one or more reporting servers.
See [“Configuring reporting servers”](#) on page 150.
8. Optional: Set up the search server if you want to use the Global Search feature.
See [“Configuring a search server”](#) on page 152.
9. Click **Validate** to save and validate the deployment.

During the validation process, the installation app installs the agent software on the remote servers, starts the agents, validates the deployment properties, and verifies that the prerequisites for the installation are complete.

For example, the following image shows an application server card after validation is complete. The **Agent On** icon is green, indicating that the agent is installed and running on the remote server.

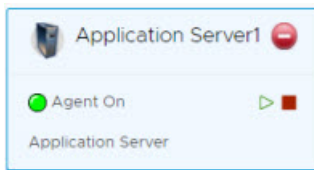


Figure 12. Agent software is running on Application Server1

Note: If you installed the agent software manually, the installation app does not install or start the agents.

You can download a validation report. Click the link at the top of the page.

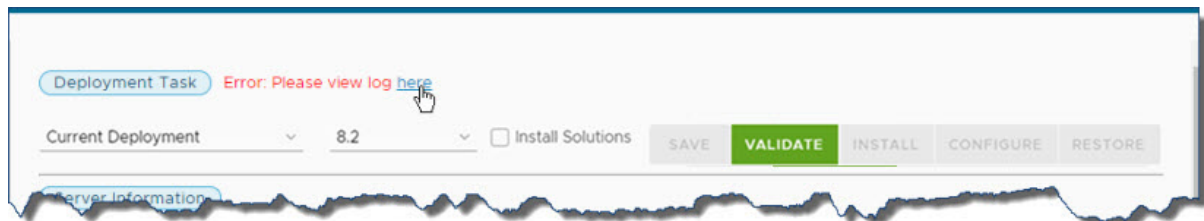


Figure 13. Click to download a validation report

The validation reports are also stored in the `<installation_server_home>/src/deployment/<deployment-name>/validation` directory.

Fix any errors and review the warnings. Click **Save**, and then click **Validate**. When the **Install** button is available, you can continue. If fixing issues requires an update to the environment variables on any servers, you must restart the installer server/agent on that server before re-validating.

10. Click **Install**.

The installation server stages the assets onto the servers in your deployment.

Tip: You can log out and close the browser window. The **Install** process continues to run. When you log in to the installation app again, the app shows the status of your deployment. You can also close the browser window during the **Configure** process.

11. Click **Configure**.

The installation server sets up and configures the IBM OpenPages with Watson components.

12. Review the log files.

For more information, see [“Log files” on page 427](#).

13. Install the latest OpenPages fix pack.

For more information, see [Chapter 11, “Fix packs,” on page 279](#).

14. If you disabled the antivirus software on remote servers, re-enable the antivirus software.

15. Optional: Download the deployment properties so that you can use the properties file for future installations.

Click , and then click **Download Properties**.

Considerations for IBM OpenPages solutions

When you install or migrate, you can choose to install solutions. Do one of the following steps:

- If you are performing a fresh installation of IBM OpenPages with Watson and you want to install OpenPages solutions, enable the **Install Solutions** check box.

Note: If you are doing a silent installation, set the module property to true in the `deploy.properties` file.

- If you are migrating to 8.2 and your source environment already has solutions, clear the **Install Solutions** check box.

Note: If you are doing a silent installation, set the module property to false in the `deploy.properties` file.

- If you are migrating to 8.2 and your source environment does not have solutions, you can install them after you complete the migration to 8.2. For more information, see [“Adding solutions to a deployment” on page 418](#).

Super Administrator

IBM OpenPages with Watson uses the concept of a Super Administrator account. You set up the Super Administrator as part of the installation. The account has complete access to all objects, folders, role templates, and groups in the OpenPages system.

In a new installation, the Super Administrator is the only user in the system. You can change the login user name and password during or after installation.

In the OpenPages documentation, the Super Administrator account is called `OpenPagesAdministrator`.

Do not use the following user names, which are reserved by OpenPages:

- OPSystem
- OpenPages
- OpenPagesApplicationUsers
- OPAdministrators

Configuring the database server (Db2)

You can use an IBM Db2 database server in your IBM OpenPages with Watson deployment.

About this task

Complete all of the fields on the **Database Server** card. You might need some information from your database administrator to complete the card.

Determine if the OpenPages database schema is installed.

- If the database schema is not yet installed, you can use the OpenPages installation app to install it. For the **Install Database** option, click **Full Database**. You must provide DBA credentials to install the database schema.
- If your database administrator completed only the database schema installation steps that require DBA privileges, use the OpenPages installation app to complete the installation. For the **Install Database** option, click **Only Non-DBA**.
- If your database administrator has already installed the database schema, you do not need to install the database. For the **Install Database** option, click **Already Installed**.

If your database administrator installed the database schema or completed the DBA installation steps, determine if your database administrator customized the table space names.

- If the table space names are customized, deselect the **Use Default Database** option. Type the custom table space names in the table space fields.
- If the table space names are not customized, enable the **Use Default Database** option.

If the database is not already installed or if your database uses custom table space names, you need the values from the `sql-wrapper.sql` file to complete the **Database Server** card.

Procedure

1. Click the **Database Server** card in the left pane.
2. Type a **Nickname** for the server.
The name is displayed on the server card.
3. Type the **Host Name** of the server. Use the fully qualified domain name (FQDN).
4. Select the **Operating System** of the server.
5. Click **Install Database** and choose one of the following options:
 - **Full Database**: Click this option if the database is not installed yet. The installation app will complete both the DBA and non-DBA portions of the database installation.
 - **Only Non-DBA**: Click this option if your database administrator completed the DBA portion of the database installation. The installation app will complete the database installation.
 - **Already Installed**: Click this option if the database is already installed.
6. If your database uses custom table space names, disable the **Use Default Database** option.
Ensure that you know the custom names. You need to enter them in a later step.
7. For the **Database Vendor**, select **DB2**.
8. Type the port number of the IBM Db2 database server in the **Database Port** field.
9. Type the name of the OpenPages database instance in the **Alias** field.
In the `sql-wrapper.sql` file, the **Alias** is specified by the `opx_db2_db_name` parameter.
10. If you chose to install the full database, type the **DBA Username** and the **DBA Password**.
The user that you specify must have both DBADM and SECADM privileges.
You need to provide the DBA credentials if you selected **Full Database** for the **Install Database** option.
In the `sql-wrapper.sql` file, the **DBA Username** is specified by the `opx_db2_instance_owner` parameter.
11. Type the credentials of the OpenPages schema owner in the **OP Database Username** and **OP Database Password** fields.
In the `sql-wrapper.sql` file, the **OP Database Username** is specified by the `opx_db_owner` parameter.
12. Type the OpenPages super administrator credentials in the **OP Admin Username** and **OP Admin Password** fields.
For more information, see [“Super Administrator”](#) on page 144.

13. Select the default currency to use in the OpenPages database.

You need to select the **Base Currency** if you selected **Full Database** or **Only Non-DBA** for the **Install Database** option.

In the `sql-wrapper.sql` file, the **Base Currency** is specified by the `opx_base_currency_iso_code` parameter.

14. Type the absolute path of the OpenPages storage directory in the **OP Storage Directory** field.

If the database installation is not complete and is being completed by the installation app, you must provide an LFS path for the storage directory. It can be updated to a UNC path after the installation is complete.

If the database installation is already complete, you can use either an LFS path or a UNC path, depending on which storage type is in place at this point in the installation. The selected storage type must match the current storage type that is defined in the database. For more information, see [“Updating the location of the openpages-storage directory \(Db2\)” on page 161](#) or [“Updating the location of the openpages-storage directory \(Oracle\)” on page 163](#).

15. If you selected the **Install Solutions** check box, configure the metrics for solutions.

- **Module Assessment Method:** Select the risk assessment method.
- **Total Likelihood Count:** The Total Likelihood Count identifies the scale of inherent and residual risk likelihood. Select the maximum value for the scale.
- **Total Impact Count:** The Total Impact Count identifies the scale of inherent and residual risk impact. Select the maximum value for the scale.

The count that you specify determines the number of choices available for inherent and residual impact and likelihood fields in risk objects. For example, if **Total Impact Count** is set to 4, then the available choices for Inherent Impact, Residual Impact, Audit Inherent Impact, and Audit Residual Impact are: 1, 2, 3, 4.

You can modify these settings at a later time. **Total Likelihood Count** is called **YMAX** in the registry settings and **Total Impact Count** is called **XMAX**.

16. If your database uses custom table space names, complete the table space name fields.

You need to provide the table space names if the **Use Default Database** option is disabled.

In the `sql-wrapper.sql` file, the table space names are specified by the `opx_dflt_*_ts` parameters.

17. If you want to use the rollback feature for this server, enable the **Rollback on failure** option.

When **Rollback on failure** is enabled and an error occurs, the operation that caused the failure is rolled back. You can then fix the error and continue with the installation. The installation process resumes at the operation that was rolled back.

For example, if an error occurs during the **Install** process, fix the error and then click **Install** to continue.

18. Click **Save**.

Configuring the database server (Oracle)

You can use an Oracle database server in your IBM OpenPages with Watson deployment.

About this task

Complete all of the fields on the **Database Server** card. You might need some information from your database administrator to complete the card.

Determine if the OpenPages database schema is installed.

- If the database schema is not yet installed, you can use the OpenPages installation app to install it. For the **Install Database** option, click **Full Database**. You must provide DBA credentials to install the database schema.

- If your database administrator completed only the database schema installation steps that require DBA privileges, use the OpenPages installation app to complete the installation. For the **Install Database** option, click **Only Non-DBA**.
- If your database administrator has already installed the database schema, you do not need to install the database. For the **Install Database** option, click **Already Installed**.

If your database administrator installed the database schema or completed the DBA installation steps, determine if your database administrator customized the table space names.

- If the table space names are customized, deselect the **Use Default Database** option. Type the custom table space names in the table space fields.
- If the table space names are not customized, enable the **Use Default Database** option.

If the database is not already installed or if your database uses custom table space names, you need the values from the `sql-wrapper.sql` file to complete the **Database Server** card.

Procedure

1. Click the **Database Server** card in the left pane.
2. Type a **Nickname** for the server.
The name is displayed on the server card.
3. Type the **Host Name** of the server. Use the fully qualified domain name (FQDN).
4. Select the **Operating System** of the server.
5. Click **Install Database** and choose one of the following options:
 - **Full Database:** Click this option if the database schema is not installed yet. The installation app will complete both the DBA and non-DBA portions of the database schema installation.
 - **Only Non-DBA:** Click this option if your database administrator completed the DBA portion of the database schema installation. The installation app will complete the database schema installation.
 - **Already Installed:** Click this option if the database schema is already installed.
6. If your database uses custom table space names, disable the **Use Default Database** option.
Ensure that you know the custom names. You need to enter them in a later step.
7. For the **Database Vendor**, select **Oracle**.
8. Type the port number of the Oracle database server in the **Database Port** field.
9. Complete the identification information that will be used to build the JDBC connection string for the OpenPages database.
 - To use the system identifier, click **SID** and type the system identifier in the **Identifier** field.
 - To use the service name, click **Service Name** and type the name in the **Identifier** field.
10. Type the name of the OpenPages database alias in the **Alias** field. In the `sql-wrapper.sql` file, the **Alias** is specified by the `opx_dflt_sid` parameter.
11. If you chose to install the full database, type the **DBA Username** and the **DBA Password**.
The user that you specify must have SYSDBA privileges.

You need to provide the DBA credentials if you selected **Full Database** for the **Install Database** option.

In the `sql-wrapper.sql` file, the **DBA Username** is specified by the `opx_oracle_dba_user` parameter.
12. Type the credentials of the OpenPages schema owner in the **OP Database Username** and **OP Database Password** fields.

In the `sql-wrapper.sql` file, the **OP Database Username** is specified by the `opx_db_owner` parameter.
13. Type the OpenPages super administrator credentials in the **OP Admin Username** and **OP Admin Password** fields.

For more information, see “Super Administrator” on page 144.

14. Select the default currency to use in the OpenPages database.

You need to select the **Base Currency** if you selected **Full Database** or **Only Non-DBA** for the **Install Database** option.

In the `sql-wrapper.sql` file, the **Base Currency** is specified by the `opx_base_currency_iso_code` parameter.

15. Type the absolute path of the OpenPages storage directory in the **OP Storage Directory** field.

If the database installation is not complete and is being completed by the installation app, you must provide an LFS path for the storage directory. It can be updated to a UNC path after the installation is complete.

If the database installation is already complete, you can use either an LFS path or a UNC path, depending on which storage type is in place at this point in the installation. The selected storage type must match the current storage type that is defined in the database. For more information, see “Updating the location of the openpages-storage directory (Db2)” on page 161 or “Updating the location of the openpages-storage directory (Oracle)” on page 163.

16. If you selected the **Install Solutions** check box, configure the metrics for solutions.

- **Module Assessment Method:** Select the risk assessment method.
- **Total Likelihood Count:** The Total Likelihood Count identifies the scale of inherent and residual risk likelihood. Select the maximum value for the scale.
- **Total Impact Count:** The Total Impact Count identifies the scale of inherent and residual risk impact. Select the maximum value for the scale.

The count that you specify determines the number of choices available for inherent and residual impact and likelihood fields in risk objects. For example, if **Total Impact Count** is set to 4, then the available choices for Inherent Impact, Residual Impact, Audit Inherent Impact, and Audit Residual Impact are: 1, 2, 3, 4.

You can modify these settings at a later time. **Total Likelihood Count** is called **YMAX** in the registry settings and **Total Impact Count** is called **XMAX**.

17. If your database uses custom table space names, complete the table space name fields.

You need to provide the table space names if the **Use Default Database** option is disabled.

In the `sql-wrapper.sql` file, the table space names are specified by the `opx_dflt_*_ts` parameters.

18. Type the path to the data home directory for the OpenPages database in the **Oracle Data Home Directory** field.

You need to provide the data home directory path if you selected **Full Database** for the **Install Database** option.

To find the **Oracle Data Home Directory**, log in to the OpenPages database and then run the following SQL:

```
$ sqlplus openpage/"password"@OP
SQL> select file_name from dba_data_files where TABLESPACE_NAME = 'SYSTEM';
```

The SQL returns the path to the **Oracle Data Home Directory**:

```
FILE_NAME
<path_to_oracle_data_home>/system01.dbf
```

For example, for a non-PDB database that is called OP: `/home/oracle/app/oradata/OP`
Or, for a PDB database that is called OP: `/home/oracle/app/oradata/OPCDB/OP`

19. Type the **Oracle Cognos JDBC Username** and the **Oracle Cognos JDBC Password**.
20. Type the TNS alias of the Cognos database in the **Oracle Cognos DB Alias** field.

Note: If you are using the same database instance for Cognos and OpenPages, you must use the same alias as the OpenPages database.

21. If you want to use Oracle Text, enable the **Oracle Enable Text Search** option.

When the Oracle Text feature is enabled, you can filter based on the contents of fields with long string data types.

In the `sql-wrapper.sql` file, the **Oracle Enable Text Search** option is specified by the `flag_install_oracle_text` parameter.

22. If you want to skip the database memory configuration checks during the installation, enable the **Oracle Skip DB Memory Check** option.

Your database administrator might ask you to disable the memory checks. For more information, see [“Memory validation step fails for an Oracle database” on page 459](#).

23. If you want to use the rollback feature for this server, enable the **Rollback on failure** option.

When **Rollback on failure** is enabled and an error occurs, the operation that caused the failure is rolled back. You can then fix the error and continue with the installation. The installation process resumes at the operation that was rolled back.

For example, if an error occurs during the **Install** process, fix the error and then click **Install** to continue.

24. Optional: Click **Save**.

Configuring application servers

You can use one or more application servers in your IBM OpenPages with Watson deployment.

About this task

You can scale the application server by adding horizontal or vertical cluster members.

- To add horizontal cluster members, add an **Application Server** card for each cluster member.
- To add vertical cluster members, use the **OP Vertical Cluster Number** field to specify the number of cluster members.

You must configure a load balancer to distribute the incoming requests across the cluster members.

For more information, see [“Configure clustered environments” on page 31](#).

Procedure

1. Click the **Application Server1** card in the left pane.

Application Server1 is the admin application server.

2. Type a **Nickname** for the server.

The name is displayed on the server card.

3. Type the **Host Name** of the server. Use the fully qualified domain name (FQDN).

4. If you are on the **Application Server1** card, select the **Operating System** of your application servers.

The **Operating System** that you select on the **Application Server1** card sets the operating system for all application servers in your deployment.

5. If the server is on a different physical machine than the installation server, enable the **Remote Deploy** option.

The agent software is installed on the remote server automatically.

Complete the following fields:

- **Agent Port:** Type the port number for the agent software to use.

Note: If the host name is the same in any two cards, port synchronization will work only if you complete the host information before you complete the **Agent Port** field. Ensure that the port

number is the same on any two cards where the host name is the same. If the port number is not the same on both cards, you will encounter exceptions during the validation phase where agents are installed automatically on target systems.

- **SSH Port** (Linux only): Type the Secure Shell (SSH) port number of the remote server.
- **Local User Name** and **Local User Password**: Type the credentials of the OpenPages installation user on the remote server. The account is used to install the agent software on the remote server. You can specify a local account that is on the remote server or a service account, for example `<domain>/<user name>`.

Note: If you installed the agent manually, you can leave the **Local User Name** and **Local User Password** fields empty. Ensure that the agents are started before you install OpenPages.

- **Agent Directory**: Type the absolute path to the directory on the remote server where you want the agent software installed.

Note: If you are using Microsoft Windows, the maximum length of the path is 25 characters.

6. Type the absolute path of the OpenPages home directory in the **OP Home Directory** field.

You can use different home directories for each application server in your deployment.

7. Type a name for the application server in the **OP Server Name** field.
8. Type the starting port number for OpenPages services in the **OP Cluster Start Port** field.

The field defines the start of a contiguous range of 20 port numbers from the starting port that can be used for OpenPages services that run on the application server.

9. If you want to add vertical cluster members to the server, type a number greater than 1 in the **OP Vertical Cluster Number** field.
10. Type the absolute path of the directory to use for the OPBackup and OPRestore utilities in the **OP Backup Restore Directory** field.
11. Type the absolute path of the database client home directory in the **DB Client Directory** field.
12. Type the absolute path of the **Java Home Directory** on the server.

The **Java Home Directory** is where the JRE of the IBM SDK is installed, for example `C:\IBM\java_8.0_64` or `/opt/IBM/java_8.0_64`. The path that you enter must match the path in the `JAVA_HOME` system environment variable on the server

13. If you want to use the rollback feature for this server, enable the **Rollback on failure** option.

When **Rollback on failure** is enabled and an error occurs, the operation that caused the failure is rolled back. You can then fix the error and continue with the installation. The installation process resumes at the operation that was rolled back.

For example, if an error occurs during the **Install** process, fix the error and then click **Install** to continue.

14. Optional: Click **Save**.

Configuring reporting servers

You can use one or more reporting servers in your IBM OpenPages with Watson deployment.

About this task

You can scale the reporting server by adding horizontal members. To add horizontal cluster members, add a **Reporting Server** card for each cluster member.

You must configure additional Cognos dispatchers to ensure that the incoming requests are distributed across the reporting servers.

For more information, see [“Configure clustered environments” on page 31](#).

Procedure

1. Click the **Report Server1** card in the left pane.
2. Type a **Nickname** for the server.
The name is displayed on the server card.
3. Type the **Host Name** of the server. Use the fully qualified domain name (FQDN).
4. Select the **Operating System** of the server.
5. If the server is on a different physical machine than the installation server, enable the **Remote Deploy** option.

The agent software is installed on the remote server automatically.

Complete the following fields:

- **Agent Port:** Type the port number for the agent software to use.

Note: If the host name is the same in any two cards, port synchronization will work only if you complete the host information before you complete the **Agent Port** field. Ensure that the port number is the same on any two cards where the host name is the same. If the port number is not the same on both cards, you will encounter exceptions during the validation phase where agents are installed automatically on target systems.

- **SSH Port** (Linux only): Type the Secure Shell (SSH) port number of the remote server.
- **Local User Name** and **Local User Password:** Type the credentials of the OpenPages installation user on the remote server. The account is used to install the agent software on the remote server. You can specify a local account that is on the remote server or a service account, for example `<domain>/<user name>`.

Note: If you installed the agent manually, you can leave the **Local User Name** and **Local User Password** fields empty. Ensure that the agents are started before you install OpenPages.

- **Agent Directory:** Type the absolute path to the directory on the remote server where you want the agent software installed.

Note: If you are using Microsoft Windows, the maximum length of the path is 25 characters.

6. Type the absolute path of the **Cognos Home Directory**.
7. Type the **Cognos Port** and **Cognos Dispatcher Port**
8. Type the Cognos application URL context root in the **URL Context Root** field.
9. Type the Cognos Framework Manager port in the **Framework Port** field.
10. Type the **Framework Output Directory** property.
11. Type the absolute path of the directory on the reporting server where you want to install IBM OpenPages CommandCenter in the **Command Center Home Directory**.
12. Type the absolute path of the directory to use for the OPCCBackup and OPCCRestore utilities in the **Command Center Backup Directory** field.
13. Type the absolute path to the home directory of the database client that is used to connect to the OpenPages database in the **DB Client Directory** field.
14. Type the absolute path of the **Java Home Directory** on the reporting server.

If you are using the IBM Java that is supplied with Cognos, the **Java Home Directory** is where the Cognos IBM Java is installed.

The path that you enter must match the path in the JAVA_HOME system environment variable on the reporting server.

15. If you want to use the rollback feature for this server, enable the **Rollback on failure** option.

When **Rollback on failure** is enabled and an error occurs, the operation that caused the failure is rolled back. You can then fix the error and continue with the installation. The installation process resumes at the operation that was rolled back.


For example, if an error occurs during the **Install** process, fix the error and then click **Install** to continue.

16. Optional: Click **Save**.

Configuring a search server

You can use one search server in your IBM OpenPages with Watson deployment. The search server is optional. Configure a search server if you want to use global search.

Procedure

1. Click the server list, select **Global Search Server**, and then click . Click **Continue** to confirm.
A **Global Search** card is added in the left pane.

2. Type a **Nickname** for the server.

The name is displayed on the server card.

3. Type the **Host Name** of the server. Use the fully qualified domain name (FQDN).

4. Select the **Operating System** of the server.

5. If the server is on a different physical machine than the installation server, enable the **Remote Deploy** option.

The agent software is installed on the remote server automatically.

Complete the following fields:

- **Agent Port:** Type the port number for the agent software to use.

Note: If the host name is the same in any two cards, port synchronization will work only if you complete the host information before you complete the **Agent Port** field. Ensure that the port number is the same on any two cards where the host name is the same. If the port number is not the same on both cards, you will encounter exceptions during the validation phase where agents are installed automatically on target systems.

- **SSH Port** (Linux only): Type the Secure Shell (SSH) port number of the remote server.

- **Local User Name** and **Local User Password:** Type the credentials of the OpenPages installation user on the remote server. The account is used to install the agent software on the remote server. You can specify a local account that is on the remote server or a service account, for example `<domain>/<user name>`.

Note: If you installed the agent manually, you can leave the **Local User Name** and **Local User Password** fields empty. Ensure that the agents are started before you install OpenPages.

- **Agent Directory:** Type the absolute path to the directory on the remote server where you want the agent software installed.

Note: If you are using Microsoft Windows, the maximum length of the path is 25 characters.

6. Type the absolute path of the directory where you want to install global search in the **Search Home Directory** field.

The directory that you specify is the SEARCH_HOME directory for your deployment. The opsearchtools.jar file, Apache Solr, and other global search files are installed in this directory. The global search indexing directory is also stored under the **Search Home Directory**.

7. Select a language from the **Search Language** list.

The language that you select is used by the search server for indexing.

8. Type the absolute path of the **Java Home Directory** on the server.

The **Java Home Directory** is where the IBM SDK is installed, for example C:\IBM\java_8.0_64 or /opt/IBM/java_8.0_64. The path that you enter must match the path in the JAVA_HOME system environment variable on the server

9. If you want to use the rollback feature for this server, enable the **Rollback on failure** option.

When **Rollback on failure** is enabled and an error occurs, the operation that caused the failure is rolled back. You can then fix the error and continue with the installation. The installation process resumes at the operation that was rolled back.

For example, if an error occurs during the **Install** process, fix the error and then click **Install** to continue.

10. Optional: Click **Save**.

Post installation tasks

After you install IBM OpenPages with Watson, you must perform some post installation tasks.

You can also modify the installation environment to improve performance, enhance security, or change default settings. For example, you can tune the application servers or configure LDAP.

As part of the post installation tasks, you can configure OpenPages with Watson to use Transport Layer Security (TLS) to ensure that all data passed between the application server and a browser remains private.

For information about TLS and other configurations, such as changing port numbers or changing passwords, see the *IBM OpenPages with Watson Administrator's Guide*.

After you complete the installation, consider backing up your environment by running OPBackup and OPCCBackup.

Updating WebSphere Liberty on application servers

You can update IBM WebSphere Liberty on the IBM OpenPages with Watson application servers. This task is optional.

Before you begin

Ensure that JAVA_HOME is defined.

About this task

Do this task on the admin application server and each non-admin horizontal cluster member.

Note: All application servers in your environment must use the same version of WebSphere Liberty.

Procedure

1. Download the WebSphere Liberty Kernel package. Copy the .zip file to a temporary directory on each application server.
The package is available from <https://developer.ibm.com/wasdev/downloads/#asset/runtimes-wlp-kernel>.
2. Log on to an application server as a user with administrative privileges.
3. Back up your current WebSphere Liberty installation.
 - a) Stop the OpenPages services.
For more information, see the *IBM OpenPages with Watson Installation and Deployment Guide*.
 - b) Go to the <OP_HOME> directory.
 - c) Rename the wlp directory to wlp_backup.
4. Install the new version of WebSphere Liberty.
 - a) Extract the downloaded .zip file to the temporary directory on the application server.
 - b) Copy the wlp directory from the temporary directory to the <OP_HOME> directory.
 - c) Copy the etc directory from <OP_HOME>/wlp_backup to <OP_HOME>/wlp.

- d) If the application server cannot access the internet, continue with the steps in the following topic: [“Updating WebSphere Liberty features manually”](#) on page 154.
- e) Go to the <OP_HOME>/wlp/bin directory, and then run the following command:

Linux

```
./installUtility install --acceptLicense <server_name>
```

Windows

```
installUtility.bat install --acceptLicense <server_name>
```

Where <server_name> is the name of the application server. If your application server uses vertical cluster members, run this command on <server_name>Server1.

- f) Restart the OpenPages application servers.

For more information, see the *IBM OpenPages with Watson Installation and Deployment Guide*.

5. Repeat steps 3 and 4 on each horizontal cluster application server.

Updating WebSphere Liberty features manually

If your application servers cannot access the internet, do the following steps to download and install WebSphere Liberty features manually.

Before you begin

Ensure that JAVA_HOME is defined.

Verify that you have the WebSphere Liberty Kernel package and that you have a backup of the <OP_HOME>/wlp directory. See [“Updating WebSphere Liberty on application servers”](#) on page 153.

About this task

The version of WebSphere Liberty that is included with IBM OpenPages with Watson 8.2.0.x uses the following features:

```
wasJmsServer-1.0
wasJmsClient-2.0
distributedMap-1.0
appSecurity-2.0
ejbLite-3.2
jaxws-2.2
jdbc-4.1
jndi-1.0
localConnector-1.0
jsp-2.3
jaxb-2.2
passwordUtilities-1.0
jca-1.7
concurrent-1.0
websocket-1.1
javaMail-1.6
servlet-4.0
spnego-1.0
samlweb-2.0
openidconnectclient-1.0
transportSecurity-1.0
mdb-3.2
jwt-1.0
mpjwt-1.1
io.openliberty.servlet.internal-4.0
```

For information about these features, see the [WebSphere documentation](#).

Procedure

1. Log on to a server that has access to the internet.

2. Create a temporary directory.
3. Extract the WebSphere Liberty Kernel package to the temporary directory.
4. Go to the `<temp_dir>/wlp/bin` directory.

Where `<temp_dir>` is the name of the temporary directory that you created.

5. For each feature listed in [About this task](#), run the following command:

Linux

```
./installUtility download <feature name> --location=<temp_dir>/repo
```

Windows

```
installUtility.bat download <feature name> --location=<temp_dir>/repo
```

Where `<feature_name>` is the name of the feature to install.

6. Copy the contents of the `<temp_dir>/repo/features` directory to the following directory on each application server: `<OP_HOME>/temp/wlp/repo/features`.
7. Install the new features that you downloaded.
 - a) Go to the `<OP_HOME>/wlp/bin` directory, and then run the following command:

Linux

```
./installUtility install --acceptLicense <server_name>
```

Windows

```
installUtility.bat install --acceptLicense <server_name>
```

Where `<server_name>` is the name of the application server. If your application server uses vertical cluster members, run this command on `<server_name>Server1`.

- b) Restart the OpenPages application servers.

For more information, see the *IBM OpenPages with Watson Installation and Deployment Guide*.

8. Repeat step 7 on each horizontal cluster application server.

OpenPages with Watson CommandCenter post-installation tasks

After you install IBM OpenPages CommandCenter on the reporting servers, some post installation tasks are required. You must update the CommandCenter configuration files to ensure that OpenPages components can communicate with each other.

Copying the IBM Global Security Kit files to the Db2 server installations on Windows operating systems

On Windows operating systems, you must copy the 32-bit version of the IBM Global Security Kit (GSK) files to the IBM Db2 server instance location. You must copy the files before you generate the reporting framework.

Procedure

1. Log on to the database server computer.
2. Go to the `<DB2_HOME>\bin` directory for the IBM OpenPages with Watson database instance and create a folder named `icc`.
3. Copy the contents of the `C:\Program Files (x86)\IBM\gsk8\lib` directory to the `<DB2_HOME>\bin\icc` directory.

Updating IBM WebSphere Application Server Liberty for the Framework Model Generator

You can update the IBM WebSphere Application Server Liberty profile for the IBM OpenPages with Watson Framework Model Generator. Update WebSphere Liberty after you install, upgrade, or migrate IBM OpenPages with Watson.

Before you begin

Ensure that JAVA_HOME is defined.

About this task

You can update WebSphere Liberty by using IBM Installation Manager. Open IBM WebSphere and click the link to download and install updates. For more information, see [Installing Liberty on distributed operating systems by using the GUI](#) in IBM Documentation.

Alternatively, you can download the update and install it manually.

Procedure

1. Log on to the active reporting server as a user with administrative privileges.
2. Go to the Framework Model Generator home page, `http://<server name>:<server port>`
3. Click the link to download WebSphere Application Server Liberty Runtime. Save the .zip file to a temporary directory.
4. Back up your current WebSphere Liberty installation.
 - a) Stop the Framework Model Generator.
For more information, see the *IBM OpenPages with Watson Installation and Deployment Guide*.
 - b) Go to the <CC_HOME> directory.
 - c) Rename the wlp directory to wlp_backup.
5. Install the new version of WebSphere Liberty.
 - a) Extract the downloaded .zip file to the temporary directory on the active reporting server.
 - b) Copy the wlp directory from the temporary directory to the <CC_HOME> directory.
6. Configure WebSphere Liberty.
 - a) Go to the <CC_HOME>/wlp_backup/bin directory and copy the script file server or server.bat to the <CC_HOME>/wlp/bin directory
 - b) If you are using Windows, copy the Windows services files prunsrv.exe and openpages_wlp_svc_setup.bat from <CC_HOME>/wlp_backup/bin to <CC_HOME>/wlp/bin.
 - c) Copy the IBMOpenPagesFrameworkModelGenerator directory from <CC_HOME>/wlp_backup/usr/servers to <CC_HOME>/wlp/usr/servers.
7. Start the Framework Model Generator.
For more information, see the *IBM OpenPages with Watson Installation and Deployment Guide*.

Creating the reporting schema and framework





To see the default IBM OpenPages with Watson reports, you must create a reporting schema and update the reporting framework.

Before you begin

- Start the Framework Model Generator. For more information, see [“Starting and stopping the OpenPages with Watson Framework Model Generator service on Windows” on page 318](#) or [“Starting and stopping the OpenPages with Watson Framework Model Generator service on Linux” on page 318](#).

- If you are using clustered environments, ensure you have configured them before you create the reporting schema and framework. For more information, see [“Configure clustered environments”](#) on page 31.

Procedure

1. In a web browser, open OpenPages with Watson.
`http://<openpages_server>:<port>/openpages`
2. Log on to the application as a user with administrative privileges.
3. Click , and then click **Enable System Admin Mode**.
4. Click  > **System Configuration** > **Reporting Schema**.
5. Click **Create**.
6. After the create operation finishes, click  > **Disable System Admin Mode**.
7. Click  > **Cognos Analytics** > **Reporting Framework Generation**.
8. On the **Reporting Framework** page, click **Update**.
9. In the **Reporting Framework Generation** panel, select **Framework Model** and **Labels** and other options you want for the relational data model.
10. Click **Submit**.
11. To view the progress of the update, click **Refresh**.

The **Percent Complete** column on the **Reporting Framework** table updates the percentage of completion.

Results

Updating the reporting framework process takes approximately 30 minutes or longer.

OpenPages with Watson CommandCenter portal security

After installation, you can restrict which user groups are allowed to modify reports. To grant IBM OpenPages with Watson CommandCenter administrative rights, create a group in the OpenPages application or use an existing group, such as OPAdministrators. This is optional.

To restrict user access to administrative functions within the IBM Cognos Analytics, use IBM Cognos Administration. To prevent users from deleting, changing, or saving reports, restrict access to the OpenPages reports that are in Public Folders. You can also restrict users from running reporting tools, such as Cognos Analytics - Reporting, or from modifying reports.

For more information, see the *IBM OpenPages with Watson Administrator's Guide*.

Creating an open session command block for the OpenPages data source

You must create an open session command block for the OpenPages data source in IBM Cognos Analytics.

Procedure

1. Log on to IBM Cognos Analytics as a user with administrative privileges..
 - In the Task Focused UI, click **Analytics**.
 - Or, go to the following URL: `http://<hostname>/ibmcognos/bi`
Where <hostname> is the name of the Cognos server.
2. Click **Manage** > **Administration Console** to launch the **IBM Cognos Administration** page.
3. Click the **Configuration** tab.

- Click **OpenPages DataSource**.

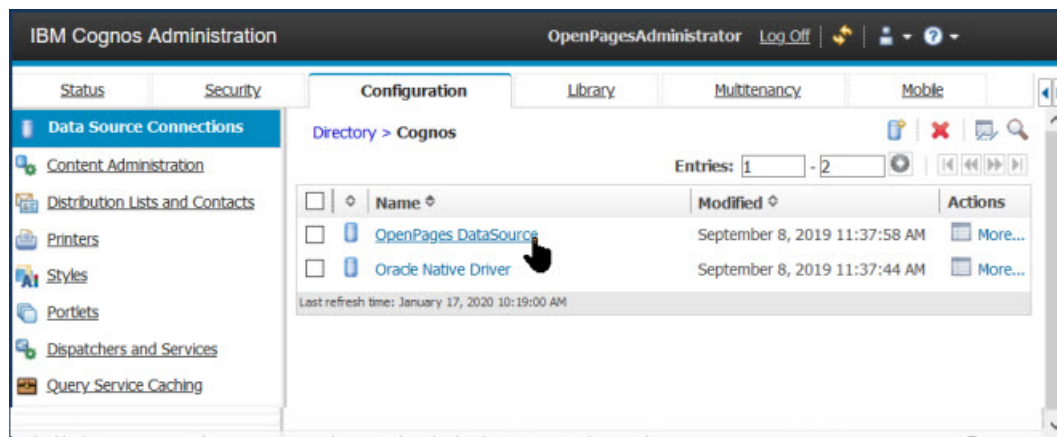



Figure 14. The Configuration tab in Cognos Configuration

- In the **Actions** column, click .
- Click the **Connection** tab.
- Expand the **Commands** section.
- Next to the **Open session commands**, click **Set**.
- In the **XML database commands** box, paste the following text:

```
<commandBlock>
<commands>
<sqlCommand>
<sql>begin OP_SESSION_MGR.SET_ACTOR_ID_PRIVATE (#$account.parameters.openPagesUserId#);
OP_CRYPT_MGR.SET_ENCRYPTION_PARAMS (#$account.parameters.openPagesEncryptKey#,
#$account.parameters.openPagesEncryptAlgorithm#,
#$account.parameters.openPagesEncryptPrefix#);
end;
</sql>
</sqlCommand>
</commands>
</commandBlock>
```

- Click **OK** to save your changes.
- Click **OK** again.
- Restart Cognos.

Loading the Cognos dashboard integration after installing

After you install IBM OpenPages with Watson, you can load an integration configuration so that you can use Cognos Analytics dashboards within OpenPages.

Procedure

- Copy the `CommandCenter-integration-op-config.xml` and `CommandCenter-integration-op-file-content.zip` files from the OpenPages installation media to the administrative application server.

The files are located in the `/OP_<version>_Main/OP_<version>_Configuration/CommandCenter/loader-data` directory.

- Open a command line.

If you are using Microsoft Windows, open a command prompt with the **Run as administrator** option.

- Go to the `<OP_HOME>/bin` directory.
- Run the following command to load the files.

Replace `<loader-file-path>` with the location of the `CommandCenter-integration-op-config.xml` and `CommandCenter-integration-op-file-content.zip` files.


```
ObjectManager.cmd|sh 1 c <OpenPages Administrator user> <OpenPages Administrator password>  
<loader-file-path> CommandCenter-integration
```

5. If you encounter any errors, review the log file, `<loader-file-path>/ObjectManager.log`.

Configuring OpenPages applications to use a domain account on Windows operating systems

In a clustered environment, the IBM OpenPages with Watson application services access a file share. The account that starts the services must have permissions to the file share.

Configuring the OpenPages applications to use a domain account must be done for new installations and migrations.

About this task

By default, on Windows operating systems, services run under the `LocalSystem` account. This account cannot access a shared drive on another computer. In a horizontal cluster, configure the OpenPages application services on all application servers to run under a domain account that has access to the shared drive.

For application servers, the following OpenPages service must have permissions to the file share:

- `<server_name>Server<#>`

For the OpenPages installation server, the following application service must have permissions to the file share:

- `ibmopenpageswithwatsoninstaller<version>.exe`

Procedure

1. Log on to each application server as a user with administrative privileges.
2. Open the **Services** control panel.
3. Stop each of the OpenPages services.
 - a) Right-click the service name, and select **Properties** from the menu.
 - b) In the **Properties** window, click the **Log On** tab.
 - c) Select **This account**.
 - d) Type a domain, account name, and password for at least one user who has access to the shared drive.
 - e) Click **OK** to continue.

Configuring file share permissions on Linux operating systems

For clustered IBM OpenPages with Watson environments that run on Linux operating systems, configure the same user name and password on all systems. File share permissions are the same on all systems. If you are using a network file share (NFS), ensure that users have read and write access to the file share.

Sharing a network OpenPages storage directory on Linux operating systems

When you install IBM OpenPages with Watson, you specify the **OP Storage Directory** location on the **Database Server** card. The storage location is a directory where attached files and forms that are associated with OpenPages objects are stored.

If you pointed to a location on the local computer and you are using a horizontal cluster for the application servers, you must change the pointer to a shared network storage location.

After you share the directory, use the `update-storage` script to update the database with the shared network location.

Procedure

1. Mount the storage directory on the admin application server to the non-admin server.
 - a) Log on to the OpenPages admin application server as the root user or a user that belongs to the System group, and open a shell.
 - b) Go to the /etc directory, and open the hosts file in a text editor.
 - c) Add the IP address and name of each OpenPages horizontal cluster member.
 - d) Save and close the hosts file.
 - e) Create a file with the name exports in the /etc directory.

Important: Ensure that you have full rights to the local installation directory.

- f) Open the exports file in a text editor and add the full path to the storage directory followed by *(insecure,rw,async,no_root_squash).

```
/opt/OpenPages/openpages-storage *(insecure,rw,async,no_root_squash)
```

- g) Export all file systems that are named in /etc/exports directory by using the following command:

```
exportfs -a
```

The **exportfs** command maintains the current table of exported file systems for NFS in the /var/lib/nfs/etc file.

- h) Restart the NFS server.

Use the following command:

```
service nfs restart
```

The NFS server processes requests from the NFS clients.

- i) Use the following command to check that the openpages-storage directory is exported and ready for mounting:

```
showmount -e
```

Ensure that the openpages-storage directory is listed.

2. Mount the storage directory from the admin application server on the horizontal cluster member.
 - a) Log on to the OpenPages horizontal cluster member as the root user or a user that belongs to the System group.
 - b) Open a shell as a user with administrative privileges.
 - c) Go to the /etc directory.
 - d) Open the hosts file in a text editor and add the IP address and name of each OpenPages horizontal cluster member.
 - e) Save and close the hosts file.
 - f) Run the following command to mount the storage directory:

```
mount <nfsservername> <mountpoint>
```

- <nfsservername> is the name of the OpenPages admin application server and the location of the openpages-storage directory on the admin server.
- <mountpoint> is the name and path of the openpages-storage directory on the horizontal cluster member.

Example:

```
mount server.openpages.com:/usr/OpenPages/openpages-storage
/usr/OpenPages/openpages-storage
```

3. Update the location of the openpages-storage directory in the database.
 - Db2: [“Updating the location of the openpages-storage directory \(Db2\)”](#) on page 161
 - Oracle: [“Updating the location of the openpages-storage directory \(Oracle\)”](#) on page 163

Sharing a network OpenPages storage directory on Windows operating systems

When you install IBM OpenPages with Watson, you specify the **OP Storage Directory** location on the **Database Server** card. The storage location is a directory where attached files and forms that are associated with OpenPages objects are stored.

If you pointed to a location on the local computer and you are using a horizontal cluster for the application servers, you must change the pointer to a shared network storage location. Ensure that all cluster members can access the directory. If you are using a search server, ensure that the search server can also access the shared network location.

After you share the directory, use the update-storage script to update the database with shared network location.

Updating the location of the openpages-storage directory (Db2)

In the database, update the location of the **openpages-storage** directory.

If you are using Microsoft Windows, you can also use this procedure to change the storage type from LFS to UNC.

Before you begin

Stop the IBM OpenPages with Watson services if they are running.

Procedure

1. Log on to the target environment as a user with administrative permissions. You can use any system with access to CLPPlus that can connect to the database server.
2. Open a command or shell window.
3. Locate the update-storage.sql script.

The script is stored in the following directories. You can use the script in either location.

- /OP_<version>_Main/OP_<version>_Configuration/Database/DB2/INSTALL_SCRIPTS
 - /OP_<version>_Main/OP_<version>_Configuration/Database/DB2/UPGRADE_SCRIPTS
4. Run the update-storage.sql script to update the openpages-storage directory location in the database:

```
clpplus -nw <op_db_user>/\ '<op_db_password>\'@<database_host>:
<database_port>/<database_name> @sql-wrapper update-storage <log_file>
<database_host> <database_port> <database_name> <op_db_user>
<op_db_password> <storage_type> <storage_server_name> <host_name>
<os_type> <path_or_unc_name>
```

Table 53. Parameters in the update-storage.sql script (Db2)

Parameter	Description
<op_db_user>	OpenPages user name for accessing the OpenPages database.

Table 53. Parameters in the update-storage.sql script (Db2) (continued)	
Parameter	Description
<op_db_password>	The OpenPages password for accessing the OpenPages database. If the password contains special characters, surround the password in quotation marks: <ul style="list-style-type: none"> Windows: 'password' Linux: \'password\'
<database_host>	Name of the Db2 server host machine that contains the OpenPages database.
<database_port>	Port number of the Db2 database instance that is installed on the database server. For Db2, the default port is 50000.
<database_name>	Name of the OpenPages database.
<log_file>	The name of the log file that the script creates and writes information to.
<storage_type>	The type of file storage to be used. Valid values are as follows: <ul style="list-style-type: none"> LFS (local file system) UNC (Universal Naming Convention) - for Windows only. Note: After you move from LFS to UNC, you cannot go back to using LFS.
<storage_server_name>	The name of the storage server.
<host_name>	The host name of the machine.
<os_type>	The type of operating system. Valid values are as follows: <ul style="list-style-type: none"> Windows Unix
<path_or UNC_name>	The file path or UNC of the storage location. If the path contains backslashes, wrap the path in single quotation marks.

Examples

• LFS

Windows

```
clpplus -nw openpage/'password'@myserver.ibm.com:50000/opx
@sql-wrapper update-storage output.log myserver.ibm.com 50000 OPX openpage 'password'
LFS eng11 eng11 Windows 'C:\IBM\OpenPages\openpages-storage'
```

Linux

```
clpplus -nw openpage/\'password\'@myserver.ibm.com:50000/opx
@sql-wrapper update-storage output.log myserver.ibm.com 50000 opx openpage \'password\'
LFS eng11 eng11 Unix /usr/opdata/openpages-storage
```

• UNC

Windows

```
clpplus -nw openpage/'password'@myserver.ibm.com:50000/opx
@sql-wrapper update-storage output.log myserver.ibm.com 50000 OPX openpage 'password'
UNC eng11 eng11 Windows openpages-storage
```

Updating the location of the openpages - storage directory (Oracle)

In the database, update the location of the **openpages - storage** directory.

If you are using Microsoft Windows, you can also use this procedure to change the storage type from LFS to UNC.

Before you begin

Stop the IBM OpenPages with Watson services if they are running.

Procedure

1. Log on to the target environment as a user with administrative permissions. You can use any system with access to SQL*Plus that can connect to the database server.
2. Open a command or shell window.
3. Locate the `update-storage.sql` script.

The script is stored in the following directories. You can use the script in either location.

- `/OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/INSTALL_SCRIPTS` directory.
 - `/OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/UPGRADE_SCRIPTS`
4. Run the `update-storage.sql` script to update the openpages - storage directory location in the database:

```
sqlplus /nolog @sql-wrapper.sql update-storage.sql <log_file> <oracle_tns_alias>  
<op_db_user> <op_db_password> <storage_type> <storage_server_name> <host_name>  
<os_type> <path_or_UNC_name>
```

Table 54. Parameters in the `update-storage.sql` script (Oracle)

Parameter	Description
<log_file>	The name of the log file that the script will create and write information to.
<oracle_tns_alias>	The database alias for the OpenPages database instance, as set during the Oracle database installation.
<op_db_user>	The user name for accessing the OpenPages database.
<op_db_password>	The password for accessing the OpenPages database. If the password contains special characters, surround the password in quotation marks: <ul style="list-style-type: none">• Windows: "password"• Linux: 'password'
<storage_type>	The type of file storage to be used. Valid values are: <ul style="list-style-type: none">• LFS (local file system)• UNC (Universal Naming Convention) - for Windows only Note: After you move from LFS to UNC, you cannot go back to using LFS.
<storage_server_name>	The name of the storage server.
<host_name>	The host name of the machine.

Table 54. Parameters in the update-storage.sql script (Oracle) (continued)	
Parameter	Description
<os_type>	The type of operating system. Valid values are: <ul style="list-style-type: none"> • Windows • Unix
<path_or UNC_name>	The file path or UNC of the storage location. If the path contains backslashes, wrap the path in single quotation marks.

Examples

- LFS

Windows

```
sqlplus /nolog @sql-wrapper.sql update-storage output.log OP openpage "password"
LFS eng11 eng11 Windows 'C:\IBM\OpenPages\openpages-storage'
```

Linux

```
sqlplus /nolog @sql-wrapper.sql update-storage /home/op/upd-storage-output.log
op openpage 'password' LFS eng11 eng11 Unix /usr/opdata/openpages-storage
```

- UNC

Windows

In the following example, openpages-storage is the UNC share name of the storage location. The openpages-storage location is accessible to all horizontal cluster members as \testserver1\openpages-storage.

```
sqlplus /nolog @sql-wrapper.sql update-storage c:\temp\update-storage-output.log
op openpages "password" UNC eng11 eng11 Windows openpages-storage
```

Configuring IBM HTTP Server to balance the load on application servers

In a typical configuration that uses IBM HTTP Server to load balance the IBM OpenPages with Watson application servers, IBM HTTP Server is installed on a separate computer.

Web server plug-ins enable IBM HTTP Server to communicate requests for dynamic content, such as servlets, to the application server. A configuration file is used for each plug-in.

Open a port for the load-balancer, for example port 80.

Before you begin

If you are configuring the OpenPages environment for TLS/SSL, configure TLS before you configure the plugin-cfg.xml file. For more information, see the *IBM OpenPages with Watson Administrator's Guide*.

Procedure

1. On each application server, set up a unique cloneId for the server.
 - a) Go to the following directory: <WLP_USER_DIR>/servers/<server_name>Server<#>/configDropins/overrides/op-apps.xml
 - b) Set the cloneId attribute in the <httpSession> element to a value that is unique across your application servers.

```
<httpSession cloneId=<unique_ID>
```

For example

```
<httpSession cookieSecure="true" invalidationTimeout="90m" cloneId="Server1Server1" />
```

- c) Make note of each cloneId. You need this information in a later step.
2. Set up matching LTPA keys on each application server.
 - a) On any of the application servers, locate the `<OP_HOME>/wlp-user/servers/<server_name>Server<#>/resources/security/ltpa.keys` file.
 - b) Copy the `ltpa.keys` to the `$<OP_HOME>/wlp-user/servers/<server_name>Server<#>/resources/security/` directory on each application server.

For more information, see [Creating a Liberty cluster with security considerations](#).

If you want to customize the LTPA key file or its location, see [Configuring LTPA in Liberty](#).

3. Copy the `<OP_HOME>/wlp-user/servers/<server_name>Server<#>/logs/state/plugin-cfg.xml` file from the OpenPages application server to the load-balancer server. Put the file in the `<IHS_HOME>/Plugins/config/<webserver_name>` directory.

If you don't have a `<IHS_HOME>/Plugins/config/<webserver_name>` directory, copy the file to the `<WAS_HOME>/Plugins/config/<webserver_name>` directory on the load-balancer server.
4. If you are using Linux, set 755 permissions on each directory in the `<IHS_HOME>/Plugins/config/<webserver_name>` path and on the `plugin-cfg.xml` file.
5. Open the `plugin-cfg.xml` file. Review the settings.
6. For each application server, add the server's cloneId to the `<server>` element.

```
CloneID="Server1Server1"
```

For example:

```
<Server CloneID="Server1Server1" ConnectTimeout="5" ExtendedHandshake="false"
LoadBalanceWeight="20" MaxConnections="-1"
Name="OpenPagesNodeServer1Server1" ServerIOTimeout="900" WaitForContinue="false">
<Server CloneID="Server2Server1" ConnectTimeout="5" ExtendedHandshake="false"
LoadBalanceWeight="20" MaxConnections="-1"
Name="OpenPagesNodeServer2Server1" ServerIOTimeout="900" WaitForContinue="false">
```

7. Configure the session affinity cookies.

Verify that the `plugin-cfg.xml` file defines the following cookies in the `<UriGroup>` that is used by the `<Route>`:

```
<UriGroup Name="default_host_OpenPagesCluster_URIs">
  <Uri AffinityCookie="OPJSESSIONID" AffinityURLIdentifier="opjsessionid" Name="/"
opstartup_OPAdmin/*"/>
  <Uri AffinityCookie="OPJSESSIONID" AffinityURLIdentifier="opjsessionid" Name="/"
publishweb/*"/>
  <Uri AffinityCookie="OPJSESSIONID" AffinityURLIdentifier="opjsessionid" Name="/*"/>
  <Uri AffinityCookie="OPJSESSIONID" AffinityURLIdentifier="opjsessionid" Name="/grc/*"/>
</UriGroup>
```


8. Open the `<IHS_HOME>/conf/httpd.conf` file, and add or modify the following line to point to the `plugin-cfg.xml` file.

```
WebSpherePluginConfig
<path>/plugin-cfg.xml
```

For example:

```
WebSpherePluginConfig
/opt/IBM/HTTPServer/Plugins/config/<webserver_name>/plugin-cfg.xml
```

9. Ensure that the **IgnoreAffinityRequests** setting in the `<ServerCluster>` section is set to `false`.
10. Save and close the file.
11. Restart IBM HTTP Server.
12. Log in to OpenPages as a user with administrative privileges.

13. Click  > **System Configuration** > **Settings**.
14. Expand **Platform** > **Reporting Schema** > **Object URL Generator**.
15. Type the **Host**, **Port**, and **Protocol** of the load balancer.

If you are using a single server, type the **Host**, **Port**, and **Protocol** of the admin application server.

What to do next

If you are using SAML single sign-on, additional configuration is required. See [“Configuring the HTTP Server for SAMLV2.0 single sign-on”](#) on page 166.

Configuring the HTTP Server for SAMLV2.0 single sign-on

If you are using SAML V2.0 for single sign-on, extra configuration is required on the IBM HTTP Server and on the IBM OpenPages with Watson application servers.

Before you begin

- IBM HTTP Server is configured. See [“Configuring IBM HTTP Server to balance the load on application servers”](#) on page 164.

About this task

These steps use Microsoft Active Microsoft Directory Federation Server (ADFS) as the Identity Provider (IdP), but you can use any IdP that supports the SAML 2.0 protocol.

Procedure

1. Configure SAML SSO for OpenPages.
For more information, see [“Configuring SAML single sign-on”](#) on page 321.
2. Go to the following directory: `<WLP_USER_DIR>/servers/<server_name>Server<#>/configDropins/overrides`
3. Open the `OP_SSO_SAML_config.xml` file.
4. Add the following lines to the `<samlWebSso20>` element:

```
spHostAndPort="http://<IHS_host>:<IHS_port>
createSession="true"
```

Replace `<IHS_host>` and `<IHS_port>` with the host name and port of the load balancer or proxy server. Use HTTPS if you are using TLS.

For example:

```
<server>
  <featureManager>
    <feature>samlWeb-2.0</feature>
  </featureManager>
<!-- SAML SSO configuration - Single IdP -->
<samlWebSso20 id="<saml_id>"
spHostAndPort="http://<IHS_host>:<IHS_port>
createSession="true"
disableLtpaCookie="false"
allowCustomCacheKey="false"
mapToUserRegistry="No"
idpMetadata="<OP_HOME>/wlp-usr/servers/<server_name>Server<#>/resources/security/
FederationMetadata.xml"
enabled="true"
spLogout="false"
nameIDFormat="unspecified">
<authFilter id="samlAuthFilter">
<requestUrl id="openpagesUrl" urlPattern="/grc/api" matchType="notContain"/>
</authFilter>
</samlWebSso20>
</server>
```


Make a note of the `<saml_id>`. You need it in a later step.

5. Generate an X509 certificate for signing the SAML authentication request. Use the certificate on all application servers.

This step is required, whether use SSL with OpenPages or not.

- a) Create a keystore that contains only the certificate for signing the SAML authentication request.

Note: If SSL is enabled in your environment and you already have a separate keystore and truststore, you can use your existing truststore instead of creating a new one.

```
keytool -genkeypair -v -alias alias -dname "CN=localhost, OU=Organizational Unit, O=Organization, L=Location, ST=State, C=Country" -keystore jks_keystore -keypass key_pass -storepass keystore_passwd -keyalg key_algorithm -keysize keysize -validity validity
```

For example:

```
keytool -genkeypair -v -alias cert -dname "CN=exampleCA, OU=Example Org, O=Example Company, L=San Francisco, ST=California, C=US" -keystore cert.jks -keypass <password> -storepass <password> -keyalg RSA -keysize 4096 -validity 9999
```

- b) Put the keystore file in the `<OP_HOME>/wlp-user/servers/<server_name>Server<#>/resources/security` directory on each application server.
- c) Update the `OP_SSO_SAML_config.xml` file on each application server.

Add or update the following lines before the `<samlWebSso20>` element:

```
<sslDefault sslRef="defaultSSLConfig" />
<ssl id="defaultSSLConfig" keyStoreRef="defaultKeyStore"
trustStoreRef="defaultTrustStore" clientAuthenticationSupported="true" />
<keyStore id="defaultKeyStore" location="<default_keystore_file>"
type="<default_keystore_type>" password="<default_keystore_password>" />
<keyStore id="<saml_keystore_id>" location="<saml_keystore_file>"
type="<saml_keystore_type>" password="<saml_keystore_password>" />
```

Note: If SSL is enabled in your environment and you are not using the default SSL configuration, make the following changes:

- Replace `defaultSSLConfig`, with the name of your SSL configuration.
- If you're not using the default keystore and truststore, update `defaultKeyStore`, `defaultTrustStore`, and the `keyStore id="defaultKeyStore"` line.

Replace the following values:

- `<saml_keystore_id>`: Type the ID of the keystore that you created in step 5a. You can use any ID.
- `<saml_keystore_file>`: Type the full the path and filename of the keystore you created in step 5a.
- `<saml_keystore_type>`: Enter the keystore type, for example PKCS12
- `<saml_keystore_password>`: Type the keystore's password

For example:

```
<server>
  <featureManager>
    <feature>samlWeb-2.0</feature>
  </featureManager>
<!-- SAML SSO configuration - Single IdP -->

<sslDefault sslRef="defaultSSLConfig" />
<ssl id="defaultSSLConfig" keyStoreRef="defaultKeyStore" trustStoreRef="defaultTrustStore"
clientAuthenticationSupported="true" />
<keyStore id="defaultKeyStore" location="<OP_HOME>/wlp-user/servers/<server_name>Server<#>/
resources/security/key.p12" type="PKCS12" password="<password>" />
<keyStore id="<samlKeyStore" location="<OP_HOME>/wlp-user/servers/<server_name>Server<#>/
resources/security/SamlKeystoreFile.p12" type="PKCS12" password="<password>" />

<samlWebSso20 id="<saml_id>"
spHostAndPort="http://<IHS_host>:<IHS_port>"
createSession="true"
disableLtpaCookie="false"
allowCustomCacheKey="false"
```

```
mapToUserRegistry="No"
idpMetadata=<OP_HOME>/wlp-usr/servers/<server_name>Server<#>/resources/security/
FederationMetadata.xml"
enabled="true"
spLogout="false"
nameIDFormat="unspecified">
<authFilter id="samlAuthFilter">
<requestUrl id="openpagesUrl" urlPattern="/grc/api" matchType="notContain"/>
</authFilter>
</samlWebSso20>
</server>
```

6. Regenerate the service provider metadata.

- a) Export the SAML Service Provider metadata from WebSphere Liberty by going to the following URL in a browser:

```
https://<op_app_server>:<op_port>/ibm/saml20/<saml_id>/samlmetadata
```

- Replace <op_app_server> and <op_port> with the host and port of the OpenPages application server.
- Replace <saml_id> with the id attribute that you specified in the <samlWebSso20> element in the OP_SS0_SAML_config.xml file.

For example:

```
https://my.app.server:10111/ibm/saml20/defaultSP/samlmetadata
```

- b) Import the SAML Service Provider metadata to the ADFS server. In the ADFS **Server manager**, click **Tools > AD FS Management > Add Relying Party Trust**.
7. Open the <IHS_HOME>/Plugins/config/<webserver_name>/plugin-cfg.xml file. Review the settings.
 8. Add the following line to the <UriGroup element>:

```
<Uri AffinityCookie="OPJSESSIONID" AffinityURLIdentifier="opjsessionid" Name="/ibm/
saml20/*"/>
```

For example:

```
<UriGroup Name="default_host_OpenPagesCluster_URIs">
  <Uri AffinityCookie="OPJSESSIONID" AffinityURLIdentifier="opjsessionid" Name="/
opstartup_OPAdmin/*"/>
  <Uri AffinityCookie="OPJSESSIONID" AffinityURLIdentifier="opjsessionid" Name="/
publishweb/*"/>
  <Uri AffinityCookie="OPJSESSIONID" AffinityURLIdentifier="opjsessionid" Name="/*"/>
  <Uri AffinityCookie="OPJSESSIONID" AffinityURLIdentifier="opjsessionid" Name="/grc/*"/>
  <Uri AffinityCookie="OPJSESSIONID" AffinityURLIdentifier="opjsessionid" Name="/ibm/
saml20/*"/>
</UriGroup>
```

9. Repeat these steps on each application server.

Configuring property files for load balancing

Some configuration is required when using IBM HTTP Server as a load balancer in a WebSphere Liberty environment.

Procedure

1. On the load-balancing web server, go to the following directory: <IHS_HOME>/Plugins/config/<webserver_name>/
2. Open the plug-in file (plugin-cfg.xml) in a text editor to make the following changes:
 - a) Change the **IgnoreAffinityRequests** setting to true.
 - b) Change the **ServerIOTimeout** setting for all servers to a value that allows sufficient time for the IBM OpenPages with Watson application to respond to request from a client.

- c) Save and close the file.
3. Edit the `<IHS_HOME>/conf/httpd.conf` file in a text editor.
 - a) To load the required modules, add or uncomment the following lines

```
LoadModule negotiation_module modules/mod_negotiation.so
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_ajp_module modules/WebSphereCE/mod_proxy_ajp.so
LoadModule proxy_balancer_module modules/WebSphereCE/mod_proxy_balancer.so
LoadModule proxy_connect_module modules/mod_proxy_connect.so
LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule status_module modules/mod_status.so
LoadModule was_ap22_module modules/mod_was_ap22_http.so
```

- b) Modify the **ServerName** setting to point to the host name where you installed the IBM HTTP Web Server.

```
ServerName=MYSERVERNAME.DOMAIN.COM
```

- c) Modify the **ServerRoot** setting to point to the installation location of IBM HTTP Web Server. For example,

```
ServerRoot=/usr/IBM/HTTPServer/htdocs
```

- d) Add the `Allow from all` attribute to each `Directory` element.

```
<Directory>
Options Indexes FollowSymLinks
AllowOverride None
Order allow,deny
Allow from all
</Directory>
```

- e) Uncomment the parameter **ExtendedStatus** setting and set the value to `On`.
- f) Set the location tags for `server-status` and `server-info`.

For example,

```
<Location /server-status>
SetHandler server-status
Order Deny,Allow
Deny from all
Allow from all
</Location>

<Location /server-info>
SetHandler server-info
Order Deny,Allow
Deny from all
Allow from all
</Location>
```

4. Save and close the file.
5. Restart the IBM HTTP server.

Configuring property files for each OpenPages instance

You must edit the server properties file on each IBM OpenPages with Watson application server in the horizontal cluster to point to the load balancer.

Procedure

1. Log on to the OpenPages application server as a non-root user who has administrative privileges.
2. Go to the `<OP_HOME>/aurora/conf/` directory.
3. Open the `aurora.properties` file in a text editor.
 - a) Edit the **application.url.path** to point to the fully qualified domain name of the load balancer.

```
application.url.path=http\://<op-load-balancer.domain.com>\:<port>/openpages
```

- b) Save and close the file.
4. Go to the <OP_HOME>/aurora/conf/<server_name>Server<#> directory
5. Open each Server<#>-server.properties file in a text editor.
 - a) Edit the url.path to point to the fully qualified domain name of the load balancer.

```
url.path.openpages=http\://<op-load-balancer.domain.com>\:<port>/openpages
```

- b) Save and close each Server<#>-server.properties file.
6. Open each Server<#>-sosa.properties file in a text editor.
 - a) Edit the **application.url.path** to point to the fully qualified domain name of the load balancer.

```
application.url.path=https\://<op-load-balancer.domain.com>\:<port>/openpages
```

- b) Save and close each Server<#>-sosa.properties file.
7. Restart the web server.

Customizing the load balancer for large data sets

For databases with a large data set, some IBM OpenPages with Watson reports might time out before completion. If you experience problems with reports that are timing out, change configuration settings in the IBM HTTP Web Server configuration file.

Change the following settings:

Timeout

The number of seconds IBM HTTP Web Server waits to receive a GET request between receipt of TCP packets on a POST or PUT request and between ACKs on transmissions of TCP packets in responses.

KeepAliveTimeout

The number of seconds IBM HTTP Server waits for a subsequent request before closing the connection.

Note: A high value for the setting can cause performance problems, especially if the higher timeout causes server processes to wait for idle clients.

Procedure

1. Log on to load balancing web server as a user with administrative privileges.
2. Open httpd.conf in a text editor.
3. Change the **KeepAliveTimeout** property to a higher value.

```
KeepAliveTimeout 1800
```

4. Add and then set the **Timeout** property.

Ensure that the setting prevents timeout errors.

For example, Timeout 1800
5. Save and close the file.
6. Restart IBM HTTP Web Server.

Load balancing the reporting server

IBM OpenPages with Watson CommandCenter uses Cognos Analytics, which can scale horizontally. To scale OpenPages CommandCenter vertically within the same environment, increase the number

of processes that are available to handle requests. Depending on the load, you can configure more dispatchers.

About this task

To scale OpenPages CommandCenter horizontally, install more environments and register the IBM Cognos dispatchers. Incoming requests are distributed across the multiple environments.

The number of dispatchers you need depends on the operating system, system resources, the number of users, and other factors.

For more information about configuring dispatchers for your environment, see the [IBM Cognos documentation](#).

When you design and implement the infrastructure for the IBM Cognos reporting servers, the following OpenPages components determine how many reporting servers are required for the OpenPages solution:

- The number of computed fields on an object type.
- The complexity of the computed fields on an object type.
- The number of reporting fragments on an object type.
- The complexity of the computed fields on an object type.
- The number of embedded reports on the classic home page.
- Whether reporting fragments and computed fields are set to appear automatically.
- The number of IBM Cognos reports available to users.
- The complexity of IBM Cognos reports available to users.
- The custom components using the OpenPages reporting framework.

You should review the IBM Cognos log files and metrics to determine whether more reporting servers are required in the environment if timeout errors occur or issues occur as a result of excessive load.

Procedure

1. On the load-balancer server, stop IBM HTTP Server.
For example, in the `<IHS_HOME>/bin` directory, run the following command: `httpd -k stop`.
2. Open the `<IHS_HOME>/Plugins/config/OP/merged-plugin-cfg.xml` file in a text editor.
3. Change the session affinity from **JSESSIONID** to **opsosa**.

For example, change the file so that it looks like the following:

```
<UriGroup Name="default_host_OpenPagesCluster_URIs">
  <Uri AffinityCookie="opsosa" AffinityURLIdentifier="opsosa" Name="/opws/*"/>
  <Uri AffinityCookie="opsosa" AffinityURLIdentifier="opsosa"
    Name="/opstartup_OPAdmin/*"/>
  <Uri AffinityCookie="opsosa" AffinityURLIdentifier="opsosa" Name="/opx/*"/>
  <Uri AffinityCookie="opsosa" AffinityURLIdentifier="opsosa" Name="/publishweb/*"/>
  <Uri AffinityCookie="opsosa" AffinityURLIdentifier="opsosa" Name="/openpages/*"/>
  <Uri AffinityCookie="opsosa" AffinityURLIdentifier="opsosa"
    Name="/opwebservices/*"/>
  <Uri AffinityCookie="opsosa" AffinityURLIdentifier="opsosa" Name="/grc/*"/>
  <Uri AffinityCookie="opsosa" AffinityURLIdentifier="opsosa" Name="/samlsp/*"/>
</UriGroup>
```

4. Save and close the file.
5. Start IBM HTTP Server.
For example, in the `<IHS_HOME>/bin` directory, run the following command: `httpd -k start`.

Adding OpenPages servers to the Cognos Application Firewall safe list

By default, the IBM Cognos Application Firewall is enabled. Cognos Application Firewall validates domain and host names to protect URLs that are created. Cognos Application Firewall considers domain names

derived from the environment configuration properties as safe domain names. Use Cognos Configuration to add IBM OpenPages with Watson application servers to the list of valid domains and host names.

Procedure

1. Log on to the reporting server as a user with administrative privileges.
2. Start IBM Cognos Configuration.
3. In the **Explorer** pane, go to **Local Configuration > Security > IBM Cognos Application Firewall**.
4. In the **Properties** pane, click the **Valid domain names or hosts** field and click the pencil icon.
5. In the **Valid domain or hosts** window, click **Add**.
6. Enter the names of all OpenPages application servers.
7. Click **OK**.
8. Save the configuration and restart the Cognos service.

If you use Windows Services to restart the Cognos service, the service is listed as **IBM Cognos**.

Communication between OpenPages CommandCenter servers

If you install Cognos on more than one computer, you must configure the distributed installations to communicate with each other

Configure the following communication paths:

- Configure the primary Cognos server as the default active server.
- All Cognos servers must know the location of the content store database.
- All Cognos servers must know the location of the other Cognos servers.
- All Cognos servers must use the same cryptographic settings.
- All Cognos servers must have their system clock synchronized.

Configuring the active reporting server

In a clustered environment, one reporting server acts as the active server, or default primary server, and one or more reporting servers act as standby servers.

Procedure

1. Ensure that IBM OpenPages with Watson CommandCenter is not running on any server.
2. On the reporting server that is designated as the active server, start IBM Cognos Configuration.
Tip: Use the computer with the highest processor speed for the default active server.
3. In the **Explorer** pane, click **Environment**.
4. For the **Gateway URI**, change the `localhost` portion of the URL to the name of the active reporting server.
5. For the **Dispatcher URI for Gateway**, click the pencil icon next to the **Value** box.
6. In the **Current Values** list, change the `localhost` portion of the URL to the name of the active reporting server.
 - a) For each additional Cognos server, click **Add**.
 - b) Change the `localhost` portion of the URL to the name of each additional Cognos server.
 - c) Click **OK**.
7. For the **Content Manager URIs**, click the pencil icon next to the **Value** box.
 - a) In the **Current Values** list, change the `localhost` portion of the URL to the name of the primary Cognos computer.
 - b) For each additional Cognos server, click **Add**.
 - c) Change the `localhost` portion of the URL to the name of each additional Cognos server.

- d) Click **OK**.
- 8. In the **Explorer** pane, click **Security > Cryptography**.
- 9. In the **Properties** pane, under **CSK settings**, ensure that **Store symmetric key locally?** is set to **True**.
The key store must be created on the active Cognos server.
- 10. Click **File > Save**.
- 11. Click **Actions > Start**.

When the services start, this computer becomes the active reporting server.

Configuring standby reporting servers

In a clustered environment, configure one or more reporting servers to act as standby servers.

Procedure

- 1. Ensure that Cognos is running on the active Cognos server.
- 2. On the reporting server that is designated as a standby server, start IBM Cognos Configuration.
- 3. In the **Explorer** pane, click **Environment**.
- 4. In the **Environment - Group Properties** pane, click **Gateway URI**.
- 5. In the **Value** field, change the `localhost` portion of the URL to the name of the active reporting server.
- 6. In the **Environment - Group Properties** pane, click **Dispatcher URI for Gateway**.
 - a) Click the pencil icon next to the **Value** box.
 - b) In the **Current Values** list, change the `localhost` portion of the URL to the name of the active reporting server.
 - c) For each additional reporting server, click **Add**.
 - d) Change the `localhost` portion of the URL to the name of each additional Cognos server.
 - e) Click **OK**.
- 7. In the **Environment - Group Properties** pane, click **Content Manager URIs**.
 - a) Click the pencil icon next to the **Value** box.
 - b) In the **Current Values** list, change the `localhost` portion of the URL to the name of the active reporting server.
 - c) For each additional reporting server, click **Add**.
 - d) Change the `localhost` portion of the URL to the name of each additional Cognos server.
 - e) Click **OK**.
- 8. In the **Explorer** pane, under **Security**, click **Cryptography**.
- 9. In the **Properties** pane, under **CSK settings**, set **Store symmetric key locally** to **False**.
Note: The key store is created on the active reporting server. There can be only one key store in a load balanced Cognos installation.
- 10. In the **Explorer** window, under **Security, Cryptography**, click **Cognos**.
- 11. Under the **Certificate Authority settings** property group, set the **Password** property to match the one that you configured on the active reporting server.
Ensure that all other cryptographic settings match the settings that you configured on the active reporting server.
- 12. In the **Explorer** pane, under **Data Access > Content Manager**, click **Content Store**.
- 13. Ensure that the values for the content store match the active reporting server.
- 14. Click **File > Save**.
- 15. Click **Actions > Start**.

Configuring an Apache load balancer or proxy server

If you are using an external proxy server for load balancing, you must add a proxy redirection directive to the `httpd.conf` file on the proxy server. Requests sent to the proxy server are redirected to the server specified in the `httpd.conf` file.

Procedure

1. Log on to the load balancer server as a user who has administrative privileges.
2. Go to the `<Apache_Home>\conf\` directory, and open the `httpd.conf` file in a text editor.
3. Add the following lines:

```
<Location /ibmcognos/>
ProxyPass http://primary_reporting_server/ibmcognos/
SetEnv force-proxy-request-1.0 1 SetEnv proxy-nokeepalive 1
</Location>
```

Note: You must include the trailing forward slash in the `ProxyPass` directive when specifying the Cognos virtual directory (`/ibmcognos/`).

4. Save and close the file.

Using a reverse proxy server for load balancing

If you are using a reverse proxy server for load balancing, you must add a **ProxyPassReverseCookieDomain** value to the `httpd.conf` file on the reverse proxy server.

Procedure

1. Log on to the load balancer server as a user who has administrative privileges.
2. Go to the `<Apache_Home>\conf\` directory, and open the `httpd.conf` file in an editor.
3. Add a **ProxyPassReverseCookieDomain** value to the file as follows:

```
# Proxy
ProxyPass /openpages http://<hostname>:<port>/openpages
ProxyPassReverse /openpages http://<hostname>:<port>/openpages
```

```
ProxyPass /ibmcognos http://<hostname>:<port>/ibmcognos
ProxyPassReverse /ibmcognos http://<hostname>:<port>/ibmcognos
```

```
ProxyPassReverseCookieDomain <internal.domain.com> <public.domain.com>
```

4. Save and close the file.
5. Restart the web server.

Changing the CommandCenter host settings

You must update configuration files to use the IBM OpenPages with Watson CommandCenter server name and port settings.

Procedure

1. Log on to the OpenPages application server as a user with administrative privileges.
2. Stop the OpenPages services.
3. Go to the `<OP_HOME>/aurora/conf` directory.
4. In the `cognos.framework.refresh.servlet=http\://localhost\:8080/crf-refresher` property, replace `localhost\:8080` with the reporting server name and port.

Example:


```
cognos.framework.refresh.servlet=http\://ccserver\:8080/crf-refresher
```

5. In the `cognos.server=http\://localhost:80/ibm/cognos/analytics/cgi-bin/cognos.cgi` property, replace `localhost:80` with the reporting server name and port number.

Example:

```
cognos.server=http\://ccserver:80/ibm/cognos/analytics/cgi-bin/cognos.cgi
```

6. Add the following value to the `logout.url.cognos` property:

```
http\://<CommandCenter_server_name>\<CommandCenter_port>\ibm/cognos/analytics/  
cgi-bincognos.cgi? b_action\=xts.run&m\=portal/logoff.xts&h_CAM_action\=logoff
```

Example:

```
logout.url.cognos=http\://ccserver\:8080/ibm/cognos/analytics/cgi-bincognos.cgi?  
b_action\=xts.run&m\=portal/logoff.xts&h_CAM_action\=logoff
```

7. Save your changes and exit the editor.

Admin application server tuning

You can tune your admin application server settings to improve performance.

For more information see the *IBM OpenPages with Watson Administrator's Guide*

Preventing concurrency conflicts for installations that use Oracle databases

If two administrators both try to modify settings at the same time, errors might occur. To help avoid concurrency errors, run the `SQL enable-session-sleep.sql` script.

A concurrency conflict might result in the following error message:

Operation failed, security settings are being concurrently modified by another administrator.
Please try again later.

Procedure

1. On a computer that has SQL*Plus and access to the database server, log on as a user with SYSDBA permissions.
2. Go to the `/OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/INSTALL_SCRIPTS` directory.
3. Copy the `enable-session-sleep.sql` script to the local computer.
4. Run the `enable-session-sleep.sql` script.

```
sqlplus /nolog @sql-wrapper enable-session-sleep.sql <log_file_name> <connect_identifier>  
<sysdba_user_name> <sysdba_user_password> <schema_owner_name>
```

If the password contains special characters, surround the password in quotation marks:

- Windows: "password"
- Linux: 'password'

Example:

- Windows:

```
sqlplus /nolog @sql-wrapper enable-session-sleep.sql enable-session-sleep.log  
opx10g sys "pass-word" openpages
```

- Linux:

```
sqlplus /nolog @sql-wrapper enable-session-sleep.sql /tmp/log OP sys 'pass-word' openpage
```

If the process completes successfully, a message is displayed.

If the script fails, check the log files for error messages.

Optional: Increasing the paging file size on Windows computers

On computers that have 8 GB of RAM, the suggested paging file size is 16 GB.

Procedure

1. Click **Start** > **Run** and then type `sysdm.cpl`, and press Enter.
2. Click the **Advanced** tab.
3. In the **Virtual Memory** section, click **Change**.
4. If necessary, clear the **Automatically manage page file size for all drives** check box.
5. Find the list of drives and select the drive that contains your paging file.
6. Select **Custom Size**.
7. Reset both the **Initial Size** and **Maximum Size** values to higher values.
8. Click **Set**.
9. Click **OK**.

Database server tuning for Db2 databases

To improve performance, tune the database, change some of the values for database server parameters. Other changes are suggested in environments where there are heavy user loads.

Changing the Db2 varchar limit for IBM Cognos reports

Conditional statements are used in IBM OpenPages with Watson computed fields that reference data columns with **varchar** values larger than 4000. By default Cognos Analytics uses a **varchar** limit of 4000. You can ensure that errors do not occur in OpenPages reports by removing the **varchar** limit.

If you do not change the **varchar** limit, errors like the following can appear in the `cogserver.log` file.

```
RQP-DEF-0177 An error occurred while performing operation 'sqlPrepareWithOptions'
status='-120'
UDA-SQL-0458 PREPARE failed because the query requires local processing of the data.
The option to allow local processing has not been enabled.
UDA-SQL-0476 A VARCHAR column in a comparison exceeds the maximum length allowed
by the database.
This operation requires local processing of the data.
```

Procedure

1. Log on to the reporting server as a user with administrative privileges.
2. Go to the `<COGNOS_HOME>/bin` directory.
For example, go to the `C:\IBM\cognos\analytics\bin` directory.
3. Make a backup copy of the `cogdmd2.ini` file.
4. Open the `cogdmd2.ini` file in a text editor.
5. Find the following statement:

```
[Exceptions Operators DATABASE:SQL]
Varchar_Compare_Limit="4000"
```

6. Comment out the `Varchar_Compare_Limit="4000"` statement by adding a semicolon (;) in front of it.
For example,

```
[Exceptions Operators DATABASE:SQL]
;Varchar_Compare_Limit="4000"
```

7. Save and close the file.
8. Restart the Cognos Analytics services.

Activate Db2 databases to improve application start-up times

You can use the activate database command to initialize IBM Db2 databases before you start IBM OpenPages with Watson, and to keep the database initialized if the applications are stopped or disconnected.

The OpenPages database is activated when you create it during the IBM OpenPages with Watson installation process. You might want to activate the database each time that you start OpenPages to improve application start-up times.

The activate database command explicitly starts a database and makes it ready to accept connections and process requests. An explicitly activated database remains ready and primed even when there are no application connections to the database. You can activate a database during routine start-up procedures to make it ready to immediately accept connections and process requests.

Use the deactivate database command on an explicitly activated database before you stop the instance or perform an offline backup.

Note: An explicitly activated database cannot be dropped.

For example, the following sequence of commands shows how you can use the activate and deactivate commands:

1. Start the database instance:

```
db2start
```

2. Start the database:

```
db2 activate database opx
```

The database performs consistency checks, recovery tasks, and allocates memory heaps, such as buffer pools.

3. Start the OpenPages servers:

For more information, see [Chapter 12, “Starting and stopping servers,” on page 309](#).

The database connections are made immediately.

4. Stop the OpenPages servers:

For more information, see [Chapter 12, “Starting and stopping servers,” on page 309](#).

The database remains activated, ready for connections, and the buffer pools remain primed.

5. Deactivate the database:

```
db2 deactivate database opx
```

6. Back up the database:

```
db2 backup database opx to /backupdir
```

The database must not be active when you back it up.

7. Start the database:

```
db2 activate database opx
```

8. Start the OpenPages servers:

For more information, see [Chapter 12, “Starting and stopping servers,” on page 309](#).

Database server tuning for Oracle databases

To improve performance, tune the database.

Memory tuning guidelines for Oracle databases

If your application is running in a heavy-load environment, consider allocating as much memory as possible to the Oracle database instance.

The following table provides general guidelines for memory allocation on a system with 8 GB of RAM or more.

Table 55. Memory tuning guidelines for computer with 8 GB of RAM	
For this...	Allocate...
Operating system	2 GB of physical RAM for the Windows OS.
SGA Size	75% of remaining physical RAM to the SGA_TARGET parameter. Minimum allocation: 4608 MB (or 4.5 GB).
PGA Size	25% of remaining physical RAM to the PGA_AGGREGATE_TARGET parameter. Minimum allocation: 1536 MB (or 1.5 GB).

Pluggable databases

If you are using Oracle PDB, ensure that you set the tuning parameters on the pluggable database.

Computers with multiple database instances

Note: If you are planning to run multiple database instances on the same computer, adjust the memory to ensure that concurrently running instances fit into the available physical RAM. Using physical memory avoids swapping to disk.

For example, to run the IBM OpenPages with Watson database and Cognos database services on the same computer with 8 GB of RAM:

- 2 GB of RAM for the OS
- The remaining 6 GB of RAM can be split between the OpenPages database and Cognos database as follows:
 - OpenPages database instance: 2.5 GB SGA + 1 GB PGA
 - Cognos database instance: 1.5 GB SGA + 1 GB PGA

Enabling LDAP for the OpenPages application

If you are installing IBM OpenPages with Watson into an LDAP environment, you must enable LDAP. The **Openpages** module in the LDAP configuration file, `aurora_auth.config`, determines whether LDAP is enabled.

For more information, see the *IBM OpenPages with Watson Administrator's Guide*.

Note: The LDAP server for the user provisioning feature is configured separately. See "LDAP and user provisioning" in the *IBM OpenPages with Watson Administrator's Guide*.

Procedure

1. Log on to the OpenPages application server as a user with administrative privileges.

2. Use your LDAP Directory Server to add users who require access to the OpenPages application or to the OpenPages environment to the LDAP authentication server.

For more information about the steps required to add OpenPages users to the LDAP server, see the documentation for your LDAP Directory Server.

3. Log on to the OpenPages application and create the same users.
4. Stop all OpenPages services.
5. Go to the directory where you copied the `aurora_auth.config` file.
6. Open the LDAP configuration file, `aurora_auth.config`, in a text editor.
7. Rename the **Openpages** module to something different, such as `Openpages_default`.
8. Depending on your LDAP server, rename the LDAP module to **Openpages**
 - If you are using a Microsoft Active Directory server, change the **OpenpagesAD** module name to **Openpages**.
 - If you are using any other LDAP server, change the **OpenpagesIP** module name to **Openpages**.
9. Specify the correct values for the following properties in the appropriate module:

Table 56. LDAP properties	
Property	Description
provider.url	IP address and port number of the LDAP authentication server, in the <code><protocol>://<ip_address>:<port></code> format. Note: If you are configuring LDAP over SSL (LDAPS), the protocol is <code>ldaps</code> and the port is the LDAPS port.
security.search.user.dn	The fully qualified name of an administrative user on the LDAP server.
security.search.user.credentials	The password for the specified user
base.dn	The top level of the LDAP directory tree structure (Domain Name) on the LDAP server. If the users to be authenticated are in multiple locations within your Active Directory structure, list all locations explicitly. Use the distinguished names of the locations, each separated by a semi-colon.
user.attr.id	The attribute name of the user identifier. Typically a common name (CN), uid, or SAMAccountName.

For example

```
Openpages_default
{
  com.openpages.aurora.service.security.namespace.AuroraLoginModule required
  debug=false;
};

Openpages
{
  com.openpages.aurora.service.security.namespace.LDAPLoginModule required debug=false
  provider.url="ldap://10.128.25.150:389"
  security.authentication="simple"
  security.search.user.dn="CN=Administrator,CN=Users,DC=LDAPTesting,DC=local"
```

```
security.search.user.credentials="openpages"  
base.dn="CN=Users,DC=LDAPTesting,DC=local"  
user.attr.id="CN";  
};
```

10. Save and close the file.
11. Log on to the OpenPages application and change the OpenPages Administrator password to openpages.
12. Restart all OpenPages services.
13. Log on to the OpenPages application as one of the users that you created in the LDAP Directory Server.

Disabling LDAP for the OpenPages application

If LDAP is enabled on your system, the default **Openpages** module was renamed. Either the **OpenpagesIP** or **OpenpagesAD** was renamed to **Openpages**. To disable LDAP, change the name of the current **Openpages** module and change the name of the default **Openpages** module back to **Openpages**.

Note: The LDAP server for the user provisioning feature is configured separately. See "LDAP and user provisioning" in the *IBM OpenPages with Watson Administrator's Guide*.

Procedure

1. Log on to the application server as a user with administrative privileges.
2. Stop all IBM OpenPages with Watson services.
3. Go to the directory where you copied the `aurora_auth.config` file.
`<OP_HOME>/aurora/conf`
4. Open the LDAP configuration file, `aurora_auth.config`, in a text editor.
5. Change the name of the **Openpages_default** module back to **Openpages**.
6. Change the name of the current **Openpages** module to something different.
7. Save and close the file.

Accessing OpenPages


To view the application login page for your installation, type the IBM OpenPages with Watson URL into your web browser.

For default installations, type the following URL in your web browser:

`http://<openpages_server>:<port>/openpages`

If you are using an SSL connection to access the OpenPages application, you must have an SSL digital certificate. After configuring SSL, type the following URL in your web browser:

`https://<openpages_server>:<ssl_port>/openpages`

If the URL redirects you to the Task Focused UI and you want to use the Standard UI, click  > **Switch to Standard UI**

Search server post installation tasks

If you installed a search server with IBM OpenPages with Watson, ensure that you complete the following post installation tasks.

- Copy the JDBC driver from the database server to the search server. For more information, see [“Copying database driver files to the search server” on page 181](#).
- Optional: Set up SSL for the global search service. For more information, see [“Setting up a secure connection for the global search service” on page 181](#).

- Configure the location of the openpages-storage directory in the search server properties file. For more information, see [“Updating the search server properties file with the location of the OpenPages storage directory”](#) on page 184.
- Tune the search server parameter settings. For more information, see [“Search server tuning”](#) on page 185.
- Create the global search index. For more information, see [“Creating the global search index”](#) on page 186.

Note: If you are migrating from 7.2.x or 7.3.x, skip this task. You will update global search during the migration process.

For more information about the search server, see the *IBM OpenPages with Watson Administrator's Guide*.

Copying database driver files to the search server

After you install the search server, you must copy the database driver files to the search server.

Procedure

1. Copy the JDBC database drivers from the database server.
 - If you are using an Oracle 12.2.0.1, 18c, or 19c database server:
 - a. Go to the following directory: `<ORACLE_HOME>/jdbc/lib`
 - b. Copy the `ojdbc8.jar` file.
 - If you are using an IBM Db2 database server:
 - a. Go to the following directory: `<DB2_HOME>/sqllib/java`
 - b. Copy the following files:
 - `db2jcc4.jar`
 - `db2jcc_license_cu.jar`
2. Copy the files to the following directory on the search server: `<SEARCH_HOME>/opsearchtools/lib`
3. Start the global search services. For more information, see [“Start or stop the global search services”](#) on page 312.

