How-To Library

High Availability Configuration for Data Archive and the Data Vault (Version 6.4)

© Copyright Informatica LLC 2016, 2019. Informatica Corporation. No part of this document may be reproduced or transmitted in any form, by any means (electronic, photocopying, recording or otherwise) without prior consent of Informatica Corporation. All other company and product names may be trade names or trademarks of their respective owners and/or copyrighted materials of such owners.

Abstract

This article presents an example of a system configuration for Data Archive and the Data Vault designed for high availability.

Supported Versions

- Data Archive 6.4.4

Table of Contents

Overview. 2
High Availability Configuration. 3
High Availability Configuration for the ILM Repository 4
High Availability Requirements. 4
Primary Server Installation and Configuration. 5
Set the Location of the Data Vault Repository File. 5
Set the Location of the Shared Run-Time Files. 6
Failover Server Installation and Configuration. 6
Data Vault Service Configuration. 7
Data Vault Service Agent Configuration. 8
Operation. 9
Load Management. 10
Failover Management. 11
Restoring Data Visualization Report Functionality. 12
Updating the JDBC URL or Password for Non-Healthcare Reports. 12
Updating the JDBC URL or Password for Healthcare Reports. 13
Troubleshooting. 15

Overview

You can design the Data Archive system configuration to minimize service interruption and ensure continuous availability of the Data Vault. When you configure high availability, the archive processes can continue to run despite temporary network, hardware, or service failures.

One approach to high availability for Data Archive is to set up a failover server for the ILM Engine and the Data Vault Service. Set up a server cluster with at least two nodes, a primary server and a failover server. The primary server runs in active mode and the failover server runs in passive mode. If the primary server fails, the failover server takes over the archive and query processes.

The primary server, in active mode, processes all archive and query requests for the Data Vault. The failover server, in passive mode, does not process archive requests. However, to improve efficiency, you can install a Data Vault Service agent on the failover server so that it can also process queries sent to the Data Vault.

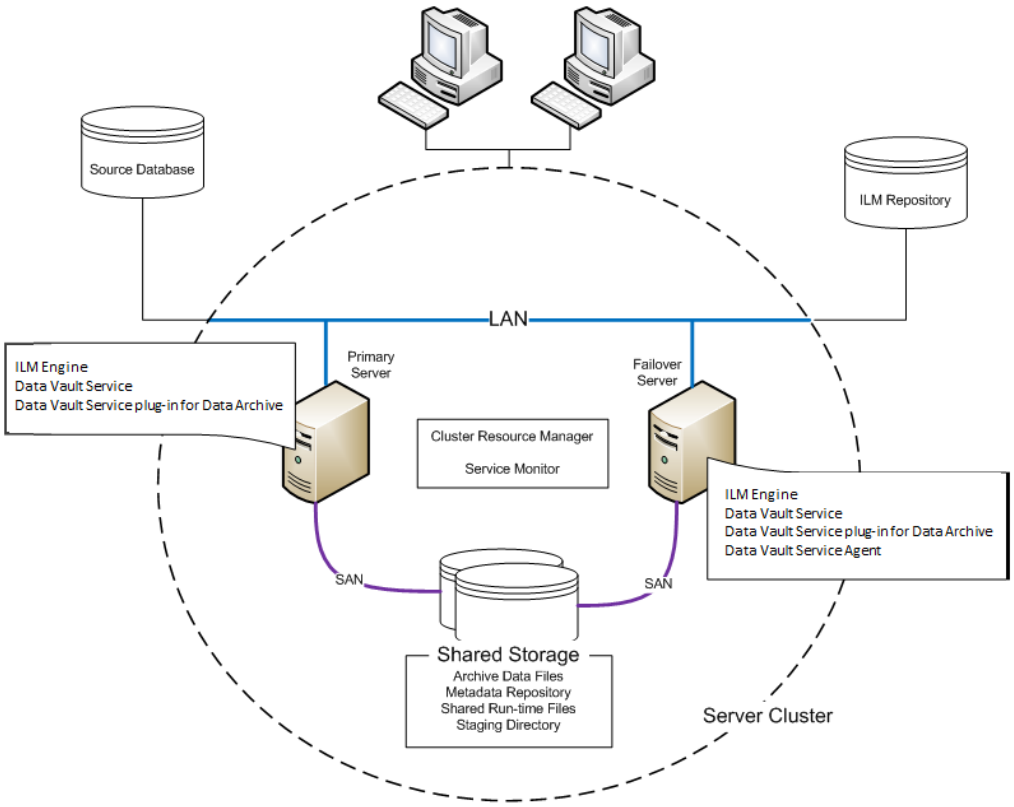
The primary and failover servers must have identical directory structures to make the switch from one server to another seamless. The primary and failover servers archive data to a network storage that must be accessible to both servers.

