Avaya Workforce Optimization

Expansion Guide

Version 15.2

February 13, 2019
Revision 1.01

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

"Documentation" means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by Avaya. You agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by You.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website:
http://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

"Hosted Service" means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK "Avaya Terms of Use for Hosted Services" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

THE AVAYA GLOBAL SOFTWARE LICENSE TERMS FOR VERINT SOFTWARE PRODUCTS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO, OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS THE SOFTWARE (AS DEFINED IN THE AVAYA GLOBAL SOFTWARE LICENSE TERMS FOR VERINT SOFTWARE PRODUCTS), AND WHO PURCHASED THE LICENSE FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. REFER TO THE AVAYA SOFTWARE LICENSE TERMS FOR VERINT SOFTWARE PRODUCTS FOR INFORMATION REGARDING THE APPLICABLE LICENSE TYPES PERTAINING TO THE SOFTWARE.

All Rights Reserved

Avaya and/or its licensors retain title to and ownership of the Software, Documentation, and any modifications or copies thereof. Except for the limited license rights expressly granted in the applicable Avaya Global Software License Terms for Verint Software Products, Avaya and/or its licensors reserve all rights, including without limitation copyright, patent, trade secret, and all other intellectual property rights, in and to the Software and Documentation and any modifications or copies thereof. The Software contains trade secrets of Avaya and/or its licensors, including but not limited to the specific design, structure and logic of individual Software programs, their interactions with other portions of the Software, both internal and external, and the programming techniques employed.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

Certain software programs or portions thereof included in the Software may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Software ("Third Party Terms"). Information regarding distributed Linux OS source code (for any Software that has distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Software, Documentation or on Avaya's website at: http://support.avaya.com/Copyright (or a successor site as designated by Avaya).

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Software is used.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud Intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com, or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, any Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

About this guide

This guide describes the options for expanding a system to a different deployment scenarios, including Data Center replacement for various purposes.

Intended audience

This guide is designed to be used by professional services staff responsible for expanding the system to a different deployment scenarios.

Document revision history

Revision	Description of changes
1.01	Removed the *Delete site servers* procedure from the *Workflow: Replace Data Center* topic.
1.00	Moved the Expansion Chapter from the Maintenance Guide to a new Expansion Guide.

Chapter 1

Local SQL Servers transposition to remote SQL Servers in L1, L2, or L3 deployment levels

In deployment levels L1, L2, and L3, it is possible to transpose the local SQL Server databases to remote SQL Servers.

Topics

Local SQL Servers transposition to remote SQL Servers overview

For deployments with remote SQL servers at L1, L2, and L3, it is possible to transpose the local SQL Servers across separate remote SQL servers.

Databases can be transposed between servers only in platform database groups. These platform database groups are based on the deployment levels and cannot be separated. Each platform database group must be hosted on a single server in the remote SQL Servers farm.

Database platform groups

A database platform group indicates the specific databases that must be in the same instance. Separating databases must comply with the platform group. Each instance must have a copy of CommonDB database (except the Reporting group).

When installing a target Data Center with local SQL Servers, all databases are already created, including the CommonDB. However, when the databases are on a remote SQL Servers, the CommonDB does not exit on the target remote SQL Servers. Therefore, copy also the CommonDB to each platform group (except the Reporting group).

Database platform group	Databases in the platform group
Framework Databases	• BPMAINDB (Framework database) • BPWHATIFDB • CommonDB
Data Warehouse	• BPWAREHOUSEDB (Framework Data Warehouse) • CentralDWH (Interaction Data Warehouse) • ETLSTAGINGDB • CommonDB
Contact & QM	• CentralContact (Contact Database) • CentralApp (QM Database) • PCMON (DPA Database) • Biometrics • CommonDB
Contact OLTP Database	• Archive (Archive Database) • LocalContact (Contact OLTP Database) • CommonDB

Database platform group	Databases in the platform group
Speech Database	• SpeechProducts (Speech Products Database) • SpeechAnalytics (Speech Analytics Database) • CommonDB
Reporting	• ReportServer • ReportServerTempDB

Workflow: transfer local SQL Servers to remote SQL Servers

For deployments levels L1, L2, or L3 with local SQL Servers, , it is possible to transfer the databases to remote SQL Servers.

Workflow

1. Stop services, page 16

   To prevent data changes during the entire process, the services on the source system must be stopped.
2. Copy data, page 17

   Copy databases between servers can be done using customer tools, for example, by backup and restore or by detach and attach.
3. Clean database sync event properties, page 10

   On all relocated databases, the Database Sync Event must be cleaned up.
4. Update Framework Database Server connection details, page 17

   Framework Database Server connection details update is required only if BPMAINDB is moved to a different server, regardless of whether it is local or remote SQL Server.
5. Update Database Server location in EM, page 18

   Each databases server role is configured with the database location of the source system. The location of each database server role must be modified to the new Database Server instance.
6. Detach and attach Report Server Databases, page 12

   Take the report server offline, detach the databases and move them to the SQL Server instance you want to use. This approach preserves permissions in the databases.
7. Detach databases from the source server, page 13

   All databases that are copied to the target servers must be detached from the source server.
8. Start services, page 13

   To activate the system with the remote SQL Servers, the services on the source system must be started.

Stop services

To prevent data changes during the entire process, the services on the source system must be stopped.

Procedure

1. On the server hosting the Databases, open the Watchdog control panel and stop the following services:
   - Watchdog
   - Integration server
2. From **Start > Run**, run services.msc and stop the **SQL Server Agent**.
3. On the Application server, stop the IIS service as follows:

- From the command line, run as administrator the command **iisreset /stop**.

Copy data

Copy databases between servers can be done using customer tools, for example, by backup and restore or by detach and attach.

Database backup and restore

Database backup is the customer's responsibility. Therefore, consult with the customer about the backup procedure.

Database backup can be done by using a SQL Server backup utility, third party products, or tools provided by the SAN vendor (for example, Snapshot and BCV).

If the customer's database backup utility requires a SQL Server agent running on the database server, run it to enable the backup process. When the backup is completed, stop the SQL Server agent.

If a restore utility is used with a backup file, and the destination server does not contain the same drive letters used in the source database, use the move argument of the restore command.

Database detach and attach

Before detaching a database, it is recommended running a full backup. Detach the database from the source database server, copy the database files (mdf, ndfs, and ldf) to the target server, and then attach the databases on the new server.

Procedure

1 Copy the databases from the server hosting the Databases to the remote SQL servers. Make sure to keep together databases of the same group as specified in the *Database groups* table.

Related topics

Database platform groups, page 15

Clean database sync event properties

On all relocated databases, the Database Sync Event must be cleaned up.

Procedure

1 Clean up the **Database Sync Event** properties by running the following SQL script on the SQL server hosting Speech Databases:

```
IF OBJECT_ID (N'[CommonDB].[dbo].[DBSync_events]', N'U') IS NOT NULL
BEGIN
DELETE FROM
[CommonDB].[dbo].[DBSync_events]
WHERE
([event_name] LIKE 'LC_%' AND DB_ID (N'LocalContact') IS NULL)
OR ([event_name] LIKE 'CA_%' AND DB_ID (N'CentralApp') IS NULL)
OR ([event_name] LIKE 'CC_%' AND DB_ID (N'CentralContact') IS NULL)
END
```

Update Framework Database Server connection details

Framework Database Server connection details update is required only if BPMAINDB is moved to a different server, regardless of whether it is local or remote SQL Server.

The server hosting the Framework Applications server role is configured with the Framework Database Server connection details of the source system. The connection details must be modified to the new Framework Database Server.

Procedure

1. Log on to each server hosting the Framework Applications server role.
2. Open command line.
3. Change directory to:

   ```
   %Impact360SoftwareDir%ProductionServer\weblogic\Impact360\ProductionDomain\Scripts
   ```
4. Run **fixSqlServerConn.cmd** with the new Framework Database Server connection details as follows:

   ```
   fixSqlServerConn.cmd <hostname> <port> <domain> <DMSA_account_username> <DMSA_account_
      password>
   ```
5. Restart the server hosting the Framework Applications server role.

Update Database Server location in EM

Each databases server role is configured with the database location of the source system. The location of each database server role must be modified to the new Database Server instance.

Procedure

1. From the portal, select System Management > Enterprise Management > Settings.
2. Verify that the Database roles are active on the new server.
3. For each database server role, do the following:
   a. Select the server name.
   b. Modify the SQL server host address and port to match the Database SQL server instance.
4. Click **Save** to save and distribute the configuration.