Setting up a secure connection for the global search service

You can configure the IBM OpenPages with Watson global search service (Apache Solr) to use a secure connection with TLS. TLS ensures that all data that is passed between the application server and the Solr service remains private.

Before you begin

On the search server and application servers, `$JAVA_HOME/bin` must be set in the `PATH` system environment variable. To verify that Java is in the `PATH` variable, run the following command:

```
java -version
```

If you get the following error, Java is not in the `PATH` variable: `Command not found`.

About this task

If you are setting up the global search component in a test environment, do not enable TLS until you resolve all installation and configuration issues.

For more information about the commands that are used in this task, see the [Apache Solr Reference Guide](#).

Important: IBM is not responsible for third-party content. At the time of publication, the information is correct.

Procedure

1. If the global search component is enabled, you must disable it.
 - a) Log on to OpenPages as a user with administrative privileges. Go to the Standard UI.
 - b) Click **Administration > Global Search**.
 - c) Click **Disable**.

2. Stop the global search services.

For more information, see [“Start or stop the global search services” on page 312](#).

3. Create a certificate for the secure connection.

- a) Go to the `<SEARCH_HOME>/solr/server/etc` folder and run the following command.

```
keytool -genkeypair -alias alias -keyalg key_algorithm
-keysize keysize -keypass key_pass -storepass keystore_passwd
-validity validity -keystore jks_keystore -ext ip_address
-dname "CN=localhost, OU=Organizational Unit, O=Organization, L=Location,
ST=State, C=Country"
```

In the following example, the command creates a self-signed certificate in a key store named `solr-ssl.keystore.jks`. The key store contains a key with an alias of `solr-ssl`, a key store password of `secret`, a trust store password of `secret`. It specifies Subject Alternative Name (SAN) values of `DNS:host1.companya.com` and `IP:127.0.0.1,192.168.7.1` to include in the certificate. (SAN values are not mandatory, and might not be specified in your environment).

```
keytool -genkeypair -alias solr-ssl -keyalg RSA
-keysize 2048 -keypass secret -storepass secret
-validity 9999 -keystore solr-ssl.keystore.jks
-ext SAN=DNS:host1.companya.com,IP:127.0.0.1,IP:192.168.7.1
-dname "CN=localhost, OU=Organizational Unit, O=Organization, L=Location,
ST=State, C=Country"
```

- b) Convert the JKS key store into PKCS12 format.

```
keytool -importkeystore -srckeystore jks_keystore
-destkeystore jks_keystore.p12 -srcstoretype source_keystore_type
-deststoretype destination_keystore_type
```

When prompted, type a destination key store password, and the source key store password that you specified in the step 3a.

- c) Convert the PKCS12 format key store, including the certificate and the key, into PEM format.

To run this command, `openssl` must be installed, and added to the `PATH` environment variable.

```
openssl pkcs12 -in <jks_keystore.p12> -out <jks_keystore.pem>
```

When you are prompted for the import password and PEM pass phrase, you can use the same password that you specified for the `<key_pass>` value in step 3a.

4. Export the certificate.

```
keytool -exportcert -keystore <jks_keystore> -alias <alias> -file <solr_certificate>
```

When you are prompted for the key store password, type the password that you specified for the `<key_pass>` value in step 3a.

5. Update the `solr.in` file.

- a) Edit the following file in a text editor:

Windows

```
<SEARCH_HOME>\solr\bin\solr.in.cmd
```


Linux

<SEARCH_HOME>/solr/bin/solr.in.sh

b) Uncomment and set the following TLS properties.

```
SOLR_SSL_KEY_STORE=etc/jks_keystore
SOLR_SSL_KEY_STORE_PASSWORD=keystore_passwd
SOLR_SSL_TRUST_STORE=etc/jks_keystore
SOLR_SSL_TRUST_STORE_PASSWORD=keystore_passwd
SOLR_SSL_NEED_CLIENT_AUTH=false
SOLR_SSL_WANT_CLIENT_AUTH=true
```

On Windows, you might need to use server/etc as the path name for the SOLR_SSL_KEY_STORE and SOLR_SSL_TRUST_STORE properties.

6. Log in to the OpenPages application as a user with administrative privileges.

7. Open the **Settings** page.

- In the Task Focused UI, click  > **System Configuration** > **Settings**.
- In the Standard UI, click **Administration** > **Settings**.

8. Update the following settings to use https instead of http.

Platform > Search > Admin > Search Server Administration URL

Platform > Search > Index > Search Server URL

Platform > Search > Request > Search Server URL

9. Copy the certificate file that you exported to the following directory on the application server.

<JAVA_HOME>/lib/security

10. Add the certificate to the IBM JRE key store file.

- a) On Windows computers, start a Command Prompt window with the **Run as administrator** option. On Linux computers, open a shell.
- b) Back up the <JAVA_HOME>/lib/security/cacerts file.
- c) Go to the <JAVA_HOME>/bin directory and run the following command.

```
keytool -importcert -alias <alias> -keystore cacerts -file <solr_certificate>
```

When prompted, type the key store password of the cacerts key store. The default password is typically changeit.

- d) Confirm that you want to trust the certificate.
- e) Restart all OpenPages services.

11. Import the certificate to the IBM WebSphere trust store.

- a) Log on to the OpenPages application server.
- b) Run the following command:

```
keytool -importcert -v -alias <CERTIFICATE_ALIAS> -file <CERTIFICATE_NAME> -keystore <STORE_PATH> -storetype PKCS12 -storepass <STORE_PASSWORD>
```

Where:

- <CERTIFICATE_ALIAS> is the alias of the certificate.
- <CERTIFICATE_NAME> is the file name of the certificate.
- <STORE_PATH> is the full path and file name of the trust store on the application server. For example: /opt/IBM/OpenPages/wlp-user/servers/<server_name>Server<#>/resources/security/key.p12
- <STORE_PASSWORD> is the password of the trust store on the application server.

For more information, see [Adding trusted certificates in Liberty](#) in the WebSphere Liberty documentation.

- c) Restart all OpenPages services.
12. Start the global search services.

For more information, see [“Start or stop the global search services” on page 312.](#)
13. If the search server is installed on a different computer than the application server, add the certificate to the IBM JRE key store on the search server.
 - a) On Windows computers, start a Command Prompt window with the **Run as administrator** option. On Linux computers, open a shell.
 - b) Go to the `<JAVA_HOME>/bin` directory and run the following command:

```
keytool -importcert -alias <alias> -keystore cacerts -file <SEARCH_HOME>/solr/server/etc/solr_certificate
```
 - c) When prompted, type the key store password of the cacerts keystore. The default password is typically changeit.

Updating the search server properties file with the location of the OpenPages storage directory

Configure the path to the openpages-storage directory in the search server properties file to enable the search server to access the directory.

About this task

When you install IBM OpenPages with Watson, a pointer to the OpenPages storage location is created. The storage location is a directory where attached files and forms that are associated with OpenPages objects are stored. The search server looks in the openpages-storage directory to index file attachments, when file attachment search is enabled.

To configure the location of the directory, share the openpages-storage directory on the admin application server, and then modify the search server properties on the search server to point to the shared network location.

Note: If you are working with a test environment in which the search server is on the same physical computer as the admin application server, you do not need to do this task.



Attention: By default, file attachment search is enabled. If you enable global search without first configuring the location of the OpenPages storage directory location, files cannot be searched.

Procedure

1. Share the openpages-storage directory on the admin application server so that it can be reached by the search server.

For more information, see [“Sharing a network OpenPages storage directory on Linux operating systems” on page 159](#) and [“Sharing a network OpenPages storage directory on Windows operating systems” on page 161.](#)

2. Log on to the search server as a user with administrative privileges.
3. Go to `<SEARCH_HOME>/opsearchtools/`.
4. Open the openpages_search.properties file in a text editor.
5. Modify the OPSearchTool.FileStorageRootPath property to specify the full path to the openpages-storage directory on the admin application server.
 - Linux: `/opt/ibm/op/openpages/openpages-storage`
 - Microsoft Windows:

Note: On Windows operating systems, escape the directory separator with a backslash (\).

- If you share is mounted to a driver letter, use the following syntax: `C:\\ibm\\op\\openpages\\openpages-storage`

- If your share is a network share, use the following syntax: \\op-server\shared\openpages-storage

For more information about the `OPSearchTool1.FileStorageRootPath` property, see the *IBM OpenPages with Watson Administrator's Guide*.

6. Disable global search and stop the global search services.

For more information, see [“Stopping the global search services by using a script” on page 313](#) or [“Stopping the global search services” on page 315](#).

7. Start the global search services.

For more information, see one of the following topics:

- [“Starting the global search services by using a script” on page 312](#)
- [“Starting the global search services on Windows” on page 313](#)
- [“Starting the global search services on Linux” on page 314](#)

Search server tuning

The standard installation of the IBM OpenPages with Watson global search component uses default parameter settings. You might need to tune some parameter settings depending on your organization's requirements and data.

There are two settings that you can configure:

- The ports used by the global search component.

For more information, see [“Changing port values for the global search component” on page 185](#).

- The amount of memory used by the search engine service and the indexer service.

For more information, see [“Allocating memory for the global search component” on page 186](#).

Changing port values for the global search component

By default, the IBM OpenPages with Watson global search component uses two ports. Port 8983 is used for indexing and searching OpenPages data. Port 8985 is used to administer global search.

About this task

If you have a firewall, ensure that these ports are enabled. If your organization uses different ports, you can change the port values.

Procedure

1. If the global search component is enabled, you must disable it.

- a) Log on to OpenPages as a user with administrative privileges. Go to the Standard UI.
- b) Click **Administration > Global Search**.
- c) Click **Disable**.

2. Stop the global search services.

For more information, see [“Start or stop the global search services” on page 312](#).

3. Log in to the OpenPages application as a user with administrative privileges, and update the following registry setting values.

- a) Click **Administration > Settings > Applications > Common > Configuration > Show Hidden Settings** and set the value to `true`.
- b) Click **Administration > Settings > Platform > Search > Admin** and update the **Search Server Administration URL** default port value (8985) to a value of your choice.
- c) Click **Administration > Settings > Platform > Search > Index** and update the **Search Server URL** default port value (8983) to a value of your choice.

- d) Click **Administration > Settings > Platform > Search > Request** and update the **Search Server URL** default port value (8983) to a value of your choice.

Ensure the port value matches the value you specified in step 3c to avoid issues for users.

4. Start the global search services.

For more information, see [“Start or stop the global search services” on page 312](#).

5. Continue with the post installation or post migration steps for global search.

Allocating memory for the global search component

You can change the amount of memory used by the Apache Solr search engine service and the indexer service for the IBM OpenPages with Watson global search component.

Procedure

1. Update the memory allocation on the computer on which you installed the search server.

Ensure you have sufficient free memory on the computer. If you set the memory too high and the computer does not have enough free memory, you might encounter performance issues.

- a) Edit the `<SEARCH_HOME>/opsearchtools/openpages_search.properties` file in a text editor.
- b) To update the amount of memory (in megabytes) to allocate to the Apache Solr service, edit the `OPSearchTool.SolrHeapSize` value.
- c) To update the amount of memory (in megabytes) to allocate to the OpenPages indexer service, edit the `OPSearchTool.IndexerHeapSize` value.

2. If the global search component is enabled, you must disable it.

- a) Log on to OpenPages as a user with administrative privileges. Go to the Standard UI.
- b) Click **Administration > Global Search**.
- c) Click **Disable**.

3. Stop the global search services.

For more information, see [“Start or stop the global search services” on page 312](#).

4. Start the global search services.

For more information, see [“Start or stop the global search services” on page 312](#).

5. Continue with the post installation or post upgrade steps for global search.

Creating the global search index

After you install IBM OpenPages, create the global search index. If you are migrating, you can skip this task.

Before you begin

The reporting schema must exist and must be enabled before you create the search index.

Procedure

1. Start the search services, if they are not already started.
2. Log on to OpenPages as a user with administrative privileges. Go to the Standard UI.
3. Click **Administration > Global Search** and click **Create**.

Creating the index also enables global search.

Click **Refresh** to update the page.

Results

Global Search is available.


If global search does not start, see [“Known problems and solutions for global search”](#) on page 434.

For more information about global search, see the *IBM OpenPages with Watson Administrator's Guide*.

Preventing orphan objects

After you install IBM OpenPages, to prevent orphan objects, you must update the Cascade Delete registry setting.

Procedure

1. Log in to OpenPages as a user with administrative privileges.
2. Click  > **System Configuration** > **Reporting Schema**.
3. Click **Common** > **Cascade Delete** > **Include Object Types**.
4. Append the registry setting value with the following string:

```
,ProjectActionItem,QuestionnaireAssessment,QuestionTemplate,  
SectionTemplate,SOXBusEntity,SOXDocument,SOXExternalDocument,  
SOXIssue,SOXMilestone,SOXSignature,SOXTask,SubSectionTemplate
```

Verification checklist

After you install the IBM OpenPages with Watson application, verify that the installation is working as expected.

Use the following checklist to verify whether the installation is successful.

Table 57. Post installation verification checklist	
Task	Guidance
Review all installation logs for errors.	For log file locations and names, see “Log files” on page 427.
Verify that the database parameters are correct.	Review the database parameters, such as NLS_LENGTH_SEMANTICS=CHAR, to ensure that they are correct.
Confirm that the reporting schema and reporting framework generated successfully.	For more information, see “Creating the reporting schema and framework” on page 156.
Confirm that base reports are functioning as expected.	Log on to the OpenPages application and run the All Documentation Cognos report.
If single sign-on (SSO) is enabled, verify that user accounts can access the environment.	Log on to the OpenPages application with an SSO user account.
Confirm that you can upload and download sample attachments.	Log on to the OpenPages application and upload and download a file attachment.
Verify that links in reports reference the correct server address and use the correct web URL parameters.	Run a report that uses OpenPages links. Select a link and confirm that the target object is rendered successfully in the OpenPages interface.

Table 57. Post installation verification checklist (continued)

Task	Guidance
For clustered environments, verify that all servers can upload and download attachments.	Upload and download files from both the admin and non-admin application servers.
Test that you can access IBM Cognos Analytics.	Type the following web URL: <code>http://server_name/ibmcognos</code> Confirm that you can log on to the portal.
Confirm that you ran the <code>enable-session-sleep.sql</code> script.	For more information, see “Preventing concurrency conflicts for installations that use Oracle databases” on page 175.
Confirm that object data is created. Do this test after you back up the database.	Log on to the OpenPages application and create sample Entity, Process, and Risk objects. Delete these objects.

Chapter 7. Migrate to a new version of IBM OpenPages with Watson

Migrate your existing version of IBM OpenPages with Watson to 8.2 to take advantage of new features, enhancements, and performance improvements.

If you are using version 8.2.0.x, you do not need to do a migration. Instead, update your deployment by installing a 8.2.0.x fix pack. For more information, see [Chapter 11, “Fix packs,” on page 279](#).

For more information about the supported software versions for OpenPages with Watson, see the [Supported Environments website](#).

If you are using 7.4.x, 8.0.x, or 8.1.x

If you are using version 7.4.x, 8.0.x, or 8.1.x, you have two options:

- Upgrade your deployment in-place. With this method, you install version 8.2 on top of your existing deployment. This method is called an *upgrade*. It is also sometimes called an "in-place upgrade" or an "over-the-top upgrade."

For more information, see the *IBM OpenPages with Watson Upgrade Guide for IBM Db2* or the *IBM OpenPages with Watson Upgrade Guide for Oracle*.

- Migrate your deployment to version 8.2. With this method, you install version 8.2 and then migrate data and files from your existing environment.

Use this method if you want to use new hardware, for example.

If you are using 7.3.x

You must do a migration.

You can migrate from IBM OpenPages with Watson version 7.3.x to 8.2.

For more information, see [“Migration overview” on page 189](#).

If your source environment is at version 7.2.x or earlier

You must first migrate to 7.3.x, 7.4.x, 8.0.x, or 8.1.x. You can then migrate to 8.2.

Migration overview

When you migrate, you do a fresh installation of IBM OpenPages with Watson 8.2 and then migrate your data. You can install IBM OpenPages with Watson in a new environment or in your existing IBM OpenPages with Watson environment in a new directory.

IBM OpenPages with Watson supports migrations from versions 7.3.x, 7.4.x, 8.0.x, and 8.1.x.

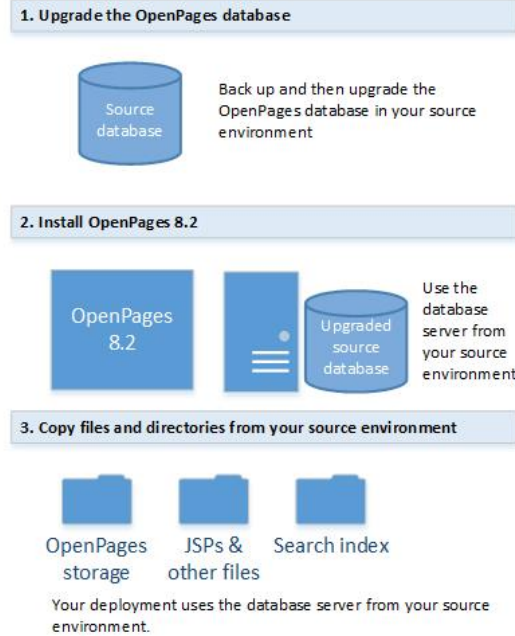
Tip: If you are using 7.4.x or later, you can either do a migration or an in-place upgrade. For more information, see [Chapter 7, “Migrate to a new version of IBM OpenPages with Watson,” on page 189](#).

If your environment was originally based on a fresh installation of 7.0.x or an earlier version, you might need to do some remediation steps. For more information, see <http://www.ibm.com/support/docview.wss?uid=swg22014144>.

If you are using the Legacy Reporting Framework, switch to the Reporting Framework V6 before you migrate to 8.2. You cannot regenerate the Legacy Reporting Framework in 8.2.

When you migrate IBM OpenPages with Watson, you can follow two main scenarios: using the database server from your source environment or using new hardware for the database server.

Scenario 1: Source database server



Scenario 2: New hardware for the database server

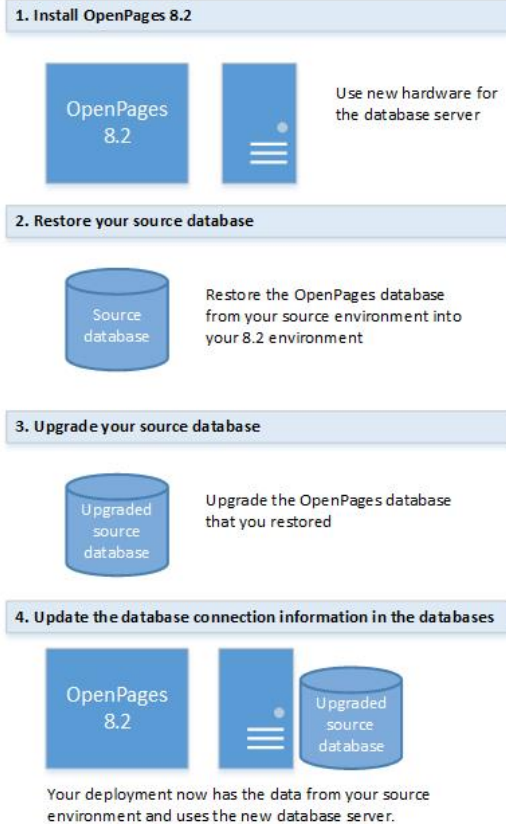


Figure 15. Migration scenarios

Migration process overview: Using the database server from your source environment

You can migrate IBM OpenPages with Watson and use the existing database server from your 7.3, 7.4/8.0, or 8.1 environment.

Use this option if you do not want to use new hardware for the database server.

Do the following tasks.

1. Install the installation server. For more information, see [“Setting up the installation server on Windows” on page 41](#) or [“Setting up the installation server on Linux” on page 43](#).
2. Ensure that the installation server is updated to the latest version. For more information, see [“Updating the installation server” on page 47](#).
3. Ensure that your source database server meets the prerequisites for OpenPages. See [“Upgrade prerequisite software” on page 196](#). Also see the following checklists:
 - [“Checklist for the database server \(Db2\)” on page 65](#)
 - [“Checklist for the database server \(Oracle\)” on page 87](#)
4. Upgrade to a supported version of Cognos Analytics. See [“Cognos Analytics upgrade process: 10.2.x to 11.1” on page 197](#) or [“Cognos Analytics upgrade process: 11.0.x to 11.1.x” on page 197](#).
5. If you use global search, prepare the search server. See [“Preparing the search server in the source environment” on page 198](#).
6. Back up the OpenPages source environment. See [“Backing up your source environment” on page 198](#).

7. Upgrade the OpenPages database in your source environment manually. See [“Upgrade the OpenPages database”](#) on page 199.
8. If you use a custom encryption keystore, copy the keystore file to each application server in your target environment. The file must be located at the same path as you used in your source environment. After you install OpenPages, update passwords to plain text to encrypt the passwords in your target environment with your custom key. See [“Migrating a custom encryption keystore”](#) on page 200.
9. Install OpenPages. On the **Database Server** card, point to the database server from your source environment. Select **Already Installed** for the **Install Database** option.
See Chapter 6, [“Install IBM OpenPages with Watson,”](#) on page 57.
10. Update the location of the OpenPages storage directory, `openpages-storage`, in the database. See one of the following topics:
 - [“Updating the location of the openpages-storage directory \(Db2\)”](#) on page 161
 - [“Updating the location of the openpages-storage directory \(Oracle\)”](#) on page 163
11. If your deployment includes a search server, update the settings for global search. See [“Updating search server settings”](#) on page 208.
12. Update the URL host pointers for Cognos reports. See [“Updating URL host pointers for reports”](#) on page 209. See [“Updating URL host pointers for reports”](#) on page 209.
13. Verify the list of valid OpenPages application server domains and host names for Cognos Analytics. See [“Verify the list of valid domains and host names for Cognos Analytics”](#) on page 210.
14. Open your deployment in the installation app and validate it.
15. Migrate the data from the source environment to your upgraded environment. See [“Migrate files”](#) on page 201.
Use the installation app to back up and restore files and directories, such as the global search index, JSPs, and other custom deliverables.
16. Upgrade the application data. See [“Upgrading application data”](#) on page 205.
17. Do the post-migration tasks. See [“Post migration tasks”](#) on page 206.
18. If you use IBM OpenPages solutions, do the post-migration tasks for solutions. See Chapter 10, [“OpenPages solutions post-migration tasks,”](#) on page 267.
19. Test the upgraded deployment.
20. Review the new and changed features for this release to check whether there is anything that affects your installation.

Note:

Fujitsu Interstage Business Process Manager is no longer supported. For more information, see the following [software announcement](#).

The database upgrade scripts remove the Fujitsu workflow schema and any references to the Fujitsu workflow schema that are contained within the OpenPages schema.

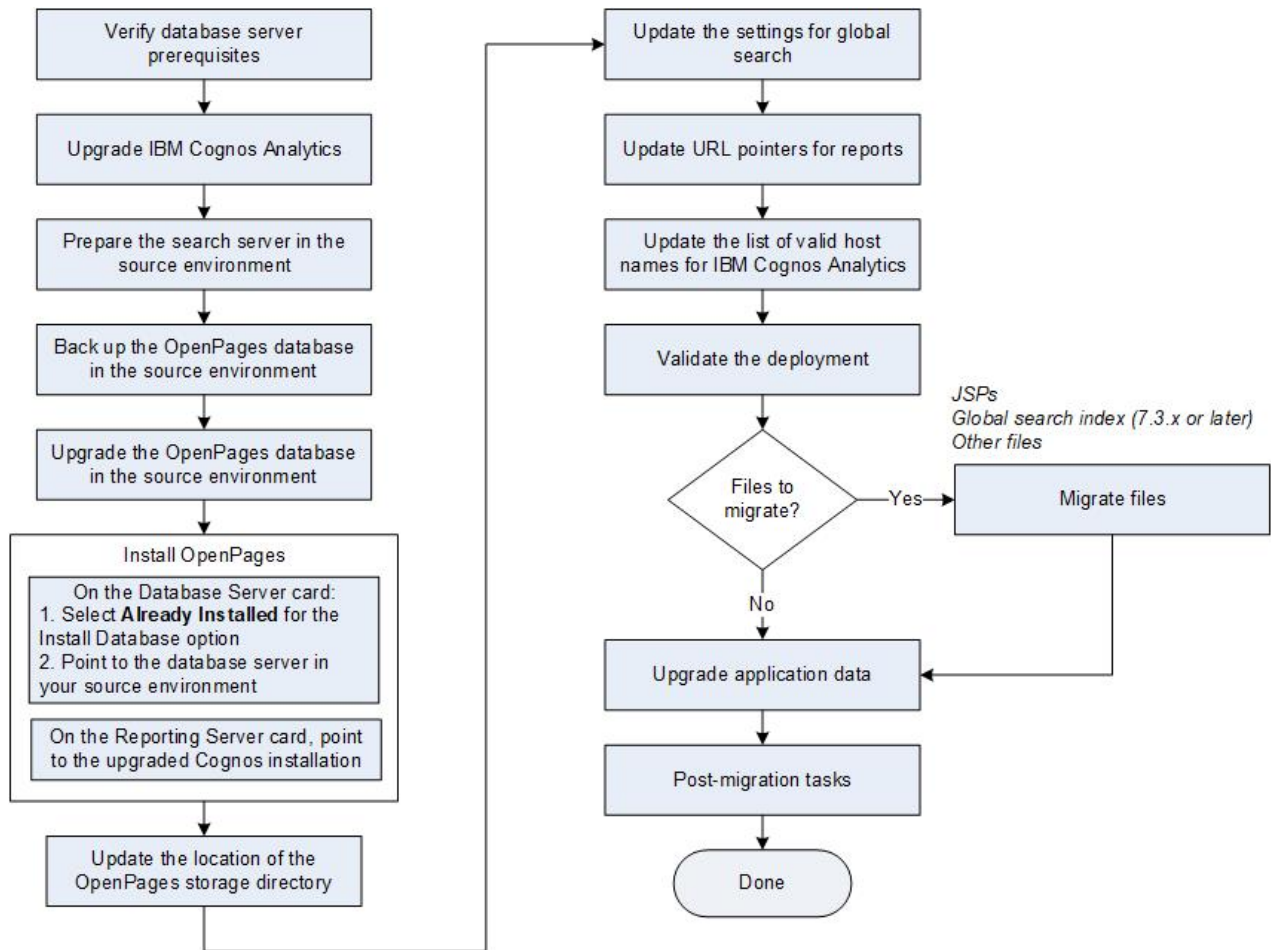


Figure 16. Migration process overview: Using the database server from your source environment

Migration process overview: Using new hardware for the database server

You can migrate IBM OpenPages with Watson and use new hardware for the database server.

Do the following tasks.

1. Install the installation server. For more information, see [“Setting up the installation server on Windows”](#) on page 41 or [“Setting up the installation server on Linux”](#) on page 43.
2. Ensure that the installation server is updated to the latest version. For more information, see [“Updating the installation server”](#) on page 47.
3. Upgrade to a supported version of Cognos Analytics. See [“Cognos Analytics upgrade process: 10.2.x to 11.1”](#) on page 197 or [“Cognos Analytics upgrade process: 11.0.x to 11.1.x”](#) on page 197.
4. If you use global search, prepare the search server. See [“Preparing the search server in the source environment”](#) on page 198.
5. Back up your existing OpenPages environment (the source environment). See [“Backing up your source environment”](#) on page 198.

Note: If you are migrating from OpenPages version 7.1.x or 7.2.x with IBM Db2 10.5, you might need to drop and re-create the reporting schema.

6. Install OpenPages. See [Chapter 6, “Install IBM OpenPages with Watson,”](#) on page 57.

If you are using your existing environment, ensure that it meets the software prerequisites. See [“Upgrade prerequisite software”](#) on page 196.

Note: You must use a new, empty directory for OpenPages.

If you are using IBM Db2

You must use the same database instance name as the database in your source environment.

Ensure that you complete the database server and OpenPages database setup tasks. See [“Checklist for the database server \(Db2\)”](#) on page 65.

If you are using Oracle

You can use a pluggable database (PDB) for the OpenPages and Cognos databases. For more information, see [“Oracle upgrade options and Oracle PDB”](#) on page 196.

You can use different names for the OpenPages schema and Cognos schema. When you restore the databases from your source environment, you must remap the schema names.

Note: If you use a different name for the OpenPages schema in the target environment, the change might impact your reports. You might need to do some remediation steps. If your reports contain references to the schema, update the reports to use the new schema name. Out-of-the-box reports are not impacted by this issue because they do not reference the schema name.

Ensure that you complete the database server and OpenPages database setup tasks. See [“Checklist for the database server \(Oracle\)”](#) on page 87.

7. Restore the OpenPages database from your source environment into the target environment. See one of the following topics:

- [“Restore the OpenPages database in your 8.2 environment \(Db2\)”](#) on page 222
- [“Restore the OpenPages database in your 8.2 environment \(Oracle\)”](#) on page 243

8. Upgrade the OpenPages database. See [“Upgrade the OpenPages database”](#) on page 199.

9. If you use a custom encryption keystore, copy the keystore file to each application server in your target environment. The file must be located at the same path as you used in your source environment. Update passwords in properties files to plain text to encrypt the passwords in your target environment with your custom key. See [“Migrating a custom encryption keystore”](#) on page 200.

10. Update the database connection information.

When you restore the database, the connection information from your source environment is imported. You need to update the connection information to use the new database.

See one of the following topics:

- [“Update the database connection information \(Db2\)”](#) on page 236
- [“Update the database connection information \(Oracle\)”](#) on page 260

11. Update the URL host pointers for Cognos reports. See [“Updating URL host pointers for reports”](#) on page 209.

12. Migrate the data from the source environment to your upgraded environment. See [“Migrate files”](#) on page 201.

Use the installation app to back up and restore files and directories, such as the global search index, JSPs, and other custom deliverables.

13. Upgrade the application data. See [“Upgrading application data”](#) on page 205.

14. Do the post-migration tasks. See [“Post migration tasks”](#) on page 206.

15. If you use IBM OpenPages solutions, do the post-migration tasks for solutions. See [Chapter 10, “OpenPages solutions post-migration tasks,”](#) on page 267.

16. Test the deployment.

17. Review the new and changed features for this release to check whether there is anything that affects your installation after the migration.

Note: Fujitsu Interstage Business Process Manager is no longer supported. For more information, see the following [software announcement](#).

During the migration process, you need to back up and then restore both the OpenPages schema and the Fujitsu workflow schema so that the database upgrade scripts can remove any references to the Fujitsu

workflow schema that are contained within the OpenPages schema. After the OpenPages schema has these references removed, the Fujitsu workflow schema is then be removed to complete the upgrade.

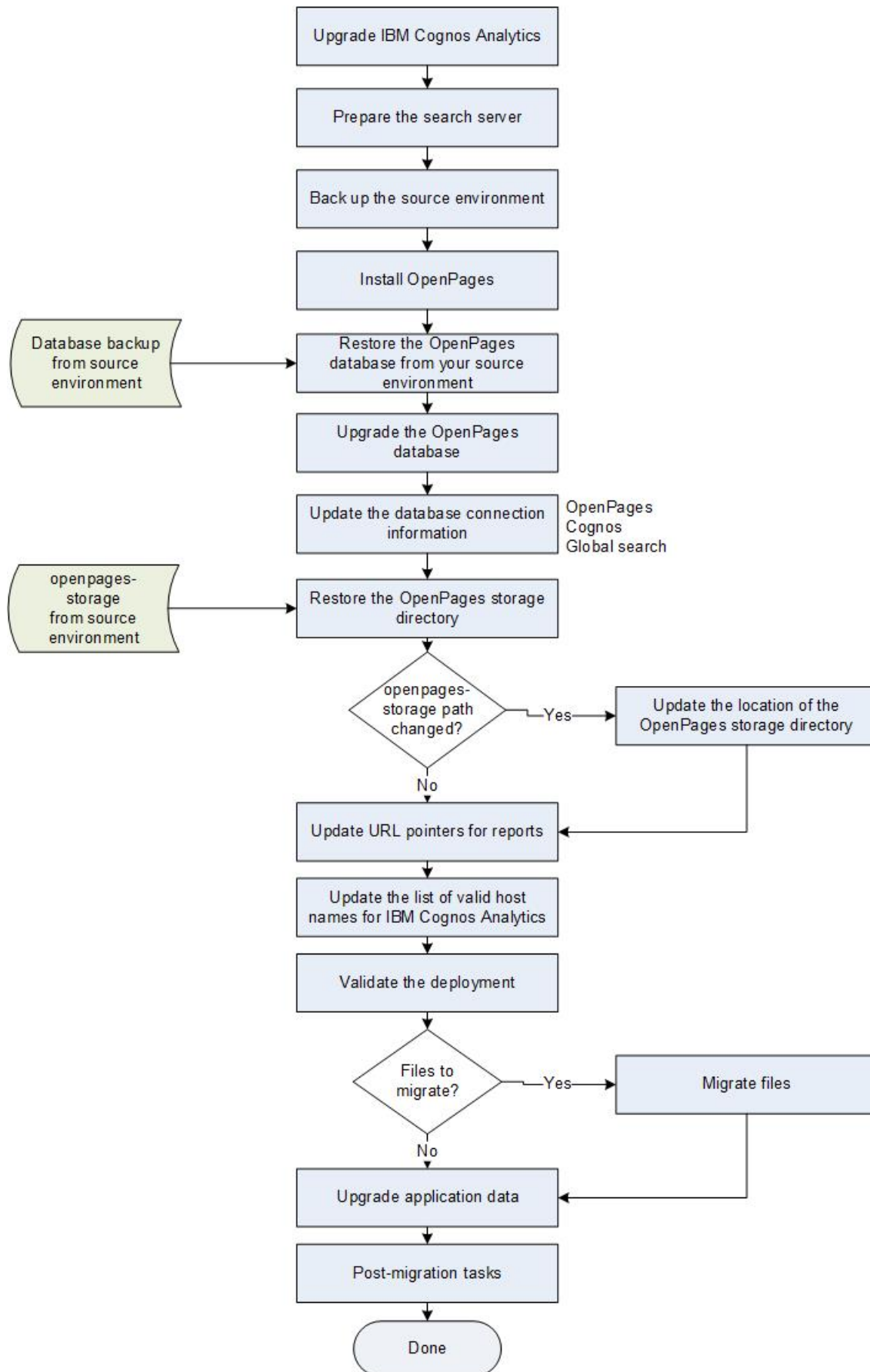


Figure 17. Migration process overview: Using new hardware for the database server

Upgrade prerequisite software

If you want to use your existing IBM OpenPages with Watson environment for the migration, ensure that it has the supported versions of the software required by IBM OpenPages with Watson

Review the software prerequisites for application servers, reporting servers, the database server, and the search server. For more information, see [“Software prerequisites” on page 33](#).

Important: Do not uninstall IBM WebSphere Application Server Network Deployment. After the migration is complete, you can do an optional task to remove it.

Important: Fix pack 8.2.0.1 supports Db2 11.5.4. If you are migrating to 8.2, complete the migration to 8.2 before you upgrade to Db2 11.5.4. Otherwise, you will see errors during the OpenPages database upgrade.

For example, if you are migrating from version 7.3.x, do the following steps:

- If you are using IBM Db2, upgrade to a supported version. See [“Upgrade Db2” on page 67](#).
- If you are using Oracle 12.1.0.2, upgrade to a supported version. See [“Upgrading Oracle from 12.1.x to 12.2.0.1” on page 93](#) or [“Oracle Database 18c or 19c installations” on page 88](#).
- Install Cognos Analytics version 11.1.3 or later continuous releases. See [“Cognos Analytics upgrade process: 10.2.x to 11.1” on page 197](#) or [“Cognos Analytics upgrade process: 11.0.x to 11.1.x” on page 197](#).

Tip: You do not need to uninstall Cognos. Cognos Analytics supports the installation of multiple versions on a server. For more information, see the [Cognos documentation](#).

- Install a supported version of IBM SDK, Java Technology Edition on each application server and the search server. See [“Getting a copy of the IBM SDK \(Windows\)” on page 60](#) or [“Getting a copy of the IBM SDK \(Linux\)” on page 63](#).

Also, ensure that your users have a supported browser. See [“Prerequisite software for OpenPages client computers” on page 38](#).

Note for 7.3.x customers:

Fujitsu Interstage Business Process Manager is not supported in IBM OpenPages with Watson version 7.4 and later. For more information, see the following [software announcement](#).

If you have Fujitsu Interstage Business Process Manager Studio installed, you can uninstall it.

Oracle upgrade options and Oracle PDB

You have several options when you migrate IBM OpenPages with Watson.

Upgrade Oracle

Note: If you are using Oracle 12.1.0.2, you must upgrade to a supported version of Oracle when you prepare your deployment for the fresh installation of OpenPages. Version 8.2 does not support Oracle 12.1.x. For more information, see [“Upgrading Oracle from 12.1.x to 12.2.0.1” on page 93](#).

Oracle 18c

If you are migrating from 8.1.x, you can upgrade to Oracle 18c at any time.

If you are migrating from 7.3.x, 7.4.x, or 8.0.x, you can upgrade to Oracle 18c during or after the migration to OpenPages 8.2. Your deployment temporarily uses a configuration that is not supported for end users. Do not allow end users to log in to OpenPages until you complete the migration to 8.2. Versions of OpenPages before 8.1.0 do not support Oracle 18c.

When you upgrade Oracle, you have two options:

- Upgrade Oracle in-place. See [“Upgrading Oracle from 12.x to 18c or 19c \(in-place\)” on page 90](#).
- Install Oracle and migrate the database. See [“Upgrading Oracle from 12.x to 18c or 19c \(migration\)” on page 91](#).

Oracle 19c

If you are migrating from 8.1.0.1 or later, you can upgrade to Oracle 19c at any time.

If you are migrating from 8.1.0.0 or earlier, you can upgrade to Oracle 19c during or after the migration to OpenPages 8.2. Your deployment temporarily uses a configuration that is not supported for end users. Do not allow end users to log in to OpenPages until you complete the migration to 8.2. Versions of OpenPages before 8.1.0.1 do not support Oracle 19c.

When you upgrade Oracle, you have two options:

- Upgrade Oracle in-place. See [“Upgrading Oracle from 12.x to 18c or 19c \(in-place\)”](#) on page 90.
- Install Oracle and migrate the database. See [“Upgrading Oracle from 12.x to 18c or 19c \(migration\)”](#) on page 91.

Oracle PDB (multitenant)

You can use a pluggable database (PDB) for the OpenPages database. OpenPages supports Oracle PDB with Oracle 12.2.0.1, 18c, and 19c.

For more information, see [Introduction to the Multitenant Architecture](#) in the Oracle documentation.

You can implement PDB when you migrate to OpenPages 8.2.

- When you install or upgrade Oracle, create a container database and a blank pluggable database for OpenPages.
- When you restore the database from your source environment into your 8.2 environment, import it into the pluggable database.
- When you update the database connection information, use the service name of the pluggable database, not the name of the container database.

You can also use a pluggable database for the Cognos content store.

Cognos Analytics upgrade process: 10.2.x to 11.1

Use these steps if you are upgrading from Cognos 10.2.x.

Note: If you are upgrading from Cognos 11.0.x, see [“Cognos Analytics upgrade process: 11.0.x to 11.1.x”](#) on page 197.

To upgrade Cognos 10.2.x, you install Cognos Analytics and then migrate your data. The Cognos Analytics documentation provides details about how to upgrade. For more information, see [Planning your upgrade to IBM Cognos Analytics](#) and [Standard upgrade process](#).

Tip: You do not need to uninstall Cognos. Cognos Analytics supports the installation of multiple versions on a server. For more information, see the [Cognos documentation](#).

During the Cognos upgrade process, you move your content store to the new version of Cognos. The Cognos documentation describes two methods for moving the content store. One of the options is to move the entire content store by backing up and restoring the database. If you want to use this option, see the following topics:

IBM Db2

- [“Backing up the Cognos database during a migration to 8.2 \(Db2\)”](#) on page 221
- [“Restoring the Cognos content store \(Db2\)”](#) on page 225

Oracle

- [“Backing up the Cognos content store during a migration \(Oracle\)”](#) on page 242
- [“Restoring the Cognos content store \(Oracle\)”](#) on page 250

Cognos Analytics upgrade process: 11.0.x to 11.1.x

Use these steps if you are upgrading from Cognos 11.0.x.

Note: If you are upgrading from Cognos 10.2.x, see [“Cognos Analytics upgrade process: 10.2.x to 11.1”](#) on page 197.

If you are currently using Cognos Analytics 11, you can do an in-place upgrade. See [“Upgrading Cognos”](#) on page 114.

The Cognos Analytics documentation provides details about how to upgrade. For more information, see [Upgrading your current version of Cognos Analytics 11](#).

During the Cognos upgrade process, you back up the Cognos content store. See the following topics:

- IBM Db2: [“Backing up the Cognos database \(Db2\)”](#) on page 411
- Oracle: [“Backing up the Cognos content store \(Oracle\)”](#) on page 413

Preparing the search server in the source environment

Before you migrate to 8.2, prepare the search server in your source environment .

About this task

The steps that you need to do depend on the version that you are migrating from.

Procedure

1. Start the search server in your source environment.
For more information, see [“Start or stop the global search services”](#) on page 312.
2. Log in to OpenPages as a user with administrative privileges.
3. Switch to the Standard UI.
4. Disable global search.
Click **Administration > Global Search** and click **Disable**.
Tip: You do not need to drop the global search index.
5. If the **Update** button is enabled, click it to update the search index.
6. Stop the search services in your source environment.
For more information, see [“Start or stop the global search services”](#) on page 312.
7. Verify that global search is fully stopped by doing the following steps:
 - a) In the directory `<SEARCH_HOME>/opsearchtools/`, examine the files `opsearchtool_openpages.state` and `opsearchtool_folderacl.state` and verify that the PID value is -1.
 - b) From a browser, point to your search server at ports 8983 and 8985 and make sure that the Solr search platform cannot be reached, for example, `https://<search-server>:8983/` and `https://<search-server>:8985/`.
If the stop verification fails, repeat the preceding step and then follow the steps in [“Forcing a reset of global search”](#) on page 435.

Backing up your source environment

Before you migrate to 8.2, back up IBM OpenPages with Watson in your source environment.

Procedure

1. Stop the application servers (admin and non-admin), reporting servers (active and standby), database server, and the search server in your source environment.
2. Back up the databases.
 - If you are using IBM Db2, see [“Back up the database \(Db2\)”](#) on page 219.

- If you are using Oracle, see [“Backing up the OpenPages database during a migration \(Oracle\)”](#) on page 241.
3. Back up the `openpages-storage` directory.

The `openpages-storage` directory can be located on a server in your deployment or it can be on a separate network share.

The default location is `<OP_HOME>/openpages-storage`.
 4. If you modified the `web.xml`, `application.xml`, or if you customized settings in the IBM WebSphere Integrated Solutions Console, make a note of your changes.

After the migration is complete, you need to re-implement your changes.
 5. If you modified the standard reports that are provided with OpenPages, copy them to your personal folders.

OpenPages standard reports can be overwritten during a migration.

After the migration, you can change the reports and restrict access to them.
 6. On each application server, as the OpenPages installation user (`opuser`), rename the top level OpenPages directory to `OpenPages-<current-version>`. For example, if you are migrating from version 7.3.0.1, rename the OpenPages directory to `OpenPages-7.3.0.1`.

You use this backup directory to restore the current OpenPages version if you need to roll back from the migration.
 7. On each reporting server, as the OpenPages installation user (`opuser`), rename the top level CommandCenter directory to `CommandCenter-<current-version>`. For example, if you are migrating from version 7.3.0.1, rename the CommandCenter directory to `CommandCenter-7.3.0.1`.

You use this backup directory to restore the current `<CC_HOME>` directory if you need to roll back from the migration.
 8. On the search server, as the OpenPages installation user (`opuser`), rename the top level OpenPages directory to `OpenPages-<current-version>`. For example, if you are migrating from version 7.3.0.1, rename the OpenPages directory to `OpenPages-7.3.0.1`.

You use this backup directory to restore the current search server version if you need to roll back from the migration.
- Note:** The search server is an optional component that was first available in OpenPages 7.2.0.0.

Upgrade the OpenPages database

The tasks that you need to do to upgrade the OpenPages database depend on the migration scenario that you are following.

Using the database server from your source environment

- Back up the database.

See one of the following topics:

 - [“Back up the database \(Db2\)”](#) on page 219
 - [“Backing up the OpenPages database during a migration \(Oracle\)”](#) on page 241
- Upgrade the database manually.

See one of the following topics:

 - [“Upgrade the databases \(Db2\)”](#) on page 226
 - [“Upgrade the OpenPages database \(Oracle\)”](#) on page 252

Using new hardware for the database server

- Back up the database in your source environment.

See one of the following topics:

- [“Back up the database \(Db2\)” on page 219](#)
- [“Backing up the OpenPages database during a migration \(Oracle\)” on page 241](#)
- Import the OpenPages database from your source environment into the database on the new database server.
See one of the following topics:
 - [“Restore the OpenPages database in your 8.2 environment \(Db2\)” on page 222](#)
 - [“Restore the OpenPages database in your 8.2 environment \(Oracle\)” on page 243](#)
- Upgrade the OpenPages database.
See one of the following topics:
 - [“Upgrade the databases \(Db2\)” on page 226](#)
 - [“Upgrade the OpenPages database \(Oracle\)” on page 252](#)
- Update the connection information in the database.
See one of the following topics:
 - [“Update the database connection information \(Db2\)” on page 236](#)
 - [“Update the database connection information \(Oracle\)” on page 260](#)

Migrating a custom encryption keystore

If you use a custom encryption keystore, you need to migrate it to your target environment.

Procedure

1. After you upgrade the databases, copy the encryption keystore file from your source environment to each application server in your target environment. The path to the file must match the path that you used in your source environment.
2. Update passwords in properties files.
If you are using the database server from your source environment, do this step after you install OpenPages and before you continue with the migration process.
If you are using a new database server, do this step before you migrate the data from the source environment to your upgraded environment.
 - a) On each application server, change the passwords in properties files to plain text, save the files, and then restart the application server.
For more information, see "Updating property files on application servers to use a custom key" in the *IBM OpenPages with Watson Administrator's Guide*.
 - b) On each reporting server, change the passwords in properties files to plain text, save the files, and then restart the reporting server.
For more information, see "Updating property files on reporting servers to use a custom key" in the *IBM OpenPages with Watson Administrator's Guide*.
 - c) If you use global search, change the passwords in properties files to plain text, save the files, and then restart the server.
For more information, see "Updating property files on the search server to use a custom key" in the *IBM OpenPages with Watson Administrator's Guide*.

The passwords are encrypted with the updated encryption key when you restart the servers.
3. If you use IBM OpenPages Loss Event Entry, re-enter the password for each locale.
 - a) Start the configuration tool. Go to `http://<server_name>:<port>/openpages/app/jspview/lossevent#/editconfig`
 - b) Log in with a user account that is a member of the OPAdministrators group.
 - c) Under the **Locales** section, expand each locale and enter the password.

d) Close the configuration tool.

The passwords are encrypted with the updated encryption key.

4. If you use LDAP for user provisioning, do the following steps:

a) Click  > **Users and Security** > **User LDAP Configuration**.

Or, in the Standard UI, click **Administration** > **User LDAP Configuration**.

b) Edit the LDAP configuration.

c) In the **Security credentials** field, re-enter the password that is used to authenticate with the LDAP server.

d) Click **Save**.

The security credentials are encrypted with the updated encryption key.

5. If you use natural language classifiers, do the following steps:

a) Click  > **Integrations** > **Mapping and Taxonomy Suggestions**.

Or, in the Standard UI, click **Administration** > **Cognitive Services** > **Natural Language Classifiers**.

b) Edit the classifier configuration.

c) In the **API Key** field, re-enter the API key of the Natural Language Classifier instance.

d) Click **Save**.

e) Repeat these steps for each classifier configuration.

The API keys are encrypted with the updated encryption key.

Migrate files

You can migrate application files from your previous installation of IBM OpenPages with Watson.

For example, your source environment might contain custom reports that you want to use in your 8.2 environment.

You can restore files onto a system that uses a different operating system than the source system. For example, if the application server in your source environment is running Microsoft Windows, you can restore the files to a Linux application server.

The topology of your source and target environments can differ. For example, if your source environment uses clustered application servers, you can migrate files to a target system that uses a single application server or to a target system that uses a different number of clustered application servers.

This video demonstrates how to migrate files. The video shows 7.4 but the steps are similar for 8.2.

<https://youtu.be/LSdcSoYbp6Q>

Backing up application files

Use the IBM OpenPages with Watson installation app to back up application files.

Before you begin

- Ensure that the installation server is updated to the latest version. For more information, see [“Updating the installation server” on page 47](#).
- Ensure that all of the servers in the source environment are stopped.
- If you use clustered application servers or reporting servers, ensure that all of the nodes are synchronized.
- Ensure that the installation server computer has sufficient disk space to store the backup files.
- Ensure that the installation server computer can access the servers in the source environment.

About this task

Your source environment might include custom files, reports, services deliverables, and other application files that you want to use in your target environment. Back up the application files in your source environment. You can then restore them in your target environment.

If your source environment includes customized JSP files, you must manually incorporate those customizations into the JSP files in your target environment. If you have already merged the edits into the JSP files that are deployed by the installer, do not include the JSP files in the backup since the restore process will overwrite your edits to the JSP files in your target environment.

If you are using clustered application servers or reporting servers, synchronize the nodes, and then back up the files on the primary server. When you restore the application files, the files are copied to each server in the cluster automatically.

Keep the following points in mind:

Application server

- Do not select the `openpages-storage` directory for the backup. The directory can be very large. Instead, copy the directory to your target environment. Or, make the directory available on a network share.

Search server


- Select the `openpages_search.properties` file for the backup. During the post migration steps, you can modify the settings in this file, if needed.
- Select the `<SEARCH_HOME>/openpages-solr-index` directory for the backup. The directory contains the global search index.

Procedure

1. Start the installation app and log in.
2. Open your deployment.
3. Click **Current Deployment** and select **File Backup**.

The left pane displays an application server card, a reporting server card, and a search server card.

4. If your source environment does not have a search server, delete the search server card.

Tip: You can add a card that you deleted. Select the server type from the list in the left pane and then click .


5. Click one of the cards and enter the hostname and other details about the server in your source environment.

On the application server card, if you are using a clustered environment, enter the information for the admin application server.

On the reporting server card, if you are using a clustered environment, enter the information for the active reporting server.

If the OpenPages installation server is installed on the same physical computer as the server that you are backing up, disable the **Remote** option.

6. Use the toggles to select the directories that you want to migrate.

Click  to view the directory path.

The **Files selected for backup** field displays the files and directories that you selected.

Note: When you select the **Model Query Subjects** toggle, the `<CC_HOME>/framework/conf` directory is displayed in the **Files selected for backup** field. However, only the static model query subjects are backed up and restored. This is intended.

7. If you want to back up and restore more files or directories, enter them in the **Additional files to backup**.

Use relative paths to specify files and directories. Paths cannot contain spaces. Separate each item with a comma. Do not enter spaces.

- On the application server card, use paths relative to the **OP Home Directory**. For example, if you want to migrate the files `/opt/IBM/OpenPages/temp/myfile.xml` and `/opt/IBM/OpenPages/mydir/otherfile.xml`, type:

```
/temp/myfile.xml,/mydir/otherfile.xml
```

- On the reporting server card, use paths relative to the **Command Center Home Directory**. For example, if you want to migrate the `/opt/OpenPages/CommandCenter/temp/myreports/` directory, type `/temp/myreports/`
- On the search server card, use paths relative to the **Search Server Home Directory**. For example, if you want to migrate the file `/opt/IBM/OpenPages/Search/temp/data.xml`, type `/temp/data.xml`

8. Decide whether you want files to be overwritten when you restore them.

If you want the files from your source environment to overwrite the files in your target environment, enable the **Overwrite files during restore** option. During the restore process, the files in your target environment will be backed up before they are overwritten.

If you do not want the files from your source environment to overwrite the files in your target environment, disable the **Overwrite files during restore** option. During the restore process, if a file exists in the target environment, the file is skipped.

9. Click **Save**.

10. Click **Backup**.

If an error occurs, a message is displayed on the server card. Click the server card, and then click ⓘ to see the error message.

The backup process creates a `.zip` file for each server card. The files are saved in the following locations:

- The files are stored on the installation server computer in: `<installation_server_home>/installer/<deployment_name>/migration/`.

The restore process uses the files in this directory.

- For remote servers, the files are stored on the source server in: `<OP_HOME>/agent/op-agent/agent/src/deployment/<deployment_name>/migration/`.
- For the application server the files are stored on the source server in the OPBackup directory, for example `<OP_HOME>/openpages-backup-restore`.
- For the reporting server the files are stored on the source server in the OPCCBackup directory, for example `<OP_HOME>/op-cc-backup-restore`.
- For the search server, the files are stored on the source server in the OPSearchBackup directory, for example, `/op-search-backup-restore`.

The files are named `op_<node_name>_<incremental_number>_source_backup_<timestamp>.zip`.

Note: The time stamp is based on the time zone of the source server computer.

If a file or directory was not found on the source server, it is skipped. For example, if a file name contains a typographical error, the file does not get backed up. The log file includes messages about any files that were skipped.

11. Download and review the log file.

Restoring application files

Use the IBM OpenPages with Watson installation app to restore application files from the source environment to your target environment.

Before you begin

- Ensure that all of the servers in the environment are stopped.

About this task

The restore process uses the files in the `<installation_server_home>/installer/<deployment_name>/migration/` directory. The files are called: `op_<node_name>_<incremental number>_source_backup_<timestamp>.zip`

Only the files with the most recent timestamps are used.

When the files from the source system are restored, any files on the target system that will be overwritten are backed up. A zip file that contains all original files that were replaced during the restore process is created. The backup files are called `op_<node_name>_<incremental number>_target_backup_<timestamp>.zip`.

- The application server files are stored in the **OP Backup Restore Directory** on the target server, for example, `/opt/IBM/OpenPages/openpages-backup-restore`.
- The search server files are stored in the **OP Backup Restore Directory** on the target server.
- The reporting server files are stored in the **Command Center Backup Directory** on the target server, for example, `/opt/IBM/OpenPages/openpages_cc_backup_restore`.

Procedure

1. Start the installation app and log in.
2. Open your target deployment.
3. Click **Restore**.
Wait for the process to complete.
4. Download the log file and review it. Look for any files or directories that were skipped.
5. If you chose **Overwrite files during restore** when you backed up files, do the following steps:
 - a) Go to the OpenPages backup directory on the admin application server: `<OP_HOME>/openpages-backup-restore` by default.
 - b) Locate the `op_app_1_target_backup_<timestamp>.zip` file.
 - c) Locate the following files in the zip file:
 - `<OP_HOME>/profiles/OpenPagesNode/installedApps/OpenPagesCell/op-apps.ear/sosa.war/images/rev/branding/productTitle_header.png`
 - `<OP_HOME>/profiles/OpenPagesNode/installedApps/OpenPagesCell/op-apps.ear/sosa.war/images/rev/branding/productTitle_about.gif`
 - d) Copy the files to the following locations on the target application server:
 - `<OP_HOME>/wlp-user/shared/apps/op-apps.ear/sosa.war/images/rev/branding/productTitle_header.png`
 - `<OP_HOME>/wlp-user/shared/apps/op-apps.ear/sosa.war/images/rev/branding/productTitle_about.gif`
 - e) Repeat this process on each application server.

Restore the storage directory in the target environment

You need to make the `<OP_HOME>/openpages-storage` directory available to the servers in your target environment.

The `<OP_HOME>/openpages-storage` directory can be stored on a server in your deployment or it can be on a separate network share.

- If the directory is on a server in your source environment, restore the backup that you created when you prepared for the migration. Copy the directory to a server in your target environment. If the `<OP_HOME>/openpages-storage` directory exists on the target server, you can overwrite it.

Or, copy the backed-up directory to a network share and give the servers in your target environment access to the network location.

- If your `<OP_HOME>/openpages-storage` directory is on a network share, ensure that the servers in your target environment can access the network location.


Note: You can also use OPBackup and OPRestore to move the openpages-storage directory.

If the location of the openpages-storage directory is different than it was in your source environment, update the OpenPages database with the location of the openpages-storage directory.

Upgrading application data

You must upgrade the application data that is required for the operation of IBM OpenPages with Watson. The application data includes localized text and other miscellaneous settings that are required by OpenPages.

Before you begin

- Ensure that the installation server is updated to the latest version. For more information, see [“Updating the installation server”](#) on page 47.
- If **System Admin Mode** is enabled in your target environment, disable it. Click , and then click **Disable System Admin Mode**.
- If IBM Cognos Configuration is open, close it.
- Ensure that the OpenPages application servers and the reporting servers are running.
- If you use a custom keystore for OpenPages, verify that the keystore file (.jks) and the `keystore.properties` file exist on each application server in your target environment. Ensure the path to the file is also the same in the source and target environments.

About this task

This video demonstrates how to upgrade application data. The video shows 7.4 but the steps are similar for 8.2:

<https://youtu.be/6SMtztzNtJw>

Procedure

1. If your source environment includes customized JSP files, you must manually incorporate those customizations into the JSP files in your target environment. Back up any customized JSP files that are located in the following directories:

```
<OP_HOME>/profiles/<OpenPages-node-name>/installedApps/  
<OpenPages-cell-name>/op-apps.ear/openpages.war
```

```
<OP_HOME>/profiles/<OpenPages-node-name>/installedApps/  
<OpenPages-cell-name>/op-apps.ear/publishweb.war
```

```
<OP_HOME>/profiles/<OpenPages-node-name>/installedApps/  
<OpenPages-cell-name>/op-apps.ear/sosa.war
```

- a) Restart the application servers in the target environment to ensure that the servers are synchronized.
- b) For each customized JSP file in your source environment, locate the JSP file in the target environment. Merge the edits into the JSP file on the administrative application server in your target environment.

JSPs are stored in the following locations:

```
<OP_HOME>/wlp-user/shared/apps/op-apps.ear/openpages.war
```

```
<OP_HOME>/wlp-user/shared/apps/op-apps.ear/publishweb.war
```

```
<OP_HOME>/wlp-user/shared/apps/op-apps.ear/sosa.war
```

- c) After all JSP file edits have been incorporated, restart the application servers.
2. Start the installation app and log in.
 3. Open your target deployment.
 4. Click **Upgrade App Data**.
 - a) If **Upgrade App Data** is not enabled, click **Validate**.

If the **Upgrade App Data** button is still not available, verify that the OpenPages database upgrade scripts completed successfully. See [“Upgrade the databases \(Db2\)”](#) on page 226 or [“Upgrade the OpenPages database \(Oracle\)”](#) on page 252.
 - b) Click **Upgrade App Data**.
 - c) Wait for the process to complete.
 5. Review the log files.

If any issues occurred, look for a log file in the <OP_HOME>/installer/migration/upgrade/addon_module/loaderdata directory. Typical data loading activity is logged in the <OP_HOME>/bin/logs directory.

Post migration tasks

Complete the following tasks after you migrate IBM OpenPages with Watson to version 8.2.

- Verify the list of valid domain names and host names.

For more information, see [“Verify the list of valid domains and host names for Cognos Analytics”](#) on page 210.

- If your OpenPages with Watson environment is using 3DES password encryption, change the encryption algorithm to AES, which is more secure.

For more information, see [“Upgrading the OpenPages password encryption algorithm to AES encryption”](#) on page 211.

- Determine if you need to update security rules. You might need to update security rules if you use reporting periods or if you plan to use reporting periods.

For more information, see [“Updating security rules”](#) on page 211.

- If you customized configuration files in your source environment, reapply or merge your changes.

For more information, see [“Custom settings in configuration files”](#) on page 212.

- If you installed a search server, you must complete some post upgrade tasks.

For more information, see [“Search server post migration tasks”](#) on page 212.

- If the OPSysSystem password is different in the source environment and the 8.2.0.x environment or if you changed the default OPSysSystem password, update the OPSysSystem password in the 8.2.0.x environment.

For more information, see [Changing the OPSystem password](#) in the *IBM OpenPages with Watson Administrator's Guide*.

- If you modified the `web.xml`, `application.xml`, or if you customized settings in the IBM WebSphere Integrated Solutions Console in your source environment, re-implement the changes.

For example, see the following topics in the *IBM OpenPages with Watson Administrator's Guide*:

- Shortening the URL for OpenPages with Watson
- Enabling secure session cookies in WebSphere Liberty
- Configuring extended access logging on WebSphere Liberty

If you use SSL with the database server, you need to re-establish the SSL certificates after you migrate. When you install IBM OpenPages with Watson, the installation process configures a keystore for IBM WebSphere Liberty. By default, the Liberty keystore is also used for the database server certificates. You can extract the certificates from the database server and then re-import them into the Liberty keystore.

Tip: If you use Db2, you can use the keystore from your source environment by changing the keystore that is used by Db2. For more information, see the *IBM OpenPages with Watson Administrator's Guide*.

- If single sign-on (SSO) was configured in the source system, you need to update the SSO configuration in your target environment.

For more information, see [Chapter 13, “Single sign-on integration for the OpenPages application server,” on page 321](#).

- If LDAP was configured in the source system and you did not migrate the `aurora_auth.config` file, you need to re-enable LDAP in your target environment.

For more information, see [“Enable LDAP after migrating” on page 213](#).

- If you use the approval app, upgrade the app.

For more information, see [“Upgrade the approval app” on page 371](#).

- If you use IBM OpenPages Loss Event Entry, upgrade it.
 - If you are using your existing hardware, see [“Upgrade process overview for Loss Event Entry” on page 378](#).
 - If you are moving IBM OpenPages Loss Event Entry to new hardware, see [“Migration process overview for Loss Event Entry” on page 381](#).

- If you want to use Dynamic Query Mode (DQM) for the OpenPages reporting framework, configure a JDBC connection to the OpenPages database.

For more information, see [“Updating the connection to the OpenPages database for Cognos \(Db2\)” on page 238](#) or [“Updating the connection to the OpenPages database for Cognos \(Oracle\)” on page 263](#).

- Update the reporting schema.

For more information, see [“Updating the reporting schema” on page 214](#).

- Regenerate the reporting framework.

Depending on your environment, you might need to regenerate the reporting framework. For more information, see [“Regenerating the reporting framework” on page 214](#).

- If you do not see the OpenPages reports and packages in the IBM Cognos Analytics, import the OpenPages Platform V6 package.

For more information, see [“OpenPages reports are not displayed in IBM Cognos Analytics” on page 464](#).

- Optional: change the singular and plural labels for the ModelReport object type to "Model Report" and "Model Reports". Make appropriate changes in other locales.
- Verify the migration.

For more information, see [“Migration verification tests” on page 215](#).

- Test Cognos Analytics.

For more information, see [“Testing Cognos Analytics after the migration” on page 216](#).

- Optional: Back up your environment.
- Optional: Remove IBM WebSphere Application Server. See [“Removing WebSphere Application Server” on page 421](#).
- Optional: If you used IBM Business Process Manager in a prior release, remove the integration. For more information, see [Removing the IBM BPM integration from OpenPages with Watson](#).

Loading the Cognos dashboard integration after migrating

After you migrate IBM OpenPages with Watson, you must load a mandatory integration configuration so that you can use Cognos Analytics dashboards within OpenPages.

Procedure

1. Copy the `CommandCenter-integration-op-config.xml` and `CommandCenter-integration-op-file-content.zip` files from the OpenPages installation media to the administrative application server.

The files are located in the `/OP_<version>_Main/OP_<version>_Configuration/CommandCenter/loader-data` directory.

2. Open a command line.

If you are using Microsoft Windows, open a command prompt with the **Run as administrator** option.

3. Go to the `<OP_HOME>/bin` directory.
4. Run the following command to load the files.

Replace `<loader-file-path>` with the location of the `CommandCenter-integration-op-config.xml` and `CommandCenter-integration-op-file-content.zip` files.

```
ObjectManager.cmd|sh 1 c <OpenPages Administrator user> <OpenPages Administrator password>
<loader-file-path> CommandCenter-integration
```

5. If you encounter any errors, review the log file, `<loader-file-path>/ObjectManager.log`.

Updating search server settings

Update the search server settings in IBM OpenPages with Watson.

Do this task if your deployment includes a search server.

You do not need to do this task if you did not install a search server.


Procedure

1. Update the database connection information for the search server.
See the following topics:
 - [“Updating the database connection information for the search server \(Db2\)” on page 238](#)
 - [“Updating the database connection information for the search server \(Oracle\)” on page 263](#)
2. If it is not already started, start the global search services.

For more information, see [“Start or stop the global search services” on page 312](#).

3. If the global search component is enabled, you must disable it.
 - a) Log on to OpenPages as a user with administrative privileges. Go to the Standard UI.
 - b) Click **Administration > Global Search**.
 - c) Click **Disable**.
4. Stop the global search services.

For more information, see [“Start or stop the global search services” on page 312](#).

5. If the global search service (Apache Solr) user name and password are different than in your source environment, update them.
 - a) Open the **Settings** page.
 - In the Task Focused UI, click  > **System Configuration** > **Settings**.
 - In the Standard UI, click **Administration** > **Settings**.

To access settings, you must have the **Settings** application permission set on your account.
 - b) Click **Applications** > **Common** > **Configuration**.
 - c) Click **Show Hidden Settings** and set the value to `true`.
 - d) Click **Platform** > **Search**.
 - e) Update the **Solr user ID** and **Solr password** settings.

Updating URL host pointers for reports

After you migrate, change port settings in a production environment, or if you want to refresh a test environment from a production database, you might need to update the URL host pointers on the application server so that links in reports work properly.

You need to update the URL host pointers if the host, port, or protocol of the application server has changed. Check the **Object Generator URL** setting to verify that the host, port, and protocol are correct. If the port, host, and protocol are correct, you do not need to do this task.


You can update links in reports by modifying URL host pointer settings, and then propagating these reporting schema changes to the application server.

To update the reporting schema, you can do either of the following:

- Run an SQL script that incrementally updates the reporting schema with the changes (recommended).

Note: For SQL tool information, see the topic "Database tool information" in the *IBM OpenPages with Watson Administrator's Guide*.
- Use the IBM OpenPages with Watson application user interface to re-create the entire reporting schema.

Procedure

1. Start the IBM OpenPages with Watson services on the admin application server.
2. Log on to the OpenPages with Watson application user interface as a user with administrator privileges.
3. Open the **Settings** page.
 - In the Task Focused UI, click  > **System Configuration** > **Settings**.
 - In the Standard UI, click **Administration** > **Settings**.

To access settings, you must have the **Settings** application permission set on your account.
4. Change the **Object URL Generator** settings.
 - a) Expand **Platform** > **Reporting Schema** > **Object URL Generator**.
 - b) Update the **Object Generator URL** settings, as required, to point to the application server (such as a test application server). Make sure to click **Save** after you modify each setting.

Table 58. Object Generator URL settings

Setting Name	Description
Host	The changed name of the application server. Example : test-eng1

Table 58. Object Generator URL settings (continued)	
Setting Name	Description
Port	The changed port number of the application server. Example : 10108
Protocol	The changed protocol for accessing the application server. Valid values are either http or https.

5. To update the changed URL setting on the application server, update the reporting schema using one of the following methods:

- Method 1: Run the following SQL script to incrementally update the reporting schema (recommended):
 - a. From a computer with a SQL tool and access to the database server, log on to SQL as the OpenPages database user (for example, openpages).
 - b. Run the following SQL statements to update the reporting schema:

```
begin
OP_RPS_MGR.SET_DETAIL_PAGE_URL_IN_RPS_RT;
end;
/
```

- Method 2: Re-create the entire reporting schema by using the application user interface. For more information, see "Creating or recreating the reporting schema" in the *IBM OpenPages with Watson Administrator's Guide*.

Verify the list of valid domains and host names for Cognos Analytics

If you imported the Cognos Analytics content store when you migrated IBM OpenPages with Watson, verify the list of valid domains and host names. Ensure that all application servers are listed. Also, verify the public domain that is used for load balanced environments on all reporting servers.

Procedure

1. Log on to the reporting server as a user with administrative privileges.
2. Start IBM Cognos Configuration.
3. In the **Explorer** pane, go to **Local Configuration > Security > IBM Cognos Application Firewall**.
4. In the **Properties** pane, click the **Valid domain names or hosts**.
5. Verify that all OpenPages application servers are listed.
6. If any application servers are missing from the list, add them.
 - a) Click the pencil icon.
 - b) In the **Valid domain or hosts** window, click **Add**.
 - c) Enter the names of the OpenPages application servers.
 - d) Click **OK**.
 - e) Save the configuration and restart the Cognos service.

If you use Windows Services to restart the Cognos service, the service is listed as **IBM Cognos**.

Upgrading the OpenPages password encryption algorithm to AES encryption

Determine the password encryption algorithm that your environment is using and upgrade it to AES encryption, if needed.

About this task

If your OpenPages with Watson environment is using the OP-CUSTOM or 3DES encryption algorithm, change the encryption algorithm to AES, which is more secure.

To determine the encryption algorithm that your environment is using, examine the ALGORITHMNAME value of the ENCRYPTIONMODULES table entry that has an INACTIVE value of 0.

Procedure

1. Edit the `<OP_HOME>/aurora/conf/aurora.properties` file and the `<OP_HOME>/aurora/bin/op-backup-restore.env` file and change any encrypted passwords to plain text.

- If you are using 3DES, look for lines that contain `{3DES}`.

For example, suppose the `aurora.properties` file contains the following line:
`database.PASSWORD={3DES}Rj+steg+3eU7kb80+\=\=`. The database password is encrypted with the 3DES algorithm. Replace the encrypted password with the password in plain text, for example, `database.PASSWORD=db_password`.

- If you are using OP-CUSTOM, the lines do not have an algorithm indicator. Look for encrypted passwords and change each of them to the password in plain text.

The passwords are encrypted with the AES algorithm when you restart the OpenPages with Watson services in step 3.

2. Open a command or shell window on the OpenPages application server.

Go to the `<OP_HOME>/bin` directory.

From the command or shell window, run the following command on a single line:

```
UpdatePasswordEncryptionAlgorithm.sh|.cmd -Mode CA -AlgorithmName AES
-ProviderName BC
-ProviderClass org.bouncycastle.jce.provider.BouncyCastleProvider -KeySize 128
-Username <OpenPagesAdministrator> -Password <OpenPagesAdministratorPassword>
```

3. Restart all OpenPages services.
4. If you are using OpenPages to authenticate users, notify all users that their passwords have been reset to 0p3nP4g3s and that they must change their passwords the next time they log into the system.

Note: If you are using Single Sign-On (SSO), LDAP, or another external system to authenticate users, passwords are not reset.

Updating security rules

If you use security rules, you might need to update the rules after you migrate to address an issue with security rules that were created before version 7.4.




About this task

Do this procedure if you use reporting periods or if you plan to use reporting periods.

Update any security rules that have both of the following properties:

- The rule uses parent-child paths, for example `FOR(Primary Parent)`, `FOR(Immediate)`, and so on
- The rule uses `FOR()` clauses that have an AND or OR clause before or after the `FOR()` clause

Procedure

1. Log on to IBM OpenPages with Watson as an administrator.
2. Click , and then click **Enable System Admin Mode**.
3. Click  > **Users and Security** > **Security Rules**.
4. For each security rule that needs to be updated, click **Edit** and then click **Save**.
5. Click  > **Disable System Admin Mode**.

Results

New SQL is generated for the rules.

Custom settings in configuration files

If you manually edited any configuration files in the previous version, you must merge your changes.

Search server post migration tasks

If you backed up and then restored the search server, complete the following post migration tasks.

- If the location of the openpages-storage directory has changed, update the search server properties file. For more information, see [“Updating the search server properties file with the location of the OpenPages storage directory” on page 184](#).
- If you migrated from 7.3.x, enable global search. For more information, see [“Enabling global search” on page 212](#).

You can also do the following optional tasks:

- Set up SSL for the global search service. For more information, see [“Setting up a secure connection for the global search service” on page 181](#).
- Tune the search server memory settings. For more information, see [“Allocating memory for the global search component” on page 186](#).

For more information about the search server, see the *IBM OpenPages with Watson Administrator's Guide*.

Enabling global search

If you migrated from 7.3.x and you used global search in 7.3.x, enable the global search feature.

Procedure

1. Start the search services, if they are not already started.
For more information, see [“Start or stop the global search services” on page 312](#).
2. Log in to OpenPages as a user with administrative privileges.
3. Go to the Standard UI.
4. Click **Administration** > **Global Search** and click **Enable**.

Results

The **Global Search** box is available in the Standard UI.

If global search does not start, see [“Known problems and solutions for global search” on page 434](#).

For more information about global search, see the *IBM OpenPages with Watson Administrator's Guide*.

Enable LDAP after migrating

If you used LDAP in your previous version of IBM OpenPages with Watson and you did not migrate the `aurora_auth.config`, you must re-enable LDAP.

Open the LDAP configuration file, `aurora_auth.config`, in a text editor.

Check that the **provider.url** points to your LDAP server. Also verify the other settings.

If the settings are not correct, see [“Enabling LDAP for the OpenPages application” on page 178](#).

Enabling a JDBC connection for the OpenPages database (Db2)

If you want to use Dynamic Query Mode (DQM) for the OpenPages reporting framework, you need to configure a JDBC connection to the OpenPages database.

Enable a JDBC connection so that your reports can run on a reporting framework that is published to Cognos in DQM mode. For more information, see the *IBM OpenPages with Watson Administrator's Guide*.

Procedure

1. Log on to IBM Cognos Analytics as a user with administrative privileges..
 - In the Task Focused UI, click **Analytics**.
 - Or, go to the following URL: `http://<hostname>/ibmcognos/bi`
Where `<hostname>` is the name of the Cognos server.
2. Click **Manage > Administration Console** to launch the **IBM Cognos Administration** page.
3. Click the **Configuration** tab.
4. Click **OpenPages DataSource** under **Data Source Connections**.
5. Click **Actions > Set Properties - OpenPages DataSource**.
6. Update the JDBC connection information.
 - a) Click the **Connection** tab.
 - b) Click the pencil icon next to the **Connection String** box to edit the field.
 - c) Click the **JDBC** tab.
 - d) Check **Enable JDBC connection**.
 - e) Enter the OpenPages database information in the **Server Name**, **Port Number**, and **Database Name** fields.

Enabling a JDBC connection for the OpenPages database (Oracle)

If you want to use Dynamic Query Mode (DQM) for the OpenPages reporting framework, you need to configure a JDBC connection to the OpenPages database.

Enable a JDBC connection so that your reports can run on a reporting framework that is published to Cognos in DQM mode. For more information, see the *IBM OpenPages with Watson Administrator's Guide*.

Procedure




1. Log on to IBM Cognos Analytics as a user with administrative privileges..
 - In the Task Focused UI, click **Analytics**.
 - Or, go to the following URL: `http://<hostname>/ibmcognos/bi`
Where `<hostname>` is the name of the Cognos server.
2. Click **Manage > Administration Console** to launch the **IBM Cognos Administration** page.
3. Click the **Configuration** tab.
4. Click **OpenPages DataSource** under **Data Source Connections**.

5. Click **Actions > More > Set Properties**.
6. Update the JDBC connection information.
 - a) Click the **Connection** tab.
 - b) Click the pencil icon next to the **Connection String** box to edit the field.
 - c) Click the **JDBC** tab.
 - d) Check **Enable JDBC connection**.
 - e) Under **Connection type**, click **Service ID**.
 - f) Enter the OpenPages database information in the **Server Name**, **Port Number**, and **Oracle Service ID** fields.
 - g) Click **OK**.
7. Click **OK**.

Updating the reporting schema

Update the reporting schema.

Procedure

1. Log in to OpenPages as a user with administrative privileges.
2. Enable System Admin Mode (SAM). Click , and then click **Enable System Admin Mode**.
3. Click  > **System Configuration > Reporting Schema**.
4. Click **Update**.
5. Click **Refresh** until the process is 100% complete.
6. Disable SAM. Click , and then click **Disable System Admin Mode**.

Regenerating the reporting framework

After you migrate IBM OpenPages with Watson you might need to regenerate the reporting framework.

About this task

If you plan to install or upgrade other components, such as IBM OpenPages Loss Event Entry, perform this task after completing all other installation or upgrade tasks.

When you generate the Reporting Framework V6, you can choose to update all or particular components of the reporting framework. For more information, see "Choosing update options in the reporting framework" in the *IBM OpenPages with Watson Administrator's Guide*.

Procedure



1. If you upgraded Cognos from 10.2.x or if the location of COGNOS_HOME is different in your source and target environments, update the `framework.properties` file.
 - a) Open the `<CC_HOME>/framework/conf/framework.properties` file in a text editor.
 - b) Update the **cognos.dir** property to point to the COGNOS_HOME directory.
For example:

```
cognos.dir=/usr/IBM/cognos/analytics
```

- c) Update the **cognos.scriptplayer** property.
For example:

```
cognos.scriptplayer=/usr/IBM/cognos/analytics/bin/BmtScriptPlayer.sh
```

2. Log on to OpenPages as a user with administrative privileges.

3. If **System Admin Mode** is enabled, disable it. Click , and then click **Disable System Admin Mode**.
4. Click  > **Cognos Analytics** > **Reporting Framework Generation**.
5. On the **Reporting Framework Operations** page, click **Update**.
6. In the **Reporting Framework Generation** window, complete the following steps:
 - a) Under **Framework Generation**, select the **Framework Model**, **Labels**, **All Models** or **Selected Models** options and any additional options for generation in the Reporting Framework V6 relational data model.
 - b) Click **Submit**.

You are returned to the Reporting Framework Operations page with the new task listed in the Reporting Framework Operations table.
7. To view the progress of the update, click **Refresh**.

Deleting Fujitsu workflow reports

If you migrated from 7.3.x, delete the workflow reports for Fujitsu.

About this task

The Fujitsu workflow reports are no longer needed and can be removed from the system.

Procedure

1. In the OpenPages Standard UI, click **Reporting** > **Cognos Analytics**.
2. Click **Team content**.
3. On the Team content page, navigate through the links as follows:
OpenPages_Platform_V6 > **Workflow Reports**
4. Hover over the **Active Tasks** report and click the ellipse button.
5. Click **Delete**.
6. Hover over the **Jobs and Tasks** report and click the ellipse button.
7. Click **Delete**.

The Fujitsu workflow reports are deleted.

Migration verification tests

After you migrate to IBM OpenPages with Watson 8.2, verify that the migration is successful and the product works as expected.

Use the following checklist to verify the migration.

Table 59. Post-migration verification checklist	
Task	Guidance
Review all installation logs for errors.	For more information, see “Log files” on page 427.

Table 59. Post-migration verification checklist (continued)

Task	Guidance
Verify that a backup of the system exists	<p>If it does not exist, create a backup of your system by running the OPBackup command from the <code><OP_HOME>/aurora/bin</code> directory.</p> <p>Verify that a compressed file was created with the correct time stamp. The file is in the OPBackup directory.</p> <p>The location of the OPBackup directory is specified by the OP Backup Restore Directory field on the Application Server card.</p> <p>For information about using the backup utility, see the <i>IBM OpenPages with Watson Administrator's Guide</i>.</p>
Confirm that the reporting schema and framework generated successfully.	For more information, see “Regenerating the reporting framework” on page 214 .
Confirm that base reports are functioning as expected.	Log on to the OpenPages application and run the All Documentation Cognos report.
If single sign-on (SSO) is enabled, verify that user accounts can access the environment.	Log on to the OpenPages application with an SSO user account.
Confirm that you can upload and download sample attachments.	Log on to the OpenPages application and upload and download a file attachment.
Verify that links in reports reference the correct server address and use the correct web URL parameters.	Run a report that uses OpenPages links. Select a link and confirm that the target object is rendered successfully in the OpenPages interface.
For clustered environments, verify that all servers can upload and download attachments.	Upload and download files from both the admin and non-admin application servers.
Validate that you can access IBM Cognos Analytics.	Type the web URL <code>http://<server_name>/ibmcognos</code> from a client system. Confirm that you can log on to the portal.

Testing Cognos Analytics after the migration

Verify that Cognos Analytics works with the IBM OpenPages with Watson environment.

Procedure

- Log on to OpenPages with Watson and verify that you can connect to the Cognos Analytics portal.
 - In a web browser, log on to the OpenPages with Watson application.
 - Go to the Standard UI.
 - To test the connection from OpenPages to the Cognos Analytics portal, click **Reporting > Cognos Analytics**.
 - Close the session.


2. From the OpenPages application, click **Reporting > All Reports**, and run some standard and custom user reports.

Configure new features


Some new features need to be configured.

Application permissions for new features in the Task Focused UI

Review the following application permissions. Add them to your role templates to give users access to the features and functionality.


Table 60. Application permissions for Task Focused UI features	
Feature	Application permissions
GRC Calculations	To give users the ability to create and manage calculations, add the SOX > Administration > Calculation permission to role templates.
Scheduler	To give users the ability to create and manage scheduled jobs, add the SOX > Administration > Scheduler permission to role templates.
Watson Assistant	To give administrators the ability to configure assistants, add the SOX > Administration > Watson Assistant permission to role templates. To give users access to the user interface that enables them to interact with assistants in OpenPages, add the SOX > User Interfaces > Watson Assistant UI permission to role templates.
LDAP server configuration for user provisioning	To give administrators the ability to configure the LDAP server for user provisioning via the Task Focused UI, add the SOX > Administration > LDAP Server permission to role templates.
Activity tab in views	To give users access to the Activity tab in views, add the Audit Trail permission to role templates.
Watson Natural Language Classifiers (also called cognitive services)	To give administrators the ability to configure cognitive services in the Task Focused UI, add the SOX > Administration > Cognitive permission to role templates.
Dashboard administration	To give administrators the ability to create and manage dashboards, add the SOX > Administration > Dashboards permission to role templates.
View Designer, Display debug info menu item	To give users access to the View Designer, add the SOX > Administration > Task Focused UI permission to role templates. This permission also controls whether the  > Other > Display debug info menu item is displayed.
Encryption keystore	To give administrators the ability to configure and manage the encryption keystore in the Task Focused UI, add the SOX > Administration > Encryption Keystore permission to role templates.

GRC Calculations

Version 8.2 includes sample calculations. When you upgrade, the installation process loads the sample calculations but does not enable them. Depending on your environment, your schema might not contain all of the object types, object associations, and fields that are used in the sample calculations. To view the sample calculations, click  > **Solution Configuration > Calculations**.

For more information, see "Setting up calculations" in the *IBM OpenPages with Watson Administrator's Guide*.

GRC Workflow

Version 8.2 includes sample workflows. When you upgrade or migrate from a release prior to 8.0.0.2, the installation process loads the sample workflows but does not enable them. Depending on your environment, your schema might not contain all of the object types, object associations, and fields that are used in the sample workflows. To view the sample workflows, click  > **Solution Configuration** > **Workflows**.

If you are upgrading or migrating from 8.0.0.2 or later, the installation process does not load the sample workflows. You can load them manually. For more information, see ["Loading the sample workflows" on page 277](#).

Rolling back an OpenPages migration

You can roll back OpenPages to the version from which it was migrated.

Before you begin

Locate the full server directory backups for each server that were when you prepared for the migration to 8.2. For information, see ["Backing up your source environment" on page 198](#).

About this task

The following steps provide a general overview of how to roll back a 8.2.0.0 migration.

Procedure

1. Ensure that the IP/DNS setup of the previous deployment is fully intact and uses the exact configuration that was in place before the OpenPages migration.
2. For the database server:

If the database server from the previous OpenPages version was upgraded:

- a. If the database software was upgraded, reinstate the previous database software version.
- b. Restore the database using the database backup created before the database upgrade.

If a new database server was introduced for the migration:

- Reinstall the former database server into the deployment. You do not need to restore the OpenPages database from a backup.

3. For all other servers in the previous deployment:

- a) If there are any remnants of the OpenPages 8.2 deployment remaining on any of the servers, rename the top level OpenPages directory to OpenPages-8.2.0.0 on each applicable server.
- b) If during the preparation for the migration you renamed the OpenPages root directory or if you created full backup directories or ZIP or tar files of each server, restore them if needed. For more information about the steps required to prepare for a rollback, see ["Backing up your source environment" on page 198](#).

After all servers are restored and all third-party products are at the versions required by the previous OpenPages deployment, the previous OpenPages deployment works without further actions.

Chapter 8. Migration task reference for Db2 databases

If you are using IBM Db2, refer to the following topics when you migrate IBM OpenPages with Watson to 8.2.

The tasks that you need to do depend on the scenario that you are following. Use the following topics to guide you through the migration process:

- [“Migration process overview: Using the database server from your source environment” on page 190](#)
- [“Migration process overview: Using new hardware for the database server” on page 192](#)

Back up the database (Db2)

Do the following procedures to back up the IBM Db2 database in your previous deployment of IBM OpenPages with Watson.

Note: In some cases, you cannot use Db2 backup and restore to move a database. For example, if the schema names in the source and target are different or if the source and target servers are using different operating systems, you cannot use Db2 backup and restore. Db2 has several tools and techniques that you can use instead. For more information about how to use these tools with OpenPages, see [Moving Db2 database objects to a new database when a backup and restore cannot be performed](#).

- If Db2 Text Search is enabled in your source environment, install and enable Db2 Text Search in your target environment.
- If Db2 Text Search is enabled in your source environment, drop the text search indexes and disable Db2 Text Search.
- Back up the OpenPages database.
- If you created a separate database for Cognos, back up the Cognos database.

If you are migrating from 7.3.x, you need to back up and then restore both the OpenPages schema and the Fujitsu workflow schema so that the database upgrade scripts can remove any references to the Fujitsu workflow schema that are contained within the OpenPages schema. Once the OpenPages schema has these references removed, the Fujitsu workflow schema will then be removed to complete this step.

If you are using 7.4.x or later, the Fujitsu workflow schema has already been removed.

Dropping the Db2 Text Search index and disabling Db2 Text Search

If Db2 Text Search is enabled in your source environment, drop the text search indexes, disable the text search service, remove the Db2 administrative task to update the indexes, and disable Db2 Text Search. Do this procedure before you back up the OpenPages database.

Procedure

1. Log on to a system as the OpenPages installation user, for example `opuser`.

You can use any system with access to CLPPlus that can connect to the database server.

2. Drop the Db2 Text Search index.

- a) Go to the `<OP_HOME>/aurora/bin/full-text-index` directory.
- b) Open a command or shell window and run the following command:

```
clpplus -nw @sql-wrapper CustomIndexing_Step5_IndexDrop.sql  
<LOG_FILE_NAME> <DB2_SERVER_NAME> <DB2_PORT_NUMBER> <DATABASE_NAME>  
<OP_DB_USER> <OP_DB_PASSWORD> <FORCE_DROP_INDEX>
```

If the <OP_DB_PASSWORD> contains special characters, surround the password in quotation marks:

- Windows: "password"
- Linux: 'password'

For example

- Windows:

```
clpplus -nw @sql-wrapper CustomIndexing_Step5_IndexDrop.sql  
CustomIndexing_Step5_IndexDrop.log localhost 50000 OPX OPENPAGE "password" Y
```

- Linux:

```
clpplus -nw @sql-wrapper CustomIndexing_Step5_IndexDrop.sql  
CustomIndexing_Step5_IndexDrop.log localhost 50000 OPX OPENPAGE 'password' Y
```

For more information, see "Drop a long string index" in the *IBM OpenPages with Watson Administrator's Guide*.