Install the Data Archive and Data Vault components on the primary and failover servers. After installation, configure the primary and failover servers to connect to the same directories for the Data Vault repository and the run-time files. Update the configuration files to use the same directories.

High Availability Configuration

A cluster resource manager (CRM) manages the servers and resources in a server cluster. A service monitoring software detects a node failure and reroutes the workload to another node.

The following diagram shows the configuration of a highly available Data Archive and Data Vault environment:



The server cluster includes the following components:

Cluster resource manager (CRM)

The CRM manages access to the servers and resources in the cluster. It also manages the changeover from one node to another.

Service monitor

The service monitor detects when the primary node is down and triggers the changeover to another node.

Primary server

The primary server is the logical server that performs all archiving processes and requests. It is always in active mode.

The primary server hosts the following Data Archive and Data Vault components:

- ILM Engine
- Data Vault Service

- Data Vault Service plug-in for Data Archive

Failover server

If the primary server fails, the failover server takes over the functions of the primary server and performs all archiving processes and requests. The failover server is in passive mode unless the primary server fails. When it is in passive mode, the failover server can process queries to the Data Vault.

The failover server hosts the following Data Archive and Data Vault components:

- ILM Engine
- Data Vault Service
- Data Vault Service plug-in for Data Archive
- Data Vault Service agent

The failover server hosts the same components as the primary server. It hosts an additional Data Vault Service agent to process queries.

The failover server must have the same directory structure as the primary server. For example, if the ILM Engine is installed in the `c:/ILM` directory in the primary server, then the ILM Engine must also be installed in the `c:/ILM` directory in the failover server.

Shared storage

The primary and failover servers connect to the same Data Vault directories. If the server cluster includes multiple storage devices, the primary server and the failover server must have access to a shared drive.

Create the following Data Archive and Data Vault directories:

- Directory for the Data Vault repository. For example: `<SANRootDirectory>/Meta/`
- Directory for the shared run-time files. For example: `<SANRootDirectory>/FAS_shared/`
- Directory for staging files. For example: `<SANRootDirectory>/Staging/`
- Directory for archive data files. For example: `<SANRootDirectory>/SCT/`

High Availability Configuration for the ILM Repository

The Data Vault Service does not specify high availability requirements for the ILM repository database. You configure high availability for the ILM repository on the database server. High availability configuration for the ILM repository database depends on the high availability features and capabilities of the database server.

High Availability Requirements

To enable the archive processes to work correctly and smoothly, the server cluster must have redundant hardware and software and must meet specific requirements.

Configure the server cluster so that it meets the following requirements:

- The server cluster must have a virtual IP address for the clients to connect to. This virtual IP address redirects to the primary node or to the failover node if the primary node is down.
- The primary node and failover node must have identical file systems and directory structures.
- The primary node and failover node must have access to the directories set up for the Data Vault in shared storage.

Primary Server Installation and Configuration

On the primary server, install Data Archive and Data Vault Service components and update the configuration files.

Install the following Data Archive and Data Vault Service components:

ILM Engine

Use the Data Archive installer to install the ILM Engine and create the ILM repository.

Data Vault Service Data Archive Plug-in

Use the Data Vault Service installer to install the plug-in for Data Archive.

Data Vault Service

Use the Data Vault Service installer to install the Data Vault Service. The Data Vault Service includes a Data Vault Service agent.

After installation, update the configuration files to connect to the directories in shared storage. Before you configure the primary server, verify that the ILM Engine and the Data Vault Service are shut down.