   Wait while the EM retrieves this configuration update from the database, processes it, and pushes it to the new server.

   During this process, a star icon * appears next to the new server name.
5. Wait for the star icon next to the server name disappears. This indicates that configuration update is completed.
6. Check the **Configuration Status** tab in EM for errors and warnings.
7. In the **Alarm Status** tab, verify that no active alarms or errors exist.
8. Verify that all jobs are created on the new database server.

Detach and attach Report Server Databases

Take the report server offline, detach the databases and move them to the SQL Server instance you want to use. This approach preserves permissions in the databases.

After you move the databases, reconfigure the report server connection to the report server database. If you run a scale-out deployment, reconfigure the report server database connection for each report server in the deployment.

Procedure

1. Back up the encryption keys for the report server database you want to move.

   You can use the Reporting Services Configuration tool to back up the keys.
2. Stop the Report Server service.

   You can use the Reporting Services Configuration tool to back up the keys.
3. Start SQL Server Management Studio and open a connection to the SQL Server instance that hosts the report server databases.
4. Right-click the report server database, point to Tasks, and click **Detach**. Repeat this step for the report server temporary database.
5. Copy or move the .mdf and .ldf files to the Data folder of the SQL Server instance you want to use. Because you move two databases, make sure that you move or copy all four files.
6. In SQL Server Management Studio, open a connection to the new SQL Server instance that hosts the target report server databases.
7. Right-click the Databases node, and then click **Attach**.
8. Click **Add** to select the report server database .mdf and .ldf files that you want to attach. Repeat this step for the report server temporary database.
9. Verify that the **RSExecRole** is a database role in the report server database and temporary database.

   RSExecRole must have select, insert, update, delete, and reference permissions on the report server database tables, and execute permissions on the stored procedures.
10. Start the Reporting Services Configuration tool and open a connection to the report server.
11. On the Database page, select the new SQL Server instance, and then click **Connect**.
12. Select the report server database that you just moved, and then click Apply.
13. On the Encryption Keys page, click **Restore**. Specify the file that contains the backup copy of the keys and the password to unlock the file.
14. Restart the Report Server service.

Related information

Detaching and Attaching the Report Server Databases in Microsoft MSDN: https://msdn.microsoft.com/en-us/library/ms156421.aspx

Detach databases from the source server

All databases that are copied to the target servers must be detached from the source server.

Procedure

1. Log on to the server hosting the source databases.
2. Open SQL Server Management Studio and connect to database server.
3. Run the following scripts:

```
execute sp_detach_db ReportServer
execute sp_detach_db ReportServerTempDB
execute sp_detach_db CommonDB
execute sp_detach_db LocalContact
execute sp_detach_db CentralApp
execute sp_detach_db CentralContact
execute sp_detach_db CentralDWH
execute sp_detach_db Archive
execute sp_detach_db BPMAINDB
execute sp_detach_db BPWHATIFDB
execute sp_detach_db BPWAREHOUSEDB
execute sp_detach_db ETLSTAGINGDB
```

Start services

To activate the system with the remote SQL Servers, the services on the source system must be started.

Procedure

1. On the server hosting the Databases, open the Watchdog control panel and start the following services:
   - Watchdog
   - Integration server
2. From **Start > Run**, run services.msc and start the **SQL Server Agent**.
3. On the Application server, start the IIS service as follows:
   - From the command line, run as administrator the command **iisreset /start**.

Chapter 2

Remote SQL instances distribution across separate remote SQL Servers

For deployments with remote SQL servers at L3 or higher level, it is possible to distribute the databases across separate remote SQL servers (level expansion).

Topics

Remote SQL instances distribution overview

For deployments with remote SQL servers at L3 or higher deployment level, it is possible to distribute the databases across separate remote SQL servers.

Databases can be transferred between servers only in platform database groups. These platform database groups are based on the deployment levels and cannot be separated. Each platform database group must be hosted on a single server in the remote SQL Servers farm.

Database platform groups

A database platform group indicates the specific databases that must be in the same instance. Separating databases must comply with the platform group. Each instance must have a copy of CommonDB database (except the Reporting group).

When installing a target Data Center with local SQL Servers, all databases are already created, including the CommonDB. However, when the databases are on a remote SQL Servers, the CommonDB does not exit on the target remote SQL Servers. Therefore, copy also the CommonDB to each platform group (except the Reporting group).

Database platform group	Databases in the platform group
Framework Databases	• BPMAINDB (Framework database) • BPWHATIFDB • CommonDB
Data Warehouse	• BPWAREHOUSEDB (Framework Data Warehouse) • CentralDWH (Interaction Data Warehouse) • ETLSTAGINGDB • CommonDB
Contact & QM	• CentralContact (Contact Database) • CentralApp (QM Database) • PCMON (DPA Database) • Biometrics • CommonDB
Contact OLTP Database	• Archive (Archive Database) • LocalContact (Contact OLTP Database) • CommonDB
Speech Database	• SpeechProducts (Speech Products Database) • SpeechAnalytics (Speech Analytics Database) • CommonDB
Reporting	• ReportServer • ReportServerTempDB

Workflow: distribute remote SQL instances

For deployments with remote SQL servers at L3 or higher deployment level, it is possible to distribute the databases across separate remote SQL servers.

Workflow

1. Stop services, page 16

   To prevent data changes during the entire process, the services on the source system must be stopped.
2. Copy data, page 17

   Copy databases between servers can be done using customer tools, for example, by backup and restore or by detach and attach.
3. Update Framework Database Server connection details, page 17

   Framework Database Server connection details update is required only if BPMAINDB is moved to a different server, regardless of whether it is local or remote SQL Server.
4. Update Database Server location in EM, page 18

   Each databases server role is configured with the database location of the source system. The location of each database server role must be modified to the new Database Server instance.
5. Update additional settings, page 18

   Depending on the databases that are relocated to the remote SQL Servers farm, additional settings are required.

Stop services

To prevent data changes during the entire process, the services on the source system must be stopped.

Procedure

1. On the server hosting the Databases, open the Watchdog control panel and stop the following services:
   - Watchdog
   - Integration server
2. From **Start > Run**, run services.msc and stop the **SQL Server Agent**.
3. On the Application server, stop the IIS service as follows:
   - From the command line, run as administrator the command **iisreset /stop**.

Copy data

Copy databases between servers can be done using customer tools, for example, by backup and restore or by detach and attach.

Database backup and restore

Database backup is the customer's responsibility. Therefore, consult with the customer about the backup procedure.

Database backup can be done by using a SQL Server backup utility, third party products, or tools provided by the SAN vendor (for example, Snapshot and BCV).

If the customer's database backup utility requires a SQL Server agent running on the database server, run it to enable the backup process. When the backup is completed, stop the SQL Server agent.

If a restore utility is used with a backup file, and the destination server does not contain the same drive letters used in the source database, use the move argument of the restore command.

Database detach and attach

Before detaching a database, it is recommended running a full backup. Detach the database from the source database server, copy the database files (mdf, ndfs, and ldf) to the target server, and then attach the databases on the new server.

Procedure

1 Copy the databases from the server hosting the Databases to the remote SQL servers. Make sure to keep together databases of the same group as specified in the *Database groups* table.

Related topics

Database platform groups, page 15

Update Framework Database Server connection details

Framework Database Server connection details update is required only if BPMAINDB is moved to a different server, regardless of whether it is local or remote SQL Server.

The server hosting the Framework Applications server role is configured with the Framework Database Server connection details of the source system. The connection details must be modified to the new Framework Database Server.

Procedure

1 Log on to each server hosting the Framework Applications server role.

2 Open command line.

3 Change directory to:

```
%Impact360SoftwareDir%ProductionServer\weblogic\Impact360\ProductionDomain\Scripts
```

4 Run **fixSqlServerConn.cmd** with the new Framework Database Server connection details as follows:

```
fixSqlServerConn.cmd <hostname> <port> <domain> <DMSA_account_username> <DMSA_account_
   password>
```

5 Restart the server hosting the Framework Applications server role.

Update Database Server location in EM

Each databases server role is configured with the database location of the source system. The location of each database server role must be modified to the new Database Server instance.

Procedure

1. From the portal, select System Management > Enterprise Management > Settings.
2. Verify that the Database roles are active on the new server.
3. For each database server role, do the following:
   a. Select the server name.
   b. Modify the SQL server host address and port to match the Database SQL server instance.
4. Click **Save** to save and distribute the configuration.