3. Run the following command to determine if Db2 Text Search is enabled.

```
select * from all_tables where table_schema = 'SYSIBMTS';
```

If the command returns any data, Db2 Text Search is enabled. Continue with the next step to disable Db2 Text Search.

4. Log on to the OpenPages database as the db2inst1 user.

```
db2 connect to opx user opuser using password
```

5. Run the following command to disable Db2 Text Search.

For more information, see [SYSTS_DISABLE procedure - Disable current database for text search](#).

```
db2 "call sysproc.systs_disable('','en_US',?)"
```

Alternatively, use these commands.

```
db2 GRANT SYSTS_ADM TO db2inst1  
db2 grant SYSTS_MGR to db2inst1  
db2 connect reset  
db2ts start for text  
export DB2DBDFT=OPX  
db2ts DISABLE DATABASE FOR TEXT
```

6. Remove the Db2 administrative task to update the indexes

For more information, see the following topic in the Db2 documentation: [Removing a task from the administrative task scheduler](#).

Backing up the OpenPages database during a migration to 8.2 (Db2)

Create a backup of the OpenPages with Watson database.

Before you begin

If Db2 Text Search is enabled in your source environment, drop the text search indexes and disable Db2 Text Search before you back up the database.

About this task

Use the utilities that are provided with IBM Db2 to back up the database.

Note: You can back up the database by using other methods. For example, you can use a combination of full and incremental backups. If you want to use an alternative method, it is critical that you have

the necessary skills available within your organization to complete all aspects of the backup and restore activity.

For information about developing a database backup and restore strategy, see [Backup overview](#) in the Db2 documentation.

For more information about the commands that are used in this procedure, see the [IBM Db2 documentation](#).

Procedure

1. Make sure that no OpenPages with Watson processes are running, such as object reset jobs.
2. Shut down all OpenPages components: application servers (admin and non-admin), reporting servers (active and standby), and the search server.

For more information, see [Chapter 12, “Starting and stopping servers,”](#) on page 309.

3. Open a command or shell window and connect to the OpenPages database as the database instance owner.

For Windows users only, you must use the **db2cmd** command in the **Command Prompt** window to initialize the Db2 command line processor (CLP).

4. Go to the `sqllib` directory.
5. Force any applications from the database.

Run the following command:

```
db2 force application all
```

6. Deactivate the database.

Run the following command:

```
db2 deactivate database <db_name>
```

7. Create a directory in which to store the backup.
8. Do an offline backup by using the `db2 backup` command.

```
db2 backup database <db_name> to <backup_directory>
```

Example:

```
db2 backup database opx to /home/db2inst1/backup
```

9. Copy the backup file to the instance owner account on the target OpenPages database server.

What to do next

If you created a separate database for Cognos, back up the Cognos database.

Backing up the Cognos database during a migration to 8.2 (Db2)

Create a backup of the Cognos database. Do this procedure if you use a separate database for Cognos.

About this task

Use the utilities that are provided with IBM Db2 to back up the database.

Note: You can back up the database by using other methods. For example, you can use a combination of full and incremental backups. If you want to use an alternative method, it is critical that you have the necessary skills available within your organization to complete all aspects of the backup and restore activity.

For information about developing a database backup and restore strategy, see [Backup overview](#) in the Db2 documentation.

For more information about the commands that are used in this procedure, see the [IBM Db2 documentation](#).

Procedure

1. Shut down all OpenPages components: application servers (admin and non-admin), reporting servers (active and standby), and the search server.

For more information, see [Chapter 12, “Starting and stopping servers,” on page 309](#).

2. Ensure that all Cognos components are shut down.
3. Open a command or shell window and connect to the Cognos database as the database instance owner.

For Windows users only, you must use the **db2cmd** command in the **Command Prompt** window to initialize the Db2 command line processor (CLP).

4. Go to the `sql1ib` directory.
5. Force any applications from the database.

Run the following command:

```
db2 force application all
```

6. Deactivate the database.

Run the following command:

```
db2 deactivate database <db_name>
```

7. Create a directory in which to store the backup.
8. Do an offline backup by using the `db2 backup` command.

```
db2 backup database <db_name> to <backup_directory>
```

Example:

```
db2 backup database cognosdb to /home/db2inst2/backup
```

9. Copy the backup file to the instance owner account on the target Cognos database server.

Restore the OpenPages database in your 8.2 environment (Db2)

Restore the OpenPages database from your previous IBM OpenPages with Watson environment into your 8.2 environment.

Note: In some cases, you cannot use Db2 backup and restore to move a database. For example, if the schema names in the source and target are different or if the source and target servers are using different operating systems, you cannot use Db2 backup and restore. Db2 has several tools and techniques that you can use instead. For more information about how to use these tools with OpenPages, see [Moving Db2 database objects to a new database when a backup and restore cannot be performed](#).

Do these tasks to restore the database:

- Restore the OpenPages database. See [“Restoring the OpenPages database \(Db2\)” on page 223](#).
- If you use Db2 Text Search, reconfigure and enable Db2 Text Search on the target database server. See [“Restore Db2 Text Search ” on page 224](#).
- If your target environment uses a later 11.x fix pack version of Db2 than your source environment, update the databases on the target database server. See [“Update the databases for a Db2 11.1.x fix pack” on page 224](#).

Restoring the OpenPages database (Db2)

Restore the OpenPages database in your target environment.

Before you begin

Determine whether you need to do a redirected database restore. You need to do a redirected restore if the DBPATH/DB_STORAGE_PATH directory in the target environment is different than in the source environment. You can run a query to check the path.

1. In the source environment, log in as the OpenPages instance owner.
2. Run the following query:

```
db2 "select DBPARTITIONNUM, substr(TYPE,1,15) as TYPE,  
substr(PATH,1,70) as PATH from sysibmadm.DBPATHS"
```

3. Log on to the target environment as the OpenPages instance owner and run the query again.

If the directories are the same, restore the database by using the steps in this topic.

If the directories are not the same, do a redirected database restore instead. For more information, see the Db2 documentation: [Performing a redirected restore operation](#).

Procedure

1. Stop all OpenPages and Cognos services in the target environment.
2. Log on to a server that has access to the target database server and has Command Line Processor Plus (CLPPlus).
3. If you are using Microsoft Windows, start the Db2 command line processor.

From the command prompt, type `db2cmd`. Or, click **Start > IBM Db2 > IBM Db2 Db2COPY1 > Command Line Tools > Db2 Command Window - Administrator**.

4. Go to the directory where you copied the database backup file for the OpenPages database.
5. Ensure that there are no connections to the database.

```
db2 list applications  
db2 force applications all
```

6. Deactivate the database.

```
db2 deactivate database <db_name>
```

7. Run the Db2 restore command to restore the OpenPages database.

```
db2 restore database <source_db_name> from <backup_directory> taken at <timestamp> into  
<target_db_name>
```

For example:

```
db2 restore database opx from /home/db2inst1/backup taken at 20171024165648 into opx
```

A warning about overwriting data is displayed.

8. Type `y` to overwrite the data.

If the version of Db2 in your target environment is a later version than in the source environment, a complete database upgrade takes place automatically during the restore process. At the end of the restore process, a message is displayed:

```
SQL2555I The database was restored and then successfully upgraded  
to the current DB2 release where you issued the RESTORE DATABASE command
```

Note: The automatic upgrade does not update the database when the source and target are at version 11.1 but at different fix pack levels. If your source is 11.1.0 and your target is 11.1.4 or a later fix pack, see [“Update the databases for a Db2 11.1.x fix pack”](#) on page 224.

9. Revalidate objects and rebind packages.

Run these commands as a user with DBADM privileges.

- a) Go to the /OP_<version>_Main/OP_<version>_Configuration/Database/DB2/INSTALL_SCRIPTS directory.
- b) Revalidate the database objects.

```
clpplus -nw <openpages_db_username>/\ '<openpages_db_password>\'  
@<hostname>:<port_number>/<database_name>  
@sql-wrapper revalidate.sql revalidate.log <openpages_db_username>
```

For example:

```
clpplus -nw openpage/\ 'password\ '@localhost:50000/opx @sql-wrapper revalidate.sql  
revalidate.log openpage
```

- c) Rebind the packages.

Note: When you run Db2 utilities, such as db2rbind, do not use quotation marks around passwords, even if they contain special characters.

```
db2rbind <database_name> -l oprbind.log all -u <dba_username> -p <dba_password> -r any
```

For example:

```
db2rbind opx -l opbind.log all -u db2inst1 -p passWORD -r any
```

What to do next

If you use a separate database for the Cognos content store, restore the Cognos content store in your target environment.

Restore Db2 Text Search

If you use Db2 Text Search, reconfigure and enable Db2 Text Search on the target database server.

For more information, see "Utilities for filtering on long string field content in a Db2 database" in the *IBM OpenPages with Watson Administrator's Guide*

For more information, see "Utilities for filtering on long string field content in a Db2 database" in the *IBM OpenPages with Watson Administrator's Guide*.

Update the databases for a Db2 11.1.x fix pack

If the version of IBM Db2 in your source environment is at a different fix pack level than the version of IBM Db2 in your target environment, you need to update the databases.

For example, if your source environment uses IBM Db2 version 11.1.1 and your target environment uses IBM Db2 11.1.4.4 or a later fix pack, you need to update the databases in the target environment to update them to version 11.1.4.4.

Note: This task applies only when the target environment is using a different fix pack level than the source. If your source environment is using version 11.1.x and your target is using version 11.5.0 or a later fix pack, you do not need to do this task.

Do this task after you have restored the databases into your target environment.

For information about how to update the databases, see the following topic in the IBM Db2 documentation: [db2updv111 - Update database to Version 11.1 fix pack command](#).

For example:

```
db2updv111 -d opx -a  
db2updv111 completed successfully for database 'opx'
```

If you are using a separate database instance for the Cognos content store, update the Cognos database also. For example:

```
db2updv111 -d cognosdb
db2updv111 completed successfully for database 'cognosdb'
```

Restoring the Cognos content store (Db2)

If you use a separate database for the Cognos content store, restore the Cognos database in your target environment.

Before you begin

Determine whether you need to do a redirected database restore. You need to do a redirected restore if the DBPATH/DB_STORAGE_PATH directory in the target environment is different than in the source environment. You can run a query to check the path.

1. In the source environment, log in as the Cognos instance owner.
2. Run the following query:

```
db2 "select DBPARTITIONNUM, substr(TYPE,1,15) as TYPE,
      substr(PATH,1,70) as PATH from sysibmadm.DBPATHS"
```

3. Log on to the target environment as the Cognos instance owner and run the query again.

If the directories are the same, restore the database by using the steps in this topic.

If the directories are not the same, do a redirected database restore instead. For more information, see the Db2 documentation: [Performing a redirected restore operation](#).

Procedure

1. Stop all Cognos services in the target environment.
2. Log on to a server that has access to the target Cognos database server and has Command Line Processor Plus (CLPPlus).
3. If you are using Microsoft Windows, start the Db2 command line processor.
From the command prompt, type db2cmd. Or, click **Start > IBM Db2 > IBM Db2 Db2COPY1 > Command Line Tools > Db2 Command Window - Administrator**.
4. Go to the directory where you copied the database backup file for the Cognos database.
5. Ensure that there are no connections to the database.

```
db2 list applications
db2 force applications all
```

6. Deactivate the database.

```
db2 deactivate database <db_name>
```

7. Run the Db2 restore command to restore the Cognos database.

```
db2 restore database <source_db_name> from <backup_directory>
      taken at <timestamp> into <target db name>
```

For example:

```
db2 restore database cognosdb from /home/db2inst1/backup taken at 20171024174956
into cognosdb
```

A warning about overwriting data is displayed.

8. Type y to overwrite the data.

If the version of Db2 in your target environment is a later version than in the source environment, a complete database upgrade takes place automatically during the restore process. At the end of the restore process, a message is displayed:

```
SQL2555I The database was restored and then successfully upgraded
to the current DB2 release where you issued the RESTORE DATABASE command
```

Note: The automatic upgrade does not update the database when the source and target are at version 11.1 but at different fix pack levels. If your source is 11.1.0 and your target is 11.1.1 or a later fix pack, see [“Update the databases for a Db2 11.1.x fix pack”](#) on page 224.

9. Revalidate objects and rebind packages in the Cognos database.

Do these steps as the instance owner for the Cognos database.

Note: When you run Db2 utilities, such as `db2 connect` or `db2rbind`, do not use quotation marks around passwords, even if they contain special characters.

- a) Revalidate the database objects.

For example:

```
db2 connect to cognosdb user db2admin using password123
db2 "call sysproc.admin_revalidate_db_objects()"
```

- b) Rebind packages in the Cognos database.

For example:

```
db2rbind cognosdb -l cogbind.log -u db2inst2 -p password123
```

Upgrade the databases (Db2)

Run scripts to upgrade the OpenPages database objects.

You must run all of the upgrade scripts in sequence to upgrade the database schema.

Two of the scripts require DBA privileges: a pre-upgrade script and a post-upgrade script. If you have DBA privileges, you can run all of the scripts. If you do not have DBA privileges, contact your database administrator.

A schema user can run the scripts that do not require DBA privileges.

Note for 7.4.x and 8.0.x customers: The database upgrade scripts modify and drop some database structures to free up space in the database. To complete the process, the `PROPERTYVALS` table needs to be reorganized. The database upgrade scripts perform the table reorganization automatically. Due to this additional operation, the database upgrade takes longer to complete than in the 7.4/8.0 release. The time to complete the reorganization depends on the size of your `PROPERTYVALS` table and the hardware capability of your database server.

Pre-upgrade step – DBA tasks

During this step, your database administrator runs a script to prepare the database for the upgrade.

You need both `DBADM` and `SECADM` privileges to run this script.

Validate the pre-upgrade step

During this step, you run a script to verify that the pre-upgrade DBA script completed successfully and that the database schema is ready for the upgrade.

Upgrade step

During this step, you run a script to upgrade the database. The script determines the current version of the database schema objects, and then runs the upgrade scripts that are needed to upgrade the database.

Post upgrade step – DBA tasks

During this step, your database administrator runs a script to complete the database upgrade and to set database tuning parameters.

You need both DBADM and SECADM privileges to run this script.

Validate the post-upgrade step

During this step, you run a script to validate the post-upgrade DBA step.

Extending database row sizes for the databases (Db2)

After you restore your IBM OpenPages with Watson database to the supported version of IBM Db2 you must manually enable the **EXTENDED_ROW_SZ** database configuration parameter.

Procedure

1. If you are using Microsoft Windows, start the Db2 command line processor.

From the command prompt, type db2cmd. Or, click **Start > IBM Db2 > IBM Db2 Db2COPY1 > Command Line Tools > Db2 Command Window - Administrator**.

2. Connect to the OpenPages database.

For example, type

```
db2 connect to OPX user <userid>
```

3. Enter the following commands:

```
db2 update db cfg using EXTENDED_ROW_SZ ENABLE
db2 update db cfg for OPX using APPLHEAPSZ 25600 APPL_MEMORY 320000
```

Preparing for the database upgrade (Db2)

Prepare for the upgrade of the database objects.

Procedure

1. Shut down all OpenPages components: application servers (admin and non-admin), reporting servers (active and standby), and the search server (if you use the global search feature).

For more information, see [Chapter 12, “Starting and stopping servers,” on page 309](#).

2. Ensure that the IBM Db2 database server is running.
3. Log on to the Db2 database server computer as a user with administrative privileges.
4. Go to the /OP_<version>_Main/OP_<version>_Configuration/Database/DB2/UPGRADE_SCRIPTS directory.
5. Verify that you have write permission on the sql-wrapper.sql file.
6. Edit the sql-wrapper.sql file.

Restriction: Change only the parameters that are described in this step.

Table 61. Parameters in the sql-wrapper.sql file for Db2 databases	
Property	Description
opx_db2_instance_owner	The database instance owner for OpenPages. The user you specify must have both DBADM and SECADM privileges. If your database administrator is going to run the scripts that require DBA privileges, you can leave this value empty when you run the non-DBA scripts.
opx_db2_server_name	The database server name
opx_db2_port_number	The database port number, for example 50000

Table 61. Parameters in the sql-wrapper.sql file for Db2 databases (continued)	
Property	Description
opx_db2_db_name	The name of the OpenPages database.
opx_db_owner	The schema owner of the OpenPages database.
opx_dflt_stor_srv_root	<p>The path to the OpenPages storage directory.</p> <p>Example:</p> <pre>define opx_dflt_stor_srv_root='/home/opuser/OP/OpenPages/openpages-storage'</pre>
opx_workflow_user	<p>The Fujitsu Interstage BPM workflow database user name.</p> <p>If you are migrating from 7.3.x, you need to provide the workflow user name to complete the upgrade. The database upgrade scripts remove any references to the workflow schema that are contained within the OpenPages schema, and then the scripts remove the workflow schema.</p> <p>If you are migrating from 7.4.x or later, the Fujitsu workflow schema was removed when you upgraded to 7.4.x or later.</p>
opx_override_version_check	<p>Use the default value, N, unless you are re-running the database upgrade scripts after a failure.</p> <p>If the database upgrade failed in the middle of the schema upgrade process, set this parameter to Y. When you re-run the upgrade script, the upgrade process resumes from the last successful schema upgrade step.</p> <p>For example, suppose you are migrating from 7.3. When you run the upgrade script, it successfully upgrades the schema from 7.3 to 8.0, but fails during the upgrade from 8.0 to 8.1. Set this flag to Y and then re-run the script. The upgrade resumes at the 8.0 to 8.1 database upgrade step.</p>
sqllib_dir	<p>The path to the Db2 client installation directory on the admin application server (App Server1)</p> <p>Example:</p> <ul style="list-style-type: none"> • Windows: define sqllib_dir='C:\IBM\SQLLIB' • Linux: define sqllib_dir='/home/db2inst1/sqllib'

7. If you want to run a custom script during the database upgrade process, see [“Running a custom script during the database upgrade \(Db2\)”](#) on page 229.
8. If your database administrator is going to run the scripts that require DBA privileges, prepare the files for your database administrator.
 - a) Go to the /OP_<version>_Main/OP_<version>_Configuration/Database/DB2/UPGRADE_SCRIPTS directory.
 - b) Open the op-dba-upgrade-file-list.txt file.
 - c) Send your DBA the sql-wrapper.sql file that you updated along with the files listed in the op-dba-upgrade-file-list.txt file.
 - d) Send your DBA the instructions to run the DBA scripts.
 - [“Running the pre-upgrade DBA script \(Db2\)”](#) on page 229
 - [“Running the post-upgrade DBA script \(Db2\)”](#) on page 232

Running a custom script during the database upgrade (Db2)

If you want to run a custom script during the database upgrade process, edit the `sql-wrapper.sql` file to specify the script to run.

About this task

You can use the `custom_data_upgrade_script` parameter to configure a custom script.

The script that you specify is run during the database upgrade step. The custom script is called by the `op-database-product-upgrade.sh/bat` script after the other upgrade steps, such as DDL changes, PL/SQL code changes, and database level data changes are complete.

Procedure

1. Open the `sql-wrapper.sql` file.
2. Verify that the `sqllib_dir` path is correct. If you are running the custom script from a computer other than the database server, update the path.
3. Edit the following parameters:

```
define custom_data_upgrade_script=no-op.sql
```

Replace `no-op.sql` with the script that you want to run.

4. Place your custom script in the same directory as the `sql-wrapper.sql` file.

Running the pre-upgrade DBA script (Db2)

Ask your database administrator to run the pre-upgrade script. Or, if you have DBADM and SECADM privileges, you can run the script.

Before you begin

- The IBM Db2 database server is running. All other OpenPages servers are stopped.
- The `JAVA_HOME` system variable is defined and points to the IBM SDK, Java Technology Edition that is installed with Db2. For example:

```
export JAVA_HOME=/db2/V11.5/java/jdk64
export PATH=$JAVA_HOME/bin:$PATH
```

If you are running the script from another host, ensure that `JAVA_HOME` is pointing to the IBM SDK, Java Technology Edition that is installed on the computer.

- `apache-ant-1.8.1` is deployed to `/OP_<version>_Main/OP_<version>_Configuration/Database/DB2/UPGRADE_SCRIPTS`
- The `DB2_HOME` system variable is defined.

About this task

Run the following script: `op-database-dba-upgrade.sh|.bat`. The script uses the properties that are defined in the `sql-wrapper.sql` file.

Procedure

1. Log on to the Db2 database server computer as a database administrator (DBA).
2. Locate the scripts.

If you are a database administrator, get the scripts from your OpenPages team.

Or, you can get the scripts from the `/OP_<version>_Main/OP_<version>_Configuration/Database/DB2/UPGRADE_SCRIPTS` directory.

3. Verify that you have execute permission on the scripts in the UPGRADE_SCRIPTS directory and its sub directories.
4. Open the sql-wrapper.sql file. Verify that the values are suitable for your environment.
 - a) For the opx_db2_instance_owner parameter, specify a user that has both DBADM and SECADM privileges.

You can run the following script to get a list of users that have the necessary privileges:

```
select grantee from syscat.dbauth where dbadmauth = 'Y' and securityadmauth = 'Y';
```

- b) If you customized the table space names, update the define opx_dflt_* parameters with the custom table space names.
5. Run the following command:
 - On Linux:

```
./op-database-dba-upgrade.sh pre '<dba_password>'
```

- On Windows:

```
op-database-dba-upgrade.bat pre "<dba_password>"
```

Note: Quotation marks are required around a password only if the password contains special characters. See [“Special characters in passwords”](#) on page 12.

6. Verify that the return code is 0, indicating success.

You can also check the log file, op-database-dba-pre-upgrade.log.

What to do next

Validate the pre-upgrade DBA script.

Validating the pre-upgrade DBA step (Db2)

Run the script to validate the pre-upgrade DBA steps.

Before you begin

- The IBM Db2 database server is running. All other OpenPages servers are stopped.
- The JAVA_HOME system variable is defined and points to the IBM SDK, Java Technology Edition that is installed with Db2. For example:

```
export JAVA_HOME=/db2/V11.5/java/jdk64
export PATH=$JAVA_HOME/bin:$PATH
```

If you are running the script from another host, ensure that JAVA_HOME is pointing to the IBM SDK, Java Technology Edition that is installed on the computer.

- apache-ant-1.8.1 is deployed to /OP_<version>_Main/OP_<version>_Configuration/Database/DB2/UPGRADE_SCRIPTS
- The DB2_HOME system variable is defined.

Procedure

1. Log on to the IBM Db2 database server computer as the OpenPages application user, opuser.
2. Go to the /OP_<version>_Main/OP_<version>_Configuration/Database/DB2/UPGRADE_SCRIPTS directory.
3. Verify that you have execute permission on the scripts in UPGRADE_SCRIPTS and its subdirectories.
4. Open the sql-wrapper.sql file. Verify that the values are suitable for your environment.

5. Run the following command:

- On Linux:

```
./op-database-product-upgrade.sh preupgrade '<op_password>'
```

- On Windows:

```
op-database-product-upgrade.bat preupgrade "<op_password>" ""
```

The second parameter is not used, but must be included in the command. Use "".

Note: Quotation marks are required around a password only if the password contains special characters. See [“Special characters in passwords” on page 12](#).

6. Verify that the script completed successfully.

Look for the following message: Status:Success or a return code of 0.

You can also check the log file, op-validate-dba-pre-upgrade.log.

What to do next

Run the script to upgrade the database objects.

Upgrading the database (Db2)

Run the script to upgrade the database schema objects and data.

Before you begin

- The IBM Db2 database server is running. All other OpenPages servers are stopped.
- The JAVA_HOME system variable is defined and points to the IBM SDK, Java Technology Edition that is installed with Db2. For example:

```
export JAVA_HOME=/db2/V11.5/java/jdk64
export PATH=$JAVA_HOME/bin:$PATH
```

If you are running the script from another host, ensure that JAVA_HOME is pointing to the IBM SDK, Java Technology Edition that is installed on the computer.

- apache-ant-1.8.1 is deployed to /OP_<version>_Main/OP_<version>_Configuration/Database/DB2/UPGRADE_SCRIPTS
- The DB2_HOME system variable is defined.

Procedure

1. Log on to the IBM Db2 database server computer as the OpenPages application user, opuser.
2. Go to the /OP_<version>_Main/OP_<version>_Configuration/Database/DB2/UPGRADE_SCRIPTS directory.
3. Verify that you have execute permission on the scripts in the UPGRADE_SCRIPTS directory and its subdirectories.
4. Open the sql-wrapper.sql file. Verify that the values are suitable for your environment.
5. Run the database upgrade script:

If you are migrating from 7.3.x

Run the following command:

- On Linux:

```
./op-database-product-upgrade.sh upgrade '<op_password>' '<workflow_password>'
```

- On Windows:

```
op-database-product-upgrade.bat upgrade "<op_password>" "<workflow_password>"
```

You need to provide the password of the Fujitsu workflow user to complete the upgrade. The database upgrade scripts remove any references to the Fujitsu workflow schema that are contained within the OpenPages schema, and then the scripts remove the Fujitsu workflow schema.

If you are migrating from 7.4 or later

Run the following command:

The second parameter is not used, but must be provided. Use a dummy value, such as xxx.

- On Linux:

```
./op-database-product-upgrade.sh upgrade '<op_password>' xxx
```

- On Windows:

```
op-database-product-upgrade.bat upgrade "<op_password>" xxx
```

Note: Quotation marks are required around a password only if the password contains special characters. See [“Special characters in passwords” on page 12](#).

6. Verify that the return code is 0, indicating success.

You can also check the log file, `op-database-product-upgrade.log`.

What to do next

Ask your database administrator to run the post-upgrade DBA script.

Running the post-upgrade DBA script (Db2)

Ask your database administrator to run the post-upgrade script. Or, if you have DBADM and SECADM privileges, you can run the script.

Before you begin

- The IBM Db2 database server is running. All other OpenPages servers are stopped.
- The JAVA_HOME system variable is defined and points to the IBM SDK, Java Technology Edition that is installed with Db2. For example:

```
export JAVA_HOME=/db2/V11.5/java/jdk64
export PATH=$JAVA_HOME/bin:$PATH
```

If you are running the script from another host, ensure that JAVA_HOME is pointing to the IBM SDK, Java Technology Edition that is installed on the computer.

- `apache-ant-1.8.1` is deployed to `/OP_<version>_Main/OP_<version>_Configuration/Database/DB2/UPGRADE_SCRIPTS`
- The `DB2_HOME` system variable is defined.
- The `op-database-product-upgrade.sh | .bat` script completed successfully.

About this task

Run the following script: `op-database-dba-upgrade.sh | .bat`. The script uses the parameters defined in the `sql-wrapper.sql` file.

Procedure

1. Log on to the IBM Db2 database server computer as a database administrator (DBA).
2. Locate the scripts that are required.

If you are a database administrator, get the scripts from your OpenPages team.

Or, you can get the scripts from the `/OP_<version>_Main/OP_<version>_Configuration/Database/DB2/UPGRADE_SCRIPTS` directory.

3. Verify that you have execute permission on the scripts in UPGRADE_SCRIPTS and its subdirectories.
4. Open the `sql-wrapper.sql` file. Verify that the values are suitable for your environment.

The user that you specify in the `opx_db2_instance_owner` parameter must have both DBADM and SECADM privileges

You can run the following script to get a list of users that have the necessary privileges:

```
select grantee from syscat.dbauth where dbadmauth = 'Y' and securityadmauth = 'Y';
```

5. Run the following command:

- On Linux:

```
./op-database-dba-upgrade.sh post '<dba_password>'
```

- On Windows:

```
op-database-dba-upgrade.bat post "<dba_password>"
```

Note: Quotation marks are required around a password only if the password contains special characters. See [“Special characters in passwords”](#) on page 12.

6. Verify that the return code is 0, indicating success.

You can also check the log file: `op-database-dba-post-upgrade.log`.

What to do next

Validate the post-upgrade DBA step.

Validating the post-upgrade DBA step (Db2)

Run the script to validate the post-upgrade DBA steps.

Before you begin

- The IBM Db2 database server is running. All other OpenPages servers are stopped.
- The `JAVA_HOME` system variable is defined and points to the IBM SDK, Java Technology Edition that is installed with Db2. For example:

```
export JAVA_HOME=/db2/V11.5/java/jdk64
export PATH=$JAVA_HOME/bin:$PATH
```

If you are running the script from another host, ensure that `JAVA_HOME` is pointing to the IBM SDK, Java Technology Edition that is installed on the computer.

- `apache-ant-1.8.1` is deployed to `/OP_<version>_Main/OP_<version>_Configuration/Database/DB2/UPGRADE_SCRIPTS`
- The `DB2_HOME` system variable is defined.

Procedure

1. Log on to the IBM Db2 database server computer as the OpenPages application user, `opuser`.

2. Go to the `/OP_<version>_Main/OP_<version>_Configuration/Database/DB2/UPGRADE_SCRIPTS` directory.
3. Verify that you have execute permission on the scripts in `UPGRADE_SCRIPTS` and its subdirectories.
4. Open the `sql-wrapper.sql` file. Verify that the values are suitable for your environment.
5. Run the following command:

- On Linux:

```
./op-database-product-upgrade.sh postdba '<op_password>'
```

- On Windows:

```
op-database-product-upgrade.bat postdba "<op_password>" ""
```

The second parameter is not used, but must be included in the command. Use `""`.

Note: Quotation marks are required around a password only if the password contains special characters. See [“Special characters in passwords” on page 12](#).

6. Verify that the script completed successfully.
Look for the following message: `Status:Success` or a return code of 0.
You can also check the log file, `op-validate-dba-post-upgrade.log`.
7. Remove the passwords from the `sql-wrapper.sql` file for security purposes.

Results

The OpenPages database is upgraded.

What to do next

Migrate the application data from your previous version of OpenPages. See [“Migrate files” on page 201](#).

Updating the location of the openpages - storage directory (Db2)

In the database, update the location of the **openpages - storage** directory.

If you are using Microsoft Windows, you can also use this procedure to change the storage type from LFS to UNC.

Before you begin

Stop the IBM OpenPages with Watson services if they are running.

Procedure

1. Log on to the target environment as a user with administrative permissions. You can use any system with access to CLPPlus that can connect to the database server.
2. Open a command or shell window.
3. Locate the `update-storage.sql` script.

The script is stored in the following directories. You can use the script in either location.

- `/OP_<version>_Main/OP_<version>_Configuration/Database/DB2/INSTALL_SCRIPTS`
- `/OP_<version>_Main/OP_<version>_Configuration/Database/DB2/UPGRADE_SCRIPTS`

4. Run the `update-storage.sql` script to update the `openpages - storage` directory location in the database:

```
clpplus -nw <op_db_user>/\ '<op_db_password>'@<database_host>:  
<database_port>/<database_name> @sql-wrapper update-storage <log_file>  
<database_host> <database_port> <database_name> <op_db_user>
```

```
<op_db_password> <storage_type> <storage_server_name> <host_name>
<os_type> <path_or UNC_name>
```

Table 62. Parameters in the update-storage.sql script (Db2)

Parameter	Description
<op_db_user>	OpenPages user name for accessing the OpenPages database.
<op_db_password>	The OpenPages password for accessing the OpenPages database. If the password contains special characters, surround the password in quotation marks: <ul style="list-style-type: none"> Windows: 'password' Linux: \'password\'
<database_host>	Name of the Db2 server host machine that contains the OpenPages database.
<database_port>	Port number of the Db2 database instance that is installed on the database server. For Db2, the default port is 50000.
<database_name>	Name of the OpenPages database.
<log_file>	The name of the log file that the script creates and writes information to.
<storage_type>	The type of file storage to be used. Valid values are as follows: <ul style="list-style-type: none"> LFS (local file system) UNC (Universal Naming Convention) - for Windows only. Note: After you move from LFS to UNC, you cannot go back to using LFS.
<storage_server_name>	The name of the storage server.
<host_name>	The host name of the machine.
<os_type>	The type of operating system. Valid values are as follows: <ul style="list-style-type: none"> Windows Unix
<path_or UNC_name>	The file path or UNC of the storage location. If the path contains backslashes, wrap the path in single quotation marks.

Examples

• LFS

Windows

```
clpplus -nw openpage/'password'@myserver.ibm.com:50000/opx
@sql-wrapper update-storage output.log myserver.ibm.com 50000 OPX openpage 'password'
LFS eng11 eng11 Windows 'C:\IBM\OpenPages\openpages-storage'
```

Linux

```
clpplus -nw openpage/\'password\'@myserver.ibm.com:50000/opx
@sql-wrapper update-storage output.log myserver.ibm.com 50000 opx openpage \'password\'
LFS eng11 eng11 Unix /usr/opdata/openpages-storage
```

• UNC

Windows

```
clpplus -nw openpage/'password'@myserver.ibm.com:50000/opx
@sql-wrapper update-storage output.log myserver.ibm.com 50000 OPX openpage 'password'
UNC eng11 eng11 Windows openpages-storage
```

Update the database connection information (Db2)

After you restore and upgrade the source database, update the connection information that is stored in the database.

If you are using the database server from your source environment, you do not need to do these tasks.

- Update the `aurora.properties` with the URL of the database server. See [“Updating the aurora.properties file \(Db2\)”](#) on page 236.
- Update the data source connection in WebSphere Liberty. See [“Updating the data source connection in WebSphere Liberty \(Db2\)”](#) on page 237.
- Update IBM Cognos Configuration with the connection information for your IBM Db2 database server. See [“Updating the Cognos content store information \(Db2\)”](#) on page 237.
- Update the database connection information for the search server. See [“Updating the database connection information for the search server \(Oracle\)”](#) on page 263.
- Configure Cognos with the connection information for the OpenPages data source. See [“Updating the connection to the OpenPages database for Cognos \(Db2\)”](#) on page 238.

If you use SSL with the database server, you need to re-establish the SSL certificates after you migrate. When you install IBM OpenPages with Watson, the installation process configures a keystore for IBM WebSphere Liberty. By default, the Liberty keystore is also used for the database server certificates. You have two options:

- You can extract the certificates from the database server and then re-import them into the Liberty keystore.
- Or, you can use the keystore from your source environment by changing the keystore that is used by Db2. For more information, see the *IBM OpenPages with Watson Administrator's Guide*.

Updating the aurora.properties file (Db2)

Update the database server URL in the `aurora.properties` file.

Procedure

1. Open a command or shell window and go to the `<OP_HOME>/aurora/conf` directory.
2. Make a backup copy of the `aurora.properties` file.
3. Open the `aurora.properties` file in a text editor.
4. Search the file for the string `database.URL`.
5. Change the value that follows the equal sign to the URL of your database server.

Use the following format:

```
jdbc\:db2\://<host_name>\:<port>/<db_name>
```

Where:

- `<host_name>` is the name of the database server, such as `eng11`.
 - `<port>` is the database port number, such as `50000`.
 - `<db_name>` is the name of the Db2 database, such as `OP`.
6. Save your changes and close the editor.

Updating the data source connection in WebSphere Liberty (Db2)

Update IBM WebSphere Liberty with the database server connection information.

Procedure

1. Log on to the application server.
2. Stop the application servers.
For more information, see [“Stopping application servers” on page 311](#).
3. Open the following file in a text editor: `<OP_HOME>/wlp-user/servers/<server_name>Server<#>/bootstrap.properties`
Where `<server_name>` is the name of the application server.
4. Update the database server connection information.

```
op.db2.databaseName=<db_name>  
op.db2.portNumber=<db_port>  
op.jdbc.host=<host_name>
```

- `<host_name>` is the name of the database server, such as eng11.
 - `<db_port>` is the database port number, such as 50000.
 - `<db_name>` is the name of the OpenPages database, for example OP.
5. Save your changes.
 6. Repeat these steps on each horizontal application server.
 7. Restart the application servers.
For more information, see [“Starting application servers” on page 309](#).

Updating the Cognos content store information (Db2)

Update IBM Cognos Configuration with the connection information for your IBM Db2 database server.

Procedure

1. Start the IBM Cognos services and the IBM OpenPages with Watson services.
2. Log on to the reporting server as a user with administrator privileges.
Note: For Windows installations, the user must belong to the DB2ADMINS group. For Linux installations, the user must belong to the db2iadm group.
3. Start Cognos Configuration.
 - On Windows computers, click **Start > IBM Cognos Analytics > IBM Cognos Configuration**.
 - On Linux, go to the `<COGNOS_HOME>/bin64` directory, type `./cogconfig.sh`, and press Enter.
4. Update the database connection information for the content store.
 - a) Under **Local Configuration > Environment > Data Access > Content Manager**, click **IBM Cognos Content Store**.
 - b) In the **Database server and port number** field, enter the name of the computer and the port number on which Db2 is running.
 - c) Click the **Value** field next to the **User ID and password** property, click the edit icon, and type the appropriate values for the Cognos user that you created for the content store database, and click **OK**.
 - d) In the **Properties** window, for the **Database name** property, type the name for your content store database.
Restriction: Do not use a name longer than eight characters and use only letters, numbers, underscores, and hyphens in the name.
5. Click **File > Save**.

6. In the **Explorer** pane, right-click the content store database connection and click **Test**.
7. Stop the IBM Cognos services and the IBM OpenPages with Watson services.

Updating the database connection information for the search server (Db2)

Update the connection information that the search server uses to access the database server.

Procedure

1. Log on to the search server as a user with administrative privileges.
2. Go to `<SEARCH_HOME>/opsearchtools/`.
3. Open the `openpages_search.properties` file in a text editor.
4. Modify the database connection properties with the values for the production database server.
Use the following examples as a guide.

```
# Database connectivity information
OPSearchTool.DatabaseType = DB2
OPSearchTool.DatabaseHostName = OP-WIN-DB2
OPSearchTool.DatabasePort = 50000
OPSearchTool.DatabaseName = OPX
OPSearchTool.DatabaseUserID = openpages_db_user_id
OPSearchTool.DatabasePassword = openpages_db_password
```

Updating the `deploy.properties` file

Update the database server host name and the database credentials in the `deploy.properties` file.

Procedure

1. If the installation app is running, log out.
2. Open a command or shell window and go to the `<installation_server_home>/src/deployment/<deployment-name>` directory.
3. Make a backup copy of the `deploy.properties` file.
4. Open the `deploy.properties` file in a text editor.
5. Go to the database server section.
6. Update the following parameters with the values for your production database server.
 - `host`
 - `db_port`
 - `dba_username`
 - `dba_password`
Note: Do not use quotation marks around the password, even if it contains special characters.
 - `op_db_username`
 - `op_db_password`
Note: Do not use quotation marks around the password, even if it contains special characters.
7. Save your changes and close the editor.

Updating the connection to the OpenPages database for Cognos (Db2)

If you are using new hardware for the database server, update Cognos with the database connection information for the OpenPages database.

Procedure

1. Start the IBM Cognos services.

2. Log on to IBM Cognos Analytics as a user with administrative privileges..
 - In the Task Focused UI, click **Analytics**.
 - Or, go to the following URL: `http://<hostname>/ibmcognos/bi`
Where <hostname> is the name of the Cognos server.
3. Click **Manage > Administration Console** to launch the **IBM Cognos Administration** page.
4. Click the **Configuration** tab.
5. Click **OpenPages DataSource** under **Data Source Connections**.
6. Click **Actions > Set Properties - OpenPages DataSource**.
7. Update the database connection string:
 - a) Click the **Connection** tab.
 - b) Click the pencil icon next to the **Connection String** box to edit the field.
 - c) On the **CLI** tab, in the **Db2 database name** box, change the Db2 database name to the Catalog Database Name of the OpenPages database in your upgraded environment.

Chapter 9. Migration task reference for Oracle databases

If you are using Oracle, refer to the following topics when you migrate IBM OpenPages with Watson to 8.2.

The tasks that you need to do depend on the scenario that you are following. Use the following topics to guide you through the migration process:

- [“Migration process overview: Using the database server from your source environment” on page 190](#)
- [“Migration process overview: Using new hardware for the database server” on page 192](#)

Backing up the OpenPages database during a migration (Oracle)

Run the OPBackup utility to back up the IBM OpenPages with Watson databases in your source environment.

About this task

Use this procedure if you are migrating to OpenPages version 8.2.

If you are migrating from 7.3.x, you need to back up and then restore both the OpenPages schema and the Fujitsu workflow schema so that the database upgrade scripts can remove any references to the Fujitsu workflow schema that are contained within the OpenPages schema. Once the OpenPages schema has these references removed, the Fujitsu workflow schema will then be removed to complete this step.

If you are using 7.4.x or later, the Fujitsu workflow schema has already been removed.

Run the OPBackup utility with the `dbonly` parameter.

Note:

You can back up the databases by using other methods. Some examples of alternative methods include:

- Doing a full physical backup by using RMAN
- Doing a combination of full and incremental backup by using RMAN
- Doing an Oracle data pump export.

If you want to use an alternative method, it is critical that you have the necessary skills available within your organization to complete all aspects of the backup and restore activity.

For more information about backing up your environment, see the *IBM OpenPages with Watson Administrator's Guide*.

Procedure

1. In your source environment, make sure that no OpenPages with Watson processes are running, such as object reset jobs.
2. Shut down all OpenPages components: application servers (admin and non-admin), reporting servers (active and standby), and the search server.
For more information, see [Chapter 12, “Starting and stopping servers,” on page 309](#).
3. Open a command or shell window on the admin application server in your source environment.
4. Go to the `<OP_HOME>/aurora/bin` directory.
5. Do a full database backup of the OpenPages schema by using OPBackup.

Windows:

```
OPBackup.cmd <backup_directory> dbonly
```

Linux:

```
./OPBackup.sh <backup_directory> dbonly
```

The <backup_directory> is the full path to a directory on the database server. This directory is where the log files are saved. If the file path is not specified, the OPBackup command uses the location that is specified by the **BACKUP_LOCATION** parameter in the <OP_HOME>/aurora/bin/op-backup-restore.env file.

Dump files are created in the OP_DATAPUMP_DIRECTORY directory.

- If you are migrating from 7.3.x, two dump files are created: one for the OpenPages schema one for the Fujitsu workflow schema.
 - If you are migrating from 7.4.x or later, one dump file for the OpenPages schema is created. The Fujitsu workflow schema was removed when you upgraded to 7.4.x or 8.0.x.
6. Examine the backup log and make note of the dump file names. The naming convention is openpage_<timestamp>.dmp and workflow_<timestamp>.dmp.
 7. Copy the .dmp files to the OP_DATAPUMP_DIRECTORY directory on the database server in your target environment.
 - a) Locate the OP_DATAPUMP_DIRECTORY directory on the target database server.

To find the OP_DATAPUMP_DIRECTORY directory, run the following SQL as the system user::

```
select directory_name, directory_path from dba_directories
where directory_name = upper ('OP_DATAPUMP_DIRECTORY');
```

- b) Copy the dump files to the OP_DATAPUMP_DIRECTORY directory on the target database server.

Copy the following files:

- openpage_<timestamp>.dmp
- workflow_<timestamp>.dmp (Applies only if you are migrating from version 7.3.x.)

Note: Make sure to copy the .dmp files with the time stamp that matches when you ran the OPBackup command.

Backing up the Cognos content store during a migration (Oracle)

You can use OPCCBackup to back up the Cognos content store.

About this task

Use this procedure if you are migrating to IBM OpenPages with Watson 8.2.

Run the OPCCBackup utility with the dbonly parameter.

Note: You can back up the content store by using other methods. Some examples of alternative methods include:

- Doing a full physical backup by using RMAN
- Doing a combination of full and incremental backup by using RMAN
- Doing an Oracle data pump export.

If you want to use an alternative method, it is critical that you have the necessary skills available within your organization to complete all aspects of the backup and restore activity.

For more information about backing up your environment, see the *IBM OpenPages with Watson Administrator's Guide*.

Procedure

1. In your source environment, make sure that no OpenPages with Watson processes are running, such as object reset jobs.
2. Shut down all OpenPages components: application servers (admin and non-admin), reporting servers (active and standby), and the search server.

For more information, see [Chapter 12, “Starting and stopping servers,” on page 309](#).

3. Ensure that all Cognos components are shut down.
4. Open a command or shell window on the admin application server in your source environment.
5. Go to the `<OP_HOME>/CommandCenter/tools/bin` directory.
6. Do a full database backup of the Cognos schema by using OPCCBackup.

Windows:

```
OPCCBackup.cmd <backup_directory> dbonly
```

Linux:

```
./OPCCBackup.sh <backup_directory> dbonly
```

The `<backup_directory>` is the full path to a directory on the database server. This directory is where the log files are saved. If the file path is not specified, the OPCCBackup command uses the location that is specified by the **OP_CC_BACKUP_HOME** parameter in the `<CC_HOME>/tools/bin/op-cc-backup-restore.env` file.

A dump file is created in the `OP_DATAPUMP_DIRECTORY` directory. The file is called `openpage_cc_<timestamp>.dmp`.

If you get the warning `tools.jar file is not found`, see the following [technote](#).

7. Copy the `.dmp` file to the `OP_DATAPUMP_DIRECTORY` directory on the database server in your target environment.
 - a) Locate the `OP_DATAPUMP_DIRECTORY` directory on the target database server.

Note:

To find the datapump directory for either the source or target database, run the following SQL query as the system user:

```
select directory_name, directory_path from dba_directories
where directory_name = upper ('OP_DATAPUMP_DIRECTORY');
```

By default, the datapump directory on the database server is `<oracle-server-directory>|admin|<sid>|dpdump`

- b) Copy the Cognos database dump files to the `OP_DATAPUMP_DIRECTORY` directory on the target database server.

Copy the following file: `openpage_cc_<timestamp>.dmp`

Note: Make sure to copy the `.dmp` file with the time stamp that matches when you ran the OPCCBackup command.

Restore the OpenPages database in your 8.2 environment (Oracle)

Import the OpenPages database from your source environment to the 8.2 environment. Do this step before you upgrade the database.

Do these tasks to restore the databases:

- Prepare the Oracle database in your 8.2 environment.
- Restore the OpenPages schema.

- If you are migrating from 7.3.x, restore the Fujitsu workflow schema.

You need to restore the Fujitsu workflow schema so that the database upgrade scripts can remove any references to the workflow schema that are contained within the OpenPages schema. Once the OpenPages schema has these references removed, the workflow schema will then be removed to complete the upgrade.

If you are using 7.4.x or later, the Fujitsu workflow schema has already been removed.

Preparing to import the OpenPages database (Oracle)

Prepare the database in your target environment before you restore the database schemas from your previous installation of OpenPages.

Before you begin

Ensure that you completed the backup of the database schemas. See [“Backing up the OpenPages database during a migration \(Oracle\)”](#) on page 241.

Procedure

1. Shut down all OpenPages components: application servers (admin and non-admin), reporting servers (active and standby), and the search server.

For more information, see [Chapter 12, “Starting and stopping servers,”](#) on page 309.

2. Log on to a server that has access to the database server and has SQL*Plus.
3. Drop the OpenPages database schema objects in your target environment.
 - a) Go to the /OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/UPGRADE_SCRIPTS/OP730X_TO_OP740X directory.
 - b) Verify that you have execute permission on the files in the /OP730X_TO_OP740X directory.
 - c) Log on to SQL*Plus as the OpenPages database user (for example: sqlplus openpages/openpages@test).
 - d) Use the spool command to create a log file.

```
spool <log_file_directory>/<log_file_name>
```

Ensure that you have write permission on the <log_file_directory>.

Example:

```
spool /tmp/AuroraDbDelete.log
```

- e) Run the AuroraDbDelete.sql script.

```
@AuroraDbDelete.sql
```

- f) Log out of SQL*Plus.
4. Completely populate the required entries in the /OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/UPGRADE_SCRIPTS/OP810X_TO_OP8200/sql-wrapper.sql file.
For more information, see [“Preparing for the database upgrade \(Oracle\)”](#) on page 252.
 5. If you are migrating from 7.3.x, create the Fujitsu workflow user on the admin application server in your target environment.

If you are migrating from 7.4.x or later, skip this step.

- a) Go to the /OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/UPGRADE_SCRIPTS/OP730X_TO_OP740X directory.
- b) Log in to SQL*Plus as a DBA user.

c) Run the following script:

- Windows:

```
@sql-wrapper ibpm-ts-and-schema-owner.sql ibpm-ts-and-schema-owner.log  
"<workflow_password>"
```

- Linux:

```
@sql-wrapper ibpm-ts-and-schema-owner.sql ibpm-ts-and-schema-owner.log  
'<workflow_password>'
```

Note: Quotation marks are required around a password only if the password contains special characters. See [“Special characters in passwords”](#) on page 12.

d) Run the following command:

```
grant create job to <workflow_db_user>;
```

The `<workflow_db_user>` is defined in the `opx_workflow_user` parameter of the `/OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/UPGRADE_SCRIPTS/OP810X_TO_OP8200/sql-wrapper.sql` file.

What to do next

Restore the database schema from your previous version of OpenPages.

Restoring the OpenPages database schemas (Oracle)

Restore the database schemas from your previous installation of OpenPages into your target environment.

Before you begin

Ensure that the following tasks are complete:

- You backed up the OpenPages databases in the source environment. See [“Backing up the OpenPages database during a migration \(Oracle\)”](#) on page 241.
- You prepared the database in your target environment for the import. See [“Preparing to import the OpenPages database \(Oracle\)”](#) on page 244.
- You copied the backup files to the database server in your target environment. Store the files in the `OP_DATAPUMP_DIRECTORY` directory.

If the OpenPages and Cognos databases are on different database servers, copy the dump files to the OpenPages database server.

About this task

Import the databases in the following order:

- OpenPages database
- Workflow database (applies only if you are migrating from 7.3.x)

If you are migrating from 7.3.x, you need to back up and then restore both the OpenPages schema and the Fujitsu workflow schema so that the database upgrade scripts can remove any references to the Fujitsu workflow schema that are contained within the OpenPages schema. Once the OpenPages schema has these references removed, the Fujitsu workflow schema will then be removed to complete this step.

If you are using 7.4.x or later, the Fujitsu workflow schema has already been removed.

If the schema names or table space names are different in the source and target environments, you must remap them during the import. See [“Remap schema and table space names \(Oracle\)”](#) on page 248.

Note: When you import, you might see an error as a result of the default data file size. For more information, see [“Issues when importing databases” on page 456](#).

Procedure

1. Shut down all OpenPages components: application servers (admin and non-admin), reporting servers (active and standby), and the search server.
For more information, see [Chapter 12, “Starting and stopping servers,” on page 309](#).
2. Log on to a server that has access to the database server and has SQL*Plus.
3. Set the NLS_LANG environment variable.

Windows

- a) In the Windows search box, type `environment variables`, and then click **Edit system environment variables**.
- b) On the **Advanced** tab, click **Environment variables**.
- c) In the **System Variables** pane, click **New**.
- d) Add the NLS_LANG variable.
For example: `NLS_LANG=AMERICAN_AMERICA.AL32UTF8`
- e) Click **OK** twice to exit.

Alternatively, you can set the environment variable globally. See Microsoft Windows Server documentation.

Linux

- a) Open a shell window.
- b) Open the user profile (for example, `.profile`) that is in the home directory of the user who is currently logged in.
- c) Set the NLS_LANG variable if it's missing from the file.
For example:

```
export NLS_LANG=AMERICAN_AMERICA.AL32UTF8
```

- d) Save the file.
- e) Refresh the profile.

For example, open a shell and run the following command:

```
. /home/oracle/.bash_profile
```

4. Import the OpenPages database schema.

Note: The Oracle Data Pump command `IMPDP` is used because the `IMP` command is not supported. For more information about Oracle Data Pump, see the *IBM OpenPages with Watson Administrator's Guide*.

Run the following command to import the OpenPages with Watson database:

```
impdp <op_db_user>/\"<op_db_password>\"@<SID> DIRECTORY=OP_DATAPUMP_DIRECTORY  
DUMPFILE=<openpages_dump_file> LOGFILE=openpages_import.log exclude=statistics
```

Table 63. Parameters and their descriptions: Importing the OpenPages database schema	
Parameter	Description
<op_db_user>	The user name for accessing the OpenPages database.
<op_db_password>	The password for accessing the OpenPages database.

Table 63. Parameters and their descriptions: Importing the OpenPages database schema (continued)	
Parameter	Description
<SID>	The Oracle System Identifier (for example, OP).If you are using a pluggable database, use the service name of the pluggable database, not the container database.
<openpages_dump_file>	The .dmp file name of the backed-up OpenPages database schema: openpage_<timestamp>.dmp. Important: Do not enter a path. Enter only the file name.
DIRECTORY	Important: Do not enter an explicit path when you specify the DIRECTORY parameter. Use OP_DATAPUMP_DIRECTORY only.

5. If you are migrating from 7.3.x, import the Fujitsu workflow database schema from the backup files.

If you are using 7.4.x or later, skip this step.

From the same command or shell window, run the following command to import the workflow database:

```
impdp <workflow_db_user>/\"<workflow_db_password>\"@<SID>
  DIRECTORY=OP_DATAPUMP_DIRECTORY DUMPFILE=<workflow_dump_file>
  LOGFILE=opworkflow_import.log exclude=statistics
```

Table 64. Parameters and their descriptions: Importing the workflow database schema	
Parameter	Description
<workflow_db_user>	The user name for accessing the workflow database.
<workflow_db_password>	The password for accessing the workflow database.
<SID>	The Oracle System Identifier (for example, OP). If you are using a pluggable database, use the service name of the pluggable database, not the container database.
<workflow_dump_file>	The .dmp file name of the backed-up workflow database schema: workflow_<timestamp>.dmp. Important: Do not enter the path. Enter only the file name.
DIRECTORY	Important: Do not enter an explicit path when you specify the DIRECTORY parameter. Use OP_DATAPUMP_DIRECTORY only.

Example

```
impdp opworkflow/\"password\"@OP DIRECTORY=OP_DATAPUMP_DIRECTORY
DUMPFILE=opworkflow_backup_YYYY_MM_DD_HH_MI_SS.dmp LOGFILE=opworkflow_import.log
exclude=statistics
```

If you receive a message that is similar to the following example, you can ignore it.

```
Processing object type SCHEMA_EXPORT/JOB
ORA-39083: Object type JOB:"WORKFLOW" failed to create with error:
```

```
ORA-27486: insufficient privileges
```

```
Failing sql is:  
BEGIN DBMS_JOB.ISUBMIT( JOB=> 4, NEXT_DATE=> TO_DATE('2019-11-01 00:00:00',  
'YYYY-MM-DD:HH24:MI:SS'), INTERVAL=> 'TRUNC(SYSDATE + 1, 'DD')', WHAT=>  
'UPDATE_SCHEMA_STATS;', NO_PARSE=> TRUE); END;  
Job "WORKFLOW"."SYS_IMPORT_FULL_01" completed with 1 error(s) at Thu Oct 31 04:43:35 2019  
elapsed 0 00:00:11
```

What to do next

If the import fails, review the log files carefully. A failure at the beginning of the process might cause a number of cascading failures that are a symptom of the root issue.

After the import completes successfully, upgrade the OpenPages database.

Remap schema and table space names (Oracle)

If the schema names or table space names are different in the source and target environments, you must remap them during the import.

Remap schema names

If the schema names are different in the source and target, you must remap the schema names. You must also run the import command as a DBA user.

Note: All references to the Fujitsu workflow schema apply only if you are migrating from 7.3.x.

OpenPages schema name is different

If the OpenPages schema name is different, remap it when you import the OpenPages schema. If you are migrating from 7.3.x, also remap the OpenPages schema name when you import the Fujitsu workflow schema.

- Add the following clause to the import command for the OpenPages schema:

```
remap_schema=<op_source>:<op_target>
```

- Add the following clause to the import command for the Fujitsu workflow schema:

```
remap_schema=<op_source>:<op_target>
```

Note: If you use a different name for the OpenPages schema in the target environment, the change might impact your reports. You might need to do some remediation steps. If your reports contain references to the schema, update the reports to use the new schema name. Out-of-the-box reports are not impacted by this issue because they do not reference the schema name.

Workflow schema name is different

If the Fujitsu workflow schema name is different but the OpenPages schema name is the same, remap the workflow schema when you import the workflow schema. Add the following clause to the import command for the workflow schema:

```
remap_schema=<workflow_source>:<workflow_target>
```

OpenPages and workflow schema names are different

If both the OpenPages and Fujitsu workflow schema names are different, do the following steps:

- Remap the OpenPages schema when you import the OpenPages schema. Add the following clause:

```
remap_schema=<op_source>:<op_target>
```

- Remap both the OpenPages schema and the Fujitsu workflow schema when you import the workflow schema. Add the following clauses:

```
remap_schema=<workflow_source>:<workflow_target>  
remap_schema=<op_source>:<op_target>
```

Example : In this example, the OpenPages schema name is different and the Fujitsu workflow schema name is the same in the source and target.

```
impdp <dba_user>/\"<dba_password>\"@OP
  DIRECTORY=OP_DATAPUMP_DIRECTORY
  DUMPFILE=openpages_backup_YYYY_MM_DD_HH_MI_SS.dmp
  LOGFILE=openpages_import.log remap_schema=opuser:openpages
  exclude=statistics
```

```
impdp <dba_user>/\"<dba_password>\"@OP
  DIRECTORY=OP_DATAPUMP_DIRECTORY
  DUMPFILE=opworkflow_backup_YYYY_MM_DD_HH_MI_SS.dmp
  LOGFILE=opworkflow_import.log remap_schema=opuser:openpages
  exclude=statistics
```

Example : In this example, both the OpenPages and workflow schema names are different.

```
impdp <dba_user>/\"<dba_password>\"@OP
  DIRECTORY=OP_DATAPUMP_DIRECTORY
  DUMPFILE=openpages_backup_YYYY_MM_DD_HH_MI_SS.dmp
  LOGFILE=openpages_import.log remap_schema=opuser:openpages
  exclude=statistics
```

```
impdp <dba_user>/\"<dba_password>\"@OP
  DIRECTORY=OP_DATAPUMP_DIRECTORY
  DUMPFILE=opworkflow_backup_YYYY_MM_DD_HH_MI_SS.dmp
  LOGFILE=opworkflow_import.log remap_schema=myworkflow:opworkflow
  remap_schema=opuser:openpages exclude=statistics
```

Example : In this example, the Cognos schema name is different.

```
impdp <dba_user>/\"<dba_password>\"@OPCC
  DIRECTORY=OP_DATAPUMP_DIRECTORY
  DUMPFILE=openpage_cc_YYYY_MM_DD_HH_MI_SS.dmp
  LOGFILE=opcognos_import.log fromuser=cognos touser=cognos
  TABLE_EXISTS_ACTION=REPLACE remap_schema=mycc:opcc
```

Remap table space names

If the source and target databases are using different table space names, include the following clause in the import command:

```
remap_tablespace=<source_tablespace_name>:<target_tablespace_name>
```

Example : In this example, the MYCRN table space is remapped to the CRN table space in the target environment.

```
impdp system/\"password\"@OPCC
  DIRECTORY=OP_DATAPUMP_DIRECTORY
  DUMPFILE=openpage_cc_YYYY_MM_DD_HH_MI_SS.dmp
  LOGFILE=opcognos_import.log fromuser=cognos touser=cognos
  TABLE_EXISTS_ACTION=REPLACE remap_tablespace=MYCRN:CRN
```

To determine the table space names that are used, do the following steps:

1. In the source environment, log in to SQL*Plus as the cognos user.
2. Run the following command to get a list of table spaces:

```
select tablespace_name from user_tablespaces;
```

3. Run the following command to get a list of table spaces that contain objects:

```
select distinct tablespace_name from user_segments;
```

4. Repeat these steps in the target environment and compare the table space names.

If you need to remap the schema and the table spaces, place the `remap_schema` parameter before the `remap_tablespace` parameter. Run the command as a DBA user.

Example : In this example, the Cognos schema name is remapped and the MYCRN table space is also remapped.

```
impdp <dba_user>/\"<dba_password>\"@OPCC DIRECTORY=OP_DATAPUMP_DIRECTORY
DUMPFILE=openpage_cc_YYYY_MM_DD_HH_MI_SS.dmp
LOGFILE=opcognos_import.log fromuser=cognos touser=cognos
TABLE_EXISTS_ACTION=REPLACE remap_schema=mycc:opcc
remap_tablespace=MYCRN:CRN
```

Restore the Cognos content store in your 8.2 environment (Oracle)

When you upgrade Cognos Analytics, you can import the content store from your source environment.

Do these tasks to restore the content store:

- Prepare the Oracle database in your 8.2 environment.
- Restore the Cognos database schema.

Preparing to import the Cognos content store (Oracle)

Prepare the database in the target environment before you restore the Cognos content store schema.

Before you begin

Ensure that you completed the backup of the content store. See [“Backing up the Cognos content store during a migration \(Oracle\)” on page 242](#).

Procedure

1. Shut down all OpenPages components: application servers (admin and non-admin), reporting servers (active and standby), and the search server.
For more information, see [Chapter 12, “Starting and stopping servers,” on page 309](#).
2. Log on to a server that has access to the database server and has SQL*Plus.
3. Drop the Cognos database schema objects in your target environment.
 - a) Log on to a server that has access to the database server and has SQL*Plus.
 - b) Log on to SQL*Plus as the Cognos database user.
 - c) Use the spool command to create a log file.

```
spool <log_file_directory>/<log_file_name>
```

Ensure that you have write permission on the *<log_file_directory>*.

Example:

```
spool /tmp/AuroraDbDelete.log
```

- d) Run the `AuroraDbDelete.sql` script.

```
@AuroraDbDelete.sql
```

- e) Log out of SQL*Plus.

Restoring the Cognos content store (Oracle)

Restore the content store from your previous installation of Cognos.

Before you begin

Ensure that the following tasks are complete:

- You backed up the Cognos content store in the source environment. See [“Backing up the Cognos content store during a migration \(Oracle\)”](#) on page 242.
- You prepared your database for the import. See [“Preparing to import the Cognos content store \(Oracle\)”](#) on page 250.
- You copied the backup files to the database server in your target environment. Store the files in the OP_DATAPUMP_DIRECTORY directory.

If the OpenPages and Cognos databases are on different database servers, copy the Cognos dump file to the Cognos database server.

- The OP_DATAPUMP_DIRECTORY is configured. For more information, see [“Configuring the Oracle data pump directory”](#) on page 459.

About this task

If the schema names or table space names are different in the source and target environments, you must remap them during the import. See [“Remap schema and table space names \(Oracle\)”](#) on page 248.

Procedure

1. Shut down all OpenPages components: application servers (admin and non-admin), reporting servers (active and standby), and the search server.
For more information, see [Chapter 12, “Starting and stopping servers,”](#) on page 309.
2. Log on to a server that has access to the database server and has SQL*Plus.
3. Import the Cognos content store.

From a command or shell window, run the following command to import the Cognos content store:

```
impdp system/"<system_password>"@<SID> DIRECTORY=OP_DATAPUMP_DIRECTORY
DUMPFILE=<cognos_dump_file> LOGFILE=opcognos_import.log fromuser=cognos touser=cognos
TABLE_EXISTS_ACTION=REPLACE exclude=statistics
```

Table 65. Parameters and their descriptions: Importing the Cognos database schema

Parameter	Description
<system_password>	The password of the SYSTEM user.
<SID>	The Oracle System Identifier (for example, OPCC). If you are using a pluggable database, use the service name of the pluggable database, not the container database.
<cognos_dump_file>	The .dmp file name of the backed-up Cognos database schema: openpage_cc_<timestamp>.dmp. Important: Do not enter the path. Enter only the file name.
DIRECTORY	Important: Do not enter an explicit path when you specify the DIRECTORY parameter. Use OP_DATAPUMP_DIRECTORY only.

Example

```
impdp system/"password"@OPCC DIRECTORY=OP_DATAPUMP_DIRECTORY
DUMPFILE=openpage_cc_YYYY_MM_DD_HH_MI_SS.dmp LOGFILE=opcognos_import.log fromuser=cognos
touser=cognos TABLE_EXISTS_ACTION=REPLACE exclude=statistics
```

What to do next

If the import fails, review the log files carefully. A failure at the beginning of the process might cause a number of cascading failures that are a symptom of the root issue.

Upgrade the OpenPages database (Oracle)

Run scripts to upgrade the OpenPages database schema. Use these topics when you are migrating to 8.2.

This video demonstrates how to upgrade the database schema by using scripts. The video shows 7.4 but the steps are similar for 8.2.

https://youtu.be/_1vVuhzcJqY

You must run all of the upgrade scripts in sequence to upgrade the database schema.

Two of the scripts require DBA privileges: a pre-upgrade script and a post-upgrade script. If you have DBA privileges, you can run all of the scripts. If you do not have DBA privileges, contact your database administrator.

A schema user can run the scripts that do not require DBA privileges.

Note for 7.4.x and 8.0.x customers: The database upgrade scripts modify and drop some database structures to free up space in the database. To gain the full benefit of these changes, the PROPERTYVALS table needs to be reorganized. You can do the table reorganization after you upgrade the database or after you complete the migration to version 8.2. For information about how to reorganize a table, see the Oracle documentation.

Pre-upgrade step – Requires DBA privileges

During this step, your database administrator runs a script to prepare the database for the upgrade.

You need SYSDBA privileges to run this script.

Validate the pre-upgrade step

During this step, you run a script to verify that the pre-upgrade script completed successfully and that the database schema is ready for the upgrade.

Upgrade step

During this step, you run a script to upgrade the schema. The script determines the current version of the database schema, and then runs the upgrade scripts that are needed to upgrade the schema.

Post upgrade step – Requires DBA privileges

During this step, your database administrator runs a script to complete the database upgrade and to set database tuning parameters.

You need SYSDBA privileges to run this script.

Validate the post-upgrade step

During this step, you run a script to validate the post-upgrade step.

Preparing for the database upgrade (Oracle)

Prepare for the upgrade of the database schema.

Procedure

1. Shut down all OpenPages components: application servers (admin and non-admin), reporting servers (active and standby), and the search server.
For more information, see [Chapter 12, “Starting and stopping servers,” on page 309](#).
2. Ensure that the Oracle database server is running.
3. Log on to the Oracle database server computer as a user with administrative privileges.
4. Go to the `/OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/UPGRADE_SCRIPTS` directory.
5. Verify that you have write permission on the `sql-wrapper.sql` file.

6. Edit the `sql-wrapper.sql` file.

Note: Change only the parameters that are described in this step.

Table 66. Parameters in the <code>sql-wrapper.sql</code> file for Oracle databases	
Property	Description
<code>opx_datafile_storage_dir</code>	Defines the physical locations of the datafiles that are associated with the tablespaces that are created. This should be set to a value that is appropriate for your environment
<code>opx_dflt_sid</code>	The TNS alias of the Oracle database for OpenPages.
<code>opx_db_owner</code>	The OpenPages database owner
<code>opx_oracle_dba_user</code>	The user name of a DBA user. If your database administrator is going to run the DBA scripts for you, then you can leave this value empty when you run the non-DBA scripts.
<code>opx_workflow_user</code>	<p>The Fujitsu Interstage BPM workflow database user name.</p> <p>If you are migrating from 7.3.x, you need to provide the workflow user name to complete the upgrade. The database upgrade scripts remove any references to the workflow schema that are contained within the OpenPages schema, and then the scripts remove the workflow schema.</p> <p>If you are migrating from 7.4.x or later, the Fujitsu workflow schema was removed when you upgraded to 7.4.x or later.</p>
<code>opx_override_ver_check</code>	<p>Use the default value, N, unless you are re-running the database upgrade scripts after a failure.</p> <p>If the database upgrade failed in the middle of the schema upgrade process, set this parameter to Y. When you re-run the upgrade script, the upgrade process resumes from the last successful schema upgrade step.</p> <p>For example, suppose you are migrating from 7.3. When you run the upgrade script, it successfully upgrades the schema from 7.3 to 8.0, but fails during the upgrade from 8.0 to 8.1. Set this flag to Y and then re-run the script. The upgrade resumes at the 8.0 to 8.1 database upgrade step.</p>

7. If you want to run a custom script during the upgrade process, see [“Running custom scripts during the database upgrade \(Oracle\)”](#) on page 254.
8. If your database administrator is going to run the scripts that require DBA privileges, prepare the files for your database administrator.
 - a) Go to the `/OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/UPGRADE_SCRIPTS` directory.
 - b) Open the `op-dba-upgrade-file-list.txt` file.
 - c) Send your DBA the `sql-wrapper.sql` file that you updated along with the files listed in the `op-dba-upgrade-file-list.txt` file.
 - d) Send your DBA the instructions to run the DBA scripts.
 - [“Running the pre-upgrade DBA script \(Oracle\)”](#) on page 254
 - [“Running the post-upgrade DBA script \(Oracle\)”](#) on page 257

Running custom scripts during the database upgrade (Oracle)

If you want to run custom scripts during the database upgrade process, edit the `sql-wrapper.sql` file to specify the scripts to run.

About this task

You can use the `custom_data_upgrade_script` parameter to configure a custom script.

The script that you specify is run during the database upgrade step. The custom script is called by the `op-database-product-upgrade.sh/bat` script after the other upgrade steps, such as DDL changes, PL/SQL code changes, and database level data changes are complete.

Procedure

1. Open the `sql-wrapper.sql` file.
2. Edit the following parameters:

```
define custom_data_upgrade_script=no-op.sql
```

Replace `no-op.sql` with the script that you want to run.

3. Place your custom scripts in the same directory as the `sql-wrapper.sql` file.

Running the pre-upgrade DBA script (Oracle)

Ask your database administrator to run the pre-upgrade script. Or, if you have SYSDBA privileges, you can run the script.

Before you begin

- The Oracle database server is running. All other OpenPages servers are stopped.
- The `JAVA_HOME` system variable is defined.
- `apache-ant-1.8.1` has been deployed to `/OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/UPGRADE_SCRIPTS`
- The `ORACLE_HOME` system variable is defined.

About this task

Run the following script: `op-database-dba-upgrade.sh | .bat`. The script uses the parameters defined in the `sql-wrapper.sql` file.

Procedure

1. Log on to the Oracle database server computer as a database administrator (DBA).
2. Locate the scripts that are required.

If you are a database administrator, get the scripts from your OpenPages team.

Or, you can get the scripts from the `/OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/UPGRADE_SCRIPTS` directory.

3. Verify that you have execute permission on the scripts.
4. Open the `sql-wrapper.sql` file. Verify that the values are suitable for your environment.
 - a) For the `opx_oracle_dba_user` parameter, enter a user that has SYSDBA privileges, for example `SYS`.
 - b) If you customized the table space names, update the `define opx_dflt_*` parameters with the custom table space names.

- c) If you want to run custom scripts during the upgrade, see [“Running custom scripts during the database upgrade \(Oracle\)”](#) on page 254.

5. Run the following command:

- On Windows:

```
op-database-dba-upgrade.bat pre "<sysdba_password>"
```

- On Linux:

```
./op-database-dba-upgrade.sh pre '<sysdba_password>'
```

Note: Quotation marks are required around a password only if the password contains special characters. See [“Special characters in passwords”](#) on page 12.

6. Verify that the return code is 0, indicating success.

You can also check the log file, `op-database-dba-pre-upgrade.log`.

What to do next

Validate the pre-upgrade script.

Validating the pre-upgrade DBA step (Oracle)

Run the script to validate the pre-upgrade DBA steps.

Before you begin

- The Oracle database server is running. All other OpenPages servers are stopped.
- The JAVA_HOME system variable is defined.
- `apache-ant-1.8.1` has been deployed to `/OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/UPGRADE_SCRIPTS`
- The ORACLE_HOME system variable is defined.

Procedure

1. Log on to the Oracle database server computer as the OpenPages application user, `opuser`.
2. Go to the `/OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/UPGRADE_SCRIPTS` directory.
3. Verify that you have execute permission on the scripts.
4. Open the `sql-wrapper.sql` file. Verify that the values are suitable for your environment.
5. Run the following command:

- On Windows:

```
op-database-product-upgrade.bat preupgrade "<op_schema_owner_password>" ""
```

The second parameter is not used, but must be included in the command. Use `""`.

- On Linux:

```
./op-database-product-upgrade.sh preupgrade '<op_schema_owner_password>'
```

Note: Quotation marks are required around a password only if the password contains special characters. See [“Special characters in passwords”](#) on page 12.

6. Verify that the script completed successfully.

Look for the following message: `Status : Success` or a return code of 0.

You can also check the log file, `op-validate-dba-pre-upgrade.log`.

What to do next

Run the script to upgrade the database schema.

Upgrading the schema (Oracle)

Run the script to upgrade the database schema.

Before you begin

- The Oracle database server is running. All other OpenPages servers are stopped.
- The `JAVA_HOME` system variable is defined.
- `apache-ant-1.8.1` is deployed to `/OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/UPGRADE_SCRIPTS`
- The `ORACLE_HOME` system variable is defined.
- The `op-database-product-upgrade.sh|.bat` preupgrade script completed successfully.

Procedure

1. Log on to the Oracle database server computer as the OpenPages application user, `opuser`.
2. Go to the `/OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/UPGRADE_SCRIPTS` directory.
3. Verify that you have execute permission on the scripts in the `UPGRADE_SCRIPTS` directory and its subdirectories.
4. Open the `sql-wrapper.sql` file. Verify that the values are suitable for your environment.
5. Run the database upgrade script:

If you are migrating from 7.3.x

Run the following command:

- On Windows:

```
op-database-product-upgrade.bat upgrade "<op_schema_owner_password>"  
"<workflow_password>"
```

- On Linux:

```
./op-database-product-upgrade.sh upgrade '<op_schema_owner_password>'  
'<workflow_password>'
```

You need to provide the Fujitsu workflow user password to complete the upgrade. The database upgrade scripts remove any references to the Fujitsu workflow schema that are contained within the OpenPages schema, and then the scripts remove the workflow schema.

If you are migrating from 7.4 or later

Run the following command:

The second parameter is not used, but must be provided. Use a dummy value, such as `xxx`.

- On Windows:

```
op-database-product-upgrade.bat upgrade "<op_schema_owner_password>" xxx
```

- On Linux:

```
./op-database-product-upgrade.sh upgrade '<op_schema_owner_password>' xxx
```

Note: Quotation marks are required around a password only if the password contains special characters. See [“Special characters in passwords” on page 12](#).

6. Verify that the return code is 0, indicating success.

You can also check the log file, `op-database-product-upgrade.log`.

What to do next

Ask your database administrator to run the post-upgrade DBA script.

Running the post-upgrade DBA script (Oracle)

Ask your database administrator to run the post-upgrade script. Or, if you have SYSDBA privileges, you can run the script.

Before you begin

- The Oracle database server is running. All other OpenPages servers are stopped.
- The JAVA_HOME system variable is defined.
- `apache-ant-1.8.1` is deployed to `/OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/UPGRADE_SCRIPTS`
- The ORACLE_HOME system variable is defined.
- The `op-database-product-upgrade.sh | .bat` upgrade script completed successfully.

About this task

Run the following script: `op-database-dba-upgrade.sh | .bat`. The script uses the parameters defined in the `sql-wrapper.sql` file.

Procedure

1. Log on to the Oracle database server computer as a database administrator (DBA).
2. Locate the scripts that are required.

If you are a database administrator, get the scripts from your OpenPages team.

Or, you can get the scripts from the `/OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/UPGRADE_SCRIPTS` directory.

3. Verify that you have execute permission on the scripts.
4. Open the `sql-wrapper.sql` file. Verify that the values are suitable for your environment. In the `opx_oracle_dba_user` parameter, enter a user that has SYSDBA privileges, for example SYS.
5. Run the following command:

- On Windows:

```
op-database-dba-upgrade.bat post "<sysdba_password>"
```

- On Linux:

```
./op-database-dba-upgrade.sh post '<sysdba_password>'
```

Note: Quotation marks are required around a password only if the password contains special characters. See [“Special characters in passwords” on page 12](#).

6. Verify that the return code is 0, indicating success.

You can also check the log file: `op-database-dba-post-upgrade.log`.

What to do next

Validate the post-upgrade DBA step.

Validating the post-upgrade DBA step (Oracle)

Run the script to validate the post-upgrade DBA steps.

Before you begin

- The Oracle database server is running. All other OpenPages servers are stopped.
- The JAVA_HOME system variable is defined.
- apache-ant-1.8.1 has been deployed to /OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/UPGRADE_SCRIPTS
- The ORACLE_HOME system variable is defined.

Procedure

1. Log on to the Oracle database server computer as the OpenPages application user, opuser.
2. Go to the /OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/UPGRADE_SCRIPTS directory.
3. Verify that you have execute permission on the scripts.
4. Open the sql-wrapper.sql file. Verify that the values are suitable for your environment.
5. Run the following command:

- On Windows:

```
op-database-product-upgrade.bat postdba "<op_schema_owner_password>" ""
```

The second parameter is not used, but must be included in the command. Use "".

- On Linux:

```
./op-database-product-upgrade.sh postdba '<op_schema_owner_password>'
```

Note: Quotation marks are required around a password only if the password contains special characters. See [“Special characters in passwords” on page 12](#).

6. Verify that the script completed successfully.

Look for the following message: Status:Success or a return code of 0.

You can also check the log file, op-validate-dba-post-upgrade.log.

7. Remove the passwords from the sql-wrapper.sql file for security purposes.

Results

The OpenPages database schema is upgraded.

What to do next

Migrate the application data from your previous version of OpenPages. See [“Migrate files” on page 201](#).

Updating the location of the openpages-storage directory (Oracle)

In the database, update the location of the **openpages-storage** directory.

If you are using Microsoft Windows, you can also use this procedure to change the storage type from LFS to UNC.

Before you begin

Stop the IBM OpenPages with Watson services if they are running.

Procedure

1. Log on to the target environment as a user with administrative permissions. You can use any system with access to SQL*Plus that can connect to the database server.
2. Open a command or shell window.
3. Locate the `update-storage.sql` script.

The script is stored in the following directories. You can use the script in either location.

- `/OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/INSTALL_SCRIPTS` directory.
 - `/OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/UPGRADE_SCRIPTS`
4. Run the `update-storage.sql` script to update the `openpages-storage` directory location in the database:

```
sqlplus /nolog @sql-wrapper.sql update-storage.sql <log_file> <oracle_tns_alias>  
<op_db_user> <op_db_password> <storage_type> <storage_server_name> <host_name>  
<os_type> <path_or UNC_name>
```

Table 67. Parameters in the `update-storage.sql` script (Oracle)

Parameter	Description
<log_file>	The name of the log file that the script will create and write information to.
<oracle_tns_alias>	The database alias for the OpenPages database instance, as set during the Oracle database installation.
<op_db_user>	The user name for accessing the OpenPages database.
<op_db_password>	The password for accessing the OpenPages database. If the password contains special characters, surround the password in quotation marks: <ul style="list-style-type: none">• Windows: "password"• Linux: 'password'
<storage_type>	The type of file storage to be used. Valid values are: <ul style="list-style-type: none">• LFS (local file system)• UNC (Universal Naming Convention) - for Windows only Note: After you move from LFS to UNC, you cannot go back to using LFS.
<storage_server_name>	The name of the storage server.
<host_name>	The host name of the machine.
<os_type>	The type of operating system. Valid values are: <ul style="list-style-type: none">• Windows• Unix
<path_or UNC_name>	The file path or UNC of the storage location. If the path contains backslashes, wrap the path in single quotation marks.

Examples

- LFS

Windows

```
sqlplus /nolog @sql-wrapper.sql update-storage output.log OP openpage "password"  
LFS eng11 eng11 Windows 'C:\IBM\OpenPages\openpages-storage'
```

Linux

```
sqlplus /nolog @sql-wrapper.sql update-storage /home/op/upd-storage-output.log  
op openpage 'password' LFS eng11 eng11 Unix /usr/opdata/openpages-storage
```

- UNC

Windows

In the following example, openpages-storage is the UNC share name of the storage location. The openpages-storage location is accessible to all horizontal cluster members as \testserver1\openpages-storage.

```
sqlplus /nolog @sql-wrapper.sql update-storage c:\temp\update-storage-output.log  
op openpages "password" UNC eng11 eng11 Windows openpages-storage
```

Update the database connection information (Oracle)

After you restore and upgrade the source database, update the connection information that is stored in the database.

If you are using the database server from your source environment, you do not need to do these tasks.

- Update the `aurora.properties` with the URL of the database server. See [“Updating the aurora.properties file \(Oracle\)”](#) on page 260.
- Update the data source connection in WebSphere Liberty. See [“Updating the data source connection in WebSphere Liberty \(Oracle\)”](#) on page 261.
- Update IBM Cognos Configuration with the connection information for your Oracle database server. See [“Updating the Cognos content store information \(Oracle\)”](#) on page 261.
- Configure Cognos with the connection information for the OpenPages data source. See [“Updating the connection to the OpenPages database for Cognos \(Oracle\)”](#) on page 263.
- Update the search server settings in OpenPages. See [“Updating search server settings”](#) on page 208.
- Update the database connection information for the search server. See [“Updating the database connection information for the search server \(Oracle\)”](#) on page 263.

Updating the aurora.properties file (Oracle)

Update the database server URL in the `aurora.properties` file.

Procedure

1. Open a command or shell window and go to the `<OP_HOME>/aurora/conf` directory.
2. Make a backup copy of the `aurora.properties` file.
3. Open the `aurora.properties` file in a text editor.
4. Search the file for the string `database.URL`.
5. Change the value that follows the equal sign to the URL of your database server.

Use the following format:

```
jdbc\:oracle\:thin\:@//<host_name>:<port>/<SID>
```

Where:

- `<host_name>` is the name of the database server, such as `eng11`.
- `<port>` is the database port number, such as `1521`.

- `<SID>` is the Oracle System Identifier, such as OP. If you are using a pluggable database, use the service name of the pluggable database, not the container database.
6. Save your changes and close the editor.

Updating the data source connection in WebSphere Liberty (Oracle)

Update IBM WebSphere Liberty with the database server connection information.

Procedure

1. Log on to the application server.
2. Stop the application servers.
For more information, see [“Stopping application servers” on page 311](#).
3. Open the following file in a text editor: `<OP_HOME>/wlp-user/servers/<server_name>Server<#>/bootstrap.properties`
Where `<server_name>` is the name of the application server.
4. Update the database server connection information.

```
op.ora.databaseName=<db_name>
op.ora.portNumber=<db_port>
op.jdbc.host=<host_name>
```

- `<host_name>` is the name of the database server, such as eng11.
- `<db_port>` is the database port number, such as 1521.
- `<db_name>` is the name of the OpenPages database, for example OP.

Note: If you are using Oracle PDB, specify the name of the container database.

5. Save your changes.
6. Repeat these steps on each application server.
7. Restart the application servers.
For more information, see [“Starting application servers” on page 309](#).

Updating the Cognos content store information (Oracle)

Update IBM Cognos Configuration with the connection information for your Oracle database server.

Procedure

1. Start the IBM Cognos services and the IBM OpenPages with Watson services.
2. Log on to the reporting server as a user with administrator privileges.
3. Start Cognos Configuration.
 - On Windows computers, click **Start > IBM Cognos Analytics > IBM Cognos Configuration**.
 - On Linux, go to the `<COGNOS_HOME>/bin64` directory, type `./cogconfig.sh`, and press Enter.
4. Update the database connection information for the content store.
 - a) Under **Local Configuration > Environment > Data Access > Content Manager**, click **IBM Cognos Content Store**.
 - b) Use the following tables to update the database connection information.

Table 68. Content store property settings for Oracle databases

Property name	Property value
Database server and port number	Type the name of the database server and the listener port that is used for the database instance.
User ID and password	Click the value field and then click the pencil icon. In the Value - User ID and password field, enter the appropriate values for the user and password for the content store database.
SID	Type the SID of the database instance.

Table 69. Content store property settings for Oracle databases (Advanced) (Oracle PDB or RAC databases)

Property name	Property value
Database server and port number	Type the name of the database server and the listener port that is used for the database instance.
User ID and password	Click the Value field and then click the pencil icon. In the Value - User ID and password field, enter the appropriate values for the content store database.
Database specifier	Type the database specifier string in the following format with no carriage returns: <ul style="list-style-type: none"> Oracle PDB databases <pre>(description=(address=(host=<server_name>)(protocol=tcp)(port=<port>)(connect_data(service_name=<service_name>)))</pre> <p>Where <service_name> is the service name of the pluggable database.</p> <p>For example, //corpserv1:1522/OP</p> Oracle RAC databases <pre>(description=(address=(host=<server_name>)(protocol=tcp)(port=<port>)(connect_data(service_name=<service_name>)))</pre>

- Click **File > Save**.
- Right-click the content store database connection and click **Test**.
- Stop the IBM Cognos services and the IBM OpenPages with Watson services.

Updating the database connection information for the search server (Oracle)

Update the connection information that the search server uses to access the database server.

Procedure

1. Log on to the search server as a user with administrative privileges.
2. Go to `<SEARCH_HOME>/opsearchtools/`.
3. Open the `openpages_search.properties` file in a text editor.
4. Modify the database connection properties with the values for the database server.

Use the following examples as a guide.

```
# Database connectivity information
OPSearchTool.DatabaseType = Oracle
OPSearchTool.DatabaseHostName = OP-WIN-ORACLE
OPSearchTool.DatabasePort = 1521
OPSearchTool.DatabaseName = OP
OPSearchTool.DatabaseUserID = openpages_db_user_id
OPSearchTool.DatabasePassword = openpages_db_password
```

If you are using a pluggable database, set `OPSearchTool.DatabaseName` to the name of the pluggable database.

Updating the `deploy.properties` file

Update the database server host name and the database credentials in the `deploy.properties` file.

Procedure

1. If the installation app is running, log out.
2. Open a command or shell window and go to the `<installation_server_home>/src/deployment/<deployment-name>` directory.
3. Make a backup copy of the `deploy.properties` file.
4. Open the `deploy.properties` file in a text editor.
5. Go to the database server section.
6. Update the following parameters with the values for your production database server.

- `host`
- `db_port`
- `dba_username`
- `dba_password`

Note: Do not use quotation marks around the password, even if it contains special characters.

- `op_db_username`
- `op_db_password`

Note: Do not use quotation marks around the password, even if it contains special characters.

7. Save your changes and close the editor.

Updating the connection to the OpenPages database for Cognos (Oracle)

If you are using new hardware for the database server, update Cognos with the database connection information for the OpenPages database.

Also, do this procedure if the following conditions apply to you:

- The Oracle database alias that you used when you installed OpenPages in your target environment is different from the alias that you used in your source environment

- You imported a 7.1.x, 7.2.x, or 7.3.x database

You need to update the connection string to use the **Oracle Cognos DB Alias** that you configured on the **Database Server** card.

Procedure

1. Start the IBM Cognos services.
2. Log on to IBM Cognos Analytics as a user with administrative privileges..
 - In the Task Focused UI, click **Analytics**.
 - Or, go to the following URL: `http://<hostname>/ibmcognos/bi`
Where <hostname> is the name of the Cognos server.
3. Click **Manage** > **Administration Console** to launch the **IBM Cognos Administration** page.
4. Click the **Configuration** tab.
5. Click **OpenPages DataSource** under **Data Source Connections**.
6. Click **Actions** > **Set Properties - OpenPages DataSource**.
7. Update the database connection string:
 - a) Click the **Connection** tab.
 - b) Click the pencil icon next to the **Connection String** box to edit the field.
 - c) Update the **SQL*Net connect string**. Type the TNS alias or the service name of the OpenPages database in your upgraded environment.