To configure the primary server, complete the following steps:

1. Set the location of the Data Vault repository file.
2. Set the location of the shared run-time files.

Set the Location of the Data Vault Repository File

Set the location of the Data Vault repository file in the `alias.conf` configuration file. Back up the `alias.conf` file before you modify it.

1. Use a text editor to open the `alias.conf` file located in the following directory: `\<Data Vault root directory>\firebird`
2. Find the line that starts with: `meta_fb=`

   The line contains the directory path and file name of the Data Vault repository file.

   For example: `meta_fb=C:\ILM-DV~4\firebird\meta_fb.fdb`

   In this example, the Data Vault repository file is: `meta_fb.fdb` and the file is located in the directory: `C:\ILM-DV~4\firebird\`
3. Copy the Data Vault repository file from the location indicated in the `meta_fb=` line to the shared storage.

   In the example, complete the following steps:

   a. Go to `C:\ILM-DV~4\firebird\`

   b. Copy the `meta_fb.fdb` file to the `<SANRootDirectory>\Meta` directory that you created in the shared storage device.
4. Update the `meta_fb=` line with the new location of the Data Vault repository file, `<SANRootDirectory>\Meta\`

   In the example, replace the old directory path `C:\ILM-DV~4\firebird\meta_fb.fdb` with the new directory path `<SANRootDirectory>\Meta\meta_fb.fdb`
5. Save the `alias.conf` file.
6. Use a text editor to open the `firebird.conf` file located in the `\<Data Vault root directory>\firebird` directory.
7. Add the following line to the end of the file: `RemoteFileOpenAbility=1`

Set the Location of the Shared Run-Time Files

Set the location of the shared run-time files in the `ssa.ini` configuration file. Back up the `ssa.ini` file before you modify it.

1. Use a text editor to open the `ssa.ini` file located in the root of the Data Vault Service directory.
2. Find the section labeled [QUERY].

   The SHAREDIR parameter in the QUERY section stores the location of the shared run-time files. The following text shows an example of the QUERY section in the `ssa.ini` file:

   ```
   [QUERY]
   THREADS=2
   MAXVMEM=4096
   MEMORY=512
   TEMPDIR=C:\Informatica\DataArchive\FAS\temp
   SHAREDIR=C:\Informatica\DataArchive\FAS\temp
   ```
3. Update the location of the shared run-time files in the SHAREDIR parameter.

   Set the value of the SHAREDIR parameter to the directory that you created in shared storage. For example, update the value of the SHAREDIR parameter with the `<SANRootDirectory>/FAS_Shared` directory you created in the shared storage area.
4. Save the `ssa.ini` file.

Failover Server Installation and Configuration

On the failover server, install Data Archive and Data Vault Service components and update the configuration files with the directories in the shared storage device. The configuration files in the failover server must point to the same directories as the primary server.

Install the following Data Archive and Data Vault Service components:

ILM Engine

Use the Data Archive installer to install the ILM Engine and create the ILM repository.

Data Vault Service Data Archive Plug-in

Use the Data Vault Service installer to install the plug-in for Data Archive.

Data Vault Service

Use the Data Vault Service installer to install the Data Vault Service. The Data Vault Service includes a Data Vault Service agent.

Data Vault Service Agent

Use the Data Vault Service installer to install the Data Vault Service agent.

After installation, you must configure the Data Vault Service and the Data Vault Service agent on the failover server. Configure the Data Vault Service component in the failover server to match the primary server. Then configure the Data Vault Service agent to match the Data Vault Service.

Before you configure the primary server, verify that the ILM Engine, Data Vault Service, and Data Vault Service agent are shut down.

Data Vault Service Configuration

Update the configuration files for the Data Vault Service before you update the configuration files for the Data Vault Service agent.

On the failover server, complete the following steps to configure the Data Vault Service:

1. Set the location of the Data Vault repository file.
2. Set the location of the shared run-time files.

Set the Location of the Data Vault Repository File

Set the location of the Data Vault repository file in the `alias.conf` configuration file. Back up the `alias.conf` file before you modify it.