   Wait while the EM retrieves this configuration update from the database, processes it, and pushes it to the new server.

   During this process, a star icon * appears next to the new server name.
5. Wait for the star icon next to the server name disappears. This indicates that configuration update is completed.
6. Check the **Configuration Status** tab in EM for errors and warnings.
7. In the **Alarm Status** tab, verify that no active alarms or errors exist.
8. Verify that all jobs are created on the new database server.

Update additional settings

Depending on the databases that are relocated to the remote SQL Servers farm, additional settings are required.

Procedure

1. If QM database is relocated, update the PPFW settings.
2. If DPA database (PCMON) is relocated, distribute DPA configuration.
3. If speech databases are relocated, distribute Speech Analytics configuration.
4. If Report Server Databases are relocated , perform Detach and attach Report Server Databases, page 12.
5. For all the relocated databases, except the QM database, clean up the **Database Sync Event** properties by running the following SQL script on the SQL server hosting Speech Databases:

```
IF OBJECT_ID (N'[CommonDB].[dbo].[DBSync_events]', N'U') IS NOT NULL
BEGIN
DELETE FROM
[CommonDB].[dbo].[DBSync_events]
WHERE
([event_name] LIKE 'LC_%' AND DB_ID (N'LocalContact') IS NULL)
OR ([event_name] LIKE 'CA_%' AND DB_ID (N'CentralApp') IS NULL)
OR ([event_name] LIKE 'CC_%' AND DB_ID (N'CentralContact') IS NULL)
END
```

Chapter 3

Data Center replacement (for upgrade to Windows 2016, level expansion, domain change)

Replace Data Center procedure enables to upgrade the OS to Windows 2016, change the Data Center to a different deployment level (expansion), or move the Data Center to a different domain with no trust. This is a side-by-side procedure where a new Data Center is deployed and data is copied from the old Data Center to the new Data Center.

Topics

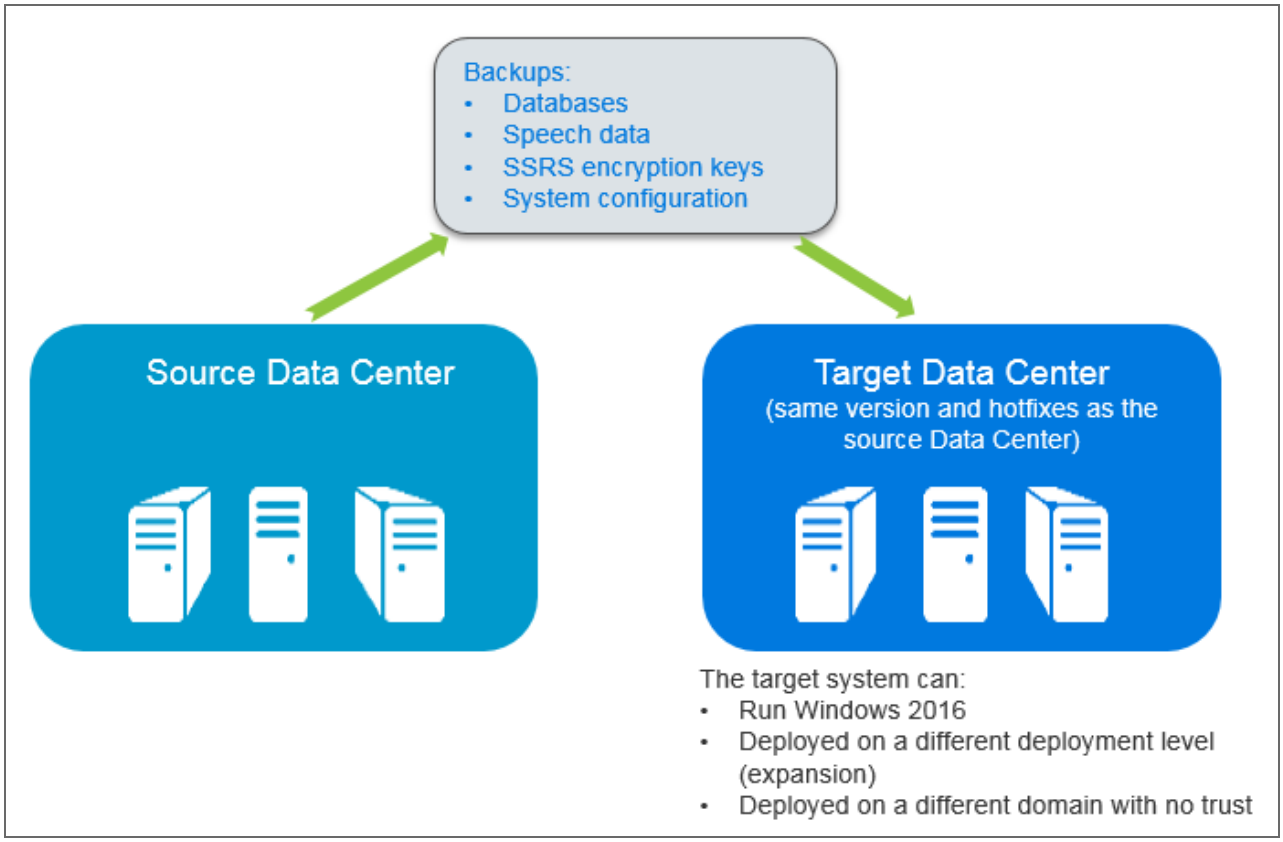
Data Center replacement overview

Replace Data Center procedure enables to upgrade the OS to Windows 2016, change the Data Center to a different deployment level (expansion), or move the Data Center to a different domain with no trust. This is a side-by-side procedure where a new Data Center is deployed and data is copied from the old Data Center to the new Data Center.

The target Data Center must identical to the source Data Center regarding the software version and hotfixes. Once the copy Data Center is completed, sites of the source system are connected to the target Data Center.

If the target Data Center is deployed on a different domain with SSO, you must create new user accounts in the target Data Center.

Copy Data Center data to new Data Center



Data Center replacement prerequisites

The source Data Center and the target Data Center must meet certain prerequisites.

The target Data Center must meet the following prerequisites:

- Same or higher database pre-allocation size of the source Data Center.
- Same software level and hotfix level in the source Data Center.
- Same installation paths as in the source Data Center.
- Same SQL Server collation as in the source Data Center.
- Same SSO and SSL setup as in the source Data Center.
- Same FirstUser account (ID -8001) as in the production system. Note the FirstUser account name for later use.
- If Disaster Recovery (DR) solution is implemented on the new environment, remove it. Once the copy DC procedure is completed, add the DR solution to the working target environment.
- If Speech Analytics is enabled on the source Data Center, the Project Name and Instance ID on the target Data Center must match the source Data Center.
- Both environments must meet the PCI requirements.
- For rollback purposes, create a snapshot or image backup of the target environment.

Workflow: Replace Data Center

Replace Data Center procedure enables to upgrade the OS to Windows 2016, change the Data Center to a different deployment level (expansion), or move the Data Center to a different domain with no trust. This is a side-by-side procedure where a new Data Center is deployed and data is copied from the old Data Center to the new Data Center.

Workflow

1 Obtain tools, page 23

The source Data Center and the target Data Center must meet certain prerequisites. To eliminate the dependency on the connection at the customer site, obtain the latest migration tools in advance.

2 Export Data Center configuration on the target system, page 24

The Export Data Center Configuration feature exports the configuration of every Data Center Zone server with active server role to an XML file.

3 Block configuration distribution on the target system, page 25

Before restoring data to the target system, the configuration distribution in the target system must be blocked to prevent the Enterprise Manager from sending configuration changes to the servers.

4 Set the target system to migration mode, page 25

To free as many system resources as possible for the migration process, stop some of the services and keep other services running. This situation is called migration mode.

5 Update EM location in source system, page 26

On the source system, the Enterprise Manager (EM) location points to the source Application Server. Update the EM location to point to the target Application Server.

6 Block configuration distribution on source system, page 26

To prevent the Enterprise Manager from sending configuration changes to the source Data Center servers, the configuration distribution in the source system must be blocked.

7 Set source DC servers to migration mode, page 27

To free as many system resources as possible for the migration process, stop some of the services and keep other services running. This situation is called migration mode.

8 Create backups of source DC, page 27

Backups of the source DC are required. These backups are restored or imported to the target DC. If a recent backup of the source DC already exits, skip this procedure.