Note: If you are using a pluggable database, use the service name of the pluggable database.
 - d) Click **Test the connection**.
 - e) Click **Test**. Verify that the test is successful. Click **Close**.
 - f) Click **Close**.
 - g) Click **OK**.
8. Click **OK**.
9. Click **Oracle Native Driver** under **Data Source Connections**.
10. Click **Actions** > **Set Properties - Oracle Native Driver**.
11. Update the database connection string:
 - a) Click the **Connection** tab.
 - b) Click the pencil icon next to the **Connection String** box to edit the field.
 - c) Update the **SQL*Net connect string**. Type the TNS alias or the service name of the OpenPages database in your upgraded environment.

Note: If you are using a pluggable database, use the service name of the pluggable database.
 - d) Click **Test the connection**.
 - e) Click **Test**. Verify that the test is successful. Click **Close**.
 - f) Click **Close**.
 - g) Click **OK**.
12. Click **OK**.

Oracle Transparent Data Encryption for migration customers

You can use Oracle Transparent Data Encryption (TDE) to encrypt the OpenPages and Cognos table spaces in the OpenPages database.

This task is optional.

For information about how to implement TDE on an existing OpenPages database, see the *IBM OpenPages with Watson Administrator's Guide*.

For more information about TDE, refer to the Oracle documentation, such as the [Oracle Database Advance Security Guide](#).

Chapter 10. OpenPages solutions post-migration tasks

If you use IBM OpenPages solutions, complete the following post-migration tasks.

Note: Version 8.2 introduces a new solution, IBM OpenPages Business Continuity Management (BCM), which is available in fresh installations only.

Version 8.2 also introduces significant enhancements to IBM OpenPages Regulatory Compliance Management (RCM). The updated solution is available in fresh installations only. If you want to update RCM to 8.2, contact IBM OpenPages Support.

If you upgraded from 8.1.0.x

- If you use IBM OpenPages Model Risk Governance and you want to use IBM OpenScale, load the required fields and field groups. See [“Updating MRG”](#) on page 275.
- If you use IBM OpenPages Third Party Risk Management (previously called OpenPages Third Party Risk Management), load the new dashboard.
- If you want to use the sample workflows that are provided with OpenPages, see [“Loading the sample workflows”](#) on page 277.
- Back up your solutions reports and then import the solutions report package to update them.

For more information, see [“Importing the solutions report packages”](#) on page 274.

If you upgraded from 8.0.0.2 or a later 8.0.0.x release

- If you use IBM OpenPages Internal Audit Management, load the timesheet helpers.

If you loaded the timesheet helpers in 8.0.0.2 or a later 8.0.0.x fix pack, reload them to get the latest updates. See [“Updating the timesheet helpers”](#) on page 273

If you did not load the timesheet helpers in 8.0.0.x, load them to get the new helpers and reports. See [“Loading the timesheet helpers”](#) on page 271.

When you are ready to start using the new timesheet entry helper, disable the old one. See [“Disabling the old timesheet entry helper”](#) on page 273.

- If you use IBM OpenPages Model Risk Governance and you want to use IBM OpenScale, load the required fields and field groups. See [“Updating MRG”](#) on page 275.
- If you use IBM OpenPages Third Party Risk Management (previously called OpenPages Third Party Risk Management), load the new dashboard.
- If you want to use the sample workflows that are provided with OpenPages, see [“Loading the sample workflows”](#) on page 277.
- Back up your solutions reports and then import the solutions report package to update them.


For more information, see [“Importing the solutions report packages”](#) on page 274.

If you upgraded from 7.4 or 8.0.0.1

- If you use IBM OpenPages Internal Audit Management, load the new timesheet helpers and reports. See [“Loading the timesheet helpers”](#) on page 271.

When you are ready to start using the new timesheet entry helper, disable the old one. See [“Disabling the old timesheet entry helper”](#) on page 273.

- If you use IBM OpenPages Model Risk Governance and you want to use IBM OpenScale, load the required fields and field groups. See [“Updating MRG”](#) on page 275.
- If you use IBM OpenPages Third Party Risk Management (previously called OpenPages Third Party Risk Management), load the new dashboard.

- If you want to use the sample workflows that are provided with OpenPages, go to  > **Solution Configuration > Workflows**. Review the workflows. Ensure that your environment has the object types, field groups, and fields that are required by the workflow. When you're ready to use a workflow, enable it.
- Back up your solutions reports and then import the solutions report package to update them.

For more information, see [“Importing the solutions report packages” on page 274](#).

If you upgraded from 7.3.x

- Configure email notifications for questionnaire assessments. See [“Configuring email notifications for questionnaire assessment triggers” on page 268](#).
- Update profiles that use the RCSA Alignment helper for IBM OpenPages Operational Risk Management. See [“Updating the RCSA Alignment helper in profiles” on page 269](#).
- Remove any scenario analysis triggers that you do not need. See [“Removing the Scenario Analysis triggers” on page 269](#).
- If you loaded the Scenario Analysis fields for IBM OpenPages Operational Risk Management, update the field dependencies. See [“Updating Scenario Analysis field dependencies” on page 270](#).
- If you did not previously load the approval app or Loss Event Entry or RCM schemas, then you can load those schemas now.
- Back up your solutions reports and then import the solutions report package to update them.

For more information, see [“Importing the solutions report packages” on page 274](#).

Configuring email notifications for questionnaire assessment triggers

If you migrated from version 7.3.x, follow these steps to update the trigger definitions to send email notifications when a questionnaire assessment is launched.

Before you begin

To do this procedure, you must have the **OpenPages Platform 3** profile associated with your user name.

About this task

The behavior of email notifications for questionnaire assessments has changed.

In IBM OpenPages with Watson 7.3.x, email notifications were sent when a questionnaire assessment was launched, regardless of the value of the `sendemail` attribute.

If you want emails to be sent when a questionnaire assessment is launched, update the `OPLC-QuestionnaireAssessment.xml` file. Set the `sendemail` attribute in the default settings section to `true`.

Procedure

1. Log in to IBM OpenPages with Watson and go to the Standard UI.
2. Click **Administration > Manage System Files > SysXMLDocument**.
3. Click **TriggerConfigFiles**, and then click **OPLC-QuestionnaireAssessment.xml**.
4. Click **View file** and save the file.
5. Open the `OPLC-QuestionnaireAssessment.xml` file in a text editor.
6. Look for the `<!-- defaultsettings used when object is being created -->` section.
7. Look for the following line:

```
<attribute name="sendemail" value="false"/>
```

8. Change the value to `true`.
9. Check out the `OPLC-QuestionnaireAssessment.xml` file.
10. Upload and check in the `OPLC-QuestionnaireAssessment.xml` file that you edited.
11. Restart all OpenPages servers.

For more information, see Chapter 12, “Starting and stopping servers,” on page 309.

Updating the RCSA Alignment helper in profiles

If you use IBM OpenPages Operational Risk Management, update the profiles that use the RCSA Alignment helper. Do this task to enable users to launch the RCSA Alignment helper from Filtered List Views in addition to Detail views.

Procedure

1. Log in to IBM OpenPages with Watson and go to the Standard UI.
2. Select **Administration > Profiles > *Profile_name***
3. Click **Object Types > RiskAssessment**.
4. Click **Navigation Views > Filtered List**.
5. Click **Included Object Fields**.
6. Click **Include**, select **RCSA Process Alignment helper**, and then click **Include**.
7. Test the helper.
 - a) Switch to the profile that you modified in step 2.
 - b) Select **Assessments > Risk Assessments**.
 - c) Locate a risk assessment that has the status **Awaiting Assessment**.
 - d) In the **RCSA Process Alignment helper** column, click **RCSA Alignment helper**.The helper is displayed.

Removing the Scenario Analysis triggers

If you migrated IBM OpenPages with Watson, you might need to remove some Scenario Analysis triggers that you do not need.

About this task

Do this task if the following statements are true.

- You have not installed the Scenario Analysis with Quantitative Data feature for IBM OpenPages Operational Risk Management
- You have installed the approval app, or you have set up a new lifecycle that uses the Loss Event, Control, or Issue object types

If you do not remove the triggers, users might encounter validation errors when they create or update Scenario Analysis objects.

To perform this procedure, you must have the **OpenPages Platform 3** profile associated with your user name.

Procedure

1. Log in to IBM OpenPages with Watson and go to the Standard UI.
2. Click **Administration > Manage System Files > SysXMLDocument**.
3. Click **TriggerConfigFiles**, and then click **openpages-solutions.xml**.
4. Click **View file** and save the file.
5. Open the `openpages-solutions.xml` in a text editor.

6. Locate the text `<!-- BEGIN: Scenario Completion Triggers -->`
7. Delete the following lines, and then save the file.

```
<!-- BEGIN: Scenario Completion Triggers -->
<trigger name="Scenario Completion Update" operation="update.object"
  type="CUSTOM"
  classname="com.openpages.ext.solutions.triggers.ScenarioCompletionTrigger"
  position="POST" objecttype="ScenarioAnalysis">
  <attribute name="content.type" value="ScenarioAnalysis" />
  <actions>
    <action type="CUSTOM"
      classname="com.openpages.ext.solutions.triggers.ScenarioCompletionTriggerAction">
    </action>
  </actions>
</trigger>
<trigger name="Scenario Completion Create" operation="create.object"
  type="CUSTOM"
  classname="com.openpages.ext.solutions.triggers.ScenarioCompletionTrigger"
  position="POST" objecttype="ScenarioAnalysis">
  <attribute name="content.type" value="ScenarioAnalysis" />
  <actions>
    <action type="CUSTOM"
      classname="com.openpages.ext.solutions.triggers.ScenarioCompletionTriggerAction">
    </action>
  </actions>
</trigger>
<!-- END: Scenario Completion Triggers -->
```

8. Check out the `openpages-solutions.xml` file.
9. Upload and check in the `openpages-solutions.xml` file that you edited.
10. Restart all OpenPages servers.

Updating Scenario Analysis field dependencies

If you migrated IBM OpenPages with Watson and you loaded the Scenario Analysis fields for IBM OpenPages Operational Risk Management, you need to update the field dependencies.

About this task

Do this task only if you loaded the Scenario Analysis fields when you upgraded, migrated, or installed a fix pack for a version prior to 8.1. For information about loading the fields, see [Loading the scenario analysis fields](#).

Procedure

1. Copy the `ScenAn-field-dependency-op-config.xml` file from the installation media to the administrative application server.

The file is located in the `/OP_<version>_Main/OP_<version>_Configuration/Modules/Upgrade/ORM/loader-data` directory.

If the file already exists, overwrite it.

2. Open a command line.

If you are using Microsoft Windows, open a command prompt with the **Run as administrator** option.

3. Go to the `<OP_HOME>/bin` directory.
4. Run the following command to load the files.

Replace `<loader-file-path>` with the location of the `ScenAn-field-dependency-op-config.xml` file.

```
ObjectManager.cmd|sh l c <OpenPages Administrator user>
  <OpenPages Administrator password> <loader-file-path>
  ScenAn-field-dependency
```

5. If you encounter any errors, review the log file, `<loader-file-path>/ObjectManager.log`.

6. Restart all OpenPages servers.

For more information, see [“Starting application servers”](#) on page 309.

7. Regenerate the reporting framework.

For more information, see [“Regenerating the reporting framework”](#) on page 214.

Note: Do this task after completing all other post-upgrade or post-migration tasks.

Loading the timesheet helpers

Do this procedure to load the timesheet helpers for the IBM OpenPages Internal Audit Management solution.

8.0.0.2 and later

If you upgraded or migrated from 8.0.0.2 or later and you loaded the timesheet helpers in 8.0.x, reload them. The timesheet helpers and reports have been updated. See [“Updating the timesheet helpers”](#) on page 273.

If you upgraded or migrated from 8.0.0.2 or later and you did not load the timesheet helpers, load the helpers to install and enable them. See [“Loading the timesheet helpers”](#) on page 271.

8.0.0.1 and earlier

If you upgraded or migrated from 8.0.0.1 or earlier, load the timesheet helpers to install and enable them. See [“Loading the timesheet helpers”](#) on page 271.

Loading the timesheet helpers

If you use the IBM OpenPages Internal Audit Management solution, load the timesheet helpers and reports.

About this task

You run a script to load the new Timesheet Entry Helper and the Timesheet Approval Helper. The script does not remove the old helpers. Your users can continue to use the old helpers.

Procedure

1. Log on to the admin application server as a user with administrative privileges.
2. Open a command prompt or shell.
3. Go to the `/OP_<version>_Main/OP_<version>_Configuration/Modules/Upgrade/IAM/` directory.
4. Open the `schema_loader_modules_properties.sh | .bat` file in a text editor.

Update the following properties:

```
OBJMGR_HOME=<full_path_to_OP_HOME/bin>
PATCH_LOADER_DATA=<full_path_to_the_IAM_directory>
OPXUserName=<Super_Administrator_user_name>
OPXUserPassword=<Super_Administrator_password>
```

Tip: In the installation app, the super administrator is set on the **Database Server** card in the **OP Admin Username** field. You can also find the user name in the `deploy.properties` file in the `op_admin_username` parameter.

Save your changes and close the file.

For example:

- Windows:

```
OBJMGR_HOME=C:\OP\OpenPages\bin
PATCH_LOADER_DATA=C:\OP_<version>_Main\OP_<version>_Configuration\Modules\Upgrade\IAM
```

```
OPXUserName=OpenPagesAdministrator
OPXUserPassword=password
```

- Linux:

```
OBJMGR_HOME=/home/opuser/OP/OpenPages/bin
PATCH_LOADER_DATA=/home/OP_<version>_Main/OP_<version>_Configuration/Modules/Upgrade/IAM
OPXUserName=OpenPagesAdministrator
OPXUserPassword=password
```

5. Run the following script:

- Windows:

```
openpages-modules-loader-data.bat
```

- Linux:

```
./openpages-modules-loader-data.sh
```

6. Edit the `schema_loader_modules_properties.sh` | `.bat` file. Set the `OPXUserPassword` property to `****`, for security reasons.

7. Log on to the active reporting server as a user with administrative privileges.

8. Open a command prompt or shell.

9. Go to the `<CC_HOME>/temp/bin` directory.

10. Run the following script to import the timesheet helper reports:

- Windows:

```
importIAMReports.bat <op_admin_username> <op_admin_password>
```

- Linux:

```
./importIAMReports.sh <op_admin_username> <op_admin_password>
```

Replace `<op_admin_user>` and `<op_admin_password>` with the user name and password of the OpenPages super administrator.

11. Configure the timesheet helpers.

For more information, see the *IBM OpenPages with Watson Administrator's Guide*.

12. When you are ready to roll out the new helpers to your users, update profiles to use the new timesheet helpers and dashboards.

Update the tabs and reports on the home page.

- Add **Timesheet Entry Helper** and **Timesheet Approval Helper**.
- Remove **Timesheet Entry** and **Administration Timesheet Entry**.

For more information, see the *IBM OpenPages with Watson Administrator's Guide*.

Update the **My Reports > OpenPages V6 > Audit Management Reports** list.

- Add the new reports: **Auditor Utilization Dashboard**, **Auditor Timesheet Dashboard**, and **Pending Timesheet Approvals Dashboard**.
- Remove any reports that you no longer need.

For more information, see the *IBM OpenPages with Watson Administrator's Guide*.

13. Optional: Disable the old **Timesheet Entry** helper.

See [“Disabling the old timesheet entry helper”](#) on page 273.

Updating the timesheet helpers

If you use the IBM OpenPages Internal Audit Management solution, update the timesheet helpers.

Procedure

1. Log on to the admin application server as a user with administrative privileges.
2. Open a command prompt or shell.
3. Go to the `/OP_<version>_Main/OP_<version>_Configuration/Modules/Upgrade/IAM/` directory.
4. Open the `schema_loader_modules_properties.sh|.bat` file in a text editor.

Update the following properties:

```
OBJMGR_HOME=<full_path_to_OP_HOME/bin>
PATCH_LOADER_DATA=<full_path_to_the_IAM_directory>
OPXUserName=<Super_Administrator_user_name>
OPXUserPassword=<Super_Administrator_password>
```

Tip: In the installation app, the super administrator is set on the **Database Server** card in the **OP Admin Username** field. You can also find the user name in the `deploy.properties` file in the `op_admin_username` parameter.

Save your changes and close the file.

For example:

- Windows:

```
OBJMGR_HOME=C:\OP\OpenPages\bin
PATCH_LOADER_DATA=C:\OP_<version>_Main\OP_<version>_Configuration\Modules\Upgrade\IAM
OPXUserName=OpenPagesAdministrator
OPXUserPassword=password
```

- Linux:

```
OBJMGR_HOME=/home/opuser/OP/OpenPages/bin
PATCH_LOADER_DATA=/home/OP_<version>_Main/OP_<version>_Configuration\Modules/Upgrade/IAM
OPXUserName=OpenPagesAdministrator
OPXUserPassword=password
```

5. Run the following script:

- Windows:

```
openpages-modules-upgrade-loader-data.bat
```

- Linux:

```
./openpages-modules-upgrade-loader-data.sh
```

6. Edit the `schema_loader_modules_properties.sh|.bat` file. Set the `OPXUserPassword` property to `***`, for security reasons.
7. Optional: If the old timesheet helpers are enabled, disable them.

Disabling the old timesheet entry helper

When you are ready to begin using the new Timesheet Entry Helper, disable the old Timesheet Entry helper.

About this task

In UAT and production environments, disable the old helper before your users begin to use the new Timesheet Entry Helper.

The script does not disable the Administration Timesheet Entry helper.

Procedure

1. Log on to the admin application server as a user with administrative privileges.
2. Open a command prompt or shell.
3. Go to the /OP_<version>_Main/OP_<version>_Configuration/Modules/Upgrade/IAM/ directory.
4. Open the schema_loader_modules_properties.sh | .bat file in a text editor.

Update the following properties:

```
OBJMGR_HOME=<full_path_to_OP_HOME/bin>
PATCH_LOADER_DATA=<full_path_to_the_IAM_directory>
OPXUserName=<Super_Administrator_user_name>
OPXUserPassword=<Super_Administrator_password>
```

Tip: In the installation app, the super administrator is set on the **Database Server** card in the **OP Admin Username** field. You can also find the user name in the deploy.properties file in the op_admin_username parameter.

For example:

- Windows:

```
OBJMGR_HOME=C:\OP\OpenPages\bin
PATCH_LOADER_DATA=C:\OP\OpenPages\Module\loaderdata\IAM
OPXUserName=OpenPagesAdministrator
OPXUserPassword=password
```

- Linux:

```
OBJMGR_HOME=/home/opuser/OP/OpenPages/bin
PATCH_LOADER_DATA=/home/opuser/OP/OpenPages/Module/loaderdata/IAM
OPXUserName=OpenPagesAdministrator
OPXUserPassword=password
```

5. Run the following script to disable the old timesheet entry helper:

- Windows:

```
disable-old-timesheet-entry-helper.bat
```

- Linux:

```
./disable-old-timesheet-entry-helper.sh
```

6. Edit the schema_loader_modules_properties.sh | .bat file. Set the OPXUserPassword property to ****, for security reasons.

What to do next

Update profiles to remove the old helper from the Home page and from the **My Reports** list.

Importing the solutions report packages

After you upgrade IBM OpenPages with Watson, import the solutions reports to update them.

For more information about importing content, see the *Cognos Analytics Administration and Security Guide*.

Procedure

1. Back up the following file if it exists: <COGNOS_HOME>/deployment/OpenPages_Solutions_V6.zip.

2. Get the latest version of the solutions report package.
 - a) Locate the solutions package file for the database that you are using. The file is located in the following directory:
 - IBM Db2: OP_<version>_Non_Embedded/OP_<version>_Configuration/Modules/Upgrade/ORM/DB2/OpenPages_Solutions_V6.zip
 - Oracle: OP_<version>_Non_Embedded/OP_<version>_Configuration/Modules/Upgrade/ORM/Oracle/OpenPages_Solutions_V6.zip
 - b) Copy the OpenPages_Solutions_V6.zip file to the following directory on the Cognos server: <COGNOS_HOME>/deployment. Overwrite the existing file.
3. From a browser, log on to the IBM Cognos Analytics.

By default, the URL is `http://<hostname>:<port>/ibmcognos/bi`

Where <hostname> is the name of the Cognos server and <port> is the Cognos gateway port number (80 by default).
4. Click **Manage > Administration Console** to open the **IBM Cognos Administration** page.
5. Click the **Configuration** tab and click **Content Administration**.

Tip: To access this area in IBM Cognos Administration, you must have the required permissions for the **Administration** secured feature.
6. On the toolbar, click **New Import**.
7. From the **Deployment archive** list, select **OpenPages_Solutions_v6**.
8. Click **Next**.
9. Type a unique name, an optional description, and a screen tip for the deployment archive, select the folder where you want to save it, and then click **Next**.
10. In the **Public folders, directory and library content** box, select **OpenPages_Solutions_v6**, and then click **Next**.
11. On the **Specify the general options** page, accept the default options and click **Next**.
12. On the **Review the summary** page, review the settings and click **Next**.
13. On the **Select an action page**, click **Finish**.
14. Click **Replace the existing entry**, and then click **OK**.
15. On the **Run with options** page, click **Run**.
16. On the **IBM Cognos software** page, click **OK**.
17. To view the imported packages and reports, click the **Home** icon, and select the folder where you imported them.

Results

You can now open the OpenPages reports in Cognos Analytics.

Updating MRG

If you use IBM OpenPages Model Risk Governance, do the following steps to update the solution.

About this task

Do these steps to enable integration between MRG and IBM Watson® OpenScale. The loader file adds the fields and field groups that are required for the integration.

Procedure

1. Copy the MRG_OpenScale_Fields-op-config.xml from the installation media to the admin application server.

The file is located in the /OP_<version>_Main/OP_<version>_Configuration/Modules/MRG/OpenScale directory.

2. Open a command line.

If you are using Microsoft Windows, open a command prompt with the **Run as Administrator** option.

3. Go to the <OP_HOME>/bin directory.
4. Run the following command to load the files.

Replace <loader-file-path> with the location of the MRG_OpenScale_Fields-op-config.xml file.

```
ObjectManager.cmd|sh 1 c <OpenPages Administrator user> <OpenPages Administrator password>
<loader-file-path> MRG_OpenScale_Fields
```

If you encounter any errors, review the log file, <loader-file-path>/ObjectManager.log.

Updating TPRM

If you use IBM OpenPages Third Party Risk Management, do the following steps to update the solution.

About this task

Do these steps to load the new dashboards for IBM OpenPages Third Party Risk Management.

Procedure

1. Create a directory on the admin application server.
2. Copy the loader files from the installation media to the directory that you created on the admin application server.
 - a) Go to the OP_<version>_Main/OP_<version>_Configuration/Modules/Upgrade/loader-data/<version>_loader_data/loaderdata/VRM/ directory.
 - b) Copy the following files to the directory that you created in step 1.

```
dv-VRM-Vendor-Manager-op-config.xml
dv-app-string-keys-VRM-Vendor-Manager-op-config.xml
```

- c) Go to the OP_<version>_Main/OP_<version>_Configuration/Modules/Upgrade/loader-data/<version>_loader_data/loaderdata/Dashboards/locales/ directory.
- d) Copy the following files to the directory that you created in step 1.

```
/en_GB/dv-app-string-keys-VRM-Vendor-Manager-en_GB-op-config.xml
/en_US/dv-app-string-keys-VRM-Vendor-Manager-en_US-op-config.xml
/es_ES/dv-app-string-keys-VRM-Vendor-Manager-es_ES-op-config.xml
/fr_FR/dv-app-string-keys-VRM-Vendor-Manager-fr_FR-op-config.xml
/de_DE/dv-app-string-keys-VRM-Vendor-Manager-de_DE-op-config.xml
/it_IT/dv-app-string-keys-VRM-Vendor-Manager-it_IT-op-config.xml
/ja_JP/dv-app-string-keys-VRM-Vendor-Manager-ja_JP-op-config.xml
/pt_BR/dv-app-string-keys-VRM-Vendor-Manager-pt_BR-op-config.xml
/zh_CN/dv-app-string-keys-VRM-Vendor-Manager-zh_CN-op-config.xml
/zh_TW/dv-app-string-keys-VRM-Vendor-Manager-zh_TW-op-config.xml
```

3. Open a command line.

If you are using Microsoft Windows, open a command prompt with the **Run as Administrator** option.

4. Go to the <OP_HOME>/bin directory.
5. Run the following commands to load the files.

Replace <loader-file-path> with the directory that you created in step 1.

```
ObjectManager.cmd|sh 1 c <OpenPages Administrator user> <OpenPages Administrator password>
<loader-file-path> dv-VRM-Vendor-Manager
ObjectManager.cmd|sh 1 c <OpenPages Administrator user> <OpenPages Administrator password>
<loader-file-path> dv-app-string-keys-VRM-Vendor-Manager
ObjectManager.cmd|sh 1 c <OpenPages Administrator user> <OpenPages Administrator password>
```

```

<loader-file-path> dv-app-string-keys-VRM-Vendor-Manager-en_GB
ObjectManager.cmd|sh 1 c <OpenPages Administrator user> <OpenPages Administrator password>
<loader-file-path> dv-app-string-keys-VRM-Vendor-Manager-en_US
ObjectManager.cmd|sh 1 c <OpenPages Administrator user> <OpenPages Administrator password>
<loader-file-path> dv-app-string-keys-VRM-Vendor-Manager-es_ES
ObjectManager.cmd|sh 1 c <OpenPages Administrator user> <OpenPages Administrator password>
<loader-file-path> dv-app-string-keys-VRM-Vendor-Manager-fr_FR
ObjectManager.cmd|sh 1 c <OpenPages Administrator user> <OpenPages Administrator password>
<loader-file-path> dv-app-string-keys-VRM-Vendor-Manager-de_DE
ObjectManager.cmd|sh 1 c <OpenPages Administrator user> <OpenPages Administrator password>
<loader-file-path> dv-app-string-keys-VRM-Vendor-Manager-it_IT
ObjectManager.cmd|sh 1 c <OpenPages Administrator user> <OpenPages Administrator password>
<loader-file-path> dv-app-string-keys-VRM-Vendor-Manager-ja_JP
ObjectManager.cmd|sh 1 c <OpenPages Administrator user> <OpenPages Administrator password>
<loader-file-path> dv-app-string-keys-VRM-Vendor-Manager-pt_BR
ObjectManager.cmd|sh 1 c <OpenPages Administrator user> <OpenPages Administrator password>
<loader-file-path> dv-app-string-keys-VRM-Vendor-Manager-zh_CN
ObjectManager.cmd|sh 1 c <OpenPages Administrator user> <OpenPages Administrator password>
<loader-file-path> dv-app-string-keys-VRM-Vendor-Manager-zh_TW

```

If you encounter any errors, review the log file, `<loader-file-path>/ObjectManager.log`.

Loading the sample workflows

If you upgraded or migrated from 8.0.0.2 or later and you want to use the sample workflows, you need to load them.

About this task

When you upgrade or migrate from 8.0.0.2 or later, the sample workflows are not loaded automatically. Your system might have workflows with the same names as the samples. Or your environment might not have all of the object types, field groups, or fields that the sample workflows require.

Analyze the sample workflow files, and then load the workflows that you want to use.

Important: If you load a sample workflow that has the same name as a workflow in your environment, your workflow will be overwritten.

Procedure

1. Log in to the admin application server as a user with administrative privileges.
2. Copy the `OP_<version>_Main/OP_<version>_Configuration/Modules/Upgrade/loader-data/8200_loader_data/loaderdata/workflows` directory in the installation media to the following directory on the admin application server:
`<OP_HOME>/addon_module/loaderdata/`
3. Locate the loader file for the sample workflow that you want to load.
For example, if you want to load the Finding workflow, locate the `sample-workflow-Finding-op-config.xml` file.
4. Analyze the file. Verify that your environment has all of the object types, fields, and field groups that are required by the workflow.
5. Load the sample workflow:
 - a) Go to the `<OP_HOME>/bin` directory.
 - b) Run the following command:

```

ObjectManager.cmd|.sh 1 c <OpenPages Administrator user>
<OpenPages Administrator password> <OP_HOME>/addon_module/loaderdata/workflows
<loader_file>


```

For example, to load the Finding workflow, run the following command:

```

ObjectManager.cmd|.sh 1 c <OpenPages Administrator user>
<OpenPages Administrator password> <OP_HOME>/addon_module/loaderdata/workflows
sample-workflow-Finding

```

- c) After the loading process is complete, review the ObjectManager log.
- 6. Repeat steps 3-5 for each sample workflow that you want to load.
- 7. Log in to IBM OpenPages with Watson.
- 8. Click  > **Solution Configuration** > **Workflows**.
- 9. Review the sample workflows that you loaded.

Chapter 11. Fix packs

A fix pack is a cumulative collection of fixes that is made available between scheduled refresh packs, manufacturing refreshes, or releases. It is intended to allow you to move to a specific maintenance level.

Fix pack process overview

Follow these steps to install a fix pack.

Prepare

1. Update the installation server to the latest version. The latest version is provided in the most recent fix pack kit. For more information, see [“Update the installation server and agents” on page 47](#).
2. If you installed the agents on remote servers manually, update the agents. For more information, see [“Updating agents manually” on page 48](#).
3. Review the list of features and fixes in the fix pack. For more information, see the following documents:
 - [New Features Guide](#)
 - [OpenPages with Watson Fix List](#)
 - [Critical installation and configuration issues for IBM OpenPages with Watson](#)
4. Back up your existing environment. For more information, see [“Back up your existing environment” on page 280](#).

This step is optional. Create a backup if you want to be able to roll back the fix pack.

5. Verify the status of the servers in your deployment. For more information, see [“Verifying servers before you install a fix pack” on page 282](#).

Install

1. Decide how you want to update the database.
 - You can use the installation app to update the database. If you use this option, you need to enter DBA credentials when you install the fix pack.
 - A database administrator can update the database manually by running scripts. After the database is updated, you can use the installation app to complete the fix pack installation. If you use this option, you do not need to enter DBA credentials when you install the fix pack.

See [“Update the OpenPages database manually \(Db2\)” on page 282](#) or [“Update the OpenPages database manually \(Oracle\)” on page 289](#).

2. Install the fix pack. For more information, see [“Installing a fix pack” on page 295](#).

Complete post installation tasks

1. Restore the solutions helpers, images, and Dojo toolkits. For more information, see [“Restoring solutions helpers, images, and other files” on page 297](#).
2. Configure new features. For more information, see [“Configure new features” on page 299](#).
3. Install solutions updates. For more information, see [“Solutions postinstallation tasks” on page 300](#).

The following procedures are optional or conditional.

Re-generate the reporting framework

This procedure is required if you added new fields and you want to report on them.

For more information, see [“Regenerating the reporting framework” on page 306](#).

Prepare for a fix pack

Before you install a fix pack, you must prepare your deployment.

Review new features and fixes

Before you can install an OpenPages fix pack, you should review new features and fixes.

For more information about new features in a fix pack, see the latest version of the [New Features Guide](#).

For additional information about OpenPages, see the latest version of the [Release Notes](#).

You can find information about defect corrections on the [OpenPages with Watson Fix List](#).

Make sure that you review the following information before you install a fix pack: [Critical installation and configuration issues for IBM OpenPages with Watson](#).

Back up your existing environment

Before you install an OpenPages fix pack, back up the OpenPages application environment, the Cognos environment, and the database.

Backing up your source environment

Before you install a fix pack, back up IBM OpenPages with Watson.

About this task

When you install a fix pack, the installation server automatically backs up most files for you. Some files need to be backed up manually, however. You also need to back up the databases and the openpages-storage directory.

Tip: The backup files that the installation server creates are stored on each server in your deployment in the `<server_home>/installer/maintenance/fix-pack-<version>/backups_from_<previous-version>` directory.

Procedure

1. Stop the application servers (admin and non-admin), reporting servers (active and standby), database server, and the search server (if you use global search).
2. Back up the OpenPages database.
 - If you are using IBM Db2, see [“Backing up the OpenPages database \(Db2\)”](#) on page 410.
 - If you are using Oracle, see [“Backing up the OpenPages database \(Oracle\)”](#) on page 412.
3. Back up the openpages-storage directory.

The openpages-storage directory can be located on a server in your deployment or it can be on a separate network share.

The default location is `<OP_HOME>/openpages-storage`.

4. Do the following steps on each application server (admin and non-admin):

- a) Create a backup directory on the application server.

Use a location that is different from the installation location, such as:

- Windows: `C:\OpenPages<current_version>Backup\OpenPages`
- Linux: `/opt/OpenPages<current_version>Backup/OpenPages`

For example, if you are installing a fix pack on top of 8.2.0.0, use 8200 in the directory name: `OpenPages8200Backup/OpenPages`.

- b) Copy the following directory to the backup directory: `<OP_HOME>/wlp-usr`

5. If you use global search, do the following steps on the search server:

- a) Create a backup directory on the search server.
Use a location that is different from the installation location, such as:
 - Windows: C:\OpenPages<current_version>Backup\OPSearch
 - Linux: /opt/OpenPages<current_version>Backup/OPSearchFor example, if you are installing a fix pack on top of 8.2.0.0, use 8200 in the directory name: OpenPages8200Backup/OPSearch.
 - b) Copy the following items to the backup directory:
 - <SEARCH_HOME>/openpages-solr-index
 - <SEARCH_HOME>/openpages-solr-requesthandler
6. If you modified the standard reports that are provided with OpenPages, copy them to your personal folders.
- OpenPages standard reports can be overwritten when you install a fix pack.
- After the fix pack is installed, you can change the reports and restrict access to them.

Backing up solutions helpers, images, and Dojo toolkits

Before you install an OpenPages fix pack, back up the solutions helpers, images, and Dojo toolkits.

About this task

Do this task if any of the following conditions apply:

- You installed the solutions schema
- You received custom deliverables from the OpenPages Technical Services Team
- You have custom code

Note: The fix pack installer backs up the `web.xml` and `application.xml` files, and then updates the files with the changes that are required for the fix pack. You do not need to manually back up and restore customizations to these files.

Procedure

1. Create a backup directory for the helpers, images, and the Dojo toolkits.
For example, C:\OpenPages<current_version>\patch\helper_backup.
2. Copy the JSP helpers and Dojo toolkits (both included with the product and customized) to the backup directory in the following locations:
 - /dojo_1.10.4/dojo/toolkit
 - /dojo_1.10.4/dojox/toolkit
 - /dojo_1.10.4/dijit/toolkit

You can find these directories in the following location: <OP_HOME>/wlp-user/shared/apps/op-apps.ear/sosa.war/.

Note: Depending on your environment, you might not have these toolkit directories. Go to step 3.

3. If you deployed a customized toolkit or helpers (for example, Helper JSPs or images) in locations other than the locations in step 2, back them up so that you can restore them after the fix pack installation is complete.

Verifying servers before you install a fix pack

Before you install a fix pack, verify the status of the servers in your deployment.

Procedure

1. Ensure that no users are logged in to the OpenPages application.
Users must not log in until the fix pack installation is complete.
2. Ensure that no database scripts are running.
Database scripts, other than the scripts for the fix pack, must not be run until the fix pack installation is complete.
3. Ensure that there are no long running OpenPages processes.
Examples of long running processes include:
 - FastMap imports
 - Global Search indexing processes
4. Do one of the following steps:
 - If you plan to use the installation app to update the database, ensure that all OpenPages application servers (admin and non-admin) and all reporting servers (active and standby) are running.
 - If you plan to update the database manually, ensure that all OpenPages application servers (admin and non-admin) and all reporting servers (active and standby) are shut down.

For information about starting and stopping servers, see [Chapter 12, “Starting and stopping servers,” on page 309](#).
5. If you use global search, ensure that the search services are stopped.
For more information, see [“Start or stop the global search services” on page 312](#).

Installation tasks for fix packs

When you install a fix pack, you can use the installation app to update the database and the application. Or you can update the OpenPages database by using scripts, and then complete the fix pack installation by using the installation app.

Note: If you use special characters in database passwords, before you install a fix pack, ensure that your database passwords do not contain the @ character. The @ character is no longer supported in database passwords.

Update the OpenPages database manually (Db2)

When you install a fix pack, you can choose to update the database by running scripts.

Use this option if you do not want to enter DBA credentials in the installation app.

It is not mandatory to update the database server manually. You can use the OpenPages installation app to update the database automatically, if you prefer.

You must run all of the upgrade scripts in sequence to upgrade the database schema.

Two of the scripts require DBA privileges: a pre-upgrade script and a post-upgrade script. If you have DBA privileges, you can run all of the scripts. If you do not have DBA privileges, contact your database administrator.

A schema user can run the scripts that do not require DBA privileges.

Pre-upgrade step – Requires DBA privileges

During this step, your database administrator runs a script to prepare the database for the upgrade.

You need both DBADM and SECADM privileges to run this script.

Validate the pre-upgrade step

During this step, you run a script to verify that the pre-upgrade DBA script completed successfully and that the database schema is ready for the upgrade.

Upgrade step

During this step, you run a script to upgrade the database. The script determines the current version of the database schema objects, and then runs the upgrade scripts required to upgrade the database to the fix pack version.

Post upgrade step – Requires DBA privileges

During this step, your database administrator runs a script to complete the database upgrade and to set database tuning parameters.

You need both DBADM and SECADM privileges to run this script.

Validate the post-upgrade step

During this step, you run a script to validate the post-upgrade DBA step.

Preparing to apply a fix pack to the database (Db2)

Prepare for the upgrade of the database objects.

Before you begin

Ensure that all OpenPages application servers (admin and non-admin), all reporting servers (active and standby), and the search server (if you use global search) are shut down. See [Chapter 12, “Starting and stopping servers,”](#) on page 309.

Procedure

1. Ensure that the IBM Db2 database server is running.
2. Log on to the Db2 database server computer as a user with administrative privileges.
3. Go to the `<fix_pack_kit>/OP_<version>_Main/OP_<version>_Configuration/Database/DB2/PATCH_SCRIPTS` directory.
4. Verify that you have write permission on the `sql-wrapper.sql` file.
5. Edit the `sql-wrapper.sql` file.

Note: Change only the parameters that are described in this step.

Table 70. Parameters in the <code>sql-wrapper.sql</code> file for Db2 databases	
Property	Description
<code>opx_db2_instance_owner</code>	The database instance owner for OpenPages. The user you specify must have both DBADM and SECADM privileges If your database administrator is going to run the DBA scripts for you, then you can leave this value empty when you run the non-DBA scripts.
<code>opx_db2_server_name</code>	The database server name
<code>opx_db2_port_number</code>	The database port number, for example 50000
<code>opx_db2_db_name</code>	The name of the OpenPages database.
<code>opx_db_owner</code>	The schema owner of the OpenPages database.

Table 70. Parameters in the <code>sql-wrapper.sql</code> file for Db2 databases (continued)	
Property	Description
<code>opx_dflt_stor_srv_root</code>	<p>The path to the OpenPages storage directory.</p> <p>Example:</p> <pre>define opx_dflt_stor_srv_root='/home/ opuser/OP/OpenPages/openpages-storage'</pre>
<code>opx_override_ver_check</code>	<p>Use the default value, N, unless you are re-running the database upgrade scripts after a failure.</p> <p>If the database upgrade failed in the middle of the schema upgrade process, set this parameter to Y. When you re-run the upgrade script, the upgrade process resumes from the last successful schema upgrade step.</p>
<code>sqllib_dir</code>	<p>The path to the Db2 client installation directory on the admin application server (AppServer1)</p> <p>Example:</p> <ul style="list-style-type: none"> • Windows: <code>define sqllib_dir='C:\IBM\SQLLIB'</code> • Linux: <code>define sqllib_dir='/home/db2inst1/sqllib'</code>

6. If your database administrator is going to run the scripts that require DBA privileges, prepare the files for your DBA.
 - a) Go to the `<fix_pack_kit>/OP_<version>_Main/OP_<version>_Configuration/Database/DB2/PATCH_SCRIPTS` directory.
 - b) Open the `op-dba-upgrade-file-list.txt` file.
 - c) Send your DBA the `sql-wrapper.sql` file that you updated along with the files listed in the `op-dba-upgrade-file-list.txt` file.
 - d) Send your DBA the instructions to run the DBA scripts.
 - [“Running the pre-upgrade DBA script for a fix pack \(Db2\)” on page 284](#)
 - [“Running the post-upgrade DBA script for a fix pack \(Db2\)” on page 287](#)

Running the pre-upgrade DBA script for a fix pack (Db2)

Ask your database administrator to run the pre-upgrade script. Or, if you have DBA privileges, you can run the script.

Before you begin

- The IBM Db2 database server is running. All other OpenPages servers are stopped.
- The `JAVA_HOME` system variable is defined and points to the IBM Software Development Kit (SDK) for Java that is installed with Db2. For example:

```
export JAVA_HOME=/db2/V11.1.01/java/jdk64
export PATH=$JAVA_HOME/bin:$PATH
```

If you are running the script from another host, ensure that `JAVA_HOME` is pointing to the IBM Software Development Kit (SDK) for Java that is installed on the computer.

- apache-ant-1.8.1 is deployed to `<fix_pack_kit>/OP_<version>_Main/OP_<version>_Configuration/Database/DB2/PATCH_SCRIPTS`
- The DB2_HOME system variable is defined.

About this task

Run the following script: `op-database-dba-upgrade.sh | .bat`. The script uses the parameters defined in the `sql-wrapper.sql` file.

Procedure

1. Log on to the Db2 database server computer as a database administrator (DBA).
2. Locate the scripts that are required.

If you are a database administrator, get the scripts from your OpenPages team.

Or, you can get the scripts from the `<fix_pack_kit>/OP_<version>_Main/OP_<version>_Configuration/Database/DB2/PATCH_SCRIPTS` directory.

3. Verify that you have execute permission on the scripts in PATCH_SCRIPTS and its subdirectories.
4. Open the `sql-wrapper.sql` file. Verify that the values are suitable for your environment.
 - a) For the `opx_db2_instance_owner` parameter, specify a user that has both DBADM and SECADM privileges.

You can run the following script to get a list of users that have the necessary privileges:

```
select grantee from syscat.dbauth where dbadmauth = 'Y' and securityadmauth = 'Y';
```

- b) If you customized the table space names, update the `define opx_dflt_*` parameters with the custom table space names.
5. Run the following command:

- On Linux:

```
./op-database-dba-upgrade.sh pre '<dba_password>'
```

- On Windows:

```
op-database-dba-upgrade.bat pre "<dba_password>"
```

Note: Quotation marks are required around a password only if the password contains special characters. See [“Special characters in passwords” on page 12](#).

6. Verify that the return code is 0, indicating success.

You can also check the log file, `op-database-dba-pre-upgrade.log`.

What to do next

Validate the pre-upgrade DBA script.

Validating the pre-upgrade DBA step for a fix pack (Db2)

Run the script to validate the pre-upgrade DBA steps.

Before you begin

- The IBM Db2 database server is running. All other OpenPages servers are stopped.

- The JAVA_HOME system variable is defined and points to the IBM SDK, Java Technology Edition that is installed with Db2. For example:

```
export JAVA_HOME=/db2/V11.5/java/jdk64
export PATH=$JAVA_HOME/bin:$PATH
```

If you are running the script from another host, ensure that JAVA_HOME is pointing to the IBM SDK, Java Technology Edition that is installed on the computer.

- apache-ant-1.8.1 has been deployed to <fix_pack_kit>/OP_<version>_Main/OP_<version>_Configuration/Database/DB2/PATCH_SCRIPTS
- The DB2_HOME system variable is defined.

Procedure

1. Log on to the Db2 database server computer as the OpenPages application user, opuser.
2. Go to the <fix_pack_kit>/OP_<version>_Main/OP_<version>_Configuration/Database/DB2/PATCH_SCRIPTS directory.
3. Verify that you have execute permission on the PATCH_SCRIPTS directory and its subdirectories.
4. Open the sql-wrapper.sql file. Verify that the values are suitable for your environment.
5. Run the following command:

- On Linux:

```
./op-database-product-upgrade.sh preupgrade '<op_password>'
```

- On Windows:

```
op-database-product-upgrade.bat preupgrade "<op_password>"
```

Note: Quotation marks are required around a password only if the password contains special characters. See [“Special characters in passwords” on page 12](#).

6. Verify that the script completed successfully.

Look for the following message: Status: Success or a return code of 0.

You can also check the log file, op-validate-dba-pre-upgrade.log.

What to do next

Run the script to upgrade the database objects.

Upgrading the database objects for a fix pack (Db2)

Run the script to upgrade the database objects.

Before you begin

- The IBM Db2 database server is running. All other OpenPages servers are stopped.
- The JAVA_HOME system variable is defined and points to the IBM SDK, Java Technology Edition that is installed with Db2. For example:

```
export JAVA_HOME=/db2/V11.5/java/jdk64
export PATH=$JAVA_HOME/bin:$PATH
```

If you are running the script from another host, ensure that JAVA_HOME is pointing to the IBM SDK, Java Technology Edition that is installed on the computer.

- apache-ant-1.8.1 is deployed to <fix_pack_kit>/OP_<version>_Main/OP_<version>_Configuration/Database/DB2/PATCH_SCRIPTS
- The DB2_HOME system variable is defined.

- The `op-database-product-upgrade.sh | .bat` preupgrade script completed successfully.

Procedure

1. Log on to the Db2 database server computer as the OpenPages application user, `opuser`.
2. Go to the `<fix_pack_kit>/OP_<version>_Main/OP_<version>_Configuration/Database/DB2/PATCH_SCRIPTS` directory.
3. Verify that you have execute permission on the scripts in the `PATCH_SCRIPTS` directory and its subdirectories.
4. Open the `sql-wrapper.sql` file. Verify that the values are suitable for your environment.
5. Run the following command:

- On Linux:

```
./op-database-product-upgrade.sh upgrade '<op_password>'
```

- On Windows:

```
op-database-product-upgrade.bat upgrade "<op_password>"
```

Note: Quotation marks are required around a password only if the password contains special characters. See [“Special characters in passwords” on page 12](#).

6. Verify that the return code is 0, indicating success.

You can also check the log file, `op-database-product-upgrade.log`.

What to do next

Ask your database administrator to run the post-upgrade DBA script.

Running the post-upgrade DBA script for a fix pack (Db2)

Ask your database administrator to run the post-upgrade script. Or, if you have DBA privileges, you can run the script.

Before you begin

- The IBM Db2 database server is running. All other OpenPages servers are stopped.
- The `JAVA_HOME` system variable is defined and points to the IBM SDK, Java Technology Edition that is installed with Db2. For example:

```
export JAVA_HOME=/db2/V11.5/java/jdk64
export PATH=$JAVA_HOME/bin:$PATH
```

If you are running the script from another host, ensure that `JAVA_HOME` is pointing to the IBM SDK, Java Technology Edition that is installed on the computer.

- `apache-ant-1.8.1` is deployed to `<fix_pack_kit>/OP_<version>_Main/OP_<version>_Configuration/Database/DB2/PATCH_SCRIPTS`
- The `DB2_HOME` system variable is defined.
- The `op-database-product-upgrade.sh | .bat` script completed successfully.

About this task

Run the following script: `op-database-dba-upgrade.sh | .bat`. The script uses the parameters defined in the `sql-wrapper.sql` file.

Procedure

1. Log on to the Db2 database server computer as a database administrator (DBA).
2. Locate the scripts that are required.

If you are a database administrator, get the scripts from your OpenPages team.

Or, you can get the scripts from the `<fix_pack_kit>/OP_<version>_Main/OP_<version>_Configuration/Database/DB2/PATCH_SCRIPTS` directory.

3. Verify that you have execute permission on the scripts in PATCH_SCRIPTS and its subdirectories.
4. Open the `sql-wrapper.sql` file. Verify that the values are suitable for your environment.

The user that you specify in the `opx_instance_owner` parameter must have both DBADM and SECADM privileges

You can run the following script to get a list of users that have the necessary privileges:

```
select grantee from syscat.dbauth where dbadmauth = 'Y' and securityadmauth = 'Y';
```

5. Run the following command:

- On Linux:

```
./op-database-dba-upgrade.sh post '<dba_password>'
```

- On Windows:

```
op-database-dba-upgrade.bat post "<dba_password>"
```

Note: Quotation marks are required around a password only if the password contains special characters. See [“Special characters in passwords”](#) on page 12.

6. Verify that the return code is 0, indicating success.

You can also check the log file: `op-database-dba-post-upgrade.log`.

What to do next

Validate the post-upgrade DBA step.

Validating the post-upgrade DBA step for a fix pack (Db2)

Run the script to validate the post-upgrade DBA steps.

Before you begin

- The IBM Db2 database server is running. All other OpenPages servers are stopped.
- The JAVA_HOME system variable is defined and points to the IBM SDK, Java Technology Edition that is installed with Db2. For example:

```
export JAVA_HOME=/db2/V11.5/java/jdk64
export PATH=$JAVA_HOME/bin:$PATH
```

If you are running the script from another host, ensure that JAVA_HOME is pointing to the IBM SDK, Java Technology Edition that is installed on the computer.

- `apache-ant-1.8.1` has been deployed to `<fix_pack_kit>/OP_<version>_Main/OP_<version>_Configuration/Database/DB2/PATCH_SCRIPTS`
- The DB2_HOME system variable is defined.

Procedure

1. Log on to the Db2 database server computer as the OpenPages application user, `opuser`.

2. Go to the `<fix_pack_kit>/OP_<version>_Main/OP_<version>_Configuration/Database/DB2/PATCH_SCRIPTS` directory.
3. Verify that you have execute permission on the scripts in PATCH_SCRIPTS and its subdirectories.
4. Open the `sql-wrapper.sql` file. Verify that the values are suitable for your environment.
5. Run the following command:

- On Linux:

```
./op-database-product-upgrade.sh postdba '<op_password>'
```

- On Windows:

```
op-database-product-upgrade.bat postdba "<op_password>"
```

Note: Quotation marks are required around a password only if the password contains special characters. See [“Special characters in passwords”](#) on page 12.

6. Verify that the script completed successfully.
Look for the following message: Status:Success or a return code of 0.
You can also check the log file, `op-validate-dba-post-upgrade.log`.

Results

The OpenPages database is upgraded to the fix pack version.

What to do next

Run the installation app or use silent mode to upgrade OpenPages to the fix pack version. For the **Install Database** option, select **Already Installed**.

Update the OpenPages database manually (Oracle)

When you install a fix pack, you can choose to update the database by running scripts.

Use this option if you do not want to enter DBA credentials in the installation app.

It is not mandatory to update the database server manually. You can use the OpenPages installation app to update the database automatically, if you prefer.

You must run all of the upgrade scripts in sequence to upgrade the database schema.

Two of the scripts require DBA privileges: a pre-upgrade script and a post-upgrade script. If you have DBA privileges, you can run all of the scripts. If you do not have DBA privileges, contact your database administrator.

A schema user can run the scripts that do not require DBA privileges.

Note: Fix pack 8.1.0.1 drops and re-creates a number of constraints and indexes. As a result, the database update scripts might take longer to run.

Pre-upgrade step – Requires DBA privileges

During this step, your database administrator runs a script to prepare the database for the upgrade.

You need SYSDBA privileges to run this script.

Validate the pre-upgrade step

During this step, you run a script to verify that the pre-upgrade DBA script completed successfully and that the database schema is ready for the upgrade.

Upgrade step

During this step, you run a script to upgrade the schema. The script determines the current version of the database schema, and then runs the upgrade scripts required to upgrade the schema to the fix pack version.

Post upgrade step – Requires DBA privileges

During this step, your database administrator runs a script to complete the database upgrade and to set database tuning parameters.

You need SYSDBA privileges to run this script.

Validate the post-upgrade step

During this step, you run a script to validate the post-upgrade DBA step.

Preparing to apply a fix pack to the database (Oracle)

Prepare for the upgrade of the database schema.

Before you begin

Ensure that all OpenPages application servers (admin and non-admin), all reporting servers (active and standby), and the search server (if you use global search) are shut down.

Procedure

1. Ensure that the Oracle database server is running.
2. Log on to the Oracle database server computer as a user with administrative privileges.
3. Go to the `<fix_pack_kit>/OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/PATCH_SCRIPTS` directory.
4. Verify that you have write permission on the `sql-wrapper.sql` file.
5. Edit the `sql-wrapper.sql` file.

Note: Change only the parameters that are described in this step.

Table 71. Parameters in the <code>sql-wrapper.sql</code> file for Oracle databases	
Property	Description
<code>opx_datafile_storage_dir</code>	Defines the physical locations of the datafiles that are associated with the tablespaces that are created. This should be set to a value that is appropriate for your environment
<code>opx_dflt_sid</code>	The TNS alias of the Oracle database for OpenPages.
<code>opx_db_owner</code>	The OpenPages database owner
<code>opx_oracle_dba_user</code>	The user name of a user with SYSDBA privileges. If your database administrator is going to run the DBA scripts for you, then you can leave this value empty when you run the non-DBA scripts.
<code>opx_override_ver_check</code>	Use the default value, N, unless you are re-running the database upgrade scripts after a failure. If the database upgrade failed in the middle of the schema upgrade process, set this parameter to Y. When you re-run the upgrade script, the upgrade process resumes from the last successful schema upgrade step.

6. If your database administrator is going to run the scripts that require DBA privileges, prepare the files for your DBA.
 - a) Go to the `<fix_pack_kit>/OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/PATCH_SCRIPTS` directory.
 - b) Open the `op-dba-upgrade-file-list.txt` file.
 - c) Send your DBA the `sql-wrapper.sql` file that you updated along with the files listed in the `op-dba-upgrade-file-list.txt` file.

d) Send your DBA the instructions to run the DBA scripts.

- [“Running the pre-upgrade DBA script for a fix pack \(Oracle\)” on page 291](#)
- [“Running the post-upgrade DBA script for a fix pack \(Oracle\)” on page 293](#)

Running the pre-upgrade DBA script for a fix pack (Oracle)

Ask your database administrator to run the pre-upgrade script. Or, if you have DBA privileges, you can run the script.

Before you begin

- The Oracle database server is running. All other OpenPages servers are stopped.
- The JAVA_HOME system variable is defined.
- apache-ant-1.8.1 is deployed to `<fix_pack_kit>/OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/PATCH_SCRIPTS`
- The ORACLE_HOME system variable is defined.

About this task

Run the following script: `op-database-dba-upgrade.sh | .bat`. The script uses the parameters defined in the `sql-wrapper.sql` file.

Procedure

1. Log on to the Oracle database server computer as a database administrator (DBA).
2. Locate the scripts that are required.

If you are a database administrator, get the scripts from your OpenPages team.

Or, you can get the scripts from the `<fix_pack_kit>/OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/PATCH_SCRIPTS` directory.

3. Verify that you have execute permission on the scripts in PATCH_SCRIPTS and its subdirectories.
4. Open the `sql-wrapper.sql` file. Verify that the values are suitable for your environment.
 - a) For the `opx_oracle_dba_user` parameter, enter a user that has SYSDBA privileges, for example SYS.
 - b) If you customized the table space names, update the `define opx_dflt_*` parameters with the custom table space names.
5. Run the following command:

- On Windows:

```
op-database-dba-upgrade.bat pre "<sysdba_password>"
```

- On Linux:

```
./op-database-dba-upgrade.sh pre '<sysdba_password>'
```

Note: Quotation marks are required around a password only if the password contains special characters. See [“Special characters in passwords” on page 12](#).

6. Verify that the return code is 0, indicating success.

You can also check the log file, `op-database-dba-pre-upgrade.log`.

What to do next

Validate the pre-upgrade DBA script.

Validating the pre-upgrade DBA step for a fix pack (Oracle)

Run the script to validate the pre-upgrade DBA steps.

Before you begin

- The Oracle database server is running. All other OpenPages servers are stopped.
- The JAVA_HOME system variable is defined.
- apache-ant-1.8.1 has been deployed to <fix_pack_kit>/OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/PATCH_SCRIPTS
- The ORACLE_HOME system variable is defined.

Procedure

1. Log on to the Oracle database server computer as the OpenPages application user, opuser.
2. Go to the <fix_pack_kit>/OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/PATCH_SCRIPTS directory.
3. Verify that you have execute permission on the scripts.
4. Open the sql-wrapper.sql file. Verify that the values are suitable for your environment.
5. Run the following command:

- On Windows:

```
op-database-product-upgrade.bat preupgrade "<op_schema_owner_password>"
```

- On Linux:

```
./op-database-product-upgrade.sh preupgrade '<op_schema_owner_password>'
```

Note: Quotation marks are required around a password only if the password contains special characters. See [“Special characters in passwords” on page 12](#).

6. Verify that the script completed successfully.
Look for the following message: Status: Success or a return code of 0.
You can also check the log file, op-validate-dba-pre-upgrade.log.

What to do next

Run the script to upgrade the database schema.

Upgrading the schema for a fix pack (Oracle)

Run the script to upgrade the database schema.

Before you begin

- The Oracle database server is running. All other OpenPages servers are stopped.
- The JAVA_HOME system variable is defined.
- apache-ant-1.8.1 is deployed to <fix_pack_kit>/OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/PATCH_SCRIPTS
- The ORACLE_HOME system variable is defined.
- The op-database-product-upgrade.sh|.bat preupgrade script completed successfully.

Procedure

1. Log on to the Oracle database server computer as the OpenPages application user, opuser.

2. Go to the `<fix_pack_kit>/OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/PATCH_SCRIPTS` directory.
3. Verify that you have execute permission on the scripts in the PATCH_SCRIPTS directory and its subdirectories.
4. Open the `sql-wrapper.sql` file. Verify that the values are suitable for your environment.
5. Run the following command:

- On Windows:

```
op-database-product-upgrade.bat upgrade "<op_schema_owner_password>"
```

- On Linux:

```
./op-database-product-upgrade.sh upgrade '<op_schema_owner_password>'
```

Note: Quotation marks are required around a password only if the password contains special characters. See [“Special characters in passwords”](#) on page 12.

6. Verify that the return code is 0, indicating success.

You can also check the log file, `op-database-product-upgrade.log`.

What to do next

Ask your database administrator to run the post-upgrade DBA script.

Running the post-upgrade DBA script for a fix pack (Oracle)

Ask your database administrator to run the post-upgrade script. Or, if you have DBA privileges, you can run the script.

Before you begin

- The Oracle database server is running. All other OpenPages servers are stopped.
- The JAVA_HOME system variable is defined.
- `apache-ant-1.8.1` is deployed to `<fix_pack_kit>/OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/PATCH_SCRIPTS`
- The ORACLE_HOME system variable is defined.
- The `op-database-product-upgrade.sh | .bat` script completed successfully.

About this task

Run the following script: `op-database-dba-upgrade.sh | .bat`. The script uses the parameters defined in the `sql-wrapper.sql` file.

Procedure

1. Log on to the Oracle database server computer as a database administrator (DBA).
2. Locate the scripts that are required.

If you are a database administrator, get the scripts from your OpenPages team.

Or, you can get the scripts from the `<fix_pack_kit>/OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/PATCH_SCRIPTS` directory.

3. Verify that you have execute permission on the scripts in PATCH_SCRIPTS and its subdirectories.
4. Open the `sql-wrapper.sql` file. Verify that the values are suitable for your environment. In the `opx_oracle_dba_user` parameter, enter a user that has SYSDBA privileges, for example SYS.
5. Run the following command:

- On Windows:

```
op-database-dba-upgrade.bat post "<sysdba_password>"
```

- On Linux:

```
./op-database-dba-upgrade.sh post '<sysdba_password>'
```

Note: Quotation marks are required around a password only if the password contains special characters. See [“Special characters in passwords” on page 12](#).

6. Verify that the return code is 0, indicating success.

You can also check the log file: `op-database-dba-post-upgrade.log`.

What to do next

Validate the post-upgrade DBA step.

Validating the post-upgrade DBA step for a fix pack (Oracle)

Run the script to validate the post-upgrade DBA steps.

Before you begin

- The Oracle database server is running. All other OpenPages servers are stopped.
- The JAVA_HOME system variable is defined.
- apache-ant-1.8.1 has been deployed to `<fix_pack_kit>/OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/PATCH_SCRIPTS`
- The ORACLE_HOME system variable is defined.

Procedure

1. Log on to the Oracle database server computer as the OpenPages application user, `opuser`.
2. Go to the `<fix_pack_kit>/OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/PATCH_SCRIPTS` directory.
3. Verify that you have execute permission on the scripts in `PATCH_SCRIPTS` and its subdirectories..
4. Open the `sql-wrapper.sql` file. Verify that the values are suitable for your environment.
5. Run the following command:

- On Windows:

```
op-database-product-upgrade.bat postdba "<op_schema_owner_password>"
```

- On Linux:

```
./op-database-product-upgrade.sh postdba '<op_schema_owner_password>'
```

Note: Quotation marks are required around a password only if the password contains special characters. See [“Special characters in passwords” on page 12](#).

6. Verify that the script completed successfully.

Look for the following message: `Status : Success` or a return code of 0.

You can also check the log file, `op-validate-dba-post-upgrade.log`.

Results

The OpenPages database schema is upgraded to the fix pack version.

What to do next

Run the installation app to upgrade OpenPages to the fix pack version. For the **Install Database** option, select **Already Installed**.

Installing a fix pack

Apply a fix pack to get the latest fixes and features.

Before you begin

- Complete the following preparation tasks:
 - Download the fix pack kit from Fix Central
 - [“Review new features and fixes” on page 280](#)
 - [“Back up your existing environment” on page 280](#)
 - [“Verifying servers before you install a fix pack” on page 282](#)
- Ensure that the installation server is updated to the latest version. For more information, see [“Updating the installation server” on page 47](#).

For example, if you are applying fix pack 8.2.0.3, the installation server must also be at version 8.2.0.3 or later.

- Ensure that IBM OpenPages with Watson 8.2.x or later is installed.

Note: You cannot use a fix pack kit to install a main release version, such as 8.2.0.0.

For example, if you are using version 7.3 and you want to move to version 8.2.0.3, migrate to OpenPages 8.2.0.0 first, then apply the 8.2.0.3 fix pack.

- If you installed the agents on remote servers manually, ensure that the agents are updated to the latest version. Also, ensure that the agents are running. For more information, see [“Updating agents manually” on page 48](#).

Note: If you used the installation server to deploy the agents automatically, you do not need to update them. The agents are updated when you update the installation server.

- If your application servers cannot access the internet and you updated WebSphere Liberty features manually in the past, do steps 1-6 in the following task: [“Updating WebSphere Liberty features manually” on page 154](#).
- If you want to update the database manually, complete the database update before you use the installation app to install the fix pack. For more information, see [“Update the OpenPages database manually \(Db2\)” on page 282](#) or [“Update the OpenPages database manually \(Oracle\)” on page 289](#).
- Ensure that IBM Cognos Configuration is not running.
- Ensure that users do not log in to or use OpenPages during the fix pack installation process.

About this task

Fix pack kits are cumulative. You can use a fix pack kit to install the current fix pack as well as previous 8.2.0.x fix packs.

For example, suppose you are using the 8.2.0.3 installation server and you have the 8.2.0.3 fix pack kit. You can install 8.2.0.3 to get the 8.2.0.1, 8.2.0.2, and 8.2.0.3 fix pack updates. Or, you can install fix pack 8.2.0.1 first, then install 8.2.0.2, and then install 8.2.0.3.

This video demonstrates how to install a fix pack: <https://youtu.be/jVKsVODP0R8>.

Procedure

1. Log on to the installation server computer as the user who installed the installation server.

Alternatively, you can log in as any user who has full permissions on the installation server directories and who can run Node.js.

2. Locate the `openpages_fixpack_<version>.zip` file on the installation media.

The file is stored in `/OP_<version>_Main/OP_<version>_Installer`.

3. Copy the `openpages_fixpack_<version>.zip` file to the following directory on the installation server:

`<Installation_server_home>/src/assets/maintenance`

Note: You do not need to copy the `openpages_fixpack_<version>.zip` file to the remote servers. The installation server pushes the file to each agent automatically, including agents that you installed and updated manually.

4. Log in to the OpenPages installation app.

For more information, see [“Logging in to the installation app” on page 49](#).

5. Open the deployment that you want to update.

If your deployment is already open, refresh the page.

6. Click the **Deployment Task** list and select **Fixpack**, and then select the fix pack version that you want to install.

If **Fixpack** is not displayed in the **Deployment Task** list, refresh the page or click **Validate**.

7. Click the **Database Server** card.

8. Click **Install Database** and select one of the following options:

- **Full Database:** Select this option if the database is not updated yet. The installation app will apply the fix pack to the database.
- **Already Installed:** Select this option if the database is already updated.

For fix packs, the **Only Non-DBA** and **Already Installed** options are equivalent.

9. If you chose **Full Database**, type the **DBA Username** and the **DBA Password**.

- IBM Db2: The user that you specify must have both DBADM and SECADM privileges.
- Oracle: The user that you specify must have SYSDBA privileges.

10. Click **Validate**.

Note: If you updated the database manually by running scripts, do not click **Validate** until all of the database scripts complete successfully.

11. Click **Install**.

Tip: You can log out and close the browser window. The **Install** process continues to run. When you log in to the installation app again, the app shows the status of your deployment. You can also close the browser window during the **Configure** process.

12. Click **Configure**.

What to do next

Do the post-installation tasks. For more information, see [“Postinstallation tasks” on page 297](#).

If you see warnings in the log files about system views, see [“Warnings about system views when loading data” on page 444](#).

Postinstallation tasks

After you install an IBM OpenPages with Watson fix pack, you must complete some additional tasks.

Restoring solutions helpers, images, and other files

Restore custom solutions helpers, images, and other custom deliverables that you backed up.

About this task

If you backed up the following items, restore them:

- Solutions schema
- Custom deliverables from the IBM OpenPages Technical Services Team
- Custom code

Review your custom code. The location of the `dojo` and `idx` files has changed. The new paths are:

- `<OP_HOME>/wlp-usr/shared/apps/op-apps.ear/sosa.war/dojo`
- `<OP_HOME>/wlp-usr/shared/apps/op-apps.ear/sosa.war/idx`

Updating the IBM OpenPages SDI Connector for UCF Common Controls Hub

If you use the IBM OpenPages SDI Connector for UCF Common Controls Hub connector, you need to update it. Do these steps after you install IBM OpenPages with Watson 8.2.0.1 or later.

Before you begin

- IBM OpenPages with Watson 8.2.0.1 or later is installed.
- You installed and configured IBM OpenPages SDI Connector for UCF Common Controls Hub in 8.2.0.0 or earlier.

About this task

Do this task if you are using IBM Security Directory Integrator 7.2.0.3. If you are using 7.2.0.5 and you already patched Java to update it to Java 8 (see step 3), you can skip this task.

Procedure

1. In IBM Security Directory Integrator, locate your `ucf_integration` project and rename it. For example, name it `old_ucf_integration`.
2. Install IBM Security Directory Integrator Fix Pack 6.
To get the installation package, see [Downloading IBM OpenPages with Watson Version 8.2 from Passport Advantage](#).
3. Patch the version of Java to update it to Java 8.
For more information, see [technote 720-iss-sdi-la0019](#).
4. On the IBM OpenPages with Watson application server, go to the `<OP_HOME>/integrations/UCF` directory and locate the `ucf_integration.xml` file.
5. Copy the file to the server where Security Directory Integrator is installed.
6. Import the `ucf_integration.xml` file as a new project in Security Directory Integrator.
 - a) Click **File > Import > IBM Security Directory Integrator > Configuration**.
 - b) Click **Next**.
 - c) Select **New Project** in the **Project** list.
 - d) Click **File**.

- e) Click the browse button next to the **Configuration File** field. Select the `ucf_integration.xml` file.
 - f) Click **Finish**.
 - g) Name the project `ucf_integration`.
 - h) Click **Finish**.
The project is displayed in the **SDI Configuration Editor** and the project files are created in your SDI workspace directory. Your project has the updated assembly lines.
7. Copy the connection properties files from your old project to your new project.
 - `op_client.properties`
 - `passwords.properties`
 8. Refresh the property files and the connector with the updated connection information.
 - a) In the Navigator pane, expand **Resources > Properties**.
 - b) Right-click **op_client**, and then click **Open**.
 - c) Click **Read properties from Server**, and then click **Send properties to Server**.
 - d) Click **Save**, and then close the window.
 - e) Right-click **passwords**, and then click **Open**.
 - f) Click **Read properties from Server**, and then click **Send properties to Server**.
 - g) Click **Save**, and then close the window.
 9. Optional: Disable the TLS 1.0 protocol in IBM Security Directory Integrator.
IBM Security Directory Integrator 7.2.0.6 supports later versions of the TLS protocol. Depending on your security requirements, you might need to disable TLS 1.0. For more information, see [Disabling TLS 1.0 for TDI/SDI](#).

Updating IBM Security Directory Integrator for the QRadar connector

If you use the QRadar® connector, you need to update IBM Security Directory Integrator. Do these steps after you install IBM OpenPages with Watson 8.2.0.1 or later.

Before you begin

- IBM OpenPages with Watson 8.2.0.1 or later is installed.
- You installed and configured the QRadar connector in 8.2.0.0 or earlier.

About this task

Do this task if you are using IBM Security Directory Integrator 7.2.0.3. If you are using 7.2.0.5 and you already patched Java to update it to Java 8 (see step 3), you can skip this task.

Procedure

1. Install IBM Security Directory Integrator Fix Pack 6.
To get the installation package, see [Downloading IBM OpenPages with Watson Version 8.2 from Passport Advantage](#).
2. Patch the version of Java to update it to Java 8.
For more information, see [technote 720-iss-sdi-la0019](#).
3. Optional: Disable the TLS 1.0 protocol in IBM Security Directory Integrator.
IBM Security Directory Integrator 7.2.0.6 supports later versions of the TLS protocol. Depending on your security requirements, you might need to disable TLS 1.0. For more information, see [Disabling TLS 1.0 for TDI/SDI](#).

Configure new features

Some new features need to be configured.

Fix pack 8.2.0.4

Upgrade from Apache Log4j 1 to Apache Log4j 2

When you install fix pack 8.2.0.4, OpenPages upgrades from Apache Log4j 1 to Apache Log4j 2.

This upgrade changes logging, and affects logging properties files, JSP loggers, and other custom code.

Logging properties files are updated as follows:

- The `log4j.properties` file is replaced with a `log4j2.properties` file.
The `log4js.properties` file exists for the following tools:
 - For global search, the log file is in the `<OPSearch_Home>/opsearchtools` directory.
 - For client tools, the log file is in `<client-tools-dir>/bin`, where `<client-tools-dir>/bin` is either `<OP_HOME>` or the directory into which the client tools are installed on a remote client.
 - For Environment Comparison, the log file is in the `<OP_HOME>/aurora/bin/compare_environments` directory.
- The `auroralogging.properties` file is updated.
- The `ObjectManagerLogging.properties` is removed and the logging for ObjectManager is now defined in the `log4j2.properties` file for client tools.

When you install the fix pack, the installation server automatically backs up these files for you. The backup files that the installation server creates are stored on each server in your deployment in the `<server_home>/installer/maintenance/fix-pack-<version>/backups_from_<previous-version>` directory.

For information about fixing JSP loggers and other custom code if they fail after installing fix pack 8.2.0.4, see [Custom code and JSP helpers may fail after installing OpenPages 8.2.0.4 or later](#).

Fix pack 8.2.0.3

New application permission for the Bulk Update feature

The behavior of the **Bulk Update** feature in grid views has changed. The feature is now available only on fields that are enabled for bulk updates. Due to this change, a new application permission is now available: **SOX > Administration > Bulk Update All Fields**. This permission enables administrators to use **Bulk Update** on all fields in a grid view, regardless of whether bulk update is enabled on the fields.

By default, all fields are disabled for Bulk Update in 8.2.0.3. Administrators must use the View Designer and update existing grid views to enable fields that are available for bulk update.

New application permissions for FastMap in the Task Focused UI

The way FastMap works in the Task Focused UI is now different than the way it works in the Standard UI. In the Standard UI, FastMap uses a JSP report and access control is handled by the Reporting folder. New application permissions are needed because the Task Focused UI doesn't use a JSP report. This means that users who used to be able to access FastMap can't access it in the Task Focused UI unless an administrator sets the application permissions for them.

To import object data and to see their import history, a user needs the application permission **All Permissions > SOX > Administration > FastMap > Import**.

To view imports performed by other users, a user needs the application permission **All Permissions > SOX > Administration > FastMap > View all history**.


Fix pack 8.2.0.2

Themes

If you want to configure custom themes, you need to add the **SOX > Administration > Solutions** permission to your role template.

For more information, see the *IBM OpenPages with Watson Administrator's Guide*.

Creating and modifying JSP system files

Access to system files in the /Reports folder has changed. By default, only super administrators and members of the OPAdministrator group can now create or modify the JSP report system files in the /Reports folder under  > **System Configuration > System Files**.

Previously, all users with the **Report** object type in their profile had access. In general, users should not change .jsp files. These files contain source code for executables that could impact the stability and security of the system if the files are not managed correctly.

For more information, see the *IBM OpenPages with Watson Administrator's Guide*.

User name display format

The default value for the user name format application text (**com.display.name.format**) has changed to %FN; %LN; - %EM (first name, last name, email).

Previously, the default value was %NM; (user name).

For more information, see the *IBM OpenPages with Watson Administrator's Guide*.

Fix pack 8.2.0.1

IBM Watson Language Translator

If you want to use IBM Watson Language Translator, update role template with these new application permissions

- Watson Language Translation
- Watson Language Translation UI

Integration with Microsoft Office

If you want to allow users to open and edit Microsoft Office files directly from OpenPages, ensure that Microsoft Office 2016 or Microsoft 365 is installed on their computers.

Also, if the OpenPages application server is using a self-signed certificate, users must import the certificate into the trust store on their local computers.

Cross-track links

The script that is used for cross-track links in reports has changed. If you have custom reports that use cross-track links, update the reports with the new script.

For more information, see the *IBM OpenPages with Watson Report Author's Guide*

Solutions postinstallation tasks

After you install an OpenPages fix pack, you might need to do some postinstallation tasks to update OpenPages solutions.

Fix pack 8.2.0.1

Fix pack 8.2.0.1 includes the following updates:

- Updates are available for IBM OpenPages Model Risk Governance. See [“Updating IBM OpenPages Model Risk Governance” on page 301](#).
- Solutions reports have been updated. Import the solutions report package to update them. See [“Importing the solutions report packages after installing a fix pack” on page 305](#).

Fix pack 8.2.0.2

Fix pack 8.2.0.2 includes the following updates:

- A new version of IBM OpenPages Financial Controls Management is available. See [“Updating IBM OpenPages Financial Controls Management”](#) on page 302.
- For the following solutions, you can replace computed fields with calculations:
 - IBM OpenPages Internal Audit Management
 - IBM OpenPages IT Governance

For more information, see [“Replacing computed fields with calculations”](#) on page 304.

- Solutions reports have been updated. Import the solutions report package to update them. See [“Importing the solutions report packages after installing a fix pack”](#) on page 305.

Fix pack 8.2.0.3

Fix pack 8.2.0.3 includes the following updates:

- The descriptions of some settings have been updated. Import the new descriptions. For more information, see [“Updating IBM OpenPages Internal Audit Management settings”](#) on page 303.
- Solutions reports have been updated. Import the solutions report package to update them. See [“Importing the solutions report packages after installing a fix pack”](#) on page 305.
- If you use IBM OpenPages Financial Controls Management, update the FCM Master V2 and FCM Certification V2 profiles to include the Action Item object type.

Updating IBM OpenPages Model Risk Governance

If you use IBM OpenPages Model Risk Governance with IBM Watson OpenScale, do the following steps to update the solution.

Procedure

1. Copy the 8.2.0.1_MRG_Additional_Loader_Files.zip from the installation media to the admin application server.

The zip file is located in the /OP_<version>_Main/OP_<version>_Configuration/Modules/MRG/OpenScale directory.

2. Expand the 8.2.0.1_MRG_Additional_Loader_Files.zip file.

You now have two loader files:

- Monitored_with_OpenScale_Filter-op-config.xml

This file contains a public filter for the Model object. The filter is called Models monitored with OpenScale. It enables users to filter on OpenScale models in grid views.

- OpenScale_Update_Metric_Last_Value_Info-op-config.xml

This file contains a workflow that updates Metrics that are associated with an OpenScale Model. The workflow updates Metrics with the most recent MetricValue values pushed from OpenScale.

3. Open a command line.

If you are using Microsoft Windows, open a command prompt with the **Run as Administrator** option.

4. Go to the <OP_HOME>/bin directory.

5. Run the following command to load the public filter.

Replace <loader-file-path> with the location of the Monitored_with_OpenScale_Filter-op-config.xml file.

```
ObjectManager.cmd|sh 1 c <OpenPages Administrator user> <OpenPages Administrator password>
<loader-file-path> Monitored_with_OpenScale_Filter
```


If you encounter any errors, review the log file, <loader-file-path>/ObjectManager.log.

6. Update the following profiles. If you use other profiles with MRG, update them also.

- **OpenPages Modules Master**

- **OpenPages MRG Master**
- **MRG Model Owner**
- **MRG Model Validation**

For information about working with profiles, see *IBM OpenPages with Watson Administrator's Guide*.

- Log in to OpenPages as an administrator.
 - Click  > **Solution Configuration** > **Profiles**.
 - Click a profile, and then click **Edit**.
 - For the **Model** object, add the Models monitored with OpenScale filter.
 - For the **Metric** object, add the following fields:
 - Metric Type
 - OpenScale Category
 - OpenScale Description
 - OpenScale Metric
 - OpenScale Metric Value
 - For the **Metric Value** object, add the following fields:
 - Metric Type
 - OpenScale Category
 - OpenScale Description
 - OpenScale Metric
 - OpenScale Metric Value
 - Click **Done**.
7. Run the following command to load the workflow:

Replace *<loader-file-path>* with the location of the OpenScale_Update_Metric_Last_Value_Info-op-config.xml file.

```
ObjectManager.cmd|sh 1 c <OpenPages Administrator user> <OpenPages Administrator password>
<loader-file-path> OpenScale_Update_Metric_Last_Value_Info
```

If you encounter any errors, review the log file, *<loader-file-path>/ObjectManager.log*.

Updating IBM OpenPages Financial Controls Management

Fix pack 8.2.0.2 includes a new version of IBM OpenPages Financial Controls Management (FCM). Do the steps in this task if you want to use the new version of FCM.

Before you begin

If you currently use IBM OpenPages Financial Controls Management, review the loader files before you do the steps in this task.

About this task

The new version of FCM includes the following components:

- New profiles, users, dashboards, and filters
- A new field group, OPSS-FCM-cert, and new fields
- New workflows for the following object types: Control, Control Eval, Process, Process Eval, Business Entity
- New system views for the following object types: Control, Control Eval, Process, Process Eval

- New calculations: Control Eval Certification and Process Eval Certification
- New reports

Procedure

1. Copy the `FCM_8202_Loader_Files.zip` from the installation media to the application server or to a computer where the ObjectManager client is installed.

The zip file is located in the `/OP_<version>_Main/OP_<version>_Configuration/Modules/FCM` directory.

2. Expand the `FCM_8202_Loader_Files.zip` file to a new directory.
3. Open a command line.

If you are using Microsoft Windows, open a command prompt with the **Run as Administrator** option.

4. Run the following command:

Linux

```
./Run_FCM_full.sh <op_admin_user> <op_admin_password>
```

Windows

```
Run_FCM_full.bat <op_admin_user> <op_admin_password>
```

If you encounter any errors, review the log file, `ObjectManager.log`.

What to do next

1. Import the solutions report package to get the new FCM reports. See [“Importing the solutions report packages after installing a fix pack”](#) on page 305.
2. After you complete all other post-installation tasks, regenerate the reporting framework. You can select all models or select only the FCM Reporting Package and the FCM SS Dashboarding models.

Updating IBM OpenPages Internal Audit Management settings

The descriptions of some settings have changed. The descriptions were updated to remove `<` and `>` characters. This task is optional.

About this task

Several IBM OpenPages Internal Audit Management settings used `<` and `>` in their descriptions. Do this task to replace `<` and `>` with `[` and `]`.

This task updates the description of the following settings:

- `/Solutions/IAM/Audit Close/Object Types to Lock`
- `/Solutions/IAM/Audit Close/Fields to Set`
- `/Solutions/IAM/Audit Close/Included Objects`
- `/Solutions/IAM/Audit Close/Object Types to Delete`
- `/Solutions/IAM/Audit Close/Included Object Paths`
- `/Solutions/IAM/Audit Close/Fields to Clear`

Procedure

1. Copy the following file from the installation media to the application server. Or, if you run ObjectManager from a remote system, such as your laptop, copy the file to the remote system.
`OpenPages-audit-close-registry-entries-op-config.xml`

The file is located in the /OP_<version>_Main/OP_<version>_Configuration/Modules/Upgrade/IAM/loader-data directory.

2. Open a command line.

If you are using Microsoft Windows, open a command prompt with the **Run as Administrator** option.

3. Go to the <OP_HOME>/bin directory.

Or, if you're running ObjectManager from a remote system, go to the openpages-tools-client/bin directory.

4. Run the following command to load the updated fields.

Replace <loader-file-path> with the location of the OpenPages-audit-close-registry-entries-op-config.xml file.

```
ObjectManager.cmd|sh 1 c <OpenPages Administrator user> <OpenPages Administrator password>
<loader-file-path> OpenPages-audit-close-registry-entries
```

If you encounter any errors, review the log file, <loader-file-path>/ObjectManager.log.

Replacing computed fields with calculations

IBM OpenPages Internal Audit Management and IBM OpenPages IT Governance use computed fields. You can update the fields to use GRC calculations and links instead of computed fields. The fields are replaced with new fields that use the same names. This task is optional.

About this task

This task makes the following changes to your environment:

- Replaces the following computed fields with calculated fields:
 - Auditable Entity: OPSS-AudEnt: Weighted Risk Score
 - Audit: OPSS-Aud: Actual T&E
 - Audit: OPSS-Aud: Actual Hours
 - Plan: OPSS-Plan: Actual Hours
 - Plan: OPSS-Plan: Actual T&E
- Replaces the following computed fields with link fields:
 - Audit: OPSS-Aud: Close Audit
 - Audit: OPSS-Aud: Plans
 - Control Plan: OPSS-RiskEnt: Baselines
 - Resource: OPSS-Res: Resource Links
- Adds a primary parent to Preference objects. This updated is required by the Auditable Entity Weighted Risk Score calculation.

If you want to review the changes before you implement them, see the files that are listed in step 1.

Procedure

1. Copy the following files from the installation media to the application server. Or, if you run ObjectManager from a remote system, such as your laptop, copy the files to the remote system.

- IAM_ITG_computed_field_replacement-op-config.xml
- IAM_computed_field_preference_updates.xls

The files are located in the /OP_<version>_Main/OP_<version>_Configuration/Modules/IAM_ITG directory.

2. Open a command line.

If you are using Microsoft Windows, open a command prompt with the **Run as Administrator** option.

3. Go to the `<OP_HOME>/bin` directory.

Or, if you're running ObjectManager from a remote system, go to the `openpages-tools-client/bin` directory.


4. Run the following command to load the updated fields.

Replace `<loader-file-path>` with the location of the `IAM_ITG_computed_field_replacement-op-config.xml` file.

```
ObjectManager.cmd|sh 1 c <OpenPages Administrator user> <OpenPages Administrator password>
<loader-file-path> IAM_ITG_computed_field_replacement
```

If you encounter any errors, review the log file, `<loader-file-path>/ObjectManager.log`.

5. Use FastMap to load the Preference object changes:

- a) Log in to OpenPages as a user with administrative privileges.
- b) Click  > **FastMap** > **FastMap Import**.
- c) Click **Choose File** and select the `IAM_computed_field_preference_updates.xls` file.
- d) Click **Import data**.
- e) Review the verification report, and then click **Import data**.

Importing the solutions report packages after installing a fix pack

After you install an IBM OpenPages with Watson fix pack, import the solutions reports to update them.

For more information about importing content, see the *Cognos Analytics Administration and Security Guide*.

Procedure

1. Back up the following file if it exists: `<COGNOS_HOME>/deployment/OpenPages_Solutions_V6.zip`.
2. From a browser, log on to the IBM Cognos Analytics.
By default, the URL is `http://<hostname>:<port>/ibmcognos/bi`
Where `<hostname>` is the name of the Cognos server and `<port>` is the Cognos gateway port number (80 by default).
3. Click **Manage** > **Administration Console** to launch the **IBM Cognos Administration** page.
4. Click the **Configuration** tab and click **Content Administration**.
Tip: To access this area in IBM Cognos Administration, you must have the required permissions for the **Administration** secured feature.
5. On the toolbar, click **New Import**.
6. From the **Deployment archive** list, select **OpenPages_Solutions_v6**.
7. Click **Next**.
8. Type a unique name, an optional description, and a screen tip for the deployment archive, select the folder where you want to save it, and then click **Next**.
9. In the **Public folders, directory and library content** box, select **OpenPages_Solutions_v6**, and then click **Next**.
10. On the **Specify the general options** page, accept the default options and click **Next**.
11. On the **Review the summary** page, review the settings and click **Next**.
12. On the **Select an action page**, click **Finish**.
13. Click **Replace the existing entry**, and then click **OK**.
14. On the **Run with options** page, click **Run**.
15. On the **IBM Cognos software** page, click **OK**.

16. To view the imported packages and reports, click the **Home** icon, and select the folder where you imported them.

Regenerating the reporting framework

After you apply a IBM OpenPages with Watson fix pack, you might need to regenerate the reporting framework.

Fix pack 8.2.0.1 adds a number of new system fields and object types. If you plan to use the new capabilities and want to be able to access the new fields and object types in reports, regenerate the reporting framework.

You also need to regenerate the reporting framework if you have added new fields and you want to use the new fields in reports.

Regenerate the reporting framework after you have completed all other installation tasks.

For more information, see the *IBM OpenPages with Watson Administrator's Guide*.

Additional tasks for fix packs

You might want to complete additional tasks for an OpenPages fix pack.

Performing a silent installation of a fix pack

You can install a fix pack from the command line.

Before you begin

- Complete the following preparation tasks:
 - [“Review new features and fixes” on page 280](#)
 - [“Back up your existing environment” on page 280](#)
 - [“Verifying servers before you install a fix pack” on page 282](#)
- Ensure that the installation server is updated to the latest version. For more information, see [“Updating the installation server” on page 47](#).
- If you installed the agent software on remote servers manually, ensure that the agent software is updated to the latest version. Also, ensure that the agents are running. For more information, see [“Updating agents manually” on page 48](#).
- Verify that your deployment meets the system requirements for the fix pack.
- If you want to update the database manually, complete the database update before you install the fix pack. For more information, see [“Update the OpenPages database manually \(Db2\)” on page 282](#) or [“Update the OpenPages database manually \(Oracle\)” on page 289](#).

Procedure

1. Log on to the installation server computer as the user who installed the installation server.

Alternatively, you can log in as any user who has full permissions on the installation server directories and who can run `Node.js`.

2. Copy the fix pack kit to the installation server.

Copy `/OP_<version>_Main/OP_<version>_Installer/openpages_fixpack_<version>.zip` from the fix pack installation media to the `<Installation_server_home>/src/assets/maintenance` directory.