1. Use a text editor to open the `alias.conf` file located in the following directory: `\<Data Vault root directory>\firebird`
2. Find the line that starts with: `meta_fb=`

   The line contains the directory path and file name of the Data Vault repository file.

   For example: `meta_fb=C:\ILM-DV~4\firebird\meta_fb.fdb`

   In this example, the Data Vault repository file is: `meta_fb.fdb` and the file is located in the directory: `C:\ILM-DV~4\firebird\`
3. Copy the Data Vault repository file from the location indicated in the `meta_fb=` line to the shared storage.

   In the example, complete the following steps:

   a. Go to `C:\ILM-DV~4\firebird\`

   b. Copy the `meta_fb.fdb` file to the `<SANRootDirectory>\Meta` directory that you created in the shared storage device.
4. Update the `meta_fb=` line with the new location of the Data Vault repository file, `<SANRootDirectory>\Meta\`

   In the example, replace the old directory path `C:\ILM-DV~4\firebird\meta_fb.fdb` with the new directory path `<SANRootDirectory>\Meta\meta_fb.fdb`
5. Save the `alias.conf` file.
6. Use a text editor to open the `firebird.conf` file located in the `\<Data Vault root directory>\firebird` directory.
7. Add the following line to the end of the file: `RemoteFileOpenAbility=1`

Set the Location of the Shared Run-Time Files

Set the location of the shared run-time files in the `ssa.ini` configuration file. Back up the `ssa.ini` file before you modify it.

1. Use a text editor to open the `ssa.ini` file located in the root of the Data Vault Service directory.
2. Find the section labeled [QUERY].

   The SHAREDIR parameter in the QUERY section stores the location of the shared run-time files. The following text shows an example of the QUERY section in the `ssa.ini` file:

```
[QUERY]
THREADS=2
MAXVMEM=4096
MEMORY=512
TEMPDIR=C:\Informatica\DataArchive\FAS\temp
SHAREDIR=C:\Informatica\DataArchive\FAS\temp
```

3. Update the location of the shared run-time files in the SHAREDIR parameter.

   Set the value of the SHAREDIR parameter to the directory that you created in shared storage. For example, update the value of the SHAREDIR parameter with the `<SANRootDirectory>/FAS_Shared` directory you created in the shared storage area.

4. Save the `ssa.ini` file.

Data Vault Service Agent Configuration

After you update the configuration files for the Data Vault Service, update the `ssa.ini` configuration file for the Data Vault Service agent.

You must update the QUERY, SERVER, and STARTER sections of the `ssa.ini` file. Before you start the configuration, verify that the Data Vault Service agent is shut down. Back up the `ssa.ini` file before you modify it.

1. Use a text editor to open the `ssa.ini` file located in the root of the Data Vault Service agent directory.
2. Find the section labeled [QUERY].

   The SHAREDIR parameter in the QUERY section stores the location of the shared run-time files.
   The following text shows an example of the QUERY section in the `ssa.ini` file:

   ```
   [QUERY]
   THREADS=2
   MAXVMEM=4096
   MEMORY=512
   TEMPDIR=C:\Informatica\DataArchive\FAS\temp
   SHAREDIR=C:\Informatica\DataArchive\FAS\temp
   ```

3. Update the location of the shared run-time files in the SHAREDIR parameter.

   Set the value of the SHAREDIR parameter to the directory that you created in shared storage. For example, update the value of the SHAREDIR parameter with the `<SANRootDirectory>/FAS_Shared` directory you created in the shared storage area.

4. Find the section labeled [SERVER].

   The HOST parameter in the SERVER section stores the host name of the server that hosts the Data Vault Service. The EXEPORT parameter stores the administration port for the Data Vault Service.
   The following text shows an example of the SERVER section in the `ssa.ini` file

   ```
   [SERVER]
   THREADS=10
   HOST=calvin
   EXEPORT=8600
   PORT=8500
   ROWSETBUFFER=64
   TEMPDIR=C:\Informatica\DataArchive\FAS\temp
   LOGDIR=C:\Informatica\DataArchive\FAS\fas_logs
   ```

5. Update the HOST parameter with the host name of the primary server.
6. Update the port number in the EXEPORT parameter with the administration port number set in the primary server.