9 Restore data to target system, page 29

Restore data from the production backup to the target system.

10 Reassign database permissions on the target systems, page 32

Reassigning the SQL Server permissions on the target system is required if the Management Service Account (MSA), Database Management Service Account (DMSA), or domain are different between the source and target systems.

11 Configure the Report Server database connection, page 33

Configure the Report Server database connection from the new server that hosts Reporting Services and has a new name. This updates the user account and password used for the database connection.

12 Restore SSRS encryption keys, page 33

The SSRS encryption keys of the source system are required in the target system.

13 Import target Data Center configurations, page 33

The data restore from source backup replaces the target Data Center (DC) configuration. Import the target configuration from the XML file you have created by the Export DC Configuration feature.

14 Update IMSA and DMSA, page 35

If the target system is in a different domain than the source system, update the MSA and DMSA accounts to the same accounts as configured in the target system.

15 Copy FIS adaptors configuration, page 35

The FIS adaptors configuration is stored in the system backup. The system backup creates a separate Windows Backup (VHD) for each drive in the destination folder.

16 Update PPFW settings, page 36

Update the Central Missions Manager (CMM) component of the Post-Processing Framework (PPFW) component with the new database server host name.

17 Stop migration mode on target system, page 36

Once the data center migration is completed, the migration mode is not required. All services must be started to enable usual operation.

18 Unblock configuration distribution on target system, page 37

During the database restore, the SSRS reports are overridden. To deploy the SSRS reports on the target servers, unblock the configuration distribution to the target managed servers.

19 Update Customer Feedback ETL configuration, page 37

If Customer Feedback Survey Servers are deployed on the production system, update the Customer Feedback ETL configuration.

20 Distribute DPA configuration, page 37

Distribute the configuration to the DPA Applications.

21 Distribute Speech Analytics configuration, page 38

Distribute the configuration to the Speech Analytics Application servers.

22 Uninstall the temporary AD LDS service, page 38

Uninstall the temporary AD LDS service created during ADAM restore.

23 Check service restart alarms and perform SAT , page 38

Check service restart alarms and verify proper operation.

Obtain tools

The source Data Center and the target Data Center must meet certain prerequisites.

To eliminate the dependency on the connection at the customer site, obtain the latest migration tools in advance.

Required tools list

Migration tool	Install or extract on
Migration Mode Tool	Extract to a server hosting any database server role on the target system
WFO Data Migration Tool from V15.1	Install the tool on the server that hosts the QM Database role

Procedure

1 Obtain the tools listed in the table from your customer representative.

Export Data Center configuration on the target system

The Export Data Center Configuration feature exports the configuration of every Data Center Zone server with active server role to an XML file.

Export the DC configuration of the target system to an XML file. This XML file is used during the Import DC configuration.

The exported XML file includes the following information:

- The parent Site Group and Site under each server resides in the Installations tree.
- The values specified for each server on its values specified for each server on its System Management > Installations > Settings page (such as, server name, ports, serial number, and HTTP alias).
- The server role configuration settings and the server role associations of the Data Center Zone server roles on each server.

The exported XML file does not include the following information:

- Enterprise settings and security settings.
- Site servers.
- Site role properties of a consolidated server.

The exported data also contains Data sources configuration. That is, the target system receives data from the production extensions. To prevent receiving data from the production extensions, remove the data sources manually from the target system after importing the DC configuration.

Procedure

1 Sign in to the target system portal as the system administrator.
2 In the Installations tree, select the **Enterprise** node.
3 In **System Management > Enterprise**, click **More Actions**, and select **Turn Advanced Mode On**.
4 Select **Data Center Migration - Internal Use Only**.
5 Click the **Export Data Center Configuration** icon .
The system creates an XML file containing the configuration of the active Data Center Zone server roles on every server in the enterprise.
6 Save the XML file to a directory. Make a note of this directory. This file is required later to complete the copy process.

Related information

Block and Unblock Configuration Distribution (*Enterprise Manager Configuration and Administration Guide*)

Block configuration distribution on the target system

Before restoring data to the target system, the configuration distribution in the target system must be blocked to prevent the Enterprise Manager from sending configuration changes to the servers.

Procedure

1. Open the Enterprise Manager and verify in the System Monitor that the configuration distribution completed successfully.
2. Verify that no configuration changes are pending to the managed servers, by ensuring that the Pending Messages icon is not displayed in Enterprise Manager.
3. Select the Enterprise (root) node in the **System Management > Enterprise >Settings** and block the configuration for the entire Enterprise.

Related information

Block and Unblock Configuration Distribution (Enterprise Manager Configuration and Administration Guide)

Set the target system to migration mode

To free as many system resources as possible for the migration process, stop some of the services and keep other services running. This situation is called migration mode.

The restore process requires exclusive lock on the database. If connections are open, they must be closed manually.

Procedure

1. Log on with the Installation Account to the source server with the Migration Mode Tool.
2. Run **Windows PowerShell** as administrator.
3. Change directory to location of the Migration Mode Tool.
4. To verify that all data center servers are identified and online, run the following command:

   ```
   ./MigrationModeTool.ps1 -action test
   ```
5. To set the data center servers to migration mode, run the following command:

   ```
   ./MigrationModeTool.ps1 -action set
   ```
6. Verify that no error messages appear.

Related information

Migration Mode Tool (*WFO V15.1 to V15.2 (Side-by-Side with optional HW Reuse) Upgrade Guide*)

Update EM location in source system

On the source system, the Enterprise Manager (EM) location points to the source Application Server. Update the EM location to point to the target Application Server.

Procedure

1. On the source system, from the Portal, select **System Management > General Settings > Enterprise Manager Location**.
2. On the Propagate Enterprise Manager Location to applications screen, change the following settings:
   a. EM Server Name: Change the name to the target Application server name. If NLB is configured, use the NLB address.
   b. Port Number: Change the value to 80.
   c. SSL Port Number: Change the value to 443.
   d. Click **Save**.

Verify network connectivity by server name/IP address as follows:

- From the source system to the target Application server.
- From the target application server to the source system.

3. Click **Update Enterprise Manager Location**.

   The EM pushes the updated location of the application server to all servers, and displays a status message about the pushed configuration for each server.
4. Click **Done**.

If errors occur, fix them before continue to next step. Otherwise, the servers with error do not receive updates from target Data Center.

5. Verify that no configuration changes are pending to the managed servers, by ensuring that the Pending Messages icon is not displayed in Enterprise Manager.

Block configuration distribution on source system

To prevent the Enterprise Manager from sending configuration changes to the source Data Center servers, the configuration distribution in the source system must be blocked.

Procedure

1. Open the Enterprise Manager and verify in the Configuration Status that the configuration distribution completed successfully.
2. Verify that no configuration changes are pending to the managed servers, by ensuring that the Pending Messages icon is not displayed in Enterprise Manager.

3 Select the Enterprise (root) node in the **System Management > Enterprise > Settings**, click **More Actions** and block the configuration for the entire Enterprise.

Related information

Block and Unblock Configuration Distribution (*Enterprise Manager Configuration and Administration Guide*)

Set source DC servers to migration mode

To free as many system resources as possible for the migration process, stop some of the services and keep other services running. This situation is called migration mode.

Procedure

1 Log on with the Installation Account to the source server with the Migration Mode Tool.
2 Run **Windows PowerShell** as administrator.
3 Change directory to location of the Migration Mode Tool.
4 To verify that all data center servers are identified and online, run the following command:
```
.\MigrationModeTool.ps1 -action test
```
5 To set the data center servers to migration mode, run the following command:
```
.\MigrationModeTool.ps1 -action set
```
6 Verify that no error messages appear.

Related information

Migration Mode Tool (*WFO V15.1 to V15.2 (Side-by-Side with optional HW Reuse) Upgrade Guide*)

Create backups of source DC

Backups of the source DC are required. These backups are restored or imported to the target DC. If a recent backup of the source DC already exits, skip this procedure.

Before you begin

1 From the source portal, select **System Management > Enterprise > Enterprise Settings** and verify that System Backup is enabled and configured.
2 Select **System Monitor** and verify that there are no pending messages or alarms.

Procedure

1 Back up databases, page 28
2 Verify Speech Analytics Index backup, page 28
3 Back up SSRS encryption keys, page 28
4 Back up system configuration manually, page 28

Back up databases

Back up all databases in the correct order.

Related topics

Databases backup (*Maintenance Guide*)

Verify Speech Analytics Index backup

Speech Analytics Index backup is maintained daily. Verify that a recent backup exists.