3. Go to the `<Installation_server_home>/src/deployment/<deployment_name>` directory.
4. Edit the `deploy.properties` file.
 - a) Change the value of the task property to `fix-pack`.

- b) Change the value of the `maintenance_version` property to the version of the fix pack that you are installing, for example 8.2.0.1.
- c) Update the value of the `install_db` property.
 - If you want the installation server to update the database to the fix pack version, change the value of the `install_db` property to `full`. This option requires DBA credentials.
 - If you updated the database manually, change the value of the `install_db` property to `done` or `nondba`.

Note: Use `done` or `nondba` only if all of the database update scripts completed successfully.

For more information, see [“Deployment file properties” on page 394](#).

- d) Save and close the file.

Tip: You can also update these properties by using the installation app. Open your deployment, click the task list and select **Fixpack**, select the fix pack version, and then click **Save**.

5. Run the silent installation from the command line.
 - a) Open a command prompt or open a shell window as an administrator.
 - b) Go to the `<Installation_server_home>` directory.
 - c) Run the following command:

```
npm run silent <deployment name> acceptLicense
```

Note: Do not close the command prompt or shell window until after the process completes.

6. Check the logs to ensure that the installation is successful.

Rolling back a fix pack

If you backed up your environment before you installed a fix pack, you can roll back the fix pack.

Before you begin

To roll back a fix pack, you need the following backup files:

- The manual backup files that you created before you installed the fix pack
- The backup files that were created by the installation server when you installed the fix pack

These backup files are stored in `<server_home>/installer/maintenance/fix-pack-<version>/backups_from_<previous-version>`. For example, on an application server the backup files are stored in `<OP_HOME>/installer/maintenance/fix-pack-<version>/backups_from_<previous-version>`

About this task

The following procedure assumes that you installed fix pack 8.2.0.1 on 8.2.0.0. It also assumes that the manual backup directories that you created use the name `OpenPages8200Backup`. Specify the name that you chose when you created the backup directories.

Procedure

1. Stop all servers:
 - OpenPages application servers (admin and non-admin)
 - IBM Cognos servers (active and standby)
 - OpenPages Framework Model Generator service
 - OpenPages search server

For more information, see [Chapter 12, “Starting and stopping servers,” on page 309](#).

2. To restore OpenPages application server directories and files, complete the following steps:
 - a) Log on to the admin application server as a user with administrative privileges and full access to the local server drives. For Linux, use a non-root user, such as the user you created for the OpenPages installation, for example `opuser`.
 - b) Copy all files and directories, except the items listed below, in the `<OP_HOME>/installer/maintenance/fix-pack-<version>/backups_from_<previous-version>` directory into the `<OP_HOME>` directory.

Do not copy the following items:
 - `roll_back_record.txt`
 - c) Copy all files and directories in the `<OP_HOME>/installer/maintenance/fix-pack-<version>/backups_from_<previous-version>/wlp-usr` directory into the `<OP_HOME>/wlp-usr` directory.
 3. To restore the IBM Cognos directories, complete the following steps:
 - a) Log on to the reporting server as a user with administrative privileges and full access to the local server drives. For Linux, use a non-root user, such as the user you created for the OpenPages installation, for example `opuser`.
 - b) Copy all files and directories, except the items listed below, in the `<CC_HOME>/installer/maintenance/fix-pack-<version>/backups_from_<previous-version>` directory into the `<CC_HOME>` directory.

Do not copy the following items:
 - COGNOS directory
 - `roll_back_record.txt`
 - c) Copy all files and directories in the `<CC_HOME>/installer/maintenance/fix-pack-<version>/backups_from_<previous-version>/COGNOS` directory into the `<COGNOS_HOME>` directory.
 4. To restore the search server directories and files, complete the following steps:
 - a) On the search server, navigate to the `<SEARCH_HOME>` directory.
 - b) Copy all files and directories, except the `roll_back_record.txt` file, in the `<SEARCH_HOME>/installer/maintenance/fix-pack-<version>/backups_from_<previous-version>` directory into the `<SEARCH_HOME>` directory.
 - c) Copy the following directories from the `OpenPages8200Backup/OPSearch` directory into the `<SEARCH_HOME>` directory:
 - `openpages-solr-index`
 - `openpages-solr-requesthandler`
 5. Restore the OpenPages database. Use the utilities that are provided with your database or use `OPRestore` and `OPCCRestore`.

For information about `OPRestore` and `OPCCRestore`, see the *IBM OpenPages with Watson Administrator's Guide*.
 6. Start all servers:
 - OpenPages application servers
 - IBM Cognos servers
 - OpenPages Framework Model Generator service
 - OpenPages search server
- For more information, see [Chapter 12, "Starting and stopping servers," on page 309](#).

Chapter 12. Starting and stopping servers

You can start and stop the IBM OpenPages with Watson application servers, the database server, the Cognos server, and the search server.

Starting application servers

You can start IBM OpenPages with Watson in Windows and Linux environments.

In a Windows environment, you can start the OpenPages with Watson application servers by using Microsoft Windows services or by running a script.

In a Linux environment, you run a script to start the OpenPages with Watson application servers.

If you are running OpenPages in a load-balanced environment, you must start the server on the cluster administrator first before starting a cluster member.

Starting application servers by using Windows services

You can start IBM OpenPages with Watson application servers by using Microsoft Windows services.

About this task

The OpenPages application service is called `<server_name>Server<#>`, where `<server_name>` is the name of the application server. You can find the server name in the following locations:

- In the installation app on the application server card
- In the `deploy.properties` file in the `op_server_name` property.

In a load-balanced environment with vertical cluster members, each vertical cluster is numbered in sequence: `<server_name>Server1`, `<server_name>Server2`, and so on.

By default, the `<server_name>Server<#>` services are configured as `Manual` (the services do not start upon reboot). You can configure a service to start automatically. In Windows Services, change the service to `Automatic`.

For the IBM OpenPages with Watson application to run, all of the required Microsoft Windows services must be started and the services of supporting applications must be running.

Tip: Alternatively, you can start all application services by using a script. For more information, see [“Starting all application services by running a script \(Windows\)”](#) on page 310.

Procedure

1. Log on to the application server as a user with administrative privileges.
2. Click **Start > Windows Administrative Tools > Services**.
3. Start each application service in sequence, starting with the `<server_name>Server1` service. Click the service, and then click **Start**.
The **Status** column might show **Running** before the startup process is done. Wait before starting the next application service.
Repeat this step for each application service that you want to start.
4. To set a service to start automatically after a restart, change its **Startup Type** to **Automatic**.
5. If you have horizontal application servers, repeat these steps on each of them.

Starting all application services by running a script (Windows)

The `StartAllServers.cmd` script, which is included with IBM OpenPages with Watson, starts all OpenPages application services on an application server.

Note: This information applies only to Microsoft Windows environments.

About this task

The script uses the following syntax:

```
StartAllServers.cmd [--clean]
```

The `--clean` option is not necessary for normal operation. IBM OpenPages Support might ask you to use this option when providing an interim fix, or if there is a suspected problem with the cached data. If you use this option, the server will be required to recompute any cached data at the next startup, which might take more time than a restart that reuses cached data.

Procedure

1. Log on to the OpenPages with Watson application server as a user with administrative privileges or as the OpenPages installation user, `opuser`.
2. Open a Command Prompt window (using the **Run as administrator** option) and do the following:
 - a) Navigate to the `<OP_HOME>\bin` directory.

Where `<OP_HOME>` is the installation location of the OpenPages with Watson application, for example: `c:\IBM\OpenPages`.

- b) Run the following command:

```
StartAllServers.cmd
```

The log file is: `<OP_HOME>\wlp-usr\servers\<server_name>\logs\messages.log`

3. If you have horizontal application servers, repeat these steps on each of them.

Starting all application servers by running a script (Linux)

The `startAllServers.sh` script, which is included with IBM OpenPages with Watson, starts all OpenPages application services on an application server.

Note: This information applies only to Linux environments.

About this task

The script uses the following syntax:

```
./startAllServers.sh [--clean]
```

The `--clean` option is not necessary for normal operation. IBM OpenPages Support might ask you to use this option when providing an interim fix, or if there is a suspected problem with the cached data. If you use this option, the server will be required to recompute any cached data at the next startup, which might take more time than a restart that reuses cached data.

The OpenPages application runs only if all of the services are started and all of the services for all supporting applications are running.

Procedure

1. Log on to the OpenPages application server as a user with administrative privileges or as the OpenPages installation user, `opuser`.
2. Open a shell window.

3. Go to the `<OP_HOME>/bin` directory.
4. Run the following script:

```
./startAllServers.sh
```

The application services on the application server are started.

The log file is: `<OP_HOME>/wlp-user/servers/<server_name>/logs/messages.log`

5. If you have horizontal application servers, repeat these steps on each of them.

Determining application readiness

This procedure lets you determine whether the application is ready to be accessed after starting up servers.

Procedure

1. Open the following log file:
`<OP_HOME>/wlp-user/servers/<server_name>/logs/messages.log`
Where `<server_name>` is the name of the application server.
2. Scroll to the end of the log file and search for the message `SRVE0242I: [op-apps] [/grc] [api-rest]: Initialization successful`. If this line appears, the server is running in production mode and the application is ready to be accessed.

Stopping application servers

You can stop IBM OpenPages with Watson application servers in Windows and Linux environments.

Stopping the application server prevents IBM OpenPages with Watson from being accessed.

Important: If you are running OpenPages with Watson in a load-balanced environment, stop `<server_name>Server1` last.

Stopping application servers by using Windows services

You can stop IBM OpenPages with Watson application servers by using Microsoft Windows services.

About this task

Stopping the application services prevents IBM OpenPages with Watson from being accessed.

Tip: Alternatively, you can stop all vertical cluster members on an application server by using a script. For more information, see [“Stopping all application servers in Windows by using a script” on page 311](#).

Procedure

1. Log on to the application server as a user with administrative privileges.
2. Click **Start > Windows Administrative Tools > Services**.
3. Click the `<server_name>Server<#>` service and then click **Stop**. Repeat this step for each application service that you want to stop. If you have horizontal application servers, repeat these steps on each of them.

Stopping all application servers in Windows by using a script

The `StopAllServers.cmd` stops all OpenPages application services on an application server. The script stops the services in the proper sequence.

Stopping the application services prevents the OpenPages application from being accessed.

Procedure

1. Log on to the OpenPages with Watson application server as a user with administrative privileges.
2. Launch a Command Prompt window (using the **Run as administrator** option).
3. Navigate to the <OP_HOME>\bin directory.
4. Run the following command:

```
StopAllServers.cmd
```

5. If you have horizontal application servers, repeat these steps on each of them.

Stopping all application servers on Linux by using a script

The stopAllServers.sh script stops all OpenPages application services on an application server. The script stops the application services in the proper sequence.

Stopping the application services prevents the OpenPages application from being accessed.

Procedure

1. Log on to the OpenPages with Watson application server as a user with administrative privileges.
2. Open a shell window and navigate to the <OP_HOME>/bin directory.
3. Run the following command:

```
./stopAllServers.sh
```

The application services on the application server are stopped.

4. If you have horizontal application servers, repeat these steps on each of them.

Start or stop the global search services

You can start and stop the global search services by using operating system services or by using scripts.

Note: Do not combine the two methods. If you start global search as a Microsoft Windows service, for example, stop global search by stopping the Windows service.

Starting the global search services by using a script

You can start the global search services by running a script from a command line.

Before you begin

On the Windows operating system, disable the Microsoft Windows service that is called **IBM OpenPages GRC - Global Search**, if it is enabled. Otherwise, the StartSearchServers.cmd script interferes with the Windows services.

Make sure that the database server is reachable and is running. Otherwise, the search services will not connect and will not start.

Procedure

1. Start the search services:
 - For Windows, at a command prompt enter the following commands:

```
cd <SEARCH_HOME>\opsearchtools\  
StartSearchServers.cmd
```

- For Linux, at a command line, enter the following commands:

```
cd <SEARCH_HOME>/opsearchtools/  
./StartSearchServers.sh
```

2. Open a browser and point to your search server at ports 8983 and 8985. Make sure that the Solr search platform can be reached.
For example, `http://<search-server>:8983/` and `http://<search-server>:8985/`.
If the verification fails, repeat the preceding step.
3. Log on to IBM OpenPages with Watson as an administrator.
4. Switch to the Standard UI.
5. Click **Administration > Global Search > Enable**.

Stopping the global search services by using a script

You can stop the global search services by running a script from a command line.

Before you begin

On the Windows operating system, disable the Microsoft Windows service that is called **IBM OpenPages GRC - Global Search**, if it is enabled. Otherwise, the `StopSearchServers.cmd` script interferes with the Windows services.

Procedure

1. Log on to IBM OpenPages with Watson as an administrator.
2. Switch to the Standard UI.
3. Click **Administration > Global Search > Disable**.
4. Stop the search services:
 - For Windows, at a command prompt, enter the following commands:

```
cd <SEARCH_HOME>\opsearchtools\  
StopSearchServers.cmd
```

- For Linux, at a command line, enter the following commands:

```
cd <SEARCH_HOME>/opsearchtools/  
./StopSearchServers.sh
```

5. For either Windows or Linux, verify that global search is fully stopped.
 - a) In the directory `<SEARCH_HOME>/opsearchtools/`, examine the files `opsearchtool_openpages.state` and `opsearchtool_folderacl.state` and verify that the PID value is -1.
 - b) Open a browser and point to your search server at ports 8983 and 8985. Make sure that the Solr search platform cannot be reached.
For example, `http://<search-server>:8983/` and `http://<search-server>:8985/`.
If the stop verification fails, repeat the preceding step and then follow the steps in [“Forcing a reset of global search” on page 435](#).

Starting the global search services on Windows

You can start global search as a Microsoft Windows service. The service is called **IBM OpenPages GRC - Global Search**.

About this task

By default, the service is set to start manually, but you can change the service to start automatically.

Note: Make sure that the database server is reachable and is up and running. Otherwise, the search services will not connect and will not start.

Procedure

1. Log on to the search server as a user with administrative privileges.
2. Click **Start > Windows Administrative Tools > Services**.
3. Locate the service that is called **IBM OpenPages GRC - Global Search**.
4. Click **Start**.
5. If you want the service to start automatically when Windows starts, change the **Startup Type** to **Automatic**.
6. Open a browser and point to your search server at ports 8983 and 8985. Make sure that the Solr search platform can be reached.
For example, `http://<search-server>:8983/` and `http://<search-server>:8985/`.
If the verification fails, repeat the preceding step.
7. Log on to IBM OpenPages with Watson as an administrator.
8. Switch to the Standard UI.
9. Click **Administration > Global Search > Enable**.

Starting the global search services on Linux

You can start global search as a service.

About this task

Use the steps in this topic as a guide. Depending on your environment and organization policies, you might decide to use a different method to set up the search service. If you want to use a different method, open the `openpages-search` file and check the commands, and the order of the commands. Modify the commands to meet the needs of your environment.

Note: Make sure that the database server is reachable and is up and running. Otherwise, the search services will not connect and will not start.

Procedure

1. Log on to the search server.
2. Open a shell as the root user.
3. Copy the `<SEARCH_HOME>/opsearchtools/openpages-search` file to the `/etc/init.d/` directory.
4. Copy the `<SEARCH_HOME>/opsearchtools/openpages-search-cfg` file to the `/etc/sysconfig/` directory.
5. Set the execution permission on the `openpages-search` file by running the following command:
`chmod +x /etc/init.d/openpages-search`
6. If you want the service to start automatically when the system restarts, run the following commands:

```
chkconfig --add openpages-search
chkconfig openpages-search on
service openpages-search start
```

7. Start the global search services by running the following command: `service openpages-search start`
8. Open a browser and point to your search server at ports 8983 and 8985. Make sure that the Solr search platform can be reached.
For example, `http://<search-server>:8983/` and `http://<search-server>:8985/`.
If the verification fails, repeat the preceding step.

9. Log on to IBM OpenPages with Watson as an administrator.
10. Click **Administration > Global Search > Enable**.

Stopping the global search services

If global search is running as a service, you can use the operating system to stop the global search services.

About this task

If you used the `StartSearchServers.sh | .cmd` script to start the global search services, use the `StopSearchServers.sh | .cmd` script to stop the services. For more information, see [“Stopping the global search services by using a script”](#) on page 313.

Procedure

1. Log on to IBM OpenPages with Watson as an administrator.
2. Click **Administration > Global Search > Disable**.
3. Log on to the search server as a user with administrative privileges.
4. Stop the search services.

Windows:

- a) Click **Start > Windows Administrative Tools > Services**.
- b) Locate the service that is called **IBM OpenPages GRC - Global Search**.
- c) Click **Stop**.

On Linux, run the following command:

```
service openpages-search stop
```

5. Verify that global search is fully stopped.
 - a) In the directory `<SEARCH_HOME>/opsearchtools/`, examine the files `opsearchtool_openpages.state` and `opsearchtool_folderacl.state` and verify that the PID value is -1.
 - b) Open a browser and point to your search server at ports 8983 and 8985. Make sure that the Solr search platform cannot be reached.
For example, `http://<search-server>:8983/` and `http://<search-server>:8985/`.
If the stop verification fails, repeat the preceding step and then follow the steps in [“Forcing a reset of global search”](#) on page 435.

Start or stop the database services

You can start and stop the database services.

For more information, see the documentation that is provided with your database server:

IBM Db2

[Managing instances](#)

Oracle

[Starting Up and Shutting Down](#)

For examples, see [“Starting and stopping the Oracle database server in a Windows environment”](#) on page 315 or [“Starting and stopping the Oracle database server in Linux environments”](#) on page 316.

Starting and stopping the Oracle database server in a Windows environment

The following steps show an example of how to start or stop an Oracle database server by using Windows services.

About this task

For more information, see the Oracle [documentation](#).

Table 72. Oracle services for OpenPages on Windows	
Service Name	Description
Oracle<ORACLE_HOME>TNSListener	Runs the Oracle Database listener service that connects the user to the Oracle database instance.
OracleService<SID>	Used to start and stop the Oracle database instance. Where <SID> represents the database instance identifier, for example OP.
OracleVssWriter<SID>	Where <SID> represents the database instance identifier, for example OP.

Procedure

1. Log on to the database server as a user with administrative privileges.
2. Click **Start > Windows Administrative Tools > Services**.
3. For each database service listed in [Table 72 on page 316](#), do the following:
 - To start the server, right-click the service name and select **Start**.
 - To stop the server, right-click the service name and select **Stop**.

Starting and stopping the Oracle database server in Linux environments

The following steps show an example of how to start or stop an Oracle database.

For more information, see the Oracle [documentation](#).

Procedure

1. Log on to the database server as a user with administrative privileges.
2. In a shell window, navigate to the following directory:

```
<ORACLE_HOME>/bin
```

For example: /opt/oracle/app/product/19.0/dbhome_1/bin.

3. To start Oracle, do the following steps.

- a) Log in to SQL*Plus.

```
sqlplus / as sysdba
```

- b) Run the following command to start Oracle.

```
startup
```

4. To stop Oracle, do the following steps.

- a) Log in to SQL*Plus.

```
sqlplus / as sysdba
```

- b) Run the following command to stop Oracle.

```
stop immediate
```

Starting and stopping the Cognos services

There are different procedures to start or stop the Cognos services in the Windows and Linux environments. The services are the IBM Cognos service and the OpenPages Framework Model Generator service

These procedures are:

- [“Using the IBM Cognos configuration tool to start and stop the IBM Cognos service” on page 317](#)
- [“Using the Windows operating system to start and stop the IBM Cognos service” on page 317](#)
- [“Using the Linux operating system to start and stop the IBM Cognos service” on page 318](#)
- [“Starting and stopping the OpenPages with Watson Framework Model Generator service on Windows” on page 318](#)
- [“Starting and stopping the OpenPages with Watson Framework Model Generator service on Linux” on page 318](#)

Using the IBM Cognos configuration tool to start and stop the IBM Cognos service

You can use the IBM Cognos Configuration tool to start or stop the IBM Cognos service.

The IBM Cognos Configuration tool displays the status of the start-up, which can be helpful with troubleshooting.

Procedure

1. Log on to the reporting server as a user with administrative privileges.
2. Start the IBM Cognos Configuration tool as follows:
 - a) Open a command prompt (using the **Run as administrator** option), or a Linux shell, and navigate to the `<COGNOS_HOME>/bin` directory.
`<COGNOS_HOME>` represents the installation location of the Cognos application.
 - b) Run one of the following commands to open the tool:
Windows
`cogconfig.bat`
Linux
`./cogconfig.sh`
3. Do one of the following:
 - To start the server, click **Actions > Start**. It might take several minutes for the service to start the first time.
If the **Start** option is not available, the service has already started.
 - To stop the service, click **Actions > Stop**.

Using the Windows operating system to start and stop the IBM Cognos service

Use the following steps to start or stop the IBM Cognos service in a Windows environment using Windows Services.

Procedure

1. Log on to the reporting server as a user with administrative privileges.
2. Click **Start > Windows Administrative Tools > Services**.
3. Do one of the following:

- To start the server, right-click the IBM Cognos service and select **Start**.
- To stop the server, right-click the IBM Cognos service and select **Stop**.

Using the Linux operating system to start and stop the IBM Cognos service

Use the following steps to start or stop the IBM Cognos service in a Linux environment using command-line scripts.

Procedure

1. Log on to the reporting server as a non-root user with administrative privileges.
2. Open a shell window and navigate to the `<COGNOS_HOME>/bin64` directory
Where `<COGNOS_HOME>` is the installation location of the Cognos application.
3. Do one of the following:
 - To start the service, enter the following command: `./cogconfig.sh -s`
 - To stop the service, enter the following command: `./cogconfig.sh -stop`

Starting and stopping the OpenPages with Watson Framework Model Generator service on Windows

Use the following steps to start or stop the IBM OpenPages with Watson Framework Model Generator service in a Microsoft Windows environment.

Procedure

1. Log on to the reporting server as a user with administrative privileges.
2. Click **Start > Windows Administrative Tools > Services**.
3. Do one of the following:
 - To start the server, right-click the `IBMOpenPagesFrameworkModelGenerator` service and select **Start**.
 - To stop the server, right-click the `IBMOpenPagesFrameworkModelGenerator` service and select **Stop**.

Starting and stopping the OpenPages with Watson Framework Model Generator service on Linux

Use the following steps to start or stop the `IBMOpenPagesFrameworkModelGenerator` service in a Linux environment.

Procedure

1. Log on to the reporting server as a non-root user with administrative privileges.
2. Open a shell window as a user with administrative privileges and navigate to the following directory:

```
<CommandCenter_Home>/wlp/bin
```

Where `<CommandCenter_Home>` is the installation location of IBM OpenPages CommandCenter. By default, this is: `/opt/IBM/OpenPages/CommandCenter`.

3. To start the service, run the following command.

```
./server start IBMOpenPagesFrameworkModelGenerator
```

4. To stop the service, run the following command.


```
./server stop IBMOpenPagesFrameworkModelGenerator
```

Chapter 13. Single sign-on integration for the OpenPages application server

IBM OpenPages with Watson can integrate into a number of single sign-on solutions, such as SAML 2.0, SPNEGO, OpenID Connect, and header-based single sign-on.

You can use one of the following integrations to configure single sign-on with OpenPages:

- SAML 2.0 single sign-on

For more information, see [“Configuring SAML single sign-on” on page 321](#).

You can also use SAML 2.0 single sign-on in mixed mode. In mixed-mode SSO, some users log in with SSO while others log in with their OpenPages credentials. For more information, see [“Configuring mixed mode single sign-on \(SAML and IBM OpenPages with Watson\)” on page 326](#).

- SPNEGO (Kerberos) single sign-on

For more information, see [“Configuring SPNEGO single sign-on” on page 331](#).

- OpenID Connect single sign-on

For more information, see [“Configuring single sign-on by using OpenID Connect” on page 336](#).

- Header-based single sign-on

For more information, see [“Configuring header-based single sign-on” on page 339](#).



Attention: OpenPages user names are case-sensitive. If you are using single sign-on (SSO) or LDAP authentication, the user name you choose here must match the user name you enter in the SSO or LDAP system.

You can enable trace logging for single sign-on events (excluding header-based single sign-on). For more information, see the *IBM OpenPages with Watson Administrator's Guide*.

For information about setting up single sign-on for reporting servers, see the [Cognos Analytics documentation](#).

Configuring SAML single sign-on

You can use SAML single sign-on with IBM OpenPages with Watson. These steps use Microsoft Active Directory Federation Server (ADFS) as the Identity Provider (IdP), but you can use any IdP that supports the SAML 2.0 protocol.

Before you begin

Your environment must meet the following prerequisites:


- An ADFS server is set up and running.
- User accounts are set up in both ADFS and OpenPages. The usernames must be the same in each system.
- OpenPages 8.2 or later is installed and the OpenPages servers are running.
- You can log in to the OpenPages application from your browser.

About this task

This video shows an example of how to configure SAML SSO: <https://youtu.be/f09YOiQcdfI>.

Procedure

1. Enable single sign-on in OpenPages.

- a) Log on to the OpenPages application as a user with administrative permissions.
 - b) Click  > **System Configuration** > **Settings**.
 - c) Click **Applications** > **Common** > **Configuration**. Change **Show Hidden Settings** to true.
 - d) Update the following settings:
 - Change **Platform** > **Security** > **Single Sign On** > **Implementations** > **Current** to HTTP-User-based
 - Change **Platform** > **Security** > **Single Sign On** > **SOX** to true
 - Change **Platform** > **Security** > **Single Sign On** > **OP** to true
2. Install SAML single sign-on for IBM WebSphere Liberty.
- a) Log on to the OpenPages application server.
 - b) Install the `samlWeb-2.0` feature by running the following command:

```
<WLP_HOME>/bin/installUtility install samlweb-2.0
```

3. Configure single sign-on in WebSphere Liberty.
- a) Go to the following directory: `<WLP_USER_DIR>/servers/<server_name>Server<#>/configDropins/overrides`
- If the directory does not exist, create it.
- b) Create a new `.xml` file (for example, `OP_SSO_SAML_config.xml`).
 - c) Add the following lines to the file.

```
<server>
  <featureManager>
    <feature>samlWeb-2.0</feature>
  </featureManager>
  <!-- SAML SSO configuration - Single IdP -->
  <samlWebSso20 id="<saml_id>"
    disableLtpaCookie="false"
    allowCustomCacheKey="false"
    mapToUserRegistry="No"
    idpMetadata="<OP_HOME>/wlp-usr/servers/<server_name>Server<#>/resources/security/
    FederationMetadata.xml"
    enabled="true"
    spLogout="false"
    nameIDFormat="unspecified">
    <authFilter id="samlAuthFilter">
      <requestUrl id="openpagesUrl" urlPattern="/grc/api" matchType="notContain"/>
    </authFilter>
  </samlWebSso20>
</server>
```

For `<saml_id>`, type an identifier for the SAML configuration. Use `defaultSP`.

Note: If you use a `<saml_id>` other than `defaultSP`, you must explicitly disable the `defaultSP` instance. For more information, see the [Liberty documentation](#).

For `idpMetadata`, replace `<OP_HOME>` and `<server_name>Server<#>` with the values for your application server. You get the `FederationMetadata.xml` file in step “7” on page 323.

The `<requestUrl>` element in this sample configuration excludes the REST API from SSO. You can change the configuration:

- If you want to use multiple filters, create additional `<requestUrl>` elements. Give each of them a unique id.

Ensure that the `<authFilter>` element does not contain `<requestUrl>` filters that conflict.

For more information, see [Authentication Filters](#) in the WebSphere Liberty documentation.

- If you want to use SSO for all OpenPages URLs, remove the `<authFilter>` element and its child `<requestUrl>` elements.

Save and close the file.

4. Export the Token-signing certificate from the ADFS server.

For more information, see the documentation that is provided with ADFS.

5. Import the Token-signing certificate to the OpenPages keystore:

```
keytool -importcert -v -alias adfs -file adfsSignedCert.cer -keystore <OP_HOME>/wlp-user/
servers/<server_name>Server<#>/resources/security/key.p12 -storetype PKCS12
```

6. Set up the relying party trust in ADFS.

For more information, see the ADFS documentation.

In this step, you export metadata from the SAML Service Provider (WebSphere Liberty) and import it into the Identity Provider (ADFS). You then define claim rules for the relying party trust.

- a) Export the metadata from WebSphere Liberty by going to the following URL in a browser:

- Replace `<op_app_server>` and `<op_port>` with the host and port of the OpenPages application server.
- Replace `<saml_id>` with the `id` attribute that you specified in the `<samlWebSso20>` element in the `OP_SSO_SAML_config.xml` file.

```
https://<op_app_server>:<op_port>/ibm/saml20/<saml_id>/samlmetadata
```

For example:

```
https://my.app.server:10111/ibm/saml20/defaultSP/samlmetadata
```

- b) Import the WebSphere Liberty metadata to the ADFS server. In the ADFS **Server manager**, click **Tools > AD FS Management > Add Relying Party Trust**.

- c) Add the following two custom claim rules to the relying party trust:

Claim rule name: GetUpn

Custom rule:

```
c:[
  Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
  Issuer == "AD AUTHORITY"
]
=>
add(
  store = "Active Directory",
  types = ("UpnHolder"),
  query = ";userPrincipalName;{0}",
  param = c.Value
);
```

Claim rule name: UpnToNameID

Custom rule:

```
c:[
  Type == "UpnHolder"
]
=>
issue(
  Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
  Value = RegexReplace(c.Value, "(?<user>[^\@]+)(?<domain>.+)", "${user}")
);
```

The WebSphere Liberty metadata is now in ADFS.

7. Export metadata from the Identity Provider (ADFS) and import it into the SAML Service Provider (WebSphere Liberty).

- a) Export the ADFS federation metadata file by going to the following URL in a browser:

Replace `<ADFS_URL>` with the ADFS server URL.

```
https://<ADFS_URL>/FederationMetadata/2007-06/FederationMetadata.xml
```

- b) Rename the exported ADFS federation metadata file to match the name that you used in the `idpMetadata` attribute in step “3.c” on page 322.
- c) Place the metadata file on the application server in the directory that you specified in the `idpMetadata` attribute value.

```
idpMetadata="<OP_HOME>/wlp-usr/servers/<server_name>Server<#>/resources/security/
FederationMetadata.xml"
```

The ADFS metadata is now in WebSphere Liberty.

8. Stop all OpenPages services.

For more information, see “[Stopping application servers](#)” on page 311.

9. Restart all OpenPages services.

Linux

Go to the `<OP_HOME>/bin` directory and run the following command:

```
./startAllServers.sh --clean
```

Windows

- If you use a script to start and stop application servers, go to the `<OP_HOME>\bin` directory and run the following command:

```
StartAllServers.cmd --clean
```

- If you use Windows services to start and stop application servers, you need to do some cleanup before you start the services. Go to the `<OP_HOME>/wlp-usr/servers/<server_name>Server<#>/workarea` directory. Remove all of the files.

10. After you confirm that single sign-on is working, do the following steps:

- a) Click  > **System Configuration** > **Settings**.
- b) Change **Platform** > **Security** > **Form Based Login** > **Enabled** to false.

11. Set user passwords to never expire. See “[Setting user passwords to never expire](#)” on page 343.

- If a user attempts to log in with an account that does not exist in OpenPages or with an account that is disabled, the user sees the following message:

```
You are not authorized to access this application.
Please contact your Administrator.
```

- You can enable trace logging for single sign-on events. For more information, see the *IBM OpenPages with Watson Administrator's Guide*.

What to do next

If you want to configure mixed-mode, see “[Configuring mixed mode single sign-on \(SAML and IBM OpenPages with Watson\)](#)” on page 326. Otherwise, change the users' passwords from their defaults in OpenPages to prevent the users from logging in with their OpenPages credentials. Note the following exceptions:

- If you are using mixed-mode SSO, do not change the passwords of users who log in by using OpenPages authentication (also called *native* authentication).
- Do not change the passwords of user accounts that access the REST API.

If you are using a load balancer or a proxy server, additional configuration is required. See [Configuring IBM HTTP Server to load balance application servers](#).


Disabling SAML single sign-on

You can disable SAML single sign-on (SSO) for IBM OpenPages with Watson.

Before you begin

The OpenPages with Watson services are running.

Procedure

1. Log on to the IBM OpenPages with Watson admin application server as a user with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
3. Expand **Platform** > **Security** > **Single Sign On**.
4. Update the following settings:
 - Click **SOX** and set its value to false.
 - Click **OP** and set its value to false.
5. Expand **Platform** > **Security** > **Form Based Login** > **Enabled**. Set its value to true.
6. Remove the override XML file that contains the SAML SSO configuration from the overrides directory.
For example, move `<WLP_USER_DIR>/servers/<server_name>Server</#>/configDropins/overrides/OP_SSO_SAML_config.xml` to a backup location.
Or, comment out the contents of the file.
7. Restart the OpenPages with Watson services.

Configuring an error page for SAML single sign-on

You can specify a page to display when an error occurs with SAML single sign-on. The page is displayed, for example, if a user attempts to log in with an account that does not exist in OpenPages, or if a problem is found with the SSO configuration. This task is optional.

Before you begin

Your environment must be configured for SAML SSO. For more information, see [“Configuring SAML single sign-on” on page 321](#).

Fix pack 8.2.0.1 or later must be installed.

About this task

By default, the message `Error 500` is displayed in the user's browser. OpenPages provides an alternate error page that you can use instead. To configure an alternate error page, update your SAML configuration.

Procedure

1. Go to the following directory: `<WLP_USER_DIR>/servers/<server_name>Server</#>/configDropins/overrides`
2. Open the file that contains the SAML SSO configuration, for example `OP_SSO_SAML_config.xml`.
3. Within the `<samlWebSso20>` element, create a new line and add the `errorPageUrl` parameter.

```
errorPageUrl="https://<server>:<port>/SAMLErrorMsg.jsp"
```

Replace `<server>` and `<port>` with the OpenPages application host name and port number.

The result is:

```
errorPageUrl="https://my.server.com:10111/SAMLErrorMsg.jsp"
```

4. Within the `<authFilter>` element, create a new line and add the following `<requestUrl>` to allow unauthenticated users to access the error page.

```
<requestUrl id="errorPage" urlPattern="SAMLErrorMsg" matchType="notContain"/>
```

Save and close the file.

For more information, see [Authentication Filters](#) in the WebSphere Liberty documentation.

For example:

```
<server>
  <featureManager>
    <feature>samlWeb-2.0</feature>
  </featureManager>
  <!-- SAML SSO configuration - Single IdP -->
  <samlWebSso20 id="<saml_id>"
    errorPageUrl="https://my.server.com:10111/SAMLErrorMsg.jsp"
    disableLtpaCookie="false"
    allowCustomCacheKey="false"
    mapToUserRegistry="No"
    idpMetadata="<OP_HOME>/wlp-usr/servers/<server_name>Server<#>/resources/security/
    FederationMetadata.xml"
    enabled="true"
    spLogout="false"
    nameIDFormat="unspecified">
    <authFilter id="samlAuthFilter">
      <requestUrl id="openpagesUrl" urlPattern="/grc/api" matchType="notContain"/>
      <requestUrl id="errorPage" urlPattern="SAMLErrorMsg" matchType="notContain"/>
    </authFilter>
  </samlWebSso20>
</server>
```

5. Stop and then restart the OpenPages services.

Configuring mixed mode single sign-on (SAML and IBM OpenPages with Watson)

You can use SAML single sign-on in mixed-mode with IBM OpenPages with Watson. In a mixed-mode configuration, most users log in by using the SAML Identity Provider (IdP) and a small subset of users log in by using their OpenPages credentials. These steps use Microsoft Active Directory Federation Server (ADFS) as the IdP, but you can use any IdP that supports the SAML 2.0 protocol.

Before you begin

Your environment must meet the following prerequisites:

- An ADFS server is set up and running.
- The user accounts for SSO users are set up in both ADFS and OpenPages. The usernames must be the same in each system.
- OpenPages 8.2 or later is installed and the OpenPages servers are running.
- You can log in to the OpenPages application from your browser.

About this task

In mixed-mode SSO, most users log in by using the IdP login page. When these users go to the OpenPages URL, the browser redirects them to the IdP login page. After they authenticate, they can access OpenPages.

Non-SSO users access OpenPages through an alias URL. When these users go to the alias URL, the browser displays the OpenPages login page. After they authenticate, they can access OpenPages.

Users who log in by using the alias URL might encounter several limitations, primarily to end user features. Mixed-mode SSO is intended to support users who have accounts that are used for administration and to support service accounts that are not covered by the IdP.

Non-SSO users might notice the following limitations:

- Cross-track links in Cognos reports might not work.

Cross-track links to OpenPages resources typically contain the OpenPages URL only, not the alias URL. As a result, non-SSO users cannot use the cross-track links directly.

- Links in JSP helpers might not work.

Some helpers might contain links to the OpenPages URL in `application.url.path`. As a result, the helpers might not work for non-SSO users.

- Some of the email notifications that are generated by OpenPages contain links to OpenPages resources. These links typically use the OpenPages URL as the base of the link. Examples include the emails generated by workflows, lifecycles, triggers, and batch notifications. You can replace these default email notifications with custom behavior to provide links for both the OpenPages and the alias URL.

These steps are written for environments that use TLS/SSL. If you do not use TLS/SSL, note the following differences:


- In step “4” on page 327, the alias that you create must be a sub-domain of the non-alias domain. For example, if your OpenPages URL is `http://myserver.mycompany.com:10108`, you can use `http://alias.mycompany.com:10108`.
- Skip step “7” on page 328b. Do not add the line `Header edit Set-Cookie (.*) "$1; SameSite=None; Secure"`.

Procedure

1. Configure SAML single sign-on.

For more information, see “[Configuring SAML single sign-on](#)” on page 321.

For non-SSO users, skip the step about setting user passwords to never expire.

2. Click  > **System Configuration > Settings**.
3. Expand **Platform > Security > Form Based Login > Enabled**. Set its value to true.
4. Create an alias URL.

Create a new DNS alias for the same IP address as the OpenPages application server. This DNS alias enables users to send requests to the same IP address by using a different URL. For example, these steps use the DNS alias `alias.openpages.com`, which means that the alias URL is `https://alias.openpages.com:10111`, where 10111 is the port number of the OpenPages application server.

You must have a DNS record for the alias URL so that end users' browsers can resolve the alias URL to the application server's address.

5. Update the single sign-on configuration in WebSphere Liberty.
 - a) Go to the following directory: `<WLP_USER_DIR>/servers/<server_name>Server<#>/configDropins/overrides`
 - b) Open the file that contains the SAML SSO configuration, for example `OP_SSO_SAML_config.xml`.
 - c) Locate the following line in the file:

```
<requestUrl id="openpagesUrl" urlPattern="/grc/api" matchType="notContain"/>
```

- d) Create a new line and add the following `<requestUrl>`.

```
<requestUrl id="openpagesAlias" urlPattern="<alias_url>" matchType="notContain"/>
```

Replace `<alias_url>` with the alias URL that you created, for example `alias.openpages.com`.

The result is:

```
<server>
  <featureManager>
    <feature>samlWeb-2.0</feature>
  </featureManager>
  <!-- SAML SSO configuration - Single IdP -->
  <samlWebSso20 id="defaultSP"
    disableLtpaCookie="false"
```

```

allowCustomCacheKey="false"
mapToUserRegistry="No"
idpMetadata="<OP_HOME>/wlp-usr/servers/<server_name>Server<#>/resources/security/
FederationMetadata.xml"
enabled="true"
spLogout="false"
nameIDFormat="unspecified">
<authFilter id="samlAuthFilter">
<requestUrl id="openpagesUrl" urlPattern="/grc/api" matchType="notContain"/>
<requestUrl id="openpagesAlias" urlPattern="alias.openpages.com" matchType="notContain"/>
</authFilter>
</server>

```

Save and close the file.

For more information, see [Authentication Filters](#) in the WebSphere Liberty documentation.

6. Configure the web server that you are using for Cognos.

Do this step so that users who log in to OpenPages by using the alias URL can access reports.

IBM HTTP Server or Apache Web Server

Add the alias URL to the Content-Security-Policy and X-Frame-Options headers on the web server.

a. On the web server, edit the following file in a text editor:

- IBM HTTP Server: <IHS_HOME>/conf/httpd.conf
- Apache Web Server: <Apache_HOME>/conf/httpd.conf

b. Look for the Content-Security-Policy and X-Frame-Options lines under LoadModule headers_module modules/mod_headers.so.

c. After the https://<opserver_host>:<opserver_port>/ lines, add the alias URL. The result is:

```

LoadModule headers_module modules/mod_headers.so
Header always set Content-Security-Policy "frame-ancestors 'self'
https://<opserver_host>:<opserver_port>/ https://<alias_hostname>:<opserver_port>;"
Header always set X-Frame-Options "ALLOW-FROM https://<opserver_host>:<opserver_port>/
https://<alias_hostname>:<opserver_port>"

```

The <alias_hostname> must be lowercase.

d. Save and close the file.

e. Restart the web server.

Microsoft Internet Information Server (IIS)

Add the alias URL to the Content-Security-Policy and X-Frame-Options headers. For more information, see the documentation that Microsoft provides for IIS.

7. Optional: Configure the Cognos web server to add the SameSite attribute to its cookies.

Do this step if your alias URL uses a different site name than your original OpenPages URL. For example, if your URLs are openpages.yourcompany.com and alias.openpages.com, your URLs are using different site names. Depending on the browsers that you use, you might need to configure Cognos to add the SameSite attribute to its cookies so that Cognos reports display properly in OpenPages.

IBM HTTP Server or Apache Web Server

a. On the web server, edit the following file in a text editor:

- IBM HTTP Server: <IHS_HOME>/conf/httpd.conf
- Apache Web Server: <Apache_HOME>/conf/httpd.conf

b. Add the following line to the bottom of the file:

```
Header edit Set-Cookie (.*) "$1; SameSite=None; Secure"
```

c. Save and close the file.

d. Restart the web server.

Microsoft Internet Information Server (IIS)

For more information, see the documentation that Microsoft provides for IIS.

8. Stop and then restart the OpenPages services.
9. If your alias URL uses a different site name than your original OpenPages URL, inform the users who will use the alias URL that they must change their browser settings to allow third-party cookies from the original OpenPages URL.

For example, if your URLs are `openpages.yourcompany.com` and `alias.openpages.com`, your URLs are using different site names. Ask users to update their browser settings to allow third-party cookies from `openpages.yourcompany.com`. In Chrome, for example, add `openpages.yourcompany.com` to the **Sites that can always use cookies** list.



Trouble:

If a user gets the following error when they run a Cognos report when they're logged in to the alias URL, check their browser settings.

```
com.openpages.security.auth.AuthenticationException: 401:Login failed with error  
response 401: Unauthorized
```

Ensure that the browser allows third-party cookies from the original OpenPages URL.

Configuring multiple IDs for a SAML identity provider

You can create multiple login points for a SAML identity provider (IdP) by configuring multiple IDs. These steps use Microsoft Active Microsoft Directory Federation Server (ADFS) as the IdP, but you can use any IdP that supports the SAML 2.0 protocol.

Before you begin

Your environment must meet the following prerequisites:

- SAML single sign-on is configured for a single ID. For more information, see [“Configuring SAML single sign-on”](#) on page 321.
- The OpenPages servers are running.
- You can log in to the OpenPages application from your browser.

Procedure

1. Configure SAML single sign-on a second time in the `<WLP_USER_DIR>/servers/<server_name>Server</server_name>/configDropins/overrides/OP_SS0_SAML_config.xml` file. Use a different `id` and a different `nameIDFormat`.

For example, suppose that your first SAML single sign-on configuration uses the following values:

```
<samlWebSso20 id="defaultSP"  
...  
nameIDFormat="unspecified">  
...  
</samlWebSso20>
```

Your second configuration might use the following values:

```
<samlWebSso20 id="secondSP"  
...  
nameIDFormat="email">  
...  
</samlWebSso20>
```

2. Use an `authFilter` in each SAML configuration to ensure that the two IDs do not conflict.

You can set up an alias URL and use a `urlPattern` to create the `authFilter`. Or you can use another supported element for `authFilter`. For more information, see the [IBM WebSphere Liberty documentation](#).

The following example uses an alias URL and `urlPattern`.

- Configuration 1

```
<samlWebSso20 id="defaultSP"
...
<authFilter id="samlAuthFilter">
<requestUrl id="openpagesUrl" urlPattern="/grc/api" matchType="notContain"/>
<requestUrl id="adminloginAlias" urlPattern="adminlogin.openpages.com"
matchType="notContain"/>
</authFilter>
</samlWebSso20>
```

- Configuration 2

```
<samlWebSso20 id="secondSP"
...
<authFilter id="samlAuthFilter">
<requestUrl id="openpagesUrl" urlPattern="/grc/api" matchType="notContain"/>
<requestUrl id="adminloginAlias" urlPattern="adminlogin.openpages.com"
matchType="contains"/>
</authFilter>
</samlWebSso20>
```

For this example, the completed file might look like this:

```
<server>
  <featureManager>
    <feature>samlWeb-2.0</feature>
  </featureManager>

  <samlWebSso20 id="defaultSP"
    disableLtpaCookie="false"
    allowCustomCacheKey="false"
    mapToUserRegistry="No"
    idpMetadata="/home/opuser/OP/OpenPages/wlp-usr/servers/opapp-OPNode1Server1/
resources/security/FederationMetadata.xml"
    enabled="true"
    spLogout="false"
    nameIDFormat="unspecified">
    <authFilter id="samlAuthFilter">
      <requestUrl id="openpagesUrl" urlPattern="/grc/api" matchType="notContain"/>
      <requestUrl id="adminloginAlias" urlPattern="adminlogin.openpages.com"
matchType="notContain"/>
    </authFilter>
  </samlWebSso20>

  <samlWebSso20 id="secondSP"
    disableLtpaCookie="false"
    allowCustomCacheKey="false"
    mapToUserRegistry="No"
    idpMetadata="/home/opuser/OP/OpenPages/wlp-usr/servers/opapp-OPNode1Server1/
resources/security/FederationMetadata.xml"
    enabled="true"
    spLogout="false"
    nameIDFormat="email">
    <authFilter id="samlAuthFilter">
      <requestUrl id="openpagesUrl" urlPattern="/grc/api" matchType="notContain"/>
      <requestUrl id="adminloginAlias" urlPattern="adminlogin.openpages.com"
matchType="contains"/>
    </authFilter>
  </samlWebSso20>
</server>
```

In this example, users access the standard URL `https://<op_app_server>:<op_port>` to log in with the `nameIDFormat="unspecified"` format and access the alias URL `https://adminlogin.openpages.com:<op_port>` to log in with the `nameIDFormat="email"` format.

3. Export the SAML Service Provider metadata from WebSphere Liberty by going to the following URL in a browser:

```
https://<op_app_server>:<op_port>/ibm/saml20/<second_saml_id>/samlmetadata
```

- Replace `<op_app_server>` and `<op_port>` with the host and port of the OpenPages application server.
- Replace `<second_saml_id>` with the `id` attribute that you specified for the second SAML configuration.

For example:

```
https://my.app.server:10111/ibm/saml20/secondSP/samlmetadata
```

4. Import the SAML Service Provider metadata to the ADFS server.
 - a) In the ADFS **Server manager**, click **Tools > AD FS Management > Add Relying Party Trust**.
 - b) Set up a second relying party trust for the second SAML id. Use the `nameIdFormat` that you specified in the `OP_SSO_SAML_config.xml` with the appropriate claim rules

5. If you're using an alias URL add the alias URL to the ADFS relying party trusts identifier, SAML Assertion Consumer endpoint, and SAML Logout.

The relying party trust must include matching URLs for where the user is redirected and where the requests originate (meaning the alias URLs).

For example, suppose that the Liberty metadata contains the following for the Assertion Consumer endpoint:

```
https://<op_app_server>:<op_port>/ibm/saml20/secondSP/acs
```

Ensure that the endpoint for the alias URL matches the URL you configured:

```
https://adminlogin.openpages.com:<op_port>/ibm/saml20/secondSP/acs
```

6. Stop and then restart the OpenPages services.

You might see the following error messages:

- CWWKS5077E: The run time cannot select the service provider (SP) from the list of service providers [defaultSP and secondSP] to process the request [https://<OP URL>:<port>/].

This error occurs when there is a conflict with the SAML IDs. Check that the `authFilter` elements are filtering the each SAML ID correctly.

- Error 500: java.lang.RuntimeException: java.lang.ClassCastException: com.ibm.ws.kernel.internal.classloader.JarResourceEntry\$JarEntryURLConnection incompatible with java.net.JarURLConnection

This error is a generic response from Liberty when it encounters a problem with the SAML authentication. Check the `Liberty console.log` or `messages.log` for more information.

Configuring SPNEGO single sign-on

You can use single sign-on with IBM OpenPages with Watson with Simple and Protected GSS-API Negotiation Mechanism (SPNEGO) web authentication. These steps use Microsoft Active Directory Federation Server (ADFS) as the Identity Provider (IdP), but you can use any IdP that supports the SPNEGO protocol.

Before you begin

Your environment must meet the following prerequisites:

- An ADFS server is set up and running.
- User accounts are set up in both ADFS and OpenPages. The usernames must be the same in each system.
- OpenPages 8.2 or later is installed and the OpenPages servers are running.

- You can log in to the OpenPages application from a client computer that is on the same domain as the ADFS server.


About this task

This task describes how to set up SPNEGO single sign-on in a Microsoft Windows environment. The steps use the following conventions:

- ADFS server and domain server: `adfs.test.server.com`
- OpenPages application server (`<op_app_server>`): `op.test.server.com`

For more information, see [Configuring SPNEGO authentication in Liberty](#) in the IBM WebSphere Liberty documentation.

Procedure

1. Enable single sign-on in OpenPages.
 - a) Log on to the OpenPages application as a user with administrative permissions.
 - b) Click  > **System Configuration** > **Settings**.
 - c) Click **Applications** > **Common** > **Configuration**. Change **Show Hidden Settings** to `true`.
 - d) Update the following settings:
 - Change **Platform** > **Security** > **Single Sign On** > **Implementations** > **Current** to HTTP-User-based
 - Change **Platform** > **Security** > **Single Sign On** > **SOX** to `true`
 - Change **Platform** > **Security** > **Single Sign On** > **OP** to `true`
2. Create a dedicated user account in ADFS for IBM WebSphere Liberty.

WebSphere Liberty uses the account to communicate with the ADFS server.

 - a) On the ADFS server, open the **Server Manager**.
 - b) Click **Tools** > **Active Directory Users and Computers**.
 - c) Create a domain user for WebSphere Liberty, for example `wlptest`.
 - d) Enable the **Password never expires** option for the `wlptest` domain user.
 - e) Open the properties of the new user and go to the **Delegation** tab.
 - f) Select the **Trust this user for delegation to any service (Kerberos only)** option and apply the change.
3. In ADFS, assign the Service Principal Name (SPN) and create a key file.
 - a) Assign the SPN.

```
setspn -S HTTP/<op_app_server> <WLP_domain_user>
```

For example:

```
setspn -S HTTP/op.test.server.com wlptest
```

Tip: If your `setspn` command does not support the `-S` option, use the `-A` option instead.

- b) Create the key file.

```
ktpass -out krb5.keytab -princ HTTP/<op_app_server>@<Kerberos_realm> -mapOp set -mapUser <WLP_domain_user>@<Kerberos_realm> -pass <WLP_domain_user_password> -crypto RC4-HMAC-NT -ptype KRB5_NT_PRINCIPAL
```

The `<Kerberos_realm>` is typically the upper case version of the domain that you are using. For example, if the domain is `opnet.com`, then the `<Kerberos_realm>` is typically `OPNET.COM`.

For example:

```
ktpass -out krb5.keytab -princ HTTP/op.test.server.com@OPNET.COM -mapOp set -mapUser
wlptest@OPNET.COM -pass <password> -crypto RC4-HMAC-NT -ptype KRB5_NT_PRINCIPAL
```

The `krb5.keytab` file is created.

- c) Verify that the Microsoft forest contains only one SPN entry.

```
ldifde -f check_SPN.txt -t 3268 -d "" -l servicePrincipalName -r
"(servicePrincipalName=HTTP/<op_app_server>)" -p subtree
```

For example:

```
ldifde -f check_SPN.txt -t 3268 -d "" -l servicePrincipalName -r
"(servicePrincipalName=HTTP/op.test.server.com)" -p subtree
```

Check that the command returns one entry. You can see the results in the `check_SPN.txt` file.

4. Configure Kerberos in WebSphere Liberty.

- Log on to the OpenPages application server.
- Copy the key file to the `/etc` directory on the OpenPages application server: `/etc/krb5.keytab`.
- Go to the `/etc` directory.
- Create a text file (for example `krb5.conf`).

Add the following lines to the file. Update the values as needed for your environment.

```
[libdefaults]
    default_realm = <Kerberos_realm>
    default_keytab_name = FILE:/etc/krb5.keytab
    default_tkt_enctypes = rc4-hmac
    default_tgs_enctypes = rc4-hmac
    forwardable = true
    renewable = true
    noaddresses = true
    clockskew = 300
    udp_preference_limit = 1
[realms]
    <KERBEROS_REALM> = {
        kdc = <domain_controller>:88
        default_domain = <default_domain>
    }
[domain_realm]
    .<DEFAULT_DOMAIN> = <Kerberos_realm>
```

The `[domain_realm]` section maps all hosts that are under the `<default_domain>` (for example `test.server.com`) to our Kerberos realm name (for example `OPNET.COM`).

For example:

```
[libdefaults]
    default_realm = OPNET.COM
    default_keytab_name = FILE:/etc/krb5.keytab
    default_tkt_enctypes = rc4-hmac
    default_tgs_enctypes = rc4-hmac
    forwardable = true
    renewable = true
    noaddresses = true
    clockskew = 300
    udp_preference_limit = 1
[realms]
    OPNET.COM = {
        kdc = adfs.test.server.com:88
        default_domain = test.server.com
    }
[domain_realm]
    .adfs.server.com = OPNET.COM
```

- e) Verify the Kerberos configuration and the keytab.

```
kinit -k -t /etc/krb5.keytab HTTP/<op_app_server>
```

For example:

```
kinit -k -t /etc/krb5.keytab HTTP/op.test.server.com
```

Look for a result that is similar to the following text:

```
Done!  
New ticket is stored in cache file /home/opuser//krb5cc_opuser
```

f) Verify the Kerberos ticket.

```
klist
```

Look for a result that is similar to the following text:

```
Credentials cache: /home/opuser//krb5cc_opuser  
Default principal: HTTP/op.test.server.com@OPNET.COM  
Number of entries: 1  
  
[1] Service principal: krbtgt/OPNET.COM@OPNET.COM  
Valid starting: Thursday, April 27, 2020 at 2:56:22 PM  
Expires: Friday, April 28, 2020 at 12:56:22 AM
```

5. Configure single sign-on in WebSphere Liberty.

a) Install the spnego-1.0 feature by running the following command:

```
<WLP_HOME>/bin/installUtility install spnego-1.0
```

b) Go to the following directory: <WLP_USER_DIR>/servers/<server_name>Server<#>/configDropins/overrides

If the directory does not exist, create it.

c) Create a new .xml file (for example, OP_SS0_SPNEG0_config.xml).

d) Add the following lines to the file.

```
<server>  
  <featureManager>  
    <feature>spnego-1.0</feature>  
    <feature>appSecurity-2.0</feature>  
  </featureManager>  
  <spnego id="op-spnego"  
    canonicalHostName="true"  
    disableFailOverToAppAuthType="true"  
    trimKerberosRealmNameFromPrincipal="true"  
    includeClientGSSCredentialInSubject="true" />  
</server>
```

If the default SPN on the OpenPages application server does not match the entry in the krb5.keytab file, you must specify the SPN in the <spnego> element:

```
<spnego id="mySpnego"  
  servicePrincipalNames="HTTP/<op_app_server>" />
```

For example:

```
<spnego id="op-spnego"  
  servicePrincipalNames="HTTP/op.test.server.com" />
```

The following example shows a complete OP_SS0_SPNEG0_config.xml file:

```
<server>  
  <featureManager>  
    <feature>spnego-1.0</feature>  
    <feature>appSecurity-2.0</feature>  
  </featureManager>  
  
  <spnego id="op-spnego"  
    canonicalHostName="false"  
    disableFailOverToAppAuthType="true"  
    trimKerberosRealmNameFromPrincipal="true"
```



```

includeClientGSSCredentialInSubject="true"
krb5Config="/etc/krb5.conf"
krb5Keytab="/etc/krb5.keytab"
servicePrincipalNames="HTTP/op.test.server.com">
<authFilter id="spnegoAuthFilter">
  <requestUrl id="openpagesUrl" urlPattern="/grc/api" matchType="notContain"/>
</authFilter>
</spnego>
</server>

```

The `<requestUrl>` element in this sample configuration excludes the REST API from SSO. You can change the configuration:

- If you want to use multiple filters, create additional `<requestUrl>` elements. Give each of them a unique id.

Ensure that the `<authFilter>` element does not contain `<requestUrl>` filters that conflict.

For more information, see [Authentication Filters](#) in the WebSphere Liberty documentation.

- If you want to use SSO for all OpenPages URLs, remove the `<authFilter>` element and its child `<requestUrl>` elements.

Save and close the file.

6. Stop all OpenPages services.

For more information, see [“Stopping application servers” on page 311](#).

7. Restart all OpenPages services.

Linux

Go to the `<OP_HOME>/bin` directory and run the following command:

```
./startAllServers.sh --clean
```

Windows

- If you use a script to start and stop application servers, go to the `<OP_HOME>\bin` directory and run the following command:

```
StartAllServers.cmd --clean
```

- If you use Windows services to start and stop application servers, you need to do some cleanup before you start the services. Go to the `<OP_HOME>/wlp-usr/servers/<server_name>Server<#>/workarea` directory. Remove all of the files.

8. Configure users' browsers.

Depending on a user's browser, you might need to do some configuration.

Google Chrome

- a. Open the **Internet Options** panel and go to the **Security** tab.
- b. In the **Local Intranet**, click **Sites > Advanced**.
- c. Add the OpenPages application server to the zone.

Microsoft browsers

See the WebSphere Liberty documentation on "Configure the client application" step in [Configuring SPNEGO authentication in Liberty](#) in the IBM WebSphere Liberty documentation.

When users access the OpenPages application URL, they are logged in automatically with their Active Directory (AD) credentials.

9. After you confirm that single sign-on is working, do the following steps:

- a) Click  > **System Configuration > Settings**.
- b) Change **Platform > Security > Form Based Login > Enabled** to false.

10. Set user passwords to never expire. See [“Setting user passwords to never expire” on page 343](#).

- If a user attempts to log in with an account that does not exist in OpenPages or with an account that is disabled, the user sees the following message:
You are not authorized to access this application.
Please contact your Administrator.
- You can enable trace logging for single sign-on events. For more information, see the *IBM OpenPages with Watson Administrator's Guide*.


Disabling SPNEGO single sign-on

You can disable SPNEGO single sign-on (SSO) for IBM OpenPages with Watson.

Before you begin

The OpenPages with Watson services are running.

Procedure

1. Log on to the IBM OpenPages with Watson admin application server as a user with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
3. Expand **Platform** > **Security** > **Single Sign On**.
4. Update the following settings:
 - Click **SOX** and set its value to false.
 - Click **OP** and set its value to false.
5. Expand **Platform** > **Security** > **Form Based Login** > **Enabled**. Set its value to true.
6. Remove the override XML file that contains the SPNEGO SSO configuration from the overrides directory.
For example, move `<WLP_USER_DIR>/servers/<server_name>Server<#>/configDropins/overrides/OP_SSO_SPNEGO_config.xml` to a backup location.
Or, comment out the contents of the file.
7. Restart the OpenPages with Watson services.

Configuring single sign-on by using OpenID Connect

You can use an OpenID Connect (OIDC) provider as the Identity Provider (IdP) when you configure single sign-on (SSO) for IBM OpenPages with Watson. These steps use IBMId as the IdP, but you can use any IdP that supports OpenID Connect.

Before you begin

Your environment must meet the following prerequisites:


- An OIDC provider is set up and running.
- User accounts are set up in both the OIDC provider and OpenPages. The usernames must be the same in each system.
- OpenPages 8.2 or later is installed and the OpenPages servers are running.
- You can log in to the OpenPages application from your browser.

About this task

This video shows an example of how to configure OIDC SSO: <https://youtu.be/BhN7MQk7100>.

For more information, see [Configuring an OpenID Connect Client in Liberty](#) in the IBM WebSphere Liberty documentation.

Procedure

1. Enable single sign-on in OpenPages.
 - a) Log on to the OpenPages application as a user with administrative permissions.
 - b) Click  > **System Configuration** > **Settings**.
 - c) Click **Applications** > **Common** > **Configuration**. Change **Show Hidden Settings** to true.
 - d) Update the following settings:
 - Change **Platform** > **Security** > **Single Sign On** > **Implementations** > **Current** to HTTP-User-based
 - Change **Platform** > **Security** > **Single Sign On** > **SOX** to true
 - Change **Platform** > **Security** > **Single Sign On** > **OP** to true
2. Install OIDC for WebSphere Liberty.
 - a) Log on to the OpenPages application server.
 - b) Install the openidConnectClient-1.0 feature by running the following command:

```
<WLP_HOME>/bin/installUtility install openidConnectClient-1.0
```

3. Configure single sign-on in WebSphere Liberty.
 - a) Go to the following directory: <WLP_USER_DIR>/servers/<server_name>Server<#>/configDropins/overrides
If the directory does not exist, create it.
 - b) Create a new .xml file (for example, OP_SSO_OIDC_config.xml).
 - c) Add the following lines to the file.

```
<server>
  <featureManager>
    <feature>openidConnectClient-1.0</feature>
  </featureManager>
  <!-- OIDC SSO configuration - Single IdP -->
  <keyStore id="defaultTrustStore" password="<keystore_password>" />
  <sslDefault sslRef="defaultSSLConfig" />
  <ssl id="defaultSSLConfig" keyStoreRef="<keystore>" trustStoreRef="defaultTrustStore" />
  <openidConnectClient id="OIDCconfig"
    clientId="<OIDC_provider_client_ID>"
    clientSecret="<OIDC_provider_client_secret>"
    discoveryEndpointUrl="<OIDC_provider_discovery_URL>"
    scope="openid"
    httpsRequired="true"
    mapIdentityToRegistryUser="false"
    validationMethod="userinfo"
    signatureAlgorithm="RS256"
    userIdentityToCreateSubject="preferred_username">
    <authFilter id="oidcAuthFilter">
      <requestUrl id="openpagesUrl" urlPattern="/grc/api" matchType="notContain"/>
    </authFilter>
  </openidConnectClient>
</server>
```

Replace the following variables with the information for you OIDC provider:

- <keystore_password>
- <keystore>
- <OIDC_provider_client_ID>
- <OIDC_provider_client_secret>
- <OIDC_provider_discovery_URL>

The <requestUrl> element in this sample configuration excludes the REST API from SSO. You can change the configuration:

- If you want to use multiple filters, create additional <requestUrl> elements. Give each of them a unique id.

Ensure that the <authFilter> element does not contain <requestUrl> filters that conflict.

For more information, see [Authentication Filters](#) in the WebSphere Liberty documentation.

- If you want to use SSO for all OpenPages URLs, remove the <authFilter> element and its child <requestUrl> elements.

Save and close the file.

4. Export the root and intermediate certificate authority certificates from your OIDC provider.

For more information, contact your OIDC provider.

5. Import the root and intermediate certificate authority certificates to the OpenPages truststore:

For example:

```
keytool -importcert -v -alias <certificate_alias> -file <path_to_certificate> -keystore
<OP_HOME>/wlp-user/servers/<server_name>Server<#>/resources/security/key.p12 -storetype PKCS12
```

6. Stop all OpenPages services.

For more information, see [“Stopping application servers” on page 311](#).

7. Restart all OpenPages services.

Linux

Go to the <OP_HOME>/bin directory and run the following command:

```
./startAllServers.sh --clean
```

Windows

- If you use a script to start and stop application servers, go to the <OP_HOME>\bin directory and run the following command:

```
StartAllServers.cmd --clean
```

- If you use Windows services to start and stop application servers, you need to do some cleanup before you start the services. Go to the <OP_HOME>/wlp-user/servers/<server_name>Server<#>/workarea directory. Remove all of the files.

8. After you confirm that single sign-on is working, do the following steps:

a) Click  > **System Configuration** > **Settings**.

b) Change **Platform** > **Security** > **Form Based Login** > **Enabled** to false.

9. Set user passwords to never expire. See [“Setting user passwords to never expire” on page 343](#).

- If a user attempts to log in with an account that does not exist in OpenPages or with an account that is disabled, the user sees the following message:

You are not authorized to access this application.
Please contact your Administrator.

- You can enable trace logging for single sign-on events. For more information, see the *IBM OpenPages with Watson Administrator's Guide*.


Disabling OpenID Connect single sign-on

You can disable OpenID Connect (OIDC) single sign-on (SSO) for IBM OpenPages with Watson.

Before you begin

The OpenPages with Watson services are running.

Procedure

1. Log on to the IBM OpenPages with Watson admin application server as a user with administrative privileges.
2. Click  > **System Configuration** > **Settings**.
3. Expand **Platform** > **Security** > **Single Sign On**.
4. Update the following settings:
 - Click **SOX** and set its value to false.
 - Click **OP** and set its value to false.
5. Expand **Platform** > **Security** > **Form Based Login** > **Enabled**. Set its value to true.
6. Remove the override XML file that contains the OIDC SSO configuration from the `overrides` directory. For example, move `<WLP_USER_DIR>/servers/<server_name>Server<#>/configDropins/overrides/OP_SSO_OIDC_config.xml` to a backup location.
Or, comment out the contents of the file.
7. Restart the OpenPages with Watson services.

Configuring header-based single sign-on

You can use header-based single sign-on for IBM OpenPages with Watson.

Before you begin

Your environment must meet the following prerequisites:


- IBM OpenPages with Watson 8.2 or later is installed and the OpenPages servers are running.
- You can log in to the OpenPages application from your browser.
- Optional: Configure a reverse proxy with a third-party authentication provider (for example, LDAP) to provide the necessary headers for OpenPages.

About this task

OpenPages uses a TAI (Trust Association Interceptor) for header-based SSO with IBM WebSphere Liberty. You can use the TAI that is provided with OpenPages or you can create your own custom header-based library (TAI).

If you change any of the OpenPages settings that are used by the header-based TAI, you must restart the OpenPages application servers for the updates to be picked up by the TAI.

Procedure

1. Enable header-based single sign-on in OpenPages.
 - a) Log on to the OpenPages application as a user with administrative permissions.
 - b) Click  > **System Configuration** > **Settings**.
 - c) Click **Applications** > **Common** > **Configuration**. Change **Show Hidden Settings** to true.
 - d) Click **Platform** > **Security** > **Single Sign On** > **Implementations** > **Header-based**.
 - e) Update the following settings:
 - **Class Name:** Type `com.openpages.singlesignon.HTTPHeaderBasedModule`
Use this value whether or not you are using a custom TAI.
 - **Encoded:** If the user name of your single sign-on system is Base64 encoded, set the value to `true`.
 - **Session Attribute:** Type the session attribute for your single sign-on system.

- **Username Attribute:** Type the user name attribute for your single sign-on system.
 - f) Click **Platform > Security > Single Sign On > Implementations**. Change **Current** to Header-based.
 - g) Click **Platform > Security > Single Sign On**. Change **SOX** to true.
2. Install single-sign on for WebSphere Liberty.
 - a) Log on to the OpenPages application server.
 - b) Install the appSecurity-2.0 feature by running the following command:

```
<WLP_HOME>/bin/installUtility install appSecurity-2.0
```

3. Configure single sign-on in WebSphere Liberty.
 - a) Go to the following directory: `<WLP_USER_DIR>/servers/<server_name>Server<#>/configDropins/overrides`
 If the directory does not exist, create it.
 - b) Create a new .xml file (for example, OP_SSO_HEADER_BASED_config.xml).
 - c) Add the following lines to the file.

```
<server>
  <featureManager>
    <feature>appSecurity-2.0</feature>
  </featureManager>
  <trustAssociation id="myTrustAssociation" invokeForUnprotectedURI="false"
failOverToAppAuthType="false">
    <interceptors id="HeaderBasedTAI" enabled="true"
      className="com.ibm.openpages.singlesignon.HTTPHeaderBasedTAI"
      invokeBeforeSSO="true" invokeAfterSSO="false" libraryRef="HeaderBasedTAI">
      <properties EXCLUDE_URI1="/grc/api" />
    </interceptors>
  </trustAssociation>
  <library id="HeaderBasedTAI">
    <fileset dir="{wlp.user.dir}/shared/apps/op-apps.ear"
includes="com.ibm.openpages.singlesignon.jar"/>
  </library>
</server>
```

The EXCLUDE_URI1="/grc/api" attribute excludes any OpenPages URI that starts with /grc/api from requiring header-based (TAI) SSO.

You can exclude other URIs by using either the EXCLUDE_URI<N> or EXCLUDE_CONTAINS<N> formats.

- The EXCLUDE_URI<N> format excludes URIs that start with a value.
- The EXCLUDE_CONTAINS<N> format excludes URIs if the value specified exists anywhere within the URI.

For example:

```
<properties EXCLUDE_URI1="/grc/api" EXCLUDE_URI2="/example"
EXCLUDE_CONTAINS1="/another_example" EXCLUDE_CONTAINS2="last_example"/>
```

This example excludes `https://my-op-server:10111/grc/api` and `https://my-op-server:10111/this/is/another_example` from SSO but not `https://my-op-server:10111/not/this/example`.

4. If you want to use a custom TAI, develop the TAI and then update the override XML file.
 For more information, see [“Custom header-based SSO library” on page 341](#).
5. Stop and then restart the OpenPages with Watson application server.
6. Set user passwords to never expire. See [“Setting user passwords to never expire” on page 343](#).

Custom header-based SSO library

You can develop a custom header-based SSO library (a trust association interceptor (TAI) class) to use with your header-based single sign-on configuration.

Note: Do not specify the custom header-based library in the **Platform > Security > Single Sign On > Implementations > Header-based > Class Name** setting. Instead, specify it in the override XML file: `<WLP_USER_DIR>/servers/<server_name>Server<#>/configDropins/overrides/OP_SSO_HEADER_BASED_config.xml`.

Review the following IBM WebSphere Liberty documentation: [Developing a custom TAI for Liberty](#).

Use the following notes to help to create a custom TAI library to use with OpenPages.

Passing custom properties

If you are passing custom properties to the TAI from the WebSphere Liberty override XML file, save them in `initialize(Properties arg0)`.

Specify when to use the TAI

Use `isTargetInterceptor(HttpServletRequest request)` to determine whether or not to use the TAI. Include something like the following code snippets:

- If you want to exclude certain URIs from using the TAI, do so in this method.
- Set up the OpenPages data source so that you can later connect to the OpenPages database and fetch the registry settings that are used for header-based SSO:

```
Context initCtx = null;
DataSource opDataSource = null;
try {
    initCtx = new InitialContext();
    opDataSource = (DataSource) initCtx.lookup("CWTxDataSource");
}
```

- Load the `aurora.properties` file to get the OpenPages database schema name:

1. Fetch the `OP_HOME` directory:

```
System.getProperty(OPENPAGES_HOME_KEY);
```

2. Build a file path that points to the `<OP_HOME>/aurora/conf/aurora.properties` file.
3. Load the `java.util.Properties` file

```
auroraProperties.load(new FileInputStream(sb.toString()));
```

4. Fetch the OpenPages schema name:

```
auroraProperties.getProperty(DB_OPENPAGES_SCHEMA_NAME_KEY);
```

- Query the OpenPages database by using the **DB_OPENPAGES_SCHEMA_NAME_KEY** and the **REGISTRYENTRIES** table to get the following registry value paths:

```
SESSION_KEY = "/OpenPages/Platform/Security/Single Sign On/Implementations/Header-based/Session Attribute";
USERNAME_KEY = "/OpenPages/Platform/Security/Single Sign On/Implementations/Header-based/Username Attribute";
ENCODED_KEY = "/OpenPages/Platform/Security/Single Sign On/Implementations/Header-based/Encoded";
FAILURE_REDIRECT_URL = "/OpenPages/Platform/Security/Single Sign On/Logon Failure Redirect URL";
```

For example:

```
SELECT value FROM openpage.REGISTRYENTRIES WHERE path = '/OpenPages/Platform/Security/
```

The `FAILURE_REDIRECT_URL` is required only if your OpenPages deployment uses the **Logon Failure Redirect URL** setting. If you did not configure that setting, you do not need to fetch this value.

Verify that the values of the registry settings that you fetched. Confirm that they contain the values that you want the TAI to use.

Authenticate incoming requests

Use `negotiateValidateandEstablishTrust(HttpServletRequest request arg0, HttpServletResponse response arg1)` to authenticate incoming requests based on the headers that are provided and any other information that is necessary for authentication.

1. Fetch the headers from the incoming request (the `arg0` that you specified in the `initialize(Properties arg0)` method) with the `SESSION_KEY` and `USERNAME_KEY`. method

For example:

```
sessionAttribute = arg0.getHeader(sessionKey);
userAttribute = arg0.getHeader(userKey);
```

2. If the keys need to be decoded from Base64, use a library such as `org.apache.commons.codec.binary.Base64` to decode them.
3. Do any other logic that is required in order to authenticate the user.
4. If you want to redirect to a page other than an HTTP 401 error, do so before you return a failing result.

Example: Returning a failing result

```
return TAIResult.create(HttpServletResponse.SC_UNAUTHORIZED);
```

Example: Redirecting to a URL

```
response.sendRedirect(failureRedirectUrl);
```

You can do a redirect to any URL or to the `FAILURE_REDIRECT_URL` that you fetched from the OpenPages settings.

If you use the URL in `FAILURE_REDIRECT_URL`, ensure that the URL is valid.

5. Before you return a successful result, you must set a custom attribute on the incoming request for OpenPages to use later.

Example: Returning a success result

```
return TAIResult.create(HttpServletResponse.SC_OK, userAttribute);
```

Example: Setting the custom attribute

```
arg0.setAttribute("OPCustomTAIHeaderBasedSSO", "true");
```

Set up the TAI in WebSphere Liberty

1. Build the TAI into a WebSphere Liberty shared library (JAR file).
2. Update the `<wlp_user_dir>/servers/<server_name>Server</server_name>/configDropins/overrides/OP_SSO_HEADER_BASED_config.xml` to use the TAI.

```
<trustAssociation id="myTrustAssociation" invokeForUnprotectedURI="false"
failOverToAppAuthType="false">
  <interceptors id="HeaderBasedTAI" enabled="true"
    className="com.ibm.openpages.singlesignon.HTTPHeaderBasedTAI"
    invokeBeforeSSO="true" invokeAfterSSO="false" libraryRef="HeaderBasedTAI">
  </interceptors>
</trustAssociation>
<library id="HeaderBasedTAI">
```



```
<fileset dir="${wlp.user.dir}/shared/apps/op-apps.ear"
includes="com.ibm.openpages.singlesignon.jar"/>
</library>
```


- In the **className** parameter, specify the new class that you created for the TAI library.
- In the **libraryRef** parameter, use the same value as the **library id** parameter. In this example, the id is `HeaderBasedTAI`, but you can use any value.
- In the **fileset dir** parameter, specify the directory where the shared library (JAR) file is stored.
- In the **includes** parameter, specify the name of the shared library (JAR) file.

Disabling header-based single sign-on

You can disable header-based single sign-on (SSO) for IBM OpenPages with Watson.

Note: If you are using SAML SSO, additional steps are required to disable SSO. See [“Disabling SAML single sign-on”](#) on page 324.


Procedure

1. Start the OpenPages with Watson services.
2. Log on to the OpenPages application as a user with administrative permissions.
3. Click  > **System Configuration** > **Settings**.
4. Expand **Platform** > **Security** > **Single Sign On**.
5. Click **SOX** and set its value to `false`.
6. Remove the override XML file that contains the header-based SSO configuration from the overrides directory.
For example, move `<WLP_USER_DIR>/servers/<server_name>Server<#>/configDropins/overrides/OP_SSO_HEADER_BASED_config.xml` to a backup location.
Or, comment out the contents of the file.
7. Restart the OpenPages with Watson services.

Setting user passwords to never expire

After you configure single sign-on, set user passwords to never expire.

Procedure

1. Click  > **Users and Security** > **Users**.
2. Type a username in the **Search** box, and then select the user that you want to edit.
3. Under **Password and Security**, click **Password never expires**. Set its value to **True**.
4. Ensure the **User must change password at next logon** option is set to **False**.


Configuring the single sign-on logout destination

To securely log out of an IBM OpenPages with Watson application session where single sign-on is enabled, configure the system to redirect the user.

Logging out of the OpenPages with Watson application does not automatically log the user out of a single sign-on system. If you use **Back** in the web browser to reenter the OpenPages application, your session is re-created. The session uses the existing, valid third-party credentials.

Procedure

1. Log on to the OpenPages application interface as a user with administrative privileges.

2. Click  > **System Configuration** > **Settings**.
3. Expand **Platform** > **Security**.
4. Click **Logout URL**.
5. In the **Value** box, type a fully qualified URL.
6. Click **Done**.

Avoiding server timeouts in single sign-on environments

If the server times out when you use single sign-on (SSO), you can increase the timeout value for WebSphere Liberty in your SSO configuration.

About this task

This topic applies to the following SSO configurations:

- SAML SSO and mixed-mode SAML SSO
- OpenID Connect (OIDC) SSO
- SPNEGO SSO

Procedure

1. Go to the following directory: `<WLP_USER_DIR>/servers/<server_name>Server<#>/configDropins/overrides`
2. Open the file that contains the SSO configuration.
For example `OP_SSO_SAML_config.xml`, `OP_SSO_OIDC_config.xml`, or `OP_SSO_SPNEGO_config.xml`.
3. Create a new line above the `</server>` tag.
4. On the new line you created, add the following element:

```
<authCache timeout="120m"/>
```

Where 120m is the timeout value. You can use a different value, if needed. For more information, see [Authentication cache \(authCache\)](#) in the Liberty documentation.

For example:

```
<server>
  <featureManager>
    <feature>samlWeb-2.0</feature>
  </featureManager>
  <!-- SAML SSO configuration - Single IdP -->
  <samlWebSso20 id="<saml_id>"
    disableLtpaCookie="false"
    allowCustomCacheKey="false"
    mapToUserRegistry="No"
    idpMetadata="<OP_HOME>/wlp-usr/servers/<server_name>Server<#>/resources/security/
    FederationMetadata.xml"
    enabled="true"
    spLogout="false"
    nameIDFormat="unspecified">
    <authFilter id="samlAuthFilter">
      <requestUrl id="openpagesUrl" urlPattern="/grc/api" matchType="notContain"/>
    </authFilter>
  </samlWebSso20>
  <authCache timeout="120m"/>
</server>
```

5. Stop and then restart the OpenPages services.

Chapter 14. QRadar integration

The IBM QRadar integration project is an optional project that you can install to import offenses from QRadar to IBM OpenPages with Watson as incidents.

You must complete the following steps to install and configure the QRadar integration project.

- Ensure IBM QRadar is installed.
- Install IBM Security Directory Integrator (SDI) 7.2 and then install Fix Pack 6. For more information, see [“Installing IBM Security Directory Integrator for QRadar integration”](#) on page 345.
- Configure Security Directory Integrator to connect to QRadar. For more information, see [“Setting up the QRadar SSL certificate”](#) on page 346.
- Import the assembly line. For more information, see [“Importing the assembly line for QRadar”](#) on page 347.
- Configure the property files. For more information, see [“Configuring the QRadar connector properties file”](#) on page 347 and [“Configuring the QRadar connector passwords properties file”](#) on page 348.

Installing IBM Security Directory Integrator for QRadar integration

If you want to use IBM QRadar with OpenPages, you need to install IBM Security Directory Integrator.

Before you begin

If you are using IBM OpenPages with Watson, install Fix Pack 8.2.0.1.

About this task

The computer where you install IBM Security Directory Integrator must meet the following requirements:

- The computer can access the IBM OpenPages REST API URL.
In IBM OpenPages for IBM Cloud Pak for Data, the computer where you install QRadar must have access to the public route URL for OpenPages.
- The computer can access QRadar.

Procedure

1. Install IBM Security Directory Integrator 7.2, and then install Fix Pack 6.
To get the installation package, see one of the following download documents:
 - For IBM OpenPages with Watson, see [Downloading IBM OpenPages with Watson Version 8.2 from Passport Advantage](#).
 - See the IBM OpenPages for IBM Cloud Pak for Data 8.2.0 download document.
2. Patch the version of Java to update it to Java 8.
For more information, see technote 720-iss-sdi-la0019.
3. Optional: Disable the TLS 1.0 protocol in IBM Security Directory Integrator.
IBM Security Directory Integrator 7.2.0.6 supports later versions of the TLS protocol. Depending on your security requirements, you might need to disable TLS 1.0. For more information, see [Disabling TLS 1.0 for TDI/SDI](#).
4. If you installed IBM Security Directory Integrator on a Microsoft Windows computer and you are using a self-signed certificate, import the OpenPages certificate into the Microsoft Windows trust store.

What to do next

[“Setting up the QRadar SSL certificate”](#) on page 346

Setting up the QRadar SSL certificate

You must specify the SSL certificate that allows IBM Security Directory Integrator (SDI) to connect to the QRadar server.

Procedure

1. Obtain the QRadar SSL certificate:

- a) Log in to the QRadar console.
- b) Use the certificate management tool in your browser to export the QRadar certificate to a file on the system where SDI is installed. For example, for Microsoft browsers, click **Control Panel > Internet Options**. Click the **Content** tab, and then click **Certificates**.

Alternatively, enter the following command to retrieve the certificate in Base-64 encoded X509 format from the QRadar server.



Attention: The command assumes that the **openssl** command is in the path. Replace **<host>** with the fully qualified host name of your QRadar server, and replace **<port>** with the port number being used. If no port number is specified in the URL when logging in to the QRadar console, specify port 80 for HTTP, or port 443 for HTTPS.

- **Windows** (You might need to press Ctrl-C to end the command):

```
openssl s_client -showcerts -connect <host>:<port> | openssl  
x509 -outform PEM > mycertfile.pem
```

- **Linux:**

```
openssl s_client -showcerts -connect <host>:<port>  
</dev/null 2>/dev/null | openssl x509 -outform PEM > mycertfile.pem
```

The Base-64 X509 encoded certificate is exported to the mycertfile.pem file.

2. From the SDI Configuration Editor, add the certificate to Security Directory Integrator.
 - a) Click **Key Manager**, then click the **Open** icon.
 - b) Select **JKS** from the **Key database type** list.
 - c) Click **Browse**, and locate the **<SDI_solutions_user_home>/Solutions/serverapi/testadmin.jks** file, then click **OK**.
 - d) At the password prompt, type **administrator**.
 - e) Select **Signer Certificates** from the **Key database content**.
 - f) Click **Add** and browse to the location of the certificate that you obtained in step 1.
 - g) Specify the label for the certificate as **administrator**, then click **Save**.
 - h) When you are prompted for the password, type **administrator**.
 - i) Close the dialog box.
3. Copy **testadmin.jks** into the following directories. Some of these directories might not exist, depending on the options that you chose when you installed Security Directory Integrator.

If required, back up the existing file in each directory before you copy the updated version.

<SDI_home>/win32_services/serverapi (Windows platforms only)

<SDI_home>/serverapi

<SDI_solutions_user_home>/serverapi

Importing the assembly line for QRadar

To run the QRadar assembly line, you import the `qradar_integration.xml` file as a new IBM Security Directory Integrator (SDI) project.

About this task

An assembly line is commonly referred to as an AL in the Security Directory Integrator documentation.

Procedure

1. Do one of the following tasks:

IBM OpenPages with Watson

Go to the `<OP_HOME>/OpenPages/integrations/ITG` directory and locate the `qradar-integration.zip` file.

IBM OpenPages for IBM Cloud Pak for Data

- a. Download the **IBM OpenPages for Cloud Pak for Data General** package from Passport Advantage.
 - b. Extract the package to a new directory, for example `/qradar_integration`.
 - c. Locate the `qradar-integration.zip` file.
2. Extract the `qradar-integration.zip` file to a new temporary directory.
 3. Import `qradar_integration.xml` from the extracted files as a new project in SDI.
 - a) Click **File > Import > IBM Security Directory Integrator > Configuration**.
 - b) Click **Next**.
 - c) Select **New Project** in the **Project** list.
 - d) In the **Configuration File** field, browse to `qradar_integration.xml` that you extracted and select it.
 - e) Click **Finish**.
 - f) In the **New Project** field, type `qradar_integration`.
The project is created in your workspace location.
 - g) Click **Finish**.
 4. Copy the `connector.properties` and `Connector-Passwords.properties` files from the files you extracted in step 2 to the `Runtime-qradar_integration` folder in your SDI workspace location.

Note: If the `Runtime-qradar_integration` folder is not visible in the SDI Configuration Editor, right-click the `qradar_integration.xml` project in the SDI Configuration Editor and click **Refresh**.

Configuring the QRadar connector properties file

You must update the `connector.properties` file with the correct configuration for the connector components.

About this task

The `qradar_integration.zip` file contains the `qradar_integration.xml` file. This is the project file that is used to import the `qradar_integration` project into IBM Security Directory Integrator (SDI).

There are also two text properties files that you can use to configure the connector-related properties in the respective **Resources > Properties** components of the `qradar_integration` project. Use the `connector.properties` text properties file to set or update the property values in the connector property store. Use the `Connector-Passwords.properties` text properties file to set or update the property values in the Connector-Passwords property store.

The non-encrypted connector properties are maintained in the `connector.properties` file. This file is one of the two property files that you manually copy into the `Runtime-qradar_integration` folder after you import the `qradar_integration` project into your SDI deployment. The properties in this file can be used to set or update the values that are stored in the connector property store located under the **Resources > Properties** project folder.

The `connector.properties` file has three sections: one shared area for email settings; one section specifically for the QRadar API Connector properties; and one section for the OpenPages Connector properties. Mandatory fields are marked as **REQUIRED** in the text properties files, and are marked with an asterisk (*) when viewed from the SDI Configuration Editor's Connection Editor in the **Connection** tab for the connector component. You can use the example values shown for each property for hints on what to specify for that property.

Procedure

1. From the SDI Configuration Editor, open the `qradar_integration` project.
2. In the Navigator pane, expand **Runtime-qradar_integration**.
3. Right-click the `connector.properties` file and open it using the **Text Editor** option.
4. Set or change the property values.
5. Save the changes and exit the text editor.
6. In the Navigator pane, expand **Resources > properties**.
7. Right-click the connector object and click **Properties Editor**.
8. Click **Read properties from Server**.
9. Click **Send properties to Server**.
10. Click the **Save** icon to save the changes in the SDI connector property store. Close the connector editor. If you are prompted to save the properties again, click **Yes**.

Configuring the QRadar connector passwords properties file

You must update the `Connector-Passwords.properties` file with the correct OpenPages password and QRadar API token values for the connector components.

About this task

The connector components use two encrypted properties: the **op_conn_password** property and the **qradarToken** property. Both properties are maintained in the `Connector-Passwords.properties` file. This file is one of the two properties files that you manually copy into the `Runtime-qradar_integration` folder after you import the `qradar_integration` project into your IBM Security Directory Integrator (SDI) deployment. You can use the properties in this file to set or update the values that are maintained in the Connector-Passwords password property store located under the **Resources > Properties** project folder.