   The default administration port is 8600.

7. Find the section labeled [STARTER].

   The AGENT_COUNT parameter stores the number of agent processes to run for query processing on the failover server.
   The following text shows an example of the SERVER section in the `ssa.ini` file

   ```
   [STARTER]
   AGENT_CONTROL=1
   AGENT_COUNT=2
   ```

```
VERBOSE=2
SERVER_CONTROL=1
AGENT_CMD=ssaagent
SERVER_CMD=ssaserver
LOGDIR=C:\Informatica\DataArchive\FAS\fas_logs
```

8. Update the AGENT_COUNT parameter with the number of agent processes you want to start for processing queries.

   The default number of agents is 2. If you want to start more agents in the failover server to process queries, set the AGENT_COUNT parameter to a higher number. Or you can set the number of agents based on the number of CPUs in the server.

9. Save the `ssa.ini` file.

Operation

Informatica ships script files to start and stop the Data Archive and Data Vault Service components. Use the script files to start the components in the primary and failover servers.

You can use the same scripts to start and stop components in the primary and failover servers. Run the scripts from the root directory of the component that you want to start or stop.

Note: If you cannot find the script files in the Data Vault Service directory, contact Informatica Global Customer Support to get the scripts.

Primary Server

The following table describes the scripts that you can use to start and stop the components on the primary server:

Component	Shell Script	Description
ILM Engine	startApplimation.sh	Starts the ILM Engine. Run the script from the root of the Data Archive directory.
	stopApplimation.sh	Stops the ILM Engine. Run the script from the root of the Data Archive directory.
Data Vault Service	fasd.sh start	Starts the Data Vault Service. Run the script from the root of the Data Vault Service directory.
	fasd.sh stop	Stops the Data Vault Service. Run the script from the root of the Data Vault Service directory.

Failover Server

The following table describes the scripts that you can use to start and stop the components on the failover server:

Component	Shell Script	Description
ILM Engine	startApplimation.sh	Starts the ILM Engine. Run the script from the root of the Data Archive directory.
	stopApplimation.sh	Stops the ILM Engine. Run the script from the root of the Data Archive directory.

Component	Shell Script	Description
Data Vault Service	fasd.sh start	Starts the Data Vault Service. Run the script from the root of the Data Vault Service directory.
	fasd.sh stop	Stops the Data Vault Service. Run the script from the root of the Data Vault Service directory.
Data Vault Service agent	fasd.sh start	Starts the Data Vault Service agent. Run the script from the root of the Data Vault Service agent directory.
	fasd.sh stop	Stops the Data Vault Service agent. Run the script from the root of the Data Vault Service agent directory.

Load Management

If you install a Data Vault Service agent on the failover server to improve query processing, you can set the priority for the Data Vault Service agents in the primary and failover servers to balance the processing load.

Set the priority level of an agent to make the most efficient use of the nodes in the cluster server. For example, you might set the agents that are hosted on a more powerful machine to a higher priority so that they perform most of the processing.

You can use the Data Vault Service Administrator tool or the command line program to set the agent priority level. To set the priority level on the command line, run the following Data Vault Service administration command:

```
Priority <host-name> <agent-ID> <priority-level>
```

To set the priority level of multiple agents in the primary and failover servers, you can create a script to run the priority command for each agent. For example, you can run the following script:

```
echo 'agents' |   ssaadmin DBA |  awk '($4 == "READY")
     { TAB[$1] += 1; print "priority " $1 " " $2 " " 100 - TAB[$1] }'
             | ssaadmin DBA
```

This script sets the priority for each agent that runs on the server cluster and displays the list of agents and priorities.

Guidelines for Setting the Agent Priority Level

Set the priority level of Data Vault agents based on how you want to distribute the processing load.