Related information

Back up Speech Analytics index (*Maintenance Guide*)

Back up SSRS encryption keys

Create a backup of the Reporting Services encryption keys only once after setting up the system.

This backup is required for restoring an existing report services server role, and when changing the management service account credentials.

Procedure

1. Open the **Reporting Services Configuration Manager**.
2. Connect to the SSRS instance.
3. Select **Encryption Keys**.
4. Click **Back Up** and specify the location to store the **rsdbkey.snk** key. It is best practice to store the key on a separate disk.
5. Enter a strong **Password** to lock the key and click **OK**.

Back up system configuration manually

The System backup includes configuration files and ADAM. The configuration files are copies of the managed server XML configuration and properties files that are not stored in any database.

System backup is defined in the Enterprise Settings. The customer provides the system backup files location (the System Backup setting is done as part of standard system settings).

Manually start the system scheduled backup.

Procedure

1. Log on to the server that hosts the QM Database role.
2. Open a command prompt as an administrator.
3. To start the backup process, run the following command: WBADMIN START BACKUP.

Restore data to target system

Restore data from the production backup to the target system.

Workflow

1 Restore databases, page 29

Regardless of the target system deployment level, restore all databases, except the CommonDB database, from the backup to the target system.

2 Restore Speech Analytics index, page 29

Restore Speech Analytics index from the backup of the production system to the target system.

3 Copy ADLDS objects, page 30

ADLDS (ADAM) contains objects such as users, groups, assignments and CD value definitions. Restore the ADLDS objects from the production system backup to the target server hosting the QM Database role under a different service name.

Restore databases

Regardless of the target system deployment level, restore from backup all databases except CommonDB to the target system.

Before restoring the databases from the production system backup to the target system, all connections to the databases must be closed.

Procedure

1 Verify that the connections to the databases are closed by running the following query:

```
Select spid,db_name(dbid) from sys.sysprocesses where spid > 50
```

2 Restore from backup all databases except CommonDB to the target system.

Related information

Restore databases (*Maintenance Guide*)

Restore Speech Analytics index

Restore Speech Analytics index from the backup of the production system to the target system.

Procedure

1 Delete all folders and files from **%IMPACT360SPEECHDATADIR%SpeechCatData**, except the following files:

- a2bow.properties
- a2bow.properties_example
- categories.xsd
- CRI_Enhanced.icd
- LMVersion.xml
- mode.icd

- SpeechCat.prop

2 Delete all files from **%IMPACT360SPEECHDATADIR%DataExports**.

3 Copy all files and folders from the **SpeechCatData** of the Speech data backup to **%IMPACT360SPEECHDATADIR%SpeechCatData**, except the following files:

- a2bow.properties
- a2bow.properties_example
- CRI_Enhanced.icd
- LMVersion.xml
- mode.icd
- SpeechCat.prop

4 Copy all files from the **DataExport** folder of the Speech data backup to **%IMPACT360SPEECHDATADIR%DataExports**.

5 If the **SpeechCatData**a folder contains the **config.prop** file, validate that the file does not contain any host names or ports that do not match the new environment.

Copy ADLDS objects

ADLDS (ADAM) contains objects such as users, groups, assignments and CD value definitions. Restore the ADLDS objects from the production system backup to the target server hosting the QM Database role under a different service name.

The result of restoring the ADLDS is that the target system contains two ADLDS services (directory and adldstemp), and two sets of data and logs folders. One set is the original target system ADLDS data and logs folders. The second set is the restored ADLDS data and logs folders.

Procedure

1 Attach system backup VHD, page 30

2 Create a temporary ADLDS service on the target system, page 30

3 Copy organization units from source ADLDS to the target directory, page 31

Attach system backup VHD

1 Open Windows Explorer.

2 Go to the shared folder where the VHD of the QM Database role is located.

3 To auto-attach the VHD file, double-click the file.

Create a temporary ADLDS service on the target system

1 Create a temporary ADLDS service using a batch file (for example: Answer.txt) as follows:

a. Copy the following sample to a text editor:

```
[ADLDSInstall]
InstallType=Unique
InstanceName=adldstemp
AddPermissionsToServiceAccount=Yes
DataFilesPath=<Enter the ADLDS path>\adldstemp\data
```

LocalLDAPPortToListenOn=50010

LocalSSLPortToListenOn=50011

LogFilesPath=<Enter the ADLDS path>\adldstemp\logs

NewApplicationPartitionToCreate="CN=Partition4,DC=cohovineyard"

ShowOrHideProgressGUI=Show

b. In the sample, modify the values of the following parameters:
   - **InstanceName**: leave the value adldstemp. This value is the instance name of the service that runs the ADLDS.
   - **LocalLDAPPortToListenOn**: leave this value, unless this port is already used by another instance. This port is used by the Interaction Migration Tool.
   - **LocalSSLPortToListenOn**: leave this value, unless this port is already used by another instance. This port is not used by the Interaction Migration Tool.
   - **DataFilesPath**: modify to the path of the data folder per your deployment.
   - **LogFilesPath**: modify to the path of the logs folder per your deployment.

c. Save the Answer.txt file in a designated location.

2 In the following command, replace the path specified after /answer: with the location of your Answer file, and run the command as administrator: %systemroot%\ADAM\adaminstall.exe /answer:E:\backup\answer.txt As a result, a service named **adldstemp** runs the ADLDS (the value specified for the InstanceName).

3 Stop the **adldstemp** service.

4 Copy the files contained in the **data** and **logs** folders from the source system backup to the **ADLDSTEMP\data** and **ADLDSTEMP\logs** folders respectively.

5 Replace the instance login user from the default to the Local System account.

6 Start the **adldstemp** service.

Copy organization units from source ADLDS to the target directory

1 On the server that hosts the QM Database role, whre the WFO Data Migration Tool from V15.1 is installed, open Command Prompt as administrator.

2 Change directory to **%IMPACT360SOFTWAREDIR%Migration V151 to V15.2\Upgrade Utils\Migrate Directory QM Objects** folder.

3 Run the **QmObjectMigration.exe**.

Set the parameters and values according to the deployment (the values to modify are indicated as bold):

QmObjectMigration.exe --SrcAdamAddress **target_server_name** --SrcAdamPort **port_set_in_answer-file** --SrcAdamUser **IMSA_domain\Install_user_name** --SrcAdamPassword **Install_user_password** --DstAdamAddress **target_server_name** --DstAdamPort **Directory service port** --DstAdamUser **IMSA_domain\IMSA_user** --DstAdamPassword **IMSA_password**

Example:

QmObjectMigration.exe --SrcAdamAddress **DC01** --SrcAdamPort **50010** --SrcAdamUser **domain\installuser** --SrcAdamPassword **Installuser password** --DstAdamAddress **DC02** --DstAdamPort **50000** --DstAdamUser **domain\IMSA user** --DstAdamPassword **IMSA password**

Reassign database permissions on the target systems

Reassigning the SQL Server permissions on the target system is required if the Management Service Account (MSA), Database Management Service Account (DMSA), or domain are different between the source and target systems.

A *Database Permissions Configuration Tool* is available to reassign database permissions on the target system for the following databases:

- Framework Database (BPMAINDB)
- Framework Data Warehouse (BPWAREHOUSEDB)
- QM Database (CentralApp)
- Contact Database (CentralContact
- Interaction Data Warehouse (CentralDWH)
- Framework Data Warehouse (ETLSTAGINGDB)
- Contact OLTP Database (LocalContact)
- DPA Database (PCMON)
- Speech Analytics Database (SpeechAnalytics)
- Speech Products Database (SpeechProducts)
- Common Database (CommonDB)

Report database permissions are not managed by the *Database Permissions Configuration Tool*. Manually modify the permissions on the SQL Server instance that hosts the report databases.

Procedure

1. Run the Database Permissions Configuration Tool locally, once per each SQL Server instance that hosts one of the databases in the table. Follow the procedure in the related information. (The tool is locate in: %Impact360SoftwareDir%CommonDB/Utils/Database Permissions Configuration Tool)
2. Manually modify the permissions on the SQL Server instance that hosts the report databases:
   a. Connect to the SQL Server that hosts the report databases.
   b. Open Microsoft SQL Server Management Studio and connect to the SQL Server instance.
   c. From Object Explorer, select **Security > Logins**.
   d. Right-click the MSA account and click **Properties**.
   e. Select **User Mapping**.
   f. In the Map column, select the **ReportServer** and **ReportServerTempDB** options.
   g. Click **OK**.