Procedure

1. Obtain the QRadar API token value:
 - a) Log in to the QRadar console.
 - b) Click **Admin > Authorized Services**.
 - c) Copy the **Authentication Token** value from the **REST Service** service name line item for use in step 5.
2. From the SDI Configuration Editor, open the `qradar_integration` project.
3. In the Navigator pane, expand **Runtime-qradar_integration**.
4. Right-click the `Connector-Passwords.properties` file and open it using the **Text Editor** option.
5. Set or change the password-related property values.

- a) Enter a clear-text value for the **op_conn_password** property after the = character.
- b) Enter the value that you obtained from the QRadar server in step 1 after the = character for the **qradarToken** property.

Note: Do not remove the {protect}- prefix from any property entry in the file. If you are updating an already-encrypted value, you can either leave the {encr} prefix after the equal sign (=) character, or you can remove it. If the {encr} prefix is removed, it is automatically reinserted after the equal sign (=) character as part of the encryption processing that occurs during step 11.

6. Save the changes and exit the text editor.
7. In the Navigator pane, expand **Resources > Properties**.
8. Right-click the Connector-Passwords object and click **Properties Editor**.
9. Click **Read properties from Server**.
10. Click **Send properties to Server**.
11. Click **Save** to save the changes in the SDI Connector-Passwords password property store. Close the Connector-Passwords editor. If you are prompted to save the properties again, click **Yes**.

Note: After this step is complete, the values in the Connector-Passwords property store and the values in the Connector-Passwords.properties text file are automatically encrypted. If needed, the {encr} tag is automatically inserted before the property value of each property in the Connector-Properties.properties text file.

Chapter 15. IBM OpenPages SDI Connector for UCF Common Controls Hub

IBM OpenPages SDI Connector for UCF Common Controls Hub is an optional connector that you can install. Use the connector to import data from the Unified Compliance Framework (UCF) Common Controls Hub into OpenPages.

You must have a UCF Common Controls Hub Basic Subscription with the API Access add-on to use the connector.

Complete the following steps to install and configure the UCF connector.

- Obtain an API token from UCF. To get your token, log in to UCF Common Controls Hub. Click **Settings > API Manager > API Keys**. Click **Create Credentials**.
- Install IBM Security Directory Integrator 7.2 and then install Security Directory Integrator Fix Pack 6.

For more information, see [“Installing IBM Security Directory Integrator for IBM OpenPages SDI Connector for UCF Common Controls Hub” on page 351](#).

Note: IBM Security Directory Integrator is the latest name for IBM Tivoli Directory Integrator.

- If you are using IBM OpenPages with Watson, install the UCF connector. For more information, see [“Installing IBM OpenPages SDI Connector for UCF Common Controls Hub” on page 352](#).

If you are using IBM OpenPages for IBM Cloud Pak for Data, skip this step.

- Import the assembly lines. For more information, see [“Importing the assembly lines for UCF” on page 353](#).
- Configure the property files. For more information, see [“Configuring the connection information” on page 354](#).
- Configure OpenPages. For more information, see [“Configuring OpenPages for UCF integration” on page 355](#).

For information about how to use the UCF connector, see the *IBM OpenPages with Watson Administrator's Guide*.

Installing IBM Security Directory Integrator for IBM OpenPages SDI Connector for UCF Common Controls Hub

If you want to use IBM OpenPages SDI Connector for UCF Common Controls Hub, you need to install IBM Security Directory Integrator.

Before you begin

If you are using IBM OpenPages with Watson, install Fix Pack 8.2.0.1.

About this task

The computer where you install IBM Security Directory Integrator must meet the following requirements:

- The computer can access the IBM OpenPages REST API URL.

In IBM OpenPages for IBM Cloud Pak for Data, the computer where you install IBM Security Directory Integrator must have access to the public route URL for OpenPages.

- The computer can access UCF Common Controls Hub.

Procedure

1. Install IBM Security Directory Integrator 7.2, and then install Fix Pack 6.
To get the installation package, see one of the following download documents:
 - For IBM OpenPages with Watson, see [Downloading IBM OpenPages with Watson Version 8.2 from Passport Advantage](#).
 - See the IBM OpenPages for IBM Cloud Pak for Data 8.2.0 download document.
2. Patch the version of Java to update it to Java 8.
For more information, see [technote 720-iss-sdi-la0019](#).
3. Optional: Disable the TLS 1.0 protocol in IBM Security Directory Integrator.
IBM Security Directory Integrator 7.2.0.6 supports later versions of the TLS protocol. Depending on your security requirements, you might need to disable TLS 1.0. For more information, see [Disabling TLS 1.0 for TDI/SDI](#).
4. If you installed IBM Security Directory Integrator on a Microsoft Windows computer and you are using a self-signed certificate, import the OpenPages certificate into the Microsoft Windows trust store.

What to do next

IBM OpenPages with Watson

[“Installing IBM OpenPages SDI Connector for UCF Common Controls Hub” on page 352](#)

IBM OpenPages for IBM Cloud Pak for Data

[“Importing the assembly lines for UCF” on page 353](#)

Installing IBM OpenPages SDI Connector for UCF Common Controls Hub

You must run the IBM OpenPages SDI Connector for UCF Common Controls Hub installation program on the OpenPages admin application server.

About this task

Do this task if you are using IBM OpenPages with Watson.

If you are using IBM OpenPages for IBM Cloud Pak for Data, skip this task. Go to [“Importing the assembly lines for UCF” on page 353](#).

Procedure

1. Download the IBM OpenPages SDI Connector for UCF Common Controls Hub installer package from [IBM Passport Advantage](#).
2. Extract the package files.
3. On the admin application server, run IBM Installation Manager.
4. Add the UCF connector repository to IBM Installation Manager.
 - a) Click **File > Preferences**.
 - b) Click **Repositories** and then click **Add Repository**.
 - c) Select the UCF connector installer package.
 - d) Click the `repository.config` file.
 - e) Click **OK**.
 - f) Click **OK** to return to the main IBM Installation Manager page.
5. Click **Install**.
6. Select **IBM OpenPages SDI Connector for UCF Common Controls Hub** and **Version 8.2**, and click **Next**.

7. Accept the license agreement and click **Next**.
8. Type the location of your IBM OpenPages with Watson installation directory (*OP_HOME*).
9. Click **Next**.
10. Click **Next**. If any errors appear on the page, follow the instructions to fix them before you continue.
If you see warning messages about the 64-bit version of IIM, you can ignore them.
11. Click **Install**.

What to do next

[“Importing the assembly lines for UCF” on page 353](#)

Importing the assembly lines for UCF

To import the UCF assembly lines, you import the `ucf_integration.xml` file as a new IBM Security Directory Integrator (SDI) project.

About this task

The UCF connector uses three assembly lines to import objects.

- UCF Authority Documents to OP Mandates
- UCF Citations to OP Submandates
- UCF Controls to OP Requirements

You use a project file, `ucf_integration.xml`, to import the assembly lines and other project files into Security Directory Integrator.

An assembly line is commonly referred to as an AL in the Security Directory Integrator documentation.

Procedure

1. Do one of the following tasks:

IBM OpenPages with Watson

Go to the `<OP_HOME>/integrations/UCF` directory and locate the `ucf_integration.xml` file.

IBM OpenPages for IBM Cloud Pak for Data

- a. Download the **IBM OpenPages for Cloud Pak for Data SDI Connector for UCF Common Controls Hub** package from Passport Advantage.
 - b. Extract the package to a new directory, for example `/ucf_integration`.
 - c. Locate the `ucf_integration.xml` file.
2. Copy the file to the server where Security Directory Integrator is installed.
 3. Import the `ucf_integration.xml` file as a new project in Security Directory Integrator.
 - a) Click **File > Import > IBM Security Directory Integrator > Configuration**.
 - b) Click **Next**.
 - c) Select **New Project** in the **Project** list.
 - d) Click **File**.
 - e) Click the browse button next to the **Configuration File** field. Select the `ucf_integration.xml` file.
 - f) Click **Finish**.
 - g) Name the project `ucf_integration`.
 - h) Click **Finish**.

The project is displayed in the **SDI Configuration Editor** and the project files are created in your SDI workspace directory.

4. Copy the UCF connector property files into your project runtime SDI workspace directory.

The workspace directory is where the projects, files, and folders that you create in Security Directory Integrator are stored, for example C:\Users\<user>\Documents\SDI\workspace\ucf_integration\Runtime-ucf_integration.

- a) Go to the directory that contains the UCF integration files:

IBM OpenPages with Watson

Go to the <OP_HOME>/integrations/UCF directory.

IBM OpenPages for IBM Cloud Pak for Data

Go to the /ucf_integration directory. This is the directory where you extracted the files in step “1.b” on page 353.

- b) Copy the following files to the Runtime-ucf_integration directory.

- passwords.properties
- op_client.properties

5. Right-click the **ucf_integration** project in the **SDI Configuration Editor** and click **Refresh**.

Results

In Security Directory Integrator, the **AssemblyLines** folder contains the UCF assembly lines. In addition, the **Resources > Properties** folder contains the UCF property files.

What to do next

[“Configuring the connection information” on page 354](#)

Configuring the connection information

You must configure the connection information that the UCF connector uses to connect to OpenPages and to UCF Common Controls Hub. You configure the connection information by updating property files and by entering passwords in the IBM Security Directory Integrator Configuration Editor. Do this procedure after you import the assembly lines.

About this task

The UCF connector includes two text files that contain the assembly line properties.

The property files are in the **Runtime-ucf_integration** folder of the **ucf_integration** project.

op_client.properties

The op_client.properties file stores the connection information for OpenPages.

passwords.properties

The passwords.properties file contains the OpenPages password and your UCF token. The values are encrypted.

Note: Do not edit this file. Set the values by using the Security Directory Integrator Configuration Editor.

Procedure

1. From the Security Directory Integrator Configuration Editor, open the **ucf_integration** project.
2. In the Navigator pane, expand **Runtime-ucf_integration**.
3. Right-click the op_client.properties file and click **Text Editor**.
4. Set or change the property values.

Table 73. Properties in the <i>op_client.properties</i> file	
Property	Description
op_api_root	The OpenPages REST API root The default (typical) value is <code>/grc/api</code> . The <code>op_api_root</code> is appended to the <code>op_url</code> to form the full URL to access the OpenPages REST API.
op_url	The OpenPages URL For IBM OpenPages with Watson, use the format <code>https://<host>:<port></code>
op_user	The OpenPages user name that the UCF connector uses to log in to OpenPages Use an account with administrative privileges. The user account must have security permissions to create and update the mandate, submandate, and requirements object types.

For example:

```
op_api_root=/grc/api
op_url=https://op_server:10111
op_user=ucf
```

5. Save the changes and exit the text editor.
6. Right-click the `passwords.properties` file and click **Text Editor**.
7. Type the password of the OpenPages user that you used in the `op_client.properties` file.
8. Enter your UCF Common Controls Hub token in the `ucf_api_token` parameter.

To get your token, log in to UCF Common Controls Hub. Click **Settings** > **API Manager** > **API Keys**. Click **Create Credentials**.

If you are unable to create a token, contact UCF Common Controls Hub.

9. Save the changes and exit the text editor.

The values in the `passwords.properties` file are automatically encrypted.
10. Refresh the property files and the connectors with the updated connection information.
 - a) In the Navigator pane, expand **Resources** > **Properties**.
 - b) Right-click **op_client**, and then click **Open**.
 - c) Click **Read properties from Server**, and then click **Send properties to Server**.
 - d) Click **Save**, and then close the window.
 - e) Right-click **passwords**, and then click **Open**.
 - f) Click **Read properties from Server**, and then click **Send properties to Server**.
 - g) Click **Save**, and then close the window.

What to do next

[“Importing business entities” on page 356](#)

Configuring OpenPages for UCF integration


Importing business entities

Import the business entities that are used by UCF into OpenPages. When the UCF connector imports data into OpenPages, the business entities are used for the imported objects.

About this task

The UCF Entities.xlsx file contains the business entity structure for UCF. Import this file by using FastMap.

Procedure

1. Log in to OpenPages as a user with administrative privileges.
2. Click  > **FastMap Import**.

The **FastMap Import** tab displays a list of your imports. If you have the application permission to see imports performed by other users, you can click the **View** dropdown and select **All imports**. The **Created By** column is added to the grid if you select this view.

3. Click **Choose File** and select the UCF Entities.xlsx file.

IBM OpenPages with Watson


The file is located in the <OP_HOME>/integrations/UCF directory.

IBM OpenPages for IBM Cloud Pak for Data

Go to the /ucf_integration directory. This is the directory where you extracted the UCF package files.

4. Click **Import data**.
5. Review the verification report, and then click **Import data**.

The import process begins. The progress of the import is displayed in the **FastMap Import Status** window. Click **Refresh** to update the window.

6. Verify the import.
 - a) Log in to OpenPages as a user with administrative privileges.
 - b) Click  > **Organization** > **Business Entities**.
 - c) Search for the **UCF** business entity. Click its name.

The updates are complete if the UCF business entity has two child entities, Authority Documents and Harmonized Controls.

Note: If UCF Common Controls Hub adds new control impact zones or adds new authority document guidance areas in future, you need to update OpenPages. For more information, see [“Update business entities, fields, and field groups” on page 358](#).


What to do next

[“Updating object type relationships for UCF” on page 356](#)

Updating object type relationships for UCF

The IBM OpenPages SDI Connector for UCF Common Controls Hub requires an additional object type relationship. Business Entity must be a parent of Requirement. Your environment might already have this object type relationship configured.

Procedure

1. Determine whether you need to update object type relationships:
 - a) Log in to OpenPages.
 - b) Click  > **Solution Configuration** > **Objects**.

c) Click **Requirement**.

d) Click **Relationships**.

If **Business Entity** is listed, your environment has the required object relationships for UCF. You do not need to do the remaining steps in this task. Go to [“Updating UCF fields” on page 357](#).

Otherwise, continue to step 2.

2. If you are using IBM OpenPages for IBM Cloud Pak for Data, verify that ObjectManager is installed on a remote computer that has access to the cluster.

For more information, see "Installing tools and utilities" in the *IBM OpenPages with Watson Administrator's Guide*.

3. Locate the req-op-config.xml file.

IBM OpenPages with Watson

Go to the <OP_HOME>/integrations/UCF directory. Copy the req-op-config.xml file to the administrative application server.

IBM OpenPages for IBM Cloud Pak for Data

Go to the /ucf_integration directory. This is the directory where you extracted the UCF package files. Copy the req-op-config.xml file to the computer where you installed ObjectManager.

4. Go to the ObjectManager /bin directory:

IBM OpenPages with Watson

- a. Log in to the admin application server.
- b. Open a command line. If you are using Microsoft Windows, open a command prompt with the **Run as administrator** option.
- c. Go to the <OP-HOME>/bin directory.

IBM OpenPages for IBM Cloud Pak for Data

- a. On the computer where you installed ObjectManager, open a command line. If you are using Microsoft Windows, open a command prompt with the **Run as administrator** option.
- b. Go to the openpages-tools-client/bin directory.

5. Run the following command.

Replace <loader-file-path> with the location of the req-op-config.xml file.

```
ObjectManager.cmd|sh 1 c <OpenPages Administrator user> <OpenPages Administrator password>  
<loader-file-path> req
```

6. If you encounter any errors, review the log file, <loader-file-path>/ObjectManager.log.

What to do next

[“Updating UCF fields” on page 357](#)

Updating UCF fields

The IBM OpenPages SDI Connector for UCF Common Controls Hub requires certain enumerated string values for the UCF fields in OpenPages.

About this task

If you are installing the UCF connector, you might need to add the enumerated values to the UCF fields.


You can also use this task if UCF Common Controls Hub adds new authority document categories. In step [“5” on page 358](#), update the fields with the new values. For more information, see [“Update business entities, fields, and field groups” on page 358](#).

IBM OpenPages SDI Connector for UCF Common Controls Hub uses the following fields:

- **UCF-Mand** field group, **UCF Category** field
- **UCF-SubMand** field group, **UCF Guidance Area** field
- **UCF-Req** field group, **UCF Guidance Areas** field

The changes that you need to make are the same for each field.

Procedure

1. Log in to OpenPages as a user with administrative privileges.
2. Click  > **Solution Configuration > Objects**.
3. Click **Mandate**, and then click **Fields**.
4. Under **UCF-Mand**, click **UCF Category**.
5. Verify that the following values are displayed in the **Enumerated String Values** list. If any values are missing, add them.
 - Risk Management Organizations
 - Banking and Finance Organizations
 - Energy Organizations
 - Healthcare and Life Science Organizations
 - Payment Card Organizations
 - Records Management Organizations
 - Security and Privacy Organizations
 - International
 - North America
 - Australia-Oceania
 - Asia
 - Configuration
 - South America
 - Africa
 - Europe
6. Click **Done**.
7. Go back to the **Objects** list, click **Sub-Mandate**, and then click **Fields**.
8. Under **UCF-SubMand**, click **UCF Guidance Area**.
9. Repeat step “5” on page 358 to update the values, and then click **Done**.
10. Go back to the **Objects** list, click **Requirement**, and then click **Fields**.
11. Under **UCF-Req**, click **UCF Guidance Areas**.
12. Repeat step “5” on page 358 to update the values, and then click **Done**.

Results

The field definitions for UCF are updated.

Update business entities, fields, and field groups

If UCF Common Controls Hub adds new control impact zones or adds new authority document guidance areas, you need to update IBM OpenPages with Watson.

You need to update OpenPages in the following cases:

- The assembly line reports that an impact zone is missing.

In this case, you need to add a business entity with the same name as the missing control impact zone. The parent of the new business entity must be /Library/UCF/Harmonized Controls.

For example: /Library/UCF/Harmonized Controls/<Impact Zone Name>

- The assembly line reports that a mandate cannot be created because an authority document's guidance area could not be found.

In this case, you need to add a business entity with the same name as the authority document's guidance area. The parent of the new business entity must be /Library/UCF/Authority Documents.

For example: /Library/UCF/Authority Documents/<Guidance Area Name>

Next, add the new business entity name as an enumerated string value to the fields UCF-Mand:UCF Category, UCF-SubMand:UCF Guidance Area, and UCF-Req:UCF Guidance Areas.

For information about updating fields, see [“Updating UCF fields” on page 357](#).

For business entities, you can add them in OpenPages. Alternatively, you can use FastMap to import them.

Chapter 16. Approval app

The approval app is an optional feature that leverages the power of IBM OpenPages with Watson and provides an easy-to-use interface for quickly taking action on a review, approval, or attestation request with confidence and full knowledge of the context surrounding the request. The approval app works with objects that are set up for the configurable lifecycle.

By using the approval app, a casual or infrequent user of IBM OpenPages with Watson is able to make well-informed decisions for GRC tasks guided by information from the system quickly and easily, without the need for extensive training in OpenPages. If you want to see all of the items sent to you in the approval app, you can go to your To Do list by clicking the IBM OpenPages with Watson logo. You simply make the decision (or respond to certification language or questions), with your comments if necessary, and click the relevant button to submit. You can use this feature on tablets and mobile devices as well, for increased flexibility.

Deployment process overview for the approval app

If you upgraded or migrated IBM OpenPages with Watson and you previously did not use the approval app, you need to deploy and configure it.

If you deployed the approval app in version 7.2.0.1 or later, you need to upgrade the approval app. You do not need to deploy it. For more information, see [“Upgrade the approval app” on page 371](#).

If you did a fresh installation of OpenPages, not an upgrade or migration, you do not need to deploy the approval app. The app is installed when you install OpenPages. You can configure the approval app. For more information, see the *IBM OpenPages with Watson Administrator's Guide*.

If you upgraded or migrated OpenPages and you are deploying the approval app for the first time, complete these steps to deploy the approval app:

1. Complete the pre-deployment tasks for the approval app. Check system requirements and back up your environment. For more information, see [“Pre-upgrade tasks for the approval app” on page 362](#).
2. Make sure that you have all of the object types and field groups - along with the associations - loaded onto your system. For more information, see [“Ensuring that you have the fields and field groups required for the approval app profile” on page 363](#).
3. If you want to configure the approval app profile for selected object types only, exclude the object types that you don't want. For more information, see [“Excluding object types from the approval app profile” on page 364](#).
4. Modify the **Trigger Configuration Files** registry setting. For more information, see [“Updating triggers for the approval app” on page 369](#).
5. Load the approval app profile and enable the app. For more information, see [“Loading the approval app profile” on page 370](#).
6. Complete the approval app deployment. For more information, see [“Completing the approval app deployment” on page 371](#).

Depending on your environment, you might need to do some additional tasks.

1. If you want to report on the fields and field groups for the approval app, regenerate the reporting framework. For more information, see the *IBM OpenPages with Watson Administrator's Guide*.
2. If you needed to add the object types, fields, and field groups that are required for the approval app and you use global search, re-create the search index.

Pre-upgrade tasks for the approval app

Before you upgrade the approval app, ensure that your system meets the system requirements, back up IBM OpenPages with Watson files, and gather the information that is required to complete the installation.

Ensure that you completed the upgrade or migration to version 8.2 or later. The OpenPages database upgrade must be complete before you upgrade the approval app.

If you want to be able to restore your environment to its current state, back up the OpenPages application environment, the IBM Cognos environment, and the database.

Gather the following information. You need this information to complete the installation.

- The user name and password of the OpenPages administrator on the admin application server
- The path of the OpenPages home directory, *OP_HOME*

Preparing for the deployment of the approval app

You must perform some preparation tasks before you deploy the approval app.

Procedure

1. Complete the upgrade to IBM OpenPages with Watson version 8.2.
2. Ensure that there are no long running OpenPages processes, such as a FastMap import process or a global search indexing process.
3. Check the status of the OpenPages servers. Verify that the following servers are running: the OpenPages application servers (admin and non-admin), reporting servers (active and standby), the Framework Model Generator, the database server, and the search server (optional).

For information about starting and stopping servers, see [Chapter 12, “Starting and stopping servers,” on page 309](#).

Supported data types and field types in the approval app

These data types and field types are supported by the approval app.

Note: If a field type is configured but not supported, the field type is ignored, that is, no error is produced.

- Date
- Boolean
- Integer
- Decimal
- Currency. For more information about the currency data type, see [Data types](#).
- The following system fields: Name, Description, Created By, Created On, Modified By, and Modified On.
- All text field types: URL, text box, text area, rich text. Includes support for rendering mathematical equations in rich text fields.
- All seven actor field display types: User Dropdown, User Selector, User/Group Selector, Multi User Selector, Multi User Group Selector, and Multi Group Selector.
- Business entity selector
- File attachments, with a link to view each attachment.
- Single-select enumerated fields and multi-select enumerated fields.
- Primary Parent hierarchy fields and Business Entity hierarchy fields.
- Hidden dependent fields.

If you have set up Field Level Security in OpenPages for specific fields, the value of the field in the approval app is hidden by a black bar with the word Confidential on it. For more information, see [Field Level Security](#).

The approval app does not support the following data types and field types:

- Report fragments
- Computed fields
- The following system fields: Folder or Location, Comments, Derived fields, and Orphan fields.

Ensuring that you have the fields and field groups required for the approval app profile

Make sure that you have all of the out-of-the-box fields and field groups required for the approval app profile loaded onto your system.

About this task

The approval app profile supports four object types (objects in parentheses are the related objects):

- SOXControl (SOXBusEntity, SOXDocument, SOXTest, SOXIssue, SOXRisk, SOXProcess)
- SOXIssue (SOXBusEntity, SOXTask (Action Item), SOXDocument)
- Incident (SOXBusEntity, SOXIssue, SOXDocument)
- LossEvent (SOXBusEntity, LossImpact, LossRecovery, SOXIssue, SOXRisk, SOXDocument, SOXProcess)

These object types use the following field groups, as well as the field groups that are loaded as a part of approval app installation:

SOXRisk

Uses OPSS-Rsk, OPSS-Risk, OPSS-Risk-Qual, OPSS-Risk-Quant, OPSS-Risk-Accp.

SOXTest

Uses OPSS-Shared-Test, OPSS-Test.

SOXTask

Uses OPSS-AI.

SOXIssue

Uses OPSS-Iss.

SOXControl

Uses OPSS-Ctl, OPSS-Ctl-Fin.

Incident

Uses OPSS-Inc, OPSS-Inc-IT.

LossEvent

Uses OPSS-LossEv, OPSS-Shared-Basel.

LossImpact

Uses OPSS-LossIm.

LossRecovery

Uses OPSS-LossRe.

In the Standard UI, click **Administration > Object Types**. Check that all of the object types, field groups, and fields are listed in the system.

You can also review the approval app Automated Form Configuration (AFCON) spreadsheet, Deck_AFCON_<version>.xls, to make sure that you have everything you need in your system. You can find the AFCON spreadsheet in the OP_<version>_Main/OP_<version>_Configuration/Approval_App/ directory.

If you upgraded or migrated from version 7.2.x and you are deploying the approval app for the first time, you might want to configure the approval app profile only for selected object types. For more information, see [“Excluding object types from the approval app profile” on page 364](#). If you performed a new installation, this step is not required.

Note: This topic lists the objects, field groups, and fields that you need to add if you have the 7.2 solutions schema. If you do not have the 7.2 solutions schema or if you customized the solutions schema, additional changes might be required. For more information, see [“Notes for users who do not have the 7.2 or later solutions schema” on page 368.](#)

Excluding object types from the approval app profile

If you migrated from version 7.2.x and you are deploying the approval app for the first time, you might want to configure the approval app profile for selected object types only and exclude others. If you performed a new installation of IBM OpenPages with Watson, this step is not required.

About this task

The approval app profile supports four object types. (See [“Ensuring that you have the fields and field groups required for the approval app profile” on page 363.](#))

You can choose to exclude any of these object types from the approval app profile. For example:

- You might not need Incidents because you don't use the Incident object type.
- You might have a customized process for an existing Loss Event object type to which you don't want to make any changes, but you might want to use the other object types for the approval app.

For a specific example of how to remove the LossEvent object type, see [“Excluding the Loss Event object type from the approval app profile” on page 365.](#)

Important: If you exclude an object type, you must also remove any objects that are associated exclusively with the object type.

Use the following steps to exclude an object from the four objects that are supported by the approval app profile. To do this procedure, you must use the **OpenPages Platform 3** profile.

Procedure

1. In the `Load_End_User_App_Schema.sh|.bat` file, comment out the commands that load the files that are related to the object types from the loader file. Do this step to exclude loading the objects when you load the approval app profile.
 - For a Windows computer: In the `Load_End_User_App_Schema.bat` file, comment out the block of code relevant to the object type you want to exclude by adding `REM` at the beginning of each line.
 - For a Linux computer: In the `Load_End_User_App_Schema.sh` file, comment out the block of code relevant to the object type you want to exclude by adding `#` at the beginning of each line.

For an example of the code to be commented out, see step 1 in [“Excluding the Loss Event object type from the approval app profile” on page 365.](#)

2. Edit the `deck_config.json` file to exclude the object types.

- a) Locate the `deck_config.json` file.

The approval app working directory is: `<OP_HOME>/installer/migration/upgrade/addon_module/loaderdata/deck`.

- b) Unzip `deck-config-opx-op-file-content.zip`.
- c) Locate the `End User Applications Config` folder.
- d) Locate the `deck_config.json` file.
- e) Make a backup copy of `deck_config.json` in case you need to repeat any steps.

For more information, see "Configuring the JSON file for the approval app" in the *IBM OpenPages with Watson Administrator's Guide*.

After you edit and save the file `deck_config.json`, you must copy it back to the `End User Applications Config` directory and zip it back into `deck-config-opx-op-file-content.zip`.

3. Edit the Deck_AFCON_<version>.xls spreadsheet to remove the object, the associated objects, and the related views.

The file is stored in: OP_<version>_Main/OP_<version>_Configuration/Approval_App/.

Note: Before you start to edit the AFCON spreadsheet, make a backup copy of the AFCON spreadsheet. If you run into difficulties, you can start again from the backup copy.

4. Follow the steps in the AFCON user manual to generate the .xml file from the updated AFCON spreadsheet for the approval app profile.

The AFCON user manual is stored on the installation media AFCON-RAFCON/Afcon.zip.

The AFCON tool generates four .xml files:

- IBM_OP_DECK_object-profile-op-config.xml
- IBM_OP_DECK_object-strings-op-config.xml
- IBM_OP_DECK_rule-based-security-op-config.xml
- IBM_OP_DECK_schema-op-config.xml

5. Rename the IBM_OP_DECK_object-profile-op-config.xml file to deck-profile-op-config.xml and paste it in the approval app working directory. Ignore all of the other files.

The approval app working directory is: <OP_HOME>/installer/migration/upgrade/addon_module/loaderdata/deck.

Alternatively, you can edit the profile .xml file manually to match your requirements. You must remove the object type and its associated parent and child object types in the following sections: objectProfile and ObjectProfileViewSet.

6. Back up the openpages-solutions.xml file.

a) Go to **Administration > Manage System Files > SysXMLDocument**.

b) Expand the **TriggerConfigFiles** folder.

c) Download the openpages-solutions.xml and name it openpages-solutions-bk.xml.

If you want to exclude Loss Event but you want to include Issue, you must copy the triggers for Issue from OpenPages version 7.2.0.1 or later and replace the triggers for Issue in the OpenPages 7.2 version of the file.

Note: You can get a copy of the version 7.2 openpages-solutions.xml file from the installation media. The file is located in OP_<version>_Main/OP_<version>_Configuration/Modules/Upgrade/ORM/triggers/7.2_openpages_solutions/.

Excluding the Loss Event object type from the approval app profile

If your organization currently uses the Loss Event object type and you don't want to make changes to that process, but you want to use the approval app for the other object types, this task provides detailed steps on how to exclude the Loss Event object type from the approval app.

About this task

If you migrated from version 7.2.x and you are deploying the approval app for the first time, you might want to configure the approval app profile to exclude the Loss Event object type.

The approval app profile supports four object types. One of these is the Loss Event object type.

You may want to exclude the Loss Event object type for the following reasons:

- You may already be using the Loss Event object type and its triggers.
- You don't have the Loss Event object type deployed in OpenPages.

Important: If you exclude an object type, you must also remove any objects associated exclusively with the object type. For example, if you want to exclude the Loss Event object type, you must remove the associated objects LossImpact and LossRecovery. However, note that you must keep the objects

SOXIssue, SOXDocument, SOXRisk, SOXProcess, and SOXBusEntity because they are also associated with SOXControl, which is still included in the profile.

Use the following steps to exclude the Loss Event object type from the four objects supported by the approval app profile. To perform this procedure, you must use the **OpenPages Platform 3** profile.

Procedure

1. Edit the `openpages-deck-schema-loader-data.txt` file by commenting out the lines that are related to the objects that you want to exclude.

For example, to exclude the Loss Event object type, in the Loading Deck Schema block, comment out `deck-schema-lossevent` and, in the Loading Deck Lifecycle block, comment out `deck-lifecycle-lossevent`.

```
# Loading Deck Schema
deck-schema-control
deck-schema-control-questions
deck-schema-issue
# deck-schema-lossevent

# Loading Deck lifecycle
deck-lifecycle-control
deck-lifecycle-incident
deck-lifecycle-issue
# deck-lifecycle-lossevent

# Loading Deck profile
Deck_object-profile
```

2. Edit the `deck_config.json` file to exclude the Loss Event object type.

- a) Locate the `deck_config.json` file.

The file is stored in: `<OP_HOME>/installer/migration/upgrade/addon_module/loaderdata/deck`.

- b) Unzip `deck-config-opx-op-file-content.zip`.
- c) Go to the folder `End User Applications Config`.
- d) Locate the file `deck_config.json`.
- e) Make a backup copy of `deck_config.json` in case you need to repeat any steps.

For more information, see "Configuring the JSON file for the approval app" in the *IBM OpenPages with Watson Administrator's Guide*.

To exclude the Loss Event object type, remove "LossEvent" from the `objectTypes` block:

Before:

```
"objectTypes" : ["SOXControl", "SOXIssue", "LossEvent", "Incident"],
```

After:

```
"objectTypes" : ["SOXControl", "SOXIssue", "Incident"],
```

Also, remove the following code from the `objects` block:

```
{
  "type" : "LossEvent",
  "fieldTitle" : "Name",
  "fieldDesc" : "Description",
  "lifecycle" : {
    "enabled" : true,
    "stageMap" : {
      "Awaiting Approval" : {"showInList": true},
      "Awaiting Approval L1" : {"showInList": true},
      "Awaiting Approval L2" : {"showInList": true}
    }
  },
  "widgetList" : [
    {

```



```

        "name" : "details",
        "type" : "activityView",
        "activityView" : "OP-Deck-LE",
        "parentViews" : [
            {
                "type" : "SOXRisk",
                "activityView" : "OP-Deck-LE-Risk"
            }
        ]
    },
    ]
}

```

After you edit and save the `deck_config.json` file, copy it back to the /End User Applications Config folder and zip it back into `deck-config-opx-op-file-content.zip`.

3. Edit the `Deck_AFCON_<version>.xls` spreadsheet to remove the Loss Event object, the associated objects, and the related views.

The file is stored in: `OP_<version>_Main/OP_<version>_Configuration/Approval_App/`.

Note: Before you start to edit the AFCON spreadsheet, make a backup copy of the AFCON spreadsheet. If you run into difficulties, you can start again from the backup copy.

- a) Delete the worksheets Loss Event, Loss Impact, Loss Recovery, AV - OP-Deck-LE, and AV - OP-Deck-LE-Risk.
 - b) From the Labels - Object Types worksheet, delete the rows related to Loss Event, Loss Impact, and Loss Recovery.
 - c) From the Default Views worksheet, delete the rows related to Loss Event, Loss Impact, and Loss Recovery.
 - d) From the Overviews worksheet, delete the rows related to Loss Event, Loss Impact, and Loss Recovery (Note: No change in the case of Loss Event).
 - e) From the Date Dimension Associations worksheet, delete the rows related to the field groups associated to Loss Event, Loss Impact, and Loss Recovery. In this case, delete all rows related to OPSS-LossEv, OPSS-LossIm, and OPSS-LossRe.
 - f) From the Navigational Views Order worksheet, delete the rows related to Loss Event, Loss Impact, and Loss Recovery.
 - g) From the Object Views Order worksheet, delete the rows related to Loss Event, Loss Impact, and Loss Recovery.
4. Follow the steps in the AFCON user manual to generate the .xml files from the updated AFCON spreadsheet for the approval app profile.

The AFCON user manual is stored on the installation media `AFCON-RAFCON/Afcon.zip`.

The AFCON tool generates four .xml files:

- `IBM_OP_DECK_object-profile-op-config.xml`
 - `IBM_OP_DECK_object-strings-op-config.xml`
 - `IBM_OP_DECK_rule-based-security-op-config.xml`
 - `IBM_OP_DECK_schema-op-config.xml`
5. Rename the `IBM_OP_DECK_object-profile-op-config.xml` file to `deck-profile-op-config.xml` and paste it in the approval app working directory, `<OP_HOME>/installer/migration/upgrade/addon_module/loaderdata/deck`. Ignore all the other files.

Alternatively, you can edit the profile .xml file manually to match your requirements. You must remove the object type and its associated parent and child object types in the following sections: `objectProfile` and `ObjectProfileViewSet`.

6. Before you proceed to step 7, make sure that you understand the following background information about copying the SOXIssue trigger content from OpenPages version 7.2.0.1 or later to the `openpages-solutions.xml` file from OpenPages version 7.2.

When OpenPages version 7.2 is installed, the `openpages-solutions.xml` file is stored in the **SysXMLDocument > TriggerConfigFiles** folder.

For the present example where Loss Event is excluded from the approval app, you must modify the `openpages-solutions.xml` file from OpenPages version 7.2 and replace the trigger content for the SOXIssue object with the trigger content for the SOXIssue object from the version of `openpages-solutions.xml` from OpenPages version 7.2.0.1 or later.

Because you are excluding the Loss Event object type from the approval app, you want to retain the OpenPages 7.2 triggers from the OpenPages 7.2 Loss Event triggers, while updating the SOXIssue triggers with the newer version needed for the approval app.

For the SOXIssue object, the triggers in OpenPages version 7.2.0.1 or later are changed to work with the approval app. So you must copy the SOXIssue trigger content from the OpenPages version 7.2.0.1 or later `openpages-solutions.xml` file into the `openpages-solutions.xml` file in OpenPages version 7.2 and then save the file.

7. Download the `openpages-solutions.xml` file.

- a) Go to **Administration > Manage System Files > SysXMLDocument**.
- b) Expand the **TriggerConfigFiles** folder.
- c) Download the `openpages-solutions.xml` and name it `openpages-solutions-72.xml`.

8. Edit the `openpages-solutions.xml` file.

The file is stored in: `<OP_HOME>/installer/migration/upgrade/addon_module/loaderdata/deck`.

- a) Unzip `deck-lifecycle-trigger-op-file-content.zip`.
- b) Make a backup copy of `openpages-solutions.xml` in case you need to modify it again. Name it `openpages-solutions-backup.xml` and save it.
- c) Edit `openpages-solutions.xml` from OpenPages version 7.2.0.1 or later. Locate the following section and copy it:

```
<!-- T-009 Issue Life Cycle Status Update Trigger Begin -->
...
</trigger>
```

- d) Edit the `openpages-solutions.xml` file from OpenPages version 7.2. Using the lines you copied in step 8c, replace the matching `.xml` snippet in the existing OpenPages version 7.2 version that you downloaded. Save the file.
- e) Take the `openpages-solutions.xml` you saved in step 8d and copy it back to the approval app working directory.
- f) Zip the file `deck-lifecycle-trigger-op-file-content.zip` and be sure that `deck-lifecycle-trigger-op-file-content.zip` is under the approval app working directory.

Note: You can get a copy of the version 7.2 `openpages-solutions.xml` file from the installation media. The file is located in `OP_<version>_Main/OP_<version>_Configuration/Modules/Upgrade/ORM/triggers/7.2_openpages_solutions/`.

The approval app working directory is: `<OP_HOME>/installer/migration/upgrade/addon_module/loaderdata/deck`.

Now you are ready to load the approval app profile. For more information, see [“Loading the approval app profile”](#) on page 370.

Notes for users who do not have the 7.2 or later solutions schema

If you do not have the 7.2 or later solutions schema in your environment or if you customized the solutions schema, you might need to add or modify objects, field groups, and fields before you load the approval app profile.

For example, if you installed version 7.1 with solutions and then migrated to 8.2, your environment has the 7.1 solutions schema. The 7.1 solutions schema might not have all of the objects, field groups, and fields that you need for the approval app.

Examine the approval app Automated Form Configuration (AFCON) spreadsheet, Deck_AFCON_<version>.xls. Perform the following checks:

- Make sure that you have the objects, field groups, and fields for the approval app.
- Make sure that the attributes match, for example make sure that the display type of each field is defined correctly.
- Make sure that you have any prerequisites for the objects, field groups, and fields.

You can find the Deck_AFCON_<version>.xls spreadsheet in the OP_<version>_Main/OP_<version>_Configuration/Approval_App/ directory.

Updating triggers for the approval app

If you upgraded or migrated IBM OpenPages with Watson and you are deploying the approval app for the first time, you need to modify the **Trigger Configuration Files** registry setting for the approval app profile.

Before you begin

Upgrade or migrate to IBM OpenPages with Watson 8.2.

Make sure your system has the required fields and field groups as described in [“Ensuring that you have the fields and field groups required for the approval app profile ” on page 363.](#)

About this task

The **Trigger Configuration Files** registry setting defines the trigger files to load when IBM OpenPages with Watson starts. For more information, see the *IBM OpenPages with Watson Trigger Developer Guide*.

The trigger files set the lifecycle for the included object types on the system. Lifecycles define the stages that an object type can follow. At each stage, the system:

- Identifies a lifecycle assignee
- Defines the actions available to move to a different stage
- Automatically sends an email to the new lifecycle assignee (LCAssignee)
- Defines other attributes that are related to the current stage

Procedure

1. Log on to IBM OpenPages with Watson as a user with administrative privileges.
2. In the Standard UI, click **Administration > Settings > GRM > Trigger Configuration Files**.
3. Update the value for the **Trigger Configuration Files** setting.

Add the following files, separated by commas.

- OPLC-LossEvent.xml
- OPLC-SOXControl.xml
- OPLC-SOXIssue.xml

For example:

```
OPLC-LossEvent.xml,OPLC-SOXControl.xml,OPLC-SOXIssue.xml
```

Note: If you want to exclude an object type from the approval app, do not include the related OPLC-*<object type>*.xml file in the **Trigger Configuration Files** registry setting.

Loading the approval app profile

If you upgraded or migrated IBM OpenPages with Watson and you are deploying the approval app for the first time, you need to load the approval app profile and enable the app.

Before you begin

You must install IBM OpenPages with Watson 8.2 before you load the profile and enable the approval app.

Make sure that your system has the required fields and field groups as described in [“Ensuring that you have the fields and field groups required for the approval app profile”](#) on page 363.

If you upgraded or migrated IBM OpenPages with Watson and you are deploying the approval app for the first time, modify the **Trigger Configuration Files** registry setting before you load the approval app profile. For more information, see [“Updating triggers for the approval app”](#) on page 369.

About this task

In addition to the approval app profile, the scripts make the following changes:

- Load schema changes for three object types (SOXControl, SOXIssue, LossEvent)
- Load lifecycle schema changes for 4 object types (Incident, SOXControl, SOXIssue, LossEvent)
- Load Certification Questions (for SOXControl)
- Load `deck_config.json`
- Load the lifecycle trigger definition XML files (see step 1)
- Enable the approval app

Procedure

1. If you have an existing profile with an **LCAssignee** field for the object types that are supported by the lifecycle, perform the following steps to specify the display type of the field as **Multi Valued User/Group Selector**.
 - a) Go to the profile in which you want to make changes. In the Standard UI, click **Administrator > Profiles**.
 - b) Click the object type that includes the **LCAssignee** field.
 - c) Click **LCAssignee**.
 - d) In the **Object Field Information** section, click **Edit**.
 - e) From the **Display Type** drop-down, click **Multi Valued User/Group Selector**.
 - f) Click **Save**.

This specifies the display type of the **LCAssignee** field for all the object types that are supported by the lifecycle to be **Multi Valued User/Group Selector**. You can now have multiple assignees.

Tip: You can check if you have an existing profile with an **LCAssignee** field. **LCAssignee** is a specific field in a specific field group **OPLC-Std**. In version 7.2, this field was only in Incident and Questionnaire Assessment object types. You can look in each object type and see if it includes the **OPLC-Std** field group. Then, for each of those object types, look in each profile that object type is included in.

2. Load the approval app profile and enable the app.
 - Windows:
 - a. Go to the approval app working directory: `<OP_HOME>/installer/migration/upgrade/addon_module/loaderdata/deck`.
 - b. Update `openpages_domain_folder`, `login_username`, and `login_password properties` in `Environment_Variables.bat`.
 - c. Run `Load_Deck_Schema.bat`. Wait for the script to complete before you continue to the next step.

- d. Run `Load_End_User_App_Schema.bat`.
- e. For security purposes, remove the password from the `Environment_Variables.bat` file.
- Linux:
 - a. Go to the approval app working directory: `<OP_HOME>/installer/migration/upgrade/addon_module/loaderdata/deck`.
 - b. Update `openpages_domain_folder`, `login_username`, and `login_password` properties in `Environment_Variables.sh`.
 - c. Run `Load_Deck_Schema.sh`
 - d. Run `Load_End_User_App_Schema.sh`. Wait for the script to complete before you continue to the next step.
 - e. For security purposes, remove the password from the `Environment_Variables.sh` file.

Completing the approval app deployment

Complete the remaining steps to deploy the approval app.

Procedure

1. Restart the OpenPages server on all application servers. For information about starting and stopping servers, see [Chapter 12, “Starting and stopping servers,”](#) on page 309.
2. Perform any conditional tasks required by your environment.
For more information, see [“Conditional steps for the approval app”](#) on page 371.

Results

The approval app is deployed.

Conditional steps for the approval app

Depending on your environment, you might need to perform some additional tasks.

Perform these tasks after you complete all other deployment tasks. If you are installing other IBM OpenPages with Watson components, such as a fix pack or IBM OpenPages Loss Event Entry, perform these steps after all components are installed.

If you want to report on the fields and field groups for the approval app, regenerate the reporting framework. For more information, see [Regenerating the reporting framework](#).

If you added the objects, fields, and field groups required for the approval app and you use global search, re-create the global search index.

Upgrade the approval app

If you deployed the approval app in version 7.2.0.1 or a later 7.2.x fix pack and you then upgraded or migrated IBM OpenPages with Watson to version 8.2 or later, you need to perform some additional steps to upgrade the approval app.

Note: If you did these steps in a previous release, you do not need to do them again in 8.2.

1. Complete the pre-upgrade tasks for the approval app. Check system requirements and back up your environment. For more information, see [“Pre-upgrade tasks for the approval app”](#) on page 362.
2. Update the approval app configuration file. For more information, see [“Updating the approval app configuration file”](#) on page 372.
3. Upgrade the approval app. For more information, see [“Upgrading the approval app”](#) on page 373.

Pre-upgrade tasks for the approval app

Before you upgrade the approval app, ensure that your system meets the system requirements, back up IBM OpenPages with Watson files, and gather the information that is required to complete the installation.

Ensure that you completed the upgrade or migration to version 8.2 or later. The OpenPages database upgrade must be complete before you upgrade the approval app.

If you want to be able to restore your environment to its current state, back up the OpenPages application environment, the IBM Cognos environment, and the database.

Gather the following information. You need this information to complete the installation.

- The user name and password of the OpenPages administrator on the admin application server
- The path of the OpenPages home directory, *OP_HOME*

Updating the approval app configuration file

When you upgrade the approval app, you need to update the `deck_config.json` configuration file.

Note: If you did these steps in a previous release, you do not need to do them again in 8.2.

Before you begin

To do this procedure, you must use the **OpenPages Platform 3** profile.

Procedure

1. Back up the `deck_config.json` file.
 - a) In the Standard UI, click **Administration > Manage System Files > SysXMLDocument**.
 - b) Click **End User Applications Config > deck_config.json**.
 - c) Click **View file** and save it.
2. Delete the `deck_config.json` file.
 - a) Return to the **End User Applications Config** folder.
 - b) Click the check box next to **deck_config.json**, and then click **Delete**.
 - c) Click **OK**.
3. Update the `deck-config-opx-op-file-content.zip` file.
 - a) Go to the `<OP_HOME>/installer/migration/upgrade/addon_module/loaderdata/deck` directory on the application server.
 - b) Use a compression utility to open or extract the `deck-config-opx-op-file-content.zip` file.
 - c) Replace the `deck_config.json` file in the `.zip` file with the `deck_config.json` that you backed up.
 - d) Use a compression utility to recompress the `deck-config-opx-op-file-content.zip` file.

Note: Make sure that the files are packaged back into the `deck-config-opx-op-file-content.zip` file with the same directory structure as in the original `.zip` file.
4. Load the `deck_config.json` file.
 - a) Select the check box next to the **End User Applications Config** folder.
 - b) Click **Add New**.
 - c) Click **Browse** and select the `deck_config.json` file.

Upgrading the approval app

If you deployed the approval app in IBM OpenPages with Watson version 7.2.0.1 or later and then upgraded or migrated IBM OpenPages with Watson, you need to upgrade the app.

Before you begin

Complete this task after you upgrade or migrate IBM OpenPages with Watson.

Procedure

1. Log on to the OpenPages admin application server as a user with administrative privileges.
2. Start the IBM OpenPages with Watson services on all application servers.
For more information, see [Chapter 12, “Starting and stopping servers,”](#) on page 309.
3. On Windows computers, start a Command Prompt window with the **Run as administrator** option. On Linux computers, open a shell.
4. Go to the approval app working directory: `<OP_HOME>/installer/migration/upgrade/addon_module/loaderdata/deck`.
5. Update the following properties in the `Environment_Variables.bat | .sh` file.
 - `openpages_domain_folder`: Type the location of the `<OP_HOME>/bin` directory.
 - `login_username`: Type the OpenPages Administrator user name. (You can find the user name in the installation app or in the `op_admin_username` property in the `deploy.properties` file.)
 - `login_password`: Type the password of the OpenPages Administrator.
 - `loader_data_folder`: Type the location of the `<OP_HOME>/Module/loaderdata/deck` directory.
 - `OBJ_STATUS_FILE`: Type the path and file name that you want to use for the object loading status log file, such as: `<OP_HOME>/Module/logs/ApprovalApp_objmgrloadingstatus.properties`
 - `OBJ_LOADER_FILE`: Type the path and file name that you want to use for the object loading error log file, such as: `<OP_HOME>/Module/logs/ApprovalApp_ObjectManagerLoadStatus.log`
6. Run the upgrade script.
 - Windows: `Upgrade_Deck.bat`
 - Linux: `./Upgrade_Deck.sh`
7. For security purposes, remove the password from the `Environment_Variables.bat | .sh` file.
8. Restart the OpenPages services on all application servers. For more information, see [Chapter 12, “Starting and stopping servers,”](#) on page 309.

Chapter 17. Loss Event Entry

Users across an organization can create loss events quickly and easily with IBM OpenPages Loss Event Entry. It is easy to use and task-focused for users with no experience with IBM OpenPages with Watson.

Users can access OpenPages Loss Event Entry without a sign-in account for IBM OpenPages with Watson. You can set up a link to OpenPages Loss Event Entry on your organization's intranet. When users click the link, they see the user interface in the language of their choice, and dates and numbers are formatted in ways that are familiar to them. Users can immediately begin entering information. When they submit a loss event, a confirmation email is sent to them.

OpenPages Loss Event Entry is integrated fully with IBM OpenPages with Watson. The following is an example of the workflow:

- Create a loss event in OpenPages Loss Event Entry.
- Triage, investigate, and enrich the loss event information in IBM OpenPages with Watson.
- Review and approve the loss event in the approval app.

Installation process overview for Loss Event Entry

If you want to use IBM OpenPages Loss Event Entry, you need to do some tasks to install it.

Do this task if you are doing a fresh installation of OpenPages Loss Event Entry. If you are upgrading or migrating, see [“Upgrade process overview for Loss Event Entry” on page 378](#) or [“Migration process overview for Loss Event Entry” on page 381](#).

During the installation of IBM OpenPages Loss Event Entry, you can choose to load the default data required for OpenPages Loss Event Entry automatically or manually. The default data includes the field groups, fields, users, role templates, profile, and other data needed for OpenPages Loss Event Entry.

If you want to load OpenPages Loss Event Entry data automatically, complete the following steps:

1. Install IBM OpenPages with Watson.
2. Install OpenPages Loss Event Entry.
3. Change OpenPages Loss Event Entry user passwords.
4. Configure OpenPages Loss Event Entry.

If you want to load OpenPages Loss Event Entry data manually, complete the following steps. Choose this option if you want to customize the field groups, fields, users, groups, profile, and other data used in OpenPages Loss Event Entry.

1. Install IBM OpenPages with Watson.
2. Install OpenPages Loss Event Entry.
3. Load the OpenPages Loss Event Entry data manually.
4. Change OpenPages Loss Event Entry user passwords.
5. Configure OpenPages Loss Event Entry.

Depending on your environment, you might also need to regenerate the reporting framework. If you installed OpenPages and then regenerated the reporting framework, you might need to regenerate it again after you install OpenPages Loss Event Entry.

Pre-installation tasks for Loss Event Entry

Before you install IBM OpenPages Loss Event Entry, ensure that your system meets the system requirements, back up IBM OpenPages with Watson files, and gather information required to complete the installation.

Ensure that the following software is installed:

- IBM OpenPages with Watson
- IBM Installation Manager 1.8.7 or later

If you want to be able to restore your environment to its current state, back up the OpenPages application environment, the IBM Cognos environment, and the database.

Gather the following information. You need this information to complete the installation.

- The user name and password of the OpenPages administrator on the admin application server
- The path of the OpenPages home directory, *OP_HOME*

Installation tasks for Loss Event Entry

After you complete the per-installation tasks, you can install IBM OpenPages Loss Event Entry.

Preparing for the installation of Loss Event Entry

To ensure that the IBM OpenPages Loss Event Entry Installer is able to perform all necessary steps, you must perform some preparation tasks.

Procedure

1. Ensure that there are no long running OpenPages processes, such as a FastMap import process or a global search indexing process.
2. Check the status of IBM OpenPages with Watson servers. Verify that the following servers are running: the application servers (admin and non-admin), reporting servers (active and standby), the Framework Model Generator, and the database server.

For information about starting and stopping servers, see [Chapter 12, “Starting and stopping servers,” on page 309](#).

Installing Loss Event Entry

You must run the IBM OpenPages Loss Event Entry installation program on the OpenPages admin application server.

Procedure

1. Make sure that the OpenPages servers are running. See [“Preparing for the installation of Loss Event Entry” on page 376](#).
2. Download the OpenPages Loss Event Entry 8.2 installer package from [IBM Passport Advantage](#).
3. Extract the package files.
4. On the admin application server, start IBM Installation Manager.
5. Add the OpenPages Loss Event Entry repository to IBM Installation Manager.
 - a) Click **File > Preferences**.
 - b) Click **Repositories** and then click **Add Repository**.
 - c) Select the OpenPages Loss Event Entry installer package.
 - d) Click the `repository.config` file.
 - e) Click **OK**.
 - f) Click **OK** to return to the main IBM Installation Manager page.
6. Click **Install**.
7. Select **IBM OpenPages Loss Event Entry** and **Version 8.2**, and click **Next**.
8. Accept the license agreement and click **Next**.
9. Click **Next**.

Note: The installation directory does not impact the installation process. The files are installed to the same directory as the IBM OpenPages with Watson installation (*OP_HOME*).

10. In the Features list, make sure that **IBM OpenPages Loss Event Entry 8.2** is selected and click **Next**.
11. In the **Enter the location of your OpenPages installation** field, enter the path to the OpenPages home directory, *OP_HOME*. Type the path or click **Browse** to select the directory. This directory contains the *openpagesregistry.xml* file and the *bin* subdirectory.
12. In the **User Name** field, enter the user name for the administrator account on the OpenPages admin application server.
13. In the **Password** field, enter the password for the administrator account on the OpenPages admin application server.
14. Click one of the options for loading the default data. The default data includes the default users, groups, role templates, fields, field groups, profile, and other data used in OpenPages Loss Event Entry.
 - If you choose to load the data automatically, the installation program loads the default data used in OpenPages Loss Event Entry.
 - If you choose not to load the default data automatically, the installation program creates the files on your system but does not load them. You must load the data files manually before you use OpenPages Loss Event Entry. Select this option if you want to customize the data before loading it. For information about loading the data manually, see [“Manual data loading for Loss Event Entry” on page 383](#).
15. Click **Next**. If any errors appear on the page, follow the instructions to fix them before you continue.

If you see validation errors during the data load process, see [“Data validation errors when installing Loss Event Entry” on page 458](#).
16. Click **Finish**.

What to do next

- If you chose not to load the data automatically, load the data manually before performing the post-installation tasks. See [“Manual data loading for Loss Event Entry” on page 383](#).
- If you chose to load the data automatically, continue with [“Post-installation tasks for Loss Event Entry” on page 377](#).

Log files for Loss Event Entry

If errors occur when you install IBM OpenPages Loss Event Entry, you can review the log files.

The ObjectManager log files generated when loading the default data for OpenPages Loss Event Entry are located in *<OP_HOME>/LossEventEntry/logs/*.

If you see validation errors about data that already exists, see [“Data validation errors when installing Loss Event Entry” on page 458](#).

Post-installation tasks for Loss Event Entry

After you install IBM OpenPages Loss Event Entry, you need to complete some additional tasks.

Certain prerequisites must be met to configure and use OpenPages Loss Event Entry.

- Setting passwords
- Configuring OpenPages Loss Event Entry

If you chose not to load the OpenPages Loss Event Entry default data automatically during the installation process, load the data manually before performing the post-installation tasks.

Setting passwords for Loss Event Entry users

After you have installed IBM OpenPages Loss Event Entry, you need to configure the passwords for the Loss Event Entry users.

Before you begin

If you chose not to load the default data automatically during the installation process, load the data manually before setting passwords.

About this task

When you set passwords in the configuration tool and save your changes, the passwords are updated in IBM OpenPages with Watson. Passwords are encrypted.

Procedure

1. Start the configuration tool. Go to `http://<server_name>:<port>/openpages/app/jspview/lossevent#/editconfig`
2. Log in with a user account that is a member of the OPAdministrators group.
3. Under the **Locales** section, expand each locale and enter a password.
4. Close the configuration tool.
5. Log in to OpenPages as an administrator.
6. Click **Administration > Users**.
7. In the **View, Edit, or Disable User** field, search for the user account for each locale that you configured in step 3.
8. On the **User Information** panel, click **Reset Password**.
9. Select **User cannot change password**, and then select **Password never expires**.
10. Repeat steps 7-9 for each Loss Event Entry user.

Configuration of Loss Event Entry

You can configure IBM OpenPages Loss Event Entry to meet the needs of your organization.

The configuration tool enables you to customize OpenPages Loss Event Entry. For more information, see the *IBM OpenPages with Watson Administrator's Guide*.

Conditional steps for Loss Event Entry

Depending on your environment, you might need to perform some additional tasks.

Perform these tasks after you complete all installation and post-installation tasks. If you are installing other IBM OpenPages components, such as a fix pack or the approval app, perform these steps after all components are installed.

If you want to report on the fields and field groups for OpenPages Loss Event Entry, regenerate the reporting framework. For more information, see the *IBM OpenPages with Watson Administrator's Guide*.

If you needed to add the objects, fields, and field groups required for OpenPages Loss Event Entry and you use global search, re-create the search index. See [“Creating the global search index” on page 186](#).

Upgrade process overview for Loss Event Entry

If you upgraded IBM OpenPages with Watson, you need to upgrade IBM OpenPages Loss Event Entry. You also need to upgrade OpenPages Loss Event Entry if you migrated from OpenPages 7.2.x or later, you previously installed OpenPages Loss Event Entry, and you are using your existing hardware for OpenPages Loss Event Entry.

Complete the following steps:

1. Complete the pre-installation tasks for OpenPages Loss Event Entry. For more information, see [“Pre-installation tasks for Loss Event Entry” on page 375](#).
2. Complete the preparation tasks for installing OpenPages Loss Event Entry. For more information, see [“Preparing for the installation of Loss Event Entry” on page 376](#).
3. Optional: If you customized the OpenPages Loss Event Entry data files, back up the files.
4. Upgrade OpenPages Loss Event Entry.
5. Update the OpenPages Loss Event Entry configuration file.

Depending on your environment, you might also need to regenerate the reporting framework. If you upgraded or migrated OpenPages and then regenerated the reporting framework, you might need to regenerate it again after you install OpenPages Loss Event Entry.

Upgrading Loss Event Entry

You can upgrade IBM OpenPages Loss Event Entry.

Before you begin

Before you upgrade, complete the following tasks:

- [“Pre-installation tasks for Loss Event Entry” on page 375](#)
- [“Preparing for the installation of Loss Event Entry” on page 376](#)

About this task

If you upgraded IBM OpenPages with Watson, you need to upgrade IBM OpenPages Loss Event Entry.

You also need to upgrade OpenPages Loss Event Entry if you migrated from OpenPages 7.2.x or later, you previously installed OpenPages Loss Event Entry, and you are using your existing hardware for OpenPages Loss Event Entry.

If you migrated and you are using new hardware for OpenPages Loss Event Entry, see [“Migration process overview for Loss Event Entry” on page 381](#).

Procedure

1. Make sure that the OpenPages servers are running. See [“Preparing for the installation of Loss Event Entry” on page 376](#).
2. Download the IBM OpenPages Loss Event Entry 8.2 installer package from [IBM Passport Advantage](#).
3. Extract the package files.
4. On the admin application server, start IBM Installation Manager.
5. Add the OpenPages Loss Event Entry repository to IBM Installation Manager.
 - a) Click **File > Preferences**.
 - b) Click **Repositories** and then click **Add Repository**.
 - c) Select the OpenPages Loss Event Entry installer package.
 - d) Click the `repository.config` file.
 - e) Click **OK**.
 - f) Click **OK** to return to the main IBM Installation Manager page.
6. Click **Update**.
7. Select **IBM OpenPages Loss Event Entry**, and click **Next**.
8. Select **Version 8.2**, and then click **Next**.
9. Accept the license agreement and click **Next**.
10. In the Features list, make sure that **IBM OpenPages Loss Event Entry 8.2** is selected and click **Next**.

11. In the **Enter the location of your OpenPages installation** field, enter the path to the OpenPages home directory, *OP_HOME*. Type the path or click **Browse** to select the directory. This directory contains the *openpagesregistry.xml* file and the *bin* subdirectory.
12. In the **User Name** field, enter the user name for the administrator account on the OpenPages admin application server.
13. In the **Password** field, enter the password for the administrator account on the OpenPages admin application server.
14. Click the option to not load the data automatically.
15. Click **Next**. If any errors appear on the page, follow the instructions to fix them before you continue.
16. Click **Update**.
17. Click **Finish**.

What to do next

Update the OpenPages Loss Event Entry configuration file. For more information, see [“Updating the Loss Event Entry configuration file”](#) on page 380.

Updating the Loss Event Entry configuration file

After you upgrade or migrate IBM OpenPages Loss Event Entry, you need to update the *lossevent_config.json* configuration file.

Before you begin

To perform this procedure, you must use the **OpenPages Platform 3** profile.

Procedure

1. Back up the *lossevent_config.json* file.
 - a) Switch to the Standard UI.
 - b) From the menu bar, click **Administration > Manage System Files > SysXMLDocument**.
 - c) Click **End User Applications Config > lossevent_config.json**
 - d) Click **View file** and save it.
2. Delete the *lossevent_config.json* file.
 - a) Return to the **End User Applications Config** folder.
 - b) Click the check box next to **lossevent_config.json**, and then click **Delete**.
 - c) Click **OK**.
3. Add the Japanese locale to the *lossevent_config.json* file.
 - a) Open the *lossevent_config.json* file that you downloaded.
 - b) Add the following text at the end of the file, after the *zh_CN* locale.

```
"ja_JP": {  
  "user": "LEE_JA_JP",  
  "password": "",  
  "enabled": true  
}
```

The updated file now includes the Japanese locale:

```
"zh_CN": {  
  "user": "LEE_ZH_CN",  
  "password": "",  
  "enabled": true  
},  
"ja_JP": {  
  "user": "LEE_JA_JP",  
  "password": "",  
  "enabled": true  
}
```

```

        "enabled":true
      }
    }
  }
}

```

- c) Save the file.
4. Update the lossevent-entry-config-opx-op-file-content.zip file.
 - a) Go to the <OP_HOME>/LossEventEntry directory on the application server.
 - b) Use a compression utility to open or extract the lossevent-entry-config-opx-op-file-content.zip file.
 - c) Replace the lossevent_config.json file in the .zip file with the lossevent_config.json that you updated.
 - d) Use a compression utility to recompress the lossevent-entry-config-opx-op-file-content.zip file.

Note: Make sure that the files are packaged back into the lossevent-entry-config-opx-op-file-content.zip file with the same directory structure as in the original .zip file
5. Update OpenPages Loss Event Entry.
 - a) Update the <OP_HOME>/LossEventEntry/Environment_Variables.bat|sh file with the values for your environment.
 - b) Go to <OP_HOME>/LossEventEntry/upgrade.
 - c) Open a command line and run Upgrade_LossEvent_Entry_App_Schema.bat|sh.
 - d) Remove the password from the login_password variable in the Environment_Variables.bat|sh file.
6. Update and review the settings in the OpenPages Loss Event Entry configuration tool.
 - a) Open the OpenPages Loss Event Entry configuration tool in a browser.
For example, navigate to `http://<hostname>:10108/openpages/app/jspview/lossevent#/editconfig`
 - b) Update the password for the Japanese locale user.
 - c) Review the other configuration settings.
 - d) Click **Save** to load the configuration.

Migration process overview for Loss Event Entry

You can migrate IBM OpenPages Loss Event Entry to a new environment. Do this task if you migrated from OpenPages 7.2.x or later, you previously installed OpenPages Loss Event Entry, and you are using new hardware for OpenPages Loss Event Entry.

Complete the following steps.

1. Install OpenPages Loss Event Entry in the target environment. Choose the option to not load the data automatically. For more information, see [“Installation process overview for Loss Event Entry”](#) on page 375.
2. Optional: If you customized the OpenPages Loss Event Entry data files in the source environment and you want to keep a copy, back up the data files.

The data files are stored in the OpenPages Loss Event Entry working directory, <OP_HOME>/LossEventEntry/.
3. Update the OpenPages Loss Event Entry configuration file. For more information, see [“Updating the Loss Event Entry configuration file”](#) on page 380.

Additional tasks for Loss Event Entry

Silent installation for Loss Event Entry

You can run a silent installation by using the Silent mode in IBM Installation Manager.

Before you perform a silent installation, ensure that you have prepared your system for deploying IBM OpenPages Loss Event Entry.

You can generate a response file by using IBM Installation Manager, or you can create one manually. A template for creating a response file, called `response_template.xml`, is stored in the OpenPages Loss Event Entry installer package in the `OP_version_LOS_EV_EN` directory. The response file must contain the following code. Update the variables with the values for your environment:

Profile name

The name of the profile you want to use for OpenPages Loss Event Entry

Install location

The installation directory has no impact on the installation. OpenPages Loss Event Entry is installed to the same directory as IBM OpenPages with Watson, `OP_HOME`. Specify a directory that does not exist in your environment.

Path to OpenPages home

The absolute path to the OpenPages home directory, `OP_HOME`. This directory should contain the file `openpagesregistry.xml` and the subdirectory `bin`.

OpenPages administrator user name

The user name of the administrator account on the OpenPages admin application server.

OpenPages administrator password

The password for the administrator account on the OpenPages admin application server.

true or false

Choose an option for loading the default data for OpenPages Loss Event Entry. Enter `true` to load all default data, or enter `false` to load data manually later.

If you are upgrading or migrating OpenPages Loss Event Entry, enter `false`.

```
<?xml version='1.0' encoding='UTF-8'?>
<agent-input>
  <server>
    <repository location='((Path to repository for OpenPages Loss Event Entry))' />
  </server>
  <profile id='((Profile name))' installLocation='((Install location))'>
    <data key='user.OPHome,com.ibm.openpages.lossevententry'
      value='((Path to OpenPages home))' />
    <data key='user.OPAdminUsername,com.ibm.openpages.lossevententry'
      value='((OpenPages administrator user name))' />
    <data key='user.OPAdminPassword,com.ibm.openpages.lossevententry'
      value='((OpenPages administrator password))' />
    <data key='user.LoadAll,com.ibm.openpages.lossevententry'
      value='((true or false))' />
  </profile>
  <install>
    <offering profile='((Profile Name))' id='com.ibm.openpages.lossevententry' />
  </install>
</agent-input>
```

If you are upgrading OpenPages Loss Event Entry, follow these guidelines:

- The `repository location` must be the same as in the previous installation.
- The `Profile name` and `Install location` must be the same in the previous installation.

If you do not know the profile name and install location, check the list of installed packages in IBM Installation Manager. Run the command `imcl listInstalledPackages -verbose`. Look for the package group containing the OpenPages Loss Event Entry package. The name of the package group is the profile name, and the installation directory is the install location. For more information, see the [IBM](#)

[Installation Manager documentation \(https://www.ibm.com/support/knowledgecenter/SSDV2W_1.8.5/com.ibm.cic.commandline.doc/topics/t_imcl_viewing_installed_packages.html\)](https://www.ibm.com/support/knowledgecenter/SSDV2W_1.8.5/com.ibm.cic.commandline.doc/topics/t_imcl_viewing_installed_packages.html).

- The value for LoadAll should be false.

For more information about how to generate a response file to run the installer silently, see [Response files \(https://www.ibm.com/support/knowledgecenter/SSDV2W_1.8.5/com.ibm.silentinstall12.doc/topics/c_silent_response_files.html\)](https://www.ibm.com/support/knowledgecenter/SSDV2W_1.8.5/com.ibm.silentinstall12.doc/topics/c_silent_response_files.html).

Manual data loading for Loss Event Entry

If you did not load the IBM OpenPages Loss Event Entry default data when you installed OpenPages Loss Event Entry, you can load the data manually. You also need to load the data manually if you have customized the data files.

Before you load the data, ensure that you have the object types and field groups required by the OpenPages Loss Event Entry profile.

Objects and field groups required for the Loss Event Entry profile

To load the Loss Event Entry profile successfully, you need to make sure you have all of the required object types and field groups loaded in your system.

In the Standard UI, click **Administration > Object Types** and check that all of the following object types are listed.

- LossEvent
- LossImpact
- LossRecovery
- SoxBusEntity
- SoxDocument
- Preference

These object types use the following field groups:

- OPSS-LossEv (LossEvent)
- OPSS-Shared-Basel (LossEvent)
- OPSS-LossIm (LossImpact)
- OPSS-LossRe (LossRecovery)
- OPSS-Pref (Preference)

You can also review the IBM OpenPages Loss Event Entry Automated Form Configuration (AFCON) spreadsheet to make sure that you have everything you need on your system. You can find the AFCON spreadsheet in the <OP_HOME>/LossEventEntry/ directory, along with the other loader files.

Note: This topic discusses the objects and field groups that you need to add if you have the 7.2 solutions schema. If you do not have the 7.2 or later solutions schema or if you customized the solutions schema, additional changes might be required. For more information, see [“Notes for users who do not have the 7.2 or later solutions schema” on page 383](#).

Notes for users who do not have the 7.2 or later solutions schema

If you do not have the 7.2 or later solutions schema in your environment or if you customized the solutions schema, you might need to add or modify objects, field groups, and fields before you use IBM OpenPages Loss Event Entry.

For example, if you installed version 7.1 with solutions and then upgraded to 7.2, your environment has the 7.1 solutions schema. The 7.1 solutions schema might not have all of the objects, field groups, and fields that you need for OpenPages Loss Event Entry.

Examine the OpenPages Loss Event Entry Automated Form Configuration (AFCON) spreadsheet. Look for any gaps:

- Are any objects, field groups, or fields for OpenPages Loss Event Entry missing from your schema?
- Do the attributes match? For example, is the display type of each field defined correctly?
- Does your schema have the prerequisites for the objects, field groups, and fields for OpenPages Loss Event Entry?

You can find the AFCON spreadsheet in the `<OP_HOME>/LossEventEntry/` directory.

Address each gap that you identify. For example, if your schema is missing a field, you could add the field to your schema or you could remove the field from the profile that you use for OpenPages Loss Event Entry. You can make changes by using the OpenPages application or by using the AFCON tool.

Loading the Loss Event Entry data manually

You can load the data used by IBM OpenPages Loss Event Entry manually. For example, if you have customized the data, such as the fields or field groups, you need to load the data manually to apply your changes.

About this task

You can load OpenPages Loss Event Entry data manually by using a script: `Load_LossEvent_Entry_App_Schema.bat` (Windows) or `Load_LossEvent_Entry_App_Schema.sh` (Linux).

The script performs the following actions:

- Adds a new user group, called Loss Event Entry
- Adds users, and adds the new users to the Loss Event Entry user group

The user accounts connect OpenPages Loss Event Entry to IBM OpenPages with Watson. Each user account is associated with a specific locale. When a user starts OpenPages Loss Event Entry, the user is logged in to OpenPages automatically with the user account for their locale.

- LEE_EN_US
- LEE_EN_GB
- LEE_IT_IT
- LEE_PT_BR
- LEE_FR_FR
- LEE_ES_ES
- LEE_DE_DE
- LEE_ZH_TW
- LEE_ZH_CN
- LEE_JA_JP

- Adds a new role template, called Loss Event Entry

The role template controls access to IBM OpenPages with Watson by users of OpenPages Loss Event Entry.

- The role template includes six object types: LossEvent, LossImpact, LossRecovery, SoxBusEntity, SoxDocument, and Preference.
- The role template configures the following security permissions:
 - **Read** access to all six object types
 - **Write** access for LossEvent, LossImpact, LossRecovery and SoxDocument only
 - **Associate** access to SoxBusEntity, LossEvent, LossImpact, LossRecovery and SoxDocument only

- **Delete** access to none of the object types
- No application permissions
- Adds two new field groups and associates them with the LossEvent object.
 - OPSS-LE-BE includes fields to identify the entities involved in the loss event being created
 - OPSS-LE-Contact includes fields for the submitter of the loss event to provide their identifying information
- Adds a new profile, Loss Event Entry.

The profile includes creation views for LossEvent, LossImpact, and LossRecovery. This profile drives the views in OpenPages Loss Event Entry.

- Assigns the Loss Event Entry profile to each of the nine new users
- Assigns the Loss Event Entry role template to each of the nine new users, at the root business entity security context point.

The XML files are located in the directory `<OP_HOME>/LossEventEntry/`. The following list describes the files:

- lossevent-entry-users-op-config.xml (Users and groups)
- lossevent-entry-role-template-op-config.xml (Role templates)
- lossevent-entry-schema-op-config.xml (Schema)
- LEE_object-profile-op-config.xml (Loss Event Entry profile)
- lossevent-entry-config-opx-op-config.xml (JSON configuration file)
- OpenPages-registry-entries-LEE-op-config.xml (Registry setting)
- lossevent-entry-app-string-keys-op-config.xml (Application text)
- lossevent-entry-object-strings-op-config.xml (Object strings)
- locales/<locale>/lossevent-entry-app-strings-<locale>-op-config.xml (Application text translations for each locale)

Procedure

1. Load the OpenPages Loss Event Entry data (users, groups, fields, field groups, and so on).

To load the data on a Microsoft Windows computer, perform the following steps:

- a) Go to `<OP_HOME>\LossEventEntry\`.
- b) Open the `Environment_Variables.bat` file and update the `openpages_domain_folder`, `login_username`, and `login_password` properties.
- c) Run `Load_LossEvent_Entry_App_Schema.bat`.
- d) For security purposes, remove the password from the `Environment_Variables.bat` file.


To load the data on a Linux computer, perform the following steps:

- a) Go to `<OP_HOME>/LossEventEntry/`.
- b) Open the `Environment_Variables.sh` file and update the `openpages_domain_folder`, `login_username`, and `login_password` properties.
- c) Run `Load_LossEvent_Entry_App_Schema.sh`.
- d) For security purposes, remove the password from the `Environment_Variables.sh` file.

2. Optional: Add LossEvent to the list of object types that are disabled for the **Add New** wizard.

OpenPages Loss Event Entry is more full-featured than the **Add New** wizard for loss events. You might want all users, including those that have access to IBM OpenPages with Watson, to use OpenPages Loss Event Entry to report loss events.

- a) In the Standard UI, click **Administration > Settings > GRCM > Add New Wizard**.
- b) Expand **GRCM > Add New Wizard**.

- c) Click **Object Types Disabled**
 - d) In the **Value** field, add the LossEvent object to the list.
 - e) Click **Save**.
3. Optional: Configure autonaming for the LossEvent, LossRecovery, and LossImpact object types. OpenPages Loss Event Entry users are unlikely to know the naming convention for new loss events, loss impacts, and loss recoveries. To avoid failures caused by duplicate names, enable autonaming for these object types.
- a) Click  > **System Configuration > Settings**.
Or, in the Standard UI, click **Administration > Settings**.
 - b) Go to **Applications > GRCM > Auto Naming**.
 - c) Expand the object type, and then expand **Auto-named**. Set **New Object** to true and **Can be Edited** to false.

Chapter 18. IBM OpenPages Third Party Risk Management

IBM OpenPages Third Party Risk Management supports organizations in organizing and centralizing information about their vendors.

As a solution it provides a configurable and customizable platform, allowing firms to:

- Create, maintain, and document all vendors and engagements
- Classify or "tier" vendors as low, medium, or high criticality
- Use standard risk assessments to identify and mitigate risk in a specific way for individual vendors
- Leverage the questionnaire assessment capability to conduct vendor or engagement tiering using information that you gather with risk or compliance questionnaire assessments

In previous releases, IBM OpenPages Third Party Risk Management was named Vendor Risk Management. The original name and the acronym, VRM, still exist in internal names for profiles and role templates.

Installation process overview for IBM OpenPages Third Party Risk Management

If you had a fresh installation of IBM OpenPages with Watson version 7.2 with solutions and then upgraded or migrated to version 7.3.0.1 or later, you need to do some steps to install IBM OpenPages Third Party Risk Management.

Important:

- If you have a fresh installation of 7.4 or later with solutions, you do not need to do these steps. IBM OpenPages Third Party Risk Management is installed when you do a fresh installation of version 7.4 or later with solutions.
- If you upgraded to version 7.4 or later from version 7.3.0.1 or later, you do not need to do these steps.
- If you customized the 7.3 solutions schema, you need to analyze your environment. Determine if any remediation steps are required and complete the remediation work before you install IBM OpenPages Third Party Risk Management.

The IBM OpenPages Third Party Risk Management installation process makes the following updates to your IBM OpenPages with Watson environment:

- Registers the TPRM solution with the IBM OpenPages with Watson application
- Creates TPRM objects
- Creates relationships between TPRM objects and other objects
- Creates default profiles for TPRM
- Creates the role templates for TPRM

Complete these steps to install IBM OpenPages Third Party Risk Management:

1. Upgrade or migrate to IBM OpenPages with Watson version 8.2.
2. Complete the pre-installation tasks for IBM OpenPages Third Party Risk Management. Check system requirements and back up your environment. For more information, see [“Pre-installation tasks for IBM OpenPages Third Party Risk Management” on page 388.](#)
3. Complete the preparation tasks for IBM OpenPages Third Party Risk Management. For more information, see [“Preparing for the installation of IBM OpenPages Third Party Risk Management” on page 388.](#)

4. Run the scripts that load TPRM into your system. For more information, see [“Loading the IBM OpenPages Third Party Risk Management solution”](#) on page 389.
5. Configure the new menu items. For more information, see [“Configuring menu items for IBM OpenPages Third Party Risk Management”](#) on page 390. This step is optional.
6. Complete the installation. For more information, see [“Completing the IBM OpenPages Third Party Risk Management installation”](#) on page 390.

Pre-installation tasks for IBM OpenPages Third Party Risk Management

Before you install IBM OpenPages Third Party Risk Management, back up IBM OpenPages with Watson files, and gather information required to complete the installation.

Ensure that IBM OpenPages with Watson 8.2 or later is installed.

To load the profiles for TPRM, you need to have the approval app schema. Determine if your environment has the approval app schema. If you do not have the approval app, do one of the following:

- Deploy the approval app to load the schema. For more information, see [Chapter 16, “Approval app,”](#) on page 361.
- Use the Automated Form Configuration (AFCON) spreadsheets to update the TPRM (VRM) profiles to remove all references to the fields that are not in your schema. The spreadsheets are in the Profiles subdirectory in the /OP_<version>_Main/OP_<version>_Configuration/Modules/TPRM/OpenPages_TPRM.zip file.

If you want to be able to restore your environment to its current state, back up the OpenPages application environment, the reporting environment, and the database.

Gather the following information. You need this information to complete the installation.

- The user name and password of the OpenPages administrator on the admin application server
- The path of the OpenPages home directory, <OP_HOME>

Preparing for the installation of IBM OpenPages Third Party Risk Management

You must perform some preparation tasks before you install IBM OpenPages Third Party Risk Management.

Procedure

1. Ensure that there are no long running OpenPages processes, such as a FastMap import process or a global search indexing process.
2. Check the status of the OpenPages servers. Verify that the following servers are running: the OpenPages application servers (admin and non-admin), reporting servers (active and standby), the Framework Model Generator, the database server, and the search server (if you use the global search feature).
3. Locate the installation file, OpenPages_TPRM.zip.

The file is in the /OP_<version>_Main/OP_<version>_Configuration/Modules/TPRM directory.

Note: TPRM was previously named IBM OpenPages Vendor Risk Management (VRM). The TPRM profiles and role templates still use "VRM" in their names.

Loading the IBM OpenPages Third Party Risk Management solution

You must load the IBM OpenPages Third Party Risk Management solution to create TPRM objects, relationships, profiles, and role templates.

Before you begin

Complete the tasks that are described in [“Preparing for the installation of IBM OpenPages Third Party Risk Management” on page 388](#) and [“Pre-installation tasks for IBM OpenPages Third Party Risk Management” on page 388](#).

About this task

The TPRM installation kit contains four folders:

Base

Contains scripts that create TPRM objects and relationships. They also register the TPRM solution with the OpenPages application.

Extended

Contains scripts that create relationships between TPRM objects and other objects in the solutions schema.

Profiles

Contains scripts that create three profiles for TPRM: VRM Master Profile, VRM Vendor Profile, VRM Vendor Manager Profile.

RoleTemplates

Contains scripts that create the TPRM (VRM) role template and the sample VRM user.

Note: TPRM was previously named IBM OpenPages Vendor Risk Management (VRM). The TPRM profiles and role templates still use "VRM" in their names.

Procedure

1. Go to the `/OP_<version>_Main/OP_<version>_Configuration/Modules/TPRM` directory on the installation media. Locate the `OpenPages_TPRM.zip` file.

2. Extract the `OpenPages_TPRM.zip` file to a new directory on the admin application server.

You now have the following subdirectories: Base, Extended, Profile, and RoleTemplates.

3. Go to the Base directory.

4. Edit the `Environment_Variables.cmd | .sh` file.

Set the following parameters for your environment:

- Windows: `openpages_domain_folder`, `administrator_username`, and `administrator_password`
- Linux: `openpages_domain_folder`, `login_username`, and `login_password`.

5. If you are using Windows, open a command prompt by using the **Run as administrator** option. Go to the Base directory.

6. Run the loader script.

- On Windows operating systems, run the `Start.cmd` script.

```
Start.cmd
```

- On Linux operating systems, run the `Start.sh` script.

```
./Start.sh
```

7. Verify that the script ran successfully. Check for the message `Done! No errors detected`. If it is not displayed, check the `Schema_Load.log` file for errors.

8. Repeat these steps for the Extended directory.

9. Repeat these steps for the Profiles directory.
10. Repeat these steps for the RoleTemplates directory.
11. Remove the administrator password from the `Environment_Variables.cmd | .sh` file.

Configuring menu items for IBM OpenPages Third Party Risk Management

After you load TPRM, for users with access to the Vendor objects, the **Vendor** menu is displayed at the end of the menu list. You can move the **Vendor** menu to a location of your choosing. This step is optional.

For information, see "Menus: Modify the order of menus" in the *IBM OpenPages with Watson Administrator's Guide*.

Completing the IBM OpenPages Third Party Risk Management installation

Complete the remaining steps to install IBM OpenPages Third Party Risk Management.

Procedure

1. Restart the OpenPages admin application server. For information about starting and stopping servers, see [Chapter 12, "Starting and stopping servers,"](#) on page 309.
2. If you use global search, update the search index.
 - a) Start the search server if it is not already started.
 - b) Log in to OpenPages with an administrative account. Switch to the Standard UI.
 - c) Click **Administration > Global Search** and click **Update**.
3. If you want to report on the fields and field groups for TPRM, regenerate the reporting framework. For more information, see the *IBM OpenPages with Watson Administrator's Guide*.

Do this step after you have completed all other installation tasks. For example, if you want to install other features or apps, regenerate the reporting framework after all of the features and apps are installed.

Results

IBM OpenPages Third Party Risk Management is installed.

Chapter 19. Uninstalling OpenPages with Watson

Use the uninstall process to remove the IBM OpenPages with Watson software.

When you uninstall OpenPages, the uninstall process takes the following actions.

- Removes the OpenPages application.
- Removes IBM WebSphere Liberty for OpenPages.
- Deletes the OP_HOME directory structure, including the WLP_USER_HOME directory.
- Deletes the CC_HOME directory structure.
- Reverts changes to Cognos Analytics that were made for OpenPages.
- Deletes the search directory structures.

For the openpages-storage directory:

- Deletes the openpages-storage directory when Application Server1 is uninstalled, even if openpages-storage is on a network share. If it cannot be deleted, you can delete it manually after the uninstall process is finished.

For databases:

- Deletes the OpenPages data sources and reports from the Cognos Analytics content store.

Uninstalling OpenPages with Watson

Use these steps to uninstall IBM OpenPages with Watson.

Before you begin

Decide whether you need to uninstall OpenPages or roll back to a previous version. If you migrated to 8.2.0.0 and you want to roll back to your previous version, do not do these steps. Instead, see [“Rolling back an OpenPages migration”](#) on page 218.

About this task

This video demonstrates how to uninstall IBM OpenPages with Watson. The video shows 7.4 but the steps are similar for 8.2.

<https://youtu.be/hU979Hice44>

Procedure

1. Stop the OpenPages search server.

You can leave the application servers running or stop them. The reporting server must be running.

2. If you are using Windows, close any command prompts, folders, and files that are accessing the <OP_HOME>, <CC_HOME>, or <SEARCH_HOME> directories.
3. If the OpenPages storage directory is mounted to an application server (Linux), unmount it.
4. Uninstall the OpenPages application. You can either do the following steps or run the silent install with the task value in the `deploy.properties` set to `uninstall`. For more information, see [Appendix A, “Silent installations,”](#) on page 393.
 - a) Open your deployment in the installation app. For more information, see [“Creating a deployment”](#) on page 141.
 - b) Click the task list and select **Uninstall**.
 - c) Click **Validate**.

d) Click **Uninstall**.


e) When the process completes, check the log files for any errors:

```
<install_server_home>/src/deployment/<deployment_name>/logs/nodes/  
<Server>/uninstall.log
```

Where *<Server>* depends on the server and how it is named in the `deploy.properties` files. The error is displayed in the user interface. You can download the log file.

If **Uninstall** is still enabled in the installation app, the uninstall process did not complete.

5. On each remote server:

a) If it is running, stop the agent. Go to the server card and click  or manually stop the agent with the `npm run stop` command.

b) Log on to the remote server.

c) Go to the `<agent_home>/install/<OS_type>` directory.

d) Run the uninstall script.

- Windows

```
uninstall.bat
```

- Linux:

```
./uninstall.sh
```

e) Delete the agent directory.

6. Uninstall the installation server.

a) Log out and close the installation app.

b) Stop the installation server. For more information, see [“Stopping the installation server” on page 53](#).

c) Go to the `<installation_server_home>/install/<OS_type>` directory.

d) Run the uninstall script.

- Windows

```
uninstall.bat
```

- Linux:

```
./uninstall.sh
```

e) Delete the `<installation_server_home>` directory where the installation app was installed, for example, `NewInstaller`.

What to do next

1. Drop the OpenPages database schema objects. For more information, see [“Dropping the OpenPages database for IBM Db2 ” on page 452](#) or [“Dropping the full schema in an Oracle database” on page 453](#).
2. Drop the Cognos Analytics content store schema objects. If you are using IBM Db2, use Db2 utilities to drop the content store. If you are using Oracle, see [“Dropping the Cognos content store \(Oracle\)” on page 454](#).
3. Verify that the `OP_HOME` directory does not exist.
4. Verify that the `CC_HOME` directory does not exist.
5. Verify that the `SEARCH_HOME` directory does not exist.
6. Verify that the `openpages-storage` directory does not exist.
7. You can now reinstall OpenPages.

Appendix A. Silent installations

You run a silent installation from the command line by using inputs that you provide in a deployment configuration file.

Creating a deployment file by using the installation server

You can use the installation server to save a deployment file that you can use to run a silent installation.