Use the following guidelines when you set the priority level of an agent:

- You can set the priority level to a number between zero and two million. A high number indicates a high priority.
- If you set the agent priority level to 0 or 1, the Data Vault Service assigns the following status to the agent:
  - Priority level 0. Indicates that the agent is not available to process any task. The Data Vault Service does not assign a task to an agent with a priority level of 0. To make the agent available to process tasks, change the priority level to a value higher than 0.
  - Priority level 1. Indicates that the agent primarily processes high-priority tasks such as registering data files or other administration tasks. The Data Vault Service can assign query tasks to an agent with priority level 1 if the agent is not busy and the Data Vault Service receives a high volume of queries.
- The Data Vault Service assigns tasks based on the availability and priority level of an agent. For example, the agent on one node has a priority level of 100 and the agent on a second node has a priority level of 90. The Data Vault Service assigns a task to the agent on the first node because it has the highest priority level. If the

Data Vault Service receives another query and the agent on the first node is still busy with the first task, the Data Vault Service assigns the next task to the agent on the second node. However, if the agent on the first node has completed the first task and is available, then the Data Vault Service assigns the task to the agent on the first node.

- The Data Vault Service uses an algorithm to ensure that agents process the most number of queries possible. For example, two agents are available to process queries and the Data Vault Service receives one query that generates ten long-running tasks and a second query that generates four tasks. The Data Vault Service does not wait until all tasks for the first query are completed before it assigns the tasks of the second query to an agent. It balances the task assignment between the two agents so that agents process the two queries in parallel.

Failover Management

In this high availability configuration, the primary server performs all archive and query processes and the failover server performs only query processes. When the primary server is down, the failover server takes over all archive and query processes.

The CRM distributes query processing between the primary server in active mode and the failover server in passive mode. If the service monitor detects that the primary server has stopped responding and cannot reestablish a connection, the CRM switches the failover server from passive to active mode.

The CRM performs the following actions:

1. Stops the Data Vault Service agents on the failover server.
2. Starts the ILM Engine on the failover server.
3. Starts the Data Vault Service on the failover server.
4. Redirects incoming HTTP requests to the IP address of the failover server.

The failover server performs all archive and query processes until the primary server is restored.

Restoring Primary Server Operation

Before you can switch processing back to the primary server, you must shut down the ILM Engine in the failover server.

When the primary server is restored, you must perform the following actions to switch processing back to the primary server:

On the failover server:

1. Stop the ILM Engine.
2. Stop the Data Vault Service.
3. Start the Data Vault Service agents.
4. Redirect incoming HTTP requests to the IP address of the primary server.

On the primary server:

1. Start the ILM Engine.
2. Start the Data Vault Service.

The service monitor can perform all start and stop operations using shell scripts.

Guidelines for Server Operation

Use the following guidelines when you start or stop the Data Vault Service components:

- Only one Data Vault Service can be running in the server cluster at any time. The Data Vault Service on the primary server and the Data Vault Service on the failover server cannot be running at the same time. If a Data Vault Service is running, you must shut it down before you start another Data Vault Service.
- On the failover server, you cannot run the Data Vault Service and the Data Vault Service agent at the same time. You must stop the Data Vault Service before you start the Data Vault Service agent. If the Data Vault Service agent is running, you must shut down the agent before you start the Data Vault Service.

Restoring Data Visualization Report Functionality

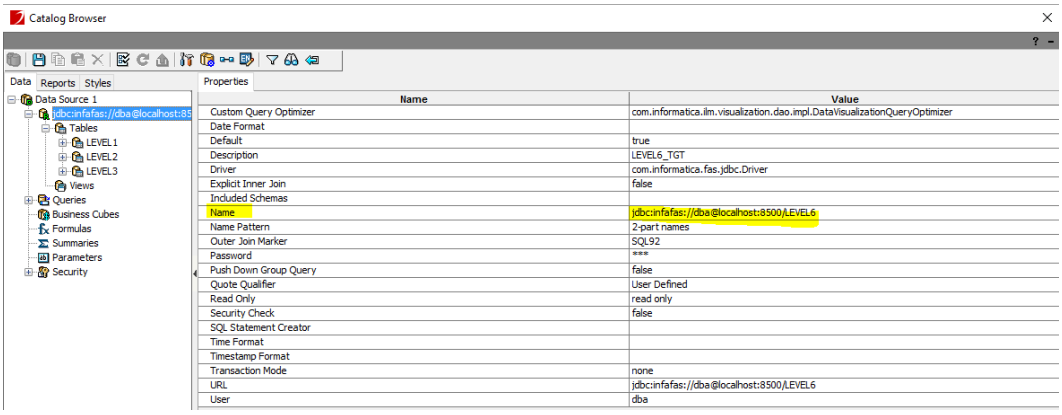
If the primary Data Vault server fails, and the failover server takes over, existing Data Visualization reports in Data Archive may stop working. This happens because the JDBC URL in the report catalog points to the failed primary server. Existing Data Visualization reports may also stop working if the Data Vault user password expires.