Related information

Assign DB permissions automatically (*SQL Server Installation and Upgrade Guide*)

Configure the Report Server database connection

Configure the Report Server database connection from the new server that hosts Reporting Services and has a new name. This updates the user account and password used for the database connection.

Procedure

1. Log on to the server that hosts the Reports server role with a user that has access to the databases.
2. Open the **Reporting Services Configuration Manager**, and connect to the new server hosting the report services.
3. On the **Report Server Status** page, click **Start** (to start the SQL Server Reporting Services).
4. On the left pane, select Database, then click **Change Database**.
5. Select **Choose an existing report server database** option, and click **Next**.
6. Select the SQL Server that hosts the report server database in the target system and click **Test Connection**. Then, click **Next**.
7. In Report Server Database, select the **ReportServer** database. Then, click **Next**.
8. In Credentials, specify the credentials that the report server connects to the report server database. Then, click Next.
9. Click **Next** and then **Finish**.

Restore SSRS encryption keys

The SSRS encryption keys of the source system are required in the target system.

Procedure

1. Open the **Reporting Services Configuration Manager**.
2. Select **Encryption Keys**.
3. Click **Restore** and then select the **rsdbkey.snk** file backed up from the source system.
4. Enter the **Password** used to lock the key when backing up the SSRS encryption keys.
5. Run this query to remove the source server name from the database on the target reporting server. This prevents a scale-out deployment error being raised.

```
USE ReportServer
Declare @servername sysname = 'source server name'
Delete from keys where MachineName = @servername
```

Where: @servername is the server name hosting Reporting Services role on the source system.

Import target Data Center configurations

The data restore from source backup replaces the target Data Center (DC) configuration. Import the target configuration from the XML file you have created by the Export DC Configuration feature.

Importing this XML file performs the following:

- Deletes from the Installations tree all existing servers that have active DC server roles.

- Adds to the Installations tree the target servers captured in the XML file, their server role configurations and associations, and their Installation tree parent nodes.

Before you begin

Verify that you have the XML file with target DC configuration (exported in an earlier procedure). This XML file must be in a directory that is accessible from the computer on which you perform this procedure.

Procedure

1. Set the data center servers to import migration mode as follows:
   a. Log on with the Installation Account to the target server with the Migration Mode Tool.
   b. Run **Windows PowerShell** as administrator.
   c. Change directory to the location of the Migration Mode Tool.
   d. To set the data center servers to import migration mode, run the following command:
   ```
   .\MigrationModeTool.ps1 -action import
   ```
   e. Verify that no error messages appear.
2. Sign in to the Enterprise portal as *superuser*.
3. From the Installations tree, select the **Enterprise** node.
4. Click **More Actions**, and select **Turn Advanced Mode On**.
5. Click **System Management > Enterprise > Data Center Migration - Internal Use Only**.
6. Click the **Import Data Center Configuration** icon .
7. Click **Choose File**. Browse to and select the XML file that contains the target DC configuration (exported in an earlier procedure).
8. Click **Import**.

   A confirmation message is displayed, stating that importing the file deletes all servers that have active Data Center Zone server roles from the Installations tree. The deleted servers are replaced with the data center servers specified in the imported XML file.
9. Click **Yes**.

   The import data center process starts. This process replaces all data center servers in the Installations tree with the data center servers specified in the XML file.

   When the **Status** column displays the **Completed** status for all Installations tree nodes, the import is successful.

   Do not restart the WFO service yet. Restart is required in a later stage. If the Status column displays Fails for an Installation tree node, troubleshoot the problem causing the failure, and then retry the data center import.
10. Once the DC configuration import completes successfully, restart the Application Server.

    If the Application Servers are clustered, stop the WFO_ProductionDomain_ProductionServer service on each Application Server in the cluster. Then, start the service one at a time.

The exported data also contains Data sources configuration. That is, the target system receives data from the production extensions. To prevent receiving data from the production extensions, remove the data sources manually from the target system after importing the DC configuration.

Related topics

Data Center import process troubleshooting, page 39

Update IMSA and DMSA

If the target system is in a different domain than the source system, update the MSA and DMSA accounts to the same accounts as configured in the target system.

Procedure

1. Sign in to the target portal.
2. Select **System Management > Enterprise > Enterprise Settings**.
3. Update the Management Service Account (MSA) and the Database Management Service Account (DMSA).

Copy FIS adaptors configuration

The FIS adaptors configuration is stored in the system backup. The system backup creates a separate Windows Backup (VHD) for each drive in the destination folder.

Copy the FIS adaptors configuration from the VHD file of the production system to the target system.

The location of the system backup VDH output is set at the enterprise level. When the location is used by multiple server roles, a new folder is created for each server.

Depending on the deployment level, the FIS adapters can be hosted in the one of the following platforms: Consolidated, Data Center, Database, Framework Database & Reporting, Framework Database, and Framework Integration Service.

Consolidating FIS adaptors from multiple servers to fewer servers is not supported. In this case, consolidate the FIS adaptors manually.

Separating FIS adaptors from fewer servers to multiple servers is not supported. In this case, separate the FIS adaptors manually.

Procedure

1. COPY the FIS adaptors configuration file from the system backup as follows:
   a. From the system backup VHD files of the production system backup, copy the **BPX-Server.XML** file, located in **%IMPACT360SOFTWAREDIR%IntegrationServer\FusionExchange**.
   b. Replace the existing **BPX-Server.XML** in the corresponding location on the target system servers.
2. Clear old FIS Servers entries from BPMAINDB as follows:
   a. Open SQL Server Management Studio and connect to the Framework Database (BPMAINDB).
   b. Execute the following query:

```
USE BPMAINDB
Declare @server sysname = 'source server name'
DELETE ISERVER where HOSTADDR = @server
```

   Where:

   @server represents any server entry in the ISERVER table, which contains the production server name.

Update PPFW settings

Update the Central Missions Manager (CMM) component of the Post-Processing Framework (PPFW) component with the new database server host name.

Perform this procedure on these servers:

- Consolidated servers
- Servers that host the QM Database

Procedure

1. Browse to the restored VHD file location.
2. Find this file:

   HKEY_LOCAL_MACHINE_SOFTWARE_Wow6432Node_Impact360_PPFWCenter.reg
3. Right-click the file and select Edit.
4. Search for the source QM Database server name.

   If the source server name exists in the reg file, then edit the file to replace the source server name with the target server name.

   Sometimes, the server name does not exist in the file. This depends on how the system is configured.
5. If changes were made to the file, double-click the edited file to import the registry changes.

Stop migration mode on target system

Once the data center migration is completed, the migration mode is not required. All services must be started to enable usual operation.

Procedure

1. Log on with the Installation Account to the server with the Migration Mode Tool.
2. Run **Windows PowerShell** as administrator.
3. Change directory to location of the Migration Mode Tool.
4. To verify that all data center servers are identified and online, run the following command:

   ```
   ./MigrationModeTool.ps1 -action test
   ```
5. To stop the migration mode of data center servers, run the following command:

   ```
   ./MigrationModeTool.ps1 -action stop
   ```
6. Verify that no error messages appear.

Related information

Migration Mode Tool (*WFO V15.1 to V15.2 (Side-by-Side with optional HW Reuse) Upgrade Guide*)

Unblock configuration distribution on target system

During the database restore, the SSRS reports are overridden. To deploy the SSRS reports on the target servers, unblock the configuration distribution to the target managed servers.

Procedure

1. Select **System Management > Enterprise > Settings**. Then, select the Enterprise (root) node.
2. Click **More Actions** and select **Unblock Configuration Distribution**.
3. Verify in the System Monitor that the configuration distribution completed successfully.
4. Verify that no configuration changes are pending to the managed servers, by ensuring that the Pending Messages icon is not displayed in Enterprise Manager.

Related information

Block and Unblock Configuration Distribution (*Enterprise Manager Configuration and Administration Guide*)

Update Customer Feedback ETL configuration

If Customer Feedback Survey Servers are deployed on the production system, update the Customer Feedback ETL configuration.

Procedure

1. Select **System Management > Customer Feedback > Settings**.
2. Update the **Customer Recording File Location**.
3. If the **Enable Survey Load and Purge** option is cleared on the production system, select this option to schedule the ETL to run.
4. Click **Save**.
5. Verify the ETL status from **System Management > Customer Feedback > ETLStatus**.
6. If the status displays errors related to ETL loading, restart the **I360 CF Tomcat** service on the server hosting Framework Data Warehouse role.