Procedure

1. Open Google Chrome or Microsoft Edge.
2. Go to the URL for the installation app.
For example, go to `https://<host>:8443`

Replace `<host>` with the name of the computer where you set up the installation server, and ensure that you use the correct port number. 8443 is the default port number.

For example, `https://appserver1.mycompany.com:8443`

If you are running the installation server on your local computer, go to `https://localhost:8443`

3. Enter your credentials, and click **Login**.
4. Click **Create New**, enter a name for the deployment in **Deployment Name**, and click **Create**.
5. Enter the values for the installation that you want to deploy, and click **Save**.

If you are going to run the installation on a different computer from where you are running the installation app, click the gear icon, and then click **Download Properties**.

The installation server creates a directory for the deployment and a `deploy.properties` file. The deployment directory uses the **Deployment Name** value. The directory is in the `OP_<ver>_Installer/src/deployment` directory where you are running the installation server.

Creating a deployment file manually

You can manually create a deployment file for your silent installation by using one of the template files that are provided with the installation.

Procedure

1. On the computer where you copied the installation files, go the deployment directory.
For example, go to the `/home/opuser/OP_<version>_Installer/src/deployment` directory on Linux operating systems or the `C:\OP_<ver>_Installer\src\deployment` directory on Microsoft Windows operating systems.
2. Create a directory for the deployment that you want to run.
For example, create a directory that is named `myopininstall`. If you used the above path, the full path would be `/home/opuser/OP_<ver>_Installer/src/deployment/myopininstall`

Important: Do not use spaces or special characters in the directory name.

3. Copy the `deploy-unix.properties` or the `deploy-win.properties` file to the directory that you created.
4. Go to the deployment directory, and open the `deploy-unix.properties` or `deploy-win.properties` file in a text editor.
5. Enter the values to use for your deployment, and save the file.

For more information about the properties, see [“Deployment file properties” on page 394](#).

- On Microsoft Windows operating systems, all path properties must use double backslashes. For example, C:\\app\\Administrator\\product\\19.0.0\\client
- If you are using the remote deploy option, `remote_deploy=true`, you must provide values for the following properties:
 - `agent_port` is the port number for the agent to use
 - `agent_directory` is the folder on the remote server where you want to install the agent
 - `local_username` is the user name on the remote server that you want to use to run the installation on the remote server. The user must have administrative privileges on the remote server.
 - `local_password` is the password for the administrative user on the remote server.
 - On Linux operating systems, you must enter the `ssh_port` value for the port number to use on the remote server.

If you are not using the remote deploy option, `remote_deploy=false`, these values are not used.

6. Rename the `deploy-unix.properties` or `deploy-win.properties` file to `deploy.properties`

Deployment file properties

The `deploy.properties` file is used by the silent installation command for a new installation, a file migration, or to upgrade the application data.

You must modify the `task` value in the `deploy.properties` file to indicate a new installation, a file migration, or to upgrade the application data. The rest of the properties in the file stay the same for a new installation, a file migration, or to upgrade the application data.

Table 74. Deployment file properties		
Property	Values	Description
task	fresh upgrade file-migration upgrade-app-data current-deployment uninstall fix-pack	fresh for a new installation upgrade for an in-place upgrade file-migration to migrate from an existing installation upgrade-app-data to upgrade the application data current-deployment to modify an existing environment, such as adding a server uninstall to uninstall an environment fix-pack to install a fix pack, see “Performing a silent installation of a fix pack” on page 306
module	true false	The <code>module</code> value indicates whether to install the IBM OpenPages solutions. For more information, see “Considerations for IBM OpenPages solutions” on page 144 .

Table 74. Deployment file properties (continued)

Property	Values	Description
os	windows linux	The host computer operating system.
remote_deploy	true false	This value determines whether the installation is on a different host than the computer that runs the installation server.
auto_roll_back	true false	This value determines whether the installation will roll back a failed operation.
install_db For more information, see: <ul style="list-style-type: none"> • “Configuring the database server (Db2)” on page 144 • “Configuring the database server (Oracle)” on page 146 	full nondba done	<p>full to install the full database. This option requires DBA credentials.</p> <p>nondba if the DBA installation actions are already complete. The installer will perform the non-DBA installation steps.</p> <p>done if the database installation is already complete.</p> <p>Note: For fix packs, the nondba and done options are equivalent. The database update must be complete before you use these options for a silent fix pack install.</p>
db_type	Oracle DB2	Oracle for an Oracle database DB2 for an IBM Db2 database.

Table 74. Deployment file properties (continued)

Property	Values	Description
java_home_directory	The absolute path to JAVA_HOME on the server	<p>For application servers, use the path to the IBM SDK.</p> <p>For reporting servers, use the path to the IBM Java JRE that is supplied with Cognos or the Java that you configured for Cognos.</p> <p>For each server, the path that you enter must match the path specified in the JAVA_HOME system environment variable on the server.</p> <p>If the reporting server is deployed on the same server as an application server, do the following:</p> <ul style="list-style-type: none"> • On the server, set JAVA_HOME to the JRE of the IBM SDK. • For the java_home_directory property in the [report server1] section, use the same path as you specified for JAVA_HOME.

Modifying the migration properties file

If you are migrating any files from an existing OpenPages environment, you can do so by using the silent installation commands. You must edit the migration.properties file that is provided with the installation files.

Procedure

1. On the computer where you copied the installation files, go the deployment directory.
For example, go to the /home/opuser/OP_<ver>_Installer/src/deployment directory on Linux operating systems or the C:\OP_<ver>_Installer\src\deployment directory on Microsoft Windows operating systems.
2. Copy the migration.properties file to the directory where you saved the deploy.properties file.

For more information about the location, see [“Creating a deployment file manually”](#) on page 393.
3. Go to the directory, and open the migration.properties file in a text editor.
4. Edit the values to match your existing OpenPages environment.
5. Save and close the file.

Running the silent installation commands

After you create the deployment properties file, you can run the silent installation from the command line.

You use the silent installation command for:

- A fresh installation, where task = fresh in the deploy.properties file.

- A in-place upgrade, where `task = upgrade` in the `deploy.properties` file. For more information, see *IBM OpenPages with Watson Upgrade Guide for IBM Db2* or *IBM OpenPages with Watson Upgrade Guide for Oracle*.
- A back up and restore task to migrate from your existing OpenPages deployment to 8.2. The `deploy.properties` must have `task = file-migration`, and you must configure the `migration.properties` file. The `file-migration` task also performs the `upgrade-app-data` task.
- An application data upgrade task, where `task = upgrade-app-data` in the `deploy.properties` file.

If you are migrating from an existing installation, you must follow this process:

1. Run a fresh install of OpenPages.

The `task` value in the `deploy.properties` file is set to `fresh`:

```
task = fresh
```

2. Upgrade the database. For more information, see

- [Chapter 8, “Migration task reference for Db2 databases,” on page 219](#)
- [Chapter 9, “Migration task reference for Oracle databases,” on page 241](#)

3. Do one of the following:

- Run a file migration to backup and restore any files to the new installation.

The `task` value in the `deploy.properties` file is set to `file-migration`:

```
task = file-migration
```

You must also edit the `migration.properties` file to match your existing environment. (The OpenPages environment that you are migrating from.)

The `file-migration` task will also perform the `upgrade-app-data` task.

- If you do not want to do a backup/restore, you must run the upgrade application data task.

The `task` value in the `deploy.properties` file is set to `upgrade-app-data`:

```
task = upgrade-app-data
```

For more information, see [“Upgrading application data” on page 205](#).

For more information about migration upgrades, see [“Migration overview” on page 189](#).

Procedure

1. On the computer where you copied the installation files, go to the `OP_<ver>_Installer` directory.
2. Ensure you have the correct value for the `task` that you want to run set in the `deploy.properties` file.
3. Run the following command:

```
npm run silent <deployment_name> acceptLicense
```

Where `<deployment_name>` is the name for the deployment that you used in the installation app and the deployment folder that you created in the `OP_<ver>_Installer/src/deployment` directory.

Note: Do not close the command prompt or shell window until after the process completes.

Appendix B. Install OpenPages by using Docker

You can use Docker to install IBM OpenPages with Watson. Use Docker to quickly install a small environment for testing or demonstration purposes.

For information about Docker technology, see www.docker.com.

You can install all of the OpenPages components on one computer, or you can separate the database components from the application components.

After you install OpenPages, review the postinstallation tasks to see if any of them apply to you. See [“Post installation tasks” on page 153](#).

Installing Docker

You must install Docker. If you are installing Docker on a Linux operating system, you must also install Docker Compose.

Before you begin

Ensure that you have a minimum of 16 GB of RAM.

Ensure that you have 100 GB of free disk space on the computer on which you install Docker. On Linux operating systems, the 100 GB of free disk space must be on the disk or partition that contains the Docker data directory, by default `/var/lib/docker`. Or, configure Docker to use a different directory on a disk or partition that has 100 GB of free space.

On Linux operating systems, the Linux kernel 3.10 or later is required.

On Linux operating systems, you must also enable the extras repositories. For example,

- On Red Hat Enterprise Linux operating systems, use the following command to enable the extra RHEL repositories:

```
sudo yum-config-manager --enable rhel-7-server-extras-rpms
```

- On CentOS, use the following command:

```
sudo yum-config-manager --enable extras
```

If you are going to run IBM OpenPages with Watson in a distributed environment, you must install Docker on two computers.

About this task

OpenPages supports the following Docker software versions:

- Docker Engine for Linux: 18.09.2
- Docker Desktop for Windows: 2.0.0.3
- Docker Toolbox for Windows: 18.09.2
- Docker Desktop for Mac: 2.0.0.3

Procedure

1. Install Docker.

For more information about installing Docker, see the product documentation:

- For Linux operating systems, see [Get Docker CE for CentOS](https://docs.docker.com/engine/installation/linux/docker-ce/centos/) (<https://docs.docker.com/engine/installation/linux/docker-ce/centos/>).

- For Microsoft Windows operating systems, see [Install Docker for Windows](https://docs.docker.com/docker-for-windows/install/) (https://docs.docker.com/docker-for-windows/install/).

For some versions of Microsoft Windows, you might have to install Docker Toolbox. For more information, see [Install Docker Toolbox on Windows](https://docs.docker.com/toolbox/toolbox_install_windows/) (https://docs.docker.com/toolbox/toolbox_install_windows/).

- For macOS operating systems, see [Install Docker for Mac](https://docs.docker.com/docker-for-mac/install/) (https://docs.docker.com/docker-for-mac/install/).

2. If you are installing on Linux operating systems, do the following steps:

- a) Create a Docker group and add your user name to the group to allow for easier installation. For more information, see [Manage Docker as a non-root user](https://docs.docker.com/engine/installation/linux/linux-postinstall/) (https://docs.docker.com/engine/installation/linux/linux-postinstall/).
- b) Configure Docker to start when the computer starts up. For more information, see [Configure Docker to start on boot](https://docs.docker.com/engine/installation/linux/linux-postinstall/) (https://docs.docker.com/engine/installation/linux/linux-postinstall/).

- c) Configure the image size limit for Docker.

If your Docker installation uses the `devicemapper` storage driver, configure Docker to increase the base device size (the default is 10 GB, and one of the OpenPages Docker images is larger than that). Do this step before you download any images to your host.

Check if Docker is using `devicemapper`:

```
docker info | grep "Storage Driver"
```

If the result is `Storage Driver: devicemapper`, do the following steps:

- i) Create a file `/etc/docker/daemon.json` with the following content:

```
$ sudo tee /etc/docker/daemon.json <<-EOF
{
  "storage-driver": "devicemapper",
  "storage-opts": ["dm.basesize=50G"]
}
EOF
```

If the `daemon.json` file already exists, edit it to include the lines in curly braces.

- ii) Stop the Docker Engine, flush the changes, clean up local containers and images, and then restart Docker.

```
sudo systemctl stop docker
sudo systemctl daemon-reload
sudo rm -rf /var/lib/docker
sudo systemctl start docker
```

- d) Install Docker Compose. For more information, see [Install Docker Compose](https://docs.docker.com/compose/install/) (https://docs.docker.com/compose/install/).

3. On Microsoft Windows or macOS operating systems, you must configure resource allocations.

Microsoft Windows

- a. Right-click the Docker icon on the Windows Taskbar, and click **Settings**.
- b. On the **Advanced** tab, allocate at least 4 CPUs, 16 GB for memory, and 100 GB for the disk image.
- c. Click **Apply**.

macOS

- a. Click the Docker icon on the Menu bar, and click **Preferences**.
- b. On the **Advanced** tab, allocate at least 4 CPUs, 16 GB for memory, and 100 GB for the disk image.

4. On Microsoft Windows operating systems, set Docker to use Linux containers.

For more information, see [Switch between Windows and Linux containers](#).

5. If you are using Docker Toolbox on Microsoft Windows, you must create the Docker machine that is suitable to install OpenPages into.

- a) Open the Docker Quickstart Terminal.
- b) Run the following command to remove the default machine:

```
docker-machine rm -f default
```

- c) Run the following command to create a machine that is suitable for OpenPages:

```
docker-machine create --driver virtualbox --virtualbox-disk-size "100000"
--virtualbox-cpu-count "4" --virtualbox-memory "12288" default
```

- d) Run the following command and record the machine IP address. You must use the IP address to access the OpenPages URL.

```
docker-machine ip
```

- e) Stop the Docker machine:

```
docker-machine stop
```

- f) Start the Docker machine:

```
docker-machine start
```

- g) If you encounter performance issues, do the following steps:

- i) Stop the Docker machine: `docker-machine stop`

- ii) Open the Virtual Box application. Click the default VM that was created by Docker Toolbox. Click **Virtual Box > default > Settings > Network > Adapter 1 > Advanced**. Change the adapter type to **PCnet-Fast III (Am79C973)**.

- iii) Restart the docker machine: `docker-machine start`

Installing OpenPages on a single server by using Docker

After you install Docker, you can load and then start the OpenPages application.

About this task

This video demonstrates how to install OpenPages on a single server using Docker:

<https://youtu.be/zKJWCtTyYhA>

Procedure

1. On the computer where you installed Docker, create a directory for the files.
For example, create a directory that is named `OPDocker`.
2. If you are installing OpenPages on a single computer, copy the following downloaded files to the directory that you created:

- `op<version>.tar.gz`
- `.env`
- `docker-compose.yml`

Tip: Check the `.env` file name. On Microsoft Windows operating systems, the leading dot might be removed when you download the file.

3. In a terminal window, go to the directory where you copied the files, and run the following command to load the Docker containers:

```
docker load -i op<version>.tar.gz
```

The command can take some time to run as it loads all of the software and the database content.

You might get an error like this: `ApplyLayer exit status 1 stdout: stderr: write <some file>: no space left on device.`

If you get this error but your host still has sufficient disk space, do step 2c in [“Installing Docker”](#) on page 399, and then reload the Docker images from the `op<version>.tar.gz` file.

4. Ensure that the **HOSTNAME** variable is set to the fully qualified domain name (FQDN) of the computer where you are installing the Docker containers.

Microsoft Windows operating systems

In a PowerShell terminal, run the following command: `echo $env:HOSTNAME`

Linux operating systems

In a terminal window, run the following command: `echo $HOSTNAME`

If the value is not set, you can set it in the terminal window or add it to the `.env` file that you copied with the `op<version>.tar.gz` and `docker-compose.yml` files.

5. Open the `.env` file, and ensure that the **OPVER** variable value matches the version of OpenPages that you are installing.

Tip: You can set the timezone for the Docker container by editing the `.env` file. The default timezone is Eastern Time (UTC-5:00).

6. On all operating systems, run the following command:

```
docker-compose up -d
```

Starting the application can take some time. Wait at least 10 minutes before you can access the application.

After the application starts, you can access it at `https://<hostname>:10111/`

For information about the log in credentials, see the `cheatsheet_deployment_info.txt` text file that is provided with the installation files.

What to do next

- When you access OpenPages for the first time, you get a security warning about the HTTPS connection. Go to the advanced options in your browser and accept the exception.
- The Cognos embedded reports might not work initially due to the same security warning. Click **Cognos Analytics** and accept the security exception. Reload the embedded report.

Installing OpenPages in a distributed environment by using Docker

After you install Docker, you can load and then start the OpenPages application. In a distributed environment, you use two Docker instances. One instance runs the database container and the other runs the application containers.

Before you begin

Install Docker. For more information, see [“Installing Docker”](#) on page 399.

For access by a single user, ensure that you have a minimum of 12 GB or higher RAM on both Host A and Host B. For access by multiple users, the minimum is 24 GB or higher RAM for Host A and Host B.

About this task

Do the steps in this task to set up two containers:

- Host A: Runs the Dockers instances `opdb` (the database for OpenPages) and `opreportdb` (the database for cognos)
- Host B: Runs the Dockers instances `opapp` (OpenPages application server), `opreport` (cognos report server), and `opsearch` (OpenPages global search server)

Note: For information about how to use a database outside of a Docker container while running OpenPages in Docker containers, see "Scenario 2" in the `cheatsheet_separate_db_host.txt` file.

100GB free disk space

Procedure

1. On the Docker instance where you run the database container (Host A), do the following steps:

- a) Copy the following downloaded files to the directory:

- `op<version>.tar.gz`
- `db.env`
- `dc-db-db2.yml`

- b) In a terminal window, go to the directory where you copied the files, and run the following command:

```
docker load -i op<version>.tar.gz
```

The command can take some time to run as it loads all of the software and the database content.

2. On the Docker instance where you run the application containers (Host B), do the following steps:

- a) Copy the following downloaded files to the directory:

- `op<version>.tar.gz`
- `app.env`
- `dc-app-db2.yml`

- b) In a terminal window, go to the directory where you copied the files, and run the following command to load the Docker containers:

```
docker load -i op<version>.tar.gz
```

The command can take some time to run as it loads all of the software and the database content.

You might get an error like this: `ApplyLayer exit status 1 stdout: stderr: write <some file>: no space left on device.`

If you get this error but your host still has sufficient disk space, do step 2c in [“Installing Docker” on page 399](#), and then reload the Docker images from the `op<version>.tar.gz` file.

3. On all operating systems, on the Docker instance where you run the database container (Host A), do the following steps:

- a) Rename `db.env` to `.env`.

- b) Ensure that the **OPVER** variable value in the `.env` file matches the version of OpenPages that you are installing.

Tip: You can set the timezone for the Docker container by editing the `.env` file. The default timezone is Eastern Time (UTC-5:00). The timezone must be the same on Host A and Host B.

- c) Run the following command:

```
docker-compose -f dc-db-db2.yml up -d
```

4. On all operating systems, on the Docker instance where you run the application container, do the following steps:

- a) Rename `app.env` to `.env`.

- b) Open the `.env` file in a text editor.

- c) Change the **OPDB_HOST** and **OPREPORTDB_HOST** values to the fully qualified domain name or IP address of the computer where the database container is running.

- d) Ensure that the **OPVER** variable value in the `.env` file matches the version of OpenPages that you are installing.

Tip: You can set the timezone for the Docker container by editing the `.env` file. The default timezone is Eastern Time (UTC-5:00). The timezone must be the same on Host A and Host B.

- e) Ensure that the **HOSTNAME** variable is set to the fully qualified domain name (FQDN) of the computer where the application server container (Host B) is running.

Microsoft Windows operating systems

In a PowerShell terminal, run the following command: `echo $env:HOSTNAME`

Linux operating systems

In a terminal window, run the following command: `echo $HOSTNAME`

If the value is not set, you can set it in the terminal window or add it to the `.env` file.

- f) Save and close the file.

- g) Run the following command:

```
docker-compose -f dc-app-db2.yml up -d
```

Starting the application can take some time. Wait at least 10 minutes before you can access the application.

After the application starts, you can access it at `https://`

`<hostname_for_application_server>:10111/`

`<hostname_for_application_server>` is the computer where you installed the application server container (Host B). The `<hostname_for_application_server>` is the value that you specified for the **HOSTNAME** in step 4e.

For information about the log in credentials, see the `cheatsheet_deployment_info.txt` text file that is provided with the installation files.

Installing only the OpenPages applications by using Docker

If you already have an IBM Db2 instance, you can restore the OpenPages and Cognos databases to your Db2 instance, and then install the OpenPages applications by using Docker.

Procedure

1. Load the OpenPages Docker containers.

- a) On Microsoft Windows operating systems, ensure that the **HOSTNAME** variable is set on both Docker instances.

In a PowerShell terminal, run the following command:

```
echo $env:HOSTNAME
```

If the value is not set, you can set it in the terminal window or to the `.env` file that you use in step 4 below.

- b) On all operating systems, on the Docker instance where you want to run the application containers, copy the following downloaded files to the directory:

- `op<version>.tar.gz`
- `app.env`
- `dc-app-db2.yml`

- c) On all operating systems, in a terminal window, go to the directory where you copied the files, and run the following command:

```
docker load -i op<version>.tar.gz
```

The command can take some time to run as it loads all of the software and the database content.

2. Create a backup of the OpenPages and Cognos databases from the Docker container.

- a) Run the following command to create a backup of the OpenPages database to a `/tmp` directory:

```
docker run --rm -v /tmp:/tmp ip-op-gic-docker-local.artifactory.swg-devops.com/op/
opdbdata_db2:<opversion> sh -c 'cp /home/db2inst1/backup/*.gz /tmp/'
```

- b) Run the following command to create a backup of the Cognos database to a /tmp directory:

```
docker run --rm -v /tmp:/tmp ip-op-gic-docker-local.artifactory.swg-devops.com/op/
opreportdbdata_db2:<opversion> sh -c 'cp /home/db2inst1/backup/*.gz /tmp/'
```

3. Restore the databases to your Db2 instance.

- a) Copy the two *.gz files to the computer where Db2 is installed.

- b) Run the following command to restore the databases:

```
db2 restore database <database alias> from <backup directory>
```

You must run the command for the OpenPages database and the Cognos database. Ensure that the Db2 database instance that you restore the OpenPages database to has Oracle compatibility enabled.

4. Start the OpenPages application servers.

- a) On the computer where you copied the downloaded files, rename app.env to .env.

- b) Open the .env file in a text editor.

- c) Change the **OPDB_*** values to the database connection parameters for the OpenPages database.

- d) Change the **OPREPORTDB_*** values to the database connection parameters for the Cognos database.

- e) Ensure that the **OPVER** variable value in the .env file matches the version of OpenPages that you are installing.

- f) Save and close the file.

- g) Run the following command:

```
docker-compose -f dc-app-db2.yml up -d
```

Starting the application can take some time. Wait at least 10 minutes before you can access the application.

After the application starts, you can access it at `https://<hostname_for_application_server>:10111/`

`<hostname_for_application_server>` is the computer where you installed the application server container.

For information about the log in credentials, see the `cheatsheet_deployment_info.txt` text file that is provided with the installation files.

Note: The Cognos data source signon credentials are not updated by the container startup. You must manually update the signon credentials after the Cognos server starts. For more information, see [Modifying a signon in the Cognos documentation](#).

Accessing the applications

The application URLs and credential information for OpenPages and Cognos installations from Docker are provided in the `cheatsheet_deployment_info.txt` file that is provided with the installation source files.

Stopping and starting OpenPages services deployed to Docker and other tasks

You stop and start the OpenPages application services by using `docker-compose` commands, and you can perform additional tasks by using Docker commands.

Procedure

1. To stop the OpenPages application, run the following command in a terminal window:

```
docker-compose stop
```

2. To start the OpenPages application, run the following command in a terminal window:

```
docker-compose start
```

3. You can use the following commands to check the status of the OpenPages containers:

- Use the following command to list all of the active containers, the original images of containers, and the start-up command configurations:

```
docker ps
```

- Use the following command to list all of the active containers and the stopped containers:

```
docker ps -a
```

If a container is stopped that should be active, you can restart it by running the following command:

```
docker-compose start <container_name>
```

- Use the following command to show the CPU, memory, and I/O usage for the containers:

```
docker stats
```

- Use the following command to show the console output for the container:

```
docker logs <container_name>
```

- Use the following command to run commands on the container:

```
docker exec <container_name> <command>
```

For example, you can access the container by using the following command:

```
docker exec -it <container_name> /bin/bash
```

- Use the following command to access the bash terminal for a container:

```
ssh -l <user> -p <port> <localhost | docker_host_IP>
```

For the credential and port information, see the `cheatsheet_deployment_info.txt` file that is provided with the installation source files.

4. Some additional tasks are documented in the `cheatsheet_misc_operations.txt` file that is provided with the installation source files.

For example, migrating data into containers, taking a backup, persisting your customizations as your own images, and transferring a deployment from one system to another.

Uninstalling OpenPages from Docker

You can uninstall the OpenPages containers and also free up the disk space that is allocated to the contains by using Docker commands.

Procedure

1. Use the following command to stop and remove the OpenPages containers:

```
docker-compose down -v
```

2. Use the following command to remove the images to free up disk space:

```
docker rmi -f $(docker images -q)
```

Appendix C. Additional tasks

After you install IBM OpenPages with Watson, you can do some additional tasks.

Adding servers to an OpenPages with Watson deployment

You can add non-admin application servers and standby reporting servers to your IBM OpenPages with Watson deployment.

This video demonstrates how to add servers to a deployment. You can add non-admin application servers and standby reporting servers to create or expand a horizontal cluster. You can also add vertical cluster members to an application server. The video shows 7.4 but the steps are similar for 8.2.

<https://youtu.be/hn7bYmvrTrQ>

Adding servers to a deployment (horizontal cluster members)

You can add servers to a IBM OpenPages with Watson deployment. You can add non-admin application servers and standby reporting servers to increase the number of horizontal cluster members.

Before you begin

Review the following checklist before you add servers to your installation:

- Ensure that the installation server is updated to the latest version. For more information, see the *IBM OpenPages with Watson Installation and Deployment Guide*. The latest version is available in the OpenPages fix pack kit.
- Ensure that the installation server can communicate with all of the servers in your deployment, including the servers that you want to add.
- Ensure that the servers you want to add can access the `openpages-storage` directory.
- Prepare the servers that you want to add to your deployment. For more information, see the following topics in the *IBM OpenPages with Watson Installation and Deployment Guide*
 - [“Checklist for Windows servers” on page 59](#)
 - [“Checklist for Linux servers” on page 60](#)

On the server that you are adding, configure the same file system user names and passwords that you are using for the other servers in your deployment. Also, use the same file share permissions on all servers.

- [“Checklist for application servers” on page 64](#)
- [“Checklist for reporting servers” on page 110](#)
- For application servers, ensure that the same version of IBM SDK, Java Technology Edition is installed on each server.

Procedure

1. Verify the status of the servers in your deployment. All servers must be running, except for the search server, which must be stopped.
See [Chapter 12, “Starting and stopping servers,” on page 309](#).
2. Start the installation app and log in.
3. Open your deployment.
4. Do one of the following steps on the server that you want to add:
 - Update the antivirus policy on the remote server to allow `Node.js`.

- Disable antivirus software on the remote server. You can re-enable it after you complete the installation of the new servers.
5. Add a new horizontal cluster member:
 - a) Click the server list and click the type of server that you want to add.
 - Click **Application Server** to add a non-admin application server horizontal cluster member.
 - Click **Reporting Server** to add a standby reporting server horizontal cluster member.

A new server card is added to your deployment.
 - b) Enter values for the server.

If you are adding application servers, you must enter unique names in the **OP Server Name** field.

If you are adding reporting servers, you must configure additional Cognos dispatchers to ensure that the incoming requests are distributed across the reporting servers.

For more information, see the *IBM OpenPages with Watson Installation and Deployment Guide*.
 6. Click **Validate** to save and validate the deployment.

During the validation process, the installation app installs the agent software on the remote servers, starts the agents, validates the deployment properties, and verifies that the prerequisites for the installation are complete.

For example, the following image shows an application server card after validation is complete. The **Agent On** icon is green, indicating that the agent is installed and running on the remote server.

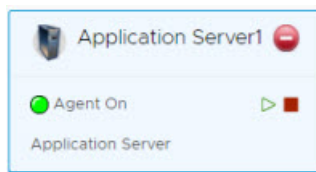


Figure 18. Agent software is running on Application Server1

You can download a validation report. Click the link at the top of the page.

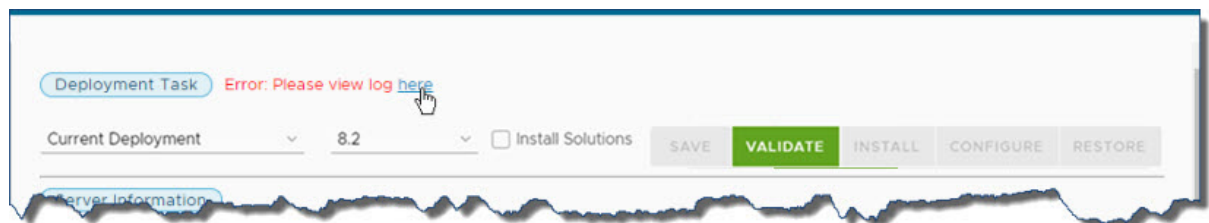


Figure 19. Click to download a validation report

The validation reports are also stored in the `<installation_server_home>/src/deployment/<deployment-name>/validation` directory.

Fix any errors and review the warnings. Click **Save**, and then click **Validate**. When the **Install** button is available, you can continue. If fixing issues requires an update to the environment variables on any servers, you must restart the installation server/agent on that server before re-validating.

7. Click **Install**.

The installation server stages the assets onto the new servers in your deployment.

Tip: You can log out and close the browser window. The **Install** process continues to run. When you log in to the installation app again, the app shows the status of your deployment. You can also close the browser window during the **Configure** process.

8. Click **Configure**.

The installation server sets up and configures the IBM OpenPages with Watson components.

9. Start the search server.

The installation server restarts the other servers in your deployment automatically.

10. Do the post installation tasks.

If you added a non-admin application server, do the following tasks:

- If the server is running on Windows, configure the OpenPages services to run under a domain account. See [“Configuring OpenPages applications to use a domain account on Windows operating systems”](#) on page 159.
- If the server is running on Linux, configure file share permissions. See [“Configuring file share permissions on Linux operating systems”](#) on page 159.
- Configure the load balancer. See [“Configuring IBM HTTP Server to balance the load on application servers”](#) on page 164.
- Verify that you have shared the `openpages-storage` directory so that the non-admin application server can access it. See [“Sharing a network OpenPages storage directory on Linux operating systems”](#) on page 159 or [“Sharing a network OpenPages storage directory on Windows operating systems”](#) on page 161.

If you added a standby reporting server, do the following tasks:

- Configure the load balancer. See [“Load balancing the reporting server”](#) on page 170.

Results

When the installation is complete, ensure that you can log in to OpenPages and complete tasks such as creating or updating objects, and running reports.

Adding non-admin application servers to a deployment (vertical cluster members)

You can add non-admin application servers to a IBM OpenPages with Watson deployment by increasing the number of vertical cluster application servers.

Before you begin

Review the following checklist before you add servers to your installation:

- Ensure that the installation server is updated to the latest version. For more information, see the *IBM OpenPages with Watson Installation and Deployment Guide*. The latest version is available in the OpenPages fix pack kit.
- Ensure that the installation server can communicate with all of the servers in your deployment.

Procedure

1. Decide which application server you want to modify. Ensure that the server has sufficient hardware resources to support vertical cluster members.

Open the [Software Product Compatibility Report](#) report for OpenPages. Click the **Hardware** tab. Review the detailed system requirements for application servers.

2. Verify the status of the servers in your deployment. All servers must be running, except for the search server, which must be stopped.

See [Chapter 12, “Starting and stopping servers,”](#) on page 309.

3. Start the installation app and log in.
4. Open your deployment.
5. Click the **Application Server** card of the server you want to modify.
6. Add vertical cluster members by increasing the value in the **OP Vertical Cluster Number** field.

Note: Do not decrease the number of vertical cluster members. A decrease in the value can cause validation errors.

7. Click **Validate** to save and validate the deployment.

You can download a validation report. Click the link at the top of the page.

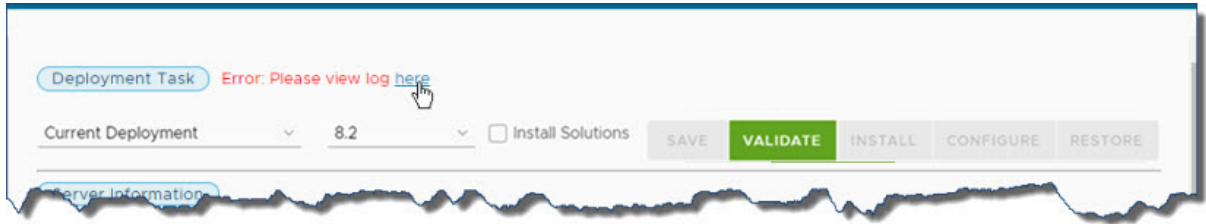


Figure 20. Click to download a validation report

The validation reports are also stored in the `<installation_server_home>/src/deployment/<deployment-name>/validation` directory.

Fix any errors and review the warnings. Click **Save**, and then click **Validate**. When the **Install** button is available, you can continue. If fixing issues requires an update to the environment variables on any servers, you must restart the installation server/agent on that server before re-validating.

8. Click **Install**.

The installation server stages the assets onto the new servers in your deployment.

Tip: You can log out and close the browser window. The **Install** process continues to run. When you log in to the installation app again, the app shows the status of your deployment. You can also close the browser window during the **Configure** process.

9. Click **Configure**.

The installation server sets up and configures the IBM OpenPages with Watson components.

10. Start the search server.

The installation server restarts the other servers in your deployment automatically.

Results

When the installation is complete, ensure that you can log in to OpenPages and complete tasks such as creating or updating objects, and running reports.

What to do next

Update the load balancer with information for the new non-admin application server. See [“Configuring IBM HTTP Server to balance the load on application servers”](#) on page 164.

Backing up the OpenPages database (Db2)

Create a backup of the OpenPages with Watson database.

Before you begin

If Db2 Text Search is enabled in your source environment, drop the text search indexes and disable Db2 Text Search before you back up the database.

About this task

Use this procedure if your OpenPages database is at version 7.4.x or later. If you are backing up a 7.3 database, see the *IBM OpenPages with Watson Installation and Deployment Guide*.

Use the utilities that are provided with IBM Db2 to back up the database.

Note: You can back up the database by using other methods. For example, you can use a combination of full and incremental backups. If you want to use an alternative method, it is critical that you have the necessary skills available within your organization to complete all aspects of the backup and restore activity.

For information about developing a database backup and restore strategy, see [Backup overview](#) in the Db2 documentation.

For more information about the commands that are used in this procedure, see the [IBM Db2 documentation](#).

Procedure

1. Make sure that no OpenPages with Watson processes are running, such as object reset jobs.
2. Shut down all OpenPages components: application servers (admin and non-admin), reporting servers (active and standby), and the search server.

For more information, see the *IBM OpenPages with Watson Installation and Deployment Guide*.

3. Open a command or shell window and connect to the OpenPages database as the database instance owner.

For Windows users only, you must use the **db2cmd** command in the **Command Prompt** window to initialize the Db2 command line processor (CLP).

4. Go to the `sqllib` directory.
5. Force any applications from the database.

Run the following command:

```
db2 force application all
```

6. Deactivate the database.

Run the following command:

```
db2 deactivate database <db_name>
```

7. Create a directory in which to store the backup.
8. Do an offline backup by using the `db2 backup` command.

```
db2 backup database <db_name> to <backup_directory>
```

Example:

```
db2 backup database opx to /home/db2inst1/backup
```

Backing up the Cognos database (Db2)

Create a backup of the Cognos database. Do this procedure if you use a separate database for Cognos.

About this task

Use the utilities that are provided with IBM Db2 to back up the database.

Note: You can back up the database by using other methods. For example, you can use a combination of full and incremental backups. If you want to use an alternative method, it is critical that you have the necessary skills available within your organization to complete all aspects of the backup and restore activity.

For information about developing a database backup and restore strategy, see [Backup overview](#) in the Db2 documentation.

For more information about the commands that are used in this procedure, see the [IBM Db2 documentation](#).

Procedure

1. Shut down all OpenPages components: application servers (admin and non-admin), reporting servers (active and standby), and the search server.

For more information, see the *IBM OpenPages with Watson Installation and Deployment Guide*.

2. Ensure that all Cognos components are shut down.
3. Open a command or shell window and connect to the Cognos database as the database instance owner.

For Windows users only, you must use the **db2cmd** command in the **Command Prompt** window to initialize the Db2 command line processor (CLP).

4. Go to the `sqllib` directory.
5. Force any applications from the database.

Run the following command:

```
db2 force application all
```

6. Deactivate the database.

Run the following command:

```
db2 deactivate database <db_name>
```

7. Create a directory in which to store the backup.
8. Do an offline backup by using the `db2 backup` command.

```
db2 backup database <db_name> to <backup_directory>
```

Example:

```
db2 backup database cognosdb to /home/db2inst2/backup
```

Backing up the OpenPages database (Oracle)

Run the OPBackup utility to back up the IBM OpenPages with Watson database.

About this task

Use this procedure if your OpenPages database is at version 7.4.x or later. If you are backing up a 7.3 database, see the *IBM OpenPages with Watson Installation and Deployment Guide*.

Run the OPBackup utility with the `dbonly` parameter.

Note:

You can back up the databases by using other methods. Some examples of alternative methods include:

- Doing a full physical backup by using RMAN
- Doing a combination of full and incremental backup by using RMAN
- Doing an Oracle data pump export.

If you want to use an alternative method, it is critical that you have the necessary skills available within your organization to complete all aspects of the backup and restore activity.

For more information about backing up your environment, see the *IBM OpenPages with Watson Administrator's Guide*.

Procedure

1. Make sure that no OpenPages with Watson processes are running, such as object reset jobs.

2. Shut down all OpenPages components: application servers (admin and non-admin), reporting servers (active and standby), and the search server.

For more information, see the *IBM OpenPages with Watson Installation and Deployment Guide*.

3. Open a command or shell window on the admin application server.
4. Go to the `<OP_HOME>/aurora/bin` directory.
5. Do a full database backup of the OpenPages schema by using OPBackup.

Windows:

```
OPBackup.cmd <backup_directory> dbonly
```

Linux:

```
./OPBackup.sh <backup_directory> dbonly
```

The `<backup_directory>` is the full path to a directory on the database server. This directory is where the log files are saved. If the file path is not specified, the OPBackup command uses the location that is specified by the **BACKUP_LOCATION** parameter in the `<OP_HOME>/aurora/bin/op-backup-restore.env` file.

A dump file is created in the `OP_DATAPUMP_DIRECTORY` directory.

To find the `OP_DATAPUMP_DIRECTORY` directory, run the following SQL as the system user:

```
select directory_name, directory_path from dba_directories
where directory_name = upper ('OP_DATAPUMP_DIRECTORY');
```

6. Examine the backup log and make note of the dump file name. The naming convention is `openpage_<timestamp>.dmp`.

Backing up the Cognos content store (Oracle)

You can use OPCCBackup to back up the Cognos content store.

About this task

Run the OPCCBackup utility with the `dbonly` parameter.

Note: You can back up the content store by using other methods. Some examples of alternative methods include:

- Doing a full physical backup by using RMAN
- Doing a combination of full and incremental backup by using RMAN
- Doing an Oracle data pump export.

If you want to use an alternative method, it is critical that you have the necessary skills available within your organization to complete all aspects of the backup and restore activity.

For more information about backing up your environment, see the *IBM OpenPages with Watson Administrator's Guide*.

Procedure

1. Make sure that no OpenPages with Watson processes are running, such as object reset jobs.
2. Shut down all OpenPages components: application servers (admin and non-admin), reporting servers (active and standby), and the search server.

For more information, see the *IBM OpenPages with Watson Installation and Deployment Guide*.

3. Ensure that all Cognos components are shut down.
4. Open a command or shell window on the admin application server in your source environment.
5. Go to the `<OP_HOME>/CommandCenter/tools/bin` directory.

6. Do a full database backup of the Cognos schema by using OPCCBackup.

Windows:

```
OPCCBackup.cmd <backup_directory> dbonly
```

Linux:

```
./OPCCBackup.sh <backup_directory> dbonly
```

The *<backup_directory>* is the full path to a directory on the database server. This directory is where the log files are saved. If the file path is not specified, the OPCCBackup command uses the location that is specified by the **OP_CC_BACKUP_HOME** parameter in the *<CC_HOME>/tools/bin/op-cc-backup-restore.env* file.

A dump file is created in the OP_DATAPUMP_DIRECTORY directory. The file is called *openpage_cc_<timestamp>.dmp*.

To find the OP_DATAPUMP_DIRECTORY directory, run the following SQL as the system user:

```
select directory_name, directory_path from dba_directories
where directory_name = upper ('OP_DATAPUMP_DIRECTORY');
```

If you get the warning *tools.jar file is not found*, see the following [technote](#).

Updating host names

If the host name of one of the servers in your IBM OpenPages with Watson deployment changes after you install OpenPages, you need to update your configuration with the new host name.

Depending on which server in the deployment changed, follow the steps in one or more of the following documents:

- If the host name of your database server changed, follow the steps in [How to Change the Hostname of an IBM DB2 Database Server for OpenPages](#) or [How to Change the Hostname of an Oracle Database Server for OpenPages](#).
- If the host name of one of your OpenPages application servers, the load balancer for your application servers, or the server that hosts the OpenPages storage directory changed, or if the OpenPages application URL changed, follow the steps in [How to Change the Hostname, URL, or Storage Directory of an OpenPages Application Server](#).
- If the host name of one of your OpenPages reporting servers or the load balancer for your reporting servers changed, or if the Cognos Gateway URL changed, follow the steps in [How to Change the Hostname or URL of an OpenPages Reporting Server](#).
- If the host name of your OpenPages global search server changed, follow the steps in [How to Change the Hostname of a Global Search Server for OpenPages](#).

Refreshing an 8.2 environment with data from an 8.1.x or earlier environment

You can refresh the data in an 8.2 environment with data from your source environment.

Do this task if the following conditions are true:

- You previously migrated to IBM OpenPages with Watson 8.2.0.x. During the migration upgrade, you restored data from a 7.3.x, 7.4.x, 8.0.x, or 8.1.x environment (the source environment) into your 8.2.0.x environment (the target environment).
- You now want to refresh your 8.2.0.x environment with a more recent backup of the data from your source environment.

Before you begin

- You have a working OpenPages 8.2.0.x environment.
- You have backups from a working OpenPages source environment (7.3.x, 7.4.x, 8.0.x, or 8.1.x). Your backup must include the databases, OpenPages storage directory, and any files that you customized, such as JSPs. For more information, see [“Backing up your source environment”](#) on page 198.

Back up the databases and the OpenPages storage directory at the same time to ensure that they are in sync.

- Ensure that no users are logged in to the OpenPages application in your 8.2.0.x environment.
- Ensure that no database scripts are running in your 8.2.0.x environment. Database scripts, other than the scripts that you use in this procedure, must not be run until the refresh is complete.
- Ensure that there are no long running OpenPages processes, such as FastMap imports or global search indexing processes.

You can use SQL to check whether processes are running. See the following [technote](#).

- If processes are running and the application servers are running, wait for the processes to complete.
- If processes are running and the application servers are stopped, follow the instructions in the [technote](#) to stop the processes.

About this task

Do the following steps in your 8.2.0.x environment.

Tip: Back up your 8.2.0.x environment before you begin.

Procedure

1. Drop the search index.
 - a) Start the search server in your 8.2.0.x environment.
See [“Start or stop the global search services”](#) on page 312.
 - b) Log on to OpenPages as a user with administrative privileges. Go to the Standard UI.
 - c) Click **Administration** > **Global Search** and click **Disable**.
2. Stop all servers, including all application servers, all reporting servers, and the search server (if you use the global search feature).
See [Chapter 12, “Starting and stopping servers,”](#) on page 309.
3. Restore the most recent database backups from your source environment into the 8.2.0.x database.
 - For IBM Db2, see [“Restore the OpenPages database in your 8.2 environment \(Db2\)”](#) on page 222 and [“Restoring the Cognos content store \(Db2\)”](#) on page 225.
 - For Oracle, see [“Restore the OpenPages database in your 8.2 environment \(Oracle\)”](#) on page 243 and [“Restore the Cognos content store in your 8.2 environment \(Oracle\)”](#) on page 250.
4. Restore the most recent backup of the OpenPages storage directory from your source environment into your 8.2.0.x environment.
See [“Restore the storage directory in the target environment”](#) on page 205.
5. Restore any customized files, such as JSP helpers.
6. Run the 8.2 database upgrade scripts manually.
 - For IBM Db2, see [“Upgrade the databases \(Db2\)”](#) on page 226.
 - For Oracle, see [“Upgrade the OpenPages database \(Oracle\)”](#) on page 252.
7. Run the 8.2.0.x fix pack database upgrade scripts manually.
 - For IBM Db2, see [“Update the OpenPages database manually \(Db2\)”](#) on page 282.
 - For Oracle, see [“Update the OpenPages database manually \(Oracle\)”](#) on page 289.

8. If the location of the OpenPages storage directory is different in your source and target environments, update the location of the directory in the database.
 - For IBM Db2, see [“Updating the location of the openpages-storage directory \(Db2\)”](#) on page 161.
 - For Oracle, see [“Updating the location of the openpages-storage directory \(Oracle\)”](#) on page 163.
9. Start all servers in your 8.2.0.x environment.
See [Chapter 12, “Starting and stopping servers,”](#) on page 309.
10. Upgrade the application data to 8.2.
For more information, see [“Upgrading application data”](#) on page 205.
11. Do all of the post-migration tasks for 8.2.
See [“Post migration tasks”](#) on page 206.

You do not need to drop or re-create the reporting schema.

You need to regenerate the reporting framework only if the object model changed in the source environment after you upgraded to 8.2.0.x. For example, if you upgraded to 8.2.0.x and then users added, modified, or removed fields, objects, object types, or relationships in the source environment, then you need to refresh the reporting framework.
12. Upgrade the application data from 8.2.0 to the 8.2.0.x fix pack that is installed in your environment.
For more information, see [“Upgrading application data to 8.2.0.x”](#) on page 416.
13. Do all of the post-upgrade steps for 8.2.0.x fix packs.
See [Postinstallation tasks](#).
14. If the OPSys password is different in the source environment and the 8.2.0.x environment or if you changed the default OPSys password, update the OPSys password in the 8.2.0.x environment.

For more information, see [Changing the OPSys password](#) in the *IBM OpenPages with Watson Administrator's Guide*.
15. Start the search server and re-create the search index.

If the host name of the search server is different in the source and target environments, see [Update the global search settings](#).

If you migrated from 7.3.x or later and you use global search, see [Enabling global search](#).

If the location of the OpenPages storage directory has changed, update the search server properties file. For more information, see [Updating the search server properties file with the location of the OpenPages storage directory](#).

Upgrading application data to 8.2.0.x

Use these steps to upgrade the application data from 8.2.0.0 to an 8.2.0.x fix pack.

About this task

After you upgrade the application data to 8.2.0.0, upgrade it to 8.2.0.1 or a later fix pack.

Upgrade the application data by running the application data load scripts in ascending order, starting with 8.2.0.1, up to and including the fix pack version that is installed in your environment.

For example, if your upgraded environment is using 8.2.0.3, upgrade the application data to 8.2.0.1 by running `openpages-8-2-0-1-loader-data.bat | . sh`, then upgrade it to 8.2.0.2 by running `openpages-8-2-0-2-loader-data.bat | . sh`, and then upgrade it to 8.2.0.3 by running `openpages-8-2-0-3-loader-data.bat | . sh`.

In the following steps, `<latest_fix_pack_version>` is the fix pack version that is installed in your environment and `<loader_data_version>` is the version of the application data that you are loading.

Procedure

1. Log on to the admin application server in your 8.2.0.0 environment.
2. Go to the `<OP_HOME>/bin` directory.
3. Edit the `<OP_HOME>/bin/ObjectManager.properties` file and update the following settings as shown:

```
configuration.manager.vendor.mode=true
configuration.manager.disable.triggers=true
```

4. Save and close the file.
5. Update the application data from 8.2.0.0 to 8.2.0.x.
 - a) Edit the following file: `<OP_HOME>/installer/maintenance/fix-pack-<latest_fix_pack_version>/OP_HOME/addon_module/loaderdata/<loader_data_version>_loader_data/schema_loader_properties.sh|.bat`
 - Set the `OPXUserPassword` property to the clear-text, decrypted password of the OpenPages administrator user.
 - Save your changes and close the file.
 - b) Open a shell or command prompt and go to the following directory: `<OP_HOME>/installer/maintenance/fix-pack-<latest_fix_pack_version>/OP_HOME/addon_module/loaderdata/<loader_data_version>_loader_data`
 - c) Run the following script.

Replace x with the version that you are loading.

Windows

```
openpages-8-2-0-<x>-loader-data.bat
```

Linux

```
./openpages-8-2-0-<x>-loader-data.sh
```

- d) Verify the upgrade. Open the `ObjectManager.log` file. Look for any errors with a time stamp that matches the date and time that you upgraded the application data.
 - e) Edit the following file: `<OP_HOME>/installer/maintenance/fix-pack-<latest_fix_pack_version>/OP_HOME/addon_module/loaderdata/<loader_data_version>_loader_data/schema_loader_properties.sh|.bat`
 - Replace the password in the `OPXUserPassword` property with `*****` to remove the password from the file.
 - Save your changes and close the file.
 - f) Repeat steps a-e to load the application data for each fix pack version up to and including the fix pack version that is installed in your environment.
6. Edit the `ObjectManager.properties` file and update the following settings as shown:

```
configuration.manager.vendor.mode=false
configuration.manager.disable.triggers=false
```

7. Save and close the file.
8. Restart all servers, including all application servers, all reporting servers, and the search server (if you use the global search feature).

See [Chapter 12, “Starting and stopping servers,”](#) on page 309.

Adding solutions to a deployment

If your deployment is at version 8.2.x and it does not have IBM OpenPages solutions, you can add them to your deployment.

About this task

Do this task to do a fresh installation of solutions.

For example:

- If you did a fresh installation of 8.2 and you did not install solutions at that time, you can add them.
- If you migrated to 8.2 and your source environment did not include solutions, you can add them after you complete the migration to 8.2.

Note: Do this task only if solutions are not installed.

If you want to install solutions silently, open the `deploy.properties` file. In the `[deploy]` section, set the `module` property to `true`. In the `[db]` section, set the `module_likeliness_count`, `module_impact_count`, and `module_assessment_method` properties. For more information, see [Appendix A, “Silent installations,” on page 393](#).


Procedure

1. Open the installation app and log in.
2. Open your deployment.
3. Click the **Deployment Task** list and select **Current deployment**.
4. Enable the **Install Solutions** check box.
5. Click the **Database Server** card and configure the metrics for solutions:
 - **Module Assessment Method:** Select the risk assessment method.
 - **Total Likelihood Count:** The Total Likelihood Count identifies the scale of inherent and residual risk likelihood. Select the maximum value for the scale.
 - **Total Impact Count:** The Total Impact Count identifies the scale of inherent and residual risk impact. Select the maximum value for the scale.
6. Click **Validate** to save and validate the deployment.
7. Click **Install**.


Tip: You can log out and close the browser window. The **Install** process continues to run. When you log in to the installation app again, the app shows the status of your deployment. You can also close the browser window during the **Configure** process.

8. Click **Configure**.
9. For each sample user that you want to keep, change the user's password.

To do this step, you need to be an administrator with the **Reset Password** permission. For more information, see the *IBM OpenPages with Watson Administrator's Guide*.

 - a) Log in to OpenPages.
 - b) Click  > **Users and Security** > **Domains & Groups**.
 - c) Click **Groups**, and then click **Sample Users**.
 - d) Click a sample user, such as **ORM**.
 - e) Click **Reset Password**.
 - f) Type the new password, and then click **Save**.
10. For each sample user that you don't need, disable the user.

To do this step, you need to be an administrator with the **Manage** permission. For more information, see the *IBM OpenPages with Watson Administrator's Guide*.

- a) Log in to OpenPages.
- b) Click  > **Users and Security** > **Domains & Groups**.
- c) Click **Groups**, and then click **Sample Users**.
- d) Click a sample user, such as **ORM**.
- e) Click **Disable**.
- f) Review the options, and then click **Disable**.

Some options require additional permissions. For more information, see the *IBM OpenPages with Watson Administrator's Guide*.

Results

The IBM OpenPages solutions are installed.

Enabling only the Task Focused UI

You can configure your deployment to use only the Task Focused UI. With this option, users and administrators see only the Task Focused UI and cannot switch to the Standard UI.

About this task

Important: If you use global search, such as the Global Search widget on Dashboard tabs, do not remove the Standard UI. The user interface for administering global search is not available in the Task Focused UI.

Procedure

1. Log on to the IBM OpenPages with Watson application server as a user with administrative permissions.
2. Stop all OpenPages services.
For more information, see [“Stopping application servers” on page 311](#).
3. Go to the `<OP_HOME>/wlp-user/servers/<server_name>Server<#>/configDropins/overrides/` directory.

Where `<server_name>` is the name of the application server.

4. In a text editor, open the `op-apps.xml` file and look for the `<enterpriseApplication>` element.
5. Replace the `<enterpriseApplication>` element with the following text:

```
<enterpriseApplication id="op-apps">
  <!-- Specify an alternative context-root here for the primary OpenPages web
  application -->
  <web-ext id="sosa" moduleName="sosa" context-root="disabled" />
  <!-- START CUSTOM UI CONFIG -->
  <web-ext id="taskui" moduleName="taskui" context-root="/openpages" />
  <web-bnd moduleName="taskui">
    <virtual-host name="default_host" />
  </web-bnd>
  <web-bnd moduleName="sosa">
    <virtual-host name="disabled_host" />
  </web-bnd>
  <!-- END CUSTOM UI CONFIG -->
</enterpriseApplication>
```

6. If you use a shortened URL for OpenPages, update the following line:

```
<web-ext id="taskui" moduleName="taskui" context-root="/openpages" />
```

For example:

```
<web-ext id="taskui" moduleName="taskui" context-root="/" />
```

7. Clean up your environment. Do these steps to remove third-party technologies that you no longer need.

a) Go to the following directory: `<OP_HOME>/wlp-usr/shared/apps/op-apps.ear/publishweb.war/WEB-INF/lib`

Remove the following files:

- `struts.jar`
- `struts-legacy.jar`

b) Go to the following directory: `<OP_HOME>/wlp-usr/shared/apps/op-apps.ear/sosa.war/WEB-INF/lib`

Remove the following files:

- `struts.jar`
- `struts-legacy.jar`

c) Go to the following directory: `<OP_HOME>/applications`

Extract the `op-apps.ear/` file.

Remove the following files from `publishweb.war`:

- `WEB-INF/lib/struts.jar`
- `WEB-INF/lib/struts-legacy.jar`

Re-compress the `publishweb.war` file and place it back in `<OP_HOME>/applications/op-apps.ear`.

Tip: If you're on Linux, you can use the command line:

```
cd <OP Home>/applications
unzip op-apps.ear publishweb.war
zip -d publishweb.war WEB-INF/lib/struts.jar
zip -d publishweb.war WEB-INF/lib/struts-legacy.jar
zip -u op-apps.ear publishweb.war
```

d) Go to the following directory: `<OP_HOME>/applications`

Extract the `op-apps.ear/sosa.war` file.

Remove the following files:

- `WEB-INF/lib/struts.jar`
- `WEB-INF/lib/struts-legacy.jar`

Recompress the `sosa.war` file and place it back in `<OP_HOME>/applications/op-apps.ear`.

Tip: If you're on Linux, you can use the command line:

```
cd <OP Home>/applications
unzip op-apps.ear sosa.war
zip -d sosa.war WEB-INF/lib/struts.jar
zip -d sosa.war WEB-INF/lib/struts-legacy.jar
zip -u op-apps.ear sosa.war
```

8. Restart all OpenPages services.

Linux

Go to the `<OP_HOME>/bin` directory and run the following command:

```
./startAllServers.sh --clean
```

Windows

- If you use a script to start and stop application servers, go to the `<OP_HOME>\bin` directory and run the following command:

```
StartAllServers.cmd --clean
```

- If you use Windows services to start and stop application servers, you need to do some cleanup before you start the services. Go to the `<OP_HOME>/wlp-usr/servers/<server_name>Server<#>/workarea` directory. Remove all of the files.
9. If this is a load-balanced environment, repeat this procedure for each application server in the load-balanced environment.

Removing WebSphere Application Server

If you upgraded or migrated, you might want to remove IBM WebSphere Application Server from your environment. IBM OpenPages with Watson 8.2 and later uses IBM WebSphere Liberty. This task is optional.

About this task

Do this task after you complete the upgrade or migration to IBM OpenPages with Watson 8.2 or later.

Standalone deployments

Do these steps if you used a standalone deployment in your pre-8.2 environment or if you are migrating from 7.3.x.

Procedure

1. Stop all IBM WebSphere Application Server profiles.
For example, on Microsoft Windows, stop all services that are named `IBMWAS<version>Service - <profile_name>`.
2. Do the following steps on each application server:
 - a) Go to the `<WAS_HOME>` directory.
 - b) If you are using Microsoft Windows, run the following command for each profile – servers, nodes, and the deployment manager:


```
WASService -remove <profile_name>
```
 - c) Run the following command:


```
./manageprofiles.sh|bat -deleteAll
```
 - d) Delete the `<OP_HOME>/profiles` directory.
 - e) Delete the following file: `<OP_HOME>/aurora/conf/was-admin-users.properties`
 - f) Uninstall WebSphere Application Server.

Shared-cell deployments

Do these steps if you used a shared cell in your pre-8.2 environment.

Procedure

1. Stop all IBM WebSphere Application Server services.
For example, on Microsoft Windows, stop all services that are named `IBMWAS<version>Service - <profile_name>`.
2. Do the following steps on each application server:
Do not change the deployment manager when you do these steps.
 - a) Go to the `<WAS_HOME>` directory.
 - b) If you are using Microsoft Windows, run the following command for each profile, except the deployment manager:

```
WASService -remove <profile_name>
```

Note: Do not remove the deployment manager profile.

c) Run the following command:

```
./manageprofiles.sh|bat -delete -profileName <OP_node_name>
```

Repeat this step for each node.

d) Delete the <OP_HOME>/profiles directory.

e) Run the following command:

```
./manageprofiles.sh|bat -validateAndUpdateRegistry
```

f) Uninstall WebSphere Application Server on each application server, excluding the server where the deployment manager is installed.

3. Do the following steps on the deployment manager.

a) Go to the <DmgrProfileHome>/bin directory.

b) Run the following command:

```
./cleanupNode.sh|bat <node_name> -username <was_admin_user> -password <was_admin_password>
```

Repeat this step for each node.

4. Log on to the IBM WebSphere Integrated Solutions Console and do the following steps:

a) Go to **Environment > Shared libraries**. Select the following libraries and click **Delete**:

- JSON4J_Apache.jar
- op-ext-lib
- op-isolated-lib
- openpages-ext.jar

b) Go to **Applications > All applications**. Select the op-apps application and click **Remove**. Click **OK** to confirm.

c) Go to **Resources > JDBC > Data sources**. Select the CWTxDataSourceXA data source, and then click **Delete**.

d) Go to **Resources > JDBC providers**. Select either of the following providers (depending on your database type) and click **Delete**.

- OpenPages Oracle JDBC Provider (XA)
- OpenPages DB2 Universal JDBC Driver Provider (XA)

e) Go to **Security > Global Security**. Click **Java Authentication and Authorization Service > J2C authentication data**. Select OpenPages JDBC authentication entry, and then click **Delete**.

f) Go to **Service integration > Buses**. Select the OPSIBusName bus and click **Delete**.

g) Go to **Servers > Clusters > WebSphere application server clusters**. Select OpenPagesCluster and click **Delete**. Click **OK** to confirm.

h) Go to **System administration > Deployment manager**. Click **Java and Process ManagementProcess definition**. Click **Java Virtual Machine**. In the **Generic JVM arguments** box, remove -Dopenpages.home=<OPHome>, and then click **OK**.

i) Go to **System administration > Deployment manager**. Click **Java and Process Management > Process definition**. Click **Java Virtual Machine**, and then click **Custom properties**. Select the ws.ext.dirs property, and then click **Delete**.

j) Save your changes.

5. If the deployment manager is installed on a server that is separate from all other IBM OpenPages with Watson servers, delete the <OP_HOME> directory.

Appendix D. Troubleshooting problems

Troubleshooting is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and how to resolve the problem.

Review the following table to help you to resolve a problem.

Table 75. Troubleshooting actions	
Action	Description
Apply all known fix packs and interim fixes (iFixes).	A product fix might be available to fix the problem. See “Getting fixes” on page 424.
Ensure that the configuration is supported.	Review the software and hardware requirements in the Supported Environments document.
Look up error message codes by selecting the product from the IBM Support Community and then typing the error message code into the Search support box.	Error messages give important information to help you identify the component that is causing the problem. For information about viewing installation log files, see “Log files” on page 427.
Reproduce the problem.	Try to reproduce the problem on a test system, for example.
Check the installation directory structure and file permissions.	The installation location must contain the appropriate file structure and file permissions.
Review relevant documentation, such as fix lists, technotes, and forums.	Search the IBM knowledge bases to determine whether your problem is known, has a workaround, or if it is already resolved and documented. See “Searching knowledge bases” on page 424.
Review recent changes in your computing environment.	Sometimes installing new software or software updates can cause compatibility issues.
Collect diagnostic data.	This data is necessary for IBM OpenPages Support to effectively troubleshoot and assist you in resolving the problem. You can also collect diagnostic data and analyze it yourself. See “Collect log files and diagnostic data” on page 428.

For more additional troubleshooting strategies, see [Techniques for troubleshooting problems](#)

Troubleshooting resources

Troubleshooting resources are sources of information that can help you resolve a problem that you have with a product. Many of the resource links provided can also be viewed in a short video demonstration.

To view the video version, search for "troubleshooting" through either Google search engine or YouTube video community.

Searching knowledge bases

You can often find solutions to problems by searching IBM knowledge bases. You can optimize your results by using available resources, support tools, and search methods.

About this task

You can find useful information by searching the [IBM Documentation](#). However, sometimes you must look beyond the documentation to answer your questions or resolve problems.

Procedure

To search knowledge bases for information that you need, use one or more of the following approaches:

- Find the content that you need by using the [IBM Support portal](#).

The IBM Support portal is a unified, centralized view of all technical support tools and information for all IBM systems, software, and services. Go to the IBM Support portal to access the IBM electronic support portfolio from one place. You can tailor the pages to focus on the information and resources that you need for problem prevention and faster problem resolution.

- Search for content by using the IBM masthead search.

You can use the IBM masthead search by typing your search string into the **Search** field at the beginning of any [ibm.com](#)® page.

- Search for content by using any external search engine, such as Google, Yahoo, or Bing.

If you use an external search engine, your results are more likely to include information that is outside the [ibm.com](#) domain. However, sometimes you can find useful problem-solving information about IBM products in newsgroups, forums, and blogs that are not on [ibm.com](#).

Tip: Include "IBM" and the name of the product in your search if you are looking for information about an IBM product.

- Join the IBM Governance, Risk and Compliance (GRC) Community. The IBM GRC Community is a communication forum where IBM can share information about OpenPages with the worldwide community of users. Contact IBM Support for instructions to join.

Getting fixes

A product fix might be available to resolve your problem.

Procedure

To find and install fixes:

- Determine which fix you need. Go to [OpenPages with Watson 8.2 Fix List](#). The Fix List shows a comprehensive list of defect corrections for major releases, fix packs, and interim fixes.
- At the bottom of the Fix List, click the link to the download document for the fix you want to apply.
- Download the fix.
- Apply the fix. Follow the instructions in the "Installation Instructions" section of the download document.
- Subscribe to receive weekly email notifications about fixes and other IBM Support information. For more information, see ["Subscribing to Support notifications"](#) on [page 426](#).

Contacting IBM Support

IBM Support assists with product defects, answers FAQs, and helps users resolve problems with the product.

Before you begin

After you tried to find your answer or solution by using other self-help options such as Technotes, you can contact IBM Support.

Before you contact IBM Support, your company or organization must have an active IBM maintenance contract, and you must be authorized to submit problems to IBM. For information about the types of available support, see [Support portfolio](#). For information about how to request access to your company's IBM Support account, see [Requesting access to your company's IBM Support account](#).

About this task

You can open a case from the web, chat, or by phone. For more information, see [Get help with your products](#).

Procedure

To contact IBM Support about a problem:

1. Define the problem, gather background information, and determine the severity of the problem.
For more information, see [Getting IBM support](#).
2. Gather the following diagnostic information:
 - Environment type (such as production or development).
 - Application, release, and patch level (such as IBM OpenPages with Watson 8.2.0.1 or IBM OpenPages for IBM Cloud Pak for Data 8.2.2).
 - Description of the issue.
 - Detailed steps to reproduce the issue.
 - Screen captures of the issue.
 - Expected and actual results.
 - OpenPages with Watson log files (for more information, see [Collect logs and diagnostic data](#)).
 - Any workarounds that you have implemented.
 - The date and time that the issue was encountered.
 - Database type and version (such as Oracle 19c or IBM Db2 11.5).
3. Submit the problem to IBM Support in one of the following ways:
 - Online through IBM Support. You can open, update, and view all of your cases from the Service Request portlet on the **Service Request** page. This video demonstrates how to open a case from the IBM Support Community: [Open and manage cases](#).
 - By phone: For the phone number to call in your region, see the [Directory of worldwide contacts](#) web page.

For more information, see [Get help with your products](#).

Results

If the problem that you submit is for a software defect or for missing or inaccurate documentation, IBM Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever possible, IBM Support provides a workaround that you can implement until the APAR is resolved and a fix is delivered. IBM publishes resolved APARs on the IBM Support website daily, so that other users who experience the same problem can benefit from the same resolution.

[“Contacting IBM Support” on page 424](#)

[“Exchanging information with IBM” on page 426](#)

Exchanging information with IBM

To diagnose or identify a problem, you might be necessary to provide IBM Support with data and information from your system. In other cases, IBM Support might provide you with tools or utilities to use for problem determination.

Sending information to IBM Support

To reduce the time that is required to resolve your problem, you can send trace and diagnostic information to IBM Support.

About this task

To submit diagnostic information to IBM Support, add the files to your support case. For more information, see [How to Open a Case](#).

Receiving information from IBM Support

Occasionally IBM OpenPages Support might ask you to download diagnostic tools or other files. You can use FTP to download these files.

Before you begin

Ensure that IBM OpenPages Support provided you with the preferred server to use for downloading the files and the exact directory and file names to access.

Procedure

To download files from IBM Support:

1. Use FTP to connect to the site that IBM OpenPages Support provided and log in as anonymous. Use your email address as the password.
2. Change to the appropriate directory:
 - a) Change to the `/fromibm` directory.

```
cd fromibm
```

- b) Change to the directory that IBM OpenPages Support provided.

```
cd nameofdirectory
```

3. Enable binary mode for your session.

```
binary
```

4. Use the **get** command to download the file that IBM OpenPages Support specified.

```
get filename.extension
```

5. End your FTP session.

```
quit
```

Subscribing to Support notifications

To stay informed of important information about the IBM products that you use, you can subscribe to notifications.

About this task

By subscribing to receive notifications about IBM OpenPages with Watson or IBM OpenPages for IBM Cloud Pak for Data, you can receive important technical information and updates for specific IBM Support tools and resources.

Procedure

1. Go to the [IBM Support portal](#).
2. Sign in using your IBM ID and password.
3. Click the person icon and select **Settings**.
4. Expand **Case notification settings** and select the options you prefer.

Log files

Use the installation log files and validation reports to help troubleshoot problems that occur during the installation.

Installation log files

Log files for a deployment are stored on the installation server in the `<installation_server_home>/src/deployment/<deployment-name>/logs/nodes` directory.

For example, if your deployment is named "CorporateFinance", the log files for each deployed server are located in: `<installation_server_home>/src/deployment/CorporateFinance/logs/nodes`

The nodes directory contains a subdirectory for each server in your deployment, for example:

```
Application Server1
Application Server2
Database Server
Global Search Server
Report Server1
```

As a deployment progresses through the **Validate**, **Install**, and **Configure** phases, the following log files are created in the subdirectories:

- `pre-vali.log`
- `install.log`
- `config.log`

You might also see a `restart.log` file in the application server subdirectories.

When a component is installed remotely, the log files are copied from the remote server to the appropriate subdirectory on the installation server automatically. For example, if `Application Server2` is installed on a remote computer, the files from the remote computer are copied to the `Application Server2` directory on the installation server computer.

The subdirectories also contain JSON files that contain metadata relevant to the deployment of that server. Do not delete the JSON files.

The base directory, `<installation_server_home>/src/deployment/<deployment-name>/logs/` also contains a log file that is named `installer.log` that contains logging information about the installation server.

Most log file entries contain a time stamp followed by the log message's status (`error`, `warn`, or `info`). Examine the log files for entries that contain `error` for any issues that might need to be addressed.

The `info` entries are primarily progress messages.

The `warn` entries indicate that a non-fatal issue was encountered. Some post-installation action might be needed.

The `error` entries indicate that an issue occurred. In most cases, you must take corrective action in order for the deployment to proceed.

Validation reports

During a deployment, the validation process runs at various points. If you are using the installation app, for example, the validation process runs each time that you click **Validate**.

The status of each validation is summarized in a color-coded `Validation_Report.pdf` file. If you are using the installation app, you can click a link to download the validation report.

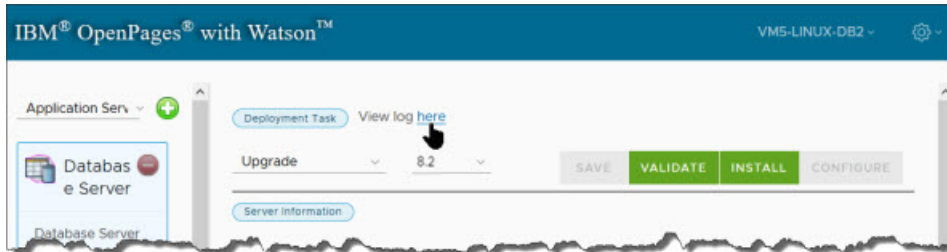


Figure 21. Viewing the validation log

The validation reports are stored on the installation server in the `<installation_server_home>/src/deployment/<deployment-name>/validation` directory.

On the individual servers where the installer agents are running, validation reports for each server are stored in a validation subdirectory within each server-specific directory. For example: `<agent_install_home>/src/deployment/<deployment-name>/logs/nodes/Database Server/validation`.

New PDF files are generated each time that a validation is run.

Collect log files and diagnostic data

You can use the LogCollector tool to collect log files and diagnostic data from the IBM OpenPages with Watson environment and from OpenPages databases.

Note: If you're using IBM OpenPages for IBM Cloud Pak for Data, use the IBM Cloud Pak® for Data web client to collect log files and diagnostic data.

The LogCollector tool collects log files and diagnostic data on an application server.

In a horizontal cluster environment, run the tool on each application server in your environment.

In a vertical cluster, with multiple application servers that are installed on the same machine, the tool gathers logs from all servers. The tool gathers logs from reporting servers only when they are installed on the same machine as one of the application servers. If the search server is also installed on the same machine, for example in a development environment, the tool also collects the search server logs.

The LogCollector tool is in the `<OP_HOME>/bin` directory.

The tool uses the following command options:

Note: For all command options, the long name command option uses two hyphens (--), whereas the short name uses only 1 hyphen (-).

--configuration or -c

Use to specify a configuration file path.

If you do not include this option, the default is `LogCollector.xml`.

Using `--configuration` or `-c` is optional.

--database or -d

Use to collect log and diagnostic data from only the database.

--file or -f

Use to collect only log and diagnostic files.

--location or -l

Use to specify the path where the output file will be stored.

If you specify both `-l` and `-t`, use `-t` for the file name and `-l` for the path. For example, `-l /temp -t test.zip` creates `/temp/test.zip`.

If you don't specify `-l`, the default location is the directory from which you run the command.

--property or -p

Use to set property values.

Using `--property` or `-p` is optional. If you do not include this option, the utility automatically retrieves these values from the local configuration. You need to supply these property values only if you want to override the default behavior.

You must include `-p` for each property that you use. For example, `-p DB_OP_USER <username> -p DB_OP_PASSWORD <password>`. The properties that you can use are:

Property	Description
DB_OP_USER	The OpenPages database username
DB_OP_PASSWORD	<p>The OpenPages database user's password</p> <p>If the password contains special characters, surround the password in quotation marks:</p> <ul style="list-style-type: none"> Windows: "password" Linux: 'password' <p>For more information, see “Special characters in passwords” on page 12.</p>
DB_TYPE	The database type. This value can be <code>db2</code> or <code>oracle</code> .
DB_URL	The database JDBC URL.

--target or -t

Use to specify a target package file.

If you do not include this option, the default is `LogCollector_<timestamp>.zip`. Using `--target` or `-t` is optional.

--help or -h

Use to display command help.

Example: Getting all information

1. Log in as the Super Administrator user.
2. Open a command line window.
3. Go to the `<OP_HOME>/bin` directory. For example, on Microsoft Windows operating systems, go to `C:\IBM\OpenPages\bin`. On Linux operating systems, go to `/opt/IBM/OpenPages/bin`.
4. Enter the following command:

On Microsoft Windows operating systems: `LogCollector.cmd`

On Linux operating systems: `./LogCollector.sh`

The tool generates a package file that is named `LogCollector_<timestamp>.zip` in the `<OP_HOME>/bin`.

Example: Specifying a target package file

1. Log in as the Super Administrator user.
2. Open a command line window.
3. Go to the `<OP_HOME>/bin` directory. For example, on Microsoft Windows operating systems, go to `C:\IBM\OpenPages\bin`. On Linux operating systems, go to `/opt/IBM/OpenPages/bin`.
4. Enter the following command:

On Microsoft Windows operating systems: `LogCollector.cmd -t LogCollector.zip`

On Linux operating systems: `./LogCollector.sh -t LogCollector.zip`

The tool generates a package file that is named `LogCollector.zip` in the `<OP_HOME>/bin` directory.

Example: Getting information for the database

1. Log in as the Super Administrator user.
2. Open a command line window.
3. Go to the `<OP_HOME>/bin` directory. For example, on Microsoft Windows operating systems, go to `C:\IBM\OpenPages\bin`. On Linux operating systems, go to `/opt/IBM/OpenPages/bin`.
4. Enter the following command:

On Microsoft Windows operating systems: `LogCollector.cmd -d`

On Linux operating systems: `LogCollector.sh -d`

The tool generates a package file that is named `LogCollector_<timestamp>.zip` in the `<OP_HOME>/bin`.

Example: Getting information from a database and specifying the connection information

This example shows how to use the `-d` and `-p` options. Use `-p` when you want to override the database connection information that is configured on your local server.

1. Log in as the Super Administrator user.
2. Open a command line window.
3. Go to the `<OP_HOME>/bin` directory. For example, on Microsoft Windows operating systems, go to `C:\IBM\OpenPages\bin`. On Linux operating systems, go to `/opt/IBM/OpenPages/bin`.
4. Enter the following command:

On Microsoft Windows operating systems:

```
LogCollector.cmd -d -p DB_TYPE db2 -p DB_URL jdbc:db2://localhost:50000/OPX
-p DB_OP_USER openpage -p DB_OP_PASSWORD "password"
```

On Linux operating systems:

```
./LogCollector.sh -d -p DB_TYPE db2 -p DB_URL jdbc:db2://localhost:50000/OPX
-p DB_OP_USER openpage -p DB_OP_PASSWORD 'password'
```

The tool generates a package file that is named `LogCollector_<timestamp>.zip` in the `<OP_HOME>/bin`.

Order of starting and stopping services

To restart the servers in an IBM OpenPages with Watson environment, you must stop and start them in sequence. Restarting the servers in order ensures that the OpenPages application server and Cognos Analytics can connect to the database server.

Use the following sequence to stop the servers:

1. Stop the services on the Search server.
2. Stop the services on the Cognos Analytics reporting server(s).
3. Stop the services on the OpenPages application server(s).
4. Stop the services on the database server.

Use the following sequence to start the servers:

1. Start the services on the database server.
2. Start the services on the OpenPages application server(s).
3. Start the services on the Cognos Analytics reporting server(s).
4. Start the services on the Search server.

Manually creating the reporting table space and user for Oracle databases

After you create the Cognos content store, you can manually create the content store user and the content store table space. This user must be able to create, alter, and drop tables, triggers, views, procedures, and sequences, and have the CONNECT and RESOURCE roles.

Procedure

1. Log on to the reporting server as a user with administrative privileges.
Note: For Linux operating systems, log in as a non-root user.
2. Copy the OP_<version>_Configuration/Database/ORACLE/COGNOS directory to the local system.
3. Log on to SQL*Plus by using the following command:

```
sqlplus system/"<system_password>"@<oracle_tns_alias>
```

To create the table space in the OpenPages database instance, enter the *oracle_tns_alias* of the OpenPages database. The database alias for the OpenPages database instance, as set during the Oracle database installation, is *oracle_tns_alias*. If necessary, you can retrieve this alias from the *tnsnames.ora* file.

If you created a separate database instance for the content store, create the table space in the content store database instance. Enter the *oracle_tns_alias* of the content store database.

4. At the SQL prompt, type the following command:

```
@cognosdbcreate.sql <cognos_user> <cognos_password>  
<oracle_data_home> <tablespace_name> <log_file>
```

Table 76. Parameter descriptions for the *cognosdbcreate.sql* script for Oracle databases

Script parameters	Description
cognos_user	Specifies the new user name for the content store database
cognos_password	Specifies the password for the cognos_user

Table 76. Parameter descriptions for the *cognosdbccreate.sql* script for Oracle databases (continued)

Script parameters	Description
oracle_data_home	Specifies the location of the Oracle data home directory for the content store database instance. On Windows operating systems: <ORACLE_BASE>\oradata\<SID>
tablespace_name	Specifies the name of the exported table space.
log_file	Specifies the file name and location of the log file to create.

Oracle package dependencies

To function correctly, the IBM OpenPages with Watson Oracle packages must have access to some standard Oracle objects.

In a standard Oracle deployment, database users can access the objects that are listed in the following tables. Some customer environments might restrict the default Oracle access model and remove public access from some of these objects. To use the OpenPages with Watson application, users require access to all objects in the tables.

The following tables list the standard Oracle objects to which the OpenPages application requires access. The tables show the base object, the object name, and the public synonym for the Oracle database objects.

Table 77. Base objects for the package object type

Base Object	Object Name	Public Synonym
SYS.DBMS_LOB	DBMS_LOB	PUBLIC.DBMS_LOB
SYS.DBMS_LOCK	DBMS_LOCK	PUBLIC.DBMS_LOCK
SYS.DBMS_JOB	DBMS_JOB	PUBLIC.DBMS_JOB
SYS.DBMS_OUTPUT	DBMS_OUTPUT	PUBLIC.DBMS_OUTPUT
SYS.DBMS_RANDOM	DBMS_RANDOM	PUBLIC.DBMS_RANDOM
SYS.DBMS_SESSION	DBMS_SESSION	PUBLIC.DBMS_SESSION
SYS.DBMS_SNAPSHOT	DBMS_MVIEW	PUBLIC.DBMS_MVIEW
SYS.DBMS_SQL	DBMS_SQL	PUBLIC.DBMS_SQL
SYS.DBMS_STANDARD	DBMS_STANDARD	PUBLIC.DBMS_STANDARD
SYS.DBMS_STATS	DBMS_STATS	PUBLIC.DBMS_STATS
SYS.DBMS_UTILITY	DBMS_UTILITY	PUBLIC.DBMS_UTILITY
SYS.ODCICONST	ODCICONST	PUBLIC.ODCICONST
SYS.PLITBLM	PLITBLM	PUBLIC.PLITBLM

<i>Table 77. Base objects for the package object type (continued)</i>		
Base Object	Object Name	Public Synonym
SYS.STANDARD	STANDARD	N/A
SYS.UTL_I18N	UTL_I18N	PUBLIC.UTL_I18N

<i>Table 78. Base objects for the view object type</i>		
Base Object	Object Name	Public Synonym
SYS.ALL.PROCEDURES	ALL_PROCEDURES	PUBLIC.ALL_PROCEDURES
SYS.ALL_TAB_PRIVS	ALL_TAB_PRIVS	PUBLIC.ALL_TAB_PRIVS
SYS.NLS_SESSION_PARAMETERS	NLS_SESSION_PARAMETERS	PUBLIC.NLS_SESSION_PARAMETERS
SYS.PRODUCT_COMPONENT_VERSION	PRODUCT_COMPONENT_VERSION	PUBLIC.PRODUCT_COMPONENT_VERSION
SYS.USER_CONS_COLUMNS	USER_CONS_COLUMNS	PUBLIC.USER_CONS_COLUMNS
SYS.USER_CONSTRAINTS	USER_CONSTRAINTS	PUBLIC.USER_CONSTRAINTS
SYS.USER_DB_LINKS	USER_DB_LINKS	PUBLIC.USER_DB_LINKS
SYS.USER_IND_COLUMNS	USER_IND_COLUMNS	PUBLIC.USER_IND_COLUMNS
SYS.USER_INDEXES	USER_INDEXES	PUBLIC.USER_INDEXES
SYS.USER_OBJECTS	USER_OBJECTS	PUBLIC.USER_OBJECTS
SYS.USER_SEGMENTS	USER_SEGMENTS	PUBLIC.USER_SEGMENTS
SYS.USER_SEQUENCES	USER_SEQUENCES	PUBLIC.USER_SEQUENCES
SYS.USER_SOURCE	USER_SOURCE	PUBLIC.USER_SOURCE
SYS.USER_TAB_COLS	USER_TAB_COLS	PUBLIC.USER_TAB_COLS
SYS.USER_TAB_COLUMNS	USER_TAB_COLUMNS	PUBLIC.USER_TAB_COLUMNS
SYS.USER_TABLES	USER_TABLES	PUBLIC.USER_TABLES
SYS.USER_TABLESPACES	USER_TABLESPACES	PUBLIC.USER_TABLESPACES

Table 78. Base objects for the view object type (continued)		
Base Object	Object Name	Public Synonym
SYS.USER_TRIGGERS	USER_TRIGGERS	PUBLIC.USER_TRIGGERS

Users also require access to all synonyms. If any public synonyms are removed from a default Oracle deployment, you must create a private synonym to the object in the OpenPages with Watson application user schema.

If these permissions are not available to `public` when you install OpenPages with Watson, the installation process grants the required permissions directly to the `openpages` database user automatically. Alternatively, you can grant these permissions back to `public` before you run the OpenPages with Watson installation process. If you want to do this, follow these steps to grant explicit permission to an object:

1. Log on to a computer with SQL*Plus and access to the database server.
2. From the command line, log on to SQL*Plus:

```
sqlplus sys/\"<password>\"@<tns_alias> as sysdba
```

3. At the SQL prompt, type the following command for the objects that are listed in [Table 77 on page 432](#):

```
grant execute on <object_name> to public;
```

Type the following command for the objects listed in [Table 78 on page 433](#):

```
grant select on <object_name> to public;
```

Each package object requires the EXECUTE permission. All other objects require the SELECT permission.

Known problems and solutions for global search

Issues that are related to the IBM OpenPages with Watson global search component are most commonly encountered when you are setting it up or when it is updated to synchronize the search index for changes that are made to the OpenPages with Watson schema (such as adding or removing object types or fields).

When an administrative operation fails, you can normally resolve these issues by clicking **View Log** to see the log message for the failed global search operation.

The most common failure is that the search service is not started, for which you see this error:

"Could not establish connection to the search engine. Please contact your system administrator."

Ensure that the search service is started or restart to try to resolve the issue.

Global search start fails

If you configured the global search services to start and stop by using a script and you forgot to stop global search before rebooting the system, when you attempt to start the global search services, the services will fail to start. To fix this issue complete the following steps.

Procedure

1. Log on to the search server as a user with administrative privileges.
2. Open a command line on the search server.
3. Go to the `<SEARCH_HOME>/opsearchtools/` directory and run the following commands.

On Microsoft Windows operating systems, run:

```
opsearchtool.cmd clearState -indexname openpages  
opsearchtool.cmd clearState -indexname folderacl
```

On Linux operating systems, run:

```
./opsearchtool.sh clearState -indexname openpages  
./opsearchtool.sh clearState -indexname folderacl
```

Global search setup fails

In some rare cases, the global search component might encounter a failure during the creation of the search index, before the operation completes. The failure might be caused by hardware issues, database issues, or a power outage, for example. When this happens, the state of the global search setup is in an undefined state and the **Enable** button might become available, giving the misleading impression that global search was set up successfully. To recover from this state, investigate the root cause, resolve it, and then set up global search again.

Procedure

1. Investigate and resolve the root cause of the failure.
2. Log on to OpenPages as a user with administrative privileges.
3. Click **Administration > Global Search**.
4. Click **Drop** to drop the search index.
5. Wait for the drop process to complete.

If the **Drop** button is not available or if the drop process fails, see [“Forcing a reset of global search” on page 435](#).

6. Click **Create** to re-create the search index.

Forcing a reset of global search

In some rare cases, it might be necessary to reset the IBM OpenPages with Watson global search component if you cannot restore it from the **Global Search** administration page. These issues might prevent you from successfully completing tasks in the global search administration page. To resolve these issues, complete the following steps.

Procedure

1. If you started a global search indexing process from the OpenPages user interface, click **Administration > Global Search**. Make a note of the **Id** of the indexing process. You need the **Id** in step “9” on page 436.
2. Log on to the search server as a user with administrative privileges.
3. Open a command line on the search server.
4. Go to the `<SEARCH_HOME>/opsearchtools/` directory to run the commands in the following steps.



Attention: At the successful completion of each command, the statement "Normal completion of command" should appear. If it does not, contact Customer Support to diagnose the issue.

5. Ensure that Solr is running and is reachable on port 8983. If Solr is not running, then run the following command to start it.

Microsoft Windows:

```
opsearchtool.cmd startSolr
```

Linux:

```
./opsearchtool.sh startSolr
```

6. Run the following commands to stop indexing.

Microsoft Windows:

```
opsearchtool.cmd stopIndexing -indexname openpages  
opsearchtool.cmd stopIndexing -indexname folderacl
```

Linux:

```
./opsearchtool.sh stopIndexing -indexname openpages  
./opsearchtool.sh stopIndexing -indexname folderacl
```

7. Verify that no opsearchtool.jar processes are running.

On Microsoft Windows operating systems, use the task manager to see whether any opsearchtool.jar processes are running. If there are, terminate them.

On Linux operating systems, use the ps command to see whether any opsearchtool.jar processes are running. If there are, terminate them.

8. Run the following commands to clear any PID states that might still be set if the opsearchtool.jar processes did not end successfully.

Microsoft Windows:

```
opsearchtool.cmd clearState -indexname openpages  
opsearchtool.cmd clearState -indexname folderacl
```

Linux:

```
./opsearchtool.sh clearState -indexname openpages  
./opsearchtool.sh clearState -indexname folderacl
```

9. If a global search indexing process was started from the OpenPages user interface, run the following commands:

Replace %lrpf-pid% with the **Id** of the indexing process.