In either case you can restore the functionality of existing reports without having to update the JDBC URL or the Data Vault user password in every report catalog and republish them. Instead, you can configure an XML file to specify an updated JDBC URL or Data Vault password.

Updating the JDBC URL or Password for Non-Healthcare Reports

To restore the functionality of existing Data Visualization reports that are not generated through the Application Retirement for Heathcare Accelerator, complete the following steps:

1. Download the catalog from the instance of JReport Designer connected to the Data Archive server.
2. In JReport Designer, open the downloaded catalog and find the catalog name from the catalog browser.



3. Stop the Data Archive server.
4. From the Data Archive server location, open the following file: `webapp\visualization\reporthome\bin\datasource.xml`.
5. Add the following syntax to the file and update the property values per the catalog connection properties:

```
<datasource>
    <catalog-connection-name> </catalog-connection-name>
    <driver> </driver>
    <user> </user>
    <password> </password>
```

```
    <connection-type> </connection-type>
    <url> </url>
<datasource>
```

Property	Description
catalog-connection-name	Tag value must match the name present in the catalog browser.
driver	"com.informatica.fas.jdbc.Driver" is always the driver tag value.
user	Give the Data Vault user name in plain text. During server start-up the user and password tags are replaced with the tag "<encrypt-sign>" which contains the encrypted value of the user name and password.
password	Give the Data Vault password in plain text. During server start-up the user and password tags are replaced with the tag "<encrypt-sign>" which contains the encrypted value of the user name and password.
connection-type	"JDBC" is always the connection-type tag value.
url	The updated JDBC URL that you want to use.

The following image shows an example of the configuration file before server startup:

```
<datasource>
    <catalog-connection-name>jdbc:infafas://dba@localhost:8500/LEVEL6</catalog-connection-name>
    <driver>com.informatica.fas.jdbc.Driver</driver>
    <user>dba</user>
    <password>dba</password>
    <connection-type>jdbc</connection-type>
    <url>jdbc:infafas://dba@localhost:8500/LEVEL61</url>
</datasource>
```

The following image shows an example of the configuration file after server startup:

```
<datasource>
    <catalog-connection-name>jdbc:infafas://dba@localhost:8500/LEVEL6</catalog-connection-name>
    <driver>com.informatica.fas.jdbc.Driver</driver>
    <encrypt-sign>JGX7qfMro9f/AAaxicD13J3c7myNwsgUCwgDRecmuc/TguDI</encrypt-sign>
    <connection-type>jdbc</connection-type>
    <url>jdbc:infafas://dba@localhost:8500/LEVEL61</url>
</datasource>
```

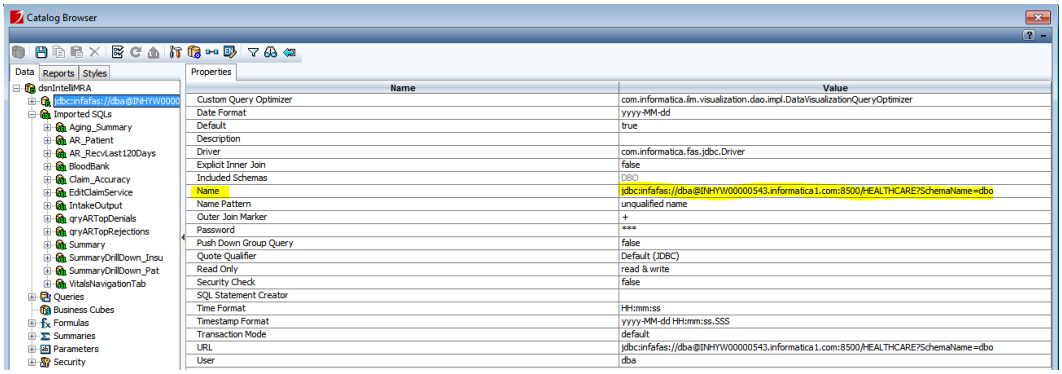
6. Repeat the previous step for all report catalogs present in the environment.
7. Start the server and verify that you can run the reports.