Distribute DPA configuration

Distribute the configuration to the DPA Applications.

Procedure

1. Sign in to the portal.
2. Select **System Management > Enterprise > Settings.**
3. Select **DPA Applications**, and click **Save**.

For a cluster deployment, the role is on the primary Application Server.

Distribute Speech Analytics configuration

Distribute the configuration to the Speech Analytics Application servers.

Procedure

1. Sign in to the portal.
2. Select **System Management > Enterprise > Settings.**
3. Select the **Speech Application Service**, and click **Save**.

   The Enterprise Manager distributes the configuration to the Speech Application Service, which in turn, overwrites the configuration files.

Uninstall the temporary AD LDS service

Uninstall the temporary AD LDS service created during ADAM restore.

Procedure

1. Open the **Windows Control Panel** and select **Uninstall a program**.
2. Select **AD LDS Instance verintadlds** and click **Uninstall**.
3. Detach the VHD file of the production system backup (attached earlier) as follows: Right-click the **HD** in **My Computer** and click **Eject**.

Check service restart alarms and perform SAT

Check service restart alarms and verify proper operation.

Procedure

1. Open the Alarm Dashboard.
2. Check for service restart alarms and follow the instruction to correct it.
3. Perform Site Acceptance Tests (SAT).

Related information

Site Acceptance Tests (SAT)

Data Center import process troubleshooting

When you import a data center, the **Failed** status can display for an Installations tree node on the Data Center Migration Status - Internal Use Only screen. Refer to the **Error Message** value for information that can help you troubleshoot an import process failure.

The most common reasons the system returns a **Failed** status for an imported Installations tree node are:

- Two nodes of different types have the same node name under the same parent node
- Two servers have the same host name
- Server or network issues

Two nodes of different types have the same node name under the same parent node

Two nodes of different types have the same node name and exist under the same parent node. The Installations tree does not allow this configuration. For example, assume that the Installations tree has a Site Group named “Human Resources” and a Site named “Rome Human Resources.” The import fails if you import a Server node with the logical name “Rome Human Resources” into the Site named “Rome Human Resources.” The import fails because the Site node and Server node have the same logical name and exist under the same Site Group (parent) node. In this scenario, you can rename the Site node to a different name and then retry the data center import.

This is the table style for Notes. The term “logical name” refers to the name of the server that is specified in the Name field of the System Management > Enterprise > Settings screen. The logical name is different from the host name.

Two servers have the same host name

Two servers have the same host name. The Installations tree does not allow this configuration.

You cannot import a Data Center Zone server that has the same host name as a Site Zone server that exists in the Installations tree. In this scenario, the import fails for the Data Center Zone server. Change the host name of the Data Center Zone server or Site Zone server and retry the import.

You can import a Data Center Zone server that has the same host name as a Data Center Zone server that exists in the Installations tree. In this scenario, the import process deletes the existing Data Center Zone server and then creates the imported Data Center Zone server.

Server or network issues

A server that the import attempts to replace is down, or network connectivity to the server is lost. Investigate and resolve the problem with the server, then retry the data center import.

Related topics

Retry a Data Center Import, page 40
Validate the Server Role configuration, page 40
Resolve Server Role Validation configuration problems, page 41
Update Instance IDs of Speech Analytics Application Servers, page 41

Retry a Data Center Import

When you import a data center using the **Import Data Center Configuration**feature, the system can return the **Failed** status for one or more Installations tree nodes. If the system returns the **Failed** status, troubleshoot the reason for the failure, and then retry the Data Center Import.

When you retry the data center import, the system performs the following:

- Examines the last data center configuration XML file that was imported.
- Determines if any Installations tree nodes exist in that XML file that have not yet been imported successfully into the Installations tree.
- Attempts to import into the Installations tree any nodes it finds in the XML file that have not yet been imported.

Before you begin

- You have received the **Failed** status for an Installations tree node when using the **Migration Import** feature to import a data center.
- You have performed troubleshooting and corrected the reason the Installations tree node failed to import.

Procedure

1. Select **System Management > Enterprise > Data Center Migration Status - Internal Use Only**.
2. Click the **Retry** icon .

If you receive the **Failed** status for an Installations tree node after retrying the data center import, you can troubleshoot the problem again and then retry the data center import again.

Validate the Server Role configuration

The Data Center server role configuration is validated against the last successfully imported data center configuration.

If the server role configuration has not been successfully imported, the server role configuration is validated against the production server role configuration.

When you validate the server role configuration, a Role Validation screen displays all critical configuration differences between the imported server role configuration settings and the exported server role configuration settings.

Troubleshoot and resolve each of these server role configuration differences to avoid serious problems on the migrated servers.

Before you begin

Verify that you have imported the data center configuration successfully and the Advanced mode is on.

Procedure

1. Click **System Management > Enterprise > Data Center Migration - Internal Use Only**.
2. Click the **Server Role Validation** icon .

3 On the Role Validation screen, each item listed represents a critical server role setting that is configured in a way that could adversely affect server performance.

Resolve each configuration problem listed on the screen.

Review the information appearing in the **Description** column on the screen to understand the particular configuration problem associated with each item.

4 Click **Close** after you have resolved all problems that caused each server role setting to display on the Role Validation screen.

Related topics

Resolve Server Role Validation configuration problems, page 41

Resolve Server Role Validation configuration problems

There are some common configuration problems that cause server role settings to display on the Role Validation screen when you validate the server role configuration. Resolve these configuration problems to ensure that the migrated server operates correctly.

The possible problem can be one of the following or both:

- A server role setting has a different New Value (imported value) than Old Value (exported value).
- The Contact OLTP Database server role has different retention values than the old values.

Procedure

1 If a server role setting has a different New Value than Old Value, for each imported server role setting listed on the Role Validation screen that has a different New Value than Old Value, manually change the current value (or New Value) back to the Old Value.

For example, go to the **System Management > Enterprise > Settings** screen for the server role, and manually change the setting to the Old Value.

2 If the Contact OLTP Database server role has different retention values than the old values, ignore the alarm and leave the new value.

Update Instance IDs of Speech Analytics Application Servers

Each Speech Application Server is assigned with an Instance ID as part of the Installation flow. When copying Speech Application Server data to another Speech Application Server, it is required to update the Instance ID in the target Speech Analytics Application Server to the same value as in the source Speech Analytics Application Server (production system).

The IFA-conf.xml located in %Impact360SoftwareDir%Conf\roles\IFA on each of the production Speech Analytics Application Server.