Microsoft Windows:

```
opsearchtool.cmd syncIndex -terminatepid %lrpf-pid%  
opsearchtool.cmd fullIndex -indexname openpages -terminatepid %lrpf-pid%  
opsearchtool.cmd fullIndex -indexname folderacl -terminatepid %lrpf-pid%
```

Linux:

```
./opsearchtool.sh syncIndex -terminatepid %lrpf-pid%  
./opsearchtool.sh fullIndex -indexname openpages -terminatepid %lrpf-pid%  
./opsearchtool.sh fullIndex -indexname folderacl -terminatepid %lrpf-pid%
```

10. Run the following commands to reset global search.

Microsoft Windows:

```
opsearchtool.cmd resetSolr -indexname openpages  
opsearchtool.cmd resetSolr -indexname folderacl  
opsearchtool.cmd resetDb  
opsearchtool.cmd stopSolr  
opsearchtool.cmd startSolr
```

Linux:

```
./opsearchtool.sh resetSolr -indexname openpages  
./opsearchtool.sh resetSolr -indexname folderacl  
./opsearchtool.sh resetDb
```

```
./opsearchtool.sh stopSolr  
./opsearchtool.sh startSolr
```

11. Log on to OpenPages as a user with administrative privileges.
12. Click **Administration > Global Search**.
13. Click **Create** to re-create the search index.

What to do next

Resetting the global search component does not change your global search settings, such as object types, fields that are enabled for search, registry settings, or property settings. The reset disables the global search component. You must enable it again to make it available to users.

Checking for global search setup issues and periodic monitoring

When the incremental indexer is running during global search setup or after setup, some records might not get indexed due to issues with the record, other system errors, or application errors.

About this task

If the issues are not unrecoverable, they do not impede the setup process or the incremental indexer. However, the records that do not get indexed are logged in an error-log file, with an error message that explains the issue so you can take appropriate action. The error-log files are never rotated. Periodically examine this directory for new error files.

Procedure

1. Log on to OpenPages as a user with administrative privileges.
2. Go to the directory `<SEARCH_HOME>/opsearchtools/logs_error/`.
3. Examine this directory for new error files.

Encryption of long strings in OpenPages running on Oracle

Before encrypting long strings in OpenPages running on Oracle, refer to the following technote. The Technote describes a potential issue and how to resolve it by obtaining the appropriate patch from Oracle support and applying it to your environment.

Creating the global search index

After you install IBM OpenPages, create the global search index. If you are migrating, you can skip this task.

Before you begin

The reporting schema must exist and must be enabled before you create the search index.

Procedure

1. Start the search services, if they are not already started.
2. Log on to OpenPages as a user with administrative privileges. Go to the Standard UI.
3. Click **Administration > Global Search** and click **Create**.

Creating the index also enables global search.

Click **Refresh** to update the page.

Results

Global Search is available.

If global search does not start, see [“Known problems and solutions for global search”](#) on page 434.

For more information about global search, see the *IBM OpenPages with Watson Administrator's Guide*.

Before you contact IBM OpenPages Support

When you contact IBM OpenPages Support, you need to collect diagnostic data and provide a detailed use case of the issue.

About this task

Before you contact IBM OpenPages Support to help with resolving global search issues, follow these steps to collect diagnostic data.

Note: You do not need to stop global search, the OpenPages application server, the database server, or any other application when you run the **collectDiagData** command.

Procedure

1. Log in to the OpenPages global search server as a user with administrative privileges.
2. Open a command prompt or a shell window.
3. Go to the `<SEARCH_HOME>/opsearchtools/` folder and run the following commands:

- Microsoft Windows:

```
mkdir diag
opsearchtool.cmd collectDiagData -diagpath diag
```

- Linux:

```
mkdir diag
./opsearchtool.sh collectDiagData -diagpath diag
```



Attention: The **collectDiagData** command might report warning messages that look as if the command failed. This warning can happen due to a number of reasons, such as the data that is being collected cannot be accessed or is not yet available. If you see any such warnings, capture them and include them as part of the diagnostic data to IBM OpenPages Support.

4. Add the contents of the new folder that is created under the diag folder to a compressed file.
5. Send the compressed file and complete details about your issue to IBM OpenPages Support.

Installation issues and solutions

Error messages and log files provide you with information about errors that occur during the installation process. Use the error messages and log files to determine which part of the process failed.

Review common problem scenarios, recovery methods, and ways to get help if you encounter a problem during software installation. You can diagnose problems when the installation and configuration is unsuccessful.

Error: Cannot manage agent without connection information

When you install IBM OpenPages with Watson, apply a fix pack, or apply an interim fix, you see an error that an agent cannot be managed.

On the server card, the **Local User Name** and **Local User Password** fields are empty. Or, if you are running a silent installation, the `local_username` and `local_password` parameters are empty.

When you do not provide the local account credentials, you must install, update, stop, and start the agent manually. Otherwise, you see the following error:

```
Error: Cannot manage agent without connection information.
```




The error can occur in the following cases:

- The agent is not running on the remote server. This situation can occur when an agent is installed or updated manually and the agent was not started on the remote server.

To resolve the issues, start the agent on the remote server, and then continue with the installation. See [“Starting the installation agent manually” on page 54](#).

- The agent software is at a different version than the installation server. This situation can occur when an agent was installed manually, the installation server was updated, and the agent was not updated.

To resolve the issue, update the agent to the latest version and then click **Validate**. See [“Updating agents manually” on page 48](#).

- The  or  button on the server card was clicked.

To resolve the issue, start or stop the agent manually instead. See [“Starting the installation agent manually” on page 54](#) and [“Stopping the installation agent manually” on page 54](#).

Alternatively, provide the local account credentials.

- If you are using the installation app, enter values in the **Local User Name** and **Local User Password** fields on the server card.
- If you are running a silent installation, enter values in the `local_username` and `local_password` parameters of the `deploy.properties` file.

You can specify a local account that is on the remote server or a service account, for example `<domain>/<user name>`. The user must have administrative privileges on the remote server.

Error starting the installation app

If you try to start the installation app on Linux operating systems but enter the command incorrectly, and you try to start it again, you can receive an error.

For example, you can receive an error such as:

```
*****
ERROR: Error occurred during OpenPages Installer startup.
Although, OpenPages Installer was successfully installed.
Try starting OpenPages Installer using startup.sh script.
Location: /home/opuser/OP_8.2_Installer/startup.sh
*****
```

This error can occur due to time out settings. You can check the log to verify whether the installation app started.

Silent installation hangs

During a silent installation of IBM OpenPages with Watson, the installation process appears to hang. For example, the process is taking a very long time and there are a couple of components that are not finished and do not appear to be progressing.

Additionally, the installation logs contain the following messages:

```
[31merror[39m: Error: read ECONNRESET
    at exports._errnoException (util.js:1022:11)
    at TLSSocket.onread (net.js:610:25)
```

To resolve this problem:

1. Stop the installation server. For more information see, [“Stopping the installation server” on page 53](#).
2. Restart the installation server. For more information, see [“Starting the installation server” on page 53](#).
3. Run the installation again.

Validation error: OpenPages connection refused

When you upgrade, you see a validation error that says the connection to OpenPages was refused.

In the validation report, you see the following message:

error: Validation Platform Data Load: OpenPages connection refused. Make sure OpenPages is running.

The error can occur if you use single sign-on (SSO) and you configured it to require an SSO login to access the REST API URLs under `/grc/api/*`.

To resolve the error, do the following steps:

- Disable SSO.
- Return to the installation app and open your deployment. Click **Validate**.

Restoring the installation server

You can restore the installation server, if needed.

Before you begin

Ensure that you have the IBM OpenPages with Watson 8.2 package from Passport Advantage.

Download the latest fix pack kit to get the latest version of the installation server software.

Procedure

1. Log out of the installation app.
2. Log on to the OpenPages installation server computer as the user who installed the installation server.
Alternatively, you can log in as any user who has full permissions on the installation server directories and who can run `Node .js`.
3. Stop the installation server if it is running.
See [“Stopping the installation server” on page 53](#).
4. If you started the installation agents on remote servers manually, stop the agent on each remote server.
See [“Stopping the installation agent manually” on page 54](#).
5. Back up the `<installation_server_home>/src/deployment` directory.
6. Uninstall the installation server.
 - a) Go to the `<installation_server_home>/install/<OS type>` directory.
 - b) Run the uninstall script.
 - Windows

```
uninstall.bat
```
 - Linux:

```
./uninstall.sh
```
 - c) Delete the `<installation_server_home>` directory where the installation app was installed, for example, `NewInstaller`.
7. Install the installation server by using the 8.2 package from Passport Advantage.
For more information, see [“Setting up the installation server on Windows” on page 41](#) or [“Setting up the installation server on Linux” on page 43](#).
8. Update the installation server by using the latest fix pack kit from Fix Central.
For more information, see [“Updating the installation server” on page 47](#).

Note: If you installed the agent software on remote servers manually, ensure that the agent software is at the same version as the installation server.

9. Restore the /deployment directory that you backed up in step 5.

Restoring an installation agent

You can restore an installation agent on a remote server, if needed.

Before you begin

Ensure that you have the IBM OpenPages with Watson 8.1 package from Passport Advantage.

Download the latest fix pack kit to get the latest version of the installation server software.

Procedure

1. Log on to the remote server as the user who installed the agent software.

If you did not install the agent manually, you can log in as any user who has full permissions on the agent directories and who can run Node .js.

2. Stop the installation agent if it is running.

See [“Stopping the installation agent manually” on page 54](#).

3. Uninstall the installation agent.

a) Go to the <agent_home>/install/<OS type> directory.

b) Run the uninstall script.

- Windows

```
uninstall.bat
```

- Linux:

```
./uninstall.sh
```

c) Delete the <agent_home> directory.

4. If the agent was installed by using the installation app, do the following steps:

a) Log in to the installation app and open your deployment.

b) Click the **Deployment Task** list and select **Current Deployment**.

Tip: If you previously installed the agents manually and you now want to use the installation app to install them, complete the **Local User Name** and **Local User Password** fields on the remote server's card.

c) Click **Validate**.

The installation server installs the agent software on the remote server. It also updates the agent software, if needed.

5. If the agent was installed manually, do the following steps:

a) Install the agent software on the remote server. Use the 8.1 package from Passport Advantage.

For more information, see [“Installing agents manually” on page 45](#).

b) Update the agent software to the same version as the installation server.

For more information, see [“Updating agents manually” on page 48](#).

Global search fails to validate during upgrade

If the global search server fails to validate when you upgrade OpenPages, it can be because the host name in the URL points to the source server rather than the new target server.

About this task

Modify and run the following SQL statement to update the registry settings that define the admin and index/request URLs for global search on the target server.

Procedure

1. Modify the lines in bold in the following SQL statement.

For example:

```
vcSearchAdminURL REGISTRYENTRIES.DESCRPTION%Type := 'http://search.example.com:8985';  
vcSearchURL      REGISTRYENTRIES.DESCRPTION%Type := 'http://search.example.com:8983';
```

Oracle:

```
Declare  
  vcSearchAdminURL REGISTRYENTRIES.DESCRPTION%Type := '{full admin URL}';  
  vcSearchURL      REGISTRYENTRIES.DESCRPTION%Type := '{full request/index URL}';  
  recActor          ACTORINFO%Rowtype;  
Begin  
  -- get the system user  
  op_actor_mgr.get_actorinfo(OP_Actor_Mgr.gc_System_User, recActor);  
  -- set registry values  
  op_registry_mgr.set_registry_entry  
  (  
    p_parent_path      => '/OpenPages/Platform/Search/Admin',  
    p_name             => 'Search Server Administration URL',  
    p_description       => 'URL for Search Server Administration',  
    p_value            => vcSearchAdminURL,  
    p_is_hidden        => 'Y',  
    p_is_encrypted      => 'N',  
    p_is_protected     => 'Y',  
    p_actor_id         => recActor.actorid,  
    p_is_done_by_vendor => OP_Globals.sc_true,  
    p_behavior         => OP_Registry_Mgr.OPT_RE_Set_Defaults  
  );  
  op_registry_mgr.set_registry_entry  
  (  
    p_parent_path      => '/OpenPages/Platform/Search/Index',  
    p_name             => 'Search Server URL',  
    p_description       => 'URL for Search Server Index',  
    p_value            => vcSearchURL,  
    p_is_hidden        => 'Y',  
    p_is_encrypted      => 'N',  
    p_is_protected     => 'Y',  
    p_actor_id         => recActor.actorid,  
    p_is_done_by_vendor => OP_Globals.sc_true,  
    p_behavior         => OP_Registry_Mgr.OPT_RE_Set_Defaults  
  );  
  op_registry_mgr.set_registry_entry  
  (  
    p_parent_path      => '/OpenPages/Platform/Search/Request',  
    p_name             => 'Search Server URL',  
    p_description       => 'URL for Search Request',  
    p_value            => vcSearchURL,  
    p_is_hidden        => 'Y',  
    p_is_encrypted      => 'N',  
    p_is_protected     => 'Y',  
    p_actor_id         => recActor.actorid,  
    p_is_done_by_vendor => OP_Globals.sc_true,  
    p_behavior         => OP_Registry_Mgr.OPT_RE_Set_Defaults  
  );  
  Commit;  
End;  
/
```

Db2:

```
Declare
  vcSearchAdminURL REGISTRYENTRIES.DESCRPTION%Type := '{full admin URL}';
  vcSearchURL      REGISTRYENTRIES.DESCRPTION%Type := '{full request/index URL}';
  recActor         ACTORINFO%Rowtype;
Begin
  -- get the system user
  op_actor_mgr.get_actorinfo_by_actor_name(OP_Actor_Mgr.gc_System_User, recActor);
  -- set registry values
  op_registry_mgr.set_registry_entry_with_behavior
  (
    p_parent_path      => '/OpenPages/Platform/Search/Admin',
    p_name             => 'Search Server Administration URL',
    p_description       => 'URL for Search Server Administration',
    p_value            => vcSearchAdminURL,
    p_is_hidden        => 'Y',
    p_is_encrypted      => 'N',
    p_is_protected      => 'Y',
    p_actor_id         => recActor.actorid,
    p_is_done_by_vendor => OP_Globals.sc_true,
    p_behavior         => OP_Registry_Mgr.OPT_RE_Set_Defaults
  );
  op_registry_mgr.set_registry_entry_with_behavior
  (
    p_parent_path      => '/OpenPages/Platform/Search/Index',
    p_name             => 'Search Server URL',
    p_description       => 'URL for Search Server Index',
    p_value            => vcSearchURL,
    p_is_hidden        => 'Y',
    p_is_encrypted      => 'N',
    p_is_protected      => 'Y',
    p_actor_id         => recActor.actorid,
    p_is_done_by_vendor => OP_Globals.sc_true,
    p_behavior         => OP_Registry_Mgr.OPT_RE_Set_Defaults
  );
  op_registry_mgr.set_registry_entry_with_behavior
  (
    p_parent_path      => '/OpenPages/Platform/Search/Request',
    p_name             => 'Search Server URL',
    p_description       => 'URL for Search Request',
    p_value            => vcSearchURL,
    p_is_hidden        => 'Y',
    p_is_encrypted      => 'N',
    p_is_protected      => 'Y',
    p_actor_id         => recActor.actorid,
    p_is_done_by_vendor => OP_Globals.sc_true,
    p_behavior         => OP_Registry_Mgr.OPT_RE_Set_Defaults
  );
Commit;
End;
```

2. Run the SQL statement in SQL*Plus (Oracle) or CLPPLUS (Db2) as the OpenPages database user.
3. Rerun the upgrade validation and verify that global search can now validate.

Docker containers not starting

After installing OpenPages by using Docker, not all of the containers have started and you cannot access the OpenPages application URL.

To resolve this, you can start the containers again by using the following command:

```
docker-compose [-f <yml file>] start
```

Application URL is missing the domain of the host after a Docker deployment

After you install IBM OpenPages with Watson by using Docker, the application URL contains only the host name rather than the fully qualified domain name. Additionally, you cannot access the JSP helper pages or the Cognos Analytics page from the OpenPages application.

The application URL is set when the Docker container starts and it is based on the **HOSTNAME** environment variable of the computer where you run the `docker-compose -f <yml_file> up` command. The

container startup finds the fully qualified domain name automatically. However, you can set the host of the application URL explicitly by updating the **HOSTNAME** variable on the computer. For example, you can set the host of the application URL to **myhost.mydomain.com** and redeploy OpenPages on Docker by using the following commands:

```
export HOSTNAME=myhost.mydomain.com
docker-compose -f <yml_file> down
docker-compose -f <yml_file> up -d
```

The `docker-compose -f <yml_file> down` command is needed only if you have already deployed OpenPages on Docker.

If you deploy OpenPages on Docker in a distributed environment (for example, one database server host and another application server host), the **HOSTNAME** environment variable is looked up only by the containers on the application server host. You do not need to redeploy the containers on the database server host if you change the application URL.

Errors while loading data after you upgrade

After you upgrade, you see errors such as the following while you load data:

```
Caused by: java.lang.ClassNotFoundException: org.springframework.context.ApplicationContextAware
    at java.net.URLClassLoader.findClass(URLClassLoader.java:609)
    at com.ibm.ws.bootstrap.ExtClassLoader.findClass(ExtClassLoader.java:243)
    at java.lang.ClassLoader.loadClassHelper(ClassLoader.java:850)
    at java.lang.ClassLoader.loadClass(ClassLoader.java:829)
    at com.ibm.ws.bootstrap.ExtClassLoader.loadClass(ExtClassLoader.java:134)
    at java.lang.ClassLoader.loadClass(ClassLoader.java:809)
    ...
2018-03-02 09:08:08
CODE      : OP-00550
LEVEL     : 4
NAME      : com.openpages.sdk.trigger.grc.GRCTriggerCacheException
ERROR #   : TOKAUSA9HXAY
TOKEN ID  : 465433
USER      : OpenPagesAdministrator
MESSAGE   : Cache may not be setup correctly.
    at com.openpages.sdk.trigger.grc.GRCTriggerRuleDefinition.getInstance
    (GRCTriggerRuleDefinition.java:111)
    at com.ibm.openpages.api.service.local.trigger.GRCTriggerManager.
processTriggerRule(GRCTriggerManager.java:237)
    ... 62 more

...
02 Mar 2018 09:08:08,849
ERROR ConfigurationManager on OPServer1
Loader EXCEPTION (Line: 88 Column: 53): Unable to create a new folder resource.
[P=630037:0=0:CT](ConfigurationManager.java:8112)
```

These errors can occur if triggers are still enabled during the data load. You can resolve this problem by disabling the triggers, and then reloading the data. After you successfully load the data, ensure that you re-enable the triggers.

For more information about disabling triggers, see [Disabling triggers when migrating environments](#) in the *IBM OpenPages with Watson Administrator's Guide*.

Warnings about system views when loading data

When you install, upgrade (in-place or migration), or install a fix pack, you see warnings about system views during the data load process.

The warnings are similar to the following text:

```
LOAD INFO (Line: 49 Column: 22): Object schema does not match the view being loaded.
The validation warnings:
    [Default:Status] Object field "Status" does not exist.
The system view is still loaded.
```

These warnings can occur in the following cases:

- You install version 8.2 without solutions
- You upgrade or migrate to version 8.2
- You install a fix pack in an environment that was upgraded from a pre-7.4 version, and the deployment does not include solutions.

You can ignore these warnings.

Example:

```

Loading OpenPages Configuration (system-views/sv-Documentation) from folder: /home/opuser/IBM/
OpenPages/Module/loaderdata as OpenPagesAdministrator ...

Processing started at Tue Jul 02 10:08:34 CST 2019

Loading Responsive Views ...
LOAD INFO (Line: 49 Column: 22): Object schema does not match the view being loaded. The
validation warnings:
  [Default:Status] Object field "Status" does not exist.
The system view is still loaded.
LOAD INFO (Line: 148 Column: 22): Object schema does not match the view being loaded. The
validation warnings:
  [Documentation Information:Author] Object field "Author" does not exist.
  [Documentation Information:Status] Object field "Status" does not exist.
  [Documentation Information:Display Text] Object field "Display Text" does not exist.
The system view is still loaded.
LOAD INFO (Line: 238 Column: 22): Object schema does not match the view being loaded. The
validation warnings:
  [General:group1:Author] Object field "Author" does not exist.
  [General:group1:Status] Object field "Status" does not exist.
  [General:Display Text] Object field "Display Text" does not exist.
  [Sections:Parent Sections:Status] Object field "Status" does not exist.
The system view is still loaded.
  3 total

```

Password confirmation field is empty after you import deployment properties

After you import a `deploy.properties` file, the confirmation field for the **Local User Password** for a server is empty.

This issue can occur when the following conditions are true:

- The `deploy.properties` file has a value for `local_password` for the server.
- The `deploy.properties` file has `remote_deploy` set to `false` for the server.
- After you import the file, you enable **Remote Deploy** in the installation app for the server.

To resolve the issue, do one of the following steps:

- Set `remote_deploy` to `true` for the server and then reimport the file.
- In the installation app, clear the **Local User Password** field on the server card and then re-enter the value for both this field and the confirmation field.

Update to IBM Installation Manager 1.8 is blocked when the data location is the same as the installation location

Starting with IBM Installation Manager version 1.8, you are blocked from using a data location that is within the IBM Installation Manager installation location.

About this task

In older IBM Installation Manager versions, you are not blocked from using a data location within the IBM Installation Manager installation location. When you try to update an older version that was installed by using a data location within the IBM Installation Manager installation location, you receive an error message.

For example, if the older Installation Manager version was installed in the /opt/IBM/IM directory by using the /opt/IBM/IM/dataLocation directory as the data location, the following error message is displayed when you update to IBM Installation Manager version 1.8.x:

```
CRIMA1261E ERROR: The installation directory ("/opt/IBM/IM") must not be the
same directory, a parent directory, or sub-directory of the Installation
Manager data directory ("/opt/IBM/IM/dataLocation")
```

This issue occurs when one of the following scenarios occur:

1. Using an IBM Installation Manager version earlier than 1.8.x (for example, 1.7.3), you install the Installation Manager that uses a data location within the installation location. For example:

```
installc -acceptLicense -dataLocation /opt/IBM/IM/dataLocation
-installationDirectory /opt/IBM/IM
```

2. Using an IBM Installation Manager version 1.8.0 or higher installer, you update the installed IBM Installation Manager. For example:

```
Installc -acceptLicense -dataLocation /opt/IBM/IM/dataLocation
```

Putting the data location within the installation location violates basic assumptions about the separation of the installation artifacts and the runtime data of IBM Installation Manager, which can lead to errors. IBM Installation Manager 1.8 was intentionally changed to no longer allow this situation. When the software detects this situation, it displays the preceding error message.

To resolve this issue, you must reinstall IBM Installation Manager in a new location that does not collide with the data location.

Unfortunately, the **-reinstallim** option does not work in this particular case because the data location is incorrectly located in the IBM Installation Manager installation location. You must manually reinstall IBM Installation Manager as follows:

Procedure

1. Delete the IBM Installation Manager installation location.

Normally, this means deleting the entire /opt/IBM/IM directory (the installation location in the preceding example), but because the data location was incorrectly put within the installation location, delete only the subdirectories of the /opt/IBM/IM directory, excluding the data location directory. Delete eclipse, license, and properties. The /opt/IBM/IM/dataLocation directory must remain.

2. Run IBM Installation Manager version 1.8.5 or higher installer to reinstall Installation Manager. Specify an installation location that does not collide with the data location. For example:

```
installc -acceptLicense -dataLocation /opt/IBM/IM/dataLocation
-installationDirectory /opt/IBM/IM/installLocation
```

3. To confirm that all previously installed products are still available, start the installed Installation Manager and click **File > View Installed Packages** to see the list of installed products.

Note: The instructions for manually reinstalling Installation Manager are derived from [Manually reinstalling Installation Manager](#), except that in this case, care must be taken not to delete the data location that was incorrectly put in the IBM Installation Manager installation location.

SQL0569N Authorization ID *user_name* does not uniquely identify a user, a group or a role in the system error

The IBM OpenPages with Watson installation app might indicate that the installation is successful. However, you might see a message similar to the following text in the log file:

```
SQL0569N Authorization ID "user_name" does not uniquely identify a user,
a group or a role in the system error
```

Ensure that on Linux operating systems, the user name for the OpenPages database user account is not the same as the group name. For example, `opuser:opuser` is not allowed.

For information about installation log files, see [“Log files” on page 427](#).

OpenPages with Watson and software that is installed in a directory that contains spaces

If you installed software that IBM OpenPages with Watson uses into a directory with spaces, you must use the Windows short file name convention for the directory location.

For example, in the IBM OpenPages with Watson installation app, when you configure the home directory for Cognos, instead of entering the C:\Program Files\IBM\cognos\analytics directory, enter C:\PROGRA~1\IBM\cognos\analytics.

Garbled characters are displayed on the OpenPages with Watson home page when you log in for the first time

You might see garbled characters on the IBM OpenPages with Watson home page (http://server_name:port/openpages) if the Db2 database does not have sufficient memory.

The following SQL errors are in the <OP_HOME>/aurora/log files or the ObjectManager.log file:

```
com.ibm.db2.jcc.am.SqlException: DB2 SQL Error:
SQLCODE=-20442, SQLSTATE=57011, SQLERRMC=null, DRIVER=3.64.104
```

To resolve the problem, increase the memory that is available to the Db2 database by running the following commands, one by one, as the database instance owner:

```
db2 connect to <database_name> user <DB2_instance_owner> using <password>
db2 update db cfg for <database_name> using APPLHEAPSZ 512 APPL_MEMORY 80000
db2 terminate
db2start
```

Reload the configuration data. For more information, see [“Manually loading the configuration data after a new installation” on page 447](#).

If the problem still exists, keep doubling the sizes for the APPLHEAPSZ and APPL_MEMORY settings, up to 2048,000 or acquire more memory (RAM).

Example: APPLHEAPSZ 1024 APPL_MEMORY 160000

```
db2 connect to <database_name> user <DB2_instance_owner> using <password>
db2 update db cfg for <database_name> using APPLHEAPSZ 1024 APPL_MEMORY 160000
db2 terminate
db2start
```

Example: APPLHEAPSZ 2048 APPL_MEMORY 320000

```
db2 connect to <database_name> user <DB2_instance_owner> using <password>
db2 update db cfg for <database_name> using APPLHEAPSZ 2048 APPL_MEMORY 320000
db2 terminate
db2start
```

Manually loading the configuration data after a new installation

The installation program for IBM OpenPages with Watson automatically loads the application data and enables user access to the standard Cognos Analytics reports. In limited situations, you can manually load the level-0 schema.

Before you begin

IBM OpenPages with Watson must be installed.

The OpenPages services must be running.

About this task

If the loader file execution that occurs during the fresh installation has errors, you can correct the issues that caused the errors and then run the fresh installation loader file manually.

Procedure

To manually load the level-0 schema, use the following steps:

1. Log on to the OpenPages admin application server as a user with administrative privileges.
2. Go to the `<OP_HOME>/addon_module/loaderdata` directory.
3. Make a backup copy of the `schema_loader_properties.sh|.bat` file.
4. Open the original `schema_loader_properties` file in a text editor.
5. In the following line, update the password for the OpenPages Super Administrator to clear text.

```
SET OPXUserName=<Super_Administrator_user_name>
SET OPXUserPassword=*****
```

The default user name is `OpenPagesAdministrator`.

The password for the `OPXUserName` user is masked by asterisks (**). Replace the mask with clear text.

6. Save and close the file.
7. Go to the `<OP_HOME>/bin` directory.
8. Edit the `ObjectManager.properties` file and update the following settings as shown:

```
configuration.manager.vendor.mode=true
configuration.manager.disable.triggers=true
configuration.manager.force.update.object.strings=false
configuration.manager.force.update.application.strings=false
```

9. Save and close the file.
10. To load the default configuration, run the `openpages-level0-loader-data.sh|.bat` script.

Tip:

Redirect the output to a log file so that you can conveniently track the progress:

- Windows: `openpages-level0-loader-data.bat > openpages-level0-loader-data.log`
- Linux: `./openpages-level0-loader-data.sh > openpages-level0-loader-data.log`

The script takes some time to finish loading the data. For example, the data might take two hours to load.

11. Go to the `<OP_HOME>/bin` directory.
12. Edit the `ObjectManager.properties` file and update the following settings as shown:

```
configuration.manager.vendor.mode=false
configuration.manager.disable.triggers=false
```

13. Save and close the file.
14. Go to the `<OP_HOME>/addon_module/loaderdata` directory.
15. Open the `schema_loader_properties` file in a text editor.
16. In the following line, hide the clear text password for the OpenPages Super Administrator by changing it to asterisks (**).

```
SET OPXUserPassword=*****
```

17. Save and close the file.
18. Restart the OpenPages services.

Manually loading the configuration data after a migration

When you migrate IBM OpenPages with Watson to version 8.2, IBM OpenPages with Watson automatically loads the application data and enables user access to the standard Cognos Analytics reports. In limited situations, you can manually upgrade the loader configuration data.

Before you begin

IBM OpenPages with Watson must be installed.

The OpenPages services must be running.

About this task

If the upgrade loader files that are executed during the migration have errors, you can correct the issues that caused the errors and then run the upgrade loader files manually.

Procedure

1. Log on to the OpenPages admin application server as a user with administrative privileges.
2. Go to the `<OP_HOME>/installer/migration/upgrade/addon_module/loaderdata` directory.
3. Make a backup copy of the `schema_loader_properties.sh|.bat` file.
4. Open the original `schema_loader_properties` file in a text editor.
5. In the following line, update the password for the OpenPages Super Administrator to clear text.

```
SET OPXUserName=<Super_Administrator_user_name>  
SET OPXUserPassword=*****
```

The default user name is `OpenPagesAdministrator`.

The password for the `OPXUserName` user is masked by asterisks (`***`). Replace the mask with clear text.

6. Save and close the file.
7. Go to the `<OP_HOME>/bin` directory.
8. Edit the `ObjectManager.properties` file and update the following settings as shown:

```
configuration.manager.vendor.mode=true  
configuration.manager.force.update.object.strings=false  
configuration.manager.force.update.application.strings=false  
configuration.manager.disable.triggers=true
```

9. Save and close the file.
10. Depending on your upgrade path, run the scripts in the order that is listed:

Upgrade path	Windows files to run
7.3 to 8.2	<ul style="list-style-type: none">• <code>openpages-op730x-to-7400-loader-data.bat</code>• <code>openpages-op800x-to-8100-loader-data.bat</code>• <code>openpages-op810x-to-8200-loader-data.bat</code>• <code>op-sysviews-loader.bat</code>• <code>op-sampleWorkflows-upgrade-loader.bat</code>
7.4 or 8.0.0.1 to 8.2	<ul style="list-style-type: none">• <code>openpages-op800x-to-8100-loader-data.bat</code>• <code>openpages-op810x-to-8200-loader-data.bat</code>• <code>op-sysviews-loader.bat</code>• <code>op-sampleWorkflows-upgrade-loader.bat</code>

Upgrade path	Windows files to run
8.0.0.2 or a later 8.0.0.x fix pack to 8.2	<ul style="list-style-type: none"> • openpages-op800x-to-8100-loader-data.bat • openpages-op810x-to-8200-loader-data.bat • op-sysviews-loader.bat
8.1.x to 8.2	<ul style="list-style-type: none"> • openpages-op810x-to-8200-loader-data.bat

Upgrade path	Linux files to run
7.3 to 8.2	<ul style="list-style-type: none"> • openpages-op730x-to-7400-loader-data.sh • openpages-op800x-to-8100-loader-data.sh • openpages-op810x-to-8200-loader-data.sh • op-sysviews-loader.sh • op-sampleWorkflows-upgrade-loader.sh
7.4 or 8.0.0.1 to 8.2	<ul style="list-style-type: none"> • openpages-op800x-to-8100-loader-data.sh • openpages-op810x-to-8200-loader-data.sh • op-sysviews-loader.sh • op-sampleWorkflows-upgrade-loader.sh
8.0.0.2 or a later 8.0.0.x fix pack to 8.2	<ul style="list-style-type: none"> • openpages-op800x-to-8100-loader-data.sh • openpages-op810x-to-8200-loader-data.sh • op-sysviews-loader.sh
8.1.x to 8.2	<ul style="list-style-type: none"> • openpages-op810x-to-8200-loader-data.sh • op-sysviews-loader.sh

11. Go to the <OP_HOME>/bin directory.

12. Edit the ObjectManager.properties file and update the following settings as shown:

```
configuration.manager.vendor.mode=false
configuration.manager.disable.triggers=false
```

13. Save and close the file.

14. Go to the <OP_HOME>/installer/migration/upgrade/addon_module/loaderdata directory.

15. Open the schema_loader_properties file in a text editor.

16. In the following line, hide the clear text password for the OpenPages Super Administrator by changing it to asterisks (***) .

```
SET OPXUserPassword=*****
```

17. Save and close the file.

18. Restart the OpenPages services.

Manually loading the configuration data after a fix pack

When you apply a fix pack, IBM OpenPages with Watson automatically loads the application data. You can load the application configuration data manually, if needed.

Before you begin

The IBM OpenPages with Watson fix pack must be installed.

The OpenPages services must be running.

About this task

If errors occur when the fix pack loader files are loaded during the fix pack installation, you can correct the issues that caused the errors and then load the fix pack loader files manually.

Load the loader data up to and including the fix pack version that you are installing. Load the files in ascending order, starting with the earliest fix pack version where errors or warnings occurred.

For example, suppose that you are applying fix pack 8.2.0.3 and you never applied fix pack 8.2.0.2. Some warnings were logged for the 8.2.0.2 loader files, so you want to load the data manually. Run the following scripts in the following order:

- `<OP_HOME>/OpenPages/installer/maintenance/fix-pack-8-2-0-3/OP_HOME/addon_module/loaderdata/8-2-0-2_loader_data/openpages-8-2-0-2-loader-data.sh|.bat`
- `<OP_HOME>/OpenPages/installer/maintenance/fix-pack-8-2-0-3/OP_HOME/addon_module/loaderdata/8-2-0-3_loader_data/openpages-8-2-0-3-loader-data.sh|.bat`

In the following steps, `<latest_fix_pack_version>` is the fix pack version that you are installing and `<loader_data_version>` is the fix pack version loader data that you are loading manually.

Procedure

1. Log on to the OpenPages admin application server as a user with administrative privileges.
2. Go to the `<OP_HOME>/bin` directory.
3. Edit the `ObjectManager.properties` file and update the following settings as shown:

```
configuration.manager.vendor.mode=true
configuration.manager.force.update.object.strings=false
configuration.manager.force.update.application.strings=false
```

4. Save and close the file.
5. Go to the `<OP_HOME>/OpenPages/installer/maintenance/fix-pack-<latest_fix_pack_version>/OP_HOME/addon_module/loaderdata/<loader_data_version>_loader_data` directory.
6. Make a backup copy of the `schema_loader_properties.sh|.bat` file.
7. Open the original `schema_loader_properties` file in a text editor.
8. In the following line, update the password for the OpenPages Super Administrator (OPXUserName).

```
SET OPXUserPassword=*****
```

The password is masked by asterisks (***). Replace the mask with clear text.

9. Save and close the file.
10. Run the loader file script.

Windows

```
openpages-<loader_data_version>-loader-data.bat
```

Linux

```
chmod 755 openpages-<loader_data_version>-loader-data.sh
./openpages-<loader_data_version>-loader-data.sh
```

11. Go to the `<OP_HOME>/OpenPages/installer/maintenance/fix-pack-<latest_fix_pack_version>/OP_HOME/addon_module/loaderdata/<loader_data_version>_loader_data` directory.
12. Open the `schema_loader_properties` file in a text editor.

13. In the following line, hide the clear text password for the OpenPages Super Administrator by changing it to asterisks (***).

```
SET OPXUserPassword=*****
```

14. Save and close the file.
15. Repeat steps 5-14 for each fix pack in ascending order, up to and including the most recent fix pack that you are installing.
16. Go to the `<OP_HOME>/bin` directory.
17. Edit the `ObjectManager.properties` file and update the following settings as shown:

```
configuration.manager.vendor.mode=false
```

18. Save and close the file.
19. Restart the OpenPages services.

Dropping the OpenPages database for IBM Db2

You can drop the IBM OpenPages with Watson database. You can also uncatalog the node.

Procedure

1. Open a command or shell window.
2. For Windows users only, type the following command in the **Command Prompt** window to initialize the Db2 command line processor (CLP):

db2cmd

3. Run the following command:

```
db2 drop db <DATABASE_NAME>
```

Where `<DATABASE_NAME>` is the name of the OpenPages database.

For example, if the name of the OpenPages database is `op`, run `db2 drop database op`.

4. To uncatalog the node, run the `db2-uncatalog-node.bat | .sh` script.

Note: In most situations, uncataloging the node is unnecessary.

```
db2-uncatalog-node.bat | .sh <node_name>
```

Troubleshooting Oracle schema creation

If you encounter problems when you run the scripts to create the Oracle database schema during a fresh installation, you can run scripts to drop a portion or all of the schema objects.

Note: This information applies to non-TDE databases only.

- You can drop the schema objects that were created when you ran the non-DBA script (`op-database-product-install.sh | .bat`).

Use this option to remove all of the schema objects from the OpenPages database schema user. See [“Dropping OpenPages schema objects in an Oracle database” on page 453](#).

After you drop the schema objects, you can rerun the `op-database-product-install.sh | .bat` script. See [“Running the steps that do not require DBA privileges” on page 140](#).

- You can drop the database objects created by both the `op-database-dba-install.sh | bat` and `op-database-product-install.sh | .bat` scripts.

Use this option to remove all of the schema objects from the OpenPages database schema user, drop the tablespaces, and drop the OpenPages user. See [“Dropping the full schema in an Oracle database” on page 453](#).

After you complete this step, rerun the scripts to create the OpenPages database schema objects. See [“OpenPages database schema creation for Oracle” on page 132](#).

Dropping OpenPages schema objects in an Oracle database

You can run the `AuroraDbDelete.sql` script to remove all of the schema objects from the OpenPages database schema user.

Procedure

1. Log on to the Oracle database server as a user with administrative privileges. Or, log on to a server that has access to the database server and has SQL*Plus.
2. Go to the `/OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/INSTALL_SCRIPTS` directory.
3. Verify that you have execute permission on the files in the `INSTALL_SCRIPTS` directory. If not, change the permission on the file by using the **chmod** command.
4. Log on to SQL*Plus as the OpenPages database user.
5. Use the `spool` command to create a log file.

```
spool <log_file_directory>/<log_file_name>
```

Ensure that you have write permission on the `<log_file_directory>`.

Example:

```
spool /tmp/AuroraDbDelete.log
```

6. Run the `AuroraDbDelete.sql` script.

```
@AuroraDbDelete.sql
```

7. Log out of SQL*Plus.

Dropping the full schema in an Oracle database

You can run the `init-db-cleanup.sql` script to drop the OpenPages database schema. The script drops the objects that the `op-database-dba-install.sh|.bat` and `op-database-product-install.sh|.bat` scripts created.

About this task

The `init-db-cleanup.sql` script drops the schema and removes the OpenPages table spaces.

Procedure

1. Log on to the Oracle database server as a user with administrative privileges.
2. Go to the `/OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/INSTALL_SCRIPTS` directory.
3. Verify that you have execute permission on the files in the `INSTALL_SCRIPTS` directory. If not, change the permission on the file by using the **chmod** command.
4. Log on to SQL*Plus as the OpenPages database user.
5. Run the `init-db-cleanup.sql` script.

Syntax:

```
sqlplus /nolog @sql-wrapper init-db-cleanup.sql <log_file> <oracle_tns_alias> <sysdba_user>  
<sysdba_password> <op_user>
```

Table 79. Parameters of the <i>init-db-cleanup.sql</i> script for Oracle databases	
Parameter	Description
<log_file>	Optional: The path and name of a log file
<oracle_tns_alias>	The TNS alias of the Oracle database instance
<sysdba_user>	A user with SYSDBA privileges
<sysdba_password>	The password of the SYSDBA user If the password contains special characters, surround the password in quotation marks: <ul style="list-style-type: none"> Windows: "password" Linux: 'password'
<op_user>	The OpenPages schema owner

For example:

- Windows:

```
sqlplus /nolog @sql-wrapper.sql init-db-cleanup.sql log_file.txt OP system
openpages "openpages"
```

- Linux:

```
sqlplus /nolog @sql-wrapper.sql init-db-cleanup.sql log_file.txt OP system
openpages 'openpages'
```

What to do next

Run the database schema creation scripts in a clean database environment. See [“OpenPages database schema creation for Oracle” on page 132](#).

Dropping the Cognos content store (Oracle)

You can drop the Cognos content store schema objects.

Procedure

1. Shut down all OpenPages components: application servers (admin and non-admin), reporting servers (active and standby), and the search server.
For more information, see [Chapter 12, “Starting and stopping servers,” on page 309](#).
2. Log on to the Oracle database server as a user with administrative privileges. Or, log on to a server that has access to the database server and has SQL*Plus.
3. Go to the /OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/INSTALL_SCRIPTS directory.
4. Log on to SQL*Plus as the Cognos database user.
5. Use the spool command to create a log file.

```
spool <log_file_directory>/<log_file_name>
```

Ensure that you have write permission on the <log_file_directory>.

Example:

```
spool /tmp/AuroraDbDelete.log
```

6. Run the AuroraDbDelete.sql script.


```
@AuroraDbDelete.sql
```

7. Log out of SQL*Plus.

Updating the services for multiple Db2 instances

IBM Db2 database instances must be able to communicate through the network. If you have multiple Db2 instances on the same computer, ensure that the SVCENAME and listener port are configured. Otherwise, connection errors might occur.

To verify that the Db2 database instances are configured for network communication:

- DB2SET must show TCPIP for the DB2COMM setting.
- The SVCENAME in the DBM configuration must show a valid TCP service name and TCP port number.

If you changed either the Db2 registry (DBSET) or the Database Manager configuration, ensure that you stop and restart Db2.

Procedure

1. Log on to the database server as the Db2 instance owner.
2. To reserve a TCP port for the service, append the information to the services file.

On Windows, edit the %systemroot%\system32\drivers\etc\services file

On Linux, edit the /etc/services file.

To reserve TCP port 5500 for the service named *db2c_opdb*, append the following line to the end of the services file:

```
db2c_opdb 5500/tcp
```

3. Update the database manager configuration.

db2 update database manager configuration using svcename 55000

4. Ensure that TCP communication is set for the database instance.

```
db2cmd -i -w
db2set DB2COMM=npipe,tcpip
db2stop
db2start
```

5. Stop and then restart the Db2 server.

```
db2stop
db2start
```

OP-03620: The Reporting Schema has not been instantiated error

You log on to the IBM OpenPages with Watson home page, and the following error message is displayed.





The Home Page cannot be viewed without a valid Reporting Schema.
Please contact your System Administrator. OP-03620:
The Reporting Schema has not been instantiated. Please instantiate it
before executing this operation.

This error occurs if the reporting schema has not yet been created.

To resolve the problem, enable **System Admin Mode**, and generate the reporting schema.

Procedure

1. In a web browser, open OpenPages with Watson.
`http://<openpages_server>:<port>/openpages`
2. Log on to the application as a user with administrative privileges.

3. Click , and then click **Enable System Admin Mode**.
4. Click  > **System Configuration > Reporting Schema**.
5. Click **Create**.
6. After the create operation finishes, click  > **Disable System Admin Mode**.
7. Click  > **Cognos Analytics > Reporting Framework Generation**.
8. On the **Reporting Framework** page, click **Update**.
9. In the **Reporting Framework Generation** panel, select **Framework Model** and **Labels** and other options you want for the relational data model.
10. Click **Submit**.
11. To view the progress of the update, click **Refresh**.

The **Percent Complete** column on the **Reporting Framework** table updates the percentage of completion.

Issues when importing databases

When you import the IBM OpenPages with Watson database during an upgrade or migration, you might see an error as a result of the default data file size.

If an error occurs, increase the default data file size as follows.

1. On a computer that has SQL*Plus, log on as a user, such as SYSTEM, who has database administration permissions.
2. Run the following SQL statements:

```
ALTER TABLESPACE INDX ADD DATAFILE
    'C:\app\Administrator\oradata\OP\INDX02.DBF'
    SIZE 128 M AUTOEXTEND ON    NEXT 128 M MAXSIZE 34359721984;

Alter database datafile 'C:\app\Administrator\oradata\OP\AURORA.DBF'
resize      2000m;
```

Logging in to Cognos Analytics fails

If you cannot log in to Cognos Analytics after you add a reporting server to an OpenPages deployment, you might need to check that the application URL is set correctly.

About this task

Follow these steps if you cannot log in to Cognos Analytics and the following error is issued:

```
java.net.MalformedURLException: For input string: "undefined"
```

Procedure

1. Go to the <COGNOS_HOME>/configuration directory.
2. Open the OpenPagesSecurityProvider_OpenPagesSecurityRealm.properties file in a text editor.
3. Ensure that the value for the openpages.application.url property matches the OpenPages application URL on the admin application server. Make the necessary change and save the file.
4. Restart Cognos Analytics.

Cognos content store import fails

If you use the database export and import option to restore the IBM Cognos content store, the import might fail if the table space name differs in the target environment.

To resolve this issue, you must update the table space name in the target environment:

1. Check the table space name in the target environment.

- a. Log on as an OpenPages user.
- b. Run the following command:

```
select tablespace_name from user_tablespaces;
```

2. Update the table space name.

- a. Log on as SYSTEM using SQL*Plus.
- b. Run the following scripts:

```
alter tablespace ctn RENAME TO cognos;
```

3. Drop the Cognos database schema.

- a. Go to the /OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/INSTALL_SCRIPTS directory.
- b. Log on to SQL*Plus as the Cognos database user.
- c. Use the spool command to create a log file.

```
spool <log_file_directory>/<log_file_name>
```

Ensure that you have write permission on the <log_file_directory>.

Example:

```
spool /tmp/AuroraDbDelete.log
```

- d. Run the AuroraDbDelete.sql script.

```
@AuroraDbDelete.sql
```

- e. Log out of SQL*Plus.

4. Go the /OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/INSTALL_SCRIPTS directory, and run the following script:

```
impdp <system_user>/\"<system_password>\"@<alias>  
full=Y file=<filename.dmp> log=<filename.log>  
directory=<OP_DATAPUMP_DIRECTORY>  
fromuser=<cognos_user> touser=<cognos_user> EXCLUDE=INDEX
```

Updating the Oracle client path on the reporting server

On a Linux system that uses an Oracle database, if you change the Oracle client location after you install Cognos Analytics and IBM OpenPages with Watson, then you must update the Oracle client path on the reporting server. To update the Oracle client path, edit the PATH and LD_LIBRARY_PATH environment variables in the BMTScriptPlayer.sh file.

Procedure

1. On the reporting server, navigate to the <COGNOS_HOME>/bin directory, and open the BMTScriptPlayer.sh file.
2. Update the Oracle client path in the following environment variables: PATH and LD_LIBRARY_PATH.

3. After you update the `BMTScriptPlayer.sh` file, verify that you can generate the OpenPages framework.

Issues when you use IBM Installation Manager on Linux

When you use the IBM Installation Manager on the Linux operating system to install IBM OpenPages with Watson, then an error message might be displayed.

Add the following line to the `IBMIM.ini` file, which you can find in `<installation location>/eclipse: -Dorg.eclipse.swt.internal.gtk.cairoGraphics=false`. Save the file and restart IBM Installation Manager.

Issues with IBM Db2 and Oracle after upgrading to RHEL 7.2

When you are using Red Hat Enterprise Linux 7.2, you might encounter issues with IBM Db2 and Oracle due to a known issue in RHEL 7.2.

For example, the OpenPages database instance on Db2 might crash with the following error displayed by the `db2diag` tool:

```
CALLER : OS, -, unspecified_system_function      OSERR: EIDRM (43)

2016-09-29-11.18.10.184984-240 I2604417E2069      LEVEL: Severe (OS)
PID       : 27510      TID : 140561960920832 PROC : db2sysc 0
INSTANCE: db2inst1      NODE : 000      DB : OPX
HOSTNAME: op-host-01
EDUID    : 197      EDUNAME: db2agntdp (OPX ) 0
FUNCTION: DB2 UDB, oper system services, sqlWaitEDUWaitPost, probe:100
MESSAGE : ZRC=0x8300002B=-2097151957
```

To fix the issue, edit the `/etc/systemd/logind.conf` file, set `RemoveIPC=no`, and then restart the corresponding service or reboot.

For more information, see <https://access.redhat.com/solutions/2062273>.

libdb2.so cannot be loaded

When you are using Linux for the reporting server, you might get an error that `libdb2.so` cannot be loaded.

```
UDA-SQL-0569 library to control program function (libdb2.so)
can not be loaded
UDA-SQL-0571 The operating system returned an error message (libpam.so.0:
can not open shared object file: No such file or directory).
```

To fix the issue, update `pam.x86_64` and then install `pam.i686`. For example, run `yum install pam.x86_64` and then run `yum install pam.i686`.

Data validation errors when installing Loss Event Entry

If data validation errors about existing data occur when you install IBM OpenPages Loss Event Entry, review the log files.

The log files for OpenPages Loss Event Entry are located in `<OP_HOME>/LossEventEntry/logs/`.

Validation errors can occur when OpenPages Loss Event Entry data exists in the OpenPages database.

If you chose to load the data automatically, run the OpenPages Loss Event Entry installer again and use the option to manually load the data. When the installation completes, load the data manually. You might see errors about existing data, but you can ignore them.

If you chose to load the data manually and you see errors about existing data, you can ignore them.

For information about installing OpenPages Loss Event Entry, see [Chapter 17, “Loss Event Entry,”](#) on page 375.

Memory validation step fails for an Oracle database

When you install OpenPages with an Oracle database, you get an error that the memory validation step failed.

OpenPages uses Automatic Shared Memory Management (ASMM) and requires the following configuration:

- **SGA Size:** 1024
- **PGA Size:** 768
- **Block Size:** 8192
- **Processes :** 250

Review these requirements with your database administrator. If your environment meets these requirements, for example if you are using an alternative method for managing memory, you can override the memory check and complete the installation.

1. Open the `sql-wrapper.sql` file in the `/OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/INSTALL_SCRIPTS` directory.
2. Change the `dba_override_asmm_check` property to Y.

```
define dba_override_asmm_check='Y'
```

3. Run the `op-validate-dba-install.sh | .bat` script.
4. Resume the installation of OpenPages.

Configuring the Oracle data pump directory

For an Oracle deployment, you can run a script to create or update the Oracle data pump directory location.

For example, if the database backup or restore process is not successful, configure the Oracle data pump storage directory, and then run the backup or restore process again.

Procedure

1. Go to the `/OP_<version>_Main/IBM_Java/<OS>/java_8.0_64/lib` directory and copy the `tools.jar` file to the `<COGNOS_HOME>/ibm-jre/jre/lib` directory.
2. Log on to a computer that has the SQL*Plus utility and a connection to the OpenPages CommandCenter database instance.
3. Go to the `/OP_<version>_Main/OP_<version>_Configuration/Database/ORACLE/UPGRADE_SCRIPTS` directory.
4. From the command line, run the `update-datapump-directory.sql` script.

```
sqlplus /nolog @sql-wrapper update-datapump-directory <log_file_name>  
<tns_name_alias> SYSTEM <password> <create/update>  
<directory_location> <user_name>
```

The following table describes the variables in the script.

Table 80. Descriptions for variables in the <code>update-datapump-directory.sql</code> file	
Variable	Description
<code><log_file_name></code>	The user-defined name of the log file that the script creates to store information.
<code><tns_name_alias></code>	The database Oracle TNS entry that is used by the OpenPages CommandCenter database instance on the reporting server computer.

Table 80. Descriptions for variables in the <code>update-datapump-directory.sql</code> file (continued)	
Variable	Description
<code><password></code>	<p>The password for the Oracle SYSTEM user account.</p> <p>If the password contains special characters, surround the password in quotation marks:</p> <ul style="list-style-type: none"> • Windows: "password" • Linux: 'password'
<code><create/update></code>	Use <code>create</code> to create the directory or <code>update</code> to update its location.
<code><directory_location></code>	The full directory path to the location on the database server where the backup files are stored.
<code><user_name></code>	The user name of the Cognos account for the OpenPages CommandCenter database schema (content store).

Example:

```
sqlplus /nolog @sql-wrapper update-datapump-directory.sql C:\temp\update-datapump.log
OP SYSTEM "password" create d:\cc_backup cognos
```

```
sqlplus /nolog @sql-wrapper update-datapump-directory.sql /tmp/log
op SYSTEM 'password' create TESTDIR openpage
```

CM-CFG-5114: The Cognos service does not start

When you start Cognos Analytics, it fails to start and you see a message that the content store is locked.

CM-CFG-5114 An error occurred while locking the content store database.

For example:

```
CM-CFG-5063 A Content Manager configuration error was detected
while connecting to the content store.
CM-CFG-5114 An error occurred while locking the content store database.
```

This error is a known issue in Cognos Analytics. For information about how to resolve the issue, see [Problems With Starting the Cognos Service After Running the OpenPages OPCCBackup Utility \(Error: CM-CFG-5114\)](#).

CM-CAM-4005 Unable to authenticate

You might see a CM-CAM-4005 Unable to authenticate error in the reporting server log during the Import Solutions Reports phase of the installation.

This error can happen when the reporting server is installed on the same computer as an IBM OpenPages application server and the computer is running Linux.

The error occurs because the Cognos startup script (`cogconfig.sh`) uses the Java that is specified by `$JAVA_HOME`. When the reporting server is installed on the same computer as another OpenPages component, `$JAVA_HOME` might not point to the Java that is needed by Cognos Analytics.

You can resolve the problem by modifying the startup script.


1. Open the `<COGNOS_HOME>/bin64/cogconfig.sh` script in a text editor.


2. Comment out the first, second, and fourth lines. Leave the third line unchanged.

```
#if [ "$JAVA_HOME" = "" ]  
#then  
    JAVA_HOME=./jre  
#fi
```

3. Save the file.
4. Resume the installation.

Agent does not exist on remote server

When you click  in a server card of the installation app, the server card might display the following message: Agent does not exist at <directory> on <remote-server-name>.

This issue occurs if the **Agent Directory** field was changed on the remote server's card after **Validate** was clicked and the original agent on the remote server was not stopped before the **Agent Directory** field was changed. If **Validate** is clicked again, the installation proceeds using the original agent. The error displays if you click  in that server's card because no agent exists at the specified location.

To fix the issue, complete the following steps:

1. Log on to the remote server as the installation user and manually stop the original agent:

```
# cd <original-agent-directory>  
# npm stop
```

2. Go to the installation directory:

```
# cd <original-agent-directory>/install/<platform>
```

Where <platform> is Linux or Windows.

3. Run the uninstall script:

- Windows

```
uninstall.bat
```

- Linux:

```
./uninstall.sh
```

4. Delete the original agent directory.
5. Return to the installation app and click **Validate**.

The agent software is installed in the new directory location and the agent software starts.

Errors during database server validation (Db2)

If you have insufficient memory available on your IBM Db2 server you might encounter a functional issue during the installation of IBM OpenPages with Watson. You might see errors during the database server validation process.

The functional issue can be resolved by applying the workaround that is described in the following technote: [IT19442: A DB2 FENCED ROUTINE MAY FAIL WITH ERROR SQL1646N DUE TO SHARED MEMORY PERMISSION PROBLEMS](http://www.ibm.com/support/docview.wss?uid=swg1IT19442) (<http://www.ibm.com/support/docview.wss?uid=swg1IT19442>).

However, insufficient memory allocation on your Db2 server can also lead to significant performance problems. Allocate more memory to the Db2 server before you continue with the installation of IBM OpenPages with Watson.

Rollback errors during a database upgrade

When you upgrade the OpenPages database, the upgrade script reports the following error: [exec] Load PL/SQL package failed. Please check log file..

Review the AuroraProcCreate.log file. The AuroraProcCreate.log file that you need to check depends on the release that the upgrade script was applying when the error occurred. If you're upgrading across multiple releases, such as 7.3 to 8.2, you might need to look in multiple AuroraProcCreate.log files.

Examples:

- If you are upgrading from OpenPages 8.1 to OpenPages 8.2, look at the AuroraProcCreate.log file in the /OP810X_TO_OP8200 directory. For Db2 the path is /OP_<version>_Main/OP_<version>_Configuration/Database/DB2/UPGRADE_SCRIPTS/OP810X_TO_OP8200
- If you are upgrading from OpenPages 7.3 to OpenPages 8.2, look at the AuroraProcCreate.log file in each of the following directories: /OP730X_TO_OP7400, /OP740X_TO_OP8100, and /OP810X_TO_OP8200.

Note: The directory names change for each OpenPages release.

In the AuroraProcCreate.log file, look for a message that is similar to the following example:

```
SQL0911N The current transaction has been rolled back because of a deadlock
or timeout. Reason code "2". LINE NUMBER=1. SQLSTATE=40001
```

If you see this message, it's likely that one or more OpenPages components were running during the database upgrade.

To resolve the error, do the following steps:

1. Shut down all OpenPages components. For more information, see [Chapter 12, “Starting and stopping servers,”](#) on page 309.
2. Rerun the database upgrade script that failed with the [exec] Load PL/SQL package failed. Please check log file error.

Note: If you are upgrading across multiple releases, you might need to set opx_override_ver_check to Y. For more information, see [“Preparing for the database upgrade \(Db2\)”](#) on page 227.

Error: Cannot run schema upgrade

When you install a fix pack or interim fix, you see an error during validation that the schema cannot be upgraded.

The error message you see is similar to the following text:

```
OP schema version is "<previous_version>", but installer cannot
run schema upgrade since 'install_db' is 'done' in [db] section.
Schema upgrade to <new_version> must be completed manually.
```

The message can occur in the following cases:

- If you are using the installation app:
 - The **Install Database** option is set to **Already Installed** or **Only Non-DBA**
 - The database has not been updated to the fix pack or interim fix version
- If you are using silent mode:
 - The install_db parameter is set to done or nondba
 - The database has not been updated to the fix pack or interim fix version

To resolve the error, do one of the following steps:

- Run the scripts to update the database. See [“Update the OpenPages database manually \(Db2\)”](#) on page 282 or [“Update the OpenPages database manually \(Oracle\)”](#) on page 289.

If you are using the installation app, complete the database update, open your deployment, and then click **Validate** to confirm that the error is resolved.

If you are using silent mode, complete the database update and then run the silent install again.

- Change the deployment properties to do the database update.

If you are using the installation app, set the **Install Database** option to **Full Database**. Enter DBA credentials on the **Database Server** card, click **Validate**, and then continue with the installation process.

If you are using silent mode, set the `install_db` parameter to `full`. Enter DBA credentials in the `dba_username` and `dba_password` parameters, and then run the silent install again.

Loading the application and object strings

If errors occurred when the application data was loaded during the fix pack installation, you can load the application strings manually.

Procedure

1. Log in to the application server as a user with administrative privileges.
2. Go to the `<OP_HOME>/bin` directory.
3. Edit the `ObjectManager.properties` file and update the following settings as shown:

```
configuration.manager.vendor.mode=true
```

4. Save and close the file.
5. Load the application strings.

Run the following command:

```
ObjectManager.cmd|.sh l c <OpenPages Administrator user>  
<OpenPages Administrator password> <OP_HOME>/installer/maintenance/  
fix-pack-8.2.0.<x>/OP_HOME/addon_module/loaderdata/ common-app-strings-<version>
```

6. After the `ObjectManager` loading is complete, review the log and make sure that the process completed.
7. Go to the `<OP_HOME>/bin` directory.
8. Edit the `ObjectManager.properties` file and update the following settings as shown:

```
configuration.manager.vendor.mode=false
```

9. Save and close the file.

One or more required WLP features unavailable

When you install a fix pack or interim fix, you see an error that some required WebSphere Liberty features are unavailable.

The error message you see is similar to the following text:

```
One or more required WLP features for version <version> are unavailable.  
Download the features manually and copy them to the server.
```

The message can occur in the following situation:

- Your application server does not have internet access.
- You updated WebSphere Liberty features manually after you installed OpenPages.

To resolve the error, do the following steps:

- Do steps 1-6 in the following topic: [“Updating WebSphere Liberty features manually” on page 154.](#)
- Continue the fix pack or interim fix installation.

If you are using the installation app, click **Validate**, and then continue with the installation process.

If you are using silent mode, run the silent install again.

OpenPages reports are not displayed in IBM Cognos Analytics

After you install or upgrade IBM OpenPages with Watson, if you do not see the OpenPages reports and packages in the IBM Cognos Analytics, you can import them manually.

For more information about importing content, see the *Cognos Analytics Administration and Security Guide*.

Procedure

1. If you use solutions, get the latest version of the solutions report package.
 - a) Back up the following file if it exists: `<COGNOS_HOME>/deployment/OpenPages_Solutions_V6.zip`.
 - b) Locate the solutions package file for the database that you are using. The file is located in the following directory:
 - IBM Db2: `OP_<version>_Main/OP_<version>_Configuration/Modules/Upgrade/ORM/DB2/OpenPages_Solutions_V6.zip`
 - Oracle: `OP_<version>_Main/OP_<version>_Configuration/Modules/Upgrade/ORM/Oracle/OpenPages_Solutions_V6.zip`
 - c) Copy the `OpenPages_Solutions_V6.zip` file to the following directory on the Cognos server: `<COGNOS_HOME>/deployment`. Overwrite the existing file.

Note: You do not need to copy the platform reports package from the installation media. The package is placed on the Cognos server automatically when you install OpenPages.

2. Log on to IBM Cognos Analytics as a user with administrative privileges..
 - In the Task Focused UI, click **Analytics**.
 - Or, go to the following URL: `http://<hostname>/ibmcognos/bi`
Where `<hostname>` is the name of the Cognos server.
3. Click **Manage > Administration Console** to launch the **IBM Cognos Administration** page.
4. Click the **Configuration** tab, and then click **Content Administration**.

Tip: To access this area in IBM Cognos Administration, you must have the required permissions for the **Administration** secured feature.

5. On the toolbar, click **New Import**.
6. From the **Deployment archive** list, select the package that you want to import.
 - To import the platform reports, select the **OpenPages Platform v6** package.
 - To import the solutions reports, select the **OpenPages_Solutions_v6** package.
7. Click **Next**.
8. Type a unique name, an optional description, and a screen tip for the deployment archive, select the folder where you want to save it, and then click **Next**.
9. In the **Public folders, directory and library content** box, select the package that you are importing, and then click **Next**.
 - If you are importing the platform reports, select **OpenPages Platform v6**.
 - If you are importing the solutions reports, select **OpenPages_Solutions_v6**.
10. On the **Specify the general options** page, accept the default options and click **Next**.
11. On the **Review the summary** page, review the settings and click **Next**.
12. On the **Select an action page**, click **Finish**.
13. On the **Run with options** page, click **Run** and then, on the **IBM Cognos software** page, click **OK**.

14. To view the imported packages and reports, click the **Home** icon, and select the folder where you imported them.

Results

You can now open the OpenPages reports in Cognos Analytics.

Troubleshooting IBM OpenPages with Watson solutions

Solve common problems that might occur when you install or remove the IBM OpenPages with Watson solutions.

Reporting Framework generation fails with BC error

During installation, Reporting Framework generation might fail with a BC (8.2.0.2 or later) or CAMCryptoBC error.

About this task

A BC error occurs if the `bcprov-jdk15to18-1.68.jar` file that is provided with IBM OpenPages with Watson is missing from the Java location that is used by the IBM Cognos server or if the `BouncyCastleProvider` is not registered in the JRE master security provider file, `java.security`.

The following circumstances can cause the error:

- During the OpenPages upgrade process, the Java that is used for the Cognos server was changed to version 1.8.
- During the Cognos fix pack installation process, the Java that is used for the Cognos server was updated or overwritten.
- The Java used for the Cognos server was updated.

To resolve the issue, check each reporting server in your environment. Verify that the JRE that is used to run the Cognos software contains the `bcprov-jdk15to18-1.68.jar` file that is supplied with OpenPages. If the JRE does not have a copy of the `bcprov-jdk15to18-1.68.jar` file, you can get a copy of the file from any OpenPages application server in the `<OP_HOME>/temp/jre/lib/ext/` directory.

The names of the following items changed in 8.2.0.2:

- `bcprov-jdk14-145.jar` is `bcprov-jdk15to18-1.68.jar` in 8.2.0.2 or later
- `org.bouncycastle145.jce.provider.BouncyCastleProvider` is `org.bouncycastle.jce.provider.BouncyCastleProvider` in 8.2.0.2 or later
- `CAMCryptoBC` is `BC` in 8.2.0.2 or later

Procedure

1. If the Cognos software is using the JRE that is installed with Cognos, do the following steps:

- a) Copy the `bcprov-jdk15to18-1.68.jar` file to the `<COGNOS_HOME>/analytics/jre/lib/ext` directory.

Note: If you are using Cognos Analytics 11.1.5 or later, copy the file to `<COGNOS_HOME>/analytics/ibm-jre/lib/ext`.

- b) Register the `BouncyCastleProvider` in the JRE master security provider file, if it is not already registered.

To register the provider, add the following line to the `java.security` file that is stored in the `<COGNOS_HOME>/analytics/jre/lib/security` directory.

```
security.provider.<#>=
    org.bouncycastle.jce.provider.BouncyCastleProvider
```

Note: If you are using Cognos Analytics 11.1.5 or later, the `java.security` file is in the `<COGNOS_HOME>/analytics/ibm-jre/lib/security` directory.

Where: The number sign, `<#>`, is one increment above the last number in the list. For example, `security.provider.9`.

2. If the Cognos software is using the JRE that is installed with IBM SDK, Java Technology Edition, do the following steps:

- a) Copy the `bcprov-jdk15to18-1.68.jar` file to the `<JAVA_HOME>/lib/ext` directory.
- b) Register the `BouncyCastleProvider` in the JRE master security provider file, if it is not already registered.

To register the provider, add the following line to the `java.security` file that is stored in the `<JAVA_HOME>/lib/security` directory.

```
security.provider.<#>=
    org.bouncycastle.jce.provider.BouncyCastleProvider
```

Where: The number sign, `<#>`, is one increment above the last number in the list. For example, `security.provider.9`.

3. If the Cognos software is using a JRE that is installed in another location on the reporting server, do the following steps:

Replace `<JAVA_LOCATION>` with the directory where the JRE is installed.

- a) Copy the `bcprov-jdk15to18-1.68.jar` file to the `<JAVA_LOCATION>/lib/ext` directory.
- b) Register the `BouncyCastleProvider` in the JRE master security provider file, if it is not already registered.

To register the provider, add the following line to the `java.security` file that is stored in the `<JAVA_LOCATION>/lib/security` directory.

```
security.provider.<#>=org.bouncycastle.jce.provider.BouncyCastleProvider
```

Where: The number sign, `<#>`, is one increment above the last number in the list. For example, `security.provider.9`.

Enabling the new timesheet entry helper

If you disabled the new Timesheet Entry Helper in 8.0.x, you can re-enable it.

About this task

This procedure does not impact the Timesheet Approval Helper.

Procedure

1. Log on to the admin application server as a user with administrative privileges.
2. Open a command prompt or shell.
3. Go to the `<OP_HOME>/Module/loaderdata/IAM` directory.
4. Open the `schema_loader_modules_properties.sh | .bat` file in a text editor.

Update the following properties:

```
OBJMGR_HOME=<full_path_to_OP_HOME/bin>
PATCH_LOADER_DATA=<full_path_to_the_IAM_directory>
```

```
OPXUserName=<Super_Administrator_user_name>  
OPXUserPassword=<Super_Administrator_password>
```

Tip: In the installation app, the super administrator is set on the **Database Server** card in the **OP Admin Username** field. You can also find the user name in the `deploy.properties` file in the `op_admin_username` parameter.

For example:

- Windows:

```
OBJMGR_HOME=C:\OP\OpenPages\bin  
PATCH_LOADER_DATA=C:\OP\OpenPages\Module\loaderdata\IAM  
OPXUserName=OpenPagesAdministrator  
OPXUserPassword=password
```

- Linux:

```
OBJMGR_HOME=/home/opuser/OP/OpenPages/bin  
PATCH_LOADER_DATA=/home/opuser/OP/OpenPages/Module/loaderdata/IAM  
OPXUserName=OpenPagesAdministrator  
OPXUserPassword=password
```

5. Run the following script to install and enable the Timesheet Entry Helper:

- Windows:

```
enable-new-timesheet-entry-helper.bat
```

- Linux:

```
./enable-new-timesheet-entry-helper.sh
```

6. Edit the `schema_loader_modules_properties.sh | .bat` file. Set the `OPXUserPassword` property to `****`, for security reasons.

What to do next

Update profiles to use the Timesheet Entry Helper on the Home page and in the **My Reports** list.

Manually installing IBM OpenPages solutions

If your deployment is at version 8.2.x and it does not have IBM OpenPages solutions, you can add them to your deployment.

Before you begin

IBM OpenPages with Watson 8.2.x is installed.

Solutions are not installed.

About this task

Do this task to do a fresh installation of solutions by running scripts.

You can also install solutions by using the installation app. For more information, see [“Adding solutions to a deployment”](#) on page 418.

Procedure

1. Log on to the OpenPages admin application server as a user with administrative privileges.
2. Go to the
OP_<version>_Main\OP_<version>_Configuration\Modules\Fresh_Install\loaderdata directory.
3. Make a backup copy of the `schema_loader_properties.sh | .bat` file.

4. Open the original `schema_loader_properties` file in a text editor.
5. In the following line, update the password for the OpenPages Super Administrator to clear text.

```
SET OPXUserName=<Super_Administrator_user_name>  
SET OPXUserPassword=*****
```

The default user name is `OpenPagesAdministrator`.

The password for the `OPXUserName` user is masked by asterisks (**). Replace the mask with clear text.

6. Save and close the file.
7. Go to the `<OP_HOME>/bin` directory.
8. Edit the `ObjectManager.properties` file and update the following settings as shown:

```
configuration.manager.vendor.mode=true  
configuration.manager.disable.triggers=true  
configuration.manager.force.update.object.strings=true  
configuration.manager.force.update.application.strings=true
```

9. Save and close the file.
10. Run the `openpages-solutions-schema-loader.sh | .bat` script.

Tip: Redirect the output to a log file so that you can conveniently track the progress:

- Windows: `openpages-level0-loader-data.bat > openpages-level0-loader-data.log`
- `./openpages-level0-loader-data.sh > openpages-level0-loader-data.log`

Windows:

```
openpages-solutions-schema-loader.bat > openpages-solutions-schema-loader.log
```

Linux:

```
./openpages-solutions-schema-loader.sh > openpages-solutions-schema-loader.log
```

11. Check the log file for any errors.
12. Optional: Load the approval app schema by running the `Load_End_User_App_Schema.sh | .bat` script.

For more information, see step 2 in [“Loading the approval app profile” on page 370](#)

13. Go to the `<OP_HOME>/bin` directory.
14. Edit the `ObjectManager.properties` file and update the following settings as shown:

```
configuration.manager.vendor.mode=false  
configuration.manager.disable.triggers=false  
configuration.manager.force.update.object.strings=false  
configuration.manager.force.update.application.strings=false
```

15. Save and close the file.
16. Go to the `OP_<version>_Main\OP_<version>_Configuration\Modules\Fresh_Install\loaderdata` directory.
17. Open the `schema_loader_properties` file in a text editor.
18. In the following line, hide the clear text password for the OpenPages Super Administrator by changing it to asterisks (**).

```
SET OPXUserPassword=*****
```

19. Save and close the file.
20. Restart the OpenPages services.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service. This document may describe products, services, or features that are not included in the Program or license entitlement that you have purchased.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Location Code FTO
550 King Street
Littleton, MA

01460-1250
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

Copyright

Licensed Materials - Property of IBM Corporation.

© Copyright IBM Corporation, 2003, 2023.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written.

These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Trademarks

IBM, the IBM logo and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at ["Copyright and trademark information."](#)

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

The registered trademark Linux is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Red Hat®, JBoss®, OpenShift®, Fedora®, Hibernate®, Ansible®, CloudForm, RHCA®, RHCE®, RHCSA®, Ceph®, and Gluster® are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.



Index

A

- access-web-browser [180](#)
- administrator
 - Super Administrator [144](#)
- agents
 - restoring [441](#)
- AL32UTF8 character set [95](#)
- all-in-one deployment [109](#)
- application files
 - migrating [201](#)
- application readiness [311](#)
- application server
 - configuring single sign-on [321](#), [325](#), [326](#), [329](#), [331](#), [336](#), [339](#), [344](#)
 - default port [124](#)
 - paging file size and [176](#)
 - post-installation tasks [175](#)
 - scaling [31](#)
 - server topology [28](#)
 - software prerequisites [33](#)
- application servers
 - prerequisite software [35](#)
 - prerequisite tasks for Oracle database [99](#)
 - starting Windows service [309](#)
 - stopping Windows service [311](#)
 - users and groups for Linux servers [84](#), [99](#)
- application, starting [309](#)
- approval app
 - data types [362](#)
 - deploying [361](#)
 - excluding specific object types [364](#), [365](#)
 - field types [362](#)
 - fields and objects [363](#)
 - loading profile [370](#)
 - loading triggers [369](#)
 - upgrading [371](#)
- architecture
 - platform [27](#)
- ASM [136](#)
- AuroraDbDelete.sql [244](#), [250](#), [454](#)
- automatic restart [309](#)

B

- backups
 - before applying a fix pack [280](#)
 - before migrating [198](#)
 - Dojo toolkits for fix packs [281](#)
 - overview for fix packs [280](#)
 - solutions helpers for fix packs [281](#)
- BC error
 - fixing [465](#)
- bcprov-jdk*.jar [465](#)
- BouncyCastleProvider [465](#)

C

- CAMCryptoBC error
 - fixing [465](#)
- cataloging
 - OpenPages database [86](#)
- certificates
 - OpenPages CommandCenter [173](#)
- client systems
 - prerequisites [33](#)
- cluster
 - horizontal [407](#)
 - vertical [409](#)
- clustered environment
 - horizontal [31](#)
 - load balancing and [170](#)
 - vertical [31](#)
- Cognos
 - services [317](#)
- Cognos Analytics
 - reporting server [29](#)
- Cognos Business Intelligence
 - installing [112](#)
- command block
 - creating for OpenPages data sources [157](#)
- CommandCenter
 - framework generator [29](#)
 - host settings [174](#)
 - port settings [174](#)
 - reporting server [29](#)
 - scaling [31](#)
- CommandCenter tasks [155](#)
- concurrency conflict [175](#)
- configuration changes [212](#)
- configuration data
 - manually loading after fix pack [450](#)
 - manually loading after installation [447](#)
 - manually loading after upgrade [449](#)
- configuration options [115](#)
- configuring
 - Apache Web Server [116](#)
- connectors [351](#)
- content store
 - configuring a connection [118](#)
 - configuring a connection to Db2 database [117](#)
 - manually creating tablespace and user [431](#)
 - restoring [250](#)
- content store database
 - overview [29](#)
- CPU
 - requirements [39](#)
- creating
 - database schema [132](#)
 - reporting schema [156](#), [214](#), [282](#)
 - tablespaces [136](#)
 - tablespaces and users [79](#)
- creating for application server installations [63](#)

D

- database
 - cataloging [86](#)
 - using scripts to update for fix packs [282](#), [289](#)
- database client
 - 64-bit installations [99](#)
- database components
 - creating [79](#), [136](#)
- database instance
 - create [95](#)
- database listener
 - installing [95](#)
- database schema
 - creating [132](#)
- database schemas
 - custom data [130](#), [140](#)
 - custom upgrades [229](#), [254](#)
 - restoring [245](#)
- database server
 - creating a database instance [95](#)
 - default port [124](#)
 - listener, installing [95](#)
 - net service name, adding [96](#)
 - OpenPages repository [28](#)
 - prerequisites [33](#)
 - server topology [28](#)
 - standard objects [432](#)
- Db2
 - restoring databases [222](#)
 - restoring Db2 Text Search [224](#)
- DB2
 - activating the database [177](#)
 - backing up the Cognos database [221](#), [411](#)
 - backing up the OpenPages database [220](#), [410](#)
 - disabling text search [76](#), [219](#)
 - dropping reporting schema for fix packs [282](#)
 - memory allocation error [461](#)
 - restoring the Cognos database [225](#)
 - restoring the OpenPages database [223](#)
 - upgrading [67](#)
 - varchar limit [176](#)
- default definition values
 - verifying [79](#), [136](#)
- deleting
 - Fujitsu reports [215](#)
- deleting Fujitsu reports
 - reports [156](#), [214](#), [215](#), [274](#), [305](#), [464](#)
- disk space
 - requirements [39](#)
- Dojo toolkits
 - backing up for fix packs [281](#)
- domain account [159](#)
- domains
 - updating [210](#)

E

- enabling
 - Data Execution Prevention [59](#)
 - reporting framework [214](#)
- encryption keystore
 - migrating [200](#)
- environment variables

- environment variables (*continued*)
 - Oracle client [103](#), [104](#)
 - setting [108](#), [109](#)
- environment variables on Linux
 - reporting server [29](#), [31](#), [33](#), [37](#), [122–124](#), [170](#), [176](#)
- environment variables on Windows operating system
 - reporting server [29](#), [31](#), [33](#), [37](#), [122–124](#), [170](#), [176](#)
- error messages
 - OP-03620 [455](#)

F

- file descriptor limits
 - setting on Linux operating systems [61](#)
- Fix Central [424](#)
- fix packs
 - additional tasks [306](#)
 - backing up helpers and Dojo toolkits [281](#)
 - backups for existing environments [280](#)
 - installation process overview [279](#)
 - installation tasks [282](#)
 - loading application and object strings using loader file [463](#)
 - patching the installation server [47](#)
 - postinstallation tasks [297](#)
 - preinstallation tasks [280](#)
 - restoring solutions helpers [297](#)
 - roll back [307](#)
 - running installation [295](#)
 - silent installation [306](#)
 - using scripts to update database [282](#), [289](#)
 - verifying servers [282](#)
- Framework Model Generator
 - starting and stopping on Windows [318](#)
- Framework Model Generator service
 - starting and stopping on Linux [318](#)

G

- generating the framework
 - reports [156](#), [214](#), [215](#), [274](#), [305](#), [464](#)
- global search
 - adding a search server [152](#)
 - starting services [312](#)
 - stopping services [313](#)
 - storage directory [184](#)
- global search index
 - creating [186](#), [212](#), [437](#)
- groups
 - creating for Linux installations [87](#)

H

- hardware
 - requirements [39](#)
- horizontal cluster [31](#)
- horizontal cluster members [407](#), [409](#)
- horizontal scaling [31](#)
- host names
 - updating [210](#)

I

- IBM Cognos service
 - starting and stopping [317](#)
 - starting and stopping on Linux [318](#)
 - starting and stopping on Windows [317](#)
- IBM HTTP Server
 - configuring [116](#)
- IBM OpenPages GRC SDI Connector for UCF Common Controls Hub [351](#)
- IBM OpenPages Third Party Risk Management [387](#)
- installation
 - default ports [124](#)
 - setting environment variables for Oracle database software [108](#), [109](#)
- installation app
 - logging in [49](#)
 - passwords [51](#)
 - user accounts [50](#)
- installation server
 - fix packs [295](#)
 - restoring [440](#)
 - updating [47](#)
- installation tasks
 - overview for fix packs [282](#)
 - preparing the search server [198](#)
 - process overview for fix packs [279](#)
 - verifying servers [282](#)
- installation user [62](#)
- installing
 - 64-bit Oracle database client [99](#)
- installing, troubleshooting [438](#)

K

- Kerberos [331](#)

L

- LDAP
 - disable [180](#)
- libdb2.so [458](#)
- Linux installations
 - creating database server users [87](#)
- listener
 - installing [95](#)
- load balancing
 - configurations [31](#)
 - raising the Oracle connection limit [97](#)
- load-balancing
 - about [170](#)
 - reporting server configuration [170](#)
- loader file
 - loading application and object strings for fix packs [463](#)
- log files
 - location [427](#)
 - silent installations [393](#), [427](#)
 - troubleshooting [424](#), [426](#), [427](#), [455](#), [465](#)

M

- memory allocation error [461](#)
- migrating

- migrating (*continued*)
 - testing the installation [215](#)
- migration
 - application files [201](#)
- migration upgrade
 - overview [189](#)
- migration, rolling back [218](#)
- mixed mode SSO [326](#)
- multiple users [175](#)

N

- net service name
 - instance
 - adding [96](#)
- new features in version 7.3.0.1 [25](#)
- new features in version 7.4.0 [24](#)
- new features in version 8.0.0.1 [23](#)
- new features in version 8.0.0.2 [22](#)
- new features in version 8.1.0 [20](#)
- new features in version 8.1.0.1 [20](#)
- new features in version 8.2.0 [18](#)
- new features in version 8.2.0.1 [16](#)
- new features in version 8.2.0.2 [15](#)
- new features in version 8.2.0.3 [15](#)
- new features in version 8.2.0.4 [15](#)

O

- OP-03620 [455](#)
- OPBackup [241](#), [242](#), [412](#), [413](#)
- OPCCBackup [242](#), [413](#)
- OPCCRestore [250](#)
- OpenID Connect [336](#)
- OpenID Connect SSO [338](#)
- OpenPages database
 - Oracle compatibility mode [81](#)
- openpages-storage directory [205](#)
- OPRestore [244](#), [250](#)
- Oracle
 - backing up databases [241](#), [242](#), [412](#), [413](#)
 - initialization parameters [95](#)
 - restoring databases [243](#), [250](#)
 - standard objects [432](#)
- Oracle Admin Client
 - installing on application servers [99](#)
- Oracle Automatic Storage Management [136](#)
- Oracle client path
 - updating on report server [457](#)
- Oracle compatibility mode
 - OpenPages database [81](#)
- Oracle database instance
 - starting [98](#)
- Oracle database server
 - installing [88](#), [92](#)
- Oracle Instant Client [103](#), [104](#)
- ORACLE_HOME
 - setting [108](#), [109](#)
- orphan objects
 - preventing [187](#)

P

- package dependencies [432](#)
- packages
 - importing [274](#), [305](#), [464](#)
- paging file size
 - increasing on application server [176](#)
 - increasing on reporting server [176](#)
- PATH variable
 - adding ORACLE_HOME [108](#), [109](#)
 - modifying for installations that use Oracle [108](#), [109](#)
- platform
 - architecture [27](#)
- ports
 - default [124](#)
 - fixed [124](#)
- post-installation tasks
 - application server [175](#)
- postinstallation tasks
 - overview for fix packs [297](#)
 - restoring solutions helpers [297](#)
 - updating reporting schema [214](#)
- preinstallation tasks
 - backups for fix packs [280](#)
 - overview for fix packs [280](#)
- prerequisite software
 - application servers [35](#)
- prerequisites
 - client systems [33](#)
 - hardware [39](#)
 - software [33](#)
- problem determination
 - exchanging information with IBM Support [426](#)

Q

- QRadar [345](#)

R

- RAM
 - requirements [39](#)
- related information [1](#)
- Reporting Framework
 - BC error [465](#)
 - CAMCryptoBC error [465](#)
- reporting schema
 - dropping for fix packs [282](#)
 - updating [214](#)
- reporting server
 - default port [124](#)
 - load balancing [31](#)
 - load balancing and [170](#)
 - paging file size and [176](#)
 - prerequisites [33](#)
 - server topology [29](#)
 - software requirements [37](#)
- reporting server on Linux
 - environment variables [103](#), [104](#), [108](#), [109](#), [122](#), [123](#)
- reporting server on Windows operating system
 - environment variables [103](#), [104](#), [108](#), [109](#), [122](#), [123](#)
- reports
 - importing [274](#), [305](#), [464](#)

- resources [423](#)
- restoring after upgrade
 - custom configuration changes [212](#)
- roll back
 - fix packs [307](#)
- rolling back a migration upgrade [218](#)

S

- SAML SSO [324](#)
- scaling the application [31](#)
- schema
 - reporting [214](#), [282](#)
- scripts
 - using to update database for fix packs [282](#), [289](#)
- SDI [351](#)
- search index
 - creating [186](#), [212](#), [437](#)
- search server
 - configuring [152](#)
 - upgrade tasks [198](#)
- securing access to the OpenPages CommandCenter [157](#)
- Security Directory Integrator [351](#)
- server topology
 - application server [28](#)
 - database server [28](#)
 - reporting server [29](#)
- servers
 - adding cluster members [407](#), [409](#)
 - topology [29](#)
- service name, adding [96](#)
- services
 - Cognos [317](#)
 - starting [309](#)
 - starting and stopping Cognos service [318](#)
 - starting and stopping Framework Model Generator service [318](#)
 - starting and stopping IBM Cognos service [317](#)
 - stopping [311](#)
- setting on Linux operating systems
 - file descriptor limits [61](#), [64](#)
- sharing network storage [161](#)
- silent installation
 - fix packs [306](#)
- silent installations
 - log files [427](#)
 - overview [393](#)
- single server
 - configuring for Oracle databases [109](#)
- single sign-on
 - configuring for logging out [343](#)
 - disabling [324](#), [336](#), [338](#), [343](#)
 - error page [325](#)
 - header-based [339](#)
 - OIDC [336](#)
 - SAML [321](#), [329](#)
 - SAML mixed-mode [326](#)
 - setting passwords to never expire [343](#)
 - SPNEGO or Kerberos [331](#)
 - timeout [344](#)
- software
 - requirements [33](#)
- software requirements
 - reporting server [37](#)

- solutions
 - manually installing after installation [467](#)
- solutions helpers
 - backing up for fix packs [281](#)
 - restoring [297](#)
- SPNEGO [331](#)
- SPNEGO SSO [336](#)
- SSL
 - with OpenPages [180](#)
- SSO [321](#)
- starting
 - OpenPages [180](#)
 - OpenPages with Web browser [180](#)
- starting and stopping
 - Framework Model Generator service [318](#)
 - IBM Cognos service [317](#), [318](#)
- storage directory [184](#)
- Super Administrator [144](#)

T

- table spaces
 - customizing [135](#)
- tablespaces
 - creating [136](#)
 - customizing [135](#)
- tablespaces and users
 - creating [79](#)
- testing
 - database server connections [98](#)
- third-party software
 - requirements [33](#)
- topology
 - servers [29](#)
- troubleshooting
 - contacting IBM Support [424](#)
 - exchanging information with IBM Support [426](#)
 - fixes
 - installing [424](#)
 - getting fixes [424](#)
 - reporting schema not instantiated error [455](#)
 - searching knowledge bases [424](#)
 - solutions installation problems [465](#)
 - subscribing to Support notifications [426](#)
- troubleshooting, installation issues and solutions [438](#)

U

- UCF [351](#)
- understanding symptoms of a problem [423](#)
- update-storage script [161](#)
- updating the reporting framework
 - reports [156](#), [214](#), [215](#), [274](#), [305](#), [464](#)
- upgrades
 - restoring solutions helpers [297](#)
- upgrading custom changes
 - configuration files [212](#)
- users
 - creating for Linux installations [87](#)
- users and groups for application servers [62](#)
- users and groups for Db2 database client software [84](#)
- users and groups for Oracle database client software [99](#)

V

- validation reports
 - log files [427](#)
- verifying the installation
 - upgrading [216](#)
- vertical cluster [31](#)
- vertical scaling [31](#)
- video documentation resources [423](#)
- virtualization
 - supported configurations [39](#)
- VRM, *See* IBM OpenPages Third Party Risk Management

W

- Windows services
 - starting [309](#)
 - stopping [311](#)