Updating the JDBC URL or Password for Healthcare Reports

To restore the functionality of existing Data Visualization reports that are generated through the Application Retirement for Heathcare Accelerator, for example Patient Information reports, complete the following steps:

1. Download the catalog from the instance of JReport Designer connected to the Data Archive server.

2. In JReport Designer, open the downloaded catalog and find the catalog name from the catalog browser.



3. Stop the Data Archive server.
4. From the Data Archive server location, open the following file: `webapp\visualization\reporthome\bin\datasource.xml`.
5. Add the following syntax to the file and update the property values per the catalog connection properties:

```
<datasource>
    <catalog-connection-name> </catalog-connection-name>
    <driver> </driver>
    <user> </user>
    <password> </password>
    <connection-type> </connection-type>
    <url> </url>
<datasource>
```

Property	Description
catalog-connection-name	Tag value must match the name present in the catalog browser.
driver	"com.informatica.fas.jdbc.Driver" is always the driver tag value.
user	Give the Data Vault user name in plain text. During server start-up the user and password tags are replaced with the tag "<encrypt-sign>" which contains the encrypted value of the user name and password.
password	Give the Data Vault password in plain text. During server start-up the user and password tags are replaced with the tag "<encrypt-sign>" which contains the encrypted value of the user name and password.
connection-type	"JDBC" is always the connection-type tag value.
url	The updated JDBC URL that you want to use.

The following image shows an example of the configuration file before server startup:

```
<datasource>
    <catalog-connection-name>jdbc:infafas://dba@INHYW00000543.informatica1.com:8500/HEALTHCARE?SchemaName=dbo</catalog-connection-name>
    <driver>com.informatica.fas.jdbc.Driver</driver>
    <user>dba</dba>
    <password>dba</password>
    <connection-type>jdbc</connection-type>
    <url>jdbc:infafas://dba@INHYW00000543.informatica.com:8500/HEALTHCARE?SchemaName=dbo</url>
</datasource>
```

The following image shows an example of the configuration file after server startup:

```
<datasource>
    <catalog-connection-name>jdbc:infafas://dba@INHYW00000543.informatica1.com:8500/HEALTHCARE?SchemaName=dbo</catalog-connection-name>
    <driver>com.informatica.fas.jdbc.Driver</driver>
    <encrypt-sign>4mSFqDsrA9YQMgaxkcG93N3cLkFMesLEIAOTRzPUZRkQ</encrypt-sign>
    <connection-type>jdbc</connection-type>
    <url>jdbc:infafas://dba@INHYW00000543.informatica.com:8500/HEALTHCARE?SchemaName=dbo</url>
</datasource>
```

6. Repeat the previous step for all report catalogs present in the environment.
7. Start the server and verify that you can run the reports.

Troubleshooting

If you encounter problems with the high availability system configuration, contact Informatica Global Customer Support.

If you encounter problems with setup, startup, or archive processing, provide the following log files from the primary and failover nodes:

Primary Node

<DataArchiveRootDirectory>/ILM/logs/applimation.log

<DataVaultServiceRootDirectory>/ILM-FAS/fas_logs/ssa*.log

Failover Node

<DataArchiveRootDirectory>/ILM/logs/applimation.log

<DataVaultServiceRootDirectory>/ILM-FAS/fas_logs/ssa*.log

If you encounter problems with query processing, provide the following log files from the primary and failover nodes:

Primary Node

<DataVaultServiceRootDirectory>/ILM-FAS/fas_logs/ssa*.log

<DataVaultServiceRootDirectory>/ILM-FAS/fas_agent_logs/agent*.log

Failover Node

<DataVaultServiceAgentRootDirectory>/ILM-FAS-AGENT/fas_agent_logs/agent*.log

Author