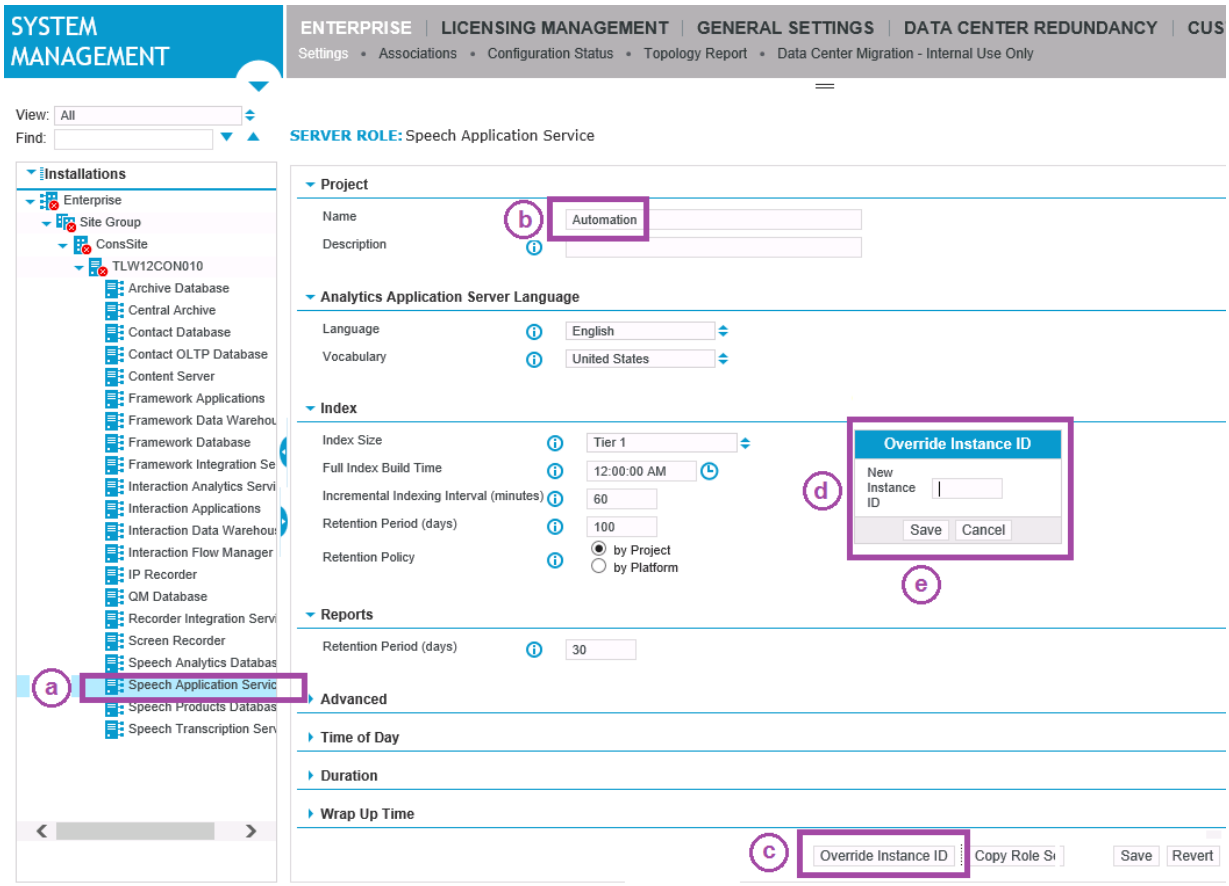
Procedure

1 Sign in to the portal as the system administrator.

2 In the Installations tree, select the **Enterprise** node.

3 Click **More Actions**, and select **Turn Advanced Mode On**.

4 From the installation tree, expand the Speech Analytics Application server and do the following:
   a. Select the **Speech Application Service**.
   b. Look for the **Name** of the Project.
   c. Click **Override Instance ID**.
   d. Set the Instance ID as per the source Speech Analytics Application servers mapping.
   e. Click **Save**.
5 Wait until configuration distribution is completed.
6 Verify Instance ID:
   a. For each Speech Analytics Application Server, go to %Impact360SpeechDataDir%SpeechCatData, and open the **SpeechCat.Prop** file with a text editor.
   b. Verify that the source Instance ID appears instead of the target Instance ID.



Data Center rollback

Data center rollback consists on retrieving the previous Data Center with the same configuration as it was before the replacement.

Workflow

1. Start migration mode in target system, page 43.
   Stop the target data center services to prevent configuration distribution to source site servers.
2. Stop migration mode in source system, page 44.
   All services must be started on the source system to enable usual operation.
3. Update the Enterprise Manager location to source system, page 44.
4. Change the Enterprise Manager Location settings back to the location of the source Application Server or Load Balancer.
5. Distribute configuration from source data center, page 44.
   Unblock the configuration distribution on source system and distribute configuration to all site servers.
6. Refresh cache and reset watermark in all site servers, page 45
   For hybrid systems with V15.1 recorders or earlier, refresh cache and reset watermark in all site servers.
7. Check service restart alarms, page 46.
   Check service restart alarms and verify proper operation.
8. Reconfigure all desktops to point to original Data Center.

Related information

Desktop Applications Deployment Reference and Installation Guide

Start migration mode in target system

Stop the target data center services to prevent configuration distribution to source site servers.

Procedure

1. Log on with the Installation Account to the target server installed with the Migration Mode Tool.
2. Run **Windows PowerShell** as administrator.
3. Change directory to location of the Migration Mode Tool.
4. To verify that all data center servers are identified and online, run the following command:
   `.\MigrationModeTool.ps1 -action test`
5. To start the migration mode of data center servers, run the following command:
   `.\MigrationModeTool.ps1 -action set`
6. Verify that no error messages appear.

Related information

Migration Mode Tool (*WFO V15.1 to V15.2 (Side-by-Side with optional HW Reuse) Upgrade Guide*)

Stop migration mode in source system

All services must be started on the source system to enable usual operation.

Procedure

1. Log on with the Installation Account to the source server with the Migration Mode Tool.
2. Run **Windows PowerShell** as administrator.
3. Change directory to location of the Migration Mode Tool.
4. To verify that all data center servers are identified and online, run the following command:
   ```
   .\MigrationModeTool.ps1 -action test
   ```
5. To stop the migration mode of data center servers, run the following command:
   ```
   .\MigrationModeTool.ps1 -action stop
   ```
6. Verify that no error messages appear.

Related information

Migration Mode Tool (*WFO V15.1 to V15.2 (Side-by-Side with optional HW Reuse) Upgrade Guide*)

Update the Enterprise Manager location to source system

Change the Enterprise Manager Location settings back to the location of the source Application Server or Load Balancer.

Procedure

1. Select **System Management > General Settings > Enterprise Manager Location**.
2. In the **EM Server Name** field, specify the host name, IP address, or fully-qualified domain name (FQDN) of the server that hosts the Framework Applications server role or the name of the Load Balancer.
3. Update the Port Number and SSL Port Number to the correct ports Weblogic is listening on in source Application Servers (default 7001 and 7002).
4. Click **Save**.
5. Click **Update Enterprise Manager Location**.
6. Click **Done**.

Distribute configuration from source data center

Unblock the configuration distribution on source system and distribute configuration to all site servers.

Procedure

1. In the Installations tree, select the **Enterprise** node.
2. Click **More Actions > Unblock Config Distribution**.
3. When prompted with “Do you want to proceed?”, click **OK**.
4. Click **Save** and wait for the distribution to complete.

5 Verify configuration has been distributed successfully and that there are no alarms indicating distribution errors.

Related topics

Troubleshoot configuration distribution failures, page 45

Troubleshoot configuration distribution failures

If the configuration distribution to all site servers fails, check the error and perform the relevant steps.

Procedure

1 If **Enterprise Manager** and **Enterprise Manager Agent authentication** errors appear, verify that he Enterprise Manager Location on the site servers is properly updated:
   a. On a source site server, browse to %Impact360SoftwareDir%Conf\applications\authconfig.xml.
   b. Verify that the **Primary-Server-Host** contains the source Application server or Load Balancer name.
   c. Verify that the **Secondary-Server-Host** contains the V15.2 Application server or Load Balancer name.
2 If a **sequence number already processed** error appears (due to sequence number sent by V15.1 DC is lower than the sequence number sent by V15.2 DC), do the following:
   a. Connect to the source Recorder and delete the **Cache-Manifest.xml** file from %IMPACT360SOFTWAREDIRE%Conf\cache\.
   b. Log on to source system as administrator.
   c. Navigate to **System Management > Enterprise > Settings**.
   d. Select the Enterprise node and click **More Actions > Turn Advanced Mode On**.
   e. Select the Recorder from installation tree, click **More Actions**, then click **Refresh Cache**.

Refresh cache and reset watermark in all site servers

For hybrid systems with V15.1 recorders or earlier, refresh cache and reset watermark in all site servers.

As part of the post data center migration procedures, migration mode is stopped and configuration distribution is unblocked. If configuration distribution from V15.2 data center has been already done, to override the configuration, perform full configuration distribution from the source data center to the source site servers.

In addition, all site servers for which the configuration distribution was unblocked could potentially mark calls into the V15.2 data center. To remark those calls into the source data center, log on to the Recorder Manager on each of the site servers and reset the consolidation watermark.

Procedure

1 Log on to source with administrator account
2 Select **System Management > Enterprise > Settings**.
3 Perform full configuration distribution:
   a. From the enterprise level, click **More Actions > Turn Advanced Mode On**.
   b. In the Installations pane, select a site server.

c. Click **More Actions**, then click **Refresh cache**.

4 Reset the consolidation watermark:

a. In the Installations pane, select a site server.

b. Click **Launch** to open the Recorder Manager application.

c. Select **General Setup > Database > Database Settings**.

d. Click the server for which the Contact Database Service appears in the **Type** column.

e. Click **Edit**.

f. Reset the Watermark setting to specify the date-time when the migration downtime started.

g. Click **Save**.

5 Repeat Step 3 and Step 4 for each site server that has received configuration distribution from the V15.2 data center.

Check service restart alarms

Check service restart alarms and verify proper operation.

Procedure

1 Open the Alarm Dashboard.

2 Check for service restart alarms and follow the instruction to correct it.

3 For each site recorder, launch the **Recorder Manager** directly and check for restart alarms.